Volume No.03, Special Issue No. 02, February 2015 ISSN (online): 2348 – 7550

IPV6 DEPLOYMENT - BENEFIT & OPPORTUNITIES IN INDIA WITH WORLD-WIDE EXPERIENCES

Shivendra Gurha

Department of Computer Application, P.D.M.P.G. College, Farrukhabad, (India)

ABSTRACT

The current standard protocol, IPV4, has reached its limit in terms of addressing possibilities, being limited by the 32-bits addressing scheme. Its successor, IPV6, had been devised since the mid 1990's. In addition to handling the address limitations, IPV6 also includes a number of improved features, making it superior to IPV4 in several aspects. However, its deployment has taken much longer than expected. This paper presents how the design IPV6 improved over IPV4, the additional benefits of the new design, and challenges faced for the deployment of IPV6. It then outlines the deployment strategies adopted by different countries. It finally discusses how India can benefit from the IPV6 deployment and what lessons it can draw from deployment experiences obtained elsewhere.

Keywords Addressing Scheme, Deployment, IPV4, IPV6, Tunnelling.

I. INTRODUCTION

IPV4 has been the standard protocol over the Internet for more than two decades. It has proven to be robust , easily implemented and interoperable and had stood the test of scaling an internetwork to a global utility of the size of today's internet [Davies, 2008]. However, in spite of this, IPV4 has serious addressing, routing and security limitations, that had been identified since the mid 90's [Melford, 1997]. Its use of 32-bits addresses is a major limitation in the number of devices that can have an IP address and is a major hurdle for end-to-end communication in ubiquitous computing and the exponential growth of devices that can connect to the Internet. Additionally, the classes A,B and C address allocation is inherently inefficient and besides addresses have been distributed in an inequitable way, resulting in a bias with more than 70% of the global IPV4 addresses belonging to organizations in the US from the early days [Hagen, 2004].

The next IP generation, IPV6, has been proposed since the mid 90's [Hiden, 1996] and has been quite widely deployed since. It has major technical advantages, such as a virtually inexhaustible number of IP address (5 x1028 for each of the 6 billion persons in the world today). However, the deployment of has a price tag and the need and merit of its deployment has continuously been debated, resulting in a large number of organizations showing reluctance to completely change to IPV6. This explains why the globe is not fully IPV6 yet. There is the large base of IPV4 infrastructure that already exists and the large base of IPV4 applications that may need to be IPV6-enabled [Bouras, 2005]. Thus researchers have tried to address the limitations in number of addresses through alternative solutions such as CISR and NAT. While the alternative solutions fill the gap in the short term, IPV6 provides a more durable solution and the protocol goes beyond the addressing issue. It improves on a number of existing features while also including additional features resulting in an improved efficiency and quality of communication.

With the many advantages, it provides IPV6 will open up opportunities that would either not be possible or would be inefficient under IPV4. India will need to seriously consider the shift to IPV6 in the near future, so as to be able to benefit of the multiple advantages and opportunities presented by IPV6. This paper presents the differences of IPV6 and IPv4,discusses the opportunities and challenges that its deployment presents for India. The rest of the paper is structured as follows: discusses how the design of IPV6 addresses, presents the deployment strategies adopted in different developed countries and policies of various level in India.

II. DIFFERENCES BETWEEN IPV4 AND IPV6

There are some major differences between IPv4 and IPv6 shows in table no 2.1

Table 2.1

S.No.	IPv4	IPv6
1.	Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length
2.	IPSec support is optional.	IPSec support is required
3.	No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
4.	Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host
5.	Header includes a checksum.	Header does not include a checksum.
6.	Header includes options.	All optional data is moved to IPv6 extension headers.
7.	Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbour Solicitation messages.
8.	Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
9.	ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
10.	Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
11.	Must be configured either manually or through DHCP	Does not require manual configuration or DHCP.
12.	Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.

