The Regulatory Authority

The Ministry of Information and Communications Technology

('ictQATAR')

IPv6 Implementation Strategy for the State of Qatar

January 2014

Table of Contents

1 Introduction

1.1 The Importance of the Internet Protocol

The Internet Protocol (IP) is the global *de facto* Layer 3 standard for data networks. It allows traffic to traverse both the World Wide Web and private networks by routeing data from source to destination using an IP address. The dependency on such networks to support modern society cannot be over emphasised, with applications ranging from email and Web browsing through to sophisticated government and enterprise networks all relying on IP as the underlying protocol.

By their very nature, public IP addresses need to be unique on a global basis, and therefore the allocation of addresses must also be managed on a global basis to avoid the inadvertent duplication of address allocations. This function is undertaken by the Internet Assigned Numbers Authority (IANA) which allocates IP addresses to the four regional bodies which then have responsibility for distributing these to their respective regions.

The current version of IP, termed IPv4, was specified in the 1970s; at that time, the explosive growth in the Internet and IP-based networks in general could not have been anticipated. As a consequence the available pool of 2^{32} addresses has proved to be insufficient, a fact actually identified in the late 1990s, when a new version of IP, termed IPv6, was ratified. IPv6 has a vastly extended range of 2^{128} addresses, and also incorporates a number of other functional enhancements over IPv4. The use of IPv6 did not, however, commence immediately because adequate reserves of IPv4 address remained at the time and, through the use of techniques such as Network Address Translation (NAT), the use of the IPv4 address pool was further extended.

IANA announced in February 2011 that its pool of IPv4 addresses was finally exhausted. Although the IANA IPv4 address exhaustion date has passed without any calamitous results, the date by which Internet service providers (ISPs) or similar bodies can no longer allocate new IPv4 addresses is rapidly approaching.

Despite the recognition that IPv6 will eventually need to be adopted, preparations around the world for the migration from IPv4 have been limited, and this is largely due to the fact that existing users do not see any pressing need for adopting IPv6.

The market's failure to act more quickly can be attributed to:

- A lack of actual deadlines for those involved
- The fact that the current 'work-arounds' of using NAT and Dynamic Host Configuration Protocol (DHCP) have proved adequate to date
- Inadequate promotion of IPv6 to customers by the supply side of the market
- Failure to grasp the benefits of adopting IPv6, and therefore failure to recognise the incentives.

Given the dependency on IP to support many essential activities within modern economies, it is recognised that the shortage of IP addresses will, at some stage, have an adverse impact on economic growth, and in particular the risk exists that countries will fall behind their peer group if they fail to act in a timely manner on IPv6 adoption.

The perceived failure of markets to react with sufficient urgency to addressing the need to commence IPv6 migration activities has led a number of governments worldwide to play an increasingly active role in encouraging IPv6 adoption, and to recognise that intervention is required to minimise the disruption and impact that would otherwise be caused by the global exhaustion of IPv4 addresses.

Governments and regulators may therefore need to encourage the timely and efficient adoption of IPv6 (and a move to the co-existence of IPv4 and IPv6 – known as 'dual stack') and to minimise the impact of the exhaustion of IPv4 addresses on individual stakeholder groups and the consequential impact on their productivity.

In recognition of this, ictQATAR has recently undertaken a study into the state of IPv6 readiness across the State of Qatar's IP ecosystem. The output of this study has been used in the development of this strategic plan for the national implementation of IPv6.

It includes an implementation and adoption roadmap, tasks involved with governance and transition management and the associated budget planning and procurement activities.

ictQATAR believes that the timely adoption of IPv6 by Qatar's ICT ecosystem can best be achieved if it is driven by a focused team dedicated to the task. ictQATAR therefore proposes to spearhead an IPv6 task force. This team will initiate and co-ordinate a number of IPv6-related activities.

During the initial phase of the IPv6 study for the State of Qatar, stakeholders were asked about the role of government and regulators in encouraging the deployment of IPv6 – for themselves and the wider ecosystem. The majority requested that ictQATAR should play a leading role in the planning and adoption of IPv6 on a national level.

1.2 Why IPv6 is important to the State of Qatar?

1.2.1 Maintaining the Development Growth of Qatar

Qatar is a rapidly developing nation in economic, cultural and social terms. To support this development requires an advanced ICT infrastructure capable of meeting the demand this generates and also to act as a catalyst for further development. The resultant growth of demand for IP address space can only be satisfied in the future by introducing IPv6. Furthermore, as Qatar will need to communicate with the rest of world to maintain economic growth, the international adoption of IPv6 means Qatar must also follow suit or it will effectively become isolated from the emerging global IPv6 community, this will affect areas such as ecommerce, education etc.

1.2.2 Alignment with Qatar National Policies

There are two key relevant visionary policies, namely the ictQATAR ICT Vision 2015 and Qatar Vision 2030, which have been identified as being particularly relevant in the context of the migration to IPv6. Both policies have a high dependency on the availability of world-class networks and ICT systems for their successful execution.

In this context, the timely migration to IPv6 will ensure adequate quantities of IP addresses are available and that Qatar is able to connect with the rest of world as IPv6 networks and websites become increasingly prevalent. These two policies are described further below.

ictQATAR ICT Vision 2015

The ictQATAR ICT Vision 2015 was developed to define the areas where ICT-related systems will deliver the aspiration for Qatar to move to a knowledge-based economy. This goal is dealt within Qatar's digital agenda, and its five-year plan. Implicit to delivering this is the ability to expand the ICT ecosystem in Qatar.

Qatar's five-year ICT plan defined the following measurable goals:

- Double the ICT sector's contribution to GDP (USD3 billion)
- Double the ICT workforce (40 000)
- Achieve ubiquitous high-speed broadband access for households and businesses (95%)
- Achieve mass ICT and Internet adoption by all segments of society (90%)
- Achieve wide accessibility and effectiveness of all key government services (160 online services).

It is evident that to deliver the latter four goals will require substantial expansion of the IP ecosystem, with an associated increase in the number of IP addresses required. The availability of adequate IP address capacity is, therefore, of paramount importance to achieve this.

Of the five strategic thrusts identified within ICT Vision 2015 as listed below, it is evident that to deliver the majority will require an adequate supply of IP address capacity given the implicit expansion of connected devices.

- Improving Connectivity – ensuring the deployment of an advanced, secure infrastructure.
- Boosting Capacity – enhancing digital literacy and developing skills to enable innovation.
- Fostering Economic Development – creating an environment for an innovative and vibrant ICT industry.
- Enhancing Public Service Delivery – ensuring the use of innovative applications to improve delivery of public services.
- Advancing Societal Benefits – leveraging ICT to improve the ways society and government provide education, healthcare and services to Qatar's people.

Qatar Vision 2030

The Qatar Vision 2030 encompasses many aspirational aims for Qatar, with a particular emphasis on moving to a knowledge-based economy.

"… to build efficient delivery mechanisms for public services; create a highly skilled and productive labour force; and support the development of entrepreneurship and innovation capabilities. If attained, these achievements would in turn provide a broader platform for the diversification of Qatar's economy and its positioning as a regional hub for knowledge and for high value industrial and service activities."

There is, again, an implicit requirement to provide an ICT infrastructure that can support the delivery of this vision, of which the migration to IPv6 will be a key component.

1.2.3 Support for Qatar 2022 World Cup

The hosting of the 2022 World Cup in Qatar will require a massive increase in IP address capacity to support both broadcast and Internet connectivity associated with the tournament. The extensive use of IPv6 in the 2008 Olympics in Beijing was widely publicised, and illustrated the heavy dependency on IP addresses to support these international sporting events.

The 2022 World Cup will be an important showcase for Qatar, and an ideal opportunity to demonstrate the advanced ICT infrastructure within the state to the rest of the world. It can be reasonably anticipated that demand for broadcast and Internet connectivity will have continued to grow in the intervening period, so adequate preparation to build the infrastructure for this event will be of paramount importance.

1.3 Why is a National IPv6 Strategy Required for the State of Qatar?

It is recognised that the global migration to IPv6 will take many years to complete, but there are good reasons for commencing preparatory work at the earliest opportunity for the following reasons:

- To ensure, wherever possible, that any systems purchased in the future are IPv6 ready, thus minimising the risk of stranded assets
- To ensure organizations in Qatar are able to communicate with IPv6 sites in the rest of world allowing, for example, ecommerce to proceed seamlessly.
- To future proof new projects such as 'smart city' initiatives where the use of IPv6 will deliver many benefits, and where a later retrofit to IPv6 would be both expensive and disruptive.

The complexity of the IP ecosystem does however mean that it is difficult for a single player to unilaterally adopt IPv6 because of the dependency on other players across the ecosystem e.g. equipment suppliers, application, network operators etc.

A national strategy will therefore provide a framework for the well co-ordinated and orchestrated adoption of IPv6 across the national ecosystem by ensuring the various building blocks are in place in a timely manner to enable end-user organizations to progressively move to IPv6. It will also allow progress to be monitored against a common timeline and, where necessary, permit intervention to be triggered if progress is stalled for any reason.

1.4 Who are the Players in the IP Ecosystem?

The IP ecosystem is broadly split between service providers and service users. The service providers can be categorised as follows:

- Hardware vendors
- Fixed network operators
- Mobile network operators
- ISPs
- Software vendors
- Hosting providers.

The service user sector is more complex, but can be categorised as follows:

- Government ministries and agencies
- Education
- Enterprises, e.g.
  - utilities
  - banking & insurance
  - manufacturing & production
  - service sector
  - entertainment
- Private individuals.

1.5 Summary of the Strategic Objectives

The IPv6 strategy aims to provide the following:

- To provide guidance to each group of stakeholders on the activities and associated implementation timing to meet with internationally accepted best-practice guidelines on IPv6 migration
- To provide a national timetable for IPv6 migration
- To identify the players across the IP ecosystem and their interdependencies
- To provide supporting information, through the auspices of an IPv6 task force to be established, that will assist organizations to develop their migration plans and, where necessary, the associated business case.

2 Findings from Qatar's IPv6 Assessment Study

The initial phase evaluated existing plans and performed a high-level assessment – based on questionnaire responses and face-to-face interviews – of the current infrastructure of the State of Qatar. The next task was to undertake a gap analysis, comparing the existing situation with the desired outcome (i.e. timely migration to IPv6). This phase also outlined the development of a roadmap, identifying the training and awareness-raising that needs to take place to support migration.

The state of IPv6 readiness in Qatar was generally found to be on a par with the majority of other developed countries, in that a diminishing pool of IPv4 addresses still remained with national service providers, and little provision has been made for the introduction of IPv6. The gaps that were identified were based on a comparison with an ideal 'should-be' situation based on industry knowledge.

The IPv6 adoption strategies that had commenced implementation were examined, and further enquiries were made to gain a comprehensive understanding from the stakeholders as to their plans.

In general, there were found to be minimal IPv6 implementation plans in place throughout Qatar, with only pockets of work done to date, reinforcing the need for a national IPv6 strategy to be created and published.

The potential for gaining a return on investment through early adoption of IPv6 may exist in some areas, e.g. hosting of regional IPv6 websites, and is worthy of further investigation.

The dominant role of service providers in the IP ecosystem became apparent during the study, and it is therefore vital that they take a lead role in enabling IPv6 readiness activities. It was a matter of concern that some of the organizations consulted identified service providers as inhibiting progress towards achieving this goal.

The raising of IPv6 awareness levels across all stakeholder groups is a measure that can be taken immediately, as this should help stimulate activity in undertaking IPv6 readiness activities.

It was concluded that while Qatar compares reasonably well with its peer group countries, there is a need to commence a number of activities, including the creation of an IPv6 adoption strategy, in order to ensure IPv6 readiness is achieved in a timely manner.

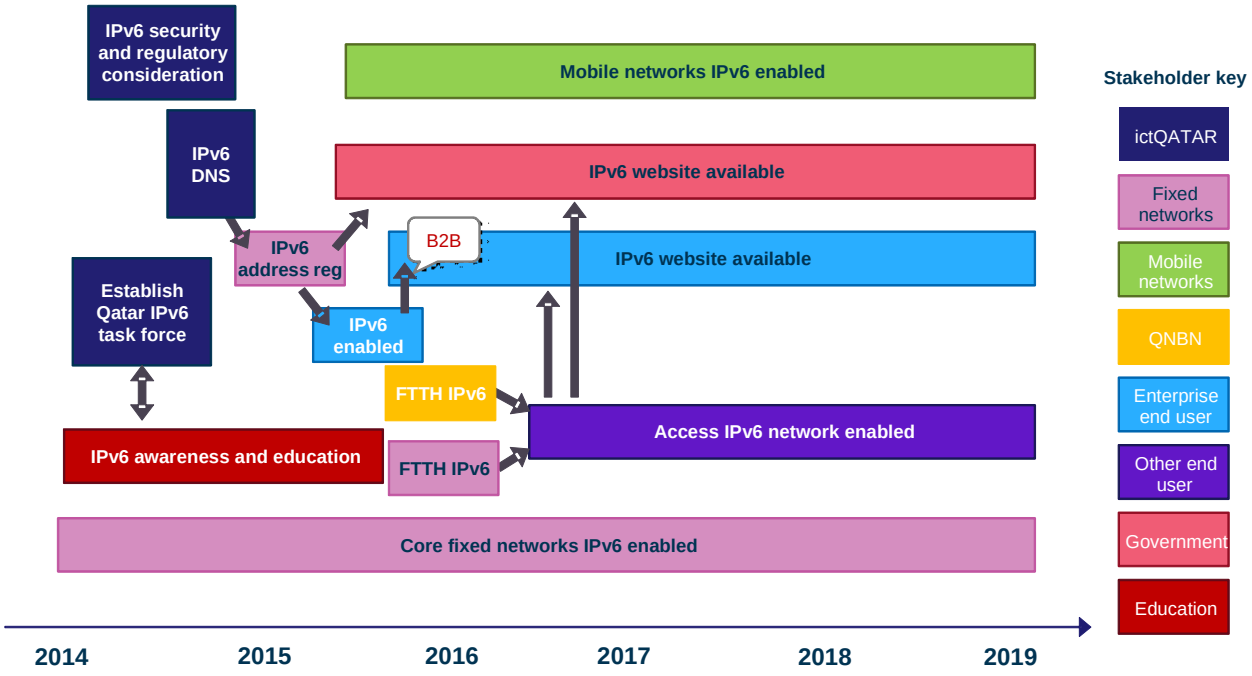
3 IPv6 Implementation Plan for the State of Qatar

The international timetable for IPv6 adoption is not particularly well defined and there is a degree of interpretation as to what is an acceptable state of readiness at this point in time. It is clear, however, that by planning the implementation across the entire ecosystem stakeholders can make the necessary provisions for investment and ensure systems are made ready in a timely manner.

