Indian Council for Research on International Economic Relations

POLICY BRIEF

on IPV6 Transition in India

JUNE 2020

IPV6 Transition in India

Rajat Kathuria

Satya N Gupta

Isha Suri

Disclaimer:

Opinions and recommendations in the report are exclusively of the author(s) and not of any other individual or institution, including ICRIER. This report has been prepared in good faith on the basis of information available at the date of publication. All interactions and transactions with industry sponsors and their representatives have been transparent and conducted in an open, honest and independent manner as enshrined in ICRIER Memorandum of Association. ICRIER does not accept any corporate funding that comes with a mandated research area which is not in line with ICRIER's research agenda. The corporate funding of an ICRIER activity does not, in any way, imply ICRIER's endorsement of the views of the sponsoring organization or its products or policies. ICRIER does not conduct research that is focused on any specific product or service provided by the corporate sponsor

Contents

List of Tables

List of Figures

List of Abbreviations

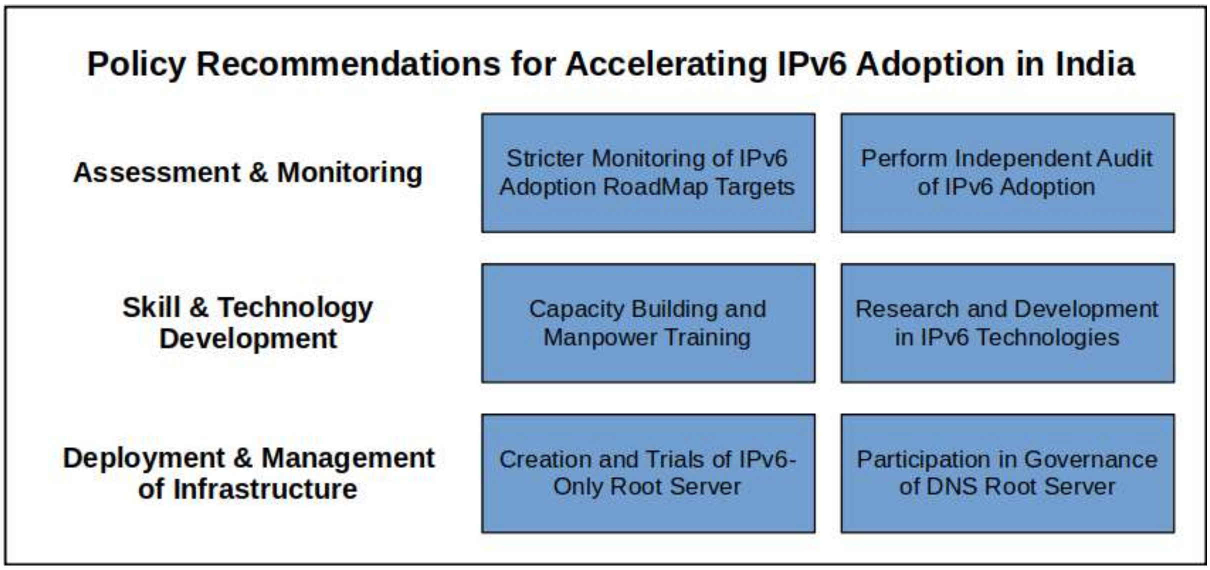
6ORS	V6 Only Root Server
ACTO	Association of Competitive Telecom Operators
AI	Artificial Intelligence
APNIC	Asia Pacific Network Information Centre
ARP	Address Resolution Protocol
AUSPI	Association of Unified Telecom Service Providers of India
CDAC	Centre for Development of Advanced Computing
CDOT	Centre for Development of Telematics
CIDR	Classless Inter-Domain Routing
CMAI	CMAI Association of India
COE	Centre of Excellence
CPE	Consumer Premises Equipment
CTO	Commonwealth Telecommunications Organisation
DHCP	Dynamic Host Configuration Protocol
DHCS	Dynamic Host Configuration Server
DNS	Domain Name Server
DoT	Department of Telecommunications
DRDO	Defence Research and Development Organisation
DSCP	Differentiated Services Code Point
ECN	Explicit Congestion Notification
GMP	Group Management Protocol
GoI	Government of India
HRD	Human Resource Development
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IHL	Internet Header Length
IISc	Indian Institute of Science
IIT	Indian Institute of Technology
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Providers
ISPAI	Internet Service Providers Association of India
IT	Information Technology
ITES	Information Technology Enabled Services
M2M	Machine to Machine

MAC	Media Access Protocol
MeitY	Ministry of Electronics and Information Technology
NASSCOM	National Association of Software and Services Companies
NAT	Network Address Translation
NDP	Neighbour Discovery Protocol
NOS	National Occupational Standards
QoS	Quality of Service
R&D	Research and Development
RFC	Request for Comments
RIP	Routing Information Protocol
RIR	Regional Internet Registry
SNMP	Simple Network Management Protocol
SSC	Sector Skill Councils
TEC	Telecommunication Engineering Center
TEMA	Telecom Equipment Manufacturers Association
ToS	Type of Service
TTL	Time to Live
TVs	Televisions
VLSM	Virtual Length Subnet Mask
VPN	Virtual Private Network

Executive Summary

Internet Protocol (IP) is a set of rules governing the format of data transferred between computers over the internet or any local area network. The existing protocol supporting the internet today - Internet Protocol Version 4 (IPv4) - provides the world with roughly 4 billion IP addresses, inherently limiting the number of devices that can have a unique, globally routable address on the internet. While the Information Technology (IT) community has come up with workarounds to address this shortage in the IPv4 environment, the adoption and deployment of Internet Protocol Version 6 (IPv6) which has an exponentially large number of IP addresses is the only long-term solution to this problem. The wide-scale implementation of IPv6 in existing and newer networks is essential to the continued growth of the Internet and the development of novel applications that can leverage the increase in mobile internet connectivity.

The adoption of IPv6 is vital for addressing the depletion of IPv4 addresses and ensure the growth of the Internet in a developing nation like India. The Government of India has already put initiatives in place to promote the adoption of IPv6 in existing and developing network infrastructure. These initiatives focus on preparedness for the future of networking and internet technology by enabling networks to support IPv6 addresses and data packets. However, this critical transition should be done methodically and mindfully, with complete awareness of the benefits, challenges, and caveats surrounding the adoption of IPv6 to avoid any significant disruptions. This document strives to outline issues around the IPv4 to IPv6 transition and provides an overview of the initiatives taken by government agencies tasked with IPv6 transition. This report analyses various issues and challenges related to adoption and migration to IPv6, and provides implementable recommendations to the Government of India on accelerating IPv6 adoption and transition in India.



Policy Recommendations for Accelerating IPv6 Adoption in India

Assessment & Monitoring	Stricter Monitoring of IPv6 Adoption RoadMap Targets	Perform Independent Audit of IPv6 Adoption
Skill & Technology Development	Capacity Building and Manpower Training	Research and Development in IPv6 Technologies
Deployment & Management of Infrastructure	Creation and Trials of IPv6-Only Root Server	Participation in Governance of DNS Root Server

1. Background

The internet is a publicly owned, openly-accessible global interconnected network of networks that has driven education, industrial and other areas of productivity in recent decades. An estimated 4.4 billion[1] people (as of April 2019) globally use the internet for browsing, email communication, accessing multimedia content and services, playing online games and using social networking applications.

Internet Protocol (IP) addresses are the unique numbers assigned to every computer or device connected to the internet. The currently used version of the Internet Protocol, IPv4, was developed in the 1980s and has served the global Internet community for over three decades. The IPv4 has a capacity of just over 4 billion IP addresses, which while adequate for the experiment that the internet started as in the 1980s, are grossly insufficient at present with years of rapid Internet expansion across the globe. Over the years, the pool of available IPv4 addresses has been entirely allocated to Internet services providers (ISPs), Telcos and users. Furthermore, the rapid growth in the number of internet-connected devices (smartphones, tablets, laptops, and others) has led to an imminent shortage of IP addresses for every device under the current IPv4 addressing scheme. This depletion of available Internet addresses will hinder and limit the growth of the internet and associated applications and services in the coming years. At present, an estimated 4.3 billion of the approximately 7.5 billion people on the planet are connected to the internet[2,3], with each user having more than one device with network connectivity[4].

The problem of IP address scarcity is exacerbated given these numbers, with the number of Internet-connected devices projected to increase to 29 billion by 2022, 18 billion of which are estimated to be related to the Internet-of-Things (IoT) ecosystem[5]. This growth is anticipated to be driven by an increase in the number of users, along with a surge in Internet-connected devices per user, including computers, smartphones, TVs, tablets, game consoles, smart appliances, and smart-grid utility meters. Furthermore, the free pool of IPv4 addresses held by the Internet Assigned Numbers Authority (IANA) was depleted in February 2011. While each of the Regional Internet Registries (RIRs) still had a free pool of addresses previously assigned to it by IANA, these pools were also exhausted sometime between 2011 and 2013[6]. Public IPv4 addresses have become a scarce resource with the depletion of these RIR address pools, and

[1] Statista - Global digital population as of April 2019 (in millions) https://www.statista.com/statistics/617136/digital-population-worldwide/

[2] Data from World Bank Last updated: Jul 6, 2018

[3] https://www.internetworldstats.com/stats.htm

[4] Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. Available at: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[5] Internet of Things forecast – Ericsson Mobility Report - https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[6] https://ipv4.potaroo.net/

this is a challenge that must be addressed by enterprise IT organisations as well as ISPs and web properties such as Yahoo and Google.

The IPv6, developed to replace IPv4, allows for approximately 340 undecillion (10^{38}) addresses and can lead to improvements such as simplified configuration, improved Quality of Service (QoS), and built-in security. The large number of IP addresses offered by IPv6 provides an opportunity to build better network architectures by simplifying address assignment and removing Network Address Translation[7] (NAT) devices which have been used to expand address capacity in the IPv4 scheme. The use of IPv4 address conservation methods, such as Classless Inter-Domain Routing (CIDR) for aggregating IP addresses and Dynamic Host Configuration Protocol (DHCP) for assigning temporary IP addresses to devices[8] can also be removed with IPv6 usage, providing a path to achieving always-on broadband connectivity. IPv6 also provides improved support for headers and extensions enabling faster and more efficient configuration options for communication devices connecting to the internet, while also easing the complexity of providing end-to-end security.

The exhaustion of IPv4 addresses will make it impossible for additional internet-enabled devices to connect to the network, necessitating the migration to IPv6. However, this transition continues to be in the initial stages. According to the Google IPv6 traffic graph, which is one of the barometers for global IPv6 deployment, the availability of IPv6 connectivity among Google users as of September 2019 is 25.85%[9]. While this figure has increased every year, it continues to be reasonably small despite the criticality of deploying IPv6.

