ICT AUTHORITY

Outcomes of the Consultation held on the Transition from IPv4 to IPv6 in Mauritius and the Recommendations thereon

July 2011

Table of Contents

1. Executive Summary

The Internet is in transition. All the IPv4 addresses have already been allocated by IANA to the Regional Internet Registries; the Internet is in the progress of migrating to the new IPv6 address space.

The exhaustion of IPv4 addresses and the transition to IPv6 could result in significant, but not insurmountable, problems for Internet services. In the short term, to allow the network to continue to grow, engineers have developed a series of kludges. These kludges include more efficient use of the IPv4 address resource, conservation, and the sharing of IPv4 addresses through the use of Network Address Translation (NAT). While these provide partial mitigation for IPv4 exhaustion they are not a long-term solution, they increase network costs, and merely postpone some of the consequences of address exhaustion without solving the underlying problem.

The short term solutions are nevertheless necessary because there is not enough time to completely migrate the entire public Internet to "native IPv6" where end users can communicate entirely via IPv6. Network protocol transitions require significant work and investment, and with the exhaustion of IPv4 addresses looming, there is insufficient time to complete the full IPv6 transition.

But the short-term solutions become problematic in the long run. The "solution to the solution" as it is called, is to complete the transition to a native IPv6 network. A native IPv6 network will restore end-to-end connectivity with a vastly expanded address space, improve network performance, and should decrease costs. Completing the transition of the public Internet to IPv6 will take time.

The World IPv6 Day came and passed on June the 8th 2011. According to the Internet Society (ISOC), the event organiser, more than 1,000 Internet service providers and websites, including Akamai, Facebook, Google, Limelight, Microsoft, and Yahoo!, attempted for 24 hours to see if they are ready for IPv6, and what problems might appear when IPv6 is enabled for many of their websites. The test demonstrated that “major websites around the world are well-positioned for the move to a global IPv6-enabled Internet, enabling its continued exponential growth”

To crystalise Government's efforts in sustaining the effective operation of the Internet in Mauritius, the ICT Authority issued a consultation paper on "Issues pertaining to Transition from IPv4 to IPv6 in Mauritius" in March 2011 highlighting the need for migration to IPv6.

Concurrently, the Authority carried out a technical survey with all local ISPs to assess their state of readiness to offer IPv6 services to the public in Mauritius. Out of the 11 ISPs surveyed, 8 replies were received. Out of these 8 ISPs, only 4 ISPs offer Internet services to the general public, 3 offer services to businesses only and 1 ISP does not have a subscriber base. For ISPs which offer Wimax, IPSHDSL and fibre based Internet services, these services are already IPv6 compatible. Out of the 3G mobile based Internet services available for 2 ISPs, only one of these services is IPv6 compatible. However, ADSL based Internet services which are offered by ISPs are not IPv6 compatible. Moreover, only 2 ISPs include support for DNS AAAA queries over IPv6 and for reverse DNS for IPv6 addresses.

The Authority has also come out with recommendations, which are based on the written responses received. It has been concluded that migration to IPv6 should not be mandated but facilitated by the Government.

The major recommendations are as follows:-

1. **Setting up of a National IPv6 Task Force**

   The IPv4-to-IPv6 transition is encountering multiple challenges. These challenges impact on public policy considerations in different ways. These issues require effective monitoring in order to positively influence the course of the transition. In order to chart out an effective way forward, there is a need to set up a **National IPv6 Task Force** in order to look into key IPv6 issues.

2. **Leadership role of Government for IPv6 migration**

   a. It is proposed that Government sets the example to the operational deployment and use of IPv6 through the designation of an IPv6 Transition Public Agency with a time lined Action Plan.

   b. Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2013;

c. Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2015.

d. Usage of IPv6 in the platforms/applications pertaining to e-governance could be mandated. The Government could also mandate IPv6 compatibility in its own procurement of IT systems and networks;

e. Hold workshops and seminars, to bring awareness about IPv6 among service providers and end-users community to be conducted through governmental agencies.

3. Regulatory issues related to transition from IPv4 to IPv6.

a. Issuance of appropriate directives to monitor the assignment of IP addresses from local ISPs to Mauritian end users as and when required.

b. Amendment to the definition of IP address mentioned in ISP licence to enable 128 bits to be used as needed for IPv6 based addressing.

c. The Authority, in consultation with the National IPv6 Task Force will also look into the possibility of ensuring that all imported communication network and customer premises equipment is either IPv6 compatible or that the vendor can prove that there is a clear upgrade roadmap to support IPv6.

d. Investigate in the possibility to make disbursement from the Universal Service Fund (USF) for the deployment of experimentation programme with IPv6. It is, therefore, suggested that this proposal be examined at the level of the National IPv6 Task Force and eventually be referred to the USF Ministerial Committee for its consideration.

4. The deployment strategy for Mauritius

The NO-NAT proposed by AfriNIC so as to benefit from the available AfriNIC IPv4 address pool as an instrumental measure in a clean implementation of an IPv6 supported Infrastructure is a proposal which requires further investigation. This topic will be discussed in depth at the level of the National IPv6 Task force to assess the policy, legal and practical implications therein.

2. Public Consultation Paper on Issues Pertaining to Transition from IPv4 to IPv6 in Mauritius

Analysis of Stakeholders' comments and ICTA's observations and recommendations

Comments from stakeholders have been compiled in section 5 (page 26) of this report. The questions set out in the Consultation Paper as well as ICTA's observations and recommendations have been listed below:-

1) Should the regulator play a regulatory role in the transition from IPv4 toIPv6 for the country or do you think the industry has the capability handle it on its own?

The regulatory approach favoured by the ICTA for Internet regulation focuses on the development of a competitive and dynamic environment in a light-handed manner, by ensuring to the extent possible the minimum necessary barriers to development and deployment of Internet services. The ISPs have opined that the adoption of IPv6 should be left to the industry as a technology option and the regulator should not mandate this as per current practice internationally. It is therefore proposed that the regulator in Mauritius aligns itself with the international trends and adopt a technology-neutral, light-handed approach rather than mandating the use of any particular technology for service providers.

To facilitate the transition to IPv6 in the future, it is also necessary that public agencies are involved in awareness and education programmes about IPv6. Moreover, it is felt that in terms of the facilitation and awareness, the different stakeholders involved should have an important role to play also in terms disseminating the relevant information to the different target groups. Issues to be dealt with for the service /content providers group will be different from issues to be discussed in the consumer group. It is the considered view that, in terms of the foregoing discussions, an IPv6 sensitisation campaign involving the different stakeholders within the Mauritian context will need to be carefully constituted to ensure optimised results.

For example, based on the results of the survey carried out with the ISPs, it is found that there is no consumer demand for IPv6. Public Internet services are generally reachable today via IPv4, so there is no perceived need by consumers to run IPv6. Moreover, consumers have “Customer Premises Equipment” (CPE) that may only be IPv4 enabled. If the Internet service provider migrates to IPv6, the service provider risks upsetting consumers whose equipment may no longer work properly and therefore consumers need to be aware of this risk.

On the other hand, according to results of the same survey carried out with ISPs, the implementation of the transition solution does not seem to be the priority of any of the local ISPs presently. One potential reason for this situation is that without a clear return-on-investment to the ISP, other than being able to offer IPv6 connectivity, making the investment may appear to be problematic. In fact, ISPs will have to bear an additional cost as the result of the transition without an improvement of service to customers, the moreso that the transition method may potentially deteriorate initial end-to-end connectivity and quality-of-service. ISPs who deploy transition solutions might then incur increased costs while offering inferior service.

The cost of transitioning to IPv6 could also be problematic. Costs involved in the IPv6 transition include renumbering networks, running two separate networks (IPv4 and IPv6) simultaneously, upgrading relevant software and hardware, training staff, and testing implementations. The cost of IPv6 will involve capital investment and ongoing operational costs that will have to be diverted from other business goals. Some networks operators may be reluctant to spending financial resources to make the transition until absolutely required. Conversely, early IPv6 movers in other countries who were able to incorporate IPv6 into the regular lifecycle of their networks, indicate that they were able to migrate their networks to IPv6 with little additional money set aside for the IPv6 transition, suggesting that, with planning, anticipated expenses could be mitigated.

