TRANSITIONAL SURVEY ON IPv4-IPv6

Sheryl Radley[1], **Shalini Punithavathani D.**[2], **Indumathi L.K.**[3]

[1&2]Government College of Engineering - Tirunelveli,
[3]National College of Engineering, Marudakulam,
Email: [1]sherylradley@gmail.com, [2]shalini@gcetly.ac.in, [3]induseenu7980@gmail.com

Abstract

Pv4/IPv6 transition rolls out many challenges to the world of internet. IETF proposes various transition techniques including dual IP stack, IP translation and tunnelling transition mechanisms. The transition between the IPv4 internet and IPv6 internet will be a long process as they are completely two separate protocols. IPv4 host and routers will not be able to deal directly with IPv6 traffic and vice versa. A detailed study is made on the IPv6 addressing architecture. Out of the three mechanisms Tunnelling proves to be most effective. Tunnelling mechanism support 'link to link' IP connectivity across an 'unlike' network. The 6rd mechanism that are used for IPv4/IPv6 transition mechanism permits an Ipv6 mobile node to roam into Ipv4 based network and get serviced besides roaming in IPv6 based network. This paper aims at a comparative study on the three transition techniques such as Softwire mesh which supports Dual Stack, NAT444 which supports translation and IPv6 Rapid Development (6rd) mechanism in tunnelling mechanism.

Key words IPv4/6 transition, tunnelling, Dual Stack, 6rd, Softwire mesh, NAT444.

I. INTRODUCTION

In the Internet, data is transmitted in the form of network packets. IPv4 was the first version of the Internet protocol that was widely deployed in order to provide unique global computer addressing to make sure that two entities can uniquely identify one another. IPv4 addresses are being exhausted [4]. IPv6-also known as IPng has been selected from several proposed alternatives as a suitable successor of the existing Internet Protocol. IPv6 specifies a new packet format, designed to minimize packet header processing by routers. However, in most respects, IPv6 is a conservative extension of IPv4. IPv6 address is represented by 8 groups of 16-bit values from 0000FFFF, each group represented as 4 hexadecimal digits and separated by colons (:). IPv6 has 128 bits and allows approximately 340 undecillion addresses. Hence the transition from IPv4-IPv6 has become an increasingly vital for the world of internet where IPv4 and IPv6 are intercompatible protocols.

Numerous of techniques have been proposed over these years to support the continuous growth of the global Internet required for overall architecture development to accommodate the new technologies, that support the ever growing number of users, applications, appliances and services such as NAT-PT, Transport Relay Translation, Static tunnelling, Dynamic Tunnelling [1], 6 over 4 Tunnelling, 6 to 4 tunnelling, 4 over 6 Tunnelling, 4 to 6 tunnelling, Intrasite Automatic Tunnelling Addressing, Teredo [5], have been developed to support the interoperability between IPv4 and IPv6.

The transition techniques are broadly divided into three categories: Dual Stack, Translation and Tunnelling. Both IPv4and IPv6 networks allow nodes using auto configuring Protocol to manage the resource's address space. The auto configuration protocol must be able to select, allocate and assign an unique network address to an unconfigured node. Auto-configuring protocols can be classified as stateful and stateless. Ipv6 provides high security which has encryption and authentication options when compared to IPv4. It also augments for better network management and routing efficiency. The processing has been simplified since no fragmentation is needed due to availability of large address space which also avoids subnetting which is essential needed in IPv4. It has been recognised as the future protocol by IETF, Eurescom, 3GPP and other vendors as there are available resources to help build IPv6 integration plan. IPv6 can be applied for multimedia news on demand, direct online trading, newspaper printing, VoIPv6. Some of the universal applications are mail, FTP, Web server/browser, Multimedia web, audio-video tools and games.

