هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

IPv6 Policies, Procedures and Guidelines
Kingdom of Saudi Arabia

June 2009, Riyadh, Saudi Arabia

Table of Contents

Table of Figures

1. Executive Summary

The CITC IPv6 projects aims at raising the awareness and encouraging the adoption of IPv6 nationwide. As part of the project, a series of deliverables and studies have been conducted and which are publicly available on the Saudi Arabia IPv6 Task Force homepage (www.ipv6.org.sa).

As part of the project, the deliverable "IPv6 Policies, Procedures and Guidelines" aims at giving directions to different types of stakeholders in terms of:

1. **Procurement Policies** addressing the necessity of the inclusion of IPv6 compliance in ICT procurement and periodical IT cycles of organizations. This will ensure that IPv6 capable ICT products will be procured.

2. **Procedures** and conditions as set by RIPE NCC to acquire IPv6 address blocks will be presented and explained so as to assist LIRs and local stakeholders in getting familiarized on how to acquire IPv6 addresses.

3. **Guidelines** for assessing the IPv6 readiness level of an organization, which follows a tiered approach of five (5) levels of readiness based on the amount of IPv6 work that has been done at the organization. The aim of the IPv6 Readiness Guideline is to present an overall and high-level characterization assessment of the IPv6 readiness of an organization, which makes it easier to understand from the decision making or business planning point of view. Much of the content of the readiness assessment refers to the work that has been done by the **Alliance for Telecommunications Industry Solutions (ATIS)[1].**

The other set of guidelines relate to a high level approach in determining and planning an **IPv6 Adoption Plan** and phased into two (2) stages:

- Business planning
- Technical planning

Transition Mechanisms are listed, to give background information on the technical measures necessary to move a network from IPv4-only to IPv4-and-IPv6 as well as IPv6 considerations for various types of stakeholders (ISPs, Enterprise and others).

[1] http://www.atis.org/

2. Introduction

IPv6 currently presents the only certain alternative for IPv4 whose imminent exhaustion is expected to happen in 2011 for IANA and 2012 for Regional Internet Registries (RIRs)[2]. As previously indicated in the deliverable "IPv6 Status Quo and Readiness Assessment", local stakeholders not adopting IPv6 are running the risk of facing a shortage of IP addressing. This scenario could hamper the further development of the internet infrastructure as well as the provisioning of ICT services and applications.

2.1. Project Background

The **Communication and Information Technology Commission (CITC)[3]** was created in 5/3/1422H and changed its name to the current one on 21/5/1424H. Its vision is that Saudi Arabia should benefit from universally available, high quality and affordable communications and information technology services. Its mission is to provide a fair, clear and transparent regulatory environment to promote competition, to safeguard public interest and stakeholder rights, to enable universal availability of advanced ICT services and optimize utilization of scarce resources, to increase ICT awareness and usage to enhance national efficiency and productivity and to build a professional and motivated CITC team.

The Internet Services Department of CITC aims at creating the right environment for the development of Internet Services in Saudi Arabia. It has several responsibilities including but not limited to the Domain Name Management for .sa names, content filtering policy definition and implementation, internet exchange management and others.

Aiming at fulfilling its missions, CITC decided early 2008 to create the right environment for a migration to **Internet Protocol version 6 (IPv6)**, which appears now as a certain long term means to address the imminent exhaustion of IPv4. In order to facilitate the adoption efforts of IPv6 in Saudi Arabia, CITC has launched the **IPv6 Sub-project** as part of the **Internet Services Development Phase II** initiative which was launched with the purpose to implement part of the outcome initiatives of the previous **Internet Services Development Phase I**.

2.2. Purpose and Objectives of the Document

The CITC IPv6 Project aims at establishing a national IPv6 Task Force[4] in order to raise the awareness and encourage the deployment of IPv6 nationwide. As part of the project, an IPv6 Strategy consisting of a set of ten (10) initiatives covering both infrastructure and awareness aspects of IPv6 was proposed to be eventually owned and driven by the IPv6 task force. The initiatives entail a set of activities by and impacts on local stakeholders from both the Public sector (CITC, Ministries, e-Gov, academia and research institutions) and the Private sector (service providers, content providers, the enterprise and ICT vendors).

The **"IPv6 Countries Benchmark Study**" of the CITC IPv6 Project has shown that different types of stakeholders pass through many common preparation and implementation phases while adapting to IPv6. These include establishing a business case for IPv6, current state assessment and IPv6 readiness analysis, impact and risks analysis, planning the IPv6 adoption, implementation, reporting, testing and others. The IPv6 Benchmark study has also shown that in order to assist stakeholders

[2] http://www.potaroo.net/tools/ipv4/
[3] http://www.citc.gov.sa/
[4] http://www.ipv6.net.sa/

through these preparatory and adoption IPv6 efforts while minimizing risks and impacts, IPv6 best practices related to: policies, procedures and guidelines have to be established by the leading IPv6 stakeholders such as: ICT Ministries and Regulators, Major Service Providers, Major ICT Vendors and others.

The objective of this document is to define a set of procurement policies, guidelines and procedures to assist local stakeholders in their IPv6 adoption efforts. The targeted audiences of the report are both managerial/decision making and ICT operational personnel at both the Public sector (CITC, Ministries, e-Gov, academia and research institutions) and the Private sector (service providers, content providers and the enterprise). These could benefit from the content of this report in order to get directions on: how to amend their ICT procurement policies to cover IPv6 compliance, how to apply RIPE NCC standard procedures to acquire IPv6 address blocks, and finally, guidelines that address both business and operational aspects of IPv6 such as: IPv6 readiness assessment and IPv6 adoption planning.

2.3. Structure of the Document

The structure of the document is as follows:

- Executive Summary
- Introduction
- Procedures
- Guidelines
- Network Transition Mechanisms
- Public Services Transition Considerations
- Phases of Adoption
- Different Stakeholders Considerations
- Appendix

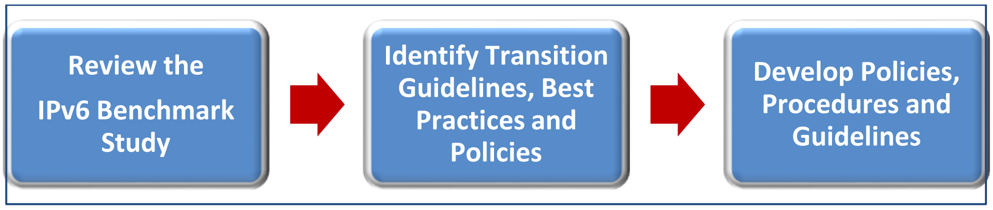
2.4. Methodology

The methodology used to develop the "IPv6 Policies, Procedures and Guidelines" was to review the research of the various IPv6 best practices, guidelines and policies that were encountered in the **"IPv6 Countries Benchmark Study".** These include various sources with an emphasis on transition guidelines and recommended approaches extracted from IPv6 transition documents, presentations, reports, analysis and other publicly available documents and articles.

Data were collected from the active stakeholders involved in the national IPv6 efforts such as Ministries, Government Agencies, Telecom operators, Network Information Centers (NICs) and IPv6 taskforces. Data were also collected from the IPv6 Forum, IPv6 Summits Agendas, IANA, Regional Internet Registries (RIRs), Local Internet Registries (LIRs) and others.

Figure 1 below presents the flow of the constituent elements of the methodology used to develop the policies, procedures and guidelines in this report.

Figure 1- IPv6 Policies, Procedures and Guidelines development Methodology


Review the
IPv6 Benchmark Study
Identify Transition Guidelines, Best Practices and Policies
Develop Policies, Procedures and Guidelines

3. Procurement Policies

Policies in general pertain to high level directions and future activities of the organization. Procedures are often setup to implement the high level policies.

The introduction and implementation of a new technology such as IPv6 could be hindered and slowed by administrative and bureaucratic processes. It is essential ICT procurement policies are reviewed and amended to consider and include IPv6 compliance.

The process of reviewing and amending ICT procurement high level policies and legislations should be done in a timely manner to introduce IPv6 so as to assist the migration to IPv6 interoperable infrastructures.

Addressing procurement policies carry a high level of importance as is the in case in the introduction of any new technology or service into the organization's business and ICT models. IPv6 is no different. Organizations should address the following in regards to ICT procurement policies so as to fully include and comply with IPv6 support as a requirement in all ICT purchases:

- Standard acquisition and procurement language
- Standard contractual language

ICT Procurement policies in this context pertain to any related purchasing activity that addresses both the human and technology aspects of the ICT infrastructure environment of an organization and these include the procurement of:

- Software/Hardware
- Internet Service Connectivity
- Networking Operations and Support Contracts
- Network Consultancy services
- Networking Training Courses (to include IPv6 in curricula)
- Any other ICT procurement/contractual activity which is IP related

The amendment of these policies to include IPv6 will also help shape the general direction of the organization towards IPv6 due to their wide scope of impact. The actual implementation details of IPv6 planning and deployment is left to a subsequent stage and to the professional ICT and business key personnel.

4. Procedures

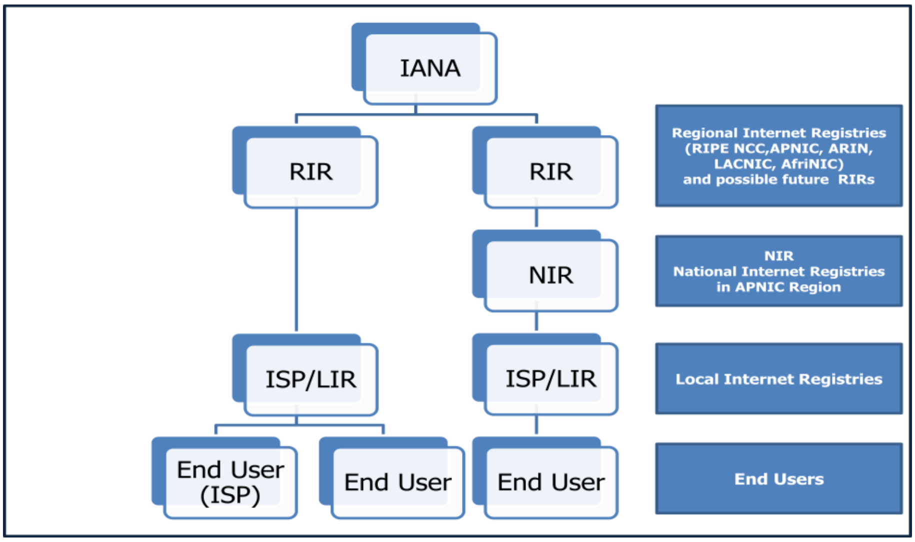
The purpose of this section is to highlight the required procedures that local stakeholders should follow in order to request IPv6 address space. The underlying principles are similar to the procedures to request IPv4 address space, but for IPv6 requests, there are significant differences regarding the justification requirements and sizes of address blocks assigned/allocated. For that reason, and to have all the references in a single location, this section is included even if some of the audience might be familiar with these matters already.

In general, there are three (3) sources from which to obtain IPv6 address space and these are:

1. An upstream 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. A local internet registry (LIR).
   A LIR can provide provider aggregateable (PA, non-portable) IPv6 address space, or can assign provider independent (PI, portable) IPv6 address space to end users.
3. The Regional Internet Registry (RIR), which is RIPE NCC for LIRs in Saudi Arabia.
   To receive IPv6 address space directly from the RIPE NCC, a requester needs to become a paying member of the RIPE NCC.

Figure 2 below depicts the hierarchy of global management of IPv6 addresses.

Figure 2- Hierarchy of Global Management of IPv6 Addresses


IANA
RIR
RIR
NIR
ISP/LIR
ISP/LIR
End User (ISP)
End User
End User
Regional Internet Registries (RIPE NCC,APNIC, ARIN, LACNIC, AfriNIC) and possible future RIRs
NIR National Internet Registries in APNIC Region
Local Internet Registries
End Users

The purpose of this section is to present the required procedures that should be followed by local internet registries (LIRs) in order to request IPv6 address space from the relevant Regional Internet Registry (RIR), which is the RIPE NCC in the case of Saudi Arabia.

