EACO East African Communications Organisation

Communications for all in East Africa

EAST AFRICA REGIONAL STRATEGY ON MIGRATION FROM IPv4 TO IPv6

Prepared by EACO

July 2021

Contents

ACROYNMS

AFRINIC	African Network Information Centre
ALGs	Application-Level Gateways
AH	Authentication Header
ccTLD	country code top-level domain
CPE	Customer Premise Equipment
DSTM	Dual Stack Transition Mechanism
EAC	East African Community
EGP	Exterior Gateway Protocols
ESP	Encapsulating Security Payload
IANA	Internet Assigned Numbers Authority
IDA	Infocomm Development Authority
IETF	Internet Engineering Task Force
IGOP	Interior Gateway Protocols
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPV6	Internet Protocol version 6
IPSec	Internet Protocol Security
ISP	Internet Service Provider
MIPv6	Mobile IPv6
NAT	Network Address Translation
NAT-PT	Network Address Translation - Protocol Translation
NAv6	National Advanced IPv6 Centre
ND	Neighbor Discovery
NGTrans	Next Generation Transition

NIST	National Institute of Standards and Technology
NMS	Network Management Systems
OGCIO	Office of the Government Chief Information Officer
PA	Provider Aggregateable
PI	Provider Independent
PTR	Pointer Record
RIR	Regional Internet Registries
ROI	Return on Investment
RR	Resource Records
SIIT	Stateless IP/ICMP Translation
SLAAC	Stateless Address Auto-configuration
TCP	Transmission Control Protocol
TLD	Top Level Domain
VoIP	Voice over IP

EAST AFRICA REGIONAL STRATEGY ON MIGRATION FROM IPv4 TO IPv6

1. BACKGROUND

In February 2011, the Internet Assigned Numbers Authority (IANA)allocated two large blocks of Internet Protocol version 4 (IPv4) address space to APNIC – the Regional Internet Registries (RIR) for the Asia Pacific Region - causing the global IPv4 pool to deplete to a critically low level. This triggered the "Global Policy for the Allocation of the Remaining IPv4 Address Space". Each RIR then received one /8 each - 'the final /8' - which is around 16.8 million IPv4 addresses, depleting IANA's pool of available IPv4 address space and setting the ball rolling for global IPv4 exhaustion.

The five RIRs continued to distribute IPv4 address space as per their own regional, community-developed policies and, in April 2011, APNIC was the first RIR to exhaust its free pool of IPv4 space, meaning it had no more IPv4 address space left to allocate to its members except for those addresses it had received in the final /8. The RIPE NCC (Europe, the Middle East and parts of Central Asia) followed quickly in 2012. LACNIC (Latin America and the Caribbean) reached its final /8 in June 2014 and, in September 2015, ARIN allocated the final IPv4 addresses in its free pool, leaving African Network Information Centre (AFRINIC) as the only RIR with an as-yet unrestricted pool of IPv4 address space from which to allocate to its members. All this changed on 31 March 2017.

RIR members in other regions are no longer able to request IPv4 address space from their RIR unless they meet specific requirement. RIPE NCC Members, for example, can get a one-time /22 (1,024 addresses) but they must already have an IPv6 allocation to be eligible. IPv4 Transfers, within and between regions, are permitted in some of the RIR regions but there is no provision for transfers within, in or out of the AFRINIC region.

On 31 March 2017, AFRINIC hit a historic milestone as it announced that it had reached Phase 1 of its IPv4 Exhaustion process. As the last of the world's five Regional Internet Registries (RIRs) to begin allocating IPv4 address space from the final /8 of address space it received from the IANA in 2011, this marks a historic turning point in the evolution of the Internet.

It is difficult to predict how long AFRINIC's /8 of IPv4 space will last and, now that AFRINIC is in Phase 1 of IPv4 exhaustion, it is now more important than ever that all members understand the urgent need for IPv6 deployment. As of September 2017, over 40% of the membership has an IPv6 allocation, which is currently free of charge, but only 352,583,680/64 out of 152,521,885,696/64 allocations are advertised **(0.002%).** As obtaining IPv4 address space in Africa is set to become more difficult, more and more network operators will hopefully kick their IPv6 deployment plans. There is a policy in process to mandate the acquisition of IPv6 bloc when requesting IPv4 in the soft landing period at AFRINIC. To crystallize Government's efforts in sustaining the effective operation of the Internet in the East African region, the NRAs should issue a consultation paper on issues pertaining to Transition from IPv4 to IPv6 in their respective countries highlighting the need for migration to IPv6. The following are recommendations from some NRAs that carried out the assessment.

a. ISPs should acquire, deploy the IPv6 in their core network because some software and equipment for customers are IPv6 compliant.
b. The regulatory authority to develop the roadmap and hold the consultation with ISPs to acquire the IPv6 and implement them.
c. The regulatory authority will 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.
d. The regulatory authority will also be prepared to consider and introduce regulatory measures to ensure that consumers' interests are met such as the Internet access services provided to consumers should be capable of allowing end users on either address type (IPv4 or IPv6) to access content regardless of its address type.

2. EXECUTIVE SUMMARY

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).

IPv6 is the next-generation Internet protocol that will replace IPv4, providing a vastly expanded address space. Mobile IPv6 (MIPv6) is used to ensure a continuous IP connectivity for mobile devices, such as laptops, PDAs and smart phones. The security aspects have been already considered at the beginning of IPv6 development.

This model guideline is written on the foundation laid down by the AFRNIC guide for migration to IPv6.

The East African Community (EAC) IPv6 ecosystem consists of many stakeholders like Government organizations, Internet service providers, content and application providers, equipment manufacturers, cloud computing / data centers providers etc. On the road to IPv6 adoption, it is to be ensured that all stakeholders perform the IPv6 journey in a coordinated manner. The transition from IPv4 to IPv6 is a popular issue and one, which the industry will spend more time managing in the coming years. The transition is complex and will require IPv6 support by an end-to-end industry ecosystem. The ecosystem includes customer premise equipment, modems/home gateways, network systems, management (OSS/BSS, tools), content and applications.

2.1 The Role of Government

The EACO Members States are currently focused on achieving high penetration of next generation broadband and mobile networks. These infrastructures will help achieve more societies that are inclusive and give national economies a competitive edge. The steady growth of broadband and mobile networks, leading to universal network access, requires an adequate supply of IP addresses. Broadband and mobile network deployment planning checklists must include IPv6 readiness at the service provider level. Government also needs to make sure its electronic government services support IPv6 for equal accessibility across their population and encourage collaboration between public and private sectors.

2.2 Internet Service Provider Decision Makers

Service providers play a key role in IPv6 deployment. Networks are growing rapidly with higher subscription rates, and service providers need to think about sustaining future growth without relying on IPv4. The most effective way to manage the shortage of IPv4 addresses is to allow networks to support both IPv4 and IPv6 simultaneously. Providers should consider how to extend the life of their IPv4 address pools while enabling customers to connect via IPv6. There may be risks associated with delaying IPv6 deployment, so it is advised that decision makers consider IPv6 when planning for the short, mid, and long term to enable IPv6 access via Customer Premise Equipment (CPE).