The dual stack in transition mechanism is used to run both IPv4 and IPv6 parallely. It allows hosts to simultaneously reach IPv4 and IPv6 content making it a flexible coexistence strategy [2]. Translation techniques include transformation of both protocol header and protocol payload which introduces an intermediate element between IP end-point and thus breaks the end-to-end model [11]. Tunnelling technique is used for IPv4 networks to interoperate with IPv6 networks and vice-versa by transferring Protocol Data Unit by encapsulating carrier protocol. The encapsulation takes place at the peer level or below, is named as encapsulation mechanism. The addressing involved in IPv6 are Unicasting, Multicasting and Anycasting. Unicasting are classified into many types such as special unicast address, link local unicast address, site local unicast address, aggregatable unicast address. There is no broadcasting address present in IPv6 whereas IPv4 supports broadcasting. The addressing is not done for the entities but for the end interface of the end system that needs to be connected with another specific end system. Table 1 below highlights the different Internet Protocol version available and their current status.

Table1. IP Versions

Version		Year	Current Status
0	IP	March 1977 version	(deprecated)
1	IP	January 1978 version	(deprecated)
2	IP	February 1978 version A	(deprecated)
3	IP	February 1978 version B	(deprecated)
4	IPv4	September 1981 version	(current widespread)
5	ST	Stream Transport	(not a new IP
6	IPv6	December 1998 version	(formerly SIP
7	CATNIP	IPng evaluation	(formerly TP/IX; deprecated)
8	Pip	IPng evaluation	(deprecated)
9	TUBA	IPng evaluation	(deprecated)
10-15		Unassigned	

Table 2 below highlights the distinction between IPv4 and IPv6 [7]. From the table below the different features for both Ipv4 and IPv6 is given.

Features	IPv	IPv6
Address	32 bits	128 bits
Addressing	Anycast, Unicast, Multicast, Broadcast	Anycast, Unicast
ARP	Used to resolve an IPv4 address	Replaced by Neighbour Discovery
Checksum in header	Included	Not included
Fragmentation	Done by the Routers and Source Node	Only by the Source Node
Header includes Option	Required	IPv6 Extension Header
IP Configuration	Manually or DHCP	Auto-Configuratio n or DHCP
DNS	Use Host address (A) resource records	Use host address (AAAA) resource records
IPSec Support	Optional	Required
QoS	Differentiated Services	Use traffic classes and flow label.
Mobility	Use Mobile IPv4	MIPV6 with faster handover
IGMP	Use to manage local subnet group	Replaced with MLD

II. TWO TRANSITION TECHNIQUES

Dual Stack: The Dual Stack Technique is also called as native dual stack or Dual IP layer. Both protocols IPv4 and IPv6 run parallel on the same network infrastructure which does not require encapsulate IPv6 inside IPv4 and vice versa. Outdated equipments do not support Ipv6, hence it becomes important to have a network which supports both IPv4/6 network. Modes of operation of IPv6/IPv4 are:

1. IPv6-only operation where an IPv6 node has its stack enabled and its Ipv4 stack disabled. 2. IPv4-only operation where an IPv4/IPv6 node has its IPv4 stack enabled and its Ipv6 stack disabled. 3. IPv4/IPv6 operation where an IPv4/IPv6 node has both stacks enabled. Fig.1. shows dual stack mechanism.

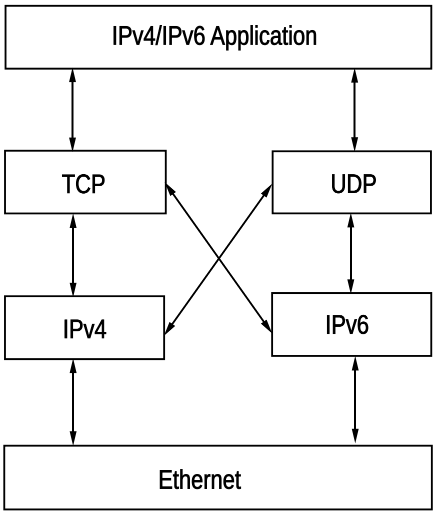

Fig.1 Dual Stack Mechanism

A common dual-stack migration strategy makes a transition from the core to the edge. This includes enabling two TCP/IP protocol stacks on the WAN core routers. In a common dual stack migration firstly the perimeter routers and firewalls, then the server-farm routers and finally the desktop access routers. Once the network supports IPv6 and IPv4 protocols, the process will enable dual protocol stacks on the servers and then the edge entities. The dual stack doubles the communication requirements, which in turn causes performance degradation.

