Report for IDA

# IPv6 adoption guide for Singapore

*15 March 2011*

*Ref: 16946-113(p)*

analysys mason

Tech Mahindra
IT Services and Telecom Solutions

# Contents

Analysys Mason Limited and Tech Mahindra Limited maintain that all reasonable care and skill have been used in the compilation of this publication. However, to the extent permitted by law, neither Analysys Mason Limited, Tech Mahindra Limited nor the Infocomm Development Authority of Singapore (IDA) shall be responsible or liable for reliance by any person on the information, opinions, and/or conclusions contained herein, nor shall be liable for loss or damage (including any direct, indirect, incidental or consequential losses) whatsoever or howsoever arising out of the use of this publication.

Analysys Mason Pte Ltd
#10-02 Robinson Centre
61 Robinson Road
Singapore 068893
Tel: +65 6493 6038
Fax: +65 6720 6038
singapore@analysysmason.com
www.analysysmason.com

Registered in England: Analysys Mason Limited
Bush House, North West Wing, Aldwych
London WC2B 4PJ, UK
Reg. No. 5177472

# 1 Introduction

## 1.1 Background

The Infocomm Development Authority of Singapore (IDA), in its role as national planner for ICT development of the nation, is leading a national effort to drive Internet Protocol version 6 (IPv6) adoption in Singapore and encourage efficient use of the remaining pool of IPv4 addresses to minimise the risks of depletion.

To meet this objective, the IDA appointed Analysys Mason and Tech Mahindra to carry out an in-depth study to collect the data necessary to draw informed conclusions on the current status of IPv6 in Singapore.

In line with these aims, this study has been split into two phases:

- the **survey phase**, which included face-to-face interviews with a range of stakeholders in the Singapore ICT ecosystem, as well as a web-based survey of small and medium-sized enterprises (SMEs). The outputs of this phase included the identification of the following, for each category of stakeholder:
  - their infrastructure readiness
  - the dependency of their business on IP addresses
  - the progress they have made in planning for/implementing IPv6
- the **planning phase**, which involves the development of IPv6 adoption guides for each category of stakeholder, describing the key steps required during the transition to IPv6 and the technical options and approaches that are available to different stakeholder groups.

This is the final formal deliverable of the planning phase, as the survey phase documents have already been supplied to IDA.

## 1.2 High-level view of adoption guides

Sections 4 to 8 of this document set out detailed IPv6 adoption guides for the individual stakeholder groups. These guides have been developed to assist each stakeholder group in translating strategic objectives into a practical implementation guide, taking into account the findings of the national IPv6 readiness survey for Singapore, technology roadmaps and IPv4 address exhaustion. The approach taken by each individual stakeholder will have to be tailored to take account of its own status and requirements: the guides contained in this document provide information on the key decision points that each stakeholder will need to address, and the options that are available to them.

In the remainder of this sub-section, we provide a summary of the individual adoption guides for each stakeholder category.

*System vendors*

For system vendors (including hardware and software vendors), the process of integrating IPv6 into their product portfolio will be based on a phased approach spread over one to three years, depending on the nature of the product. At this point in time, a significant proportion of vendors are at an advanced state of progress in terms of supporting IPv6 in their product portfolio.[1] The products required by operators and end users to implement IPv6 (routers etc.) have been available in the marketplace for some time, as many end users are specifying a requirement for IPv6 functionality during the procurement process. From the software vendor point of view, the market requires products capable of supporting an IPv6 application program interface (API).

*Internet service providers*

For Internet service providers, the process of adopting IPv6 will be a phased approach spread across one to three years, depending on the complexity and IPv6 readiness of the current network and systems. Given that the provision of IP-based services is fundamental to the continued existence of ISPs, it is no surprise that the ISP community has already made plans to mitigate the risks of exhaustion of the IPv4 address space.

Therefore, although the upgrade timescales proposed in Section 5 indicate a one- to three-year programme, the survey results indicate that the ISP community is already well advanced in its implementation of IPv6.

*Network providers*

For the network provider community, the process of adopting IPv6 will need to be phased over one to three years, depending on each provider’s current level of readiness. For network operators, the main challenge will be to provide IPv6 transparency across their infrastructure, such that customers who use IP can transit their IPv6 traffic across the network.

*Service providers*

For the service provider community, the adoption of IPv6 will require a phased approach spread over one to three years, depending on the complexity and IPv6 readiness of the existing environment, and the nature of the services being offered by the provider. We believe that service providers have an opportunity to benefit from their standard equipment refresh cycle to procure hardware and software items that are IPv6 compliant before August 2011, which significantly mitigates any risks associated with depletion of the IPv4 address space.

[1] Hardware vendors are more advanced than software vendors in the inclusion of IPv6 support in their portfolios (see Section 2 for a summary of the current status of IPv6 adoption among hardware and software vendors in Singapore).

An example of the equipment that service providers could procure as part of a standard equipment refresh is ‘dual-stack’ routers and switches. This would allow any legacy (IPv4-only) equipment to co-exist with IPv6 systems until the full upgrade programme has been completed.

*End users*

For end users, the process of adopting IPv6 will vary depending on the type of user. For example, multinational corporations are likely to take early measures to avoid IPv4 address shortages. In contrast, local Singapore-based companies and SMEs will migrate on an ‘as needed’ basis.

## 1.3 Document map

The remainder of this document is structured as follows:

- Section 2 provides a summary of findings from the survey phase of the project
- Section 3 provides an overview of the ICT ecosystem and the different stakeholder groups that have had adoption guides prepared for them
- Sections 4 to 8 contain a set of adoption guides for:
  - system vendors (Section 4)
  - Internet service providers (Section 5)
  - network providers (Section 6)
  - service providers (Section 7)
  - end users (Section 8).

The document also contains three annexes providing supplementary technical information:

- Annex A provides an overview of IPv6 transition mechanisms
- Annex B discusses some of the design considerations for transition mechanisms
- Annex C discusses IPv6 certification or compliance measurement programmes.

In addition to this Section 1 introduction, it is recommended that readers also study Section 2, to familiarise themselves with the overall situation in Singapore and for their own stakeholder group. They should then read at least the section (from Section 4 to 8) that is specific to their own stakeholder group. Where there is a dependency on other stakeholder groups, it will also be helpful (but not essential) for readers to understand the implications and timing of these dependencies. Therefore, selective references to parts of other sections of Sections 4 to 8 may also be helpful.

As noted earlier, the adoption guide for each stakeholder group represents a generic set of actions that will need refining for individual stakeholders, recognising their individual requirements (including technical implementation and timescales). Again, the adoption guides for other adjacent stakeholder groups on whom there is a dependency, or who are dependents themselves, will assist readers in identifying the critical path items that need to be implemented first by a given stakeholder (e.g. an ISP may lobby hardware vendors for early delivery of IPv6-ready products so that it, in turn, can offer IPv6 services to its own customers).

# 2 Summary of findings from the survey phase

IDA appointed Analysys Mason and Tech Mahindra to carry out a focus-group survey to collect the data necessary to draw informed conclusions on the current status of IPv6 in Singapore.

The focus-group survey involved five key stakeholder categories in Singapore that were identified as having a role in achieving the successful migration to IPv6 across the country in a timely manner. The categories were:

- system vendors (including hardware and software vendors)
- Internet service providers (including domestic large ISPs and domestic small ISPs)
- network providers (including international carriers, mobile operators and wireless operators)
- service providers (including data centre operators, ASP/web hosting providers and content providers)
- end users.

The survey phase included face-to-face interviews across the five key stakeholder groups, as well as a web-based survey of small and medium-sized enterprises (SMEs). The aim of the survey phase was to identify, for each category of stakeholder:

- their infrastructure readiness
- the dependency of their business on IP addresses
- the progress they have made in planning for/implementing IPv6.

The face-to-face interviews were carried out between June 2010 and August 2010. All statements referring to future plans and timings are based on the information supplied at the time of the interviews. The web-based survey of SMEs was closed on 7 September 2010, and generated a total of 231 responses.

► *Face-to-face interviews*

In general, the face-to-face interviews showed that vendors are the most prepared for IPv6, primarily driven by the recognition that they need to support the wider ecosystem and plan ahead for when IPv6 becomes more prevalent. In contrast, other stakeholders are less IPv6 ready, and are typically adopting a ‘wait and see’ approach. ASP/web hosting and content providers are at various stages of IPv6 adoption and planning, depending on their own internal assessment of the business opportunity from IPv6 and its strategic fit with their business. Large domestic ISPs and mobile operators are replacing equipment as part of the standard refresh cycle, and are seeing limited customer demand, but recognise the need to support IPv6 and have set broad timelines of the end of 2011 for this. End users and other stakeholders, such as data centre operators, are delaying the move to IPv6 until they see a push from customers or service providers.

A common theme across all stakeholders during the face-to-face interviews was the difficulty seen in establishing a business case for IPv6, although most stakeholders recognise that they will have to support IPv6 technologies at some point and are building IPv6 specifications into their procurement processes and supporting the development of basic skills.

Our approach to the face-to-face interviews enabled us to assess the following five focus areas:

- **Planning**: the degree to which IPv6 is integrated into the organisation's overall plans and strategy, including, but not limited to, its roadmap, business plans/budgets, governance and business strategy
- **Network**: the degree to which network infrastructure (core, edge and access) and its associated services ( routing, DHCP, DNS, management, security) are ready and/or enabled for IPv6
- **Applications**: the degree to which higher layers of the IT solutions (operating systems, web, email, proprietary applications) are ready and/or enabled for IPv6
- **Skills**: how prevalent IPv6 skills and knowledge are across all levels of the organisation
- **Services/products**: how IPv6 is being incorporated in services and products, and how this is being communicated to existing, and potential, customers.

Each of these factors covers a wide range of sub-elements: for example, the state of IPv6 readiness of 'applications' needs to take into account the state of IPv6 readiness of infrastructure services (DHCP, DNS), network management/OSS/BSS applications, operating systems, security applications, directory applications, web services, email services, unified communications, corporate applications and any proprietary applications within the organisation.

For each of the five focus areas listed above, we investigated four main aspects relevant to IPv6: current status; strategy; execution approach; and challenges. Prior to interviewing each organisation, we prepared a summary questionnaire covering these four aspects. This questionnaire was circulated to individual organisations in advance of the interview and, along with preliminary discussions, was used to ensure that the proposed interviewee was the appropriate person to respond.

Following circulation of the summary questionnaire, we conducted a 60- to 90-minute interview with each interviewee, and followed this up with clarification questions.

After each interview, a panel of experts from Analysys Mason and Tech Mahindra[2] reviewed the findings from the discussions and allocated a score (typically 1 or 0) for each sub-element within the five focus areas. These scores were then aggregated, and each stakeholder allocated a status for IPv6 readiness for each of the five main focus areas (planning, network, applications, skills, and services and products) against a set of pre-defined status options. Each status ranges from weak (denoted by ○○○○) to strong (denoted by ●●●●).

[2] The Analysys Mason and Tech Mahindra project team included the head of Analysys Mason's Network Practice, who has been a long-term advocate of IPv6 and has presented on IPv6 at numerous IET conferences. The lead technical consultant is the head of Tech Mahindra's IPv6 Centre of Excellence, and has worked for a range of national governments, service providers and enterprises, and is also contributing to India's national IPv6 programme and national IPv6 task force. The team also included an IT specialist with more than five years' experience at an IT infrastructure consultancy, while the overall project manager has more than ten years' experience in the TMT sector.

Our approach of breaking each focus area down in order to assess individual sub-elements ensured that stakeholders were compared in a common fashion, and minimised the need for subjective interpretation of the results. Nonetheless, the ranking of IPv6 status inevitably involved some degree of interpretation, given the need to consider such a broad spectrum of stakeholders, business models and technical architectures.

Given this, the aggregate scores were continually reviewed both across, and within, stakeholder groups over the course of the survey phase. The aim was to ensure that a consistent picture was being presented, and that stakeholders that were allocated a particular status were at a comparable stage of IPv6 adoption and readiness.

The table below summarises the findings from the face-to-face interviews, which are discussed in more detail in the text underneath.

| | *Hardware vendors* | *Software vendors* | *Domestic large ISPs* | *Domestic small ISPs* | *International carriers* | *Mobile operators* | *Wireless operators* | *Data centre operators* | *ASP/web hosting providers* | *Content providers* | *Multinational companies* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Planning* | ●●●● | ●●●● | ●●○○ | ●●●○ | ●○○○ | ●●○○ | ●○○○ | ○○○○ | ●●○○ | ●○○○ | ○○○○ |
| *Networks* | n/a[†] | n/a[†] | ●●○○ | ●●○○ | ●○○○ | ●○○○ | ○○○○ | ○○○○ | ●●○○ | ●○○○ | ○○○○ |
| *Applications* | n/a[†] | n/a[†] | ●○○○ | ●●○○ | ●○○○ | ●○○○ | ○○○○ | ○○○○ | ○○○○ | ○○○○ | ○○○○ |
| *Skills* | ●●●● | ●●●● | ●●○○ | ●●○○ | ●●○○ | ●●○○ | ●○○○ | ○○○○ | ●○○○ | ○○○○ | ○○○○ |
| *Services* | ●●●○ | ●●○○ | ○○○○ | ●○○○ | ○○○○ | ○○○○ | ○○○○ | ○○○○ | ●○○○ | ○○○○ | n/a[‡] |

Key: Weak ○○○○ ⇨ ●○○○ ⇨ ●●○○ ⇨ ●●●○ ⇨ ●●●● Strong

NB The status shown in this table for a given stakeholder group is the lowest of the statuses of the stakeholders interviewed during the survey phase, as activities to encourage IPv6 adoption should focus on bringing all stakeholders to the required level of IPv6 readiness (rather than focusing on the leading stakeholders).

† For hardware and software vendors, an assessment of IPv6 readiness of networks and applications is not relevant, as their role in the ICT ecosystem is the supply of equipment / systems to other stakeholders, and the survey focus has therefore been on the IPv6 readiness of their products.

‡ The focus of the survey has been on assessing multinational companies as end users, rather than as service providers. As such, an assessment of IPv6-enabled services and products for this category has not been conducted.

*Figure 2.1: Overall summary table of survey findings [Source: Analysys Mason, Tech Mahindra]*

► *SME web-based survey*

The SME web-based survey generated 231 responses, and gathered information from respondents about:

- their infrastructure readiness
- the dependency of their business on IP addresses
- their current use of IPv4 and IPv6 traffic
- the progress they have made in planning for/implementing IPv6.

The results showed that a relatively small number of SMEs are aware of IPv6 as a successor to IPv4 and the upcoming exhaustion of IPv4 addresses. Findings from the survey also demonstrated that there is a lack of understanding of the benefits and capabilities of IPv6. Also, very few respondents had a clear knowledge of their organisation's plans for adoption of IPv6: the findings suggest that very little is known about the resources (personnel and cost) and timelines required for IPv6 adoption. IT infrastructure readiness has largely not been assessed by the majority of the organisations that participated in the survey.

We have used the findings from the survey to guide our work on the stakeholder group adoption guides detailed in Sections 4 to 8.

# 3 Overview of the ICT ecosystem, stakeholder groups and dependencies

The adoption of IPv6 across the ICT ecosystem is a function of a complex set of interactions and dependencies between the different stakeholders, as summarised below in Figure 3.1. While end users will drive demand for more IP addresses and IPv6-capable products and services, hardware and software vendors are key enablers of IPv6 adoption: without suitable products from these two stakeholders the rest of the ecosystem will be unable to progress with the deployment of IPv6. Next, the inclusion of IPv6 support in commercial Internet services from Internet service providers and network providers is essential in further promoting IPv6 adoption, although the launch of such services will, at least in part, be driven by demand from service providers and end users. Service providers themselves are reliant on the availability of IPv6-enabled connectivity, and also on evidence of customer demand; unsurprisingly, they have been tending to adopt a 'wait and see' stance unless they have identified a specific opportunity.

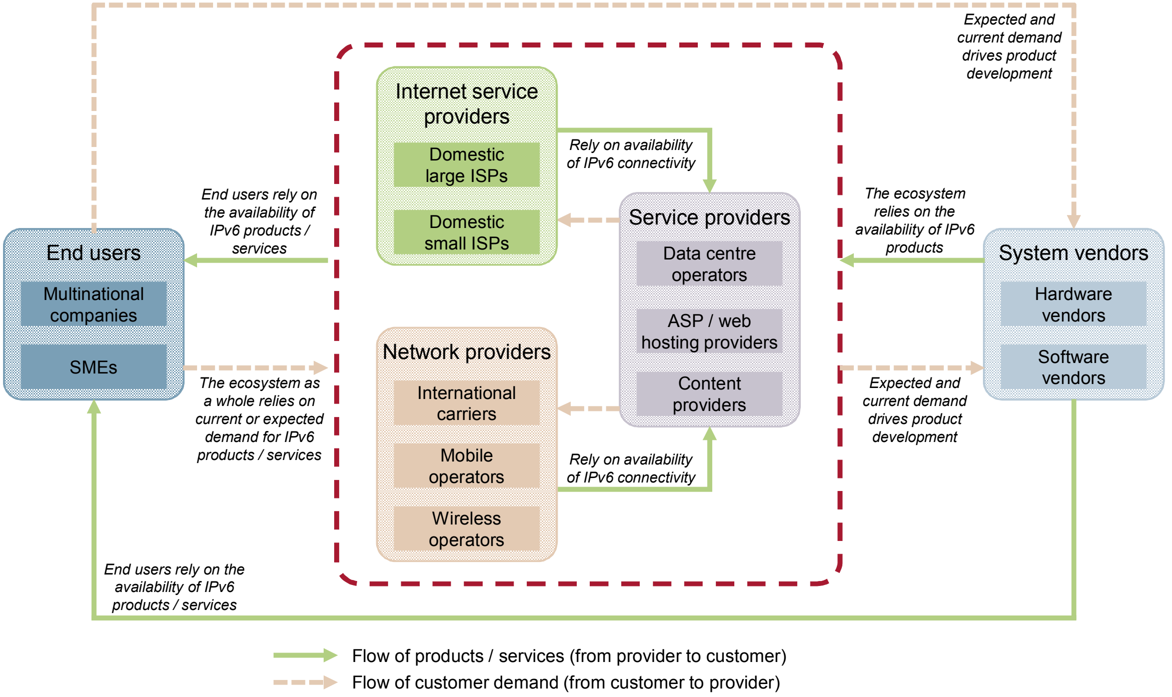

Expected and current demand drives product development
Internet service providers
Domestic large ISPs
Domestic small ISPs
Rely on availability of IPv6 connectivity
End users rely on the availability of IPv6 products / services
Service providers
Data centre operators
ASP / web hosting providers
Content providers
The ecosystem relies on the availability of IPv6 products
End users
Multinational companies
SMEs
System vendors
Hardware vendors
Software vendors
Network providers
International carriers
Mobile operators
Wireless operators
The ecosystem as a whole relies on current or expected demand for IPv6 products / services
Expected and current demand drives product development
Rely on availability of IPv6 connectivity
End users rely on the availability of IPv6 products / services
Flow of products / services (from provider to customer)
Flow of customer demand (from customer to provider)

*Figure 3.1: Summary of IPv6 dependencies between stakeholder categories [Source: Analysys Mason]*

Figure 3.2 provides further details on the role of these different groups in the adoption of IPv6 across the ICT ecosystem, and the interdependencies between them.

| *Stakeholder group* | *Description* | *Role in IPv6 adoption across the ICT ecosystem* |
|---|---|---|
| **System vendors** | | |
| Hardware vendors | Manufacture and/or sell computing hardware, such as routers, switches and servers | Provide the electronic computing hardware that forms the building blocks on which the ICT industry operates.<br>The ability of the wider ICT industry to adopt IPv6 is contingent on hardware vendors having an IPv6-ready product portfolio and end-to-end IPv6 solutions conforming to functional, performance and multi-vendor interoperability criteria |
| Software vendors | Develop and sell software solutions, such as operating systems, commercial off-the-shelf (COTS) applications, or proprietary applications | Provide software applications and solutions which, together with computing hardware, help the ICT industry realise its business goals in an efficient and effective manner<br>The ability of the ICT industry to adopt IPv6 is dependent on the availability of IPv6-ready software, which ensures that computing solutions are available as IPv6 is adopted and new applications utilising IPv6 features are brought into place.<br>Software vendors are dependent on the availability of IPv6-ready hardware from hardware vendors to provide IPv6-ready software application and solutions |
| **Internet service providers** | | |
| Domestic large ISPs† | Provide Internet services to business and residential customers in Singapore, and hold more than 30% of the retail broadband market | The inclusion of IPv6 support in commercial Internet services is essential in the wider adoption of IPv6 across Singapore and will also help encourage hardware and software vendors to roll out their IPv6-ready solutions<br>Domestic large ISPs are reliant on the availability of both IPv6-ready hardware and software from vendors to enable their own networks to offer IPv6 services to end users |
| Domestic small ISPs† | Provide Internet services to business and residential customers in Singapore, and which hold less than 30% of the retail broadband market | In addition, domestic small ISPs often position themselves as front-runners in adopting new technologies and providing innovative services. They can therefore accelerate IPv6 adoption through increasing awareness of IPv6.<br>Domestic small ISPs are reliant on the availability of both IPv6-ready hardware and software from vendors to enable their own networks to offer IPv6 services to end users |
| **Network providers‡** | | |
| International carriers | Operate global telecoms networks and sell connectivity and managed services to multinational companies as their main business | Enable global Internet connectivity of businesses, and also play an important part in helping to establish Singapore as a regional Internet services hub<br>Reliant on availability of IPv6-ready hardware and software solutions from vendors to IPv6 enable networks. Also need to balance the requirement to support IPv6 in Singapore against the demand and support for IPv6, both in Singapore and globally |
| Mobile operators | Operators of mobile (cellular) networks in Singapore, which offer voice and broadband services | The inclusion of IPv6 support in commercial Internet services, including mobile broadband, is an essential factor in the wider adoption of IPv6<br>Mobile operators will be reliant on the availability of both IPv6-ready/enabled hardware and software from vendors – and handset manufacturers in particular – to allow their own networks to be able to offer IPv6 services to end users |
| Wireless operators | Operators of wireless networks (e.g. Wi-Fi networks), which use these to offer Internet services to end users | As for domestic large ISPs |

| *Stakeholder group* | *Description* | *Role in IPv6 adoption across the ICT ecosystem* |
|---|---|---|
| **Service providers** | | |
| Data centre operators | Providers of shared/managed facilities to house computer systems and associated components to end users | Data centres generally use IP addresses that are provided by their customers, rather than procuring their own ranges.<br>Data centre operators are reliant on customer demand, IPv6-enabled connectivity from service providers, and the availability of IPv6-ready hardware and software solutions from vendors to IPv6 enable their own networks, and offer IPv6 business services accordingly. However, when the customer supplies its own equipment and connectivity, data centre operators play more of a supporting role in IPv6 adoption |
| ASP/web hosting providers | Providers of shared services for organisations across Singapore, helping them to make cost savings and access 'best-of-breed' technology | ASP/web hosting providers will need to ensure that proprietary applications support IPv6 and work with vendors to source IPv6-enabled applications<br>They play a supporting role, as they require IPv6 connectivity from service providers and IPv6-ready hardware and software solutions from vendors. They are likely to be one of the front-runners in adopting IPv6 ahead of customer demand given the typical product lifecycles |
| Content providers | Providers of content (e.g. news, search results, financial information, entertainment, communication and collaboration tools, etc.) to end users | Content providers play a significant role in the Internet ecosystem, as they create and provide the information which is accessed and exchanged across the Internet<br>They are reliant on the availability of IPv6-enabled data centre solutions, ASP/web hosting providers, connectivity from service providers and IPv6-ready hardware and software solutions |
| **End users** | | |
| Multinational companies | Large corporates, which have to ensure that their networks and services in Singapore are able to communicate and operate with networks in other countries | Unlikely to drive the adoption of IPv6 across the rest of the ecosystem, but will adopt IPv6 themselves, should there be a demonstrable business case<br>Reliant on the availability of IPv6-enabled international carriers, data centre operators, ASP/web hosting providers, connectivity from service providers and IPv6-ready hardware and software solutions |

† Domestic large ISPs and domestic small ISPs can also be classified as international carriers, as they sometimes operate international networks in addition to their domestic Internet services. However, for this report, the international carriers category includes carriers whose main business in Singapore is to serve multinational clients.

‡ Fixed network providers are covered in the domestic large ISP and domestic small ISP categories.

*Figure 3.2: Stakeholder groups covered by face-to-face interviews, and the role they can play in IPv6 adoption across the ICT ecosystem [Source: Analysys Mason]*

# 4 IPv6 adoption guide: System vendors

The system vendors category incorporates the suppliers of both hardware and software. A transition to IPv6 will have an impact on all vendors with products that depend on an IP address, as they will need to take action to ensure these products can operate in an IPv6 environment. Hardware vendors manufacture and/or sell hardware, such as routers, switches and servers, whereas software vendors develop and sell software solutions, such as operating systems, commercial off-the-shelf (COTS) applications and proprietary applications. They both therefore form a key element of the ICT industry – by providing the building blocks on which the rest of the industry operates. The ability of the wider ICT industry to adopt IPv6 is contingent on hardware and software vendors, including IPv6 support across their product portfolio, and on them ensuring IPv6 interoperability across different vendor solutions. The overall IPv6 enablement of this industry segment is important in initiating and promoting IPv6 adoption – not just in Singapore, but around the world.

Section 4.1 sets out a summary of the IPv6 adoption guide; Section 4.2 provides a summary of the survey results; and Section 4.3 provides a summary of the drivers and timelines for this stakeholder category to adopt IPv6. Sections 4.4 to 4.7 provide details for each phase of the adoption, including planning, architecture and design, deployment (production) and support.

## 4.1 IPv6 adoption guide: overall summary

For system vendors, the process of adopting IPv6 will be a phased approach spread across one to three years, depending on the IPv6 readiness of their current systems. In general, it can be assumed that products required by operators and end users to implement IPv6 (e.g. routers) will be required in the marketplace ahead of applications that will subsequently operate in an IPv6 environment. The four main phases of IPv6 adoption are:

- **planning**: IPv6 awareness and skill building activities are undertaken, and the plans for IPv6 adoption are prepared. Vendors participate in and/or track work undertaken by industry standards bodies, and identify products and applications that require/are capable of upgrading to operate in an IPv6 environment
- **architecture and design**: a programme is begun to specify architecture/design changes for hardware and systems that can be made IPv6 ready
- **deployment**: the production phase commences to upgrade existing products and/or produce new products that are IPv6 compatible
- **support**: IPv6 products are monitored for performance and reliability, and a customer support system is put in place for the IPv6 services provided to customers, to ensure they have a seamless and smooth experience of IPv6 services.

Details of the four phases and the activities involved in each are illustrated in Figure 4.1. We provide details of the key activities within each phase in later sections of this adoption guide.

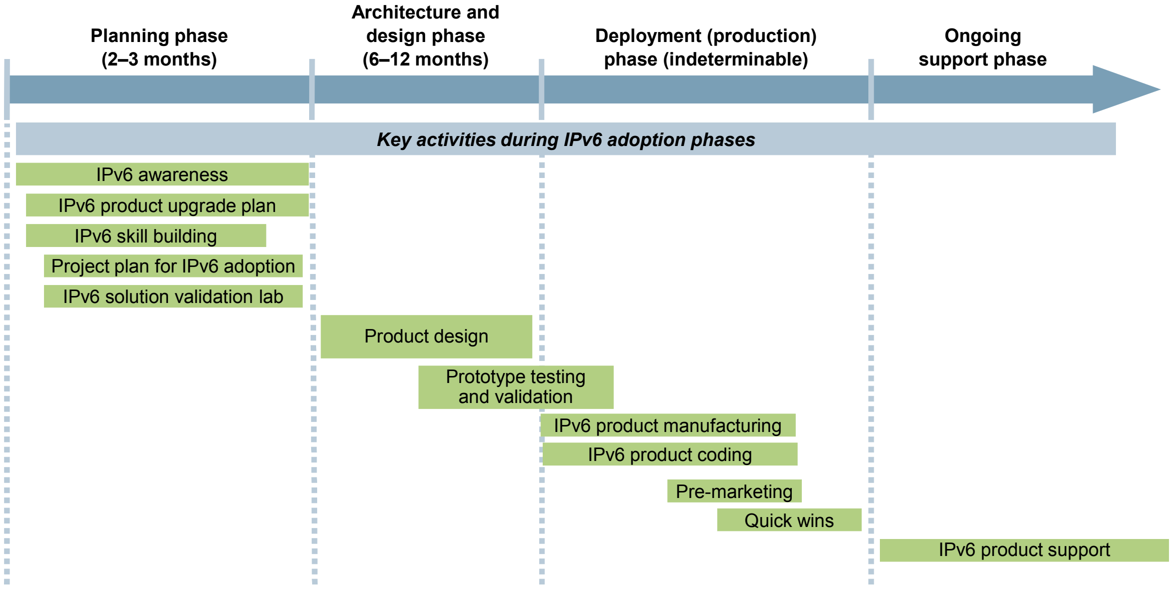

Planning phase (2–3 months)
Architecture and design phase (6–12 months)
Deployment (production) phase (indeterminable)
Ongoing support phase
Key activities during IPv6 adoption phases
IPv6 awareness
IPv6 product upgrade plan
IPv6 skill building
Project plan for IPv6 adoption
IPv6 solution validation lab
Product design
Prototype testing and validation
IPv6 product manufacturing
IPv6 product coding
Pre-marketing
Quick wins
IPv6 product support

*Figure 4.1: Activities involved in the IPv6 adoption phases for system vendors [Source: Analysys Mason, Tech Mahindra]*

## 4.2 Summary of findings from survey phase

The system vendor category includes hardware and software vendors. Figure 4.2 and Figure 4.3 summarise the findings of the survey phase for each of these stakeholder groups.

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • IPv6 adoption plans and roadmap in place, and work has been underway since the late 1990s or early 2000s<br>• Primary business drivers were a wish to be ahead of the technology demand curve, and the US government mandates for IPv6 adoption | ●●●● |
| Skills | • Strong IPv6 skills in place | ●●●● |
| Services and products | • The network operating system is IPv6 ready and, in turn, the majority of the current product portfolio is IPv6 ready<br>• No specific end-to-end IPv6 solutions have been validated<br>• A few innovative products and solutions based on IPv6 features are being designed, relating to energy management and greenhouse crop management | ●●●○ |

*Figure 4.2: Summary of IPv6 readiness among hardware vendors in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • IPv6 architecture and designs across products in place<br>• IPv6 trial and commercial products available<br>• Teams for IPv6 adoption identified – monitoring and tracking in place | ●●●● |
| Skills | • Advanced IPv6 product architecture and design skills in place | ●●●● |
| Services and products | • Operating systems are IPv6 enabled<br>• Significant focus on IPv6 enabling enterprise applications and products<br>• Lack of focus on IPv6 enabling consumer-oriented products<br>• IPv6 trial and commercial products available | ●●○○ to ●●●○ |

*Figure 4.3: Summary of IPv6 readiness among software vendors in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

## 4.3 IPv4 exhaustion timelines and business impact

As end users begin to plan their IPv6 migration path, they will consult their suppliers to determine when their IPv6-ready products will become available. If end users have a pressing business need to use IPv6 due to the exhaustion of IPv4 addresses, they will require their suppliers to make available IPv6-ready products. The timely availability of IPv6-ready products will be imperative if suppliers are to meet their customers' needs. If existing suppliers fail to meet the timeline driven by the market, end users may be forced to move to a competitor.

Results from the IPv6 readiness survey indicated that many end users were not as advanced with their preparation as they should be, given the projected date for exhaustion of IPv4 addresses.[3] This represents a business opportunity for suppliers to proactively market IPv6 products and stimulate greater interest. For suppliers that focus on the ISP and network operator sectors, demand for IPv6 products will arise earlier than it does from the end-user market, because ISP/operator systems will require upgrading before they can market IPv6 services.

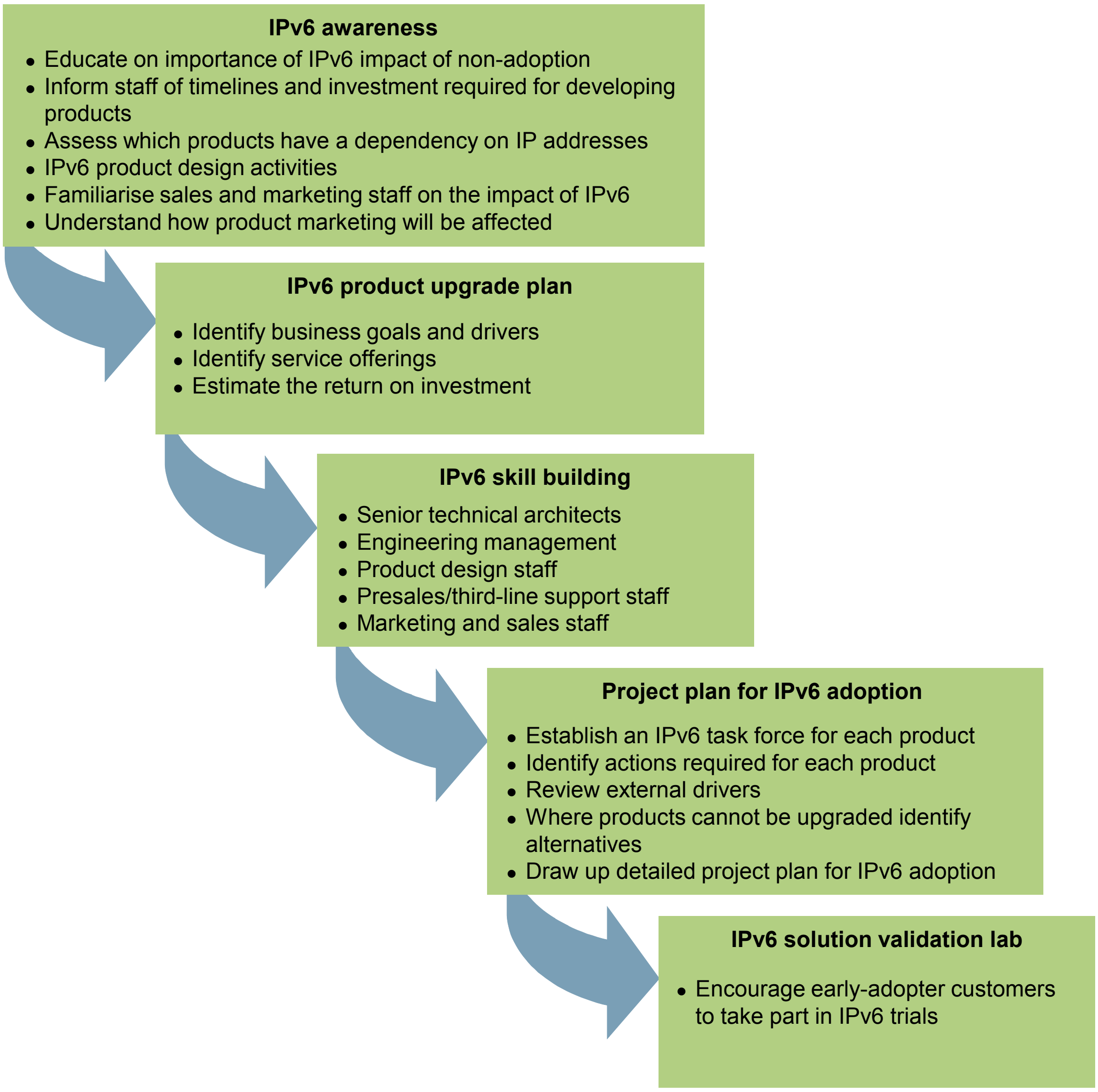
If suppliers cannot address the needs of their customers by providing IPv6-compatible products in a timely manner this represents a risk to their businesses, because they could find some of their market share captured by competitors who are more advanced with their IPv6 products. The survey phase showed that both hardware and software vendors supported IPv6 across some part of their product portfolio (the majority of the portfolio in the case of hardware vendors), but there were still some gaps, with vendors having IPv6 capabilities on the roadmap in a number of cases.

[3] August 2011, as of February 2011.

## 4.4 IPv6 adoption guide: planning phase

During this phase a supplier will draw up a detailed IPv6 adoption project plan and start to build awareness, and skills where necessary, within its organisation. The duration of this phase will vary depending on the extent of work required; for larger suppliers it could require multiple teams working in parallel across a product range. As well as the development of a detailed project plan, this phase includes key activities, such as building IPv6 awareness across the organisation, developing an IPv6 business services plan, conducting an IPv6 readiness assessment across existing product ranges, and assessing the potential to launch new IPv6-based products.

Details of the activities to be accomplished in this phase are provided in schematic format below, and discussed in greater detail in the remainder of this section.



**IPv6 awareness**

- Educate on importance of IPv6 impact of non-adoption
- Inform staff of timelines and investment required for developing products
- Assess which products have a dependency on IP addresses
- IPv6 product design activities
- Familiarise sales and marketing staff on the impact of IPv6
- Understand how product marketing will be affected

**IPv6 product upgrade plan**

- Identify business goals and drivers
- Identify service offerings
- Estimate the return on investment

**IPv6 skill building**

- Senior technical architects
- Engineering management
- Product design staff
- Presales/third-line support staff
- Marketing and sales staff

**Project plan for IPv6 adoption**

- Establish an IPv6 task force for each product
- Identify actions required for each product
- Review external drivers
- Where products cannot be upgraded identify alternatives
- Draw up detailed project plan for IPv6 adoption

**IPv6 solution validation lab**

- Encourage early-adopter customers to take part in IPv6 trials

*Figure 4.4: Summary of activities in IPv6 planning phase for system vendors [Source: Analysys Mason, Tech Mahindra]*

### 4.4.1 IPv6 awareness

An IPv6 awareness programme ensures that the importance of IPv6 adoption, the key areas of impact, the costs and the timelines are shared across the organisation.

A few key aspects to be considered when preparing to raise awareness of IPv6 in an organisation are shown in Figure 4.5.

| *IPv6 awareness* | |
|---|---|
| *Overall aims* | Raise IPv6 awareness across all key stakeholders within the organisation to educate them on the importance of IPv6 adoption, the scope of activities to be accomplished, and the likely timelines |
| *Approx. duration* | 1–2 months |
| *Key tasks* | The awareness programme must be targeted at multiple segments:<br>• **senior management** – the following aspects must be covered:<br>– importance of IPv6, and the business impact of non-adoption<br>– timelines and the investment required for developing IPv6 products<br>• **product engineering management** – the following aspects must be covered:<br>– assessing which products have a dependency on IP addresses<br>– defining a set of activities to be initiated to design and implement IPv6 functionality into the product<br>• **sales and marketing staff** – the following must be covered:<br>– familiarising sales and marketing staff on the impact of IPv6<br>– understanding how product marketing will be affected |
| *Stakeholders* | • Senior management, product engineering management, sales and marketing |
| *Dependencies* | • No dependencies on other tasks |

*Figure 4.5: Summary of IPv6 awareness activity for system vendors [Source: Analysys Mason, Tech Mahindra]*

### 4.4.2 IPv6 business services plan

An IPv6 business services plan for a system vendor identifies the products and services that should support IPv6. This provides an essential input to later activities during the planning phase, and ensures that the correct priority is given to development, production and marketing activities.