A high-level implementation plan to specifically deliver IPv6 across Qatar's IP ecosystem is shown in Figure 3.1 that takes into account both national and international drivers. The proposed activities during 2014 are to enable the Qatar Domain Name Registry System (DNS) to be 'IPv6-ready', and to publish IPv6 security recommendations as well as regulatory considerations. There are several activities that need to be achieved to improve IPv6 awareness and education should start as soon as possible. The establishment of a national IPv6 task force for the State of Qatar would further this aim.

Figure 3.1 provides a pragmatic view of an achievable roadmap to implement IPv6 across the Qatar ecosystem, taking into account local considerations, e.g. Ooredoo digital subscriber line (DSL) customer premises equipment (CPE) not being IPv6-compatible.

Figure 3.1: High-level IPv6 implementation plan for Qatar



4 Framework for Developing an IPv6 Adoption Strategy

The national adoption strategy must deliver a coherent plan for ensuring Qatar achieves IPv6 readiness at least in step with its peer group, and where appropriate, seek tactical opportunities to make early use of IPv6 where this delivers tangible benefits. The strategy is therefore based on ensuring the building blocks are in place for this to happen.

It is proposed that the national IPv6 strategy will comprise three main phases to promote and support the adoption of IPv6 across the ICT ecosystem.

- **Planning**: creation of an IPv6 task force, which will include all the stakeholders involved in the ICT ecosystem in Qatar.
- **Implementation**: instigation of an IPv6 awareness and education programme, working with suppliers and industry at national, regional and international levels. Financial support will also be provided to encourage enterprise stakeholders to become early adopters. In addition, a small number of government-led projects will be identified as IPv6 exemplars.
- **Support**: an ongoing initiative to provide appropriate support to stakeholders in Qatar's ICT ecosystem until IPv6 readiness is achieved.

5 IPv6 Implementation/Adoption Roadmap and Project Plan

5.1 Introduction

As described in section 4, the three main phases to promote and support the adoption of IPv6 across Qatar's ICT ecosystem are as follows.

- Planning
- Implementation
- Support.

These phases are described in detail in the following sections.

5.2 IPv6 Strategy Planning Phase

During the planning phase, ictQATAR will establish the environment required to foster IPv6 adoption across the ICT ecosystem in Qatar, which will involve the creation of an IPv6 task force.

The task force will draw expert resources from within ictQATAR, as well as other relevant government, academic and private-sector organizations, to ensure that a broad perspective is provided in terms of the requirements for transition to IPv6. The task force will facilitate, fund and/or regulate the implementation of the national strategy, making sure that Qatar's ICT ecosystem is ready for the adoption of IPv6, and that Qatar is seen as a regional leader in this respect. Key aspects to be considered when establishing the IPv6 task force are shown in Figure 5.1.

Figure 5.1: Summary of the activities required to establish an IPv6 task force

Establish Qatar's IPv6 Task Force

Purpose:

To create a task force that can support the implementation of the entire national strategy, making sure that Qatar's ICT ecosystem is ready for the arrival of IPv6

Stakeholders

ictQATAR, other government organizations, representatives from the stakeholder community and academia

Tasks to be undertaken

The key tasks in the creation of the IPv6 task force are outlined below.

- **Define the governance structure** – agree its aims and objectives, executive management involvement, communications, project management, operations management, and decision-making authority.
- **Agree the terms of reference** – define the task force's high-level goals and programme duration.
- **Recruit resources** – identify and recruit a leadership team and workforce. The individuals involved should have project/programme management and ICT skills; there should also be internal and/or external IPv6 experts.
- **(Potentially) source facilities** – find and rent/procure office accommodation for the task force.

Duration

2–3 months

5.3 IPv6 Strategy Implementation Phase

Implementation of the national strategy will involve three areas of activity:

- Education and awareness raising

- Industry development and collaboration to create initial demand for IPv6 and to stimulate supply
- Encourage early adopters in the public and private sectors.

These are described further below.

5.3.1 Education and Awareness

Results from the survey phase indicated that end users[1] and other stakeholders, such as service providers and operators, are generally delaying the move to IPv6 until they see positive reasons for change. This stance, if it continues, could eventually present a risk to some organizations, and to Qatar's economy as a whole.

International initiatives of the kind discussed in Section 5.5 demonstrate that in other countries, governments – in collaboration with other stakeholders – are embarking on a programme of education aimed at raising awareness of IPv6 within their own ICT ecosystems. We believe that a similar programme in Qatar could bring a range of benefits. Figure 5.2 summarises a number of tasks that might be used to educate the stakeholder community and raise IPv6 awareness in Qatar.

Figure 5.2: Summary of activities required to raise awareness and provide IPv6 education

Education and awareness raising

Purpose:

To raise awareness of IPv6 within the end-user community and also to focus on the SME sector

Stakeholders

IPv6 task force, ictQATAR and government organizations, system vendors, service providers, academia

Tasks to be undertaken

The key tasks involved in IPv6 education and raising awareness are:

- overseeing the creation of media for sharing best practice and learnings from areas/sectors (and potentially other countries) that have already introduced IPv6 schemes (e.g. special interest groups, seminars, forums for sharing case studies and white papers)
- providing centralised resources for training and skills development among technical staff
- collaborating with vendors to develop/provide technical training on IPv6-based products
- running demonstrations of IPv6 implementations, including workshops on IPv6 configuration
- organizing and hosting regional/global conferences on IPv6
- encouraging academic research related to IPv6, to develop relevant skills in graduates, and to encourage the development of new and innovative solutions and services.

Dependencies on other parts of the plan?

The success of this part of the plan is highly dependent on the IPv6 task force (to manage and co-ordinate it)

Duration

12–24 months

5.3.2 Industry Development and Collaboration

Industry development and collaboration will be very important in the process. Stakeholders indicated that the government should encourage co-working between system vendors and service providers in order to establish the successful roll-out of IPv6 in Qatar. A number of these activities could potentially be incorporated into the task force function. Some of the tasks involved in this phase of the strategy are shown in Figure 5.3.

[1] SMEs were not covered in the survey, but experience from other national surveys conducted around the world has shown awareness in this group to be generally lower than for larger organizations.

Figure 5.3: Summary of tasks required to encourage collaboration within the ICT industry in the development of IPv6

Industry collaboration

Purpose:

To ensure all ICT stakeholders communicate ideas and collaborate in the development of IPv6 adoption

Stakeholders

IPv6 task force, ictQATAR and other government organizations, system vendors, service providers, MNOs

Tasks to be undertaken

The key tasks involved in promoting industry collaboration are:

- ensuring imported goods to Qatar are IPv6-compatible
- providing and disseminating guidelines on technology solutions and standards to improve confidence and consistency in IPv6 adoption
- providing clear timescales for service providers and other players in terms of supporting IPv6 and providing IPv6 services (this may include mandating a specific deadline)
- working with regional and global industry bodies and policy makers on a unified approach to IPv6 adoption/migration
- promoting the growth of IPv6 content availability
- encouraging end users in the private sector to migrate to IPv6
- encouraging the development of IPv6 interoperability and international roaming guidelines for mobile operators.

Dependencies on other parts of the plan?

The success of this part of the plan is highly dependent on the IPv6 task force to manage it.

Duration

12–24 months

5.4 IPv6 Strategy Ongoing Support Phase

After the implementation, the national strategy will move on to the support phase, focusing on the continuation and expansion of the industry development and collaboration tasks started during the implementation phase.

The support phase can begin when the majority of stakeholder organizations within the ICT ecosystem can operate over the Internet using IPv6 (regardless of whether they use IPv6 or IPv4 for their internal networks). In reality, the transition from the implementation phase to the ongoing support phase is unlikely to be clearly defined.

It is anticipated that the IPv6 task force will be able to begin scaling down its activities by late 2015, as the programme should be maturing by then; a decision on when to disband the task force could be made at this stage.

One of the core elements of the support phase will be active monitoring by ictQATAR of progress towards IPv6 adoption within the ICT ecosystem (e.g. through regular surveys or industry workshops). This will allow ictQATAR to review and refine the national strategy as required, focusing on areas with the most favourable cost–benefit equation; it will ensure that activities do not continue beyond their useful life.

In addition, the ongoing support phase should promote the development of new opportunities and applications that make use of the benefits of IPv6 and provide either cost savings or productivity gains to end users. Examples of these initiatives could include the ‘Internet of Things’, smart or green ICT (e.g. smart buildings and metering) and support for the development of IPv6-capable operations support systems/business support systems (OSS/BSS).

5.5 International Benchmarking of IPv6 Strategies

In preparing this strategy, we have referred to international best practice in the promotion of IPv6, taking account of the Qatar context as established during the survey phase. A number of examples of how governments elsewhere have become involved in promoting the adoption of IPv6 are summarised below.

- The Infocomm Development Authority of Singapore (IDA) launched its 'IPv6 transition programme' to encourage IPv6 adoption and it has been running for the last two years. The programme is a national effort to address the issue of IPv4 exhaustion and to facilitate the smooth transition of the Singapore ICT ecosystem to IPv6. IPv6 transition programme promotes readiness for, and adoption of, IPv6 in the local industry through a series of projects (training, grants, events, etc.).
- In September 2010, the US government set a target for all federal agencies to upgrade public/external-facing networks and services to native IPv6 by the end of September 2012, and for internal client applications that communicate with public Internet servers and support enterprise networks to be upgraded to native IPv6 by the end of September 2014. The initiative also requires agencies to designate a transition manager and to ensure that procurement of networked IT complies with the USGv6 profile and test programme. While this initiative focuses on IPv6, the US government recognises that support for IPv4 will need to continue and has indicated that IPv4 should continue to be run for the foreseeable future, to ensure interoperability. The USA is also planning to run a series of workshops to refine best practice for upgrading to IPv6 and to test commercial products.
- The Indian government has established an IPv6 task force and stated that all ISPs and telecoms companies should be 'IPv6 compliant' and offer IPv6-based services by the end of 2011. In addition, federal government agencies and state governments were required to adopt the new version of the protocol by March 2012.
- The Japanese government established the 'IPv6 Promotion Council' in 2000 to encourage IPv6 adoption, promote R&D, provide training and operate an IPv6 test-bed. A number of initiatives to promote IPv6 adoption have been launched, and the government has also issued a mandate requiring agencies to purchase hardware and software systems that support IPv6.
- The Malaysian government established the National Advanced IPv6 Centre (NAv6) in 2005. It serves as the national centre for IPv6 research, human resource development and monitoring of IPv6 development for Malaysia. As part of its mission, NAv6 planned and implemented appropriate programmes designed to meet a target of the end of 2010 for Malaysia to be an IPv6-enabled nation. By March 2010, the NAv6 was claiming that "Malaysia has made good progress, [but] still [a] long way to go".[2]
- The Hong Kong government has IPv6-enabled the majority of its Web services, with 85% of government sites reported as IPv6 ready in Q1 2011.[3] In March 2013 the Office of the Government Chief Information Officer (OGCIO) claimed "the Internet Infrastructure in Hong Kong is ready for IPv6 deployment".

5.6 IPv6 Implementation Risks

In this section, the risks and uncertainties linked to the implementation of IPv6, in Qatar are analysed. We discuss the risks from the perspective of the various stakeholders including system vendors, end users, service providers etc. Also discussed are mitigation steps that need to be implemented to ensure that the risks identified are minimised or negated.

A number of risks that have been identified, along with potential mitigation measures, are listed in Figure 5.4.

---

[2] See http://meetings.apnic.net/__data/assets/pdf_file/0004/18904/State-of-IPv6-_01_IPv6-Adoption,-the-current-scenario-of-Malaysia-_Rajakumar.pdf

[3] See http://www.ipv6world.asia/gov.php

Figure 5.4: Risks and mitigation

Risk	Description	Risk/impact level	Mitigation
Services providers continue with measures to delay IPv6 implementation	Service providers may delay the launch of IPv6 services by using measures such as carrier-grade NAT to spin out the use of IPv4 address space.	Low to medium risk/high impact.	ictQATAR should encourage service providers to adopt IPv6 at the earliest opportunity.
IPv4 addresses exhausted	It is no longer possible to assign further IPv4 addresses in Qatar once the existing pool is depleted.	Low risk if the timetable is followed, but an increasingly high impact over time if not.	• Ensure timely availability of IPv6 addresses. • Tactical purchase of IPv4 address space as a contingency.
Qatar gets left behind compared with international peers	A large proportion of organizations adopt a 'do-nothing' approach, meaning Qatar falls behind its peer group in terms of Internet infrastructure readiness. As Qatar develops its knowledge-based economy as part of delivering the Qatar National Vision[4], ICT will be a major enabler and the adoption of IPv6 will therefore be an important component in achieving this. The impact of late adoption could manifest itself in a number of ways, typically: • users are unable to access IPv6 websites outside of Qatar • new/existing businesses in Qatar are unable to launch new websites • users using IPv6 address schemes cannot transit carrier networks for wide-area network (WAN) connectivity.	It is likely that the majority of end users will, over time, adopt IPv6 if the necessary infrastructure/services are available. This is therefore classified as low risk/high impact.	Publicity will be the principle measure of mitigation: • IPv6 task force to publish information, organize events etc. • suppliers to provide regular IPv6 information updates to their customers • ictQATAR to undertake periodic audits to ensure progress is being made • increase the awareness of impact of deploying IPv6 through various initiatives, e.g. seminars.

