ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 4, April 2016**

# A Detail Comparative Review on IPv4/IPv6 Dual Stack Co-existence Techniques

Piyush Sharma[1], Ms. Renu Singla[2],

M. Tech Student, Dept. of CSE, Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India[1]

Asst. Prof., Dept. of CSE, Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India[2]

**ABSTRACT**: IPv4/IPv6 transition rolls out several issues to the internet world. IETF introduces some transition mechanisms involving IP transition, dual IP stack and tunneling transition techniques. A explained study is performed on the IPv6 addressing architecture. Out of the three techniques Tunneling proves to be most efficient in the study which has been performed. The 6rd technique that is utilized for IPv4/IPv6 transition technique allows an IPv6 mobile node to roam into IPv4 based network and achieved serviced besides roaming in IPv6 based network. This paper targets at a comparative study on the three transition mechanisms i.e. Software mesh which survive Dual Stack, NAT444 which supports translation and IPv6 Rapid Development (6rd) technique in tunneling mechanism.

**KEY WORDS***:* IPv4/6 transition, Dual Stack, tunnelling, 6rd, Software mesh, NAT444

## I. INTRODUCTION

In the Internet, data is exchanged in the form of network packets. IPv4 was the first version of the Internet protocol that was broadly spread for providing unique global computer addressing to make confirm that two entities can uniquely identify one another. IPv4 addresses are being depleted [4]. IPv6-also called IPng has been chosen from various introduced options as a proper successor of the available Internet Protocol. IPv6 mentions a new packet format, intended to reduce packet header processing by routers. Since, in most respects, IPv6 is an extended version of IPv4. IPv6 address is shown by 8 groups of 16-bit values from 0000-FFFF, every group shown as 4 hexadecimal digits and distinguished by colons (:). IPv6 has 128 bits and permits about 340 undecillion addresses. Thus the transition from IPv4-IPv6 has become an increasingly critical for the internet world where IPv4 and IPv6 are inter-compatible protocols. Multiple mechanisms have been introduced over these years to help the continuous development of the global Internet needed for total architecture development to accomplish the new techniques, that support the ever increasing no. of subscribers, appliances, applications and services i.e. transport Relay translation, NAT-PT have been evaluated for supporting the interoperability between IPv4 and IPv6. The transition mechanisms are widely classified into three categories: Translation, Dual Stack and Tunnelling. Both IPv4and IPv6 networks permit nodes utilizing auto configuring Protocol to maintain the resource's address space. The auto configuration protocol must be capable to choose, assign and allocate a unique network address to an un-configured node. Auto-configuring protocols can be categorized as state full and stateless. Ipv6 offers high security which has authentication and encryption options in comparison of IPv4. It also increases for better routing efficiency and network management. The processing has been simplified however no fragmentation is required because of existence of large address space which also neglects subnetting which is necessarily required in IPv4.

Much work and care have been given to the transition to IPv6, and much work has already been begun on measuring the security significances during this time [3, 4]. However, the Internet has been suffered by various worms; it is required to explore the worms activities in IPv4-IPv6 dual-stack networks. The random address space scanning is the most famous technique applied by the worms to discover dangerous targets in IPv4 networks. The efficiency of this technique attributes to the 32-bit IPv4 address which permits the random-scanning worms to examine all possible hosts [5, 6]. It is normally considered that the IPv6 protocol can offer better security against these worms because of its 128-bit large address space, so that the possibility to attain a valid address in the IPv6 address space by random-scanning is very less. Hence, the transition from IPv4 to IPv6 is assumed as an efficient method to preventing worms from dispersing [7]. It is seen in this research paper that the dual-stack worm can gather the IPv6 addresses of all active hosts

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

on the connection-local rapidly and efficiently, which result in accelerated worm dispersing on the IPv6 subnets. In actuality, those "isolated IPv6 islands" would really become the "hotbeds" for the dual-stack worm, particularly in the worm-propagation beginning phase. In another words, one infected host could infect all dangerous hosts on the same connection in a less time, while it may consider much higher time to infect the hosts in IPv4 networks with random-scanning technique. As a result, the deployment of IPv6 is not able to prevent the worm propagation as what was desired, but rather has opposite impact. However, it is risky to introduce a real worm into real networks, simulation and modelling are done to examine the features of the worm propagation and to inquire the defence mechanisms. In this research paper, the dual-stack worm is inquired by exploring its similar scanning mechanism to the self replicating natures of biological viruses.