A few key aspects to be considered when preparing an IPv6 business services plan are shown in Figure 4.6; further details specific to system vendors are provided in the rest of this sub-section.

| *IPv6 business services plan* | |
|---|---|
| *Overall aims* | Identify business roadmap, covering business goals and drivers, identifying service offerings to be delivered using IPv6 and return-on-investment implications |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 business services plan needs to:<br>• **identify business goals and drivers** that are linked to IPv6 adoption<br>• **identify service offerings** that should support IPv6, in line with the business goals and drivers<br>• **estimate the return on investment** (either in terms of incremental revenue or cost savings compared to the case without IPv6) |
| *Stakeholders* | • Senior management, product department, sales and marketing |
| *Dependencies* | • The IPv6 awareness programme needs to be underway before the IPv6 business services plan can be started |

*Figure 4.6: Summary of IPv6 business services plan for system vendors [Source: Analysys Mason, Tech Mahindra]*

### *Business goals and drivers*

The typical business goals of a system vendor are to:

- **protect existing revenues** by ensuring products are made IPv6 compatible, and thus retain existing customers who might otherwise source IPv6 products from an alternative supplier
- **ensure that the upgrade of current products is undertaken in a cost-effective and timely manner**, to minimise development costs and disruption to production, and align the availability of products with market demand
- **develop new products** that take advantage of new opportunities created by IPv6-based services.

These business goals are based on ensuring that system vendors have the right products in the market at the right time. System vendors are well placed to push the adoption of IPv6 by educating existing customers on its benefits, and could thus generate increased revenues during this period. However, a failure to meet the expectations of the market could result in a loss of business to competitors.

*Service offerings*

Hardware suppliers are not directly dependent on IP address availability in their business but, because hardware is the first layer of the IT infrastructure, it is critical for this stakeholder group to integrate IPv6 functionality into its product portfolio. A lack of IPv6 support could hinder the IPv6 adoption process across the ecosystem, and also result in a potential loss of business to the supplier. When IPv6 usage starts to increase, it will be equally important for hardware vendors to provide solutions for both IPv4 and IPv6 environments, as well as transition technologies (i.e. interim solutions to enable dual working between IPv4 and IPv6). Similarly, software vendors are not directly dependent on IP address availability in their business. The IP stack is generally transparent to the application layer, with the exception of operating systems. However, once customers start using IPv6 addresses it will be critical for software vendors to make sure they support end-user requirements by providing products that support both IPv4 and IPv6, otherwise they will lose market share and revenues as end users will be forced to move to alternative suppliers whose products do support IPv6.

*Return on investment*

A key part of the process of identifying which services should be IPv6 enabled is to estimate the return on investment from doing so. In assessing this, system vendors need to consider the following:

- **incremental revenue from IPv6 enablement** when compared to not IPv6 enabling (e.g. incremental revenue through the introduction of new value-added services or avoiding revenue being ‘lost’ to competitors through not having IPv6-enabled services)
- **cost implications of IPv6 enablement**, such as development costs for hardware upgrades and recoding of applications.

### 4.4.3 IPv6 skill building

IPv6 skill building ensures that all stakeholders across the organisation have the required skills to contribute to, and participate in, the IPv6 adoption process, including implementation. The survey results indicated that skill levels appear to be already sufficiently high among the suppliers questioned. However, this may not be a universal situation, so it is recommended that the skill building process is at least checked to verify that the organisation has achieved the required skill levels. An overview of the IPv6 skill building process is provided in Figure 4.7.

| *IPv6 skill building* | |
|---|---|
| *Overall aims* | • Ensure that IPv6 skills are built across the various levels of the organisation (engineering management, engineering staff, etc.), so that they can participate in, and contribute to, the IPv6 adoption process<br>• Provide skills to design and engineering teams to enable them to implement the IPv6 adoption programme |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 skill building programme encompasses various layers of the organisation:<br>• **senior technical architects/engineering management** – skills in the following areas must be covered:<br>– IPv6 product design change implications<br>– IPv6 software design change implications<br>• **product design staff** – the following areas must be covered:<br>– Implementing IPv6 functionality into existing systems<br>• **pre-sales / third-line support** – need the ability to advise customers on technical issues surrounding IPv6 implementation<br>• **marketing & sales** – the following areas must be covered:<br>– sufficient knowledge to communicate facts to customers through direct and indirect means |
| *Stakeholders* | HR, training department, engineering management, senior technical architects, engineering staff, marketing & sales |
| *Dependencies* | The IPv6 awareness activity should have been completed before the IPv6 skill building activity begins, although it can be started in advance of full completion of the IPv6 awareness activity |

*Figure 4.7: Summary of IPv6 skill building activity for system vendors [Source: Analysys Mason, Tech Mahindra]*

### 4.4.4 Project plan for IPv6 adoption

The project plan for IPv6 adoption should set out the detailed set of activities to be carried out, spanning assessing products for their suitability to be made IPv6-ready, through to assessing the market in terms of the required timetable for product availability, design, production and product release.

| *Project plan for IPv6 adoption* | |
|---|---|
| *Overall aims* | • Establish the organisation’s current portfolio of systems/applications that require some form of action to enable them to be IPv6 compatible<br>• Draw up a detailed project plan, including the various sub activities required for each product to become IPv6-ready |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The key tasks in preparing the IPv6 adoption project plan are:<br>• establish an IPv6 task force for each product<br>• identify the necessary actions required for each product<br>• review external drivers (e.g. government mandates)<br>• where products cannot be upgraded, identify alternative solutions for the market<br>• draw up a detailed project plan for IPv6 adoption<br>The assessment of a product’s suitability for making IPv6-ready mentioned above needs to cover the following areas:<br>• **hardware-based products** – routers, switches, etc.<br>• **application-based products** – any applications with an IP stack or some IP-dependent interface<br>The product development plan for integrating IPv6 functionality will detail the set of activities that must be completed. The plan must cover the following areas:<br>• undertake design work for each product<br>• prototyping<br>• accreditation as required |
| *Stakeholders* | • **Product team** – internal product development/support teams<br>• **Marketing & Sales** – responsible for ensuring the product meets market requirements and for handling the customer interface |
| *Dependencies* | • The IPv6 awareness programme needs to be completed before the IPv6 readiness programme can begin, to ensure that stakeholders understand the importance of the readiness assessment, and are willing to participate fully in it<br>• The IPv6 business services plan needs to be prepared to identify which services should support IPv6 |

*Figure 4.8: Summary of project planning for IPv6 adoption activity for system vendors [Source: Analysys Mason, Tech Mahindra]*

### 4.4.5 Quick wins

The readiness survey indicated that system vendors are generally ahead of the other stakeholders in implementing IPv6 within their products, and there are probably very few opportunities for them to achieve early wins at this stage. The most promising area is likely to be in encouraging customers to take part in some form of early pilot.

| *IPv6 quick wins* | |
|---|---|
| *Overall aims* | • Identify and implement initial 'quick win' projects |
| *Approx. duration* | 2–3 months |
| *Key tasks* | It is assumed that there will be very limited opportunities for internal 'quick win' projects at this stage, although some customer-facing activities could be potentially beneficial:<br>• **Encourage early adopter customers to take part in IPv6** trials so that experience can be gained; this could potentially have a 'snowball effect', whereby interest is stimulated in the wider market |
| *Stakeholders* | Marketing and sales, product technical support groups |
| *Dependencies* | The IPv6 awareness programme and the IPv6 skill building programmes should be completed before starting this activity |

*Figure 4.9: Summary of IPv6 'quick win' activity for system vendors [Source: Analysys Mason, Tech Mahindra]*

## 4.5 IPv6 adoption guide: architecture and design phase

In this phase, the supplier defines how migration to IPv6 will be achieved for current IPv4-based hardware and applications. In this context, system vendors need to publish the details for their respective products.

The IPv6 solution architecture and design phase needs to cover the areas outlined below.

- **Hardware** – how the hardware will be re-engineered to incorporate IPv6 in future products, and whether (and, if so, how) existing hardware can be upgraded.
- **Applications** – how IPv6 functionality will be incorporated into existing applications, and how existing versions can be upgraded.

Figure 4.10 indicates the activities involved in the design phase for system vendors.

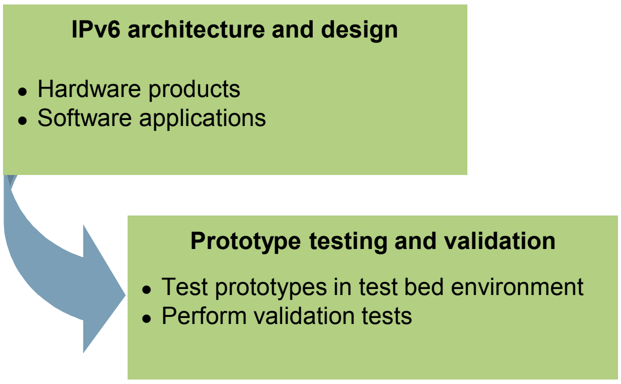

IPv6 architecture and design
• Hardware products
• Software applications
Prototype testing and validation
• Test prototypes in test bed environment
• Perform validation tests

*Figure 4.10: Architecture and design phase activities for system vendors [Source: Analysys Mason, Tech Mahindra]*

The remainder of this section summarises the design phase activities suggested for system vendor stakeholders.

### 4.5.1 Product design

*Architecture and design – hardware*

The development and release of a product architecture and design for end users to deliver IPv6-enabled services on their infrastructure are the main deliverables from this activity. The key tasks are identified in Figure 4.11.

| *IPv6 services architecture and design* | |
|---|---|
| *Overall aims* | Publish an IPv6 service architecture and design, which will help to ensure existing IPv4 services are IPv6-enabled, and to introduce new IPv6 services accordingly |
| *Approx. duration* | 1–2 months |
| *Key tasks* | • Develop the design and architecture for IPv6 products and services |
| *Stakeholders* | Technical architects, software engineering team, vendors, end-user customers |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can begin |

*Figure 4.11: Summary of IPv6 service architecture and design activity (hardware) for system vendors [Source: Analysys Mason, Tech Mahindra]*

*Architecture and design – software applications*

The development and release of product information relating to the architecture and design for end users to deliver IPv6-enabled services on their infrastructure are the main deliverables from this activity. The key tasks are identified in Figure 4.12.

| *IPv6 product architecture and design* | |
|---|---|
| *Overall aims* | Publish information about how applications that currently work in an IPv4 environment can be upgraded to run on an IPv6-enabled network |
| *Approx. duration* | 2–4 months |
| *Key tasks* | • Produce a detailed description of the upgrade path that must be followed for each product<br>• Estimate any costs that may be incurred<br>• Define timescales for availability |
| *Stakeholders* | Technical architects, software engineering team, sales & marketing teams, end-user customers |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can begin |

*Figure 4.12: Summary of IPv6 service architecture and design activity (software applications) for system vendors [Source: Analysys Mason, Tech Mahindra]*

### 4.5.2 Testing and validation

A key stage in the product development cycle for any system vendor wishing to provide products for use in an IPv6 network environment is to acquire the ‘IPv6-ready’ logo for its products from the IPv6 Forum.[4] This logo confirms that the products have been tested, and are certified as compliant with the new version of the protocol.

In order to obtain the IPv6-ready accreditation, products have to undergo testing at a facility approved by the IPv6 Forum.[5] There are two levels of testing:

- **conformance testing** – aimed at validating a product to IETF RFC standards. This is accomplished through specific tools which emulate an environment of reference for the tested product and ascertain its conformance to the IPv6 specifications
- **interoperability testing** – whereby the tested product is interconnected with other products (routers, switches and servers) supporting typical configurations. The test scenarios aim to verify whether the product is able to interact with IPv6 products from different manufacturers.

| *IPv6 product testing and validation* | |
|---|---|
| *Overall aims* | Confirm that the products have been tested and are certified as compliant with the new version of the protocol, and obtain accreditation in the form of the ‘IPv6-ready’ logo |
| *Approx. duration* | 2–3 months |
| *Key tasks* | • Conformance testing<br>• Interoperability testing |
| *Stakeholders* | Technical architects, software engineering team, sales & marketing teams, testing centres, IPv6 Forum representatives |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can begin |

*Figure 4.13: Summary of IPv6 product testing and validation tasks for system vendors [Source: Analysys Mason, Tech Mahindra]*

## 4.6 IPv6 adoption guide: deployment phase

During the deployment phase, the system vendor should be engaged in tasks such as product manufacture (in the case of the hardware supplier) and software development (applicable to both hardware and application vendors). Other tasks within this phase include product coding, pre-marketing activities and the realisation of any quick wins that might apply. These activities are summarised in schematic form below, and discussed in greater detail in the rest of this section.

[4] See http://www.ipv6ready.org/

[5] See http://www.ipv6forum.com/

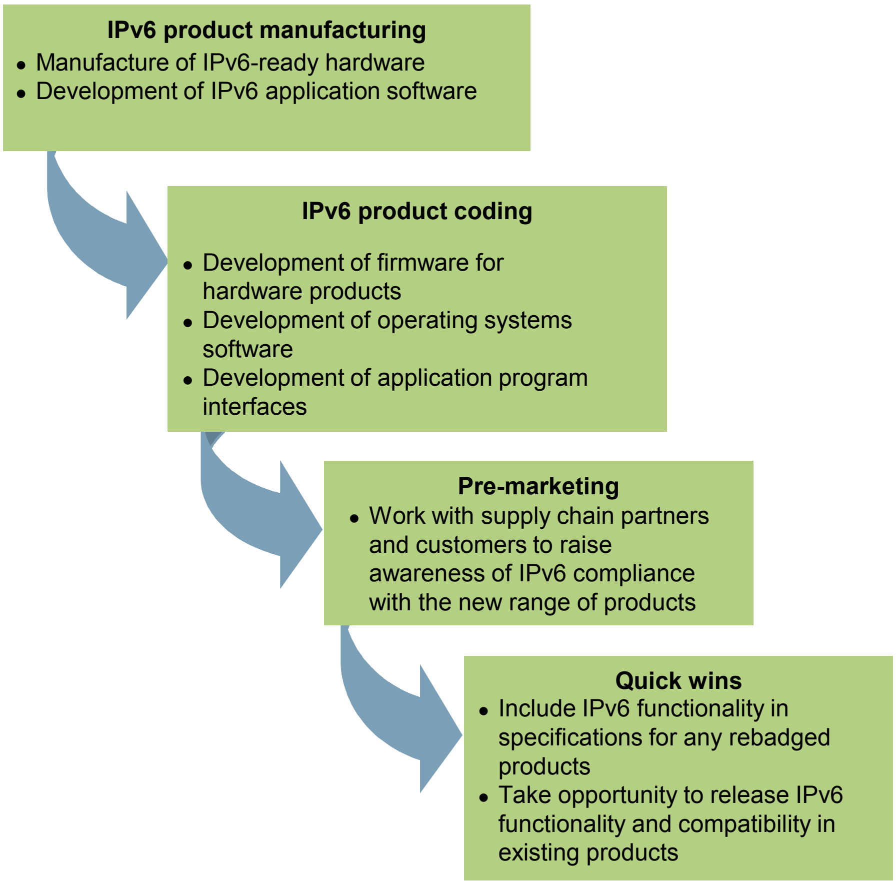

IPv6 product manufacturing
- Manufacture of IPv6-ready hardware
- Development of IPv6 application software
IPv6 product coding
- Development of firmware for hardware products
- Development of operating systems software
- Development of application program interfaces
Pre-marketing
- Work with supply chain partners and customers to raise awareness of IPv6 compliance with the new range of products
Quick wins
- Include IPv6 functionality in specifications for any rebadged products
- Take opportunity to release IPv6 functionality and compatibility in existing products

*Figure 4.14: Summary of deployment phase tasks for system vendors [Source: Analysys Mason/Tech Mahindra]*

### 4.6.1 IPv6 product manufacturing

The purpose of this group of tasks in the adoption plan is for system vendors to produce IPv6-ready equipment for use by other members of the stakeholder community (notably ISPs, network providers and end users). This production can be in the form of upgrades to existing product ranges, or totally new products based on an IPv6 platform.

| *IPv6 product manufacturing* | |
|---|---|
| *Overall aims* | Produce a range of products for the marketplace which are certified and tested as IPv6 compliant |
| *Approx. duration* | 6–24 months |
| *Key tasks* | • Manufacture of IPv6 compliant hardware<br>• Development of IPv6 application software |
| *Stakeholders* | Manufacturing operations, software development department |
| *Dependencies* | The planning phase needs to be completed before this task can begin |

*Figure 4.15: Summary of IPv6 product manufacturing tasks for system vendors [Source: Analysys Mason, Tech Mahindra]*

### 4.6.2 IPv6 product coding

The purpose of this group of tasks is to develop an IPv6 compliant code for hardware being built elsewhere and, in the case of software developers, to build appropriate IPv6 application programme interfaces into application software.

| *IPv6 product coding* | |
|---|---|
| *Overall aims* | Build IPv6 ready system software and firmware design for hardware products being manufactured |
| *Approx. duration* | 6–24 months |
| *Key tasks* | • Development of firmware for hardware products<br>• Development of operating systems software<br>• Development of application program interfaces |
| *Stakeholders* | Technical architects, software engineering team |
| *Dependencies* | The planning phase needs to be completed before this task can begin |

*Figure 4.16: Summary of IPv6 product coding tasks for system vendors [Source: Analysys Mason, Tech Mahindra]*

### 4.6.3 Pre-marketing

Prior to the launch of IPv6-ready products, the objective of this task within the overall plan is to raise the level of IPv6 awareness within the supply chain and the customer environment, and to enforce the marketing message that all of the system vendor's products are IPv6 ready.

| *IPv6 product pre-marketing* | |
|---|---|
| *Overall aims* | To inform the system vendor's own supply ecosystem and customer base that all future products delivered will be certified as IPv6 ready |
| *Approx. duration* | 6–12 months |
| *Key tasks* | • Work with supply chain partners and customers to raise awareness that the new range of products will be IPv6 ready |
| *Stakeholders* | Marketing department, procurement department, sales force, supply chain partners, customers |
| *Dependencies* | The planning phase needs to be completed before this task can begin |

*Figure 4.17: Summary of IPv6 product pre-marketing tasks for system vendors [Source: Analysys Mason, Tech Mahindra]*

### 4.6.4 Quick wins

The purpose of this activity is to identify and exploit any opportunities for the system vendor to accelerate its adoption programme by leveraging any IPv6 functionality inherent within its existing product line. As an example, there is a possibility that IPv6 functionality might already be available within subcomponents or rebadged products, although not currently used.

| *IPv6 quick wins* | |
|---|---|
| *Overall aims* | • Identify and implement initial 'quick win' projects |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The types of project chosen will depend on the current status of an organisation, and are difficult to specify. However, some examples could include:<br>• inclusion of IPv6 functionality in specifications for any rebadged products<br>• taking the opportunity to include IPv6 functionality and compatibility in existing products |
| *Stakeholders* | Corporate management team, procurement team, technical architects |
| *Dependencies* | The planning phase needs to be completed before this task can begin |

*Figure 4.18: Summary of IPv6 'quick win' activity for system vendors [Source: Analysys Mason, Tech Mahindra]*

## 4.7 IPv6 adoption guide: ongoing support phase

### 4.7.1 IPv6 product support

From the system vendor's point of view, support for IPv6 products is very much a 'business as usual' activity, given that knowledge gained, and documentation developed, during production of the products will be available during the support phase.

Technical support staff will have been trained prior to product release, and support team structures and methodologies will already be in place to provide support for legacy products.

Therefore, the key tasks of a system vendor within the support phase are to:

- ensure that support staff are trained in IPv6
- ensure that documentation is kept up to date
- ensure that a formal ICT support framework (such as ITIL) is adopted and maintained within the organisation.

# 5 IPv6 adoption guide: Internet service providers

ISPs enable the provision of Internet services to every sector of the Singaporean economy, and play a key role in building, running and managing the Internet backbone network. The inclusion of IPv6 support in commercial Internet services is essential in the wider adoption of IPv6, and will also help encourage hardware and software vendors to roll out their IPv6-ready solutions. Also, the provision of innovative solutions can also help to increase awareness and adoption of IPv6 in the wider ecosystem.

Section 5.1 sets out a summary of the IPv6 adoption guide; Section 5.2 provides a summary of the survey results, and Section 5.3 provides a summary of the drivers and timelines for this stakeholder category to adopt IPv6. Sections 5.4 to 5.7 provide details for each phase of the adoption, including planning, architecture and design, deployment and support.

## 5.1 IPv6 adoption guide: overall summary

For Internet service providers, the process of adopting IPv6 will be a phased approach spread across one to three years, depending on the complexity and IPv6 readiness of the current network and systems. The four main phases of IPv6 adoption are:

- **planning**: IPv6 awareness and skill building activities are undertaken, and the plans for IPv6 adoption are prepared. In addition, a few 'quick win' projects are identified to build confidence and understanding of IPv6
- **architecture and design:** the target and transition designs for the network, applications and services that will run on IPv6 are defined
- **deployment**: the IPv6 solution is deployed across the network, applications and services area, with quick win projects implemented at the start of the deployment phase
- **support**: IPv6 services are monitored for performance and reliability, and a customer support system is put in place for the IPv6 services provided to customers, to ensure they have a seamless and smooth experience of IPv6 services.

Details of the four phases, and the activities involved in each, are illustrated in Figure 5.1. We provide details of the key activities within each phase in later sections of this adoption guide.

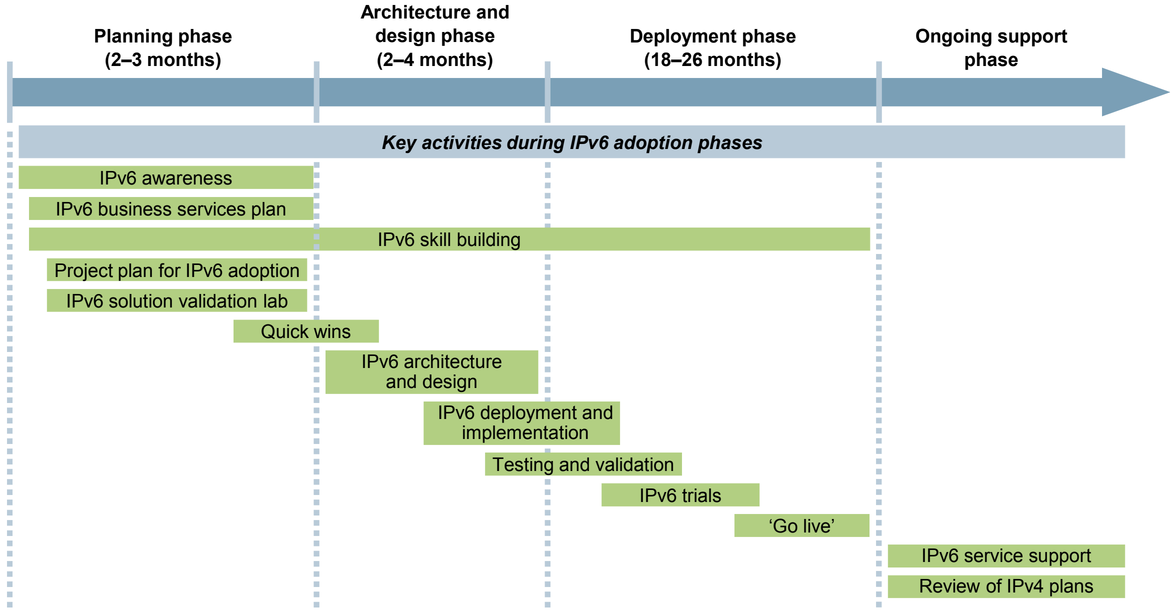

Planning phase (2–3 months)
Architecture and design phase (2–4 months)
Deployment phase (18–26 months)
Ongoing support phase
Key activities during IPv6 adoption phases
IPv6 awareness
IPv6 business services plan
IPv6 skill building
Project plan for IPv6 adoption
IPv6 solution validation lab
Quick wins
IPv6 architecture and design
IPv6 deployment and implementation
Testing and validation
IPv6 trials
'Go live'
IPv6 service support
Review of IPv4 plans

*Figure 5.1: Activities involved in the four IPv6 adoption phases for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

## 5.2 Summary of findings from survey phase

The ISP category includes domestic large ISPs and domestic small ISPs. Figure 5.2 and Figure 5.3 summarise the findings of the survey phase for each of these stakeholder groups.

| *Area* | *Summary of current status* | *Status* |
|---|---|---|
| Planning | • A broad timeline of the end of 2011 has been identified for IPv6 adoption<br>• Design and roll-out plan not in place<br>• IPv6 business strategy not in place – new IPv6 services and products not planned<br>• Teams for IPv6 adoption identified – monitoring and tracking not in place | ●●○○ |
| Networks | • Initial stages – only edge of core network IPv6 enabled<br>• Content delivery infrastructure working in IPv4 environment only<br>• IPv6 solutions being tested in lab – no live deployment | ●●○○ |
| Applications | • Initial stages – limited, or no, IPv6 readiness assessment undertaken<br>• IPv6 enablement of applications not done | ●○○○ |
| Skills | • Basic skills in place – advanced design and architecture training planned | ●●○○ |
| Services | • Only IPv6 transit services being provided<br>• No new IPv6 services available – no plan in place | ○○○○ |

*Figure 5.2: Summary of IPv6 readiness among domestic large ISPs in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

| *Area* | *Summary of current status* | *Status* |
|---|---|---|
| Planning | • Varied status – ranging from IPv6 architecture designed and rolled out, to network IPv6 ready, but not enabled<br>• Varied status – ranging from IPv6 trial and commercial services available, to no IPv6 service currently in place<br>• IPv6 business strategy not in place – no mapping in place between new IPv6 services/products and revenue generation<br>• Teams for IPv6 adoption identified – monitoring and tracking in place | ●●●○ to ●●●● |
| Networks | • Varied status – ranging from edge of core network IPv6 enabled, to IPv6 ready, but not yet IPv6 enabled<br>• Varied status – ranging from access network IPv6 enabled, to IPv6 ready, but not yet IPv6 enabled | ●●○○ to ●●●○ |
| Applications | • Varied status – ranging from application infrastructure IPv6 enabled, to IPv6 ready, but not yet IPv6 enabled | ●●○○ to ●●●● |
| Skills | • Advanced IPv6 solution architecture and design skills in place | ●●○○ to ●●●● |
| Services | • The status of current services was variable, ranging from IPv6 trial and commercial services available, to awaiting business demand to roll out IPv6 services<br>• The status of new services was also variable, ranging from considering the launch of native IPv6 services on the next-generation broadband network (NGNBN), to awaiting business demand before developing and rolling out new IPv6 services | ●○○○ to ●●●○ |

*Figure 5.3: Summary of IPv6 readiness among domestic small ISPs in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

## 5.3 IPv4 exhaustion timelines and business impact

As ISPs come under increasing pressure to introduce IPv6 to meet business goals and cope with the evolution of service offerings, it is imperative for them to synchronise the introduction of IPv6 service offers with the IPv4 address exhaustion timeline. They need to analyse the impacts that any gap between these two timelines would have on the business.

Figure 5.4 shows a high-level view of the typical timelines for the introduction of IPv6 services by an ISP, assuming that no services are currently offered, and starting from February 2011.

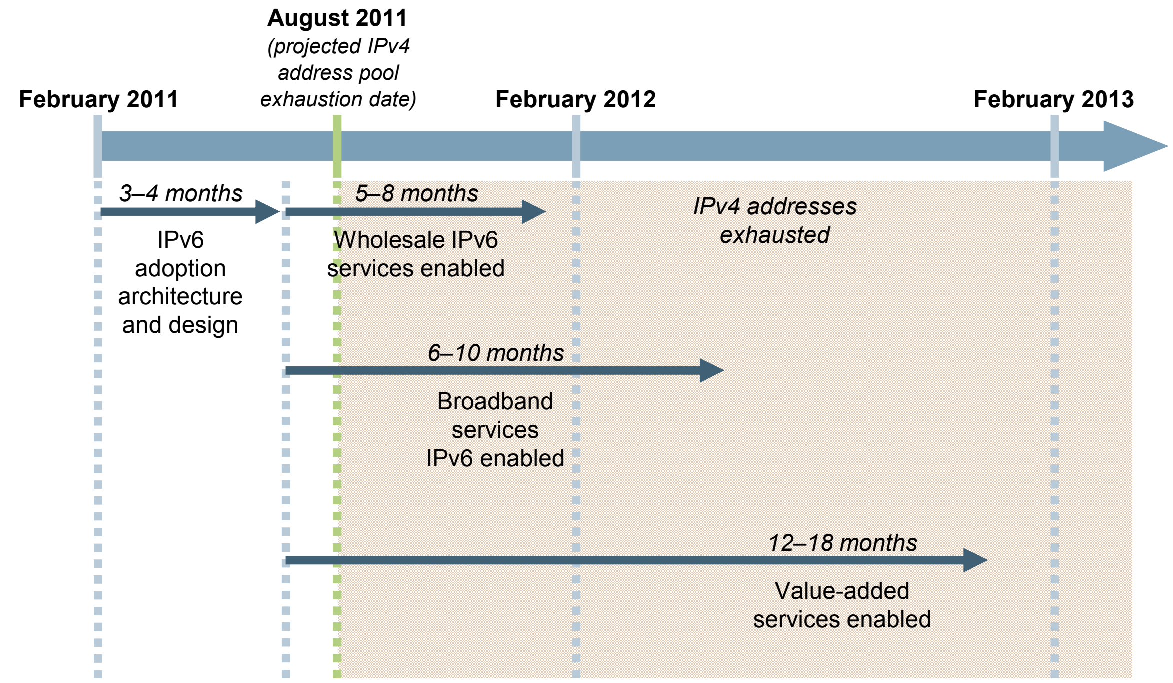

August 2011
(projected IPv4 address pool exhaustion date)
February 2011
February 2012
February 2013
3–4 months
IPv6 adoption architecture and design
5–8 months
Wholesale IPv6 services enabled
IPv4 addresses exhausted
6–10 months
Broadband services IPv6 enabled
12–18 months
Value-added services enabled

*Figure 5.4: IPv6 adoption timelines and impact on business for ISPs [Source: Analysys Mason, Tech Mahindra]*

The figure shows how Internet service providers that begin the process of adopting IPv6 today (February 2011), having done no work on IPv6 until now, will not complete IPv6 enablement of their business service offerings until *after* the projected exhaustion of IPv4 addresses. This could potentially have an impact on the business opportunities available to this industry segment in the IPv6 arena, and may also affect the ability of the businesses to grow in line with market demand.

For a single Internet service provider, the main impact of being unprepared for IPv6 and running out of IPv4 addresses will be restrictions on its ability to expand its customer base and develop new value-added services. In such a scenario, enterprise or individual customers can switch Internet service providers, assuming there is one which can either offer IPv6 services, or still has unused IPv4 addresses to allocate. If this is the case, the first Internet service provider will inevitably lose business.

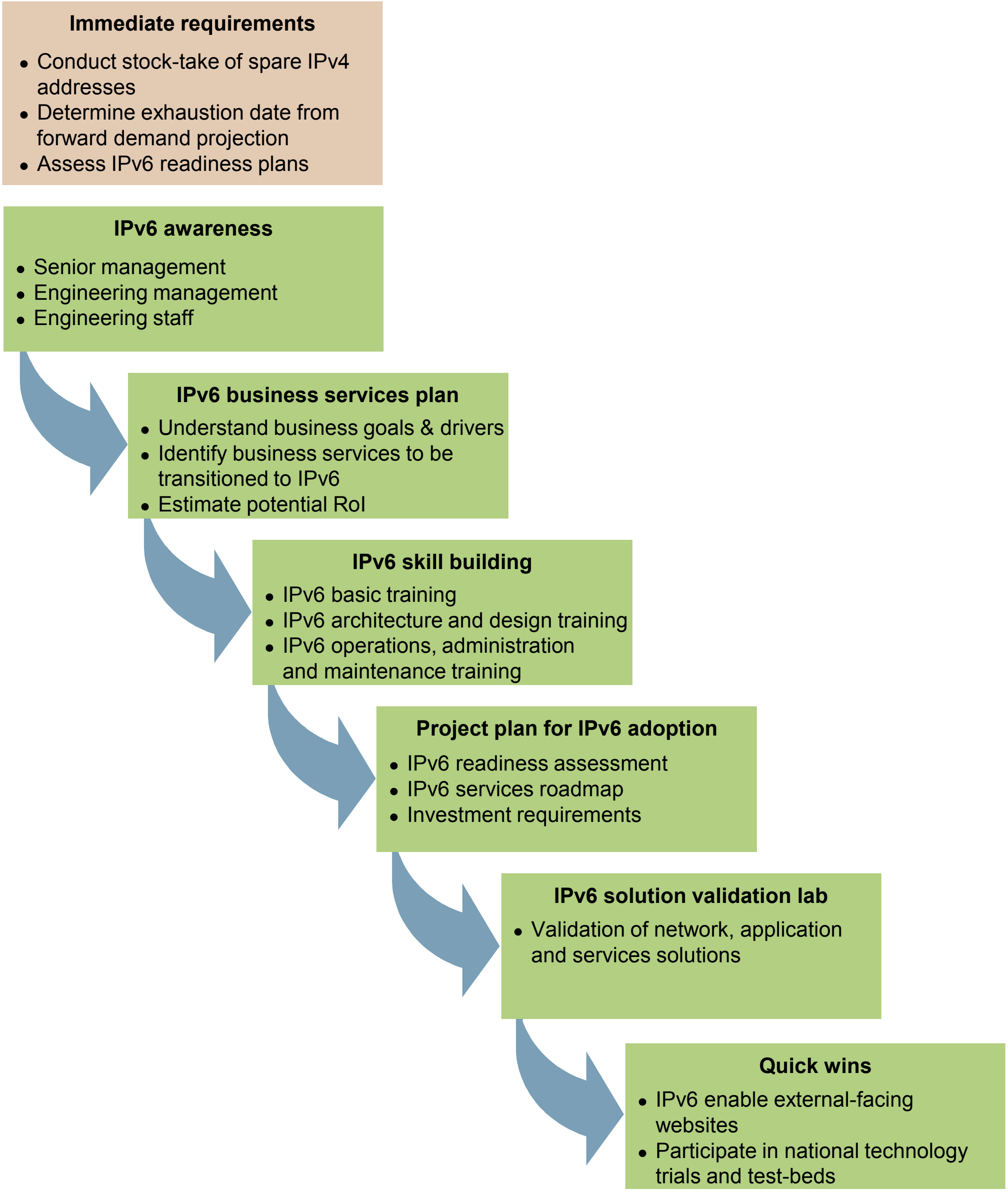
At a stakeholder category level, the Internet service providers need to plan IPv6 enablement of their business offerings accordingly, so that the Internet ecosystem across Singapore can continue to function normally and grow.

For all Internet service providers there could be two main impacts of non-readiness for IPv6 once IPv4 address allocations are exhausted.

- Businesses across the ecosystem in Singapore that do not have significant remaining IPv4 address pools, or are dependent on Internet service providers for IPv4 addresses, would be unable to procure new broadband connections to support business expansion. Similarly, new enterprises would be unable to obtain a broadband connection, or develop services requiring a public IP address (websites etc.). These two critical issues would have a direct impact on Singapore's GDP, and reduce the emergence of new, and innovative, companies.
- Individual users would be unable to obtain new fixed IP addresses, which would limit the development of Internet applications (e.g. VPN connectivity), create inequalities between those with, and without, fixed IP addresses, and have an indirect impact on Singapore's GDP.

## 5.4 IPv6 adoption guide: planning phase

During this phase an Internet service provider will draw up a detailed IPv6 adoption project plan, and start to build awareness and skills within the organisation. This phase could last between two and three months. As well as involving the development of a detailed project plan, this phase includes key activities such as building IPv6 awareness across the organisation, developing an IPv6 business services plan, conducting an IPv6 readiness assessment across information technology infrastructure, building IPv6 skills among staff, and implementing a few 'quick win' projects, such as setting up an IPv6 solution validation lab. The details of the activities to be accomplished in this phase, and the associated timelines, are provided in the remainder of this section.



**Immediate requirements**

- Conduct stock-take of spare IPv4 addresses
- Determine exhaustion date from forward demand projection
- Assess IPv6 readiness plans

**IPv6 awareness**

- Senior management
- Engineering management
- Engineering staff

**IPv6 business services plan**

- Understand business goals & drivers
- Identify business services to be transitioned to IPv6
- Estimate potential RoI

**IPv6 skill building**

- IPv6 basic training
- IPv6 architecture and design training
- IPv6 operations, administration and maintenance training

**Project plan for IPv6 adoption**

- IPv6 readiness assessment
- IPv6 services roadmap
- Investment requirements

**IPv6 solution validation lab**

- Validation of network, application and services solutions

**Quick wins**

- IPv6 enable external-facing websites
- Participate in national technology trials and test-beds

*Figure 5.5: IPv6 planning phase activities for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### 5.4.1 Immediate actions for ISPs that have yet to make provisions for IPv6 deployment

The key role of ISPs in the IPv6 deployment sequence, and the increased urgency arising from the final depletion of new IPv4 address blocks, means there is no longer time for ISPs to follow the suggested phased approach if they have yet to start, or are behind with, their preparations. ISPs in this position must therefore accelerate their progress in preparing for IPv6 by immediately undertaking the following actions:

- a stock-take of available IPv4 addresses
- a projection of requirements for IPv4 addresses (driven by their forward demand projection) to determine the exhaustion date for stockpiled addresses
- an internal assessment of IPv6 readiness plans, so that they can be re-aligned to meet the exhaustion date above.

### 5.4.2 IPv6 awareness

An IPv6 awareness programme ensures that the importance of IPv6 adoption, the key areas of impact, the costs and the timelines are shared across the organisation.

A few key aspects to be considered when preparing to raise awareness of IPv6 in an organisation are shown in Figure 5.6.

| *IPv6 awareness* | |
|---|---|
| *Overall aims* | Raise IPv6 awareness across all key stakeholders within the organisation to educate them on the importance of IPv6 adoption, the scope of activities to be accomplished, and the likely timelines |
| *Approx. duration* | 1–2 months |
| *Key tasks* | The awareness programme must be targeted at multiple segments:<br>• **senior management** – the following aspects must be covered:<br>– importance of IPv6, and the business impact of non-adoption<br>– timelines and the cost of IPv6 adoption<br>• **engineering management** – the following aspects must be covered:<br>– various aspects of network, application and services that would be affected as a result of IPv6 adoption<br>– the set of activities to be initiated to design, implement and validate the IPv6 solutions and services<br>• **engineering staff** – the following must be covered:<br>– IPv6 technology basics<br>– the mechanisms for transition to IPv6<br>– guidelines for operating and maintaining IPv6-enabled networks and solutions |
| *Stakeholders* | • Senior management, engineering management, training department |
| *Dependencies* | • No dependencies on other tasks |

*Figure 5.6: Summary of IPv6 awareness activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### 5.4.3 IPv6 business services plan

An IPv6 business services plan for an Internet service provider identifies the services that should support IPv6. This provides an essential input to the later activities within the planning phase, and ensures that the high-priority/high-impact services remain the focus for IPv6 adoption.