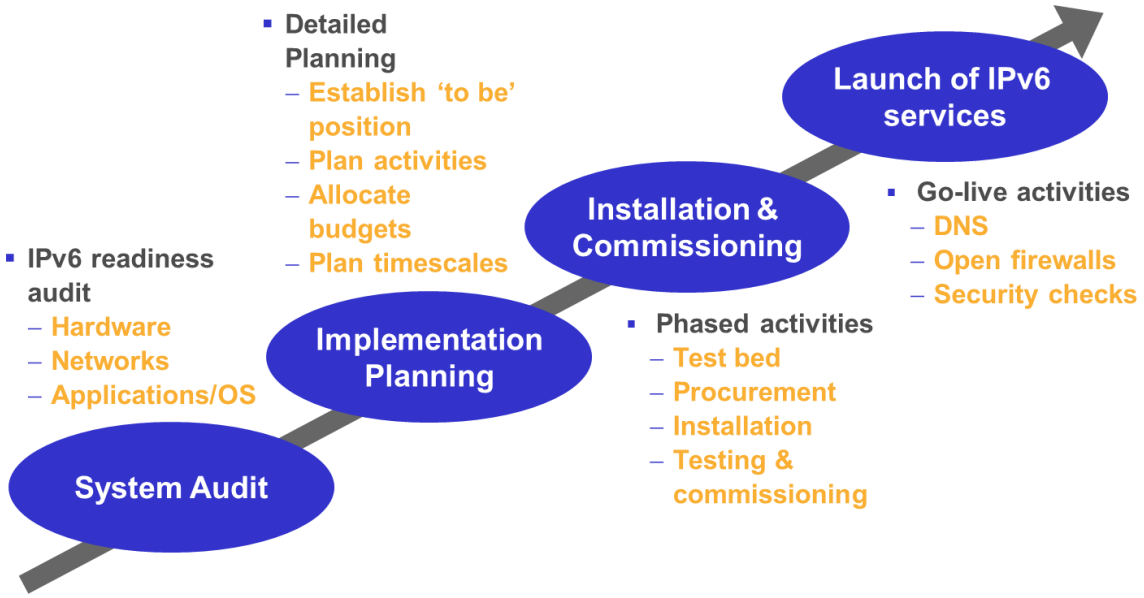
[4] http://www2.gsdp.gov.qa/www1_docs/QNV2030_English_v2.pdf

Risk	Description	Risk/impact level	Mitigation
End users cannot obtain IPv6 addresses/other services	The end-user market wants to implement IPv6 but is prevented due to the inability to obtain address blocks, IPv6-compatible network services etc.	Medium risk/high impact.	ictQATAR may intervene if the supply side of the market is not meeting demand in a timely manner. As above, publicising routes for obtaining IPv6 address blocks directly from the Réseaux IP Européens Network Co-ordination Centre (RIPE NCC) may also be helpful.
Lack of IPv6 compatibility on operating systems	Users with old operating systems (OS) such as Windows XP unable to access IPv6 Internet sites.	Medium risk to SMEs who may not have upgraded to later OS. Impact will be limited to small groups of SMEs.	Ensure familiarity levels are raised across all sectors as to the need for action.
Security breach	A publicised security breach attributed to IPv6 that reduces user confidence and delays implementation.	Low risk/potentially high impact depending on stakeholder group.	• Task force can provide advice on suitable training and ensure this aspect is published. • Service providers take responsibility for ensuring their customer systems are secure. • Increase the awareness of security risks behind deploying IPv6.
Delays to upgrade of DSL CPE routers	A large proportion of current Ooredoo CPE DSL router stock is not IPv6 compatible, this is scheduled for change out by 2015, but any delay beyond this would affect IPv6 take-up in the domestic/SOHO and SME markets.	Low risk/high impact.	ictQATAR to monitor the situation and encourage Ooredoo to complete the change-out of legacy routers by 2015.
Delay to launch of IPv6 DNS in Qatar	ictQATAR cannot resource the provision of the national IPv6 DNS in a timely manner.	Low risk/high impact.	ictQATAR to ensure funding and resources are available to establish IPv6 DNS.

5.7 IPv6 Implementation/Adoption Roadmap Review

The implementation/adoption roadmap and project plan will be a living document to be regularly updated at ictQATAR programme reviews, and which will act as a framework for the monitoring of the programme. Figure 5.5 shows the high-level roadmap of activities which individual organizations will have to implement in order to launch IPv6 services. While this will vary slightly depending on the organization type, the overall structure should be followed.

Figure 5.5: IPv6 implementation roadmap [Source: Analysys Mason 2013]



6 Qatar IPv6 Task Force

As previously mentioned, an IPv6 task force drawing resources from the different departments within ictQATAR will be established, and will include other relevant government, academic and private-sector representatives. This is to ensure that a cross-functional view is taken of the requirements for transition to IPv6 and to minimise duplication of effort.

The task force will be established and will act as a driver for IPv6 in Qatar. It will play an active role throughout the implementation of IPv6 in Qatar. Its role is to facilitate, educate, fund and/or regulate the implementation of the entire national strategy, making sure that Qatar's ICT ecosystem is ready for the adoption of IPv6, and that Qatar is seen as a regional leader in deployment of the technology.

Key tasks to be performed by the IPv6 task force are shown in Figure 6.1.

Figure 6.1: IPv6 task force key tasks

Key Task	Description
Raise awareness on the exhaustion of IPv4 and the impact of IPv6 on proliferation of the Internet and broadband in the country	• Activities related to publicity and education • Organizing training programmes, workshops, conferences and tutorials • Advice to the government on policy issues dealing with IPv6
Encourage all stakeholders to begin the initial phases of IPv6 readiness	• Synchronise the activities of various stakeholders • Identify the issues to solve by each player • Encourage information sharing among member organizations • Advise member organizations on IPv6 technical issues during the transition process • Identify challenges and solutions using IPv6 • Reach out to new stakeholders suffering from IPv4 address exhaustion
Develop transition plans in subsequent phases to support a smooth and wide transition to IPv6	• Conduct surveys and studies, and review the progress by different organizations and the country as a whole during the transition process
Seek international co-operation in IPv6-related areas	• Increase co-ordination with international organizations, neighbouring and other countries for IPv6 deployment • Seek international collaboration with other similar task force organizations throughout the world

The specific activities of the task force are addressed in the following section.

7 IPv6 Task Force Activities

The proposed brief for the task force is based on the models adopted by other countries. Its role will be to provide the strategic national directions for the movement of IPv6 in Qatar. It includes providing the vision, mission and strategic plan for IPv6 implementation in Qatar. The task force will have a range of members, from service providers to key government organizations, Industry associations, educational institutions and different industry stakeholders. The main activities proposed for the task force are summarised below.

7.1 Training and Awareness

There is a requirement for having an adequate pool of IPv6-trained resources in the task force to transfer knowledge in both the government and the private sectors. This knowledge transfer will be performed by conducting workshops, seminars and conferences for the benefit of all stakeholders following the 'train the trainer' concept. It will be responsible for developing the trained resources required by different organizations to deal with IPv6 transition issues.

7.2 Monitor IPv6 Action Plan and Network Implementation

The task force will monitor the progress of IPv6 action plans and network migration scenarios. Different organizations are likely to have different network scenarios, so they will have unique needs. This task force will assist them to create a tailor-made action plan for their transition to IPv6.

7.3 Standards and Specifications

The task force will co-ordinate with ictQATAR in the development of common IPv6 specifications for the State of Qatar, which will be followed by all stakeholders. It will also co-ordinate with the IPv6 Ready Logo committee of the IPv6 Forum to plan and advise different stakeholders and organizations such as vendors, websites etc. for obtaining the IPv6 Ready Logo. It will also interact with other international standardisation bodies to participate in the development of standards and specifications.

7.4 IPv6 Transition

The task force will work to plan the IPv6 transition networks which will accommodate dual stacking and will co-ordinate with the service providers/organizations to establish this 'transition pipe' which will then act as an IPv6 backbone network.

7.5 IPv6 Test Bed

During the transition period, stakeholders are likely to need an IPv6 network for demonstrating and experimenting with different IPv6 transition scenarios. ictQATAR will co-ordinate with stakeholders to establish test facilities for IPv6, either in their organization or managed by a stakeholder.

This activity is not possible on an existing ISP network carrying commercial traffic. Therefore, a separate testing network is needed for simulating a commercial network. The task force will plan and build this IPv6 test network, which can then be used for experimentation by different vendors and organizations from the public and the private sectors. This network can also be used for training personnel to operate IPv6 networks.

7.6 Pilot Projects

IPv6 has many capabilities which are new and do not exist in IPv4. These capabilities can be demonstrated through pilot projects relevant to the industry and government. These pilot projects will provide the necessary experience for large-scale implementations by organizations. This group

will plan and prepare project reports, prepare the funding models and co-ordinate with different government and service providers to take up the deployment of pilot projects to demonstrate IPv6 capabilities.

7.7 Applications Support

The task force will facilitate the migration of existing content and applications to IPv6, and the development of new content and applications on IPv6. It will extend its support to all member organizations. This group will consist of members from software and content developers.

7.8 Knowledge Resource Development

It is also important to develop the IPv6 knowledge base in the country. This can be achieved with the active participation of the education sector. The members of this working group will be drawn from relevant educational institutions.

7.9 IPv6 Implementation in the Government

The task force will work with different government organizations regarding the implementation of IPv6. The members will be drawn from officers in various government organizations.

8 IPv6 Adoption: System Vendors

The 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. For the purposes of this strategy the following classifications have been used:

- Hardware vendors, which manufacture and/or sell hardware, such as routers, switches and servers
- Software vendors, which develop and sell software solutions, such as operating systems, commercial off-the-shelf (COTS) applications and proprietary applications.

They therefore provide the foundation on which the rest of the industry operates.

For the wider ICT industry to adopt IPv6, hardware and software vendors must include IPv6 support across their product portfolio, and must ensure IPv6 interoperability across different solutions. The overall IPv6 enablement of this part of the ecosystem is important in driving IPv6 adoption.

No direct engagement was made with vendors because the vast majority have already published their IPv6 implementation plans in the public domain.

8.1 IPv4 Exhaustion Timelines and Business Impact

End users planning their IPv6 migration path will consult suppliers to determine when their IPv6-ready products will be available. If end users have a pressing business need for IPv6, they will need their suppliers to make IPv6-ready products available. The timely availability of such products will be imperative if suppliers are to meet their customers' needs. If existing vendors fail to meet the timeline driven by the market, end users will be forced to move to a competitor.

Results from the IPv6 readiness survey indicated that many end users were not as advanced with their preparations as they should be, given the rapidly approaching exhaustion of IPv4 addresses. This represents a business opportunity for vendors to proactively market IPv6-ready products and stimulate greater interest.

For vendors that focus on supplying network operators (e.g. Ooredoo and Vodafone Qatar) the demand for IPv6 products will arise earlier than it does from the end-user market, because operator systems will require upgrading before they can market IPv6 services.

9 IPv6 Adoption Guide: Internet Service Providers

While there are no organizations in Qatar whose sole business is to act as an ISP, the two main service providers (Ooredoo and Vodafone Qatar) both act as providers of Internet services and play a key role in building, running and managing the Internet backbone network. Such service providers need to provide IPv6 support as part of commercial Internet services in order to enable wider adoption of IPv6; it will also help to encourage hardware and software vendors to rollout their IPv6-ready solutions.

9.1 IPv6 Adoption Guide: Overall Summary for Internet Service Providers

ISPs will need to adopt a phased approach to IPv6, 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 outlined below.

- **Planning**: IPv6 awareness and skill building activities need to take place while the plans for IPv6 adoption are prepared. In addition, some 'quick-win' projects need to be 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 need to be defined.
- **Deployment**: the IPv6 solution then needs to be deployed across the network, applications and service areas, with quick-win projects implemented at the start of the deployment phase.
- **Support**: IPv6 services will be monitored for performance and reliability, and a customer support system needs to be put in place for the IPv6 services provided to customers, to ensure they have a seamless and smooth experience.

9.2 IPv4 Exhaustion Timelines and Business Impact

ISPs will come under pressure to introduce IPv6 to meet business goals and keep up with the evolution of service offerings; it is therefore imperative for them to synchronise the introduction of IPv6 service offers with the IPv4 address exhaustion timeline. They need to analyse the impact of any difference in these two timelines on the business.

ISPs that begin the process of adopting IPv6 immediately, without prior work, will not complete IPv6 enablement of 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, and the ability of the businesses to grow.

For a single ISP, the main impact of being unprepared for IPv6 and running out of IPv4 addresses will be restrictions on expanding its customer base and developing new services. In such a scenario, customers could choose to switch ISPs (assuming there is one that offers IPv6 services, or still has unused IPv4 addresses), resulting in the first ISP losing business.

For all ISPs there could be two main impacts of non-readiness for IPv6 after IPv4 address exhaustion, as follows.

- Businesses across the ecosystem in Qatar that do not have significant remaining IPv4 address pools, or are dependent on ISPs for IPv4 addresses, would be unable to procure new broadband connections to support 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 Qatar'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 Qatar's GDP.

9.3 IPv6 Adoption Guide: Planning Phase

For the planning phase, which could last between two and three months (some of the activities below should be done in parallel), ISPs need to draw up a detailed IPv6 adoption project plan, and start to build awareness and skills within their organizations. IN addition to the project plan, during this phase ISPs should focus on building IPv6 awareness across the organization, developing an IPv6 business services plan, conducting an IPv6 readiness assessment across its infrastructure, building IPv6 skills among staff, and implementing some immediate 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.

9.3.1 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 organization.

A few key aspects to be considered when preparing to raise awareness of IPv6 in an organization are shown in Figure 9.1.

Figure 9.1: Summary of IPv6 awareness activity for ISPs

IPv6 awareness
Purpose: *To raise IPv6 awareness across key personnel within the organizations to educate them on the importance of IPv6 adoption, the scope of activities required, and the likely timelines*
Stakeholders
Senior management, engineering management and staff, training department
Tasks to be undertaken
The awareness programme must be targeted at multiple segments: • **senior management**, covering: ω the importance of IPv6 and the business impact of non-adoption ω the timelines and the cost of IPv6 adoption • **engineering management**, covering: ω network elements, applications and services affected as a result of IPv6 adoption ω activities to be initiated to design, implement and validate IPv6 solutions and services • **engineering staff**, covering: ω IPv6 technology basics ω the mechanisms for transition to IPv6 ω Guidelines for operating and maintaining IPv6-enabled networks and solutions.
Dependencies on other parts of the plan?
None
Duration
1–2 months

9.3.2 IPv6 Business Services Plan

An ISP's IPv6 business services plan identifies the services that should support IPv6. This is a key input for the planning phase, and allows ISPs to focus on the high-priority and high-impact services during IPv6 adoption.