## II. LITERATURE SURVEY

**Sheetal Borse et al. [1]** : Here, in this paper authors discusses various techniques for migration of IPv4 to IPv6 protocol through dual stack mechanism in Local Area Network(LAN).For the implementation purposes, they used Packet Tracer version 6.0.1 software. Performance is analysed using the Ping connectivity and Round Trip Time (RTT) of IPv4/IPv6 networks. After the simulation results, authors conclude that transition platform IPv4 based websites can be accessed and web page is displayed, yet, IPv6 based webpage can also be displayed unless the webpage is present at the server side.

**Ali Albkerat et al. [2] :** In this paper, authors analysed the various IPv6 transition technologies. In their work authors compares the performance of IPv4 and IPv6 in order to show the effects of transition strategy on network behaviour. In their work for performance evaluation, authors used the OPNET modeller that contains a WAN, a LAN, hosts and servers. After the simulation results, authors conclude that IPv6 has higher throughput. CPU utilization is lower for IPv4, IPv6 and dual stack than manual and 6to4 and also dual stack has less delay with TCP.

**Sheryl Radley et al. [3] :** Here authors present the evaluation and study of the Transition Techniques addressed on IPv4-IPv6 . In their work authors aimed 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 mechanism in tunnelling mechanism. For the simulation purpose, authors used NS-2 simulator. After the simulation result, authors conclude that effective way of transition is IPv6 Rapid Development method. The tunnelling mechanism shows a higher throughput value when compared to the other two mechanisms.

**Febby Nur Fatah et al. [4]:** In this paper authors analysed the performance of Dual Stack IPv4-IPv6 system in university network by using of jitter and delay period in interconnection. In their work, authors calculated the jitter and delay period by transferring different files with different size. For performance analysis, technique used by authors is the method by direct measurement of performance on the model or network prototype. After the implementation, authors conclude that Dual Stack system is most trustworthy implementation for migration of IPv4 to IPv6 system. Also IPv6 system is more stable and there is less jitter than IPv4.

**Table 1 below shows the various Internet Protocol version existed and their current status.**

| 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 1983 version | (current widespread) |
| 5 | ST(IPv5) | Stream Transport | (not a new IP, little use) |
| 6 | IPv6 | December 1998 version | (formerly SIP,SIPP) |
| 7 | CATNIP | IPng evaluation | (formerly TP/IX;deprecated) |
| 8 | Pip | IPng evaluation | (deprecated) |
| 9 | TUBA | IPng evaluation | (deprecated) |
| 10-15 | | Unassigned | |

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

**Table 2 below represents the difference between IPv4 and IPv6 [7]. From the table below the several characteristics for both Ipv4 and IPv6 is provided.**

| FEATURES | IPv4 | IPv6 |
|---|---|---|
| Addressing | Anycast, Unicast,Multicast,Broadcast | Anycast,Unicast,Multicast |
| Address | 32 bits | 128 bits |
| Checksum in Header | Included | Not Included |
| ARP | Used to resolve an IPv4 address | Replaced by Neighbor Discovery |
| Header includes option | Required | IPv6 Extension Header |
| Fragmentation | Done by the Routers and Source node | Only by the Source Node |
| DNS | Use Host address(A) resource records | Use host address(AAAA)resource records |
| IP Configuration | Manually or DHCP | Auto-Configuration or DHCP |
| QoS | Differentiated Services | Use traffic classes and flow level |
| IPsec Support | Optional | Required |
| IGMP | Use to manage local subnet group | Replaced with MLD |
| Mobility | Use Mobile IPv4 | MIPv6 with Faster Handover routing |

The three mechanisms were compared for a scenario consisting three networks, IPv4 only network, IPv6 network and both IPv4 and IPv6 network. Packets were of same data rate made to propagate with same bandwidth [9]. There was no intermediary node as such.

