Ministry of Information and Communication Technology

National IPv6 Implementation Strategy for the State of Qatar

Consultation Document

RATANM 2012-30
July 2013
# Table of Contents

1. **Background** ......................................................................................................................... 4
2. **Consultation Questions** ......................................................................................................... 5
3. **Instructions for Responding to this Consultation** ................................................................. 5
4. **Introduction** ........................................................................................................................ 7
5. **Summary of findings from Qatar’s IPv6 Assessment Study** ..................................................... 8
   5.1 IPv6 implementation plan for the state of Qatar ................................................................. 8
   5.2 Conclusions .......................................................................................................................... 9
6. **Current IPv6 adoption strategy and implementation plan** ..................................................... 10
7. **IPv6 Implementation/Adoption Roadmap and Project Plan** .................................................. 11
   7.2.1 Create an IPv6 task force ............................................................................................... 11
   7.3.1 Educational and awareness ......................................................................................... 12
   7.3.2 Industry development and collaboration .................................................................. 13
8. **Adoption roadmap** ................................................................................................................ 18
9. **IPv6 Taskforce** ................................................................................................................... 19
10. **IPv6 Taskforce Activities** .................................................................................................... 21
    10.1 Training and Awareness ................................................................................................. 21
    10.2 Monitor IPv6 Action Plan and Network implementation ................................................ 21
    10.3 Standards and Specifications ....................................................................................... 21
    10.4 IPv6 Transition ............................................................................................................. 21
    10.5 IPv6 Test Bed .............................................................................................................. 21
    10.6 Pilot Project .................................................................................................................. 22
    10.7 Applications support ..................................................................................................... 22
    10.8 Knowledge Resource development ............................................................................ 22
    10.9 IPv6 implementation in the Government ................................................................ 22
11. **IPv6 adoption: System vendors** ......................................................................................... 23
    11.1 IPv4 exhaustion timelines and business impact ............................................................... 23
12. **IPv6 adoption guide: Internet Service Providers** ................................................................... 24
    12.1 IPv6 adoption guide: overall summary ........................................................................... 24
    12.2 IPv4 exhaustion timelines and business impact ............................................................. 25
    12.3 IPv6 adoption guide: planning phase ............................................................................. 25
       IPv6 awareness .................................................................................................................. 26
       IPv6 business services plan ............................................................................................. 26
       IPv6 skill building ............................................................................................................ 28
       Project plan for IPv6 adoption ....................................................................................... 29
       IPv6 solution validation lab ............................................................................................. 30
    Quick wins 31
    12.4 IPv6 adoption guide: architecture and design phase ....................................................... 31
       Architecture and design – services ................................................................................... 31
       Options for transition approaches/mechanisms for network architecture and design ....... 36
    1.1.2 Architecture and design – applications ....................................................................... 37
    12.5 IPv6 adoption guide: deployment phase .......................................................................... 39
       12.5.1 IPv6 deployment and implementation .................................................................. 39
       12.5.2 Infrastructure IPv6 upgrade .................................................................................... 40
       12.5.3 IPv6 connectivity .................................................................................................. 40
       12.5.4 Core network ........................................................................................................ 40
       12.5.5 Access network ..................................................................................................... 40
       12.5.6 Applications and service operations ....................................................................... 41
12.5.7 Services ........................................................................................................... 41
12.5.8 IPv6 test and validation ................................................................................... 41
12.5.9 IPv6 trials ...................................................................................................... 43
12.5.10 IPv6 ‘go live’ ............................................................................................... 43
12.6 IPv6 adoption guide: ongoing support phase ...................................................... 43
12.6.1 IPv6 service support ...................................................................................... 44
12.6.2 Review IPv4 plans ....................................................................................... 44

13 IPv6 adoption guide: Network providers .............................................................. 45
13.1 IPv6 adoption guide: overall summary .............................................................. 45
13.2 IPv4 exhaustion timelines and business impact ................................................ 45
  13.2.1 Mobile operators ......................................................................................... 45
13.3 IPv6 adoption guide: planning phase ............................................................... 46
  13.3.1 IPv6 awareness .......................................................................................... 46
  13.3.2 IPv6 business services plan ........................................................................ 46
  13.3.3 Project plan for IPv6 adoption ..................................................................... 47
  13.3.4 IPv6 solution validation lab ........................................................................ 47
  13.3.5 Quick wins .................................................................................................. 47
13.4 IPv6 adoption guide architecture and design phase .......................................... 47
  13.4.1 Network operators ..................................................................................... 47
  13.4.2 Mobile operators ....................................................................................... 48
13.5 IPv6 adoption guide: deployment phase ............................................................ 48
  13.5.1 IPv6 deployment and implementation ....................................................... 48
  13.5.2 IPv6 test and validation ............................................................................. 49
  13.5.3 IPv6 trials .................................................................................................. 49
  13.5.4 IPv6 ‘go live’ ............................................................................................. 49
13.6 IPv6 adoption guide: ongoing support phase .................................................... 49
  13.6.1 IPv6 service support .................................................................................. 49
  13.6.2 Review IPv4 plans ..................................................................................... 49

14 IPv6 adoption guide: Service providers ............................................................... 50
14.1 IPv6 adoption guide: overall summary ............................................................. 50
14.2 IPv4 exhaustion timelines and business impact ................................................ 50
14.3 IPv6 adoption guide: planning phase ............................................................... 51
  14.3.1 IPv6 awareness .......................................................................................... 51
  14.3.2 IPv6 software compatibility check .............................................................. 51
  14.3.3 IPv6 skill building ...................................................................................... 52
  14.3.4 Project plan for IPv6 adoption ..................................................................... 52
  14.3.5 Equipment refresh ..................................................................................... 53
  14.3.6 Quick wins .................................................................................................. 54
14.4 IPv6 adoption guide: architecture and design phase ........................................ 54
  14.4.1 Architecture and design – networks ............................................................ 54
  14.4.2 Architecture and design – systems and services ......................................... 55
14.5 IPv6 adoption guide: deployment phase ............................................................ 56
  14.5.1 IPv6 deployment and implementation ....................................................... 56
  14.5.2 IPv6 test and validation ............................................................................. 56
  14.5.3 IPv6 trials .................................................................................................. 56
  14.5.4 IPv6 ‘go live’ ............................................................................................. 57
14.6 IPv6 adoption guide: ongoing support phase .................................................... 57

15 IPv6 adoption guide: End users ........................................................................... 58
15.1 IPv6 adoption guide: overall summary ............................................................. 58
15.2 IPv4 exhaustion timelines and business impact ................................................ 59
15.3 IPv6 adoption guide: planning phase ............................................................... 59
  15.3.1 IPv6 awareness .......................................................................................... 59
  15.3.2 IPv6 business requirements plan ............................................................... 60
  15.3.3 Business goals and drivers ....................................................................... 60
  15.3.4 Return on investment ................................................................................ 62
  15.3.5 IPv6 skill building ...................................................................................... 62
  15.3.6 Project plan for IPv6 adoption ................................................................... 63
15.3.7 IPv6 solution trial ................................................................. 64
15.3.8 Quick wins ........................................................................ 65
15.4 IPv6 adoption guide: architecture and design phase ...................... 66
  15.4.1 Architecture and design – networks ..................................... 66
  15.4.2 Architecture and design – transition technology approaches/mechanisms .................................................. 67
  15.4.3 Architecture and design – applications .................................. 67
15.5 IPv6 adoption guide: deployment phase ........................................... 68
  15.5.1 IPv6 deployment and implementation ................................... 68
  15.5.2 IPv6 trials ........................................................................ 69
  15.5.3 IPv6 ‘go live’ ..................................................................... 69
15.6 IPv6 adoption guide: ongoing support phase ................................... 69

16 IPv6 adoption governance/transition management ................................ 70
  16.1 Key adoption challenges .......................................................... 70
  16.2 Documentation templates and documentation roadmap .................. 71

17 Procurement plan and budget planning ............................................... 72
  17.1 Items to be procured ................................................................ 72
  17.2 Budget outline ....................................................................... 72
  17.3 Inclusion of IPv6 in future procurement specification ..................... 73

18 Training .................................................................................... 74

19 Conclusions ................................................................................ 79
1 Background

The Internet Assigned Numbers Authority (IANA) announced in February 2011 that its pool of IPv4 addresses was finally exhausted. While 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 must be adopted at some stage, it is apparent that preparations around the world to mitigate the effects of the forecast exhaustion of IPv4 have been limited to date. This is largely due to the fact that existing users do not see any pressing need for adopting IPv6.

Governments have therefore started to play an increasingly active role in encouraging IPv6 adoption, and recognize that intervention is required to minimise the disruption and impact that would otherwise be caused by the global exhaustion of IPv4 addresses.

There are a number of reasons why the market has generally failed to act in a timely manner to adopt IPv6, including:

- The lack of hard deadlines associated with the need to adopt IPv6, and the fact that earlier forecasts of exhaustion dates proved pessimistic
- The fact that the current ‘work-arounds’ of using Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) have proved adequate to date, making the end-user community generally indifferent to the need to adopt IPv6
- A lack of understanding of the business and financial benefits of adopting IPv6, which means that there has been little incentive for end-user organisations to consider migrating from IPv4
- Inadequate promotion of IPv6 to customers by the supply side of the market, which has led to a perception that IPv6-ready equipment and services are not available in the market.

This suggests that a more proactive approach may be required from governments and regulators 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 minimise the impact of the exhaustion of IPv4 addresses on individual stakeholders and productivity.
2 Consultation Questions

In-keeping with an open, transparent process Ministry of Information and Communication Technology invites stakeholders to express their views on the issue and/or to respond to the questions raised below:

1. Do you accept the general principle/timeframes proposed for IPv6 implementation in Qatar to enable continued development of the national IP ecosystem?
2. Do you consider the findings of Ministry of Information and Communication Technology’s study into the current state of IPv6 readiness in Qatar are representative for your sector and others you are familiar with?
3. Do you consider the recommendations and timescales associated with the implementation activities for your sector to be reasonable and achievable?
4. Would your organization be willing to participate in the ‘IPv6 Task Force’ that is proposed in this strategy document.
5. Do you consider the brief for the Task Force to be sufficiently comprehensive to meet your organisations needs, if not please provide suggestions as to how the scope should be changed to achieve these needs.
6. Have you identified any other shortcomings or omissions in this IPv6 strategy document that you feel should be addressed for completeness?