III. CHALLENGES FOR IPV6 DEPLOYMENT

In this paper IP Next Generation overview (Hinden, 1996), R Hinden argued that IPng or IPv6 would be a necessity with the proliferation of nomadic personal computing devices. He argued that the nature of nomadic computing requires an Internet protocol with built in authentication and confidentiality, thus being a major catalyst for IPv6. He also proposed that the different TV channels and Video on Demand would be another major driving force for IPv6. Another idea put forward by him is device control, where different everyday life devices will be controlled via the Internet. He also predicted that there would need to be a major shift towards the new IP in the 1999's to 2003's. The same report reveals that only 0.12 % of IPV6 native traffic flowed in the Amsterdam Internet Exchange. These numbers seem very small. However, the IPV4 address space is expected to be exhausted in 2012 (CXOtoday, 2009; Eustace, 2009) and the need for IPv6 will become imminent. In the following sections, we discuss some of the reasons why IPv6 has had such a slow start and adoption given the initial predictions and also the challenges involved for the deployment of IPv6. Then the costs involved for deploying IPv6 and solutions are also discussed.

IPv4 will be used for years even after IPv6 has been deployed. IPv6 and IPv4 are two different protocols, where resources available over IPv6 are not reachable from an IPv4 node and vice versa. But, the layers in the Internet Architecture are independent of each other, thus enabling both IPv4 and IPv6 transmission to run in parallel, on the same network. Therefore, the transition mechanism requires that IPv4 and IPv6 hosts are able to interoperate. The IPv6 deployment between hosts and routers need to done incrementally, with few interdependencies and low start-up cost. Finally, it should be easy for system users, network operators and administrators to address [Bradner & Mankin, 1995]. Moreover, the IPv6 has been present for many years, but there has been a poor growth in its deployment across the Internet [Eustace, 2009]. The objective of IPv6 was to have most computers and networks working on a dual-stack by this time, until IPv6 gradually takes over. Dual-stack enables both IPv4 and IPv6 to coexist, where servers and clients will speak both protocols and application or service can use either protocol to communicate.

During the transition, the organization should expect that most systems software will need to be upgraded. Hardware which have only IPv4 implementations should be considered for replacement and before buying any new hardware, the organization should ensure that the new hardware provides for IPv6 support. There are different strategies to transition to IPv6. The easiest migration process can be through an upgrade of the whole network, Operating Systems and Application. This will provide all the good features of IPv6, but it is expensive. The next choice is to have an incremental deployment, which in addition to the good features of IPv6, it allows lower cost and risk management. Finally, one can wait for the last minute to deploy, and not benefit from the IPv6 features. The consequence will be loss of market shares and lagging behind the market trend.

IPv6 deployment encounters many challenges. One of the biggest hurdle to move to IPv6 is the business need [Botterman, 2009]. The issue is that if customers do not require IPv6, there is no ability for providers to charge for IPv6. Consequently, there is no extra money for investing in new hardware and software. For an organization to build a short term IPv6 business case does not make sense. Nevertheless, not having any customer demand is not a fundamental problem, since deployment of IPv6 will happen anyway. The customer needs are more towards contents and services, such as Google, Skype and many more, and they are not interested in the protocol being used and IPv6 do not provide such new services. Developing countries which

are now deploying IPv6 will have an advantage since new IPv6 capable hardware will be used instead of investing in any hardware upgrade.

The next IPv6 deployment gap is that considerations for porting software applications and services are not expanding fast enough. The alternative is to centralize the applications and use IPv6 tunneling to connect with IPv6 hosts and routers over existing IPv4 Internet. The applications do not provide IPv6 support in software Infrastructure, for example, the 3G IP Multimedia Subsystems (IMS) are limited in deploying IPv6 on Fixed Mobile Convergence between Wireless and Broadband. Enterprise Resource Applications (e.g SAP, Oracle, DB2, Finite Element Analysis) and Media Entertainment Applications, such as Gaming, Virtual Life, Content Distribution, Peer-to-peer File Sharing are also taking a long time to be ported on IPv6 [Bound, 2007]. Another important requirement while deploying IPv6 is the Security Infrastructure and many organizations are already using IPv4 security software infrastructure for Intrusion Detection, Network Edge Packet Filters and Custom Firewalls. These security software still requires to be adapted to IPv6. Even full featured Network Management platforms that are used to manage IPV4 network elements and processes need to be upgraded to support IPv6.

Many organizations are also not interested in transitioning to IPv6 because their customers and employees cannot use IPv6. The compelling immediate action within the IPv6 deployment process is to have IPv6 supported 'small gateways' for private homes. Thus, allowing larger IPv6 deployment possibilities.

