ICTA

INFORMATION & COMMUNICATION
TECHNOLOGIES AUTHORITY

IPv6 GUIDE for BUSINESSES

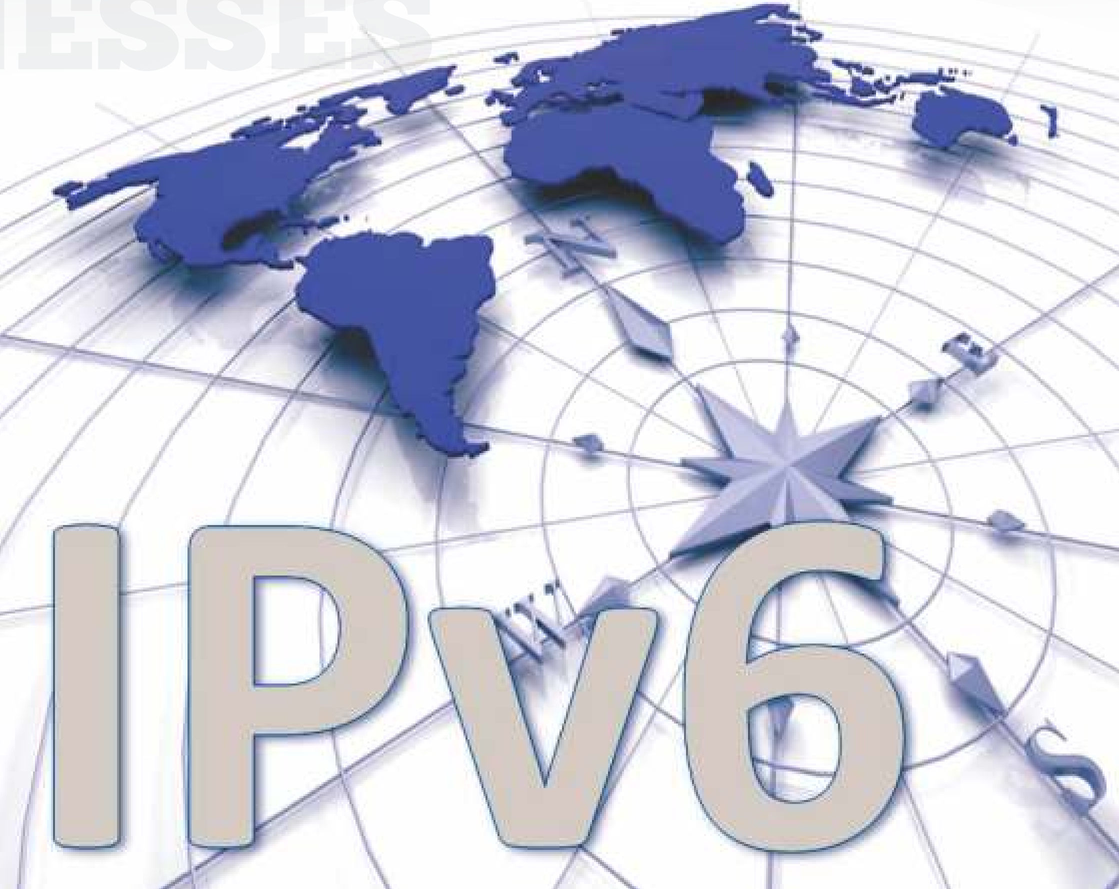

Table of Contents

List of Abbreviations

AAA	>	Authentication, Authorization and Accounting
BGP	>	Border Gateway Protocol
DHCP	>	Dynamic Host Configuration Protocol
DNS	>	Domain Name System
HTTP	>	Hypertext Transfer Protocol
IANA	>	Internet Assigned Numbers Authority
IMAP	>	Internet Message Access Protocol
IPv4	>	Internet Protocol Version 4
IPv6	>	Internet Protocol Version 6
MIB	>	Management Information Base
MRTG	>	Multi Router Traffic Grapher
OSPF	>	Open Shortest Path First
POP3	>	Post Office Protocol 3
RIR	>	Regional Internet Registry
ROI	>	Return on Investment
SMTP	>	Simple Mail Transfer Protocol
SNMP	>	Simple Network Management Protocol
VPN	>	Virtual Private Network

Introduction

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

In March 2011, the ICT Authority issued a Consultation Paper on "Issues pertaining to Transition from IPv4 to IPv6 in Mauritius" highlighting the need for migration to IPv6. Thereafter, in September 2011, the Authority came out with a set of recommendations which were based on the written responses received following the public consultation exercise. The main conclusion is that migration to IPv6 should not be mandated but facilitated by the Government and a set of recommendations was proposed.