4.1. Address Allocation and Assignment

The Réseaux IP Européens Network Coordination Centre[5] (RIPE NCC) is the Regional Internet Registry (RIR) that assigns and allocates IPv6 address space for the RIPE NCC service region and which covers Europe, the Middle East and parts of Asia.

To "**Allocate"** pertains to the distribution of address space to Internet Registries (IRs) for the purpose of subsequent distribution (allocation or assignment) by them. Example: Allocation of IPv6 address space from RIPE NCC to a Local Internet Registry (LIR).

To **"Assign"** pertains to the delegation of address space to an ISP or End User **for the purpose of specific use within the Internet Infrastructure that they operate.** ."Assignments must only be made for specific purposes documented by specific organizations and are not to be sub-assigned to other parties."

RIPE NCC allocates and assigns IPv6 addresses according to

- The IPv6 Address Allocation and Assignment Policy
- The IPv6 Address Space Policy for Internet Exchange Points (IXPs)
- The IPv6 Addresses for Internet Root Servers

1. The **IPv6 Address Allocation and Assignment Policy**

Requesting an IPv6 address space allocation requires a RIPE NCC Membership. Smaller ISPs and End Sites can obtain IPv6 address space from their upstream provider.

Allocations

- RIPE NCC to LIRs

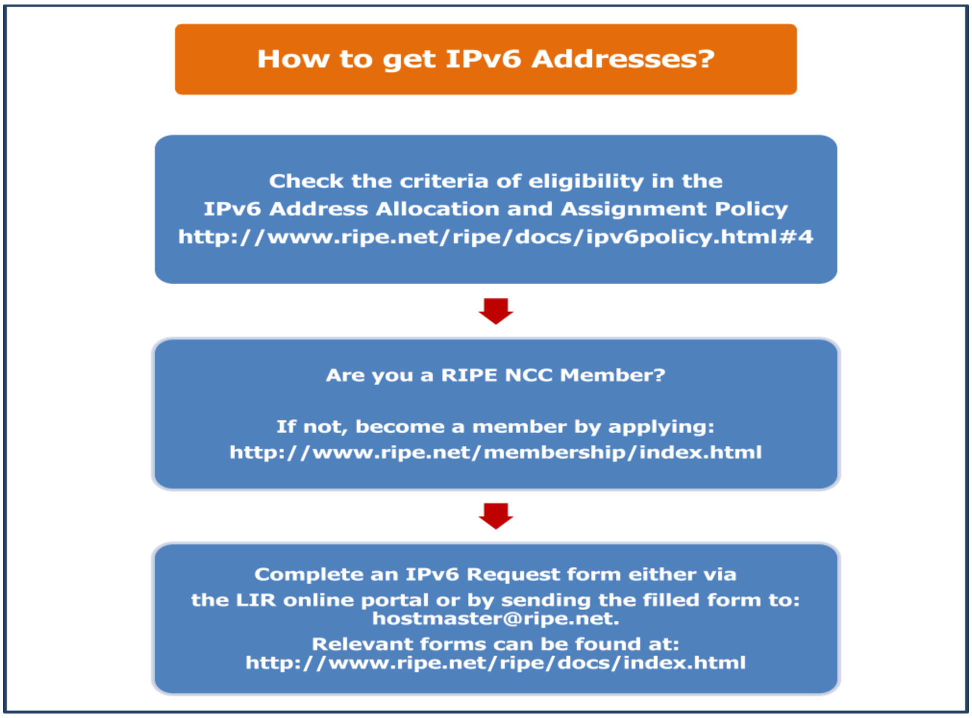
RIPE NCC members can get an IPv6 Address Allocation by completing the **IPv6 Allocation Request Form**[6]. In order to receive the allocation, it will be needed to:

- ✓ Be a Local Internet Registry (LIR)
- ✓ Advertise the IPv6 allocation as a single prefix if the prefix is to be used on the Internet
- ✓ Have a plan for making sub-allocations to other organizations and/or End Site assignments **within two years**

Figure 3- Steps to Acquire IPv6 Address Space from RIPE NCC

[5] http://www.ripe.net/rs/ipv6/

[6] http://www.ripe.net/ripe/docs/ripe-425.html



How to get IPv6 Addresses?

Check the criteria of eligibility in the IPv6 Address Allocation and Assignment Policy http://www.ripe.net/ripe/docs/ipv6policy.html#4

Are you a RIPE NCC Member?

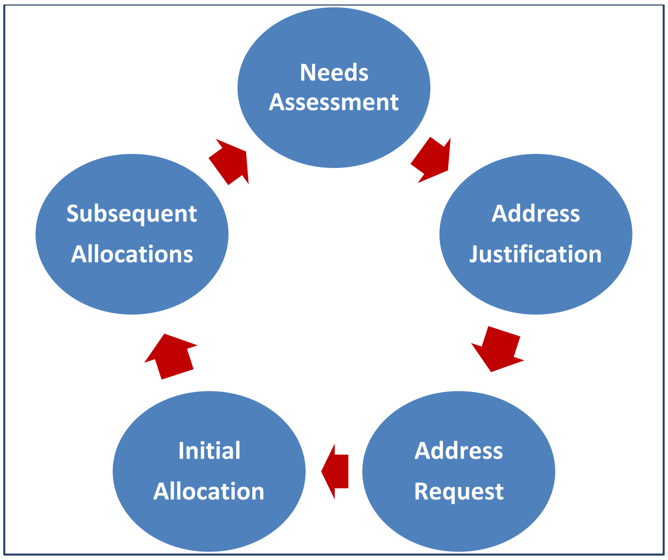
If not, become a member by applying: http://www.ripe.net/membership/index.html

Complete an IPv6 Request form either via the LIR online portal or by sending the filled form to: hostmaster@ripe.net.
Relevant forms can be found at: http://www.ripe.net/ripe/docs/index.html

Organizations meeting the initial allocation criteria described above are entitled to receive **a minimum allocation of /32**. In order to qualify for an initial allocation greater than /32, organizations should submit reasonable justifications for the request.

For subsequent allocations following the initial one, organizations should satisfy the evaluation threshold utilization of the past address allocation in terms of the number of sites in units of /56 assignments. **Appendix A** provides a table showing the number of equivalent absolute and percentage address utilization figures for IPv6 prefixes (in units of /56) that are required to satisfy the utilization threshold evaluation of previous IPv6 allocations. The absolute and percentage values are calculated for IPv6 allocation sizes ranging from /10 to /32.

Figure 4- IPv6 Address Allocation Cycle



When the organization satisfies the utilization threshold criteria, it will be eligible for an additional allocation that results in the doubling of the address space allocated to it. Where possible, the allocation will be made from an adjacent address block, meaning that its existing allocation is extended by one bit to the left. If an organization needs more address space, it must provide documentation justifying its requirements for a two-year period. The allocation made will be based on this requirement.

○ LIRs-to-ISPs

There is no specific allocation policy for the LIR-to-ISP case. Each LIR may develop its own policy to allocate IPv6 address space to subordinate ISPs considering the optimum usage of the IPv6 address block allocated to the LIR by RIPE NCC. All sub-allocations and assignments should be registered for accounting purposes either by the LIR or the subordinate ISPs in such a way that the RIPE NCC can evaluate the utilization for the purposes of acquiring a subsequent IPv6 allocation.

• Assignment

As stated earlier, IPv6 assignments pertain to the delegation of address space to an ISP or End User by LIRs/ISPs for the purpose of specific use **within** the Internet Infrastructure that they operate.

The size of the assignment is a local decision for the LIR or ISP to make. LIRs/ISPs are able to assign IPv6 address blocks to end sites with a size between a /64 (a single subnet within the end site) and a /48 (up to 65 536 routed subnets within the end site).

In case a single end site requests an assignment shorter than a /48, it needs to supply documented justifications to back up its request. Such requests will be processed and reviewed at the concerned RIR/NIR (RIPE NCC in our case).

Requests of IPv6 end user assignments are done by filling the appropriate form: **"IPv6 End User Site Assignment Request Form"**[7]

Other assignment guidelines are available at RIPE NCC homepage for cases such as **Internet Experiments** that require numbering resources for the period that the requesting organization will be running the tests.

2. The IPv6 Address Space Policy for Internet Exchange Points

RIPE NCC IXP members can acquire IPv6 address space by using the form **"IPv6 Internet Exchange Points Assignment Request Form"**[8]**.** In case the organization is confident it will not use more than one subnet, it is addressed a /64 assignment, otherwise, it will be given a /48 prefix.

3. The IPv6 Addresses for Internet Root Servers

[7] http://www.ripe.net/ripe/docs/ipv6-assignment-request.html
[8] http://www.ripe.net/ripe/docs/ipv6request-exchangepoint.html

Internet DNS root server (as listed in the root-servers.net zone) in the RIPE region will be assigned a block of IPv6 address space **for purposes of root server operations**. The size of the block shall be the same as the size of the minimum allocation to Local Internet Registries (LIRs) valid at the time of the root server assignment (currently it is /32).

The assigned prefix should be used only for root server operations and functions such as monitoring, statistics, others and is bound to the root server service itself. Such prefixes are not associated to the particular organizations operating the root servers and such organizations should not utilize the IPv6 prefix for purposes other than those related to the root server itself.

In case the operational responsibility of a DNS root server moves to a new organization, the IPv6 address space associated with the root sever will be returned to the RIPE NCC with the possibility of reassigning the prefix to the new organization. If the root name server changes its location to outside the geographical scope of the RIPE NCC region, the address space must be returned to RIPE NCC and a new assignment should be requested from the appropriate RIR covering the new geographical area.

If the root server stops operating within the RIPE region, the address space will be returned to the RIPE NCC and marked as "reserved" for a suitable long period of time.

4. IPv6 Address Space for DNS Anycast Servers

Entities operating the name servers for a Top Level Domain, e.g. the .SA TLD registry, can receive a /48 IPv6 prefix for the purpose of setting up a DNS anycast cloud. This prefix is only to be used for the anycast name server setup and must be returned if it is no longer in use.

5. IPv6 Provider Independent address space

Since May 2009, Provider Independent IPv6 address space is available in the RIPE region9.

Typically, IPv6 PI space is used for enterprise customers that are not an LIR themselves but want or need to be independent of any specific upstream provider, and hence require their own independent address space, which is portable among different upstream providers. LIRs that are approached by their customers for IPv6 PI space should consider the impact on the global routing system (extra routes that need to be globally visible, scalability issues in BGP) before forwarding the request to the RIPE NCC, and should recommend the use of provider aggregateable space where technically possible.

The current policy requirements to be eligible for a PI assignment are:

- must not be an LIR (LIRs should use a /32 provider allocation)
- must be multihomed
- must fulfill contractual requirements with a sponsoring LIR or with the RIPE NCC[10]

The RIPE NCC will typically assign a /48 block per PI request. If a larger address space is required, documentation for the requirements must be provided to the RIPE NCC.

[9] http://www.ripe.net/ripe/docs/ripe-466.html#PIAssignments
[10] http://www.ripe.net/ripe/docs/contract-req.html

IPv6 PI space can be requested via an existing RIPE member (sponsoring LIR), or directly from the RIPE NCC[11][12]. In the latter case, the requesting organization must join the RIPE NCC in a special category for end-user organizations that are not LIRs ("Direct Assignment User")[13].

[11] http://www.ripe.net/ripe/docs/ripe-468.html
[12] http://www.ripe.net/ripe/docs/ripe-467.html
[13] http://www.ripe.net/rs/independent-resources.html

5. Guidelines

This section presents guidelines for an organization attempting a move towards IPv6 adoption.