3 Instructions for Responding to this Consultation

3.1 Consultation Procedures

All interested parties are invited to submit responses to the questions specifically identified in this document and to provide their views on any other relevant aspects. Comments should reference the number of the question being addressed or the specific section of this document if not responding to a particular question.

Ministry of Information and Communication Technology asks that, to the extent possible, submissions be supported by examples or relevant evidence. Any submissions received in response to this consultation will be carefully considered by Ministry of Information and Communication Technology when progressing to revised RAS Instruction. Nothing included in this consultation document is final or binding. However, Ministry of Information and Communication Technology is under no obligation to adopt or implement any comments or proposals submitted.

Responses should be submitted by email to Eng. Omer El Farouk, Technical Affairs Dpt. (omohammed@ict.gov.qa) and the deadline for receipt is close of business on 5th of September 2013.

Any submissions received in response to this consultation will be carefully considered by Ministry of Information and Communication Technology when preparing the Order. Nothing included in this consultation document is final or binding. However, Ministry of Information and Communication Technology is under no obligation to adopt or implement any comments or proposals submitted.
3.2 Publication of Comments

In the interests of transparency and public accountability, Ministry of Information and Communication Technology intends to publish the submissions to this consultation on its website at www.ictqatar.qa. All submissions will be processed and treated as non-confidential unless confidential treatment of all or parts of a response has been requested.

In order to claim confidentiality for information in submissions that stakeholders regard as business secrets or otherwise confidential, stakeholders must provide a non-confidential version of such documents in which the information considered confidential is blacked out. This “blackened out” text should be contained in square brackets. From the non-confidential version it has to be clear where information has been deleted. To understand where redactions have been made, stakeholders must add indications such as “business secret”, “confidential” or “confidential information”.

A comprehensive justification must be provided for each and every part of the submission required to be treated as confidential. Furthermore, confidentiality cannot be claimed for the entire document or whole sections of the document as it is normally possible to protect confidential information with limited redactions.

While Ministry of Information and Communication Technology will endeavor to respect the wishes of respondents, in all instances the decision to publish responses in full, in part or not at all, remains at the sole discretion of Ministry of Information and Communication Technology. By making submissions to Ministry of Information and Communication Technology in this consultation, respondents will be deemed to have waived all copyright that may apply to intellectual property contained therein.

If you have any questions or concerns, please contact Eng. Omer Mohammed (ofdul@ict.gov.qa), Internet Domain Section Manager directly.
4 Introduction

This consultation document presents a draft strategic plan for the national implementation of IPv6 in the state of Qatar. It includes an implementation and adoption roadmap, tasks involved with governance and transition management and the associated budget planning & procurement activities. Ministry of Information and Communication Technology are seeking the views of the various stakeholders across the ICT sector in Qatar on this draft strategic plan.

Ministry of Information and Communication Technology has recently undertaken a study into the state of IPv6 readiness across the State of Qatar IP ecosystem, the output of this study has been used in the development of this strategic plan for the national implementation of IPv6. This includes an implementation and adoption roadmap, tasks involved with governance and transition management, and procurement & budget planning.

Ministry of Information and Communication Technology believe that the timely adoption of IPv6 by Qatar’s ICT ecosystem can be best achieved if it is driven by a focused team dedicated to the task. Ministry of Information and Communication Technology therefore propose to spearhead an IPv6 task force led by the Technology and Planning Group. 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 their opinions on what government support they felt could be beneficial in encouraging the deployment of IPv6, both for themselves and the wider ecosystem. The proposed strategy takes these views into account.
5 Summary of findings from Qatar’s IPv6 Assessment Study

The initial phase evaluated existing plans and performed a high level assessment, based on questionnaire response and face-to-face interviews, of the current infrastructure. It then went on 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 an education and awareness 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 we identified were compared with an ideal ‘should be’ situation based on our industry knowledge.

The road map presented in Figure 5.1 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 Premise Equipment (CPE) not being IPv6 compatible.

5.1 IPv6 implementation plan for the state of Qatar

A high-level implementation plan to deliver IPv6 across Qatar’s IP ecosystem is shown in Figure 5.1. Proposed activities during 2014 are to enable Qatar DNS or (Qatar Domains Registry System) 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 taskforce for State of Qatar would further this aim.

Figure 5.1: High-level IPv6 implementation plan for Qatar
5.2 Conclusions

Whilst the IPv6 readiness study demonstrated that Qatar compares reasonably well with its peer group countries, there is a need to commence a number of measures to ensure IPv6 readiness is achieved across the national IP ecosystem in a timely manner.

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 however clear 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. The potential for gaining a Return On Investment (ROI) through early adoption of IPv6 may exist in some areas e.g. hosting of regional IPv6 web sites, and are worthy of further investigation.

The dominant role of Ooredoo 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 organisations consulted identified Ooredoo 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 measures.
6 Current IPv6 adoption strategy and implementation plan

6.1 Current IPv6 adoption strategy

The Phase 1 analysis concluded that whilst Qatar compares reasonably well with its peer group countries, there is a need to commence a number of measures including the creation of an IPv6 Adoption strategy in order to ensure IPv6 readiness is achieved across the national IP ecosystem in a timely manner.

6.2 IPv6 transition strategy

As part of understanding an organisation’s stage of adoption, an assessment was made of the available IPv6 transition strategy, where they existed. In the absence of a comprehensive national IPv6 adoption strategy few transition plans were found to be in place.

6.3 Current IPv6 implementation

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

There was found to be minimal IPv6 implementation currently 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. Understanding this will helped assess the implementation status across the various stakeholder segments of the Qatar IT eco-system. This helped in developing and refining the IPv6 adoption strategy for Qatar.
7 IPv6 Implementation/Adoption Roadmap and Project Plan

7.1 Introduction

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

- Planning: creation of an IPv6 task force. During this phase, plans for the wider national strategy will be finalised.
- Implementation: instigation of an IPv6 awareness and education programme in collaboration with suppliers and industry bodies on a national, regional and global basis. During this phase, financial support will also be provided to persuade enterprise stakeholders to become early adopters. In addition, a few government-based ‘quick win’ projects will be identified to build confidence and understanding of IPv6.
- Support: an on-going initiative to provide appropriate support to stakeholders in Qatar’s ICT ecosystem until IPv6 readiness is achieved, continue the work of the centre for innovation, and continue liaison with supplier and industry bodies.

7.2 Planning phase

During the planning phase Ministry of Information and Communication Technology will need to establish the environment required to foster IPv6 adoption across the IT ecosystem in Qatar.

7.1.1 Create an IPv6 task force

An IPv6 taskforce will be established which draws expert resources from within Ministry of Information and Communication Technology, as well as other relevant government, academia and private sector organisations, to ensure that a cross-functional view is taken of the requirements for transition to IPv6 and minimise duplication of effort. The role of the task force will be to facilitate, 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 Qatar is seen as a regional leader in deployment of the technology.

Key aspects to be considered when establishing the IPv6 task force are shown in Figure 7.1.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>The role of the task force will be to facilitate, fund and/or regulate the implementation of the entire national strategy, making sure that Qatar’s ICT ecosystem is ready for the arrival of IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approx. duration</td>
<td>2–3 months</td>
</tr>
</tbody>
</table>
Key tasks

The key tasks in creation of the IPv6 task force are:

- To recruit personnel – identify and recruit a strong leadership team and a dedicated workforce comprising individuals with skills in project and programme management and ICT, as well as internal and/or external IPv6 experts. We suggest that individuals could be seconded from Ministry of Information and Communication Technology or other government organisations, plus representatives from the stakeholder community.
- To agree the terms of reference – define the task force’s mission in terms of high-level goals and programme duration.
- To define the governance structure – its aims and objectives, executive management involvement, communications and reporting, project management, operations management, structure/process choices and decision making authority.
- (Potentially) To source suitable operating facilities (locate and procure appropriate office accommodation for the task force team).

Stakeholders

Ministry of Information and Communication Technology, other government organisations, nominations from the stakeholder community and academia.

Figure 7.1: Summary of the activities required to establish an IPv6 task force

7.3 Strategy Implementation phase

Following the establishment of a task force, implementation of the IPv6 national strategy will involve three key areas of activity, as identified by stakeholders during the survey phase and confirmed from international examples of similar initiatives:

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

7.3.1 Educational 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 organisations, and to Qatar’s economy as a whole.

International initiatives of the kind discussed in Section 0 demonstrate that governments in collaborations with other stakeholders in other countries 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 7.2 summarises a number of tasks that might be used to educate the stakeholder community and raise IPv6 awareness in Qatar.

Overall aims

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

Approx. duration

12-24 months.

---

\(^1\) SMEs were not covered in the survey, but experience from other national surveys conducted around the world have shown awareness in this group to be generally lower than for larger organisations.
Key tasks

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

- organise the establishment of special interest groups, fora and seminars to share best practice and learnings from IPv6 implementation by early adopters within Qatar and, potentially, by organisations overseas
- provide centralised resources for training and skills development among technical staff
- collaborate with vendors to develop and provide detailed technical training on IPv6-based products
- identify and document best practice in IPv6 migration, and develop case studies and white papers for specific sectors
- run demonstrations of IPv6 implementations, including workshops on IPv6 configuration
- organise and host regional/global conferences on IPv6
- encourage academic research and projects related to IPv6, as a way of both developing IPv6 skills among recent graduates, and developing new and innovative solutions and services

Stakeholders

IPv6 task force, Ministry of Information and Communication Technology and government organisations, system vendors, service providers, academia

Dependencies

The success of this series of activities is highly dependent on the existence of the IPv6 task force (to run it and to provide a repository for documentation and educational material).

Figure 7.2: Summary of activities required to raise awareness and provide IPv6 education

7.3.2 Industry development and collaboration:

A key area in which the government can encourage IPv6 adoption across the ICT ecosystem relates to industry development and collaboration. Several stakeholders indicated that the government should be encouraging collaboration between systems vendors and service providers as a key element in 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 7.3.