While IPv6 does provide a substantial number of IP addresses for any conceivable situation well into the foreseeable future, the transition to IPv6 is complicated by the fact that IPv6 is not backwards compatible with IPv4. At present, the majority of internet services and content are based on IPv4, with the latest generation of devices supporting both IPv4 and IPv6 in a dual-stack configuration. However, as the number of internet-connected devices continues to grow, user devices supporting only IPv6 will inevitably emerge. Consequently, a dual-protocol internet will need to provide some gateway functionality to allow interoperability between single stack end systems that only support either IPv4 or IPv6. Without this functionality in place, services and devices will not have access to the whole expanse of the internet.

IPv4 and IPv6 schemes cannot communicate directly with each other. Therefore, while migrating to an IPv6 environment, it must be ensured that the network devices and equipment are IPv6 compatible. Generally, new network hardware and software will have to be acquired to make the network IPv6 ready. An implementable migration roadmap is required to be

[7] J. Rosenberg, R. Mahy, and P. Matthews, “Traversal Using Relays around NAT (TURN),” draft-ietf-behave-turn-08, 2008.

[8] Amer Nizar Abu Ali, “Comparison study between IPV4 & IPV6”, International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012

[9] https://www.google.com/intl/en/ipv6/statistics.html

developed to prepare for the transition to IPv6. The investment of resources like time, money, and proper skill training is necessary for successful adoption of IPv6.

This paper provides a brief overview of the state of the IPv4 to IPv6 transition in India and the world. The need for the adoption of IPv6 in India and the world are discussed, and an outline of the technologies available to enterprise IT organisations and ISPs to transition to IPv6 is presented. The various initiatives undertaken by the government so far in this regard are summarised along with the challenges involved in the IPv4 to IPv6 transition. Finally, a set of policy recommendations is provided for ensuring an accelerated and smooth transition to IPv6 in India.

2. The Rationale for IPv6

The rapid pace of economic development in India requires an advanced IT infrastructure that is capable of meeting the demand generated while also acting as a catalyst for further development. Increasing globalisation and the international adoption of IPv6 also requires India to follow suit to keep up with the rest of the world lest it affects development in industries and areas reliant on the internet and communication technologies. The consequent increase in demand for IP address spaces can only be satisfied in the near future through gradual phasing out of IPv4 and increasing adoption of IPv6 in the internet infrastructure.

While the global migration from IPv4 to IPv6 will take many years to complete, India must prioritise and push forth with this transition for the following reasons:

- to ensure, wherever possible, that any systems purchased in the future are IPv6 ready, thus minimising the risk of them becoming stranded assets.
- to provide individuals and organisations in India can communicate with IPv6 services in the rest of the world, allowing for industries such as e-commerce and education to proceed seamlessly.
- to future proof new projects such as ‘Smart City’ and ‘Internet of Things’ initiatives where the use of IPv6 from the very beginning is essential to reap benefits, as a later retrofit to IPv6 would be both expensive and disruptive.

However, the complexity of the IP ecosystem makes it difficult for a single player to unilaterally adopt IPv6 because of the dependency on other players across the ecosystem like equipment suppliers, application, and network operators. This paper seeks to provide a framework for a well-coordinated adoption of IPv6 across the national ecosystem by ensuring that various building blocks essential for the transition to IPv6 are in place.

Prompt and efficient adoption of IPv6 offers India the potential for accelerating innovation and progress of the internet and related technologies. Countries such as China, Australia, South

Korea, and New Zealand[10], have already taken a keen interest in the deployment of IPv6. India must also invest in IPv6 based services and devices in order to secure a competitive advantage.

2.1 Benefits of IPv6 Adoption

IPv6 adoption can potentially reshape and redefine markets. One of the most significant benefits of IPv6 adoption is the development of the Internet of Things (IoT) based devices and services. The economic and social impact of IoT has been speculated to be even more significant than the industrial revolution[11]. The connectivity of smart devices, such as RFIDs, sensor, actuators, and other machine-to-machine communication devices to the internet makes up the IoT ecosystem, with the accumulation of data, applications, and services benefiting new business and market opportunities. The two significant factors that are expected to drive the adoption of IPv6 in India considering these issues are as follows:

a) *the need for additional address space; and*
b) *the emergence of new applications and devices which require more addresses and efficient network infrastructure.*

IPv6 is a component of the country's digital infrastructure that will support the development and use of innovations that utilise the features of IPv6. The adoption and assimilation of IPv6 will provide a platform for new services and technologies while increasing the number of users using the services and technologies. Country/Organisations that delay IPv6 adoption, on the other hand, may find it difficult to connect to other countries/organisations who have shifted to IPv6, and their ageing infrastructure could lead to increases in support costs and risk when integrating new IPv6 applications and services. IPv6 adoption is also essential to provide next-generation network services, which are crucial for the advancement of an organisation's operations in the net-centric world.

2.2 The Need for Transition to IPv6

IPv6 is playing a critical role in Internet development, providing new services and business opportunities for large-scale IP network applications - including smartphones, smart grids, Next-Generation Networks, and Cloud Computing – all of which will drive unprecedented demand for IP addresses

- IPv6 has an abundance of addresses.
- IPv6 based networks are easier to manage.
- IPv6 ensures end-to-end transparency.
- IPv6 has improved security features.

[10] IPv6 Deployment Strategies in APEC Economies - Asia-Pacific. Available at: https://www.apec.org/-/media/APEC/Publications/2017/8/IPv6-Deployment-Strategies-in-APEC-Economies/217_TEL_IPv6-Infomation-Paper.pdf

[11] Ludvig Ahlinder, Anders Eriksson - Accelerating Adoption of IPv6, KTH Information and Communication Technology, Stockholm, Sweden.

- IPv6 has improved mobility capabilities.
- IPv6 will encourage further innovation

The IPv6 is emerging to form the basis of the present-day and future broadband Internet services. As such, IPv6 based networks are anticipated to replace IPv4-based networks to overcome the limitations of IPv4.[12]

3. The State of IPv4 & IPv6 Worldwide

3.1 The State of IPv4

3.1.1 IPv4 in India

IPv4, the original version of the internet protocol was developed about 25 years ago at the initial stages of the internet. This version of IP (known as version 4 or IPv4) has not been substantially changed since it was published in 1981 *(ref IETF RFC 791)*. Although IPv4 has proven to be easily implementable and interoperable, the initial design failed to anticipate some of the following issues:

- The exponential evolution of the Internet and its users and hence, the impending exhaustion of the IPv4 address space
- The ability of backbone routers (for internet) to maintain large routing tables
- The need for simpler and automatic configuration of IP addresses.
- The requirement of security at the IP layer
- Enhanced support for real-time delivery of data, also known as Quality of Service (QoS) for applications like VOIP.

With the USA being a pioneer in the development of the internet, organisations and companies based in the US garnered a majority of IPv4 addresses, with the remaining chunk being distributed amongst the rest of the world. India, with a population of 1.3 billion, has merely 85 million[13] IPv4 addresses compared to the 304 million held by China, and more than a billion by the USA.

With APNIC, the IP address registry for Asia-Pacific, having exhausted its capacity of IPv4 addresses back in 2011[14], India has had to rely on Network Address Translation (NAT) devices for using IPv4 while increasing adoption of the internet throughout the country. The use of NAT has increased the complexity in its internet infrastructure with the division of the internet into smaller independent address administrations that specifically facilitate the casual use of

[12] "Internet Society, Number Resource Organization, and Regional Internet Registries Reinforce Importance of IPv6 Deployment for the Future of the Internet" – Available at - https://web.archive.org/web/20120609063734/http://www.internetsociety.org/news/internet-society-number-resource-organization-and-regional-internet-registries-reinforce

[13] https://ipfinder.io/countries/

[14] https://ipv4.potaroo.net/

private address assignments[15]. The use of such private addresses in the network results in ambiguity as the process of resolving the to or from addresses becomes dependent on the network node where the question originated.[16] The result of this division is the enforcement of a client/server architecture over a peer-to-peer one, with the servers needing to exist in the public address realm.

This small chunk of IPv4 addresses is inadequate to serve the needs of the entire population with the advent of new technologies like IoT and M2M communications. The adoption of IPv6 is the only option for India to achieve 100% digital penetration of the internet in this scenario. This will eventually help in it becoming a conducive market for the development of technologies like IoT and M2M communications that will also need IP addresses. The increased reliance on conventional IPv4 techniques may make the transition to IPv6 even more complex and costlier in the future.

3.1.2 IPv4 in the World

During the development of the internet in the 1980s, a total of 4.3 billion IPv4 addresses were considered to be sufficient. Consequently, many organisations purchased a large number of address spaces and far too many addresses than what they needed, with almost 50% of the addresses being allocated by 1990.[17] Subsequently, international organisations like the ICANN and their RIRs (Regional Internet Registries) like APNIC, evolved policies to control new assignments of IP addresses as per the demonstrated need. This has led to a skewed distribution of IPv4 addresses among different countries in the world. The increased use and complete allocation of the IPv4 address space have led to it becoming a scarce resource that is not enough to sustain the continued growth of the Internet.

3.2 The State of IPv6

3.2.1 IPv6 in India

IPv6 is designed to solve the problems of address depletion and security inherent in the IPv4. The use of IPv6 also expands the capabilities of the internet to enable a variety of valuable scenarios, including peer-to-peer as well as mobile applications. As such, India lags in overall migration to the IPv6 network. A government roadmap and a policy framework are imperative for efficient and proper migration to IPv6 in time. The data available for significant ISPs and Telcos in India shows that most of these players, barring new telcos such as Reliance Jio, do not prioritise network migration to IPv6. While, some of the more prominent service providers and telcos have reserved IPv6 addresses from the APNIC, and their network is almost IPv6 ready, they are yet to undertake this migration. As far as the international scenario is concerned, the status of transition inspires more confidence; however, the transition may take a more

[15] IEFT RFC 1918: Address Allocation for Private Internets – Available at: https://tools.ietf.org/html/rfc1918

[16] IETF RFC 2101: IPv4 Address Behaviour Today – Available at: https://tools.ietf.org/html/rfc2101

[17] National IPv6 Deployment Roadmap v-I - Department of Telecommunications, GoI.

extended period of time. Considering the growth of internet users in India and the importance of the government's role in the migration to IPv6, an analysis of Indian internet network and telecom market must be performed, and a detailed migration roadmap must be prepared with clearly defined roles and responsibilities for each stakeholder.

The Government of India took cognisance of the issue in 2004 and consequently placed network migration as one of its main agendas. Department of Telecommunications (DoT) was handling the primary role of this network migration and undertook a series of training workshops and awareness programmes throughout the country[18]. The development of an IPv6 transition plan in consultation with relevant stakeholders and the creation of a national IPv6 taskforce was the significant areas of focus of the government. Also, as a continuity of policy decisions, India published National IPv6 Deployment Roadmap Version I in 2010[19] and a second version of the Roadmap in 2013[20]. Also, the NDCP-2018 clearly states the use of IPv6 to all the existing communication systems, equipment, networks and devices[21].