**Table 3: The table below represents the comparison between several transition mechanisms**

| Features | Dual Stack Technique | Translation Technique | Tunneling technique |
|---|---|---|---|
| IPv4 and IPv6 | Both needed | Either or can be converted | Either or can be tunneled |
| Throughput | High | High compared to tunneling | Low compared to Dual Stack |
| Latency | Medium | High | Low |
| Over head | High | Very high | Low |
| Load balance | External appliance required | Hardware required | Can be configured |
| Security Forensic | Most preferred | Medium | Low |
| Security | Medium | High | Very High |

## III. THE IPv4-IPv6 TRANSLATION SYSTEM

The transition phase from IPv4 to IPv6 has elicited several talks among the Internet community, as a lot of network administrators and companies are reluctant, confronting what they perceive as a major challenge with high costs. Apart from the hardware part and network issue, a very significant view is the modification (porting) of available applications so that they get IPv6 enabled. It is a essential step in the broader adoption of IPv6, not only because without them the novel infrastructure becomes waste for the subscriber, but also because applications have the capability to clearly establishes the benefits of IPv6. Mostly network applications in presence today assume the usage of the IPv4 protocol, so the transition to IPv6 has to be accomplished by the new applications development and/or the modification of the available ones, so that they can be utilized in IPv6 environments. It has usually established that the complexity of modifying available applications varies importantly from one situation to another. The principle rule of address translation is to demonstrate the mapping technique between receiver and sender, which can map message sequence on a specific protocol to another protocol sequences. Protocol conversion is a mechanism of the mapping from one sequence to another. The general technique of IPv4-IPv6 translation is the mapping of the IP header among the two protocols, substituting the header from sender to recipient; whether the higher layer of the two protocols carries out the similar substitution is based on differences among them [13,14,15]. In RFC6052 [15], a basic framework of stateless address translation is described. The IPv4 and IPv6 address structures are shown by Figure 1. The IPv6 address header is changed by neglecting or adjusting default for some information fields in the IPv4 protocol. Generally, the header of the two protocols is quite same that some fields can be directly copied between two protocols. In actual, others require to carry out translation.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

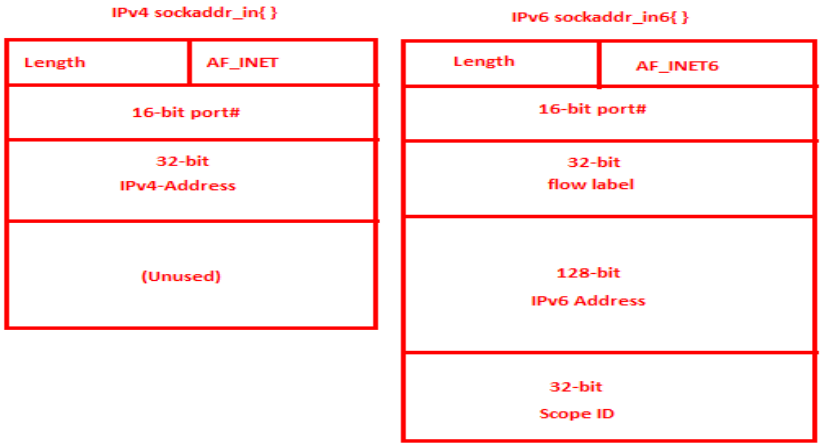


**Fig. 1: IPv4 and IPv6 address structures**

Mostly network applications in presence today assume the usage of the IPv4 protocol, so the transition to IPv6 has to be accomplished by the new applications development and/or the modification of the available ones, so that they can be utilized in IPv6 environments. It has usually established that the complexity of modifying available applications varies importantly from one situation to another. The principle rule of address translation is to demonstrate the mapping technique between receiver and sender, which can map message sequence on a specific protocol to another protocol sequences. Protocol conversion is a mechanism of the mapping from one sequence to another. The general technique of IPv4-IPv6 translation is the mapping of the IP header among the two protocols, substituting the header from sender to recipient; whether the higher layer of the two protocols carries out the similar substitution is based on differences among them [13,14,15]. In RFC6052 [15], a basic framework of stateless address translation is described. The IPv4 and IPv6 address structures are shown by Figure 1. The IPv6 address header is changed by neglecting or adjusting default for some information fields in the IPv4 protocol. Generally, the header of the two protocols is quite same that some fields can be directly copied between two protocols. In actual, others require to carry out translation.