2.3 Mobile network service provider decision-makers

The mobile market is growing rapidly. Mobile devices may access networks via wireless or mobile networks. One mobile handset, such as a smartphone or a tablet, may easily require at least two IP addresses. The increase of mobile handset usage has created a huge demand for IP addresses, which will significantly increase the costs and scalability issues associated with mobile network services. IPv6 provides a long-term scalable solution and lower maintenance than IPv4 deployed in NAT environments.

2.4 Enterprise Decision Makers

Businesses with an online presence should prepare for an increase of customers accessing their online content from mobile devices. Some of these new users may require access via IPv6 in the future. To prepare for these new users, enterprises must ensure their service, hosting, and application providers, as well as system integrators, are IPv6-ready.

3. INTERNATIONAL BENCHMARKING OF IPV6 STRATEGIES

In preparing this strategy, we have referred to international best practice in the promotion of IPv6, taking account of the EAC context. A number of examples of how governments elsewhere have become involved in promoting the adoption of IPv6 are summarized below:

a. The Infocomm Development Authority of Singapore (IDA) launched its 'IPv6 transition programme' to encourage IPv6 adoption and it has been running for the last two years. The programme is a national effort to address the issue of IPv4 exhaustion and to facilitate the smooth transition of the Singapore ICT ecosystem to IPv6. IPv6 transition programme promotes readiness for, and adoption of, IPv6 in the local industry through a series of projects (training, grants, events, etc.).

b. The Indian government has established an IPv6 task force and stated that all ISPs and telecoms companies should be 'IPv6 compliant' and offer IPv6-based services by the end of 2011. In addition, federal government agencies and state governments were required to adopt the new version of the protocol by March 2012.

c. The Malaysian government established the National Advanced IPv6 Centre (NAv6) in 2005. It serves as the national centre for IPv6 research, human resource development and monitoring of IPv6 development for Malaysia. As part of its mission, NAv6 planned and implemented appropriate programmes designed to meet a target of the end of 2010 for Malaysia to be an IPv6-enabled nation. By March 2010, the NAv6 was claiming that "Malaysia has made good progress, but are still a long way to go".

d. The Hong Kong government has IPv6-enabled the majority of its Web services, with 85% of government sites reported as IPv6 ready in Q1 2011.3 In March 2013 the Office of the Government Chief Information Officer (OGCIO) claimed "the Internet Infrastructure in Hong Kong is ready for IPv6 deployment".

4. TECHNICAL BENEFITS

4.1 Increased Address Space

The main difference between the IPv6 and IPv4 protocols is that IPv6 uses addresses that are 128-bits long (96-bits more than IPv4). An IPv6 address is written in hexadecimal notation, such as 2001:db8:74a3:0042:1000:4e2e:0370:7328. IPv6 provides 3.4 x 1038 = 340 trillion trillion trillion addresses - about 670 quadrillion addresses per square millimetre of the Earth's surface.

4.2 Security

IPv4 also offers Internet Protocol Security (IPSec) support. However, IPv4's support for IPSec is optional. By contrast, the RFC 4301 mandates for IPv6 to use IPSec in all nodes. IPSec consists of a set of cryptographic protocols that provide for securing data communication and key exchange. IPSec uses two wire-level protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). The first protocol provides for authentication and data integrity. The second protocol provides for authentication, data integrity, and confidentiality. In IPv6 networks both the AH header and the ESP header are defined as extension headers. Additionally, IPSec provides for a third suite of protocols for protocol negotiation and key exchange management known as the Internet Key Exchange (IKE). This protocol suite provides the initial functionality needed to establish and negotiating security parameters between endpoints. Additionally, it keeps track of this information to guarantee that communication continues to be secure up to the end.

4.3 Mobility

Mobile IPv6 (MIPv6) is an enhanced protocol supporting roaming for a mobile node, so that it can move from one network to another without losing IP-layer connectivity (as defined in RFC 3775). RFC 3344, IP Mobility Support for IPv4, describes Mobile IP concepts and specifications for IPv4. Nevertheless, using Mobile IP with IPv4 has various limitations, such as limited address space, dependence on address resolution protocol (ARP), and challenges with handover when a device moves from one access point to another. Mobile IPv6 uses IPv6's vast address space and Neighbor Discovery (RFC 4861) to solve the handover problem at the network layer and maintain connections to applications and services if a device changes its temporary IP address. Mobile IPv6 also introduces new security concerns such as route optimization (RFC 4449) where data flow between the home agent and mobile node will need to be appropriately secured.

4.4 Quality of Services (QoS)

IP (for the most part) treats all packets alike, as they are forwarded with best effort treatment and no guarantee for delivery through the network. TCP (Transmission Control Protocol) adds delivery confirmations but has no options to control parameters such as delay or bandwidth allocation. QoS offers enhanced policy-based networking options to prioritize the delivery of information. Existing IPv4 and IPv6 implementations use similar QoS capabilities, such as Differentiated Services and Integrated Services, to identify and prioritize IP-based communications during periods of network congestion. Within the IPv6 header, two fields can be used for QoS, the Traffic Class and Flow Label fields. The new Flow Label field and enlarged Traffic Class field in the main IPv6 header allow more efficient and better differentiations of various types of traffic. The new Flow Label field can contain a label identifying or prioritizing a certain packet flow such as voice over IP (VoIP) or videoconferencing, both of which are sensitive to timely delivery. IPv6 QoS is still a work in progress.

4.5 Route Aggregations

IPv6 incorporates a hierarchal addressing structure and has a simplified header allowing for improved routing of information from a source to a destination. The large amount of address space allows organizations with large numbers of connections to obtain blocks of contiguous address space. Contiguous address space allows organizations to aggregate addresses under one prefix for identification on the Internet. This structured approach to addressing reduces the amount of information Internet routers must maintain and store and promotes faster routing of data. Additionally, it is envisioned that IPv6 addresses will primarily be allocated only from Internet Service Providers (ISPs) to customers. This will allow ISPs to summarize route advertisements to minimize the size of the IPv6 Internet routing tables, which eventually increases routing efficiency.

4.6 Neighbor Discovery and Address Auto-Configuration

Neighbor Discovery (ND) is the mechanism responsible for router and prefix discovery, duplicate address and network un-reachability detection, parameter discovery, and link-layer address resolution. This protocol is entirely network-layer based. ND operates in tandem with auto-configuration, which is the mechanism used by IPv6 nodes to acquire either stateful or stateless configuration information. In the stateless mode, all nodes get what they need for global communication, including potential illegal ones. In stateful mode, configuration information can be provided selectively, reducing the possibility for rogue nodes. Both ND and address auto-configuration contribute to make IPv6 more secure than its predecessor. IPv6 provides for TTL values of up to 255; it prevents against outside sourcing of ND packets or duplicate addresses.

5. DRAWBACKS OF TRANSITIONING TECHNIQUES

Apart from Dual-Stacking, all the transition technologies described in this guideline impose certain limitations in the form of reducing network capacity or speed by introducing additional processing and overhead. Or, in case of translation or address sharing, the need for Application Layer Gateways (ALG) could restrict further innovation and the deployment of new protocols and services throughout the Internet. These technologies should only be deployed when there are no alternatives available and used only temporary for as long as the need exists. Whenever possible the use of Dual Stack is recommended.