Some of the critical statistics for India as obtained from the APNIC are in the Table[22] below:

Table 1: India IPv6 Capable and IPv6 Preferred

AS Name	IPv6 Capable	IPv6 Preferred
RELIANCEJIO - IN Reliance Jio Infocomm Limited	93.95%	93.61%
BHARTI-MOBILITY - AS-AP Bharti Airtel Ltd.	49.36%	49.12%
HUTCHVAS - AS Vodafone Essar Ltd.	50.48%	50.16%
ICLNET-AS-AP – Idea Cellular Limited	50.69%	50.15%
BSNL – NIB – National Internet Backbone	0.08%	0.05%

According to Google's statistics, India has reached an IPv6 adoption rate of around 35.95% at the end of June 2019[23]. Also, APNIC places India at more than 50% preferring IPv6.

So far, the Indian industry has not engaged on the large-scale deployment of IPv6 apart from a few Telcos and ISPs such as Reliance JIO that have undertaken this transition independently without any policy support from the government. As such, Reliance Jio has more IPv6 users than all other IPv6-capable Indian ISPs collectively, and over 90% of its traffic uses IPv6. With

[18] Consultation Paper on Issues Relating to transition of IPv4 to IPv6 in India – Available at: https://main.trai.gov.in/consultation-paper-issues-relating-transition-ipv4-ipv6-india

[19] Government of India, (2010). National IPv6 Deployment Roadmap Version I. [online], Available: http://www.dot.gov.in/sites/default/files/National-Ipv6-Deployment-Roadmap.pdf

[20] Government of India, (2013). National IPv6 Deployment Roadmap Version II. [online], Available: http://www.dot.gov.in/sites/default/files/Roadmap%20Version-II%20English%20_1.pdf

[21] National Digital Communications Policy 2018, GoI

[22] APNIC - Use of IPv6 for India (IN) – Available at: https://stats.labs.apnic.net/ipv6/IN

[23] Google IPv6 Statistics, Available at: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

an estimated 279 million users, India accounts for half of global IPv6 users (June 2018). [24] However, most of these users are by virtue of large private players such as Reliance Jio, and smaller ISPs are yet to transition to IPv6 in India. Lack of smaller players making the shift can be attributed to a lack of clear guidelines by the government to facilitate this transition. Since the number of internet users in India is anticipated to increase massively in the near future and the pool of Ipv4 addresses on the verge of exhaustion, smaller Indian ISPs will also be compelled to deploy Ipv6. Therefore, it is imperative for the government to lay down useful policy guidelines to enable complete transition to the Ipv6 technology.

3.2.2 IPv6 in the World

Around the world, various countries have put in initiatives to encourage the transition to IPv6 amongst the organisations and application developers in their region. Some of the recent efforts by other governments are listed below:

- **Australia -** The Australian government has released a set of revised guidelines[25] in 2009, according to which, agencies should have IPv6 capable hardware and software platforms by 2012, and be able to operate dual-stack IPv4/IPv6 environments by 2015.

- **Japan -** The Japanese government established the ‘IPv6 Promotion Council’ in 2000 to encourage IPv6 adoption, promotion of R&D, and to provide training and operate an IPv6 test-bed. Many initiatives to promote IPv6 adoption have been launched, and the government has also issued a mandate requiring agencies to purchase hardware and software systems that support IPv6. Also, in March 2001, Japan established the “e-Japan Priority Policy Program,” which states – *‘it would realise an Internet environment enabled with IPv6 by 2005’*[26]. Japanese Telecommunications Company NTT became the world’s first Internet Service Provider (ISP) to offer internet on IPv6 to the public. Most of the ISPs in Japan are providing commercial IPv6 services these days. Other Asian countries like China and South Korea, are the leading countries in Asia as far as IPv6 network migration is concerned within the region, while countries such as Thailand, Malaysia, Sri Lanka and Indonesia are at an embryonic stage of IPv6 adoption and have recently started IPv6 initiatives with mandates for IPv6 adoption and transition setting a target within the year 2016[27].

- **Singapore -** The Infocomm Development Authority of Singapore (IDA) launched its ‘IPv6 transition programme in 2012’ to encourage IPv6 adoption, which continues to be ongoing. The programme is a national effort to address the issue of IPv4 exhaustion

[24] State of IPv6 Deployment 2018 | Internet Society – Available at: https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

[25] Australian Government Information Management Office: “A Strategy for the Implementation of IPv6 in Australian Government Agencies”, July 2009.

[26] http://www.v6pc.jp/en/index.phtml

[27] Sébastien Ziegler et all. (2013). IoT6 – Moving to an IPv6-Based Future IoT. FIA 2013, LNCS 7858, pp. 161–172, 2013

and to facilitate the smooth transition of the Singapore ICT ecosystem to IPv6. The IPv6 Transition Programme is a national effort spearheaded by IDA in its role as the national planner for Infocomm Development, to address the issue of IPv4 exhaustion and to facilitate the smooth transition of the Singapore Infocomm ecosystem to IPv6. Developed by the Singapore IPv6 Task Force, it involves a two-pronged approach to drive IPv6 adoption in the nation as well as encourage the efficient use of the remaining pool of IPv4 addresses to minimise the risks of depletion.

- **China -** China supports 49.5% of its network on IPv6[28] , and the Chinese Government launched the China Next Generation Internet project (CNGI), a five-year plan to empower the research community and the industry to conduct research and implementation of IPv6 in China. The programme is supervised and coordinated by eight ministries, including the China Reform and Development Commission, Ministry of Industry and Information Technology, Ministry of Education and China National Science Foundation Commission. Almost all significant ISPs in China participated in this programme. China Telecom, China Unicom, China Netcom (now merged with Unicom), China Mobile and China Rail-com (now merged with China Mobile) built indigenous IPv6 backbone networks based on dual-stack technologies[29]. Now, the IPv6 policy of China has mandated mobile internet, cloud computing and other new businesses to use IPv6[30]. Likewise, China Mobile is in the process of upgrading its entire network to IPv6 achieving targets of more than 3 million IPv6 users since 2016 and is promoting the use of IPv6 in 3G and 4G mobile internet as well[31].

- **Malaysia -** The Malaysian IPv6 Council developed the IPv6 Roadmap as a strategic implementation plan for IPv6 adoption and transition in Malaysia and proposed IPv6 enabled networks of ISPs by 2006, at e-Government Network by 2008 and in overall Malaysia by 2010. However, it was revised in 2010 with 2015 set as the deadline for a complete migration to an IPv6 enabled network in Malaysia. Malaysian Communications and Multimedia Commission (MCMC) is currently taking steps to make sure that all ISP's are ready to provide the IPv6 services[32].

- **France -** The French IPv6 Task Force has worked towards the transition to IPv6 in France. The v6 (IPv6) has been deployed over an internal network in France between sites of the France Telecom Research & Development since 1998. The carrier, France

[28] http://ipv6-test.com/stats/country/CN

[29] CNGI-CERNET2: an IPv6 Deployment in China. Available: http://www.sigcomm.org/sites/default/files/ccr/papers/2011/April/1971162-1971170.pdf

[30] Zhiqiang, Li, (2013). IPv6 Development in China. [online]. Available: http://conference.apnic.net/data/36/ipv6-in-china-lizhiqiang_1377575316.pdf

[31] Zhiqiang, Li, (2013). IPv6 Development in China. [online]. Available: http://conference.apnic.net/data/36/ipv6-in-china-lizhiqiang_1377575316.pdf

[32] MEWC, (2008). National Strategic IPv6 Roadmap. [online]. Available: http://www.nav6.org/Home/National%20Strategic%20IPv6%20Roadmap%20%5BLast%20Updated%2010%20June%202008%5D.pdf

Telecom, has deployed an IPv6 native backbone network to help customers to move forward[33].

- **Austria -** The ACONET (Austrian Academic Computer Network), the Austrian NRN (National Research Network) first started experiments with IPv6 in the late 1990s, and the Austrian IPv6 Task Force was established in 2004. Since then ACONET has gone on to provide academic institutions within Austria with IPv6 services[34]. Later on, Telecom Austria was involved in IPv6 related international projects like Global Communication Architecture and Protocols for new QoS services over IPv6 networks[35].

- **Finland -** A National IPv6 working group established in Finland in 2002 acted as the Finish IPv6 Task Force supported by the Finnish Communications Regulatory Authority. The group promotes the adoption of the IPv6 protocol in the national communications network, examining and monitoring the mechanisms necessary for transitioning to IPv6 and preparing the related guidelines to ensure interoperability of communications networks, equipment, and services[36].
-
- **USA -** The U.S. Federal Government recognised the importance of the adoption and transition to IPv6 in the year 2005 and pledged to generate the memorandum for transition planning for migration of US federal backbone networks by 2008. The Federal Chief Information Officers (CIO) Council with the Federal IPv6 Taskforce published the second version of the roadmap for IPv6 adoption in July 2012 as an update to the first version released in May 2009, with the purpose to help federal government agencies and industry leaders to integrate IPv6 in enterprise networks[37]. The US[38] government had announced an upgrade to their public-facing websites and services in September 2010, with a transition to native IPv6 support to be completed by 30 September 2012. The directive also required federal agencies to upgrade internal client applications that communicate with public internet servers to use native IPv6 by 30 September 2014.

[33] European Commission IPv6 Portal website, [online], available: http://www.eu.ipv6tf.org/PublicDocuments/IPv6_Commercial_Deployment_in_Europe.pdf

[34] ACONET, [online]. Available: http://www.aco.net/ipv6.html?&L=1

[35] IPv6 Cluster, IPv6 Research and Development in Europe, (2002). [online]. Available: http://www.consulintel.es/pdf/ipv6_research_and_development_in_europe.pdf

[36] Finnish IPv6 Task Force, [online], available: http://www.fi.ipv6tf.org

[37] U.S. IPv6 roadmap, (2012). Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government. [online], Available: https://cio.gov/wp-content/uploads/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf

[38] Memorandum for Chief Information Officers of Executive Departments and Agencies, Federal Government of US, “Transition to IPv6”, 28 September 2010

The position of different countries for the allocation of IPv4 & IPv6 addresses is summarised below.

Table 2: IPv4 & IPv6 Address Allocation to Different Countries as of June 2019[39]

Country	IPv4 Addresses Allocated	IPv6 Addresses Allocated
China	34,04,48,000	20,30,40,28,67,69,152
United States of America	1,60,61,18,400	19,89,07,30,15,93,088
Germany	12,32,64,384	8,98,63,63,52,06,144
United Kingdom	12,02,89,048	8,40,31,04,77,29,152
Russia	4,58,55,488	4,58,40,20,32,51,712
Japan	20,42,67,008	4,30,57,59,52,19,969
Australia	4,85,26,080	3,88,60,93,60,52,736
South Korea	11,24,62,336	2,25,78,64,34,02,753
India	4,10,76,224	71,55,44,57,92,768

4. IPv4 to IPv6 Transition

IPv6 transition is an eventuality that industry players will have to accept and manage proactively. As full IPv4 exhaustion draws closer, India will have to assist stakeholders like ISPs/Telcos and vendors to manage the IPv4 exhaustion while stepping up efforts to raise awareness and develop IPv6 competencies in the industry, and also create initial IPv6 supply and demand. The government also needs to monitor the transition closely and may introduce regulatory measures where necessary to ensure that businesses and consumers can enjoy seamless access to the Internet.