***1. Dual Stack:*** The Dual Stack mechanism is also known as Dual IP layer or native dual stack. Both protocols IPv4 and IPv6 run parallels on the same network infrastructure which does not need encapsulation of IPv4 inside IPv6 and vice versa. Outdated resources do not support IPv6, thus it becomes significant to have a network which provides support to both IPv6 and IPv4 network. Operation of modes IPv6/IPv4 are: 1. IPv6-only operation where an IPv6 node has its stack enabled and its Ipv4 stack not enabled. 2. IPv4-only operation where an IPv4/IPv6 node has its IPv4 stack enabled and its Ipv6 stack not enabled. 3. IPv4/IPv6 operation where an IPv6/IPv4 node has both stacks enabled. A general dual-stack migration mechanism as represented in fig 2, builds a transition from the core to the edge. This involves enabling two TCP/IP protocol stacks on the WAN core routers. In a general dual stack migration firstly the perimeter routers, and firewalls, then the server-farm switches and at last the desktop access routers. Once the network provides support to IPv4 and IPv6 protocols, the process will enable dual protocol stacks on the servers and then the edge entities. The dual stack doubles the communication needs, which leads to performance reduction

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

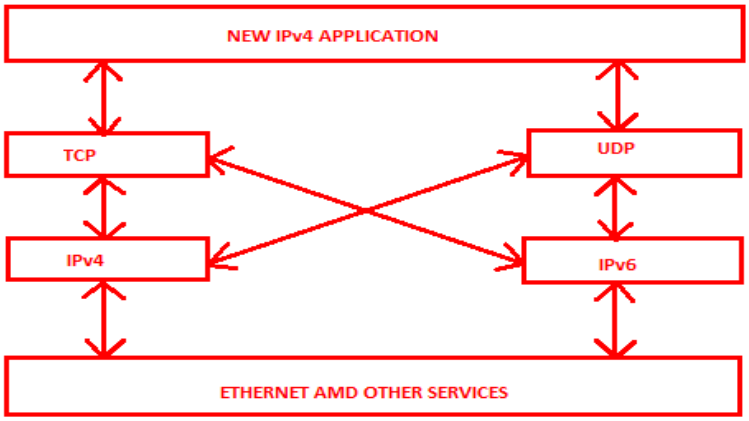


**Fig 2: Dual Stack Mechanism**

**2. Translational Transition mechanism**: It can be categorized as stateful and stateless technique. Stateless technique includes Bump in stack (BIS), Stateless Internet Protocol/ Control Messaging Protocol Translation (SIIT) and Bump in Application Programming Interface (BIA). The Stateful technique is categorized as Transport Relay Translator (TRT) and Network Address Translation-Protocol Translation (NAT-PT) [14]. In translation mechanism IP address information in IP packet headers is altered while in transit across a routing device. The IPv6 packets itself gets translated into IPv4 packet at the time of translation, and after translation vice versa. The translation can be performed from one-one to one-many. Network Address Translation (currently broadly utilized in IPv4) permits a small no. of public addressees to be shared by a large no. of hosts utilizing private addresses. It offers security advantages by building host more complicated to address directly by foreign machines on public internet.

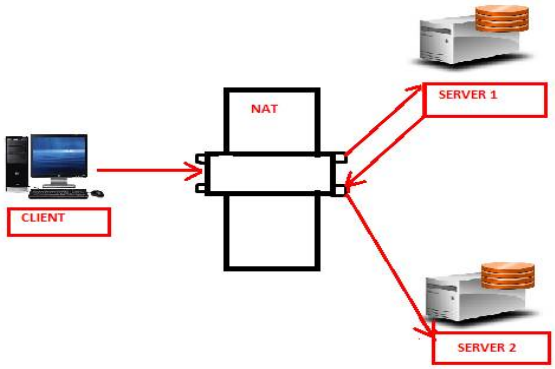


**Fig 3: IPv4/6 Translational Mechanism**

## IV. ISSUES TO BE CONSIDERED WHILE TRANISTION

Dual Stack transition assures and supports any kind of communication without regarding of the IP version which causes to doubling the communication processing needs. Performance reduction also happens in DS transition mechanism [17]. Translation technique results to complexity as end to end system is interfered by an element. While translating between IVI (IPv4/IPv6) [7], compatibility with all the existed applications must be considered into account. Issues arise because of lacking of public addresses in translation technique. Tunneling can be utilized for any version of protocol. The data to be transferred are compressed while tunneling which enhances the throughput of network. Tunneling technique enhances security between the entities end. However only one router takes care of tunneling in summation to routing the load/CPU utilization on that specific router is comparatively high and also it results to single point failure [11]. Trouble shooting gets more complicated as a node runs into hop count problems or Maximum Transmission Unit size problems, as well as fragmentation issues. Configuration must be automatic or dynamic. For encapsulation, tunnel end points should hold a track on peer end point [3].