6. IPV6 IMPLEMENTATION CONSIDERATION

6.1 Equipment

Equipment that are old will potentially have issues supporting IPv6. Major reinvestment is required for replacement. The above shortcomings should be taken into consideration by organizations when they do the network infrastructure planning in the course of their IPv6 transition.

6.2 Dual Stack

It is imperative to have system supporting dual stack implementation. Connectivity on pure IPv6 will be meaningless as content are primarily hosted on IPv4 network. Dual stack platform allows gradual migration from IPv4 to IPv6.

6.3 Local Domain (ccTLD)

Local domain is crucial and imperative to encourage the domain migration for local content hosts. Therefore, country code top-level domain (ccTLD) domain registry plays an important role to support the IPv6 implementation for local domain. If this is not addressed, it will hinder the migration plan.

6.4 IPv6 Features

IPv4 and IPv6 are not compatible with each other. So, IPv6 software patches may not compliment the features available in IPv4. As such, people involved in IPv6 network infrastructure planning should do relevant study to decide on the features to be included in their organizations production network.

6.5 Native IPv6 Support

Implementer shall prioritize implementation of IPv6 on a new network since the native protocols are more stable and reliable.

6.6 IPv6 Cost

Though IPv6 software patches are made available free by vendors, minimum hardware upgrade is unavoidable. If proper planning is made, most of the hardware upgrades cost for IPv6 implementation could be absorbed through the natural upgrade/purchase cycle performed by organizations.

7. IPV6 READINESS LEVEL ASSESSMENT GUIDELINE

The IPv6 Readiness Assessment aims to evaluate a high-level view of where the organization stands in general in terms of IPv6 readiness. An organization would be identified in a certain level if it satisfies a set of particular criteria of that level. These criteria would be aspects related to elements such as presence of IPv6 plans, development of an IPv6 business case, establishment of IPv6 training courses and other high-level business oriented rather than technical aspects of IPv6. Five (5) levels of readiness are identified with level Zero (0) being the lowest level and level Four (4) the highest level of IPv6 readiness respectively.

- **Level 0**

An organization would be characterized as being in Level 0 IPv6 readiness if it has neither considered the implementation of IPv6 in its infrastructure nor the implications of the IPv4 exhaustion problem.

- **Level 1**

An organization would be characterized as being in Level 1 IPv6 readiness if it is actively considering IPv6 migration or IPv4 address exhaustion but has not yet prepared a plan to adopt IPv6. It is recommended that organizations at Level 1 to start the following activities:

a. Consultations of internal or external IPv6 expertise to establish recommendations regarding IPv6 migration or contingency measures to address the IPv4 exhaustion problem
b. Discussions of IPv6 migration or IPv4 exhaustion implications at senior and decision making levels involving senior business and technical personnel
c. Identification of business drivers for IPv6
d. Identification of associated costs and risks in regards to a move towards IPv6

- **Level 2**

An organization would be characterized as being in Level 2 IPv6 readiness if it has an IPv6 adoption plan in place and has just started identifying critical issues (IPv6 Technical Architecture Design). It is recommended that organizations at Level 2 start the following activities:

a. Development of an IPv6 business case with timescales for implementing IPv6 along with a dedicated needed budget for IPv6 migration
b. Establishment of an IPv6 Transition Group that would plan, co-ordinate, track and communicate the progress of the IPv6 program across the organization
c. Identification of critical issues through inventorying the infrastructure for IPv6 capabilities and impacted sectors

d. Development of the IPv6 infrastructure design, IPv6 deployment plan, IPv6 training plans and IPv6 testing plan

- **Level 3**

An organization would be characterized as being in Level 3 IPv6 readiness if it has an IPv6 plan in place along with a complete plan to address critical issues (as opposed to only identifying them in the previous level 2). Organizations at Level 3 are expected to already have a funded IPv6 program that is working on inventorying the infrastructure and identifying the IPv6 impacts to and current IPv6 capabilities of the infrastructure. It is also expected that the organization has engaged in a lab testing of the IPv6 design and planned infrastructure.

It is also expected that the organization at this stage have already completed an:

a. IPv6 infrastructure design
b. IPv6 deployment plan
c. IPv6 training plan
d. IPv6 field trials plan

- **Level 4**

An organization would be characterized as being in Level 4 IPv6 readiness if it started its IPv6 migration program along with a full assessment of IPv6 capabilities in its networks and applications and already started addressing IPv6 critical issues (IPv6 Technical Architecture Design). It is recommended that organizations at Level 4 proceed with:

a. Their implementation of an IPv6 deployment plan across the organization. The deployment project plan would implement elements of the IPv6 Architecture Design Plan
b. IPv6 training plan
c. IPv6 field trials plan
d. Engagement with IPv6 Customers

8. IPV6 ADOPTION PLAN GUIDELINE

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

a. Business Planning: which covers the business case of the organization in regards to foreseen drivers and economic value of adopting IPv6
b. Technical Planning: which covers technical aspects of the organization’s ICT infrastructure towards IPv6 interoperability

8.1 Business Planning

The Business Planning phase of the IPv6 Adoption consists of four (4) activities, which will:

a. Identify Business Drivers
b. Identify Benefits, Costs, Risks
c. Develop a Business Case for IPv6
d. Establish an IPv6 Transition Group

8.1.1 Identify Business Drivers

Stakeholders should identify reasons and drivers to adopt 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:

i. IPv4 Address Exhaustion: The availability of IP addressing secures business continuity and as of this moment, IPv6 is the only long term solution once IPv4 is depleted
ii. Governmental mandates to implement and adopt IPv6 would drive stakeholders such as service providers and vendors already dealing with the government to speed up plans for IPv6 adoption to secure their governmental clients who would otherwise seek IPv6 compliant services from other suppliers
iii. The prospects of new applications requiring IPv6 large address pool such as control and sensors applications, home and personal networks and services and devices, secure peer-to-peer applications and others

8.1.2 Identify Benefits, Costs, Risks

Benefits:

Organizations should identify how IPv6 benefits and enables particular lines of business and programs. Organizations should identify if IPv6 would: Increase business opportunities (maintain existing services and create new ones)

i. Improve network efficiency, performance, cost savings (removal of NAT and more efficient address space management for example)
ii. Simplify operations (auto-configuration features)
iii. Provide a strategic and advantageous position towards other competitors
iv. Costs; Organizations should identify costs incurred by an IPv6 adoption plan. Costs include those related to both technology costs and human related costs.

Technology costs can be traced to:

1. Planning and engineering the adoption plan such as: design, implementation, testing, deployment and other IT/Networking technical operations
2. Operational and running costs resulting from running IPv6 networks side by side with the existing IPv4 infrastructure
3. Procurement costs of required infrastructure changes and upgrades. Best practices have shown that costs in this regards would be of minimal economic impact if such upgrades and changes are done as part of the ICT life cycle management process and not as sudden isolated upgrades. Costs in this area are related to:
   - Hardware and Software
   - Applications
   - Operational Support Systems and Network Management Systems (NMS)

Human and personnel training related costs:

As in 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:

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

The National Institute of Standards and Technology (NIST) study “IPv6 Economic Impact Assessment” estimated the costs to be incurred by the introduction of IPv6 in the USA at 25 billion USD for the period (1997-2025). The study noted that such a cost is relatively small as compared to the overall ICT expenditures.