The planning and implementation phases of an IPv6 adoption effort could be better undertaken when the organization assesses where it currently stands as far as IPv6 is concerned. It is recommended the organization undertakes a high level IPv6 Readiness Assessment program, which will better position the organization for deciding the details of the later stage of planning and implementation.

This section presents two types of guidelines:

1. IPv6 Readiness Levels Assessment Guidelines
2. IPv6 Adoption Plan Guideline

These guidelines took much from the work that has been done by both of the **Alliance for Telecommunications Industry Solutions (ATIS)**[14] **and other major ICT Vendors.**

5.1. IPv6 Readiness Levels Assessment Guideline

This section presents an approach for evaluating the IPv6 readiness of an organization from a **business and decision making point of view**. The IPv6 Readiness Assessment aims not at evaluating details such as ratios and numbers on low level details of the IPv6 aspects of the networking infrastructure but rather 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.

For each level of readiness, a **set of recommendations** are given that would serve as the next steps an organization should take to move to the next level in its road towards IPv6. The **recommendations** will be elements of the IPv6 Adoption Plan discussed in the next sub-section **"IPv6 Adoption Plan" (Section 6.2.).** As such, both the IPv6 Assessment level and the IPv6 Adoption Plan would be two inter-dependent and complementary phases.

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.

Table 1- IPv6 Readiness Levels with Characteristics

Level	Characteristics
Level 0	No consideration for IPv6 migration or IPv4 exhaustion
Level 1	Is considering an IPv6 adoption but no plan has been developed
Level 2	Has an IPv6 plan in place but without full identification of critical issues
Level 3	Has an IPv6 plan in place and a complete plan to address critical issues
Level 4	Already started deploying IPv6 and Addressing Critical Issues

[14] http://www.atis.org/

The suggested levels of readiness are:

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

Organizations identified as being in Level 1 are expected to eventually accomplish the following milestones:

Milestone	Section
Identify business drivers and requirements for IPv6	5.2.1.1
Identify the associated costs and risks incurred by an IPv6 adoption plan	5.2.1.2

- **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:

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

  Organizations identified as being in Level 2 are expected to eventually accomplish the following milestones:

Milestones	Section
Develop a business case and set aside a budget to implement IPv6	5.2.1.3
Establish a Transition Group to oversee the IPv6 transition	5.2.1.4

- **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:

- IPv6 infrastructure design
- IPv6 deployment plan
- IPv6 training plan
- IPv6 field trials plan

Organizations identified as being in Level 3 are expected to eventually accomplish the following milestones:

Milestones	Section
Inventory all IP aware assets	5.2.2.1
Develop an Architecture Design for IPv6 Transition	5.2.2.2

- **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:

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

Organizations identified as being in Level 4 are expected to eventually accomplish the following milestones:

Milestones	Section
Establish a Training Program	5.2.2.4

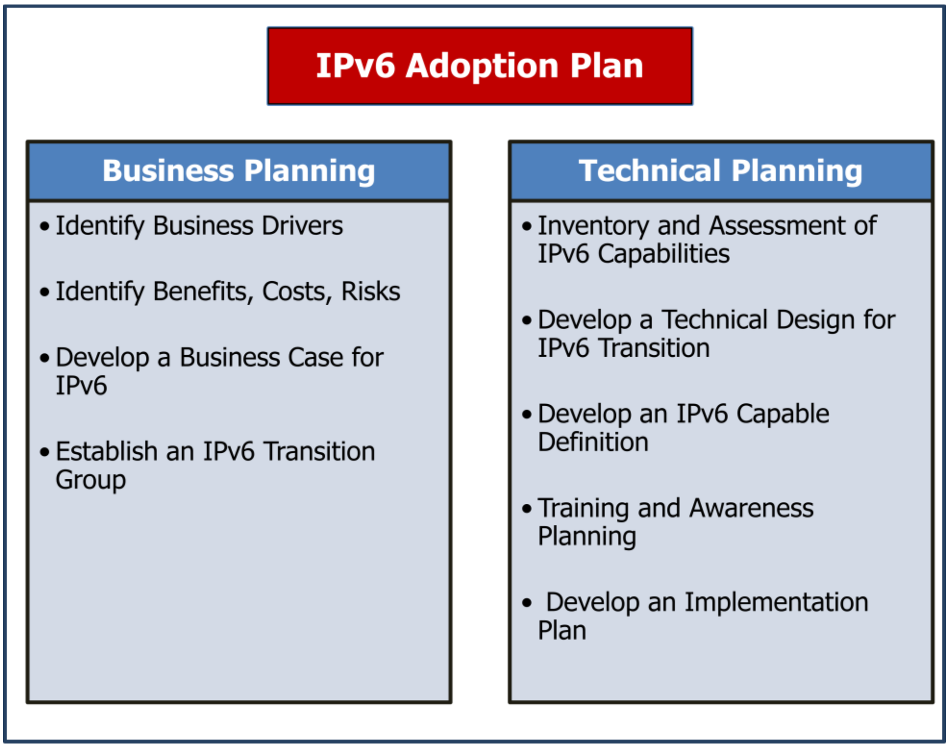
Finalize the IPv6 Implementation Plan	5.2.2.5

5.2. 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:

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

Figure 5- IPv6 Adoption Plan Tracks



IPv6 Adoption Plan

Business Planning

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

Technical Planning

- Inventory and Assessment of IPv6 Capabilities
- Develop a Technical Design for IPv6 Transition
- Develop an IPv6 Capable Definition
- Training and Awareness Planning
- Develop an Implementation Plan

5.2.1. Business Planning

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

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

5.2.1.1. 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:

- 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
- 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
- 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

5.2.1.2. 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)
  - 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

- **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:
    - 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 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:
    - 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

The National Institute of Standards and Technology (NIST) study "IPv6 Economic Impact Assessment"[15] 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.

The study also noted that in the US, most of the costs would be incurred by users (approximately 92%) with ISPs and vendors accounting for 0.5 and 8% respectively. **Table 2** below as taken from the study details the percentage distribution costs of a transition to IPv6 incurred by users.

Table 2- Distribution of IPv6-Related Transition Costs for Users[16]

	Distribution of Total Transition Costs
Category	Internal Network Costs
Network management software (upgrade)	18%
Network testing	17.60%
Installation effort	24%
Maintaining network performance	16%
Training (sales, marketing, and tech staff)	24.40%

Table 3 below as taken from the study details the percentage distribution costs of a transition to IPv6 incurred by ISPs in the US.

Table 3- Distribution of IPv6-Related Transition Costs for ISPs[17]

	Distribution of Total Transition Costs	
Category	Internet Provisioning Costs	Internal Network Costs
Network management software (upgrade)	19.30%	1.20%
Network testing	18.30%	1.20%
Installation effort	10.70%	1.60%
Maintaining network performance	12.00%	1.10%
Training (sales, marketing, and technical staff)	33.00%	1.60%

- **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.

[15] http://www.nist.gov/director/prog-ofc/report05-2.pdf
[16] The percentages in this table sum to 100 percent, comprising the distribution of all costs necessary for users to move to IPv6.
[17] The percentages in this table all sum to 100 percent, comprising the distribution of all costs necessary for ISPs to move to IPv6.

- 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.
- 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
- Technical
  Like any technology upgrade, technical risks would 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
  - Reliability risks would arise in introducing a new IP protocol and if it will maintain the same level of reliability offered by IPv4
  - Interoperability risks in between different types of IPv6 stacks, between IPv6 and other protocols and interoperability with the present IPv4 networks

5.2.1.3. 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.

5.2.1.4. 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:

- 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

- 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

- 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. Governance should mainly address:

- Policy
- Roles and responsibilities
- Management structure
- Performance measurement
- Reporting

Organizations should decide whether or not to establish specialized sub-groups to address IPv6 aspects in a categorized form. The sub-groups could include:

- IPv6 Network Sub Working Group (SWG)
    - Routing
    - Addressing
    - DNS
- IPv6 Applications SWG
- IPv6 Security SWG
- IPv6 Network Management SWG

5.2.2. Technical Planning

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

- Inventory and Assessment of IPv6 Capabilities
- Develop a Technical Design for IPv6 Transition
- Develop Impact Analysis
- Develop an Implementation Plan
- Training and Awareness Planning

5.2.2.1. 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:

- 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

Auditing can also include:

- Contracts for presence or absence of IPv6 specific and complying language
- Procurement activities for presence or absence of terms such as: IPv6, IPv6-capable, IPv6 upgradeable, IPv6 incapable, etc.

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.

5.2.2.2. 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:

- IPv6 Addressing Plan
- IPv6 Routing
- IPv6 Interconnection (peering and transit connectivity)
- IPv6 Transition Mechanism
- Network Services
- Security
- OSS, BSS and Network Management
- Applications
- Scalability and Reliability
- Service Level Agreements (SLAs)
- Testing

The above lists most of the major areas but is not meant to be an exhaustive list.

- **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.

- **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.

- **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 will interconnect its internal sites.
  Existing IPv4 interconnections to other networks (public and private peerings, 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 (relates to ICT procurement policies).

- ## IPv6 Network Transition Mechanism and Strategies

  Organizations should 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. Organizations shall consider that following elements:

  - Current network infrastructure
  - IPv6 traffic forecast
  - IPv6 capable applications/end systems,
  - IPv6 deployment plan

  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

  IPv6 network transition strategies are high level approaches related to where the IPv6 implementation starts and its propagation and these include:

  - **Core-to-edge:** transition in this case begins at core backbone sections of the network and propagation of IPv6 implementation propagates to cover other sites into Local Area Networks (LANs), end stations and finally to the applications
  - **Edge-to-core:** transition in this case follows an opposite approach to the previous one with IPv6 implementation starting at the applications and end stations and propagating towards the core backbone networks

  Other types of network transition strategies are geographical where transition occurs based on the geographical location of the network and Subnet where transition is aligned with network subnet segments.

- ## Network Services

  Organizations 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, Authorization & Accounting (AAA)

- ## Multi-homing

  Organizations that are currently multihomed for IPv4 need to evaluate the potential approaches to multihoming with IPv6.

  Fundamentally, the options are very similar in IPv6 to IPv4:

- BGP multihoming with provider independent (PI) or an organization’s own LIR address space
- Multihoming to two different providers, using address space from both providers.
- Multihoming with multiple links (for redundancy) to the same provider, using address space from the provider. This will not give provider redundancy, but will protect against a single link outage.

- **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. The current model of security is enclave based and centrally administered. However, it is expected that future models will push security towards the hosts and be integrated with policy-based networking. Security models during the IPv4/IPv6 coexistence may look very differently from the future IPv6 more dominant internet and as such, organizations should plan to evolve their security architecture throughout their IPv6 migration process.

As more 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.

IPv6 networks will face similar security challenges faced by IPv4. However, the organization should 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 organization’s network infrastructure to external threats. Special attention should be given to automated tunneling applications or services. To minimize 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
- Organizations not leveraging new security features

A security transition plan should be closely developed and coordinated with both the overall IPv6 transition process and the **organization’s existing security policies and practices**. The plan should include but not limited to the following:

- Threats, Vulnerabilities and Risks
  - Threats to be covered and addressed and primarily the same faced by IPv4 based networks. New threats should be identified as IPv6 is deployed in new areas and services such as wireless and others
  - Vulnerabilities that are unique and specific to IPv6
  - Risks (likelihood of successful attacks)

- Mitigation and management techniques (technical, procedural and others)
- Recommended approaches to enhance the overall security status and levels
- Security tools: Organizations should assess the available security options in the market
- Certifications and Accreditations: Organizations should investigate the required Q&A procedures

- **OSS, BSS & Network Management**
  Operations Support Systems (OSS), Business Support Systems (BSS) and Network Management Systems (NMS) will require modification in order to support the IPv6 capable infrastructure. Any system that monitors and manage IPv4 networks, modes and traffic will require such a modification to support the same management functionalities for IPv6.