The above examples give an indication of the different types of awareness campaign to be undertaken for the different targeted groups.

Recommendations

1. ***In order, to facilitate the transition to IPv6 for future, it is necessary that Government provides an initial form of catalyst by creating awareness and***

providing education about IPv6. Workshops and seminars, to bring awareness about IPv6 among service providers and end-users community could be conducted through governmental agencies.

2. ***In the short term, private sector organisations should be sensitised to undertake a careful analysis of their business cases for IPv6 adoption and plan for the forthcoming emergence of IPv6 traffic on both internal and external networks. Today, everyone should be impressed upon that this is an urgent issue which can be successfully handled only with good planning. Companies should be encouraged to share best practices on IPv6 uptake for all businesses to benefit, particularly for small- and medium-sized enterprises. Even if businesses do not have immediate plans to implement IPv6, preparing for the unavoidable transition now as opposed to later will only decrease the burden on IT administrators. This process doesn't have to be daunting if a thoughtful approach is taken. Plans should accommodate an implementation spanning a maximum of three to four years. When IPv6 gains momentum, migration to the new protocol will be swift, and those who haven't planned ahead risk finding themselves at a disadvantage.***

2) **If yes, what regulatory steps and policy initiatives, you believe are required?**

The IPv4-to-IPv6 transition is encountering multiple challenges. These challenges impact public policy considerations in different ways. These issues require effective monitoring in order to positively influence the course of the transition.

Recommendations

1. ***In order to chart out an effective way forward, we strongly recommend the setting up a National IPv6 Task Force in order to look into key IPv6 issues with the mandate of developing strategies for the eventual nationwide deployment of IPv6 by focusing on key areas such as:***
   a. ***Awareness creation,***
   b. ***Capacity building,***
   c. ***Research and Policy development.***

2. ***It is also proposed that Government leads the way by example; in this regard it is suggested that Government and public institutions be required to commit to the operational deployment and use of IPv6. For instance, usage of IPv6 in the platforms/applications pertaining to e-governance could be mandated. The Government could also mandate IPv6 compatibility in its own procurement of IT systems and networks.***

3. ***The Action Plan proposed below describes specific steps that may be adopted by governmental agencies to expedite the operational deployment and use of IPv6.***

    a. ***Governmental agencies will need transition to IPv6 in order to:***

    1. ***Reduce complexity and increase transparency of Internet services by eliminating the architectural need to rely on Network Address Translation (NAT) technologies;***
    2. ***Enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future governmental IT systems; and***
    3. ***Enable the Internet to continue to operate efficiently through an integrated, well- architected networking platform and accommodate the future expansion of Internet- based services.***

    b. ***In order to facilitate timely and effective IPv6 adoption, governmental agencies shall:***

    1. ***Designate an IPv6 Transition Public Agency. The IPv6 Transition Public Agency will be the lead the agency for IPv6 transition activities;***

    2. ***Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2013;***

3. ***Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2015.***

4. It has also been suggested in the public consultation process that Government can consider providing for limited time tax incentive on importing equipment that are in line with the IPv6 roadmap implementation for private companies. However, such an IPv6 roadmap implementation assumes that the approved roadmap is issued as a result of a policy directive enforced through legislation so that of any form of tax incentive can become enforceable. The practical implications of this measure will need to be further investigated at the level of the National IPv6 Task Force to ensure the deployment of an appropriate enforcement framework.

5. In terms of regulatory issues related to transition from IPv4 to IPv6, there is a need to amend the definition of IP address mentioned in ISP licence to enable 128 bits to be used as needed for IPv6 based addressing.

6. The Authority, in consultation with the National IPv6 Task Force will also look into the possibility of ensuring that all imported communication network and customer premises equipment are either IPv6 compatible or that the vendor can prove that there is a clear upgrade roadmap to support IPv6.

3) **Which transition mechanism/strategy do you consider is best suited for migration from IPv4 to IPv6?**

Transition mechanisms allow organisations that currently depend on IPv4 networks to become IPv6 enabled also. These generic mechanisms may be classified as:

- Dual-stack hosts and routers
- Tunneling
- Translators

Dual-stack Hosts and Routers

Initially, IPv6 users will require ongoing interaction with existing IPv4 nodes. This can be achieved by using a dual-stack IPv4–IPv6 approach. With this transition mechanism, a host has access to both IPv4 and IPv6 resources. Routers running either of the two protocols can forward traffic for both IPv4 and IPv6 end nodes. In addition, dual-stack machines can use IPv4 when communicating with native IPv4 hosts, or IPv6 when communicating with IPv6 hosts.

Tunneling

Transition mechanisms that allow IPv6 hosts to communicate via intervening IPv4 networks are based on a technique known as tunneling, which ensures there is no disruption to the end-to-end IP communications model. With IPv6-over-IPv4 tunneling, IPv6 packets are carried within IPv4 packets. Tunneling is a solution utilised when there is no native IPv6 connectivity between different points on the network. IPv6 packets are encapsulated within IPv4 packets, carried across an IPv4 network to the other side where the IPv4 packet is removed and the IPv6 packets continue on their way. Conversely, IPv4 packets can also be tunneled across IPv6 networks. Because the nodes support both protocols, IPv6/IPv4 nodes may be configured with both IPv4 and IPv6 addresses. IPv6/IPv4 nodes use IPv4 mechanisms (e.g., DHCP) to acquire their IPv4 addresses, and IPv6 protocol mechanisms (e.g., stateless address autoconfiguration [RFC2462] and/or DHCPv6) to acquire their IPv6 addresses.

Tunnel brokers (TBs), which have been commercially available on the web for some time, relieve some of the burden associated with setting up tunnels manually. A TB is a dual-stack server that facilitates tunneling through an IPv4 network to which the server client must be connected in small, isolated IPv6 sites.

For example, a client may request tunneling through a web server. To enable this request, the client receives the configuration information needed to establish a pseudo-automatic tunnel whenever the client triggers tunnel set-up. At the same time, the TB automatically establishes the side of the tunnel bordering the IPv6 network. In this way, users can access their web sites and connect to native IPv6 networks and services.

Translators

To enable communication between IPv4 and IPv6-only domains, a combination of dual-stack nodes and translation techniques at the network, transport and application layers must be applied. Network Address Translation with Protocol Translation (NAT-PT) translates IP addresses and protocol fields between IPv6 and IPv4 domains are one such translation technique. The Dual Stack Translation Mechanism (DSTM) which enables communication between IPv6 hosts (with both IPv6 and IPv4 capabilities) and IPv4-only hosts is another such technique.

Other Transition Considerations

On the software side, if the source code for an application is available, it is easy to modify or port it to work with both IPv6 and IPv4 stacks in the host. This is because IPv6 does not modify the Application Programming Interface (API) between an application and the IP stack. Since most software vendors, such as Microsoft, which supports IPv6 in Windows, have or are migrating their software to support IPv6, the acquisition costs would be no different than the costs associated with upgrading traditional software.

As with IPv4, IPv6 requires robust DNS services, such as name-to-address and address-to-name translations, as well as DHCP IPv6 implementation. This is necessary when administrators want greater configuration control than that provided automatically by IPv6. A new resource record type named "AAAA" has been defined for IPv6 addresses [RFC3596]. Since IPv6/IPv4 nodes must be able to interoperate directly with both IPv4 and IPv6 nodes, they must provide resolver libraries capable of dealing with IPv4 "A" records as well as IPv6 "AAAA" records.

For service providers, a key consideration is when to make the transition to IPv6. The transition will require time, effort, financial resources and training to ensure that they, and their customers, will benefit from the enhanced productivity, reliability, and other features enabled by IPv6.