Risks

Organizations 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 minimize the impacts in the event those risks happen and occur. These include: business, legal and technical risks.

1. **Business:** Organizations 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.

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

iii. **Technical:** Like any technology upgrade, technical risks would arise and these include:

   a. 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

   b. Reliability risks would arise in introducing a new IP protocol and if it will maintain the same level of reliability offered by IPv4

   c. Interoperability risks in between different types of IPv6 stacks, between IPv6 and other protocols and interoperability with the present IPv4 networks

8.1.3 Develop a Business Case for IPv6

The business case should be formulated making use of the already identified business drivers as well as benefits, costs and risks. The business case should justify the costs in terms of the identified benefits as well as the impacts both business and technical. In other words, the organization should decide if the costs as well as other impact are worth the prospective return.

8.1.4 Establish an IPv6 Transition Group

Organizations should establish an IPv6 Transition group office that will plan, coordinate, track and communicate progress of the IPv6 adoption project throughout the whole organization. The office will allocate the required resources to support the adoption effort. This is critically important in large organizations with large ICT infrastructures at across several sites. Members of the transition group should have their roles clearly identified with the corresponding responsibilities and should include technical, business and managerial decision making personnel. The transition group will undertake tasks at the corporate level and these include:

i. Building overall IPv6 awareness: the transition group should familiarize the organization with IPv6 in general, IPv6 impact to their working areas and IPv6 importance to the organization as whole and ultimately build a sense of urgency for adopting IPv6 and raise the priority for establishing IPv6 interoperability against other projects in the organization

ii. Develop an overall transition plan for the whole organization and ensure that all IPv6 related tasks across the organization are well synchronized, consistent and prioritized. The plan should include: clear and defined milestones with specific dates, areas that will be impacted by the IPv6 transition effort along and the groups to address such impacts.

iii. Governance: the IPv6 transition group should establish and manage a governance structure to ensure a smooth and successful IPv6 transition. The governance structure should highlight modes of communication and keep track of the transition progress against the clear predefined and measurable milestones. Governance should also address IPv6 procurement opportunities within the organization and for example cover the inclusion of IPv6 in ICT procurement policies.

8.2 Technical Planning

The technical planning of the IPv6 Adoption program includes five (5) activities as follows:

i. Inventory and Assessment of IPv6 Capabilities
ii. Develop a Technical Design for IPv6 Transition
iii. Develop Impact Analysis
iv. Develop an Implementation Plan
v. Training and Awareness Planning

8.2.1 Inventory and Assessment of IPv6 Capabilities

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

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

Auditing can also include:

a. Contracts for presence or absence of IPv6 specific and complying language
b. Procurement activities for presence or absence of terms such as: IPv6, IPv6-capable, IPv6 upgradeable, IPv6 incapable, etc.
c. Auditing can also be extended to include the determination of the future IPv6 needs within the organization. For this, the organization should identify all locations, facilities and buildings, platforms, personnel, devices and others.

8.2.2 Develop a Technical Design for IPv6 Transition

The organization shall develop an overall IPv6 design for the various impacted operational areas/aspects of the network and provide functional equivalence to IPv4 to ensure a smooth transition. The design should also take into account any new networks and the traffic growth that the organization foresees. The design should address operational and technical elements including:

1. IPv6 Addressing Plan
2. IPv6 Routing
3. IPv6 Interconnection (peering and transit connectivity)
4. IPv6 Transition Mechanism
5. Network Services
6. Security
7. OSS, BSS and Network Management
8. Applications
9. Scalability and Reliability
10. Service Level Agreements
11. Testing

i. IPv6 Addressing Plan

The IPv6 Addressing Plan should identify the organization'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 should consider the different sections of the organization's network such as: the intranet, extranet, external sites not managed by the organization, services such as Layer 3 VPNs and others. If the organization provides IP connectivity to other organizations, these networks also need to be considered in the addressing plan.

The addressing plan should consider supporting an efficient and scalable routing schema. Other considerations include the decision between Provider Independent (PI) or Provider Aggregateable (PA) IPv6 prefixes.

Conditions should be set to decide in between Stateless Address Auto-configuration (SLAAC) or Stateful Configuration, usage and management of privacy extensions and multiple prefix addresses on a single interface. Scalability and Reliability should also be considered when developing the IPv6 address plan.

ii. IPv6 Routing

Organizations should 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 …) and what adaptations need to be done to enable IPv6 routing**.**

iii. IPv6 Interconnection

Organizations should identify their IPv6 connectivity needs (native, tunneling) and consider which of their service providers will be able to meet their needs. The organization should also decide which type of IPv6 connectivity would interconnect its internal sites. Existing IPv4 interconnections to other networks (public and private peering, upstream/transit connections) need to be assessed regarding their IPv6 capabilities and plans need to be made to get IPv6 enabled at these interconnections. Upstream/Transit connections might need to be moved to other providers if the current provider is not having a useful IPv6 offering.

8.2.3 IPv6 Implementation Requirements

The recommended IPv6 requirements listed below shall be reviewed from time to time to accommodate the development and challenges on IPv6 that may happen over time.

The basic requirements to implement IPv6 network should comprise of the IPv6 requirements as shown in Table below. The minimum requirements should be extended to the other optional requirements depending on the network capabilities.

No.	IPv6 Features	RFC
1	Internet Protocol, Version 6 (IPv6) Specification	RFC 2460
2	Neighbor Discovery for IP Version 6 (IPv6)	RFC 2461
3	IPv6 Stateless Address Auto configuration	RFC 2462
4	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	RFC 4443
5	Path MTU Discovery for IP version 6	RFC 1981
6	Use of BGP-4 Multi-protocol Extensions for IPv6 InterDomain Routing	RFC 2545
7	IP Version 6 Addressing Architecture	RFC 4291
8	IPv6 Global Unicast Address Format	RFC 3587
9	DNS Extensions to Support IP version 6	RFC 1886

Migration Mechanisms (Additional features)

No.	IPv6 Features	RFC
1	Transition Mechanisms for IPv6 Hosts and Routers	RFC 2893
2	Connection of IPv6 Domains via IPv4 Clouds	RFC 3056

Inter-ISP Connectivity (Additional features)

No.	IPv6 Features	RFC
1	Multi-protocol Extensions for BGP-4	RFC 2858

Internal IGP (Additional Features)

No.	IPv6 Features	RFC
1	OSPF For IPv6	RFC 2740
2	RIPng for IPv6	RFC 2080

Advanced Services

No.	IPv6 Features	RFC
1	IPv6 Multicast Address Assignments	RFC 2375
2	Security Architecture for the Internet Protocol	RFC 2401
3	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	RFC 2474
4	An Architecture for Differentiated Services Framework	RFC 2475
5	Mobility Support in IPv6	RFC 3775

Dial-up or xDSL

No.	IPv6 Features	RFC
1	IP Version 6 over PPP	RFC 2472
2	RADIUS and IPv6	RFC 3162

9. IPV6 NETWORK TRANSITION MECHANISM AND STRATEGIES

The Internet Engineering Task Force (IETF)'s Next Generation Transition (NGTrans) working group has defined three (3) main migration techniques.