Against this backdrop, the Authority in an effort to encourage the adoption of IPv6 in Mauritius is issuing this IPv6 Guide for Businesses on the 6th of June 2012 when major ISPs, home networking equipment manufacturers, and web companies around the world are coming together to permanently enable IPv6 for their products and services. The ICT Authority has also permanently IPv6 enabled its website (www.icta.mu) and has registered in the participants' list of the World IPv6 launch event organised by the Internet Society (www.worldipv6launch.com).

The present Guide highlights the steps to be followed by an organisation going for IPv6 adoption. The planning and implementation phases of an IPv6 adoption effort can be optimised once an organisation is in a position to assess where it currently stands as far as IPv6 is concerned. The purpose of the IPv6 Guide for Businesses is to describe the planning and implementation steps required for the deployment of IPv6 at the level of the organisation.

1. Request for IPv6 address space

In general, there are two sources from which IPv6 address space can be obtained; they are:

1) An Internet Service Provider. In this case, IPv6 addresses are not portable and must be surrendered back to the service provider once the end user decides to change the provider.

2) The Regional Internet Registry (RIR), which is AfriNIC in Mauritius. To receive IPv6 address space directly from AfriNIC, a requester needs to become a paying member of AfriNIC.

2. IPv6 Adoption Plan Guidelines

This section presents a high level overview of the required and necessary steps by an organisation to adopt IPv6. The steps are gathered along two major tracks:

- Business Planning: This covers the business case of the organisation by taking into account the drivers and economic value of adopting IPv6.
- Technical Planning: which covers technical aspects of the organisation's ICT infrastructure towards IPv6 interoperability.

3. Business Planning

The Business Planning phase of the IPv6 adoption consists of four activities:

- Identify Business Drivers;
- Identify Benefits, Costs, Risks;
- Develop a Business Case for IPv6; and
- Establish an IPv6 Transition Group

3.1 Identify Business Drivers

Stakeholders should identify reasons and drivers for the adoption of IPv6 and establish a connection that links business goals and requirements to IPv6 interoperability. Though different types of stakeholders would establish different drivers, the following list includes a common set of business requirements and drivers behind IPv6 adoption and implementation:

- IPv4 Address Exhaustion: The availability of IP addressing secures business continuity since IPv6 is the only long term solution once IPv4 is depleted.
- Governmental mandates to implement and adopt IPv6 in the public sector will drive stakeholders such as service providers and vendors already dealing with the government to speed up plans for IPv6 adoption.
- The prospects of new applications requiring IPv6 large address pool such as secure peer-to-peer applications and others.

3.2 Identify Benefits, Costs, Risks

3.2.1 Benefits

Organisations should identify how IPv6 benefits and enables particular lines of business and programmes. Organisations should identify how IPv6 will:

- Increase business opportunities (maintain existing services and create new ones)
- Improve network efficiency, performance, cost savings (removal of NAT and more efficient address space management for example)
- Simplify operations (auto-configuration features)
- Provide a strategic and advantageous position towards other competitors.

3.2.2 Costs

Organisations should identify costs incurred by an IPv6 adoption plan in terms of:

- Planning and engineering the adoption plan such as: design, implementation, testing, deployment and other IT/Networking technical operations.
- Operational and running costs resulting from running IPv6 networks side by side with the existing IPv4 infrastructure.
- Procurement costs of required infrastructure changes and upgrades. Best practices have shown that costs in this regard would be of minimal economic impact if such upgrades and changes are done as part of the ICT life cycle management process and costs in this area are related to:
  - Hardware and Software
  - Applications
  - Network Management Systems

3.2.3 Human and personnel training related costs

As with the introduction of any new technology, it is expected that IPv6 will incur costs at the personnel level as a result of the challenges and time associated with the changes in business practices. These can be identified as costs of:

- Training and educating ICT personnel on the IPv6 technology
- Costs incurred by the possibility of lower productivity during the period of adjustment in terms of both provisioning of new services and product development.

3.2.4 Risks

Organisations should perform an analysis to identify risks associated with an IPv6 adoption plan. For each type of risk, mitigation measures should be established in order to prevent those risks as well as contingency measures that would minimise the impacts in the event those risks happen and occur. These include: business, legal and technical risks.

Business

Organisations should establish a Return on Investment (ROI) study on costs incurred by implementing IPv6, taking into account the growing costs for continued usage of IPv4.

Legal

Privacy risks may develop due to IPv6 unique identifiers. This might allow others to track and trace users' and clients' identities. Organisations and network operators should be aware of any legal requirements and safeguard their clients' identities and privacies.