A few key aspects to be considered when preparing an IPv6 business services plan are shown in Figure 5.7; further details specific to Internet service providers are provided in the rest of this sub-section.

| *IPv6 business requirements plan* | |
|---|---|
| *Overall aims* | Identify business roadmap, covering business goals and drivers, identifying service offerings to be delivered using IPv6 and return-on-investment implications |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 business services plan needs to:<br>• **identify business goals and drivers** that are linked to IPv6 adoption<br>• **identify service offerings** that should support IPv6, in line with the business goals and drivers<br>• **estimate the return on investment** (either in terms of incremental revenue or cost savings compared to the case without IPv6) |
| *Stakeholders* | • Senior management, product department, engineering management |
| *Dependencies* | • The IPv6 awareness programme needs to be underway before the IPv6 business services plan can be started |

*Figure 5.7: Summary of IPv6 business services plan for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

*Business goals and drivers*

The typical business goals of Internet service providers are to:

- **cover a larger consumer base,** including both business and residential consumers, through an increased network footprint and range of broadband access services
- **increase take-up of broadband services** across both business and residential consumers
- **increase take-up of managed or value-added services** by developing new, innovative services and service bundles that can generate incremental, profitable revenue growth.[6]

[6] This is a particular focus for small ISPs.

The above business goals drive the construction of larger networks, higher take-up, and the introduction of new and innovative managed, or value-added, services. This results in increased consumption of IP addresses by Internet service providers and consumers. As indicated by the findings of the survey phase, Internet service providers are operating predominantly in an IPv4 environment, with core networks currently IPv6 enabled, but access networks and applications still running in an IPv4 environment, although some of the small Internet service providers have adopted a more progressive stance on IPv6.

With exhaustion of the IPv4 address pool looming, and a need to continue to grow their businesses, Internet service providers, and especially large Internet service providers, will need to put IPv6 high on their list of business priorities. Current projections (as of February 2011) place the exhaustion date for the IPv4 address pool available to APNIC in August 2011. We estimate that typical IPv6 adoption timelines among Internet service providers will vary from 18 to 36 months, depending on their current status. In light of these tight timelines, it is important for IPv6 adoption to be one of the business priorities and goals of Internet service providers.

*Service offerings*

As IPv4 exhaustion is a threat to business goals, the next logical step is to plan and prioritise which service offerings should be IPv6 enabled to ensure business continuity. This will allow Internet service providers to plan IPv6 enablement of the required network infrastructure and applications.

Based on customer demand and revenue and fit with business goals, the various IPv4 business and residential service offerings should be assessed for the suitability of offering comparable IPv6-enabled products and services. This initial assessment will need to be cross-checked against the current IPv6 status of the networks and applications that would be required by these services in order to develop a roadmap for the introduction of IPv6 products and services that are broad equivalents of existing IPv4 products and services.

In addition, Internet service providers could consider the potential for introducing new IPv6-based services that would support new revenue streams, although the revenue potential of these new services would need to be assessed against the costs of deployment. Some potential new services could include:

- energy-saving ‘green’ initiatives (green buildings, smart grids, etc.)
- managed services (e.g. IPv6-enabled cloud computing services).

The typical business service offerings of an Internet service provider across Singapore include:

- **broadband services** – broadband Internet connections for retail customers
- **wholesale services** – provision of Internet connectivity to carriers
- **value-added services** – innovative applications and services for customers.

*Return on investment*

A key part of the process of identifying which services should be IPv6 enabled is to estimate the return on investment from doing so. In assessing this, Internet service providers need to consider:

- **incremental revenue from IPv6 enablement** when compared to not IPv6 enabling (e.g. incremental revenue through the introduction of new value-added services or avoiding revenue 'lost' to competitors through not having IPv6-enabled services)
- **cost savings from IPv6 deployment**, such as lower costs through a reduction in the complexity of address management
- **cost implications of IPv6 enablement**, such as additional hardware requirements, upgrading of applications and opex implications of running dual IPv4 and IPv6 for some period of time.

### 5.4.4 IPv6 skill building

IPv6 skill building ensures that all stakeholders across the organisation have the required skills to contribute to, and participate in, the IPv6 adoption process, including implementation. A summary of the IPv6 skill building activities is provided in Figure 5.8.

| *IPv6 skill building* | |
|---|---|
| *Overall aims* | • Ensure that IPv6 skills are built across the various levels of the organisation (engineering management, engineering staff, etc.), so that they can participate in, and contribute to, the IPv6 adoption process<br>• Provide skills to engineering teams to enable them to implement the IPv6 adoption programme |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 skill building programme encompasses various layers of the organisation:<br>• **senior technical architects/engineering management** – skills in the following areas must be covered:<br>– IPv6 solution architecture and design<br>– IPv6 migration planning and processes<br>– IPv6 service design<br>• **engineering staff** – the following areas must be covered:<br>– IPv6 technology basics<br>– the mechanisms for transition to IPv6<br>– operating and maintaining IPv6-enabled networks and solutions |
| *Stakeholders* | HR, training department, engineering management, senior technical architects, engineering staff |
| *Dependencies* | The IPv6 awareness activity should have been completed before the IPv6 skill building activity begins, although it can be started in advance of full completion of the IPv6 awareness activity |

*Figure 5.8: Summary of IPv6 skill building activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### 5.4.5 Project plan for IPv6 adoption

The project plan for IPv6 adoption sets out the detailed set of activities to be carried out, spanning IPv6 solution architecture, design, deployment, trials and 'go live'. During the process of developing a detailed project plan, an Internet service provider must also carry out an IPv6 readiness assessment across network and applications. This assessment will highlight gaps between the current status and the eventual target of providing seamless IPv6 services, and information that will serve as inputs to the detailed project plan.

| *Project plan for IPv6 adoption* | |
|---|---|
| *Overall aims* | • Establish the organisation’s current status of IPv6 adoption across network, applications and services<br>• Draw up a detailed project plan, including the various activities to be completed for IPv6 adoption and a roadmap to ensure provision of seamless IPv6 services |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The key tasks in preparing the IPv6 adoption project plan are:<br>• establish an IPv6 consultancy team, made up of internal and / or external IPv6 experts, to have responsibility for preparing the project plan for IPv6 adoption<br>• conduct an IPv6 readiness assessment to identify the gaps in IPv6 adoption across network, applications and services<br>• map the current status of IPv6 adoption<br>• draw up a detailed project plan for IPv6 adoption<br>The project planning for achieving IPv6 readiness mentioned above needs to cover the following areas:<br>• **network infrastructure** – routers, switches, security devices, DNS, DHCP, NTP, addressing delegation mechanisms, etc., spread across the core network, broadband network, mobile network, etc.<br>• **application infrastructure** – network management, OSS/BSS, human resources (HR), enterprise resource planning (ERP) applications, etc.<br>• **services infrastructure** – the current, and planned, business services offered to customers, and the status of their IPv6 enablement<br>The project plan for IPv6 adoption will detail the set of activities that must be completed in order to IPv6 enable the network, applications and services. The plan must cover the following areas:<br>• architecture and design<br>• deployment and implementation<br>• test and validation<br>• trials<br>• ‘go live’ for IPv6 services |
| *Stakeholders* | • **IPv6 consultancy team** – a team of internal and/or external IPv6 experts responsible for preparing the project plan for IPv6 adoption. Depending on the organisation, this team may have further responsibility for execution of the project plan itself<br>• **Engineering management** – will help to provide all the inputs required for the readiness assessment, and will also identify key individuals within the business for this activity |
| *Dependencies* | • The IPv6 awareness programme needs to be completed before the IPv6 readiness programme can begin, to ensure that stakeholders understand the importance of the readiness assessment, and are willing to fully participate in it<br>• The IPv6 business services plan needs to be prepared to identify which services should support IPv6 |

*Figure 5.9: Summary of project planning for IPv6 adoption activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### 5.4.6 IPv6 solution validation lab

The IPv6 business services plan will identify the IPv6 solutions and services to be deployed and rolled out on the network. Before starting implementation, these solutions and services will need to be validated in a controlled lab environment, with the business services plan (and project plan) revised (if needed) based on the results of the validation activity.

| *IPv6 solution validation lab* | |
|---|---|
| *Overall aims* | Verify and validate the proposed IPv6-based solution (architecture, design and services) before they are rolled out in a live environment |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 solution validation lab should ensure that the IPv6 migration solution architecture included in the project plan must be validated in terms of its ability to support the required services (e.g. features and functional and performance aspects). This validation needs to cover:<br>• **IPv6 network solution** – the network solution proposed in the project plan needs to be tested for adherence to functional and performance guidelines and SLAs within the organisation<br>• **IPv6 application solution** – the various commercial and proprietary applications must be validated for their ability to function under the IPv4/IPv6 solution proposed in the project plan to a level that meets functional and performance requirements within the organisation<br>• **IPv6 services** – the business and residential services which are planned to be rolled out need to be validated in terms of functional performance and reliability in the network and application environment laid out in the project plan<br>The project plan will need to be reviewed and revised, as appropriate, based on the output of the validation lab trials |
| *Stakeholders* | Technical architects, engineering management |
| *Dependencies* | • The start of this programme is dependent on completion of the IPv6 skill building programme<br>• The IPv6 business services plans needs to be underway before this programme can start, as services to be validated need to be identified (although this programme can start slightly ahead of the identification of services) |

*Figure 5.10: Summary of IPv6 solution validation lab activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### 5.4.7 Quick wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organisation, and in giving staff the opportunity to use the theoretical skills they have gained earlier in the process, as well as to build confidence in the technology. Figure 5.11 summarises this activity, and provides a couple of examples of quick-win initiatives.

| *IPv6 quick wins* | |
|---|---|
| *Overall aims* | • Identify and implement initial 'quick win' projects<br>• Strengthen the IPv6 thought process across the organisation, develop and embed theoretical skills, and build confidence in IPv6 as a technology |
| *Approx. Duration* | 2–3 months |
| *Key tasks* | The types of project chosen will depend on the current status of an organisation, and are difficult to specify. However, some examples could include:<br>• **IPv6 enable the external-facing websites**, which would help the organisation to position itself as an IPv6 leader, and also further establish IPv6 as an internal initiative<br>• **participate in national technology trials and test-beds**, which would provide knowledge and insight that will increase familiarity with IPv6, and inform the decision-making process during subsequent phases |
| *Stakeholders* | Corporate IT management team, procurement team, technical architects |
| *Dependencies* | The IPv6 awareness programme, and the IPv6 skill-building programmes, should be completed before starting this activity |

*Figure 5.11: Summary of IPv6 'quick win' activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

## 5.5 IPv6 adoption guide: architecture and design phase

In this phase, target and transition designs for the network, applications and services are defined to IPv6 enable current IPv4-based services and support the introduction of new IPv6 services.

The IPv6 solution architecture and design phase needs to cover the areas outlined below.

- **Services** – the various IPv4 services planned to be IPv6 enabled are prioritised, and the new services planned to be introduced are finalised, based on the initial work carried out during the planning phase. This prioritisation helps in building the network and application solution architecture and designs.
- **Network** – the various network solutions are architected and designed to support the planned IPv6 services, including the IPv4 run-out scenario and transition to a complete IPv6-only ecosystem.
- **Applications** – the various solutions are architected and designed to support the planned IPv6 services and network solution.

The remainder of this section summarises the key activities in each of these areas, with annexes providing supporting technical details.

### 5.5.1 Architecture and design – services

The development of an architecture and design for the IPv6-enabled services to be offered by Internet service providers will affect the network solutions architecture and applications solution architecture that are subsequently developed. The key tasks are identified in Figure 5.12, and are discussed further below.

| *IPv6 services architecture and design* | |
|---|---|
| *Overall aims* | Build an IPv6 service architecture and design, which will help to ensure existing IPv4 services are IPv6 enabled, and to introduce new IPv6 services accordingly |
| *Approx. duration* | 1–2 months |
| *Key tasks* | • The architecture and design for services needs to develop the design and architecture for IPv6 products and services |
| *Stakeholders* | Technical architects, software engineering team, vendors |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can be initiated |

*Figure 5.12: Summary of IPv6 service architecture and design activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

Based on the IPv6 products and services identified during the planning phase, the next stage is to develop a design and architecture for these products and services.

The architecture and design process needs to consider the various IPv6 transport mechanisms (e.g. dual-stack, Teredo tunnel, ISATAP) as part of the product offering, as well as the IPv6 features required by the products, and any security considerations and SLAs. A summary of key transport mechanism technologies is provided in Annex A.

### 5.5.2 Architecture and design – networks

Once the architecture and design for the IPv6 services are finalised, a network solution architecture and design that is aligned with the products and services will have to be prepared.

The network solution architecture would need to consider the various stages through which the organisation’s network would pass (e.g. IPv4-only, support for both IPv4 and IPv6, and IPv6-only). Based on the current status of IPv6 readiness and IPv4 address availability, the solution should consider a back-up solution for a scenario where the organisation has run out of IPv4 addresses, but has not yet fully adopted IPv6.

| *IPv6 network solution architecture and design* | |
|---|---|
| *Overall aims* | Prepare an IPv6 network solution architecture and design which will help to enable IPv6 on the current IPv4-based services and introduce new IPv6 services |
| *Approx. duration* | 1–2 months |
| *Key tasks* | Ensure that the IPv6 network solution architecture and design – of both core and access networks – covers the following areas:<br>• **IPv4/IPv6 interconnectivity** – individual IPv4 and IPv6 networks are connected via various tunnelling mechanisms, dual stack, etc.<br>• **IPv6 routing** – the reachability of the network elements across IPv4 and IPv6 topologies must be ensured, through appropriate deployment of the IPv6 routing protocol<br>• **IPv6 security** – the various network solutions that are designed must ensure that the security aspects of the planned network roll-out are considered and in place<br>• **quality of service (QoS)** – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance<br>• **multicast services** – the various multicast services across the IPv6 network must be designed in accordance with the planned services<br>• **traceability of traffic sessions** – if required for regulatory purposes, recording of the various IPv6 sessions taking place across the network should be incorporated |
| *Stakeholders* | Technical architects, engineering management, network engineering team |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can be initiated, and the architecture and design for services needs to be completed, or almost completed |

*Figure 5.13: Summary of IPv6 network solution architecture and design activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

The network solution architecture and design for a given IPv6 product, or service, will need to take account of the requirements for both the core network and the access network.

The typical service provided by the **core network** is MPLS VPN, and the core network will need to be configured to support IPv6 based on the planned services. Usually, the core network of an Internet service provider should be the first network component to be IPv6 enabled, and during the survey phase we found that the majority of Internet service providers had already configured either 6PE or 6VPE on their core network, although the access network was still operating in an IPv4 environment.

**Access networks** help in extending the reach of the services to the customers, and provide the 'last mile' connection. The IPv6 solution for the access network will need to take into account the IPv6 services to be offered.

For both the core and access networks, an Internet service provider will need to consider a wide range of components, such as: IPv4/IPv6 interconnectivity, IPv6 routing, IPv6 security, QoS, multicast services, and traceability of traffic sessions. For the core and access networks, these issues are outlined in Figure 5.14. This is followed by a summary of the range of options available to an Internet service provider in moving to IPv6, with further technical details provided in Annex B.

| | *Core network* | *Access network* |
|---|---|---|
| IPv4/IPv6 interconnectivity | The IPv6 connectivity across the upstream service provider and peers needs to be considered, based on the services planned<br>The details of the IPv6 connectivity across the autonomous systems, and the routes to be announced, should also be planned in line with the expected service offerings<br>The design options thatcan be considered for providing IPv6 MPLS VPN connections are: configured tunnels; 6PE; 6VPE | Based on the access network design, the IPv6 connectivity to the core needs to be planned:<br>• a Layer 3 access network provider would need to consider forwarding access traffic through the IPv6 core using one (or more) of the following options: IPv6 tunnelling; native IPv6 deployment; MPLS 6PE deployment<br>• a Layer 2 access network provider does not have any IPv6 considerations for the access network |
| IPv6 routing | Based on the services and the IPv6 topologies being rolled out, the related IPv6 routing protocols would need to be selected and IPv6 enabled. This would include:<br>• interior gateway routing (IGP) protocol, where the options are IS-IS or OSPFv3<br>• exterior gateway routing protocol (EGP), which is delivered using BGP<br>Based on the computing resources of the routers and the performance requirements, the IPv4 and IPv6 routing can be achieved using either a single process or a dual process design | For the access network, routing options include:<br>• static routes<br>• RIPng<br>• OSPFv3<br>The relevant choice of routing option will depend on the IPv6 services to be rolled out, and the size and topology of the access network. When DHCP prefix delegation is used, route distribution also needs to be considered as part of the access network architecture and design |
| IPv6 security | The IPv6 security architecture would need to include the deployment of the various mechanisms (such as access lists and intrusion detection/prevention) that are used to provide a secure IPv6 Internet transaction environment<br>Ingress filtering should be deployed toward the customers to ensure traceability, to prevent DoS attacks using spoofed addresses, and to prevent illegitimate access to the management infrastructure. Ingress filtering can be carried out using access lists or unicast reverse path forwarding | The access network design should ensure that the Internet service provider's networks and its subscribers are protected from attacks by one of its own customers. The design options in this area include:<br>• unicast reverse path forwarding<br>• IPv6 access lists.<br>In addition to these, security mechanisms, such as a firewalls and IDS/IPS, should be considered |
| Quality of service | The IPv6 QoS design should take into consideration the various traffic engineering aspects and performance SLAs, which need to be adhered to, for the various classes of traffic | |
| Multicast services | Based on the services planned to be rolled out, the IPv6 multicast services will need to be designed accordingly, which would include BGP-MPLS multicast services. The protocols that can considered during the design are PIM-SM and PIM-SSM | The IPv6 multicast design across the access network would need to consider IGMPv3/MLDv2 |
| Traceability of traffic sessions | Traceability of traffic sessions is typically required by regulators across the globe and, if so, the systems to record and log the traffic sessions across the core network should be included in the architecture and design<br>This is accomplished by mapping a DHCP response to a physical connection and storing the results in a database. It can also be achieved by assigning a static address or prefix to the customer, or through the use of a tunnel server | |

*Figure 5.14: Considerations for the design and architecture of core and access networks [Source: Analysys Mason, Tech Mahindra]*

### 5.5.3 Options for transition approaches/mechanisms for network architecture and design

During the architecture and design phase, it is important for stakeholders to choose the right technical approach or ‘mechanism’ to enable their networks to make the transition towards IPv6. The choice of mechanism will depend on the current IPv4 environment and the planned IPv6 network, applications and services.

The IPv6 transition mechanisms for networks, which are discussed in more detail in Annex B, include:

- IPv6 in IPv4 tunnels
- dedicated IPv6 links
- dual-stack networks.

As the introduction of IPv6 across the network has to be achieved with minimal disruption to the existing network, it should be a gradual transition. The various IPv6 network transition phases for a stakeholder are shown in Figure 5.15, and explained below.

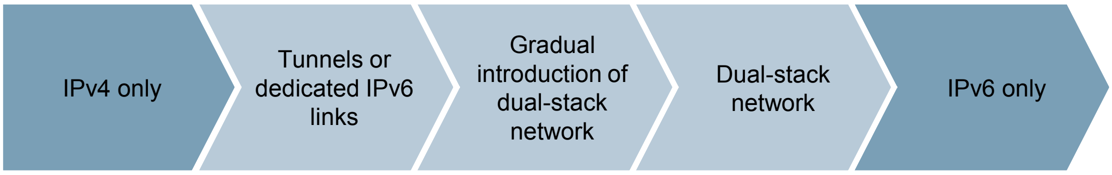

IPv4 only
Tunnels or dedicated IPv6 links
Gradual introduction of dual-stack network
Dual-stack network
IPv6 only

*Figure 5.15: Full range of transition phases that might be involved in migration from IPv4 to IPv6 [Source: Analysys Mason]*

The starting point for all stakeholders is an IPv4-only network. In this scenario, the stakeholder can connect to an IPv6 network using either IPv6 tunnelling mechanisms or separate dedicated IPv6 connections or links.

Tunnelling would be an interim temporary solution, which can be implemented with the smallest requirement for infrastructure upgrades and investment. The downside is that this model does not scale as the number of users increases.

As IPv6 adoption progresses, dual-stack network components (see Annex A for examples) are gradually introduced into the network, leading to a reduction in the usage of tunnels or dedicated IPv6 links.

The next step is for all network components across the organisation to be dual-stack ready and enabled – this allows the organisation to provide seamless IPv6 capabilities and services. This also sets the stage for gradually turning off IPv4 services and progressing towards IPv6-only services.

The final outcome is to turn off the IPv4 capabilities on the dual-stack routers, leaving only IPv6 services available to the customers.

This approach can be adopted across all stakeholder segments, and can be executed in sequence; alternatively, a stakeholder may choose to miss out some phases for business or technical reasons.

The choice of transition mechanism – tunnelling, dual-stack networks or dedicated links – will depend on the type of network that is being IPv6 enabled and the services to be supported. Annex B provides technical details on the choice of transition mechanisms for the different core network and access network scenarios listed below.

*Core network scenarios*

- Currently running an IPv4 network to offering initial IPv6 service, or interconnected IPv6 islands, or links to remote IPv6
- Backbone network – deploying MPLS (isolated IPv6 domains to communicate with each other, over IPv4 backbone)
- Backbone network – deploying ATM, Frame Relay or dWDM (establish communication between IPv6 domains)
- Small networks (IPv4 and IPv6 applications to co-exist)

*Figure 5.16: Core network scenarios detailed in Annex B [Source: Analysys Mason, Tech Mahindra]*

*Access network scenarios*

**Service offerings**

- IPv6 service offerings replicate IPv4 service offerings
- New IPv6 service offerings in addition to IPv4 service offerings

**Broadband access network**

- Cable network – bridged CMTS network
  - cable modem and CMTS operate in an IPv4 environment
  - cable modem and the CMTS bridge all data traffic supporting native IPv6 unicast and multicast traffic
- Cable network – routed CMTS network
  - IPv4 cable network with IPv6 tunnel running between host and the edge router
  - IPv4 cable network with gateway router at customer site
  - dual-stack cable network with IPv6 support for cable modem and CMTS
  - dual-stack cable network with IPv6 support for standalone gateway router and CMTS
  - dual-stack cable network with IPv6 support for embedded gateway router/cable modem and CMTS
- DSL and Ethernet
  - Point-to-point model
  - PPP terminated aggregation (PTA) model
  - L2TP access aggregation (LAA) model

*Figure 5.17: Core network scenarios detailed in Annex B [Source: Analysys Mason, Tech Mahindra]*

### 5.5.4 Architecture and design – applications

Once the IPv6 service architecture and the network architecture are finalised, an application architecture and design, which is aligned with them, can be prepared. This will consider the approach to configuring the relevant OSS/BSS, network management and network monitoring applications to support the planned IPv6 services. The key tasks are highlighted in Figure 5.18, and addressed in more detail in the subsequent text.

| *IPv6 application solution architecture and design* | |
|---|---|
| *Overall aims* | Prepare an IPv6 application solution architecture and design, which will help enable IPv6 on the current IPv4-based services and introduce new IPv6 services |
| *Approx. duration* | 1–2 months |
| *Key tasks* | The IPv6 application solution architecture and design needs to cover the following areas:<br>• ensure **network management and monitoring applications/solutions** are seamlessly able to support and monitor IPv4 and IPv6 networks<br>• ensure **applications, such as customer relationship management (CRM) and billing systems**, are able to support IPv6- and IPv4-based connectivity and services<br>• **ensure proprietary applications** are able to support both IPv6- and IPv4-based connectivity services |
| *Stakeholders* | Technical architects, software engineering team, vendors |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can begin, and the architecture and design for services need to be completed; the architecture and design for networks can be prepared in parallel |

*Figure 5.18: Summary of IPv6 application solution architecture and design activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

The application infrastructure in an Internet service provider helps in the provision of service offerings to customers. The IPv6 readiness assessment conducted in the planning phase will provide a list of IPv6-compliant and non-compliant applications. Applications that are found to be non-IPv6 compliant will need either to be upgraded to an IPv6-compliant version, or replaced with new software that provides the same functionality and is also IPv6 compliant.

The key tasks are addressed in more detail below.

*Network management and monitoring applications/ solutions*

As IPv6 adoption is initiated across network management and monitoring systems, as a first step, network device configuration and regular network management and monitoring operations can be performed over an IPv4 transport layer, as an IPv6 management information base (MIB) can be reached from an IPv4 network. In the case that ICMPv6 messages are used for monitoring, IPv6 connectivity would be required for management applications.

As a second step, IPv6 transport can be provided for any of these network and service operation applications, which would help to provide seamless IPv6 management and monitoring.

*Customer relationship management / billing systems*

The CRM and billing applications would need to support IPv6-related products and services, even if the CRM and billing systems themselves were operating in an IPv4 environment, as the required information and data processing would be independent of the IPv4/IPv6 operating environment.

As IPv6 adoption progresses, CRM and billing applications can also start to operate in an IPv6 environment.

*Proprietary applications*

For any proprietary applications that need to be IPv6 enabled to support the IPv6 services and products being offered to consumers, the required effort to develop the software for IPv6 compliance would need to be put in place.

## 5.6 IPv6 adoption guide: deployment phase

In this phase, the IPv6 adoption project plan developed during the planning phase and the solutions architected during the architecture and design phase are implemented, and IPv6 is enabled across the organisation. An overview of the activities involved in this phase is provided in Figure 5.19, and each area is discussed in further detail in the following sub-sections.

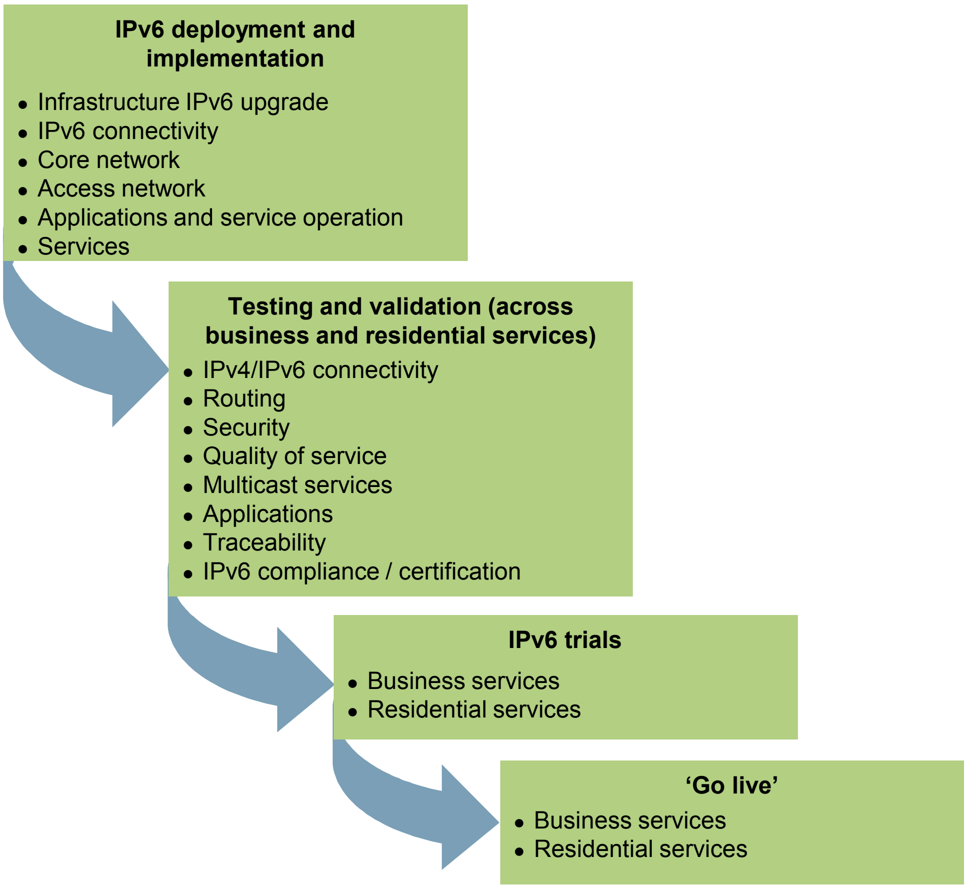


*Figure 5.19: Summary of deployment phase for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### 5.6.1 IPv6 deployment and implementation

Once the architecture and designs for services, network and applications have been identified, the next step is to deploy these solutions to be able to launch IPv6 service offerings.

| *IPv6 deployment and implementation* | |
|---|---|
| *Overall aims* | Deploy IPv6 across the network and applications of the Internet service provider to support the launch of IPv6 service offerings |
| *Approx. duration* | 3–4 months |
| *Key tasks* | The IPv6 deployment and implementation would cover the following areas:<br>• **infrastructure IPv6 upgrade** of the hardware and software systems (if they are not IPv6 ready), or replacement with IPv6-compliant software<br>• **IPv6 connectivity** – IPv6 addresses are purchased, and IPv6 connectivity with upstream providers and other peers is established<br>• **core network** – IPv6 is adopted across the core network, comprising the network, security, applications, services elements<br>• **access network** – the IPv6 network is adopted across the access network wherein the network elements, routing, security, applications, services etc. are upgraded to IPv6<br>• **applications and service operations** – the various applications, such as network management, monitoring, customer relationship management, etc. are IPv6 enabled<br>• **services** – the various services spread across the business and residential customers are IPv6 enabled |
| *Stakeholders* | Technical architects, network engineering team and software engineering team |
| *Dependencies* | The IPv6 service, network and application architecture need to be mostly completed before deployment and implementation can be started |

*Figure 5.20: Summary of IPv6 deployment and implementation activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

We discuss the key aspects of the six tasks identified above in the rest of this sub-section.

*Infrastructure IPv6 upgrade*

Based on a comparison of the solution architecture and design (across networks, applications and services) and the findings of the IPv6 readiness assessment from the planning phase, organisations can prepare a list of the infrastructure that would need to be upgraded to IPv6 to support the planned services and products. The process of upgrading this infrastructure should be initiated as a first step in the deployment of IPv6.

*IPv6 connectivity*

To support the launch of IPv6 services and products, an Internet service provider would have to:

- obtain an IPv6 prefix allocation from APNIC
- enable IPv6 peering with upstream providers and other peers.

### *Core network*

The core network primarily comprises high-speed core and edge routers. During this task, IPv6 would be enabled in the core network, based on the network architecture and design developed in the previous activity. As such, it should consider the areas outlined earlier in Figure 5.14, namely:

- IPv4/IPv6 interconnectivity
- IPv6  routing
- IPv6 security
- QoS
- multicast services
- traceability of traffic sessions.

### *Access network*

The access network primarily comprises the network from the edge of the core to the customer premises. During this task, IPv6 will be enabled in the access network, based on the network architecture and design developed. As such, it will consider the areas outlined earlier in Figure 5.14 (IPv4/IPv6 interconnectivity, IPv6  routing, IPv6 security, QoS, multicast services, and traceability of traffic sessions).

| *Area for consideration* | *Description* |
|---|---|
| IPv4/IPv6 interconnectivity | IPv6 connectivity of the access network to the core should be deployed according to the design through one of the options outlined below<br>A Layer 3 access network provider would forward access traffic through the IPv6 core using one (or more) of:<br>• IPv6 tunnelling<br>• native IPv6 deployment<br>• MPLS 6PE deployment |
| IPv6  routing | Based on the network design, the  routing protocol (e.g. RIPng, OSPFv3) should be configured. Where DHCP prefix delegation is used, the route distribution would also be configured |
| IPv6 security | The access network design is configured to provide security in an IPv6 environment through the use of unicast reverse path forwarding, IPv6 access lists, and security mechanisms, such as a firewall, IDS/IPS, etc. |
| Quality of service | The IPv6 QoS design should be configured across the network to ensure that the traffic engineering requirements and SLAs committed to the customers are met |
| Multicast services | If required as part of the network design, IPv6 multicast would be enabled using IGMPv3/MLDv2 protocols |
| Traceability of traffic sessions | Traceability of traffic sessions is implemented by recording and logging the details of the traffic sessions. This is accomplished by mapping a DHCP response to a physical connection and storing the results in a database. It can also be achieved by assigning a static address or prefix to the customer, or through the use of a tunnel server |

*Figure 5.21: Considerations for the access network design for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### *Applications and service operations*

The applications and service operations solutions help in enabling IPv6 products and services solutions across an Internet service provider. The following need to be considered in enabling IPv6 across applications and serviced operations.

| *Area for consideration* | *Description* |
|---|---|
| IPv6 address management system | An IPv6 address management system would have to be brought into place, this would help plan, provision and manage the IPv6 address allocation and lifecycle, across the IPv6 eco-system of a domestic large service provider |
| IPv6 enable the network management and monitoring applications | The network management and monitoring applications would need to be IPv6 enabled, wherein they operate in a dual-stack or IPv6 environment. This would help in managing and monitoring the various IPv6-enabled resources |
| Accounting, billing applications are IPv6 enabled | The IPv6 enablement of the accounting, billing and other corporate applications, would help in ensuring that the customer support system for the IPv6 services being rolled out is in place |

*Figure 5.22: Considerations for the application and service operation design for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### *Services*

After IPv6 roll-out has been completed across the network and the applications areas, the next stage is to enable the services. The various aspects that need to be implemented for IPv6 enablement of a service are outlined below.

| *Area for consideration* | *Description* |
|---|---|
| Business services | The business services across the service provider are IPv6 enabled, typically starting with MPLS VPN services and to corporate business customers IPv6 transit and peering services |
| Residential services | Data, voice and video service to the customers are IPv6 enabled |

*Figure 5.23: Considerations for service design for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### 5.6.2 IPv6 test and validation

| *IPv6 test and validation* | |
|---|---|
| *Overall aims* | Validate IPv6 services across the network and applications across the Internet service provider |
| *Approx. duration* | 3–4 months |
| *Key tasks* | IPv6 test and validation will cover the following areas of **business and residential** IPv6 products and services:<br>• **IPv4/IPv6 connectivity** will be validated<br>• **IPv6 routing** the network elements across IPv4 and IPv6 topologies will be reachable through the appropriate IPv6 routing protocol<br>• **IPv6 security** – the security aspects of the network will be validated<br>• **QoS** aspects will be validated across the network<br>• **multicast services** as per the service design will be validated across the network<br>• **applications** – the various applications will be validated for their IPv6 support<br>• **traceability of traffic sessions** – the various IPv6 sessions established across the network will be recorded for regulatory purposes, and the reliability of the system will be validated<br>• **IPv6 compliance / certification (optional)** – the IPv6 services are tested against a range of certifications or compliance measurement programmes |
| *Stakeholders* | Technical architects, network engineering team, software engineering team |
| *Dependencies* | The IPv6 services solution roll-out should be completed |

*Figure 5.24: Summary of IPv6 test and validation activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

The test and validation activities help in assessing the reliability and performance of the various business and residential services. The various aspects that need to be tested and validated as part of the IPv6 adoption process are outlined below.

- **IPv4/IPv6 interconnectivity** – organisations should verify the 'reachability' of individual IPv6 networks through IPv4 networks in which IPv6 transition mechanisms are implemented. Similarly, the reachability of IPv4 networks through an IPv6 network should also be verified.
- **IPv6 routing** – organisations should verify the ability to navigate the IPv6 topology through the implemented IPv6 routing protocol. This includes verifying that the routing tables include all the IPv6 routes that are required to reach the various elements in the IPv6 topology.
- **IPv6 security** – organisations should verify and validate the IPv6 security implemented across the network by conducting vulnerability and penetration tests.
- **QoS** – organisations should verify the performance and reliability of the various classes of QoS that have been implemented, by injecting traffic and conducting stress tests.
- **Multicast –** organisations should validate the ability of various multicast services to distribute services in a seamless manner, by assessing service performance against pre-determined specifications.

- **Applications** – organisations should validate the functional and performance aspects of various applications and related solutions in an IPv6 environment.
- **Traceability of traffic sessions –** organisations should validate that the various IPv6 traffic sessions are being correctly recorded/logged, and that the implemented tracing system is reliable.
- **IPv6 compliance / certification (optional)** – once all other test and validation tasks have been completed, an Internet service provider may choose to apply for IPv6 compliance or certification testing to indicate that their services meet known standards. Currently, no standards or certifications have been mandated in Singapore, so this step is optional for Internet service providers. Details of the compliance and certification programmes that are currently available, including a summary of what each of these measure, is available in Annex C.

### 5.6.3 IPv6 trials

| *IPv6 trials* | |
|---|---|
| *Overall aims* | IPv6 trials are conducted with a few trusted customers |
| *Approx. duration* | 3–4 months |
| *Key tasks* | IPv6 trials are conducted with customers, covering:<br>• **business services** – wholesale Internet/MPLS VPN services and managed network services are validated for reliability and performance<br>• **residential services** – broadband services are validated for reliability and performance |
| *Stakeholders* | Business teams, engineering management, account management, operations and support |
| *Dependencies* | IPv6 testing and validation should be completed before trials |

*Figure 5.25: Summary of IPv6 trials activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

After the network, applications and services have been IPv6 enabled, and the solutions have been tested and validated, the next stage in the IPv6 adoption process of an Internet service provider is to run a commercial IPv6 trial with a few customers. As part of the trials, the following services will be validated for their conformance to functional and performance specifications:

- **business services** – the corporate IPv6 MPLS VPN, transit, etc. services will be validated for their compliance with IPv6 functions and features, and also for their performance aspects
- **residential services** – home services, such as voice, data and video services, will be validated for their IPv6 functional and performance compliance.

### 5.6.4 IPv6 ‘go live’

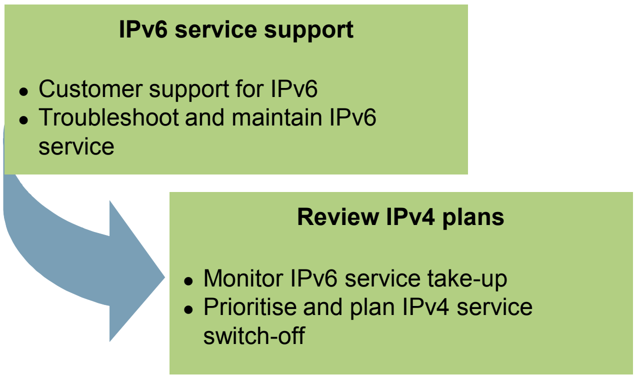
| *IPv6 ‘go live’ trials* | |
|---|---|
| *Overall aims* | IPv6 services are rolled out commercially |
| *Approx. duration* | 3–4 months |
| *Key tasks* | IPv6 services are made available commercially to customers, and rolled out on a large scale, including:<br>• **business services** – provision of current wholesale MPLS VPN services and managed network services to customers<br>• **residential services** – provision of broadband services to customers |
| *Stakeholders* | Business teams, engineering management, marketing operations |
| *Dependencies* | The IPv6 trials must be completed before IPv6 ‘go live’ |

*Figure 5.26: Summary of IPv6 ‘go live’ trials activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

After the service, network and application solutions to support the provision of IPv6 services and products have been deployed, and the Internet service provider has conducted successful commercial trials, the Internet service provider can decide whether to launch commercial IPv6 services.