Translational Transition mechanism: It can be classified as stateful and stateless mechanism. Stateless mechanism involves Stateless Internet Protocol/ Control Messaging Protocol Translation (SIIT), Bump in stack (BIS) and Bump in Application Programming Interface (BIA). The Stateful mechanism is classified as Network Address Translation-Protocol Translation (NAT-PT and Transport Relay Translator (TRT). In translation technique IP address information in IP packet headers is modified while in transit across a traffic routing device. When translation occurs, the IPv6 packets itself gets converted into IPv4 packet after translation, and vice versa. The translation can be done from one-one to one-many. NAT allows a small number of public addressees to be shared by a large number of hosts using private addresses. It provides security benefits by making host more difficult to address directly by foreign machines on public internet.

Network Address Translation is shown in figure 2. NAT has serious drawbacks in terms of the quality of internet connectivity and requires careful attention in its implementation. The translation methods have been devised to alleviate the issues encountered. NAT is highly complex along with performance reduction and lack of public addresses. Address, port substitution, TCP/UDP checksum recomputing, application layer translation and IP/ICMP protocol translation are all required to accomplish proper translation. Both Stateful and stateless translation mechanisms are highly unscalable. For example stateless translation has to consume IPv4 address for IPv6 hosts. It is no scalable since IPv6 address space is much larger than IPv4. Meanwhile Stateful translation requires translator to maintain both address and port mapping.

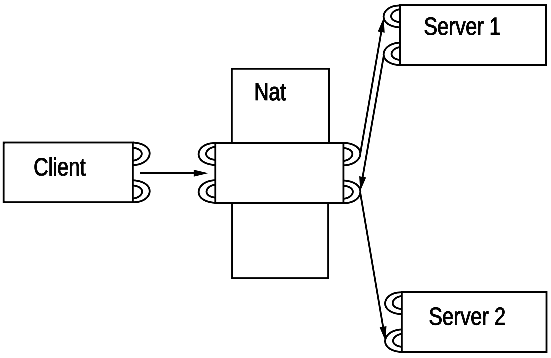

Fig. 2 IPv4/6 Translational Mechanism

III. ISSUES TO BE CONSIDERED WHILE TRANISTION

Dual Stack transition supports and ensures any type of communication regardless of the IP version which leads to doubling the communication processing requirements. Performance degradation also occurs in DS transition technique. Translation mechanism leads to complexity as end to end system is interrupted by an element. While translating between IVI (IPv4/IPv6) [7], compatibility with all the available applications must be taken into consideration. Problems arise due to lack of public addresses in translation mechanism. Tunnelling can be used for any protocol version. The data to be transmitted are compressed while tunnelling which increases the network throughput. Tunnelling mechanism increases security between the ends of the entities. Since only one router is used in tunnelling, when additional load is put on that particular router it leads to single point failure [11]. All the transmission in that path will be affected due to single point failure. Trouble shooting gets more complex as a node runs into hop count or Maximum Transmission Unit (MTU) size issues, as well as fragmentation problems. Configuration must be dynamic or automatic. For encapsulation, tunnel end points should keep a track on peer end point.