Overall aims

To ensure that all stakeholder groups within the ICT ecosystem communicate ideas and collaborate in the development of IPv6 adoption

Approx. duration

12–24 months

Key tasks

The key tasks involved in promoting industry development and collaboration on IPv6 are:

- taking a role to ensure imported goods to Qatar are IPv6 compatible
- provide and communicate guidelines on technology solutions and standards to improve confidence and consistency in IPv6 adoption
- provide a clear timeline as to when service providers and other players need to support IPv6 and provide IPv6 services (potentially setting a mandate for this)
- work with regional and global industry bodies and policy makers in other markets to define a unified approach to IPv6
- promote the growth of IPv6 content availability
- develop and promote increased IPv6 peering among suppliers
- position the government as a role model in IPv6 adoption, with the aim of encouraging end users in the private sector to migrate to IPv6
- encourage the development of IPv6 interoperability and international roaming guidelines for mobile operators

Stakeholders

IPv6 task force, Ministry of Information and Communication Technology and other
government organisations, system vendors, service providers, MNOs

**Dependencies**

The success of this series of activities is highly dependent on the existence of the IPv6 task force to run it.

---

**Figure 7.3:** Summary of tasks required to encourage collaboration within the ICT industry in the development of IPv6

### 7.4 On-going support phase

Following the implementation phase, the national strategy will move into a support phase. This will focus on the continuation and expansion of the industry development and collaboration tasks started during the implementation phase, in support of the co-existence of IPv4 and IPv6 and eventual full migration to IPv6.

The support phase of the proposed strategy can be deemed as beginning when the majority of stakeholder organisations within the ICT ecosystem have the capability to operate over the Internet using IPv6, irrespective of whether they use IPv6 or IPv4 on 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.

Following the implementation phase, one of the key elements of the ongoing support phase will be active monitoring by Ministry of Information and Communication Technology of progress towards IPv6 adoption within the ICT ecosystem (e.g. through regular surveys or industry workshops). This will allow Ministry of Information and Communication Technology to review and refine the national strategy as needed, focusing efforts on those areas with the most favourable cost–benefit equation, and will ensure that activities do not continue beyond their useful life.

In addition, the ongoing support phase will need to promote and encourage 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 smart metering) and support for the development of IPv6-capable Operations Support Systems / Business Support Systems (OSS/BSS).

### 7.5 International Benchmarking

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 their “IPv6 transition programme” to encourage IPv6 adoption and it has been running for the last 2 years. The programme is a national effort to address the issue of IPv4 exhaustion and to facilitate the smooth transition of the Singapore Infocomm ecosystem to IPv6. IPv6 transition programme promotes readiness and adoption of IPv6 in the local industry through a series of projects (training, grants, market place, 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, still long way to go’.

- 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. In March 2013 the Office of the Government Chief Information Officer (OGCIO) claimed ‘the Internet Infrastructure in Hong Kong is ready for IPv6 deployment’.

### 7.6 Risks

In this section, the risks and uncertainties linked to the implementation of IPv6, specifically in Qatar are analysed. We discuss the risks from the perspective of the various stakeholders such as System Vendors, End-Users etc. Also discussed are mitigation steps that need to be implemented to ensure that the risks identified are minimised or negated. There are a number of risks identified, and along with potential mitigation measures, are listed in in Figure 7.4 below.

---


### Figure 7.4: Risks and mitigation

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Risk/impact level</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services providers continue with measures to delay IPv6 implementation</td>
<td>Service providers may delay launch of IPv6 services by using measures such as Carrier grade NAT to spin out use of IPv4 address space</td>
<td>Low to med risk/high impact</td>
<td>Ministry of Information and Communication Technology encourage Service Providers to adopt IPv6 at the earliest opportunity.</td>
</tr>
</tbody>
</table>
| IPv4 addresses exhausted | Inability to assign further IP (v4) addresses in Qatar once existing pool is depleted. | Low risk if timetable followed, but increasing 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 | Large proportion of organisations adopt “do nothing” approach such that as a nation Qatar falls behind peer group in terms of the internet infrastructure readiness  
As Qatar develops its knowledge based economy as part of delivering the Qatar National Vision⁴, ICT will be a major enabler and the adoption of IPv6 will therefore be an important component in achieving this. | 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  
• IPv6 task force publish information, organise events etc.  
• Suppliers provide regular IPv6 information updates to their customers  
• Ministry of Information and Communication Technology undertake periodic audits to ensure progress is being made  
• Increase the awareness of impact of deploying IPv6 |
| End users cannot obtain IPv6 addresses/other services | If the end user market wants to implement IPv6 but is prevented due to inability to obtain address blocks, IPv6 compatible network services etc. | Medium risk/high impact | Ministry of Information and Communication Technology 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 RIPE may also be helpful. |
| Lack of IPv6 compatibility on operating systems | Users with Old operating systems like Windows XP unable to access the IPv6 internet sites | Medium risk to SMEs who may not have upgraded to later OS/ Impact will limited to small groups of SMEs | Ensure familiarity levels are raised across all sectors as to need for action. |

---

⁴ [http://www2.gsdp.gov.qa/www1_docs/QNV2030_English_v2.pdf](http://www2.gsdp.gov.qa/www1_docs/QNV2030_English_v2.pdf)
<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Risk/impact level</th>
<th>Mitigation</th>
</tr>
</thead>
</table>
| Security breach                   | A publicised security breach attributed to IPv6 that reduces user confidence and delays implementation | Low risk/ potentially high impact depending on stakeholder | • 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 | Large proportion of current Ooredoo CPE DSL router stock is not IPv6 compatible, this is schedule for change out by 2015, but any delay beyond this would impact IPv6 takeup in the domestic/SOHO and SME markets | Low risk/High impact | Ministry of Information and Communication Technology to monitor situation and encourage Ooredoo to complete the change-out of legacy routers by 2015 |
| Delay in launch of IPv6 DNS in Qatar | Ministry of Information and Communication Technology cannot resource the provision of the national IPv6 DNS in a timely manner | Low risk/High impact | Ministry of Information and Communication Technology to ensure funding and resources are available to establish IPv6 DNS |
8 Adoption roadmap

The implementation/adoption roadmap and project plan will be a living document to be regularly updated at Ministry of Information and Communication Technology programme reviews, and which will as a framework for the monitoring of the programme. Figure 8.1 shows the high-level roadmap which organisations will have to implement in order to launch IPv6 services. While this will vary slightly depending on the organisation type, the overall structure should be followed.

Figure 8.1: IPv6 implementation roadmap
9 IPv6 Taskforce

As previously mentioned, an IPv6 task force to be established which draws resources from the different departments within Ministry of Information and Communication Technology, as well as other relevant government, academia and private sector representatives. This is to ensure that a cross-functional view is taken of the requirements for transition to IPv6 and minimise duplication of effort. The taskforce will be immediately 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 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 9.1.

**Figure 9.1: IPv6 Taskforce key tasks**

<table>
<thead>
<tr>
<th>Key Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raise awareness on the exhaustion of IPv4 &amp; impact of IPv6 on proliferation of Internet and broadband in the country</td>
<td>• Activities related to publicity and education&lt;br&gt;• Organizing training programmes, workshops, conferences and tutorials&lt;br&gt;• Advice to the Government on Policy issues dealing with IPv6</td>
</tr>
<tr>
<td>Encourage all stakeholders to begin the initial phases of IPv6 readiness</td>
<td>• To synchronize the activities of various stakeholders&lt;br&gt;• List up the issues to solve by each player&lt;br&gt;• Information sharing among member organizations&lt;br&gt;• Advise to member organizations on IPv6 technical issues during the transition process&lt;br&gt;• Identification of challenges and solutions using IPv6&lt;br&gt;• Outreach to new stakeholders suffering from IPv4 address exhaustion</td>
</tr>
<tr>
<td>Development of transition plans in subsequent phases to support a smooth and wide transition to IPv6</td>
<td>• Conduct surveys, studies and review of the progress by different organizations and the country as a whole during the transition process</td>
</tr>
<tr>
<td>International cooperation in IPv6 related areas</td>
<td>• Increasing coordination with international organizations, neighbouring and other countries for IPv6 deployment&lt;br&gt;• International collaboration with other similar Task Force organizations throughout the world</td>
</tr>
</tbody>
</table>
10 IPv6 Taskforce 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 organisations, Industry associations, educational institutions and different industry stakeholders. The main activities proposed for the task force are summarized below.

10.1 Training and Awareness

There is a requirement for having an adequate pool of IPv6 trained manpower in the taskforce to perform knowledge transfers in both the government and the private sector. This knowledge transfer will be performed by conducting workshops, seminars and conferences for benefit of all stakeholders following the “Train the Trainer” concept. It will be responsible for developing the trained manpower required by different organizations in the government and the private sector to deal with the different types of IPv6 transition issues.

10.2 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 in their organization. This task force will assist them to create a tailor made action plan for them for transition to IPv6.

10.3 Standards and Specifications

Task force will coordinate with Ministry of Information and Communication Technology for development of common IPv6 specifications for the State of Qatar, which will be followed by all stakeholders. It will also coordinate with the IPv6 Ready Logo committee of the IPv6 Forum to plan and advise different stakeholders and organizations like vendors, Websites etc. for obtaining the IPv6 Ready Logo. It will also interact with other international standardization bodies to participate in various standards and specification development processes.

10.4 IPv6 Transition

The task force will work to plan the IPv6 transition networks which will accommodate dual stacking and coordinate with the service providers/organization to establish this “Transition Pipe” which will then act as an IPv6 backbone network.

10.5 IPv6 Test Bed

During the transition period stakeholders are likely to need an IPv6 network for demonstrating and experimenting with different IPv6 transition scenarios. Ministry of Information and Communication Technology will coordinate 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. Task force will plan and build this IPv6 test network, which can then be used for experimentation by different vendors and organizations both from the public and the private sector. This network can also be used for training of personnel for operating IPv6 networks.
10.6 Pilot Project

IPV6 has many capabilities which are new and do not exist in IPv4. These capabilities can be demonstrated through pilot projects relevant for the industry and Government. These pilot projects will provide the necessary experience for large scale implementations by the organizations. This group will plan, prepare project report, prepare the funding models and coordinate with different government and service providers to take up the deployment of such pilot projects to demonstrate the IPv6 capabilities.

10.7 Applications support

The task force will facilitate the transition of existing content and applications and 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.

10.8 Knowledge Resource development

In addition to different activities it is also important to develop the IPv6 knowledge base in the country. This knowledge base can be developed with active participation of the educational institutes. The members of this working group will be drawn from relevant educational institutes.

10.9 IPV6 implementation in the Government

The task force will pursue with different government organisations for implementation of IPv6. The members will be drawn from officers in various government organisations.
11 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 study the following classifications have been used:

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

They both therefore form a key element of the ICT industry by providing the building blocks on which the rest of the industry operates.

