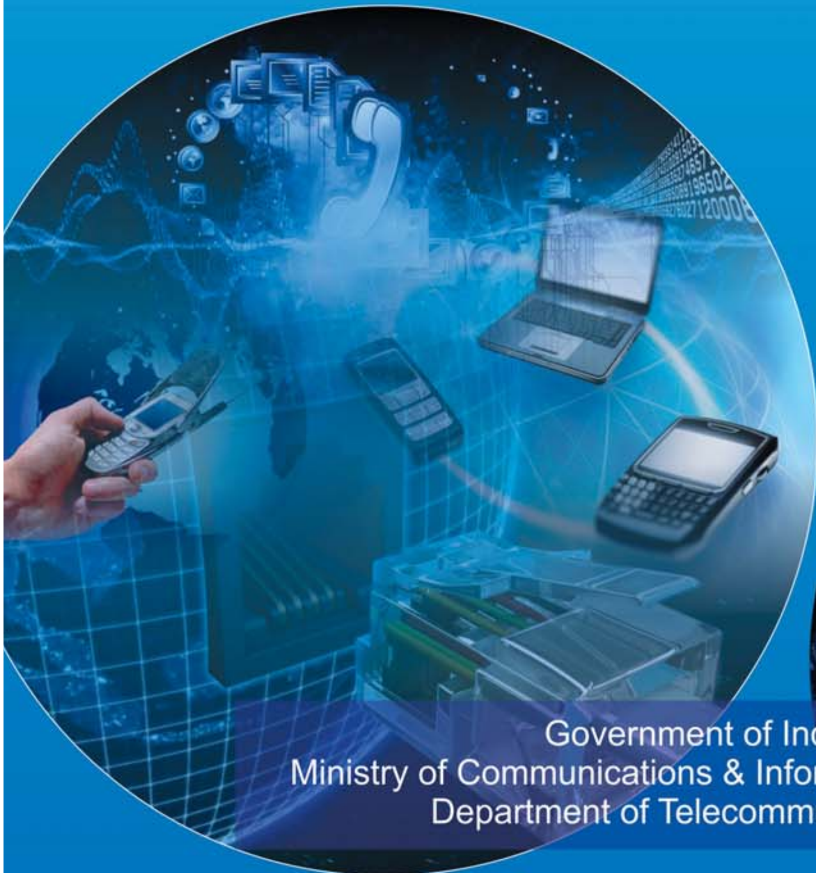
सत्यमेव जयते

National IPv6 Deployment Roadmap
Version-II



Government of India
Ministry of Communications & Information Technology
Department of Telecommunications

Foreword

The Government has envisaged providing ‘Broadband on Demand’ by the year 2015 in the recently unveiled National Telecom Policy (NTP)-2012. This is due to the fact that Internet acts as a catalyst for socio-economic development of a country and serves as an effective medium for delivery of various citizen centric services even in remote and rural areas. Since the current version of the Internet Protocol (IPv4) has almost run out of addresses, the broadband revolution that is on the verge of sweeping the country is sure to ride on next generation Internet Protocol version 6 (IPv6) which has many inherent advantages as well. The NTP-2012 recognises the futuristic role of IPv6 and aims to achieve substantial transition to IPv6 in the country in a phased and time bound manner. The adoption of IPv6 based innovative applications in areas like rural emergency healthcare, tele-education, smart metering, smart grid, smart building, smart city etc. have enormous potential to boost the socio-economic development of the country thereby improving the quality of life of common man.

It is against this backdrop that the ‘National IPv6 Deployment Roadmap Version-II’ is being released by Networks & Technologies (NT) Cell, DoT. This is in continuation of earlier ‘National IPv6 Deployment Roadmap’ released by DoT in July 2010 whose prime objectives have already been achieved. The recommendations, some of which are mandatory in nature, have been formulated and firmed up after extensive discussions with all stakeholders including industry associations and Government organisations and adopting the pragmatic approach while incorporating the relevant view points. Efforts have been made to incorporate all relevant inputs, material and experience gained during last two and half years since the release of earlier Roadmap. It is hoped that this document will prove to be an important milestone in the journey of IPv6 transition and adoption of IPv6 based projects in different sectors of the economy. I sincerely hope that with this initiative and the support of all stakeholders, the above aim envisaged in NTP-2012 will be timely achieved.

(R M Agarwal)

DDG (NT)

Executive Summary

This document is written on the foundation laid down by the National IPv6 Deployment Roadmap-I, which was released by the Government in July 2010. Chapter-1 of this document gives us a brief introduction about IPv6, the targets set by the Government in Roadmap-I and why there is a need to release a second Roadmap for continuing the IPv6 journey in the country.

A number of initiatives were taken by the Government for IPv6 proliferation in the country. A significant outcome of the first Roadmap was the formation of the India IPv6 Task Force, which was an attempt to bring all the industry stakeholders to a common platform to decide and debate on the issues for encouraging the adoption of IPv6 across the country. A number of activities were carried out under the guidance of India IPv6 Task Force like conducting training programmes on IPv6, empanelment of IPv6 consultants for the Government organisations, provision of IPv6 test bed by TEC, formation of IRINN by DeitY in India, celebration of 'World IPv6 Launch Day' and 'World IPv6 Day', periodic release of IPv6 newsletters by NT Cell, DoT and many other such activities. A brief about all such activities are covered in Chapter-2.

Adoption of IPv6 has picked up across the world and especially in the Asian region because of the severe shortage of IPv4 addresses. Chapter-3 gives a glimpse into the various activities taken up by different stakeholders across the world. The international scenario on IPv6 gives us a direction as to where the world is heading and what the future holds for our country.

The Indian IPv6 ecosystem consists of many stakeholders like the Government organizations, service providers, content and application providers, equipment manufacturers, cloud computing / data centres providers etc. On the road to IPv6 adoption it is to be ensured that all stakeholders perform the IPv6 journey in a coordinated manner. It is said that the strength of a chain is known by the strength of its weakest link; similarly, it is necessary that none of the key stakeholders is left behind in IPv6 adoption otherwise the whole ecosystem will be affected. Chapter-4 gives the status, details of challenges faced and strategies to be adopted by the different stakeholders in the IPv6 ecosystem including the timelines to be adopted by them in order to achieve the coordinated transition to IPv6 by all stakeholders.

One important aspect of IPv6 adoption is standardization. New technologies are adopted faster when standards are in place. IPv6 being a new protocol, the standards are still evolving worldwide. In India, TEC is responsible for formulating various standards and specifications for equipments used by the telecom operators for providing telecom and internet services. For IPv6 testing of equipments TEC has installed one IPv6 test bed in Delhi. Chapter-5 gives the details of standardization activities in India and about the IPv6 test bed for the benefit of manufacturers and other stakeholders for getting their networking equipments tested for IPv6 readiness, if required.

IPv6 adoption needs coordination with different types of stakeholders. The first institution created by the Government to facilitate this coordination was the India IPv6 task Force with many Working Groups entrusted with different activities. The main purpose of the task force was to give the initial push required by the industry to move on the road to IPv6 adoption, which it has successfully done. However, in the long term permanent institutional support is required in different forms to

solve the issues which all stakeholders will face during IPv6 transition. In this regard, two important institutions, namely, the 'Indian IPv6 Centre of Innovation' and the 'Indian Registry for Internet Names and Numbers (IRINN)' have been approved by the Government. Chapter-6 gives the details of these two institutions, their status & structure, their functions and their roles with respect to IPv6 adoption by India.

Chapter-7 explains some of the case studies on practical IPv6 adoption by some of the organizations so that these may be referred to when other organizations plan for their own IPV6 adoption. Besides, this chapter also suggests some monitoring mechanisms for reviewing the progress of different stakeholders and to know how successful the country is on the path of IPv6 adoption. The statistics collected through the monitoring mechanism will set the direction for future IPv6 policy and remedial actions required, if any. There is also need to have adequately trained IPv6 talent pool within the country to facilitate this transition. This talent pool will be required by the different organizations when they work on IPv6 adoption. This chapter briefly describes the types of courses which are needed to create a mix of basic, professional and expert level talent pool. With this objective, separate action is being taken by the DoT for standardization of IPv6 course content and empanelment of the training institutions.

Chapter-8 gives the summary of recommendations and actionable points for different stakeholders especially the timelines as discussed in different parts of this Roadmap.

Acknowledgements

The Internet acts as a catalyst for socio-economic development of a country and serves as an effective medium for delivery of various citizen centric services even in remote and rural areas. Since the current version of the Internet Protocol (IPv4) has almost run out of addresses, the next wave of broadband revolution is sure to ride on next generation Internet Protocol version 6 (IPv6) . The NTP-2012 also recognises the futuristic role of IPv6 and aims to achieve substantial transition to IPv6 in the country in a phased and time bound manner. During the last two and half years, a lot of interactions have taken place with different stakeholders during different IPv6 events and the suggestions, opinions and feedback given by everyone have helped us in formulating this document.

We are thankful to Shri R Chandrashekhar, Secretary (T), Shri J K Roy, Member (T) and Shri R.K. Bhatnagar, Advisor (T) who have guided us on regular basis during different interactions, meetings and discussions. Without their guidance, it would not have been possible for us to reach this stage.

We express our thanks to Shri J. Satyanarayana, Secretary (DeitY), Shri S.C. Misra, Member (Services), Ms. Sadhana Dikshit, Member (Finance), Shri N Ravi Shankar, Administrator (USOF), Smt. Rita Teaotia, Addl. Secretary (T), Shri Anil Kaushal, Sr.DDG TEC, Shri R. K. Upadhyaya, CMD, BSNL, Shri A. K. Garg, CMD, MTNL and Shri V.V.R. Sastry, Executive Director, C-DOT for their valuable guidance and support which has been of great help to us .

We are thankful to Mr. Latif Ladid, President IPv6 Forum for the valuable support during the formulation of this document.

We take this opportunity to show our thanks to officers of DoT, TEC, committee members, contributing organisations and special invitees who have contributed greatly in the formulation of this document.

We are also thankful to the representatives of industry associations like IPv6 Forum, ISPAI, AUSPI, COAI, FICCI, TEMA, CMAI and others for their continuous support.

We would like to express our special thanks to all the officers and staff of NT Cell, DoT for their various inputs and continuous support during the entire period of preparation of this Roadmap.

We would like to sincerely thank everyone who has contributed directly or indirectly during the preparation of this document.

R.M. Agarwal, DDG (NT), DoT, New Delhi
B.K. Nath, Director (I), TEC, New Delhi
Manish K. Agarwal, Director (NT-II), DoT, New Delhi
(Members of Drafting Committee)

Contributors

a) The following members of the 'National IPv6 Deployment Roadmap Ver-II' committee have contributed in the formulation of the recommendations contained in this Roadmap:

Sl.No.	Name	Designation	Organisation
1	Sh. R M Agarwal*	DDG (NT)	DoT
2	Sh. J M Suri	DDG(I)	TEC, DoT
3	Sh. B K Nath*	Director (I)	TEC, DoT
4	Sh. Manish K Agarwal*	Director(NT-II)	DoT
5	Sh. Aurindam Bhattacharya	Group Leader	C-DOT
6	Sh. Naveen Dhar	Manager	Tata Communications
7	Sh. Rohan Mitra	Manager	Yahoo India Pvt. Ltd.
8	Sh. Sriniwas Gudipudi	Director	Neosixth Technologies
9	Sh. Raman Agarwal	Addl. GM	BSNL
10	Sh. Ashish Garg	Manager	AUSPI
11	Sh. Raj Sahakari	Sr Consultant	Tech Mahindra
12	Sh. Mahesh Gupta	Vice President	CISCO

**: These members were members of drafting committee as well.*

b) The following special invitees during the meeting of the committee have also contributed in the formulation of the key recommendations contained in this Roadmap:

Sl. No.	Name	Designation	Organisation
1	Sh. L Mathur	Jt. Secretary	ISPAI
2	Sh. Amod Malviya	Vice President	Flipkart
3	Sh. Anup Pandey	Chief Strategy Officer	Sixmatrix & IPv6 Forum Volunteer
4	Sh. D R Goyal	Deputy Director	MTS

c) The contribution of the following officers of NT Cell, DoT is special in the formulation of this Roadmap :

Sl. No.	Name	Designation
1	Sh. N Ram	Director (NT-I)
2	Smt. Reena Malhotra	Director (NT-III)
3	Sh. S K Madhukar	ADG(NT)

d) The contribution of following individuals in the formulation of this Roadmap is acknowledged:

Sl.No.	Name	Organisation
1	Dr. Govind	NIXI
2	Sh. Vipin Tyagi	C-DOT
3	Sh. Rajesh Chharia	ISPAI
4	Sh. R R Mittar	TEC

5	Sh. Neeraj Verma	BSNL
6	Sh. Navpreet Singh	IIT, Kanpur
7	Sh. Tsuyoshi Kinoshita	CISCO
8	Sh. Sureswaran Ramdass	NAV6, Malaysia
9	Sh. N K Goyal	CMAI
10	Sh. Naresh Ajwani	VNL
11	Sh. Virat Bhatia	FICCI
12	Sh. Avinash Joshi	Tech Mahindra
13	Sh. Badri Narayan	Tata Communications
14	Sh. Anurag Verma	Tulip

e) The following organisations have contributed in the development of this Roadmap:

Sl. No	Organisation
1	Security Cell, DoT
2	DS Cell, DoT
3	IP Cell, DoT
4	FEB Cell, DoT
5	C&A Cell, DoT
6	TEC
7	C-DOT
8	BHEL
9	NIXI
10	IPv6 Forum
11	Tata Communications
12	Cisco
13	Airtel
14	Flipkart
15	Tech Mahindra
16	Sixmatrix
17	Tulip
18	ISPAI
19	AUSPI
20	COAI
21	FICCI
22	HCL

f) The following officials of NT Cell, DoT have provided continuous back end support during the entire period of preparation of the Roadmap:

Sl. No.	Name
1	Smt. Varalakshmi Nagaraju
2	Sh. Devi Dass
3	Sh. Sanjeev Kumar
4	Smt. Saraswati

Contents

PART A

CHAPTER 1

Background and Introduction

1.1 Introduction

Information and Communications Technology (ICT) has been recognised the world-over as a key enabler for socio-economic development of a country. It acts as a catalyst for rapid growth and modernisation of various sectors of the economy and serves as an effective medium for delivery of various citizen centric services even in remote and rural areas thus bridging the digital divide. Accordingly, the Government has envisaged providing 'Broadband on Demand' by the year 2015 in the National Telecom Policy (NTP)-2012 to ensure equitable and inclusive development across the nation. Further, a target of 175 million and 600 million broadband connections by the year 2017 and 2020 respectively has been set. Since the current version of the Internet Protocol (IPv4) has almost run out of free IPv4 addresses, the broadband revolution that is on the verge of sweeping the country is sure to ride on next generation Internet Protocol version 6 (IPv6) .

1.1.1 IP, IPv4 and IPv6

The Internet Protocol (IP) is basically a communications protocol used for relaying packets of data across a network. The most part of present day Internet, which has today become indispensable for socio economic activities, runs on IPv4 i.e. Internet Protocol version 4.It is about 27 year old protocol having many limitations. The biggest limitation is its 32-bit addressing space resulting in about 4.3 billion IP addresses only. The rapid growth of internet, wireless subscribers and deployment of NGN technology is leading to accelerated consumption of IP addresses with the result that IPv4 addresses are almost exhausted today. India has at present about 35 million IPv4 addresses against a user base of about 360 million data users which are primarily mobile data subscribers. Envisaging the shortage of IPv4 addresses, Internet Protocol version 6 (IPv6) was developed by the Internet Engineering Task Force (IETF) way back in early 1990s. The IPv6 improves on the addressing capacities of IPv4 by using 128 bits addressing instead of 32 bits, thereby practically making available an almost infinite pool of IP addresses. Besides, it has several inherent advantages as well.

1.1.2 Features of IPv6

The IPv6 offers several advantages over IPv4 as below:

a) Security – Internet Protocol Security (IPSec) is a part of the IPv6 base protocol suite. It supports end-to-end security, authentication and non-repudiation thereby simplifying end to end security into applications.

b) Auto configuration – This is a plug and play feature which simplifies network configuration especially when the number of devices / nodes is very large like in typical sensor networks. It helps networks to quickly respond to crisis situations and facilitate adhoc network reorganisations.

c) Simplified Header format with better Quality of Service (QoS) – The header format has been simplified in IPv6 which helps in faster routing and switching. There is also a traffic class and flow label field, improving streaming for several applications such as VoIP, interactive gaming, e-commerce, videos etc.

d) IP Host Mobility – This feature enables a mobile node to arbitrarily change its location on an IP network while still remaining reachable and maintaining existing connections. Some practical uses of Mobile IPv6 could be enterprise on the move (e.g. courier

companies etc.), globally reachable home networks and internet enabled transport (cars, buses, trucks etc).

e) Innovative Applications – IPv6 has been designed with many new features which make it possible to develop innovative applications which are not easily possible in the current IPv4 protocol e.g. Centralized Building Management System, Intelligent Transport Systems, Rural Emergency Health Care, Tele-education / Distance Education, Smart Grids etc.

f) Multicast – The ability to send a single packet to multiple destinations (multicast) conserves bandwidth with efficient auto-configuration and service discovery.

g) Support for Jumbograms – The limit of payload size is not there in IPv6 and its size can be as large as possible depending upon the Maximum Transmission Unit (MTU). This greatly improves performance on high MTU paths.

1.2 Roadmap (Version-I)

The earlier Roadmap (Version- I) was released on 20th July, 2010. At that time, the Indian ecosystem was in nascent stage of IPv6 adoption with low awareness level among the stakeholders. During the discussion with industry members and stakeholders, it emerged that there is a need to crystallize and firm up the transition strategy from IPv4 to IPv6 to facilitate the widespread introduction of IPv6 in India. Accordingly, a policy document titled 'National IPv6 Deployment Roadmap' was released by DoT. It was the first initiative of its kind by a Government anywhere in the world. The main focus of the roadmap was to educate/ sensitise the Indian ecosystem about the issues related to IPv6 and enable it to take the first step in the transition towards IPv6. The following key policy guidelines were therefore incorporated in the roadmap:

i) All Major Service Providers (having at least 10,000 internet customers or STM-1 bandwidth) will target to handle IPv6 traffic and offer IPv6 services by December-2011

ii) All Central and State Government Ministries and Departments, including its PSUs, shall start using IPv6 services by March-2012.

iii) Creation of IPv6 Task Force

1.3 Need of Roadmap Version-II

As a result of the initiatives undertaken by DoT, majority of the major service providers in India have become ready to handle IPv6 traffic & offer IPv6 services. The Central and State Government Ministries and Departments, including their PSUs have been sensitised about transition to IPv6 and they are now geared up to take the next step forward with some of them already using IPv6 services. An India IPv6 Task Force headed by Secretary (T) with 3-tier structure consisting of Oversight Committee, Steering Committee and 10 Working Groups has also been formed. Thus, with the achievement of prime objectives envisaged in the first Roadmap, the Indian ecosystem has come of age and attained maturity level. Further, there is a need to consolidate the gains and build further on the milestones achieved. The NTP-2012 also recognises futuristic roles of Internet Protocol Version 6 (IPv6) and its applications in different sectors of Indian economy. The relevant extracts of the NTP 2012 related to IPv6 are as under:

Preamble

- NTP-2012 recognises futuristic roles of Internet Protocol Version 6 (IPv6) and its applications in different sectors of Indian economy.

Objectives

- Achieve substantial transition to new Internet Protocol (IPv6) in the country in a phased and time bound manner by 2020 and encourage an ecosystem for provision of a significantly large bouquet of services on IP platform.

Telecom Enterprise Data Services, IPv6 Compliant Networks and Future Technologies

- To recognize the importance of the new Internet Protocol IPv6 to start offering new IP based services on the new protocol and to encourage new and innovative IPv6 based applications in different sectors of the economy by enabling participatory approach of all stake holders.
- To establish a dedicated centre of innovation to engage in R & D, specialized training, development of various applications in the field of IPv6. This will also be responsible for support to various policies and standards development processes in close coordination with different international bodies.

As IPv6 is not backward compatible with IPv4, the transition to IPv6 is likely to be a complex, mammoth and long term exercise during which both IPv4 and IPv6 will co-exist. The basic purpose of Roadmap Ver-II is to take the next step forward and lay down the important milestones to facilitate substantial transition of our country to IPv6 in a phased and time bound manner. The policy guidelines have been framed after extensive consultations/ discussions with all stakeholders in order to ensure that they are implementable and practical in nature.

PART A

CHAPTER 2

Initiatives Undertaken

Initiatives Undertaken

Since the release of Roadmap Ver-I in July 2010, a large number of initiatives for IPv6 adoption have been undertaken which have been summarised in this chapter.

2.1 India IPv6 Task Force

In accordance with the policy guidelines stated in Roadmap Ver-I, a 3-tier India IPv6 Task Force Task comprising of 2 Committees and 10 Working Groups was formed in December 2010 to plan, co-ordinate and drive the IPv6 adoption across the nation. Each tier has members from different organizations / stakeholders in PPP mode. The structure and details of the Task Force are as under:

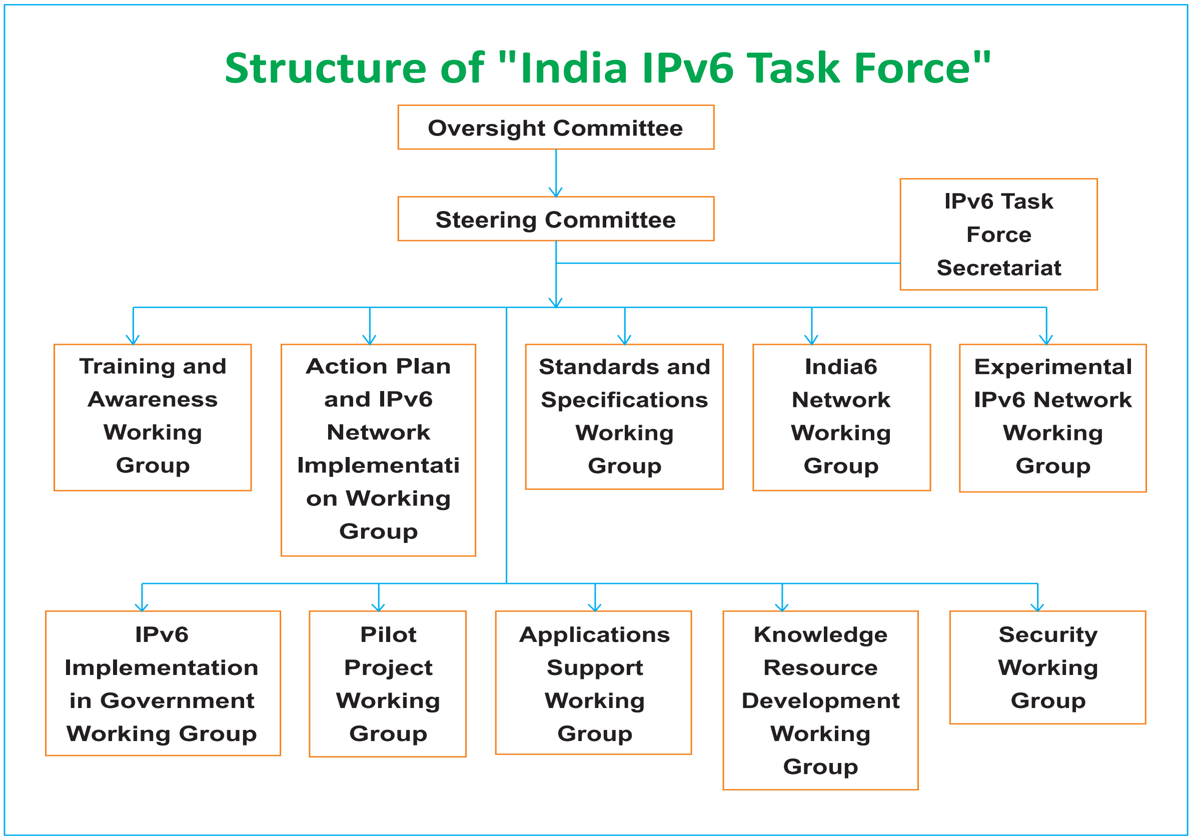

Structure of "India IPv6 Task Force"
Oversight Committee
Steering Committee
IPv6 Task Force Secretariat
Training and Awareness Working Group
Action Plan and IPv6 Network Implementati on Working Group
Standards and Specifications Working Group
India6 Network Working Group
Experimental IPv6 Network Working Group
IPv6 Implementation in Government Working Group
Pilot Project Working Group
Applications Support Working Group
Knowledge Resource Development Working Group
Security Working Group

Figure 1: Structure of India IPv6 Task Force

Oversight Committee - This is the apex body for making policy decisions and responsible for guiding the task force by taking strategic decisions. The Oversight Committee is headed by Secretary (T), DoT as its Chairman. Besides, it has members from DoT, TEC, DeitY, C-DOT, PSUs like BSNL & MTNL, industry associations like CMAI, NASSCOM, COAI, AUSPI, ISPAI, ACTO, TEMA, IPv6 India Forum etc alongwith representative of various stakeholders. It is scheduled to meet every four months.

Steering Committee – The Steering Committee is the second level body for coordinating the activities of the Task Force. It oversees the activities of the different Working Groups constituted under the Task Force for timely and smooth transition in the country. The Steering Committee is headed by Advisor (T), DoT. Besides, it has members from DoT, TEC, DeitY, C-DOT, PSUs like BSNL & MTNL, various

ministries of the Government, industry associations alongwith representative of various stakeholders. It is scheduled to meet every two months.

Working Groups – There are ten Working Groups and each one is responsible for the specific activities associated with transition to IPv6. One of the member organisations of each Working Group is the lead organisation in that group who is responsible for funding the activities of the respective working group in addition to other activities like place of meetings, logistics, selection of members etc. It is scheduled to meet at least once every month. The details are as under:

WG Number	Name	
WG-1	**Training & Awareness**	• Hands-on trainings in association with APNIC, IISc and other organizations. • Trainings for nodal officers from Government. • Conducting Workshops, seminars and conferences.
WG-2	**Action Plan & IPv6 Network Implementation**	• Primarily responsible for studying the different network scenarios and come up with action plans for individual service providers / organizations. • Service Providers to be perused for IPv6 implementation.
WG-3	**Standards & Specifications**	• Development of common IPv6 specifications for the country, which will be followed by all stakeholders
WG-4	**India6 Network**	• To plan transition pipe, make a project report and also coordinate with the selected service provider/organization to build this "Transition Pipe" called "India6 network" which will then act as an IPv6 backbone network."
WG-5	**Experimental IPv6 Network**	• Setting up of an IPv6 network for demonstrating and experimenting with different IPv6 transition scenarios.
WG-6	**Pilot Project**	• 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.
WG-7	**Application Support**	• To facilitate the transition of existing content and applications and development of new content and applications on IPv6.
WG-8	**Knowledge Resource Development**	• To develop the IPv6 knowledge base in the country with active participation of the educational institutes. • Pursue with the Ministry of HRD to take up study of IPv6 related issues by educational institutes, involve in basic research on IPv6 etc.
WG-9	**IPv6 Implementation in the Government Network**	• Pursue with different government departments for implementation of IPv6.
WG-10	**Network Security Group**	• Define security policies, technical architectures and best practices for IPv6 security adoption in India.

Besides, a Standing Committee has been formed to ensure proper co-ordination between DoT and DeitY. It consists of senior officers from DoT and DeitY as its members. In addition, an IPv6 Core Committee has been constituted to look into various IPv6 transition issues, doubts raised by various stakeholders and resolving the same on regular basis. The IPv6 Core Committee consists of members from DoT, DeitY, TEC and various industry representatives.

To provide various technical inputs to the Core Committee, an Expert Group has also been formed. It is a resource pool to address various technical issues/ problems encountered during IPv6 adoption. It consists of the members from premium Indian institutes (like IITs, IISc etc.), World IPv6 Forum, NAv6 Malaysia and representatives of various stakeholders.

2.2 Steps Taken For IPv6 Proliferation

A large number of steps have been taken for transition from IPv4 to IPv6 as under:

2.2.1 Meetings / Seminars /Workshops

i) Regular meetings of the Oversight Committee, Steering Committee and Working Groups have taken place since their formation. As lead organisation of 'Action Plan & IPv6 Network Implementation' Working Group, NT Cell, DoT has held a large number of review meetings to pursue with major service providers (10 meetings), content & application providers (4 meetings), OEM & equipment vendors (4 meetings) and end user device manufacturers (2 meetings). Besides, various meetings (20 nos.) have been conducted with Central and State Government ministries, departments and their PSUs to sensitise and gear them up for transition to IPv6. An activity sheet (attached as Annexure-A) has been prepared and circulated to all Government organisations to help them in the task.

ii) NT Cell, DoT in association with BSNL, the lead organisation of 'Training and Awareness Working Group' has also organised a large number (24 nos.) of IPv6 awareness workshops state wise across the length and breadth of the country for the benefit of key decision makers in the Government organisations and other stakeholders. All these workshops were attended by about 100-125 nos. of participants from various departments / ministries of the State including top ranking officers of the level of Chief Secretary / Principal Secretary (IT). The details of the workshops are attached as Annexure-B. In addition, BSNL has also conducted 22 nos. IPv6 training programmes at ALTTC, Ghaziabad and 14 nos. at the premises of the various Government organisations on their request.

iii) As lead organisation of 'Application Support' Working Group, Tech Mahindra with the support of DoT, ERNET and Airtel carried out a testing activity to test the various applications currently used in the customer environment for different IPv6 transition scenarios. A scenario of an IPv6 user connecting to an IPv4 website using NAT64 mechanism was created. The key findings which were presented in the workshop of content & application providers held on 04-05-2012 at Mumbai were as below:

- Instant messaging applications were unable to work normally on NAT64 due to lack of IPv6 support on the IM clients.