According to the feedback obtained from ISPs, the Dual Stack transition method is the preferred solution. However, when ISPs were asked how they plan to connect IPv6-only customers to IPv4-only services, two of them plan to run NAT-PT, one ISP replied that this is part of their commercial plan and others simply have no plan. Although most ISPs see a need for IPv4-IPv6 interworking at the network layer, many of them do not see a need for an ISP to operate the resulting translator. Yet, their customers will be the first to suffer when IPv6-only clients cannot reach IPv4-only services.

Recommendations

The transition to IPv6 from IPv4 will be a gradual process, during which the two protocols are expected to coexist for several years. This evolution requires communication between IPv6 nodes across IPv4 zone. It also requires transition mechanisms for IPv6 hosts and routers to enable IPv6–IPv4 communications. In view of the Regulator's technology-neutral and light-handed approach, the Authority does not intend to mandate any specific transition mechanism/strategy best suited for migration from IPv4 to IPv6.

4) **Do you consider that the allocation of permanent IP addresses to a broadband user is a must or not?**

For Broadband connections, permanent IP address is not a `must' requirement though it is desirable for some applications. On the other hand, a permanent IP address allocation may lead to increased privacy risk for the users as once its address is intercepted it will remain exposed. As per most of the stakeholders the choice of IP address should be left to the end users who can opt for the same in accordance with their applications needs.

Moreover, the assignment of static or dynamic IP addresses to end users is an operational decision based on issues such as overhead incurred when assigning static addresses, customer requirements, and many technical concerns based on the network infrastructure and applications being used. Therefore, it would be inappropriate for a regulator to mandate a single solution i.e. static IP address, when that solution may not necessarily technically feasible for all, and may not be the best solution.

Recommendations

There is no need of mandating allocation of a permanent IP address to a broadband subscriber and this option is to be left to the user.

5) **Do you believe that the present mandate of the regulator regarding numbering administration is by extension applicable to IPv6?**

IP addresses are managed regionally and in a hierarchical manner. ICANN, as part of its IANA functions, allocates IP address space from the pools of unallocated address space to the RIRs according to their needs as described by its global policy. Each RIR currently obtains /8s IPv4 address space and /12s IPv6 address space from the IANA pool. RIRs allocate IP address space to their memberships such as Local Internet Registries (LIRs) or National Internet Registries (NIRs) according to their needs as described by each regional policy. The minimum IPv4 allocation sizes from RIRs depend on each regional policy, which vary from /22 to /20, while the minimum IPv6 allocation size from RIRs is generally fixed as /32. These delegated address spaces are allocated or assigned to their members such as ISPs or end-users.

In terms of the addressing structure is concerned, IPv6 still carries a network and a host portion as for IPv4, but is organised differently. The network portion is divided up several times itself, in a hierarchical manner, beginning with the IANA portion:

- RIRs receive allocations from IANA (based on IPv6 utilisation policy defined in RFC 3194)
    - Currently in /12 units
- Every ISP receives a /32 (or more) from RIRs
    - Providing 65,536 site addresses (/48)
- Every end user’s site receives a /48 from an ISP
    - Providing 65,536 /64 (LAN) addresses
- Every end user’s LAN segment receives a /64
    - Providing 2^{64} interface addresses per LAN
- Every end user’s device interface receives a /128
    - May be EUI-64 (derived from interface MAC address), random number (RFC 3041), autoconfiguration, or manual configuration

Up to now, 40 million IPv4 addresses have already been issued by AfriNIC and the present pool of AfriNIC for IPv4 is around 74 million IPv4 addresses. The current monthly consumption of IPv4 addresses from AfriNIC is around 720,000.

As per information obtained from AfriNIC, Mauritian AfriNIC members currently have been allocated the following Internet resources:

- 1,861 /24 IPv4 addresses which is roughly 0.5 Million IPv4 addresses
- 11 /32 IPv6 addresses which roughly correspond to 47.2 Billion IPv6 addresses
- 17 Autonomous system numbers

Differing points of view have been expressed with respect to IP address allocation. Some take the view that the current IP address management has been worked well and there is no need to change it; on the other hand, others have argued for the need to review the current system because of the rapid increase of demand and use of the Internet, in order to ensure equitable distribution of resources and access for all into the future. In response to that position, some have argued that any changes in the allocation mechanism would result in technical risks such as disruption of the current routing aggregation. In fact, it is also believed that the current regional allocation scheme is the maximum (and optimum) level of decentralisation: any further decentralisation would have negative effects, in particular with respect to routing.

Recommendations

The ICT Authority will not extend its mandate to act as an intermediary entity between AfriNIC and its Mauritian members to allocate IP addresses at the national level. However, there could be a need for the Regulator to monitor assignment of IP addresses by ISPs to Mauritian end users. As indicated by AfriNIC, Mauritian operators that meet the defined criteria obtain their resources based on the same process as used for all the other from the 54 countries covered by AfriNIC. However the policy used by LIRs (Local Internet registries – The AfriNIC members) are decided only by them and could be monitored by the Regulator to ensure that they also follow the same principle as the global and regional one and that there is no abuse in the way IP addresses are assigned down to end user or enterprise's networks. On this score, the ICT Authority will do due diligence to this measure through the issuance of appropriate directives to monitor the assignment of IP addresses from local ISPs to Mauritian end users based on international best practices as and when required.

6) **Do you find or have you ever encountered any problem with the existing system of IP address allocation in Mauritius?**

No problem has been flagged out in the allocation of IP addresses from AfriNIC to its Mauritian members. However, as previously indicated by AfriNIC and reiterated by ISOC, monitoring of assignment of IP addresses from Mauritian ISPs to end users is required. ***Therefore, the same analysis made in 5) above applies here also.***

7) **If yes, is there a need to create a neutral entity to handle IP address allocation at the national level?**

Having a separate authority managing IP address will not remove the burden created by operators that receive these addresses and apply there own policy in the way the assign them to their customers (being individual or enterprises). ***Therefore, the same analysis made in 6 & 7 applies here also.***

8) **Are Mauritian ISPs presently involved in any experimentation programme with IPv6 in an effort to move towards commercial IPv6 based services?**

According to the survey carried out with ISPs, none of them is involved in IPv6 experimentation.

One possible reason is that unlike the previous NCP-to-IPv4 transition in 1983 (the transition from the protocol used with the original ARPANET to the current TCP/IP), there is no flag date by which the transition must be achieved. There is no hard and fast deadline creating urgency, which has been the key to previous successful transitions. Some experts predict that the transition will be protracted. However others project that there will be a network effect whereby, when sufficient amounts of online assets have migrated to IPv6, networks will tip to IPv6 and IPv4 will fade. At this point the transition could accelerate.

IPv6 is a new network protocol which will require new training, experience, and implementations. During the transition, new vulnerabilities could be introduced, and IPv4 security devices and software may be of limited use. As network operators have done when introducing anything new into networks, operators will have to work with and test IPv6 implementations in order to ensure security.

If precautions aren't taken, the transition from IPv4 to IPv6 could be cause for network security concerns. Without proper perimeter security, hackers could use IPv6 to gain access to a LAN, which could compromise both IPv6 and IPv4 network assets. Therefore, the same care taken to write and implement an IPv4 security policy should be taken with IPv6, even with all its benefits. Introducing IPv6 into a network, like any other new protocol, requires that firewalls and other security measures be well thought-out and tested.

Recommendations

It is proposed to investigate into the possibility of making disbursement from the Universal Service Fund (USF) for the deployment of experimentation programme with IPv6. It is, therefore, suggested that this proposal be examined at the level of the National IPv6 Task Force and eventually be referred to the USF Ministerial Committee for its consideration.

9) **Any other issue/ comments pertaining to transition to IPv6 in Mauritius that you may wish to flag out.**

One of the more passionate points of discussion surrounding IPv6 involves Network Address Translation (NAT) boxes. A NAT box is a host on the Internet with an IP address that has behind it a network of privately addressed computers. A specific block of addresses has been set aside for private use and is not advertised by networks to the public Internet. Since these addresses only work internally and cannot be used to communicate on the public Internet, they can be reused over and over again behind NATs.