According to the IPv6 Deployment Survey commissioned by the European Commission, cost is one of the major barrier to deploy IPv6 [Botterman, 2009]. Normally, when deploying a network Infrastructure, network, security, Human Resource Training, Contents Management and Administrative cost are considered. But, in general when considering deploying an IPv6 Infrastructure mainly the 'cost' of Training, Network Upgrade and Dual Stack operation is being foreseen.

Training cost, is probably the highest among the costs. Even though, IPv6 is not 'so different' compared with IPv4, the hurdle is that staffs do not have enough knowledge and experience with IPv6. Thus, training in IPv6 is perceived to be expensive. However, many organizations have recurrent training for many other new technologies and protocols and, if well-planned, the cost for providing IPv6 training should not be considered as high.

The cost of IPv6 deployment depends on many factors. In order to minimize costs while moving to IPv6, organizations have to carefully choose when to start IPv6 deployment [6DISS, 2007]. The size of the network, current hardware and software being used and how soon the network should be IPv6 ready are other components that need considerations while deploying IPv6. But, the key for transitioning for a new protocol, technology and services or IPv6 is planning ahead and that helps to minimize costs.

Organizations often do not consider the cost for not deploying IPv6 and those cost are hidden and difficult to realize. Many studies already demonstrated that operating a network with NAT means extra complexity and cost [Christman, 2005; The TCP Guide, 2005; Huston, 2009; IEEE-USA, 2009]. VoIP, triple play, end-to-end security, peer-to-peer, on-line gaming, and many other new applications cost even higher to be deployed on IPv4, since they do not operate easily through NAT and require co operation of NAT vendors [IEEE-USA, 2009]. It is also more expensive for developing applications to traverse NAT and work across different network scenarios [Huston, 2009]. Moreover, most security precautions were ignored in IPv4 and NAT complicates deployment for secure applications [Christman, 2005].

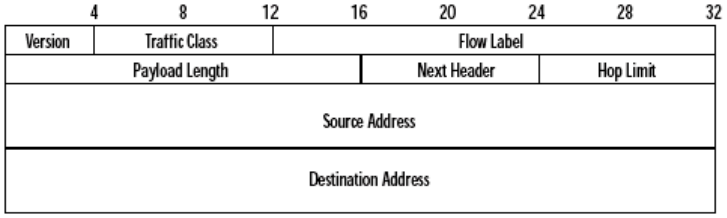
IV. BENEFITS OF IPV6

IPv6 improves on the addressing capacities of IPv4 by using 128 bits for addressing instead of 32, thereby making available an almost infinite pool of IP addresses. Also IPv6 is supposed to be providing various enhancements with respect to security, routing, address auto configuration, mobility & QOS etc.

The following are the important features of IPv6 protocol, which may play an important role in the growth of Internet in the country due to its advance capabilities.

4.1 New Header Format

The IPv6 header has a new format that is designed to keep header overhead to a minimum. The streamlined IPv6 header is more efficiently processed at intermediate routers with lower processing costs.



Figures No. 4.1.1

In the Fig.4.1.1, The first 64 bits of the packet include only 6 parameters. They are:

- Version Field (4 bits)
- Traffic Class (8 bits)
- Flow Label (24 bits)
- Length of the Payload (16 bits)
- Type of Next Header (8 bits)
- Hop Limit (8 bits)

The IPv6 header is composed of a 64 bit header, followed by the source and destination IP addresses (each 128 bits long)

4.2 Large Address Space

IPv6 has 128 bits (16 bytes) source and destination IP addresses. This will enable to accommodate 2128 hosts. Even though only a small number of IPv6 addresses are currently allocated for use by hosts, there are plenty of addresses available for future use.

Jumbogram-IPv4 limits packets to 65535 (2^{16}–1) octets of payload. An IPv6 node can optionally handle packets over this limit; it can be as large as 4294967295 (2^{32}–1) octets. The use of jumbogram is indicated by the Jumbo Payload Option header.

4.3 Efficient and Hierarchical Addressing and Routing Infrastructure

IPv6 global addresses used on the IPv6 portion of the Internet are designed to create an efficient, hierarchical, and submersible routing infrastructure that is based on the common occurrence of levels of Internet service providers.