- **Applications**
  Organizations should identify the applications it needs to interoperate with IPv6. This includes Operating Systems, databases and applications. 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. An applications IPv6 transition plan includes the identification of:

  - Application requirements: functionality requirements, standardized APIs, IPv6 capability requirements, Dual use (IPv4 & IPv6) or single use (IPv4 or IPv6), IPv6-capable transition requirements

  - Transition approach: One set of applications that support both IPv4 & IPv6, Separate applications running in native IPv4 or IPv6 mode, Timing of application transition with network transition

  - Application audit & analysis: identify all applications in use within the agency today, determine if they are impacted, identify method of transition

  - Application Transition Resources and these include:
    - Personnel that will modify the applications
    - Contractor
    - Internal
    - Budget considerations
    - Prioritization versus other upgrades and patches
    - Rolling in new versions of software

  - Support for legacy applications:
    - Length of time they will be supported
    - Transition mechanisms to be used to extend life

- **IPv6 New Features**
  Organizations should evaluate how to benefit and leverage on the new features introduced by IPv6 such as: Much larger address space (more flexibility in network design and implementation), Stateless Address Auto-configuration (SLAAC), Mobile IPv6, flow label, etc.

- **Service Level Agreements**
  Organizations should develop Service Level Agreements (SLAs) that reflect the changes incurred by introducing IPv6. This includes SLAs that reflects IPv6 policies and service level requirements for both IPv4 and IPv6

- **Testing**

Testing is a critical activity that needs to be performed when introducing a new technology especially when the scope of introduction is as pervasive and comprehensive as is the case with IPv6. Organizations should introduce a clear, comprehensive and solid testing program to verify their ongoing and final IPv6 deployments. A testing program could potentially save organizations from facing operational problems arising in the future from bad IPv6 implementations. Testing should address every implementation and be done prior to introduction into production networks so avert any possible unwanted impacts.

A testing plan should be based on the organization's definition of what "IPv6 Capable" is (see next section). It is essential that organizations keep in close contact with their vendors during testing to report and resolve any problems that arise.

Integrating the organizations IPv6's testing environment with other stakeholders IPv6 testing environments will leverage testing capabilities, share resources and help reduce costs and budgetary requirements. Connecting several IPv6 test labs would create an IPv6 testing network.

A typical testing plan should address planning and implementation aspects of testing and includes but is not limited to the following:

- **Test strategy**
  - Identification of which implementations will be tested and which will not be tested along with justifications
  - Decision between Industry-based or agency-based testing guidelines
  - Establishment of Overall testing timelines and frames

- **Testing methods** which could include:
  - Conformance: Testing of an element in isolation based on a set of standard specifications for protocols, hardware and software
  - Interoperability: Testing to determine if the hardware and software interact properly with other elements within the enterprise and interconnected networks
  - Performance: Testing the hardware and software performance based on a set of stress criteria
  - Functional: Testing the functionality of the hardware and software in an operational-like environment based on a set of system requirements
  - Operational testing: Testing the hardware and software in limited operational settings such as pilots and field trials

- **Types of testing**: analysis, modeling & simulation, lab, pilots, proof of concept, etc.

- **Testing Prioritization and synchronization**
  - Identification of testing priorities
  - Identification of any testing order schemas
  - Identification of testing with the available capabilities

- **Testing schedule** that details when tests will be performed and results expected

- **Testing reporting requirements**
  - Identification of types of reporting and templates
  - Identification of mandatory and voluntary reporting

Organizations should establish a matrix in order to help identify the overall scope of the testing required, the methods (as discussed above), environments (and personnel assigned for these tasks.

Local stakeholders should not limit their testing resources to those within the organization but should rather seek to share and utilize testing results and methodologies already adopted by other stakeholders. This sharing approach, as expected, would reduce costs and budgetary requirements in addition to the possibility of fine tuning and improvement of testing methodologies by accumulating over previous experiences.

5.2.2.3. Develop an IPv6 Capable Definition

Organizations should define what "IPv6 Capable" is for each platform and service in the organization. Organizations should develop their own IPv6 compliance standard for each IP aware platform and service. The development of this own IPv6 compliance standard should be based on commercial and industry standards best practices. For all platforms and systems needing to transition to IPv6, the following impact analysis should be initiated:

- Assess when such platforms will be IPv6 ready
- Determine the required resources for equipment upgrades, training, budgeting, etc
- Identify the impact to the supporting services and customers

5.2.2.4. Training and Awareness Planning

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

The developed training plan should address and specify:

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

- The Training Content and Material which should not be one track but varied into several types:
    - **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 would be to manage and operate IPv6 capable networks
    - **Specialized** training targets subject matter experts (SMEs) and is geared towards by specific and focused IPv6 related aspects such as mobility, security and other specific areas

- The delivery mechanism which could include:
    - Centralized training sessions
    - Internal or external training workshops
    - Industry conferences
    - Vendor sponsored training
    - Outside classroom training
    - In-house training provide by experts

- The Training schedule
    - What types of training are required and when?
    - Who needs to be trained and when?

  - When should training materials and logistics be available and in place

- The Training resources
  - The instructors and IPv6 qualified personnel to undertake the training sessions
  - The sources of IPv6 training materials which could include:
    - ICT Vendors' IPv6 technology guidelines, white papers
    - IPv6 dissemination material of major IPv6 deployment and research projects (6bone,6net and others)
    - Internal IPv6 established courses by IPv6 qualified ICT personnel

5.2.2.5. Develop an Implementation Plan

Organizations should develop an overall implementation plan for the whole of the organization. The plan should include the following elements:

- Identify a list of projects to be implemented along with dependencies and a prioritization ranking of these projects
- Establish an IPv6 testing environment for hands-on experience, verification of network architecture plans, designs and IP aware devices and assets that need to be tested or verified in an IPv6 environment before deployment in production networks
- Prioritize IPv6 deployment and ensure it is included within the IT/Networking infrastructure refresh and upgrade cycles

6. Network Transition Mechanisms

The transition to IPv6 affects a wide range of IT related areas in a corporation. The single area that is common to about all stakeholders migrating towards IPv6 is the network involved – as opposed to, for example, running and migrating an e-mail server, which only a subset of the stakeholders will ever do.

For this reason, this section will focus on the generic aspects of a network migration towards IPv6. Later sections will then cover migrating public services (section 8) and specific aspects for individual stakeholder classes (section 10).

Section 7.1 will cover "core network" technologies, that is, what options exist for migrating the inside part of a given network. It is mostly targeted to stakeholders running large networks, like ISPs, FBPs or larger enterprises. For smaller networks with only a single site and few routers, it can be skipped.

Section 7.2 will cover "edge network" or "access network" issues, that is, the various technologies that are used to interconnect different networks – networks to each other, ISP networks to their customers, etc. This section is important for all stakeholders that operate some sort of network infrastructure. SOHO users that don't operate their own router but get fully managed services from their ISP could skip it.

6.1. Core Network

Core infrastructures where present in organizations such as service providers and larger enterprises are mainly deployed and designed following two main paths:

- MPLS core, IPv4 packets are encapsulated in MPLS
- Native IPv4 core

This section aims at addressing IPv6 transition mechanisms that could be deployed in each of the above two cases.

The next section (7.2) will cover the edges of the network (access network) and point out aspects specific to certain access technologies, e.g. DSL or Cable Modem.

6.1.1. MPLS Core

The key element of an MPLS core is that the routers in the "middle" of the network (named "P" routers in MPSL terminology) can transport packets that they would not be able to handle natively. MPLS networks are typically used for some or all of the following services:

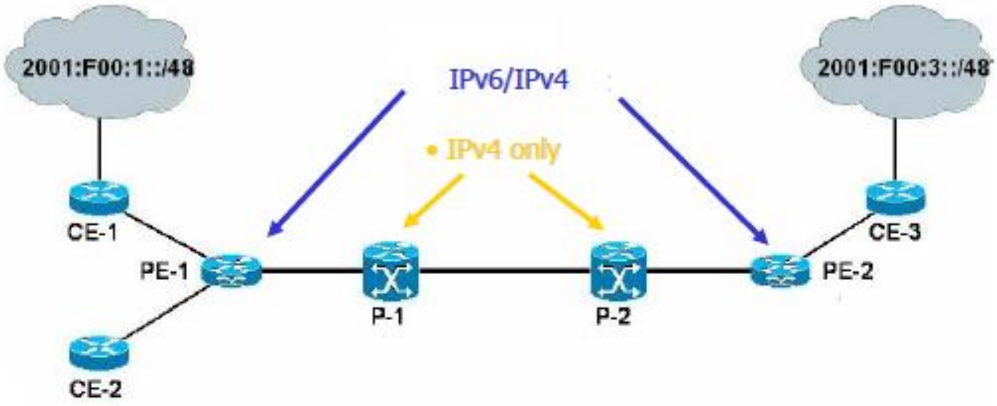
- IPv4 traffic engineering (MPLS TE is used to move the routing decision away from the P routers, and to the edge routers that set up MPLS paths across the core)
- IPv4 Layer 3 VPN products for customers (MPLS is used to handle separate the routing decisions for different customers, and potentially handle overlapping address assignments. Again, the edge routers do the routing decisions, not the core routers.)
- Layer 2 VPNs, where Ethernet frames (for example) are tunneled across the ISP core network to offer "transparent Ethernet circuits" to customers.

Common to all scenarios is that the P routers have no knowledge about the IPv4 or even layer2 addresses in the packets that are transported across the network. All switching is done based on the

MPLS labels that the edge routers ("PE" routers in MPLS terminology) prepend to the packets – which implies that the edge routers need to understand these protocols, of course. Given this basic infrastructure, addition of IPv6 is fairly straightforward. Two techniques are common to add "full IPv6 routing" to an ISP MPLS network:

- **6PE**

  6PE is typically deployed by ISPs or other large network operators that have an existing MPLS core network and already support MPLS VPNs.6PE is a good transition mechanism when the ISP or enterprise organization wants to avoid either to fully upgrade its core network or to deploy IPv6-over-IPv4 tunneling. As requirement to deploy 6PE, the ISP or organization has to upgrade the provider Edge (PE) routers to support IPv6. However, and quite important for an IPv6 roll-out with little impact to the rest of the network, the Core (P) routers don't need any changes in terms of configuration or software

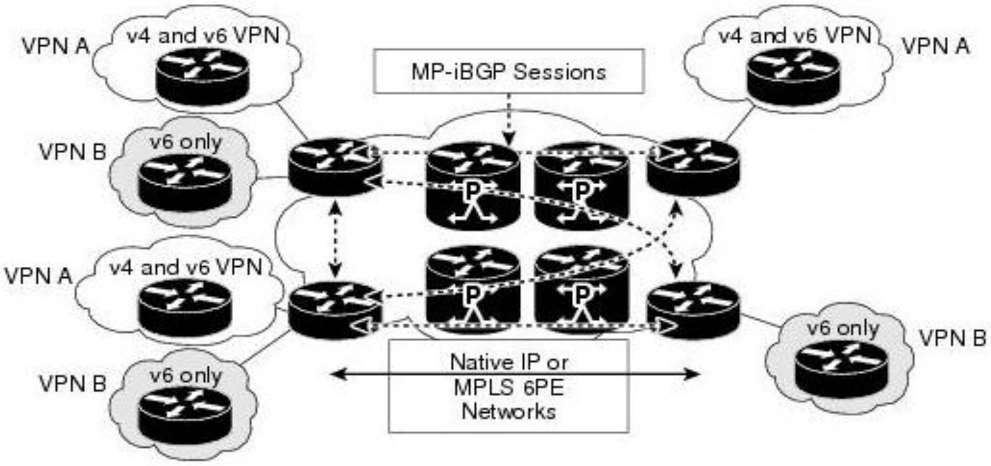


  The customer Edge (CE) routers and PE Routers that are running IPv6 are connected with logical or physical native IPv6 interfaces. Exchange of routing information between CE and 6PE routers is done with the normal IPv6 routing protocols – for example, OSPF or eBGP dynamic routing, or statically configured routes. From the customer edge perspective, 6PE is indistinguishable from a fully native IPv6 backbone at the provider.
  6PE is providing native IPv6 services to customer without changing the IPv4 MPLS core network, thus minimizing operational cost and risk.
  While 6PE is typically deployed by backbone providers (ISP/DSP), it can also be deployed by a large enterprise backbone to interconnect the different locations of the enterprise. In this case, the "customer edge" would be every individual location, while the "provider edge" is the interconnecting network, run by the enterprise backbone network group. The same technical considerations apply.