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 4, April 2016**

## V. IPV6 TO IPV4 AUTOMATIC TUNNELLING MECHANISM

Automatic tunnelling means to a tunnel configuration that does not require direct management. An automatic IPv*6 to IPv4* tunnel enables an isolated IPv6 domain to be linked over an IPv4 network and then to a remote IPv6 networks. This tunnel handles the IPv4 infrastructure as a virtual non broadcast connection, so the IPv4 address inserted in the IPv6 address is utilized to determine the other end of the tunnel. The inserted IPv4 address can easily be extracted and the entire IPv6 packet provided over the IPv4 network, hidden in an IPv4 packet. No configured tunnels are needed to forward packets among *6to4*- capable IPv6 sites anywhere in IPv4 Internet. Fig 5 illustrates the *6to4* address format structure. The prefix field (FP) value is 0x001, which determines global unicast address. The Top-Level Aggregation identifier field (TLA) is allocated by the IANA for the IPv*6 to IPv4* technique. Thus, the IPv6 address prefix is 2002::/16 and the 32 bits after 2002::/16 show the IPv4 address of the gateway machine of the network in question. The packets hence know the way to any other network. The *6to4* technique is the most broadly extensively utilized automatic tunnelling mechanism [14]. It involves a technique for allocating an IPv6 address prefix to a network node with a global IPv4 address.

***IPv6 Tunnel Broker:*** The IPv6 Tunnel Broker offers an automatic configuration facility for IPv6 over IPv4 tunnels to subscribers linked to the IPv4 Internet [15]. IPv4 connectivity between the subscriber and the service supplier is needed.

I. The subscriber contacts Tunnel Broker and performs the registration mechanism.
II. The subscriber contacts Tunnel Broker again for authorization and offering configuration information (operating system, IP address, IPv6 support software, etc.).
III. Tunnel Broker sets up the network side end-point, user terminal and the DNS server.
IV. The tunnel is active and the subscriber is linked to IPv6 networks.

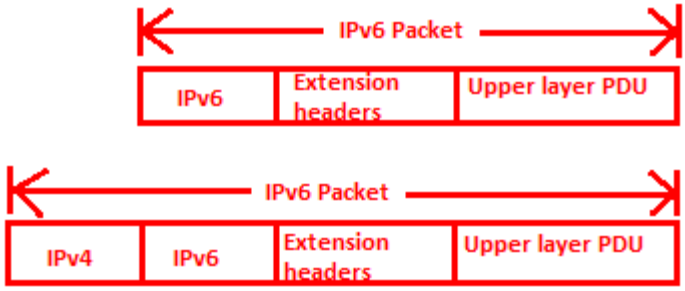


**Figure 4: *6over4* Address Link Layer Identifier**

## VI. IPV4/IPV6 TRANSLATION MECHANISM

The basic service of translation in IPv4/IPv6 transition is to translate IP packets. Many translation techniques depend on the SIIT (Stateless IP/ICMP Translation algorithm) algorithm [16]. The SIIT algorithm is utilized as a basis of NAT-PT (Network Address Translation-Protocol Translation) and the BIS (Bump In the Stack) techniques,

**1. Bump-In-the-Stack Mechanism:** BIS mechanism (RFC 2767) involves a translator module and a TCP/IPv4 protocol module, which Contain three bump components and is layered above an IPv6 module (Fig 6) [17]. Packets from IPv4 applications propagate into the TCP/IPv4 protocol module. The detected packets are translated into IPv6 packets and then sent to the IPv6 protocol module. The three bump components are the extension name resolver, which analyzes DNS lookups to find whether the peer node is IPv6- only; the address mapper, which assigns a local IPv4 address to the IPv6 peer and caches the address mapping; and the translator, which interprets packets between IPv6 and IPv4 protocol.