9.1 Dual Stack Network

This approach requires hosts and routers to implement both IPv4 and IPv6 protocols. This enables networks to support both IPv4 and IPv6 services and applications during the transition period in which IPv6 services emerge and IPv6 applications become available. At present, the dual stack approach is a fundamental mechanism for introducing IPv6 in existing IPv4 architectures and will remain heavily used in the near future. The drawback is that an IPv4 and IPv6 addresses must be available for every dual stack machine.

9.2 Tunneling

Tunneling enables the interconnection of IP clouds. For instance, separate IPv6 networks can be interconnected through a native IPv4 service by means of a tunnel. IPv6 packets are encapsulated by a border router before transportation across an IPv4 network and de-encapsulated at the border of the receiving IPv6 network. Tunnels can be statically or dynamically configured or implicit (6 to 4, 6 over 4). The TB (Tunnel Broker) approach has been proposed to automatically manage tunnel requests coming from the users and ease the configuration process. ISATAP (Intra Site Automatic Tunnel Addressing Protocol) is a recent technique to avoid tunnel manual configuration. In later stages of transition, tunnels will also be used to interconnect remaining IPv4 clouds through the IPv6 infrastructure.

9.3 Translation mechanism

Translation is necessary when an IPv6 host has to communicate with an IPv4 host. The IP header at least has to be translated but the translation will be more complex if the application processes IP addresses. Such translation inherits most of the problems of IPv4 Network Address Translators. ALGs (Application-Level Gateways) are required to translate embedded IP addresses, recomputed checksums, etc. SIIT (Stateless IP/ICMP Translation) and NAT-PT (Network Address Translation - Protocol Translation) are the associated translation techniques. A blend of translation and the dual stack model, known as DSTM (Dual Stack Transition Mechanism), has been defined to allow for the case where insufficient IPv4 addresses are available. Similar to the tunneling techniques, translation can be implemented in border routers and hosts. This complex set of coexistence and transition techniques can be “mixed and matched” in many ways.

10. NETWORKS SERVICES

10.1 Domain Name System

The Domain Name System (DNS) does domain name-to-IP address mappings and vice versa. This allows for the usage of domain names instead of memorizing long internet protocol addresses of internet hosts. The case is no different with IPv6 addresses that are longer and harder to memorize than IPv4 addresses.

DNS resolves domain names upon request of end stations into the corresponding IP addresses by maintaining bindings or mappings between IP addresses and their domain names. These bindings are called resource records (RR) or also referred to as A-records for the 32-bits IPv4 addresses. However, A-Records cannot be used for the 128-bits long IPv6 addresses.

The IETF RFC 3596 (Category Standards Track) defines a new DNS record type for IPv6 hosts: the AAAA type record (called "quad-A"). The corresponding reverse lookup domain is IP6.ARPA. AAAA resource records map domain names to 128-bit IPv6 addresses and allows for forward resolution, which returns a 128-bit IPv6 address for a corresponding domain name. Reverse resolution in contrast resolves an IPv6 address into the corresponding domain name. Reserve resolution represents an IPv6 address using a pointer record (PTR).

For the purpose of DNS adoption of IPv6, two aspects should be distinguished and taken care of: Capability of processing IPv6 DNS resource records (AAAA) for forward resolution as well as reverse resolution.

It might not be feasible to add an additional AAAA entry for every name in the domain. If an AAAA record is found in the DNS for a given host name, most current applications (web browsers, mail clients) will try to use IPv6 to connect to the host, and fall back to IPv4 if IPv6 is not working. This is reasonable when the host actually has working IPv6 connectivity. If the host does not have working IPv6 at all, or the IPv6 connectivity is significantly worse than the IPv4 connectivity, this application behavior will cause slower performance and delays for user applications trying to access the host. For this reason, AAAA records should not be added graciously to every host, without first giving consideration to the actual reachability of the host using IPv6.

For experimental usage, until IPv6 connectivity is considered good enough, the IPv6 address (AAAA record) can be added to an ipv6.domainname.org subdomain, e.g. www.domainname.com has only an A records, while www.ipv6.domainname.com has the IPv6 AAAA record – this way, the user can decide whether to try IPv6 or not.

In the long run this is not a suitable approach, though – applications and networks need to handle IPv6-by-default, and users will not type in extra letters into their web browsers to get IPv6 connectivity. So in the long run, as soon as IPv6 connectivity to the machines is leaving the experimental phase, both IPv4 and IPv6 address (A and AAAA record) should be added to the normal domain name.

For initial testing, it might be advisable to delegate the ipv6.domainname.org sub-domain to a different set of name servers, to be able to experiment with adding AAAA records to zones without endangering the production domainname.org zone. Given that the AAAA support in all major DNS software implementation is quite mature, this is only recommended for the initial test phase. After this, there should not be dedicated name servers for IPv6 sub-domains, but IPv4 and IPv6 should be fully integrated into the main DNS zone.

Besides storing IPv6 addresses inside DNS zones, DNS servers also need to communicate with other machines.

Communication among DNS servers, and between client hosts and DNS servers, is done using IPv4 or IPv6 protocols. It is important to point out that the transport technology used to access the DNS server is independent of the record queried. So a client can use IPv4 packets to query a DNS server for IPv6 AAAA records, or the client can use IPv6 packets to query a DNS server for IPv4 A and IPv6 AAAA records, or any other possible combination – the transport protocol has no influence on the query and response.

This implies that the IPv6 network connectivity for the DNS servers can and should be evaluated independently of the availability of IPv6 information (AAAA records) inside the DNS data.

It is recommended that IPv6 transport is enabled towards the DNS servers as soon as the quality of the available IPv6 network connection is good enough to use it as a production service. Since DNS queries will be able to use both IPv4 and IPv6, enabling IPv6 has little risk, and will actually improve reliability in case there is a problem with IPv4 connectivity and IPv6 connectivity still works.

Besides the DNS resolvers and DNS servers in each organization, there are a number of "special" DNS servers in the Internet:

a. The DNS root servers that give out referrals for the top-level domain (TLD) name servers. The root name servers have IPv6 connectivity already and can store AAAA records for the TLD domain name servers.

b. The ccTLD name servers. To achieve a complete IPv6 Internet, the name servers for all TLDs need to be reachable using IPv6 transport, and need to be able to store AAAA records for second-level domains (glue records).

10.2 Web

As soon as IPv6 usage becomes more prominent, it is important that these users are able to reach the "Internet face" of a corporation, namely its E-Mail and HTTP servers, over IPv6. 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 small:

i. enable IPv6 connectivity towards the machine (dual-stack IPv4 and IPv6 network)
ii. turn on IPv6 networking in the server machine's network configuration
iii. enable IPv6 (if necessary) in the web server configuration
iv. 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.
v. enter the IPv6 address of the machine (AAAA record) into the DNS server

For larger web sites with load-balancing to multiple HTTP servers in the back end, more details need to be taken into account. For a quick solution, it is possible to use a "reverse proxy" solution that provides IPv6 connectivity to the customers, and requests the pages using IPv4 from the primary web server, but in the long run, this has the danger of providing worse performance and thus worse user experience than a fully integrated solution. Detailing the steps that need to be done for a multi-tiered web site (Firewall, Load-Balancer, multiple web servers, database servers) is basically similar to the single machine case:

a. enable IPv6 connectivity to the platform
b. Make sure that all involved products have full IPv6 support (firewalls, load-balancer, and server). Especially for the load-balancers, this might require hardware or software upgrades.
c. test the application for hidden IPv4 dependencies
d. enable IPv6 in the DNS

10.3 Mail

E-Mail falls into the same category as HTTP: for communication with other parties in an Internet that moves towards IPv6, it is important that e-mail can be sent to parties that have no IPv4 anymore – thus, 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:

a. Enable IPv6 connectivity to the server
b. 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.
c. Besides mail transport, it might be necessary to check any sort of IPv4-based logging, statistics or anti-spamming tool in use for IPv6 capability.
d. 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 organization 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 signal this to the vendors early in the process so that the rollout of IPv6-enabled E-Mail-Services are not hindered by vendors that are slow to upgrade their appliances.