- **6VPE**

  6VPE is a transition solution that smoothly introduces IPv6 VPN service in a scalable way, without any IPv6 addressing restrictions. It does not jeopardize a well-controlled service provider IPv4 backbone or any customer networks. VPN service backbone stability is a key issue for those service providers who have recently stabilized their IPv4 infrastructure. For IPv4 VPN customers, IPv6 VPN service is the same as MPLS Layer3 VPN for IPv4.

  The IPv6 MPLS VPN service model is similar to that of IPv4 MPLS L3 VPNs. Service providers who have already deployed MPLS IPv4 VPN services over an IPv4 backbone can deploy IPv6 MPLS VPN services over the same IPv4 backbone by upgrading the PE router IOS version and dual-stack configuration, without any change on the core routers. IPv4 services can be provided in parallel with IPv6 services. A PE-CE link can be an IPv4 link, an IPv6 link, or a combination of an IPv4 and IPv6 link (dual-stack), as shown in the following diagram:



- **Ethernet-over-MPLS**

Tunneling of customer packets via transparent Layer 2 circuits (Ethernet-over-MPLS, AToM, etc.) does not require any changes at any part of the MPLS network to enable IPv6 capability, and thus, such technologies are agnostic to the introduction of IPv6 and do not need to be covered here.

6.1.2. Native IPv4 Core

For service providers or large networks operating a core network without MPLS, IPv6 capabilities need to be engineered into the existing network. Consideration needs to be given to the costs of implementation and the risk of service interruption by modifying a production network to support a completely new service (IPv6).

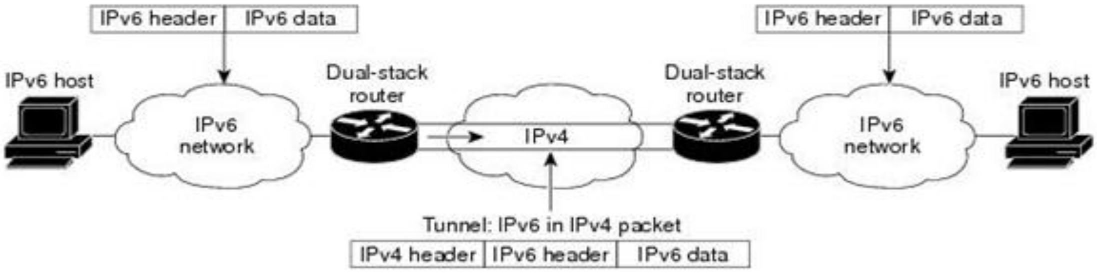
A number of different approaches exist that will be explained in the following sub-sections. At the end of this section, a comparison table summarizes benefits and drawbacks of each individual approach.

- **Tunneling IPv6 in IPv4**

IPv6 tunneling enables IPv6 hosts and routers to connect with other IPv6 hosts and routers over the existing IPv4 Internet. IPv6 tunneling encapsulates IPv6 datagrams within IPv4 packets. The encapsulated packets travel across an IPv4 Internet until they reach their destination host or router. The IPv6-aware host or router decapsulates the IPv6 datagrams, forwarding them as needed. IPv6 tunneling eases IPv6 deployment by maintaining compatibility with the large existing base of IPv4 hosts and routers.

IPv4/IPv6 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Tunneling can be used in a variety of ways:

1- **Router-to-Router:** IPv4/IPv6 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes.
2- **Host – to – router:** IPv4/IPv6 hosts can tunnel IPv6 packets to an intermediary IPv4/IPv6 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path.
3- **Host – Host:** IPv4/IPv6 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes
4- **Router – Host** IPv4/IPv6 routers can tunnel IPv6 packets to their final destination IPv4/IPv6 host. This tunnel spans only the last segment of the end-to-end path.

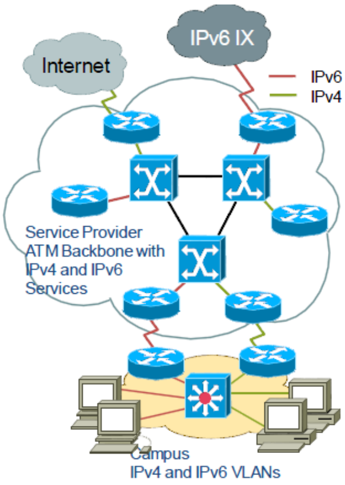


The benefit of tunneling IPv6 in IPv4 is that it is a quick and easy way to implement IPv6 connectivity between nodes without having to upgrade the IPv4-only infrastructure between the IPv6 nodes.

Possible drawbacks of tunneling include path MTU problems (due to extra overhead of the additional tunneling header), bad performance (due to processing overhead in the encapsulating or decapsulating routers) and troubleshooting impairments (due to the topology hidden by the tunnel). Also, tunnels can lead to extra latency if the endpoints are selected without care.

In general, IPv4-in-IPv6 tunneling is recommended only as a first step to gain momentum. In the medium term, tunnels should be migrated to dual-stack IPv4+IPv6 topology, as explained in the next sections.

- **Native IPv6-only infrastructure**


IPv6 IX
Internet
IPv6
IPv4
Service Provider ATM Backbone with IPv4 and IPv6 Services
Campus IPv4 and IPv6 VLANs

If the existing IPv4 infrastructure cannot be upgraded to support IPv6, and tunneling solutions are undesirable, Native IPv6 could be deployed on dedicated IPv6-only data links. Some examples for different applications in an enterprise are explained in the following scenarios:

1- Dedicated Data links between core routers inside the organization infrastructure.
2- Dedicated Data Links to IPv6 customers; in this scenario an IPv6 dedicated link will connect the CE router to the organization or the ISP using IPv6 addresses
3- Connection to global native IPv6; in this scenario a dedicated IPv6 link will be used to connect the Internet gateway to an International internet Exchange.

To deploy IPv6-only machines in some portion of the corporate network would require network address translation between the IPv6-only portion and the ”legacy” IPv4 portion, including the rest of the Internet. It is thus recommended to postpone deploying IPv6-only networks at edge networks (offices, enterprises) to a later state, when a larger part of the core Internet is IPv6 capable. The preferred approach is thus Dual-Stack IPv4 and IPv6, as detailed in the next section.

- **Dual Stack IPv4-IPv6**

Dual stack IPv4-IPv6 refers to the deployment scheme whereby network nodes incorporate both IPv4 and IPv6 protocol stacks in parallel. A dual-stack node has complete support for both protocol versions. IPv4 applications will use IPv4 and IPv6 applications will use IPv6. Dual stack helps with the basic incompatibility of IPv4 and IPv6: IPv4 nodes cannot communicate to IPv6 nodes and vice-versa. In communication with an IPv6 node, such a dual-stack node behaves like an IPv6-only node; and in communication with an IPv4 node, it behaves like an IPv4-only node. Thus, a dual-stack node can communicate with both IPv4 and IPv6 nodes, which is clearly a useful capability.

In this scenario, routers must be configured to allow for both: IPv4 and IPv6 forwarding.

Depending on the routers currently in use in the network that should be dual-stack enabled, different measures need to be done:

- If the router hardware does not support IPv6, the routers need to be exchanged. Fortunately, most major router vendors have shipped IPv6-capable hardware for a number of years, so the normal procurement/upgrade cycles usually have made sure that IPv6 capable hardware is available.
- If the operating software on the routers does not support IPv6, a network wide software upgrade must be planned, lab tested, and implemented.
- IPv6 addresses need to be added to all IPv4 links (in the network, and towards customer edges) to make them dual-stack.
- IPv4 routing protocols need to be extended to be IPv4+IPv6 dual-stack (e.g. for BGP or IS-IS) or IPv6 routing protocols need to be run in parallel to IPv4 (OSPFv3).
- The network monitoring needs to be upgraded to monitor IPv6 availability and quality as well as IPv4

Obviously, this is more work than setting up IPv6-over-IPv4 tunnels. Nevertheless, in the long run this is a much better sustainable strategy than tunneling, because it is easier to monitor and assure IPv6 network performance. Especially when IPv4 stops being the dominant protocol, it is well-advised to not build networks that rely on IPv4 as the underlying infrastructure for tunnels.

- **Comparison between approaches**

Transition Approach	**Benefits**	**Drawbacks**
IPv6 tunnels over IPv4 infrastructure	• Rapid deployment • IPv6 can be deployed at the network edges without hardware/ software / configuration changes to the intermediate nodes • IPv6 test networks can be interconnected over existing IPv4 infrastructure without affecting production IPv4 network	• Dependency on IPv4 network: operational problems with IPv4 routing or transport directly affect IPv6 • MTU problems: extra overhead due to tunneling header reduces available packet size for IPv6, and can cause hard to trace operational problems (path MTU discovery, black-holing) • Tunnel topology typically does not reflect physical topology, so IPv6 routing can be worse than IPv4 routing (longer paths, higher latency, worse performance) • Encapsulation and decapsulation typically cause higher CPU load on edge routers • Scalability limitations when the number of IPv6 edge routers (= tunnel end points) grows • Higher operational expenses to maintain
Dedicated IPv6-only infrastructure	• Fully independent IPv4 and IPv6 infrastructure, so problems with IPv6 technology cannot impact IPv4 network	• Higher expenses due to extra physical links and extra hardware required • Typically worse performance for IPv6 due to non-optimal topology • Higher operational expenses due to extra network components and different topology for IPv6 and IPv4 • Traffic shifting from IPv4 to IPv6 requires network hardware changes (upgrading of IPv6 access links, even if enough bandwidth available on IPv4 links)
Dual-stack IPv4 + IPv6	• IPv4 and IPv6 routing protocols and packet forwarding are fully independent • IPv6 can be monitored without dependency on underlying IPv4 effects • Optimum routing paths and best performance for IPv6 is much easier to achieve • Scalability for IPv6 as good as for IPv4 (that is: no extra scalability concerns introduced by migration technology) • Future migration path to IPv6-only network	• Much higher effort for initial set up • operational changes throughout the whole network needed

The benefits and drawbacks in the previous table lead to the following recommendations for the typical cases:

- for the initial experiments and tests, use tunneling technologies to quickly set up IPv6 connectivity and gain operational experience
- for the production network, use dual-stack IPv4 + IPv6 whenever possible, to achieve full performance and lower operational cost for IPv6.
- Dedicated IPv6-only links should only be used in exceptional circumstances.

6.2. Access Networks (Edge Networks)

The term "Access Networks" or "Edge Networks" describes the technology used to connect different networks together. Examples of these include:

- Peerings between ISPs or DSPs
- Connection of customers to their ISP by DSL, Wireless, Fiber, etc.
- Connection of ISPs to larger (transit/upstream) ISP networks
- Interconnection of different sites in an Enterprise network

The challenges faced at the network edge are similar to section 7.1.2, "Native IPv4 core", because the most common case for an existing access/edge network is "IPv4 only". Everything explained in this section about the considerations and recommendations for moving towards a dual-stack network applies here as well, especially for the migration approaches:

- IPv6 tunneling to circumvent IPv4-only devices that cannot be upgraded
  - Potential tunneling mechanisms could, for example, be 6to4, Teredo, 6rd or manually configured tunnels
  - A point of reference for this is the French DSL provider "free"[18] that is using the 6rd tunneling technique to tunnel around IPv4-only DSLAMs, until the DSLAMs can be upgraded.
- Enabling dual-stack IPv4 and IPv6 in the Infrastructure where applicable
  - This is the recommended long-term approach.