Technical

Like any technology upgrade, technical risks can arise and these include:

- Security risks may develop if transition mechanisms are not implemented properly. Different transition mechanisms have different security problems, for example: IPv6 unwanted packets might be channeled through an IPv4 tunnel. Security devices that do not have filtering and inspection capabilities of IPv6 packets will allow IPv6 malicious packets through the network;
- Interoperability risks can arise between different types of IPv6 stacks, between IPv6 and other protocols and interoperability with the present IPv4 networks.

3.3 Develop a Business Case for IPv6

The business case can be formulated by making use of the already identified business drivers as well as benefits, costs and risks. The business case can justify the costs in terms of the identified benefits. In other words, the organisation can then decide if the costs incurred are worth the prospective return.

3.4 Establish an IPv6 Transition Group

Organisations can establish an IPv6 Transition group that will plan, coordinate, track and communicate progress of the IPv6 adoption project throughout the whole organisation. The IPv6 transition group shall establish and manage a governance structure to ensure a smooth and successful IPv6 transition. It shall also familiarise the organisation with IPv6 in general, IPv6 impact to their working areas and IPv6 importance to the organisation as a whole and ultimately build a sense of urgency for adopting IPv6. Governance can also address IPv6 procurement opportunities within the organisation and, for example, cover the inclusion of IPv6 in ICT procurement policies.

4. Technical Planning

An inventory of all IP based equipment and applications need to be undertaken to identify which assets of the current state infrastructure will need to be upgraded to support IPv6. Examples of assets to be assessed in the inventory include:

- Address allocation needs for both present and future;
- Network Hardware equipment: routers, switches, firewalls, intrusion detection systems and others;
- Network Services: DNS, DHCP, AAA, etc;
- Network Management Systems: MIBS, SNMP, NetFlow, MRTG, etc;
- Applications: Operating Systems, Databases, Operational and Business supports systems and applications, applications under procurement or under development;

5. IPv6 Addressing Plan

The IPv6 Addressing Plan will identify the organisation's IP addressing requirements in terms of allocation, management and acquisition covering the needs for the next few years to come based on their level of business activities and foreseen or forecasted IP address usage growth.

The addressing plan needs to consider the different sections of the organisation's network such as: the intranet, extranet, external sites not managed by the organisation, services such as Layer 3 VPNs and others. If the organisation provides IP connectivity to other organisations, these networks also need to be considered in the addressing plan.

6. IPv6 Routing

Organisations shall identify the changes required to support IPv6 routing in the existent IPv4 routing schema of their infrastructure.

The main consideration here is which routing protocols are in use (static, OSPF, BGP, etc) and what adaptations need to be made to enable IPv6 routing.

7. IPv6 Network Transition Mechanism and Strategies

Organisations shall consider that IPv4 and IPv6 will co-exist and run side by side for a long period of time when deciding which transition mechanism will be adopted to migrate into an IPv6 interoperable infrastructure without disrupting the existent IPv4 operation.

IPv6 network transition mechanisms fall into three main categories:

- Dual Stack: this mechanism allows any IP aware entity on the network (node, device, applications, etc) to support both IPv4 and IPv6 stacks;
- Tunneling: allows IPv6 packets to be sent over existing IPv4 networks by encapsulating them in IPv4 packets. This is usually used at the start of migration to IPv6. As IPv6 usage grows and becomes dominant, the few remaining IPv4 entities could use the opposite schema in encapsulating IPv4 packets or tunneling them through IPv6 packets;
- Translation: this mechanism allows the translation of an IP version to another and allows communication between an IPv4-only device and another IPv6-only device. Network Protocol Translators are used to implement this mechanism.

8. Network Services

Organisations should evaluate and understand the impact of IPv6 on network services and address such impacts. The following lists some of the major network services to be impacted by an IPv6 interoperability plan:

- Domain Name Service
- Dynamic Host Configuration Protocol (DHCP)
- Authentication, Authorisation & Accounting (AAA)

9. Security

IPv4 and IPv6 will coexist together for many years. During this overlapping period, a security model that takes into account both protocols must be planned and tested very carefully. Security models during the IPv4/IPv6 coexistence may look very different from the future IPv6 more dominant Internet and as such, organisations shall plan to evolve their security architecture throughout their IPv6 migration process. As the Internet moves towards "Next Generation Networks" and more and more IPv6 is deployed, it is expected that security should be built from the start and not redesigned with the introduction of every new type of application.