- Applications that require point to point connections need to be supported by Application Layer Gateway (ALG).
- Public facing websites and applications should adopt IPv6 (dual-stack) due to the following reasons:
  - Avoid traversing multiple gateways – reduce impact on performance.
  - Have a straight path with IPv6 and IPv4 – better user experience.
  - Reduce risk to online businesses – ensure business continuity.

iv) A special workshop on IPv6 for officers of units/ organisations under Dept of Financial Services was organised on 08th October, 2012 at Sanchar Bhawan, DoT HQ, New Delhi. The workshop was attended by more than 60 nos. of senior officers. The presentations on the following topics were made:

- Progress of IPv6 transition across various stakeholders.
- IPv6: issues involved in implementation.
- Relevance of IPv6 to banking and finance domain and transition considerations.
- IPv6: bringing a change in financial sector.
- IPv6 implementation at the internet edge.
- Security considerations in IPv6.
- IPv6 Ready Logo certification for ISP's, WWW etc.

v) A two days seminar on IPv6 for officers of DoT was organised on 05th and 06th November 2012 at Sanchar Bhawan, DoT HQ, New Delhi. More than 80 participants attended the two days seminar covering various topics and issues of IPv6 at length. The following topics were covered:

- Government initiatives and progress of IPv6 transition across various stakeholders.
- Why IPv6?
- IPv6 addressing.
- IPv6 applications, driving factors, 6LoWPAN and Internet of Things (IoT).
- Transition techniques and strategies for IPv6 transition.
- How to start IPv6 deployment?
- Security in IPv6: issues and best practices.
- National Optical Fibre Network (NOFN): empowering rural India by digital convergence.
- Case study on transition to IPv6: BHEL, Airtel & Tulip Telecom.
- NIC: transition plan, address plan, SWAN & SDC address plan, transition techniques etc.

A Quiz Contest was also organised at the end to add flavour and awareness in the seminar. The average grading awarded to this seminar based on the feedback from participants was 9.3 (on a scale of 0-10).

2.2.2 Empanelment of Consultants

In response to the demand and need of various Government organisations and to further facilitate them in IPv6 transition, 11 organisations have been selected and empanelled by DoT to provide IPv6 consultancy and/or implementation of IPv6 services. The consultants are as below:

Empanelled Consultants for IPv6 Implementation	
• NIT Hamirpur	• Ernst & Young
• TCS	• Neosixth Technologies
• C-DOT	• Tech Mahindra
• ERNET	• TCIL
• Pricewatershouse Coopers	• HCL
• BITCOE (IIT Kanpur)	

However the Government organizations are free to appoint any other competent consultant for their IPv6 requirement. The empanelled consultants have been categorized into three types viz. A, B and C depending on the scope of consulting service as detailed below:

I. Type A - IPv6 Consulting:

The scope involves defining and carrying out consulting activities related to IPv6 transition strategy and planning, through modes like interviews and sessions with various stakeholders to understand and charter a strategy plan for IPv6 Implementation. This includes:

❖ IPv6 Transition Assessment and Gap Analysis:

a. IPv6 Awareness across organization.

b. Current State of IPv6 readiness.

c. Existing IPv6 Adoption Plans and their State.

d. Infrastructure Readiness and network audit.

e. Detailed IPv6 Training and Education Roadmap and Plan.

❖ Strategy Planning:

a. Detailed IPv6 Implementation / Adoption Roadmap and Project Plan.

b. Detailed IPv6 Adoption Governance / Transition Management.

c. Procurement plan and Budget Planning for network infrastructure equipment, systems and 3rd party applications.

d. Current IPv6 adoption strategy and implementation plans.

e. Key adoption challenges.

f. Creating documentation templates and comprehensive documentation roadmap.

❖ Network Planning and Design:

a. Addressing Planning based on existing and future requirements.

b. Creating an IPv6 Network Architecture as per requirements.

c. IPv6 Integration Planning - Transition Methodology Options – Identification, Evaluation and Selection.

d. Network Design and configuration planning, as per selected transition methodology.

e. Identification of applications and services for transition.

f. Security Planning and considerations.

g. Network Implementation and Test Planning.

h. Documenting all the activities carried out in standardized formats.

II. Type B - End-to-End IPv6 Consulting:

The scope of work covers all aspects which include IPv6 Project Management in addition to IPv6 consulting mentioned above. The responsibility encompasses the complete monitoring and supervision of the actual implementation and ensuring a timely delivery by the implementation organization. The details of Project Management activities are as mentioned below:

To create a project plan for IPv6 project management and carry out IPv6 project management activities for IPv6 adoption including:

a. Detailed Project Management Plan – Objectives and Approach, Stakeholders Identification, Project Scope and Timelines, Cost Management, Resource Planning, Document Management, Change Management, Risk Management and Risk Mitigation Plan, Procurement Management, Configuration Management etc.

b. Project – Execution and Progress Tracking.

III. Type C - IPv6 Implementation:

The scope of work for IPv6 Implementation covers all aspects of implementation of IPv6 as given below –

a. Applications and services transition.

b. Test IPv6 Network Implementation execution.

c. Production Network Implementation execution.

d. Test Plan creation and validation for test and production networks.

e. Post Implementation Support, Training and Knowledge Transfer to Staff.

2.2.3 Testbed

There was a need to have IPv6 test bed in India so that the vendors and stakeholders can test their equipments for IPv6 compatibility and readiness. Accordingly, an IPv6 test bed has been installed by Telecom Engineering Centre (TEC), the technical wing of DoT, to foster explicit IPv6 harmonisation

across the entire ecosystem. The above test bed is under validation and in the process of acquiring IPv6 Ready Logo certification. Till such time the lab gets ready, DoT has given approval for the purchase of products certified by ‘World IPv6 Forum’ through their ‘IPv6 Ready Logo’ Program. The details of the various products certified are available on the IPv6 Ready Logo website - https://www.ipv6ready.org . Besides, IPv6 standards have been released by TEC after taking into consideration the USGv6 and IPv6 Ready Logo standards. Further, TEC is in the process of framing standards for IPv6 ready handsets to provide momentum to IPv6 based services.

2.2.4 Initiatives in association with DeitY

i) DoT has been working in close association with DeitY to ensure smooth and seamless adoption of IPv6 and its co-existence with IPv4. In order to lead by example, it has been decided that the websites of all Government organisations maintained by NIC shall be transited to IPv6 (dual stack) by December 2012. NIC has made significant progress on this issue and has already completed transition of considerable number of websites to IPv6 including that of DoT. Further, the applicants are being encouraged to host their websites on dual stack when they approach for domain name registration/renewal. All nodes of NIXI have been upgraded and made IPv6 ready. Besides, NIXI has conducted 12 nos. of IPv6 trainings/ workshops in association with APNIC. It has also sponsored free of cost training program to 115 engineers across the country for IPv6 online training. To address the various issues being faced by the stakeholders regarding IP address allocation from APNIC, the Indian Registry for Internet Names and Numbers (IRINN) has been approved by APNIC in India for allocation of IPv6 address in a systematic manner with a large pool to cater to all future requirements. The IRINN is expected to start functioning shortly. At present, the major requirement of IPv6 address blocks of Government organisations is being taken care of by NIC. In addition, case has been taken up with Computer Emergency Response Team India (CERT-In) for empanelment of security audit teams for IPv6 as has been done for IPv4.

ii) In order to tap the several features of IPv6 which make it possible to develop new applications which were not possible in the IPv4 protocol, State Governments are being encouraged for various pilot projects in association with DeitY in areas like Centralised Building Management System, Intelligent Transport Systems, Rural Emergency Health Care, Tele-education / Distance Education, Smart Grids etc. National Knowledge Network (NKN) and other educational networks are to be on IPv6 so as to proliferate IPv6 in educational institutions and encourage them to develop novel applications exploiting the features of IPv6.

2.2.5 World IPv6 Launch Day (06-06-2012)

The **‘World IPv6 Launch Day’** was celebrated across the world on 6th June, 2012 whereupon major Internet Service Providers, networking equipment manufacturers and web companies around the world (like Google, Yahoo, Facebook, Youtube, Bing etc.) came together to permanently enable the next generation Internet Protocol (IPv6) for their products and services. It was intended to motivate organizations across the industry to prepare for and permanently enable IPv6 on their products and services. Its logo was aptly titled ‘Launch into the Future’. It built on the successful one-day ‘World IPv6 Day’ event held last year on 8th June wherein a successful 24-hour global-scale trial of IPv6 was done.

On this occasion, an event was organised by DoT at Sanchar Bhawan, New Delhi. The event was chaired by Shri R. Chandrashekhar, Secretary (T), DoT. There were around 100 invitees from DoT, DeitY, major Service Providers, Content & Application Providers, ICT Vendors, Telecom Industry Associations, BSNL, MTNL, C-DOT etc. Besides, invitees from press and media were also present.

Shri R. M. Agarwal, DDG (NT), DoT presented the status of IPv6 implementation in the country. A presentation regarding case study for service providers, application & content providers and NIC initiatives was also made by respective stakeholders. Shri J. K. Roy, Member (T), DoT in his address said that the transition to IPv6 is likely to be a complex and long term exercise and added that efforts are being made to have IPv6 Ready Logo Certification for the TEC Test Bed at the earliest. Smt. Rita Teaotia, Addl. Secretary, DeitY said that Government websites on NICNET shall be transited to IPv6 (dual stack) by December, 2012.

Shri R. Chandrashekhar, Secretary (T), DoT said that the Government believes in leading by example and will continue to put in place measures to ensure smooth and seamless adoption of IPv6 so that advantages of unique IP addresses may be taken by all including IP based devices. He further said that the innovative applications exploiting the new features of IPv6 will further drive the proliferation of IPv6 in the country.

In continuation of above, a conference titled **'IPv6 Launch Event: Switch to v6'** was jointly organized by DoT and M/s Cisco on 07-06-2012 which was attended by around 100 top dignitaries from key government and enterprise organizations. Eminent speakers from Government and leading organizations shared some interesting insights and perspectives regarding IPv6 transition. This was followed by an interactive session wherein questions were answered and key information was shared in the quality panel discussions held at the forum.

2.2.6 World IPv6 Day (08-06-2011)

As a precursor to World IPv6 Launch Day, the **'World IPv6 Day'** was celebrated on 8th June, 2011 across the world. Its aim was to motivate organizations across the Internet industry such as web service providers, hardware vendors, operating system makers and other key players to prepare themselves for successful transition from IPv4 to IPv6. The major web companies and other industry participants successfully enabled and tested IPv6 on their websites for 24 hours on this day.

A function was organised by DoT at Sanchar Bhawan, New Delhi to mark the occasion which was attended by senior officers of DoT, TEC, BSNL & MTNL and industry representatives. The first 'India IPv6 Task Force Newsletter' was released on this day by Shri R Chandrashekhar, Secretary (T) alongwith a 'Compendium on IPv6 Activities' compiled by Telecommunication Engineering Center (TEC).

Major service providers and content providers across India like Tata Communications, Airtel, Reliance, Google, Yahoo and others participated in the World IPv6 Day and reported that the event proceeded without any hitch with no major outages or security breaches being reported. Various IPv6 Awareness Workshops were organised on this day including one by Internet Service Providers Associations of India (ISPAI) at India Habitat centre, New Delhi. This day led to increased awareness about IPv6 and its adoption across organisations.

2.2.7 India IPv6 Task Force Newsletter

As lead organisation of ‘Action Plan & IPv6 Network Implementation’ Working Group, NT Cell, DoT has been regularly releasing the ‘India IPv6 Task Force Newsletter’ on bimonthly basis. It serves as microcosm of Indian IPv6 ecosystem and reflects the happenings taking place therein. It contains details of policy decisions/ guidelines with respect to IPv6, important meetings alongwith outcomes, awareness workshops, IPv6 readiness status of different stakeholders, upcoming events, events around the world etc. A total of six issues have been released so far. It has been widely appreciated by all segments of stakeholders and serves a useful purpose of spreading IPv6 awareness in the country. It is available on the website of DoT at http://dot.gov.in/ipv6/ipv6newsletter.html.

Besides, the details of all the activities undertaken by DoT with respect to IPv6 are regularly updated on its website under IPv6 activity link http://dot.gov.in/ipv6/ipv6activities.html. Further, the major service providers have been directed to provide a link in their respective websites to IPv6 activity link of DoT website.

2.3 Efforts at International Level

i) As the age of IPv6 dawns on the Indian ICT horizon, India is making its presence felt at various international forums. A delegation from DoT participated in the Asia Pacific Network Information Centre (APNIC)-32 meeting in Busan (South Korea) from 28th August to 1st September, 2011. The proposal submitted by DoT to APNIC community regarding reservation of a contiguous IPv6 address block for different organisations / stakeholders in an economy was discussed.

ii) A team from NAv6 Centre of Excellence, University Sains Malaysia visited DoT and TEC on 12th December, 2011. The team was led by Prof. Sureswaran Ramadass, Director, NAv6 Centre of Excellence, Malaysia. He presented the vision of the University Sains Malaysia highlighting how life can be eased with the help of technology especially with the use of IPv6 .He also gave useful insights on various aspects of IPv6 transition like planning of IPv6 adoption strategy, estimation of IPv6 budget / costs, training issues etc. A few key highlights of the presentation were:

- Although Asia has more than half of the world’s population, yet it controls only about 9% of the allocated IPv4 addresses.
- IPv6 is gaining momentum globally and more so in Asia. The growth rate of Asian ISPs is very high and they have no choice but to start using IPv6.
- Approximately 70% of the total costs involved in IPv6 adoption is towards training while hardware and software upgrades account for remaining 30%.
- IPv6 adoption costs would be relatively low if the hardware and software upgrades are done through regular upgrade cycles.

iii) The National IPv6 Task Force activities and the progress towards the same were presented by Shri R M Agarwal DDG (NT), in Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) meeting held at New Delhi on 27th Feb 2012. The key highlights-achievements and the future plans of the National IPv6 Task Force were presented.

iv) The National IPv6 Task Force activities and the status of IPv6 adoption in India were presented by Shri N Ram, Director (NT) in the APNIC meeting at New Delhi on 29th Feb 2012. In the presentation, achievements and the future plans of the IPv6 implementation were shared.

v) Mr. Latif Ladid, President IPv6 Forum visited Sanchar Bhawan, Department of Telecommunications on March 2nd 2012. He interacted with the members of the National IPv6 Task Force, Service Providers and Central Government IPv6 Nodal officers. An informative presentation was made by him conveying the following key points:

- IPv6 adoption across the globe is on the rise.
- Presence of Indian Service Providers on IPv6 is on the rise but still only a few Service Providers are present.
- IPv6 adoption takes time and has to be thoroughly planned.
- India is among the 2nd largest user of the key internet sites – Google, Facebook, Twitter and so forth, but none of these websites is Indian.
- More and more of Indian websites and content should be encouraged and made available on internet.
- BSNL, having the largest broadband retail network, has the potential to be the torch bearer of IPv6 adoption across the nation.
- IPv6 adoption by BSNL would spur the IPv6 proliferation across all segments of Indian ecosystem.

Mr. Latif Ladid also visited the TEC IPv6 test bed and interacted with the TEC/DoT officers with regards to the IPv6 Ready Logo certification and the processes therein.

vi) Shri R M Agarwal, DDG (NT) and Shri Nitin Jain DDG (DS) participated in the 43rd Internet Corporation for Assigned Names and Numbers (ICANN) meeting held in San Jose, Costa Rica from March 11th – 16th, 2012.

vii) The first India Internet Governance Conference (IIGC) was organised on 4th – 5th October 2012 at Federation House, Tansen Marg, New Delhi-110001 by Federation of Indian Chambers of Commerce and Industry (FICCI) in association with DoT/DeitY. The conference covered a wide range of topics: from network neutrality to global internet governance models; from effective management of the transition to IPv6 to making broadband access available to all etc. A special session on **'Managing Critical Internet Resources – Transition to IPv6, Machine to Machine Communications and Internet of Things'** was held in the conference which was well received by the audience of about more than 200 participants. The session was moderated by Shri R M Agarwal, DDG (NT) and had prominent international and national speakers like Prof. Sureswaran Ramadass, Director NAv6, Malaysia, Mr. Tsuyoshi Kinoshita, MD, Cisco Systems, Japan, Prof. K. Gopinath, Professor, IISc, Mr. B. Nagaraj, Senior VP, RIL, Mr. P. Badrinarayan, Vice President, TCL, Mr. Durga Prasad Allada, VP, Mahindra Satyam, Mr. Anup Pande, CSO, Sixmatrix and Mr. Ram Moham, CTO, Afilias etc. on the panel. The discussion focused on how fast adoption of IPv6 is vital for growth of broadband alongwith various IPv6 based innovative applications like tele-education, tele-health, emergency response system, smart grid etc. which are needed for socio-economic growth of the country.

viii) During the India Telecom- an annual international conference & exhibition organized by Department of Telecommunications (DoT) and Federation of Indian Chambers of Commerce & Industry (FICCI) during December 13th–15th, 2012, a special session titled **'Critical Internet Resources and Way Forward'** was held on 14th December 2012, Commission Room, FICCI, Federation, House, Tansen Marg, New Delhi. The session was addressed by Sh. R. Chandrashekhar, Secretary (T), Sh. J. Satyanarayana, Secretary, DeitY, Sh. J K Roy, Member(T), DoT, Mr. Latif Ladid, President, IPv6 Forum, Mr. Sanjaya,Sr. Director, APNIC, Sh. Ramesh Chandra, GM, Bharti Airtel Limited, Dr. Avinash Joshi, Tech Mahindra, Mr. Sanjoy Dass, Head, Technical Sales, Nokia India Pvt. Ltd, Mr. Arvind Mathur, Strategic & Technology Officer, Cisco and was moderated by Shri R M Agarwal, DDG (NT). With the intent to understand the potential of IPv6 in accelerating telecom sector and its impact on Indian economy, the session focused on the following topics:

(i) Importance of IPv6 in India and its impact on socio-economic fabric of the country.

(ii) IPv6 Transition – a Global Perspective.

(iii) Role of APNIC in IPv6 adoption.

(iv) Initiatives by DeitY for transitioning e-Governance services to IPv6.

(v) Role of IPv6 in Service Providers network.

(vi) Emergence of newer applications on IPv6.

(vii) IPv6 readiness of end user devices.

(viii) Case study of IPv6 transition in a State.

(ix) National IPv6 Deployment Roadmap Version-II.

The session was followed by panel discussions and question/answer session.

Apart from the initiatives mentioned in this chapter, continuous efforts are being made to encourage IPv6 transition in the country. Some of the noteworthy efforts currently in pipeline are establishment of Centre of Innovation (CoI) and empanelment of institutes for imparting training in the field of IPv6 the details of which have been mentioned in subsequent chapters 6 and 7 respectively.

PART B

CHAPTER 3

International Scenario

3.1 International Scenario

Global Internet users are currently estimated at 2 billion Internet users and are further projected to climb to 2.6-2.9 billion by 2015. The Internet accounted for 21 percent of the GDP growth in mature economies over the past 5 years. As a result, Governments, policy makers and businesses globally have recognized the enormous opportunities the Internet can create and its impact on economic growth and prosperity. With the global IPv4 address pool having been exhausted the global economies and businesses are faced with the major challenge of maintaining business continuity and sustaining growth during the transition phase to IPv6. This chapter provides an insight on the global status of IPv6 adoption vis a vis adoption in India.

3.1.1 Global Status

Global free IPv4 address space is exhausted at IANA on 3rd Feb 2011 and the RIRs also have exhausted or are on the verge of exhausting their free IPv4 blocks. The IPv4 exhaustion timeframe across all the RIRs is projected as below:

RIR	Projected IPv4 Exhaustion Period
ARIN	June 2013
APNIC	April 2011
AfriNIC	Nov 2014
RIPE	Aug 2012
LACNIC	Feb 2014

The five distinct regions identified in terms of their IPv6 adoption status are as below:

a) **North America:** IPv6 adoption in the North America is at 1.97%. That translates into an estimated IPv6 user base of 3.5 million users, the largest base of IPv6 users in the world. In September 2010, the US Federal CIO released a new IPv6 directive that established a step-wise approach for agencies transitioning to IPv6. This approach focused Federal agencies on meeting a short-term goal of making their external and public-facing services IPv6 operational by the end of FY2012. A mid-term goal was established to make agency internal services IPv6 operational by the end of FY2014. These goals would provide agencies with the operational infrastructure to build truly robust IPv6-enabled end-to-end services in the future that would take advantage of advanced IPv6 capabilities and features. A detailed roadmap is published by the federal agency http://www.ipv6forum.com/dl/presentations/USGv6Roadmap.pdf.

Additionally US is also leading in activities related to IPv6 both in terms of standardization and deployment/testing. Test and research networks of 6bone (www.6bone.net), 6 REN (www.6ren.net) and 6TAP (www.6tap.net) have their origin in this region.

b) **Latin America:** The IPv6 adoption status in Latin America is at a very nascent stage with the countries of Brazil, Argentina, Venezuela, Columbia, Chile and Peru beginning their IPv6 transition.

c) **Europe:** IPv6 adoption in Europe is gaining significant momentum with RIPE NCC having announced its final /8 allocation policy for IPv4 address pool in August 2012. The Commission of the European Communities released document "Advancing the Internet Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe" (http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_en.pdf.) In this Communication, the Commission sets Europe a target of getting 25% of EU industry, public authorities and households to use IPv6 by 2010.On a percentage basis, Romania is leading the deployment with 8.43% per cent adoption rate followed by France at 4.69% .The rest of the Eurozone including UK too has got initiated on IPv6 rollout with adoption rates at an average of 0.5%.

d) **Asia Pacific:** The impact of IPv4 exhaustion is more acute in this region since APNIC having exhausted its IPv4 address pool has initiated the final /8 allocation policy. With India and China evolving in to large internet economies the need for IPv6 adoption is more significant in Asia Pacific. Correspondingly activities have been initiated by the region towards the IPv6 transition.

- Regarded as one of the first countries to adopt IPv6, Japan began deploying the next-generation Internet protocol in the late 1990s through its Widely Integrated Distributed Environment (WIDE) Project. In March 2000, Japanese Telecommunications Company NTT became the world's first ISP to offer IPv6 services to the public. Millions of smartphones, tablets and other devices in homes, offices and public spaces throughout Japan rely on the country's long-standing IPv6 network. Japan ranking highly at 2.04% user penetration on IPv6 and is also leading the IPv6 initiatives on WIDE (www.v6.wide.ad.ip), KAME (www.kame.net) and TAHI (www.tahi.org).
- As the country with the largest population of Internet users, China launched its five-year plan for early IPv6 adoption in 2006. The program, known as the China Next Generation Internet (CNGI) project, has been instrumental in helping the country build the world's largest IPv6 network. China showcased its CNGI project at the 2008 Olympic Games in Beijing. Its expansive next-generation network connects millions of devices, users, and security and transportation systems throughout the country. China which is often held up as an example of a country that really needs IPv6, has penetration of approximately 0.67% on IPv6. Next Generation Internet project (CNGI), is a five-year plan with the objective of cornering a significant proportion of the Internet space by implementing IPv6 early. China showcased CNGI and its IPv6 network infrastructure at the 2008 Olympics in Beijing, using IPv6 to network everything from security cameras and taxis, to the Olympic events cameras.
- India with its large base of mobile users close to 900 million and internet users close to 23 million is poised for a major IP growth with the broadband users targeted to 600 million by 2020 and advent of newer services like 3G, LTE and cable digitization. IPv6 adoption rate in India is at a nascent stage with 0.24% adoption but is soon catching up with the rest of the economies with major thrust and support from the DoT, Government of India.
- In 2008, the Australian Government Information Management Office (AGIMO) initiated a three-stage plan for the country's transition from IPv4. The AGMIO established a December 31, 2012 deadline requiring every Commonwealth agency to have IPv6 compliance for all Internet gateways, applications and customer-facing systems. The

AGMIO serves as Australia's nominated agency for IPv6-related strategy, guidance and governance. A strategy for the Implementation of IPv6 in Government Agencies (http://www.finance.gov.au/e-government/infrastructure/docs/Endorsed_Strategy_for_the_Transition_to_IPv6_for_Australian_Government_agencies.pdf) was released in 2008 wherein the strategy outlined a three-stage process to transition to IPv6 with target dates set for implementation of IPv6 across Australian Government agencies to be completed by the end of December 2012.

- In Singapore IPv6 Transition Programme is a national effort spearheaded by IDA (Infocomm Development Authority) to address the issue of IPv4 exhaustion and to facilitate the smooth transition of the Singapore Infocomm ecosystem to IPv6. The programme also promotes readiness and adoption of IPv6 in the local industry through a series of projects. IDA has also published an indepth guide on the status of IPv6 in Singapore(http://www.ida.gov.sg/~/media/Images/Infocomm%20Landscape/Technology/IPv6/download/IPv6AdoptionGuideforSingapore.pdf).
- In 2004, South Korea initiated widespread transition from IPv4 via IT839, making it one of Asia Pacific's earliest adopters of the next-generation Internet protocol. The policy, established by the Ministry of Information and Communication, required the mandatory upgrade to IPv6 in the public sector by 2010.
- Taiwan with 0.6% of IPv6 adoption is ahead of the few of the larger economies on IPv6 adoption curve .Taiwan National IPv6 program mandating IPv6 transition by 2016, the country is well on its way to achieve IPv6 ready status in the future.
- The rest of the Asia Pac region of Hong Kong ,Thailand, Malaysia, Sri Lanka and Indonesia are at a nascent stage of IPv6 adoption and have got started on IPv6 initiatives with mandates for IPv6 transition around 2015-16 timeframes.

e) **Africa:** Africa being a late entrant in to the technology landscape also has the advantage of direct IPv6 implementation .The IPv6 initiative in Africa is being led by AfriNIC. AfriNIC has set up a virtual IPv6 lab that is used by educational institutions in Africa as a test bed to increase IPv6 hands-on experience in the region. The region is witnessing slow but steady growth in IPv6 uptake through various government initiatives .Kenya is one of the countries leading in IPv6 awareness and adoption -- the .ke domain registry is IPv6-capable, and the registry managers are working with the government to train and sensitize on the need for IPv6 adoption. But it is not all smooth sailing for most African countries. Some have yet to invest in critical Internet infrastructure like IXPs and ccTLD registries, while others are grappling with access issues.

3.1.2 Key Global Statistics on IPv6

a. Google, one of the most widely used search engine, regularly collects statistics about the IPv6 adoption on the internet by measuring the availability of IPv6 connectivity among Google users. The IPv6 adoption across the globe is rapidly increasing as shown in the adjacent figure 2.

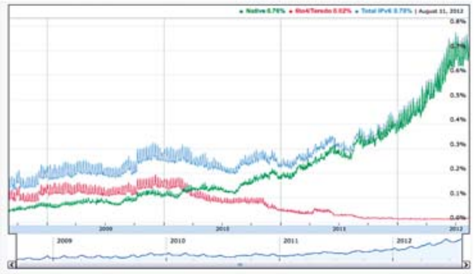


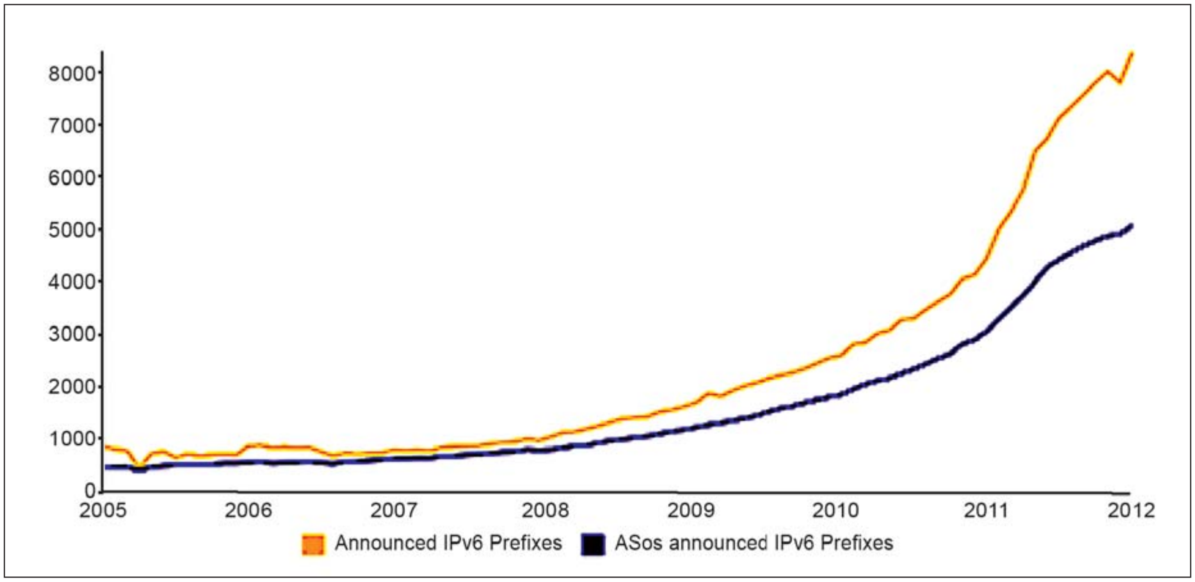
Figure 2: Percentage of users accessing Google over IPv6

b. Globally the number of IPv6 Internet population as of October 2012 stands at about 3.9 million of the total 2 billion or 0.19% of Internet population. The IPv6 adoption status across some of the major countries as in October 2012 is as shown in the table below:

Country	IPv6 adoption %
United States	1.7%
France	4.69%
United Kingdom	0.5%
Germany	0.21%
Czech Republic	1.09%
Romania	8.43%
Brazil	0.04%
Russia	0.2%
India	0.24%
China	0.67%
Japan	2.04%
Australia	0.31%
New Zealand	0.29%
Taiwan	0.60%
South Africa	0.14%
Central African Republic	0.41%

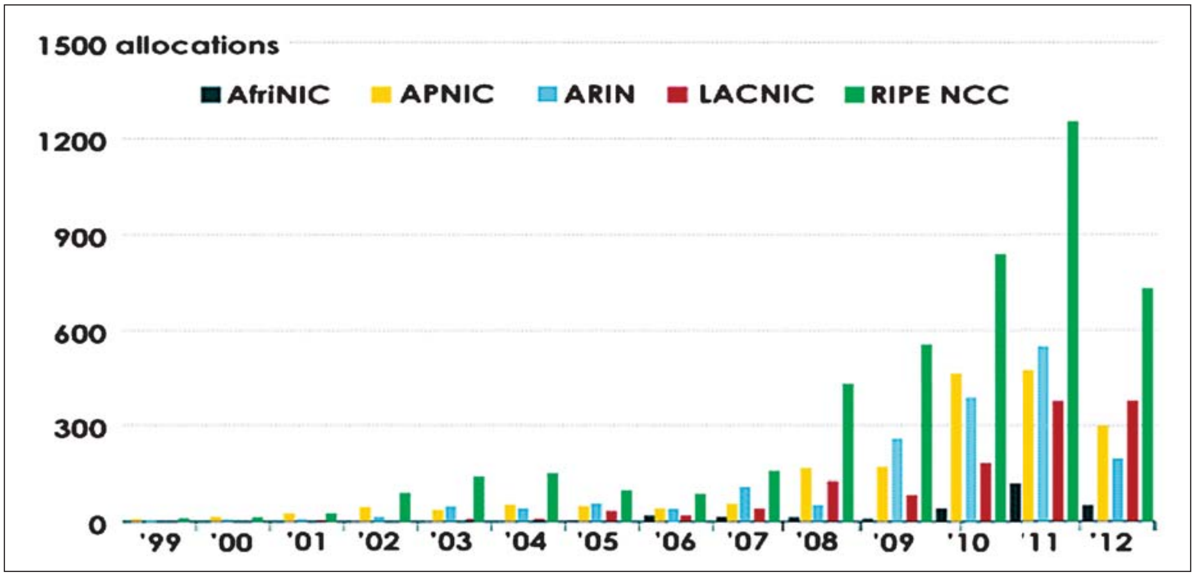
Source : http://www.google.com/intl/en/ipv6/statistics.html

c. The global IPv6 prefixes and AS announcing IPv6 are also on the rise and the graph below shows the IPv6 prefixes actually in use on the Internet.