An example of a NAT might be an off-the-shelf Wi-Fi access point that a residential user might use for home Internet access. The ISP assigns to that subscriber an IP address which is assigned to whatever computer the subscriber attaches at the end of the network. The subscriber attaches the Wi-Fi router. Behind the Wi-Fi router could be all of the computers in the house; the router assigns them IP addresses from the private IP address space. In this way, a subscriber with one public IP number can have multiple computers attached to the Internet. Commercial ISPs may utilise private IP numbers for their subscribers, and corporate LANs may also utilise private IP addresses.

Network operators utilise NATs for various objectives. First, NATs are used to conserve the scarce numbering resource; one public address maps to multiple private addresses. Second, NATs are also used for network management and security, creating single points of entry into networks. After the transition to IPv6, with the dramatically increased address space, NATs would no longer be necessary in order to deal with the scarce numbering resource. It is expected that with IPv6 the use of NATs will likely decrease although it may not disappear. NAT boxes have drawbacks. While NAT has to some extent delayed the exhaustion on IPv4 address space for the short term, it complicates general application bi-directional communication. NAT boxes break the end-to-end nature of Internet communications, and thus interfere with some Internet applications and services, and create an impediment to innovation.

NAT boxes may work well when traffic originates from within the private network and the NAT box can track which host to return traffic to (someone on the network requests a webpage, and the NAT box knows who to return the webpage to). NAT boxes do not work so well when the traffic originates outside the network trying to reach someone inside the network (for example, someone trying to set up a VoIP call with someone inside the network. Since the request from the VoIP outsider came to the NAT box IP address, the NAT box has no idea which computer inside the network the outsider is actually trying to reach).

NAT boxes present barriers to applications which seek to take advantage of IP address transparency. They inject non-standardized intelligence into the network, requiring application developers to conform to each non-standardised implementation. They require a conversion from the public address space to private address spaces, which degrade the performance of some applications. NATs also result in less accurate geolocation, make identification and blocking of abuse more difficult, and frustrate IP-based authentication.

In terms of the practical consequences of IPv6 for ordinary Internet users, ideally, if the service providers and the other people in the industry - the content providers, etc. - all do their jobs right and on time, when ordinary Internet users will be forced to move to IPv6, they will not notice the change. The difference it will make over time is because IPv6 restores what's called the "end to end model" the ability for any arbitrary host "A" on the network to offer services to or connect to services on any other arbitrary host "B," assuming that it's permitted by policy at both ends, there will be many new applications which were not available in the IPv4 world due to the widespread use of network address translation.

However, that situation is unfortunately likely to get worse before it gets better, because there is not enough time for the different stakeholders to do what is required to be done on time for the end user not to notice this transition. As there are simply not enough IPv4 addresses to provide a globally unique (public) address to all of the devices already connected to the Internet, network operators have been forced to deploy NAT in their LANs. The end user will probably be going through a period where he/she is behind a NAT444, where not only does he/she has the NAT gateway that he/she is used to at home, but the address on the outside of that will no longer be a public address; it will become an intermediary address that then goes through another layer of NAT at the carrier. This is fine for web browsing and many other client side applications but it is a major problem for server and peer to peer applications (VoIP, gaming, webcams, VPNs, bittorrent, video streaming, chat, etc) where communication needs to be initiated from the outside in.

Recommendations

The deployment of the NO-NAT strategy for Mauritius proposed by AfriNIC so as to benefit from the available AfriNIC IPv4 address pool as an instrumental measure in a clean implementation of an IPv6 supported Infrastructure is a proposal which requires further investigation. This topic can be discussed in depth at the level of the National IPv6 Task force to assess the policy, legal and practical implications therein.

3. **Compiled responses to technical questionnaire sent to Mauritian ISPs**

The purpose of this survey was to obtain a view of the IPv6 experience, plans, and requirements of Mauritian ISPs. This questionnaire is based on RFC 6036 - Emerging Service Provider Scenarios for IPv6 Deployment. As already stipulated to the ISPs, replies to this questionnaire will be kept strictly confidential and only combined results will be published without identifying information about individual ISPs in any published results.

A detailed summary of the replies has been produced and the raw technical questions have been listed below. The general comments are a compilation of the responses received from eight ISPs who replied before the cutoff date for this analysis.

This document describes practices and plans that are emerging among Internet Service Providers for the deployment of IPv6 services. They are based on practical experience so far, as well as current plans and requirements, reported in a survey of a number of ISPs carried out in March 2011.

1. **Introduction**

As is well known, the approaching exhaustion of IPv4 address space will bring about a situation in which Internet Service Providers (ISPs) are faced with a choice between one or more of three major alternatives:-

i) Squeeze the use of IPv4 addresses even harder than today, using smaller and smaller address blocks per enterprise customer, and possibly trading address blocks with other ISPs.

ii) Install multiple layers of Network Address Translation (NAT) or share IPv4 addresses by other methods such as address-plus-port mapping.

iii) Deploy IPv6 and operate IPv4-IPv6 coexistence and interworking mechanisms.

This document focuses on alternative (iii), while recognising that many ISPs may be obliged by circumstances to prolong the life of IPv4 by using (i) or (ii) while preparing for (iii).

This document describes IPv6 deployment scenarios already adopted or currently planned by a set of ISPs who responded to a technical questionnaire. It is, therefore, a factual record of the responses from those ISPs. It makes no recommendations; the best choice of scenarios will depend on the circumstances of individual ISPs.

We consider various aspects of IPv6 deployment: addressing, routing, DNS, management, and IPv4-IPv6 coexistence and interworking. Out of these 8 ISPs, only 4 ISPs offer Internet services to the general public, 3 offer services to businesses only and 1 ISP does not have a subscriber base. For ISPs which offer Wimax, IPSHDSL and fibre based Internet services, these services are already IPv6 compatible. Out of the 3G mobile based Internet services available for 2 ISPs, only one of these services is IPv6 compatible. However, ADSL based Internet services which are offered by ISPs are not IPv6 compatible. Moreover, only 2 ISPs include support for DNS AAAA queries over IPv6 and for reverse DNS for IPv6 addresses.

2. Survey of ISP's Experience, Plans, and Requirements

2.1 General Questions about IP Service

Out of the 8 ISPs, only 6 offer services to the public. 5 offer origin-only IP service; 1 respondent offers both origin-only and transit service; 1 ISP offer dial-up service and 1 ISP does not offer any service to the public.

The following access technologies are used: ADSL, Wimax, PS networks, IPFR, Dialup, IPLC, xDSL, IPSHDSL, IPFR, IP over copper/fibre.

Most ISPs provide Customer Premises Equipment (CPE) to some or all of their customers, but these CPE are often unable to support IPv6 except for the Wimax based CPEs.

Estimates of when ISPs will run out of public IPv4 address space for internal use vary widely, between "now" and "never". Public IPv4 address space for customers is mainly expected to run out between 2012 and 2014.

2.2 Requirements for IPv6 Service

Out of 8 ISPs, 7 reported to have never received request from customers for IPv6. For the time being, only one customer is using IPv6 in Mauritius. Predictions for when 10% of customers will require IPv6 range from 2012 to 2016, and for 50% from 2014 to 2021. These ISPs require IPv6 to be a standard service between 2013 and 2015.

2.3 Status and Plans for IPv6 Service

To date, 7 out of the 8 ISPs do not offer IPv6 as a regular service and the only 1 ISP has 1 customer who uses IPv6. Planned dates for regular service are between end 2011 and 2013.