## 5.7 IPv6 adoption guide: ongoing support phase

In this phase, the focus is on providing service support for IPv6 products and services, monitoring take-up and, potentially, gradually switching off IPv4 services.



**IPv6 service support**

- Customer support for IPv6
- Troubleshoot and maintain IPv6 service

**Review IPv4 plans**

- Monitor IPv6 service take-up
- Prioritise and plan IPv4 service switch-off

*Figure 5.27: Summary of ongoing support phase for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

### 5.7.1 IPv6 service support

| *IPv6 service support* | |
|---|---|
| *Overall aims* | IPv6 customers are supported, and service performance is stabilised |
| *Approx. duration* | Ongoing |
| *Key tasks* | The customer support system for IPv6 products and services must ensure that customers have a seamless service experience:<br>• **customer support** – the various trouble tickets raised for IPv6 will be analysed, and the respective troubleshooting and maintenance team will ensure that the issue is resolved as soon as possible, and common/regular faults are identified and addressed<br>• **troubleshoot and maintain IPv6 service** – the customer support team will work closely with the technical architects to fine tune the IPv6 system and help ensure that it is robust/stable |
| *Stakeholders* | Business teams, engineering management, marketing operations |
| *Dependencies* | IPv6 services are commercially available |

*Figure 5.28: Summary of IPv6 service support activity for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

Once IPv6 services have been launched on a commercial basis, the IPv6 networks, applications and services should be monitored for functional performance and adherence to the SLAs.

### 5.7.2 Review IPv4 plans

| *Review IPv4 plan* | |
|---|---|
| *Overall aims* | Review the IPv4 services and plan a phase-out approach |
| *Approx. duration* | Ongoing |
| *Key tasks* | After successfully rolling out commercial IPv6 services, the Internet service provider will need to:<br>• **monitor IPv6 service take-up** to provide inputs to the product management team for the development of future IPv6 products, and to identify IPv4 products that could be phased out<br>• **prioritise and plan IPv4 service switch-off**, including a timeline and a phased approach for ending IPv4 services |
| *Stakeholders* | Business teams, engineering management, marketing operations |
| *Dependencies* | IPv6 services are commercially available |

*Figure 5.29: Summary of IPv4 review plans for Internet service providers [Source: Analysys Mason, Tech Mahindra]*

Following the introduction of IPv6 services, an Internet service provider would need to consider the scope for retiring IPv4 products and services to reduce the operational requirements for maintaining and running both an IPv4- and IPv6-capable network. To inform this process, the Internet service provider should monitor take-up of IPv6 services, and identify IPv4 products that could potentially be retired, and also identify new IPv6 products that could be launched.

# 6 IPv6 adoption guide: Network providers

Network providers will be key players in delivering IPv6 services to the end user. The variety of physical media in use are broadly split between wireline and wireless technologies, which, in turn, can be further sub-divided into specific system types. There are interdependencies between the fixed and mobile domains (e.g. mobile networks rely on extensive fixed core networks). There are also multiple interfaces between networks owned by different operators that must operate at compatible protocol levels; that is, if IPv6 traffic is to successfully transit across several discrete networks, all of those networks must be IPv6 enabled.

Individual network providers may provide one, or more types, of service within their portfolio, but for clarity this section classifies the services by technology category, as follows:

- mobile network providers offering GSM and 3G services (and planning for LTE deployment)
- fixed international network providers offering IP connectivity
- wireless (fixed) network providers offering broadband IP-based services, such as WiMAX.

Fixed national network providers offering IP connectivity (ISPs) are included within Section 5 above. Carriers can provide services at a purely national level and/or on an international basis.

Section 6.1 sets out a summary of the IPv6 adoption guide; Section 6.2 provides a summary of the survey results, and Section 6.3 provides a summary of the drivers and timelines for this stakeholder category to adopt IPv6. Sections 6.4 to 6.7 provide details for each phase of the adoption, including planning, architecture and design, deployment and support.

## 6.1 IPv6 adoption guide: overall summary

For network operators, the main challenge will be to provide IPv6 transparency across their infrastructure, such that customers who use IP can transit their IPv6 traffic across the network. The four main phases of IPv6 adoption are:

- **planning**: IPv6 awareness and skill building activities are undertaken, and the plans for IPv6 adoption are prepared. In addition, a few ‘quick win’ projects are identified to build confidence and understanding of IPv6
- **architecture and design**: the target and transition designs for the network, applications and services that will run on IPv6 are defined
- **deployment**: the IPv6 solution is deployed across the network, applications and services area, with quick win projects implemented at the start of the deployment phase
- **support**: IPv6 services are monitored for performance and reliability, and a customer support system is put in place for the IPv6 services provided to customers, to ensure they have a seamless and smooth experience of IPv6 services.

Details of the four phases, and the activities involved in each, are illustrated in Figure 6.1. We provide details of the key activities within each phase in later sections of this adoption guide.

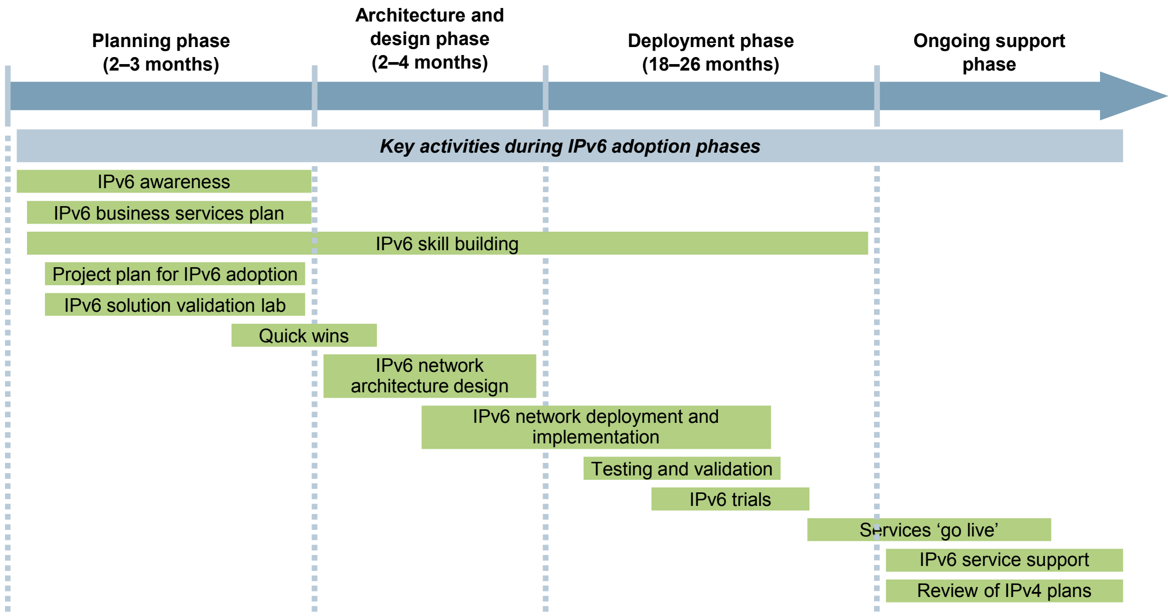

Planning phase (2–3 months)
Architecture and design phase (2–4 months)
Deployment phase (18–26 months)
Ongoing support phase
Key activities during IPv6 adoption phases
IPv6 awareness
IPv6 business services plan
IPv6 skill building
Project plan for IPv6 adoption
IPv6 solution validation lab
Quick wins
IPv6 network architecture design
IPv6 network deployment and implementation
Testing and validation
IPv6 trials
Services 'go live'
IPv6 service support
Review of IPv4 plans

*Figure 6.1: Activities involved in the four IPv6 adoption phases for network providers [Source: Analysys Mason, Tech Mahindra]*

## 6.2 Summary of findings from survey phase

The network operator category includes mobile operators, international carriers and wireless operators. Figure 6.2 to Figure 6.4 summarise the findings from the survey phase for each of these stakeholder groups.

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • A broad timeline of the end of 2011 has been identified for IPv6 adoption<br>• Design and roll-out plan not in place<br>• IPv6 business strategy not in place – no new IPv6 services or products planned<br>• Teams for IPv6 adoption identified – monitoring and tracking process not in place | ●●○○ |
| Networks | • Initial stages – only the edge of backhaul is IPv6 enabled (where shared with domestic large ISPs)<br>• IPv6 solutions being tested in lab – no live deployment | ●○○○ |
| Applications | • Initial stages – limited, or no, IPv6 readiness assessment undertaken<br>• IPv6 enablement of applications not undertaken | ●○○○ |
| Skills | • Basic skills in place – advanced design and architecture training planned | ●●○○ |
| Services | • No mobile IPv6 services available – no plan in place | ○○○○ |

*Figure 6.2: Summary of IPv6 readiness among mobile operators in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • Initial stages of planning for IPv6 adoption, understanding the budget impact and return on investment details<br>• Business driver – varied status ranging from being ahead of the technology demand curve to business continuity | ●○○○ to ●●●○ |
| Networks | • The core network of one service provider is IPv6 enabled at the edge, while others still operate in an IPv4 environment<br>• The wireless networks have not been assessed for IPv6 readiness, but are assumed to be IPv6 ready, due to recent technology refreshes | ○○○○ to ●○○○ |
| Applications | • Varied status – ranging from plans to make applications IPv6 ready, to no IPv6 readiness assessment completed | ○○○○ to ●○○○ |
| Skills | • Varied status – ranging from architecture and design skills in place for one operator, to other having basic IPv6 skills in place | ●○○○ to ●●○○ |
| Services | • Varied status – ranging from plans in place to IPv6 enable the current services and roll out new IPv6 services, to no plans in place | ○○○○ to ●○○○ |

*Figure 6.3: Summary of IPv6 readiness among wireless operators in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • Varied status – one carrier is providing IPv6 commercial services, but others are not planning to offer services<br>• Varied status – one carrier has identified teams for IPv6 adoption, but others have not yet started identifying a team<br>• IPv6 services not included in product portfolio or marketing plans | ●○○○ to ●●●● |
| Networks | • Varied status – one carrier has IPv6 enabled the edge of its core network, but others have not yet assessed IPv6 readiness of their network | ●○○○ to ●●●● |
| Applications | • Varied status – one carrier has IPv6 enabled the applications, but others have not yet assessed the IPv6 readiness of applications | ●○○○ to ●●●● |
| Skills | • IPv6 skill development plan in place – internal training or vendor product training | ●●○○ to ●●●● |
| Services | • Varied status – one carrier has IPv6 commercial or trial services available, but others have yet to plan them | ○○○○ to ●●●○ |

*Figure 6.4: Summary of IPv6 readiness among international carriers in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

## 6.3 IPv4 exhaustion timelines and business impact

Because mobile operators and wireless Internet providers require IP addresses they will come under increasing pressure to introduce IPv6 to meet business goals and cope with the evolution of service offerings as the exhaustion of IPv4 addresses approaches. It is therefore imperative for them to synchronise the timeline for the introduction of IPv6 with the timeline for exhaustion of both IPv4 addresses available from APNIC, and their own allocation of IPv4 addresses. They need to analyse the impacts that any gap between these timelines would have on their business. International carriers will not be directly affected by IPv4 address exhaustion, but the provision of IPv6 transparent network services must be aligned with the needs of their customers migrating to IPv6.

The use of IPv6 within the core of next-generation networks (NGNs) will, however, have an impact on other aspects of network providers' businesses if they are building such networks; due to the specialist nature of the NGNs, this has not been specifically covered within this report.

Figure 6.5 provides a high-level view of typical timelines for the introduction of IPv6 services by network providers, assuming that no services are currently offered, and starting from February 2011.

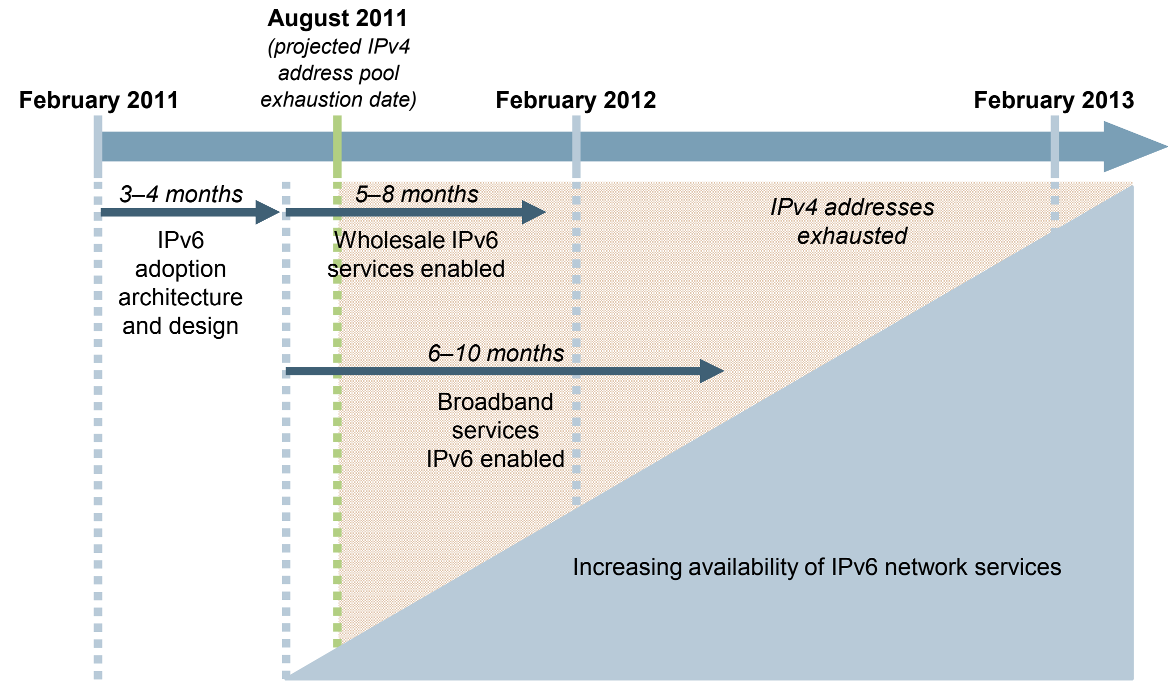

August 2011
(projected IPv4 address pool exhaustion date)
February 2011
February 2012
February 2013
3–4 months
IPv6 adoption architecture and design
5–8 months
Wholesale IPv6 services enabled
IPv4 addresses exhausted
6–10 months
Broadband services IPv6 enabled
Increasing availability of IPv6 network services

*Figure 6.5: IPv6 adoption timelines and impact on business for network providers [Source: Analysys Mason, Tech Mahindra]*

### 6.3.1 Mobile operators

For mobile operators, the indicated timeline for IPv4 exhaustion is a less pressing issue than it is for some other stakeholder groups (e.g. ISPs), as they hold blocks of addresses and make use of other techniques to reuse their IP address pool (e.g. DHCP). The broad timeline for IPv6 adoption stated by mobile operators during the survey phase was the end of 2011, and so the planning process should already be well underway if mobile operators are to achieve this date (and it was generally the case during the interviews in the survey phase that mobile operators had started the planning process).

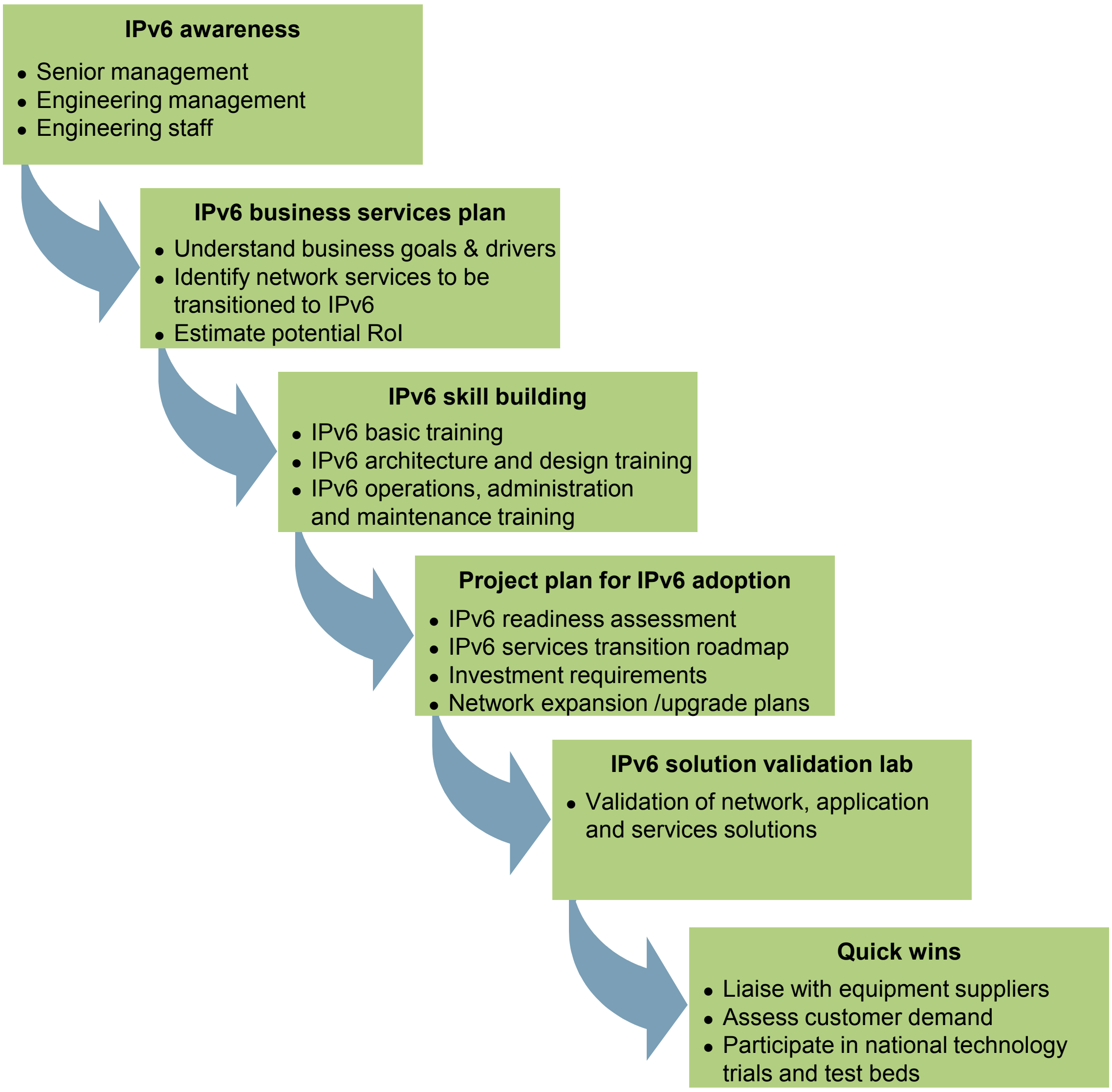
The future deployment of LTE (or 4G) networks, which are to be based on IPv6, will require enhancement of the existing packet-switched domain as a precursor to deploying any new systems.

### 6.3.2 International operators

The timeline for IPv6 deployment by international carriers will be largely driven by customer demand; that is, the exhaustion of IPv4 addresses will not have a direct impact on this category. Results from the survey indicated that one operator is already offering IPv6 services, which suggests that other operators will need to follow suit in order to avoid progressively losing market share due to their inability to meet customer needs.

## 6.4 IPv6 adoption guide: planning phase

During this phase a network provider will draw up a detailed project plan for IPv6 adoption, and start to build awareness and skills within the organisation. This phase could last between two and three months, and will include activities such as: building IPv6 awareness across the organisation, developing an IPv6 business services plan, conducting an IPv6 readiness assessment across information technology infrastructure, building IPv6 skills among staff, and implementing a few ‘quick win’ projects, such as setting up an IPv6 solution validation lab. These are shown in schematic form in Figure 6.6, and discussed in greater detail in the remainder of this section.



**IPv6 awareness**

- Senior management
- Engineering management
- Engineering staff

**IPv6 business services plan**

- Understand business goals & drivers
- Identify network services to be transitioned to IPv6
- Estimate potential RoI

**IPv6 skill building**

- IPv6 basic training
- IPv6 architecture and design training
- IPv6 operations, administration and maintenance training

**Project plan for IPv6 adoption**

- IPv6 readiness assessment
- IPv6 services transition roadmap
- Investment requirements
- Network expansion /upgrade plans

**IPv6 solution validation lab**

- Validation of network, application and services solutions

**Quick wins**

- Liaise with equipment suppliers
- Assess customer demand
- Participate in national technology trials and test beds

*Figure 6.6: IPv6 planning phase activities for network providers [Source: Analysys Mason, Tech Mahindra]*

### 6.4.1 IPv6 awareness

An IPv6 awareness programme ensures that the importance of IPv6 adoption, the key areas of impact, the costs and the timelines are shared across the organisation. A few key aspects to be considered when preparing to raise awareness of IPv6 in an organisation are shown in Figure 6.7.

| *IPv6 awareness* | |
|---|---|
| *Overall aims* | Raise IPv6 awareness across all key stakeholders within the organisation to educate them on the importance of IPv6 adoption, the scope of activities to be accomplished, and the likely timelines |
| *Approx. duration* | 1–2 months |
| *Key tasks* | The awareness programme must be targeted at multiple segments:<br>• **senior management** – the following aspects must be covered:<br>– importance of IPv6, and the business impact of non-adoption<br>– timelines and the cost of IPv6 adoption<br>• **engineering management** – the following aspects must be covered:<br>– various aspects of network, application and services that would be affected as a result of IPv6 adoption<br>– the set of activities to be initiated to design, implement and validate the IPv6 solutions and services<br>• **engineering staff** – the following must be covered:<br>– IPv6 technology basics<br>– the mechanisms for transition to IPv6<br>– guidelines for operating and maintaining IPv6-enabled networks and solutions |
| *Stakeholders* | • Senior management, engineering management, training department |
| *Dependencies* | • No dependencies on other tasks |

*Figure 6.7: Summary of IPv6 awareness activity for network providers [Source: Analysys Mason, Tech Mahindra]*

### 6.4.2 IPv6 business services plan

An IPv6 business services plan for a network provider identifies the services that should support IPv6. This provides an essential input to the later activities within the planning phase, and ensures that high-priority/high-impact services remain the focus for IPv6 adoption.

A few key aspects to be considered when preparing an IPv6 business services plan are shown in Figure 6.8; further details specific to network providers are provided in the rest of this sub-section.

| *IPv6 business requirements plan* | |
|---|---|
| *Overall aims* | Identify business roadmap, covering business goals and drivers, identifying service offerings to be delivered using IPv6 and return-on-investment implications |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 business services plan needs to:<br>• **identify business goals and drivers** that are linked to IPv6 adoption<br>• **identify service offerings** that should support IPv6, in line with the business goals and drivers<br>• **estimate the return on investment** (either in terms of incremental revenue or cost savings compared to the case without IPv6) |
| *Stakeholders* | • Senior management, product department, engineering management |
| *Dependencies* | • The IPv6 awareness programme needs to be underway before the IPv6 business services plan can be started |

*Figure 6.8: Summary of IPv6 business services plan for network providers [Source: Analysys Mason, Tech Mahindra]*

### *Business goals and drivers*

The typical business goals of network providers are to:

- **ensure their product portfolio** matches the prevailing market demand
- **launch new value-added services** to provide additional revenue streams
- **improve their operating efficiency** by reducing the number of technology platforms.

To some extent, all of the above business goals are based on the operators' ability to offer IPv6-compatible services, or to use IPv6 within their core infrastructure. Results from the survey indicated that all the network providers were aware of the need to consider IPv6 in their future investment plans.

### *Service offerings*

The typical business service offerings of network providers across Singapore include:

- **mobile services** – multimedia mobile services providing broadband Internet connections for personal and business customers
- **fixed terrestrial networks** – offering IPv6 connectivity on an any-to-any basis across an IP VPN cloud
- **wireless networks (fixed)** – offering Internet connectivity via an ISP or, potentially, IPv6 connectivity on an any-to-any basis across a VPN cloud.

*Return on investment*

A key part of the process of identifying which services should be IPv6 enabled is to estimate the return on investment from doing so. In assessing this, network providers need to consider:

- **incremental revenue from IPv6 enablement** when compared to not IPv6 enabling (e.g. incremental revenue through the introduction of new value-added services or avoiding revenue being 'lost' to competitors through not having IPv6-enabled services)
- **cost savings from IPv6 deployment**, such as lower costs achieved through simplification of the network infrastructure
- **cost implications of IPv6 enablement**, such as additional hardware requirements and upgrades to applications (although these can be phased in over a period of time).

### 6.4.3 Project plan for IPv6 adoption

The project plan for IPv6 adoption sets out the detailed set of activities to be carried out, spanning IPv6 solution architecture, design, deployment, trials and 'go live'. There will be some variation between the tasks undertaken by various categories of network provider, but the generic process will remain valid. During the process of developing a detailed project plan, a network provider must also carry out an IPv6 readiness assessment across network and applications. This assessment will highlight gaps between the current status and the eventual target of providing seamless IPv6 services, information that will serve as inputs to the detailed project plan.

| *Project plan for IPv6 adoption* | |
|---|---|
| *Overall aims* | • Establish the organisation’s current status of IPv6 adoption across network, applications and services<br>• Draw up a detailed project plan, including the various activities to be completed for IPv6 adoption, and a roadmap to ensure provision of seamless IPv6 services |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The key tasks in preparing the IPv6 adoption project plan are:<br>• establish an IPv6 consultancy team, made up of internal and/or external IPv6 experts, with responsibility for preparing the project plan for IPv6 adoption<br>• conduct an IPv6 readiness assessment to identify the gaps in IPv6 adoption across network, applications and services<br>• engage with existing vendors who provide systems affected by IPv6 adoption<br>• map the current status of IPv6 adoption<br>• draw up a detailed project plan for IPv6 adoption<br>The IPv6 readiness assessment mentioned above needs to cover the following areas:<br>• **network infrastructure** – routers, switches, security devices, DNS, DHCP, NTP, addressing delegation mechanisms, etc., spread across the core network, broadband network, mobile network, etc.<br>• **application infrastructure** – network management, OSS/BSS (for the IPv6 adoption processes for corporate applications, such as human resources (HR), enterprise resource planning (ERP), etc. (Please refer to the End User section of this document, Section 8)<br>• **services infrastructure** – the current, and planned, business services offered to customers, and the status of their IPv6 enablement<br>The project plan for IPv6 adoption will detail the set of activities that must be completed in order to IPv6 enable the network, applications and services. The plan must cover the following areas:<br>• architecture and design<br>• deployment and implementation<br>• test and validation<br>• trials<br>• ‘go live’ for IPv6 services |
| *Stakeholders* | • **IPv6 consultancy team** – a team of internal and/or external IPv6 experts responsible for preparing the project plan for IPv6 adoption. Depending on the organisation, this team may have further responsibility for execution of the project plan itself<br>• **Engineering management** – will help to provide all the inputs required for the readiness assessment, and will also identify key individuals within the business for this activity |
| *Dependencies* | • The IPv6 awareness programme needs to be completed before the IPv6 readiness programme can begin, to ensure that stakeholders understand the importance of the readiness assessment, and are willing to participate fully in it<br>• The IPv6 business services plan needs to be prepared to identify which services should support IPv6 |

*Figure 6.9: Summary of project planning for IPv6 adoption activity for network providers [Source: Analysys Mason, Tech Mahindra]*

### 6.4.4 IPv6 solution validation lab

The IPv6 business services plan will identify the IPv6 solutions and services to be deployed and rolled out on the network. Before starting implementation, these solutions and services will need to be validated in a controlled lab environment, with the business services plan (and project plan) revised (if needed) based on the results of the validation activity.

| *IPv6 solution validation lab* | |
|---|---|
| *Overall aims* | Verify and validate the proposed IPv6-based solution (architecture, design and services) before they are rolled out in a live environment |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 solution validation lab should ensure that the IPv6 migration solution architecture included in the project plan is validated, in terms of its ability to support the required services (e.g. features and functional and performance aspects). This validation needs to cover:<br>• **IPv6 network solution** – the network solution proposed in the project plan needs to be tested for adherence to functional and performance guidelines and SLAs within the organisation<br>• **IPv6 application solution** – the various commercial and proprietary applications must be validated for their ability to function under the IPv4/IPv6 solution proposed in the project plan to a level that meets functional and performance requirements within the organisation<br>• **IPv6 services** – the business and residential services that are planned to be rolled out need to be validated in terms of functional performance and reliability in the network and application environment laid out in the project plan<br>The project plan will need to be reviewed and revised, as appropriate, based on the output of the validation lab trials |
| *Stakeholders* | Technical architects, engineering management |
| *Dependencies* | • The start of this programme is dependent on completion of the IPv6 skill building programme<br>• The IPv6 business services plan needs to be underway before this programme can start, as services to be validated need to be identified (although this programme can start slightly ahead of the identification of services) |

*Figure 6.10: Summary of IPv6 solution validation lab activity for network providers [Source: Analysys Mason, Tech Mahindra]*

### 6.4.5 Quick wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organisation, and in giving staff the opportunity to use the theoretical skills they have gained earlier in the process, as well as to build confidence in the technology. Figure 6.11 summarises this activity, and provides a couple of examples of quick-win initiatives.

| *IPv6 quick wins* | |
|---|---|
| *Overall aims* | • Identify and implement initial 'quick-win' projects<br>• Strengthen the IPv6 thought process across the organisation; develop and embed theoretical skills, and build confidence in IPv6 as a technology |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The types of project chosen will depend on the current status of an organisation and are difficult to specify. However, some examples could include:<br>• **liaison with equipment vendors**, to determine when an IPv6-ready release will be available<br>• **participate in national technology trials and test-beds**, to provide knowledge and insight that will increase familiarity with IPv6 and inform the decision-making process during subsequent phases |
| *Stakeholders* | Network management team, procurement team, technical architects |
| *Dependencies* | The IPv6 awareness programme and the IPv6 skill-building programmes should be completed before starting this activity |

*Figure 6.11: Summary of IPv6 'quick win' activity for network providers [Source: Analysys Mason, Tech Mahindra]*

## 6.5 IPv6 adoption guide architecture and design phase

### 6.5.1 Network operators

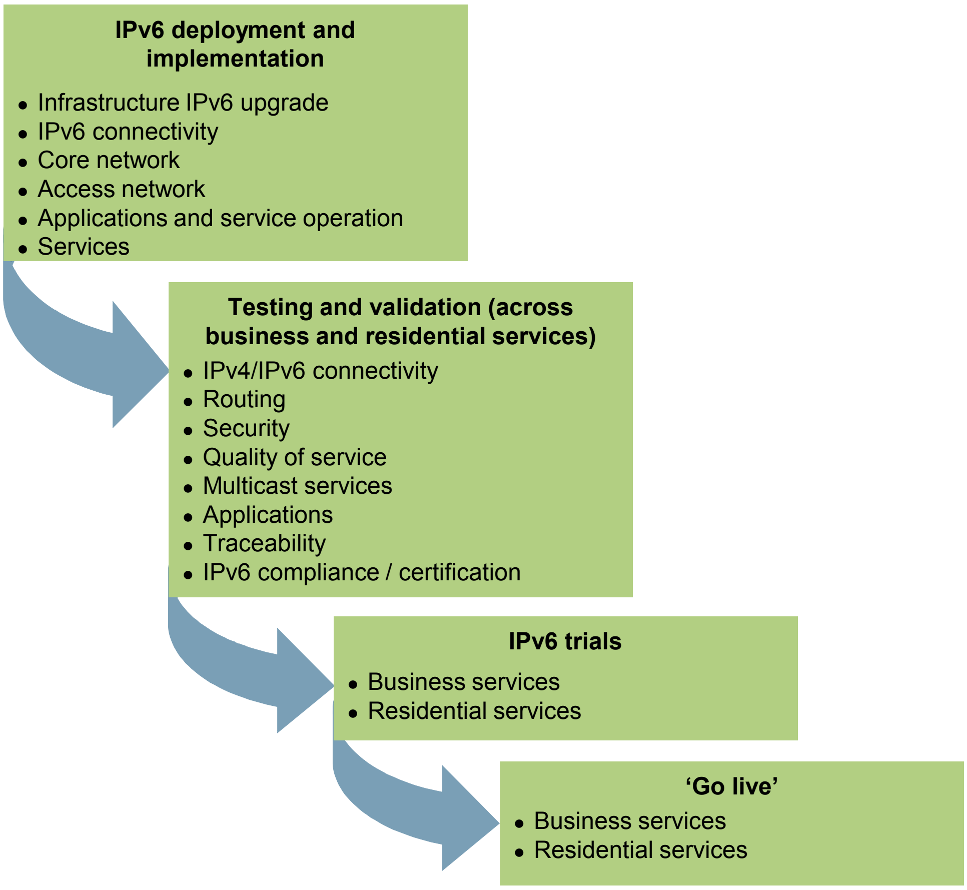
The architecture changes are unlikely to be substantial, as existing networks will generally be fully upgradable. However, network operators will need to consider the provision of interim solutions (e.g. tunnelling) if customers require IPv6 connectivity prior to the roll-out of full IPv6-enabled networks.

### 6.5.2 Mobile operators

The architecture changes needed to incorporate IPv6 into the core networks are largely determined by the standards body (3GPP), and despite a certain degree of variation between individual vendor solutions there should be no requirement for mobile operators to change vendors. IPv6-compatible handsets will all be standards based and there will no requirement for operators to take any action other than ensuring that the main handset manufacturers release compatible devices within the required timetable. Given the global nature of the handset market, this is not an issue that is specific to Singapore, but it will still be prudent for mobile operators to track developments.

## 6.6 IPv6 adoption guide: deployment phase

In this phase, the IPv6 adoption project plan developed during the planning phase and the solutions architected during the architecture and design phase are implemented, and IPv6 is enabled across the organisation. An overview of the activities involved in this phase is provided in Figure 6.12, and each area is discussed in further detail in the following sub-sections.



**IPv6 deployment and implementation**

- Infrastructure IPv6 upgrade
- IPv6 connectivity
- Core network
- Access network
- Applications and service operation
- Services

**Testing and validation (across business and residential services)**

- IPv4/IPv6 connectivity
- Routing
- Security
- Quality of service
- Multicast services
- Applications
- Traceability
- IPv6 compliance / certification

**IPv6 trials**

- Business services
- Residential services

**'Go live'**

- Business services
- Residential services

*Figure 6.12: Summary of deployment phase for network providers [Source: Analysys Mason, Tech Mahindra]*

### 6.6.1 IPv6 deployment and implementation

Once the architecture and designs for services, network and applications have been identified, the next step is to deploy these solutions to be able to launch IPv6 service offerings.

| *IPv6 deployment and implementation* | |
|---|---|
| *Overall aims* | Deploy IPv6 across the fixed and wireless networks to support the launch of IPv6 service offerings |
| *Approx. duration* | 12–24 months |
| *Key tasks* | IPv6 deployment and implementation will cover the following areas:<br>• **infrastructure IPv6 upgrade** of the hardware and software systems (if they are not IPv6 ready), or replacement with IPv6-compliant software<br>• **IPv6 connectivity** – IPv6 addresses are purchased and IPv6 connectivity is established with upstream providers and other peers<br>• **core network** – IPv6 is adopted across the core network, comprising the network, security, applications and service elements<br>• **access network** – the IPv6 network is adopted across the access network (that is, the network elements,  routing, security, applications, services, etc. are upgraded to IPv6)<br>• **applications and service operations** – the various applications, such as network management, monitoring, customer relationship management, etc. are IPv6 enabled<br>• **handsets (mobile only)** – IPv6-compatible handsets are sourced<br>• **fixed wireless terminals (fixed wireless access)** – source IPv6-compatible wireless terminals |
| *Stakeholders* | Technical architects, network engineering team, software engineering team, marketing & sales, procurement |
| *Dependencies* | The IPv6 service, network and application architecture need to be mostly completed before deployment and implementation can begin |

*Figure 6.13: Summary of IPv6 deployment and implementation activity for network providers [Source: Analysys Mason, Tech Mahindra]*

### *Infrastructure IPv6 upgrade*

Based on a comparison of the solution architecture and design (across networks, applications and services) and the findings of the IPv6 readiness assessment from the planning phase, network providers will generally be able to prepare a list of the infrastructure that will need to be upgraded for IPv6 to support the planned services and products. The process of upgrading this infrastructure should be initiated as a first step in the deployment of IPv6.

The survey of mobile operators revealed that they currently have IPv6-ready operating systems across their servers and desktop/laptop infrastructure, though these are not yet IPv6 enabled. For example, servers primarily run Windows 2003 or Unix variants, which are IPv6 ready via service pack upgrade, while laptops/desktops mainly run Windows XP SP2 or Windows 7, which are IPv6 ready. Corporate applications, such as web and email, have not yet been assessed for IPv6 readiness. One operator has OSS/BSS applications that are IPv6 ready, but not yet IPv6 enabled.

### 6.6.2 IPv6 test and validation

| *IPv6 test and validation* | |
|---|---|
| *Overall aims* | Validate IPv6 services across the network and applications of the network provider |
| *Approx. duration* | 3–4 months |
| *Key tasks* | IPv6 test and validation will cover the following areas of **business and residential** IPv6 products and services:<br>• **IPv4/IPv6 connectivity** is validated<br>• **IPv6 routing** – the network elements across IPv4 and IPv6 topologies are reachable through the appropriate IPv6 routing protocol<br>• **IPv6 security** – the security aspects of the network are validated<br>• **QoS** aspects are validated across the network<br>• **multicast services** as per the service design are validated across the network<br>• **applications** – the various applications are validated for their IPv6 support<br>• **traceability of traffic sessions** – the various IPv6 sessions established across the network are recorded for regulatory purposes, and the reliability of the system is validated<br>• **IPv6 compliance / certification (optional)** – the IPv6 services are tested against a range of certifications or compliance measurement programmes |
| *Stakeholders* | Technical architects, network engineering team, software engineering team |
| *Dependencies* | The IPv6 services solution roll-out should be completed before this activity commences |

*Figure 6.14: Summary of IPv6 test and validation activity for network providers [Source: Analysys Mason, Tech Mahindra]*

The test and validation activities help in assessing the reliability and performance of the various business and residential services. The various aspects which need to be tested and validated as part of the IPv6 adoption process are outlined below.