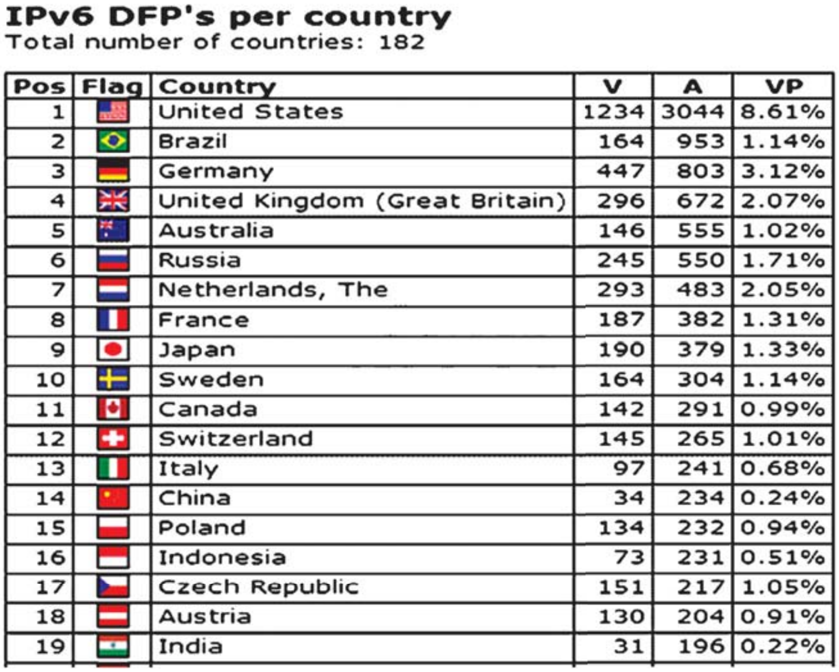


The globally announced IPv6 prefixes are nearing 8000. The no. of Autonomous System (AS) announcing IPv6 is also on the rise and currently stands at nearly 6000.

d. During the last few years the allocation of IPv6 prefixes by the RIRs to the ISPs is also rapidly increasing as evident from the graph below:



e. There are 13657 Default Free Prefixes (DFP) allocated to about 182 countries. Of these 5970 are visible on the Internet. India is at position 19 as can be seen below:A large number of organizations from India have obtained IPv6 prefixes. Some of them are being actively used but most are dormant. Details may be seen in the table given in Annexure C. It is expected that with increasing adoption of IPv6 by customers, more and more IPv6 prefixes will become visible on the Internet.



IPv6 DFP's per country

Total number of countries: 182

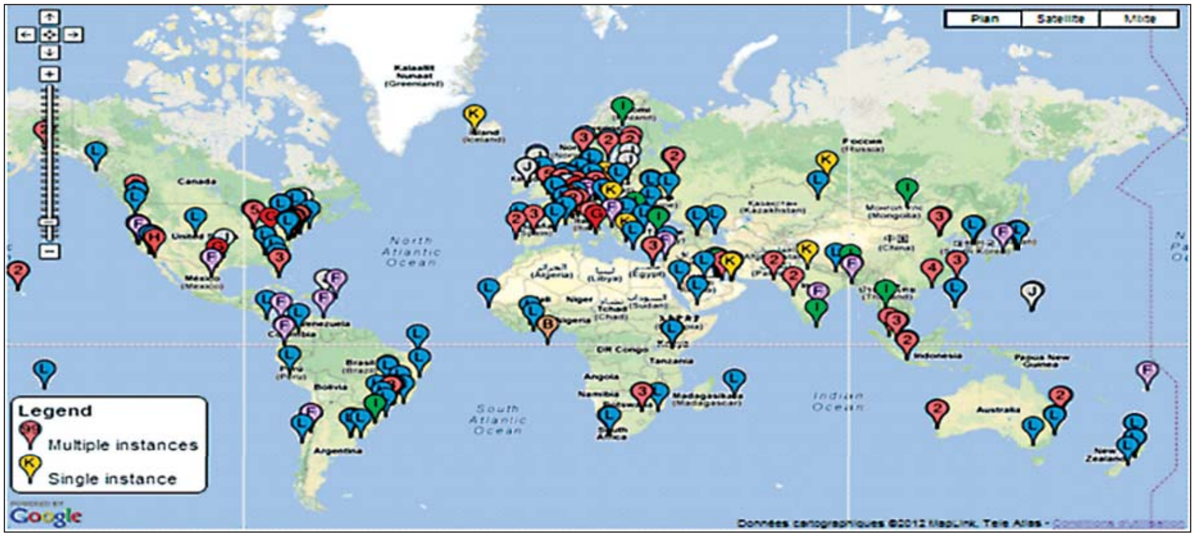
Pos	Flag	Country	V	A	VP
1	🇺🇸	United States	1234	3044	8.61%
2	🇧🇷	Brazil	164	953	1.14%
3	🇩🇪	Germany	447	803	3.12%
4	🇬🇧	United Kingdom (Great Britain)	296	672	2.07%
5	🇦🇺	Australia	146	555	1.02%
6	🇷🇺	Russia	245	550	1.71%
7	🇳🇱	Netherlands, The	293	483	2.05%
8	🇫🇷	France	187	382	1.31%
9	🇯🇵	Japan	190	379	1.33%
10	🇸🇪	Sweden	164	304	1.14%
11	🇨🇦	Canada	142	291	0.99%
12	🇨🇭	Switzerland	145	265	1.01%
13	🇮🇹	Italy	97	241	0.68%
14	🇨🇳	China	34	234	0.24%
15	🇵🇱	Poland	134	232	0.94%
16	🇮🇩	Indonesia	73	231	0.51%
17	🇨🇿	Czech Republic	151	217	1.05%
18	🇦🇹	Austria	130	204	0.91%
19	🇮🇳	India	31	196	0.22%

f. It is expected that there will be nearly two-and-a-half networked devices for every person on the planet – roughly 19 billion connected devices by 2016. It's not only people that are being connected, but also machines. Two billion M2M (machine to machine) connections are expected by 2015. Not surprisingly, global IP traffic has increased eightfold over the past five years and will increase threefold over the next five. The global IPv6 traffic is nearly 1% of the total traffic and is growing steadily as more connections are beginning to originate on IPv6.

g. Nearly 3000+ websites globally are on IPv6. Major contents providers like Google, Akamai, Yahoo, Facebook, You Tube etc. which account for significant percentage of Internet traffic have enabled IPv6 on their websites.

h. Every new Top Level Domain is compulsorily required to support IPv6.The root name servers contain NS records listing the name servers for the Top Level Domains (TLDs) and A and AAAA glue records to get to those name servers. Top level domains include domain name suffixes such as .com .net .org .us .ca .in etc. Each TLD has specific authoritative name servers. To support IPv6 these name servers should have an IPv6 address themselves and native IPv6 connectivity so that they can be reached over IPv6. Globally the number of Top Level Domains (TLDs) stands at 316 with 217 TLDs having IPv6 name servers.

i. There are 13 root servers globally out of which 9 can be queried over IPv6. These 13 root servers have multiple mirrors across the world in different locations. The Google map below shows the locations of these root servers and mirrors. Of these, 329 mirrors are IPv6 capable. Further, 48% of the rDNS name servers are reachable via IPv6. Of these, 70.1% are such that IPv6 access is as fast as or faster than IPv4 (within 1 ms).



3.1.3 Summary

With the increasing dependency of global economies on Internet to conduct business, the countries are required to plan for their Internet transition to IPv6 well in time. Most of the countries at present are at nascent stages but the right planning and strategy along with support from regulatory bodies and Governments should see considerable uptake over the next few years. The planning by both mature and emerging economies for substantial transition to IPv6 for catalysing their Internet proliferation will result in improved user experience and quality of life of its citizens.

PART B

CHAPTER 4

Status, Challenges & Strategy Alongwith Transition Plan of Various Stakeholders

4.1 Government Organisations

4.1 Government Organisations

The power of Information and Communications Technology (ICT) to accelerate development has been universally accepted by the Governments all over the world. It enables the Governments to reach out to its citizens even in rural and remote corners of the country. Accordingly, a large number of initiatives have been undertaken in India by various Central Ministries and State Governments in recent years to usher in an era of e-Governance. The National e-Governance Plan of Government of India seeks to create the right governance and institutional mechanisms in order to deliver public services in a transparent ,efficient and effective way at the doorsteps of citizens through easy and reliable access over the internet. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is evolving and large-scale digitization of records is taking place to create a citizen-centric environment for governance. In order that the e-Governance infrastructure is robust, scalable and does not become obsolete in near future, IPv6 adoption is a necessity. Besides, the Government organisations, which include various Central and State Government Ministries / Departments including their PSUs, are one of the largest users of information technology products and services in the country. The Government organisations therefore form an important element of the ecosystem and can lead by example through timely adoption of IPv6 within their networks.

4.1.1 Status

As a result of the initiatives undertaken since the release of Roadmap Ver-I, the Central and State Government Ministries / Departments, including their PSUs have been sensitised about transition to IPv6 and they are now geared up to take the next step forward. Some of the states like Tamilnadu, Karnataka, Gujarat, Madhya Pradesh, Manipur, Assam, Nagaland etc. have already taken the lead in the direction of IPv6 adoption. A few organisations like BHEL have even transited their network to IPv6 thereby setting examples for others to follow. The Government organisations are further being encouraged to take up various pilot projects regarding IPv6 based innovative applications.

The Government organisations are proceeding in a step by step manner as per activity sheet (attached as Annexure-A) which has been prepared specially for Government organisations keeping their networks in mind. Accordingly, the nodal officers for IPv6 implementation have been appointed in 100% and 95% of the States and Central Government Ministries/ Departments respectively. Further, the status of the activity sheet has been received from 63% and 43% of the States and Central Government Ministries/ Departments respectively. The overview of status is as in Figure 3.

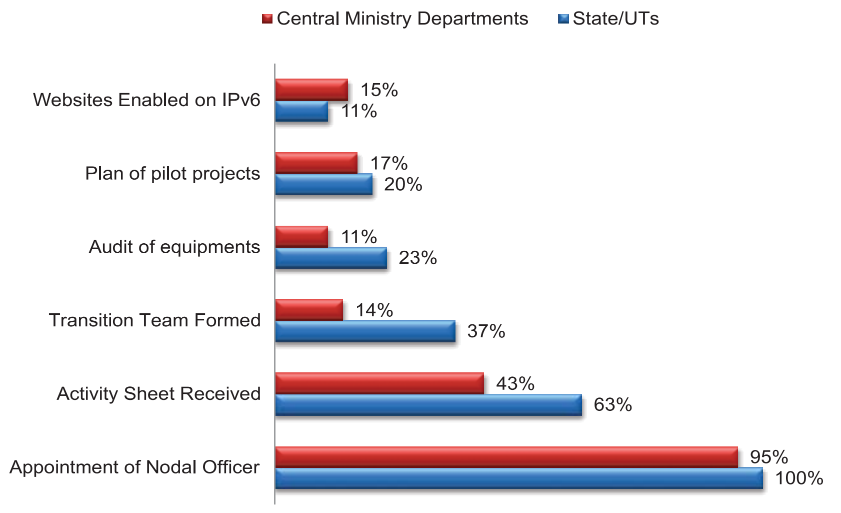


Figure 3 :IPv6 Status in State and Central Government

4.1.2 Challenges

The following are the challenges faced by the Government organisations at present:

- The basic challenge that faces the Government organisations is the lack of awareness about the IPv6 adoption and the issues involved therein. Although the Central and State Government Ministries / Departments, including their PSUs have been sensitised about transition to IPv6 through a large number of meetings and workshops throughout the country, the concept is yet to percolate to all levels of management. There is still little appreciation of the fact that IPv6 adoption is an eventuality that is to be accepted and managed proactively. The point that needs to be driven across is that it is prudent to get the IPv6 implementation done in a planned way rather than against time. The general misconception amongst Government organisations that there is no immediate requirement / urgency of planning the IPv6 adoption at present needs to be dispelled.
- Due to lack of awareness, the funds for IPv6 transitions have not been provisioned in the IT budgets by a majority of the Government organisations. The lack of funds would have serious implications on the timely adoption of IPv6 in the Government organisations and could critically impact the ability to meet the e-Governance goals.
- There is a severe shortage of skilled IPv6 trained human resources capable of managing the end to end IPv6 transition in the Government organisations. There is a need to build specialised skills within these organizations failing which IPv6 adoption pace and timelines may get impacted.
- There is a considerable legacy infrastructure and applications that would have to be upgraded/replaced as part of the IPv6 adoption in the Government organisations. Till such time these legacy infrastructures and applications are identified and gradually upgraded/phased out, the Government organisations would have bottlenecks in achieving complete transition to IPv6.

4.1.3 Strategy & Transition Plan

The Government organizations are recommended to follow a phased transition approach spread over a period of time depending on the complexity and the IPv6 readiness of the current networks and systems. They should follow the steps outlined in the activity sheet (attached as Annexure-A) to achieve IPv6 transition in their organisation. The main stages involved have been described below:

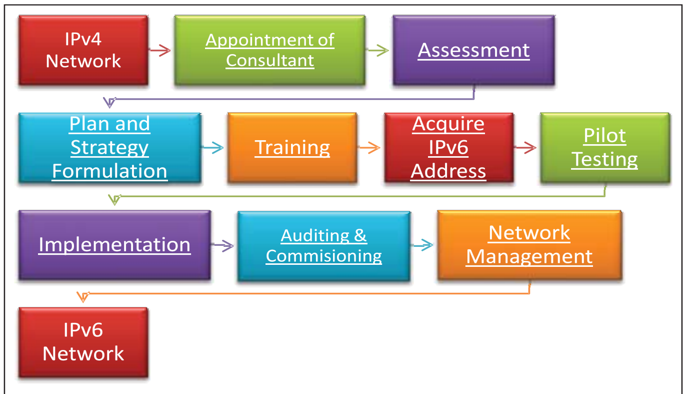


Figure 4: Step by step approach to IPv6 implementation

a) Appointment of Consultant: After the appointment of nodal officer and formation of transition team, it would be prudent to consider appointment of consultants with proven credentials in the IPv6 domain to guide on the roadmap for IPv6 adoption in the organisation in case sufficient expertise is not available in-house. As detailed in chapter 2, 11 organisations have been selected and empanelled by DoT to provide IPv6 consultancy and/or implementation of IPv6 services. However the Government organizations are free to appoint any other suitable consultant for their IPv6 requirement.

b) Assessment:The transition plan should be discussed with all stakeholders and a detailed assessment across the following should be conducted:

   i. Network Assessment

   ii. Application Assessment

   iii. Services Assessment

   iv. Security Assessment

c) Plan and Strategy Formulation: This involves detailed planning and formulation of a transition strategy on the basis of assessment gaps identified in the existing network and the plan for the future networks and services. The equipment report thus prepared should be got audited by the consultants or by an outside agency (whatever is considered as suitable) after which an equipment replacement plan is to be prepared and initiated to phase out non-compliant hardware and software.

d) Training: In order to have a seamless transition with minimum disruption due to human error or lack of knowledge, it is of utmost importance to develop skilled IPv6 trained human resources within the organisation. The required persons are to be identified for IPv6 training and arrangements for their training to be made. This can go on as a parallel and continuous activity.

e) Acquire IPv6 Address: The required IPv6 address blocks are to be acquired as per the IPv6 address plan firmed up during the planning and strategy formulation stage. It is recommended that addresses may be obtained from IRINN (Internet Registry for Internet Names and Numbers), formed in India recently, resulting in high flexibility and availability. The addresses thus obtained are called Provider Independent Addresses. However, the addresses can also be obtained from service provider(s) in which case they are called Provider Assigned Addresses. Such addresses result in dependency on service provider(s).

f) Pilot Testing: A pilot test network either centrally or in one of the organizations has to be set up for the purpose of detailed testing of the networks, applications and services before transition to IPv6. The process will cover testing of the IPv6 readiness across hardware, applications, services and their capability to interoperate with IPv4 for a seamless transition. The security audit will also be included in this process.

g) Implementation: On successful completion of testing, it is required that organizations implement the transition plan as per the plan finalised in step (c).This involves deployment of equipment in the network and transition of applications.

h) Auditing & Commissioning: Post implementation it is important to audit the network and applications to be able to run all the services seamlessly. Hence it is advisable to get the audit of networks and applications done for complete IPv6 readiness. Post successful audit the networks and applications will be certified as IPv6 ready for the services checked in audit. These audits will have to be conducted on a regular basis as and when any changes in network / application take place.

i) Network Management: Since IPv6 is a new protocol, the IPv6 network management is important to take care of any issues arising post implementation.

The Annexure D lists the suggested best practices in transition mechanism and the IPv6 feature support required across networks, applications and services touch points in a typical Government organisation scenario. The Government organizations should however discuss and plan the same in consultation with an IPv6 expert depending on their network status and complexity.

Central Government Ministry Scenario:

The transition plan of IT network of a typical Central Government Ministry alongwith the steps involved is as under:

The network comprises of layers as below :

1. Gateway Router: The router connects the department network to the NIC network or external internet .The router is to be configured with the IPv6 address to support dual stack. In the event the router does not support dual stack it is to be replaced with the new router with IPv6 support. The uplink peering with NIC/Internet is to be configured for IPv6 peering.
2. Firewall: The firewall protects the department network from external attacks. The firewall is to be configured with IPv6 to support dual stack. In the event the firewall does not support dual stack it is to be replaced with the new firewall with IPv6 support. The firewall is to be configured with IPv6 Access Control Lists (ACL's) to protect against the network attacks similar to IPv4 ACL's.
3. Layer 3 Switch: The Layer 3 switch is used to connect all the department PC systems to the network. The Layer 3 switch is to be checked for IPv6 support for VLAN, MLDv2 and ICMPv6.
4. PC systems: The end user operating systems are to be enabled with IPv6 protocol stack. In case the existing operating systems do not support IPv6 they are to be upgraded to IPv6 supporting operating system. Once upgraded the systems can be configured in dual stack mode with both IPv4 and IPv6 addresses.

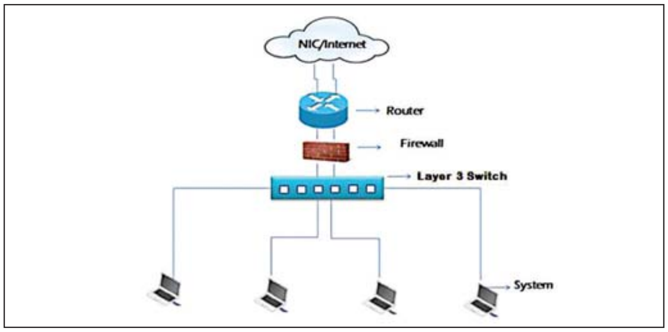


Figure 5: IT Network of a Typical Central Government Ministry

State Government Scenario:

The SWAN and SDC are crucial components for IPv6 transition in a state. A State Wide Area Network (SWAN) is one of the core infrastructure components under the National e-Governance Plan of the Government of India. The main purpose of this network is to create a dedicated Closed User Group (CUG) network and provide secured and high speed connectivity for Government functioning connecting State Head Quarters, District Head Quarters and Blocks Head Quarters. State Data Centres (SDC) are multiple data centers set up in various states of India to provide fundamental IT infrastructure for various e-Governance programs being run as part of National e-Governance Plan of India. The main purpose of these centres is to provide a physical facility for hosting various state level e-government applications. Both the SWAN and the SDC need to adopt IPv6 so that various e-services are delivered in a seamless manner to the citizens. The States need to incorporate the provision of funds for IPv6 implementation in SWAN / SDC etc. in their IT projects and if needed, they should revise their existing project estimates for the same. Similarly, the pilot projects for innovative IPv6 based applications should preferably be add-on with the existing IT projects and not standalone projects.

The basic strategy to be kept in mind by all Government organisations regarding IPv6 transition is that they should first focus on making public / external face of all Government projects for delivery of citizen centric services IPv6 ready (Dual Stack). Attempting all-at-once cutover should be discouraged. Efforts must be made to align and integrate the transition of the rest of the components with the product / technology life cycles as per the need of the organisation so as to alleviate large scale capital deployments to support the transition.

The Government organisations should integrate IPv6 requirements into their acquisition and upgrade plans and procure only ‘IPv6 Ready’ equipments. They should include IPv6 readiness in proposals for all new projects. Although directives to such effect have been issued way back in 2009 but due to lack of awareness, a few instances have been noticed where this requirement was omitted in RFPs floated for procurement of equipments. Hence, there is a need to reiterate it.

Therefore, the following are the recommendations:

- ❖ **The Government organisations should prepare a detailed transition plan for complete transition to IPv6 (dual stack) by December 2017 based on the network complexity & equipment/ technological life cycles. The plan should be prepared latest by December 2013 and accordingly the required budgetary provisions should be made in their demand for grant. For this purpose, it is recommended that a dedicated transition unit in each organisation should be formed immediately to facilitate entire transition.**

- ❖ **All new IP based services (like cloud computing, data centres etc.) to be provisioned for / by the Government organisations should be on dual stack supporting IPv6 traffic with immediate effect.**

- ❖ **The public interface of all Government projects for delivery of citizen centric services should be dual stack supporting IPv6 traffic latest by 01-01-2015. The readiness of Government projects in turn will act as a catalyst for private sector transition from IPv4 to IPv6.**

- The Government organisations should procure equipments which are also IPv6 Ready (Dual Stack) and go for deployment of IPv6 ready (Dual Stack) networks with end to end IPv6 supported applications. The equipment should be either TEC certified or IPv6 Ready Logo certified.

- The Government organisations should go for IPv6 based innovative applications in their respective areas like smart metering, smart grid, smart building, smart city etc.

- The Government organisations should develop adequate skilled IPv6 trained human resources within the organisation through periodic trainings over a period of one to three years to have a seamless transition with minimum disruption.

- The IPv6 should be included in the curriculum of technical courses being offered by various institutes / colleges across the country.

4.2 Service Providers

4.2 Service Providers

In a service provider network, IPv6 adoption is a fairly complex solution as it will involve a host of elements in the network. Service providers will have to do a detailed audit of their network elements to enlist the components as mentioned here to determine their IPv6 readiness. The various elements which will be involved during the process of transition are given below –

- **Basic network infrastructure –** This will include hardware support, connectivity, IP addressing, routing protocols, instrumentation etc.
- **Networked infrastructure services –** These include components like DNS, DHCP, Load balancing and content switching, Security elements (firewalls, IDS, IPS etc.), CDN elements, Optimization elements (SSL acceleration etc.), VPN access elements.
- **Infrastructure device enablement –** These will include mobility, email, VoIP, collaboration devices and gateways, Datacenters (Compute, storage, Virtualization elements etc.)
- **Middleware and databases –** Many databases and middlewares may be used by the service providers in their networks. All these should be identified and checked for IPv6 readiness. These may include the following –
  - Databases – MySQL, Microsoft SQL, Oracle, DB2 etc.
  - Application Servers – Weblogic, Liferay etc.
  - Webservers – Apache, IIS etc.
  - Middlewares – Messaging, Web services gateway etc.

4.2.1 Status

During the implementation of Roadmap-I the main focus has been to pursue the major service providers to transit to IPv6. It was envisaged that with the transition of major service providers, it will be much simpler for the minor service providers to transit because in most cases the minor service providers are dependent on the major service providers. In this regard, most of the major service providers have become ready to offer IPv6 services. The existing status of implementation of IPv6 by major service providers is given in Annexure E.

4.2.2 Challenges

There are many challenges being faced by service providers at present. Some of the many challenges faced by them are:

- Content & Application Providers need to be ready on IPv6 also.
- End User Devices on IPv6 are minuscule in India. There is a special need to focus on them, especially mobile handsets to make them IPv6 ready.
- Push from Government is needed to generate demand.
- Core network of service providers is ready for IPv6 but traffic is minuscule. Access layer also needs to be made available on IPv6.
- Broadband growth is not encouraging.
- ISPs/ Vendors/Content Providers/End user device vendors are all looking for business case and therefore IPv6 adoption is slow.

4.2.3 Transition Strategies

There are 3 well known transition strategies – dual stack, tunneling and translation – and their use will depend upon the specific situation. However, in most cases dual stack would be the most preferable solution for enterprise IPv4/IPv6 co-existence strategy. Tunneling will be required when there will be a need to connect islands of IPv4 or IPv6. Translation may be done to connect an IPv4 network to an IPv6 network or vice-versa. But translation is least preferred because it may adversely affect the applications working. If there is no impact on the working of applications of an organization then translation may be used. However, dual-stack is preferable solution. Another solution could be 6PE where service providers have MPLS backbones.

Apart from above, large service providers are also looking at CGN (Carrier Grade NAT) as intermediate solution to facilitate the IPv6 adoption process. However, CGN is having its own set of issues which makes the CGN solution expensive in the long run. This is mainly because of the requirement of additional application level gateways (ALGs), extensive log-keeping required on the CGN device due to security requirements and also performance degradation of the network thereby impacting the user experience. Therefore, CGN may be deployed only for a short period of time till the adoption of IPv6 picks up. Thereafter, the CGN equipments will be phased out and the service providers will move towards native IPv6. Therefore, service providers should keep in mind that even if CGN solution is available, it is a dead investment for the long run and therefore, it is always preferable to adopt native IPv6 from day one. The strategies for different network scenarios are explained below:

4.2.3.1 Wireless Networks (GSM & CDMA)

The rapid uptake of data services by mobile users and increased penetration of smartphones is rapidly exhausting the available IPv4 address pools with the operators. Even private IPv4 addresses defined in RFC 1918 are becoming scarce, e.g. a 10.0.0.0 block can provide only 16.7 million IPv4 addresses. The GSM networks have already evolved to 3G and data speeds are improving with HSPA, HSPA+ etc. thereby making data access on mobile very comfortable. Therefore, subscribers using data services are increasing rapidly. Since 3GPP (Rel. 9 and above) has already defined the standards for IPv6 deployment in mobile networks, operators should look to implement IPv6 at the earliest.

The implementation of data access in GPRS/UMTS networks is depicted in the figure below:

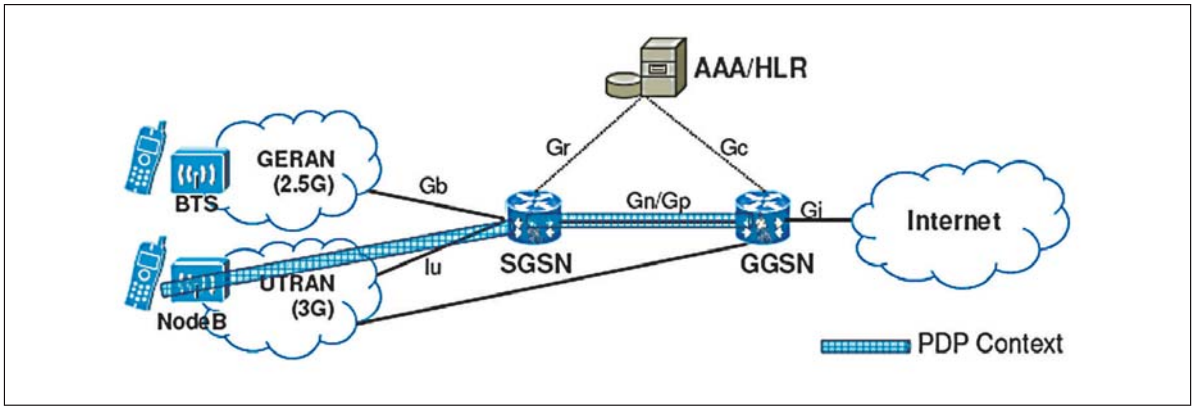


Figure 6: Implementation of data access in GPRS/UMTS networks

The SGSN and the GGSN are the critical elements in mobile networks, which will handle the PDP contexts/bearers for data traffic. The following are the possibilities:

(i) UE-GGSN link is IPv4 only.

(ii) UE-GGSN link is IPv6 only.

(iii) UE-GGSN link transports both IPv4 and IPv6 (It has a /64 prefix and IPv4 address configured).

Different elements, their design considerations and the impact of IPv6 on them are described in the table below:

Element	Design Consideration when IPv6 is used for internet and applications	Impact of IPv6
eNodeB	Radio layer. Can also use IPv4 backhaul	No
RNC	lu-CS/lu-PS can use IPv4 backhaul	No
SGSN	Initiate mobile APN query and authentication	Yes
HLR/HSS	IPv6 capable	Yes
GGSN	IPv6 PDP, standard IPv6 features, prefix allocation	Yes
Billing	Mediation and processing of IPv6 CDRs	Yes
Inventory System	IP address inventory to be updated with IPv6 addresses	Yes
CRM & provisioning system	IPv6 address to be assigned to customer & configured in various systems	Yes
DPI, Quote Server	Prepaid implementation, IPv6 parsing and CDR capability	Yes
WAP, Data accelerator	IPv6 packet compressions, cache capability	Yes
Firewalls	IPv6 rules capability, performance	Yes
DNS	IPv6 DNS capability	Yes
Device manager, PCRF	Attributes for IPv6 and policy enforement	Yes
Gi Router	Carry IPv6 and IPv4 packets natively.	Yes

All above devices are required to upgrade to support IPv6 in user plane and use IPv4 in transport and management plane. RAN, RNC, NB, eNB shall also be required to support IPv6 at later stage for end to end management and control plane on IPv6.The ultimate goal is to replace the use of IPv4 addresses in the transport network with IPv6 addresses from end-to end. **Therefore, all new GSM/ CDMA customer connections provided by Service Providers on or after 30-06-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.**

4.2.3.2 LTE Deployments

World over the mobile operators are making serious efforts towards the deployment of all IP based 4G networks for broadband access. The race to 4G is being driven by competition among operators to capture the market share among the advanced subscribers using various types of smartphone devices and applications that drive mobile data traffic growth. There are more than 113 operators in 46 countries already committed to LTE trials and deployments. Many operators are investing in HSPA+ RAN equipment and IP capable backhaul to offer true high speed mobile broadband performance as a key step to 4G LTE.