11. PHASES OF ADOPTION

Most existing networks will not be able to convert all of their network and all their services to a fully dual-stacked IPv4+IPv6 environment at once – usually due to one of the following reasons:

a. too many components affected
b. too many service affecting changes at the same time
c. not enough human resources to do large number of changes at the same time

d. no business case for converting specific parts of the network right away
e. Stoppers in converting specific parts of the network

The best approach for a given network depends on local factors that need to be determined when setting up the IPv6 adoption plan for this specific environment.

11.1 Service Providers

i. Backbone Network provides connectivity between provider access networks and to other ISP networks through peering. Backbone routers, border routers and parts of the provider edge network equipment reside in the backbone network
ii. Provider Access Networks each of which connects one or more customers. The other part of the Provider Edge equipment (not residing at the backbone) as well and customer premises equipment (CPE) reside in the provider access network

Transition mechanisms from IPv4 to IPv6 differ depending on the network segment. RFC 4029 “Scenarios and Analysis for Introducing IPv6 into ISP Networks” identifies four stages during the transition as follows:

I. Stage 1: Launch

The Launch stage is the first stage where the ISP is still an IPv4-only ISP with IPv4 only customers. Obvious preparatory actions at this stage include obtaining a prefix IPv6 allocation from AFRINIC, typically a /32 prefix. Other preparatory steps include establishing IPv6 connectivity with an upstream provider and IPv6 peering. IPv6 Peering with other ISPs can be done through the national IXP.

II. Stage 2a: Backbone

At this stage, the ISP backbone supports both IPv4 and IPv6 but with IPv4-only connection networks at the provider access network segment. The backbone can be made IPv6 compliant through software and hardware upgrades.

At this stage, the provider access segment provides IPv4-only connectivity to customers. ISPs can provide IPv6 connectivity through a tunneling mechanism. The tunnel will be terminated at the CPE (which should be IPv6 compliant) or other customer internal network IPv6 compliant gateway device.

III. Stage 2b: Customer Connection

At this stage, and opposite to the previous one, the backbone supports IPv4 only while the access network supports both IPv4 and IPv6. Unlike the previous stage, the customer can establish native IPv6 connectivity to the ISP. IPv6 traffic is eventually transported at the IPv4-only backbone by tunneling over IPv4. It should be noted that a main difference between stages 2a and 2b is that in stage 2b, the customer does not need to support both IPv4 and IPv6 but only IPv6.

IV. Stage 3 Complete

This stage can be considered the final step of introducing IPv6 as far as the ISPs network segments are concerned. Both of the backbone and provider access networks are able to provide native IPv4 and IPv6 connectivity. From the perspective of the service provider, the difference between this stage and the previous ones is obvious; the backbone has become IPv6 supportive. From the perspective of the customer, nothing has changed as the connection requirement for IPv6 traffic exchange is the same. The transition will start at stage 1 and could possibly proceed into three different directions (2a or 2b or 3). Hence, the ISP could first upgrade the backbone network or upgrade the provider access network. The final stage will be introducing IPv6 at both the access and backbone network segments. Interior Gateway Protocols (IGP) as well as Exterior Gateway Protocols (EGP) need to support the new Internet Protocol deployment IPv6 for the successful routing of IPv6 traffic.

BGP can be used for both IPv6 and IPv4. The most common practice is to use separate BGP sessions each for IPv4 and IPv6 (and not one session) to advertise IPv4 and IPv6 prefixes between two peers.

12. REGULATORY COMPLIANCE

The best mechanism to check compliant is through self-declaration by the organization to the regulatory authority. This is in accordance with the direction towards self-regulation. The key requirements from the Regulatory Authority on the compliance:

a. Acquire IPv6 addresses from AFRINIC
b. Announce IPv6 global addresses
c. Support IPv6 capable DNS.

The Regulatory Authority may send a letter requesting for the self-declaration to the relevant organizations. The organization may revert within fourteen (14) working days.

12.1 Timeline

The organization must submit the Declaration Form upon request to the regulatory authority on the IPv6 network implementation readiness before the stipulated deadline determined by the regulator as per appendix 2.

12.2 Responsibility

The organization may be responsible to declare to the Regulatory Authority on the status of IPv6 network implementation. The declaration as per Appendix 1 must be submitted and undersigned by one (1) key personnel in the organization either the Chief Executive Officer or the Chief Technical Officer or someone who is of equivalent stature.

12.3 Records

The organization shall keep a set of the followings for auditing and monitoring purposes.

a. IPv6 network (architecture) diagram
b. Test records conducted on all the features implemented for future verification by the Regulatory Authority
c. Implementation and maintenance records.

12.4 Audit

The Regulatory Authority may conduct audit on the organizations that have declared to be IPv6 compliant to verify their readiness.

12.4 Notice

The Regulatory Authority may give thirty (30) working days' notice to the organization through an official letter to the Chief Executive Officer or Chief Technical Officer.

APPENDIX

Appendix 1: IPv6 Implementation Checklist

No.	IPv6 Features	RFC	Status Yes/No/NA
1	Internet Protocol, Version 6 (IPv6) Specification	RFC 2460	
2	Neighbor Discovery for IP Version 6 (IPv6)	RFC 2461	
3	IPv6 Stateless Address Auto configuration	RFC 2462	
4	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	RFC 4443	
5	Path MTU Discovery for IP version 6	RFC 1981	
6	Use of BGP-4 Multi-protocol Extensions for IPv6 InterDomain Routing	RFC 2545	
7	IP Version 6 Addressing Architecture	RFC 4291	
8	IPv6 Global Unicast Address Format	RFC 3587	
9	DNS Extensions to Support IP version 6	RFC 1886	

Director General/CEO
National Regulatory Authority
....

Dear Sir/Madam,

DECLARATION FOR THE SUBMISSION OF IPv6 COMPLIANCE

Company Name :			
Network	**MNO,ISP, FNO**	**Fixed**	**Core**
			Edge/access
			Core and edge/access
			Peering
		Mobile	**Core**
			Edge/access
			Core and edge/access
	RETAIL-ISP	**Fixed**	**Core**
			Edge/access

			Core and edge/access
			Core
			Edge/access
			Core and edge/access
IP Address			
Declaration Date			

Appendix 2: Responsibility Matrix and Timeline

I. Government Organizations

	Timeline	Responsible
The Government organizations should prepare a detailed transition plan for complete transition to IPv6 (dual stack) based on the network complexity & equipment / technological life cycles. A Strategy for the Implementation of IPv6 in Govern ment Agencies		
All new IP based services (like cloud computing, data centers etc.) to be provisioned for / by the Government organizations should be on dual stack supporting IPv6 traffic with immediate effect.		
The public interface of all Government projects for delivery of citizen centric services should be dual stack supporting IPv6 traffic. The readiness of Government projects in turn will act as a catalyst for private sector transition from IPv4 to IPv6.		
The Government organizations should procure equipment, which are also IPv6 Ready (Dual Stack) and go for deployment of IPv6 ready (Dual Stack) networks with end-to-end IPv6 supported applications.		
The Government organizations should go for IPv6 based innovative applications in their respective areas like smart metering, smart grid, smart building, smart city etc.		