The organisation shall address threats that arise from the transition program itself. Examples of such threats include:

- Poorly implemented IPv6 stacks;
- Few network protection devices/tools support IPv6 such as Firewalls and Intrusion Detection. In such a case, malicious IPv6 packets encapsulated into IPv4 traffic can traverse the network and expose the organisation's network infrastructure to external threats. Special attention should be given to automated tunneling applications or services. To minimise these problems, mechanisms and policies need to be developed to provide more secured automated capabilities

- New types of attacks and threats
- Poorly implemented IPv6 routing protocols and routing plans
- Inconsistent IPv4/IPv6 security features
- Few IPv4 network management tools ported to IPv6

10. Applications

Organisations shall identify the applications they need to interoperate with IPv6. This includes operating systems, databases and application software. IPv6-ready applications can take advantage of IPv6-only network features like enhanced multicasting, anycast, and embedded IPSecurity (IPsec). Application development environments need new IPv6 libraries and APIs so developers can access IPv6 networking features. Applications need to be audited to determine the level of existing support for IPv6 and the scope of work required for the transition.

11. Training and Awareness Planning

IPv6 training shall address business and technical aspects of the IPv6 migration project. Training shall include all personnel involved in the migration process and address both technical and business (decision making) personnel.

The developed training plan shall address and specify:

- The target audience and who needs to be trained (engineers, programmers, decision makers, managers, etc.)

- The training content and material in terms of:
  - Awareness: this type of training gives a general overview of IPv6 as a technology, the business drivers and needs behind IPv6, general deployment aspects and overview of potential benefits /applications / services introduced by IPv6.
  - Architectural training provides detailed information about IPv6 and it targets IT/Networking personnel who will design, implement and test IPv6.
  - Operational training will address personnel whose primary responsibility is to manage and operate IPv6 capable networks.
  - Specialised training targets subject matter experts and is geared towards specific, and focused IPv6 related aspects such as mobility, security and other specific areas.

12. Web facing servers

As a first phase of adopting IPv6 usage within the organisation, it is important that users are able to reach the “Internet face” of the organisation, namely its HTTP servers and E-Mail over IPv6.

12.1 HTTP servers

For the HTTP server, the necessary effort depends on the size of the HTTP platform and hardware and software used. In the easiest case, a standard HTTP server is used (Microsoft IIS or Apache 2.0 and up) on a single server. In this case, the necessary effort to make the site accessible over IPv6 is fairly small:

- enable IPv6 connectivity towards the machine (dual-stack IPv4 and IPv6 network);

- turn on IPv6 networking in the server machine's network configuration;
- enable IPv6 (if necessary) in the web server configuration;
- test the setup from an IPv6-enabled client, making sure that no parts of the application assume IPv4 addresses (in cookies, access permissions, logging) – if any IPv4 dependency is found, the respective part of the software needs to be upgraded, but for a "basic" web site this is usually fairly straightforward; and
- enter the IPv6 address of the machine (AAAA record) into the DNS server.

12.2 E-Mail

E-mail servers need to be IPv4 and IPv6 capable. The E-Mail protocols themselves (SMTP, POP3 and IMAP) are agnostic to the question of IPv4 or IPv6, so this boils down to providing reliable IPv6 transport to the machines, and verifying IPv6 support in the applications in use.

The necessary steps are very similar to what needs to be done for HTTP servers:

- Enable IPv6 connectivity to the server.
- Check the products in use for IPv6 support for mail transport – working solutions include, for example, Microsoft Exchange on Windows Server 2008, or sendmail, exim or postfix on Linux.
- Besides mail transport, it might be necessary to check any sort of IPv4-based logging, statistics or anti-spamming (like "greylisting") tool in use for IPv6 capability.
- Enable global IPv6 visibility by adding an AAAA record to the DNS.

For E-mail, a special caveat applies: some setups use anti-spam filtering in the form of dedicated appliances that receive the e-mail first, before handling it to the actual e-mail servers. If such appliances are in use, an organisation needs to make sure that the anti-spam vendor will offer full IPv6 transport (which relates to the ICT procurement policies). It is especially important to point this out to the vendors early in the process so that the roll-out of IPv6-enabled E-Mail Services are not hindered by vendors that are slow to upgrade their appliances.

Conclusion

It is hoped that this guide will be a useful instrument that can assist organisations in their endeavour to adopt IPv6. For any further queries and/or suggestions that may arise, the Authority has set up a dedicated discussion forum accessible on its website (www.icta.mu) where active participation of different stakeholders is strongly encouraged.

ICTA

INFORMATION & COMMUNICATION
TECHNOLOGIES AUTHORITY

Information & Communication Technologies Authority

Level 12, The Celicourt
6, Sir Celicourt Antelme Street, Port Louis, Mauritius

Tel: (+230) 211 5333/4 | Fax: (+230) 211 9444
E-mail: icta@intnet.mu | Website: www.icta.mu