The ability of the wider ICT industry to adopt IPv6 is contingent on hardware and software vendors, including IPv6 support across their product portfolio, and on them ensuring IPv6 interoperability across different vendor solutions. The overall IPv6 enablement of this industry segment is important in initiating and promoting IPv6 adoption – not just in Qatar, but around the world.

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

11.1 IPv4 exhaustion timelines and business impact

As end users begin to plan their IPv6 migration path, they will consult their suppliers to determine when their IPv6-ready products will become available. If end users have a pressing business need to use IPv6 due to the exhaustion of IPv4 addresses, they will require their suppliers to make available IPv6-ready products. The timely availability of IPv6-ready products will be imperative if suppliers are to meet their customers’ needs. If existing 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 preparation 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 the network operator sectors (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.
12 IPv6 adoption guide: Internet Service Providers

Whilst there are no organizations in Qatar whose sole business is to act as an Internet Service Provider (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. The inclusion of IPv6 support in commercial Internet services is essential in the wider adoption of IPv6, and will also help encourage hardware and software vendors to roll out their IPv6-ready solutions. Also, the provision of innovative solutions can also help to increase awareness and adoption of IPv6 in the wider ecosystem.

12.1 IPv6 adoption guide: overall summary

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

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

Details of the four phases, and the activities involved in each, are illustrated in Figure 12.1. We provide details of the key activities within each phase in later sections of this adoption guide.
12.2 IPv4 exhaustion timelines and business impact

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

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

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

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

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

- Businesses across the ecosystem in Qatar that do not have significant remaining IPv4 address pools, or are dependent on Internet service providers for IPv4 addresses, would be unable to procure new broadband connections to support business expansion. Similarly, new enterprises would be unable to obtain a broadband connection, or develop services requiring a public IP address (websites etc.). These two critical issues would have a direct impact on 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.

12.3 IPv6 adoption guide: planning phase

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

An IPv6 awareness programme ensures that the importance of IPv6 adoption, the key areas of impact, the costs and the timelines are shared across the organisation. A few key aspects to be considered when preparing to raise awareness of IPv6 in an organisation are shown in Figure 12.2.

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

Figure 12.2: Summary of IPv6 awareness activity for Internet service providers

IPv6 business services plan

An IPv6 business services plan for an Internet service provider identifies the services that should support IPv6. This provides an essential input to the later activities within the planning phase, and ensures that the high-priority/high-impact services remain the focus for IPv6 adoption. A few key aspects to be considered when preparing an IPv6 business services plan are shown in Figure 12.3; further details specific to Internet service providers are provided in the rest of this subsection.

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

Figure 12.3: Summary of IPv6 business services plan for Internet service providers
Business goals and drivers

The typical business goals of Internet service providers are to:

- **cover a larger consumer base**, including both business and residential consumers, through an increased network footprint and range of broadband access services
- **increase take-up of broadband services** across both business and residential consumers
- **increase take-up of managed or value-added services** by developing new, innovative services and service bundles that can generate incremental, profitable revenue growth.
The above business goals drive the construction of larger networks, higher take-up, and the introduction of new and innovative managed, or value-added, services. This results in increased consumption of IP addresses by Internet service providers and consumers. As indicated by the findings of the survey phase, the incumbent internet service provider is operating predominantly in an IPv4 environment, with core networks currently IPv6 enabled, but access networks and applications still running in an IPv4 environment.

**Service offerings**

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

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

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

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

**Return on investment**

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

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

**IPv6 skill building**

IPv6 skill building ensures that all stakeholders across the organisation have the required skills to contribute to, and participate in, the IPv6 adoption process, including implementation. A summary of the IPv6 skill building activities is provided in Figure 12.4.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>Approx. duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that IPv6 skills are built across the various levels of the organisation (engineering management, engineering staff, etc.), so that they can participate in, and contribute to, the IPv6 adoption process</td>
<td>2–3 months</td>
</tr>
<tr>
<td>Provide skills to engineering teams to enable them to implement the IPv6 adoption programme</td>
<td></td>
</tr>
</tbody>
</table>
Key tasks
The IPv6 skill building programme encompasses various layers of the organisation:

- **senior technical architects/engineering management** – skills in the following areas must be covered:
  - IPv6 solution architecture and design
  - IPv6 migration planning and processes
  - IPv6 service design
- **engineering staff** – the following areas must be covered:
  - IPv6 technology basics
  - the mechanisms for transition to IPv6
  - operating and maintaining IPv6-enabled networks and solutions

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

Dependencies
The IPv6 awareness activity should have been completed before the IPv6 skill building activity begins, although it can be started in advance of full completion of the IPv6 awareness activity.

Figure 12.4: Summary of IPv6 skill building activity for Internet service providers

Project plan for IPv6 adoption

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

**Overall aims**
- Establish the organisation’s current status of IPv6 adoption across network, applications and services
- Draw up a detailed project plan, including the various activities to be completed for IPv6 adoption and a roadmap to ensure provision of seamless IPv6 services

**Approx. duration**
2–3 months

**Key tasks**
The key tasks in preparing the IPv6 adoption project plan are:
- establish an IPv6 consultancy team, made up of internal and / or external IPv6 experts, to have responsibility for preparing the project plan for IPv6 adoption
- 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 project planning for achieving IPv6 readiness mentioned above needs to cover the following areas:
- **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 (HR), enterprise resource planning (ERP) applications, etc.
- **services infrastructure** – the current, and planned, business services offered to customers, 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

Stakeholders

- **IPv6 consultancy team** – a team of internal and/or external IPv6 experts responsible for preparing the project plan for IPv6 adoption. Depending on the organisation, this team may have further responsibility for execution of the project plan itself
- **Engineering management** – will help to provide all the inputs required for the readiness assessment, and will also identify key individuals within the business for this activity

Dependencies

- The IPv6 awareness programme needs to be completed before the IPv6 readiness programme can begin, to ensure that stakeholders understand the importance of the readiness assessment, and are willing to fully participate in it
- The IPv6 business services plan needs to be prepared to identify which services should support IPv6

Figure 12.5: Summary of project planning for IPv6 adoption activity for Internet service providers

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.

| Overall aims | Verify and validate the proposed IPv6-based solution (architecture, design and services) before they are rolled out in a live environment |
| Approx. duration | 2–3 months |
| Key tasks | The IPv6 solution validation lab should ensure that the IPv6 migration solution architecture included in the project plan must be validated in terms of its ability to support the required services (e.g. features and functional and performance aspects). This validation needs to cover: |
| | - **IPv6 network solution** – the network solution proposed in the project plan needs to be tested for adherence to functional and performance guidelines and SLAs within the organisation |
| | - **IPv6 application solution** – the various commercial and proprietary applications must be validated for their ability to function under the IPv4/IPv6 solution proposed in the project plan to a level that meets functional and performance requirements within the organisation |
| | - **IPv6 services** – the business and residential services which are planned to be rolled out need to be validated in terms of functional performance and reliability in the network and application environment laid out in the project plan |
| | The project plan will need to be reviewed and revised, as appropriate, based on the output of the validation lab trials |

Stakeholders

- Technical architects, engineering management

Dependencies

- The start of this programme is dependent on completion of the IPv6 skill building programme
- The IPv6 business services plans needs to be underway before this programme can start, as services to be validated need to be identified (although this
programme can start slightly ahead of the identification of services)

Figure 12.6: Summary of IPv6 solution validation lab activity for Internet service providers

Quick wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organisation, and in giving staff the opportunity to use the theoretical skills they have gained earlier in the process, as well as to build confidence in the technology. Figure 12.7 summarises this activity, and provides a couple of examples of quick-win initiatives.

| Overall aims | Identify and implement initial ‘quick win’ projects
| | Strengthen the IPv6 thought process across the organisation, develop and embed theoretical skills, and build confidence in IPv6 as a technology |
| Approx. Duration | 2–3 months |
| Key tasks | The types of project chosen will depend on the current status of an organisation, and are difficult to specify. However, some examples could include: |
| | **IPV6 enable the external-facing websites**, which would help the organisation to position itself as an IPv6 leader, and also further establish IPv6 as an internal initiative |
| | **participate in national technology trials and test-beds**, which would provide knowledge and insight that will increase familiarity with IPv6, and inform the decision-making process during subsequent phases |
| Stakeholders | Corporate IT management team, procurement team, technical architects |
| Dependencies | The IPv6 awareness programme, and the IPv6 skill-building programmes, should be completed before starting this activity |

Figure 12.7: Summary of IPv6 ‘quick win’ activity for Internet service providers

12.4 IPv6 adoption guide: architecture and design phase

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

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

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

Architecture and design – services

The development of an architecture and design for the IPv6-enabled services to be offered by Internet service providers will affect the network solutions architecture and applications solution architecture that are subsequently developed. The key tasks are identified in Figure 12.8, and are discussed further below.
IPv6 services architecture and design

Overall aims
Build an IPv6 service architecture and design, which will help to ensure existing IPv4 services are IPv6 enabled, and to introduce new IPv6 services accordingly

Approx. duration
1–2 months

Key tasks
- The architecture and design for services needs to develop the design and architecture for IPv6 products and services

Stakeholders
Technical architects, software engineering team, vendors

Dependencies
The IPv6 readiness assessment and project plan need to be completed before this activity can be initiated

Based on the IPv6 products and services identified during the planning phase, the next stage is to develop a design and architecture for these products and services. The architecture and design process needs to consider the various IPv6 transport mechanisms (e.g. dual-stack, Teredo tunnel, ISATAP) as part of the product offering, as well as the IPv6 features required by the products, and any security considerations and SLAs. Architecture and design – networks

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

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

IPv6 network solution architecture and design

Overall aims
Prepare an IPv6 network solution architecture and design which will help to enable IPv6 on the current IPv4-based services and introduce new IPv6 services

Approx. duration
1–2 months

Key tasks
Ensure that the IPv6 network solution architecture and design – of both core and access networks – covers the following areas:
- IPv4/IPv6 interconnectivity – individual IPv4 and IPv6 networks are connected via various tunnelling mechanisms, dual stack, etc.
- IPv6 routing – the reachability of the network elements across IPv4 and IPv6 topologies must be ensured, through appropriate deployment of the IPv6 routing protocol
- IPv6 security – the various network solutions that are designed must ensure that the security aspects of the planned network roll-out are considered and in place
- quality of service (QoS) – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance
- multicast services – the various multicast 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