The first wave of commercial LTE networks will be initially supported by only USB data cards, embedded modems etc. offering high speed mobile internet access for notebook and netbook computers. New LTE operators are looking for a growing portfolio of LTE smartphones from leading vendors like Apple, RIM, Samsung, Motorola, LG, HTC, Nokia, Sony-Ericcson etc. In India various providers like Reliance Infotel Broadband, Aircel, Airtel, Qualcomm, Tikona, Augere, MTNL, BSNL are considering TDD-LTE deployments in the 2.3Ghz band after winning BWA spectrum. It is expected that LTE deployments will go through 3 phases –

(i) **Initial launch –** Data only. Most operators have begun their LTE deployments this way, providing LTE dongles and Data cards. This phase is expected to last about 2 years.

(ii) **Mass market –** Data only. In this phase the LTE deployments would be targeted towards the mass market and include netbooks, dual mode smartphones, dongles, data cards etc. This phase is expected to last about 3 years.

(iii) **Mass market –** Data and voice. The LTE deployments would mature to include LTE smartphones, netbooks, data cards, dongles providing both voice and data. Market adoption rates would be much higher as compared to phase-1 and phase-2.

As regards IPv6, the adoption of IPv6 is going to be particularly important for wireless carriers that are expecting a surge in mobile data traffic in the next few years, as they will need a fresh batch of Internet addresses to handle the multitude of wireless devices that will hook onto their networks. Some of the leading wireless carriers in the world have already made support of IPv6 compulsory and the support of IPv4 optional. The situation of IPv4 addresses in India (about 35 million IPv4 addresses) is already poor so deployment of IPv6 should be compulsory for all LTE operators. Since the operators are deploying new LTE networks the support for IPv6 should be insisted upon by them to their vendors at this stage itself. **Hence, all new LTE customer connections provided by Service Providers with effect from 30-06-2013 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.**

4.2.3.3 Wireline Networks

Broadband access on wire line networks is not growing fast enough as compared to wireless networks. The PSUs, BSNL and MTNL are large players in this segment because of their already established legacy wire line infrastructure. Few other service providers like Airtel are also providing wireline broadband access in major cities. Service providers will have to transit existing wireline connections to IPv6 and provide new wireline connections on IPv6. **Therefore, all new retail wireline customer connections provided by Service Providers on or after 30-06-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.**

Regarding transition of existing wireline connections, the main issue concerning IPv6 deployment is that the majority of the existing CPEs working at customer's premises are not IPv6 ready. As a step towards complete IPv6 deployment, these CPEs will have to be changed gradually over a period of time till the expiry of their life or when asked for by the customers. The CPEs are however of two types –

- **Service provider Owned CPEs -** It is easier to track and replace/upgrade these CPEs. All new CPEs deployed at customer premises from 30-06-2014 must be IPv6 ready only. **The Service Providers shall endeavor to progressively replace/ upgrade the Service Providers owned CPEs which are not IPv6 ready as per the following timelines:**

- o **Replacement / upgradation of 25% of CPEs by December 2014.**
- o **Replacement / upgradation of 50% of CPEs by December 2015.**
- o **Replacement/ upgradation of 75% of CPEs by December 2016.**
- o **Replacement/ upgradation of 100% of CPEs by December 2017.**

- **Customer Owned CPEs –** These CPEs are deployed by customers after purchasing from the open market. In this case, it would be difficult to pursue the customers to replace their CPEs. **Therefore, regarding the customer owned CPEs which are not IPv6 ready, the Service Providers shall educate and encourage their customers to replace/ upgrade such CPEs to IPv6 ready ones.** The service providers can resort to customer education programmes to tell them about the advantages of replacing their existing IPv4 CPEs with IPv6 ready CPEs. It is expected that with the passage of time, when IPv6 contents grow, customers will be self motivated to replace their old IPv4 only CPEs.

4.2.3.4 Enterprise Networks

For Enterprise Customers two main challenges are:

- ■ Readiness of Content on IPv6 and
- ■ IPv6 readiness of Customer IT Infrastructure/ Application.

Service Provider would enable IPv6 on new connections but customer has to overcome the above challenges by upgrading the infrastructure on v6 and adopting transitions mechanism like NAT 64 or alternate solution to access v4 content. Enterprise Customers have to start with dual-stack approach, allowing both IPv4 and IPv6 addresses to co-exist until the transition to IPv6 is complete. This approach will make sure that the transition occurs with minimal impact on customers.

At the moment getting IPv4 addresses are basically free for enterprises (usually included in the Internet connection fee and a relatively small component of the overall cost). Those enterprises that have agreements to use provider-allocated (PA - also called provider-aggregatable) addresses may find it difficult to change providers, due to an inability to acquire new PA space, thus increasing “lock-in.” The IPv6 strategies for enterprise customers should be as under:

- ■ Proper plan should be there to move smoothly and seamlessly from IPv4 to IPv6.
- ■ Always procure equipment /applications that support and are compatible with IPv4 and IPv6.
- ■ Check with Upstream service provider the no of IPv4 addresses available. This will help Enterprise to plan for faster IPv6 transition if there is shortage of IPv4 addresses.
- ■ Not implementing IPv6 can limit enterprise customers from doing business with other region who are ready with IPv6.
- ■ Mandatory Training /Workshop is required on IPv6 for all enterprises customers.

The enterprise network functions can be classified into three sections –

- **Internet presence:** All the services and content offered by the enterprise to the Internet community. This includes customers and partners of companies, students of schools, citizens of governments, potential donors to charities, and so on. The services and content are usually located in an Internet data center. In Indian scenario, most of these data centers are owned by the Telecom and Internet Service providers.
- **Intranet end-user Internet connectivity:** How the enterprise employees and applications access services and content on the Internet.
- **Intranet applications:** All the services and content located inside the enterprise and accessed only by enterprise users and applications. The services and content are located in the enterprise data center.

These sections are explained below:

Internet Presence

The IPv4 Internet will not stop working for existing users on the day when there are no more IPv4 addresses available from the RIRs. However, all new users in future will be using IPv6 addresses. This means that the Internet presence of an enterprise should support both the existing IPv4 users and the new IPv6 users. An enterprise Internet presence usually consists of three basic services offered to its partners, customers, and to the Internet community –

- Email,
- Web servers, and
- Domain Name System (DNS).

Enabling IPv6 on those three services will make the enterprise present on both the IPv4 Internet and IPv6 Internet. Certain operational support systems, network operations procedures and security components like firewalls/UTMs must also become IPv6-aware. **Therefore, all new enterprise customer connections (both wireless and wireline) provided by Service Providers on or after 01-01-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.**

Regarding the existing enterprise customers which are not IPv6 ready, the Service Providers shall educate and encourage their customers to switch over to IPv6.

Intranet end-user Internet connectivity

IPv4 address exhaustion may impact enterprise customers who do not have excess IPv4 addresses today and have a growing internal user base. But Enterprises generally use private IPv4 network address space along with NAT and application proxies which will dampen the impact of exhaustion. Providing IPv6 Internet access will allow internal users to reach content on the outside IPv6 Internet. There are a couple of deployment scenarios for an enterprise connecting to the IPv6 Internet –

- If the enterprise already has IPv4 access, then add IPv6 to provide a dual-stack solution; this is the most probable scenario for the next several years.

- If the enterprise cannot get IPv4 Internet connectivity from its ISP, it will be necessary to obtain IPv6 addresses and rely on the ISP to carry the IPv6 traffic to the IPv6 Internet.

In the case of adding IPv6 to an existing IPv4 Internet access, the enterprise has a few choices –

- **Use of application proxies (including web and email proxies) between the intranet and the IPv6 Internet -** The intranet users can still be IPv4-only, as the proxies will be able to do the AFT (Address Family Translation). When application proxies are not used, the enterprise needs to obtain a globally routable IPv6 address block large enough for the whole organization from its ISP or, in the case of having more than one ISP, request provider-independent IPv6 addresses from their Regional Internet Registry.
- **Native access from intranet users to the IPv6 Internet -** This obviously requires that the intranet hosts and all network devices are also dual stack.
- **Tunneled access from intranet users to the IPv6 Internet -** This requires that the intranet hosts are dual stack, but the intranet network does not need to be dual stack as tunnels can be used to transport IPv6 packets.

In the above cases, the choice of the solution and timeframe will depend upon the specific scenario faced by the enterprise and accordingly it has to be worked out in consultation with the ISP.

Intranet Applications

IPv4 address exhaustion only concerns the Internet and not the internal networks (the intranet) of most enterprises. Existing enterprises' networks often use private IPv4 addresses (RFC 1918) internally and rely on a perimeter NAT to access the Internet by sharing a few (or even one) public IPv4 addresses for all their internal users. There will be no reason for this to change when IPv4 addresses are no longer available. Internal applications will be able to use IPv4 for years even after the Internet stops using IPv4 and uses only IPv6.

Public IPv4 address space exhaustion might not be the primary driver for IPv6 adoption in some enterprises. However, many enterprises do have public IPv4 address running on their Intranet, for example, in the data center. If this is the case, the enterprise needs to plan for the impact of not being able to obtain additional public IPv4 addressing in the future. However, transition to IPv6 for intranet applications will most likely be a matter of choice for the organization rather than a compulsion.

Despite above reasons regarding IPv6 adoption by enterprises, it would be prudent for enterprises to plan for proper transition to IPv6. They can start with their external public facing entities starting with Internet presence and ending with Intranet applications. They should consult their service provider for the same.

4.2.3.5 Checklist for IPv6 Readiness Assessment

During the process of adoption of IPv6 many questions may arise. In this context a checklist is attached at Annexure F which will clarify many of the general issues concerning the adoption of IPv6 by service providers or an enterprise.

4.3 Content & Application Providers

4.3 Content & Application Providers

The exponential and explosive growth of internet over the past few years can be rightly attributed to the availability of numerous user friendly applications and content over the internet. As a result, the internet has evolved from a medium of mass information dissemination to a platform for delivering various services like social networking, internet banking, e-commerce, e-governance etc. The content and application providers, therefore, form an important link in the value chain of the ICT ecosystem. As majority of the major service providers in India are ready to handle IPv6 traffic & offer IPv6 services, IPv6 based services are gradually being made available today to customers on pan India basis across all segments i.e. Fixed, Mobile and Enterprise. It is now the turn of content and application providers to take the lead.

4.3.1 Status

As a result of the initiatives undertaken since the release of Roadmap Ver-I, there has been a marked improvement in the awareness level of content and application providers with respect to IPv6. From being thought of as something that they have to deal with in distant future, there is a growing realization amongst content and application providers that IPv6 is right there upon them. The World IPv6 Launch Day (06-06-2012) and World IPv6 Day (08-06-2011) have further contributed to this realization with some of the major content providers like Google, Yahoo, Facebook, Youtube, Bing etc. permanently enabling IPv6 for their products and services with effect from 06th June 2012. In order to lead by example, it has been decided that the websites of all Government organisations maintained by NIC shall be transited to IPv6 (dual stack) by December 2012. NIC has made significant progress on this issue and has already completed transition of considerable number of websites to IPv6 including that of DoT. Further, the content providers are being educated and encouraged to host their websites on dual stack when they approach for domain name registration/renewal. A few leading Indian content providers like Flipkart etc. have also transited their websites to IPv6.

4.3.2 Challenges

The foremost challenge still remains the lack of awareness about the IPv6 adoption and a proper understanding of the issues involved. Although there has been a marked improvement in the awareness level of content and application providers with respect to IPv6 adoption, yet there remains a general perception in their minds that the transition is likely to be a costly affair. However, contrary to popular belief, the transition is not a costly issue as has been demonstrated by some Indian content providers like Flipkart etc. In fact, all that it took for Flipkart to transit their website to dual stack was deployment of four engineers for two weeks time.

Another important issue concerning the content and application providers is the need to make the payment gateways IPv6 ready. With mobile phone fast transitioning itself from a mere communication device to an instrument of empowerment for accessing a whole gamut of services including m-payment, it becomes all the more necessary to make the payment gateways IPv6 ready so as to ensure seamless delivery of services. This in turn is likely to have a multiplier and transformational impact on the whole environment. The matter has already been taken up by DoT with Department of Financial Services (DFS), Ministry of Finance and Reserve Bank of India to get it done by December 2012 and the work is under progress.

Other bottlenecks faced are the low subscriber base of native IPv6 users and the lack of IPv6 ready end user devices like mobile handsets, data card dongles, CPEs etc in the ecosystem. Further, the availability of IPv6 trained manpower is also an issue which needs to be taken care of.

4.3.3 Strategy & Transition Plan

The content and application providers need to take the first step towards IPv6 adoption immediately without any further delay for the following reasons:

- IPv6 adoption is essential from the stand point of business continuity. It is a reality that the numbers of native IPv6 customers are going to be sizeable very soon. Since IPv6 is not backward compatible with IPv4, these native IPv6 customers will be able to access content on IPv4 only with the help of some transition mechanisms like NAT etc. Every NAT suffers from a performance overhead, adding some additional latency to the customer experience, potentially leading to business risk.
- Since IPv6 adoption is an eventuality no business can shy away from, it makes sense to start early. In this way, the organisations can afford to go through the learning curve without much impact on their services since the number of IPv6 consumers is low today.
- IPv6 adoption helps organisations to gain the early mover advantage and be one step ahead of competition.

Since IPv4 and IPv6 will co-exist for a long time to come, it is beneficial for content and application providers to go for dual stack approach. The following transition plan is therefore recommended:

❖ **All contents (e.g. websites) and applications providers should target to adopt IPv6 (dual stack) for new contents & applications by 30-06-2014 and for existing ones latest by 01-01-2015.**

❖ **The complete financial ecosystem including payment gateways, financial institutions, banks, insurance companies, etc. should transit to IPv6 (dual stack) latest by 30-06-2013.**

❖ **The new registrations on '.in' domain to be compulsorily on dual stack with effect from 01st January 2014.The entire '.in' domain should migrate to IPv6 (dual stack) latest by June 2014.**

4.4 Equipment Manufacturers

4.4 Equipment Manufacturers

The equipment manufacturers in the IPv6 ecosystem can be broadly classified in two categories. The first category (hereinafter referred to as network equipment manufacturers) comprises of the manufacturers of those equipments that are used in the networks of service providers to provide service to the customers. The manufacturers of equipment / devices that are used by the end-users in order to make use of the services provided by the service providers form the second category (hereinafter referred to as end user devices manufacturers). In order to ensure seamless delivery of services on IPv6 platform, on one hand it is important that the service providers are ready to offer them who in turn depend on the backend readiness and support of network equipment manufacturers. On the other hand, it is equally significant that the end user devices manufacturers do not lag behind in this regard so that the user is able to the feel the enhanced user experience on an IPv6 network with the active support of content and application providers.

4.4.1 Status

A majority of network equipment manufacturers are well aware of the issue and adequately prepared as far as IPv6 readiness of their product offerings is concerned. As described in chapter 4.2, majority of the major service providers in India are ready to handle IPv6 traffic & offer IPv6 services at present. This has been made possible because of the support of network equipment manufacturers as the equipments form the bedrock of telecom networks. The status of some of them has been tabulated in Annexure G. As clear from the status, the manufacturers which are not ready / partially ready are likely to be so in next 1-2 years time.

In contrast, the manufacturers of end user devices like mobile handsets, data cards dongles, tablets, smart phones, DSL modems/routers etc. do not appear to be fully geared up to meet the IPv6 challenge . At present, barring a few high end devices like smart phones, tablets etc. only a small fraction (less than 5%) of these devices is IPv6 ready. Nevertheless, it is notable that most personal computers running recent operating system versions are IPv6 ready.

In order to take care of the testing and certification issues of the manufacturers, an IPv6 test bed has been installed by Telecom Engineering Centre (TEC) wherein the equipments can be tested and certified for IPv6 compatibility, readiness, conformability and interoperability. This test bed will greatly benefit manufacturers especially Indian ones as it obviates the need to take the route of expensive testing and certification process of other countries. IPv6 standards for India have already been released by TEC after taking into consideration the USGv6 and IPv6 Ready Logo standards. Further, TEC is in the process of framing standards for IPv6 ready mobile handsets.

4.4.2 Challenges

The main challenge of the equipment manufacturers is the low demand due to slow uptake of services on IPv6 platform and low subscriber base of IPv6 users in the country. The low awareness levels among the customers of end user devices about IPv6 also need to be addressed. As contents and applications gradually start transiting to IPv6 and various features of IPv6 especially the better multimedia performance and IPv6 based innovative applications are appreciated far and wide, the equipment manufacturers in general and end user devices manufacturers in particular will be stimulated to switch over to IPv6 with in an accelerated time frame.

4.4.3 Strategy & Transition Plan

With major service providers in India ready to handle IPv6 traffic & offer IPv6 services, the network equipment manufacturers are geared up as far as IPv6 adoption in their product offerings is concerned. They are likely to further improve upon their preparedness in synchronization with the service providers as the latter move forward in accordance with the timelines set in Chapter 4.2.

However, the readiness of end user devices still remains as area of concern. With the Government envisaging providing ‘Broadband on Demand’ by the year 2015 under NTP-2012 and setting a target of 175 million and 600 million broadband connections by the year 2017 and 2020 respectively to ensure equitable and inclusive development, the next wave of broadband revolution is sure to ride on IPv6 resulting in an exponential demand of IPv6 ready end user devices. Besides, the evolution of mobile handset from being a simple voice phone to a veritable computing device with internet connection, a m-commerce instrument, a digital camera, a music system, a positioning device, a mobile TV, a video phone, a messaging device, a video player and a voice phone all rolled into one further underscores the need for such devices to be next generation Internet Protocol ready. In addition, there is a requirement of Law Enforcement Agencies (LEA) for easy monitoring and tracking of such devices in the national interest for which IPv6 offers a better solution as each device can be assigned a unique public IPv6 address. The Government organisations have already been directed to procure IPv6 ready equipments only.

The increase in demand of IPv6 ready end user devices will not be restricted in terms of traditional broadband or mobile connection devices. With rapid advances being made in machine to machine communication, cloud computing, tracking and positioning, controlling devices and processes, smart meters, smart grids, smart homes , smart cities and various others innovative IPv6 based applications, the number of connected devices and human being would together exceed all estimates that are being made today.

Therefore, there is a strong incentive for the equipment manufacturers to plan early and move ahead in the direction of IPv6 adoption. The following transition plan is therefore recommended:

- ❖ **All mobile phone handsets/ data card dongles/ tablets and similar devices used for internet access supporting GSM /CDMA version 2.5G and above sold in India on or after 30-06-2014 shall be capable of carrying IPv6 traffic either on dual stack (IPv4v6) or on native IPv6.**
- ❖ **All wireline broadband CPEs sold in India on or after 01-01-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.**

4.5 Cloud Service Providers/ Data Centres

4.5 Cloud Service Providers / Data Centres

As IPv6 is adopted across the internet eco-system, the IPv6 adoption by Data Centers/ Cloud Service Providers is a critical component, whereby the applications and services being used by enterprises and end-users can be IPv6 enabled. The IPv6 adoption across the Data Center/ Cloud Services provider will accelerate and hasten the IPv6 adoption by the content and application providers.

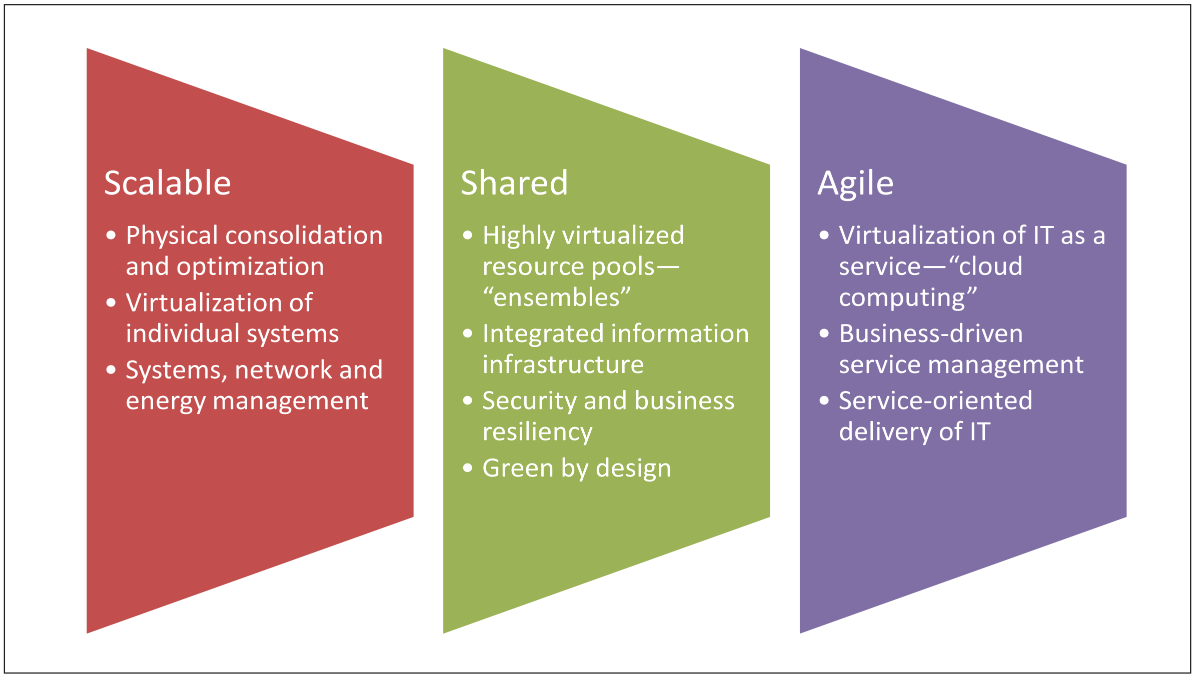
In addition to encouraging the content/ applications providers to adopt IPv6, the IPv6 cloud services will also bring in IT infrastructural efficiencies. Today newer services are evolving and spreading at a faster pace which has resulted in need of scalable and agile computing systems. IPv6 provides the required networking related capabilities for scalability. The coming together of cloud and IPv6 introduces a major technology inflection in the area of Next Generation Data Centers.

IPv6 cloud – complex but justified

IPv6 and cloud computing are technologies which impact every aspect of the IT eco-system, wherein the hardware, software & IT processes need to be adapted for IPv6. The exercise of building the IPv6 cloud is an involved and complex exercise, requiring coordination across multiple strata of technologies.

Cloud computing and IPv6 are technologies which when implemented together build a system that provides the resources and capabilities to scale up cloud deployments. IPv6 simplifies the manageability of distributed cloud resources and consumers. Executing one transition without the other is likely to lead to suboptimal or short-term solutions.

Features of a scalable, shared and agile cloud data centre



Scalable

- Physical consolidation and optimization
- Virtualization of individual systems
- Systems, network and energy management

Shared

- Highly virtualized resource pools—“ensembles”
- Integrated information infrastructure
- Security and business resiliency
- Green by design

Agile

- Virtualization of IT as a service—“cloud computing”
- Business-driven service management
- Service-oriented delivery of IT

As the computing needs of organizations grow, the computing and the related networking needs grow as well. The fact that IPv4 address space is exhausted is known, and would lead organizations to adopt IPv6, so that the computing and the networking needs grow together in tandem. As these organizations adopt cloud, they would also need to work with their Service Providers to ensure that the networking related resources are available, be it from IPv4 or IPv6 perspective.

IPv6 and Cloud – The Components

The legacy Data Centers which were typically built to support 1:1 infrastructure needs, wherein one physical server supported a single application has evolved to a virtualized environment wherein a single machine or a cluster of machines, come together to provide services across multiple servers and softwares.

The new Data Center systems have evolved to be a more agile and scalable IT computing hub, wherein the various services provided are as follows:

IaaS – Infrastructure as a Service

PaaS – Platform as a Service

SaaS – Software as a Service

A cloud is a virtualized data center to achieve the following objectives:

- Elasticity: Ability to scale virtual machines resources up or down
- On-demand usage: Ability to add or delete computing power (CPU, memory) and storage according to demand
- Pay-per-use: Pay only for what you use
- Multitenancy: Ability to have multiple customers access their servers in the data center in an isolated manner

4.5.1 Status

The IPv6 adoption by Data Center Operators and Cloud Service Providers is in very initial stages today. The Data Centers/Cloud Services provided by large Internet Service Providers (ISP) are preparing to provide IPv6 services whereas the independent Data Center/Cloud Service providers are yet to initiate the journey towards IPv6 adoption. Since Cloud is comparatively new concept and most of the Cloud Data Center are built in last two-three years, it will be easier to transit to IPv6 as hardware replacement requirement will be minimal.

IPv4 exhaustion timelines and timeline impact

The impact of the IPv4 address pool exhaustion on the Data Center/Cloud Service providers varies based on the services provided and the customer base served. The impact of exhaustion will be higher in the case where public services are provided to the various customers.

The ISPs typically provide public Data Center/Cloud services in addition to having their own private captive data centers. This segment of the industry would be the torch bearer of IPv6 adoption across the IT eco-system, wherein both the network and the data center services would be provisioned for IPv6 first accordingly. In case this segment of the industry does not adopt IPv6 in the foreseeable future, the lack of IPv4 address pool will result in many of the downstream service providers and content providers/applications providers, being unable to plan for their further growth of network and services, resulting in stagnation of their internet business due to lack of IPv4 addresses, which would be detrimental to their existence.

The Data Center/Cloud service providers will be significantly impacted by the exhaustion of the IPv4 address pool as they are dependent on the internet service providers for the address pool resources and network connectivity requirements.

4.5.2 Challenges

Business Drivers:

The lack of interest in IPv6 Services from end customers has been a cause of concern among the Data Center/Cloud service providers towards IPv6 adoption.

This has resulted in lack of motivation for the IPv6 adoption across the Data Centers/Cloud Service Providers, wherein it has placed difficulties in justifying the budget allocation for the IPv6 adoption across the organizations.

In addition to the above there is also lack of awareness about new IPv6 based Business services which can be launched to help create new revenue streams.

Hardware/Software:

The limited availability of IPv6 ready hardware and software for creating cloud infrastructure from all manufacturers is also a challenge for IPv6 adoption by data centres/ cloud service providers.

Network Connectivity:

The lack of adequate IPv6 network connectivity, more so in the area of access networks and mobile networks has resulted in lack of retail end-user customers, which impacts the IPv6 business case for content and application service providers and thereby the Data Center/Cloud services providers.

Skills Availability:

The lack of adequate IPv6 skills has been a challenge towards IPv6 adoption, by the Data center/Cloud services provider, more so in the following areas:

- Networking
- Data Center
- Network Management

4.5.3 Strategy & Transition Plan

The IPv6 adoption across the Data center/Cloud Service Providers would require a phased approach spread across a few years, wherein the technology adoption and the business demand would go hand in hand.

Area	Strategy
Business Drivers	• Awareness need to be built for in-house working team as well as for the end customers towards IPv6. • IPv6 ready setup may be focused as USP in marketing campaigns.
Network Connectivity	• Detail IPv6 networking compliance • Upgrade upstream connectivity to IPv6/ Dual stack • Prompt end users to have IPv6 connectivity
Hardware and Software	• Assess the requirement of hardware and software upgrade to IPv6. • Set up gradation plan keeping in mind lifecycle and end users requirements. • All new hardware/ software procured should be IPv6 ready.
Skills	• Both networking and system administration skill set should be upgraded to IPv6 in a time bound manner.
Pilot Projects	• Initiate IPv6 pilot projects to have confidence as well as a model for end customers.

The approach can take into consideration 2 categories of data centers –

(i) Old data centers – The old data centers will typically have hardware and software resources which are not IPv6 ready. Therefore, they will need some time to replace and upgrade their data centres to make them IPv6 ready. They may need one- two years time for this.

(ii) New data centers – Data centers being established newly can choose to be IPv6 ready from day one by choosing the appropriate hardware and software. They can provide services using IPv6 connectivity immediately.

The Cloud Service Providers / Data Centres are encouraged to adopt IPv6 across their commercial and captive infrastructures. The IPv6 adoption by this segment of the industry would enable the ICT eco-system in India to adopt IPv6 services at a faster pace. The details of IPv6 adoption by Cloud Service Providers / Data Centres is given in Annexure H.

Accordingly, it is recommended that **all public cloud computing service / data centres providers should target to adopt IPv6 (dual stack) latest by 30-06-2014.**

4.6 Security Best Practices

4.6 Security Best Practices

This basic purpose of this chapter is to help organizations understand IPv6 security implications and best practices to mitigate vulnerabilities in IPv6 deployment. Just like the early deployment of many technologies, security is often left to the final stages of implementation which introduces many challenges and also complicates the security deployment at later stage. The intent of this chapter is to improve the security of IPv6 deployments from day one. This chapter provides guidelines to organizations to aid in securely deploying IPv6.

While IPv6 is not directly compatible with its predecessor, it poses many of the same risks associated with IPv4. In addition, IPv6 offers a number of new capabilities that could potentially introduce additional vulnerabilities and threats to agencies. But, if implemented properly, IPv6 has the potential to provide a foundation for creating a secure infrastructure for an organization as well as the Internet as a whole. IPv6 provides many additional security features over IPv4 like extension header based IPSec support and Secure Neighbour Discovery Protocol (SeND).