One important difference between network edges and network core is that the number of different technologies seen at the network edge is much higher, and some of them need to be given special consideration:

- DSL and dialup technology using PPP/L2TP
  - PPP is fully capable of running in a multi-protocol environment, so enabling IPv6 can be done by upgrading the PPP endpoints only. The Infrastructure and technology does not have to be changed.

[18] http://www.free.fr/

- For account provisioning, the RADIUS backend systems at a service provider that provides PPP-based access might need to be extended to handle IPv6 configuration.
- For providers that want to do dynamic assignment of IPv6 addresses to their customers (as opposed to static configuration on the PPP client device), the DHCP-PD technology can be used to dynamically and automatically delegate an IPv6 network prefix (e.g. a /56 or /48) towards the customer network. (DHCP-PD = Dynamic Host Configuration Protocol / Prefix Delegation)

- Cable Modem
  - Cable modems follow the DOCSIS standard. DOCSIS version 3.0 contains specifications how to run IPv6 on cable networks and should be used as a technology reference. Upgrades to the cable modems and cable head-ends might be necessary to get support for DOCSIS 3.0.
- Fiber connections, digital SDH (E1, E3, …) lines, MPLS based products
  - These links are normally transparent to the type of data transported. So in most cases it is sufficient to enable IPv6 in the devices on both ends to enable dual-stack IPv4 and IPv6 connectivity on these links.
  - MPLS based access technologies, like Layer 2 VPN or Layer 3 VPN solutions, usually don't present the MPLS packet layer to the network edge, but are used underneath. The "customer" or "edge" side is plain Ethernet (L2 VPN) or normal IP (L3 VPN), and therefore no special consideration is needed for the underlying MPLS. The network core side needs to be approached differently with MPLS, of course, and is handled in the previous section.
- Wireless connections (WLAN, WiMax)
  - For wireless access links, the feasibility of enabling IPv6 depends on the specific adaption of the network layer to the wireless layer. If the wireless technology uses standard Ethernet or PPP framing, enabling IPv6 is as straightforward as for the already-mentioned technologies. Details on the technical implementations should be discussed in specialized forums for the respective technology (WiMAX forum, etc.)

7. Public Services transition considerations

This section gives an overview of the public main services of DNS, Web and Mail in the context of IPv6. An overview on what should be done on each is given.

Section 11.3 in the appendix has step-by-step check lists to help in deploying these recommendations.

7.1. 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.

Example DNS entry, as used for the Saudi-Arabian IPv6 Task Force web site:

```
www.ipv6.org.sa  A  86.111.196.86
                 AAAA  2001:1490:100:23::10
```

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:

- 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.
- the country code (ccTLD) **top level domain 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). For the Saudi-Arabian ".sa" domain, please see the document IPv6 D1 for a detailed assessment and the Saudi Arabian IPv6 road map (D5) for proposed implementation measures.

7.2. 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 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.
- enter the IPv6 address of the machine (AAAA record) into the DNS server (see section 8.1, DNS)

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 out of scope for this document, but basically it's similar to the single machine case:

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

7.3. 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, 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.

- Test with a "friendly user" base
- 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 roll-out of IPv6-enabled E-Mail-Services are not hindered by vendors that are slow to upgrade their appliances.

8. 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:

- too many components affected
- too many service affecting changes at the same time
- not enough human resources to do large number of changes at the same time
- no business case for converting specific parts of the network right away
- show-stoppers in converting specific parts of the network, e.g. "extra license fees for IPv6 on gear that is going to be replaced next year anyway" or "no IPv6 available yet for www load-balancer in use"

For this reason, most networks will do a phased adoption, with some parts first and other parts later.

The feasibility of a phased adoption very much depends on the specifics of the network in question, but in general, there are a few typical scenarios that are to be expected.

- **Example 1**: a small enterprise that is co-locating their corporate web server in a different datacenter, and not in their own office network. The provider that delivers IP connectivity to their office network has no IPv6 offerings yet, but the provider for the datacenter that hosts the WWW server is offering IPv6.
  For this scenario, enabling IPv6 on the WWW server is fairly easily and quickly done, but enabling IPv6 on the office network has to wait for the ISP to deploy IPv6 (or needs changing ISP)

- **Example 2**: an Internet Service Provider (ISP) that has received a few customer requests for IPv6 but has only limited resources for IPv6 related work available.
  In this case, the ISP might upgrade those parts of the transport network that are needed to get IPv6 connectivity to those pilot customers, but might not be able to upgrade everything else in their network (DNS servers, Mail servers, WWW servers, etc) at the same time.

- **Example 3**: the DNS registrar for a country top-level domain (e.g. .SA) has IPv6 capable machines, has well-trained personnel, but cannot get IPv6 connectivity from their provider.
  In this example, the DNS registrar could opt to prepare all their systems to handle IPv6 records in the registry database (e.g. Glue records with AAAA addresses), and prepare all their machines to be IPv6 compliant, while waiting for their provider to get ready. In parallel, to get IPv6 transport to their top level name servers, the registrar could run a secondary name server hosted at a different provider that already has IPv6 connectivity.

- **Example 4**: a large DSL-based Internet provider that wants to offer IPv6 connectivity to all their end customers, but is deploying IP DSLAMs that cannot easily be upgraded to handle IPv6 packets.
  This provider could implement IPv6 in their backbone network (dual-stack), and then set up IPv6-in-IPv4 tunnels towards the ISP-provided router at the DSL customer site (CPE router). This way, the customer can receive IPv6 connectivity without having to worry about tunneling (the tunnels are all handled by the provider gear) and the provider can upgrade the rest of their network without haste.
  (This is the way the second-largest French ISP, http://free.fr/ is deploying IPv6 with good success)

- **Example 5**: a very large enterprise is not yet seeing much demand for IPv6 on their external web services, but they have high operational costs due to IPv4 constraints in their existing network (RFC 1918 address collisions in VPNs and between sites after mergers, subnet size management, etc.).
  For this network, deploying IPv6 internally just to be able to enjoy the cost savings due to the larger address space and avoidance of VPN address collisions would give direct benefits, while external connectivity to "the Internet" could still be IPv4-only, using an IPv4/IPv6 dual-stacked proxy for their Internet gateway (IPv6 to the inside clients, IPv4 to the world).
  (This is what Microsoft is doing internally)

Eventually, all these scenarios will lead to full IPv6 deployment on all parts of the network, at which point the work can start to remove IPv4.

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

9. Different Stakeholders Considerations

This section zooms into special considerations related to different types of stakeholders. The Internet Engineering Task Force IPv6 Operations Working Group (v6ops) identifies four types of networks:

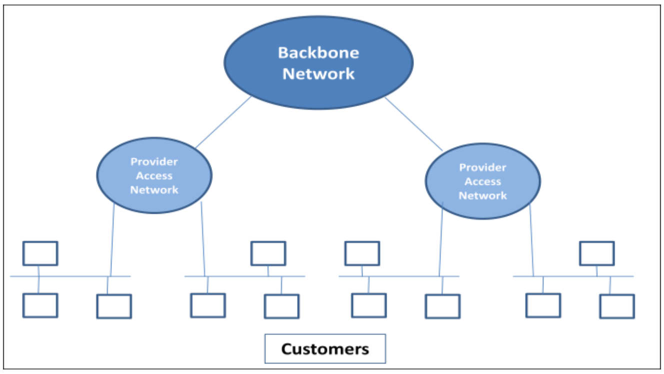
- ISPs
- Enterprise Networks
- Unmanaged Networks (such as SOHO and residential users)
- Cellular Networks

Much of the presented material in the following sections rely on work done by the Engineering Task Force IPv6 Operations Working Group (v6ops) published RFCs which are still not standards but rather categorized as informational.

9.1. Service Providers

Figure 6 presents a general overview of an internet service provider network topology, which consists of:

Figure 6- General ISP Network Layout



- **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
- **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 RIPE, typically a /32 prefix. Other preparatory steps include establishing IPv6 connectivity with an upstream provider and IPv6 peering. In the case of Saudi Arabia, regular ISPs are required to obtain IPv6 upstream connectivity from one of the FBPs.

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. **MPLS core and IPv4 native core IPv6** transition mechanisms have been addressed in section 7.1.

At this stage, and as earlier stated, 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

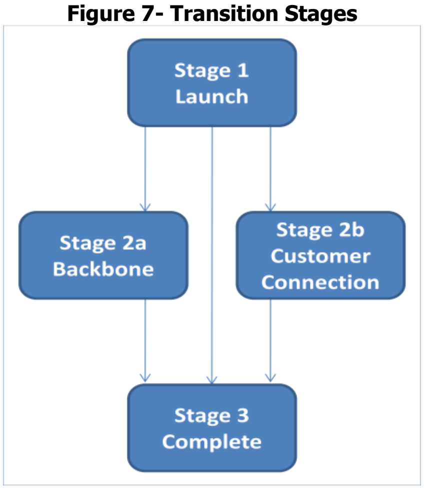
At this stage, and opposite to the previous one, the backbone supports IPv4 only while the access network supports both IPv4 and IPv6. Unlike the previous stage, the customer can establish native IPv6 connectivity to the ISP.IPv6 traffic is eventually transported at the IPv4-only backbone by tunneling 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.

Figure 7- Transition Stages



The transition will start at stage 1 and could possibly proceed into three different directions (2a or 2b or 3). So 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.

The topology of the network could be different for each of IPv4 and IPv6. This means some links may be dedicated for IPv4-only traffic while others for IPv6-only traffic or some routers maybe dual-stack while others maybe IPv4-only while others IPv6-only. In such a case, the routing protocols should be configured to deal with multiple topologies.

One of the decisions that should be made is whether the IGP process should be separate or the same for both of IPv4 and IPv6. Having a separate routing process ensures that in case IPv4 routing goes down, the IPv6 routing process stays running. This comes at the expense of more memory and CPU resources for route calculations.

Possible combination scenarios for separate routing processes are:

Figure 8- Separate Interior Routing Processes Combinations (excluding the less used RIP and RIPng options)

IPv4	IPv6
OSPFv2	OSPFv3
OSPFv2	IS-IS
IS-IS	OSPFv3

For same routing process, the scenario is IS-IS for both IPv4 and IPv6.

Decision on whether to have a separate or same routing process depends on the risk expectation of the network designers for the routing infrastructure. If no risk factors are perceived, it is recommended to go for a same routing scenario as this saves time and OPEX by not managing two different routing protocols and topologies.

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.

Other important considerations for service providers addressed in this document are those related to Network and Service Operations. The following set of activities falling under network and service operations must be addressed for IPv6 compatibility as far as IPv6 is concerned:

- Setting up IPv6 connectivity to upstream providers and peers
- IPv6 network device configuration
- IPv6 network Management
- IPv6 Monitoring
- IPv6 Customer Management
- IPv6 network and service operation security

Some of the above operations might require native IPv6 transport and some will not. For example, some monitoring functions require the availability of IPv6 transport. This is the case when ICMPv6 message are used by the monitoring applications. Regular network device configuration and other routine management operations can be performed over an IPv4 transport at the beginning.

9.2. Enterprise

This section aims at presenting IPv6 transition considerations at the Enterprise type of stakeholder as per the work done by the IETF RFC 4057 "IPv6 Enterprise Network Scenarios".

It should be noted here that it is not realistic to define every possible IPv6 transition or adoption enterprise scenario. Every enterprise has to decide its own scenario based on its current status and its business needs.

The following is non-exhaustive list of ICT aspects that need to be addressed at the enterprise as far as IPv6 is concerned:

- **DNS**

  DNS operations have now to support both IPv4 and IPv6 DNS records. The enterprise needs to determine all current DNS IPv4 operations and investigate which ones are supported for IPv6 and which are not. For technical details on aspects that need to be addressed while adapting a DNS system to IPv6, please refer to the work done in the earlier section 8.1.