IV. TUNNEL-BASED TRANSITION IN IPv4/6 ACCESS AND BACKBONE NETWORK

Tunnelling techniques are more preferable than dual stack and translation techniques. Tunnels are used to carry one protocol inside another. Most access network operate over IPv4.Users of these network might desire to get connected to IPv6 internet. Therefore, ISP should provide IPv6 access over IPv4 only network, which could be achieved through IPv6 over IPv4 tunnel. These tunnels take IPv6 packets and encapsulate them in IPv4 packets to be sent across portions of the network that haven't yet been upgraded to IPv6. Tunnels can be created where there are IPv6 islands separated by an IPv4 ocean, which will be the norm during the early stages of the transition to IPv6. Later there will be IPv4 islands that will need to be bridged across an IPv6 ocean. Tunnels are classified as: manual and dynamic [1]. Manually configured IPv6 tunnelling requires configuration at both ends of the tunnel, whereas dynamic tunnels are created automatically based on the packet destination address and routing. Dynamic tunnelling techniques simplify maintenance compared with statically configured tunnels, but static tunnels make traffic information available for each endpoint, providing extra security against injected traffic. Fig. 3. shows the Tunnelling mechanism.

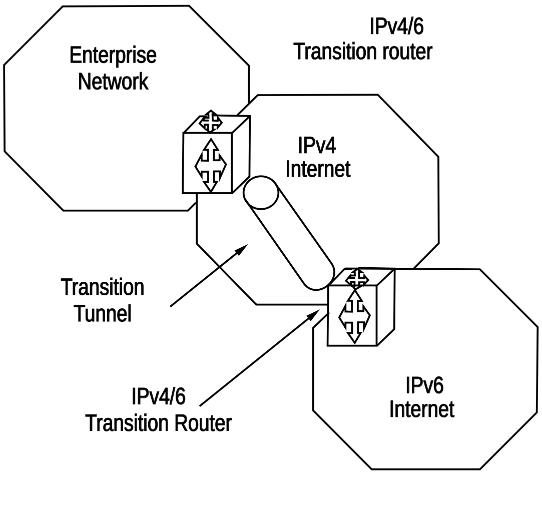

Fig. 3 Tunnelling Mechanism

Some of the tunnelling techniques are Automatic tunnelling using IPv4 Compatible address, 6 over 4 tunnelling, 4 over 6 tunnelling, 6 to 4 tunnelling, 6 in 4 tunnelling, Intrasite, Terado, IPv6 Rapid Development (6rd), Automatic tunnelling Addressing Protocol (ISATAP). With dynamic tunnels it isn't easy to track who is communicating over the transient tunnels and the tunnel destination end point is unknown. Tunnelling creates situations in which traffic will be encapsulated, and many firewalls will not be able to inspect the traffic if it is in a tunnel. Tunnels will constantly have to be changed and monitored as the transition progresses. Dynamic tunnel techniques do not create tunnel interfaces that can be monitored with SNMP. Dynamic tunnel techniques such as 6 to 4 use 2002::/16 addresses, which means that it will be needed to re-address the network twice as part of the transition to IPv6.

V. NETWORK ADDRESS TRANSLATION 666

In NAT, an IP address from a private address pool is translated to a globally unique, publicly reachable IP address. Optionally, the mechanism translates source port information so that many private IP addresses can share a limited number of global IP addresses. NAT666 is an extension of the traditional NAT mechanism. It involves two layers of address and port translation. The first takes place at the Customer Premises Equipment (CPE) and the second at the ISP, Which uses a capability known as Large Scale Network Address Translation (LSN). The term NAT666 signifies translation from one IPv6 block to a second IPv6 block, followed by a third IPv6 block. As shown in the figure [], the first block is a private address at the CPE. The second one is another private IP address block between the CPE and the ISP, and the third is a globally reachable public block.