II. Service Providers: Enterprise Customers

	Timeline	Responsible
All new enterprise customer connections (both wireless and wireline) provided by Service Providers shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.		
Regarding the existing enterprise customers, which are not IPv6 ready, the Service Providers shall educate and encourage their customers to switch over to IPv6. Retail Customers (Wireline)		
All new retail wireline customer connections provided by Service Providers shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.		
The Service Providers shall endeavor to progressively replace/ upgrade the Service Providers owned CPEs which are not IPv6 ready as per the following timelines	1. Replacement / upgradation of 25% of CPEs by (Timelines…………) 2. Replacement / upgradation of 50% of CPEs by…………… 3. Replacement / upgradation of 75% of CPEs by ………….. 4. Replacement / upgradation of 100% of CPEs by …………………………..	

Regarding the customer owned CPEs, which are not IPv6 ready, the Service Providers shall educate and encourage their customers to replace/ upgrade such CPEs to IPv6 ready ones. Retail Customers (Wireless)		
All new LTE customer connections provided by Service Providers shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.		
All new GSM/ CDMA customer connections provided by Service Providers shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.		

III. Content & Application Providers

	Timeline	
All contents (e.g. websites) and applications providers should target to adopt IPv6 (dual stack) for new contents & applications.		
The complete financial ecosystem including payment gateways, financial institutions, banks, insurance companies, etc. should transit to IPv6 (dual stack)		

The new registrations on "ccTLD" domain to be compulsorily on dual stack.		
The entire "ccTLD" domain should migrate to IPv6 (dual stack).		

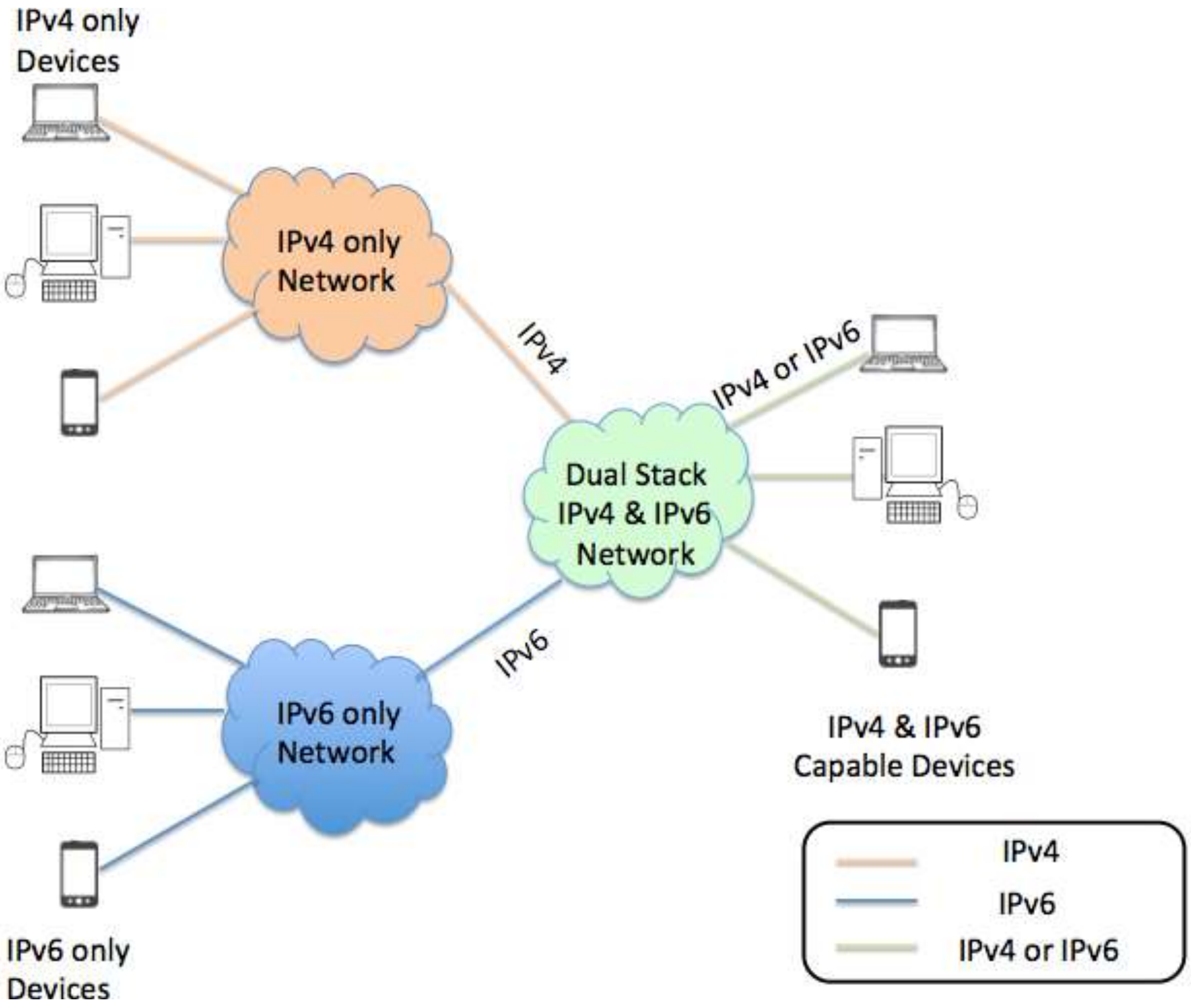
IV. Equipment Manufacturers

	Timeline	
All mobile phone handsets/ data card dongles/ tablets and similar devices used for internet access supporting GSM / CDMA version 2.5G and above sold in Rwanda shall be capable of carrying IPv6 traffic either on dual stack (IPv4v6) or on native IPv6.		
All wireline broadband CPEs sold in Rwanda shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.		