Stakeholders
Technical architects, engineering management, network engineering team

Dependencies
The IPv6 readiness assessment and project plan need to be completed before this activity can be initiated, and the architecture and design for services needs to be completed, or almost completed
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 routing, IPv6 security, QoS, multicast services, and traceability of traffic sessions. For the core and access networks, these issues are outlined in Figure 12.10.
| IPv6/IPv6 interconnectivity | The IPv6 connectivity across the upstream service provider and peers needs to be considered, based on the services planned. The details of the IPv6 connectivity across the autonomous systems, and the routes to be announced, should also be planned in line with the expected service offerings. The design options that can be considered for providing IPv6 MPLS VPN connections are: configured tunnels; 6PE; 6VPE. | Based on the access network design, the IPv6 connectivity to the core needs to be planned:  
- a Layer 3 access network provider would need to consider forwarding access traffic through the IPv6 core using one (or more) of the following options: IPv6 tunnelling; native IPv6 deployment; MPLS 6PE deployment  
- a Layer 2 access network provider does not have any IPv6 considerations for the access network. |
| IPv6 routing | Based on the services and the IPv6 topologies being rolled out, the related IPv6 routing protocols would need to be selected and IPv6 enabled. This would include:  
- interior gateway routing (IGP) protocol, where the options are IS-IS or OSPFv3  
- exterior gateway routing protocol (EGP), which is delivered using BGP.  
Based on the computing resources of the routers and the performance requirements, the IPv4 and IPv6 routing can be achieved using either a single process or a dual process design. | For the access network, routing options include:  
- static routes  
- RIPng  
- OSPFv3.  
The relevant choice of routing option will depend on the IPv6 services to be rolled out, and the size and topology of the access network. When DHCP prefix delegation is used, route distribution also needs to be considered as part of the access network architecture and design. |
| IPv6 security | The IPv6 security architecture would need to include the deployment of the various mechanisms (such as access lists and intrusion detection/prevention) that are used to provide a secure IPv6 Internet transaction environment. Ingress filtering should be deployed toward the customers to ensure traceability, to prevent DoS attacks using spoofed addresses, and to prevent illegitimate access to the management infrastructure. Ingress filtering can be carried out using access lists or unicast reverse path forwarding. | The access network design should ensure that the Internet service provider’s networks and its subscribers are protected from attacks by one of its own customers. The design options in this area include:  
- unicast reverse path forwarding  
- IPv6 access lists.  
In addition to these, security mechanisms, such as firewalls and IDS/IPS, should be considered. |
| Quality of Service | The IPv6 QoS design should take into consideration the various traffic engineering aspects and performance SLAs, which need to be adhered to, for the various classes of traffic. |  |
| Multicast services | Based on the services planned to be rolled out, the IPv6 multicast services will need to be designed accordingly, which would include BGP-MPLS multicast services. The protocols that can 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 so, 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. |  |

Figure 12.10: Considerations for the design and architecture of core and access networks
Options for transition approaches/mechanisms for network architecture and design

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

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

As the introduction of IPv6 across the network has to be achieved with minimal disruption to the existing network, it should be a gradual transition. The various IPv6 network transition phases for a stakeholder are shown in Figure 12.11.

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

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

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

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

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

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

Once the IPv6 service architecture and the network architecture are finalised, an application architecture and design, which is aligned with them, can be prepared. This will consider the approach to configuring the relevant OSS/BSS, network management and network monitoring applications to support the planned IPv6 services. The key tasks are highlighted in Figure 12.14, and addressed in more detail in the subsequent text.

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

The application infrastructure in an Internet service provider helps in the provision of service offerings to customers. The IPv6 readiness assessment conducted in the planning phase will provide a list of IPv6-compliant and non-compliant applications. Applications that are found to be...
non-IPv6 compliant will need either to be upgraded to an IPv6-compliant version, or replaced with new software that provides the same functionality and is also IPv6 compliant. The key tasks are addressed in more detail in Figure 12.15.
As IPv6 adoption is initiated across network management and monitoring systems, as a first step, network device configuration and regular network management and monitoring operations can be performed over an IPv4 transport layer, as an IPv6 management information base (MIB) can be reached from an IPv4 network. In the case that ICMPv6 messages are used for monitoring, IPv6 connectivity would be required for management applications.

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

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

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

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

Figure 12.15: Key tasks

### 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 organisation.

#### 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 to be able to launch IPv6 service offerings.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>Deploy IPv6 across the network and applications of the Internet service provider to support the launch of IPv6 service offerings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approx. duration</td>
<td>3–4 months</td>
</tr>
<tr>
<td>Key tasks</td>
<td>The IPv6 deployment and implementation would cover the following areas:</td>
</tr>
<tr>
<td></td>
<td>• <strong>infrastructure IPv6 upgrade</strong> of the hardware and software systems (if they are not IPv6 ready), or replacement with IPv6-compliant software</td>
</tr>
<tr>
<td></td>
<td>• <strong>IPv6 connectivity</strong> – IPv6 addresses are purchased, and IPv6 connectivity with upstream providers and other peers is established</td>
</tr>
<tr>
<td></td>
<td>• <strong>core network</strong> – IPv6 is adopted across the core network, comprising the network, security, applications, services elements</td>
</tr>
<tr>
<td></td>
<td>• <strong>access network</strong> – the IPv6 network is adopted across the access network wherein the network elements, routing, security, applications, services etc. are upgraded to IPv6</td>
</tr>
<tr>
<td></td>
<td>• <strong>applications and service operations</strong> – the various applications, such as network management, monitoring, customer relationship management, etc. are IPv6 enabled</td>
</tr>
<tr>
<td></td>
<td>• <strong>services</strong> – the various services spread across the business and residential customers are IPv6 enabled</td>
</tr>
</tbody>
</table>

**Stakeholders**

Technical architects, network engineering team and software engineering team

**Dependencies**

The IPv6 service, network and application architecture need to be mostly completed before deployment and implementation can be started
12.5.2 Infrastructure IPv6 upgrade

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

12.5.3 IPv6 connectivity

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

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

12.5.4 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 developed in the previous activity. As such, it should consider the areas outlined earlier in Figure 12.10, namely:

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

12.5.5 Access network

The access network primarily comprises the network from the edge of the core to the customer premises. During this task, IPv6 will be enabled in the access network, based on the network architecture and design developed. As such, it will consider the areas outlined earlier in Figure 12.10 (IPv4/IPv6 interconnectivity, IPv6 routing, IPv6 security, QoS, multicast services, and traceability of traffic sessions).

<table>
<thead>
<tr>
<th>Area for consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4/IPv6 interconnectivity</td>
<td>IPv6 connectivity of the access network to the core should be deployed according to the design through 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.</td>
</tr>
<tr>
<td>IPv6 routing</td>
<td>Based on the network design, the routing protocol (e.g. RIPng, OSPFv3) should be configured. Where DHCP prefix delegation is used, the route distribution would also be configured.</td>
</tr>
<tr>
<td>IPv6 security</td>
<td>The access network design is configured to provide security in an IPv6 environment through the use of unicast reverse path forwarding, IPv6 access lists, and security mechanisms, such as a firewall, IDS/IPS, etc.</td>
</tr>
<tr>
<td>Quality of service</td>
<td>The IPv6 QoS design should be configured across the network to ensure that</td>
</tr>
</tbody>
</table>
the traffic engineering requirements and SLAs committed to the customers are met

<table>
<thead>
<tr>
<th>Multicast services</th>
<th>If required as part of the network design, IPv6 multicast would be enabled using IGMPv3/MLDv2 protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceability of traffic sessions</td>
<td>Traceability of traffic sessions is implemented by recording and logging the details of the traffic sessions. This is accomplished by mapping a DHCP response to a physical connection and storing the results in a database. It can also be achieved by assigning a static address or prefix to the customer, or through the use of a tunnel server</td>
</tr>
</tbody>
</table>

Figure 12.17: Considerations for the access network design for Internet service providers

12.5.6 Applications and service operations

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

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

Figure 12.18: Considerations for the application and service operation design for Internet service providers

12.5.7 Services

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

<table>
<thead>
<tr>
<th>Area for consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business services</td>
<td>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</td>
</tr>
<tr>
<td>Residential services</td>
<td>Data, voice and video service to the customers are IPv6 enabled</td>
</tr>
</tbody>
</table>

Figure 12.19: Considerations for service design for Internet service providers

12.5.8 IPv6 test and validation

A summary of IPv6 test and validation activities for Internet service providers is set out in Figure 12.20

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>Validate IPv6 services across the network and applications across the Internet service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approx. duration</td>
<td>3–4 months</td>
</tr>
<tr>
<td>Key tasks</td>
<td>IPv6 test and validation will cover the following areas of business and residential IPv6 products and services:</td>
</tr>
<tr>
<td></td>
<td>• IPv4/IPv6 connectivity will be validated</td>
</tr>
</tbody>
</table>
IPv6 routing the network elements across IPv4 and IPv6 topologies will be reachable through the appropriate IPv6 routing protocol

IPv6 security – the security aspects of the network will be validated

QoS aspects will be validated across the network

multicast services as per the service design will be validated across the network

applications – the various applications will be validated for their IPv6 support

traceability of traffic sessions – the various IPv6 sessions established across the network will be recorded for regulatory purposes, and the reliability of the system will be validated

IPv6 compliance / certification (optional) – the IPv6 services are tested against a range of certifications or compliance measurement programmes

Stakeholders Technical architects, network engineering team, software engineering team

Dependencies The IPv6 services solution roll-out should be completed

Figure 12.20: Summary of IPv6 test and validation activity for Internet service providers

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

IPv4/IPv6 interconnectivity – organisations should verify the 'reachability' of individual IPv6 networks through IPv4 networks in which IPv6 transition mechanisms are implemented. Similarly, the reachability of IPv4 networks through an IPv6 network should also be verified.

IPv6 routing – organisations should verify the ability to navigate the IPv6 topology through the implemented IPv6 routing protocol. This includes verifying that the routing tables include all the IPv6 routes that are required to reach the various elements in the IPv6 topology.

IPv6 security – organisations should verify and validate the IPv6 security implemented across the network by conducting vulnerability and penetration tests.