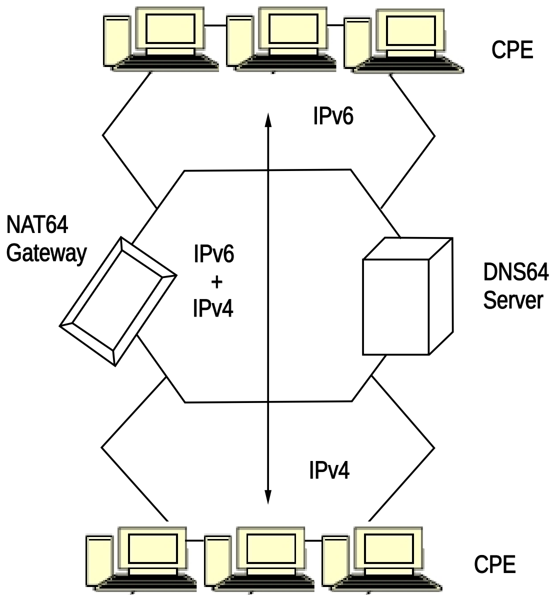

Fig. 4 NAT64 Tunnelling Mechanism

NAT 666 does not require the replacement of existing CPE devices. It utilizes the proven NAT technology. It also does not require changing other network elements such as Domain Name Service. But then there could be a potential overlap between the customers's private address block and the private address block used between the CPE and the service provider. This could result in misrouting of packets. The classic disadvantages of NAT666 technology, is masking of end users IP address and breaking end -to-end communication even more for application that embed IP addresses inside the payload of the packet, such as media applications, because it involves invoking the NAT mechanism twice for transmission. The routing of packets between two different customers behind the same LSN is also challenging and may require a change in firewall policies. The NAT64 mechanism is used for both the transition of coexistence of IPv4 and IPv6. It works together with DNS64, essentially a DNS translation service, to enable client-server communication between an IPv6only client and an IPv4-only server and vice versa. It allows for peer-to-peer communication that originates from an end-node running either of the two protocols. NAT64 utilizes a preassigned IPv6 prefix to algorithmically translate IPv4 addresses of IPv4 servers. The NAT64 is completely transparent to end-users because address translation occurs at the service provider network edge and it involves no change in client-end CPE devices as shown fig. 4.. It also allows transition to IPv6 while preserving existing IPv4-based infrastructure. It facilitates coexistence of IPv4-only and IPv6 only devices while ensuring seamless communication between the two during the transition period.

VI. SOFTWIRE MESH

The internet needs to be able to handle both IPv4 and IPv6 packets. However, It is expected that some constituent networks of the internet will be 'single protocol' network. One kind of single protocol network can parse only IPv4 packets and can process only IPv4 routing information; another can pass only IPv6 packets and process only IPv6 routing information. It is nevertheless required that either kind of single protocol network be able to provide transit service for the 'other 'protocol. This is done by passing the 'other kind ' of routing information from one edge of the single protocol network to the other and by tunnelling the 'other kind' of data packets from one edge to other. This tunnelling is a softwire mesh mechanism. The Softwire mesh extends with extra hop. There occurs an increased NLOS coverage when one or more nodes are added to go around obstacle. The adaption of alternative paths in case of failure or performance degradation also occurs in Softwire mesh mechanism. The cons of SWM is that there is as increased delay is introduced due to multiple hops which in turn leads to complexity of protocols and planning in the initial network coverage that is the network seeding.

VII. 6RD MECHANISM

IPv6 rapid development is a stateless, automatically configuring, naturally scalable, resilient, point to multi point tunnelling mechanism. IPv6 to IPv4 encapsulation is used in tunnelling mechanism. The 6rd model is used to deploy IPv6 over the existing IPv4 infrastructure of service providers. The mechanism relies upon algorithm mapping between IPv4 and IPv6 addresses assigned for use within the service provider network. A 6rd mechanism requires deploying 6rd aware CPE and one or more 6rd aware border relay routers. The CPE device encapsulates IPv6 packets, which are then carried over the service provider's IPv4 network to border relay routers. The 6rd relay routers then decapsulates the packet and forwards it natively to 6rd delegated Prefix End User Address Space an IPv6 network as shown in figure [12].

The model enables service providers to offer IPv6 services alongside IPv4 services, while making minimal upgrades to their existing IPv4 infrastructure. The model can be decommissioned upon completion of a service provider's IPv4 network migration to a dual stack model. The two main components of 6rd model are: 1). Customer Equipment: IPv6 traffic coming from the end user hosts is encapsulated in IPv4 also encapsulated and 6rd traffic received from the Internet through the BR router is de-capsulated. 2). Border Relay: router provides connectivity between the CE routers and the IPv6 network. The drawback of 6rd is that, it requires upgrading CPE devices constantly. Service providers easily accommodate new customers with new equipment, but it may not be economical to upgrade existing customers.