4.6.1 Background

Due to the exhaustion of free IPv4 (Internet Protocol version 4) address space and internet device explosion, Government and private agencies have started using the IPv6 (Internet Protocol version 6) protocol into their networks. Switching from IPv4 to IPv6 will not be possible in an instant way but over a period of time with IPv4/IPv6 coexistence. During this phase, transition techniques like dual-stack, tunnelling and translation have to be deployed. As IPv6 becomes more popular, the attacks on it will increase. This is similar to the case that as the popularity of web browsers like Internet Explorer, Chrome, Firefox etc. grew, so did the number of people working to find flaws with them. IPv6 is likely to follow the same course as the number of deployments increase and it becomes a focus of new security research. The process of finding and correcting vulnerabilities will only make IPv6 stronger. The attacker community is gaining interest in IPv6 as it is an easy route for them with lack of IPv6 expertise in organizations. It is therefore important for organizations to improve the security of IPv6 deployments from day one.

IPv6 has some advantages over IPv4 but also have few unique security vulnerabilities. The transition to IPv6 is inevitable; therefore organizations should understand the threats that exist in IPv6 networks and protect against them. Organizations are most likely to face the below mentioned security challenges during the deployment process:

- An attacker community that most likely has more experience and comfort with IPv6 than an organization in the early stages of deployment.
- Difficulty in detecting unknown or unauthorized IPv6 assets on existing IPv4 networks.
- Added complexity while operating IPv4 and IPv6 in parallel.
- Proliferation of transition-driven IPv6 (or IPv4) tunnels, which complicate defences at network boundaries
- If organizations elect to deploy IPv6 without security, it is like running a backdoor protocol to the dual-stack systems that could potentially be exploited

Security vulnerabilities that exist for IPv4 also generally apply to IPv6 however there are additional vulnerabilities that exist for IPv6 but do not apply to IPv4. These fall in three major categories:

1. IPv6 Basic Protocol Vulnerabilities :

Attacks against ICMPv6: ICMPv6 is a required component of IPv6.

Extension Header (EH) attacks: EHs need to be accurately parsed.

Auto configuration: NDP attacks are simple to perform.

Mobile IPv6 attacks: Devices that roam are susceptible to vulnerabilities.

2. IPv6 Transition Mechanism Protocol Vulnerabilities :

Attacks on transition mechanisms: transition techniques are required by IPv6 for transition mechanisms like Dual-stack, Tunnelling, NAT etc.

3. IPv6 Operational Vulnerabilities:

Operation vulnerabilities: Complex IPv6 filtering, padding option and new extension header introduction.

4.6.2 Proposed Approach for Secure IPv6 Deployment

Organizations should understand the security risks of deploying IPv6, as well as strategies to mitigate such risks. Below is the recommended approach for secure IPv6 deployment:

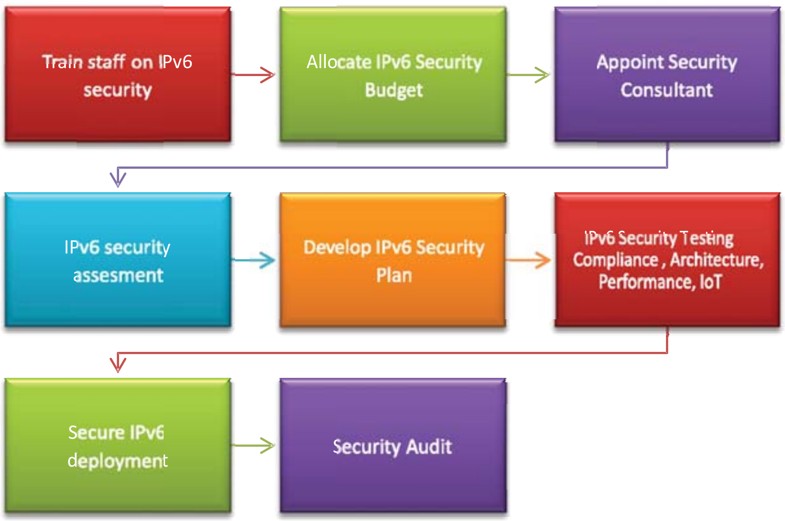

Train staff on IPv6 security
Allocate IPv6 Security Budget
Appoint Security Consultant
IPv6 security assesment
Develop IPv6 Security Plan
IPv6 Security Testing Compliance , Architecture, Performance, IoT
Secure IPv6 deployment
Security Audit

Figure 7 : Secure IPv6 Deployment

Step-1: Train Staff on IPv6 security:

Organizations must understand the differences between IPv4 and IPv6 and know how those differences have security implications. IPv6 is going to coexist with IPv4 for a foreseeable future which means the network is as secure as the least secure protocol; organizations should have the security architecture in place for both protocols. Since both protocols do not inter-operate, it requires a transition technique such as tunnelling, NAT etc. Organizations need to ensure a secure transition deployment.

As a first step, organizations should look to build IPv6 security skill sets equalling to IPv4 security skill sets. Organizations should provide IPv6 security training for key operational personnel and policy makers. The individuals should have enough information to be able to formulate IPv6 policy and guidance for the organization, and to implement enough security safeguards to enforce the policies.

Organizations should look to build IPv6 security skill sets equalling that of IPv4. Below are the suggested topics which should be covered in depth in IPv6 security skill set development:

- IPv6 and IPv4 security differences
- IPv6 Security Features
- IPv6 Security Issues
- IPv6 Security monitoring
- IPv6 Network attacks
- IPv6 Security threat mitigation
- Secure transition mechanisms
- IPv6 Security best practices

Step-2: Allocate IPv6 Security Budget:

Organizations should do the budget allocation for IPv6 security in addition to IPv4. Budget calculation should be based on efforts required for security assessment, design, testing and deployment. Organizations should allocate additional budget if any hardware upgrade is required to meet the security requirements.

Step-3: Appoint Security Consultant:

Organizations may choose to appoint external security consultants or internal staff for conducting IPv6 security posture analysis, build IPv6 security plan, testing and deployment. Based on organizations' IPv6 security skill sets and the business needs, some or all of these activities can be outsourced to experienced consultants.

Step-4: IPv6 Security Assessment:

IPv6 security assessment helps to understand the risks posed to an organization by vulnerabilities present in the organization's IP-networked systems including IPv6 and IPv4. Security assessment should capture network, applications and services security posture and highlight the vulnerabilities with possible mitigation techniques.

Step-5: Develop IPv6 Security Plan:

While IPv6 provides the foundation for the development and implementation of a more secure network, organizations must be concerned with potential issues the new protocol may create. Examples of these issues are:

- Poorly implemented IPv6 stacks
- Few network protection devices/tools support IPv6
- Improperly configured network elements like firewalls, IDS, IPS etc.
- New attacks
- Poorly implemented IPv6 routing protocols
- Inconsistent IPv4/IPv6 security features
- Few IPv4 network management tools ported to IPv6

- Organizations not leveraging new security features
- New/existing applications unable to leverage new IPv6 features

The development of the IPv6 Security Plan should include a core understanding of all of the components necessary to secure the organization's networks.

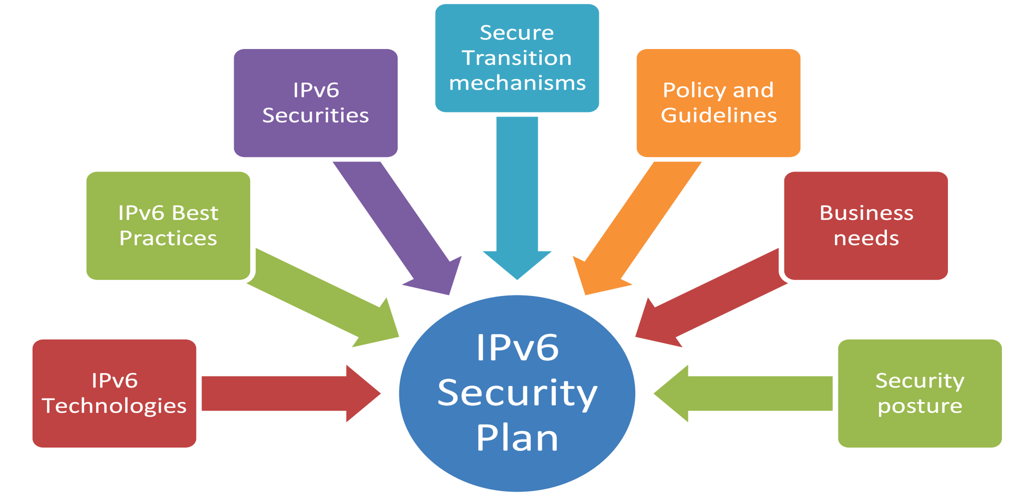


Figure 8: IPv6 Security Plan

Organizations should build the security plan by giving due consideration to all the above points.

Step-6: IPv6 Security Testing:

Validation of IPv6 features, interoperability and performance issues become critical factors for organizations for smooth transition to IPv6. Since IPv6 is a new protocol stack it becomes important to test the protocol implementations in vendor hardware and software as this could become critical. Below are the suggested tests, organizations should perform before deployment:

- IPv6 security conformance testing
- IPv6 security Inter-op testing
- IPv6 security performance testing
- IPv6 security design validation Testing

Step-7: Secure IPv6 Deployment:

On successful completion of testing it is required that organizations implement the transition plan.

Step-8: IPv6 Security Audit:

Organizations should have a regular audit policy to ensure that new vulnerabilities are adequately addressed in the network. It is recommended to have periodic security audits (e.g. at least one security audit every year) to assess the security state of the network so that appropriate actions can be taken proactively.

4.6.3 IPv6 Security Best Practices

In order to achieve security parity with IPv4 networks, the emerging IPv6 networks should be protected against all attacks for which IPv4 networks are currently protected. They should additionally be protected against new attacks that are specific to new features. Below are a few best practices for reference:

- Encourage staff to increase their knowledge of IPv6 to a level comparable with their current understanding of IPv4
- Plan a phased IPv6 deployment utilizing appropriate transition mechanisms to support business needs; don’t deploy more transition mechanisms than necessary
- Plan for a long transition period with dual IPv4/IPv6 co-existence
- Apply an appropriate mix of different types of IPv6 addressing (privacy addressing, unique local addressing, sparse allocation, etc) to limit access and knowledge of IPv6-addressed environments.
- Use automated address management tools to avoid manual entry of IPv6 addresses as they are prone to error because of their length and form of notation.
- Develop a granular ICMPv6 (Internet Control Protocol for IPv6) filtering policy. Ensure that ICMPv6 messages that are essential to IPv6 operation are allowed, but others are blocked. Security firewalls will have to be configured accordingly for IPv6.
- IPv6 brings many new vulnerabilities; organizations should test all products/solutions for IPv6 security before deploying in the network.
- Be aware of extension header threats and filter extension headers appropriately
- Drop packets containing Routing Header Type 0 and unknown option headers whenever possible.
- Deny packets that do not follow the rules for extension headers.
- Perform Unicast RPF filtering to prevent spoofed source addresses.
- Deploy DNSSEC
- Restrict who can send messages to multicast group addresses
- Use IPSec (Internet Protocol Security) to authenticate and provide confidentiality to assets that can be tied to a scalable trust model (an example is access to Human Resources assets by internal employees that make use of an organization’s Public Key Infrastructure (PKI) to establish trust).
- Identify capabilities and weaknesses of network protection devices in an IPv6 environment.
- Enable controls that might not have been used in IPv4 due to a lower threat level during initial deployment (implementing default deny access control policies, implementing routing protocol security, etc).
- Pay close attention to the security aspects of transition mechanisms such as tunnelling protocols.
- Use Control Plane Policing for granular control over the router’s processes

- Ensure that IPv6 routers, packet filters, firewalls, and tunnel endpoints enforce multicast scope boundaries and make sure that Multicast Listener Discovery (MLD) packets are not inappropriately routed.
- Use QoS policy to control misbehaving IPv6 applications and ICMPv6 flooding
- Use Access Control Lists (ACL) to selectively filter IPv6 traffic.
- Harden IPv6 firewalls.
- Filter ICMPv6 messages on LAN devices but do not block NDP.
- Follow the vendor offering, which should include protection against RA, ND, and DHCP attacks
- Use authenticated DHCPv6 if applicable.
- Deploy SeND to secure the LAN.
- Use the management plane of your devices to observe IPv6 performance.
- Harden your computers against malicious IPv6 packets.
- Check on what ports your computer is listening for connections.
- Review your neighbour cache for unauthorized systems.
- Check for undesired tunnel interfaces.
- Make sure that your IPv6 hosts are not unintentionally forwarding IPv6 packets.
- Leverage IPv6-capable stateful firewall.
- Secure deployment of tunnelling

PART C

CHAPTER 5

Standards & Testbed

5.1 Standards & Testbed

Present telecom technologies/networks are moving rapidly towards IP. Next Generation Networks (NGN) based on IP technologies are poised to register global expansion at a fast pace. IPv6 is a relatively new protocol when compared to the length of time IPv4 has been in use. The extensive adoption of IPv6 has started only recently because of the exhaustion of the free IPv4 addresses because of which the organizations have no option but to adopt IPv6 for ensuring the continued growth of the Internet and other networks dependent on IP technology.

Standardization is a very important aspect in the growth and adoption of any new technology and the same is in case of IPv6 also. Since IPv6 is relatively new, many aspects of the technology are still being standardized and for this many global organizations like the IPv6 Forum, IETF, 3GPP etc. are working to make its use unambiguous in different types of networks and scenarios. One big problem being faced by users is how to ensure whether the IPv6 features promised in a particular product by some vendor are complete or not. In case of India, manufacturers and vendors of IP products are very few and most of them are imported. So it is high time to set up world class testing infrastructure in the country to ensure interoperability, end to end performance, benchmarking, secure application delivery, seamless mobility etc., for smooth uptake and growth of IPv6 and other NGN technologies in the country. Establishing test labs in the country will ensure that only the right products are imported and deployed by the service providers and other users. Some service providers have their own in-house labs to do this kind of a testing but smaller organizations have nowhere to go for such kind of a testing / validation. The IPv6 lab installed by TEC is the first public facility of this kind where anyone can bring an IP product and get it tested for IPv6 readiness by paying a small fee.

5.1.1 About TEC & its Activities

TEC, the technical arm of DoT, is involved in formulation of Standards and Fundamental Technical Plans and bringing out specifications and common standards with regard to telecom network equipment, services and interoperability. It also interacts with multilateral agencies like APT, ETSI and ITU etc. for standardization. It develops expertise to imbibe the latest technologies & results of R&D and also provides technical support to DOT and technical advice to TRAI & TDSAT. To keep pace with the advancement of technology and in order to meet the requirements of setting up NGN test & certifications labs, TEC has taken the initiative to setup following labs in TEC:

a) Transport Lab

b) Control Lab

c) Service/application Lab

d) Access Lab

e) Customer Premises Equipment (CPE) (including terminals) Lab

f) These labs are proposed to be set up in phased manner in such a fashion that different labs classified under separate disciplines in telecom are envisaged to be integrated at the backend into a single test bed. Each lab has been conceptualized as a test bed created by a host of DUTs (Device Under Test) offered by Telecom Equipment vendors connected in a network configuration. This network would be connected by test equipment that are themselves capable of emulating large virtual networks behind their connecting ports, and subjecting the test bed with simulated traffic relating to different tests. The testing shall require the utilization of multiple scripts (coded programs) that will facilitate automated testing. The test solution providers may have a back-end tie-up with original test equipment manufacturers. These labs are envisaged to be self contained and centrally managed for all test operations and report generation. They are intended to serve Indian and International Telecom equipment manufacturers, Telecom operators, Regulators, Application/Content Service Providers, independent Software developers, R&D Institutions, Educational Institutes, Chipset manufacturers etc., for conformance, performance, functional and interoperability among public networks and to benchmark devices/applications/networks/ services for all real life scenarios. TEC shall maintain the confidentiality of test results. Test results shall not be shared with any other party without specific advice from concerned applicant. However, clients could publish/advertise/ share test results with due intimation to TEC.

To start with and in the first phase, TEC has installed NGN Transport Lab in New Delhi. The lab is equipped with –

(i) Testing & Measurement System for IPv6 Conformance & interoperability.

(ii) Testing & Measurement system for L2-L7 testing including Session Border Control Function for IP based network elements

(iii) Router, Firewall, LAN/Ethernet Switch, Blade Server, Management console and work stations etc.

(iv) Exploitation Room Accessories including, Plasma display unit, overhead projector & screen, heavy duty printer, copier/scanner etc.

(v) IPv6 Test Bed

The IPv6 test bed installed in NGN Transport Lab, TEC, New Delhi shall provide testing for conformance, performance, functional and interoperability testing of DUTs (Device Under Test) for following protocols.

(i) **IPv6 Core Protocols** like IPv6 Addressing Architecture, Neighbor Discovery, IPv6 Stateless Address Auto configuration, Path MTU Discovery (PMTU), Internet Control Message Protocol for IPv6 (ICMPv6) which enables hosts and routers that use IPv6 communication to report errors and send simple echo messages, Multicast Listener Discovery (MLD) which enables one to manage subnet multicast membership for IPv6

(ii) **IPSec,** which is a protocol suite for Security Architecture for the Internet Protocol communications by authenticating and encrypting each IP packet of a communication session.

(iii) **IKEv2,** which is the protocol used to set up a security association (SA) in the IPSec protocol suite.

(iv) **MIPv6** is the IP mobility implementation for IPv6.

(v) **NEMO:** The growing use of IP devices in portable applications has created the demand for mobility support for entire networks of IP devices. Network Mobility (NEMO) solves this problem by extending Mobile IP.

(vi) DHCPv6 is the Dynamic Host Configuration Protocol for IPv6. DHCPv6 may be a more suitable solution to assign addresses, name servers and other configuration information as is being done today with DHCP for IPv4.

(vii) SIP (Session Initiation Protocol) is an IETF-defined signaling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP).

(viii) Management (SNMP-MIBs) is a Management Information Base, a key component of SNMP (Simple Network Management Protocol). More specifically, an MIB is a group of managed objects within a network.

(ix) MLDv2 Interoperability Tests (RFC 3810, RFC 4604)

(x) MLDv2 Router Conformance (RFC 3810, RFC 4606)

Augmentation of IPv6 Testbed:

The existing IPv6 test bed may be augmented in future to include the following -

Figure 9: NGN Transport Lab

(i) 6LoWPAN testing: 6LoWPAN is an acronym for IPv6 over Low power Wireless Personal Area Networks. The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks. 6LoWPAN provides a means for carrying packet data in the form of IPv6 over IEEE 802.15.4 networks. The 6LoWPAN system is used for a variety of applications including wireless sensor networks.

(ii) IPv6 compliance testing for mobile handsets: Efforts are being made to enhance the capability of the existing test bed, so that testing of IPv6 compliant mobile handsets as per RFC 3314 and 3316 may be performed.

(iii) Cloud testing: Existing test bed may also be augmented to include the capabilities for testing cloud features.

5.1.2 IPv6 Standards

a) Most of the high end networking equipments are currently being imported by the vendors and manufacturers from other countries. Many of these vendors are getting their products certified for IPv6 readiness from the IPv6 ready logo committee, which runs the 'IPv6 Ready Logo Program'. This is a globally recognised program, which is run by the IPv6 Forum for certification of equipments, ISPs and websites for IPv6 readiness. The details of this program are given in Annexure-I.

b) In India, TEC has established an IPv6 Test Bed in NGN lab Phase-I project for testing of IPv6 protocols with the purpose of giving approvals/certificates to equipments being offered for IPv6 readiness testing by different vendors. Since, TEC lab is the first public facility in the country of this kind, it is expected that the lab will get many requests from industry for IPv6 testing. In this regard the offered equipments will be tested for IPv6 readiness based on specifications developed by various International bodies like IPv6 Forum, IETF etc. and TEC. The NGN test lab equipments have been installed and the equipment vendors in industry, primarily dealing with IP-based equipments, have been informed that the NGN lab of TEC can be used for readiness testing of the IPv6 protocols.

c) TEC has also released a document "Standard on IPv6" in March 2011. The purpose of the TEC Standard on IPv6 is to give the details of the IPv6 specifications, especially the details of the different RFCs specified by IETF (feature wise), which have to be complied for meeting the requirement of IPv6 readiness by the equipments. TEC standard on IPv6 is not product specific but covers various specifications relevant for IPv6. Different products have different features so they implement only subsets from the given set of specifications, i.e. they will comply only with specific RFCs depending upon the feature offered. The TEC standard on IPv6 was made by TEC in 2011. Since IPv6 is maturing fast, there is a possibility that for different features new RFCs may be added from time to time and also included by the vendor in its test offering. In that case these additional RFCs for different features shall also be tested for certification. In remaining cases the RFCs mentioned in the TEC standard for different features in the product shall be tested by TEC. A summary list of RFCs is given in Annexure J for reference.

PART C

CHAPTER 6

Institutional Support for IPv6 Adoption

6.1 Centre of Innovation for IPv6

The futuristic role of Internet Protocol version 6 (IPv6) and its applications in different sectors of Indian economy has been recognised in NTP-2012 .Accordingly, a dedicated Centre of Innovation (CoI) was envisaged in NTP-2012 as under:

'To establish a dedicated Centre of Innovation to engage in R & D, specialized training, development of various applications in the field of IPv6. This will also be responsible for support to various policies and standards development processes in close coordination with different international bodies'.

To achieve the above objective, a committee was constituted for firming up the detailed modalities, structure, scope of work and other details etc. for the CoI. The broad objectives of the CoI as outlined by the committee are as under:

- To implement IPv6 based pilot projects which can showcase the technology and in turn more similar projects get implemented across country.
- To develop model Experimental IPv6 Network.
- Technical support (directly & through empanelled agencies) to Central and State Government units and other stakeholders to facilitate smooth implementation in their IPv6 deployment in the country and find solutions to any problems that would be faced from time to time during the process of transition.
- New application developments in the field of IPv6 as well as the porting of existing applications to the new IPv6 specifications.
- Conducting certified training programmes, seminars, workshops, awareness Research and development in collaboration with IITs, IISc, NITs & other R&D organisations for creation of RFC/New applications, IPRs etc.
- Closely work with Indian Telecom Standards & Development Organisation (Indian TSDO) for Standards & Specification development in the field of IPv6.
- To collaborate with all international bodies in this field so that India is able to establish a lead role in IPv6 related international policies and standards.
- Development of core competencies for new emerging technologies in future viz. Cloud services, machine to machine communication, Internet of things.
- Consultancy support at National / International level.
- Auditing of the networks & its certification.
- Promotion of Research & Development (R&D) around IPv6 related technologies.
- Any other work, role and function assigned by Government from time to time.

The CoI is in the process of being set up as per the recommendations of the committee and is expected to start working shortly. Once it is established, it will take over the functions of India IPv6 Task Force as envisaged in 'National IPv6 Deployment Roadmap Version-I' that was released in July 2010.

6.1.2 Functions of CoI

The roles and functions associated with CoI are as follows:

1) Training & Knowledge Resource Development

Training Requirement:

a. In Central Government, there are about 94 departments and ministries. Each department may have 100 different units/branches/subordinate offices etc. Even if, each department/ ministry needs 4 IPv6 trained personnel per unit , the training requirement of Central Government departments would be around 37600.

b. We have 34 States/ Union Territories and each State has about 100 subordinate departments etc. Even if, each department/ministry needs 4 IPv6 trained personnel per unit, the training requirement of State Government departments would be around 13600.

c. We have 250 central PSUs. If on average, each PSU requires 50 IPv6 trained personnel, the training requirement of central PSU would be around 12500.

d. Similarly, it is estimated that State PSU taken together will need around 12500 IPv6 trained engineers/personnel.

e. Even with the most conservative figures, the requirement of IPv6 trained engineers/ personnel in private sector is estimated to be double of the Government requirement, giving us a figure of 152400.

So even with the most conservative figures, the IPv6 training requirement of the country is 228600. In case of Government Organizations, training cost needs to be subsidized from DoT as emerged from various review meetings with Government sectors.

Standardization of IPv6 Courses:

In India, presently no standard IPv6 courses are being offered by any recognized institute. There is a need to define IPv6 training and certification programs at par with the global standards and based on industry best practices. The courses offered will be able to fulfill Government technical requirement in new emerging fields like Machine to Machine Communication, Cloud computing and services. It will also be able to create a job market for IPv6.

The globally recognized IPv6 courses vary in duration from 5 days to 15 days. Considering the figure of 2, 28,600 personnel to be trained and minimum 5 days training requirement, the total man-days of training requirement is 11,43,000. No single institution can undertake this much training requirement. Therefore empanelment of the Institutes for imparting IPv6 training is required.

2) Experimental IPv6 Networks

As the deployment of IPv6 in networks start, different stakeholders will need an IPv6 network for demonstrating and experimenting with different IPv6 transition scenarios. This activity is not possible on an existing ISP network carrying commercial traffic. Therefore, there is a need for building up an experimental IPv6 network containing all the components of IPv6 in the network. On this network, different vendors can test their equipment or applications for IPv6 conformity and inter-operability of the products. The tests can be carried out on payment basis decided by the provider of the experimental IPv6 network. The network will simulate a core network and the access network.

3) Pilot Projects

IPv6 pilot projects are required to build confidence in IPv6 as a technology and demonstrate its capabilities. Pilot projects will show case RoI in IPv6 investment, application of IPv6 in e-governance/ citizen services and strengthen the belief that IPv6 applications can impact/ enhance the lives of our citizens that in turn will create market demand.

Pilot projects like smart building, smart grid, smart cities, Intelligent Traffic management system, Smart health Care systems, Intelligent warfare systems, Intelligent Railway freight management system, Disaster Management etc are to be taken up for showcasing the IPv6 capabilities and elaborating RoI on IPv6.

4) R & D, Application Development & Support:

The main thrust in this activity will be to work on IPR, RFC, to take up security concerns in IPv6 technology, to build up new concepts for IPv6 technology and to showcase the same through Pilot Projects. The research scholars of premier institutes may be funded by CoI to carry out specific jobs against defined deliverables. This way a large pool of IPv6 experts will be created in the country which will be used for developing new RFCs and IPRs. It will also facilitate the transition of existing content and applications and development of new content and applications on IPv6.

5) Consultancy Support to Government Organizations:

CoI would be responsible for development and empanelment of IPv6 consultants in India which may support Government organisations and other private organisations for their IPv6 related implementations and adoption of pilot projects. In the beginning CoI may need to fund the Government Organizations for consultancy services and implementation as emerged during different review meetings with the Government organisations coordinated by NT cell, DoT. CoI would also provide consultancy services in different countries on commercial basis.

6) IPv6 Network Auditing:

Right now there is no organisation responsible for auditing of IPv6 networks. A large number of networks are transiting to IPv6 but their capabilities cannot be ascertained so CoI would be responsible for development of auditing teams in the country so that networks being transited to IPv6 may be properly audited for seamless and smooth working of different applications in the network.

7) International Collaboration Regarding Policies & Standards:

CoI will collaborate with different international organisations like ICANN, IETF, APNIC, IANA, IPv6 Forum, ITU etc. in the matters related to IPv6 activities so as to keep India at par with other countries. CoI will also see to it that sufficient number of IPRs and RFCs are developed in the country. It will also be helpful in the visibility of CoI across globe.

6.2 Indian Registry for Internet Names & Numbers (IRINN)

Govt. of India, Department of Electronics & Information Technology (DeitY) endorsed the operations of National Internet Registry (NIR) to National Internet Exchange of India (NIXI). NIR is an entity under the umbrella of a Regional Internet Registry (RIR) which is Asia Pacific Network Information Centre (APNIC).

NIR is entrusted with the task of coordinating IP Address allocation with other Internet resource management functions at national level in the country. NIXI was recognized by APNIC in March 2012 to become the NIR for the country. The NIR has been named as Indian Registry for Internet Names and Numbers (IRINN). Collective efforts of NIXI and ISPAI have led to the formation of IRINN in the country.

IRINN is a division functioning under NIXI and provides allocation and registration services of Internet Protocol addresses (IPv4 & IPv6) and Autonomous System numbers to its Affiliates to the Internet communities. It is a not-for-profit, Affiliates based entity, with the primary goal of allocation of Internet resources to its Affiliates. It also encourages/promotes activities related to research, education and training covering the areas of Internet Resources.

6.2.1 IRINN Structure

IRINN is a division within the administrative structure under NIXI.

6.2.2 IRINN Policy Features

The IRINN policy is allied with Global and Asia Pacific Network Information Centre (APNIC) policies and following bottom up process for any policy changes. IRINN affiliates have freedom to choose the Registry (IRINN/APNIC). IRINN operates in a way that is consistent with regional and global resource management policies. IRINN will be developing local policies and take public positions in the best interest of its affiliates and take part in regulatory consideration where ever appropriate.

I. How to become IRINN's Affiliate

To become an affiliate, individual/organization must submit their allocation proposal with supporting information and justification.

II. Category of Affiliates:

a) **Affiliates –** Individuals, Corporate Bodies, Academic Institutions, incorporated or established in India, under the Indian laws, as the case may be, shall become a direct Affiliate of IRINN, provided such organizations do not operate any business similar to a LIR.

b) **LIR (ISP) Affiliates -** A Local Internet Registry (LIR) is an IR that primarily assigns address space to the users of the network services that it provides. LIRs are generally ISPs licensed by the Department of Technology (DoT), Government of India and Data Centre Operations whose customers are primarily end users and possibly other ISPs.

III. Services for affiliates

a) Web based portal

IRINN provides a web based portal where affiliates can manage their information such as, Billing details, Administrative details, Login details, Add/Manage/Delete Affiliates contacts, Resource Request, View/Manage Resources, Second Opinion Request, Raise Request, Request History, Whois/rDNS management, Transfer Resources, De-Allocate resource, Online Payment, Payment History and submit Affiliates feedback etc. IRINN offers real time online chat support for its services.

b) Training and education

IRINN would be organizing training on Internet resources from time to time. Affiliates are encouraged to attend IRINN training either online or in person. IRINN's Training Program and other educational initiatives respond to the needs of Affiliates and other stakeholders. Affiliates can learn about the structure, operational, and technical features of IPv6, including planning, building, and configuring an IPv6 network.

PART D

CHAPTER 7

The Road Ahead

7.1 Case Studies

7.1.1 BHEL

Introduction

BHEL is an integrated power plant equipment manufacturer and one of the largest engineering and manufacturing companies in India. It is one of India's nine largest Public Sector Undertakings or PSUs, known as the 'Navratnas' or 'the nine jewels'.