4.4 Stateless and Stateful Address Configuration

IPv6 supports both stateful address configuration, such as address configuration in the presence of a DHCP server, and stateless address configuration (address configuration in the absence of a DHCP server). With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses) and with addresses derived from prefixes advertised by local routers. Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

4.5 Built-in Security

Support for IPSec is an IPv6 protocol suite requirement. This requirement provides a standards-based solution for network security needs and promotes interoperability between different IPv6 implementations.

4.5.1 Data Confidentiality

The IPSec sender can encrypt packets before sending them across a network'

4.5.2 Data Integrity

The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

4.5.3 Data Origin Authentication

The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.

4.5.4 Anti-Replay

The IPSec receiver can detect and reject replayed packets.

4.6 Support for QOS

New fields in the IPv6 header define how traffic is handled and identified. Traffic identification using a Flow Label field in the IPv6 header allows IPv6 routers to identify and provide special handling for packets belonging to particular packet flow between source and destination. Support for QOS can be achieved even when the packet payload is encrypted through IPSec.

V. TRANSITION MECHANISMS FOR IPV6

To coexist with an IPv4 infrastructure and to provide an eventual transition to an IPv6-only infrastructure, generally following mechanisms are used:

- Dual IP layer
- IPv6 over IPv4 tunnelling
- DNS infrastructure

5.1 Dual IP Layer

The dual IP layer is an implementation of the TCP/IP suite of protocols that includes both an IPv4 Internet layer and an IPv6 Internet layer. This is the mechanism used by IPv6/IPv4 nodes so that communication with both

IPv4 and IPv6 nodes can occur. A dual IP layer contains a single implementation of Host-to-Host layer protocols such as TCP and UDP. All upper layer protocols in a dual IP layer implementation can communicate over IPv4, IPv6, or IPv6 tunnelled in IPv4.

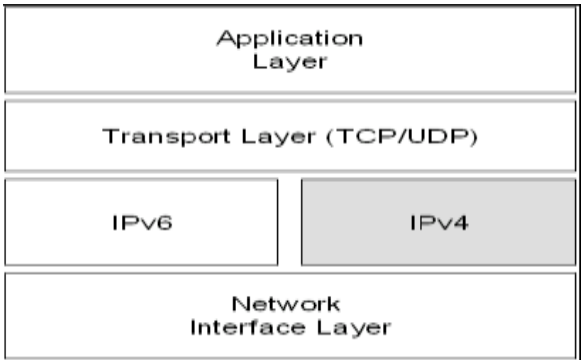


Figure No. 5.1.1

5.2 IPv6 over IPv4 Tunnelling

IPv6 over IPv4 tunnelling is the encapsulation of IPv6 packets with an IPv4 header so that IPv6 packets can be sent over an IPv4 infrastructure. Within the IPv4 header:

• The IPv4 Protocol field is set to 41 to indicate an encapsulated IPv6 packet.

• The Source and Destination fields are set to IPv4 addresses of the tunnel endpoints. The tunnel endpoints are either manually configured as part of the tunnel interface or are automatically derived from the sending interface, the next-hop address of the matching route, or the source and destination IPv6 addresses in the IPv6 header.

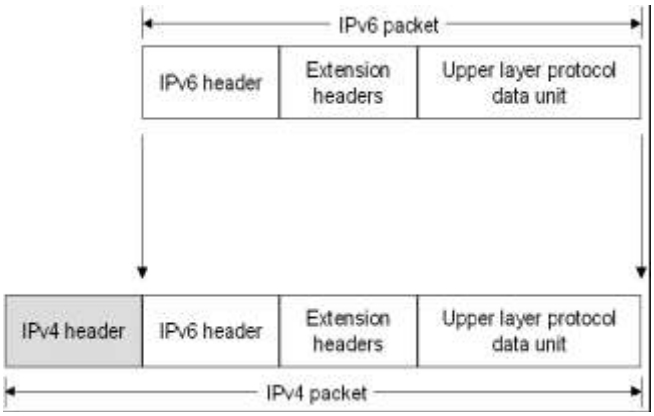


Figure No. 5.2.1

For IPv6 over IPv4 tunnelling, the IPv6 path maximum transmission unit (MTU) for the destination is typically 20 less than the IPv4 path MTU for the destination. However, if the IPv4 path MTU is not stored for each tunnel, there are instances where the IPv4 packet will need to be fragmented at an intermediate IPv4 router. In this case, IPv6 over IPv4 tunnelled packet must be sent with the Don't Fragment flag in the IPv4 header set to 0.