QoS – organisations should verify the performance and reliability of the various classes of QoS that have been implemented, by injecting traffic and conducting stress tests.

Multicast – organisations should validate the ability of various multicast services to distribute services in a seamless manner, by assessing service performance against pre-determined specifications.

Applications – organisations should validate the functional and performance aspects of various applications and related solutions in an IPv6 environment.

Traceability of traffic sessions – organisations should validate that the various IPv6 traffic sessions are being correctly recorded/logged, and that the implemented tracing system is reliable.

IPv6 compliance / certification (optional) – once all other test and validation tasks have been completed, an Internet service provider may choose to apply for IPv6 compliance or certification testing to indicate that their services meet known standards. Currently, no standards or certifications have been mandated in Qatar, so this step is optional for Internet service providers. Details of the compliance and certification programmes that are currently available, including a summary of what each of these measure, is available in Annex C.
12.5.9 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 Internet service provider is to run a commercial IPv6 trial with a few customers.

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

Figure 12.21: Summary of IPv6 trials activity for Internet service providers

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.

12.5.10 IPv6 ‘go live’

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

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

Figure 12.22: Summary of IPv6 ‘go live’ trials activity for Internet service providers

12.6 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.
12.6.1 IPv6 service support

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

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

Figure 12.23: Summary of IPv6 service support activity for Internet service providers

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.

12.6.2 Review IPv4 plans

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

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

Figure 12.24: Summary of IPv4 review plans for Internet service providers

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

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

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

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

Fixed national network providers offering IP connectivity (ISPs) are included within Section 12 above. Carriers can provide services at a purely national level and/or on an international basis.

13.1 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 12.1):

13.2 IPv4 exhaustion timelines and business impact

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

13.2.1 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.

---

5 Note that Ooredoo and Vodafone both provide wire line and wireless services in the product portfolio.
13.3 IPv6 adoption guide: planning phase

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

13.3.1 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 organisation. The IPv6 awareness programme for network operators is, essentially, the same as that set out for ISPs (see section 0).

13.3.2 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 0). Those aspects specific to operators are set out below.

13.3.2.1 Business goals and drivers

The typical business goals of network providers are to:

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

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

13.3.2.2 Service offerings

The typical business service offerings of network providers across 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
- wireless networks (fixed) – offering Internet connectivity via an ISP or, potentially, IPv6 connectivity on an any-to-any basis across a VPN cloud.
13.3.2.3 Return on investment

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

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

13.3.3 Project plan for IPv6 adoption

The structure of the project plan for IPv6 adoption is, essentially, the same as that set out for the Internet Service Provider (set out in section 0).

13.3.4 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.

13.3.5 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.

13.4 IPv6 adoption guide architecture and design phase

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

13.4.1 Network operators

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

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

13.5 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 organisation.

13.5.1 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.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>Deploy IPv6 across the fixed and wireless networks to support the launch of IPv6 service offerings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approx. duration</td>
<td>12–24 months</td>
</tr>
</tbody>
</table>

**Key tasks**

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

**Stakeholders**

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

**Dependencies**

The IPv6 service, network and application architecture need to be mostly completed before deployment and implementation can begin

![Figure 13.1: Summary of IPv6 deployment and implementation activity for network providers](image)

13.5.1.1 Infrastructure IPv6 upgrade

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

13.5.2 IPv6 test and validation

IPv6 test and validation activities for network operators are similar to those set out for Internet service providers is set out in section 12.5.8. The test and validation activities help in assessing the reliability and performance of the various business and residential services.

13.5.3 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 12.5.9)

13.5.4 IPv6 ‘go live’

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

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

13.6 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.

13.6.1 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.

13.6.2 Review IPv4 plans

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

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

- **Data centre operators** play an important role in the ICT ecosystem by hosting and supporting the back-end systems of various organisations across Qatar. As these organisations make progress towards adopting IPv6, the back-end systems hosted by data centre operators will also need to be capable of adopting IPv6.

- **ASP/web hosting providers** play a significant role in the ICT ecosystem of Qatar, by providing shared services for the various organisations across the country, which help them to make cost savings and access ‘best of breed’ technology. ASP/web hosting providers will need to ensure that the services they offer end users support IPv6, either by confirming that proprietary applications support IPv6, or by working with vendors to source IPv6-enabled applications.

- **Content providers** also play an important role in the Internet ecosystem, as they create and provide the information which is accessed and exchanged across the Internet. Their role involves making the Internet useful and valuable to users through the continued creation of new applications and tools which have an impact on daily life (including entertainment, search engines, communication and collaboration tools, etc.).

14.1 IPv6 adoption guide: overall summary

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

As with the Internet service provider stakeholder group, the four main phases of IPv6 adoption are: planning, architecture and design, deployment and support.

14.2 IPv4 exhaustion timelines and business impact

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

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

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

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

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

14.3.1 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 organisation. Some key aspects to be considered when preparing to raise awareness of IPv6 in a service provider are shown in Figure 14.1.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>Raise IPv6 awareness across all key stakeholders associated with the organisation to educate them on the importance of IPv6 adoption, the scope of activities to be accomplished, and the likely timelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approx. duration</td>
<td>1–2 months</td>
</tr>
<tr>
<td>Key tasks</td>
<td>The awareness programme must be targeted at multiple segments:</td>
</tr>
<tr>
<td></td>
<td>• <strong>senior management and sales/marketing</strong> – the following aspects must be covered:</td>
</tr>
<tr>
<td></td>
<td>− importance of IPv6, and the business impact of non-adoption</td>
</tr>
<tr>
<td></td>
<td>− timelines and the cost of IPv6 adoption</td>
</tr>
<tr>
<td></td>
<td>− various aspects of network, application and services that would be affected as a result of IPv6 adoption</td>
</tr>
<tr>
<td></td>
<td>− the set of activities to be initiated to design, implement and validate the IPv6 solutions and services</td>
</tr>
<tr>
<td></td>
<td>• <strong>engineering staff</strong> – the following must be covered:</td>
</tr>
<tr>
<td></td>
<td>− IPv6 technology basics</td>
</tr>
<tr>
<td></td>
<td>− the mechanisms for transition to IPv6</td>
</tr>
<tr>
<td></td>
<td>− guidelines for operating and maintaining IPv6-enabled networks and solutions</td>
</tr>
<tr>
<td></td>
<td>• <strong>customers and suppliers</strong> – the following must be covered:</td>
</tr>
<tr>
<td></td>
<td>− importance of IPv6, and the business impact of non-adoption</td>
</tr>
<tr>
<td></td>
<td>− timelines for IPv6 adoption</td>
</tr>
<tr>
<td></td>
<td>− various aspects of network, application and services that would be affected as a result of IPv6 adoption</td>
</tr>
</tbody>
</table>

| Stakeholders | Senior management, engineering management and staff, sales and marketing, training department, customers and suppliers |
| Dependencies | No dependencies on other tasks |

Figure 14.1: Summary of IPv6 awareness activities for service providers

14.3.2 IPv6 software compatibility check

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

### Overall aims

- Carry out a comprehensive audit of the existing software environment in order to ascertain whether applications and system software is ready for the upgrade to IPv6
- Provide information software developers and suppliers to enable them to implement code changes needed as part of the IPv6 adoption programme

### Approx. duration

2–3 months

### Key tasks

The IPv6 software compatibility check primarily involves operational staff, for example:

- **senior technical architects/IT management** – checks on the following areas must be covered:
  - software components offered as part of a service to customers
  - operating systems software
  - data centre automation packages
  - operational management systems

- **IT development staff** – the following areas must be covered:
  - application programming interfaces
  - operating system calls
  - network management protocol calls
  - system management routines

### Stakeholders

IT management, senior technical architects, IT staff

### Dependencies

The IPv6 software compatibility check shall be carried out as early as possible in the upgrade process in order to allow time for corrective action to be taken, if required.

---

**Figure 14.2:** Software compatibility checks for service providers

### 14.3.3 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 0.

### 14.3.4 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’. 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 14.3).

### Overall aims

- Establish the current status of IPv6 adoption across the service provider’s network, applications and services
- Draw up a detailed project plan, including the various activities to be completed for IPv6 adoption and a roadmap to ensure provision of seamless IPv6 services
Approx. duration 2–3 months

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

- 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 mentioned above needs to cover the following areas:

- **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 (HR), enterprise resource planning (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

Stakeholders

- **IPv6 work group team** – a team of internal and/or external IPv6 experts responsible for preparing the project plan for IPv6 adoption. Depending on the organisation, this team may have further responsibility for execution of the project plan itself
- **IT management** – will help to provide all the inputs required for the readiness assessment, and will also identify key individuals within the business for this activity

Dependencies

- The IPv6 awareness programme needs to be completed before the IPv6 readiness programme can begin, to ensure that stakeholders understand the importance of the readiness assessment, and are willing to participate fully in it
- The IPv6 business requirements plan needs to be prepared, to identify which services will need to be supported by IPv6

Figure 14.3: Summary of project planning for IPv6 adoption activity for service providers

14.3.5 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 their infrastructure are replaced at regular intervals. As part of this process, it is good business practice to ensure that all hardware components requiring access to an IP addresses are procured as IPv6 compliant (or capable of running dual protocol stacks) as part of the requirements specification.

Overall aims

- Ensure that IPv6 compatibility is guaranteed within all hardware procured by the organisation
- Include IPv6 in all requirements specifications for new hardware

Approx. duration Ongoing
Key tasks

The IPv6 skill building programme encompasses various layers of the organisation:

- **senior technical architects/IT management** – skills in the following areas must be covered:
  - ensure that IPv6 compatibility is included within all technical specifications

- **procurement staff** – the following areas must be covered:
  - ensure that IPv6 compatibility is drafted in to all supply contracts for computer hardware

Stakeholders

IT management, senior technical architects, IT staff, procurement department

Dependencies

None

Figure 14.4: Equipment refresh for service providers

14.3.6 Quick wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organisation, and in giving IT staff the opportunity to use the theoretical skills they have gained earlier in the process, as well as to build confidence in the technology. Essentially this is the same process as set out for ISPs in section 0.

14.4 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 various network solutions to support the planned IPv6 services, including the IPv4 run-out scenario and transition to a complete IPv6-only ecosystem.