2.4 IPv6 Technologies

Turning to technology choices, the choice of approach is a dual-stack routing backbone, and the reason given is simplicity and cost. 5 out of the 8 ISPs don't see IPv6 as an opportunity to restructure their network topology. When asked which types of equipment are unable to support IPv6, the answers were CPE devices, ADSL Modems, BRAS, IPDSLAMs, routers and switches. When asked if such devices can be field-upgraded to support IPv6, the answers varied: 5 yes, 2 partially, 1 “don’t know”. Out of 8 ISPs, only 2 include support for DNS AAAA queries over IPv6.

The ISPs surveyed have been allocated prefixes of /32, and only 1 ISP offer a /48 prefix to its customers.

Only one ISP currently operates dual-stack SMTP, POP3, IMAP and HTTP services. Considering IPv4-IPv6 interworking, 5 ISPs stated that IPv4-IPv6 interworking is needed. On the other hand, only two run or plan to run NAT-PT (Protocol Translation) which includes DNS translation.

Among those who do not plan a translator, when asked how they plan to connect IPv6-only customers to IPv4-only services, only one respondent replied this is part of their commercial plan and others simply have no plan.

Although most ISPs see a need for IPv4-IPv6 interworking at the network layer, many of them do not see a need for an ISP to operate the resulting translator. Yet, their customers will be the first to suffer when IPv6-only clients cannot reach IPv4-only services.

When asked about plans for Mobile IPv6 (or Nemo mobile networks), four ISPs said yes, and two said no, with the others ‘not applicable’.

3. **Gap Analysis**

The survey has shown a certain number of desirable features to be missing, either in relevant specifications, or in many products. This section summarises those gaps.

3.1 Product Issues

As noted above, numerous models of various types of product still do not support IPv6:

- CPE devices
- Handsets
- DSLAMs
- Routers
- Cisco 1800 and 3700 series
- ADSL Modems
- BRAS
- IPDSLAMs
- Switches
- Firewalls
- Intrusion detection systems
- Accounting and billing systems

4. **Security Considerations**

ISPs did not register any general concerns about IPv6 security. However, we note that most of firewall and intrusion detection products for ISPs are still reported not to support IPv6.

5. **Acknowledgements**

We are grateful to all the ISPs who answered the questionnaire.

4. Questionnaire sent to all ISPs in March 2011

This appendix reproduces the technical body of the questionnaire that was made available for ISPs to express their requirements, plans, and experience.

I. General questions about IP service

1. Do you offer origin-only (stub, end-user) IP service, transit IP service, or both?
2. Approximate number of private/small office customers (one IPv4 address)
3. Approximate number of corporate customers (block of IPv4addresses, not included in Q2)
4. Do you offer IP multicast service?
5. Do any of your customers require multihoming to multiple ISPs?
6. Access technologies used (ADSL, etc.)
7. Do your customers use CPE that you supply?
   - 7.1. What % of customers?
   - 7.2. Does the CPE that you provide support native IPv6?
8. When do you expect to run out of public IPv4 address space inside your own network?
   - 8.1. Do you run private (RFC1918) addresses and NAT within your network (i.e., a second layer of NAT in the case of customers with their own NAT)?
   - 8.2. What % of your IPv4 space is needed for your own use (not for customers)?
9. When do you expect to run out of public IPv4 address space for customers?
   - 9.1. Do you offer private (RFC1918) addresses to your customers?

II. Questions about requirements for IPv6 service

10. Are some big customers requesting IPv6?
11. When do you predict 10% and 50% of your customers to require IPv6 service?
12. When do you require IPv6 to be a standard service available to all customers?
13. When do you predict IPv6 traffic to reach 50% of total traffic?

III. Questions about status and plans for IPv6 service

14. Do you currently offer IPv6 as a regular service?

    14.1. What % of your customers currently use IPv6?

    14.2. When do you plan to start IPv6 deployment?

    14.3. When do you plan to offer IPv6 as a special or beta-test service to customers?

15. When do you plan to offer IPv6 as a regular service to all customers?

IV. Questions about IPv6 technologies

16. Which basic IPv6 access method(s) apply:

    16.1. dual stack routing backbone?

    16.2. separate IPv4 and IPv6 backbones?

    16.3. 6to4 relay?

    16.4. Teredo server?

    16.5. Tunnel broker? If so, which one?

    16.6. Something else? Please briefly describe your method:

    16.7. If possible, please briefly explain the main reasons issues behind your choice.

17. Which types of equipment in your network are unable to support IPv6?

    17.1. Can they be field-upgraded to support IPv6?

    17.2. Is any equipment 100% dedicated to IPv6?

18. Is IPv6 an opportunity to restructure your whole topology?

19. Do you include support for DNS AAAA queries over IPv6?

20. Do you include support for reverse DNS for IPv6 addresses?

21. What length(s) of IPv6 prefix do you have or need from the registry?

22. What length(s) of IPv6 prefix are offered to customers?

    22.1. Do any customers share their IPv6 prefix among multiple hosts?

23. Do any of your customers prefer to use PI IPv6 prefixes instead of a prefix from you?

24. How are IPv6 prefixes delegated to CPEs? (Manual, PPPoE, RADIUS, DHCPv6, stateless autoconfiguration/RA, etc...)

25. Are your SMTP, POP3 and IMAP services dual-stack?

26. Are your HTTP services, including caching and webmail, dual-stack?

27. Are any other services dual-stack?

28. Is each of the following dual-stack?

    28.1. Firewalls

    28.2. Intrusion detection

    28.3. Address management software

    28.4. Accounting software

    28.5. Monitoring software

    28.6. Network management tools

29. Do you or will you have IPv6-only customers?

30. Do you have customers who have explicitly refused to consider IPv6?

31. How many years do you expect customers to run any IPv4-only applications?

32. Is IPv6-IPv4 interworking at the IP layer needed?

33. Do you include a NAT-PT IPv6/IPv4 translator?

    33.1. If yes, does that include DNS translation?

    33.2. If not, do you plan to operate an IPv6/IPv4 translator?

    33.3. If not, how do you plan to connect IPv6-only customers to IPv4-only services?

    33.4. If you offer IP multicast, will that need to be translated too?

34. Any plans for Mobile IPv6 (or Nemo mobile networks)?

35. What features and tools are missing today for IPv6 deployment and operations?

36. Any other comments about your IPv6 experience or plans? What went well, what was difficult, etc.

5. Compilation of stakeholders' comments on Public Consultation paper

Following the consultation paper published on the website of the ICTA on 17 March 2011, inviting views and comments from the public, four submissions were accordingly received. The ICT Authority is grateful to Mauritius Telecom, Internet Society of Mauritius, AfriNIC, Mr. S. Juddoo and Mr. S. Moonesamy for their contribution thereon. The document below is a compilation of the comments from our stakeholders:-

1) **Respondent 1**

i) Page 2

IPv6 does not provide a better Quality of Service or better security than IPv4 (through IPSec). IPv6 has been designed to improve forwarding and routing within the Internet by means of a simplified header and natural address aggregation capabilities. IPv6 also provides the tools for security (security optional header, OS field) and QoS policy enforcement purposes that are equivalent to IPv4.

ii) Page 3

The World IPv6 Day on 8 June 2011, sponsored by Internet Society, is not the first global IPv6 trial conducted at the scale of the Internet. The late 6-Bone overlay network was used for that purpose between 1996 and 2006. Router vendors, academics and service providers were connected.

iii) Page 4

The notion of "neutral agency" to manage IP addresses within Mauritius should deserve some elaboration as address space management technically assumes the involvement of a Local Internet Registry. Currently, IP resources like IP addresses are requested directly from AfriNIC.

iv) Pages 4/5

Regional Internet Registry (RIR) structures manage both IPv4 and IPv6 address spaces. The ability for Mauritius to acquire additional IPv4 address blocks should be moderated by the Fair Usage policies generally enforced by RIRs.

v) Page 9

Both H323 and SIP-based VoiP services have been extensively deployed and operated since the beginning of 2000. IPv6 will not be a key differentiator in that area as the primary difference will be dependent on the actual VoiP service design. IPv6 will avoid complex VPN-based VoiP design schemes that are used to accommodate inevitable private IP overlapping schemes at the cost of extra management complexity and possibly degraded QoS.

vi) Page 10

The creation of a National Internet Registry contradicts current organisations that rely upon one or several non-governmental Local Internet Registry (LIR). In addition, National Internet Registries would not facilitate the resolution of cyber-crimes since LIRs are chartered to assign local IP addresses and are required to report to the RIR about such allocation. Thus, the information required by legal authorities can be accessed and provided by the LIR without the need for specific government structure.