Key considerations for an IPv6 business services plan are shown in Figure 9.2; further details specific to ISPs are provided in the rest of this sub-section.

Figure 9.2: Summary of IPv6 business services plan for ISPs

IPv6 business requirements
Purpose: *To identify the roadmap of business goals and drivers, the service offerings to be delivered using IPv6, and the implications in terms of return on investment*
Stakeholders
Senior management, engineering management, product department
Tasks to be undertaken
The IPv6 business services plan needs to: • **identify business goals and drivers** linked to IPv6 adoption • **identify service offerings** that should support IPv6, in line with those business goals and drivers • **estimate the return on investment** (either in terms of incremental revenue or cost savings compared to no IPv6)
Dependencies on other parts of the plan?
The IPv6 business services plan cannot commence until: • the IPv6 awareness programme is underway
Duration
2–3 months

Business Goals and Drivers

The typical business goals of ISPs 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.

The above business goals drive the construction of larger networks, an increase in take-up, and the introduction of new and innovative managed, or value-added, services. This results in increased consumption of IP addresses by ISPs and consumers. Like many other countries, the survey phase confirmed that the incumbent ISP is operating predominantly in an IPv4 environment: core networks currently are IPv6 enabled, but access networks and applications are still running in an IPv4 environment.

Service Offerings

ISPs should then plan and prioritise which service offerings should be IPv6 enabled (and as a consequence the supporting network infrastructure and applications) to ensure business continuity.

Using criteria such as customer demand, revenue and fit with business goals, ISPs should assess IPv4 business and residential service offerings for their suitability to offer comparable IPv6-enabled products and services. This assessment will need to take into consideration the current IPv6 status of the networks and applications that would be required by these services.

In addition, ISPs could consider the potential for introducing new IPv6-based services that would support new revenue streams, although the revenue potential of these services would need to be assessed against the costs of deployment. New services could include energy-saving initiatives (green buildings, smart grids, etc.) and managed services (e.g. IPv6-enabled cloud computing services).

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, ISPs need to consider:

- **Incremental revenue** when compared to not IPv6 enabling (this could include revenue through introducing IPv6-enabled services or avoiding lost revenue to competitors which already have IPv6 services)
- **Cost savings from IPv6 deployment**, e.g. through a reduction in the complexity of address management
- **Cost implications of IPv6 enablement**, such as additional hardware, upgrading applications, and the expense of running a dual-stack (IPv4 and IPv6) system initially.

9.3.3 IPv6 Skill Building

IPv6 skill building ensures that all stakeholders across the organization 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 9.3.

Figure 9.3: Summary of IPv6 skill-building activity for ISPs

IPv6 skill building

Purpose:

To ensure that IPv6 skills are developed within the ISPs at all levels of the organization (engineering management, engineering staff, etc.), so that they can support the IPv6 adoption process, and

To provide skills to ISPs' engineering teams that will allow them to participate in the IPv6 adoption programme

Stakeholders

HR, training department, engineering management, senior technical architects, engineering staff

Tasks to be undertaken

The IPv6 skill-building programme involves several grades of personnel within ISPs:

- **senior technical architects/engineering management**, covering:
  - IPv6 solution architecture and design
  - IPv6 migration planning and processes
  - IPv6 service design
- **engineering staff**, covering:
  - the basics of IPv6 technology
  - the mechanisms for transition to IPv6
  - operating and maintaining IPv6-enabled networks and solutions.

Dependencies on other parts of the plan?

The IPv6 skill-building activity cannot commence until:

- the IPv6 awareness activity has been completed (although it can be started in advance of *full* completion)

Duration

2–3 months

9.3.4 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'. When developing a detailed project plan, an ISP must also carry out an IPv6 readiness assessment across networks and applications. This will highlight gaps between the current position and the end goal of end-to-end IPv6 services; and this information will inform the project plan.

Figure 9.4: Summary of project planning for IPv6 adoption activity for ISPs

Project plan for IPv6 adoption

Purpose:

To establish the current state of IPv6 adoption and IPv6 readiness within the ISPs' networks, applications and services, and

To draw up a detailed project plan, covering the tasks required for IPv6 adoption and a roadmap for provision of seamless 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 organization, this team may have further responsibility for execution of the project plan itself)
- **Engineering management** – will help to provide all the inputs required for the 'current state' assessment, and will identify individuals within the business to support adoption

Tasks to be undertaken

The key tasks in preparing the IPv6 adoption project plan are:

- establish an IPv6 consultancy team (internal and/or external IPv6 experts) responsible for preparing the project plan
- undertake an assessment of IPv6 readiness, identifying any gaps in IPv6 adoption across networks, applications and services
- map the current status of IPv6 adoption
- draw up a detailed project plan for IPv6 adoption.

The project plan needs to cover:

- **Network infrastructure** – routers, switches, security devices, DNS, DHCP, NTP, addressing delegation mechanisms, etc., across the core network, broadband network, mobile network, etc.
- **Application infrastructure** – network management, OSS/BSS, HR, enterprise resource planning (ERP) applications, etc.
- **Services infrastructure** – current and planned services offered to customers, and their IPv6 enablement.

The project plan will provide the tasks and activities that are required to IPv6 enable the networks, applications and services. The plan must cover:

- architecture and design
- deployment and implementation
- test and validation
- trials
- 'go live' for IPv6 services.

Dependencies on other parts of the plan?

- 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
- The IPv6 business services plan needs to be prepared to identify which services should support IPv6

Duration

2–3 months

9.3.5 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.

Figure 9.5: Summary of IPv6 solution validation lab activity for ISPs

IPv6 solution validation lab

Purpose:

To verify and validate the proposed IPv6-based solution (architecture, design and services) before it is rolled out in a live environment

Stakeholders

Technical architects and engineering management

Tasks to be undertaken

The IPv6 solution validation lab should validate the architecture included in the project plan, and should include its ability to support the required services. Validation should cover:

- **IPv6 network solution**
  - this needs to be tested for adherence to functional and performance guidelines and SLAs
- **IPv6 application solution**
  - both commercial and proprietary applications should be validated to ensure they can function appropriately using the proposed IPv4/IPv6 solution
- **IPv6 services**
  - business and residential services should be validated in terms of functional performance and reliability across both the network and application environments.

The project plan will need to be reviewed, and revised if necessary, based on the validation lab outputs.

Dependencies on other parts of the plan?

IPv6 solution validation work can only start once

- the IPv6 skill-building programme is completed
- the IPv6 business services plans is underway (as services to be validated need to be identified)

Duration

3–6 months

9.3.6 Quick Wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organization, 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 9.6 summarises this activity, and provides a couple of examples of quick-win initiatives.

Figure 9.6: Summary of IPv6 'quick-win' activity for ISPs

IPv6 quick wins

Purpose:

To identify and implement 'quick-win' projects, and

To strengthen the IPv6 'thought process' in ISPs, develop and embed theoretical skills, and build confidence in IPv6 as a technology

Stakeholders
Corporate IT management team, procurement team, technical architects
Tasks to be undertaken
Projects will depend on the current status of an organization; some examples could include: • **IPv6 enable external-facing websites**, which would help the organization to position itself as an IPv6 leader, and also establish IPv6 as an internal initiative • **participate in national technology trials and test-beds**, which would provide insights into IPv6, while also informing the decision-making processes
Dependencies on other parts of the plan?
IPv6 'quick-wins' tasks can only start once • the IPv6 awareness programme is completed • the IPv6 skill-building programme is completed
Duration
2–3 months

9.4 IPv6 Adoption Guide: Architecture and Design Phase

In this phase, target and transition designs for the network, applications and services are defined to move current IPv4-based services to IPv6, as well as allowing the introduction of new IPv6 services. The IPv6 solution architecture and design phase needs to cover the areas outlined below.

- **Services** – ISPs need to prioritise the IPv4 services to be IPv6 enabled are prioritised, as well as identifying new services, based on the initial work carried out during the planning phase. This prioritisation helps in the design of the network and application architecture.
- **Network** – the network solutions are designed to support the planned IPv6 services.
- **Applications** – the various applications are 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.

9.4.1 Architecture and Design – Services

The development of an architecture and design for the IPv6-enabled services to be offered by ISPs will affect the network solutions architecture and applications solution architecture that are subsequently developed. The key tasks are identified in Figure 9.7, and are discussed further below.

Figure 9.7 Summary of IPv6 service architecture and design activity for ISPs

IPv6 services architecture and design
Purpose: *To build an IPv6 service architecture and design, which will help to ensure existing IPv4 services are IPv6 enabled, and to introduce new IPv6 services*
Stakeholders
Technical architects, software engineering team, vendors
Tasks to be undertaken
• Develop the design and architecture for IPv6 products and services • Define which services/products need to be re-designed to be IPv6 compatible.
Dependencies on other parts of the plan?
The service architecture and design activity can only start once: • the IPv6 readiness assessment and project plan have been completed
Duration
1–2 months

The next stage is to develop a design and architecture for the IPv6 products and services identified in the planning phase.

This process needs to consider various IPv6 transport mechanisms (e.g. dual-stack, Teredo tunnel, ISATAP) as part of the product offering; it also needs to be cognisant of the IPv6 features required by the products, and security and service level agreements (SLAs).

9.4.2 Architecture and Design – Networks

Once the service architecture and design are finalised, a network solution architecture and design aligned to the products and services will have to be prepared.

The network solution architecture needs to consider the various stages in the migration (e.g. IPv4 only, support for both IPv4 and IPv6, and IPv6 only). Given the current position in terms of IPv4 address availability, the solution should also consider a back-up solution for a scenario where the organization has run out of IPv4 addresses, but has not completed the transition to IPv6.

Figure 9.8: Summary of IPv6 network solution architecture and design activity for ISPs

IPv6 network solution architecture and design

Purpose:

To prepare an IPv6 network solution architecture and design that will help to enable IPv6 on the current IPv4-based services and introduce new IPv6 services

Stakeholders

Technical architects, engineering management, network engineering team

Tasks to be undertaken

Ensure that the IPv6 network solution architecture and design – of both core and access networks – covers the following areas:

- **IPv4/IPv6 interconnectivity** – the various tunnelling mechanisms, dual stack, etc.
- **IPv6 routeing** – allowing the reachability of the network elements across IPv4 and IPv6 topologies to be ensured
- **IPv6 security** – security aspects of the planned network roll-out must be considered and be in place
- **quality of service (QoS)** – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance
- **multicast services** – these services across the IPv6 network must be designed in accordance with the planned services
- **traceability of traffic sessions** – if required for regulatory purposes, recording of the various IPv6 sessions taking place across the network should be incorporated.

Dependencies on other parts of the plan?

IPv6 network solution architecture and design can only start once:

- the IPv6 readiness assessment and project plan are completed
- the architecture and design for services is completed, or almost completed

Duration

1–2 months

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 a service provider should be the first network component to be IPv6 enabled.

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. Key enablers here will be IPv6 enabling Ooredoo's CPE DSL routers and the completion of the QNBN, both due for completion by 2015.

For both the core and access networks, service providers will need to consider a wide range of components, such as: IPv4/IPv6 interconnectivity, IPv6 routeing, IPv6 security, QoS, multicast services, and traceability of traffic sessions. For the core and access networks, these issues are outlined in Figure 9.9.

Figure 9.9: Considerations for the design and architecture of core and access networks

	Core network	Access network
IPv4/IPv6 interconnectivity	Appropriate interconnectivity across the upstream service provider and other peers needs to be provisioned, based on the services planned. The details of the IPv6 connectivity across the autonomous systems, and the routes to be announced, should similarly be planned in line with the expected service offerings. The design options that can be considered for providing IPv6 MPLS VPN connections include configured tunnels, 6PE and 6VPE.	Based on the access network design, the IPv6 connectivity to the core needs to be planned: • 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 and MPLS 6PE deployment • a Layer 2 access network provider does not have to take into account any IPv6 considerations for their access network.
IPv6 routeing	Based on the services and the IPv6 network topologies being deployed, the related IPv6 routeing protocols would need to be selected and IPv6 enabled. This would include: • interior gateway routeing (IGP) protocol, where the options are IS-IS or OSPFv3 • exterior gateway routeing protocol (EGP), which is delivered using BGP. IPv4 and IPv6 routeing can be achieved using either a single process or a dual process in the router hardware platform.	For the access network, routeing options include: • static routes • RIPng • OSPFv3. The relevant choice of routeing option will depend on the IPv6 services to be deployed, and the size and topology of the access network. When the 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 should include mechanisms, such as access lists and intrusion detection/prevention, to provide a secure IPv6 Internet transaction environment. Ingress filtering should be deployed toward the end user network 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 ISP's networks and its subscribers are protected from attacks by one of its own customers. The design options in this area include: • unicast reverse path forwarding • IPv6 access lists. In addition to these, security mechanisms, such as a firewalls and IDS/IPS, should be considered.
QoS	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 planned services for deployment, the IPv6 multicast services will need to be designed accordingly, which would include BGP-MPLS multicast services. The protocols that can be 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 this is the case, the systems to record and log the traffic sessions across the core network should be included in the architecture and design. 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.	

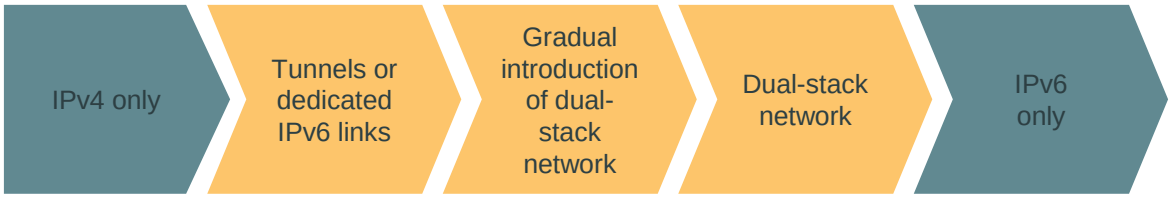
9.4.3 Options for Transition Approaches/Mechanisms for Network Architecture and Design

During the architecture and design phase, it is important that stakeholders choose the right technical approach to IPv6 enabling their networks. The approach will depend on the existing IPv4 environment and the planned IPv6 network, applications and services.