- **IPv4/IPv6 interconnectivity** – organisations should verify the ‘reachability’ of individual IPv6 networks through IPv4 networks in which IPv6 transition mechanisms are implemented. Similarly, the reachability of IPv4 networks through an IPv6 network should also be verified.
- **IPv6 routing** – organisations should verify the ability to navigate the IPv6 topology through the implemented IPv6 routing protocol. This includes verifying that the routing tables include all the IPv6 routes that are required to reach the various elements in the IPv6 topology.
- **IPv6 security** – organisations should verify and validate the IPv6 security implemented across the network by conducting vulnerability and penetration tests.
- **QoS** – organisations should verify the performance and reliability of the various classes of QoS that have been implemented, by injecting traffic and conducting stress tests.
- **Multicast –** organisations should validate the ability of various multicast services to distribute services in a seamless manner, by assessing service performance against pre-determined specifications.

### 6.6.3 IPv6 trials

| *IPv6 trials* | |
|---|---|
| *Overall aims* | IPv6 trials are conducted with a few trusted customers |
| *Approx. duration* | 3–4 months |
| *Key tasks* | IPv6 trials are conducted with customers, covering:<br>• **fixed network services** – international MPLS VPN services are validated for reliability and performance<br>• **mobile network services** – mobile data services are validated for reliability and performance |
| *Stakeholders* | Business teams, engineering management, account management, operations and support |
| *Dependencies* | IPv6 testing and validation should be completed before trials are held |

*Figure 6.15: Summary of IPv6 trials activity for network providers [Source: Analysys Mason, Tech Mahindra]*

After the network, applications and services have been IPv6 enabled and the solutions have been tested and validated, the next stage in the IPv6 adoption process of a network provider is to run a commercial IPv6 trial with a few customers. As part of the trials, all the services and systems affected must be validated for their conformance to functional and performance specifications.

### 6.6.4 IPv6 'go live'

| *IPv6 'go live'* | |
|---|---|
| *Overall aims* | IPv6 services are rolled out commercially |
| *Approx. duration* | 3–4 months |
| *Key tasks* | IPv6 services are made available commercially to customers, and rolled out on a large scale, including:<br>• **business services** – provision of current wholesale MPLS VPN services and managed network services to customers<br>• **residential services** – provision of broadband services to customers |
| *Stakeholders* | Business teams, engineering management, marketing operations |
| *Dependencies* | The IPv6 trials must be completed before IPv6 'go live' |

*Figure 6.16: Summary of IPv6 'go live' activity for network providers [Source: Analysys Mason, Tech Mahindra]*

After the service, network and application solutions to support the provision of IPv6 services and products have been deployed, and the network provider has conducted successful commercial trials, it can decide whether to launch commercial IPv6 services.

## 6.7 IPv6 adoption guide: ongoing support phase

In this phase, the focus is on providing service support for IPv6 products and services, monitoring take-up and, potentially, gradually switching off IPv4 services.

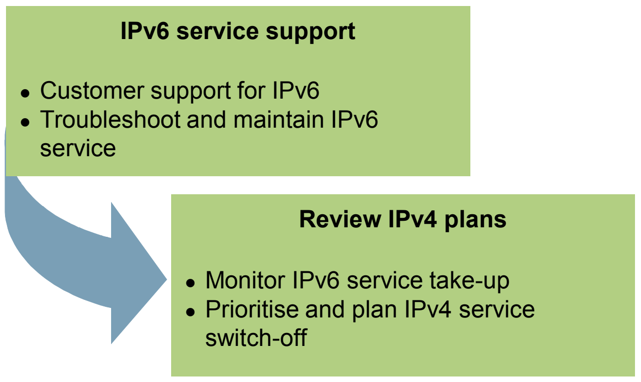

IPv6 service support
• Customer support for IPv6
• Troubleshoot and maintain IPv6 service
Review IPv4 plans
• Monitor IPv6 service take-up
• Prioritise and plan IPv4 service switch-off

*Figure 6.17: Summary of ongoing support phase for network providers [Source: Analysys Mason, Tech Mahindra]*

### 6.7.1 IPv6 service support

| *IPv6 service support* | |
|---|---|
| *Overall aims* | IPv6 customers are supported and service performance is stabilised |
| *Approx. duration* | Ongoing |
| *Key tasks* | The customer support system for IPv6 products and services must ensure that customers have a seamless service experience:<br>• **customer support** – the various trouble tickets raised for IPv6 will be analysed and the respective troubleshooting and maintenance team will ensure that the issue is resolved as soon as possible, and common/regular faults will be identified and addressed<br>• **troubleshoot and maintain IPv6 service** – the customer support team will work closely with the technical architects to fine tune the IPv6 system and help ensure that it is robust/stable |
| *Stakeholders* | Business teams, engineering management, marketing operations |
| *Dependencies* | IPv6 services are commercially available |

*Figure 6.18: Summary of IPv6 service support activity for network providers [Source: Analysys Mason, Tech Mahindra]*

Once IPv6 services have been launched on a commercial basis, the IPv6 networks, applications and services should be monitored for functional performance and adherence to the SLAs.

### 6.7.2 Review IPv4 plans

| *Review IPv4 plan* | |
|---|---|
| *Overall aims* | Review the IPv4 services and plan a phase-out approach |
| *Approx. duration* | Ongoing |
| *Key tasks* | After successfully rolling out commercial IPv6 services, the network provider will need to:<br>• **monitor IPv6 service take-up** to provide inputs to the product management team for the development of future IPv6 products and to identify IPv4 products that could be phased out<br>• **prioritise and plan IPv4 service switch-off**, including a timeline and a phased approach for ending IPv4 services |
| *Stakeholders* | Business teams, engineering management, marketing operations |
| *Dependencies* | IPv6 services are commercially available |

*Figure 6.19: Summary of IPv4 review plans for network providers [Source: Analysys Mason, Tech Mahindra]*

Following the introduction of IPv6 services, network providers need to consider the scope for retiring IPv4 products and services to reduce the operational requirements associated with maintaining and managing both an IPv4- and an IPv6-capable network. To inform this process, the network operator should monitor take-up of IPv6 services, and identify IPv4 products that could potentially be retired, and also identify new IPv6 products that could be launched.

# 7 IPv6 adoption guide: Service providers

For the purposes of this report, we have grouped three stakeholder categories with similar characteristics in respect of IPv6 requirements into one service provider category, namely data centre providers, ASP/web hosting providers and content providers:

- **Data centre operators** play an important role in the ICT ecosystem by hosting and supporting the back-end systems of various organisations across Singapore. As these organisations make progress towards adopting IPv6, the back-end systems hosted by data centre operators will also need to capable of adopting IPv6.
- **ASP/web hosting providers** play a significant role in the ICT ecosystem of Singapore, by providing shared services for the various organisations across the country, which help them to make cost savings and access 'best of breed' technology. ASP/web hosting providers will need to ensure that the services they offer end users support IPv6, either by confirming that proprietary applications support IPv6, or by working with vendors to source IPv6-enabled applications.
- **Content providers** also play an important role in the Internet ecosystem, as they create and provide the information which is accessed and exchanged across the Internet. Their role involves making the Internet useful and valuable to users through the continued creation of new applications and tools which have an impact on daily life (including entertainment, search engines, communication and collaboration tools, etc.).

Section 7.1 sets out a summary of the IPv6 adoption guide; Section 7.2 provides a summary of the survey results, and Section 7.3 provides a summary of the drivers and timelines for this stakeholder category to adopt IPv6. Sections 7.4 to 7.7 provide details for each phase of the adoption, including planning, architecture and design, deployment and support.

## 7.1 IPv6 adoption guide: overall summary

For the service provider community, the process of adopting IPv6 will require a phased approach spread across one to three years, depending on the complexity and IPv6 readiness of the existing environment.

As with the Internet service provider stakeholder group, the four main phases of IPv6 adoption are:

- **planning**: IPv6 awareness and skill building activities are undertaken, and the plans for IPv6 adoption are prepared. In addition, a few 'quick win' projects are identified to build confidence and understanding of IPv6
- **architecture and design:** the target and transition designs for the network, applications and services that will run on IPv6 are defined
- **deployment**: the IPv6 solution is deployed across the network, applications and services area, with quick win projects implemented at the start of the deployment phase
- **support**: IPv6 services are monitored for performance and reliability; a customer support system is put in place for the IPv6 services provided to customers, to ensure they have a seamless and smooth experience of IPv6 services.

Details of the four phases, and the activities involved in each, are illustrated in Figure 7.1. We provide details of the key activities within each phase in later sections of this adoption guide.

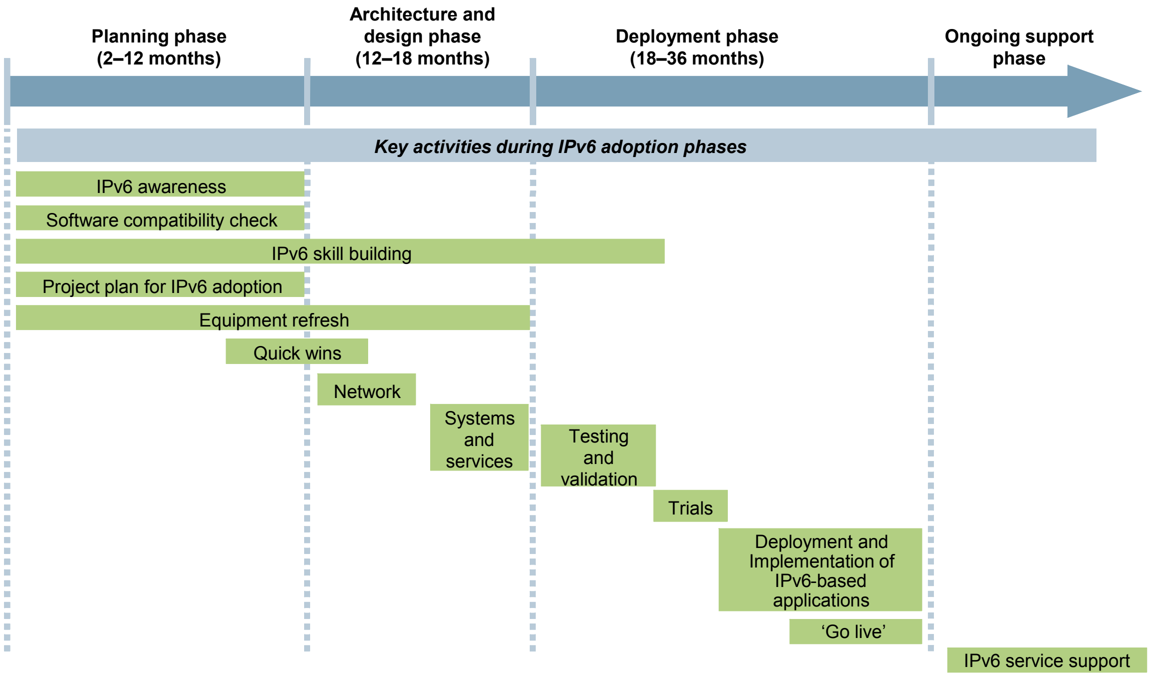

Planning phase (2–12 months)
Architecture and design phase (12–18 months)
Deployment phase (18–36 months)
Ongoing support phase
Key activities during IPv6 adoption phases
IPv6 awareness
Software compatibility check
IPv6 skill building
Project plan for IPv6 adoption
Equipment refresh
Quick wins
Network
Systems and services
Testing and validation
Trials
Deployment and Implementation of IPv6-based applications
'Go live'
IPv6 service support

*Figure 7.1: Activities involved in the four IPv6 adoption phases for service providers [Source: Analysys Mason, Tech Mahindra]*

## 7.2 Summary of findings from survey phase

The service provider category includes data centre operators, ASP/web hosting providers and content providers. Figure 7.2 to Figure 7.4 summarise the findings of the survey phase for each of these stakeholder groups.

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • Varied status ranging from initial stages of planning IPv6 adoption, to not yet started<br>• Varied status ranging from internal teams having been identified, to develop an IPv6 adoption plan to no teams identified | ○○○○ to ●○○○ |
| Networks | • No IPv6 readiness assessment undertaken<br>• Networks are running in an IPv4-only environment<br>• Low, or no, awareness of IPv6 network solutions | ○○○○ to ●○○○ |
| Applications | • No IPv6 readiness assessment undertaken | ○○○○ |
| Skills | • No IPv6 skills established | ○○○○ to ●○○○ |
| Services | • No IPv6 services available – no plan in place | ○○○○ |

*Figure 7.2: Summary of IPv6 readiness among data centre operators in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • Varied status – one has an IPv6 adoption project plan in place with dates, milestones and roadmap, while another is yet to start planning, but has identified high-level timelines<br>• Varied status – one has an IPv6 adoption architecture designed and in place, while another is yet to start<br>• Varied status – one has an IPv6 business strategy in place with IPv6 services/products to be launched and revenue projections planned<br>• Teams for IPv6 adoption identified – monitoring and tracking in place | ●●○○ to ●●●● |
| Networks | • Networks are IPv6 ready<br>• For one, some parts of the network across the world are IPv6 enabled, although not in Singapore | ●●○○ |
| Applications | • Varied status – one has assessed applications for IPv6 readiness, and solutions are currently being validated in the lab, while another is yet to conduct an assessment | ○○○○ to ●●○○ |
| Skills | • Varied status – one has advanced IPv6 solution architecture and design skills in place, while another has skills among some staff and is planning to implement a wider training programme | ●○○○ to ●●●○ |
| Services | • Varied status – one is planning the launch of IPv6 services towards the end of 2011, while another is planning to provide IPv6 support for SSL | ●○○○ to ●●○○ |

*Figure 7.3: Summary of IPv6 readiness among ASP/web hosting providers, July 2010 [Source: Analysys Mason, Tech Mahindra]*

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • Varied status – some content providers have project plans in place, while others have not yet started planning<br>• Varied status – some content providers have internal teams identified for IPv6 adoption, while others have not yet started identifying a team | ●○○○ to ●●●● |
| Networks | • Varied status – one content provider is experimenting with IPv6-enabled applications in the lab, while others have not yet assessed the IPv6 readiness of their network | ●○○○ to ●●○○ |
| Applications | • Varied status – one content provider has IPv6 enabled the applications, others have not yet assessed the IPv6 readiness of applications | ○○○○ to ●●○○ |
| Skills | • Varied status – some content providers have IPv6 skill development plans in place, while others are yet to plan | ○○○○ to ●●●○ |
| Services | • Varied status – one of the content providers has enabled a number of services for IPv6, one is experimenting with IPv6 services in the lab, and another has yet to plan them | ○○○○ to ●●●○ |

*Figure 7.4: Summary of IPv6 readiness among content providers in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

## 7.3 IPv4 exhaustion timelines and business impact

For the service provider community, the business impact of the predicted exhaustion of IPv4 address pool in August 2011 varies according to the services provided by each operator, and the nature of its customer base.

Data centre operators offering private suite-based facilities will be relatively unaffected, as the IP addressing of a customer's environment will be covered under the 'end user' stakeholder group, i.e. the IP address range in use is owned by the customer. Data centre operators offering co-location services are more likely to be affected, as the IP addresses of these systems will be the service provider's responsibility.

The impact on ASP/web hosting providers and content providers will mirror that of their end-user client organisations. Therefore, those that currently use IPv4 infrastructure and applications need to start planning for migration to IPv6, before internal forces or third parties necessitate the transition due to a critical shortage of IPv4 addresses.

The service provider's IPv6 strategy should ideally be based on its own unique business case, as well as a consideration of its network infrastructure. High on the list of considerations should be the inter-relationships with other infrastructure programmes, and the need to incorporate a transition plan into the overall IT budget. Service providers considering the transition should also be mindful of issues relating to security, interoperability and performance, as well as the true costs associated with developing detailed plans to address these issues.

Survey results showed that the majority of service providers are currently engaged in an ongoing technology refresh programme, which should ensure that all new hardware and software deployed between now and August 2011 will be IPv6 compliant.

Therefore, the challenge facing the service provider community is to ensure that existing systems (hardware, operating software and applications) will be IPv6 compliant by August 2011 (or before their own remaining pool of IPv4 addresses is exhausted). Figure 7.5 shows a high-level view of the typical timelines for the introduction of IPv6 services by a service provider.

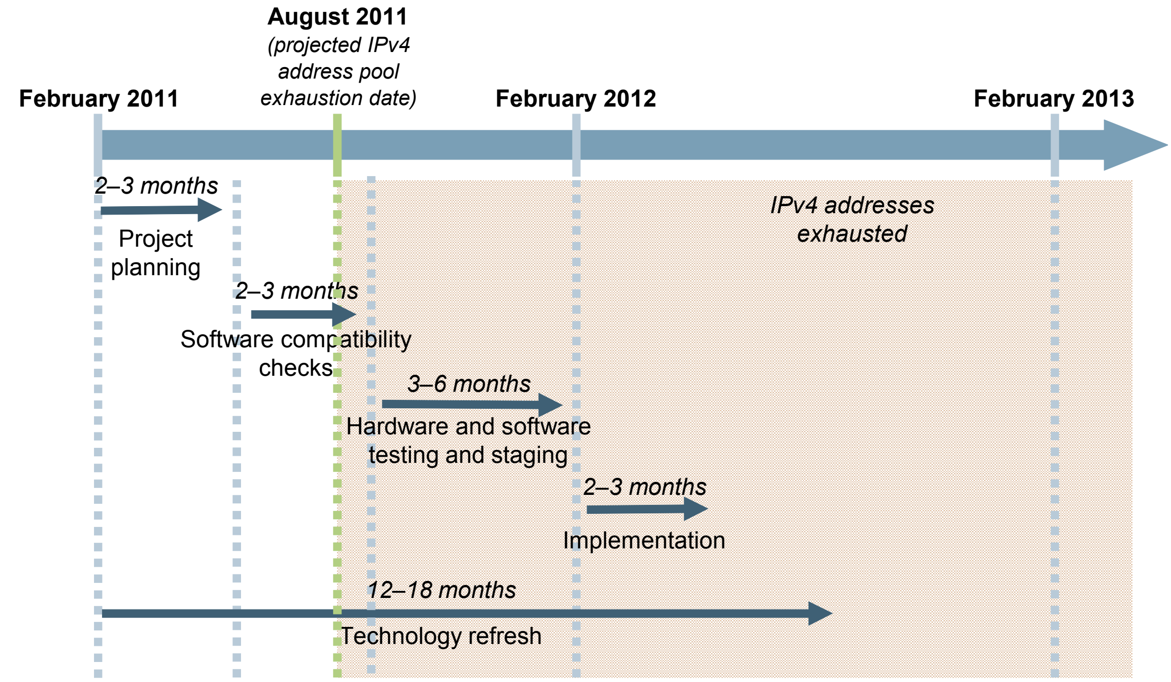
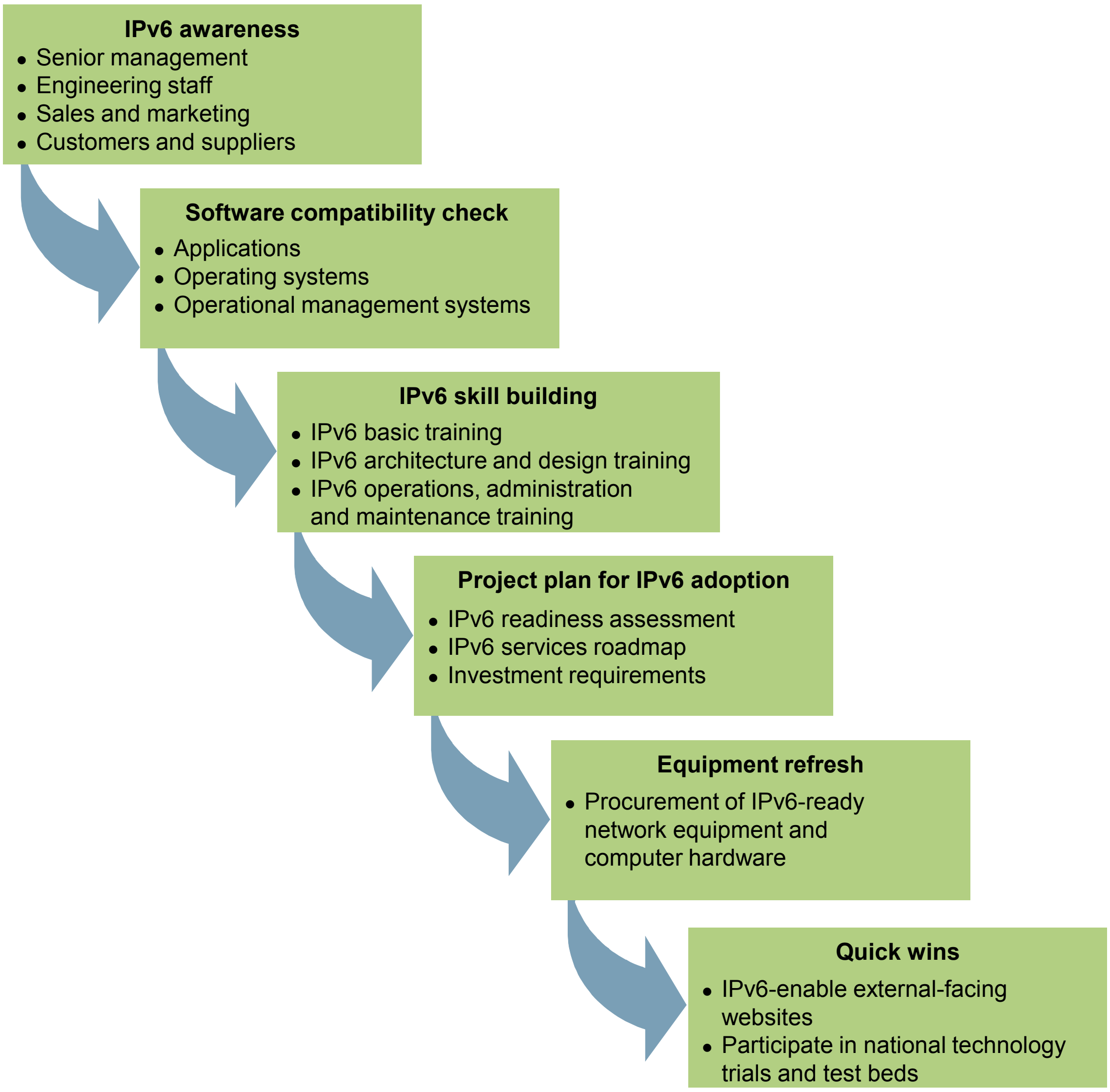


Figure 7.5: *IPv6 adoption timelines and impact on business for service providers [Source: Analysys Mason, Tech Mahindra]*

## 7.4 IPv6 adoption guide: planning phase

During this phase the service provider will draw up a detailed IPv6 adoption project plan and start to build awareness and skills within the organisation. As well as involving the development of a detailed project plan, this phase includes key activities, such as building IPv6 awareness across the organisation, conducting IPv6 readiness assessments across IT infrastructure, building IPv6 skills among staff, and implementing a few ‘quick win’ projects, such as ensuring that any new implementations are IPv6 compliant. The details of activities to be accomplished in this phase, and the associated timelines, are provided in the remainder of this section.



**IPv6 awareness**
- Senior management
- Engineering staff
- Sales and marketing
- Customers and suppliers

**Software compatibility check**
- Applications
- Operating systems
- Operational management systems

**IPv6 skill building**
- IPv6 basic training
- IPv6 architecture and design training
- IPv6 operations, administration and maintenance training

**Project plan for IPv6 adoption**
- IPv6 readiness assessment
- IPv6 services roadmap
- Investment requirements

**Equipment refresh**
- Procurement of IPv6-ready network equipment and computer hardware

**Quick wins**
- IPv6-enable external-facing websites
- Participate in national technology trials and test beds

*Figure 7.6: IPv6 planning phase activities for service providers [Source: Analysys Mason, Tech Mahindra]*

### 7.4.1 IPv6 awareness

An IPv6 awareness programme ensures that the importance of IPv6 adoption, the key areas of impact, the costs and the timelines are shared across the organisation.

A few key aspects to be considered when preparing to raise awareness of IPv6 in an organisation are shown in Figure 7.7.

| *IPv6 awareness* | |
|---|---|
| *Overall aims* | Raise IPv6 awareness across all key stakeholders associated with the organisation to educate them on the importance of IPv6 adoption, the scope of activities to be accomplished, and the likely timelines |
| *Approx. duration* | 1–2 months |
| *Key tasks* | The awareness programme must be targeted at multiple segments:<br>• **senior management and sales/marketing** – the following aspects must be covered:<br>– importance of IPv6, and the business impact of non-adoption<br>– timelines and the cost of IPv6 adoption<br>– various aspects of network, application and services that would be affected as a result of IPv6 adoption<br>– the set of activities to be initiated to design, implement and validate the IPv6 solutions and services<br>• **engineering staff** – the following must be covered:<br>– IPv6 technology basics<br>– the mechanisms for transition to IPv6<br>– guidelines for operating and maintaining IPv6-enabled networks and solutions<br>• **customers and suppliers** – the following must be covered:<br>– importance of IPv6, and the business impact of non-adoption<br>– timelines for IPv6 adoption<br>– various aspects of network, application and services that would be affected as a result of IPv6 adoption |
| *Stakeholders* | • Senior management, engineering management and staff, sales and marketing, training department, customers and suppliers |
| *Dependencies* | • No dependencies on other tasks |

*Figure 7.7: Summary of IPv6 awareness activity for service providers [Source: Analysys Mason, Tech Mahindra]*

### 7.4.2 IPv6 software compatibility check

A vital part of the IPv6 readiness programme from the service provider community's point of view will be to ensure that all legacy systems currently running on IPv4 are capable of being upgraded to IPv6. For the hardware components of systems this task is fairly straightforward, as compliance can be verified with a simple question to the equipment vendor or its local representative. The software environment is more complex, however, in that programming code often gets amended locally (due to bug fixes and/or modifications), meaning that there is a technical possibility that IP addresses have been hard-coded into some programmes.

The service provider should therefore check that all such changes have been documented, and that any references within software to IPv4 addresses can be changed to IPv6 equivalents.

| *IPv6 software compatibility check* | |
|---|---|
| *Overall aims* | • Carry out a comprehensive audit of the existing software environment in order to ascertain whether applications and system software is ready for the upgrade to IPv6<br>• Provide information software developers and suppliers to enable them to implement code changes needed as part of the IPv6 adoption programme |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 software compatibility check primarily involves operational staff, for example:<br>• **senior technical architects/IT management** – checks on the following areas must be covered:<br>– software components offered as part of a service to customers<br>– operating systems software<br>– data centre automation packages<br>– operational management systems<br>• **IT development staff** – the following areas must be covered:<br>– application programming interfaces<br>– operating system calls<br>– network management protocol calls<br>– system management routines |
| *Stakeholders* | IT management, senior technical architects, IT staff |
| *Dependencies* | The IPv6 software compatibility check shall be carried out as early as possible in the upgrade process in order to allow time for corrective action to be taken, if required |

*Figure 7.8: Software compatibility check for service providers [Source: Analysys Mason]*

### 7.4.3 IPv6 skill building

IPv6 skill building ensures that all stakeholders across the organisation have the required skills to contribute to, and participate in, the IPv6 adoption process, including implementation.

| *IPv6 skill building* | |
|---|---|
| *Overall aims* | • Ensure that IPv6 skills are built across the various levels of the organisation (IT management, IT staff, etc.), so that they can participate in, and contribute to, the IPv6 adoption process<br>• Provide skills to the IT department to enable them to implement the IPv6 adoption programme |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 skill building programme encompasses various layers of the organisation:<br>• **senior technical architects/IT management** – skills in the following areas must be covered:<br>– IPv6 solution architecture and design<br>– IPv6 migration planning and processes<br>– IPv6 service design<br>• **IT staff** – the following areas must be covered:<br>– IPv6 technology basics<br>– the mechanisms for transition to IPv6<br>– operating and maintaining IPv6-enabled networks and solutions |
| *Stakeholders* | HR, training department, IT management, senior technical architects, IT staff |
| *Dependencies* | The IPv6 awareness activity should have been completed before the IPv6 skill building activity begins, although it can be started in advance of full completion of the IPv6 awareness activity |

*Figure 7.9: Summary of IPv6 skill building activity for service providers [Source: Analysys Mason, Tech Mahindra]*

### 7.4.4 Project plan for IPv6 adoption

The project plan for IPv6 adoption sets out the detailed set of activities to be carried out, spanning IPv6 solution architecture, design, deployment, trials and ‘go live’. During the process of developing a detailed project plan, the service provider must also carry out an IPv6 readiness assessment across network and applications. This assessment will highlight gaps between the current status and the eventual target of providing seamless IPv6 services, information that will serve as inputs to the detailed project plan (see Figure 7.10).

| *Project plan for IPv6 adoption* | |
|---|---|
| *Overall aims* | • Establish the current status of IPv6 adoption across the organisation's network, applications and services<br>• Draw up a detailed project plan, including the various activities to be completed for IPv6 adoption and a roadmap to ensure provision of seamless IPv6 services |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The key tasks in preparing the IPv6 adoption project plan are:<br>• establish an IPv6 workgroup team, made up of internal and / or external IPv6 experts, to have responsibility for preparing the project plan for IPv6 adoption<br>• conduct an IPv6 readiness assessment to identify the gaps in IPv6 adoption across network, applications and services<br>• map the current status of IPv6 adoption<br>• draw up a detailed project plan for IPv6 adoption<br>The IPv6 readiness assessment mentioned above needs to cover the following areas:<br>• **network infrastructure** – routers, switches, security devices, DNS, DHCP, NTP, addressing delegation mechanisms, etc., spread across the core network, broadband network, mobile network, etc.<br>• **application infrastructure** – network management, OSS/BSS, human resources (HR), enterprise resource planning (ERP) applications, etc.<br>• **core business applications infrastructure** – the existing and planned business applications and the status of their IPv6 enablement<br>The project plan for IPv6 adoption will detail the set of activities that must be completed in order to IPv6 enable the network, applications and services. The plan must cover the following areas:<br>• architecture and design<br>• deployment and implementation<br>• test and validation<br>• trials<br>• 'go live' for IPv6 services |
| *Stakeholders* | • **IPv6 work group team** – a team of internal and/or external IPv6 experts responsible for preparing the project plan for IPv6 adoption. Depending on the organisation, this team may have further responsibility for execution of the project plan itself<br>• **IT management** – will help to provide all the inputs required for the readiness assessment, and will also identify key individuals within the business for this activity |
| *Dependencies* | • The IPv6 awareness programme needs to be completed before the IPv6 readiness programme can begin, to ensure that stakeholders understand the importance of the readiness assessment, and are willing to participate fully in it<br>• The IPv6 business requirements plan needs to be prepared, to identify which services will need to be supported by IPv6 |

*Figure 7.10: Summary of project planning for IPv6 adoption activity for service providers [Source: Analysys Mason, Tech Mahindra]*

### 7.4.5 Equipment refresh

During the survey phase, stakeholders from the service provider community indicated that, as part of a continuous hardware refresh programme, technical components within their infrastructure are replaced at regular intervals. As part of this process, it is good business practice to ensure that all hardware components requiring access to an IP addresses are procured as IPv6 compliant (or capable of running dual protocol stacks) as part of the requirements specification.

| *Equipment refresh* | |
|---|---|
| *Overall aims* | • Ensure that IPv6 compatibility is guaranteed within all hardware procured by the organisation<br>• Include IPv6 in all requirements specifications for new hardware |
| *Approx. duration* | Ongoing |
| *Key tasks* | The IPv6 skill building programme encompasses various layers of the organisation:<br>• **senior technical architects/IT management** – skills in the following areas must be covered:<br>– ensure that IPv6 compatibility is included within all technical specifications<br>• **procurement staff** – the following areas must be covered:<br>– ensure that IPv6 compatibility is drafted in to all supply contracts for computer hardware |
| *Stakeholders* | IT management, senior technical architects, IT staff, procurement department |
| *Dependencies* | None |

*Figure 7.11: Equipment refresh for service providers [Source: Analysys Mason]*

### 7.4.6 Quick wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organisation, and in giving IT staff the opportunity to use the theoretical skills they have gained earlier in the process, as well as to build confidence in the technology. Figure 7.12 summarises this activity, and provides a couple of examples of ‘quick win’ initiatives.

| *IPv6 quick wins* | |
|---|---|
| *Overall aims* | • Identify and implement initial ‘quick win’ projects<br>• Strengthen the IPv6 thought process across the organisation; develop and embed theoretical skills, and build confidence in IPv6 as a technology |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The types of project chosen will depend on the current status of an organisation, and are difficult to specify. However, some examples could include:<br>• **IPv6 enable the external-facing websites**, to help the organisation position itself as an IPv6 leader, and also further establish IPv6 as an internal initiative<br>• **IPv6 enable any newly launched customer services**, again, to help the organisation position itself as an IPv6 leader<br>• **participate in national technology trials and test-beds**, which would provide knowledge and insight that will increase familiarity with IPv6 and inform the decision-making process during subsequent phases |
| *Stakeholders* | Corporate IT management team, procurement team, technical architects |
| *Dependencies* | The IPv6 awareness programme and the IPv6 skill-building programmes should be well advanced before starting this activity |

*Figure 7.12: Summary of IPv6 ‘quick win’ activity for service providers [Source: Analysys Mason, Tech Mahindra]*

## 7.5 IPv6 adoption guide: architecture and design phase

This phase of the adoption involves transition designs for the network, applications and services to allow IPv4 and IPv6 to co-exist and work simultaneously during the transition to IPv6, and to support the introduction of new IPv6 services.

The IPv6 solution architecture and design phase needs to cover the areas outlined below.

- **Network** – architecting and designing the various network solutions to support the planned IPv6 services, including the IPv4 run-out scenario and transition to a complete IPv6-only ecosystem.

- **Systems and services** – prioritising the various IPv4-based services that are planned to be IPv6 enabled, and finalising the new business applications to be introduced, based on initial work carried out during the planning phase. This prioritisation helps in building the network and systems architecture and designs.

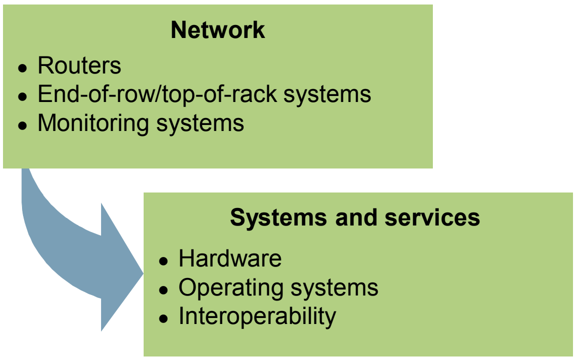


*Figure 7.13: IPv6 architecture and design activities for service providers [Analysys Mason, Tech Mahindra]*

The remainder of this section summarises the key activities in each of these areas, with annexes providing supporting technical details.

### 7.5.1 Architecture and design – networks

Once the architecture and design for the IPv6 services are finalised, a network solution architecture and design that are aligned with core business applications will have to be prepared.

The network solution architecture will need to consider the various stages through which the organisation's network will pass (e.g. IPv4-only, support for both IPv4 and IPv6, and IPv6-only). Based on the current status of IPv6 readiness and IPv4 address availability, the architecture should consider a back-up solution for a scenario where the organisation has run out of IPv4 addresses, but has not yet fully adopted IPv6.

| *IPv6 network solution architecture and design* | |
|---|---|
| *Overall aims* | Prepare an IPv6 network solution architecture and design which will help to enable IPv6 on the current IPv4-based services and introduce new IPv6 services |
| *Approx. duration* | 1–6 months |
| *Key tasks* | Ensure that the IPv6 network solution architecture and design – of both core and access networks – covers the following areas:<br>• **IPv4/IPv6 interconnectivity** – individual IPv4 and IPv6 networks are connected via various tunnelling mechanisms, dual stack, etc.<br>• **IPv6 routing** – the reachability of the network elements across IPv4 and IPv6 topologies must be ensured, through appropriate deployment of the IPv6 routing protocol<br>• **IPv6 security** – the various network solutions that are designed must ensure that the security aspects of the planned network roll-out are considered and in place<br>• **quality of service (QoS)** – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance<br>• **multicast services** – the various multicast services across the IPv6 network must be designed in accordance with the planned services<br>• **traceability of traffic sessions** – if required for regulatory purposes, recording of the various IPv6 sessions taking place across the network should be incorporated<br>• **data centre specific components** – such as top of rack (TOR) and end of row (EOR) switches |
| *Stakeholders* | Technical architects, IT management, IT staff |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can begin, and the architecture and design for services needs to be completed, or almost complete |

*Figure 7.14: Summary of IPv6 network solution architecture and design activity for service providers [Source: Analysys Mason, Tech Mahindra]*

### 7.5.2 Architecture and design – systems and services

For the service provider community, it is vital that the predicted exhaustion of the IPv4 address range in August 2011 does not lead to loss or degradation of service offered to customers. The outputs of the software compatibility check will have highlighted the changes required to any legacy systems to ensure IPv6 compliance, and any changes that are required should be made at this stage.

The key tasks are highlighted in Figure 7.15.

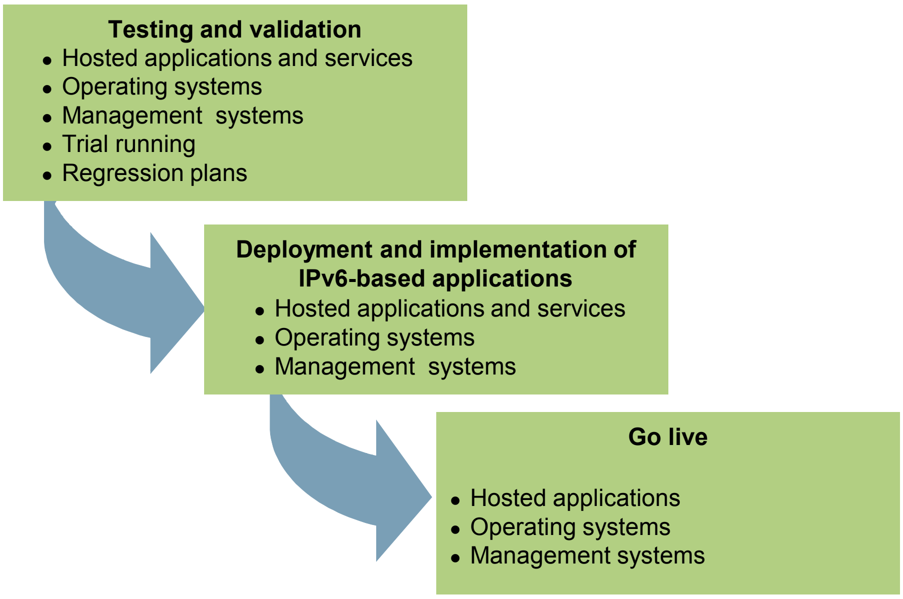
| *IPv6 application solution architecture and design* | |
|---|---|
| *Overall aims* | Prepare an IPv6 application solution architecture and design, which will help enable IPv6 on the current IPv4-based services and introduce new IPv6 services |
| *Approx. duration* | 1– 6 months |
| *Key tasks* | The IPv6 application solution architecture and design needs to cover the following areas:<br>• ensure **applications, such as ERP and CRM systems,** are able to support IPv6- and IPv4-based connectivity and services<br>• **ensure proprietary applications** are able to support both IPv6- and IPv4-based connectivity services<br>• ensure **network management and monitoring applications/solutions** are seamlessly able to support and monitor IPv4 and IPv6 networks |
| *Stakeholders* | Technical architects, IT staff, vendors |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can be initiated, and the architecture and design for services needs to be completed, while the architecture and design for networks can be prepared in parallel |

*Figure 7.15: Summary of IPv6 application solution architecture and design activity for service providers [Source: Analysys Mason, Tech Mahindra]*

The IPv6 software compatibility check conducted in the planning phase will provide a list of IPv6-compliant and non-compliant applications. Applications that are found to be non-IPv6 compliant will need either to be upgraded to an IPv6-compliant version, or replaced with new software that provides the same functionality and is also IPv6 compliant.