- **Routing**

  IPv6 routing aspects at the enterprise are similar to those faced by the internet service provider.
  Interior and Exterior Routing Protocols will be required to support both IPv4 and IPv6 protocols as well as the coexistence of both protocols in the network. Other aspects include the routing topology, ingress and egress points to provider networks and transition mechanisms including those adopted between the enterprise and the upstream provider. For a more thorough overview on routing issues, please refer to section 10.1. Service Providers

- **Configuration of Hosts**

  The enterprise will have to determine if it will use stateless or stateful configuration for its network hosts. Other considerations include how auto configuration will operate for DNS updates, how prefix delegation will be done from their upstream provider and how these prefixes will be cascaded down to the enterprise network.
  Typical cases for stateless address autoconfiguration include office networks, where it is important to have low-overhead IPv6 automatization. SLAAC only needs configuration on the routers, and no dedicated servers for DHCPv6. On the other hand, for server networks, SLAAC is less suitable due to the lack of control on the IPv6 address (the address changes if a network card needs to be replaced), so static configuration of the IPv6 addresses is better suited for most servers.
  For networks with very strict requirements regarding network access control, DHCPv6 can be deployed in a similar way to DHCPv4 – the DHCP server decides which machine is assigned what address, and keeps track of network usage. Of course this has more maintenance and setup effort than stateless autoconfiguration.

  DHCP prefix delegation is a mechanism that complements SLAAC in that the prefix to be advertised from the routers to the hosts is not statically configured, but automatically requested from an upstream router in the enterprise or at the ISP– this helps when renumbering to a new network block, because the routers do not need to be reconfigured, just the DHCP PD server configuration is adapted.

- **Security**

  Security mechanisms supported on IPv4 need to be also ported on IPv6. Adopting IPv6 should not compromise the security of the already running IPv4 network. The enterprise should closely work with their HW / SW vendors and suppliers to determine which security aspects of their infrastructure are supported as far as IPv6 is concerned and which are not. The enterprise should determine security filters and firewall requirements for IPv6 as well.

  Security elements that need to be checked and evaluated are at least:

  - Hardware firewalls – the firewall product used needs to evaluate IPv4 and IPv6 packets in a consistent way. Detailed policing for IPv4 packets but leaving IPv6 packets unchecked is unacceptable, because it opens attack paths via IPv6 transport.
  - Software firewalls – most modern operating systems include firewalls for connections to the services running on that machine. If software firewalls are part of the enterprise security policy, care needs to be taken that the products and configuration in use will also apply the same security for IPv6 as for IPv4
  - Intrusion Detection / Intrusion Prevention device. If such devices exist, they need to be upgrade to monitor for IPv6 attacks and intrusions as well as for IPv4 intrusions. If the device can only handle IPv4, a decision needs to be made according to the Enterprise security policy on whether to replace the IDS/IDP with a box that can do IPv4 and IPv6, or to remove it from the security policy altogether – but the result needs to be consistent.
  - If access lists are used in applications, like "apache" web server permit/deny rules or unix "hosts.allow" rules, these need to be maintained consistently for IPv4 and IPv6.
  - VPN client products that enable connectivity from mobile users to the enterprise networks need to be checked for IPv6 support. Even if IPv6 support is not available, the VPN client at least needs to make sure that IPv6 cannot be used to circumvent the enterprise IPv4 security policy.

- **Applications**

  Existing applications need to be adapted to IPv6.

  This basically means: assessing every single application that is used in a business critical way for IPv6 support, and if IPv6 support is not available, working with the vendor or in-house programmers to enable IPv6 support.

  No specific examples beyond the "standard Internet applications" (DNS, HTTP, E-Mail, detailed in section 8) are given, because this is an area where every enterprise knows best what sort of application is considered critical.

- **Network Management**

  Just as in the case of Service Providers, the network management operations centers of the enterprise will need to manage the introduced IPv6 network infrastructure components. Please refer to section 10.1 for more details on network management and service operations IPv6 considerations

- **Multihoming**

Multihoming in IPv6 is currently handled very similar to IPv4. See section 6.2.2.2.

9.3. SOHO

Small Office / Home Office are classified in RFC 3750 as being unmanaged networks. RFC 3750 suggests transition scenarios for such unmanaged networks usually composing of a gateway and several hosts in a single subnet. The RFC refers and investigates the four cases of:

1. A gateway with no IPv6 support
2. A dual-stack gateway connected to a dual-stack ISP
3. A dual stack gateway connected to an IPv4 ISP
4. A gateway connected to an IPv6 ISP

For cases 1 and 3 where at least one of the gateway or ISP is non-IPv6 compliant, a tunneling mechanism is required. Tunneling can be either automatic of configured.

A Configured tunneling solution gives the service provider the highest control over the tunneled IP traffic. In this case, each tunnel has to be configured at the tunnel entry and exit point manually. The manually configured tunnel option is both time and OPEX consuming in the case where a high number of IPv6 costumers are present. Configured tunnels are recommended during the early stages to support a low number of IPv6 end users. As the demand grows and more IPv6 customers need to be served, OPEX and time considerations will be higher and hence a migration to an automatic tunneling technique or dual stack is recommended.

Automatic solutions include:

- 6to4: **6to4** (sometimes written **6 to 4**) is a system that allows IPv6 packets to be transmitted over an IPv4 network (generally the IPv4 internet) without the need to configure explicit tunnels. The tunnel endpoint is automatically determined from the IPv4 address embedded in the 6to4 IPv6 address. For best results, ISPs are recommended to deploy local 6to4 relay servers (this will avoid unnecessary packet traveling, leading to higher RTTs and more load on the ISPs external links).
- Teredo: Teredo is a tunneling protocol designed to grant IPv6 connectivity to nodes that are located behind IPv6-unaware NAT devices. It defines a way of encapsulating IPv6 packets within IPv4 UDP datagrams that can be routed through NAT devices and on the IPv4 internet. Again, for best results, ISPs are recommended to deploy local Teredo relay servers.
  Teredo will be used by default by Windows Vista machines to access IPv6 servers if no native IPv6 connectivity is available.

In case 2, both the gateway and the ISP network are dual-stack enabled allowing hosts to be IPv4, dual stack or even IPv6 only.

In Case 4, a gateway connected to an IPv6 ISP, which is rather considered an advanced case of IPv6 deployment, the ISP is IPv6-only and the SOHO gateway will not be IPv4 connected. The SOHO unmanaged network hosts could be a combination of IPv4-only, IPv6-only and dual-stack hosts.

Since the service provider is not offering any type of IPv4 connectivity anymore, any interaction between the unmanaged network hosts and IPv4 hosts in the internet should be supported by an inter-protocol service offered by the provider itself. This is achieved by the provider provisioning the gateway with at least one IPv4 address over some form of IPv4-over-IPv6 tunneling. This effectively makes the gateway a dual-stack device and for the hosts of the unmanaged network, so it will be similar to cases 2 and 3 where the gateway was a dual-stack device.

9.4. End Users (Residential)

An end user internet access in a residential setup is considered a subset case of an "unmanaged network" for which the same scenarios described in the previous section 9.3 apply.

It is not expected from a home user to be managing his network and involved in any type of IPv6 related configuration. A service provider should make sure that IPv6 related matters remain transparent to the user while provisioning internet access or doing any transition from IPv4 to IPv6 as the end user at a home will not be able to manage and configure detailed IPv6 settings for his terminal device or CPE (Customer Premise Equipment).

RADIUS provisioning and DHCP Prefix Delegation (DHCP-PD) in combination with Stateless Autoconfiguration (SLAAC) can be used to remotely assign and manage IPv6 addresses for the End User network(s) with low operation overhead for the ISP.

9.5. Cellular (3GPP) Networks

The work done by the IETF addresses IPv6 considerations for connections between user equipment (handset, mobile routers) inside the mobile network and hosts in the Internet outside the mobile network. The IETF addresses both the part of the communication process inside the mobile network as well as the connection between the mobile operator edge router and internet.

IPv6 considerations between the mobile edge router and internet are very similar to that of the case of a regular ISP setting (access/edge network).

As for IPv6 considerations of connections inside the GPRS network, like the detailed specification of the signaling between a handset and the SGSN/GGSN nodes to setup an IPv6 context, these are considered out of the scope of this document, and should be discussed in the specialized forum for 3G networks (3G forum). Experience from European 3G operators suggests that 3G network equipment vendors can provide IPv6 capable equipment today, so all questions should be addressed there.

10. Appendix

10.1.IPv6 Inventory Checklist

The following checklist was developed to help the organization do an inventory of its devices / applications in relation to IPv6. The checklist should not be considered an exhaustive one as every organization should implement its own checklists. Checklists should be customized and tailored for the needs of the devices / applications of every network infrastructure context, example: special checklists for routers, NMS devices, PCs, servers. For applications, checklists could be created for databases, ERP systems and others.

Table 9- Inventory Checklist Example

Device Name	Version / OS	Device ID / Serial Number	Device Capabilities (IPv4, IPv6, Dual Stack)	Presence of Vendor / Manufacturer Upgrade plan	Required Actions to achieve dual stack capability	Indentify any reliance on IPv4 preventing adoption of IPv6 capability (OS non-IPv6, Hard coded IPv4 addressing, etc)	Identify Any technical Dependencies for IPv6 Transition (CPU, Memory, APIs, others)	Identify IPv6 characteristics that should be leveraged in case (mobile IPv6, IPSec, etc).	Indentify Risks Associated with Transition	Identify mitigation Actions for Risks	Recommended Action	Target Date for Adoption

10.2.IPv6 Readiness Levels Checklist

Table 10 below serves as a checklist reflecting the contents of section 6.1. “IPv6 Readiness Levels Assessment Guidelines”. The checklist suggests the next milestones an organization should achieve in order to move to the next level of readiness.

Level 0 in the checklist pertains to the case where none of such milestones have been achieved. Level 1 pertains to the level of readiness where only the first two milestones (6.2.1.1 and 6.2.1.2) have been achieved. In order to move into the next level of readiness, Level 2, milestones (6.2.1.3 and 6.2.1.4) must be achieved.

As the checklist shows, level 4, the highest level of readiness has all milestones checked as accomplished.

Table 10 - IPv6 Readiness Levels Checklist

Section	**Title**	**Levels**				
		0	1	2	3	4
5.2.1.1	Identify business drivers and requirements for IPv6		√	√	√	√
5.2.1.2	Identify the associated costs and risks incurred by an IPv6 adoption plan		√	√	√	√
5.2.1.3	Develop a business case and set aside a budget to implement IPv6			√	√	√
5.2.1.4	Establish a Transition Group to oversee the IPv6 transition			√	√	√
6.2.2.1	Inventory all IP aware assets				√	√
6.2.2.2	Develop an Architecture Design for IPv6 Transition				√	√
6.2.2.4	Establish a Training Program					√
6.2.2.5	Finalize the IPv6 Implementation Plan					√

10.3.IPv6 implementation checklists for public services

The following checklists are presented to aid in implementing IPv6 for public services.

A number of tasks are similar for the different types of services covered, but because every check list is supposed to cover everything that needs to be done (for the most common case), these tasks will be repeated in every check list.

10.3.1. IPv6 implementation checklist for DNS servers

Since IPv6 implementation on DNS servers has two facets (records in the DNS zones and IPv6 transport to the DNS server) there are two checklists here.