Approaches to IPv6 transition for networks include dedicated IPv6 links, IPv6 in IPv4 tunnels, and dual-stack (IPv6 and IPv4) 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 9.10.

Figure 9.10: Full range of transition phases that might be involved in migration from IPv4 to IPv6 [Source: Analysys Mason, 2013]



The starting point for all stakeholders is an IPv4-only network, from which they can connect to an IPv6 network using either IPv6 tunnelling or separate dedicated IPv6 links.

Tunnelling is an interim solution, which can mean only a small need for infrastructure upgrades, but which is not scalable.

As IPv6 adoption progresses, dual-stack network components 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 organization to be dual-stack ready and enabled – this allows the provision of seamless IPv6 capabilities and services. This also sets the stage for gradually turning off IPv4 services.

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

This approach can be adopted across all stakeholder segments, and can be executed in sequence; alternatively, a stakeholder may choose to move immediately to the later stages.

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.

Core network scenarios
• Currently running an IPv4 network to offer initial IPv6 services, 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 9.11: Core network scenarios

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
• DSL and Ethernet
– point-to-point model
– PPP terminated aggregation (PTA) model
– L2TP access aggregation (LAA) model

Figure 9.12: Core network scenarios

9.4.4 Architecture and Design – Applications

Once the service and network architecture are finalised, ISPs can move on to application architecture and design, aligned to the work already undertaken on the network and services. This design will include the relevant OSS/BSS, network management and network monitoring applications to support the planned IPv6 services. The key tasks are highlighted in Figure 9.13, and addressed in more detail in the following text.

Figure 9.13: Summary of IPv6 application solution architecture and design activity for ISPs

IPv6 application solution architecture and design
Purpose:
To prepare an IPv6 application solution architecture and design, which will help enable IPv6 on the current IPv4-based services and introduce new IPv6 services
Stakeholders
Technical architects, software engineering team, vendors
Tasks to be undertaken
The IPv6 application solution architecture and design needs to: • ensure that network management and monitoring applications/solutions are able to support and monitor dual-stack networks • ensure applications, such as customer relationship management (CRM) and billing systems, are able to support IPv6 and IPv4-based connectivity and services • ensure proprietary applications are able to do the same.
Dependencies on other parts of the plan?
IPv6 application solution architecture and design can only start once: • the IPv6 readiness assessment and project plan are completed • the architecture and design for *services* need are completed. The architecture and design for *networks* can be prepared in parallel.
Duration
1–2 months

The application infrastructure in an ISP 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 in Figure 9.14.

Figure 9.14: Key tasks

Network management and monitoring applications/ solutions	Initially, network device configuration and regular network management and monitoring operations can be performed over an IPv4 transport layer; this is because as an IPv6 management information base (MIB) can be reached from an IPv4 network. It should be noted, however, that if ICMPv6 messages are used for monitoring, IPv6 connectivity would be required. As a second step, IPv6 transport can be provided for these network and service operation applications, which would help to provide IPv6 management and monitoring.
CRM/billing	From the outset, CRM and billing applications would need to support IPv6-related products and services, even if these systems are still operating in an IPv4 environment. As IPv6 adoption progresses, the CRM and billing applications can also start to operate in an IPv6 environment.
Proprietary applications	ISPs will need to provide appropriate software development resources for any proprietary applications that need to be IPv6 enabled in order to support the IPv6 services and products being offered to consumers.

9.5 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 organization.

9.5.1 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.

Figure 9.15 Summary of IPv6 deployment and implementation activity for ISPs

IPv6 deployment and implementation

Purpose:

To deploy IPv6 across the network and applications of the ISP to support the launch of IPv6 service offerings

Stakeholders

Technical architects, network engineering team and software engineering team

Tasks to be undertaken

The IPv6 deployment and implementation would cover the following areas:

- **infrastructure IPv6 upgrade** of the hardware and software systems (if they are not IPv6 ready), or replacement with IPv6-compliant systems
- **IPv6 connectivity** – IPv6 addresses are purchased, and IPv6 connectivity with upstream providers and other peers is established
- **core network** – IPv6 is adopted across the core network
- **access network** – the IPv6 network is adopted across the access network and network elements, routeing, security, applications, services etc. are upgraded to IPv6
- **applications and service operations** – the various applications, such as network management, monitoring, CRM, etc. are IPv6 enabled
- **services** – the various services spread across the business and residential customers are IPv6 enabled.

Dependencies on other parts of the plan?

IPv6 deployment and implementation can only start once:

- the IPv6 service, network and application architecture are mostly completed

Duration

3–4 months

Key aspects of the six tasks identified above in the rest of this sub-section:

9.5.2 Infrastructure IPv6 Upgrade

By comparing the new solution design and architecture with the current state (generated through the IPv6 readiness assessment), organizations can identify the infrastructure that would need to be upgraded to IPv6 to support the planned services and products. The upgrade of this infrastructure should be initiated as a first step in the deployment of IPv6.

9.5.3 IPv6 Connectivity

To support the launch of IPv6 services and products, an ISP would have to:

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

9.5.4 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. As such, it should consider the areas outlined earlier in Figure 9.9, namely:

- IPv4/IPv6 interconnectivity
- IPv6 routeing
- 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. As such, it will consider the areas outlined earlier in Figure 9.9 (IPv4/IPv6 interconnectivity, IPv6 routeing, IPv6 security, QoS, multicast services, and traceability of traffic sessions).

Figure 9.16: Considerations for the access network design for ISPs

Area for consideration	Description
IPv4/IPv6 interconnectivity	Deploying IPv6 connectivity from the access network to the core network should use one of the options outlined below. A Layer 3 access network provider would forward access traffic through the IPv6 core using one (or more) of: • IPv6 tunnelling • native IPv6 deployment • MPLS 6PE deployment.
IPv6 routeing	Based on the network design, the routeing 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 will be designed to provide security in an IPv6 environment by using unicast reverse path forwarding, IPv6 access lists, and security mechanisms, such as a firewall, IDS/IPS, etc.
QoS	The IPv6 QoS design should be configured across the network to ensure that the traffic engineering requirements and customer SLAs are met.
Multicast services	If required as part of the network design, IPv6 multicast would be enabled using IGMPv3/MLDv2 protocols.
Traceability of traffic	Traceability of traffic sessions is implemented by recording and logging the details of 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.

Applications and Service Operations

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

Figure 9.17: Considerations for the application and service operation design for ISPs

Area for consideration	Description
IPv6 address management system	Such as system would help plan, provision and manage the IPv6 address allocation and life cycle, 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, and would operate in a dual-stack or IPv6-only environment.
Accounting, billing applications are IPv6 enabled	IPv6 enablement of corporate applications would help in ensuring that the customer support system for the IPv6 services being rolled out is in place

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 in Figure 9.18.

Figure 9.18: Considerations for service design for ISPs

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

9.5.5 IPv6 Testing and Validation

A summary of IPv6 testing and validation activities for ISPs is set out in Figure 9.19.

Figure 9.19 Summary of IPv6 testing and validation activity for ISPs

IPv6 testing and validation

Purpose:

To validate IPv6 services across ISPs' networks and applications

Stakeholders

Technical architects, network engineering team, software engineering team

Tasks to be undertaken

IPv6 testing and validation will cover the following areas of business and residential IPv6 products and services:

- **IPv4/IPv6 connectivity** will be validated
- **IPv6 routeing** the network elements across IPv4 and IPv6 topologies will be reachable through the appropriate IPv6 routeing protocol
- **IPv6 security** aspects of the network will be validated
- **QoS** aspects across the network will be validated
- **multicast services** as per the service design will be validated across the network
- **applications** will be validated for their IPv6 support
- **traceability of IPv6 traffic sessions** across the network will be recorded for regulatory purposes, and the reliability of the system will be validated
- **IPv6 compliance/certification (optional)** will ensure services are tested against certification or compliance programmes

Dependencies on other parts of the plan?

IPv6 testing and validation can only start once:

- the IPv6 services solution roll-out is completed

Duration

3–4 months

Further details on the aspects that need to be tested and validated as part of the IPv6 adoption process are outlined below.

- **IPv4/IPv6 interconnectivity** – organizations should verify the reachability of IPv6 networks through IPv4 networks in which transition mechanisms are implemented, and vice versa.
- **IPv6 routeing** – organizations should verify the ability to navigate the IPv6 topology through the implemented IPv6 routeing protocol. This includes verifying that routeing tables include all IPv6 routes required.
- **IPv6 security** – organizations should verify and validate the IPv6 security implemented across the network through appropriate checks (vulnerability and penetration tests).

- **QoS** – organizations should verify the performance and reliability of the various classes of QoS that have been implemented, by injecting traffic and conducting stress tests.
- **Multicast –** organizations should validate multicast service distribution by assessing service performance against agreed specifications.
- **Applications** – organizations should validate the functional and performance aspects of applications and related solutions in an IPv6 environment.
- **Traceability of IPv6 traffic sessions –** organizations should check that IPv6 traffic sessions are being correctly recorded/logged, and that the associated tracing system is reliable.
- **IPv6 compliance/certification (optional)** – once all other test and validation tasks have been completed, an ISP may apply for IPv6 compliance/certification testing in order to confirm and promote the fact that its services meet known standards. No standards/certifications are yet mandated in Qatar, so this is optional.

9.5.6 IPv6 Trials

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 ISP is to run a commercial IPv6 trial with a few customers.

Figure 9.20: Summary of IPv6 trials activity for ISPs

IPv6 trials
Purpose: *To ensure IPv6 trials are conducted with a limited number of trusted customers*
Stakeholders
Business teams, engineering management, account management, operations and support
Tasks to be undertaken
IPv6 trials should be conducted with customers, covering: • **business services** – Internet/MPLS VPN services and managed network services, ensuring they are validated for reliability and performance • **residential services** – broadband services, ensuring are validated for reliability and performance
Dependencies on other parts of the plan?
IPv6 trials can only start once: • IPv6 testing and validation are completed
Duration
3–4 months

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.

9.5.7 IPv6 ‘go live’

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

Figure 9.21: Summary of IPv6 'go-live' trials activity for ISPs

IPv6 'go-live' trials
Purpose: *To undertake trials to before IPv6 services are rolled out commercially*
Stakeholders
Business teams, engineering management, marketing operations
Tasks to be undertaken
IPv6 services are made available commercially to customers, and rolled out on a large scale, including: • **business services** – provision of current wholesale MPLS VPN services and managed network services to customers • **residential services** – provision of broadband services to customers
Dependencies on other parts of the plan?
IPv6 'go-live' trials must be completed before IPv6 'go live'
Duration
3–4 months

9.6 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.

9.6.1 IPv6 Service Support

The customer support system for IPv6 products and services must ensure that customers have a seamless service experience.

Figure 9.22: Summary of IPv6 service support activity for ISPs

IPv6 service support
Purpose: *To ensure IPv6 customers are supported and service performance is stabilised*
Stakeholders
Business teams, engineering management, marketing operations
Tasks to be undertaken
The customer support system for IPv6 products and services must ensure a seamless customer service experience, including: • **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 quickly, and common/regular faults are identified and addressed • **troubleshoot and maintain IPv6 service** – the customer support team will work closely with technical architects to make adjustments to the IPv6 system and help ensure that it is robust and stable
Dependencies on other parts of the plan?
Clearly, IPv6 service support can only start once IPv6 services are commercially available
Duration
Ongoing

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.

9.6.2 Review IPv4 Plans

After successfully rolling out commercial IPv6 services, the ISP will need to ensure the service remains effective.

Figure 9.23: Summary of IPv4 review plans for ISPs

Review IPv4 plan
Purpose: *To review the IPv4 services and plan the phasing out of IPv4*
Stakeholders
Business teams, engineering management, marketing operations
Tasks to be undertaken
After successfully rolling out commercial IPv6 services, the ISP will need to: • **monitor 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 • **prioritise and plan IPv4 service switch-off**, including a timeline and a phased approach for ending services
Dependencies on other parts of the plan?
The IPv4 review plan can only start once IPv6 services are commercially available
Duration
Ongoing

Once IPv6 service have been launched, ISPs need to consider how to retire IPv4 products and services; this will reduce the overheads associated with dual running. ISPs should monitor take-up of IPv6 services, and identify IPv4 services and products that could then be retired.

10 IPv6 Adoption Guide: Network Providers

Network providers (both wireline and wireless) are clearly a key part of delivering IPv6 services to the end user.[5] There are interdependencies between wireline and wireless domains (e.g. mobile networks rely on extensive fixed core networks). There are also multiple interfaces between different operators' networks that must work at compatible protocol levels – specifically in this case, IPv6 traffic will require all the networks involved to be IPv6-enabled.

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

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

Fixed national network providers offering IP connectivity (ISPs) are included within Section 9 above. Carriers can provide services at a purely national level and/or on an international basis.

10.1 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 and the predicted timescales are the same as those for an ISP (as described in Section 9.1):

10.2 IPv4 Exhaustion Timelines and Business Impact

Mobile operators and wireless Internet providers will come under increasing pressure to introduce IPv6 to cope with the evolution of services, as the exhaustion of IPv4 addresses approaches. It is therefore important to ensure that their IPv6 migration plans take account of the timeline for exhaustion of both IPv4 addresses available from Réseaux IP Européens (RIPE), and their own allocation of IPv4 addresses. 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.

10.2.1 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 and NAT).

The deployment of LTE (or 4G) networks, which are to be based on IPv6, requires enhancement of the existing packet-switched domain as a precursor to deploying any new systems. Since both Ooredoo and Vodafone already have access to IPv6 address blocks, they can deploy IPv6 services whenever they are ready.

10.3 IPv6 Adoption Guide: Planning Phase

In this phase, a network provider will draw up a detailed project plan for IPv6 adoption, and start to build awareness and skills within the organization. This phase will include activities such as building IPv6 awareness across the organization, developing an IPv6 business services plan, conducting an IPv6 readiness assessment across information technology infrastructure, building

[5] Note that Ooredoo and Vodafone both provide wireline and wireless services in their product portfolios.

