Outcomes of Public Consultation

ICTA
INFORMATION & COMMUNICATION
TECHNOLOGIES AUTHORITY

Transition from IPv4 to IPv6

Trilok Dabeesing
Director of IT
ICTA
22 September 2011

Agenda

1. IPv4 consumption in Mauritius
2. Recommendations from Public Consultation exercise
3. Compiled results of technical survey with local ISPs
4. IPv6 deployment issues
5. Who are involved in the IPv6 transition process?
6. Way forward

Launching of Public Consultation in March 2011

•Project identified under the NICTSP

•Approach adopted by the regulator: Public Consultation

•IPv4 consumption in the region and in Mauritius

  •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.

  •Around 0,5 million IPv4 addresses have been allocated in Mauritius

Should the regulator play a regulatory role in the transition from IPv4 to IPv6?

- Technology-neutral, light-handed approach

- Instead an IPv6 sensitisation campaign involving the different stakeholders within the Mauritian context recommended:
  - No consumer demand for IPv6
  - Implementation of the transition solution is not a present priority for local ISPs

- Government to provide an initial form of catalyst by creating awareness

- Private sector organisations to be sensitised to undertake careful analysis of their business cases for IPv6 adoption

What regulatory steps and policy initiatives, you believe are required?

- Setting up a National IPv6 Task Force in order to look into key IPv6 issues focusing on key areas such as:
  - Awareness creation,
  - Capacity building
  - Security
  - Research and Policy development.

- It is proposed that Government leads the way by example
  - Designate an IPv6 Transition Public Agency
  - Upgrade public facing servers and services to operationally use native IPv6 by the end of 2013
  - 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

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

- The transition to IPv6 from IPv4 will be a gradual process, during which the two protocols are expected to coexist for several years.
  - Dual Stack – In this the network stack supports both IPv4 and IPv6.
    - a host has access to both IPv4 and IPv6 resources
    - dual-stack machines can use IPv4 when communicating with native IPv4 hosts, or IPv6 when communicating with IPv6 hosts.
  - Tunneling – In this the IPv6 packets are encapsulated within IPv4 packets using protocol number 41.
    - allows IPv6 hosts to communicate via intervening IPv4 networks
  - Translation – Protocol translation between IPv4 and IPv6 are performed.
    - enable communication between IPv4 and IPv6-only domains,
  - Recommendation
    - 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.

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

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

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

- IP addresses are managed regionally and in a hierarchical manner
  - RIRs receive allocations from IANA
    - Currently in /12 units (A /12 is a block 1,048,576 times the size of the minimum allocation made by RIRs to ISPs)
  - 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 264 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)

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

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

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

- **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.

  - Having a separate authority managing IP address will not remove the need by operators that receive these addresses to apply their own policy in the way they assign them to their customers.

  - No problem has been flagged out in the allocation of IP addresses from AfriNIC to its Mauritian members.

  - However the policy used by LIRs (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.

Regulatory issues related to transition from IPv4 to IPv6

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

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

- 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.

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 with a view to moving towards commercial IPv6 based services.

- Possible reasons
  - No business drivers
  - No flag date by which the transition must be achieved

- Issues
  - 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.
  - If precautions aren't taken, the transition from IPv4 to IPv6 could be cause for network security concerns.

- 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.

  - This proposal can be examined at the level of the National IPv6 Task Force and eventually be referred to the USF Ministerial Committee for its consideration.

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

- NAT boxes break the end-to-end nature of Internet communications, and thus interfere with some Internet applications and services

- 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.

Technical survey to assess state of readiness of local ISPs

•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.

•Only 2 ISPs include support for DNS AAAA queries over IPv6 and for reverse DNS for IPv6 addresses.

Technical survey results

- Product issues
- Numerous models of various types of product still do not support IPv6:
  - CPE devices
  - DSLAMs
  - Routers
  - ADSL Modems
  - BAS
  - Switches
  - Firewalls
  - Intrusion detection systems
  - Accounting and billing systems
- Security considerations
  - Most of firewall and intrusion detection products for ISPs are still reported not to support IPv6.