5.3 DNS Infrastructure

A Domain Name System (DNS) infrastructure is needed for successful coexistence of IPv6 and IPv4 because of the prevalent use of names (rather than addresses) to refer to network resources. Upgrading the DNS infrastructure consists of populating the DNS servers with records to support IPv6 name-to-address and address-to-name resolutions. After the addresses are obtained using a DNS name query, the sending node must select which addresses are to be used for communication.

VI. DEPLOYMENT STRATEGIES/POLICIES IN INDIA AND WORLD-WIDE

6.1 National Policies [TRAI- August 2005]

6.1.1 Relevant Existing Government Policies

- The Ten Point Agenda declared by Hon'ble Minister of Communications and Information Technology on 26.05.2004 includes IPv6 as following:
- **"Migration to New Internet Protocol IPv6:** *Worldwide the new IPv6 is being implemented on the Internet to accommodate increased number of users and take care of security concerns. It would be my endeavour to bring about migration to IPv6 in India by 2006*."
- In the Broadband Policy 2004, Government has envisaged Broadband and Internet subscribers of 20 million and 40 million by 2010 respectively through various Internet and Broadband Technologies.
- Broadband policy has also defined Broadband as an "always-on data connection" that is able to support various interactive services. In order to be truly interactive, each Broadband connection may require a permanent IP address assigned to end-user.
- In order to fulfil these government policies/ objectives, India's Internet and Broadband Infrastructure should be globally competitive, secured and affordable. The present generation Internet (IPv4) may not be enough to help in achieving these objectives.

6.1.2 IPv6 Implementation Group

Department of IT commissioned several projects to facilitate the efforts of stakeholders regarding the adoption of IPv6, in creating test beds and supporting R&D activities. In addition an inter agency IPv6 Program Implementation Group (IPIG) was constituted to track and review the IPv6 implementation from time to time. Senior officers from DIT, NSC, TRAI, DRDO, ISPAI, COAI, academic institutions etc. are the members of IPIG.

6.1.2.1 Institutional Activities

Some of the Universities/ R&D institutions have been studying the technical aspects of IPv6 in India. IPv6 forum of India is organizing workshops involving the industry, ISPs, academic and research institutions to bring awareness among stakeholders. BITS Pilani is the first institution in India to connect to 6Bone (IPv6 international test bed network) and is developing IPv6 native support products. Similarly, ERNET of DIT in association with IIT Kanpur has taken up a project of setting up of IPv6 test bed at few locations in the country.

6.1.2.2 Industry Efforts

It is understood that ISPAI is motivating the member ISPs to start obtaining IPv6 address space from Asia-Pacific Network Information Centre (APNIC) and some of the ISPs have already obtained the addresses. Few ISPs are experimenting with IPv6 tunnelling over IPv4 by exchange of experimental packets to get a feel of the capabilities of IPv6. Some ISPs are getting their router software upgraded to IPv6 to make their network IPv6 compliant.

6.2 International Policies

Many countries around the globe like Japan, Korea, China, European Union, USA have set up national IPv6 networks to enable the network operators and software developers to get a hands-on feel of this technology. Some of the important ones are described below:

6.2.1 Europe

The European Commission (EC) initiated an IPv6 Task Force in April 2001 to design an "IPv6 Roadmap 2005" and delivered its recommendations in January 2002, which were endorsed by the EC.A phase II IPv6 Deployment Task Force was enacted in Sep, 2002 with a dual mandate of initiating country/regional IPv6 Task Forces across the European states and seeking global cooperation around the world.