The transition from IPv4 to IPv6 is performed in stages as IPv6 is not backward compatible with IPv4. The IETF’s RFC2893 provides the complete specification of the transition mechanism from IPv4 to IPv6. The intermediate stages of the transition use technologies that can convert between IPv4 and IPv6 to manage the migration until all nodes are IPv6 enabled with IPv6 addresses. These technologies can be used to provide a smooth transition from IPv4 to IPv6. A description of the IPv4 to IPv6 transition mechanisms is provided in the appendix.

4.1 Government Initiatives for IPv6 Transition in India:

The recently unveiled National Digital Communications Policy (NDCP) – 2018[40] envisions ‘Broadband for All’ by 2022 thereby realising the role of the internet as a catalyst for socio-economic development of the country and also as an effective medium of various citizen-centric services in today’s information economy. Since the current version of Internet Protocol

[39] APNIC Deployment Reports https://labs.apnic.net/dists/

[40] National Digital Communications Policy (NDCP) – 2018, DoT, GoI – Available at: http://dot.gov.in/sites/default/files/Final%20NDCP-2018_0.pdf

(IPv4) has almost run out of addresses, the broadband revolution is required to ride on next-generation Internet Protocol (IPv6). The NDCP - 2018 recognises the futuristic role of IPv6 and seeks to achieve a complete transition to IPv6 in the country.[41]

The Department of Telecommunication (DoT) under the Ministry of Communications, Government of India, has undertaken initiatives for migration from IPv4 to IPv6 since 2010. Owing to the efforts taken by the DoT, a majority of the service providers in India are ready to handle traffic and offer IPv6 services at present. Despite the preparedness of major service providers, there are issues to be addressed in order to ensure complete migration of the ecosystem. Some of these issues include preparedness of the content providers, equipment vendors and end-user devices. The relevant stakeholders are being pursued by the DoT through extensive discussions and meetings to resolve the challenges above. Since the migration to IPv6 is an eventuality that has to be accepted and managed proactively, the government wants it to be done in a planned way. The DoT has stated that the migration of all payment gateways, banks, financial institutions, and insurance companies, including their websites should be completed at the earliest.[42]

Currently, India has 40 million IPv4 addresses against a user base of about 600 million data users[43]. There is a legitimate security requirement to provide a unique IP address to each individual data user. Since IPv6 is not backwards compatible with IPv4, the transition to IPv6 is likely to be a complicated, mammoth and long-term exercise. Therefore, in the short term both IPv4 and IPv6 are likely to co-exist. Furthermore, the DoT released the National IPv6 Deployment Roadmap in July 2010 which focused on educating the Indian stakeholders on issues related to IPv6 and providing methods facilitating transition towards IPv6. Even though the following policy decisions were taken, they were not implemented completely:

i. All major Service Providers will seek 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; and
iii. Formation of the IPv6 Task Force.

An India IPv6 Task Force Task Force headed by Secretary (T) was formed in December 2010 to plan, coordinate and drive the IPv6 adoption across the nation. This task force constituted a 3-tier structure with 2 Committees and 10 Working Groups. Each tier comprises members from different organisations/stakeholders in the public-private partnership (PPP) model. The structure and details of the Task Force are as under:

[41] Clause 2.2(c) of the National Digital Communications Policy: Ensuring the transition to IPv6 for all existing communications systems, equipment, networks and devices.

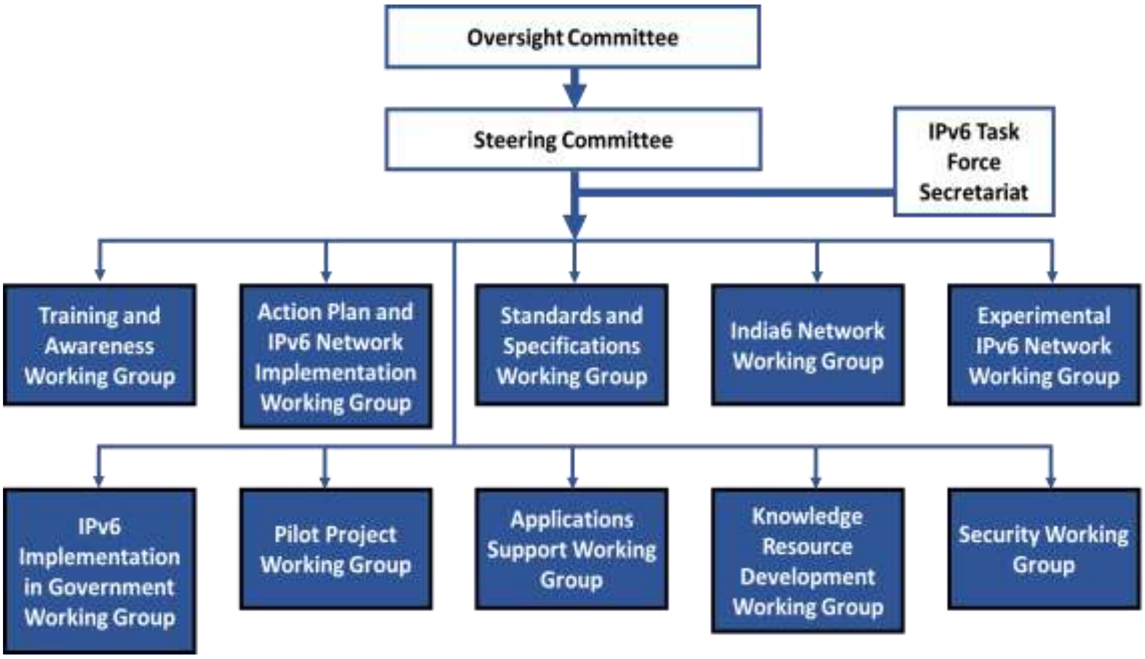
[42] National IPv6 Deployment Roadmap Version-II – Available at: http://dot.gov.in/sites/default/files/Roadmap%20Version-II%20English%20_1.pdf

[43] Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators, October – December, 2018, New Delhi, India, 4th April, 2019

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 the Secretary (T), DoT as its Chairman. It also has members from DoT, TEC, MeitY, C-DOT, PSUs like BSNL & MTNL, industry associations like CMAI, NASSCOM, COAI, AUSPI, ISPAI, ACTO, TEMA, and IPv6 India Forum along with representatives of various other 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 operations of the different Working Groups constituted under the Task Force for a timely and smooth transition in the country. The Steering Committee is headed by the Advisor (T), DoT and has members from DoT, TEC, MeitY, C-DOT, PSUs like BSNL & MTNL, various ministries of the Government, and industry associations along with representatives of multiple stakeholders. It is scheduled to meet every two months.

Figure 1: Structure of India's IPv6 Task Force


Oversight Committee
Steering Committee
IPv6 Task Force Secretariat
Training and Awareness Working Group
Action Plan and IPv6 Network Implementation 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

Source: Depart of Telecommunications, India

Working Groups – There are ten Working Groups with each one being responsible for specific activities associated with the IPv6 transition. A one-member organisation in each Working Group leads the group and is responsible for funding its events such as meetings, logistics, selection of members and the like. It is scheduled to meet at least once every month. The details of the working groups and their allotted functions are as follows:

Working Group	Tasks Allotted
WG 1 - Training & Awareness	- Hands-on training in association with APNIC and other organisations. - Training for nodal officers from the government. - Conducting workshops, seminars and conferences.
WG 2 - Action Plan & IPv6 Network Implementation	- Studying different network scenarios and coming up with action plans for individual service providers/organisations. - Service providers to be pursued for IPv6 implementation.
WG 3 - Standards and 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/organisation to build a “Transition Pipe” called “India6 network” which will 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, develop 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 through active participation of educational institutes. - Liaise with the Ministry of HRD to prepare course modules on IPv6 related issues and introduce them in educational institutes. - To promote research and development in the field of IPv6.
WG 9 - IPv6 Implementation in the Government Network	- Collaborate 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.

Additionally, a Standing Committee has been formed to safeguard proper co-ordination between DoT and MeitY. The Standing Committee consists of senior officials from DoT and MeitY as its members. Also, an IPv6 Core Committee has been created to address various IPv6 transition issues, reservations raised by various stakeholders and resolving the same regularly. The IPv6 Core Committee consists of members from DoT, MeitY, TEC and various industry representatives.

An Expert Group was also formed to provide various technical inputs to the Core Committee. Its purpose is to address various technical issues encountered during IPv6 adoption. Expert Group consists of the members from premium Indian institutes (like IITs, IISc, and NITs), World IPv6 Forum, NAv6 Malaysia and representatives of various stakeholders.

The DoT IPv6 Transition Initiatives in association with MeitY

The DoT has been working in collaboration with MeitY to safeguard smooth and seamless adoption of IPv6 and its co-existence with IPv4. In order to lead by example, it had been decided that the websites of all Government organisations maintained by NIC shall transition to IPv6 (dual-stack) by December 2012. Furthermore, it has taken the following initiatives in this regard:

National Informatics Centre (NIC) has made significant progress on this issue and has already completed the transition of a 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 the National Internet Exchange of India (NIXI) have been upgraded and made IPv6 ready. In addition, NIXI has conducted twelve IPv6 training/ workshops in association with APNIC. It has also sponsored training programs for 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, major requirements of IPv6 address blocks of Government organisations are handled by the NIC. Furthermore, the Computer Emergency Response Team India (CERT-In) has been approached for empanelment of IPv6 security audit teams.

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 MeitY in various areas including Centralised Building Management System, Intelligent Transport Systems, Rural Emergency Health Care, Tele-education / Distance Education, and Smart Grids. The National Knowledge Network (NKN) and other educational networks are to be on IPv6 to proliferate IPv6 in educational institutions and encourage them to develop novel applications exploiting the features of IPv6.

5. Challenges in IPv6 Transition

The following difficulties should be taken into account during the development of the IPv6 transition plan.

5.1. Maintaining Interoperability and Security

Organisations will need to maintain network interoperability as they transition away from today's IPv4-only environment. During the initial phases of transition, Organisations are likely to move to an environment to accommodate native IPv6 and encapsulated IPv6, in a largely IPv4 network leading to a ubiquitous dual-stack environment. As applications transition and the use of IPv4 diminishes, organisations will operate in an environment mainly over an IPv6 network. Hardware and software interoperability will be essential as these organisations move forward with their IPv6 plans and interconnect their networks across dual environments. Since maintaining interoperability and security for these types of evolving environments is the highest priority, the transition period should be kept minimal.