## 7.6 IPv6 adoption guide: deployment phase

In this phase, the IPv6 adoption project plan developed during the planning phase, and the solutions architected during the architecture and design phase are implemented, and IPv6 is enabled across the organisation. An overview of the activities involved in this phase is provided in Figure 7.16, and the activities are discussed in greater depth in the rest of this section.



**Testing and validation**

- Hosted applications and services
- Operating systems
- Management systems
- Trial running
- Regression plans

**Deployment and implementation of IPv6-based applications**

- Hosted applications and services
- Operating systems
- Management systems

**Go live**

- Hosted applications
- Operating systems
- Management systems

*Figure 7.16:* *Summary of deployment phase for service providers [Source: Analysys Mason, Tech Mahindra]*

### 7.6.1 IPv6 test and validation

| *IPv6 test and validation* | |
|---|---|
| *Overall aims* | Validate IPv6 services (network and applications) |
| *Approx. duration* | 3–6 months |
| *Key tasks* | IPv6 test and validation will cover the following areas of IPv6 products and services:<br>• **IPv4/IPv6 connectivity** will be validated<br>• **IPv6 routing** the network elements across IPv4 and IPv6 topologies will be reachable through the appropriate IPv6 routing protocol<br>• **IPv6 security** – the security aspects of the network will be validated<br>• **QoS** aspects will be validated across the network<br>• **multicast services** as per the service design will be validated across the network<br>• **applications** – the various applications will be validated for their IPv6 support<br>• **traceability of traffic sessions** – the various IPv6 sessions taking place across the network will be recorded for regulatory purposes, and the reliability of the system will be validated<br>• **IPv6 compliance / certification (optional)** – the IPv6 services are tested against a range of certifications or compliance measurement programmes |
| *Stakeholders* | Technical architects and IT staff |
| *Dependencies* | The IPv6 services solution roll-out should be completed |

*Figure 7.17:* *Summary of IPv6 test and validation activity for service providers [Source: Analysys Mason, Tech Mahindra]*

### 7.6.2 IPv6 trials

| *IPv6 trials* | |
|---|---|
| *Overall aims* | IPv6 trials are conducted within the organisation in conjunction with customers |
| *Approx. duration* | 3–4 months |
| *Key tasks* | IPv6 trials are conducted within the organisation, covering **hosted applications and internal IT services** |
| *Stakeholders* | Customers, IT staff, account management, operations and support |
| *Dependencies* | IPv6 testing and validation should be completed before trials begin |

*Figure 7.18: Summary of IPv6 trials activity for service providers [Source: Analysys Mason, Tech Mahindra]*

After the network and applications have been IPv6 enabled, and the solutions have been tested and validated, the next stage in the IPv6 adoption process is to run a number of IPv6 trials both across internal and external networks. As part of the trials, the applications will be validated for their conformance to functional specifications and SLAs.

### 7.6.3 IPv6 deployment and implementation

Once the architecture and designs for services, network and applications have been tested and trial runs are complete, the next step is to launch IPv6 services.

| *IPv6 deployment and implementation* | |
|---|---|
| *Overall aims* | Deploy IPv6 across the network and applications to support the launch of IPv6 services |
| *Approx. duration* | 3 months |
| *Key tasks* | The IPv6 deployment and implementation will cover the following areas:<br>• **infrastructure IPv6 upgrade** of the hardware and firmware systems (if they are not IPv6 ready), or replacement with IPv6-compliant firmware<br>• **IPv6 connectivity** – IPv6 addresses are purchased and IPv6 connectivity with upstream providers and other peers is established<br>• **applications and service operations** – the various applications, such as network management, monitoring, customer relationship management, etc. are IPv6 enabled<br>• **services** – the various services spread across the organisations are IPv6 enabled |
| *Stakeholders* | Technical architects and IT staff |
| *Dependencies* | The IPv6 service, network and application architecture need to be mostly completed before deployment and implementation can begin |

*Figure 7.19: Summary of IPv6 deployment and implementation activity for service providers [Source: Analysys Mason, Tech Mahindra]*

### 7.6.4 IPv6 'go live'

| *IPv6 'go live'* | |
|---|---|
| *Overall aims* | IPv6 services are rolled out across the organisation and to the customer base |
| *Approx. duration* | 1 month |
| *Key tasks* | IPv6 services are made available and rolled out internally and externally |
| *Stakeholders* | Business teams and IT staff |
| *Dependencies* | The IPv6 trials must be completed before IPv6 'go live' |

*Figure 7.20: Summary of IPv6 'go live' activity for service providers [Source: Analysys Mason, Tech Mahindra]*

After the service, network and application solutions to support the provision of IPv6 applications and services have been deployed, and the customer has conducted successful trials, the service provider can decide whether to launch the IPv6 application and services internally and externally.

## 7.7 IPv6 adoption guide: ongoing support phase

Prior to launch of live services, it is essential that adequate support mechanisms are in place, including the following:

- **Technical support** – first- through to third-line support via a help desk
- **Specialist support** – access to support from external organisations that have supplied hardware and applications.

# 8 IPv6 adoption guide: End users

End users are the category that will use, or will require provisioning of, IPv6 from service providers for systems and applications needed to support corporate activities. This category includes multinational companies (MNCs) and small and medium enterprises (SMEs).

MNCs have a significant footprint in Singapore, where regional or global headquarters connect to businesses across different nations and geographies. IPv6 enablement of this segment will ensure that MNCs based in Singapore are well placed to benefit from business opportunities based on the next generation of Internet technologies.

SMEs in Singapore that use the Internet Protocol (IP) in some capacity will need to be mindful of the exhaustion of IPv4. The characteristics of organisations in this sector vary substantially, and so there is no single approach to deploying IPv6 that will suit all SMEs.

Section 8.1 sets out a summary of the IPv6 adoption guide, Section 8.2 provides a summary of the survey results, and Section 8.3 provides a summary of the drivers and timelines for this stakeholder category to adopt IPv6. Sections 8.4 to 8.7 provide details for each phase of the adoption, including planning, architecture and design, deployment and support.

## 8.1 IPv6 adoption guide: overall summary

For end users, the process of adopting IPv6 will vary depending on the type of end user. MNCs are likely to take early measures to avoid the risk of regional IPv4 address shortages. In contrast, national companies, i.e. local Singapore-based companies and SMEs, will migrate on an ‘as needed’ basis. The four main phases of IPv6 adoption are:

- **planning**: IPv6 awareness and skill building activities are undertaken and the plans for IPv6 adoption are prepared. In addition, a few ‘quick win’ projects are identified to build confidence and understanding of IPv6
- **architecture and design:** the target and transition designs for the network, applications and services that will run on IPv6 are defined
- **deployment**: the IPv6 solution is deployed across the network, applications and services area, with ‘quick win’ projects implemented at the start of the deployment phase
- **support**: IPv6 services are monitored for performance and reliability, and a customer support system is put in place for the IPv6 services provided to customers, to ensure they have a seamless and smooth experience of IPv6 services.

Details of the four phases and the activities involved in each are illustrated in Figure 8.1. We then provide details of the key activities within each phase in later sections of this adoption guide.

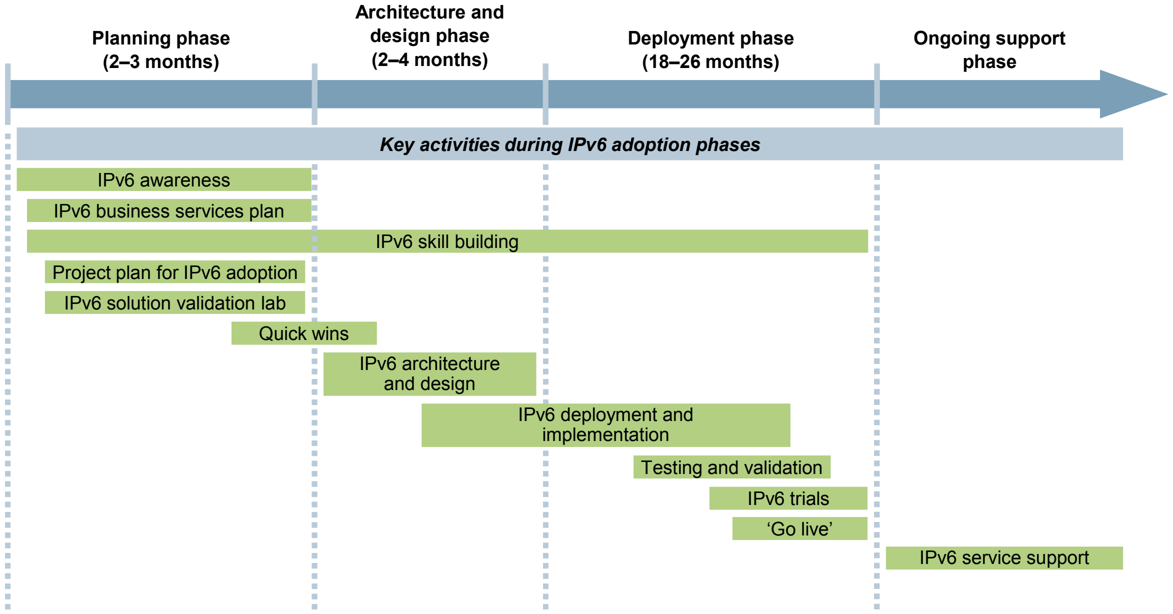

Planning phase (2–3 months)
Architecture and design phase (2–4 months)
Deployment phase (18–26 months)
Ongoing support phase
Key activities during IPv6 adoption phases
IPv6 awareness
IPv6 business services plan
IPv6 skill building
Project plan for IPv6 adoption
IPv6 solution validation lab
Quick wins
IPv6 architecture and design
IPv6 deployment and implementation
Testing and validation
IPv6 trials
'Go live'
IPv6 service support

*Figure 8.1: Activities involved in the four IPv6 adoption phases for end users [Source: Analysys Mason]*

## 8.2 Summary of survey findings

The end-user category includes MNCs and SMEs. Survey findings for MNCs are included in Figure 8.2.

| *Area* | *Summary of current status* | *Stage* |
|---|---|---|
| Planning | • One MNC has high-level plans for IPv6 adoption by 2014; others have no IPv6 adoption plans in place<br>• No business driver identified for IPv6 adoption | ○○○○ to<br>●●○○ |
| Networks | • No IPv6 readiness assessment undertaken<br>• Networks are running in an IPv4-only environment<br>• Low, or no, awareness of IPv6 network solutions | ○○○○ to<br>●○○○ |
| Applications | • No IPv6 readiness assessment undertaken | ○○○○ |
| Skills | • No IPv6 skills developed | ○○○○ to<br>●○○○ |

*Figure 8.2: Summary of IPv6 readiness among multinational companies in Singapore, July 2010 [Source: Analysys Mason, Tech Mahindra]*

SMEs were surveyed using a web-based survey, rather than face-to-face interviews. In general, the web-based survey showed that a relatively small number of SMEs are aware of IPv6 as a successor to IPv4 and the upcoming exhaustion of IPv4 addresses. Findings from the survey also demonstrated that there is a lack of understanding of the benefits and capabilities of IPv6. Also, very few had a clear knowledge as to their organisation's plans towards the adoption of IPv6, with the findings suggesting that very little is known with regards to the resource (personnel and cost) and timelines required for IPv6 adoption. IT infrastructure readiness has largely not been assessed by the majority of the organisations that participated in the survey.

## 8.3 IPv4 exhaustion timelines and business impact

As the exhaustion of the IPv4 address pool approaches, end users should be aware of the impact this could potentially have on their business. This change will affect all end users from MNCs through to SMEs. Organisations that currently use IPv4 infrastructure and applications need to start planning for migration to IPv6 now, before internal forces or third parties necessitate the transition due to a critical shortage of IPv4 addresses.

An end user's IPv6 strategy should ideally be based on its own unique business case, as well as a consideration of its network infrastructure. High on the list of considerations should be the inter-relationships with other infrastructure programmes and the need to incorporate a transition plan into the overall IT budget. End users considering the transition should also be mindful of issues relating to security, interoperability and performance, as well as the true costs associated with developing detailed plans to address these issues.

Figure 8.3 shows a high-level view of the typical timelines for the migration to IPv6 services for end users.

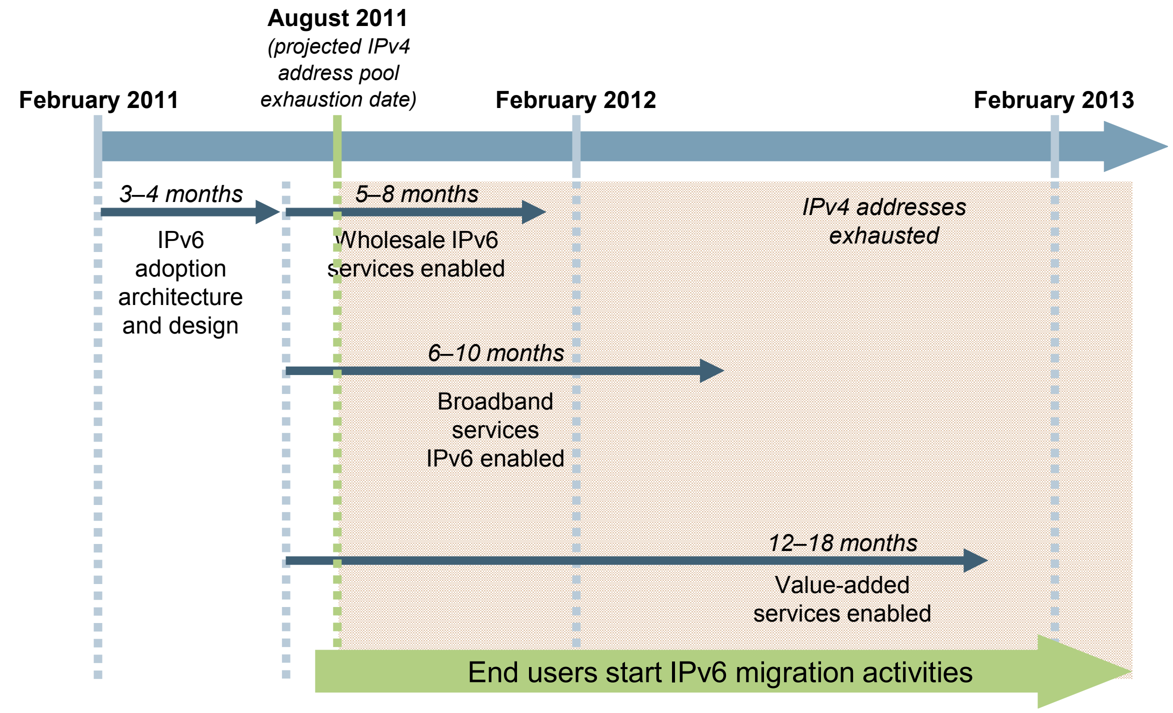

August 2011
(projected IPv4 address pool exhaustion date)
February 2011
February 2012
February 2013
3–4 months
IPv6 adoption architecture and design
5–8 months
Wholesale IPv6 services enabled
IPv4 addresses exhausted
6–10 months
Broadband services IPv6 enabled
12–18 months
Value-added services enabled
End users start IPv6 migration activities

*Figure 8.3: IPv6 adoption timelines and impact on business for end users [Source: Analysys Mason, Tech Mahindra]*

For end users, there are a number of consequences of non-readiness for IPv6 once IPv4 address allocations are exhausted.

- Businesses across the ecosystem in Singapore that do not have significant remaining IPv4 address pools, or are dependent on Internet service providers for IPv4 addresses, will be unable to obtain new IP addresses to support business expansion.
- Similarly, new enterprises will be unable to obtain a broadband connection, or develop services requiring a public IP address (websites etc.).
- There may also be an impact on the core business applications of organisations, which would thus affect business procedures, processes and practices.
- All of these factors could potentially have a direct negative impact on Singapore’s GDP by impeding business growth.

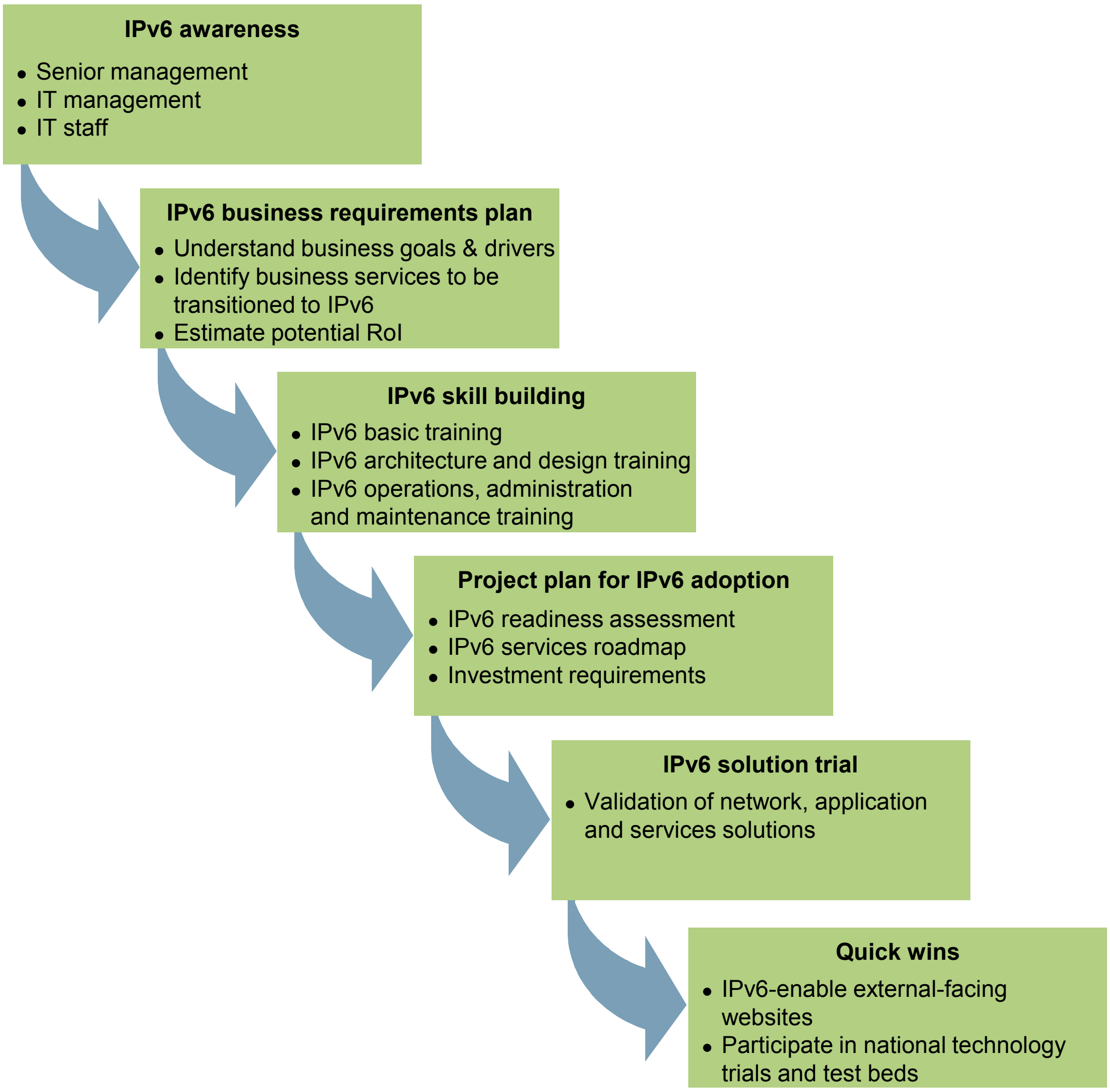
| *Category of end user* | *Expected timing of IPv6 adoption* | *Driver* |
|---|---|---|
| • MNC<br>• National<br>• SME | • Early<br>• Medium<br>• Medium/late | MNCs are likely to experience regional address shortages, and so may have an incentive to take early measures. With national companies and SMEs, migration will occur on more of an 'as needed' basis |

*Figure 8.4: Relative timing of IPv6 adoption across categories of end user [Source: Analysys Mason, Tech Mahindra]*

## 8.4 IPv6 adoption guide: planning phase

During this phase, an end user should draw up a detailed IPv6 adoption project plan and start building awareness within the organisation. This phase should also include key activities, such as determining core business applications, developing an IPv6 business plan, conducting an IPv6 readiness audit across the organisation's IT infrastructure, building IPv6 skills among staff and implementing a few 'quick win' projects, such as participating in national technology trials and test-beds. These activities are explored further in the sections below.

The duration and resources required to undertake each activity will clearly vary considerably between a small SME and large MNC. The range of estimates for the duration of tasks provided in the following sections reflects differences in the scale of activities.



**IPv6 awareness**

- Senior management
- IT management
- IT staff

**IPv6 business requirements plan**

- Understand business goals & drivers
- Identify business services to be transitioned to IPv6
- Estimate potential RoI

**IPv6 skill building**

- IPv6 basic training
- IPv6 architecture and design training
- IPv6 operations, administration and maintenance training

**Project plan for IPv6 adoption**

- IPv6 readiness assessment
- IPv6 services roadmap
- Investment requirements

**IPv6 solution trial**

- Validation of network, application and services solutions

**Quick wins**

- IPv6-enable external-facing websites
- Participate in national technology trials and test beds

*Figure 8.5: IPv6 planning phase activities for end users [Source: Analysys Mason, Tech Mahindra]*

### 8.4.1 IPv6 awareness

It is beneficial to raise awareness of IPv6 within the organisation, to ensure that the importance of IPv6 adoption, the key areas of impact, the costs and the timelines are shared across the organisation. A few key aspects to be considered when preparing to raise awareness of IPv6 in an organisation are shown in Figure 8.6.

| *IPv6 awareness* | |
|---|---|
| *Overall aims* | Raise IPv6 awareness across all key stakeholders within the organisation to educate them on the importance of IPv6 adoption, the scope of activities to be accomplished, and the likely timelines |
| *Approx. duration* | 0.5–2 months |
| *Key tasks* | The awareness programme must be targeted at multiple segments:<br>• **senior management** – the following aspects must be covered:<br>– importance of IPv6, and the business impact of non-adoption<br>– timelines and the cost of IPv6 adoption<br>• **IT management** – the following aspects must be covered:<br>– various aspects of network, application and services that would be affected as a result of IPv6 adoption<br>– the set of activities to be initiated for the design, implementation and validation of the IPv6 solutions and services<br>• **IT staff** – the following must be covered:<br>– IPv6 technology basics<br>– the mechanisms for transition to IPv6<br>– guidelines for operating and maintaining IPv6-enabled networks and solutions |
| *Stakeholders* | • Senior management, IT management, training department |
| *Dependencies* | • No dependencies on other tasks |

*Figure 8.6: Summary of IPv6 awareness activity for end users [Source: Analysys Mason, Tech Mahindra]*

### 8.4.2 IPv6 business requirements plan

It is important for the end user to assess its organisation's strategy and business requirements, as this will enable it to understand the impact of IPv6 on the business, and whether it will affect productivity and communications. It is prudent to create an IPv6 business requirements plan which identifies the services or core business applications that need to be supported by IPv6. This provides an essential input to the later activities within the planning phase, and ensures that the high-priority/high-impact services remain the focus for IPv6 adoption.

A few key aspects to be considered when preparing an IPv6 business requirements plan are shown in Figure 8.7; further details specific to end users are provided in the rest of this sub-section.

| *IPv6 business requirements plan* | |
|---|---|
| *Overall aims* | Identify business roadmap, covering business goals and drivers, identifying which core business applications will need to be delivered using IPv6 and the return-on-investment implications |
| *Approx. duration* | 0.5–3 months |
| *Key tasks* | The IPv6 business requirements plan needs to:<br>• **identify business strategy, goals and drivers** that are linked to IPv6 adoption<br>• **identify core business applications** that will require IPv6 support, in line with the business goals and drivers<br>• **estimate the return on investment** (either in terms of incremental revenue or cost savings compared to the case without IPv6) |
| *Stakeholders* | • Senior management, IT management |
| *Dependencies* | • The IPv6 awareness programme needs to be underway before the IPv6 business requirements plan can begin |

*Figure 8.7: Summary of IPv6 business requirements plan for end users [Source: Analysys Mason, Tech Mahindra]*

### *Business goals and drivers*

In general, the typical business goals of end-user organisations are to:

- improve their operating efficiency
- ensure business continuity and risk management
- ensure the long-term health and overall success of the business, and its financial strength
- generate profitable revenue growth
- grow and expand the business.

Currently, **MNCs** do not see any business need for IPv6 adoption, and have not engaged in any activities associated with IPv6 adoption. The business driver that would lead them to IPv6 adoption is business continuity and the need to manage the risk of IPv4 address exhaustion; IPv6 is not perceived as an enabler of new services, market share improvement or profit increase. Results of the survey shows that MNCs are not heavily dependent on the availability of public IPv4 addresses, and they mostly rely on private addressing. During interviews, they estimated that their current pool of available IPv4 addresses would last for the next three to four years.

The situation is similar for **SMEs**, as they do not see any business need for IPv6 adoption. The survey findings showed that a relatively small number of SMEs are aware of IPv6 as a successor to IPv4, or of the upcoming exhaustion of IPv4 addresses. There is also a lack of understanding of the benefits and capabilities of IPv6.

As of February 2011, it was projected that the IPv4 address pool available for allocation by APNIC will be exhausted by around August 2011. Typical IPv6 adoption timelines among end users will vary, with MNCs and SMEs adopting IPv6 depending on their business needs.

*Return on investment*

A key part of the process of identifying the optimal time to migrate to IPv6 is to estimate the return on investment from doing so. In the majority of cases end users are unlikely to see an actual return as such, but there will be some financial implications. In assessing these implications, end users need to consider the following:

- **incremental revenue from IPv6 enablement** when compared to not IPv6 enabling; are there any financial benefits (e.g. incremental revenue through the introduction of new value-added services)
- **cost savings from IPv6 deployment**, such as lower costs achieved through simplification and interoperability of the network infrastructure
- **cost implications of IPv6 enablement**, such as additional hardware requirements, upgrading of core business applications and operating cost implications of running dual IPv4 and IPv6 for some period of time.

### 8.4.3 IPv6 skill building

IPv6 skill building ensures that all stakeholders across the organisation have the required skills to contribute to, and participate in, the IPv6 adoption process, including implementation. A summary of the key tasks for skills building is provided in Figure 8.8.

| *IPv6 skill building* | |
|---|---|
| *Overall aims* | • Ensure that IPv6 skills are built across the various levels of the organisation (IT management, IT staff, etc.), so that they can participate in, and contribute to, the IPv6 adoption process<br>• Provide skills to the IT department to enable them to implement the IPv6 adoption programme |
| *Approx. duration* | 1–3 months |
| *Key tasks* | The IPv6 skill building programme encompasses various layers of the organisation:<br>• **senior technical architects/IT management** – skills in the following areas must be covered:<br>– IPv6 solution architecture and design<br>– IPv6 migration planning and processes<br>– IPv6 service design<br>• **IT staff** – the following areas must be covered:<br>– IPv6 technology basics<br>– the mechanisms for transition to IPv6<br>– operating and maintaining IPv6-enabled networks and solutions |
| *Stakeholders* | HR, training department, IT management, senior technical architects, IT staff |
| *Dependencies* | The IPv6 awareness activity should have been completed before the IPv6 skill building activity begins, although it can be started in advance of full completion of the IPv6 awareness activity |

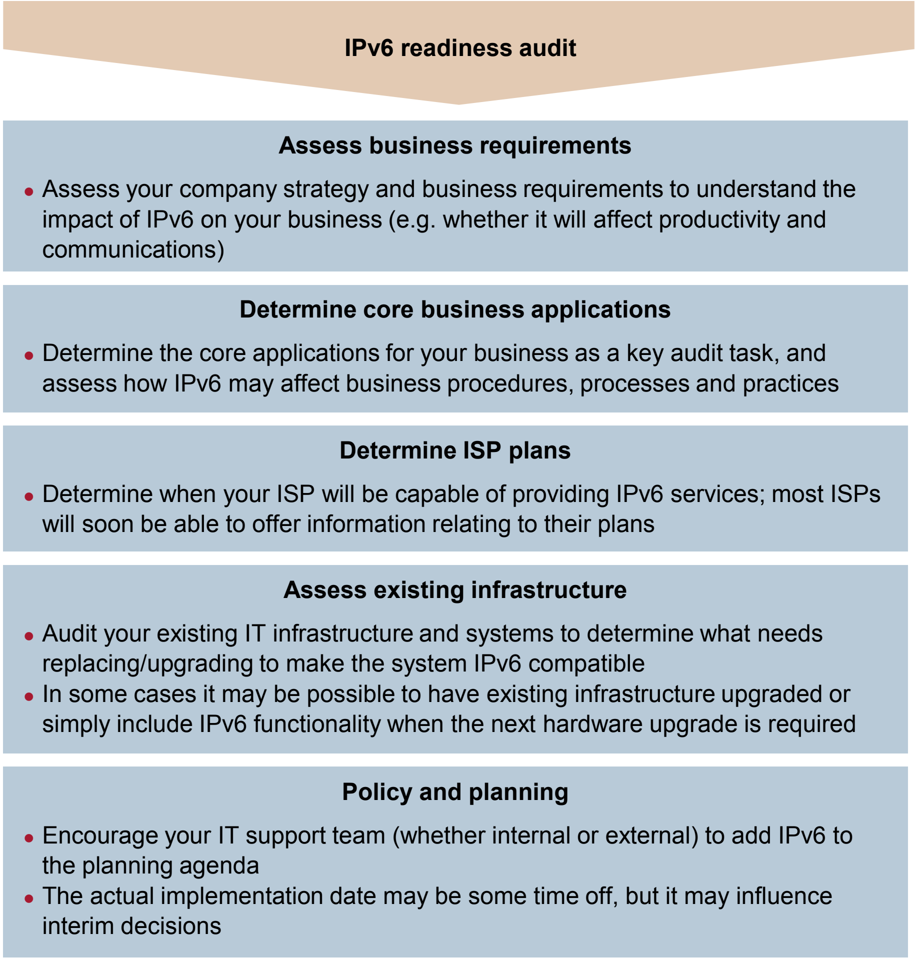
*Figure 8.8: Summary of IPv6 skill building activity for end users [Source: Analysys Mason, Tech Mahindra]*

### 8.4.4 Project plan for IPv6 adoption

The project plan for IPv6 adoption sets out the detailed set of activities to be carried out, spanning IPv6 solution architecture, design, deployment, trials and ‘go live’. During the process of developing a detailed project plan, the end user must also carry out an IPv6 readiness assessment covering network and applications. This assessment will highlight gaps between the current status and the eventual target of providing seamless IPv6 services and information that will serve as inputs to the detailed project plan. Figure 8.9 provides a summary of the project planning for the adoption of IPv6, and Figure 8.10 shows an example of an IPv6 readiness audit.

| *Project plan for IPv6 adoption* | |
|---|---|
| *Overall aims* | • Establish the organisation's current status of IPv6 adoption across network, applications and services<br>• Draw up a detailed project plan, including the various activities to be completed for IPv6 adoption and a roadmap to ensure provision of seamless IPv6 services |
| *Approx. duration* | 0.5–3 months |
| *Key tasks* | The key tasks in preparing the IPv6 adoption project plan are:<br>• establish an IPv6 workgroup team, made up of internal and/or external IPv6 experts, with responsibility for preparing the project plan for IPv6 adoption<br>• conduct an IPv6 readiness assessment to identify the gaps in IPv6 adoption across network, applications and services<br>• map the current status of IPv6 adoption<br>• draw up a detailed project plan for IPv6 adoption<br>The IPv6 readiness assessment mentioned above needs to cover the following areas:<br>• **network infrastructure** – routers, switches, security devices, DNS, DHCP, NTP, addressing delegation mechanisms, etc., spread across the core network, broadband network, mobile network, etc. Where the network is leased from a network provider, it will be necessary to engage with the provider to establish when it will be IPv6 ready. The ISP must also be consulted regarding the availability of IPv6 addresses.<br>• **application infrastructure** – network management, OSS/BSS, human resources (HR), enterprise resource planning (ERP) applications, etc.<br>• **core business applications infrastructure** – the existing and planned business applications and the status of their IPv6 enablement<br>The project plan for IPv6 adoption will detail the set of activities that must be completed in order to IPv6 enable the network, applications and services. The plan must cover the following areas:<br>• architecture and design<br>• deployment and implementation<br>• test and validation<br>• trials<br>• 'go live' for IPv6 services |
| *Stakeholders* | • **IPv6 work group team** – a team of internal and/or external IPv6 experts responsible for preparing the project plan for IPv6 adoption. Depending on the organisation, this team may have further responsibility for execution of the project plan itself<br>• **IT management** – will help to provide all the inputs required for the readiness assessment and will also identify key individuals within the business for this activity |
| *Dependencies* | • The IPv6 awareness programme needs to be completed before the IPv6 readiness programme can begin, to ensure that stakeholders understand the importance of the readiness assessment and are willing to participate fully in it<br>• The ability/willingness of third-party suppliers to engage in the planning process<br>• The IPv6 business requirements plan needs to be prepared to identify which services will need to be supported by IPv6 |

*Figure 8.9: Summary of project planning for IPv6 adoption activity for end users [Source: Analysys Mason, Tech Mahindra]*



**IPv6 readiness audit**

**Assess business requirements**

- Assess your company strategy and business requirements to understand the impact of IPv6 on your business (e.g. whether it will affect productivity and communications)

**Determine core business applications**

- Determine the core applications for your business as a key audit task, and assess how IPv6 may affect business procedures, processes and practices

**Determine ISP plans**

- Determine when your ISP will be capable of providing IPv6 services; most ISPs will soon be able to offer information relating to their plans

**Assess existing infrastructure**

- Audit your existing IT infrastructure and systems to determine what needs replacing/upgrading to make the system IPv6 compatible
- In some cases it may be possible to have existing infrastructure upgraded or simply include IPv6 functionality when the next hardware upgrade is required

**Policy and planning**

- Encourage your IT support team (whether internal or external) to add IPv6 to the planning agenda
- The actual implementation date may be some time off, but it may influence interim decisions

*Figure 8.10: An example of IPv6 readiness assessment audit and the sequence of events involved [Source: Analysys Mason, Tech Mahindra]*

### 8.4.5 IPv6 solution trial

The IPv6 readiness assessment will identify the IPv6 solutions and business applications to be deployed and rolled out across the organisation. Before starting the implementation, these solutions and applications will need to be validated in a controlled environment, with the business services plan (and project plan) revised (if needed) based on the results of the validation activity.

| *IPv6 solution trial* | |
|---|---|
| *Overall aims* | Verify and validate the proposed IPv6-based solution (architecture, design and services) before they are rolled out in a live environment |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The IPv6 solution trial lab should ensure that the IPv6 migration solution architecture included in the project plan is validated in terms of its ability to support the required business application (e.g. features and functional and performance aspects). This validation needs to cover:<br>• **IPv6 network solution** – the network solution proposed in the project plan needs to be tested for adherence to functional and performance guidelines and SLAs within the organisation<br>• **IPv6 application solution** – the various commercial and proprietary applications must be validated for their ability to function under the IPv4/IPv6 solution proposed in the project plan to a level that meets functional and performance requirements within the organisation<br>• **IPv6 services** – the business applications and services which are planned to be rolled out need to be validated in terms of functional performance and reliability in the network and application environment laid out in the project plan<br>The project plan will need to be reviewed and revised as appropriate based on the output of the validation trials |
| *Stakeholders* | Technical architects, IT management |
| *Dependencies* | • The start of this programme is dependent on completion of the IPv6 skill building programme.<br>• The IPv6 business applications plan needs to be underway before this programme can start, as applications to be validated need to be identified (although this programme can start slightly ahead of the identification of business applications) |

*Figure 8.11: Summary of IPv6 solution validation lab activity for end users [Source: Analysys Mason, Tech Mahindra]*

### 8.4.6 Quick wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organisation, and in giving IT staff the opportunity to use the theoretical skills they have gained earlier in the process, as well as to build confidence in the technology. Figure 8.12 summarises this activity, and also provides a couple of examples of quick-win initiatives.

| *IPv6 quick wins* | |
|---|---|
| *Overall aims* | • Identify and implement initial ‘quick-win’ projects<br>• Strengthen the IPv6 thought process across the organisation; develop and embed theoretical skills, and build confidence in IPv6 as a technology |
| *Approx. duration* | 2–3 months |
| *Key tasks* | The types of project chosen will depend on the current status of an organisation and are difficult to specify. However, some examples could include:<br>• **IPv6 enable the external-facing websites**, which would help the organisation to position itself as an IPv6 leader and also further establish IPv6 as an internal initiative<br>• **participate in national technology trials and test-beds**, which would provide knowledge and insight that will increase familiarity with IPv6 and inform the decision-making process during subsequent phases |
| *Stakeholders* | Corporate IT management team, procurement team, technical architects |
| *Dependencies* | The IPv6 awareness programme and the IPv6 skill-building programmes should be completed before starting this activity |

*Figure 8.12: Summary of IPv6 ‘quick win’ activity for end users [Source: Analysys Mason, Tech Mahindra]*

## 8.5 IPv6 adoption guide: architecture and design phase

This phase of the adoption activities involves transition designs for the network, applications and services to allow IPv4 and IPv6 to co-exist and work simultaneously during the transition to IPv6, and to support the introduction of new IPv6 services.

The IPv6 solution architecture and design phase needs to cover the areas outlined below.

- **Services** – prioritising the various IPv4 services that are planned to be IPv6 enabled, and finalising the new business applications to be introduced, based on initial work carried out during the planning phase. This prioritisation helps in building the network and application solution architecture and designs.

- **Network** – architecting and designing the various network solutions to support the planned IPv6 services, including the IPv4 run-out scenario and transition to a complete IPv6-only ecosystem.

- **Applications** – architecting and designing the various solutions to support the planned IPv6 services and network solution.

The remainder of this section summarises the key activities in each of these areas, with annexes providing supporting technical details.

### 8.5.1 Architecture and design – networks

Once the architecture and design for the IPv6 services are finalised, a network solution architecture and design that is aligned with core business applications will have to be prepared.