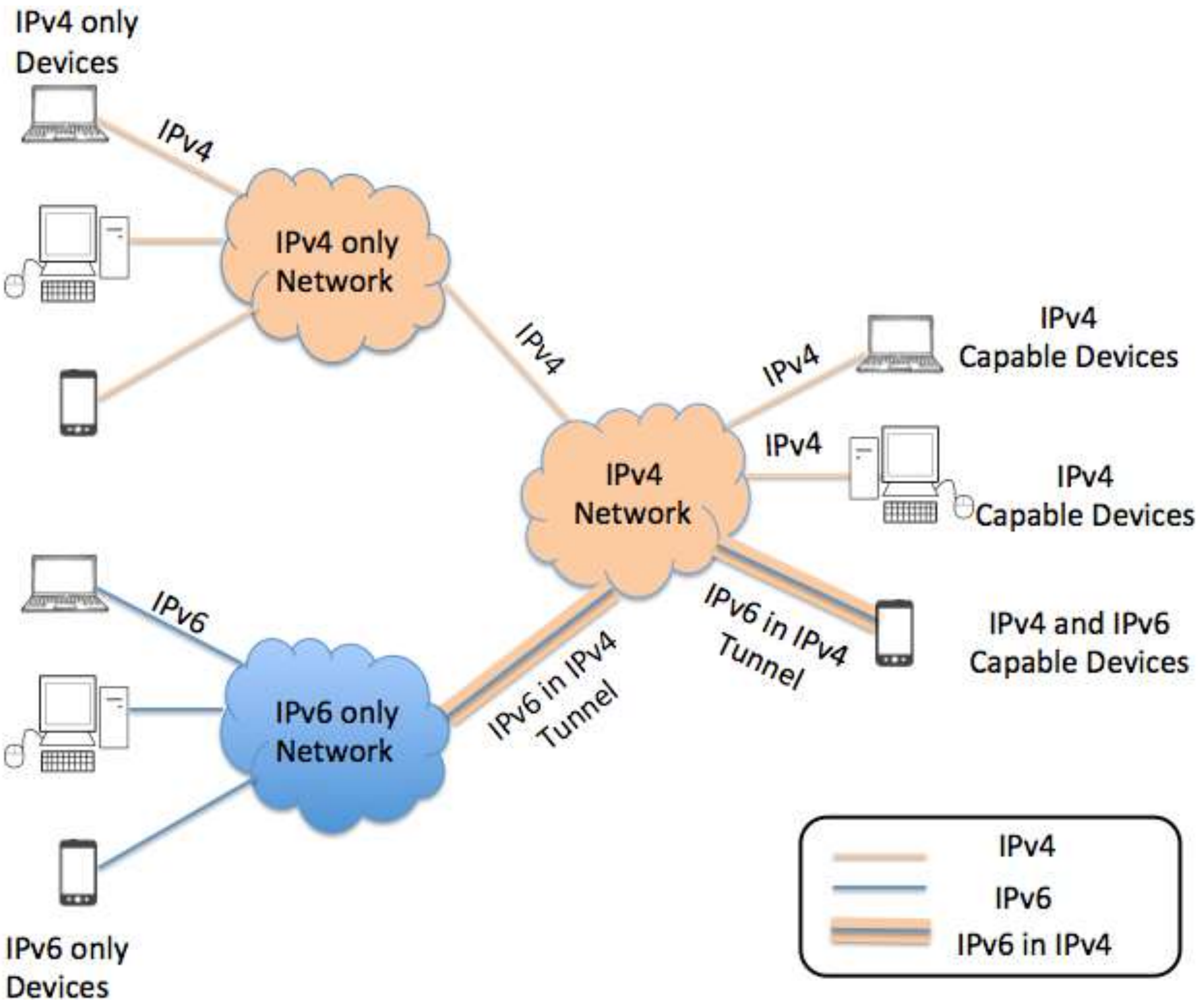
V. Cloud Computing / Data Centers

	Timeline	
All public cloud computing service / data centers providers should target to adopt IPv6 (dual stack)		

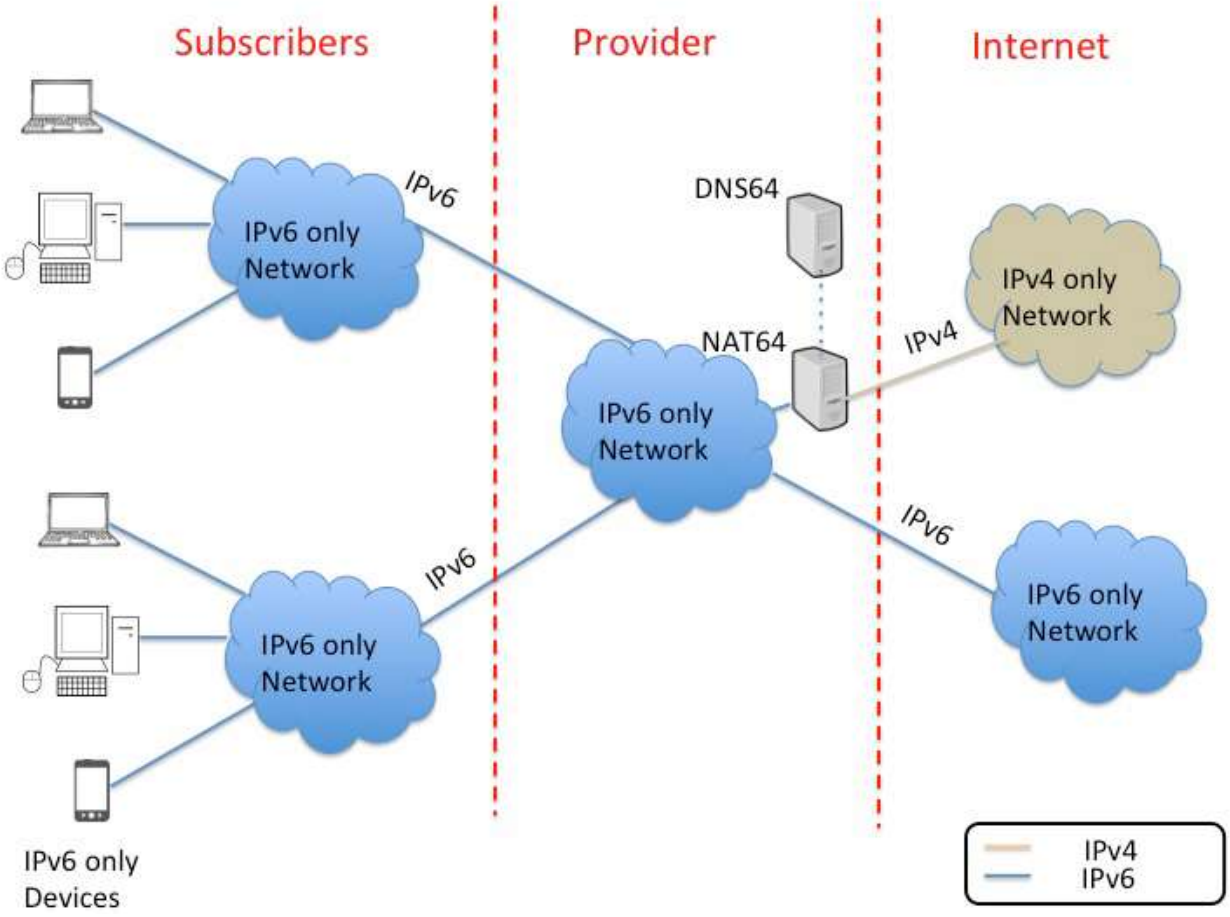
Appendix 3: Dual Stack Implementation



Appendix 4: Tunneling



Appendix 5: Translation


Subscribers
Provider
Internet
IPv6 only Network
IPv6
DNS64
NAT64
IPv4
IPv4 only Network
IPv6 only Network
IPv6
IPv6
IPv6 only Network
IPv6 only Network
IPv6 only Devices
IPv4
IPv6