There are many possible combinations of technical IPv6 transition strategies. There are also several transition mechanisms (e.g. dual-stack, tunnelling, and translation) that organisations can choose from during transition, with more methods\ emerging from the technical community. The introduction of IPv6 on an enterprise-scale will introduce several challenges including scalability, integration, and security. In the near term, there is concern about creating vulnerabilities in existing IPv4 networks by deploying IPv6 and its transition mechanisms. This risk can be mitigated by development of an overall phased approach to IPv6 network transition which addresses end-to-end interoperability, performance, and security issues. Organisations may also want to consider controlling the use of IPv6 on IPv4 networks that carry classified traffic until the networks carrying unclassified traffic have been successfully transitioned and tested. An integrated and coherent strategy should be developed to allow IPv4 and IPv6 to operate on these networks using emerging IPv6 security products. Furthermore, in many cases, there will be an on-going need for interaction with IPv4 enclaves outside of the agency requiring transition mechanisms to be planned accordingly.

5.2 Security Considerations

Several security implications of adopting IPv6 within an organisation are provided below as initial guidance to identify a network security infrastructure plan within each organisation.

- Security applications infrastructure currently used on an IPv4 network will need to be replicated, with an expectation that the same level of assurance is provided in the IPv6 network. Examples of those applications include but are not limited to Intrusion Detection, Firewalls, Network Management of IP Packets, Virus Detection, Intrusion Prevention, Secure Web Services Functions.

- If end-to-end IPsec security is to be implemented, there will be a need to identify PKI, key management, and policy management infrastructures that meet the scalability and security verification requirements for intra-network communications (e.g. nodes, devices, and sensors).
- If end-to-end IPsec security is implemented, current network perimeter security infrastructure applications, e.g. firewalls and intrusion detection systems that depend on accessing and viewing IP transport data payloads must be aware that they will not be able to observe that part of the IP packet needing deployment of alternate mechanisms.
- If VPN tunnels are used to encapsulate IPv4 within IPv6, or IPv6 within IPv4 as a transition method for deployment:
    - The tunnel endpoints between the VPN should be secured as the traffic transits the VPN.
    - When an encapsulated IPv6 packet enters or leaves the VPN and Intrusion Detection is required, it should be understood that the Intrusion Detection application or other network security method used to permit a packet on that network, has been ported to IPv6, as previously identified.
- In addition to current methods to secure IPv4 wireless networks, wireless network access from IPv6 nodes requires in-depth security analysis for implementation when used with stateless auto-configuration.
- Seamless mobility with IPv6 is required to support the necessary security as identified by the organisation to permit secure access to the network, whether across the internal network or remotely from an external network.
- IPv6 on a network should not be turned on by default unless all network security infrastructures are implemented. (Note that some products may have IPv6 enabled out-of-the-box.)

With the current upgrading of organisations' technical environments, many products have IPv6 capabilities already. Many new threats and vulnerabilities are anticipated as attackers devote more attention to IPv6. As such, careful planning and additional care to operating in a dual environment will be needed to deal with potential new threats and must be addressed by the organisations accordingly. IPv6 can be implemented securely on a network, but the guidance above is essential to do it in the most secure manner possible.

6. Costs Associated with Transition to IPv6 Network

Transition costs are likely to be incurred on account of software and hardware, training, application porting, consulting services, and operational costs. IP networks today consist of a lot more than routers, switches, mobile phones, tablets and PCs. Security and building management systems, sensors and M2M devices all will require that we analyse them for their ability to support IPv6. Even though at present, most of the available equipment is IPv6 compatible. Therefore, it's critical to ensure that legacy applications and devices can co-exist with IPv6 Network.

IPv6 is to be phased into the organisations' infrastructure and applications through their lifecycle management processes. Organisations are expected to acquire IPv6 capability while upgrading infrastructure as part of the standard technology replacement lifecycle. The availability of transition mechanisms will allow organisations to replace only that equipment deemed necessary to facilitate IPv6 integration. As existing equipment is replaced with newer systems, native IPv6 capability will be part of the equipment's basic operating capabilities. Consequently, the cost of transition from equipment replacement should be significantly minimised.

Training and imparting skills to human resources will be an essential part of the integration process. The government will potentially need to make plans for nationwide training and creation of skilled staff. The specific cost of training each person will depend upon the role they play in the integration process, and it cannot be quantified at this point in time.

Professional services will be another cost of integration. These expert services may come in the form of transition planning assistance, development of a test plan, deployment assistance, and help desk support. Regardless of the type of services acquired, professional services are likely to be a component of any organisation's transition costs.

Also, as far as the Software and Applications for the IP Networks are concerned, they generally don't care about the IP protocol of the underlying network. But some do, such as real-time services using the Session Initiation Protocol (SIP). So, Vendors and developers of SIP-based applications must reconfigure their software/applications to support IPv6 information in the SIP header. All SIP-based applications must be ready for the transition to IPv6. This reconfiguration is likely to increase the overall costs of transition, and it is dependent on the type of software.

While IPv6 will reduce network administration costs in the long run if enterprises reorganise their networking structure and operating processes to take advantage of IPv6's capabilities and remove NATs from their networks.[44] For instance, the autoconfiguration feature available in IPv6 can simplify the connection of hosts and other devices to the Internet, thus reducing management overhead for network administrators. The vast number of addresses available under IPv6 could simplify and thereby reduce the costs of subnet management because each subnet could be given substantially more address space than the number of nodes that could be connected to it.

If adoption of IPv6 motivates an organisation to dispense with NATs, network administrators could more effectively use ping, traceroute, and other tools to diagnose network problems or to debug applications between pairs of hosts. Removal of NATs could also simplify the use of multivendor networking solutions. Furthermore, decreasing the number of processing functions in a network (e.g., by eliminating NATs) could reduce the number of components

[44] March Streck Interview supra note 82. The cost to upgrade to IPv6 and adjust a network to use the capabilities of IPv6 (e.g., remove NATs) could be very costly depending on the specific setup of a particular network.

that can fail, increase network resilience, and reduce management complexity and support costs.

To the extent that the administrative cost savings of IPv6 depend on the removal of NATs, however, organisations will incur operational costs as they begin making their network backbones IPv6-ready, so they are positioned to leverage the benefits of IPv6. But keeping in view the present status of India's IPv6 nodes/users, it doesn't appear to be a significant overhaul of the existing infrastructure. As has been explained in the preceding section, only some incremental changes will be required in addition to proper skilling and training of our Network Engineers which may incur some cost. However, training of resources should be treated as an investment rather than a sunk cost for network transition. The only requirement is that all this must be facilitated through a policy framework laid down by the Government.

7. Outlook and Policy Recommendations

Despite the recognition that IPv6 will eventually need to be adopted, planning around the transition has left a lot to be desired, and this is primarily due to the fact that existing users except few do not see any pressing need for IPv6 adoption.

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

- The lack of actual deadlines for those involved
- The fact that the current 'workarounds' of using NAT and Dynamic Host Configuration Protocol (DHCP) have been considered adequate to date
- Inadequate promotion of IPv6 to customers by the supply side of the market
- Failure to grasp the benefits of adopting IPv6, and therefore inability to recognise the incentives.
- Lack of core technical expertise in IPv6 domain.

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

The government and regulators may therefore need to encourage and incentivise the timely and efficient solution for faster transition and broader adoption of IPv6, with a move towards the co-existence of IPv4 and IPv6 – known as 'dual-stack' to minimise the impact of the exhaustion of IPv4 addresses on individual stakeholder groups and the consequential effects on their productivity.

The following solutions are proposed for accelerating the pace of transition and promoting the wider adoption of IPv6 in India:

i. Stricter monitoring of roadmap targets
ii. Independent audit of IPv6 adoption in India
iii. Capacity building at different levels in government and regulatory bodies
iv. Research & Development in IPv6 technologies
v. Establishing Centres of Excellence (CoE) to develop indigenous capabilites
vi. Skill Development in IPv6 core technologies
vii. Awareness campaigns
viii. Active participation of government in discussions related to Governance Model of DNS Root Server
ix. Creation and trials of IPv6 only Root Server in India

These recommendations are described below:

i. **Stricter monitoring of roadmap targets:**
The 'National IPv6 Deployment Roadmap Version-II' should adopt a stringent monitoring mechanism with the progress of different stakeholders reviewed periodically to ascertain the path of IPv6 adoption in the country. The statistics collected through the monitoring mechanism will help in identifying loopholes and make any interventions that may be required. This monitoring should be handled by the DoT, which has a division engaged in dealing with new technologies.

ii. **Independent audit of v6 adoption in India:**
This should be done by an independent primary research organisation to ascertain that rate of IPv6 adoption in India for policymakers and regulators. As such, it is suggested that the regulator (TRAI) should engage some independent research agency to implement this, as is done by them in many other fields. The audit report must be used to understand existing gaps and a focused strategy must be used to ramp up adoption of IPv6 technology. Furthermore, the report must also analyse the efficacy of measures undertaken by the government to increase adoption of IPv6 in India.

iii. **Capacity building at different levels in Government and Regulatory Bodies:**
In order to develop an implementable policy, the Government needs to create in-house competence by inducting specialists from industry & academia. The existing members of the divisions in the government dealing with new technologies including IPv6, have to be provided with training at global level making use of the facilities of international organisations like the ITU, IEEE, IETF, CTO, and ICANN.

iv. **Research Development in v6 technologies in Academia:**
R&D is the core area where significant action is required to develop in-country expertise in the underlying technology and IPv6 as well as Root-Servers, by creating dedicated Research Chairs/ Professorships and also Masters/ Doctoral programmes funded by the government. Many countries including the US, Japan and Europe have invested significantly in developing IPv6 capabilities. In India, this can be done by establishing CoE in technical institutions of national repute in the country such as IISc,

IITs, DRDO, CDAC and CDOT. The government has already taken similar steps for 5G as well as AI & Cloud Technologies which can be an ideal role model to be replicated.

v. **Establishing CoE to develop indigenous capabilities:**
Relevant Ministries under the aegis of the Government of India must be given a mandate to establish CoEs predominantly focusing on developing competence in IPv6 technology among network operators, businesses and companies. Furthermore, the CoEs may also provide stakeholders with requisite assistance to handle technical issues while transition as well as deployment. Creating a facility which in addition to training skillforce also provides technical assistance will encourage adoption among companies.

vi. **Skill Development in IPv6 core technologies:**
Under the NSDC framework, IPv6 grassroots level core technologies should also be used as candidate technologies for computer technicians/ Engineers to make them job-ready for the field of IPv6 transition. Some Sector Skill Councils (SSCs) like IT/ITES SSC & Electronic SSC can be tasked with this job. For this SSC's will be required to create National Occupational Standards (NOS) to carve out the course contents along with time required to finish a course for different job roles at all levels ranging from Technicians, Engineers, Trainers and Research Scholars.