Roadmap of IPv6 Implementation in BHEL :

Implementation of IPv6 in BHEL was necessitated as per letter from Ministry of Communications & IT through DHI to CMD, BHEL received in June 2011. The first IPv6 awareness was created during ISSO meet in July 2011 and action plan shared with all locations. It was emphasized that all Internet Lease Line locations must coordinate with their ISPs, audit their hardwares, softwares and applications for IPv6 readiness and all Internet facing publicly accessed websites must be made IPv6 enabled. IPv6 was to run alongside IPv4 for compatibility with all IPv4 and IPv6 end users.

Listed out are the activities which were followed as per work-schedule received from ministry:

Sr. No.	Activity	Proposed Target Date	Method / Date of Milestone Achievement
1.	Appointment of Nodal Officer	31.8.2010	15/06/2011
2.	Circulation of letters, guidelines, checklist etc. to all organizations under the Ministry/Departments and orders on appointment of organizational nodal officers	15.9.2010	Done
3.	Appointment of Organizational Nodal Officers	30.9.2010	Done
4.	Form a "Ministry Transition Team" consisting of concerned officers & experts from stakeholders like service provider, vendors, software developers etc.) for giving technical advice and look into issues concerned with transition to IPv6	31.10.2010	DoT plan was adhered to.
5.	Call a meeting of all organizations under the ministry and discuss the following issues –		
	a) Instructions issued by DoT		
	b) Checklists issued by TEC		
	c) Annexure 'A' & 'B' of Roadmap		
	d) Preparation of equipment reports	30.11.2010	Done
6.	Reports preparations based on activities in Sr. No. 5	31.12.2010	18/11/2011
7.	Audit of Equipment Reports by other Agency	15.01.2011	Not Required
8.	Based on the Equipment Audit Reports, prepare an Equipment replacement plan to phase out non-compliant hardware and software. Assistance may be taken from " Transition Team"	15.02.2011	22/8/2011

9.	Based on the replacement plan, prepare a procurement plan for ministry / department	15.03.2011	25/8/2011. Done for orders through RC.
10.	Identify persons for IPv6 training and send them on training (Parallel Activity)	A continuous process	25/7/2011 .Done by all locations.
11.	Float tenders for procurement of hardware and software as per the plans	15.04.2011	RC finalized at Bhopal.
12.	IPv6 Address Allocation Policy	30.06.2011	Achieved starting Nov 2011 to early March 2012 at different locations.
13.	Set up a pilot test network either centrally or in one of the organization for testing and training	31.07.2011	Cisco router added to network. IPv6 setup done on servers. Pilot made available to all BHEL locations for support.
14.	Equipment Procurement and deployment in the network	31.10.2011	As per RC, orders placed
15.	Testing of hardware and software and transition of applications	28.02.2012	17/2/2012. Achieved by implementing Reverse Proxy and making Servers IPv6/ IPv4 dual stack
16.	Launch of IPv6 Services	31.03.2012	10/3/2012. Achieved starting Dec, 2011 at BHEL Asiad to Mid March, 2012 at all locations
17	Compliance Checklist circulated to all BHEL locations		Compliance achieved at 18 out of 20 locations by 28/3/2012, one location not hosting any public application; other at Nagpur the ISP was not IPv6 compliant.

Challenges Faced by Units for IPv6 compliance :

- Lack of knowledge for transition to IPv6.
- Checking compliance of hardware, software and applications.
- Coordinating with ISPs who themselves were in a nascent stage of IPv6 implementation.

IPv6 was covered during the ISSO meet at Company level and ensuing Action Plan for implementation of IPv6 was shared. Presentation from Cisco on IPv6 was organized for firsthand knowledge. Details on IPv6 through TEC website at www.tec.gov.in were also shared. The site provides all the technical details on IPv6, updated communications from Government on the subject, steps for audit of available infrastructure for compatibility with IPv6 etc. A two days hands on program was organized at Delhi for all locations for technical inputs on IPv6. Meanwhile at CIT Asiad IPv6 pilot was setup. This required IPv6 enabled router, firewall and switches apart from IPv6 dual stack through

ISP which took a long time to materialize. Initially lots of glitches were faced including many problems at ISP end itself and it required a lot of effort to prove to ISP where the problem was.

A 2 days training program scheduled in mid December on IPv6 basics was planned for technical staff of BHEL who were responsible for various activities required to be undertaken for deployment of IPv6 in the organisation. The participants learnt about the Govt. policies regarding IPv6 implementation, had detailed discussions on IPv6 addressing scheme along with tutorials. Demonstrations were given on how nodes are auto configured.

Since IPv6 provides a large address block for an organisation, therefore, its planning becomes very important. Address planning was discussed in detail and the participants were encouraged to plan and discuss in groups and present their understanding to the group. To have better understanding of the protocol, header comparison of IPv4 and IPv6 was shown to the participants. This was shared during the training session live and it gave confidence that it can be done. For the applications part which were not IPv6 compliant, it was decided that reverse proxy would be used. CIT Noida established the same and shared the findings with all locations. www.bhel.com became the first IPv6 enabled public site in BHEL and all other applications accessible through Noida were IPv6.

Meanwhile all the locations kept doing their work for IPv6. The main problem faced was that ISP was not responding for IPv6 and gradually with persistent pressure exerted by locations this could be sorted out. IPv6 status was regularly shared with CMD during communication meetings.

Current Status of IPv6 in BHEL

Currently all locations with Internet leased lines have made their Internet IPv6 enabled. All public facing websites are on IPv6. All major ISPs in BHEL have provided IPv6 with exception of STPI. For future readiness internal IPv6 addresses have been allocated and BHEL is ready for any active IPv6 implementation in future.

7.1.2 Smart Grid

Introduction to Smart Grid:

A Smart Grid is an electricity grid that monitors and controls suppliers and consumers of electricity, based on their behavior patterns. It uses information and communication technologies (ICT) to achieve this objective and operates in an automated way. A Smart Grid plays a significant role in enabling improved reliability and sustainability of the production and distribution of electricity, thus facilitating clean and renewable energy technologies, energy efficiency, electric vehicles and economic benefits.

Need for IPv6 in Smart Grids:

Utilities have millions of consumers and hence millions of meters to record the electricity usage of each consumer. IPv6, with its ‘limitless’ address space, provides IP addresses to each and every energy meter and thus assists in making every meter reachable, accessible and controllable from a remote central location. The second aspect is security. Since security is an integral part of IPv6, enhanced protection can be implemented in an end-to-end network. Besides, IPv6 is lightweight and can be used in devices with constraints, i.e. those with limited energy, memory and processing power.

Keeping this view in mind, Tech Mahindra and Mahindra Satyam, with the support of the Department of Telecom (Government of India), are implementing an IPv6-enabled Smart Grid as part of a Proof-on Concept (PoC) to demonstrate how new applications such as this are efficiently supported by IPv6. The PoC is being implemented at the 120 acre campus in the Mahindra Satyam Technology Center, Hyderabad, India.

The Proof-of-Concept (PoC):

The PoC is planned to be implemented in 2 phases:

- Phase-1: Smart Grid with Cellular connectivity (2-tier system)
- Phase-2: Smart Grid with 6lowPAN connectivity (3-tier system)

Phase-1:

In this phase, the solution will adopt a long-range communication technology such as GPRS/3G. The IPv6 smart metering solution will consist of a data transceiver, which is a communication module connected to the energy meter. This module will communicate with the Meter Management System (MMS) through the IPv6 protocol over GPRS/3G. The solution has been depicted in Figure-9.

This solution will enable monitoring and controlling the energy meters as per use cases discussed below, e.g. the MMS will interact at periodic user-defined intervals with the energy meter, and store energy consumption related and other meter related data, in the database. This data could then be used by business functions for appropriate decision making.

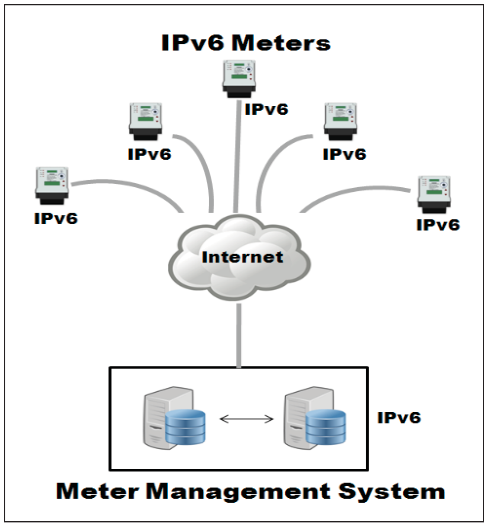


Figure- 10: IPv6 Smart Grid with Cellular Connectivity

Phase-2:

In this phase, the solution will be a combination of a long-range technology such as GPRS/3G and a short-range communication technology such as 6lowPAN. The solution will consist of 3 components, viz. meter with data transceiver, a data concentrator (DC) or a coordinator, and the meter management system (MMS). In this phase, the DC will act as a coordinating entity and will facilitate 2-way communication between the data transceiver/meter and the MMS. The data transceiver in this case will support RF-mesh based 6lowPAN communication technology. Thus, the DC will handle both short-range and long-range communication. Additionally, the DC will be responsible for maintaining a group of meters, as well as their data periodically. The solution has been depicted in Figure-10.

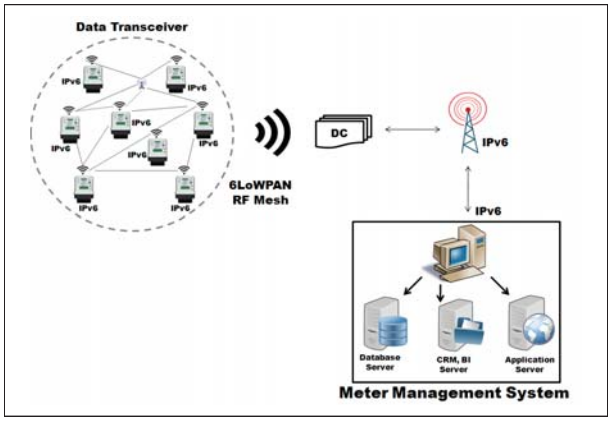


Figure- 11: IPv6 Smart Grid with 6lowPAN

This solution will again support the use cases mentioned below. For e.g. the energy meters will provide data via the transceivers to the DC, using 6lowPAN. The DC will store the data for a certain period and then transfer it to MMS via IPv6-enabled GPRS/3G. The MMS would eventually store the data in the database, to be used further for analytical purposes.

Use Cases of the IPv6 Smart Grid:

Some of the use cases that would be realized in the IPv6 Smart Grid, include

a) Collect meter data :

The Advanced Metering Infrastructure (AMI) would help the utility company to collect information from the customer's residential meter. The data could typically be - accumulated energy, demand and time-of-use information.

b) Tamper detection :

The AMI would help detect theft of services, which is one of the major threats to utilities. The utility company detects tamper/theft through communication with the meter. Tamper methods include, for example, comparison of the load profile data against historical records, or a spontaneous report of a tamper switch being triggered at the customer site.

c) Remote Connect/Disconnect :

The AMI metering would provide capabilities to improve the efficiency of the service initiation/ termination processes through remote turn on/off functions. It would also provide a capability to remotely limit usage/load, particularly as a mitigating response to constrained supply and credit & collections issues.

d) Participate in Demand-Response (DR) Programmes :

The AMI supports customer awareness of their instantaneous usage (kWH) and electricity pricing, and this in turn can help the utilities in their load reduction needs. As there is an increased electricity demand on the grid, it may result in energy shortages, therefore triggering the need for utilities to reduce energy consumption in support of the grid's stability. The AMI will facilitate load reduction at the customer's site by communicating instantaneous kWH pricing and voluntary load reduction program events to the customer.

e) Last Gasp Event :

The AMI will read the meter continuously and provide the utility's outage management system, the information to create an outage automatically when detected.

7.1.3 Flipkart

Introduction

The website www.flipkart.com is an e-commerce website, with the Internet as its only sales channel. Flipkart enabled its website to be accessible over IPv6 in time for the World IPv6 Launch on June 6th, 2012 through dedicated efforts of four engineers over a time frame of two weeks.

Business Case

With IPv6's adoption increasing across the world, and with the Indian Government's efforts towards IPv6, Flipkart's leadership recognized that customers would soon be accessing its website over IPv6 networks.

Smoother transition was another reason why Flipkart invested in IPv6 transition in early stages. IPv6 does require its own learning curve, and it would be much easier to go through that learning curve when the technology adoption on the customer side was at its infancy, than when more than 20% of its traffic shifted on to IPv6. Thus, a large reason to do the IPv6 transition early was to minimize transition risks.

A few protocol benefits of IPv6, such as better utilization of network for heavy multimedia usage, was another reason for the transition. Lastly, it was as much a matter of being ahead on the technology curve, shoulder to shoulder with technology companies across the world, which led to the decision.

Planning and Execution

The team :

A team of four engineers (1 Network engineer, 1 Production engineer, and 2 application engineers) was created in early May, 2012, towards planning and execution of the IPv6 transition.

Phase identification :

The goal of the team was identified as IPv6 enablement of www.flipkart.com, while allowing unhindered experience to existing IPv4 customers. No specific time frame was identified for any of the above. However, the team was informed that it would be a good achievement to have the website completely enabled in time for the World IPv6 Launch on June 6th, 2012.

The team identified the following:

1. Scope of the effort would be towards only the public infrastructure of www.flipkart.com. The internal networks would continue to be on IPv4. The reasoning was that it was more important to enable IPv6 customers to access www.flipkart.com first.

2. The website would be first made available over www.ipv6.flipkart.com to allow for any issues to be identified

3. Assuming no issues identified, www.flipkart.com would be made to have a AAAA entry, thus enabling it over IPv6 completely by June 6th, 2012.

Execution :

Execution wise, the following was done:

1. For training, publicly available resources on the Internet were used

2. All application related changes were identified upfront – log processing, fraud detection, client IP address storage

3. Flipkart's content delivery network was included in the change list
4. All Network components were validated as IPv6 compliant. Flipkart did not have to invest in any additional network cost
5. A separate network path for IPv6 was created to minimize impact in case something went wrong
6. Due diligence was done on Security best practices for IPv6
7. Much tighter firewall rules were applied for the IPv6 network

Testing :

Publicly available Teredo networks from Hurricane Electric were used for IPv6 testing, as IPv6 network was not easily available at that point in time.

Conclusion and Key Insights :

Flipkart was able to enable IPv6 access through www.ipv6.flipkart.com within 2 weeks of dedicated efforts of the 4 man engineering team. No specific changes were done post that, allowing it to enable IPv6 for www.flipkart.com two days prior to World IPv6 Launch Day.

A key insight post this activity was that for most websites, enabling IPv6 would be a zero cost and extremely easy activity. For any website which is using a CDN, it would just be a matter of asking the CDN to enable IPv6. Websites which log IP addresses, or do any IP address processing will have to make a few minor changes to adapt to the IPv6 addresses.

Another key learning was that e-commerce cannot be IPv6 compliant completely, without the payment gateways being IPv6 ready as well.

Lastly, security practices in IPv6 are a little different from IPv4 networks and thus should be given due attention very early; e.g. in IPv4 network, NAT-ting is often used as a substitute for firewalling as well – but this mechanism doesn't hold true for IPv6.Therefore, explicit firewall rules are needed to block generic incoming packets.

7.1.4 Tulip Telecom Limited

Introduction

Tulip Telecom Limited is one of India's leading MPLS VPN players and deals in provision and management of multi location wide area networks (WAN) for various industry verticals. Its IP/MPLS network is a carrier grade converged core infrastructure. It is amongst the first ISPs to be IPv6 certified ISP via IPv6 World Forum.

Situation

Digital revolution in the last 2 decades has given an exponential growth to the requirement of IPv4, the de facto addressing standard and thereby moving it to the brink of exhaustion. With 2 RIRs executing the phase 3 policy of IP address allocation and particularly in the Indian subcontinent context, allocations have stopped/limited whereas the consumption per user is increasing manifold which Tulip saw as deterrent to business in times to come. As a Service Provider, Tulip clearly understood that working on IPv6 was where the future business was going to be and as a technology company we thought of taking the first mover advantage.

Project V6

Making the idea work, Tulip followed the 5 step project approach:

- A governance team was set up which overlooked the entire Project and will continue to look at the evolution happening in the IPv6 arena.
- Assessment of the Infrastructure and its impact analysis was studied
- All Transition technologies were studied with the likes of NAT444, NAT64, CGN, 6PE, 6vPE, DS-Lite, etc.
- The solution identified for the rollout came to be 6vPE.

6VPE saves service providers from enabling a separate signaling plane, and it takes advantage of operational IPv4 MPLS backbones. Thus there is no need for dual-stacking within the MPLS core. 6VPE is more like a regular IPv4 MPLS-VPN provider edge, with an addition of IPv6 support within Virtual Routing and Forwarding (VRF). It provides logically separate routing table entries for VPN member devices. In nutshell, IPv6 services can coexist with IPv4 using existing infrastructure without any major changes.

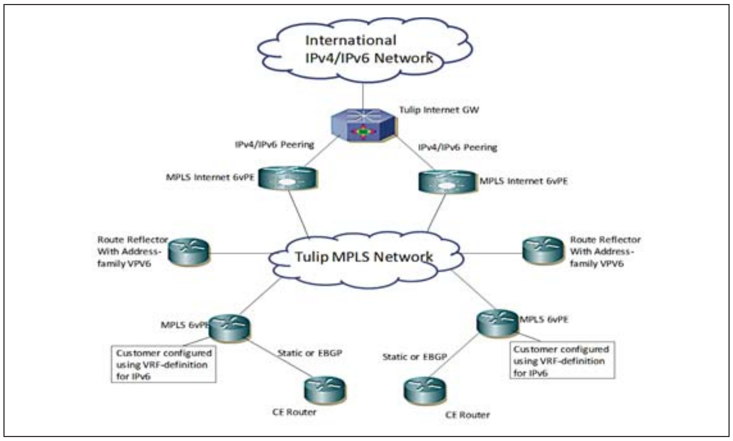
- Creating a test bed and testing the solution before go live.

Requirements for 6vPE Technique

1. The Internet Gateway router should be Dual Stack to have the IPv6 Network information.
2. The existing PE routers should be able to support Dual Stack for MPLS-VPN with features like VRF supporting IPv6, BGP supporting VPNv6 etc.
3. The existing Route Reflectors should be 6vPE capable or new Route Reflectors need to be deployed, which depends on the scale of IPv6 VPN customers.

Network Architecture for 6vPE :

The below Network Architecture depicts the 6vPE solution deployed:



Major components of the 6vPE solution:

1. **Internet Gateway-** The internet GW router peers with the Upstream Service Provider (USP) with both IPv4 and IPv6 to have reachability to both IPv4 and IPv6 Networks across the World.
2. **DNS –** For all internet customers, DNS is an important component and for V6 DNSSec has to be enabled.
3. **Route Reflector -** It is the job of Route Reflector to reflect the routes of VRFs to all the PE routers in the MPLS network. In this case of 6vPE deployment, the Route Reflectors should have capabilities to reflect the IPv6 VPN routes as well by the option of Address-family VPNv6 under the MP-BGP. For Redundancy purposes, 2 Route Reflectors are deployed in the MPLS network. All the 6vPE routers peer with these RRs to exchange the IPv6 routing information. There are separate route-reflectors for v6 and v4 in TULIP setup.
4. **MPLS 6vPE –** This is the router where customers are configured in the MPLS Network. The same Router offering MPLS services in IPv4 can be used for creating vrf for IPv6 services as well.

Benefits of the Solution :

The main benefits availed by using the 6vPE are mentioned below:

1. The Core Network remains transparent and agnostic to the v6 enablement.
2. Simplified and faster rollout as IPv6 protocol suite is selectively required to be enabled only on PE routers rendering IPv6 services and not on the entire network.
3. Operational expenditures are also limited because of the use of existing resources.

Current Status :

Tulip is at present offering numerous hosted services like Cloud Services, Unified Communication, and Video Conferencing on IPv6 and have roadmap to offer all hosted services on IPv6 enabled platform.

7.2 Monitoring Mechanisms

While the need and the benefits of IPv6 are well understood it is equally important to understand that Internet users having experience of IPv4 expect a similar or improved performance on IPv6. IPv6 deployments today are sought with apprehensions on performance degradation in the event of incorrect or partial deployments. The complexity increases further during the transition period when both IPv4 and IPv6 co-exist. With IPv6 transition having an impact on an organization's network, application and services it becomes critical to monitor and check IPv6 performance to provide an enhanced user experience.

It is intended to define checks, processes, parameters and indicators with a view to monitor the impact of IPv6 across an organization's networks, applications and services. Additionally it is also intended to define a reporting mechanism to provide detailed updated statistical information on the progress of IPv6 adoption and deployment status across the organizations which would further be collated to provide for a country level deployment status for monitoring IPv6 adoption progress.

Monitoring Challenges :

IPv6 with its vast scale poses challenges on monitoring since a single IPv6 subnet is as large as the entire Internet today. Monitoring solutions that worked for IPv4, will not work with IPv6. Apart from the scale, IPv6 deployments also pose challenge on performance and security

Performance Concerns :

- As with IPv4, IPv6 quality of service is implemented at Layer 2 and Layer 3 of the TCP/IP stack. A number of network management vendors support IPv6, but while passive network management tools may comply with the new version, some may not include the evolving set of features for IPv6 support.
- Standalone, passive monitoring may be unable to properly detect performance issues experienced by the end user since for web enabled businesses, the end user experience is the most critical element of service quality.
- Because there is a gap between IPv6 capabilities and current network management tools, active monitoring is essential.
- As with any new technology, there is a potential for flaws, which may impact uptime and performance.
- IPv6 will lead to larger networks that directly address more network devices, increasing the overall complexity.
- IPv6 end-to-end security features, while improving security, will make it harder to analyze network traffic.
- For businesses and organizations deploying IPv6 websites, performance management and service-level agreement monitoring become more complicated due to the coexistence of IPv4 and IPv6 and the exponential size of IPv6 addressing and routing.

Security Concerns :

IPv4 security issues are widely known and understood. Over the years, security vulnerabilities such as Denial of Service attacks (DOS), malicious code distribution (viruses and worms), port scanning, and fragmentation attacks have become prominent security concerns. For example, port scanning attacks are made common due to the inherent small address space in an IPv4 scheme. Scanning a whole class C network can take less than ten minutes.

IPv6 security issues are not yet fully understood. In the early stages of IPv6 deployment, there will be many issues around dual-IP stacks. Weaknesses in how these networks may interoperate will cause security issues. IP spoofing continues to be a possible security concern with IPv6 networks. While not impossible, IP flooding, or scanning for valid host addresses and services are going to be much more difficult with IPv6 than with IPv4. The concept of mobility is a feature of IPv6 networks that was not available with IPv4. This is a very complex function that must be considered when evaluating IPv6 security.

Performance monitoring of IPv6 websites and networks is critical. It will be some time before all the possible weaknesses are fully exposed. In the interim, performance monitoring will prove to be extremely effective at limiting any security threats to the IPv6 website.

Reporting Challenges :

While it is critical to monitor it is equally important to have a reporting mechanism in place .The biggest challenge on reporting is lack of understanding combined with lack of clearly defined monitoring and reporting processes in place today. Non availability of defined indicators and parameters pose further challenge with reporting. Clearly defined reporting mechanism will help effective monitoring of IPv6 adoption progress at an organization and further at the country level.

IPv6 Monitoring and Reporting:

IPv6 monitoring and reporting can be done across the following:

a. Network

b. Application

c. Services

d. Security

The following quantitative and qualitative indicators parameters are proposed for monitoring and reporting:

	Quantitative	**Qualitative**
Networks	• Type of Networks • No. of Network Elements - only IPv4, only IPv6, both IPv4 and IPv6 • No. of IPv6 Address blocks allocated and in use • Details of tunnelling or NAT solution if deployed	• Throughput • Latency • Reachability
Applications	• Type of Applications • No. of Applications • No. of Applications only IPv4, only IPv6, both IPv4 and IPv6	• Throughput • Latency • Reachability
Services	• Type of Services • No. of Services • No. of Services only IPv4, only IPv6, both IPv4 and IPv6	• Throughput • Latency • Reachability • Service Response time
Security	• No. of network and applications secured • No. of security threats detected • No of security threats mitigated	• Throughput • Latency • Reachability of Firewalls and IDS systems

Report Profiles :

The report profiles and periodicity are suggested to be built as per the table below:

	Report Profiles	Periodicity
Networks	• Network Audit Report • Inventory Report • Utilization Report • Traffic Report • Health Report	• Quarterly
Applications	• Application Audit Report • Inventory Report • Utilization Report • Traffic Report • Health Report	• Quarterly
Services	• Service Audit Report • Service Utilization Report • SLA report	• Quarterly
Security	• Security Audit report • Security threat report • Threat mitigation report	• Quarterly

It is proposed to setup an IPv6 Monitoring and Reporting Committee for defining IPv6 monitoring parameters, creation of IPv6 reporting profiles, defining IPv6 monitoring and reporting framework and finally the process to be followed. The committee will ensure that the monitoring mechanism is inclusive of latest standards and the information is collected in a comprehensible and easy manner. The required framework will be separately finalised by DoT after consultation with all stakeholders.

Monitoring and Reporting Process :

A standard process of monitoring and reporting will be put in place as shown in figure below:

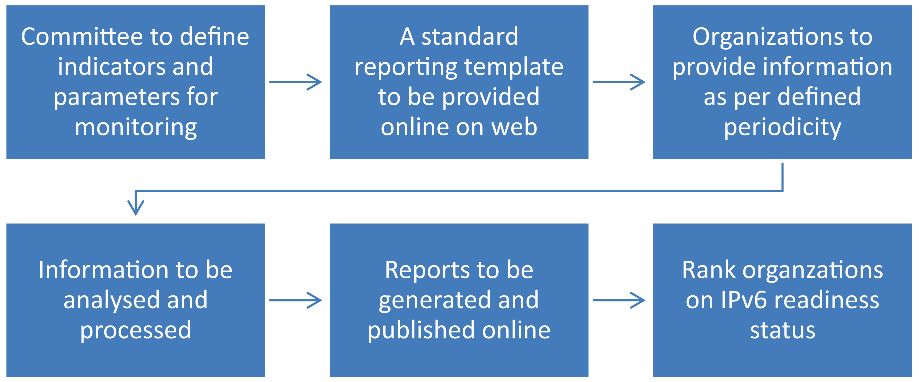

Committee to define indicators and parameters for monitoring
A standard reporting template to be provided online on web
Organizations to provide information as per defined periodicity
Information to be analysed and processed
Reports to be generated and published online
Rank organzations on IPv6 readiness status

Figure 12: Process of Monitoring & Reporting

It is proposed to setup an automated online mechanism as per the framework defined by the IPv6 Monitoring and Reporting Committee. The organizations will be required to deploy these mechanisms in place for timely reporting. Once deployed the mechanisms can be activated and organizations can follow the same to submit information as per the periodicity defined by the committee.

Upon generation of the reports, the same will be published in the public domain online. A rating and certification mechanism will be defined to rank the organizations in the order of their IPv6 readiness and user experience.

Summary

Defining a robust and scalable monitoring and reporting framework is critical to provide an enhanced user experience and visibility into the IPv6 adoption across different stakeholders. Network and website managers must have a true view into end-user connectivity and the ability to receive instant notification whenever a problem occurs. End-to-end IPv6 performance monitoring is crucial to maximize the return on investment of the deployment and to understand its effects on the IT operations and the business.

7.3 Training Facilities

It is proposed to build IPv6 talent pool in the country through training. The development of standardized and certified IPv6 training courses is required for this purpose.

7.3.1 Background

The National Telecom Policy NTP-2012 recognizes the importance of training to develop a skilled pool of IPv6 trained manpower. Trained manpower on IPv6 is required so that the adoption of IPv6 is carefully planned to minimize the technical and performance impact on the networks and to ensure that the transition happens in a seamless manner. Since free IPv4 addresses have already depleted in APNIC, moving to IPv6 is business critical for all organizations in the public and private sector.

As per the National IPv6 Deployment Roadmap, DoT has already directed different stakeholders like Central and State Government Departments, Service providers and other organisations to build IPv6 services capability and start offering IPv6 services by March 2012. However, with limited trained manpower resource availability in the country organisations are faced with the challenge of talent scarcity for implementing IPv6.This in turn is not only contributing to the delay in their adoption plans but is also a serious roadblock towards planning a seamless transition strategy for all stakeholders. The adequate availability of trained manpower resources is the first step towards preparing for the same. Therefore, it is advisable for all stakeholders to build IPv6 trained human resources within their organisations through periodic trainings.

Currently there is no structured or standardised training being offered in the country. A very small percentage of IPv6 talent pool comprises of self-trained personnel with basic theoretical understanding on IPv6. No expert level training with practical hands on experience is available in the country today. It is with this intent that DoT proposes to facilitate building up a talent pool on IPv6 in the country by standardizing the IPv6 training courses, which can be offered by different organizations.

7.3.2 Benefits of Standardized Courses

The following benefits are perceived from standardizing the IPv6 course content for industry & Government Organisations -

(i) Standard and quality courses on IPv6 based on industry and academia input.

(ii) Standard Certification recognised by industry.

(iii) Control training and certification cost benefitting both individual and industry.

(iv) Skilled talent pool made available to the industry.

(v) Job creation for the professionals.

(vi) Create an environment for research and innovations on IPv6.

(vii) Create an environment for contributions to standards on IPv6.

(viii) Create an environment for IPv6 thought leadership in the country.

(ix) Opportunity to make an impact on the international forums and make positive contributions through available IPv6 expertise.

(x) Create an opportunity for India to achieve the highest percentage of IPv6 literacy which would have positive impact on economy in future.

7.3.3 Proposal for Standardizing the IPv6 Training Courses

To address the above mentioned issues, it is proposed to build a standardised IPv6 training course certified by DoT, which can be imparted by different organizations & individuals. The training conducted according to these courses will grade the individuals into different categories which will enable organisations to select the right skill sets for their various needs. The training and certification will create 3 levels of skilled manpower:

1. Basic level
2. Professional Level
3. Expert Level

(i) **Basic Level -** This level will offer basic understanding on IPv6. Undergoing this training will ensure individuals capability to understand the fundamentals of IPv6. This is an IPv6 understanding course recommended to be attended by all technical and business personnel of an organisation.

(ii) **Professional Level -** This level will offer advanced level understanding on IPv6 transition strategies and address planning. This level will ensure individuals capability to configure and manage IPv6 networks. This course is recommended to be attended by level-1 & level-2 planning, operations and support staff of an organisation.