6.2.2 Japan

Japan took political leadership in the design of a roadmap for IPv6 in the fall of 2000 in a policy speech by Prime Minister. The Japanese government mandated the incorporation of IPv6 and set a deadline of 2005 to upgrade existing systems in every business and public sector. Japan sees IPv6 as one of the ways of helping them leverage the Internet to rejuvenate the Japanese economy. The IPv6 Promotion Council was created to address, in a comprehensive way, all issues related to the deployment and rollout of IPv6. In 2002–2003, the Japanese government created a tax credit program that exempted the purchase of IPv6-capable routers from corporate and property taxes.

6.2.3 South Korea

In 2001, the South Korean Ministry of Information and Communication announced its intention to implement IPv6 within the country. In September 2003, the Ministry adopted an IPv6 Promotion Plan with commitment for funding IPv6 routers, digital home services, applications, and other activities.

6.2.4 China

In December 2003, the Chinese government issued licenses and allocated budget for the construction of the China Next Generation Internet (CGNI). The goal is to have that network fully operational by the end of 2005. China and Japan have declared jointly in the 7th Japan-China regular bilateral consultation toward further promotion of Japan-China cooperation that IPv6 is an important matter in the area of info-communications field.

VII. OPPORTUNITIES AND CHALLENGES FOR INDIA

As other countries in the world are planning their IPV6 deployment, India will need to do the same so as to overcome the exhaustion of IPV4 addresses and also to benefit of the many advantages of IPV6. The deployment of IPV6 will improve the internet support for organizations as well as individuals in terms of the number of devices that can directly access internet services, the security of transactions, the improved quality of applications and the wider range of applications possible due to the integrated support for mobility. The deployment of IPV6 will improve organizations' abilities to offer services with real-time requirements such as live broadcasts on all kinds of personal computing devices, improved video surveillances and remote processing of complex applications.

The India software industry can also obtain direct economic opportunities from the worldwide deployment of IPV6. The software industry can participate in converting the massive amount of IPV4 applications that will need to be ported to IPV6 network. In addition to simply porting the applications, they can be further improved to benefit from the additional security and QoS support of IPV6. Additionally IPV6 presents important opportunities in terms of new kinds of secure and QoS-based applications for portable devices. The Mauritian software industry can seize the opportunity to obtain its market share from these classes of applications.

To deploy IPV6, ISPs will have to provide the required support in the network backbones of the country. Each organization of the country will then need to come up with its own strategy of transition.

VIII. CONCLUSION

In this paper, we presented the different problems associated with the IPV4. These problems include exhaustion of address space. We then proposed how IPV6 addressed many of the issues of IPV4 and also improves on the older protocol. We discussed about opportunities provided by IPV6 like enhanced security and Flow Label to implement QoS for different types of traffic. We then discussed on the hurdles encountered in IPV6 deployment, among which are technological, financial and human capacity issues. We also discuss why IPV6 has not spread according to the initial predictions, when it was being proposed. We also analyze the IPV6 deployment status around the world, noting that IPV6 accounts for limited Internet traffic. We also propose that IPV6 provides a unique opportunity for African countries, since most of these countries are not tied up with legacy hardware and technology and can invest in IPV6 ready equipment from the beginning. India IT industry is booming nowadays and IPV6 deployment can contribute to a large extent to the industry. New applications, involving mobility or that can make us of specific features of IPV6 can be developed.

REFERENCES

Books:

[1] Computer Networks , *Andrew S. Tanenbaun*.

[2] Computer Network & Communication, *V.K. jain & Naveena Bajaj*

[3] Computer Networks- Protocols, Standerds, Interfaces , *Uyless Black.*

[4] Data Communication & Networking, *Behrouz A Forouzan*.

[5] TCP?IP Protocol Suit, *Behrouz A Forouzan*

Journal Paper & Web Links:

[6] 6DISS (IPv6 Dissemination and Exploitation) (2007). IPv6 Deployment and Associated Risks (for Strategists). Retrieved on 15th December 2009 from http://www.6diss.org/

[7] Baker, F. (2009). IPv4/IPv6 Coexistence and Transition. IEFT Journal 4 (3).

[8] Bound J (2002), Dual Stack Transition Mechanism. Retrieved on 10th December 2009 from

[9] Bound, J. (2001). Internet Society: IPv6 Deployment.

[10] Bound, J. (2007). The New New Internet: IPv6 Conference, Hyatt Regency Crystal City, May 10, 2007, "IPv6 Deployment Gaps to be Completed".