The network solution architecture will need to consider the various stages through which the organisation's network will pass (e.g. IPv4-only, support for both IPv4 and IPv6, and IPv6-only). Based on the current status of IPv6 readiness and IPv4 address availability, the solution should consider a back-up solution for a scenario in which the organisation has run out of IPv4 addresses, but has not yet fully adopted IPv6.

| *IPv6 network solution architecture and design* | |
|---|---|
| *Overall aims* | Prepare an IPv6 network solution architecture and design which will help to enable IPv6 on the current IPv4-based services and introduce new IPv6 services |
| *Approx. duration* | 1–2 months |
| *Key tasks* | Ensure that the IPv6 network solution architecture and design – of both core and access networks – cover the following areas:<br>• **IPv4/IPv6 interconnectivity** – individual IPv4 and IPv6 networks are connected via various tunnelling mechanisms, dual stack, etc.<br>• **IPv6 routing** – the reachability of the network elements across IPv4 and IPv6 topologies must be ensured, through appropriate deployment of the IPv6 routing protocol<br>• **IPv6 security** – the various network solutions that are designed must ensure that the security aspects of the planned network roll-out are considered and in place<br>• **quality of service (QoS)** – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance<br>• **multicast services** – the various multicast services across the IPv6 network must be designed in accordance with the planned services<br>• **traceability of traffic sessions** – if required for regulatory purposes, recording of the various IPv6 sessions taking place across the network should be incorporated |
| *Stakeholders* | Technical architects, IT management, IT staff |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can be initiated, and the architecture and design for services needs to be completed, or almost completed |

*Figure 8.13: Summary of IPv6 network solution architecture and design activity for end users [Source: Analysys Mason, Tech Mahindra]*

### 8.5.2 Architecture and design – transition technology approaches/mechanisms

During the architecture and design phase, it is important for stakeholders to choose the right technical approach or 'mechanism' to enable their networks to make the transition towards IPv6. The choice of mechanism will depend on the current IPv4 environment and the planned IPv6 network, applications and services.

The IPv6 transition mechanisms for networks (which are discussed in more detail in Annex B) include:

- IPv6 in IPv4 tunnels
- dedicated IPv6 links
- dual-stack networks.

As the introduction of IPv6 across the network has to be achieved with minimal disruption to the existing network, it should be a gradual transition. The various IPv6 network transition phases for a stakeholder are shown in Figure 8.14, and explained below.

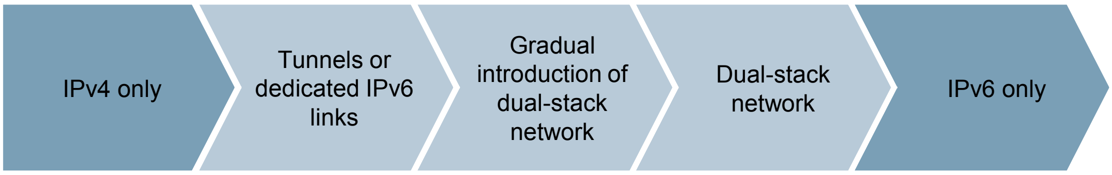

IPv4 only
Tunnels or dedicated IPv6 links
Gradual introduction of dual-stack network
Dual-stack network
IPv6 only

*Figure 8.14: Full range of transition phases that might be involved in migration from IPv4 to IPv6 for end users [Source: Analysys Mason]*

The starting point for all stakeholders is an IPv4-only network. In this scenario, the stakeholder can connect to an IPv6 network using either IPv6 tunnelling mechanisms or separate dedicated IPv6 connections or links.

Tunnelling would be an interim temporary solution, which can be implemented with the smallest requirement for infrastructure upgrades and investment. The downside is that this model does not scale as the number of users increases.

As IPv6 adoption progresses, dual-stack network components (see Annex A for examples) are gradually introduced into the network, leading to reduction in the usage of tunnels or dedicated IPv6 links.

The next step is for all network components across the organisation to be dual-stack ready and enabled – this allows the organisation to provide seamless IPv6 capabilities and services. This also sets the stage for gradually turning off IPv4 services and progressing towards IPv6-only services.

The final outcome is to turn off the IPv4 capabilities on the dual-stack routers, leaving only IPv6 services available to the customers.

This approach can be adopted across all stakeholder segments, and can be executed in sequence; alternatively, a stakeholder may choose to miss out some phases for business or technical reasons.

The choice of transition mechanism – tunnelling, dual-stack networks or dedicated links – will depend on the type of network that is being IPv6 enabled and the services to be supported.

### 8.5.3 Architecture and design – applications

Once the IPv6 network architecture is finalised, an application architecture and design, which is aligned with them, can be prepared. This will also consider the approach to configuring the relevant OSS/BSS, network management and network monitoring applications to support management of the planned IPv6 services. The key tasks are highlighted in Figure 8.15.

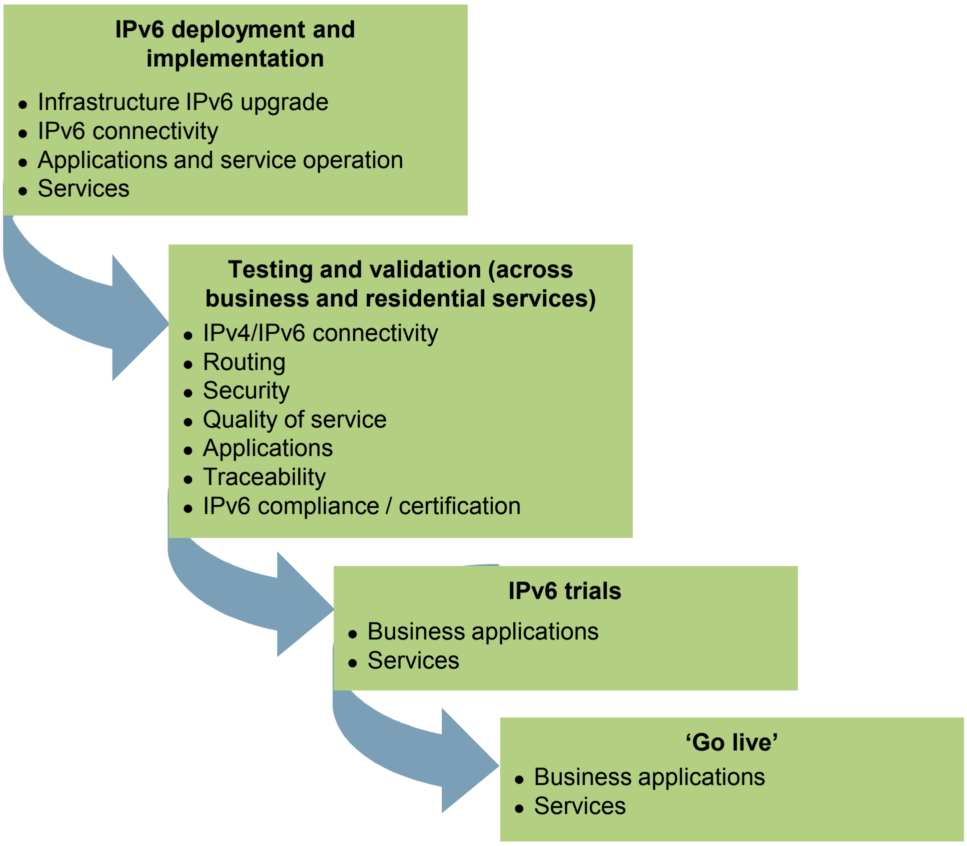
| *IPv6 application solution architecture and design* | |
|---|---|
| *Overall aims* | Prepare an IPv6 application solution architecture and design, which will help enable IPv6 on the current IPv4-based services and introduce new IPv6 services |
| *Approx. duration* | 1–2 months |
| *Key tasks* | The IPv6 application solution architecture and design needs to cover the following areas:<br>• ensure **network management and monitoring applications/solutions** are seamlessly able to support and monitor IPv4 and IPv6 networks<br>• ensure **applications such as ERP and CRM systems** are able to support IPv6- and IPv4-based connectivity and services<br>• **ensure proprietary applications** are able to support both IPv6- and IPv4-based connectivity services |
| *Stakeholders* | Technical architects, IT staff, vendors |
| *Dependencies* | The IPv6 readiness assessment and project plan need to be completed before this activity can be initiated, and the architecture and design for services needs to be completed, while the architecture and design for networks can be prepared in parallel |

*Figure 8.15: Summary of IPv6 application solution architecture and design activity for end users [Source: Analysys Mason, Tech Mahindra]*

The IPv6 readiness assessment conducted in the planning phase will provide a list of IPv6-compliant and non-compliant applications. Applications that are found to be non-IPv6 compliant will need either to be upgraded to an IPv6-compliant version, or replaced with new software that provides the same functionality and is also IPv6 compliant.

## 8.6 IPv6 adoption guide: deployment phase

In this phase, the IPv6 adoption project plan developed during the planning phase and the solutions architected during the architecture and design phase are implemented, and IPv6 is enabled across the organisation. An overview of the activities involved in this phase is provided in Figure 8.16.



**IPv6 deployment and implementation**

- Infrastructure IPv6 upgrade
- IPv6 connectivity
- Applications and service operation
- Services

**Testing and validation (across business and residential services)**

- IPv4/IPv6 connectivity
- Routing
- Security
- Quality of service
- Applications
- Traceability
- IPv6 compliance / certification

**IPv6 trials**

- Business applications
- Services

**'Go live'**

- Business applications
- Services

*Figure 8.16: Summary of deployment phase for end users [Source: Analysys Mason, Tech Mahindra]*

### 8.6.1 IPv6 deployment and implementation

Once the architecture and designs for services, network and applications have been identified, the next step is to deploy these solutions in order to launch IPv6 services. Based on a comparison of the solution architecture and design (across networks, applications and services) and the findings of the IPv6 readiness assessment from the planning phase, organisations can prepare a list of the infrastructure that would need to be upgraded to IPv6 to support the planned services and products. The process of upgrading this infrastructure should be initiated as a first step in the deployment of IPv6. A summary of deployment and implementation activities is provided below in Figure 8.17.

| *IPv6 deployment and implementation* | |
|---|---|
| *Overall aims* | Deploy IPv6 across the network and applications to support the launch of IPv6 services |
| *Approx. duration* | 3–4 months |
| *Key tasks* | The IPv6 deployment and implementation would cover the following areas:<br>• **infrastructure IPv6 upgrade** of the hardware and firmware systems (if they are not IPv6 ready) or replacement with IPv6-compliant firmware<br>• **IPv6 connectivity** – IPv6 addresses are purchased and IPv6 connectivity is established with upstream providers and other peers<br>• **applications and service operations** – the various applications such as network management, monitoring, customer relationship management, etc. are IPv6 enabled<br>• **services** – the various services spread across the organisations are IPv6 enabled |
| *Stakeholders* | Technical architects and IT staff |
| *Dependencies* | The IPv6 service, network and application architecture need to be mostly completed before deployment and implementation can begin |

*Figure 8.17: Summary of IPv6 deployment and implementation activity for end users [Source: Analysys Mason, Tech Mahindra]*

### 8.6.2 IPv6 test and validation

| *IPv6 test and validation* | |
|---|---|
| *Overall aims* | Validate IPv6 services and applications across the internal/external networks/external and also the Internet service provider |
| *Approx. duration* | 1–4 months |
| *Key tasks* | IPv6 test and validation will cover the following areas of IPv6 products and services:<br>• **IPv4/IPv6 connectivity** will be validated<br>• **IPv6 routing** – the network elements across IPv4 and IPv6 topologies will be reachable through the appropriate IPv6 routing protocol<br>• **IPv6 security** – the security aspects of the network will be validated<br>• **QoS** aspects will be validated across the network<br>• **multicast services** as per the service design will be validated across the network<br>• **applications** – the various applications in use will be validated for their IPv6 support, to include any proprietary systems<br>• **IPv6 compliance / certification (optional)** – the IPv6 services are tested against a range of certifications or compliance measurement programmes |
| *Stakeholders* | Technical architects and IT staff |
| *Dependencies* | The IPv6 services solution roll-out should be completed |

*Figure 8.18: Summary of IPv6 test and validation activity for end users [Source: Analysys Mason, Tech Mahindra]*

### 8.6.3 IPv6 trials

| *IPv6 trials* | |
|---|---|
| *Overall aims* | IPv6 trials are conducted within the organisation |
| *Approx. duration* | 3–4 months |
| *Key tasks* | IPv6 trials are conducted within the organisation, covering:<br>• networks<br>• business applications<br>• services |
| *Stakeholders* | Business teams, IT staff, account management, operations and support |
| *Dependencies* | IPv6 testing and validation should be completed before trials |

*Figure 8.19: Summary of IPv6 trials activity for end users [Source: Analysys Mason, Tech Mahindra]*

After the network and applications have been IPv6 enabled, and the solutions have been tested and validated, the next stage in the IPv6 adoption process is to run a number of IPv6 trials across both internal and external networks. As part of the trials, the applications (e.g. CRM, ERP, ecommerce systems, web hosting, etc.) will be validated for their conformance to functional and performance specifications.

### 8.6.4 IPv6 'go live'

| *IPv6 'go live'* | |
|---|---|
| *Overall aims* | IPv6 services are rolled out across the organisation |
| *Approx. duration* | 1–4 months |
| *Key tasks* | IPv6 services are made available and rolled out internally and externally |
| *Stakeholders* | Business teams and IT staff |
| *Dependencies* | The IPv6 trials must be completed before IPv6 'go live' |

*Figure 8.20: Summary of IPv6 'go live' activity for end users [Source: Analysys Mason, Tech Mahindra]*

After the service, network and application solutions to support the provision of IPv6 applications and services have been deployed and successful trials have been conducted, the end user can decide whether to launch the IPv6 application and services internally and externally.

## 8.7 IPv6 adoption guide: ongoing support phase

Prior to launch of live services, it is essential to ensure that adequate support mechanisms are in place, including:

- **Technical support** – first- through to third-line support via a help desk
- **Specialist support** – access to support from external organisations that have supplied hardware and applications.

# Annex A: Overview of IPv6 transition mechanisms

This annex provides an overview of some of the key transition mechanisms.

## A.1 Key transition mechanisms

### A.1.1 6RD

6RD specifies a protocol mechanism to deploy IPv6 to sites via a service provider's IPv4 network. 6RD builds on 6to4 tunnelling mechanism, which uses the well-known prefix (2002::/16), but in the case of 6RD the service provider's own IPv6 address prefix is used. As the service provider's IPv6 prefix is used, the operational domain of 6RD is limited to the service provider's network. The IPv6 service provided is equivalent to native IPv6.

The 6RD specification is based on the following principles:

- Ensure rapid deployment of IPv6 by Internet service providers that are still IPv4-only, without modifying their current IPv4 infrastructure. The rapidity principle implies that 6RD functions should be introduced only at the periphery of IPv4 infrastructures.  routing on these infrastructures should be that of IPv4, with no need for an independent address assignment and routing policy for IPv6.

- Ensure completeness of the IPv6 unicast service offered to their customers. Internet service providers should make no assumption about how hosts of other Internet service providers obtain their IPv6 service. The completeness principle implies that IPv6 prefixes of 6RD sites must start with prefixes that belong to the IPv6 address spaces.

- Ensure scalability of IPv6 deployment on IPv4 infrastructure. Encapsulation-decapsulation functions of IPv6 packets in IPv4 ones should be *stateless* (load sharing between a number of distributed processors should be feasible). The scalability principle implies that encapsulation functions in 6RD relays can find IPv4 destination addresses without depending on some temporary states that would relate IPv4 destinations to IPv6 ones.

- Ensure efficiency. An IPv6 packet between two IPv4 sites of the same Internet service provider should follow the *same routes* as those of IPv4 packets between the same sites. The efficiency principle implies that 6RD CPEs can recognise, in packets leaving their sites, which ones can be routed to their destination directly across the local Internet service provider IPv4 infrastructure (i.e. without having to go through a 6RD relay).

The 6RD mechanism relies upon an algorithmic mapping between the IPv6 and IPv4 addresses that are assigned for use within the service provider network. This mapping allows for automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, allowing stateless operation of 6RD. 6RD views the IPv4 network as a link layer for IPv6 and supports an automatic tunnelling abstraction similar to the Non-Broadcast Multiple Access (NBMA) model.

A 6RD domain consists of 6RD Customer Edge (CE) routers and one or more 6RD Border Relays (BRs). IPv6 packets encapsulated by 6RD follow the IPv4 routing topology within the service provider network among CEs and BRs. 6RD BRs are traversed only for IPv6 packets that are destined to or are arriving from outside the service provider's 6RD domain. As 6RD is stateless, BRs may be reached using anycast for failover and resiliency.

On the 'customer-facing' (i.e. LAN) side of a CE, IPv6 is implemented as it would be for any native IP service delivered by the service provider, and further considerations for IPv6 operation on the LAN side of the CE is out of scope for this document. On the 'service-provider-facing' (i.e. WAN) side of the 6RD CE, the WAN interface itself, encapsulation over Ethernet, ATM or PPP, as well as control protocols such as PPPoE, IPCP, DHCP, etc. all remain unchanged from current IPv4 operation. Although 6RD was designed primarily to support IPv6 deployment to a customer site (such as a residential home network) by a service provider, it can equally be applied to an individual IPv6 host acting as a CE.

6RD relies on IPv4 and is designed to deliver production-quality IPv6 alongside IPv4 with as little change to IPv4 networking and operations as possible. Native IPv6 deployment within the service provider network itself may continue for the service provider's own purposes while delivering IPv6 service to sites supported by 6RD. Once the service provider network and operations can support fully native IPv6 access and transport, 6RD may be discontinued.

6RD uses the same encapsulation and base mechanism as 6to4 and could be viewed as a superset of 6to4 (6to4 could be achieved by setting the 6RD prefix to 2002::/16). Unlike 6to4, 6RD is for use only in an environment where a service provider closely manages the delivery of IPv6 service. 6to4 routes with the 2002::/16 prefix may exist alongside 6RD in the 6RD CE router, and doing so may offer some efficiencies when communicating directly with 6to4 routers. The 6RD link model can be extended to support IPv6 multicast.

More details of 6RD are available in the IETF draft- draft-ietf-softwire-ipv6-6RD-08.txt 'IPv6 Rapid Deployment on IPv4 Infrastructures (6RD) – Protocol Specification' (see http://tools.ietf.org for this reference and subsequent ones in Annex A).

### A.1.2 Carrier-grade NAT

Carrier-grade NAT (CGN) integrates multiple transition mechanisms and can simplify the operation of end-user services during the IPv4/IPv6 migration or co-existence period. CGNs are deployed on the network side. On the user side, new CPE devices may be needed to support IPv6 adoption. Dual-stack lite is a CGN-based solution that supports transition, but it requires the Internet service provider to upgrade its network to IPv6s immediately, which many Internet service providers are hesitant to do.

The incremental carrier-grade NAT is similar to DSLite; it mainly combines v4-v4 NAT with v6-over-v4 tunnelling functions along with some minor adjustment. It can provide IPv6 access services for IPv6-enabled end hosts and IPv4 access services for IPv4 end hosts, while leaving most legacy IPv4 Internet service provider networks unchanged. The deployment of this technology has no effect at all on legacy IPv4 hosts with global IPv4 addresses. It is suitable for the initial stage of IPv4/IPv6 migration. It also supports transition towards dual-stack or IPv6-only Internet service provider networks.

Most service providers today are operating in an IPv4 environment and are starting to provide IPv6 access services for end users. However, at the initial stage of IPv4/IPv6 migration, IPv4 would represent the majority of connectivity and traffic on most Internet service provider networks. Internet service providers would like to minimise the changes on their IPv4 networks. Switching the whole Internet service provider network to IPv6-only would be considered as a radical strategy. Switching the whole Internet service provider network to dual-stack is less radical, but introduces operational costs and complications. Although some Internet service providers have successfully deployed dual-stack routers, others prefer not to do this as their first step in IPv6. However, they currently face two urgent pressures – to compensate for an immediate shortage of IPv4 addresses by deploying some method of address sharing, and to prepare actively for the deployment of IPv6 address space and services. Internet service providers facing only one of these two pressures could adopt either CGN (for shortage of IPv6 addresses) or 6RD (to provide IPv6 connectivity services). The carrier-grade NAT approach addresses all these issues at the same time by combining v4-v4 CGN with v6-over-v4 tunnelling technologies.

More details of carrier-grade NAT are available in the IETF document An Incremental Carrier-Grade NAT (CGN) for ‘IPv6 Transition draft-ietf-v6ops-incremental-cgn-01.txt’.

### A.1.3 Dual-stack lite

Dual-stack lite (DS Lite) is a promising approach that takes the best of NAT464 while avoiding its problems: it uses IPv6-only links between the provider and the customer, but does not use NAT64 translation. When a device in the customer network sends an IPv4 packet to an external destination, the IPv4 packet is encapsulated in an IPv6 packet for transport into the provider network. At the large-scale NAT, the packet is decapsulated and NAT44 is performed. Tunnelling IPv4 over IPv6 is far simpler than translation, so the performance and redundancy concerns are eliminated.

If a simple mapping from inside IPv4 source address/port to outside IPv4 source address/port was performed on outgoing packets (as is done with regular NAT44), the large-scale NAT would have no way to differentiate between overlapping IPv4 private addresses in different customer networks. Therefore an additional element is added to the address mapping: the source address of the encapsulating IPv6 packet (the address of the customer end of the IPv6 link) is added to the inside IPv4 source address and port. Because the IPv6 address is unique to each customer, the combination of IPv6 source address + IPv4 source address + port makes the mapping unambiguous. When a responding IPv4 packet is received from the outside, its IPv4 destination address and port can be correctly matched to a specific customer behind the NAT based on the IPv6 address in the mapping table. The packet's IPv4 destination address and port can then be mapped to the inside IPv4 destination address and port, encapsulated in IPv6 using the mapped IPv6 address as the IPv6 destination address, and forwarded to the customer.

The mapped IPv6 address not only disambiguates the customer private IPv4 address; it also provides the reference for the tunnel endpoint.

Assuming there are multiple end systems in the customer network, the DS Lite function occurs on a CPE device such as a home gateway. If a device sends an IPv6 packet, the packet is routed normally to the IPv6 destination. If a device sends an IPv4 packet, the CPE gateway performs the IPv4-in-IPv6 encapsulation, setting the destination address of the IPv6 packet to the address of the DS Lite enabled large-scale NAT. This model allows use of dual-stacked, IPv4-only and IPv6-only devices behind the gateway.

One of the drawbacks of DS Lite is that functionality must be added to existing customers' CPE, either through a software upgrade or by replacing the unit. This could cause inconvenience to the customers and the service provider would incur the expense of replacing installed equipment.

DS Lite capable CPE can be deployed initially only for new customers; for existing customers, CPE can be upgraded or replaced on a more casual schedule as a part of normal end-of-life equipment changes.

Another DS Lite implementation involves its use on an individual end system rather than on a CPE device. The device is dual stacked, and hence can send and receive both IPv4 and IPv6 packets. This model is relevant to customers who connect a single PC, game system, or laptop to the Internet rather than to a network behind a router; it has great potential for mobile broadband.

Mobile providers face the same problems of needing to address 'smart phones' and 4G wireless technologies such as LTE with IPv6 but providing a means for those mobile users to reach IPv4 content.

More details of DS Lite are available in the IETF document 'Deploying Dual-Stack Lite in IPv6 Network draft-boucadair-dslite-interco-v4v6-04'.

### A.1.4 NAT64

NAT64 is a mechanism for translating IPv6 packets to IPv4 packets. The translation is done by translating the packet headers according to the Stateless IP/ICMP Translation Algorithm, translating the IPv4 server address by adding or removing a /96 prefix, and translating the IPv6 client address by installing mappings in the normal NAT manner.

DNS64 is a mechanism for synthesising AAAA resource records (RR) from A RR. The synthesis is done by adding a /96 prefix to the IPv4 address to create an IPv6 address, where the /96 prefix is assigned to a NAT64 device.

Together, these two mechanisms allow an IPv6-only client to initiate communications to an IPv4-only server. These mechanisms are expected to play a critical role in the IPv4–IPv6 transition and co-existence. Due to IPv4 address depletion, it is likely that, in future, a lot of IPv6-only clients will want to connect to IPv4-only servers. The NAT64 and DNS64 mechanisms are easily deployable, since they require no changes to either the IPv6 client or the IPv6 server. For basic functionality, the approach only requires the deployment of NAT64-enabled devices connecting an IPv6-only network to the IPv4-only Internet, along with the deployment of a few DNS64-enabled name servers in the IPv6-only network. However, some advanced features require software updates to the IPv6-only hosts.

The NAT64 mechanism is implemented in an NAT64 box which has two interfaces – an IPv4 interface connected to the IPv4 network, and an IPv6 interface connected to the IPv6 network. Packets generated in the IPv6 network for a receiver located in the IPv4 network will be routed within the IPv6 network towards the NAT64 box. The NAT64 box will translate them and forward them as IPv4 packets through the IPv4 network to the IPv4 receiver. The reverse takes place for packets generated in the IPv4 network for an IPv6 receiver. NAT64, however, is not symmetric. In order to be able to perform IPv6–IPv4 translation NAT64 requires state, binding an IPv6 address and port (hereafter called an IPv6 transport address) to an IPv4 address and port (hereafter called an IPv4 transport address).

Such binding state is created when the first packet flowing from the IPv6 network to the IPv4 network is translated. After the binding state has been created, packets flowing in either direction on that particular flow are translated. The result is that NAT64 only supports communications initiated by the IPv6-only node towards an IPv4-only node. Some additional mechanisms, like ICE, can be used in combination with NAT64 to provide support for communications initiated by the IPv4-only node to the IPv6-only node.

More details on NAT64 are available in the IETF document ‘NAT64/DNS64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers draft-bagnulo-behave-nat64-00’.

## A.2 DHCP and DNS in IPv6

### A.2.1 DHCPv6

DHCPv6 protocol is a new design and carries very few remnants of DHCPv4. DHCPv4 was built from an earlier protocol called BOOTP, from which it inherited many now unnecessary features. DHCPv6 was cleaned up considerably, and contains none of the things leftover from BOOTP. DHCPv4 runs over IPv4, and supplies only 32-bit IPv4 information (assigned IPv4 addresses, IPv4 addresses of DNS servers, etc.). DHCPv6 runs only over IPv6, and supplies only 128-bit IPv6 information (assigned IPv6 addresses, IPv6 addresses of DNS servers, etc.). There is no conflict between DHCPv4 and DHCPv6 in terms of functionality or ports used, so it is possible to run both on a single, dual-stack node. Hosts communicate only with DHCPv6 servers or relay agents on their local link, using link-local addresses. DHCPv6 uses ports UDP 546 and 547 (whereas DHCPv4 uses UDP ports 67 and 68). As with DHCPv4, relay agents are used to allow hosts to communicate with remote DHCPv6 servers.

In a few simple networks, there is no need for DHCPv6, because of Stateless Address Autoconfiguration. Currently, however, DHCPv6 is the only way for IPv6-capable nodes to automatically learn the IPv6 addresses of DNS servers. This is particularly important for IPv6-only networks. For dual-stack networks, there is no conflict between DHCPv4 and DHCPv6, and both can exist even on a single node. In this case, the IPv4 side of a node would get its IPv4 configuration from the DHCPv4 server, and the IPv6 side of a node would get its IPv6 configuration from the DHCPv6 server.

IPv6-capable nodes can be informed that there is a DHCPv6 server available via two bits in the Router Advertisement message. In the Router Advertisement message there are two bits, M and O (first and second bits of the sixth byte of the Router Advertisement message), with the following semantics:

- M – 'Managed address configuration' flag. When set it indicates that addresses are available via DHCPv6. If set, then the O flag can be ignored. This enables stateful DHCPv6, where both the stateless information (IPv6 addresses of DNS and other servers) and global unicast addresses can be obtained from DHCPv6.

- O – 'Other configuration' flag. When set, it indicates that other configuration information is available via DHCPv6. This includes things such as IPv6 addresses of DNS or other servers. This is called stateless DHCPv6, and is used in conjunction with Stateless Address Autoconfiguration (for obtaining global unicast addresses).

If both M and O bits are clear, then Stateless Address Autoconfiguration (SAA) is the only way to get addresses, and there is no source of IPv6 addresses for any server, including DNS.

More details on DHCPv6 are available in the IETF document RFC 3315, 'Dynamic Host Configuration Protocol for IPv6 (DHCPv6)'.

### A.2.2 DNSv6

The computing nodes fixed or mobile can acquire one or more IPv6 addresses, default routes and some other parameters, via Neighbour Discovery (ND) for IP Version 6 and IPv6 Stateless Address Autoconfiguration; however, in order to access to additional services on the Internet that are identified by a DNS name (such as a web server), the configuration of at least one recursive DNS server is needed for DNS name resolution.

An operator or an enterprise organisation has multiple ways in which it can dissipate DNSv6 information to the end-computing nodes: these include the router advertisement (RA) option, the DHCPv6 option and the well-known anycast option. Details of how these options can be used to provide DNSv6 information to end users are provided below.

► *Router advertisement (RA) option*

The RA approach defines a new ND option, called the RDNSS option, which contains a recursive DNS server address. Existing ND transport mechanisms (i.e. advertisements and solicitations) are used. This works in the same way that nodes learn about routers and prefixes. An IPv6 host can configure the IPv6 addresses of one, or more, RDNSSs via an RA message periodically sent by a router, or solicited by a Router Solicitation (RS).

This approach needs RDNSS information to be configured in the routers doing the advertisements. The configuration of RDNSS addresses can be performed manually by an operator, or in other ways, such as automatic configuration through a DHCPv6 client running on the router. An RA message with one RDNSS option can include as many RDNSS addresses as needed.

Through the ND protocol and RDNSS option, along with a prefix information option, an IPv6 host can perform network configuration of its IPv6 address and RDNSS simultaneously. The RA option for RDNSS can be used on any network that supports the use of ND. The RA approach is useful in some mobile environments where the addresses of the RDNSSs are changing, because the RA option includes a lifetime field that allows client to use RDNSSs nearer to the client. This can be configured to a value that will require the clients to time out the entry and switch over to another RDNSS address. The preference value of RDNSS, included in the RDNSS option, allows IPv6 hosts to select primary RDNSS among several RDNSSs; this can be used for the load balancing of RDNSSs.

► *DHCPv6 option*

DHCPv6 includes the 'DNS Recursive Name Server' option, through which a host can obtain a list of IP addresses of recursive DNS servers. The DNS Recursive Name Server option carries a list of IPv6 addresses of RDNSSs to which the host may send DNS queries. The DNS servers are listed in order of preference for use by the DNS resolver on the host.

The DNS Recursive Name Server option can be carried in any DHCPv6 Reply message, in response to either a Request or an Information request message. Thus, the DNS Recursive Name Server option can be used either when DHCPv6 is used for address assignment, or when DHCPv6 is used only for other configuration information, such as stateless DHCPv6.

Stateless DHCPv6 can be deployed either by using DHCPv6 servers running on general-purpose computers, or on router hardware. Several router vendors currently implement stateless DHCPv6 servers. Deploying stateless DHCPv6 in routers has the advantage that no special hardware is required, and it should work well for networks where DHCPv6 is needed for very straightforward configuration of network devices.

However, routers can also act as DHCPv6 relay agents. In this case, the DHCPv6 server need not be on the router, it can be on a general-purpose computer. This has the potential to give the operator of the DHCPv6 server more flexibility in how the DHCPv6 server responds to individual clients (that can easily be given different configuration information based on their identity, or for any other reason). DHCPv6 currently provides a mechanism for reconfiguring DHCPv6 clients that use a stateful configuration assignment. To do this, the DHCPv6 server sends a Reconfigure message to the client. The client validates the Reconfigure message, and then contacts the DHCPv6 server to obtain updated configuration information. By using this mechanism, it is currently possible to propagate new configuration information to DHCPv6 clients as this information changes.

► *Anycast option*

Anycast uses the same  routing system as unicast. However, administrative entities are local ones. The local entities may accept unicast routes (including default routes) to anycast servers from adjacent entities. The administrative entities should not advertise their peer routes to their internal anycast servers, if they want to prohibit external access from some peers to the servers. If some advertisement is inevitable (as is the case with default routes), the packets to the servers should be blocked at the boundary of the entities. Thus, for this anycast option, not only unicast  routing, but also unicast ND protocols can be used ‘as is’.

DNS clients today already have redundancy by having multiple well-known anycast addresses configured as RDNSS addresses. The approach with well-known anycast addresses is to set multiple well-known anycast addresses in clients’ resolver configuration files from the beginning as, say, a factory default. An anycast address is an address shared by multiple servers (in this case, the servers are RDNSSs). A request from a client to the anycast address is routed to a server selected by the  routing system.

More details on DNSv6 are available in the IETF document RFC 4339, ‘IPv6 Host Configuration of DNS Server Information Approaches’.

## A.3 IPv6 network address design

The Internet Protocol Version 6 (IPv6) Addressing Architecture defines three main types of address: unicast, anycast and multicast.

As organisations adopt IPv6, they need to consider various scenarios and aspects of design and planning of an addressing scheme for an IPv6 network: the network's IPv6 addressing plan may be for an IPv6-only network, or for a dual-stack infrastructure where some, or all, devices have addresses in both protocols. If organisations take account of these considerations, this will help them to efficiently and prudently assign the IPv6 address space that has been allocated to them.

*Network-level addressing design considerations*

- *Globally Unique Addresses*

The most commonly used unicast addresses will be Globally Unique Addresses. No significant considerations are necessary if the organisation has an address space assignment and a single prefix is deployed through a single upstream provider.

However, a multi-homed site may deploy addresses from two or more service-provider-assigned IPv6 address ranges. Here, the network administrator must have awareness on where and how these ranges are used on the multi-homed infrastructure environment. The nature of the usage of multiple prefixes may depend on the reason for multi-homing (e.g. resilience failover, load balancing, policy-based routing, or multi-homing during an IPv6 renumbering event). IPv6 introduces improved support for multi-addressed hosts through the IPv6 default address selection methods. A multi-homed host may thus have two or more addresses, one per prefix (provider), and select source and destination addresses to use.

- *Unique Local IPv6 Addresses (ULAs)*

ULAs have replaced the originally conceived site-local addresses in the IPv6 addressing architecture. ULAs improve on site-local addresses by offering a high probability of the global uniqueness of the prefix used, which can be beneficial when there is (deliberate or accidental) leakage, or when networks are merged. ULAs are akin to the private address space assigned for IPv4 networks, except that in IPv6 networks we may expect to see ULAs used alongside global addresses, with ULAs used internally and globals used externally.

The ULA address range allows network administrators to deploy IPv6 addresses on their network without asking for a globally unique registered IPv6 address range. A ULA prefix is 48 bits, i.e. a /48, the same as the currently recommended allocation for a site from the globally routable IPv6 address space.

A site that wishes to use ULAs can have (a) multiple /48 prefixes (e.g. a /44), (b) one /48, or (c) a less-than-/48 prefix (e.g. a /56 or /64). In all of the above cases, the ULAs can be randomly chosen, but in case of (a) the use of randomly chosen ULAs will provide sub-optimal aggregation capabilities.

ULAs provide the means to deploy a fixed addressing scheme that is not affected by a change in service provider and the corresponding provider aggregatable (PA) global addresses. Internal operation of the network is thus unaffected during renumbering events.

A site using ULAs may or may not also deploy global addresses. In an isolated network, ULAs may be deployed on their own. In a connected network that also deploys global addresses, both may be deployed, such that hosts become multi-addressed (one global and one ULA), and the IPv6 default address selection algorithm will pick the appropriate source and destination addresses to use (e.g. ULAs will be selected where both the source and destination hosts have ULAs). Because a ULA and a global site prefix both have a length of /48, an administrator can choose to use the same subnetting (and host addressing) plan for both prefixes.

As an example of the problems ULAs may cause, when using IPv6 multicast within the network, the IPv6 default address selection algorithm prefers the ULA as the source address for the IPv6 multicast streams. This is not a valid option when sending an IPv6 multicast stream to the IPv6 Internet, for two reasons. Firstly, these addresses are not globally routable, so Reverse Path Forwarding checks for such traffic will fail outside the internal network. Secondly, the traffic is unlikely to cross the network boundary due to multicast domain control and perimeter security policies.

*Network-level design considerations*

IPv6 provides network administrators with a significantly larger address space, enabling them to be very creative in how they define logical and practical addressing plans. The subnetting of assigned prefixes can be done based on various logical schemes that involve factors such as:

- using existing systems
  - translate the existing subnet numbers into IPv6 subnet IDs
  - translate the VLAN IDs into IPv6 subnet IDs
- redesign
  - allocate according to your need
- aggregation
  - **geographical boundaries** – by assigning a common prefix to all subnets within a geographical area
  - **organisational boundaries** – by assigning a common prefix to an entire organisation or group within a corporate infrastructure
  - **service type** – by reserving certain prefixes for predefined services (such as VoIP, content distribution, wireless services, Internet access, security areas, etc.).

This type of addressing may create dependencies on IP addresses that can make renumbering harder if the nodes or interfaces supporting those services on the network are sparse within the topology. Such logical addressing plans have the potential to simplify network operations and service offerings, and to simplify network management and troubleshooting. A very large network would not need to consider using private address space for its infrastructure devices, thereby simplifying network management.

The network designer must, however, keep in mind several factors when developing these new addressing schemes for networks with and without global connectivity:

- **Prefix aggregation** – The larger IPv6 addresses can lead to larger routing tables, unless network designers are actively pursuing aggregation. While prefix aggregation will be enforced by the service provider, it is beneficial for the individual organisations to observe the same principles in their network design process.

- **Network growth** – The allocation mechanism for flexible growth of a network prefix can be used to allow the network infrastructure to grow and be numbered in a way that is likely to preserve aggregation (the plan leaves 'holes' for growth).

- **ULA usage in large networks** – Networks with a large number of 'sites' that each deploy a ULA prefix that will by default be a 'random' /48 under fc00::/7 will have no aggregation of those prefixes. Thus, the end result may be cumbersome, because the network will have large amounts of non-aggregated ULA prefixes. However, there is no rule to disallow large networks from using a single ULA prefix for all 'sites', as a ULA still provides 16 bits for subnetting to be used internally.

- **Compact numbering of small sites** – It is possible that as registry policies evolve, a small site may experience an increase in prefix length when renumbering (e.g. from /48 to /56). For this reason, the best practice is to number subnets compactly rather than sparsely, and to use low-order bits as much as possible when numbering subnets. In other words, even if a /48 is allocated, act as though only a /56 is available. This advice does not apply to large sites and enterprises that have an intrinsic need for a /48 prefix.

- **Consider assigning more than one /64 to a site** – A small site may want to enable routing among interfaces connected to a gateway device. For example, a residential gateway that receives a /48 and is situated in a home with multiple LANs of different media types (sensor network, wired, Wi-Fi, etc.), or has a need for traffic segmentation (home, work, children, etc.), could benefit greatly from multiple subnets and routing in IPv6. Ideally, residential networks would be given an address range of a /48 or /56 such that multiple /64 subnets could be used within the residence.