(iii) **Expert Level -** This level will offer detailed understanding on IPv6 network architectures and technologies like IPv6 routing protocol, 6rd,DSLite,CGN, Mobility, security and troubleshooting. This level will ensure an individual's capability to design, implement, manage and troubleshoot large and complex IPv6 networks. This course is recommended to be attended by core planning and level-3 operations and support staff of an organisation.

Accordingly Expression of Interest (EoI) will be separately floated for empanelment of the certified training organisations by DoT/ certified training agency in the country.

PART D

CHAPTER 8

Summary of Recommendations/ Actionable Points

8 Summary of Recommendations / Actionable Points

1) Government Organisations :

- The Government organisations should prepare a detailed transition plan for complete transition to IPv6 (dual stack) by December 2017 based on the network complexity & equipment/ technological life cycles. The plan should be prepared latest by December 2013 and accordingly the required budgetary provisions should be made in their demand for grant. For this purpose, it is recommended that a dedicated transition unit in each organisation should be formed immediately to facilitate entire transition.
- All new IP based services (like cloud computing, data centres etc.) to be provisioned for / by the Government organisations should be on dual stack supporting IPv6 traffic with immediate effect.
- The public interface of all Government projects for delivery of citizen centric services should be dual stack supporting IPv6 traffic latest by 01-01-2015. The readiness of Government projects in turn will act as a catalyst for private sector transition from IPv4 to IPv6.
- The Government organisations should procure equipments which are also IPv6 Ready (Dual Stack) and go for deployment of IPv6 ready (Dual Stack) networks with end to end IPv6 supported applications. The equipment should be either TEC certified or IPv6 Ready Logo certified.
- The Government organisations should go for IPv6 based innovative applications in their respective areas like smart metering, smart grid, smart building, smart city etc.
- The Government organisations should develop adequate skilled IPv6 trained human resources within the organisation through periodic trainings over a period of one to three years to have a seamless transition with minimum disruption.
- The IPv6 should be included in the curriculum of technical courses being offered by various institutes / colleges across the country.

2) Service Providers:

Enterprise Customers

- All new enterprise customer connections (both wireless and wireline) provided by Service Providers on or after 01-01-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.
- Regarding the existing enterprise customers which are not IPv6 ready, the Service Providers shall educate and encourage their customers to switch over to IPv6.

Retail Customers (Wireline)

- All new retail wireline customer connections provided by Service Providers on or after 30-06-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.
- The Service Providers shall endeavor to progressively replace/ upgrade the Service Providers owned CPEs which are not IPv6 ready as per the following timelines:

- Replacement / upgradation of 25% of CPEs by December 2014.
- Replacement / upgradation of 50% of CPEs by December 2015.
- Replacement / upgradation of 75% of CPEs by December 2016.
- Replacement / upgradation of 100% of CPEs by December 2017.

- Regarding the customer owned CPEs which are not IPv6 ready, the Service Providers shall educate and encourage their customers to replace/ upgrade such CPEs to IPv6 ready ones.

Retail Customers (Wireless)

- All new LTE customer connections provided by Service Providers with effect from 30-06-2013 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.
- All new GSM/ CDMA customer connections provided by Service Providers on or after 30-06-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.

3) Content & Application Providers:

- All contents (e.g. websites) and applications providers should target to adopt IPv6 (dual stack) for new contents & applications by 30-06-2014 and for existing ones latest by 01-01-2015.
- The complete financial ecosystem including payment gateways, financial institutions, banks, insurance companies, etc. should transit to IPv6 (dual stack) latest by 30-06-2013.
- The new registrations on '.in' domain to be compulsorily on dual stack with effect from 01st January 2014.The entire '.in' domain should migrate to IPv6 (dual stack) latest by June 2014.

4) Equipment Manufacturers:

- All mobile phone handsets/ data card dongles/ tablets and similar devices used for internet access supporting GSM / CDMA version 2.5G and above sold in India on or after 30-06-2014 shall be capable of carrying IPv6 traffic either on dual stack (IPv4v6) or on native IPv6.
- All wireline broadband CPEs sold in India on or after 01-01-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.

5) Cloud Computing / Data Centres:

- All public cloud computing service / data centres providers should target to adopt IPv6 (dual stack) latest by 30-06-2014.

CHAPTER 9

Annexures

Annexure A

IPv6 Implementation Activity Sheet

Name :

Department:

Sr. No.	Activity	Proposed Target Date	Status
1.	Appointment of Nodal Officer	31.8.2010	
2.	Circulation of letters, guidelines, checklist etc. to all organizations under the Minisrtry/Departments and orders on appointment of organizational nodal officers	15.9.2010	
3.	Appointment of Organizational Nodal Officers	30.9.2010	
4.	Form a “Ministry Transition Team” consisting of concerned officers & experts from stakeholders like service provider, vendors, software developers etc.) for giving technical advice and look into issues concerned with transition to IPv6	31.10.2010	
5.	Call a meeting of all organizations under the ministry and discuss the following issues – a) Instructions issued by DoT b) Checklists issued by TEC c) Annexure ‘A’ & ‘B’ of Roadmap d) Preparation of equipment reports	30.11.2010	
6.	Reports preparations based on activities in Sr. No. 5	31.12.2010	
7.	Audit of Equipment Reports by other Agency	15.01.2011	
8.	Based on the Equipment Audit Reports, prepare an Equipment replacement plan to phase out non-compliant hardware and software. Assistance may be taken from “ Transition Team”	15.02.2011	
9.	Based on the replacement plan, prepare a procurement plan for ministry / department	15.03.2011	
10.	Identify persons for IPv6 training and send them on training (Parallel Activity)	A continuous process	
11.	Float tenders for procurement of hardware and software as per the plans	15.04.2011	
12.	IPv6 Address Allocation Policy	30.06.2011	
13.	Set up a pilot test network either centrally or in one of the organization for testing and training	31.07.2011	
14.	Equipment Procurement and deployment in the network	31.10.2011	
15.	Testing of hardware and software and transition of applications	28.02.2012	
16.	Launch of IPv6 Services	31.03.2012	

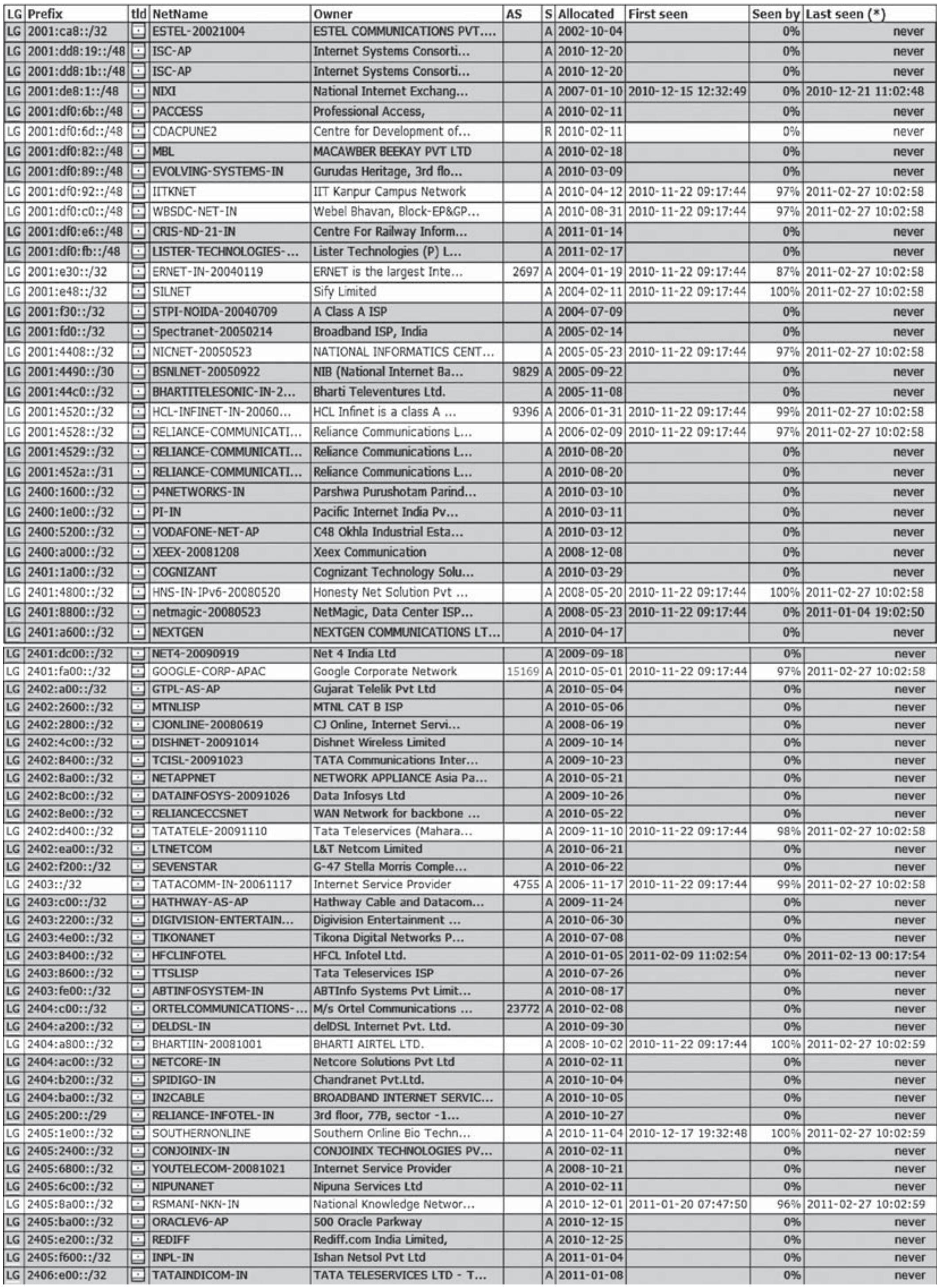
Annexure B

Details of Awareness Workshops

Sl. No.	Place	Date
1.	Lucknow	08.03.2011
2	Puducherry	19.05.2011
3	Bangalore	01.06.2011
4	Raipur	10. 06. 2011
5	Bhopal	23.06.2011
6	Kolkata	05.08.2011
7	Chennai	12.08.2011
8	Guwahati	27-09-2011
9	Chandigarh	21-10-2011
10	Gangtok	25/11/2011
11	Trivananthapuram	23/12/2011
12	Imphal	27/12/2011
13	Daman	16/01/2012
14	Ranchi	24/01/2012
15	Hyderabad	17/02/2012
16	Patna	17/02/2012
17	Itanagar	24/02/2012
18	Mumbai	05/03/2012
19	Jaipur	13/03/2012
20	Bhubneshawar	21/03/2012
21	Delhi	23/03/2012
22	Shillong	10/04/2012
23	Agartala	17/04/2012
24	Port Blair	18/10/2012

Annexure C

Status of IPv6 Prefixes in India



LG	Prefix	tld	NetName	Owner	AS	S	Allocated	First seen	Seen by	Last seen (*)
LG	2001:ca8::/32	▣	ESTEL-20021004	ESTEL COMMUNICATIONS PVT....		A	2002-10-04		0%	never
LG	2001:dd8:19::/48	▣	ISC-AP	Internet Systems Consorti...		A	2010-12-20		0%	never
LG	2001:dd8:1b::/48	▣	ISC-AP	Internet Systems Consorti...		A	2010-12-20		0%	never
LG	2001:de8:1::/48	▣	NIXI	National Internet Exchang...		A	2007-01-10	2010-12-15 12:32:49	0%	2010-12-21 11:02:48
LG	2001:df0:6b::/48	▣	PACCESS	Professional Access,		A	2010-02-11		0%	never
LG	2001:df0:6d::/48	▣	CDACPUNE2	Centre for Development of...		R	2010-02-11		0%	never
LG	2001:df0:82::/48	▣	MBL	MACAWBER BEEKAY PVT LTD		A	2010-02-18		0%	never
LG	2001:df0:89::/48	▣	EVOLVING-SYSTEMS-IN	Gurudas Heritage, 3rd flo...		A	2010-03-09		0%	never
LG	2001:df0:92::/48	▣	IITKNET	IIT Kanpur Campus Network		A	2010-04-12	2010-11-22 09:17:44	97%	2011-02-27 10:02:58
LG	2001:df0:c0::/48	▣	WBSDC-NET-IN	Webel Bhavan, Block-EP&GP...		A	2010-08-31	2010-11-22 09:17:44	97%	2011-02-27 10:02:58
LG	2001:df0:e6::/48	▣	CRIS-ND-21-IN	Centre For Railway Inform...		A	2011-01-14		0%	never
LG	2001:df0:fb::/48	▣	LISTER-TECHNOLOGIES-...	Lister Technologies (P) L...		A	2011-02-17		0%	never
LG	2001:e30::/32	▣	ERNET-IN-20040119	ERNET is the largest Inte...	2697	A	2004-01-19	2010-11-22 09:17:44	87%	2011-02-27 10:02:58
LG	2001:e48::/32	▣	SILNET	Sify Limited		A	2004-02-11	2010-11-22 09:17:44	100%	2011-02-27 10:02:58
LG	2001:f30::/32	▣	STPI-NOIDA-20040709	A Class A ISP		A	2004-07-09		0%	never
LG	2001:fd0::/32	▣	Spectranet-20050214	Broadband ISP, India		A	2005-02-14		0%	never
LG	2001:4408::/32	▣	NICNET-20050523	NATIONAL INFORMATICS CENT...		A	2005-05-23	2010-11-22 09:17:44	97%	2011-02-27 10:02:58
LG	2001:4490::/30	▣	BSNLNET-20050922	NIB (National Internet Ba...	9829	A	2005-09-22		0%	never
LG	2001:44c0::/32	▣	BHARTITELESONIC-IN-2...	Bharti Televentures Ltd.		A	2005-11-08		0%	never
LG	2001:4520::/32	▣	HCL-INFINET-IN-20060...	HCL Infinet is a class A ...	9396	A	2006-01-31	2010-11-22 09:17:44	99%	2011-02-27 10:02:58
LG	2001:4528::/32	▣	RELIANCE-COMMUNICATI...	Reliance Communications L...		A	2006-02-09	2010-11-22 09:17:44	97%	2011-02-27 10:02:58
LG	2001:4529::/32	▣	RELIANCE-COMMUNICATI...	Reliance Communications L...		A	2010-08-20		0%	never
LG	2001:452a::/31	▣	RELIANCE-COMMUNICATI...	Reliance Communications L...		A	2010-08-20		0%	never
LG	2400:1600::/32	▣	P4NETWORKS-IN	Parshwa Purushotam Parind...		A	2010-03-10		0%	never
LG	2400:1e00::/32	▣	PI-IN	Pacific Internet India Pv...		A	2010-03-11		0%	never
LG	2400:5200::/32	▣	VODAFONE-NET-AP	C48 Okhla Industrial Esta...		A	2010-03-12		0%	never
LG	2400:a000::/32	▣	XEEX-20081208	Xeex Communication		A	2008-12-08		0%	never
LG	2401:1a00::/32	▣	COGNIZANT	Cognizant Technology Solu...		A	2010-03-29		0%	never
LG	2401:4800::/32	▣	HNS-IN-IPv6-20080520	Honesty Net Solution Pvt ...		A	2008-05-20	2010-11-22 09:17:44	100%	2011-02-27 10:02:58
LG	2401:8800::/32	▣	netmagic-20080523	NetMagic, Data Center ISP...		A	2008-05-23	2010-11-22 09:17:44	0%	2011-01-04 19:02:50
LG	2401:a600::/32	▣	NEXTGEN	NEXTGEN COMMUNICATIONS LT...		A	2010-04-17		0%	never
LG	2401:dc00::/32	▣	NET4-20090919	Net 4 India Ltd		A	2009-09-18		0%	never
LG	2401:fa00::/32	▣	GOOGLE-CORP-APAC	Google Corporate Network	15169	A	2010-05-01	2010-11-22 09:17:44	97%	2011-02-27 10:02:58
LG	2402:a00::/32	▣	GTPL-AS-AP	Gujarat Telelik Pvt Ltd		A	2010-05-04		0%	never
LG	2402:2600::/32	▣	MTNLISP	MTNL CAT B ISP		A	2010-05-06		0%	never
LG	2402:2800::/32	▣	CJONLINE-20080619	CJ Online, Internet Servi...		A	2008-06-19		0%	never
LG	2402:4c00::/32	▣	DISHNET-20091014	Dishnet Wireless Limited		A	2009-10-14		0%	never
LG	2402:8400::/32	▣	TCISL-20091023	TATA Communications Inter...		A	2009-10-23		0%	never
LG	2402:8a00::/32	▣	NETAPPNET	NETWORK APPLIANCE Asia Pa...		A	2010-05-21		0%	never
LG	2402:8c00::/32	▣	DATAINFOSYS-20091026	Data Infosys Ltd		A	2009-10-26		0%	never
LG	2402:8e00::/32	▣	RELIANCECCSNET	WAN Network for backbone ...		A	2010-05-22		0%	never
LG	2402:d400::/32	▣	TATATELE-20091110	Tata Teleservices (Mahara...		A	2009-11-10	2010-11-22 09:17:44	98%	2011-02-27 10:02:58
LG	2402:ea00::/32	▣	LTNETCOM	L&T Netcom Limited		A	2010-06-21		0%	never
LG	2402:f200::/32	▣	SEVENSTAR	G-47 Stella Morris Comple...		A	2010-06-22		0%	never
LG	2403::/32	▣	TATACOMM-IN-20061117	Internet Service Provider	4755	A	2006-11-17	2010-11-22 09:17:44	99%	2011-02-27 10:02:58
LG	2403:c00::/32	▣	HATHWAY-AS-AP	Hathway Cable and Datacom...		A	2009-11-24		0%	never
LG	2403:2200::/32	▣	DIGIVISION-ENTERTAIN...	Digivision Entertainment ...		A	2010-06-30		0%	never
LG	2403:4e00::/32	▣	TIKONANET	Tikona Digital Networks P...		A	2010-07-08		0%	never
LG	2403:8400::/32	▣	HFCLINFOTEL	HFCL Infotel Ltd.		A	2010-01-05	2011-02-09 11:02:54	0%	2011-02-13 00:17:54
LG	2403:8600::/32	▣	TTSLISP	Tata Teleservices ISP		A	2010-07-26		0%	never
LG	2403:fe00::/32	▣	ABTINFOSYSTEM-IN	ABTInfo Systems Pvt Limit...		A	2010-08-17		0%	never
LG	2404:c00::/32	▣	ORTELCOMMUNICATIONS-...	M/s Ortel Communications ...	23772	A	2010-02-08		0%	never
LG	2404:a200::/32	▣	DELDSL-IN	delDSL Internet Pvt. Ltd.		A	2010-09-30		0%	never
LG	2404:a800::/32	▣	BHARTIIN-20081001	BHARTI AIRTEL LTD.		A	2008-10-02	2010-11-22 09:17:44	100%	2011-02-27 10:02:59
LG	2404:ac00::/32	▣	NETCORE-IN	Netcore Solutions Pvt Ltd		A	2010-02-11		0%	never
LG	2404:b200::/32	▣	SPIDIGO-IN	Chandranet Pvt.Ltd.		A	2010-10-04		0%	never
LG	2404:ba00::/32	▣	IN2CABLE	BROADBAND INTERNET SERVIC...		A	2010-10-05		0%	never
LG	2405:200::/29	▣	RELIANCE-INFOTEL-IN	3rd floor, 77B, sector -1...		A	2010-10-27		0%	never
LG	2405:1e00::/32	▣	SOUTHERNONLINE	Southern Online Bio Techn...		A	2010-11-04	2010-12-17 19:32:48	100%	2011-02-27 10:02:59
LG	2405:2400::/32	▣	CONJOINIX-IN	CONJOINIX TECHNOLOGIES PV...		A	2010-02-11		0%	never
LG	2405:6800::/32	▣	YOUTELECOM-20081021	Internet Service Provider		A	2008-10-21		0%	never
LG	2405:6c00::/32	▣	NIPUNANET	Nipuna Services Ltd		A	2010-02-11		0%	never
LG	2405:8a00::/32	▣	RSMANI-NKN-IN	National Knowledge Networ...		A	2010-12-01	2011-01-20 07:47:50	96%	2011-02-27 10:02:59
LG	2405:ba00::/32	▣	ORACLEV6-AP	500 Oracle Parkway		A	2010-12-15		0%	never
LG	2405:e200::/32	▣	REDIFF	Rediff.com India Limited,		A	2010-12-25		0%	never
LG	2405:f600::/32	▣	INPL-IN	Ishan Netsol Pvt Ltd		A	2011-01-04		0%	never
LG	2406:e00::/32	▣	TATAINDICOM-IN	TATA TELESERVICES LTD - T...		A	2011-01-08		0%	never

Annexure D

Best Practices in Transitioning Mechanism

Touch Points	Area	Component	Transition Mechanism	Protocol
Network	WAN	Routers	Dual Stack	OSPv3, ISISv6, BGP4 for IPv6, 6PE, 6VPE, ICMPv6
	LAN	L3 SW	Dual Stack	OSPv3, ISISv6, BGP4 for IPv6, ICMPv6
	Security	Firewall	Dual Stack	OSPv3, IPv6 ACL, NAT44, NAT64, ICMPv6
		IDS	Dual Stack,	ICMPv6
		Servers	Dual Stack	
		Desktops	Dual Stack	
		Video Conf MCU	Dual Stack	
		IP Phones	Dual Stack	
Website		Website	Dual Stack	All services to support IPv6
Applications		DNS	Dual Stack	Support AAAA records
		AAA	Dual Stack	Support RFC 3162
		DHCP	Dual Stack	DHCPv6
		EMS/NMS	Dual Stack	ICMPv6
		e-Gov Apps	Dual Stack	ICMPv6
Services		Data	Dual Stack	All services to support IPv6
		Voice	Dual Stack	All services to support IPv6
		Video	Dual Stack	All services to support IPv6

Annexure E

Status of the Major Service Providers

Name	Status
Tata Tele Services Ltd (TTSL)	Ready
Reliance Communication Infra Ltd.	Ready
Tata Communications Ltd.	Ready
Sify Technologies Ltd	Ready
HFCL Infotel Ltd (Quadrant Televentures Limited)	Ready
Ortel Communications	Ready
MTNL	Fixed ready for Leased Line enterprise customers only. Mobile to be ready by December, 2013.
BSNL	Fixed ready for Leased Line enterprise customers only. Mobile ready for three zones except West .
Airtel	Fixed ready for enterprise services. Retail wireless & wireline under service test.
Vodafone	Fixed ready for Leased Line enterprise customers only.
SSTL	Ready network wise but CPE issue.
Aircel	Ready for enterprise customers.
Other major service providers	Expected to be ready by December, 2013.

Annexure F

Checklist for IPv6 Readiness

Sl. No.	Use case	Special handling required
1.	Store IP addresses in a database	IPv6 addresses are 128-bit hexadecimal, with colons separating the octets. IPv4 addresses are 32-bit, written in decimal, with periods separating the octets. May need to adjust database fields.
2.	Store IP addresses in log files	IPv6 addresses are longer. Log files will grow faster.
3.	Monitoring tools look at IP address	IPv6 addresses are 128-bit hexadecimal, with colons separating the octets. IPv4 addresses are 32-bit, written in decimal, with periods separating the octets. Tools and analysis will need to handle 2 address formats and lengths. Also, since datacenters will translate incoming IPv6 traffic to IPv4, the IPv4 address that the back-end server will see is the IP address of the translation module. This might not meet the needs of the monitoring tool. The tool might need the customer's IP address. If so, it is possible to pass the original IPv6 address along as an X-Forwarded-For header.
4.	Analyze IP addresses stored in a database or a log file	IPv6 addresses are 128-bit hexadecimal, with colons separating the octets. IPv4 addresses are 32-bit, written in decimal, with periods separating the octets. Will need to adjust analysis to handle both formats and to handle the longer length of IPv6. Also, since datacenters will translate incoming IPv6 traffic to IPv4, the IPv4 address that the back-end server will see is the IP address of the translation module. This might not meet the needs of analysis. The analysis might need the customer's IP address. If so, it is possible to pass the original IPv6 address along as an X-Forwarded-For header.
5.	Identifying a customer by his IP address, or differentiate customers by their IP addresses	The datacenters will translate incoming IPv6 traffic to IPv4. The back-end server will see the same IPv4 address for all IPv6 users. It is possible to pass the original IPv6 address along as an X-Forwarded-For header. This will require some change in the product's code.
6.	Using IP-based geo-location	The IP-based geo-location databases are not yet ready for IPv6. Contact the vendors to find out their plans to provide IPv6 coverage. In addition, the datacenters will translate incoming IPv6 traffic to IPv4. The back-end server will see all IPv6 traffic as coming from the internal translator. It is possible to pass elements of the original request along as an XFF header. This would require some change in the product's code.
7.	My product lets the user connect to another product or website	The other product or website might not support IPv6 traffic. You need to ensure graceful handling behind the scenes if it does not. The user should not see an error message.

8.	I block/blacklist an abuser's IP address	The datacenters will translate incoming IPv6 traffic to IPv4. The back-end server will see all IPv6 traffic as coming from the internal translator, so this abuse management solution will not work properly for IPv6 users. It is possible to pass elements of the original request along as an X-Forwarded-For header. This would require some change in the product's code.
9.	I use 3rd-party utilities and open-source code in my product	Ensure that the 3rd-party utilities and open-source code handle IPv6 properly. If you are using an old version, you will probably need to upgrade to a recent version. If the utility or open-source code does not have a version that supports IPv6, then you will need to do development work.
10.	My product is installed on the end-user's box (such as WebEx Client)	A product installed on the end-user's box must be able to handle an IPv6 environment. The IPv6-to-IPv4 translation module cannot help you because it's located at the datacenter.
11.	My product is used before the traffic reaches our IPv6-to-IPv4 translator	The product must be able to handle an IPv6 environment. The IPv6-to-IPv4 translation module cannot help you because it's located at the datacenter.
12.	My product uses Akamai or other CDNs (content distribution networks used for caching popular content, etc.)	You will need to tell your CDN about your IPv6 plans. Akamai will enable v6 for you. Akamai IPv6 functionality is opt-in, not automatic.
13.	My users connect with mobile devices	You will need to check that users with various mobile devices can access your application over IPv6 as well as IPv4.
14.	My application allows users to directly connect to each other (peer-to-peer communication)	IPv6 and IPv4 cannot directly communicate with each other -- they require an intermediary. This traffic will need to route through the IPv6-to-IPv4 translation module in the datacenter. You will need to make this appear to the user to be peer-to-peer communication, even though communication between an IPv6 user and an IPv4 user is not actually peer-to-peer. Users should not see an error message or functionality failure. It should not require the user to do any special setup.

Annexure G

Status of Equipment Manufacturers

Sl. No.	Name	Product Offerings	Status / Plan
1	IBM, India	Servers & Storage Products-Hardware, All telecom & other applications/ Firmware—Software.	All the products on IPv6 supplied after 2002.
2	TEJAS	Transport Equipments—SDH/POTP/ Carrier Ethernet etc. Routers/Switches etc.	Routers/ Switches all on IPv6 (Dual Stack)
3	NSN	Complete GSM Product – BSS/OSS, Radio, Core, Packet Core, HLR, Policy Control etc.	Existing before 2011 product not on V6, but by next one and half year it will be ready. New product some are on IPv6 also.
4	Juniper	Routing/Switching & Security systems & Packet Core (mobile NT) on IPv6.	All the products on IPv6 supplied after 2002.
5	UTStar	Wire line Products like DSLM/IPDSLAM etc.	All Products are IPv6 compliant
6	Microsoft	Client OS/Server OS & applications—Window XP OS can be made V6 complaint, other products Window Vista, Window 7 are on V6.	All are IPv6 ready
7	Ericsson	GSM/CDMA Products- Switches, Routers, BTS, RNCs BSS, OSS, Packet Core, Circuit Core.	Core side Ready (SGSN/GGSN) & Transport /O & M will be ready within next one and half years.
8	Huawei	End to End Products like- Core, Access, Networks, Enterprise & Devices	For dual stack of the old network components and new it will be ready by 2015.
9	CISCO	IPNGN ,Optical Transport, Packet Core, Video, Voice and Cloud Solutions. Routers, Switches,Firewall,IDS,IP S,DPI,Packet Core, CPE,Compute Systems,Telepresence and Network Management Systems.	Cisco routing and switching systems have been IPv6 enabled since long time and all future products from Cisco Stable are planned to have embedded IPv6 support.

Annexure H

IPv6 Adoption across Cloud Service Providers/ Data Centers

The following sections give details of IPv6 adoption across a Data Center covering the following areas -

- Designing and implementing a dual-stack data center: Covering the details regarding design and implementation considerations for deploying IPv6 in the access, aggregation, and core layers of the data center.
- Implementing IPv6 in a virtualized data center: Covers considerations for implementing IPv6 in a virtualized data center.
- Designing IPv6 data center interconnect: Covers the IPv6 deployment across a Data Center

Designing and Implementing a Dual-Stack Data Center

This section considers the three network tiers of the data center (access, aggregation, and core) and gives details of design considerations and implementation for enabling dual-stack (IPv4/ IPv6) in those tiers. The access layer of the network provides connectivity for server farm end nodes residing in the data center. Design of the access layer is tightly coupled to decisions on server density, form factor, and server virtualization that can result in higher interface count requirements. Traditional data center access layer designs are strongly influenced by the need to locate switches in a way that most conveniently provides cabling connectivity for racks full of server resources.

The aggregation layer is the point in the data center where all the access layer uplinks are terminated or "aggregated." In addition to terminating the access layer uplinks, network and application services are often located in the aggregation layer and include services such as security.

The core layer is used to connect the aggregation layers(s) to the rest of the network, which can include the Internet edge, campus and WAN cores, and one or multiple data centers through various data center interconnect technologies.

Data Center Access Layer

The access layer has one goal to physically or virtually connect hosts to the network. Many types of hosts and network devices can connect these hosts to the network physically and virtually. For IPv6 in the data center access layer, a few of the considerations are as follows:

- IPv6 multicast: If hosts connected to the access layer switch need to receive IPv6 multicast, the switch needs to support IPv6 Multicast Listener Discovery (MLD) version 1 and version 2 snooping. This enables the Layer 2 hardware-supported constraint of multicast to only those ports that need to receive the multicast packets.
- IPv6 QoS: IPv6 quality of service (QoS) classification/marking might or might not take place at the access layer. Some customers perform QoS classification/marking in the access layer, aggregation layer, or even further into the network. If it is required in the

access layer, IPv6 packets should be classified and marked, allow re-marking of the packets, and trust markings that took place on the host.