ICTA experience in making its web server IPv6 ready

- **Network Side:**
  - Request IPv6 block of address with ISP
  - Configure router (SHDSL) with IPv6 – via tunneling
  - Configure firewall to support IPv6 in dual stack mode.
  - Add rule to allow IPv6 traffic on port 80 to access the Web server
  - Add AAAA record on DNS

- **Web Server Side:**
  - Enable IPv6 on the Network Interface Card (NIC) of the Web Server
  - Assign an IPv6 address on the NIC based on the block allocated by the ISP
  - Configure the Web Server Software to listen to a new address, i.e the IPv6 address

- **Problems encountered:**
  - Tunneling is slow and erratic in connectivity
  - Major modifications had to be performed on the firewall (Updating of firmware and software)
  - Firewall rules had to be modified to allow the IPv6 traffic.
  - Limited support from local firewall suppliers.
  - Only firewall is IPv6 compliant. Whereas other features such as IDS, and Mail Gateway are not compliant with IPv6.

Some thoughts on deployment of IPv6

- IPv6 has a number of benefits built into its far-larger address space. But all of these new features come at a price – good implementation practices.
- Main differentiator with IPv4
  - An IPv6 address has two parts,
    - the prefix assigned by the individual network, and
    - the access assignment value dynamically generated by each device.
- As a result, a device can have its IPv6 address refreshed as often as every 24 to 48 hours
- The dynamically changing IP addresses also mean IT managers won't be able to just mechanically map existing security policies to apply to IPv6 networks
  - Need to be redesigned to fit with IPv6's new packet structure and how the addresses are generated
- Organisations have to test the firewall to ensure the new policies handle IPv6 correctly.

Some thoughts on deployment of IPv6

- ISPs cannot treat IPv6 like it's the same as IPv4 with just more addresses
  - IPv6 offers hierarchical addressing, where the addresses can be assigned to a single device, as well as to multiple devices within a group,
  - The addresses also contain fields for quality-of-service support.
  - IPv6 also allows mobile devices to dynamically change addresses as their locations change without losing existing connections to the network
- All these things need to be considered when developing firewall rules and network policies
- IPv6 packets also have extension headers developed to improve performance by simplifying the overall structure
  - Since these headers are optional and can be used in different ways, security protocols on firewalls and other network devices need to be able to understand the variations
- The dual stack rolled out by ISPs, where customers have both a IPv4 and IPv6 address, also pose security challenges
  - Network administrators have to create firewall rules so that attackers cannot just stroll right through the hole on the IPv6 side

Who are involved in the IPv6 transition process?

Internet organisations – This includes ICANN, RIRs, and IETF who manage common IPv6 resources and services.

ISPs – ISP’s need to offer IPv6 connectivity and IPv6 based services to their customers.

Infrastructure vendors – Vendors who manufacture network equipment, operating systems & network application software.

Business and consumer application vendors – Manufacturers of business software, need to ensure that their solutions are IPv6 compatible.

End-users – This includes consumers, companies, academia, and public administrations.

Proposed structure of the National IPv6 Task Force

- Setting up of IPv6 National Task Force
  - **Oversight committee**
    - apex body for making policy decisions
    - Its role will be to provide the strategic national directions for IPv6 in Mauritius
  - **Steering committee**
    - To oversee the activities of the different working groups constituted under the Task Force for timely smooth transition in the country
  - **Working groups (**Each Working group will be responsible for specific activities associated with transition to IPv6)
    - Training and awareness working group
    - IPv6 network implementation working group
    - Standards and specifications working group
    - IPv6 implementation in government working group
    - Applications support working group
    - Security working group

Thank You

ICTA
INFORMATION & COMMUNICATION
TECHNOLOGIES AUTHORITY