vii. **Awareness Camapaigns:**
Even though, the government has recognised the importance of transitioning to Ipv6, the market is still far from complete transition to Ipv6. This lackadaisical approach is also on account of lack of awareness among relevant stakeholders which includes *inter alia* network operators, companies and technical staff. In order to bridge this gap, Meity and DoT are recommended to undertake awareness campaigns for relevant nodal officers for the government. Furthermore, regular workshops, seminars and conferences may be conducted for government personnel as well as other pertinent stakeholders.

viii. **Engagement at International Fora**
The government should actively participate in ICANN's as well as other international discussions on Proposed Governance Model for the DNS Root Server System. Expertise in the new technologies' domain can be acquired through active participation in global forums/symposiums organised by international bodies. ICANN can provide an ideal platform for such interactions and exchange of knowledge. The Government of India is always called upon to nominate the country representatives to such meetings. One of the topics under current deliberations that is relevant for the IPv6 transition is the 'Proposed Governance Model for DNS Root Server System'. It is recommended focussed approach should be adopted to actively participate in these meetings to rise towards thought leadership position.

ix. Creation and trials of v6 only Root Server (6ORS) in India:

The government should aim to experiment with the creation of an independent root-server for IPv6 *(ref: IETF RFC 7720 - DNS Root Name Service Protocol and Deployment Requirements).* This will help the country's experts to get hands-on experience of creating and running a root-server which is a critical technology for controlling and managing the internet. The IETF RFC 7720, referred above, provides for functional framework for the same. One of the CoE suggested in para (iv) above, should be assigned the task of carrying out research related to this RFC. The trials of 6ORS will also require involvement of ISPs to run real-time traffic through their network and experiment with the 6ORS platform to test the concept. This setup may need dedicated funding from the government.

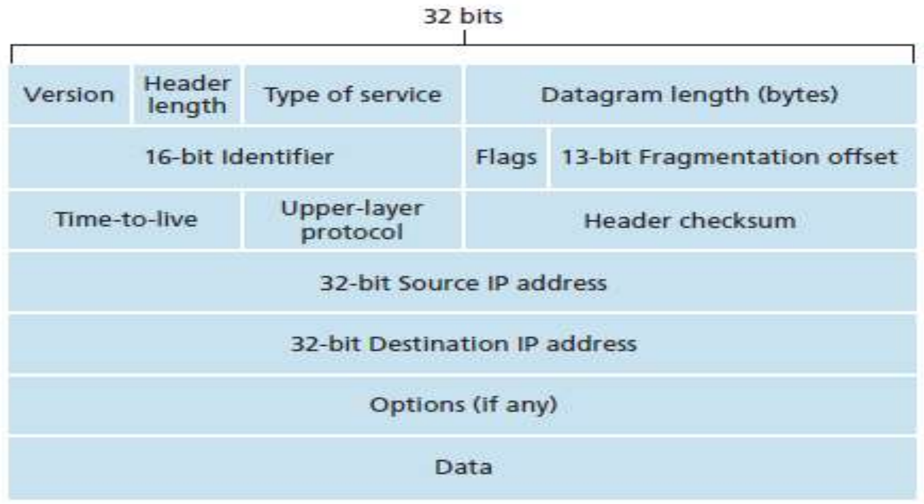
Appendix

A.1 Comparison between IPv4 and IPv6

The Internet Engineering Task Force (IETF), responsible for defining IP standards, did not consider issues such as the number of address spaces and data security in IPv4 standards that were developed during the nascent stages of the internet. The IETF created new versions of IP and IPng, now known as IPv6, to overcome the shortcomings of IPv4 and provide new functions that support the developments around the internet.[45]

As IPv4 addresses become scarce, Internet Service Providers (ISPs) have managed to keep up network connectivity by supporting the wider use of Network Address Translation (NAT) in CPE devices and the ISP's access networks. However, a more strategic solution is to undertake a transition to IPv6. Unlike IPv4 that allocates 32 bits for an IP address, IPv6 allocates 128 bits for an IP address. As a result, IPv4 provides 2^{32} (4,294,967,296) IP addresses, which is lower than the population of Earth. In contrast, IPv6 provides 2^{128} (340,282,366,920,938,463,463,374,607,431,768,211,456) IP addresses.

Figure 2: IPv4 Header Diagram



Source: Google – electronicspost.com

An Internet Protocol version 4 packet header (IPv4 packet header) contains application information, including usage and source/destination addresses. IPv4 packet headers contain 20 bytes of data and usually are 32 bits long. A packet is a network communication data unit containing fixed or variable lengths. A single packet contains three portions: a header, a body and a trailer. A 20-byte header contains 14 fields, of which 13 are mandatory fields that hold specific information such as application, data type, source/destination addresses, frame length, and communication expiry duration for acknowledgement. The data section is not followed by any checksum to validate the data packet or any other footers. The details of an IPv4 packet

[45] What is IPv6? Available at: http://IPv4.opus1.com/IPV6/whatisIPV6.html

are outlined in Figure 1 below. The header field descriptions of an IPv4 packet are described in the section.

IPv4 Packet Header Field Descriptions

Version – This is a 4-bit long field that indicates the version of the internet protocol. The value of the version field is set to 4 in case of IPv4.

Internet Header Length (IHL) – This is a 4-bit field that can take values between 5 and 15, indicating the number of 32-bit words in the header.

Differentiated Services Code Point (DSCP) – It is a 6-bit field indicating the type of service (ToS). It is defined as per the TFC 2474 and used for different use cases such as to indicate low delay, high throughput, or reliability of the transmitted data for applications like real-time data streaming or VoIP.

Explicit Congestion Notification (ECN) – It is a 2-bit field that allows for end-to-end notification of network congestion seen in the route without dropping any packets.

Total Length – This is a 16-bit field indicating the total length of the IP packet in bytes. This length includes the length of the IP header along with the length of the IP payload or data and can take on values between a minimum of 20 bytes and a maximum of 65,535 bytes.

Identification – It is a 16-bit field used as a unique identifier for an IP packet and its different fragments in case of fragmentation during the transmission.

Flag – It is a 3-bit flag that helps to find out if the packets can be fragmented or not.

Fragment Offset – It is a 13-bit long field that indicates the exact position of fragmentation of the data packets.

Time to Live (TTL) – It avoids looping in the network and helps to limit the packets that can cross the router.

Protocol – It defines the next layer protocol.

Header Checksum – This field is 16-bits long and is used to check if the received packets are error-free.

Source Address - It is the address of the sender or the source.

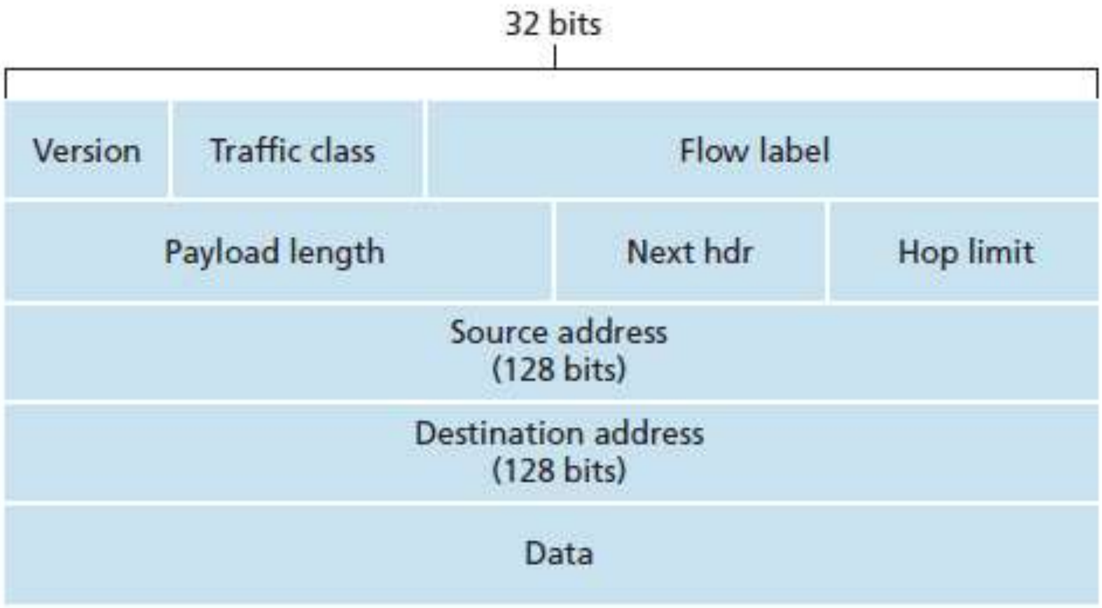
Destination Address- It is the address of the receiver.

Option - It is used only when the value of IHL is greater than 5. These may contain values such as security, timestamp, and record route.

An IPv4 address is composed of 32 binary bits. These 32 binary bits are divided into four octets of 8-bits each separated by a dot, e.g. 82.50.69.83. The IPv4 address consists of two parts: a network number and a host number. The network number is used to determine the location of the host computer network, and the host number identifies the precise computer in the network.[46]

IPv6 is the latest version of the Internet Protocol and is not directly compatible with its predecessor, the IPv4. Each IPv6 address has a length of 128 bits, which allows a vast number of IPv6 addresses compared to the number of IPv4 addresses which have a length of 32 bits. In addition to the ample address space, which was the main driver for IPv6 standardisation in 1998, it also brings several novel features over IPv4 such as fields like flow label, next header, as well as the exclusion of the header checksum. The format of the IPv6 header is shown below, and the header field descriptions are provided in the text box.

Figure 3: The IPv6 Header Format



Source: Google – electronicspost.com

Generally, IP-based networks are classified into IPv4 and IPv6 depending on the IP protocol version used. Their behaviour differs according to the features of each protocol version. Therefore, clarifying the differences between IPv4 and IPv6 is very useful for identifying the operations of IPv4 and IPv6, which influence network design and service operations.

[46] IPv4 Addressing. Available at: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd379547(v=ws.10)

IPv6 Packet Header Field Descriptions

Version – It specifies the version of the Internet Protocol, and its value is set to 6 for IPv6.

Traffic Class – It holds two values consisting of 6-bits and 2-bits. The 6-bit values are used for differentiated services to classify the packets, while the 2-bit values are used for explicit congestion notification (ECN).

Flow Label – The 20-bit flow label provides for real-time application and is used to detect spoofed packets.

Payload Length – The 16-bit payload length contains the length of the data fields in bits.

Next Header – The 8-bit selector specifies the transport layer protocol and specifies the type of next header.

Hop Limit – The 8-bit unassigned integer is decremented by 1, and the data packet is discarded when the counter reaches 0.

Source Address – The 128-bit source address indicates the originator.

Destination Address – The 128-bits source address indicates the recipient of the packet.