- IPv6 security: A variety of security-related features and technologies can be enabled in the access layer like access control lists (ACL), control-plane policing, first-hop security tools such as rogue-RA protection, and other features more protocol-independent such as private VLANs.
- IPv6 management: It is important to have device-level and system wide management support over IPv6. It is quite common to have Simple Network Management Protocol (SNMP), Secure Shell (SSH)/Telnet, HTTP, and other management access protocols supported at a device-management level. It is equally important for the “manager of manager” or system wide management tools to have rich support for IPv6-enabled endpoints and IPv6-specific feature capabilities.
- Performance: The IPv6-enabled endpoints and applications, supporting IPv6 must have equal or better performance than IPv4 in next-generation platforms.

Configuring Access Layer Devices for IPv6

Configuration of data center access layer switches for IPv6 is not complex. Unless a routed access design is used, a specialized configuration for IPv6 is unnecessary. Many of the configurations made for IPv4 equally apply to IPv6.

Network Interface Cards (NIC) -Teaming Considerations

Another consideration applicable to the access layer is for hosts connecting to the access layer using network interface card (NIC) teaming. NIC teaming is when two or more physical NICs on a server are logically bonded together to act as a single interface. This provides increased throughput to the server and offers higher availability for the physical ports on the server.

However, not every NIC-teaming vendor has native support for IPv6. A common issue around NIC-teaming-enabled hosts is when IPv6 is not supported natively in the NIC-teaming software, but the administrator already has IPv6 enabled (before creating the team) or by manually adding IPv6 addressing to the team interface later on. Depending on the operating system, things can go wrong regarding the normal and expected operation of IPv6.

Data Center Aggregation Layer

The data center aggregation layer, as its name implies, is the point at which the various access layer switches meet and are “aggregated” into a smaller number of very powerful data center switches. The aggregation layer is sandwiched in between the access and core layers and provides external connectivity to those hosts residing in the access layer by linking those hosts to the outside (for example, Internet edge, WAN, or campus) through the core layer. Besides the physical aggregation of links from access layer switches and the logical aggregation of VLANs, many of the application-focused load-balancing, security, and offload services are applied and provided at the aggregation layer. Some of these services include.

- Firewall services
- Deep packet inspection/intrusion detection/intrusion prevention services

- Server load-balancing services
- SSL offload services
- Network monitoring and analysis services

Many of these services are provided by hardware such as appliance and/or service module-based products. Because these specialized products operate at or above Layer 3, it is critical that these products support IPv6, not only through basic addressing, routing/forwarding, and management functions, but they also must provide full-service functionality all the way to Layer 7 if that is the role the product fills.

Bypassing IPv4-Only Services at the Aggregation Layer

It is common to have IPv4-only service products at the aggregation layer but there is also a need to get IPv6 through the aggregation layer in spite of these non-IPv6-capable products. IPv4 and IPv6 traffic can be processed by the service modules and appliances in three modes. They are transparent, one-arm, and routed mode. In each of these cases, IPv6 can be allowed to transit the aggregation layer of these service products, but inspection, load balancing, or any Layer 4–7 service that is provided by the module or appliance is not applied to IPv6 traffic. A few considerations for each mode are as follows:

- Transparent mode: IPv4 traffic is bridged and serviced through the module or appliance, and IPv6 traffic is bridged but not serviced through the module or appliance. Basically, an Ethertype ACL is applied to the module or appliance that enables 0x86DD (Ethertype for IPv6). After it is permitted, any traffic matching the Ethertype will be bridged through the device without inspection or processing.
- One-arm mode: This mode is the easiest mode to deploy when it comes to allowing IPv6 through the services layer. In one-arm mode, traffic is specifically forwarded to the module or appliance based on the destination IP address of a configured Virtual IP (VIP) address, through Policy-Based Routing (PBR), or through another policy-based mechanism. If there are no IPv6-enabled VIPs, PBR, or other routing policies configured, the IPv6 traffic continues on to the destination with no services applied.
- Routed mode: This mode is the most complex and difficult to deal with because it relates to getting IPv6 traffic to its destination. In routed mode, the module or appliance has Layer 3 awareness, which means that if it is not enabled for or capable of processing IPv6 packets, IPv6 will not be routed through the module or appliance. To circumvent this issue the routed mode module or appliance should be bypassed altogether in one of the following ways:
    - Route IPv6 to a dedicated VLAN or physical Layer 3–enabled port that is connected to the downstream host.
    - Configure the host network interface as a trunk. This allows the tagging of VLANs on the trunk between the downstream host, access layer switch, and aggregation layer switch. One VLAN can be for IPv4 and another VLAN for IPv6.

Deploying an IPv6-Only Server Farm

Deploying an IPv6-only server farm is another way of adopting IPv6, wherein the server farm comprises of systems comprising of only IPv6-enabled network devices, hosts, operating systems and services. This is a popular way of deploying IPv6 in the earlier stages of implementation within the enterprise because it allows isolation of IPv6 traffic, IPv6-enabled endpoints, and applications from the existing production IPv4 network.

However, this operational model can be costly, both in capital spending and in operational spending, because much of the network devices, operating system licensing cost, endpoint (that is, physical HW for servers) cost, and operational overhead are being duplicated for the two environments. Pursuing a dual-stack server farm within the data center should be the primary goal.

Supporting IPv4-Only Servers in a Dual-Stack Network

In the Data Center there could be a few IPv4-only servers. This could be due to the operating system not being upgraded to an IPv6-capable OS. It could be that the OS can support IPv6 but the application(s) running on that OS are protocol dependent—as in the case where the application has been coded to be aware of IPv4 but not IPv6.

Several options can help solve this issue for a period of time. Some of these options include IPv4/IPv6 proxies, NAT64 and SLB64.

Regardless of the method used, these options should be seen as interim solutions, and a true native dual-stack data center—including the network, application-aware services, operating systems, and applications—should be the end goal.

Deploying IPv6-Enabled Services at the Aggregation Layer

When IPv6-capable services and devices are in the aggregation layer, most of the design and deployment considerations used with IPv4 are used with IPv6. Feature parity for a given platform can prevent a perfect 1:1 mapping between IPv4 and IPv6, but for the most part, the elements needed for a highly available, secure, and well-managed services layer are the same between the two protocols.

Data Center Core Layer

The IPv6 deployment at the core layer is often simple in design and deployment. As the goal at the core is to keep the core layer a fast, controlled, scalable, and stable point in the network, there is rarely a desire to have a bunch of features enabled, services deployed, and noncritical overhead associated with the core layer switches.

Because of the reduction in the number of features needed in the core and overall design, the IPv6 configuration is usually limited to enabling IPv6 addressing on relevant Layer 3 interfaces connecting the core switches with other network blocks (for example, WAN, Internet edge, and campus) and deploying a routing protocol such as Enhanced IGRP (EIGRP) for IPv6, Open Shortest Path First version 3 (OSPFv3), or Intermediate System–to–Intermediate System (IS-IS). Additional technology deployed at the core, such as QoS and device/network security, most often use the same policies that are in place for IPv4.

Implementing IPv6 in a Virtualized Data Center

If business continuity is a key objective of an organization, it implies that the operations are up and running 24 x 7. To achieve business continuity, some organizations might implement geographic redundancy and maintain multiple data centers located in different geographic regions, each enabled with replicated applications and data.

Virtualization happens in many places such as the network, server, storage, application, desktop, and security. Combining all of these allows a more agile data center environment. This approach is much more cost effective and provides a highly available architecture with better manageability. As data centers are virtualized, the scale and use of IP addresses grow in greater proportion. Some limitations arise with using IPv4 addresses, such as native security support and, most notably, the lack of address space for the rapidly increasing number of connected end devices.

Designing IPv6 Data Center Interconnect

Data Center Interconnect is used to extend layer 2 subnets beyond the traditional Layer 3 boundaries of a data center. DCI connects multiple data centers together to highlight the virtualized data center model with application and server mobility. This mobility provides the underlying services for disaster recovery as well as data center migration, consolidation, or planned maintenance.

Design Considerations: Dark Fibre, MPLS, and IP

Different transport alternatives can be used for connecting various data center sites as follows:

- Dark Fibre (optical): This is typically a Layer 1 service. This type of service is relatively expensive, but it is popular because it serves to transport various types of traffic such as Ethernet and SAN.
- Layer 2 network: In this case, the enterprise sends the provider native Ethernet traffic that will be forwarded to the remote site. Alternatively, an overlay of a Layer 2 VPN solution such as Virtual Private LAN Services (VPLS) can be used, giving the enterprise additional operational flexibility. Regardless of the technology or transport used, IPv6 can run across this Layer 2 network between data centers.
- Layer 3 network: Enterprises can also use Layer 3 connectivity from the SP or over the SP. The enterprise edge devices establish a Layer 3 peering with the SP device or to another enterprise edge device across the SP network. An overlay technology is deployed to extend the LAN between various data center sites.

Annexure I

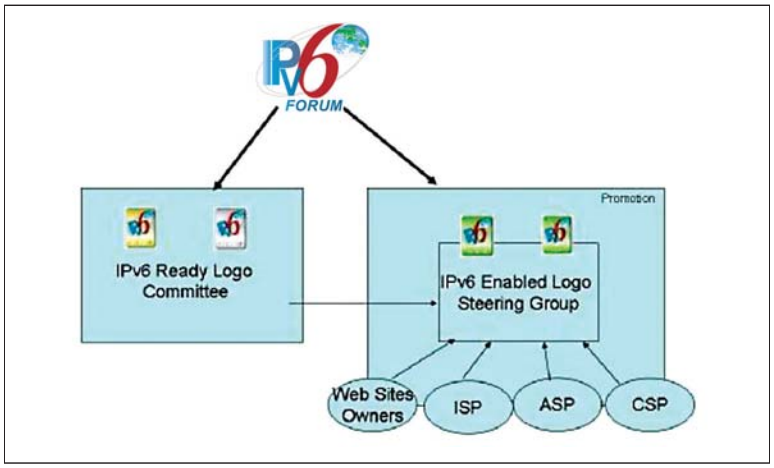
IPv6 Forum Logo Program

1. Introduction

As service providers and organizations begin their journey of IPv6 transition for their networks and websites a requirement is felt regarding compliance to IPv6 standards. The organizations are often faced with the need to ensure that the equipments and services being procured are IPv6 ready. In this regard, globally, the most well renowned program is the 'IPv6 Forum Logo Program', which is managed by the World IPv6 Forum. It is an international testing program intended to increase user confidence by demonstrating that IPv6 is currently available for today's deployment and use. The IPv6 Forum offers this program under 2 categories managed by different entities as shown below:

(i) **IPv6 Ready Logo Program -** for networking equipment vendors.

(ii) **IPv6 enabled logo program -** to recognise the readiness status of the ISPs and the websites of organizations.



These logos can be obtained by the equipment vendors as well as displayed on the organizations' and service providers' websites to announce the readiness status of their networks and website.

2. **IPv6 Ready Logo Program -** The key objectives and benefits of the IPv6 Ready Logo program are three fold:

- Verify protocol implementation and validate interoperability of IPv6 products.
- Provide access to free self-testing tools.
- Provide assistance to IPv6 Ready Logo testing laboratories across the globe.

The IPv6 Ready Logo program works under the aegis of the IPv6 Forum. The IPv6 Forum created the IPv6 Ready Logo Committee in 2002 to manage this globally unique logo program. There is no membership requirement for obtaining the IPv6 Ready Logo since the IPv6 Forum is an open, international forum of IPv6 experts.

a) <u>IPv6 Ready Logo Committee</u> - The IPv6 Ready Logo Committee assists vendors with the IPv6 Ready Logo testing and application requirements. For this purpose it approves various testing laboratories throughout the world. Currently the following testing laboratories have been approved by the IPv6 Ready Logo Committee:

- TTA (Korea)
- BII (China)
- CHT-TL (Taiwan)
- IRISA (Europe)
- UNH-IOL (US)
- JATE (Japan)
- Infoweapons, Phillipines

The approval for IPv6 Ready Logo Committee "membership" and "Approved Test Laboratories" is done by the IPv6 Ready Logo Committee Chairperson, the IPv6 Forum President and IPv6 Forum Chief Technology Officer.

b) <u>Different Phases of the IPv6 Ready Logo Program</u> - The program has 2 phases :

(i) Phase-1 – The Phase-1 program is the "Silver Logo" in which a minimum number of prescribed tests have to be passed by the equipments to be eligible for becoming IPv6 ready and receive the silver logo. Once equipment receives the silver logo it means that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations. The Phase-1 core protocols include IPv6 Specification, Neighbour Discovery, Address Auto-configuration and Internet Control Message Protocol (ICMPv6). The Phase-1 test coverage includes approximately 170 tests.

(ii) Phase-2 – The Phase-2 Gold Logo started in 2005. In this phase the equipments have to pass through more tests. The Gold Logo indicates that a product has successfully satisfied strong requirements as stated by the IPv6 Logo Committee (v6LC). These tests cover the MUSTs and SHOULDs in the IETF RFC tested. The Phase-2 IPv6 core test coverage includes approximately 450 tests. The IPv6 Forum strongly encourages vendors to obtain the IPv6 Ready Logo Phase-2. The Phase-2 Logo verifies optimum compliance because of the complete series of tests including the "MUST" and the recommended "SHOULD" for the IETF specifications tested.

c) <u>Writing Test Specifications</u> - The IPv6 Ready Logo test specifications are primarily developed by the following organizations:

- TAHI Project - Japan
- UNH-IOL (University of New Hampshire Inter Operability Laboratory)- US

Other than the above, the testing laboratories approved by the IPv6 Ready Logo Committee also contribute to the specification development process.

3. **IPv6 Enabled Program for Organizations and Websites** - The IPv6 Enabled Logo (v6eLogo) program consists of two logo sub-programs:

(i) IPv6 Enabled WWW Logo Program (v6eLogo_WWW)

(ii) IPv6 Enabled ISP Logo Program (v6eLogo_ISP)

IPv6 Enabled Steering Committee - The IPv6 Forum has created the IPv6 Enabled Steering Committee (v6eSG), to manage the IPv6 Enabled Logo Program. The IPv6 Enabled Steering Group mission is to help support IPv6 deployment on Web sites and by various service providers (e.g., ISPs, ASPs or CSPs).

IPv6 Enabled WWW Logo:

The IPv6 Enabled WWW Logo Program goal is to encourage adoption of IPv6 on the millions of web sites (WWW) at enterprises, Internet Service Providers (ISPs) and private users helping them to test and check their proper IPv6 readiness and adoption.

Requirements of IPv6 enabled website - The followings are the technical requirements, which an IPv6 enabled web site must satisfied to obtain the logo.

a) IPv6 Resolving Ability - An IPv6 enabled website must have a global IP address, and a AAAA resource record in global domain name system (DNS).

b) IPv6 HTTP Access Ability - An IPv6 enabled website must be able to provide IPv6 access for visitors to the site, via http protocol.

c) Validation Test for IPv6 WWW Site Connectivity - The following technical specification defines how the v6eSG checks to validate the website -

(i) IPv6 DNS Resolving Ability - The script implemented in the checking/validating server(s) at the v6eSG will perform tasks to validate IPv6 DNS resolving ability.

(ii) Primary Test - Two primary test cases have been designed for the validation of the (1) IPv6 DNS resolving ability and the (2) IPv6 HTTP ability for a website.

(iii) Optional - IPv6WWW Maintenance Ability tests - Optionally the following statistics are maintained automatically for v6eLogo_WWW website recipients.

- Daily Reach (DR) statistic is defined as the count of different unique IPv6 visitors' addresses every day. Each unique IPv6 address counts as one regardless of how many times that address attempted to reach the website that day.
- Weekly Reach (WR) is defined as the count of different unique IPv6 visitors' addresses every week.

(d) IPv6 Enabled WWW Logo Program Test Levels: - The IPv6 Enabled WWW Logo Program integrates two levels: basic and advanced.

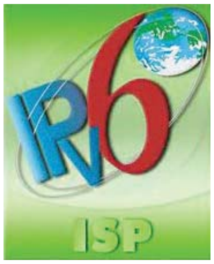
- **Basic Level -** The basic level validates the applicant web site IPv6 reachability as defined by the IPv6 Enabled WWW Logo validation specification. If the script is run successfully the applicant web site is assigned a logo ID and is listed on the IPv6 Enabled web pages.

How to apply - The process for obtaining the IPv6 WWW Logo Basic level is as following:

- ❖ Download the IPv6 Enabled WWW validation specifications from the IPv6 Enabled Logo web site.
- ❖ Fill out the Application form online and complete the IPv6 Enabled Logo Usage Agreement by filling out the entry information and pressing the “apply button” to show your intention of agreement.
- ❖ Once your application is validated and basic reachability checks are run you will receive a dynamic image logo with a script to be insert in your web site source file. The script will check the IPv6 reachability of your web site.
- ❖ Once the script is run successfully on your web site you will receive Logo ID with a unique serial number.
- ❖ Your web site will be listed on the IPv6 Enabled WWW Web Sites List.

- **Advanced Level** - IPv6 Enabled Logo Program Advanced level is under consideration of the forum.

IPv6 Enabled ISP Logo



The goal of the IPv6 Enabled ISP Logo (v6eLogo_ISP) program is for IPv6 enabled ISPs. An Internet Service Provider (ISP, also called Internet Access Provider or IAP) is an organization that offers to its customer access to the Internet and related services. Applicant ISP will be validated for IPv6 service as defined by the program. If passed, the IPv6 Forum then authorizes usage of the IPv6 Enabled ISP Logo for that ISP.

(i) **Requirements of IPv6 enabled ISP** - The followings are the technical requirements, which an IPv6 enabled ISP must satisfied to obtain the logo:

(a) **Network Accessibility Requirement** - Network accessibility is an essential requirement for ISP to provide internet services. ISP should have AS to provide network access services. The AS can be owned by the ISP itself or be leased from other ISPs, either single-homed AS (an AS with only one provider) or multi-homed AS (an AS has multiple providers). The v6eSG operates a database, the synchronous route info database, storing the latest AS related information. Each AS is defined with a unique number. The ISP’s network is considered to have met the network accessibility requirements if the corresponding AS Number exists in the synchronous Route info database.

(b) **Active IPv6 Address Requirement -** Each ISP has IPv6 address block to assign to its customers. For IPv6 Enabled ISP program, the IPv6 address block and active IPv6 address is necessary for the ISP. In order to find the active IPv6 address, the v6eSG give the applicant a section of script code to check the active IPv6 addresses on the Internet.

(c) **Persistence of IPv6 service Requirement -** An IPv6 enabled ISP must provide persistent IPv6 service to its customers. Its customers should be able to connect to the Internet via IPv6 at any time.

(ii) Validation test for IPv6 Enabled ISP logo

- **Primary Test -** The primary test cases have been designed for the validation of the ISP's Network Accessibility Requirement, which the ISP must pass.
- **Optional -** Maintenance Test - If v6eLogo_ISP recipient opts to have the maintenance tested be run. To check the maintenance ability to provide persistent IPv6 service of a v6eLogo_ISP website, the maintenance test will be automatically run by v6eSG. The v6eLogo_ISP recipient can opt-out to not have the maintenance tested run.

(iii) **IPv6 Enabled ISP Logo Program Test Levels -** The IPv6 Enabled ISP Logo Program integrates two levels: basic and advanced.

- **Basic Level -** The basic level validates the applicant IPv6 services as defined by the IPv6 Enabled ISP Logo validation specification. If the script is run successfully the applicant ISPs is assigned a logo ID and is listed on the IPv6 Enabled ISPs pages.

  How to apply - The process for obtaining the IPv6 ISP Enabled Basic level is as under:

- Download the IPv6 Enabled ISP validation specifications from the IPv6 Enabled Logo web site.
- Fill out the Application form online and complete the IPv6 Enabled Logo Usage Agreement
- Once the ISP owner's application is validated and basic reachability checks are run, a script will be provided to be inserted in a web site source file. The script will check the IPv6 reachability of the ISPs' service.
- Once the script is run successfully on the ISP a Logo ID with a unique serial number will be provided.
- The ISP will be listed on the IPv6 Enabled ISP Web Sites list.

- **Advanced Level -** IPv6 Enabled Logo Program Advanced level is under consideration of the forum.

Annexure J

List of Specifications
(IETF RFC Summary for IPv6 Readiness)

(1) Core Protocols for IPv6 Conformance

IETF Specification	Components
RFC2460	IPv6 Specification
	IPv6 Packets: send, receive
	IPv6 packet forwarding
	Extension headers: processing
	Hop-by-Hop & unrecognized options
	Fragment headers: send, receive, process
	Destination Options extensions
RFC4443	ICMPv6
RFC1981	Path MTU Discovery for IPv6
	Discovery Protocol Requirements
RFC4861	Neighbor Discovery for IPv6
	Router Discovery
	Prefix Discovery
	Address Resolution
	NA and NS processing
	Duplicate Address Detection
	Creation of Global Addresses
	Ability to Disable Creation of Global Address
RFC4862	Duplicate Address Detection
	Neighbor Unreachability Detection
	Redirect functionality
	IPv6 Stateless Address Autoconfiguration
	Creation of Link Local Addresses

[1] This list of specifications may change from time to time depending upon the standardization efforts by different International bodies, which will be accordingly updated. The list may be taken as a reference by different organizations while procuring IPv6 ready equipments, however this will also depend upon the features desired in the equipments. All equipments may not need all the features and hence all the RFCs many not be applicable. Organizations may decide their requirements in consultation with the vendors.

(2) Core Protocols for IPv6 Interoperability

IETF Specification	Components
RFC2460	IPv6 Specification
RFC4443	ICMPv6
RFC4861	Neighbour Discovery
RFC4862	Duplicate Address Detection
	IPv6 Stateless Address Autoconfiguration
RFC1981	Path MTU Discovery for IPv6
RFC4291	Internet Addressing Architecture
RFC5095	Deprecation of Type 0 Routing Headers
RFC2710	Multicast Listener Discovery for IPv6

(3) DHCPv6 Conformance and Interoperability

IETF Specification	Components
RFC3315	Dynamic Host Config Protocol (DHCPv6)
	Ability to Administratively Disable DHCP
	DHCP Client Functions
RFC3736	Stateless DHCP for IPv6
RFC3633	Prefix Delegation

(4) IPSEC (Internet Protocol Security)

IETF Specification	Components
RFC2404	Use of HMAC-SHA-1-96 within ESP and AH
RFC2410	NULL Encryption Algorithm and Its Use With IPsec
RFC2451	ESP CBC-Mode Cipher Algorithms
RFC3566	AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
RFC3602	AES-CBC Cipher Algorithm and Its Use with IPsec
RFC3686	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
RFC4301	Security Architecture for the Internet Protocol
RFC4303	IP Encapsulating Security Payload (ESP)
RFC4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC4312	Camellia Cipher Algorithm andIts Use With IPsec
RFC4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec

(a) Encryption Algorithms

Two encryption algorithms are specified by the IPv6 Forum in the categories:

(i) BASE ALGORITHM

a. 3DES-CBC

(ii) ADVANCED ALGORITHM

a. AES-CBC

b. AES-CTR

c. NULL

d. CAMELLIA-CBC

All NUTs must pass the BASE ALGORITHM tests. An NUT which supports algorithms listed as ADVANCED ALGORITHM, must pass all corresponding tests. The algorithm requirement is independent from NUT type.

(b) Authentication Algorithms

All NUTs have to pass all the tests of BASE ALGORITHM to confirm to the specifications. The NUTs, which support the algorithms that are listed as ADVANCED ALGORITHM, have to pass all the corresponding tests. The algorithm requirement is independent from NUT type.

(i) BASE ALGORITHM:

a. HMAC-SHA1

(ii) ADVANCED ALGORITHMS:

a. AES-XCBC-MAC-96

b. NULL

c. HMAC-SHA-256

(5) Internet Key Exchange V2 (LKEV2) Conformance and Interoperability

IETF Specification	Components
RFC4306	IKEv2 Protocol
RFC4307	Cryptographic algorithms for IKEv2
RFC4718	IKEv2 Clarifications and Implementation Guidelines

(6) Multicast Listener Discovery V2 (MLDV2)

IETF Specification	Components
RFC2710	Multicast Listener Discovery for IPv6
RFC3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
RFC3810	Multicast Listener Discovery v2 for IPv6
RFC4604	MLDv2 for Source Specific Multicast (SSM)
RFC4606	Using Internet Group Management Protocol Version 3 (IGMPV3) and Multicast Listener Discovery Protocol 2 (MLDv2) for Source-Specific Multicast

(7) Simple Network Management Protocol (SNMP)

IETF Specification	Components
RFC3411	SNMP v3 Management Framework
RFC3412	SNMP Message Process and Dispatch
RFC3413	SNMP Applications
	Command Responder
	Notification Generator
RFC3414	User-based Security Model for SNMPv3
RFC3416	SNMPv2
RFC3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) v2

(8) Management Information Base (MIB)

IETF Specification	Components
RFC4293	MIB for the IP
RFC4292	MIB for the IP Forwarding Table
RFC4022	MIB for TCP
RFC4113	MIB for UDP
RFC4087	MIB for IP Tunnels
RFC4807	MIB for IPSec Policy Database Configuration
RFC4295	MIB for Mobile IPv6
RFC3289	MIB for DiffServ

(9) Session Initiation Protocol (SIP)

IETF Specification	Components
RFC3261	SIP: Session Initiation Protocol
RFC3264	An Offer/Answer Model with Session Description Protocol
RFC4566	SDP: Session Description Protocol
RFC2617	HTTP Authentication: Basic and Digest Access Authentication
RFC3665	SIP Basic Call Flow Examples

CHAPTER 10

Glossary

Glossary

Sl. No.	Abbreviation	Meaning
1	2G	2nd Generation
2	3G	3rd Generation
3	ACL	Access Control Lists
4	AFT	Address Family Translation
5	ALG	Application Level Gateways
6	AMI	Advanced Metering Infrastructure
7	APNIC	Asia Pacific Network Information Centre
8	APRICOT	Asia Pacific Regional Internet Conference on Operational Technologies
9	AS	Autonomous System
10	AUSPI	Association of Unified Telecom Service Providers Association of India
11	BSNL	Bharat Sanchar Nigam Limited
12	BWA	Broadband Wireless Access
13	CCTLD, ccTLD	Country Code Top Level Domain
14	CDMA	Code Division Multiple Access
15	CDOT	Centre for Development of Telematics
16	CERT-In	Computer Emergency Response Team India
17	CGN	Carrier Grade NAT
18	CMAI	Component Manufacturers Association of India
19	CNGI	China Next Generation Internet
20	COAI	Cellular Operators Association of India
21	CoI	Centre of Innovation
22	CUG	Closed User Group
23	DC	Data Concentrator
24	DeitY	Department of Electronics & Information Technology
25	DFP	Default Free Prefixes
26	DHCP	Dynamic Host Configuration protocol
27	DIT	Department of Information Technology

28	DNS	Domain Name System
29	DoS	Denial of Service
30	DoT	Department of Telecommunications
31	DR	Demand-Response
32	DSL	Digital Subscriber Line
33	EH	Extension Header
34	ERNET	Education and Research Network
35	FICCI	Federation of Indian Chambers of Commerce and Industry
36	FTTH	Fiber To The Home
37	GDP	Gross Domestic Product
38	GIS	Geographic Information System
39	GOI	Government of India
40	GPRS	General Packet Radio Service
41	GSM	Global System for Mobile Communications
42	IANA	Internet Assigned Numbers Authority
43	ICANN	Internet Corporation for Assigned Names and Numbers
44	ICMP	Internet Control Messaging Protocol
45	ICT	Information and Communications Technology
46	IDA	Infocomm Development Authority
47	IETF	Internet Engineering Task Force
48	IIGC	India Internet Governance Conference
49	IIT	Indian Institute of Technology
50	Indian TSDO	Indian Telecom Standards & Development Organisation
51	IP	Internet Protocol
52	IPSec	Internet Protocol Security
53	IPTV	Internet Protocol Television
54	IPv4	Internet Protocol Version 4
55	IPv6	Internet Protocol Version 6
56	IRINN	Indian Registry for Internet Names and Numbers
57	ISP	Internet Service Provider

58	ISPAI	Internet Service Providers Associations of India
59	ITU	International Telecommunication Union
60	LEA	Law Enforcement Agencies
61	LIR	Local Internet Registry
62	LTE	Long Term Evolution
63	M2M	Machine to Machine
64	MIPv6	Mobile IPv6
65	MMS	Meter Management System
66	MNP	Mobile Number Portability
67	MOU	Memorandum of Understanding
68	MPLS	Multiprotocol Label Switching
69	MTNL	Mahanagar Telephone Nigam Limited
70	MTU	Maximum Transmission Unit
71	NAT	Network Address Translation
72	NAV6TF	North American IPv6 Task Force
73	NEMO	Network Mobility
74	NGN	Next Generation Networks
75	NIR	National Internet Registry
76	NIXI	National Internet Exchange of India
77	NKN	National Knowledge Network
78	NTP	National Telecom Policy
79	PA	Provider-Allocated
80	PDA	Personal Digital Assistant
81	PKI	Public Key Infrastructure
82	PoC	Proof-on Concept
83	PPP	Public Private Partnership
84	PSU	Public Sector Undertaking
85	QoS	Quality of Service
86	QoS	Quality of Service
87	RFC	Request for Comments

88	RFID	Radio Frequency Identification
89	RIR	Reginal Internet Registry
90	RTP	Real Time Transport Protocol
91	SA	Security Association
92	SDC	State Data Centres
93	SWAN	State Wide Area Network
94	SWOT	Strengths, Weaknesses, Opportunities and Threats
95	TCP	Transmission Control Protocol
96	TEC	Telecom Engineering Centre
97	TEMA	Telecom Equipment Manufacturers' Association
98	TLD	Top Level Domains
99	TRAI	Telecom Regulatory Authority of India
100	TTL	Time to Live
101	UDP	User Datagram Protocol
102	USO	Universal Service Obligation
103	USP	Upstream Service Provider
104	VAS	Value Added Service
105	VPN	Virtual Private Network
106	VRF	Virtual Routing and Forwarding
107	WAN	Wide Area Networks
108	WIDE	Widely Integrated Distributed Environment
109	WiMAX	Worldwide Interoperability for Microwave Access