*Address space conservation*

Despite the large IPv6 address space, which enables easier subnetting, it is still important to ensure an efficient use of this resource. Some addressing schemes, while facilitating aggregation and management, could lead to significant numbers of addresses being unused. Address conservation requirements are less stringent in IPv6, but they should still be observed.

The proposed Host-Density (HD) value for IPv6 is 0.94, compared to the current value of 0.96 for IPv4. It should be noted that, with IPv6, HD is calculated for sites (e.g. on a basis of /56), instead of for addresses (as is the case with IPv4).

► *Subnet prefix considerations*

An important part of an IPv4 addressing plan is deciding the length of each subnet prefix. Unlike IPv4, the IPv6 addressing architecture specifies that all subnets using Globally Unique Addresses and ULAs always have the same prefix length, of 64 bits.

The only exceptions to this rule are special addresses starting with the binary value 000, such as IPv4-compatible IPv6 addresses. Using a subnet prefix length other than a /64 will break many features of IPv6, including neighbour discovery (ND), secure neighbour discovery (SEND), privacy extensions, parts of mobile IPv6, protocol independent multicast – sparse mode (PIM-SM) with Embedded-RP, and site multihoming by IPv6 Intermediation (SHIM6), among others. A number of other features currently in development, or being proposed, also rely on /64 subnet prefixes.

In some scenarios, prefixes longer than /64 may be used for links connecting routers – usually just two routers on a point-to-point link. On links where all the addresses are assigned by manual configuration, and all nodes on the link are routers (not end hosts) that are known by the network, administrators do not need any of the IPv6 features that rely on /64 subnet prefixes. Using subnet prefixes longer than /64 is not recommended for general use, and using them for links containing end hosts would be highly problematic, as it is difficult to predict what IPv6 features the hosts will use in the future.

Using /64 subnets is strongly recommended, also for links connecting only routers. A deployment that is compliant with the current IPv6 specifications cannot use other prefix lengths.

► *Considerations for /64 prefixes*

When using a /64 subnet length, the address assignment for these addresses can be made by manual configuration, by a Dynamic Host Configuration Protocol, by stateless autoconfiguration, or by a combination thereof. Note that RFC 3177 strongly prescribes 64-bit subnets for general use, and stateless autoconfiguration on most link layers (including Ethernet) is only defined for 64-bit subnets. While, in theory, it might be possible for some future autoconfiguration mechanisms to allow the use of prefix lengths of more than 64 bits, the use of such prefixes is not recommended at this time.

► *Allocation of the IID of an IPv6 address*

In order to have a complete IPv6 address, an interface must be associated with a prefix and an interface identifier (IID).

There are various ways to allocate an IPv6 address to a device or interface. The option with the fewest caveats for the network administrator is that of addresses based on EUI-64. For manual or dynamic options, the overlap with well-known IPv6 addresses should be avoided.

► *Automatic EUI-64 format option*

When using this method, the network administrator has to allocate a valid 64-bit subnet prefix. Once that allocation has been made, the EUI-64 allocation procedure can assign the remaining 64 IID bits in a stateless manner. All the considerations for selecting a valid IID have been incorporated into the EUI-64 methodology.

## A.4 IPv6 security considerations

The transition from a pure IPv4 network to a network where IPv4 and IPv6 co-exist raises a number of extra security considerations that need to be taken into account when deploying IPv6 and operating the dual-protocol network with its associated transition mechanisms. An overview of the various IPv6 security issues is provided below, under the following three headings:

- issues due to the IPv6 protocol itself
- issues due to transition mechanisms
- issues due to IPv6 deployment.

As IPv6 is adopted across organisations, the deployments are unlikely to be replacing IPv4 with IPv6, but instead will be adding IPv6 to be operated in parallel with IPv4 over a considerable period, so that security issues with transition mechanisms and dual-stack networks will be of ongoing concern. This extended transition and co-existence period stems primarily from the scale of the current IPv4 network. It is more likely that it will take two or three capital equipment replacement cycles for IPv6 capabilities to spread through the network, and many services will remain available over IPv4 only for a significant period, while others will be offered either just on IPv6, or on both protocols. To maintain current levels of service, enterprises and service providers will need to support IPv4 and IPv6 in parallel for some time.

## A.5 IPv6 protocol-specific issues

There are significant differences between the features of IPv6 and IPv4: some of these specification changes may result in potential security issues. The following specification-related problems have been identified (but this is not necessarily a complete list):

- routing headers and hosts
- Type 2 routing headers for mobile IPv6 and other purposes
- site-scope multicast addresses
- ICMPv6 and multicast
- bogus errored packets in ICMPv6 error messages
- anycast traffic identification and security
- address privacy extensions interact with DDoS defences
- dynamic DNS: stateless address autoconfiguration, privacy extensions, and SEND
- extension headers
  - processing extension headers in middleboxes
  - processing extension header chains
  - unknown headers/destination options and security policy
  - excessive hop-by-hop options
  - misuse of Pad1 and PadN options
  - overuse of router alert option
- fragmentation: reassembly and deep packet inspection
- fragmentation related DoS attacks
- link-local addresses and securing neighbour discovery
- securing router advertisements
- host-to-router load sharing
- mobile IPv6
  - obsolete home address option in mobile IPv6.

Details of the IPv6 protocol-specific security issues and the risk mitigation plans are available in the RFC 4942.

*IPv4-mapped IPv6 addresses*

One example of this is IPv4-mapped IPv6 addresses (::ffff/96): a representation of an IPv4 address as an IPv6 address inside an operating system. Since the original specification, the use of IPv4-mapped addresses has been extended to a transition mechanism, stateless IP/ICMP translation algorithm (SIIT), where they are potentially used in the addresses of packets on the wire.

Therefore, it becomes difficult to unambiguously discern whether an IPv4 mapped address is really an IPv4 address represented in the IPv6 address format (basic API behaviour), *or* an IPv6 address received from the wire (which may be subject to address forgery etc.) (SIIT behaviour). There are a number of security issues that arise from the ambiguous behaviour when IPv4-mapped addresses are used on the wire:

- If an attacker transmits an IPv6 packet with ::ffff:127.0.0.1 in the IPv6 source address field, he might be able to bypass a node's access controls by deceiving applications into believing that the packet is from the node itself (specifically, the IPv4 loopback address, 127.0.0.1). The same attack might be performed using the node's IPv4 interface address instead.
- If an attacker transmits an IPv6 packet with IPv4-mapped addresses in the IPv6 destination address field corresponding to IPv4 addresses inside a site's security perimeter (e.g. ::ffff: 10.1.1.1), he might be able to bypass IPv4 packet filtering rules and traverse a site's firewall.
- If an attacker transmits an IPv6 packet with IPv4-mapped addresses in the IPv6 source and destination fields to a protocol that swaps IPv6 source and destination addresses, he might be able to use a node as a proxy for certain types of attack.

*Increased end-to-end transparency*

One of the major design aims of IPv6 has been to maintain the original IP architectural concept of end-to-end transparency. Transparency can help foster technological innovation in areas such as peer-to-peer communication, but maintaining the security of the network at the same time requires some modifications to the network architecture.

► *IPv6 networks without NATs*

The necessity of introducing network address translators (NATs) into IPv4 networks, resulting from a shortage of IPv4 addresses, has removed the end-to-end transparency of most IPv4 connections: the use of IPv6 would restore this transparency. However, the use of NATs, and the associated private addressing schemes, has become inappropriately linked to the provision of security in enterprise networks. The restored end-to-end transparency of IPv6 networks can therefore be seen as a threat by poorly informed enterprise network managers. Some seem to want to limit the end-to-end capabilities of IPv6, for example by deploying private, local addressing and translators, even when it is not necessary, because of the abundance of IPv6 addresses.

The details of how to design an IPv6 network to meet the perceived security and connectivity requirements implicit in the current usage of IPv4 NATs, whilst maintaining the advantages of IPv6 end-to-end transparency, are described in 'IP Version 6 Network Architecture Protection' – RFC4864.

*Enterprise network security model for IPv6*

The favoured model for enterprise network security in IPv4 stresses the use of a security perimeter policed by autonomous firewalls and incorporating the NATs. Both perimeter firewalls and NATs introduce asymmetry and reduce the transparency of communications through these perimeters. The symmetric bi-directionality and transparency that are extolled as virtues of IPv6 may seem to be at odds with this model. Consequently, network managers may even see them as undesirable attributes, in conflict with their need to control threats to, and attacks on, the networks they administer.

It is worth noting that IPv6 does not *require* end-to-end connectivity. It merely provides end-to-end addressability; the connectivity can still be controlled using firewalls (or other mechanisms), and it is indeed wise to do so.

A number of matters indicate that IPv6 networks should migrate towards an improved security model, which will increase the overall security of the network, while at the same time facilitating end-to-end communication:

- **Increased usage of end-to-end security**, especially at the network layer. IPv6 mandates the provision of IPsec capability in all nodes, and increasing use of end-to-end security is a challenge to current autonomous firewalls that are unable to perform deep packet inspection on encrypted packets. It is also incompatible with NATs because they modify the packets, even when packets are only authenticated rather than encrypted.

- **Acknowledgement that over-reliance on the perimeter model is potentially dangerous**. An attacker who can penetrate today's perimeters will have free rein within the perimeter, in many cases. Also, a successful attack will generally allow the attacker to capture information or resources and make use of them.

- **Development of mechanisms such as 'Trusted Computing'** that will increase the level of trust that network managers are able to place on hosts.

- **Development of centralised security policy repositories and secure distribution mechanisms** that, in conjunction with trusted hosts, will allow network managers to place more reliance on security mechanisms at the end points. The mechanisms are likely to include end-node firewalling and intrusion detection systems, as well as secure protocols that allow end points to influence the behaviour of perimeter security devices.

- **Review of the role of perimeter devices**, with increased emphasis on intrusion detection, and network resource protection and co-ordination to thwart distributed denial-of-service attacks.

Several of the technologies required to support an enhanced security model are still under development, including secure protocols to allow end points to control firewalls: the complete security model using these technologies is now emerging, but still requires some development.

Initial deployments will need to make use of similar firewalling and intrusion detection techniques to IPv4 that may limit end-to-end transparency temporarily, but users should be prepared to use any new security model as it develops, and avoid the need for the use of NATs by the use of suitable the architectural techniques. In particular, using NAT-PT as a general-purpose transition mechanism should be avoided, as it is likely to limit the Integrity of end-to-end security and other IPv6 capabilities in the future.

## A.6 Tunnelling

### A.6.1 IPv6 in IPv6 tunnels

IPv6 in IPv6 tunnels can be used to circumvent security checks, so it is essential to filter packets both at tunnel ingress and egress points (the encapsulator and decapsulator) to ensure that both the inner and outer addresses are acceptable, and the tunnel is not being used to carry inappropriate traffic.

### A.6.2 Tunnelling and security

The more complicated the IPv6 transition/co-existence becomes, the greater the danger that security issues will be introduced, either:

- in the mechanisms themselves, or
- in the interaction between mechanisms, or
- by introducing unsecured paths through multiple mechanisms.

These issues may or may not be readily apparent. Hence, it would be desirable to keep the mechanisms simple (as few in number as possible and built from pieces as small as possible) to simplify analysis. One case where such security issues have been analysed in detail is the 6to4 tunnelling mechanism.

As tunnelling has been proposed as a model for several more cases than are currently being used, its security properties should be analysed in more detail. There are some generic dangers associated with tunnelling:

- It may be easier to avoid ingress filtering checks.

- It is possible to attack the tunnel interface: several IPv6 security mechanisms depend on checking that the hop limit equals 255 on receipt, and that link-local addresses are used. Sending such packets to the tunnel interface is much easier than gaining access to a physical segment and sending them there.

- Automatic tunnelling mechanisms are typically particularly dangerous, as there is no pre-configured association between end points. Accordingly, at the receiving end of the tunnel, packets have to be accepted and decapsulated from any source.

Consequently, special care should be taken when specifying automatic tunnelling techniques.

*Tunnelling IPv6 through IPv4 networks may break IPv4 network security assumptions*

NATs and firewalls have been deployed extensively in the IPv4 Internet; operators who deploy them typically have some security/operational requirements in mind (e.g. a desire to block inbound connection attempts), which may, or may not, be misguided.

The addition of tunnelling can change the security model that such deployments are seeking to enforce. IPv6-over-IPv4 tunnelling using protocol 41 is typically either explicitly allowed, or implicitly disallowed. Tunnelling IPv6 over IPv4 encapsulated in UDP constitutes a more difficult problem, as UDP must usually be allowed to pass through NATs and firewalls. Consequently, using UDP implies the ability to punch holes in NATs and firewalls, although, depending on the implementation, this ability may be limited, or only achieved in a stateful manner. In practice, the mechanisms have been explicitly designed to traverse both NATs and firewalls in a similar fashion. One possible view is that the use of tunnelling is especially questionable in home and SOHO (small office/home office) environments, where the level of expertise in network administration is typically not very high; in these environments, the hosts may not be as tightly managed as in others (e.g. network services might be enabled unnecessarily), leading to possible security break-ins or other vulnerabilities.

Holes allowing tunnelled traffic through NATs and firewalls can be punched both intentionally and unintentionally. In cases where the administrator or user makes an explicit decision to create the hole, this is less of a problem, although (for example) some enterprises might want to block IPv6 tunnelling explicitly if employees were able to create such holes without reference to administrators. On the other hand, if a hole is punched transparently, it is likely that a proportion of users will not understand the consequences: and sooner or later this will very probably result in a serious threat.

When deploying tunnelling solutions, especially tunnelling solutions that are automatic and/or can be enabled easily by users who do not understand the consequences, care should be taken not to compromise the security assumptions held by the users.

It is relatively easy to determine the IPv6 address corresponding to an IPv4 address in tunnelling deployments. It is therefore vital not to rely on ‘security by obscurity’, i.e. assuming that nobody is able to guess or determine the IPv6 address of the host, especially when using automatic tunnelling transition mechanisms.

The network architecture must provide separate IPv4 and IPv6 firewalls, with tunnelled IPv6 traffic arriving encapsulated in IPv4 packets routed through the IPv4 firewall before being decapsulated, and then through the IPv6 firewall.

### A.6.3 Automatic tunnelling and relays

Two mechanisms have been specified that use automatic tunnelling and are intended for use outside a single domain. These mechanisms encapsulate the IPv6 packet directly in an IPv4 packet (in the case of 6to4) or in an IPv4 UDP packet (in the case of Teredo). In either case, packets can be sent and received by any similarly equipped nodes in the IPv4 Internet.

A major vulnerability of such approaches is that receiving nodes must allow decapsulation of traffic sourced from anywhere in the Internet. This kind of decapsulation function must be extremely well secured because of the wide range of potential sources.

An even more difficult problem is how these mechanisms are able to establish communication with native IPv6 nodes or between the automatic tunnelling mechanisms: such connectivity requires the use of some kind of 'relay'. These relays could be deployed in various locations such as:

- all native IPv6 nodes
- native IPv6 sites
- in IPv6-enabled Internet service providers, or
- just somewhere on the Internet.

Given that a relay needs to trust all the sources (e.g. in the 6to4 case, all 6to4 routers) that are sending it traffic, there are issues in achieving this trust, and at the same time scaling the relay system to avoid overloading a small number of relays. As authentication of such a relay service is very difficult to achieve, and particularly so in some of the possible deployment models, relays provide a potential vehicle for address spoofing (reflected) denial-of-service attacks, and other threats. Threats related to 6to4, and measures to combat them, are discussed in RFC3964, and threats related to Teredo, and measures to combat them, are discussed in RFC4380.

# Annex B: Transition mechanism design considerations

## B.1 Key principles for an IPv6 adoption architecture

In general, there are a few principles which should be considered when developing the architecture for an IPv6 adoption solution, and when identifying the mechanisms to be used. These should be taken into consideration when addressing the services to be deployed, the network, and the applications to be used on that network. The key principles include:

- security
- simplicity
- robustness.

*Security*: the architecture for IPv6-enabled services over an IPv6-enabled network (and the associated transition mechanisms) must not expose the services and network to significant security threats, because these may make customers and internal stakeholders hesitant to start the transition.

*Simplicity*: this includes the overall simplicity of the transition architecture (where a limited set of mechanisms or operational practices should be used that have clear uses, and which address different, clearly defined, problems) and of the transition mechanisms themselves. Simple systems have the tendency to work well, even under unexpected circumstances, and are less prone to problems with, for example, security and robustness. If complex systems are essential, it is preferable to build these from a set of simple building blocks.

*Robustness*: both the mechanisms and the architecture for the transition to IPv6 must be reliable and robust to encourage adoption. The IPv6 and the dual IPv4/6 architecture must be no less robust than the IPv4-only architecture. For example, there are some IPv4 components (for example, NATs) that are not always reliable. The success of IPv4/6 must not be dependent on how these mechanisms perform, as creating such a dependency could easily transfer these problems of IPv4 to IPv6, which would have a negative impact on the reliability and usefulness of IPv6 as a whole.

## B.2 Network transition scenarios for an Internet service provider

### B.2.1 Core network

The core network of an Internet service provider/large organisation is composed of high-speed routers forming the core, along with provider edge routers. The provider edge routers peer with other neighbouring networks and network service providers, along with implementing routing policy and security policy functions.

As IPv6 adoption is planned across the core network of a service provider, the key strategies used must ensure that the networks are upgraded in an incremental manner, with little, to no, disruption to the current IPv4 services. The various IPv6 transition mechanisms, which can be used by a service provider are:

- tunnelling – carrying of IPv6 traffic over the IPv4 network
- dedicated IPv6 links
- dual-stack (IPv4 and IPv6) – throughout the network, from all edges through the core.

The business service offerings planned and the current state of the network design, are the key drivers towards choosing the appropriate IPv6 transition mechanism.

A set of various IPv6 adoption/deployment strategies, with the details of the scenario, benefits and limitations are detailed below. An Internet service provider can choose one of the stated approaches as it proceeds towards IPv6 adoption.

| *Scenarios* | *IPv6 deployment strategy* | *IPv6 transition mechanisms* | *Benefits* | *Challenges* |
|---|---|---|---|---|
| Currently IPv4 network – offer initial IPv6 service or interconnect IPv6 islands or link to remote IPv6 networks | IPv6 over IPv4 tunnels | • Manually configured tunnels – generic routing encapsulation (GRE) tunnels<br>• Semi-automatic tunnel mechanisms – tunnel broker services<br>• Fully automatic tunnel mechanisms – IPv4-compatible and 6–4 | Minimal cost and minimal risk<br>Easy to implement | Usage of tunnelling mechanisms leads to challenges in management and diagnostics |
| Backbone network – deploying MPLS (isolated IPv6 domains to communicate with each other, over IPv4 backbone) | IPv6 over MPLS backbones | • IPv6 on the provider edge routers<br>• IPv6 tunnels on the provider edge routers<br>• IPv6 over a circuit transport over MPLS | Minimal upgrade of hardware or software | Network management challenges |

| | | | | |
|---|---|---|---|---|
| Backbone network – deploying ATM, Frame Relay, or dWDM (establish communication between IPv6 domains) | IPv6 over dedicated data links | • IPv6 using separate Frame Relay PVC or ATM PVCs separate optical links | Minimal impact on current IPv4 services<br>Seamless end-to-end IPv6 services | Challenges in network management |
| Small networks (IPv4 and IPv6 applications to co-exist) | IPv6 using dual-stack network | • Router in the network are upgraded to be dual-stack | Seamless availability of IPv4 and IPv6 services | Challenges in network management and diagnostics |

*Figure B.1: Summary core network transition scenarios [Source: Analysys Mason]*

The IPv6 adoption strategy for an Internet service provider differs based on its current state. In the case of an existing service provider offering IPv4 services, one of the preferred approaches would be using IPv6 in IPv4 tunnels; here the IPv6 services can be rolled out at the earliest with minimal investment.

The service providers that are running their WAN using either Frame Relay, ATM, dWDM or similar technologies, can use an IPv6 adoption strategy comprising using separate PVC or parallel channels of communication for IPv6 and IPv4.

The service providers that are currently running MPLS backbones, or any of the greenfield service providers, can adopt IPv6 by running IPv6 over MPLS using either tunnels, 6PE or 6vPE mechanisms.

The service providers that have a small network can adopt IPv6 by way of using the dual-stack approach – this is easy to implement.

### B.2.2 Access network

Broadband access networks are networks which carry multi-service traffic comprising of audio, video and data for end consumers. The broadband network deployments provide Internet access to subscribers and also aggregates the subscriber traffic, which is interfaced to the service provider at Layer 2 or 3.

As the Internet service providers plan to roll out IPv6 services across their network, the initial starting state is IPv4 only. The service provider can plan to replicate the IPv4 services in the IPv6 environment and offer them to the customer, or launch new IPv6 services (multicast, VoIP, etc.) *in addition* to the current IPv4 services. The IPv6 adoption scenarios and adoption/deployment strategy would vary according to which services were being offered, as shown in the high-level summary in Figure B.2.

| *Scenario* | *IPv6 adoption strategy/model* |
|---|---|
| IPv6 service offering a replica of IPv4 service offerings | • Point-to-point model<br>• PPP terminated aggregation (PTA) model<br>• L2TP access aggregation (LAA) model |
| New IPv6 service offerings *in addition* to IPv4 service offerings | Hybrid model for IPv4 and IPv6 service:<br>• IPv4 in LAA Model and IPv6 in PTA Model<br>• IPv4 in LAA model and IPv6 in modified point-to-point model |

*Figure B.2: Broadband network IPv6 adoption model [Source: Analysys Mason]*

The above scenarios and models are applicable to broadband cable, broadband DSL, and broadband FTTx/Ethernet providers, as explained further in the following sub-sections.

### *Broadband cable networks*

The broadband cable networks today primarily run on DOCSIS standards based networks. The DOCSIS 2.0 and prior specifications do not support native IPv6 transport. In light of the same, the IPv6 deployment scenarios for the existing cable networks are tunnel based. The DOCSIS 3.0 specification supports native IPv6 transport; the cable service providers, who are adopting DOCSIS 3.0, can progress towards seamless IPv6 adoption. There are two different deployment modes in current cable networks, wherein IPv6 adoption can be planned. These are outlined below, and addressed in the following figures.

- **Bridged CMTS environment**: in this scenario, both the cable modem (CM) and cable modem termination system (CMTS) bridge all data traffic. Traffic to/from host devices is forwarded through the cable network to the edge router (ER). The ER then routes traffic through the Internet service provider network to the Internet. The CM and CMTS support a certain degree of Layer 3 functionality for management purposes.
- **Routed CMTS environment**: in a routed network, the CMTS forwards IP traffic to/from hosts based on Layer 3 information using the IP source/destination address. The CM acts as a Layer 2 bridge for forwarding data traffic and supports some Layer 3 functionality for management purposes.

| *Scenario* | *Devices to be upgraded to support IPv6* | *Addressing* | *Data forwarding* | *routing* |
|---|---|---|---|---|
| *IPv6 tunnel scenarios* | | | | |
| CM and the CMTS operate in an IPv4 environment | • The host<br>• The edge router | At customer site only the host is required to be assigned IPv6 address | All IPv6 traffic will be sent to/from the edge router and the host device using one of the IPv6-in-IPv4 tunnelling mechanisms | routing configuration on the host will vary depending on the tunnelling technique used |
| CM and the CMTS operate in an IPv4 environment | • The host<br>• The gateway router<br>• The edge router | At customer site the devices which need to be assigned IPv6 address are the host and gateway router | All IPv6 traffic will be sent to/from the edge router and the gateway router, using one of the available IPv6-in-IPv4 tunnelling mechanisms | Based on the tunnelling technique used, routing configuration is adapted across the gateway router and edge router |
| *Native IPv6 scenarios* | | | | |
| CM and the CMTS bridge all data traffic supporting native IPv6 unicast and multicast traffic | The following devices need to be upgraded to dual-stack:<br>• edge router<br>• gateway router<br>• host device | IPv6 address must be provisioned for – the CM, the gateway router and the host device | The CM and CMTS must be able to bridge native IPv6 unicast and multicast traffic | The hosts install a default route that points to the edge router or the gateway router |

*Figure B.3: Summary of bridged CMTS network IPv6 transition scenarios [Source: IETF]*

| *Scenario* | *Devices to be upgraded to support IPv6* | *Addressing* | *Data forwarding* | *routing* |
|---|---|---|---|---|
| IPv4 cable network<br>IPv6 tunnel is running between host and the edge router | • The host<br>• The edge router | At customer site only the host is required to be assigned IPv6 address | All IPv6 traffic will be sent to/from the edge router and the host device using one of the IPv6 in IPv4 tunnelling mechanisms | routing configuration on the host will vary depending on the tunnelling technique used |

| | | | | |
|---|---|---|---|---|
| IPv4 cable network with gateway router at customer site | • The host<br>• The edge router<br>• The gateway router | At customer site the devices which need to be assigned IPv6 address are the host and gateway router | All IPv6 traffic will be sent to/from the edge router and the gateway router, using an available IPv6-in-IPv4 tunnelling mechanism | Based on the tunnelling technique used, routing configuration is adapted across the gateway router and edge router |
| Dual-stacked cable network with IPv6 support for CM and CMTS | • The CM<br>• The CMTS | The CM and host are assigned IPv6 address via DHCPv6 or stateless auto-configuration | All IPv6 traffic will be sent to/from the CMTS and hosts | No routing protocols are needed between the CMTS and the host since the CM and host are directly connected to the CMTS cable interface |
| Dual-stacked cable network with IPv6 support for standalone gateway router and CMTS | • The CMTS<br>• The gateway router | At customer site the devices which need to be assigned IPv6 address are the host and gateway router | All IPv6 traffic will be sent to/from the CMTS and hosts | Based on the tunnelling technique used, routing configuration is adapted across the gateway router and edge router |
| Dual-stacked cable network with IPv6 support for embedded gateway router/CM and CMTS | • The CM<br>• The CMTS<br>• The gateway router | IPv6 address assignment for the CM/GWR and host can be done via DHCPv6 or DHCP-PD | The CM/GWR will forward all IPv6 traffic to/from the CMTS/ER and hosts | The CM/GWR can use a static default route pointing to the CMTS/ER or it can run a routing protocol such as RIPng or OSPFv3 between itself and the CMTS |

*Figure B.4: Summary routed CMTS network IPv6 transition scenarios [Source: IETF]*

### *Broadband DSL networks and FTTx/Ethernet networks*

Digital subscriber line (DSL) broadband services provide users with IP connectivity over the existing twisted-pair telephone lines called the local loop. A wide range of bandwidth offerings is available, depending on the quality of the line and the distance between the customer premises equipment and the DSLAM.

In environments that support the infrastructure deploying fibre-to-the-home (FTTH) or Ethernet service to subscribers, 10/100Mbit/s Ethernet broadband services can be provided. Such services are generally available in metropolitan areas, in multi-tenant buildings where an Ethernet infrastructure can be deployed in a cost-effective manner. In such environments Metro-Ethernet services can be used to provide aggregation and uplink to a service provider.

In the scenario that the broadband DSL or FTTx/Ethernet providers are planning to adopt IPv6 in their current IPv4 networks, and replicate the IPv4 services towards the IPv6 services being offered, there are three main design approaches to providing IPv4 connectivity over a DSL infrastructure:

- point-to-point model
- PPP terminated aggregation (PTA) model
- L2TP access aggregation (LAA) model.

In the scenario that the DSL or FTTx/Ethernet broadband provider is planning to launch new IPv6 based services in addition to the current IPv4 services currently offered then hybrid IPv4-IPv6 models are to be adopted, these are:

- IPv4 in LAA model and IPv6 in PTA model
- IPv4 in LAA model and IPv6 in modified point-to-point model.

The details of the IPv6 transition scenarios for a broadband FTTx/Ethernet or DSL provider which is planning to replicate the IPv4 services and roll out IPv6 services accordingly are shown in Figure B.5. The details of the changes to the infrastructure, addressing and routing are also summarised.

| *Scenario* | *Infrastructure changes* | *Addressing* | *routing* |
|---|---|---|---|
| Point-to-point model | • The host<br>• The customer router (if present)<br>• The edge router | Hosts can use stateless auto-configuration or stateful DHCPv6 based configuration to acquire an address via the edge router<br>In the case of FTTx/Ethernet, customer router can dynamically acquire through stateless auto-configuration the IPv6 prefix for the link between itself and the edge router<br>In the case of DSL, DNS, is provided through stateful and stateless DHCPv6 | CPE devices are configured with a default route that points to the edge router |
| PPP terminated aggregation (PTA) model | • The host<br>• The customer router (if present)<br>• The BRAS<br>• The edge router | BRAS terminates the PPP sessions, and provides the subscriber with an IPv6 address from the defined pool for that profile | CPE devices are configured with a default route that points to the BRAS router |
| L2TP access aggregation (LAA) model | • The host<br>• The customer router<br>• The edge router | Edge router terminates the PPP sessions, and provides the subscriber with an IPv6 address from the defined pool for that profile | CPE devices are configured with a default route that points to the Edge router that terminates the PPP sessions |

*Figure B.5: Summary of DSL and FTTx/Ethernet network IPv6 transition scenarios [Source: IETF]*

► *Point-to-point model for DSL and FTTx/Ethernet networks*

Each subscriber connects to the DSLAM over a twisted pair (in the case of DSL), or to the network access switch over RJ-45 or fibre links (in the case of FTTx/Ethernet). In the case of DSL, they are then provided with a unique PVC that links it to the service provider. In the case of FTTx/Ethernet, each subscriber is provided with a unique VLAN on the access switch. The PVCs/VLANs can be terminated at the BRAS or at the edge router.

This DSL design is not very scalable if the PVCs are not terminated as close as possible to the DSLAM (at the BRAS), as a large number of Layer 2 circuits has to be maintained over a significant portion of the network. For FTTx/Ethernet networks, the VLANs are 802.1Q trunked to the Layer 3 device (BRAS) or the edge router.

The Layer 2 domains (for DSL) can be terminated at the edge router in three ways:

- in a common bridge group with a virtual interface that routes traffic out
- by enabling a routed bridged encapsulation feature, all users could be part of the same subnet – this is the most common deployment approach of IPv4 over DSL, but it might not be the best choice in IPv6, where address availability is not an issue
- by terminating the PVC at Layer 3, each PVC has its own prefix – this is the approach that seems more suitable for IPv6.

In this IPv6 adoption model, the host, customer router and the edge router are to be upgraded to support IPv6. The host and the customer router are to be provisioned with IPv6 address at the customer site; the host can acquire IPv6 address via DHCPv6 or stateless auto-configuration, and the customer router can acquire IPv6 address using stateless auto-configuration method. The CPEs are configured with a default route pointing to the edge router.

► *PTA model for DSL and FTTx/Ethernet networks*

PPP sessions are opened between each subscriber and the BRAS. The BRAS terminates the PPP sessions and provides Layer 3 connectivity between the subscriber and the Internet service provider.

In this IPv6 adoption model, the host, customer router, the BRAS and the edge router are to be upgraded to support IPv6. The BRAS router terminates the PPP sessions, and provides the subscriber with an IPv6 address from the defined pool for that profile. The CPE's are configured with a default route pointing to the BRAS router.

► *LAA model for DSL and FTTx/Ethernet networks*

PPP sessions are opened between each subscriber and the Internet service provider edge router/termination devices. The BRAS tunnels the subscriber PPP sessions to the Internet service provider by encapsulating them into L2TPv2 tunnels.

In aggregation models the BRAS terminates the subscriber PVCs and aggregates their connections before providing access to the Internet service provider. In order to maintain the deployment concepts and business models proven and used with existing revenue-generating IPv4 services, the IPv6 deployment will match the IPv4 one.

In this IPv6 adoption model, the host, customer router and the edge router are to be upgraded to support IPv6. The edge router terminates the PPP sessions, and provides the subscriber with an IPv6 address from the defined pool for that profile. The CPEs are configured with a default route pointing to the edge router.

► *Hybrid model for IPv4 and IPv6 service for DSL and FTTx/Ethernet networks*

In the scenario when the broadband DSL and FTTx/Ethernet service provider plans to expand its service offering with the new IPv6 deployed infrastructure, the current IPv4 based network design may not support the implementation of the same. An example of such circumstances is if the provider decides to offer multicast services over such a design, it will face the problem of overuse of NAP resources. The multicast traffic can be replicated only at the end of the tunnels by the edge router, and the copies for all the subscribers are carried over the entire NAP.

A modified point-to-point or PTA model are more suitable to support multicast services because the packet replication can be done closer to the destination at the BRAS. Such topology saves NAP resources.

The IPv6 deployment can be viewed as an opportunity to build an infrastructure that might better support the expansion of services.

# Annex C: IPv6 certification or compliance measurement programmes

As the various stakeholders across the ICT ecosystem move towards IPv6 adoption, a mechanism such as certification to measure the maturity of IPv6 adoption will have many benefits. These include:

- providing Internet service providers with an IPv6 goal that they can work towards
- creating a means of publicity and providing information to customers about the availability of IPv6-ready services
- providing a guide for users when choosing their respective Internet service provider for IPv6 services
- giving confidence to users that a standards-based approach has been taken by their Internet service provider.

IPv6 certification programmes or IPv6 compliance measurement processes ensure that critical infrastructure components, such as autonomous systems, routing tables, DNSv6 entries, WWW infrastructure, IPv6 services, and so forth, are IPv6 enabled to a known standard. These programmes comprise a self-verification process and automated scripts which verify and validate the IPv6 compliance of the requesting organisation.

The various IPv6 certification or IPv6 compliance measurement programmes available globally are summarised in Figure C.1.

| *IPv6 certification agency / compliance measurement programme* | *Certification* | *Aspects measured* |
|---|---|---|
| IPv6 Forum | IPv6-enabled Internet service provider logo (basic level) | • Verify autonomous system IPv6 enablement<br>• Verify IPv6 prefix assignment/allocation<br>• Verify IPv6 reachability |
| IPv6 Forum | IPv6-enabled WWW logo | • IPv6 DNS resolving ability<br>• IPv6 HTTP accessibility<br>• IPv6 HTTP maintenance ability |
| RIPE NCC | IPv6 Ripeness | • The Internet service provider has an IPv6 allocation<br>• The address prefix is actually routed on the Internet<br>• A route6 object is registered in the RIPE Database<br>• Reverse DNS has been set up |
| SixXS | IPv6 -enabled service provider | • Self-assessment guidelines<br>• IPv6 DNS registration – whether it is possible to register an AAAA record with the provider's DNS<br>• DNS via IPv6 – whether the DNS server is IPv6 accessible<br>• IPv6 website – whether the provider's web server is IPv6 accessible<br>• IPv4 for customers – whether a customer can get an IPv4 address for their subnet<br>• IPv6 for customers – whether a customer can get an IPv6 address for their subnet |
| Hurricane Electric | Hurricane Electric IPv6 certification | • Verify that you have IPv6 connectivity<br>• Verify that you have a working IPv6 web server<br>• Verify that you have a working IPv6 email address<br>• Verify that you have working forward IPv6 DNS<br>• Verify that you have working reverse IPv6 DNS for your mail server<br>• Verify that you have name servers with IPv6 addresses that can respond to queries via IPv6 |

*Figure C.1: IPv6 compliance certification bodies [Source: Analysys Mason, Tech Mahindra]*

Further details on each of the programmes listed above are given in the rest of this annex.

## C.1 IPv6 Forum: IPv6-enabled Logo Programme

The objective of the IPv6 Forum's IPv6-enabled Logo Programme is to increase user confidence by demonstrating that IPv6 is available and ready to be used now.

The IPv6 Forum IPv6-enabled Logo Programme currently consists of two sub-programmes:

- IPv6-enabled Internet service provider Logo Programme
- IPv6-enabled WWW Logo Programme.

### C.1.1 IPv6-enabled Internet service provider Logo Programme

This certification programme consists of two certification levels – Basic and Advanced. As of the time of writing, the advanced level certification programme was still in the process of being defined.

The basic level validation programme consists of self-validation of services through running an automated script. If the applying Internet service provider is able to successfully run the script, it is assigned a logo ID and is listed on the IPv6 Forum's website as an 'IPv6-enabled Internet service provider'. The various aspects measured include:

- network accessibility
- active IPv6 addressability
- persistence of IPv6 service.

Details on how to apply are available on the IPv6 Forum's website.

### C.1.2 IPv6-enabled WWW Logo Programme

WWW is one of the most widely used applications of Internet at present. IPv6-enabled websites have already appeared. The IPv6-enabled WWW Logo Programme objective is to encourage adoption of IPv6 in helping website owners to test and check their proper IPv6 enablement. The various aspects measured under this programme are as follows:

- IPv6 DNS resolving ability
- IPv6 HTTP accessibility
- IPv6 HTTP maintenance ability.

Details on how to apply are available on the IPv6 Forum's website.

## C.2 RIPE: IPv6 ripeness

The IPv6 ripeness programme was conducted by the RIPE NCC in each service region (Europe, the Middle East and parts of Asia) that had at least five Internet service providers. Each Internet service provider received a rating ranging from zero to four stars. Each of the Internet service providers was measured on its IPv6 readiness, with readiness across all Internet service providers in a country aggregate to measure the respective country's overall state of IPv6 readiness.

This is a self-assessment programme, and the guidelines for assessing IPv6 readiness are provided to an organisation which can verify its compliance against them.

The self-assessment measurement is based on:

- whether the Internet service provider has an IPv6 allocation
- whether the address prefix is actually routed on the Internet
- whether a route6 object is registered in the RIPE Database
- whether reverse DNS has been set up.

An organisation can award itself a star for each item with which it is compliant.

## C.3 SixXS: IPv6-enabled service provider

The SixXS web site lists various Internet service providers across the globe that are able to provide native IPv6 support to their customers. SixXS provides a set of self-assessment guidelines for Internet service providers to validate their IPv6 readiness.

An Internet service provider interested in listing itself as an IPv6-enabled service provider can conduct a self-assessment based on the following guidelines:

- IPv6 DNS registration – whether it is possible to register an AAAA record with the provider's DNS
- DNS via IPv6 – whether the DNS server is IPv6 accessible
- IPv6 website – whether the provider's web server is IPv6 accessible
- IPv4 for customers – whether a customer can get an IPv4 address for their subnet
- IPv6 for customers – whether a customer can get an IPv6 address for their subnet.

Once an Internet service provider has validated that it is compliant to all the above criteria, it can request SixXS to list it as an IPv6-enabled service provider.

## C.4 Hurricane Electric: IPv6 certification

The Hurricane Electric IPv6 certification programme helps an organisation to verify that its critical organisational infrastructure is IPv6 enabled. The various aspects that are measured under this certification programme are that an organisation has:

- IPv6 connectivity
- availability of an IPv6 web server
- availability of an IPv6 email address
- a working forward IPv6 DNS
- a working reverse IPv6 DNS for your mail server
- name servers with IPv6 addresses that can respond to queries via IPv6.

Finally, an organisation is required to prove its knowledge of IPv6 technologies through a test.