10.3.1.1. Handling of IPv6 records (AAAA) in the DNS server

Table 11 – checklist for IPv6 Records in DNS Zones

	Work / Check item	**Result**
1	set up a new sub-domain on the DNS server that can be used for tests, e.g. "ipv6.domain.com"	Zone: ________________
2	Try to enter a new host name into this zone with an AAAA record, e.g. "test.ipv6.domain.com". The IPv6 address specified is only for testing and does not need to be reachable – if no real address is available, use an address from the documentation range, e.g. 2001:db8::2 How this is done depends on the DNS software in question. For BIND, the record is entered into the DNS Zone text file ("test IN AAAA 2001:db8::2"). For Microsoft DNS, use the graphical configuration interface. For other products, check the software documentation.	Host name: ______________ IPv6 address: ____________
3	From a client machine, verify that the newly added AAAA record in the test zone is properly visible, e.g. using one of these commands: nslookup –type=any test.ipv6.domain.com dig test.ipv6.domain.com any	done: [ ]
4	If this did not show up any problems, AAAA records can now be added to the main DNS zone (domain.com) for servers that have IPv6 connectivity and need to be visible in the DNS.	conclusion, no check list item

10.3.1.2. IPv6 transport towards the DNS server

Table 12 - IPv6 Transport to DNS servers

	Work / Check item	**Result**
1	Verify availability of IPv6 connectivity towards server subnet. If no IPv6 connectivity is available yet, talk to the group that is operating the network and request IPv6 connectivity and IPv6 address range.	done: [ ]
2	Assign IPv6 address(es) out of server subnet to DNS server machine(s)	IPv6 address: ___________
3	Verify IPv6 capabilities of server operating system in use If operating system is not IPv6 capable (windows 2000 or older), upgrade to a more recent version.	done: [ ]
4	If a firewall is used before the DNS server machine, verify IPv6 capabilities of firewall in use. If existing firewall is not IPv6 capable, consider upgrading firewall, or if vendor does not offer IPv6 upgrades, consider replacing firewall with an IPv6 capable product. Optionally, consider setting up a parallel second firewall that will handle IPv6 traffic (IPv6-only firewall) until primary firewall can be upgraded.	done: [ ]
5	Configure IPv6 address and IPv6 gateway on server machine	done: [ ]
6	Permit IPv6 ping, IPv6 traceroute, and DNS queries (TCP and UDP) access from client machines used for testing on firewall (does not apply if no firewall used).	done: [ ]
7	Verify basic IPv6 connectivity to and from server using "ping" utility, e.g. outgoing towards www.kame.net and incoming from a desktop machine with IPv6 connectivity or using a public looking glass (http://www.traceroute.org)	done: [ ]
8	Verify IPv6 capabilities of DNS server software in use. If HTTP server software is not IPv6 capable (e.g. BIND 4 or very old versions of BIND 8), upgrade to a more recent version. In most cases, this is strongly recommended anyway due to security issues in old DNS server products.	done: [ ]
9	If needed, enable accepting of incoming IPv6 connections in server software configuration. See product documentation for the software in use how to do that.	done: [ ]
10	Try accessing the DNS over IPv6 transport from an IPv6-enabled client machine by querying with a tool that allows	done: [ ]

	entering of numeric DNS server addresses, e.g.: dig @2001:db8::1 www.domain.com ANY to send DNS queries to the DNS server with the IPv6 address "2001:db8::1". Verify that the result returned matches the query done over IPv4.	
11	Verify server side for dependencies on IPv4 addresses, for example in access control rules for permitted DNS clients. For most DNS servers, nothing will have to be done here.	done: [ ]
12	Open firewall for IPv6 connections from "the world" (more specific: open firewall rules to permit the same sort of incoming and outgoing connections over IPv6 that are previously permitted over IPv4). If no firewall in use, this does not apply.	done: [ ]

10.3.2. IPv6 implementation checklist for WWW servers

This checklist is meant to help in conversion of smaller setups and will not cover all extra tasks involved if the platform uses a load balancer, as the actual implementation would very much depend on the specific IPv6 implementation in the load balancer used.

Table 13 - IPv6 implementation checklist for WWW servers

	Work / Check item	**Result**
1	Verify availability of IPv6 connectivity towards server subnet. If no IPv6 connectivity is available yet, talk to the group that is operating the network and request IPv6 connectivity and IPv6 address range.	done: [ ]
2	Assign IPv6 address(es) out of server subnet to web server machine(s)	IPv6 address: ____________
3	Verify IPv6 capabilities of server operating system in use If operating system is not IPv6 capable (windows 2000 or older), upgrade to a more recent version.	done: [ ]
4	If a firewall is used before the Web server machine, verify IPv6 capabilities of firewall in use. If existing firewall is not IPv6 capable, consider upgrading firewall, or if vendor does not offer IPv6 upgrades, consider replacing firewall with an IPv6 capable product. Optionally, consider setting up a parallel second firewall that will handle IPv6 traffic (IPv6-only firewall) until primary firewall can be upgraded.	done: [ ]
5	Configure IPv6 address and IPv6 gateway on server machine	done: [ ]
6	Permit IPv6 ping, IPv6 traceroute, and HTTP access from client machines used for testing on firewall (does not apply if no firewall used).	done: [ ]
7	Verify basic IPv6 connectivity to and from server using "ping" utility, e.g. outgoing towards www.kame.net and incoming from a desktop machine with IPv6 connectivity or using a public looking glass (http://www.traceroute.org)	done: [ ]
8	Verify IPv6 capabilities of HTTP server software in use. If HTTP server software is not IPv6 capable (e.g. Apache 1.3), upgrade to a more recent version.	done: [ ]
9	If needed, enable accepting of incoming IPv6 connections in server software configuration. See product documentation for the software in use how to do that.	done: [ ]

10	Add server IPv6 address to the DNS (AAAA record), using a dedicated test domain name, e.g. www6.domain.com or www.ipv6.domain.com	done: [ ] DNS name: ____________
11	Verify visibility of IPv6 address from the client machines using "nslookup" or "dig" or similar tools	done: [ ]
12	Try accessing the web site from an IPv6-enabled client machine using http://www6.domain.com (or whatever test name was entered into DNS). If that works, verify correct operation of site. If absolute references are used in HTML code, links might point to http://www.domain.com (normal DNS name, with only IPv4 and no IPv6). In that case, either change the HTML to use relative links or statically add IPv6 address for www.domain.com to local "hosts" file.	done: [ ]
13	Verify logging and log file statistic tools used on the server side (if any), to make sure that all places will handle IPv6 addresses correctly.	done: [ ]
14	Verify server side web application for dependencies on IPv4, for example in access control, embedding in session cookies, storage of IPv4 addresses in databases, etc. – this work item cannot be specified in more detail, as the local implementations will differ widely. For many web sites, nothing at all will have to be done here, though.	done: [ ]
15	Open firewall for IPv6 connections from "the world" (more specific: open firewall rules to permit the same sort of incoming and outgoing connections over IPv6 that are previously permitted over IPv4). If no firewall in use, this does not apply.	done: [ ]
16	Remove test DNS entry, add AAAA record to standard DNS entry (http://www.domain.com).	done: [ ]
17	Monitor web site performance, and client access. If clients complain, or if web access numbers (visits/hour) suddenly drop below usual numbers, consider removing AAAA record again while investigating why problems occur.	monitoring is ongoing activity and cannot be just "ticked off"

10.3.3. IPv6 implementation checklist for E-Mail servers

This checklist will only cover the most common cases, a single "Internet facing" mail server that sends and receives mail using SMTP, and that can be accessed from clients using POP3 or IMAP protocols. For more complicated setups, like clusters or chained mail forwarders, the same principles apply, but additional steps need to be done.

Table 14 - IPv6 implementation checklist for E-Mail servers

	Work / Check item	**Result**
1	Verify availability of IPv6 connectivity towards server subnet. If no IPv6 connectivity is available yet, talk to the group that is operating the network and request IPv6 connectivity and IPv6 address range.	done: [ ]
2	Assign IPv6 address out of server subnet to e-mail server machine	IPv6 address: ____________
3	Verify IPv6 capabilities of server operating system in use If operating system is not IPv6 capable (windows 2000 or older), upgrade to a more recent version. Note: MS Exchange servers need to be upgraded to Windows Server 2008 R2 and Exchange 2007 SP1/2010 to be fully IPv6 capable.	done: [ ]
4	If a firewall is used before the e-mail server machine, verify IPv6 capabilities of firewall in use. If existing firewall is not IPv6 capable, consider upgrading firewall, or if vendor does not offer IPv6 upgrades, consider replacing firewall with an IPv6 capable product. Optionally, consider setting up a parallel second firewall that will handle IPv6 traffic (IPv6-only firewall) until primary firewall can be upgraded.	done: [ ]
5	Configure IPv6 address and IPv6 gateway on server machine	done: [ ]
6	Permit IPv6 ping, IPv6 traceroute, incoming and outgoing SMTP and incoming POP3/IMAP access from client machines used for testing on firewall (does not apply if no firewall used).	done: [ ]
7	Verify basic IPv6 connectivity to and from server using "ping" utility, e.g. outgoing towards www.kame.net and incoming from a desktop machine with IPv6 connectivity or using a public looking glass (http://www.traceroute.org)	done: [ ]

8	Verify IPv6 capabilities of E-Mail server software in use.
	If server software is not IPv6 capable (e.g. qmail), upgrade to a more recent version, install patch, or change software
		done: [ ]
		protocols in use (check/cross):
		○ SMTP

	towards an IPv6 capable version. The specifics of this action item depend on the actual protocols in use on the server. If only SMTP is used, POP3 and IMAP need not be checked. If SMTP server is IPv6 capable, but POP3 server is not, SMTP server does not need to be changed. If web access to e-mail is used, check HTTP server as well.	○ Submission (587) ○ POP3 / POP3+SSL ○ IMAP / IMAP+SSL ○ Web mail access
9	If needed, enable accepting of incoming IPv6 connections in server software configuration. See product documentation for the software in use how to do that.	done: [ ]
10	Add server IPv6 address to the DNS (AAAA record), using a dedicated test domain name, e.g. mail6.domain.com or mail.ipv6.domain.com Add MX (mail exchanger) record for test domain name to point to the same host name.	done: [ ] DNS name: ____________
11	Verify visibility of IPv6 address and MX record from the client machines using "nslookup" or "dig" or similar tools	done: [ ]
12	Configure handling of mail addresses using test domain on the server (e.g. yourname@mail6.domain.com)	done: [ ]
13	Try accessing the mail server from an IPv6-enabled client machine with the test name that was entered into DNS. Try sending a mail (SMTP/submission) and receiving of e-mail (POP3/IMAP). Try sending mails from an external, IPv6-capable sender to yourname@mail6.domain.com (the test domain) to see that mail is correctly received over IPv6. Verify that e-mail server will fall-back to IPv4 when sending to a receiver that has no IPv6 yet, by verifying that e-mail is correctly delivered to such a receiver.	done: [ ]
14	Verify logging and log file statistic tools used on the server side (if any), to make sure that all places will handle IPv6 addresses correctly.	done: [ ]
15	Verify Anti-SPAM solutions in use whether they work correctly with e-mails being received over IPv6 transport. Specifics depend on the Anti-SPAM solution in use. If Anti-SPAM solution is not IPv6 ready, upgrade. If vendor can not deliver IPv6 capable Anti-SPAM solution, consider changing vendors or running without SPAM filtering for IPv6 (most likely unsuitable for production use).	done: [ ]
16	Open firewall for IPv6 connections from "the world" (more specific: open firewall rules to permit the same sort of incoming and outgoing connections over IPv6 that are	done: [ ]

	previously permitted over IPv4). If no firewall in use, this does not apply.	
17	Remove test DNS entry, add AAAA record to standard DNS entry (http://mail.domain.com). No extra MX is needed as MX already points to mail server. Alternatively, for all domains that are received on the mail server (e.g. domain.com), an additional MX record could be added that points to an IPv6-only host name, e.g. mail6.domain.com. This is more effort to maintain, but in the case of broken SMTP senders that have problems to connect to MX hosts with IPv6, these senders can fall back to the existing, IPv4-only, MX host. Due to the extra work involved this should only be used if operational problems show up.	done: [ ]
18	Monitor E-Mail performance, and client access. If clients complain, or if e-mail frequency (messages/hour) suddenly drop below usual numbers, consider removing AAAA record again while investigating why problems occur.	monitoring is ongoing activity and cannot be just "ticked off"