Likewise, the update of the whole "Whois" database which is technically part of the LIR's mandate.

2) **Respondent 2**

On January 31 2011, the Internet Assigned Numbers Authority (IANA) allocated two blocks of IPv4 address space to APNIC, the Regional Internet Registry (RIR) for the Asia-Pacific region. On February 3, IANA allocated equally the remaining blocks to each of the five RIRs: Africa (AFRINIC), Asia Pacific (APNIC), North America (ARIN), Latin America and the Caribbean (LACNIC), and Europe and the Middle East (RIPE NCC). Each of these blocks represents about 16.7 million possible addresses. In response to IPv4 address exhaustion, the Internet Engineering Task Force (IETF) created IPv6, a new version of the Internet Protocol with a vastly expanded address space. The new version also included many desired features such as enhanced security. As work progressed, many IPv6 improvements have been incorporated into IPv4 networks, leaving a vastly increased address space as the one clear feature of IPv6.

Since the final blocks of IPv4 addresses have been allocated to AfriNIC serving the African region, which includes Mauritius, the second respondent commends the initiative of the ICTA to launch a public consultation to collect views of all stakeholders involved.

They reckon that all Internet stakeholders must now take definitive action to deploy IPv6 being given that the available IPv4 address space will be depleted at some point in time. The only way that the Internet will grow in the future hassle free is by adopting IPv6 and starting now itself.

They pointed out that the RIRs have been allocating IPv6 address space since 1999 and thousands of organizations around the world have received an IPv6 allocation to date. They acknowledge that to migrate fully to IPv6, this demands massive investment in terms of hardware and software and that the ISPs do not find a business case to do so. For the foreseeable future, the Internet must run both IP versions (IPv4 & IPv6) at the same time. When done on a single device, this is called the “dual-stack” approach. They also stress that deployment is already underway. Today, there are organizations attempting to reach your mail, web, and application servers via IPv6.

(i) **Collaborative approach to the development of the Internet in Mauritius**

The second respondent has always privileged the collaborative approach for the development of the Internet. Many different organisations and different companies make decisions every year that contribute to how the Internet develops. These wide-ranging organisations, together with the users of the Internet and the technical community developing Internet technologies and applications, require different types of coordination, each calling for specific competences and sensitivities to balance the needs of the Internet user community.

This coordination is best performed by the existing set of organisations using proven processes, which are critical for the future stability and evolution of the Internet, and should not be modified arbitrarily or abruptly. *Because of the diverse nature of these activities, it is unrealistic to expect a single body - Government or otherwise - to take on all these roles effectively.*

There has always been a need to manage the allocation of Internet resources such IP addresses, generic top-level domain names (e.g. .org), country code top-level domain names (e.g. .mu), domain names (such as www.icta.mu), and the systems that translate domain names into IP addresses (e.g. the Domain Name System or DNS). This coordination activity has been handled by long-standing, not-for-profit membership organisations such as the Regional Internet Registries (RIRs) like AfriNIC and top-level domain (TLD) registries. Coordination at a global level has been supported by ICANN (Internet Corporation for Assigned Names and Numbers). Business, technical, non-commercial, academic, governmental and end-user communities participate in ICANN. These organisations are a meeting point for bottom-up, multi-stakeholder, consensual, industrial self-regulation by the groups and individuals that use their services and resources.

The second respondent recommends that the Information and Communications Technology Authority (ICTA) plays an important role in the coordination of the Internet at the global level by joining the existing structures within the existing model. Any global action will definitely has an impact on the Internet at the local level. Henceforth, they recommend that the ICTA joins and participates actively in the Multistakeholder Advisory Group (MAG) of the Internet Governance Forum (IGF), the ICANN Government Advisory Committee (GAC) and other international organisations. The successful continued development of the Internet for the benefit of everyone can be ensured by participation in these proven processes rather than by attempting to create new untested mechanisms that are inappropriate to the unique characteristics of the Internet.

(ii) **Assessment of our readiness in Mauritius as well as the need for any regulatory intervention, and the extent to which it should be in the transition from IPv4 to IPv6**

This respondent acclaims ICTA’s initiative to access our readiness in Mauritius in relation to IPv6 deployment. However this should not be limited to IPv6 only. Other assessments are warranted like connectivity costs in Mauritius compared to other countries and assessment whether the incumbent public operator in Mauritius has significant market power.

This respondent is totally against regulation for the IPv6 deployment. They would like the ICTA to be the facilitator for IPv6 deployment rather than taking a role to regulate this process.

It is observed from International practices that IPv6 migration is not forced on the existing ISPs through a mandate but its deployment is facilitated by the Governments by setting up IPv6 test-beds, backbones and also conducting training & awareness programmes. They would urge ICTA to take this route. Also, it is important that all tests are done and confirmed and properly documented. The results might also be requested by foreign investors who want to invest in Mauritius. As an example, in a survey lasting for one year, Google found native IPv6 latency to be comparable to that of IPv4 while latency of IPv6 relay mechanisms was higher than that of IPv4. It should be noted that other research finds IPv6 latency to be much higher than that of IPv4 at this stage. This data (round trip delay) is important for foreign investors in Mauritius who want to run heavy applications offshore.

As key infrastructure to exchange local Internet traffic, support of IPv6 by Internet eXchange Points (IXPs) is a pre-requisite for fast and inexpensive IPv6 connectivity. IXP support of IPv6 is particularly important to increase interconnectedness and decrease latency. Internet exchange points provide a common location where multiple service providers can meet and exchange customer traffic. Henceforth it is primordial to ensure that the Mauritius *Internet eXchange Point (MIXP)* explicitly supports IPv6.

The transition from IPv4 to IPv6 should be left to the industry. Since the Internet has evolved so far, especially the technical side of it, by the technical community and the industry, the Internet Society of Mauritius recommends that even the transition from IPv4 to IPv6 should be left to the technical community and the industry to decide the best way forward. People want access to the entire Internet, and this means IPv4 and IPv6 websites. Offering full access requires running IPv4/IPv6 transition services and is a significant engineering project. Multiple transition technologies are available, and each provider needs to make its own architectural decisions. Content must be reachable to newer Internet customers. Content served only via IPv4 will be accessed by IPv6 customers via transition solutions run by access providers. Mail, web, and application servers must be reachable via IPv6 in addition to IPv4. Each organization must decide on timelines, and investment level will vary. I think ICTA's role here will be to coordinate with industry to support and promote awareness and educational activities.

(iii) **Assessment of the need for the setting up a neutral agency to manage IP addresses within Mauritius**

The second respondent has certain reserves as to the setting of an agency to manage IP addresses. The agency can be setup only after consultation with or approval from the Regional Internet Registry, AfriNIC. The New agency should be guided by Operational policies set up by AfriNIC, same as Operational Policies for National Internet Registries in the other RIR regions. The management of IP addresses is the responsibility of the Regional Internet Registries (RIR). The RIRs manage IP numbers as a public resource. When a registry allocates a number to an entity, it is giving that entity the ability to use that number; no property right is conferred to the recipient. IP numbers are allocated on a needs-basis pursuant to RIR policies; recipients pay fees which support the operation of the registries.

Policies for the allocation of IP addresses are developed under the regional Policy Development Process in the Public Forums of the Regional Internet Registries. These policies have been developed bottom up and are specifically designed to meet the needs of the regional Internet community. Each RIRs Public Forum is sovereign in its policy development process. The RIRs are membership-based organizations. Members are mainly Internet Services Providers (ISPs), telecommunication organizations and large corporations.