IPv6 supports Quality of Service (QoS) per-flow on the network layer. A flow is a sequence of all related packets sent from a source to a destination. This means that the flow-based QoS (which is generally determined by losses, packet delay, and bandwidth given in bits/s) will be easier to implement on the Internet.

As discussed in the preceding sections, IPv4 and IPv6 addresses are used to identify machines connected to a network. While they may be the same in principle, however, there are inherent differences in both these versions. It is crucial to note that IPv6 is much more than an extension of IPv4 addressing, and it offers many enchantments over IPv4. A detailed comparison of IPv4 and IPv6 is provided in Table 1 below:

Table 3: A comparison of the IPv4 and the IPv6 features.

Comparison	IPv4	IPv6
IP Address Size	32-bits	128-bits
Addressing Method	Numeric Address. Decimal digits separated by a dot [.].	Alphanumeric Address. Hexadecimal digits separated by a colon [:].
Example	12.244.233.165	2001:0db8:0000:0000:0000:ff00:0042:7879
No. of Header Fields	12	8

Comparison	IPv4	IPv6
Header Field Length	20	40
Checksums	Has checksum fields	Does not have checksum fields
Type of Addresses	Unicast, Broadcast, and Multicast.	Unicast, Multicast, and Anycast.
Address Classes	Five Classes – A to E.	lPv6 allows storing an unlimited number of IP Address.
Configuration	Requires configuration before use.	Network configuration is optional and based on device function as host, server or router.
Variable Length Subnet Mask (VLSM)	Supports VLSM.	No support for VLSM.
Fragmentation	Fragmentation is done by sending and forwarding routes.	Fragmentation is done by the sender.
Routing Information Protocol (RIP)	Support for RIP by the routed daemon.	No support for RIP. IPv6 uses static routes.
Network Configuration	Networks need to be configured either manually or with DHCP.	Supports automatic IP configuration capability.
Address Mask	Used for the designated network from the host portion.	Not used.
Simple Network Management Protocol (SNMP)	Supports SNMP for system management.	Has no support for SNMP.
Mobility & Interoperability	Limited interoperability and mobility due to constrained network topologies.	Ease of mobility and interoperability with embedded network devices.
Security	Optional. Application Dependent.	Mandatory. Built-in Security.
Packet Size	576 bytes	1208 bytes
Packet Fragmentation	Routers and Sending Host Allowed	Only Sending Hosts Allowed
Packet Header	Does not identify packet flow for QoS handling, including checksum options.	Packet head contains the Flow Label field that specifies packet flow for QoS handling
DNS records	Address (A) records, maps hostnames	Address (AAAA) records, maps hostnames
Address Configuration	Manual or via DHCP	Stateless address auto-configuration using Internet Control Message Protocol (ICMP) or DHCP
IP to MAC Resolution	Broadcast Address Resolution Protocol (ARP)	Multicast Neighbour Solicitation

Comparison	IPv4	IPv6
Local Subnet Group Management	Internet Group Management Protocol (GMP)	Multicast Listener Discovery (MLD)
Optional Fields	Has Optional Fields	Does not have optional fields but extension headers are available.
Dynamic Host Configuration Server (DHCS)	Clients are given dynamic addresses by a DHCS at the time of connecting to a network.	Clients are provided with a permanent address, eliminating the need for a DHCS.
Mapping	Uses ARP to map to MAC address	Uses Neighbour Discovery Protocol (NDP) to map to MAC address
Mobile Device Combability	Not suitable for mobile networks.	Better suited to mobile networks.

A.2 Salient Features of IPv6

IPv6 evolved as a result of several proposals and working groups under the Internet Engineering Task Force (IETF) over the past 20 years[47]. IPv6 retain some features of IPv4 while also providing additional services and capabilities. Some features of the IPv6 protocol are briefly explained as follows:

1. Large Address Space:

IPv6 uses 128-bit addresses, represented with eight 16-bit groups of four hexadecimal digits, which allows it to address up to 2^{128} unique devices on the network[48]. The IPv6 addresses are divided into two logical parts, a 64-bit network address and a 64-bit host address. Furthermore, IPv6 does not use address classes and instead categorises addresses into three basic types as follows[49:]

- **Unicast:** This is an identifier to a single interface in the network.
- **Multicast:** This is an identifier to a set of network interfaces. A data packet addressed to a multicast address will be delivered to all addresses in the set.
- **Anycast:** This is an identifier for a set of network interfaces, which may belong to different nodes. A data packet sent to a destination anycast address is delivered employing routing to the nearest nodes in the set as per defined routing metrics.

[47] Siddiqui, Aftab (17 July 2017). "RFC 8200 – IPv6 has been standardized" Available at: https://en.wikipedia.org/wiki/IPv6#cite_note-2

[48] RFC 4291 - IP Version 6 Addressing Architecture – Available at: https://tools.ietf.org/html/rfc4291

[49] IPv6 Addressing White Paper – Cisco – Available at: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPv6_WP.pdf

2. Header Format:

The IPv6 header is simpler and robust in comparison to the IPv4 header, which is complicated and requires maintaining large routing tables by the routers, thereby increasing routing costs. The IPv6 headers are processed more efficiently at the intermediate routers without a need for parsing through headers or computation of network-layer checksums or even fragmentation and reassembly of data packets. This efficiency allows for a reduced processing overhead for routers, making for simpler hardware and faster processing of data packets at a lower processing cost.

3. Network Layer Security (IPSec):

IPv6 includes packet encryption, i.e. Encapsulated Security Payload (ESP) and addresses authentication header (AH). This makes it more secure than its predecessor (IPv4) that does not incorporate any significant security features.

4. Quality of Service (QoS):

IPv6 header includes new fields such as traffic class and flow label that prioritise time-sensitive applications and result in low latency. Furthermore, QoS in IPv6 is also supported when the packet/payload is encrypted through IPSec. In comparison, the QoS in IPv4 relies on the type of service and has no way to differentiate between data payloads that are time-sensitive (e.g. audio and video streaming) and those that are not (e.g. regular file transfer). The issues of fragmentation, control overhead and inefficient routing in IPv4 result in high latency. Also, the identification of the payload uses the TCP or UDP port and is not possible when the IPv4 packet is encrypted.

5. Extensibility:

IPv6 is extensible for new features with the addition of extension headers after the IPv6 header. On the other hand, IPv4 can only support 40 bytes of options, while the size of IPv6 is only constrained to the size of the IPv6 packet.

6. Stateless and Stateful address configuration:

IPv6 supports both stateful address and stateless address configuration, which ultimately helps in simplifying host configuration. Stateful configuration is an address configuration in the presence of a DHCP server, while stateless address configuration is an address configuration in the absence of a DHCP server. Hosts on a link automatically configure themselves with IPv6 addresses for the link (link-local addresses) using stateless address configuration.

7. Efficient and Hierarchical Address Configuration:

IPv6 addresses are designed to create an effective routing infrastructure which is based on the common occurrence of multiple levels of ISPs. IPv6 network allows hosts to auto-configure their IPv6 addresses, based on network prefixes advertised by routers.

8. Inherent Mobility Support:

Routing is based on the subnet prefix in a packet's destination IP address. Consequently, packets that are destined for a mobile node do not reach it when it is not attached to the node's home link. The home link is the link where the node's home IPv6 subnet prefix exists. IPv6 mobility allows a mobile node to move from one link to another link without changing the mobile node's IP address. Also, it assigns an IP address to the mobile node within its home subnet prefix on its home link. This address is known as the node's home address.

A.3 IPv4 to IPv6 Transition Mechanisms

The IPv4 to IPv6 transition is handled through different intermediate mechanisms specified by the IETF RFC2893 that convert between IPv4 and IPv6. These mechanisms are as follows:

- Dual IP Layer
- Tunnelling of IPv4 over IPv6
- Translators

Dual IP Layer: A dual IP layer allows IPv6 nodes to be compatible with IPv4 nodes by providing a complete IPv4 implementation on an IPv6 network. This methodology is used by IPv6 nodes that communicate with both IPv4 and IPv6. These nodes can send both the IPv4 and the IPv6 packets depending upon the endpoints, i.e. they send IPv4 packets to IPv4 nodes and IPv6 packets to IPv6 nodes.

Limitations: In a dual-stack exchange, the devices are configured mostly only one stack, with the devices forwarding to dual-stack routers and then back to the same single-stack segment resulting in insufficient bandwidth across different parts. To fully implement an effective dual-stack, IPv6 needs to be activated in all network elements with there being significant costs involved in the redesign of the existing networks.

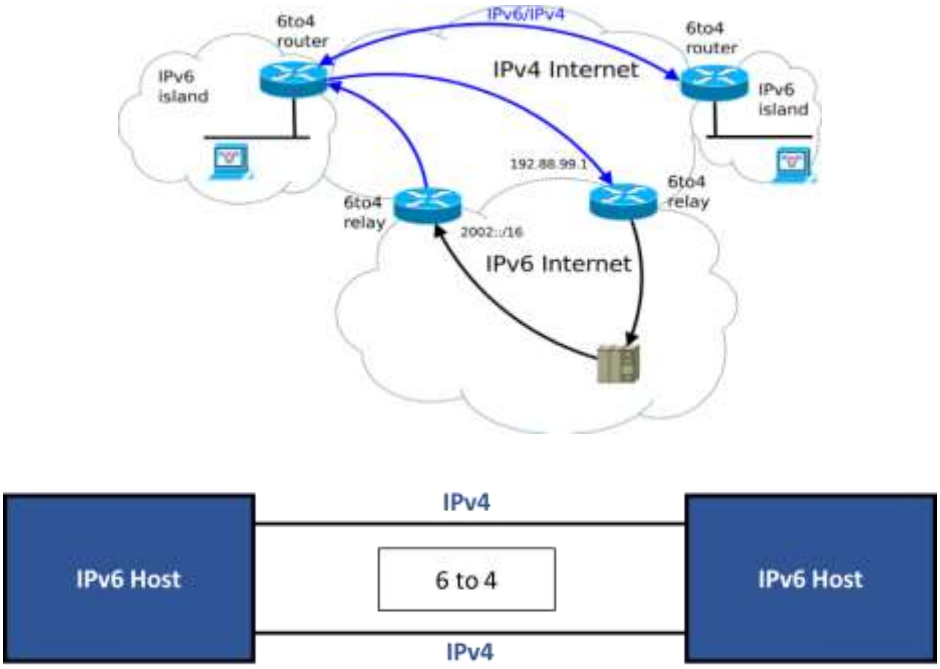
Tunnelling of IPv6 over IPv4: This is amongst the most basic techniques that can be deployed for allowing operation of two or more protocol versions on the same network. This technique involves the encapsulation of IPv6 packets within IPv4 header. A tunnel is a link between two IPv4 endpoints that must be configured by specifying the IPv6 destinations for which the packets are to be encapsulated and the remote IPv4 endpoint to which they must be sent. The following tools are used for tunnelling:

i. **6 to 4 Tunnelling (RFC 3056)[50]:** It is a method of constructing the IPv6 address directly from the IPv4 address. This mechanism enables sites to communicate over the IPv4 internet without using explicit tunnels while still communicating with IPv6 relay routers. The 6 to 4 tunnelling treats IPv4 internet as a unicast point-to-point link layer and specifies an encapsulation mechanism for transmitting IPv6 packets using the prefix. This mechanism is implemented entirely in border routers and is thus becoming a standard feature of router software. A diagram presenting the 6 to 4 tunnelling technique is provided in Figure 4 below.