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

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

Overall aims

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

Approx. duration

1–6 months
Key tasks

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

- **IPv4/IPv6 interconnectivity** – individual IPv4 and IPv6 networks are connected via various tunnelling mechanisms, dual stack, etc.
- **IPv6 routing** – the reachability of the network elements across IPv4 and IPv6 topologies must be ensured, through appropriate deployment of the IPv6 routing protocol.
- **IPv6 security** – the various network solutions that are designed must ensure that the security aspects of the planned network roll-out are considered and in place.
- **Quality of service (QoS)** – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance.
- **Multicast services** – the various multicast 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.

Stakeholders

Technical architects, IT management, IT staff

Dependencies

The IPv6 readiness assessment and project plan need to be completed before this activity can begin, and the architecture and design for services needs to be completed, or almost complete.

Figure 14.5: Summary of IPv6 network solution architecture and design activity for service providers

14.4.2 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 14.6.

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

Figure 14.6: Summary of IPv6 application solution architecture and design activity for service providers
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.

14.5 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 organisation.

14.5.1 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.

| Overall aims | Deploy IPv6 across the network and applications to support the launch of IPv6 services |
| Approx. duration | 3 months |
| Key tasks | The IPv6 deployment and implementation will cover the following areas: |
| | • **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 are purchased and IPv6 connectivity with upstream providers and other peers is established |
| | • **applications and service operations** – the various applications, such as network management, monitoring, customer relationship management, etc. are IPv6 enabled |
| | • **services** – the various services spread across the organisations are IPv6 enabled |
| Stakeholders | Technical architects and IT staff |
| Dependencies | The IPv6 service, network and application architecture need to be mostly completed before deployment and implementation can begin |

Figure 14.7: Summary of IPv6 deployment and implementation activity for service providers

14.5.2 IPv6 test and validation

IPv6 test and validation activities for are, essentially, the same as those set out for ISPs in Figure 12.20

14.5.3 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 12.5.9.
14.5.4 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.

14.6 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** – first- through to third-line support via a help desk
- **Specialist support** – access to support from external organisations that have supplied hardware and applications.
15 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, in that 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 visibly taking 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 organisations in this sector vary substantially, and so there is no single approach to deploying IPv6 that will suit all SMEs.

15.1 IPv6 adoption guide: overall summary

For end users, 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.
15.2 IPv4 exhaustion timelines and business impact

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

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

- Businesses across the ecosystem in Qatar that do not have significant remaining IPv4 address pools, 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 organisations, which would thus affect business procedures, processes and practices.

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

<table>
<thead>
<tr>
<th>Category of end user</th>
<th>Expected timing of IPv6 adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>Early/medium</td>
</tr>
<tr>
<td>National</td>
<td>Early</td>
</tr>
<tr>
<td>SME</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Medium/late</td>
</tr>
</tbody>
</table>

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.

Figure 15.1: Relative timing of IPv6 adoption across categories of end user

15.3 IPv6 adoption guide: planning phase

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

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

15.3.1 IPv6 awareness

It is beneficial to raise awareness of IPv6 within the organisation, to ensure that the importance of IPv6 adoption, the key areas of impact, the costs and the timelines are shared across the
organisation. A few key aspects to be considered when preparing to raise awareness of IPv6 in an organisation are shown in Figure 15.2.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>Raise IPv6 awareness across all key stakeholders within the organisation to educate them on the importance of IPv6 adoption, the scope of activities to be accomplished, and the likely timelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approx. duration</td>
<td>0.5–2 months</td>
</tr>
<tr>
<td>Key tasks</td>
<td>The awareness programme must be targeted at multiple segments:</td>
</tr>
<tr>
<td></td>
<td>• senior management – the following aspects must be covered:</td>
</tr>
<tr>
<td></td>
<td>– importance of IPv6, and the business impact of non-adoption</td>
</tr>
<tr>
<td></td>
<td>– timelines and the cost of IPv6 adoption</td>
</tr>
<tr>
<td></td>
<td>• IT management – the following aspects must be covered:</td>
</tr>
<tr>
<td></td>
<td>– various aspects of network, application and services that would be affected as a result of IPv6 adoption</td>
</tr>
<tr>
<td></td>
<td>– the set of activities to be initiated for the design, implementation and validation of the IPv6 solutions and services</td>
</tr>
<tr>
<td></td>
<td>• IT staff – the following must be covered:</td>
</tr>
<tr>
<td></td>
<td>– IPv6 technology basics</td>
</tr>
<tr>
<td></td>
<td>– the mechanisms for transition to IPv6</td>
</tr>
<tr>
<td></td>
<td>– guidelines for operating and maintaining IPv6-enabled networks and solutions</td>
</tr>
</tbody>
</table>

Figure 15.2: Summary of IPv6 awareness activity for end users

15.3.2 IPv6 business requirements plan

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

15.3.3 Business goals and drivers

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

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

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, MNCs do not see any business need for early IPv6 adoption, and have not engaged in any activities associated with IPv6 adoption. The business driver that would lead them to IPv6
adoption is business continuity and the need to manage the risk of IPv4 address exhaustion; IPv6 is not perceived as an enabler of new services, market share improvement or profit increase.
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 MNCs and SMEs will follow suit, depending on their business needs.

### 15.3.4 Return on investment

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

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

### 15.3.5 IPv6 skill building

IPv6 skill building ensures that all stakeholders across the organisation have the required skills to contribute to, and participate in, the IPv6 adoption process, including implementation. A summary of the key tasks for skills building is provided in Figure 15.3.

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

---

\(^6\) Analysys Mason IPv6 SME survey for IDA in Singapore 2010
15.3.6 Project plan for IPv6 adoption

The project plan for IPv6 adoption sets out the detailed set of activities to be carried out, spanning IPv6 solution architecture, design, deployment, trials and ‘go live’. During the process of developing a detailed project plan, the end user must also carry out an IPv6 readiness assessment covering network and applications. This assessment will highlight gaps between the current status and the eventual target of providing seamless IPv6 services and information that will serve as inputs to the detailed project plan. Figure 15.4 provides a summary of the project planning for the adoption of IPv6, and Figure 15.5 shows an example of an IPv6 readiness audit.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>Key tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish the organisation’s current status of IPv6 adoption across network, applications and services</td>
<td>establish an IPv6 workgroup team, made up of internal and/or external IPv6 experts, with responsibility for preparing the project plan for IPv6 adoption</td>
</tr>
<tr>
<td>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</td>
<td>conduct an IPv6 readiness assessment to identify the gaps in IPv6 adoption across network, applications and services</td>
</tr>
<tr>
<td>Approx. duration 0.5–3 months</td>
<td>map the current status of IPv6 adoption</td>
</tr>
<tr>
<td>Key tasks</td>
<td>draw up a detailed project plan for IPv6 adoption</td>
</tr>
</tbody>
</table>

The IPv6 readiness assessment mentioned above needs to cover the following areas:

- **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, human resources (HR), enterprise resource planning (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

**Stakeholders**

- **IPv6 work group team** – a team of internal and/or external IPv6 experts responsible for preparing the project plan for IPv6 adoption. Depending on the organisation, this team may have further responsibility for execution of the project plan itself
- **IT management** – will help to provide all the inputs required for the readiness assessment and will also identify key individuals within the business for this activity
Dependencies

- The IPv6 awareness programme needs to be completed before the IPv6 readiness programme can begin, to ensure that stakeholders understand the importance of the readiness assessment and are willing to participate fully in it
- 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

Figure 15.4: Summary of project planning for IPv6 adoption activity for end users

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

Assess business requirements

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

Determine core business applications

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

Policy and planning

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

Figure 15.5: An example of IPv6 readiness assessment audit and the sequence of events involved

15.3.7 IPv6 solution trial

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

Overall aims

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

Approx. duration

2–3 months
Key tasks

The IPv6 solution trial lab should ensure that the IPv6 migration solution architecture included in the project plan is validated in terms of its ability to support the required business application (e.g. features and functional and performance aspects). This validation needs to cover:

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

Stakeholders

Technical architects, IT management

Dependencies

- The start of this programme is dependent on completion of the IPv6 skill building programme.
- The IPv6 business applications plan needs to be underway before this programme can start, as applications to be validated need to be identified (although this programme can start slightly ahead of the identification of business applications)

Figure 15.6: Summary of IPv6 solution validation lab activity for end users

15.3.8 Quick wins

The initiation of a few small IPv6 projects is important in emphasising the importance of the IPv6 adoption process within the organisation, and in giving IT staff the opportunity to use the theoretical skills they have gained earlier in the process, as well as to build confidence in the technology. Figure 15.7 summarises this activity, and also provides a couple of examples of quick-win initiatives.

| Overall aims | Identify and implement initial ‘quick-win’ projects  
|            | Strengthen the IPv6 thought process across the organisation; develop and embed theoretical skills, and build confidence in IPv6 as a technology |
| Approx. duration | 2–3 months |

Key tasks

The types of project chosen will depend on the current status of an organisation and are difficult to specify. However, some examples could include:

- **IPv6 enable the external-facing websites**, which would help the organisation to position itself as an IPv6 leader and also further establish IPv6 as an internal initiative
- **participate in national technology trials and test-beds**, which would provide knowledge and insight that will increase familiarity with IPv6 and inform the decision-making process during subsequent phases

Stakeholders

Corporate IT management team, procurement team, technical architects

Dependencies

The IPv6 awareness programme and the IPv6 skill-building programmes should be completed before starting this activity

Figure 15.7: Summary of IPv6 ‘quick win’ activity for end users
15.4 IPv6 adoption guide: architecture and design phase

This phase of the adoption activities involves transition designs for the network, applications and services to allow IPv4 and IPv6 to co-exist and work simultaneously during the transition to IPv6, and to support the introduction of new IPv6 services. The IPv6 solution architecture and design phase needs to cover the areas outlined below.