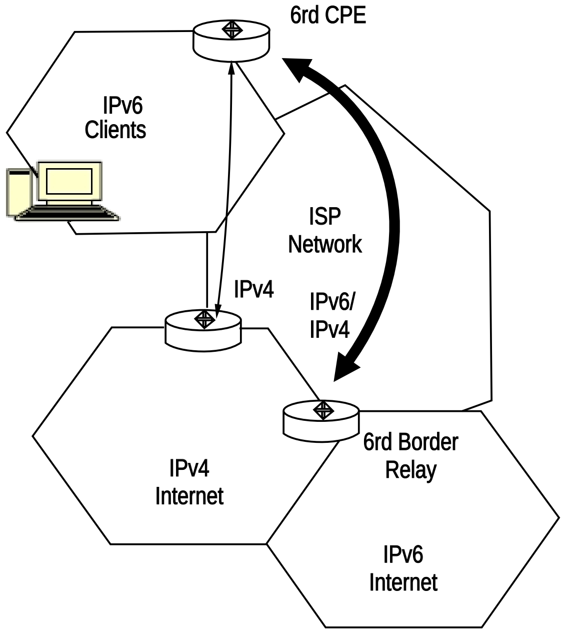

Fig. 5. IPv6 6rd Mechanism

A 6rd prefix as shown in the figure [12] is selected by the service provider for the use of 6rd domain. There is exactly one 6rd prefix for a given 6rd domain, as SP may deploy 6rd with a single 6rd domain or multiple 6rd domain. The IPv6 prefix calculated by CE for use within the customer site by combining the 6rd prefix and the CE IPv4 address obtained via IPv4 configuration methods. This prefix can be considered logically equivalent to an IPv6 delegated prefix. CE provides a range of prefixes to their sites. For a small mobile network the delegation prefix works well, but not suitable for large mobile networks. The automatic IPv6 delegation prefix solution [] is quit light weight, refreshing and return of IPv6 prefixes possible. Because it uses ICMPv6 messages for transport, it is to use retransmission to make the given solution reliable. Fig. 6. shows the frame format of 6rd prefix

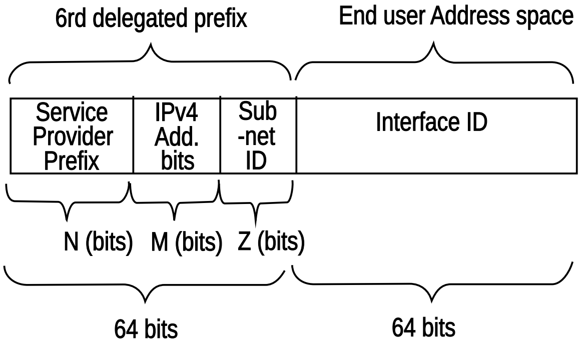

Fig. 6. Frame Format of 6rd Prefix

The 6rd delegated prefix consists of service provider prefix of N bits, IPv4 address of M bits and Subnet ID of Z bits. In 6 rd mechanism, 6rd CE LAN interface carries traffic. The multipoint interface carries tunnel encapsulation. The Service Provider Network evolves at its own pace, with its own balance of costs and incentives. 6rd border relay must have IPv6 reachability and must know ISP prefix and length, Common IPv4 bits suffix length and 6rd Relay IPv4 address.

Comparing with other tunnelling techniques, 6rd does not require extra infrastructure support and extra negotiation and therefore no complexity is included except the tunnel itself. Vendors have already implemented these transition mechanisms. To the best of our Knowledge, currently Cisco already has routers having 6rd functionality, Juniper already is using Dual Stack Lite, Huwai and Bitway have developed routers that are capable of executing Softwire mesh.