Limitations:

- There are potential issues with delay and latency through the tunnel.
- The tunnel destination point is unknown.
- Additional CPU load is required for encapsulation and de-capsulation.
- There is no built-in security[51].
- Sometimes has to be manually configured
- IPv4 packets to broadcast, multicast and loopback address must not be sent through the tunnel.

Figure 4: The 6 to 4 Tunnelling Technique

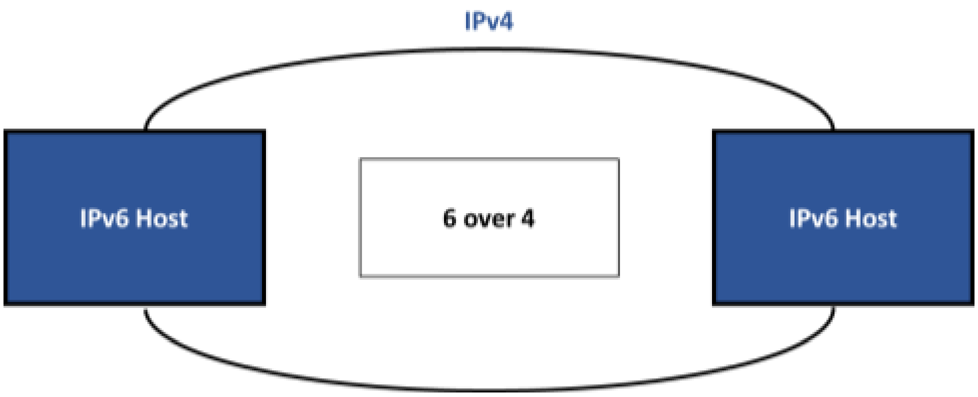


[50] IETF RFC – 3056 Connection of IPv6 Domains via IPv4 Clouds – Available at: https://tools.ietf.org/html/rfc3056

[51] Sellers, C. 2009. IPv6 Transition Mechanisms and Strategies. Available at: http://IPv4.rmv6tf.org/wp-content/uploads/2012/11/Chuck-Sellers-090421-IPV6-Transition-Mechanisms-Sellers1.pdf.

ii. **6 over 4 Tunnelling (RFC 2529)[52]:** This mechanism facilitates IPv6 connectivity within a site that lacks any IPv6 infrastructure. It describes the frame format for IPv6 packets as well as the method of forming IPv6 link-local addresses over IPv4 multicast domains. It also allows IPv6 hosts to become functional if at least one IPv6 router is located in the same domain. This technique is helpful for sites that still do not have IPv6 networks but wish to deploy one. 6 (IPv6) over 4 (IPv4) tunnelling has received limited support from the major vendors, with only two companies, Microsoft and Nokia, having implementations.

Figure 5: The 6 over 4 Tunnelling Technique



iii. **IPv6 Tunnel Broker (RFC 3053)[53]:** This technique uses dedicated servers that can automatically configure tunnels on behalf of users, reducing the management load on network administrators. It is predominantly suitable for connections between small users and an IPv6 Internet Service Provider. The tunnel broker has received support from the industry as this tool does not belong to the networks and the ISPs instead deploy tunnel brokers as a service to others.

Translators: As IPv4 and IPv6 packets are not directly compatible, translators that translate IPv4 packets into IPv6 ones and vice versa are used in the network. However, translators tend to slow down the network speed. The translation between IPv4 and IPv6 can take place at three levels, namely, the IP level, the transport level, and the application level. These are described as follows:

- **IP-Level Translation** involves the conversion of one header to another and is the simplest and the fastest mode of translation.
- **Transport-Level Translation** involves the translator works only as a relay, working on TCP/UDP flows.

[52] IETF RFC – 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels – Available at: https://tools.ietf.org/html/rfc2529

[53] IETF RFC – 3053 IPv6 Tunnel Broker – Available at: https://tools.ietf.org/html/rfc3053

- **Application-Level Translation** acts as Application Level Gateway (ALG) and is the most complex form of translation.

Following two methods are usually employed with translated IPv6 networks. These include:

i. **Network Address Translation - Protocol Translation (NAT-PT) -** NAT was instituted in the 1990s to remedy the exhaustion of IPv4 addresses before IPv6 products were developed[54]. This feature led users to overlook the complexity that NAT introduced, its trade-offs, and its effects on applications and connectivity. The NAT-PT method enables the translation of an IPv4 network address into an IPv6 network address and vice versa either by static or dynamic configuration. For those familiar with more typical NAT implementations, the operation is very similar but includes a protocol translation function. NAT-PT also ties in an Application Layer Gateway (ALG) functionality that converts the DNS mappings between protocols.
ii. **NAT64 -** One of the main limitations to NAT-PT was that it tied in ALG functionality that was considered a hindrance to deployment. The NAT64 supports both stateless address and stateful address configuration which ultimately helps in simplifying host configuration, keeping track of bindings and enabling one-to-many functionality. NAT64 also came with DNS64, both of which are configured and implemented separately.

The use of translators is fraught with several limitations and challenges, some of which are as follows:

- They are not expected to be used widely as they slow down packet flow.
- They do not allow the network to exploit specific capabilities of either protocol.
- They act as a redundant channel in online communication over the internet[55].

[54] The Changing Foundation of the Internet: Confronting IPv4 Address Exhaustion - The Internet Protocol Journal, Volume 11, No. 3 – Available at: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-41/113-ipv4.html

[55] Sellers, C. 2009. IPv6 Transition Mechanisms and Strategies. Available at: http://IPv4.rmv6tf.org/wp-content/uploads/2012/11/Chuck-Sellers-090421-IPV6-Transition-Mechanisms-Sellers1.pdf.

References

APNIC website. [online]. Available: http://labs.apnic.net/ipv4/report.html

JPNIC, Analysis and Recommendations on the Exhausting of IPv4 address space. [online]. Available: https://www.nic.ad.jp

Government of Nepal (2004), Telecommunication Policy 2004. (M. o. Communication, Ed.). [online]. Available: www.nta.gov.np/en/component/joomdoc/Policies/TelecomPolicy_2004.pdf

Mekonnen K and Abdulkadir T (2013), IPv6 Migration Framework – Case of Institutions in Ethiopia. HiLCoE Journal of Computer Science and Technology.

Amer Nizar Abu Ali, (2012), Comparison study between IPV4 & IPV6. International Journal of Computer Science Issues, ISSN (Online): 1694-0814, www.IJCSI.org

Gadgets usage statistics website, [online]. Available: http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

Dawadi BR, Joshi SR and Khanal AR (2015), Service Provider IPv6 Network Migration Strategies. Journal of Emerging Trends in Computing and Information Sciences.

Thomson S and Narten T (1998), IPv6 Stateless Address Auto-configuration, RFC2462

Conta, A., & Gupta, M. (2006). Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. RFC4443

http://www.v6pc.jp/en/index.phtml

Government of India, (2010). National IPv6 Deployment Roadmap Version I. [online], Available: http://www.dot.gov.in/sites/default/files/National-IPv6-Deployment-oadmap.pdf%201.pdf

Government of India, (2013). National IPv6 Deployment Roadmap Version II. [online], Available: http://www.dot.gov.in/sites/default/files/Roadmap%20Version-II%20English%20_1.pdf

http://ipv6-test.com/stats/country/CN

Zhiqiang, Li, (2013). IPv6 Development in China. [online]. Available: http://conference.apnic.net/data/36/ipv6-in-china-lizhiqiang_1377575316.pdf

MEWC, (2008). National Strategic IPv6 Roadmap. [online]. Available: http://www.nav6.org/Home/National%20Strategic%20IPv6%20Roadmap%20%5BLast%20Updated%2010%20June%202008%5D.pdf

European Commission IPv6 Portal website, [online], available: http://www.eu.ipv6tf.org/PublicDocuments/IPv6_Commercial_Deployment_in_Europe.pdf

ACONET, [online]. Available: http://www.aco.net/ipv6.html?&L=1

IPv6 Cluster, IPv6 Research and Development in Europe, (2002). [online]. Available: http://www.consulintel.es/pdf/ipv6_research_and_development_in_europe.pdf

Finnish IPv6 Task Force, [online], available: http://www.fi.ipv6tf.org

Danish IPv6 Taskforce, [online]. Available: http://www.ipv6tf.dk/home

UK IPv6 Council, [online]. Available: http://www.ipv6.org.uk

U.S. IPv6 roadmap, (2012). Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government. [online], Available: https://cio.gov/wp-content/uploads/downloads/2012/09 /2012_IPv6_Roadmap_FINAL_20120712.pdf

NTA MIS Reports. [online]. Available: http://nta.gov.np/en/mis-reports-en

IPv4 Addressing. 2015. IPv4 Addressing. [ONLINE] Available at: https://technet.microsoft.com/en-us/library/dd379547(v=ws.10).aspx

IBM. Comparison of IPv4 and IPv6. [ONLINE] Available at: https://IPv4-01.ibm.com/support/knowledgecenter/ssw_ibm_i_72/rzai2/rzai2compIPV4IPV6.htm

Graziani. R. 2012. IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6. 1 Edition. Cisco Press.

training.apnic.net. 1800. IPv4 to IPv6 Transition. [ONLINE] Available at: https://training.apnic.net/docs/eIP603_Transition.pdf

Sellers, C. 2009. IPv6 Transition Mechanisms and Strategies. [ONLINE] Available at: http://IPv4.rmv6tf.org/wp-content/uploads/2012/11/Chuck-Sellers-090421-IPV6-Transition-Mechanisms-Sellers1.pdf

Das, K. Network Address Translation (NAT) Pros & Cons. Network Address Translation (NAT) Pros & Cons, [Online]. Available at: http://IPv6.com/articles/nat/NAT-Pros-and-Cons.html

Cisco. NAT-PT for IPv6. [ONLINE] Available at: http://IPv4.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html

IP Addresses. 2013. IP Addresses. [ONLINE] Available at: http://www.itproportal.com/2013/07/02/ip-addresses-how-they-shaped-the-past-of-the-internet-and-what-they-will-influence-its-future/

IETF. 2010. Problem Statements of IPv6 Transition of ISP. [ONLINE] Available at: https://tools.ietf.org/html/draft-lee-v4v6tran-problem-02

Internet Engineering Task Force. 2011. Broadband Service Provider Use Case. [ONLINE] Available at: http://www.watersprings.org/pub/id/draft-tian-v4v6tran-broadband-sp-usecase-00.txt