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

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

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

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

15.4.1 Architecture and design – networks

Once the architecture and design for the IPv6 services are finalised, a network solution architecture and design that is aligned with core business applications will have to be prepared. The network solution architecture will need to consider the various stages through which the organisation’s network will pass (e.g. IPv4-only, support for both IPv4 and IPv6, and IPv6-only). Based on the current status of IPv6 readiness and IPv4 address availability, the solution should consider a back-up solution for a scenario in which the organisation has run out of IPv4 addresses, but has not yet fully adopted IPv6.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approx. duration</td>
<td>1–2 months</td>
</tr>
<tr>
<td>Key tasks</td>
<td>Ensure that the IPv6 network solution architecture and design – of both core and access networks – cover the following areas:</td>
</tr>
<tr>
<td></td>
<td>• IPv4/IPv6 interconnectivity – individual IPv4 and IPv6 networks are connected via various tunnelling mechanisms, dual stack, etc.</td>
</tr>
<tr>
<td></td>
<td>• IPv6 routing – the reachability of the network elements across IPv4 and IPv6 topologies must be ensured, through appropriate deployment of the IPv6 routing protocol</td>
</tr>
<tr>
<td></td>
<td>• IPv6 security – the various network solutions that are designed must ensure that the security aspects of the planned network roll-out are considered and in place</td>
</tr>
<tr>
<td></td>
<td>• quality of service (QoS) – performance of the planned IPv6 services must meet the SLAs, and must not affect IPv4 service performance</td>
</tr>
<tr>
<td></td>
<td>• multicast services – the various multicast services across the IPv6 network must be designed in accordance with the planned services</td>
</tr>
<tr>
<td></td>
<td>• traceability of traffic sessions – if required for regulatory purposes, recording of the various IPv6 sessions taking place across the network should be incorporated</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Technical architects, IT management, IT staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependencies</td>
<td>The IPv6 readiness assessment and project plan need to be completed before this</td>
</tr>
</tbody>
</table>
activity can be initiated, and the architecture and design for services needs to be completed, or almost completed

Figure 15.8: Summary of IPv6 network solution architecture and design activity for end users

15.4.2 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.

15.4.3 Architecture and design – applications

Once the IPv6 network architecture is finalised, an application architecture and design, which is aligned with them, can be prepared. This will also consider the approach to configuring the relevant OSS/BSS, network management and network monitoring applications to support management of the planned IPv6 services. The key tasks are highlighted in Figure 15.9.

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

Figure 15.9: Summary of IPv6 application solution architecture and design activity for end users

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.
15.5 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 organisation.

15.5.1 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. Based on a comparison of the solution architecture and design (across networks, applications and services) and the findings of the IPv6 readiness assessment from the planning phase, organisations can prepare a list of the infrastructure that would need to be upgraded to IPv6 to support the planned services and products. The process of upgrading this infrastructure should be initiated as a first step in the deployment of IPv6. A summary of deployment and implementation activities is provided below in Figure 15.10.

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

Figure 15.10: Summary of IPv6 deployment and implementation activity for end users

IPv6 test and validation will be the next activity.

<table>
<thead>
<tr>
<th>Overall aims</th>
<th>Validate IPv6 services and applications across the internal/external networks/external and also the Internet service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approx. duration</td>
<td>1–4 months</td>
</tr>
<tr>
<td>Key tasks</td>
<td>IPv6 test and validation will cover the following areas of IPv6 products and services:</td>
</tr>
<tr>
<td></td>
<td>• IPv4/IPv6 connectivity will be validated</td>
</tr>
<tr>
<td></td>
<td>• IPv6 routing – the network elements across IPv4 and IPv6 topologies will be reachable through the appropriate IPv6 routing protocol</td>
</tr>
<tr>
<td></td>
<td>• IPv6 security – the security aspects of the network will be validated</td>
</tr>
<tr>
<td></td>
<td>• QoS aspects will be validated across the network</td>
</tr>
<tr>
<td></td>
<td>• multicast services as per the service design will be validated across the network</td>
</tr>
<tr>
<td></td>
<td>• applications – the various applications in use will be validated for their IPv6 support, to include any proprietary systems</td>
</tr>
<tr>
<td></td>
<td>• IPv6 compliance / certification (optional) – the IPv6 services are tested against a range of certifications or compliance measurement programmes</td>
</tr>
</tbody>
</table>
Table 15.11: Summary of IPv6 test and validation activity for end users

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Technical architects and IT staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependencies</td>
<td>The IPv6 services solution roll-out should be completed</td>
</tr>
</tbody>
</table>

15.5.2 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 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.

15.5.3 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.

15.6 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** – first- through to third-line support via a help desk
- **Specialist support** – access to support from external organisations that have supplied hardware and applications.
16 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.**

16.1 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, whilst 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 organisational challenges e.g. decision makers reside outside of Qatar.

Ministry of Information and Communication Technology can also help facilitate measures to generally improve IPv6 awareness at a national level with a number of initiatives that either organise 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 Ministry of Information and Communication Technology focus on areas of concern that require intervention.
16.2 Documentation templates and documentation roadmap

As part of the IPv6 adoption governance and monitoring mechanism, Ministry of Information and Communication Technology would need to 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.
17 Procurement plan and budget planning

This section describes the generic procurement plan and budget planning for network infrastructure equipment, systems and 3rd 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 coordinating procurement activities, establishing firm contract deliverables, and metrics in measuring procurement activities is included.

17.1 Items to be procured

The procurement requirements will vary depending on the organisation 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 workstreams e.g. 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
- Wide Area Network (WAN) services procured from a third party
- Network hardware owned by the organisation e.g switches, routers etc.
- Computing platforms e.g. servers, PCs etc
- Operating systems.
- Mainstream Applications (MS Office etc.)
- Special applications (SAP, Oracle etc.)
- New applications that are launched specifically using IPv6 e.g. a large scale M2M application.
- Standalone procurement exercise, though could include some upgrading of existing infrastructure.
- New IPv6 specific projects e.g. IPv6 web hosting facility.

17.2 Budget outline

Budgets for BAU IPv6 implementation will vary substantially depending on the situation, but if deployment is planned across a 3 – 4 year time 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 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.

17.3 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 that IPv6 is 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.
18 Training

The training for IPv6 implementation is an early prerequisite for all stakeholder groups, with the content and depth obviously varying depending on the individual’s role. A generic framework for IPv6 training requirements is detailed in Figure 18.1, this specifies target audience, subject matter and duration.

Table 18.1: Proposed IPv6 training

<table>
<thead>
<tr>
<th>Programme Name</th>
<th>Target Audience</th>
<th>Details to be covered</th>
<th>Approx Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Awareness Programme</td>
<td>Decision Makers – CXOs Executive Management Program Managers</td>
<td>Need for IPv6 Impact of IPv6 on IT infrastructure Budgetary implications of IPv6 adoption IPv6 Project Management</td>
<td>8 hours</td>
</tr>
<tr>
<td>Introduction to IPv6</td>
<td>Technical Architects/Designers Network Implementation Team Network Maintenance Team</td>
<td>Introduction to IPv6 IPv6 Addressing DHCPv6 and DNSv6 IPv6 Routing</td>
<td>16 hours</td>
</tr>
<tr>
<td>IPv6 Adoption across Service Providers</td>
<td>Technical Architects/Designers Network Implementation Team Network Maintenance Team</td>
<td>IPv6 Routing IPv6 across MPLS IPv6 Multicast IPv6 Troubleshooting IPv6 Network Management</td>
<td>40 hours</td>
</tr>
</tbody>
</table>
The IPv6 training roadmap for Qatar will need to be ideally completed over a duration not exceeding circa 3 years, the first six months of which will focus on building national awareness about IPv6 followed by 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 18.2
### Awareness Programs
- **Name**: Awareness Programs
- **Target Audience**: Decision Makers: - CXO's Executive Management Program Managers
- **Program outcomes**: 6 months

### Introduction to IPv6
- **Name**: Introduction to IPv6
- **Target Audience**: Technical Architects/Designers Network Implementation Team Network Maintenance Team
- **Program outcomes**: 12 months

### IPv6 Adoption across Service Providers
- **Name**: IPv6 Adoption across Service Providers
- **Target Audience**: Technical Architects/Designers Network Implementation Team Network Maintenance Team
- **Program outcomes**: 18 months

### IPv6 Adoption across Enterprises
- **Name**: IPv6 Adoption across Enterprises
- **Target Audience**: Technical Architects/Designers Network Implementation Team Network Maintenance Team
- **Program outcomes**: 24 months

### IPv6 Security
- **Name**: IPv6 Security
- **Target Audience**: Security Architects/Designers Security Implementation team
- **Program outcomes**: 30 months

### Program outcomes
- **6 months**: Blue
- **12 months**: Blue
- **18 months**: Blue
- **24 months**: Blue
- **30 months**: Blue
- **36 months**: Blue
<table>
<thead>
<tr>
<th>IPv6 System Administration</th>
<th>Security Maintenance Team</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System Administration</td>
</tr>
<tr>
<td></td>
<td>Architects</td>
</tr>
<tr>
<td></td>
<td>Systems</td>
</tr>
<tr>
<td></td>
<td>Implementation team</td>
</tr>
<tr>
<td></td>
<td>Systems</td>
</tr>
<tr>
<td></td>
<td>Maintenance Team</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv6 Programming</th>
<th>Software Architects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Software Implementers</td>
</tr>
<tr>
<td></td>
<td>Software</td>
</tr>
<tr>
<td></td>
<td>Maintenance Engineers</td>
</tr>
</tbody>
</table>
The IPv6 Awareness programs 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 the project planning aspects. Subsequent to the IPv6 Awareness programmes, Technical programs related to IPv6 Design and deployment across organizations would be initiated. IPv6 Technical training programmes should include: Introduction to IPv6, to Design and deployment programs for Service Providers and Enterprises.

Subsequent to the introductory IPv6 courses, IPv6 Architecture and Design should be conducted, (enabling Qatari Architects and Designers to 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 appropriate IPv6 skills.

In addition to general IPv6 Design and deployment programs, 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 nation.

In addition to the training programme, it is imperative that Ministry of Information and Communication Technology 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. Initially they would focus on sharing an understanding of the IPv6 technologies. These would be followed by seminars detailing deployment and adoption strategies. These would be followed by seminars/conferences focused on Applications and Innovations that would serve the environment in Qatar.
19 Conclusions

The timely implementation of IPv6 across the Qatar IP ecosystem is essential to ensure Qatar’s 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 growth 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 their 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 coordinate approach is taken. There are four basic stages comprising of familiarisation, plan, implement and launch, the implications of which will significantly vary depending on the type of stakeholder i.e. 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 (BAU) activities, there are potentially further options for developing new business opportunities based on supporting IPv6 based services. In particular the hosting of local IPv6 web sites 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 (IXP) 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 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 Ministry of Information and Communication Technology with a brief to provide support across the ecosystem. The task force will also have a coordinating 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 to ensure the introduction of IPv6 into Qatar is achieved in a timely, efficient and secure manner.