IPv6 skills among staff, and implementing a few 'quick-win' projects, such as setting up an IPv6 solution validation lab.

10.3.1 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 organization. The IPv6 awareness programme for network operators is, essentially, the same as that set out for ISPs (see Section 9.3.1)

10.3.2 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. Aspects of the development of the IPv6 business service are similar to those set out for ISPs (in Section 9.3.2). Those aspects specific to operators are set out below.

Business Goals and Drivers

The typical business goals of network providers are to:

- **Ensure their products** match market demand
- **Launch new value-added services** to provide additional revenue streams
- **Improve their operating efficiency** by reducing the number of technology platforms.

Results from the survey indicated that all the network providers are aware of the need to consider IPv6 in their future investment plans.

Services

Typical business service offerings delivered by network providers in Qatar 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
- **Fixed-wireless networks** – 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; 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.

10.3.3 Project Plan for IPv6 Adoption

The structure of the project plan for IPv6 adoption is, essentially, the same as that set out for the ISP (set out in Section 9.3.4).

10.3.4 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. Again the steps involved for network operators are, essentially, the same as those set out for ISPs

10.3.5 Quick Wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the network operator, 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.

10.4 IPv6 Adoption Guide Architecture and Design Phase

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

10.4.1 Network Operators

Any changes in architecture are unlikely to be substantial, as existing networks will generally be fully upgradable. However, network operators will need to consider interim solutions (e.g. tunnelling) if customers require IPv6 connectivity prior to full IPv6 migration.

10.4.2 Mobile Operators

The standards body, 3GPP, is the key organization behind the architecture changes needed to incorporate IPv6 into the core networks 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. Handsets are developed for an international marketing, and this is therefore not an issue that is specific to Qatar, but mobile operators should still monitor developments.

10.5 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 organization.

10.5.1 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.

Figure 10.1: Summary of IPv6 deployment and implementation activity for network providers

IPv6 deployment and implementation

Purpose:

To deploy IPv6 across the fixed and wireless networks to support the launch of IPv6 services

Stakeholders

Technical architects, network engineering team, software engineering team, marketing and sales, procurement

Tasks to be undertaken

IPv6 deployment and implementation will cover:

- **infrastructure upgrade** of the hardware and software systems is needed (if they are not IPv6-ready), or replacement with IPv6-compliant software
- **IPv6 connectivity** – IPv6 addresses need to be purchased and IPv6 connectivity needs to be established with upstream providers and other peers
- **core network** – IPv6 needs to be adopted across the core network, including security, applications and service elements
- **access network** – the IPv6 network needs to be adopted across the access network (that is, the network elements, routeing, security, applications, services, etc. are upgraded to IPv6)
- **applications and service operations** – the various applications, such as network management, monitoring, CRM, etc. need to be IPv6-enabled
- **handsets (mobile only)** – IPv6-compatible handsets need to be sourced
- **fixed wireless terminals (fixed wireless access)** – IPv6-compatible wireless terminals need to be sourced

Dependencies on other parts of the plan?

IPv6 deployment and implementation can only take place once:

- the IPv6 service, network and application architecture is mostly completed

Duration

12–24 months

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 identify infrastructure elements 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.

10.5.2 IPv6 Testing and Validation

IPv6 testing and validation activities for network operators are similar to those set out for ISPs is set out in Section 9.5.5. The test and validation activities help in assessing the reliability and performance of the various business and residential services.

10.5.3 IPv6 Trials

After the network 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 operator is to run a commercial IPv6 trial with a few customers. This is, essentially, the same process as described for ISPs (in Section 9.5.6).

10.5.4 IPv6 ‘go live’

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

10.6 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.

10.6.1 IPv6 Service Support

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.

10.6.2 Review IPv4 Plans

After the introduction of IPv6 services, network providers need to consider the scope for retiring IPv4 products and services to reduce the operational challenges and costs of maintaining and managing both an IPv4 and an IPv6-capable network. 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, this process will extend over several years.

11 IPv6 Adoption Guide: Service Providers

There are three stakeholder categories with similar characteristics (in terms of IPv6 requirements), as outlined below, and these have been grouped under 'service providers'.

- **Data centre operators** – these play an important role in the ICT ecosystem by hosting and supporting the back-end systems. As organizations in Qatar progress towards adopting IPv6, the back-end systems hosted by data centre operators will also need to be IPv6 capable.
- **ASP/Web hosting providers** – these companies provided shared services for the various organizations across the country, which help them to make cost savings and access the best technology. ASP/Web hosting providers will need to ensure that the services they offer end users support IPv6 – whether this involves proprietary applications or working with vendors to source IPv6-enabled applications.
- **Content providers** – create and provide the information that is accessed and exchanged across the Internet.

11.1 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 ISP stakeholder group, the four main phases of IPv6 adoption are: planning, architecture and design, deployment and support.

11.2 IPv4 Exhaustion Timelines and Business Impact

For service providers, the business impact of IPv4 address exhaustion varies depending on the services they provide and their 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 by the customer as an end user. Data centre operators offering co-location services are more likely to be affected, as the IP addresses of these systems will be their responsibility.

The impact on ASP/Web hosting providers and content providers will mirror that of their end-user client organizations. Therefore, those that currently use IPv4 infrastructure and applications need to start planning for migration to IPv6, the shortage of IPv4 addresses becomes critical.

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. Service providers should be mindful of IPv6 transition in the context of their other High infrastructure programmes, as well as being aware of the interoperability and performance issues, and security. They must be realistic about the true costs associated with developing detailed plans to address these issues.

11.3 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 organization. As well as involving the development of a detailed project plan, this phase includes key activities, such as building IPv6 awareness across the organization, conducting IPv6 readiness assessments across IT infrastructure, building IPv6 skills among staff, and implementing some 'quick-win' projects, such as ensuring that any new implementations are IPv6 compliant.

11.3.1 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 organization. Some key aspects to be considered when preparing to raise awareness of IPv6 in a service provider are shown in Figure 11.1.

Figure 11.1: Summary of IPv6 awareness activities for service providers [Source: Analysys Mason, 2013]

IPv6 awareness

Purpose:

To raise IPv6 awareness across key stakeholders associated with the service provider to educate them on the importance of IPv6 adoption, the scope of activities required, and the likely timelines

Stakeholders

Senior management, engineering management and staff, sales and marketing, training department, customers and suppliers

Tasks to be undertaken

The awareness programme must be targeted at multiple segments:

- **senior management and sales/marketing**, covering:
  - importance of IPv6 and the business impact of non-adoption
  - timelines and costs of IPv6 adoption
  - aspects of networks, applications and services that would be affected as a result of IPv6 adoption
  - the tasks to be initiated to design, implement and validate the IPv6 solutions and services
- **engineering staff**, covering:
  - the basics of IPv6 technology
  - the mechanisms for transition to IPv6
  - guidelines for operating and maintaining IPv6-enabled networks and solutions
- **customers and suppliers**, covering:
  - importance of IPv6 and the business impact of non-adoption
  - timelines for IPv6 adoption
  - aspects of networks, applications and services that would be affected as a result of IPv6 adoption

Dependencies on other parts of the plan?

None

Duration

1–2 months

11.3.2 IPv6 Software Compatibility Check

A vital part of IPv6 readiness for service providers will be to ensure that all legacy systems running on IPv4 are capable of being upgraded to IPv6. For the hardware components, compliance can be verified by the equipment vendor. Software is more complex, however, as 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 in the software can be changed to IPv6 equivalents.

Figure 11.2: Software compatibility checks for service providers

IPv6 software compatibility check
Purpose: *To carry out an audit of the existing software in order to ascertain whether the applications and system software are ready for the upgrade to IPv6,* and *To provide software developers and suppliers with the information needed to implement code changes as part of the IPv6 adoption programme*
Stakeholders
IT management, senior technical architects, IT staff
Tasks to be undertaken
The IPv6 software compatibility check primarily involves operational staff, for example: • **senior technical architects/IT management**, with checks covering: ω software components offered as part of a service to customers ω operating systems software ω data centre automation packages ω operational management systems • **IT development staff**, with checks covering: ω application programming interfaces ω operating system calls ω network management protocol calls ω system management routines
Dependencies on other parts of the plan?
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
Duration
2–3 months

11.3.3 IPv6 Skill Building

IPv6 skill building ensures that all stakeholders across the service provider have the required skills to contribute to, and participate in, the IPv6 adoption process, including implementation. Essentially this is the same process as set out for ISPs in Section 9.3.2.

11.3.4 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 'going 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 11.3).

Figure 11.3: Summary of project planning for IPv6 adoption activity for service providers

Project plan for IPv6 adoption

Purpose:

To establish the current status of IPv6 adoption across the service providers' networks, applications and services, and

To 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

Stakeholders

- **IPv6 work group team** – a team of IPv6 experts (internal and/or external) responsible for preparing the project plan for IPv6 adoption. Depending on the organization, this team may have further responsibility for execution of the project plan itself.
- **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

Tasks to be undertaken

The key tasks in preparing the IPv6 adoption project plan are:

- 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
- conduct an IPv6 readiness assessment to identify the gaps in IPv6 adoption across network, applications and services
- map the current status of IPv6 adoption
- draw up a detailed project plan for IPv6 adoption.

The IPv6 readiness assessment needs to cover:

- **network infrastructure** – routers, switches, security devices, DNS, DHCP, NTP, addressing delegation mechanisms, etc., spread across the core network, broadband network, mobile network, etc.
- **application infrastructure** – network management, OSS/BSS, human resources, ERP applications, etc.
- **core business applications infrastructure** – the existing and planned business applications and the status of their IPv6 enablement.

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:

- architecture and design
- deployment and implementation
- test and validation
- trials
- 'go live' for IPv6 services.

Dependencies on other parts of the plan?

- 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
- The IPv6 business requirements plan needs to be prepared, to identify which services will need to be supported by IPv6

Duration

2–3 months

11.3.5 Equipment Refresh

The service provider community, in common with others in the ecosystem, will have a continuous hardware refresh programme, i.e. technical components within its 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 address are procured as IPv6-compliant (or capable of running dual protocol stacks) as part of the requirements specification.

Figure 11.4: Equipment refresh for service providers

Equipment refresh
Purpose: *To ensure that IPv6 compatibility is guaranteed within all hardware procured by the service provider,* and *To include IPv6 in all requirements specifications for new hardware*
Stakeholders
IT management, senior technical architects, IT staff, procurement department
Tasks to be undertaken
The IPv6 skill building programme encompasses various layers of the organization: • **senior technical architects/IT management** – skills in the following areas must be covered: ω ensure that IPv6 compatibility is included within all technical specifications • **procurement staff** – the following areas must be covered: ω ensure that IPv6 compatibility is drafted in to all supply contracts for computer hardware
Dependencies on other parts of the plan?
None
Duration
Ongoing

11.3.6 Quick Wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within an organization, and in giving IT staff the opportunity to use the theoretical skills they have gained earlier in the process. Essentially this is the same process as set out for ISPs in Section 9.3.6.

11.4 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 network solutions to support the planned IPv6 services.
- **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.

11.4.1 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 needs to consider the various stages in the migration (e.g. IPv4 only, support for both IPv4 and IPv6, and IPv6 only). Given the current position in terms of IPv4 address availability, the solution should also consider a back-up solution for a scenario where the organization has run out of IPv4 addresses, but has not completed the transition to IPv6.

Figure 11.5: Summary of IPv6 network solution architecture and design activity for service providers

IPv6 network solution architecture and design

Purpose:

To 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

Stakeholders

Technical architects, IT management, IT staff

Tasks to be undertaken

Ensure that the IPv6 network solution architecture and design – of both core and access networks – covers the following areas:

- **IPv4/IPv6 interconnectivity** – the various tunnelling mechanisms, dual stack, etc.
- **IPv6 routeing** – allowing the reachability of the network elements across IPv4 and IPv6 topologies to be ensured
- **IPv6 security** – security aspects of the planned network roll-out must be considered and be in place
- **QoS** – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance
- **multicast services** – these services across the IPv6 network must be designed in accordance with the planned services
- **traceability of traffic sessions** – if required for regulatory purposes, recording of the various IPv6 sessions taking place across the network should be incorporated
- **data centre specific components** – such as top-of-rack (TOR) and end-of-row (EOR) switches

Dependencies on other parts of the plan?

The IPv6 network solution architecture and design can only commence when:

- the IPv6 readiness assessment and project plan are completed
- the architecture and design for services are completed, or almost completed

Duration

1–6 months

11.4.2 Architecture and Design – Systems and Services

For the service provider community, it is vital that the exhaustion of the IPv4 address range 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 11.6.

Figure 11.6: Summary of IPv6 application solution architecture and design activity for service providers

IPv6 application solution architecture and design
Purpose: *To prepare an IPv6 application solution architecture and design, which will help enable IPv6 on the current IPv4-based services and introduce new IPv6 services*
Stakeholders
Technical architects, IT staff, vendors
Tasks to be undertaken
The IPv6 application solution architecture and design needs to cover the following areas: • ensure **applications, such as ERP and CRM systems**, are able to support IPv6 and IPv4-based connectivity and services • **ensure proprietary applications** are able to support both IPv6 and IPv4-based connectivity services • ensure **network management and monitoring applications/solutions** are seamlessly able to support and monitor IPv4 and IPv6 networks
Dependencies on other parts of the plan?
The IPv6 application solution architecture and design cannot commence until: • the IPv6 readiness assessment and project plan are completed • the architecture and design for *services* needs is completed. The architecture and design for *networks* can be prepared in parallel.
Duration
1–6 months

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.

11.5 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 organization.

11.5.1 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 implement IPv6 services.