VII. CONCLUSION

This paper dealt with the different transition mechanisms that were used for the transition between IPv4 networks to IPv6 networks and vice versa. The overall review guarantees the effective way of transition is IPv6 Rapid Development method. The work to bring out the most effective technique than IPv6 Rapid Development is on process as it causes large overhead and it is not suitable for large mobile networks. For further work, the performance of the work to be proposed can be evaluated using NS2 simulator. Furthermore, the issue of IPv4 addressing in Ipv6 network may be considered for further research.

REFERENCES

[1] Yong Cui, Jiang Dong, Peng Wu, Chris Metz,Yiu L. Lee and Alain Durand , "Tunnel-based IPv6 Transition," *IEEE Internet Computing*, 2011 IEEE.

[2] D. Shalini Punithavathani and K. Sankarnarayanan, "IPv4/IPv6 Transition Mechanism", *European Journal of Scientific Research,* ISSN 1450-216X Vol.34 No. 1 (2009), pp. 110-124.

[3] Arturo Azcorra, "Integrated Routing and Addressing for Improved IPv4 and IPv6 Coexistence", *IEEE Communication Letters, Vol. 14, No.* 5, May 2010.

[4] Li Zimu, Peng Wei and Liu Yujun, "An innovative IPv4-IPv6 Transition Way for Internet Service Provider", *2012 IEEE symposium on Robotics and Application (ISRA).*

[5] Shiang-Ming Huang, Quincy Wu, and Yi-Bing Lin, "Enhancing Teredo IPv6 Tunneling to Traverse the symmetric NAT , *IEEE communication letters, VOL. 10, No. 5,* May 2006.

[6] P. Paakkanen, J. Latvakoshi, "IPv6 Prefix Delegation-based Addressing Solution for a mobile personal Area Network",*23rd Proceedings of the Internatinal Conference on Distributed Computing Systems Workshop (ICDCSW'03),* 2003 IEEE.

[7] Ra'ed AlJa'afreh, John Mellor and IRfan Awan, "A Comparison between the Tunneling process and mapping schemes for IPv4/IPv6 Transition", *2009 International Conference on Advanced Information Networking and application workshop.*

[8] J. Gnana Jayanthi and S. Albert Rabara, "IPv6 Addressing Architecture in IPv4 Network", *2010 Second International Conference on Communication Software and Netwroks*, 2010 IEEE.

[9] Mohd.Khairil Sailan, Rosilah Hassan and Ahamed Patel, "A Comparative Review of IPv4 and IPv6 for research Test Bed", *2009 International Conference on Electrical Engineering and Informatics*, 5-7 August 2009, Selangor, Malaysia.

[10] Yingjiao Wu and Xiaoqing Zhou, "Research on the IPv6 Performance Analysis Based on Dual-Stack and Tunnel Transition." *The 6th International Conference on Computer Science & Education*, August 3-5, 2011.SuperStar Virgo, Singapore.

[11] Ruri Hiromi and Hideaki Yoshifuji," Problem on IPv4-IPv6 Transition", *Proceedings of International Symposium on Application and the Internet Workshops*, 2005.

[12] B.Haberman, J. Martin, "Automatic Prefix Delegation protocol for Internet Protocol version 6 (IPv6)" IETF, draft work in progress, URL: http://www.ietf.org/internetdrafts/draft-haberman-ipngwg-auto-prefix-02.txt.

Sheryl Radley is a Full time Research Scholar under Anna University Chennai; she is currently doing the research in New address Scheme in IPv6 in Government College of Engineering, Tirunelveli, Tamil Nadu.

D.Shalini Punithavathani is the Principal of Government College of Engineering, Tirunelveli, Tamil Nadu. She had pursued her doctorate in IPv4/IPv6 transition mechanism.

L.K Indumathi is working as a Associate Professor in National College of Engineering, Marudakulam, Tamil Nadu. She is pursuing her doctorate in IPv6 Multihoming concept.