It is important to point out that the IP address Policy Development Process described above is open, transparent and inclusive. It includes the active participation of both public and private sector bodies as well as civil society. The formal Policy Development Process, along with publicly available and archived, open mailing lists, enable Internet address management policies to take into account the broad perspectives of all relevant stakeholders. The role of the RIRs is to facilitate these processes, help their communities build consensus-based policies and then to ensure that these policies are applied fairly and consistently. Also, while RIRs are fundamentally autonomous, close cooperation is undertaken among all RIRs to maintain the consistency of policies developed, and ensure that any divergence is consistent with the technical and operational requirements of a stable Internet infrastructure.

It is important to recognise that these IP address policies are formed and approved by the

Internet community at large, not by RIRs themselves or by RIR staff. This community includes governments, civil society and RIR members and non-members. The executive boards of the RIRs, while directly elected by the RIR memberships, also do not form or approve IP address policies. Governments and their agencies have used the channel of the Governmental Advisory Committee (GAC) to comment on IP address policies and in particular to the transfer to the IPv6 address space and the establishment of new Regional Internet Registries, in particular for Africa.

(iv) **Adoption of regulatory incentives to encourage IPv6 deployment.**

The ICTA can come forward with regulations to encourage suppliers of hardware in Mauritius to sell devices which are IPv6 compatible especially equipment requiring type approval. Regulations can be made to adopt IPv6 within the government agencies in Mauritius.

(v) **Allocation of Permanent IP addresses for Broadband**

The second respondent makes a distinction between a Permanent IP address and a static IP address. While both permanent and static IP addresses are fixed IP addresses, a dynamic IP address is one which changes. While the ICTA refers to a permanent IP address as one which is supposed to provide an easy solution to the need for mobility without interrupting running communication sessions while moving a terminal from one IP network to another IP network. Therefore we support that the choice of permanent IP address should be made available to the end users who can opt for the same in accordance with their applications needs. They also support that in case a user opts for a permanent IP address, he/she should have choice to change it like a telephone number. They therefore request the ICTA to formally mandate the ISP to provide the above. Now concerning the static IP addresses, they request that the ICTA mandates the ISP to provide ALL broadband users with a static IP address. This should not be left on the users or the ISP to decide. Static IP addresses will be very useful to track down cyber criminals.

(vi) **Creation of a National Internet Registry**

The second respondent does not object to the creation of a National Internet Registry. However they have the same reserves express earlier under paragraph "Assessment of the need for the setting up a neutral agency to manage IP addresses within Mauritius". They would like to point out that they are not happy at all with the statement of the ICTA as follows:-

"Also, one of the biggest advantages of having the proposed registry will be of tremendous value for the law enforcement agencies in Mauritius. Whenever a cyber crime is committed, it is traced with the help of IP addresses. Today, in a number of cases, the law enforcement has numerous problems in getting access to the registration information of the IP addresses. However, when a national Internet registry is established in Mauritius, it would ensure that all the IP addresses will be allocated locally and that the registration information of the same will be instantaneously accessible to the law enforcement agencies. This is likely to have a positive impact on the investigation and detection of cyber crime."

They do not deny the fact that this will help in the detection of crime. However, the "data will be instantaneously accessible to the law enforcement agencies" makes them uncomfortable. Though the creation of the National Internet Registry, data to the law enforcement agencies has to be solely provided in pursuance with the different acts of parliament in Mauritius, like the Computer Misuse and Cybercrime Act 2003.

(vii) **"Whois" for domains and IP addresses**

ICANN requires registrars to provide public access to data on registered names through the Registrar Accreditation Agreement (RAA). ICANN has implemented policies and measures to improve the accuracy and availability of domain name registration records, including

- WHOIS Data Reminder Policy (WDRP),
- WHOIS Data Problem Reporting System (WDPRS), a problem reporting system that allows parties to report allegedly inaccurate WHOIS data and requires that registrars verify the data with the registrant, and
- WDRP compliance audits

The RAA requires registrars to investigate claims of WHOIS inaccuracy: "Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a

Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.

There are several other important WHOIS requirements set forth in the RAA and in various registry agreements. Both the RIRs and ICANN are already taking care of the inaccuracies in WHOIS through the mechanisms they have in place for this purpose.

(viii) **IPv6 Considerations**

IPv6 migration started slowly; little content was available, connectivity was limited, backbone services were not always abundant, IPv4 devices are embedded, and there was a lack of IPv6 exchange points. In 2010, the OECD released a report comprehensively reviewing the state of IPv6 adoption, concluding that by early 2010, IPv6 was still a small proportion of the Internet. However, several large-scale deployments are taking place or are planned. Overall, the Internet is still in the early stages of a transition whereby end hosts, networks, services, and middleware are shifting from IPv4-only to support both IPv4 and IPv6.

A significant barrier to IPv6 adoption has been a negative network effect: without much on IPv6 networks, there has been little incentive to join IPv6 networks. There was no one there with which to interact. With few end users joining IPv6 networks, there was little incentive to create IPv6 resources or content. However, with the migration of US Government networks and other major networks and services to IPv6, network effect has been shifting, creating an incentive to join.

There has not been consumer demand for IPv6. There is consumer demand for Internet access (regardless of whether IPv4 or IPv6) and for new features. Public Internet services are generally reachable today via IPv4, so there is no perceived need by consumers to run IPv6. Consumers have customer premises equipment such as cameras, TVs or game consoles that may only be IPv4 enabled. If the Internet service provider migrates to IPv6, the service provider risks upsetting consumers whose equipment may no longer work properly.

Unlike the previous transition from NCP to IPv4, there is no hard date by which the transition must be achieved. There is no hard and fast deadline creating urgency, which has been key to other successful transitions. Some experts predict that the transition will be protracted, potentially taking decades. However others project that there will be a network effect whereby, when sufficient amounts of online assets have migrated to IPv6, networks will tip to IPv6 and IPv4 will fade. At this point the transition could accelerate.

IPv6 is not backwards compatible. IPv6 networks cannot directly interconnect with IPv4 networks. As both networks will co-exist for some time, this creates an issue for how devices on IPv4 and IPv6 networks are able to interact with each other. Network engineers have been investing significant energy in developing and deploying viable and effective transition solutions. But the variety of different transition solutions also raises the concern of how well different solutions will work with each other, whether there will be conflicts and what might get broken in the process. Generally, the methods of solving this problem are known as Dual Stack and Tunneling. Further information can be provided on request.

The cost of transitioning to IPv6 could be problematic. Costs involved in the IPv6 transition include renumbering networks, running two separate networks (IPv4 and IPv6) simultaneously, upgrading relevant software and hardware, training staff, and testing implementations. The cost of IPv6 will involve capital investment and ongoing operational costs that will have to be diverted from other business goals and which can be difficult to bear in today's economic climate. Some networks may be averse to expending financial resources to make the transition until absolutely required. A report generated for the National Institute of Standards and Technology (NIST) in 2005 stated that it would take 25 years to have a total transition to IPv6 at a cost of $25B. However, without a clear return-on-investment to the ISP, other than being able to offer IPv6 connectivity, it is hard to get them to make the investment.

IPv6 is a new network protocol which will require new training, experience, and implementations. During the transition, new vulnerabilities could be introduced, and IPv4 security devices and software may be of limited use. As network operators have done when introducing anything new into networks, operators will have to work with and test IPv6 implementations in order to ensure security.

It should be noted that IPv6 support by end user device operating systems is not necessarily sufficient for these clients to be able to actually use IPv6. For example, unless an IPv6 client supports IPv6 functionalities such as DHCPv6, Neighbour Discovery and Stateless Address Autoconfiguration, it may not be able to join a new IPv6 network, even if it can send and receive IPv6 packets. Some Operating Systems require extra configuration.