Figure 11.7: Summary of IPv6 deployment and implementation activity for service providers

IPv6 deployment and implementation
Purpose: *To deploy IPv6 across the network and applications to support the launch of IPv6 services*
Stakeholders
Technical architects and IT staff
Tasks to be undertaken
The IPv6 deployment and implementation will cover: • **infrastructure IPv6 upgrade** of the hardware and firmware systems (if they are not IPv6-ready), or replacement with IPv6-compliant firmware • **IPv6 connectivity** – IPv6 addresses need to be purchased and IPv6 connectivity with upstream providers and other peers needs to be established • **applications and service operations** – the various applications, such as network management, monitoring, CRM, etc. need to be IPv6-enabled • **services** – the various services spread across the organizations need to be IPv6-enabled
Dependencies on other parts of the plan?
The IPv6 deployment and implementation cannot commence until: • the IPv6 service, network and application architecture are mostly completed
Duration
3 months

11.5.2 IPv6 Testing and Validation

IPv6 testing and validation activities are, essentially, the same as those set out for ISPs in Figure 9.19.

11.5.3 IPv6 Trials

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. Essentially, this is the same process as set out for ISPs in section 9.5.6.

11.5.4 IPv6 'go live'

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.

11.6 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** – from first to third-line support via a help desk
- **Specialist support** – access to support from external suppliers of hardware and applications.

12 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 business activities. This category includes government agencies and large national companies, through to small and medium enterprises (SMEs).

Government agencies play a significant role in the ICT ecosystem, as they are the largest users of IT in Qatar. Stakeholders across Qatar's ICT ecosystem regard the government agencies as a role model, as they provide leadership and set an example in the area of IPv6 adoption. This places a significant onus and responsibility on the government agencies to be taking visible measures to adopt IPv6.

There are a number of large companies, both national and international, which have a significant footprint in Qatar. IPv6 enablement of this segment will ensure that national companies in Qatar are well placed to benefit from business opportunities based on the next generation of Internet technologies.

SMEs in Qatar that use the Internet Protocol (IP) in some capacity will need to be mindful of the exhaustion of IPv4 and the need to communicate with customers/suppliers who are using IPv6 in the future. The characteristics of organizations in this sector vary substantially, and so there is no single approach to deploying IPv6 that will suit all SMEs.

12.1 IPv6 Adoption Guide: Overall Summary

The process of adopting IPv6 will vary, depending on the type of end user. Government agencies are likely to be early adopters in order to lead by example, and large national companies are also likely to take early measures to avoid the risk of regional IPv4 address shortages.

12.2 IPv4 Exhaustion Timelines and Business Impact

An end user's IPv6 strategy should ideally consider its own unique business case and its network infrastructure. It should take into account inter-relationships with other infrastructure programmes and the need to incorporate a transition plan into the overall IT budget. End users should also be address security, interoperability and performance issues, as well as the true costs associated with these.

For end users, the consequences of not achieving IPv6 readiness once IPv4 address allocations are exhausted are outlined below.

- Businesses which are running short of IPv4 addresses, or are dependent on 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 organizations.

All of these factors could potentially have a direct negative impact on Qatar's GDP by impeding business growth.

Figure 12.1: Relative timing of IPv6 adoption across categories of end user

Category of end user	Expected timing of IPv6 adoption	Driver
• Government • National • SME • Individuals.	• Early/medium • Early • Medium • Medium/late	Government agencies will need to lead by example, and so are likely to become early adopters. With national companies and SMEs, migration will occur on more of an 'as needed' basis

12.3 IPv6 Adoption Guide: Planning Phase

End users need to draw up detailed IPv6 adoption project plans during the planning phase, and start building awareness within their businesses/organizations. This phase should also include identifying core business applications, developing an IPv6 business plan, conducting an internal IPv6 readiness audit, building IPv6 skills among staff, and building confidence in IPv6 through 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 vary considerably between a SMEs and large multinationals. The range of estimates for the duration of tasks provided in the following sections reflects differences in the scale of activities.

12.3.1 IPv6 Awareness

It is beneficial to raise awareness of IPv6 within the organization, to ensure that the importance of IPv6 adoption, the key areas of impact, the costs and the timelines are shared across the organization. A few key aspects to be considered when preparing to raise awareness of IPv6 in an organization are shown in Figure 12.2.

Figure 12.2: Summary of IPv6 awareness activity for end users

IPv6 awareness

Purpose:

To raise IPv6 awareness across all the organizations' key stakeholders, and to educate them on the importance of IPv6 adoption, the scope of activities required, and the likely timelines

Stakeholders

Senior management, IT management, training department

Tasks to be undertaken

The awareness programme must be targeted at multiple segments:

- **senior management**, covering:
  - importance of IPv6 and the business impact of non-adoption
  - timelines and the cost of IPv6 adoption
- **IT management**, covering:
  - various aspects of network, application and services that would be affected as a result of IPv6 adoption
  - the set of activities to be initiated for the design, implementation and validation of the IPv6 solutions and services
- **IT staff**, covering:
  - IPv6 technology basics
  - the mechanisms for transition to IPv6
  - guidelines for operating and maintaining IPv6-enabled networks and solutions

Dependencies on other parts of the plan?
None
Duration
0.5–2 months

12.3.2 IPv6 Business Requirements Plan

It is important for end users understand the impact of IPv6 on their organization as part of the development of the business requirements plan, which should identify 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 and high-impact services remain the focus for IPv6 adoption.

Business Goals and Drivers

In general, the typical business goals of end-user organizations 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
- Introduce new businesses.

The primary business drivers for IPv6 adoption by **government agencies** range from being ahead of the technology demand curve to business continuity and managing the risk of IPv4 address exhaustion. Government agencies are not heavily dependent on the availability of public IPv4 addresses, as they mostly rely on private IP addressing. During interviews, it was estimated that their current pool of available IPv4 addresses would last for the next three to four years.

Generally, **multinational companies** do not see any business need for early IPv6 adoption, and have not engaged in any activities associated with IPv6 adoption. The drivers 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.

The situation is expected to be generally similar **for SMEs**, in that they will not see any immediate business need for IPv6 adoption. Earlier research[6] has indicated that there is often a lack of understanding of the benefits and capabilities of IPv6.

Typical IPv6 adoption timelines among end users will vary, with government agencies adopting IPv6 first, ahead of the technology curve and then multinational companies and SMEs will follow suit, depending on their business needs.

Return on Investment

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

- **Incremental revenue from IPv6 enablement** – are there any financial benefits (e.g. incremental revenue through the introduction of new value-added services)?

6 Analysys Mason IPv6 SME survey for IDA in Singapore 2010

- **Cost savings from IPv6 deployment** – e.g. will it allow simplification of the network infrastructure, therefore delivering lower costs?
- **Cost implications of IPv6 enablement** – will new or additional hardware be required, will applications need to be upgraded, and what will be the cost of running a dual-stack network initially?

12.3.3 IPv6 Skill Building

IPv6 skill building ensures that all stakeholders across the organization 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 12.3.

Figure 12.3: Summary of IPv6 skill building activity for end users

IPv6 skill building

Purpose:

To ensure that IPv6 skills are built across the various levels of the organization (IT management, IT staff, etc.), so that they can participate in, and contribute to, the IPv6 adoption process, and

To provide skills to the IT department to enable them to implement the IPv6 adoption programme

Stakeholders

HR, training department, IT management, senior technical architects, IT staff

Tasks to be undertaken

The IPv6 skill-building programme encompasses various layers of the organization:

- **senior technical architects/IT management**, with skills covering:
  - IPv6 solution architecture and design
  - IPv6 migration planning and processes
  - IPv6 service design
- **IT staff**, with skills covering:
  - IPv6 technology basics
  - the mechanisms for transition to IPv6
  - operating and maintaining IPv6-enabled networks and solutions

Dependencies on other parts of the plan?

The IPv6 skill building programme cannot commence until:

- the IPv6 awareness tasks have been nearly completed (tasks can start in advance of full completion)

Duration

1–3 months

12.3.4 Project Plan for IPv6 Adoption

The project plan describes detailed activities for IPv6 adoption, including 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; to highlight gaps between the existing position and full IPv6 migration. Figure 12.4 provides a summary of the project planning for the adoption of IPv6, and Figure 12.5 shows an example of an IPv6 readiness audit.

Figure 12.4: Summary of project planning for IPv6 adoption activity for end users

Project plan for IPv6 adoption

Purpose:

To establish the organizations' current status of IPv6 adoption across networks, applications and services, and

To 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

Stakeholders

- **IPv6 work group team** – a team of IPv6 experts (internal and/or external) with responsibility for preparing the project plan for IPv6 adoption. Depending on the organization, this team may have further responsibility for execution of the project plan itself.
- **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.

Tasks to be undertaken

The key tasks in preparing the project plan are:

- establish an IPv6 workgroup team, made up of IPv6 experts to have responsibility for preparing the project plan for IPv6 adoption
- conduct an IPv6 readiness assessment to identify the gaps in IPv6 adoption across network, applications and services
- map the current status of IPv6 adoption
- draw up a detailed project plan for IPv6 adoption.

The IPv6 readiness assessment needs to cover:

- **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
  - there is a need to check the availability of IPv6 addresses
- **application infrastructure** – network management, OSS/BSS, HR, ERP applications, etc.
- **core business applications infrastructure** – the existing and planned business applications and the status of their IPv6 enablement.

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:

- architecture and design
- deployment and implementation
- test and validation
- trials
- 'go live' for IPv6 services.

Dependencies on other parts of the plan?

- 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
- The process is dependent on the ability/willingness of third-party suppliers to engage in the planning process
- The IPv6 business requirements plan needs to be prepared to identify which services will need to be supported by IPv6

Duration

0.5–3 months

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 application 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
Adopt IPv6 in policy and planning ▪ Encourage your IT support team (internal or external) to add IPv6 to its planning ▪ The actual implementation date may be some time off, but it may influence interim decisions

Figure 12.5: An example of IPv6 readiness assessment audit and the sequence of events involved

12.3.5 IPv6 Solution Trial

The IPv6 readiness assessment will identify the IPv6 solutions and business applications to be deployed and rolled out across the organization. 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.

Figure 12.6: Summary of IPv6 solution validation lab activity for end users

IPv6 solution trial

Purpose:

To verify and validate the proposed IPv6-based solution (architecture, design and services) before they are rolled out in a live environment

Stakeholders

Technical architects, IT management

Tasks to be undertaken

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:

- **IPv6 network solution**
  - the network solution proposed needs to be tested for adherence to functional and performance guidelines and SLAs
- **IPv6 application solution**
  - the various commercial and proprietary applications must be validated for their ability to function under the IPv4/IPv6 solution proposed, to a level that meets functional and performance requirements within the organization
- **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

The project plan will need to be reviewed and revised as appropriate based on the output of the validation trials

Dependencies on other parts of the plan?

IPv6 solution trial cannot commence until:

- the IPv6 skill building programme is completed
- the IPv6 business applications plan is underway (as applications to be validated need to be identified – although this programme can start slightly ahead of the identification of business applications)

Duration

2–3 months

12.3.6 Quick Wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organization, 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 12.7 summarises this activity, and also provides a couple of examples of quick-win initiatives.

Figure 12.7: Summary of IPv6 'quick-win' activity for end users

IPv6 quick wins
Purpose: *To identify and implement 'quick-win' projects,* and *To strengthen the IPv6 thought process, develop and embed theoretical skills, and build confidence in IPv6 as a technology*
Stakeholders
Corporate IT management team, procurement team, technical architects
Tasks to be undertaken
The projects chosen will depend on the current status and are difficult to specify, but examples could include: • **IPv6 enable the external-facing websites**, which would help the organization to position itself as an IPv6 leader and also establish IPv6 as an internal initiative • **participate in national technology trials and test-beds**, which would provide insights that will increase familiarity with IPv6 and inform decision-making
Dependencies on other parts of the plan?
The IPv6 quick wins cannot commence until: • the IPv6 awareness programme is completed • the IPv6 skill-building programme is completed
Duration
2–3 months

12.4 IPv6 Adoption Guide: Architecture and Design Phase

This phase involves transition designs for the network, applications and services to allow a dual-stack environment, 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 IPv4 services that are planned to be IPv6-enabled, and finalising the new business applications to be introduced, based on work carried out in 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.
- **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.

12.4.1 Architecture and Design – Networks

A network solution architecture and design can now be prepared, following the finalisation of the architecture and design for the IPv6 services; this will ensure it is aligned with core business applications.

The network solution architecture needs to consider the various stages in the migration (e.g. IPv4 only, support for both IPv4 and IPv6, and IPv6 only). Given the current position in terms of IPv4 address availability, the solution should also consider a back-up solution for a scenario where the organization has run out of IPv4 addresses, but has not completed the transition to IPv6.

Figure 12.8: Summary of IPv6 network solution architecture and design activity for end users

IPv6 network solution architecture and design

Purpose:

To 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

Stakeholders

Technical architects, IT management, IT staff

Tasks to be undertaken

Ensure that the IPv6 network solution architecture and design – of both core and access networks – cover the following areas:

- **IPv4/IPv6 interconnectivity** – the various tunnelling mechanisms, dual stack, etc.
- **IPv6 routeing** – allowing the reachability of the network elements across IPv4 and IPv6 topologies to be ensured (via routeing protocols)
- **IPv6 security** – security aspects of the planned network roll-out must be considered and be in place
- **QoS** – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance
- **multicast services** – these services across the IPv6 network must be designed in accordance with the planned services
- **traceability of traffic sessions** – if required for regulatory purposes, recording of the various IPv6 sessions taking place across the network should be incorporated

Dependencies on other parts of the plan?

IPv6 network solution architecture and design cannot commence until:

- the IPv6 readiness assessment and project plan are completed
- the architecture and design for services are completed, or almost completed

Duration

1–2 months

12.4.2 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 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 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.

12.4.3 Architecture and Design – Applications

Once the IPv6 network architecture is finalised, an application architecture and design, which are aligned with it 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 12.9.

Figure 12.9: Summary of IPv6 application solution architecture and design activity for end users

IPv6 application solution architecture and design

Purpose:

To prepare an IPv6 application solution architecture and design, which will help enable IPv6 on the current IPv4-based services and introduce new IPv6 services

Stakeholders

Technical architects, IT staff, vendors

Tasks to be undertaken

The IPv6 application solution architecture and design needs to cover the following areas:

- ensure **network management and monitoring applications/solutions** are seamlessly able to support and monitor IPv4 and IPv6 networks
- ensure **applications such as ERP and CRM systems** are able to support IPv6 and IPv4-based connectivity and services
- **ensure proprietary applications** are able to support both IPv6 and IPv4-based connectivity services

Dependencies on other parts of the plan?