[11] Childress, B., Cathey, B., and Dixon, S. 2003. The Adoption of IPv6. *J. Comput. Small Coll.* 18, 4 (Apr. 2003), 153-158.

[12] Christman, C. (2005). The move on to IPv6: If you've not done so already, it's time to get ready for the next generation of IP. Retrieved on 15th Decmber 2009 from http://features.techworld.com/networking/1109/the-move-on-to-ipv6/

[13] Davies J. (2008) "Understanding IPV6", Second Edition- ISBN-10: 0-7356-2446-1, Microsoft Press.

[14] Dunmore M., "6NET- An IPV6 Deployment Guide", The 6NET consortium, September 2005.

[15] Eddy W., Ishac J., "Comparison of IPV6 and IPV4 features", Internet draft, May 2006.

[16] European IPv6 Task Force (2004) IPv6 Task Force Steering Committee. Retrieved on 12th December 2009 from http://www.ipv6.eu/admin/bildbank/uploads/Documents/Deliverables/ipv6tf-sc_pu_d2_1_1_v1_25.pdf

[17] Eustace, G. (2009). Infrastructure Support Section, Information Technology Services, Massey University.

[18] Google (2008) Global IPv6 Statistics. Retrieved on 15 December 2009 from

[19] Hagen S., "The IPV6 case: Questions and Answers", Sunny Paper, Sunny Connection AG., 2004, available at www.sunny.ch.

[20] Hinden, R. M. (1996). IP Next Generation Overview, Communications of the ACM. ACM NewYork, USA pp 61-71.

[21] IEEE-USA White Paper (2009). Next Generation Internet: IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S.

[22] Ilitsch, V. B (2008). Researchers: IPv6 traffic a mere 0.0026 percent of total. Retrieved on 14th December 2009 from http://arstechnica.com/old/content/2008/08/researchers-ipv6-traffic-a-mere-0-0026-percent-of-total.ars

[23] IPv6 Forum Taiwan (2009) Developing IPv6 Technology. Retrieved on 16th December 2009 from http://www.ipv6.org.tw/newe.html

[24] JANET (2009) UK's Education and Research Network. Retrieved on 15th December 2009 from http://www.ja.net/services/connections/janet-sites/mans

[25] Jordi (2004) Telefonica to link Europe and Latin America with IPv6 Technology. Retrieved on 15th December 2009 from http://www.ipv6tf.org/index.php?page=news/newsroom&id=317

[26] KIRK, J. (2009). IDG News Service: Europe Moving Slow on IPv6 Deployment. Retrieved on 15th December 2009 from http://www.pcworld.com/businesscenter/article/174655/europe_moving_slow_on_ipv6_deployment.html

[27] Melford B. (1997) – "TCP/IP Limitations undone", Sunworld, January 1997.

[28] MW (2008) Phones Ring Earthquake Warnings. Retrieved on 13th December 2009 from http://www.letsjapan.markmode.com/index.php/2008/12/04/phones-ring-earthquake-warnings/

[29] National Advanced IPv6 Centre (2008) IPv6 Status in Malaysia. Retrieved on 12th December 2009 from http://www.nav6.org/content_resource.php

[30] Rajahalme J., Conta A., Carpenter B. and Deering S., RFC 3697, "IPv6 Flow Label Specification", March 2004.

[31] Tantayakul, K., Kamolphiwong, S., and Angchuan, T. 2008. IPv6@HOME. In *Proceedings of the international Conference on Mobile Technology, Applications, and Systems* (Yilan, Taiwan, September 10 - 12, 2008).

[32] The 6Net Consortium (2005) An IPv6 Deployment Guide. Retrieved on 11th December 2009 from http://www.6net.org/book/deployment-guide.pdf

[33] The TCP Guide (2009). IP Network Address Translation (NAT) Protocol. Retrieve on 15th Decmber

[34] TELECOM REGULATORY AUTHORITY OF INDIA - Consultation paper On Issues Relating To Transition From IPv4 To IPv6 in India 2009. Undated

Theses:

[35] Prakash B., "Using The 20 Bit Flow Label Field In The IPV6 Header To Indicate Desirable Quality Of Service On The Internet", Master of Science Thesis, University of Colorado,2004.