3) **Respondent 3**

In Section 3, it is mentioned that:

"*So the new address space supports 2^128 (approximately 340 undecillion or 340,282,366,920,938,000,000, 000,000,000,000,000,000) address spaces*". RFC 4291 (IP Version 6 Addressing Architecture) [2] defines the addressing architecture of the IP Version 6 (IPv6) protocol. The addressing model is different from IP Version 4 (IPv4) as the current practice is for ISPs to assign a prefix instead of one IPv6 address as in IPv4 for the customer connection. As such the addressing space is much less than the number quoted above.

From Section 4:

"*For making a transition from IPv4 to IPv6, ISPs have to upgrade their networks, provide training to their system administrators and related staff and also have to conduct trial on their network before commercially deploying IPv6*". There are different strategies for making a transition from IPv4 to IPv6. The network upgrade has two components:-

– Backbone
– Customer connection.

The backbone part of the work entails upgrades to core infrastructure such as routers, DSLAMs, BRAS, etc.

The customer connection part may require a CPE upgrade and operating systems that support IPv6. Although commonly used operating systems are "IPv6 ready", there are still unresolved issues such as widespread support for DHCPv6 or DNS configuration when using stateless address autoconfiguration (SLAAC).

From section 5: "*Such devices will also require some kind of identification like telephone number in telecom networks and allocating permanent IP address to such devices can provide a mean for such identification*". IPv6 supports privacy extensions for stateless address autoconfiguration. As such IPv6 addresses are not analogous to telephone numbers and cannot be used as a reliable means for identification of an IPv6 node.

From section 5: “*Consequently, a customer must also be informed about all such charges at the time of subscribing for an Internet connection with a permanent IP address and same should be allocated only in case it is opted for by the customer*”. That recommendation sounds fine. It would be good if this paper used a better terminology as it is not clear whether this is for IPv4 or IPv6.

The yearly charge for an IPv4 address is approximately USD 0.40 (/24) and USD 0.20 (/16). The table below gives a rough approximate "cost" of an IPv4 address in some countries:

U.S.A.	USD 5.00
Canada	USD 5.00
U.K.	USD 10.00
Switzerland	USD 12.00
Australia	USD 3.00

The "cost" in Mauritius is at least ten times the charge. Customers would obviously opt out of getting a static IP address if the price is prohibitive.

In Section 6: “*In order to fulfill this extended mandate, there is a need, at the national level, to properly manage the pool of IP addresses and to undertake appropriate coordination work with existing organisations operating under the aegis of ICANN and which are responsible for the management of IP addresses at the international and regional levels”*.

There seems to be a misunderstanding about how IP address allocation works on the Internet. It is not based on a Country Internet Registry model [3]. The above mandate can only be achieved by setting up a Country Internet Registry for Mauritius. Currently, there is not any provision for the RIR serving Mauritius to recognize such a registry. Resource numbering policies for the region would have to be revised before such a registry can be operational.

It is doubtful whether such a model can gain consensus through the Policy Development Process used for handling Internet Number Resources policies within this service region. Furthermore, it would put Mauritius at a disadvantage as it will have less "weight" in the voting structure used by RIRs.

It is high time that Mauritius works on a transition plan for IPv6. It is debatable whether that should be done through regulation and that approach assumes a "Walled garden" service model. That is in stark contrast to the "open" service model which has spurred the growth of the Internet. The Background section of this paper mentions that: "*The purpose of the NRO is to undertake joint activities of the RIRs, including joint technical projects, liaison activities and IPv4 address allocation policies co-ordination but still with these measures there is relative certainty that the little "guy" such as Mauritius is not going to be in a very strong position when those last blocks of addresses are issued*".

That statement about the "little guy" highlights misunderstandings about the allocation of Number Resources. The position of a country in the various Internet communities is proportional to the amount of participation from individuals and businesses; and the involvement of regulatory bodies. The "little guy" can still make his voice heard through contributions to technical and policy discussions in these communities.

The following organisations operating in Mauritius have IPv4allocations/assignments:-
Africa Digital Bridges Networks Ltd
Board of Investment
Data Communications Limited
Emtel Limited
Ireland Blyth Informatics Ltd
Mahanagar Telephone (Mauritius) Ltd
Mauritius Internet Exchange Point
Mauritius Freeport Development Company Ltd
Telecom Plus Ltd
University of Mauritius

Most of these organisations do not participate in the development of number resources policies. It is interesting to note that there isn't any bank or government department in the above list. Most of the companies listed on the Stock Exchange of Mauritius are not on the list.

The following organisations operating in Mauritius have IPv6 allocations/assignments:-

Africa Digital Bridges Networks Ltd

Emtel Limited

Telecom Plus Ltd.

None of them have announced plans for the deployment of IPv6 to the consumer.

IPv4 allocation statistics show consumption per user as follows:-

	IPv4 address per user
U.S.A	4.90
U.K.	1.34
France	1.24
Germany	1.12
South Africa	0.40
Mauritius	0.38
Tunisia	0.26
China	0.25
Egypt	0.08

Mauritius consumes 0.40 IPv4 addresses per user. If economic factors are accounted for, that figure should have been at least 0.60. There may a run on IPv4 addresses in the region now that APNIC has activated its Final /8 policy [4]. Mauritius may be able to preempt the shortage of IPv4 addresses by taking steps to ensure that it has sufficient IPv4 address space. Even if a National Internet Registry was set up, it is unlikely that such a registry would be able to overcome the administrative and numbering policy hurdles within the next few years to solve the problem. One of the alternatives is for the regulator to encourage local ISPs to reduce the "cost" of IPv4 addresses and encourage businesses that rely on the Internet number resources to provision 50% of the IPv4 address space they need within the next year.

The deployment of IPv6 is crippled by the lack of a business case for its adoption. Some countries have tried to address that by mandating that government procurements for network services should require IPv6.

- http://www.icta.mu/documents/Consultation_IPv6.pdf
- http://www.rfc-editor.org/rfc/rfc4291.txt
- http://www.nro.net/wp-content/uploads/nro-response-to-ls-5.pdf
- http://www.apnic.net/publications/press/releases/2011/finalslash8.pdf

4) **Respondent 4**

The fourth respondent commends the ICTA for organizing this consultation which aims at raising the level of awareness within the local community on the issue of IPv4 to IPv6 transition and empowering operators in the public and private sectors to participate and collaborate on the national strategy on the matter forward. They firmly believe in the multi-stakeholder approach on Internet development and governance issues.

They also believe that governments, policy makers and regulators have a very important role to help the different sectors within its nation to overcome any potential burdens that may affect the progress of the country toward a better Internet appropriation as tool for socio-economical development. IPv6, if adopted in a timely manner would be a great innovation and economic opportunity for the entire African region.

6. List of Abbreviations

ADSL – Asymmetric Digital Subscriber Line

CIDR - Classless Inter-Domain Routing

CPE – Customer-premises equipment

DHCPv6 – Dynamic Host Configuration Protocol for IPv6

DNS – Domain Name System

HTTP – Hypertext Transfer Protocol

IANA - Internet Assigned Numbers Authority

ICANN – Internet Corporation for Assigned Names and Numbers

IETF - Internet Engineering Task Force

IMAP – Internet message application protocol

IP - Internet Protocol

IPng - IP next generation

ISP – Internet service providers

LIR - Local Internet Registry

NAT- Network Address Translation

NAT-PT – Network Address Translation/Protocol Translation

NCP – Network Control Protocol

Nemo - Network Mobility

NIR – National Internet Registry

PDA – Personal digital assistant

PI – Provider Independent

POP – Post Office Protocol

PPPoE – Point-to-Point Protocol over Ethernet

QoS – Quality of Service

RADIUS – Remote Authentication Dial In User Service

RIRs - Regional Internet Registries

SMTP – Simple Mail Transfer Protocol

SWIP – Shared Whois Project

TDM - Time-division multiplexing

VoIP – Voice over Internet Protocol

xDSL – Digital Subscriber Line (collectively to the various types of digital subscriber technologies, such as ADSL, SDSL and HDSL).