The IPv6 application solution architecture and design cannot commence until:

- the IPv6 readiness assessment and project plan are completed
- the architecture and design for *services* are completed.

The architecture and design for *networks* can be prepared in parallel.

Duration

1–2 months

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.

12.5 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 end user organization.

12.5.1 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. By comparing the solution architecture and design for the networks, applications and services and the outcomes of the IPv6 readiness assessment, organizations can prepare a list of the infrastructure that would need to be upgraded. 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 12.10.

Figure 12.10: Summary of IPv6 deployment and implementation activity for end users

IPv6 deployment and implementation

Purpose:

To deploy IPv6 across the network and applications to support the launch of IPv6 services

Stakeholders

Technical architects and IT staff

Tasks to be undertaken

The IPv6 deployment and implementation would cover the following areas:

- **infrastructure IPv6 upgrade** – the hardware and firmware systems will need to be upgraded or replaced if they are not IPv6 ready
- **IPv6 connectivity** – IPv6 addresses needs to be purchased and IPv6 connectivity must be established with upstream providers and other peers
- **applications and service operations** – the various applications such as network management, monitoring, CRM, etc. will need to be IPv6 enabled
- **services** – services will need to be IPv6 enabled

Dependencies on other parts of the plan?

IPv6 deployment and implementation cannot commence until

- the IPv6 service, network and application architecture are mostly completed

Duration

3–4 months

IPv6 testing and validation will be the next activity.

Figure 12.11: Summary of IPv6 testing and validation activity for end users

IPv6 testing and validation

Purpose:

To validate IPv6 services and applications across the internal/external networks and also the ISP

Stakeholders

Technical architects and IT staff

Tasks to be undertaken

IPv6 testing and validation will cover the following areas of IPv6 products and services:

- **IPv4/IPv6 connectivity** will be validated
- **IPv6 routeing** – the network elements across IPv4 and IPv6 topologies need to be reachable through the appropriate IPv6 routeing protocol
- **IPv6 security** – the security aspects of the network need to be validated
- **QoS** aspects need to be validated across the network
- **multicast services** as per the service design need to be validated across the network
- **applications** – various applications in use need to be validated for IPv6 support, including proprietary systems
- **IPv6 compliance/certification (optional)** – the IPv6 services need to be tested against a range of certifications or compliance measurement programmes

Dependencies on other parts of the plan?

The IPv6 testing and validation cannot commence until the IPv6 services solution roll-out is completed

Duration

3–6 months

12.5.2 IPv6 Trials

The next stage, once the network and applications have been IPv6-enabled, and the solutions have been tested and validated, 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.

12.5.3 IPv6 'go live'

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.

12.6 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** – from first to third-line support via a help desk
- **Specialist support** – access to support from external suppliers of hardware and applications.

13 IPv6 Adoption Governance/Transition Management

The adoption governance and transition management strategy defines how the IPv6 implementation plan will apply internal controls to itself. It will include:

- Criteria to assess effectiveness
  - periodically assess progress of IPv6 implementation against target metrics, e.g. surveys, measurement of IPv6 traffic levels, take-up of IPv6 addresses
- How projects will be monitored
  - meeting programme milestones
  - remaining within budget
- What standards will be applied to the projects
  - IETF, IPv6 Forum as appropriate
- What controls will be in place include decision authority
  - IPv6 task force
  - design authority
- Information that will be required for monitoring
  - benchmark data on peer Countries
  - requirements specified by international standards bodies
- Escalation routes for managing exceptions
  - regulatory at national level
  - internal route for individual players
- Any links to independent assurance such as programme reviews.

13.1 Key Adoption Challenges

To ensure the programme plan is successfully implemented, it is important to identify and understand the various IPv6 adoption challenges being faced in Qatar, in order to ensure that they are addressed as part of the IPv6 adoption plan and strategy. The following list, while not exhaustive, covers the main criteria, as follows:

- Level of content availability on IPv6
- Readiness of products and services
- Dependence from other stakeholders (national and international levels)
- Customer adoption barriers
- Internal organizational challenges, e.g. decision makers residing outside of Qatar.

ictQATAR can also help facilitate measures to improve IPv6 awareness generally at a national level, with a number of initiatives that either organize and/or sponsor, as follows:

- Support of the IPv6 task force for Qatar
- Support/incentives from regulators/government
- Industry forums in Qatar
- Education (universities, events, etc.).

Gaining an understanding of the challenges faced through an ongoing dialogue with stakeholders will help ictQATAR focus on areas of concern that require intervention.

13.2 Documentation Templates and Documentation Roadmap

As part of the IPv6 adoption governance and monitoring mechanism, ictQATAR will create a knowledge base in terms of IPv6 adoption planning templates and various reporting templates. The document categories planned would be as follows:

- Planning IPv6 adoption
- Assessing IPv6 readiness
- IPv6 technical architecture
- IPv6 enterprise architecture
- IPv6 adoption audit.

14 IPv6 Procurement Plan and Budget Planning

This section describes the generic procurement plan and budget planning for network infrastructure equipment, systems and third-party applications concerned with IPv6 deployment.

The procurement plan and budget planning defines the procurement requirements and budget for the network infrastructure equipment, systems and third-party applications, and how the process will be managed from developing procurement documentation through to contract closure. The procurement plan and budget details the following:

- Items to be procured with justification statements and timelines
- Outline budget
- Type of contract to be used
- Contract approval process
- Decision criteria
- Contract deliverables and deadlines.

This procurement management plan sets the procurement framework to deliver the IPv6 Implementation Plan. It will serve as a guide for managing procurement throughout the life of the project and will be updated as acquisition needs change. This plan identifies and defines the items to be procured, the types of contracts to be used in support of this project, the contract approval process, and decision criteria. The importance of co-ordinating procurement activities, establishing firm contract deliverables, and metrics in measuring procurement activities is included.

14.1 Items To Be Procured

The procurement requirements will vary according to the organization and nature of the networks they use. If the planning process is started early enough, the amount of specific procurement effort for IPv6 will be minimised by ‘piggy backing’ IPv6 requirements on to the back of other procurement work streams; for example, if a hardware refresh for LAN and WAN equipment is planned, the requirements for IPv6 can be simply incorporated into the equipment specification.

In general, the list will include the following categories:

- Training
- Specialist consultancy
- Project management
- WAN services procured from a third party
- Network hardware owned by the organization, e.g. switches, routers etc.
- Computing platforms, e.g. servers, PCs etc.
- OS
- Mainstream applications (MS Office etc.)
- Specialist applications (SAP, Oracle etc.)
- New applications that are launched specifically using IPv6, e.g. a large-scale M2M application
- Standalone procurement exercise, although could include some upgrading of existing infrastructure
- New IPv6-specific projects, e.g. IPv6 Web hosting facility.

14.2 Budget Outline

Budgets for business-as-usual IPv6 implementation will vary substantially depending on the situation, but if deployment is planned across a 3–4-year window, it is likely that the majority of systems can be made 'IPv6 ready' during the normal technology refresh cycle at little or no additional cost. At a minimum though, provision for training of technical support staff and project management effort should be made in the budget.

Where there is a requirement to shorten the IPv6 readiness cycle, either because there is a need to launch IPv6 services earlier or if the implementation process is delayed, then additional budget may need to be allocated.

In the case of new IPv6-specific projects, a standalone business case with an associated budget would need to be established.

14.3 Inclusion of IPv6 in Future Procurement Specification

It is recommended that IPv6 compatibility is included in all relevant future procurement specifications. This may not require IPv6 to be up and running on day 1, but it should be achieved by a defined date, and, in general, at no additional cost – both should be contractually binding.

15 IPv6 Training

The training for IPv6 implementation is an early prerequisite for all stakeholder groups, with the content and depth varying according to the individual's role.

A generic framework for IPv6 training requirements is detailed in Figure 15.1, specifying target audience, subject matter and duration.

Figure 15.1: Proposed IPv6 training

Programme name	Target audience	Details to be covered	Approx. duration
IPv6 awareness programme	Decision makers – CXOs Executive management Programme Managers	Need for IPv6 Impact of IPv6 on IT infrastructure Budgetary implications of IPv6 adoption IPv6 project management	8 hours
Introduction to IPv6	Technical Architects/Designers Network Implementation team Network Maintenance team	Introduction to IPv6 IPv6 addressing DHCPv6 and DNSv6 IPv6 routeing	16 hours
IPv6 adoption across enterprises	Technical Architects/Designers Network Implementation team Network Maintenance team	Introduction to IPv6 IPv6 addressing, DHCPv6, DNSv6 IPv6 transition mechanisms IPv6 security IPv6 applications	40 hours
IPv6 adoption across service providers	Technical Architects/Designers Network Implementation team Network Maintenance team	IPv6 routeing IPv6 across MPLS IPv6 multicast IPv6 troubleshooting IPv6 network management	40 hours
IPv6 security	Security Architects/Designers Security Implementation team Security Maintenance team	IPv6 perimeter security IPv6 host security IPv6 transition security IPv6 security best practices	40 hours
IPv6 system administration	System Administration Architects Systems Implementation team Systems Maintenance team	IPv6 provisioning on client systems IPv6 desktop security IPv6 Web servers IPv6 mail servers IPv6 network management server IPv6 enterprise security IPv6 transition techniques for System Administrators	40 hours
IPv6 software development	Software Architects Software Implementers Software Maintenance Engineers	IPv6 overview IPv6 in Java IPv6 in .Net IPv6 in PHP Programming for applications/protocols Porting IPv4 applications to IPv6 Debugging IPv6 programs	40 hours

The IPv6 training roadmap for Qatar will ideally need to be completed over a duration not exceeding circa three years. The first six months will focus on building national awareness of IPv6, followed by a period of more specific training on IPv6 networking, security programs and system administration programs. A high-level target sequence and timeline for training is depicted in Figure 15.2.

Figure 15.2: Training timeline [Source: Analysys Mason, 2013]

Name	Target audience	6 months	12 months	18 months	24 months	30 months	36 months
Awareness programmes	Decision makers: CxOs Executive management Programme Managers						
Introduction to IPv6	Technical Architects/Designers Network Implementation team Network Maintenance team						
IPv6 adoption across service providers	Technical Architects/Designers Network Implementation team Network Maintenance team						
IPv6 adoption across enterprises	Technical Architects/Designers Network Implementation team Network Maintenance team						
IPv6 security	Security Architects/Designers Security Implementation team Security Maintenance team						
IPv6 system administration	System Administration Architects Systems Implementation team Systems Maintenance team						
IPv6 programming	Software Architects Software Implementers Software Maintenance Engineers						

The IPv6 awareness programmes would need to be conducted first. The goal would be to inform senior management of the need for, and importance of, IPv6, the budgetary impact and project planning aspects.

Following the IPv6 awareness programmes, technical programmes related to IPv6 design and deployment across organizations would be initiated. IPv6 technical training programmes should include an introduction to IPv6, to design and deployment programmes for service providers and enterprises.

Subsequent to the introductory IPv6 courses, IPv6 architecture and design should be conducted, (enabling Qatari architects and designers to be equipped with those related skills). After that, courses in the area of IPv6 deployment, troubleshooting and maintenance should be conducted, whereby the network implementation and maintenance engineers would need to be equipped with the appropriate IPv6 skills.

In addition to general IPv6 design and deployment programmes, specialist courses in the area of IPv6 security, programming and system administration would need to be conducted, so that end-to-end skills in IPv6 are built across the country.

In addition to the training programme, it is imperative that ictQATAR conducts a series of seminars and conferences in IPv6 and related technologies/applications over the period to maintain the momentum of the programme. The seminars and conferences should endeavour to involve stakeholders from the local industries and also from the neighbouring nations.

The seminars and conferences would evolve over time in term of content. Initially, they would focus on sharing an understanding of the IPv6 technologies, followed by seminars detailing deployment and adoption strategies, then seminars/conferences focused on applications and innovations that would serve the environment in Qatar.

16 IPv6 Strategy Conclusions

The timely implementation of IPv6 across the Qatar IP ecosystem is essential if the country is to continue its economic growth.

The Internet now fuels growth in many facets of modern society, including business, education, health and entertainment, so a failure to provide the necessary infrastructure to support the continuing expansion of the Internet will have a detrimental impact on the nation's future economic and general development.

The dominance of Ooredoo as the incumbent national operator for both Internet services and fixed networks, means there is a heavy dependency on its active participation in an IPv6 implementation programme to enable the majority of other stakeholders to commence their migration.

A key theme for the strategy is to provide national implementation guidelines for each of the main stakeholder groups to ensure a coherent and co-ordinated approach is taken. There are four basic stages, comprising familiarisation, planning, implementation and launch, the implications of which will significantly vary depending on the type of stakeholder; for example, the implications for a service provider will be far greater than for an SME. There will also be variations in the relative starting and completion points for activities on the timeline for each stakeholder category, with hardware and software vendors generally being the leading stakeholder group, followed by service providers and, finally, end users.

In addition to adopting IPv6 into business-as-usual activities, there are potentially further options for developing new business opportunities, supporting IPv6-based services. In particular, hosting local IPv6 websites in Qatar would be a key opportunity for serving the home market and the other Gulf States. This would require the establishment of suitable peering arrangements, and the proposed Internet exchange point for Qatar would be ideally placed for providing this facility.

There are some significant changes in the provision of the security mechanisms between the IPv4 and IPv6 protocol stacks. The IPv6 stack has a number of significant enhancements over IPv4, but it is important to understand these fully before opening live IPv6 services. The arrangements for dual-IPv4/6 working add a degree of complexity because both domains must be adequately protected, particularly in terms of security resilience and data loss protection, with the latter meeting the associated government compliance rules.

A key instrument for supporting the IPv6 readiness programme will be the launch of the Qatar IPv6 task force. This will bring together all the key stakeholders into a body sponsored (initially at least) by ictQATAR with a brief to provide support across the ecosystem. The task force will also have a co-ordinating role to allow stakeholders to share information, provide a link between end users and service providers, act as a conduit for information distribution, and generally ensure the introduction of IPv6 into Qatar is achieved in a timely, efficient and secure manner.