**2. Network Address Translation-Protocol Translation:** The NAT-PT technique is a stateful IPv4/IPv6 translator [18][19]. NAT-PT nodes are at the boundary between IPv4 and IPv6 networks. Every node manages a globally routable IPv4 addresses pool, which are dynamically allocated to IPv6 nodes when sessions are started throughout the IPv4/IPv6 boundary. This technique permits native IPv6 nodes and applications to interact with native IPv4 applications and nodes, and vice versa. The NAT-PT translation architecture, shown in Fig 7, also involve one or more ALGs (Application Level Gateways). The fundamental NAT-PT function does not snoop packet payloads, and the application may thus be unknown of it. Thus, the NAT-PT technique is based on ALG agents that permit an IPv6 node to interact

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 4, April 2016**

with an IPv4 node and vice versa for particular applications. The NAT-PT technique is an interoperability solution that requires no modification or additional software, i.e. dual stacks, to be installed on any of the end subscriber nodes, either the IPv6 or the IPv4 network. This technique implements the needed interoperability functions within the core network, building interoperability between nodes easier to maintain and quicker to manifest. Tunnelling mechanisms as represented in fig 5 are more suitable as compared to dual stack and translation mechanisms. Tunnels are utilized to carry one protocol inside another. Most access network works over IPv4 [13]. Subscribers of these networks might require to get linked to IPv6 internet. Thus, ISP should offer IPv6 access over IPv4 only network, which could be obtained through IPv6 over IPv4 tunnel. These tunnels consider IPv6 packets and encapsulate them in IPv4 packets to be forwarded across network portions that haven't yet been upgraded to IPv6 [10].
Tunnels can be generated where there are IPv6 islands distinguished by an IPv4 ocean, which will be the norm during the early phases of the transition to IPv6. After that there will be IPv4 islands that will require to be bridged across an IPv6 ocean. Tunnels are categorized as: manual and dynamic [1]. Manually configured IPv6 tunneling needs configuration at both tunnel ends, whereas dynamic tunnels are generated automatically depending on the routing and packet destination address. Dynamic tunneling mechanisms simplify management as compared with statically configured tunnels, but static tunnels build traffic information existed for every endpoint, offering additional security against injected traffic [15]. Many tunneling mechanisms are Automatic tunneling utilizing IPv4 Compatible address, 4 over 6 tunneling, 6 over 4 tunneling, 6 in 4 tunneling, 6 to 4 tunneling, terado, Intrasite, Automatic tunneling Addressing Protocol (ISATAP) and IPv6 Rapid Development (6rd). With dynamic tunnels it isn't easy to track who is interacting over the transient tunnels and the tunnel destination end point is not known.

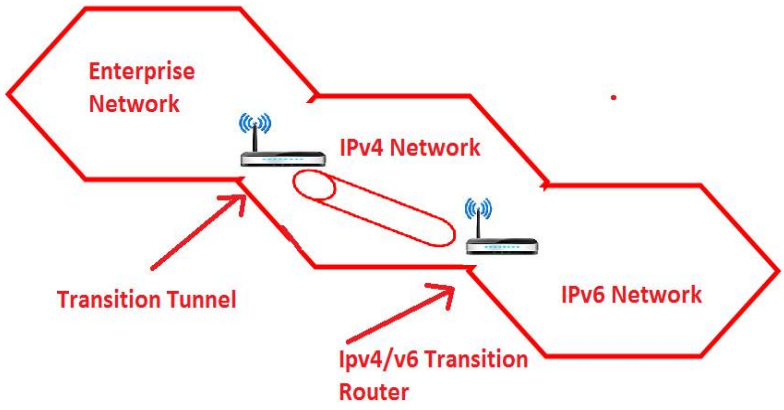


**Fig 5: Tunneling Mechanism**

## VII. NETWORK ADDRESS TRANSLATION 64

In NAT, an IP address make a private address pool is interpreted to a globally unique, publicly approachable IP address. Optionally, the technique translates source port information so that several private IP addresses can share a restricted no. of global IP addresses. NAT666 is a extended version of the conventional NAT technique. It includes two layers of port and address translation. The first occurs at the Customer Premises Equipment (CPE) and the second occurs at the ISP, Which utilizes an ability called as Large Scale Network Address Translation (LSN). The term NAT64 represents translation from one IPv6 block to a second IPv6 block, adopted by a third IPv6 block. The first block is a private address at the CPE. The second one is another private IP address block between the ISP and the CPE, and the third is a globally approachable public block.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

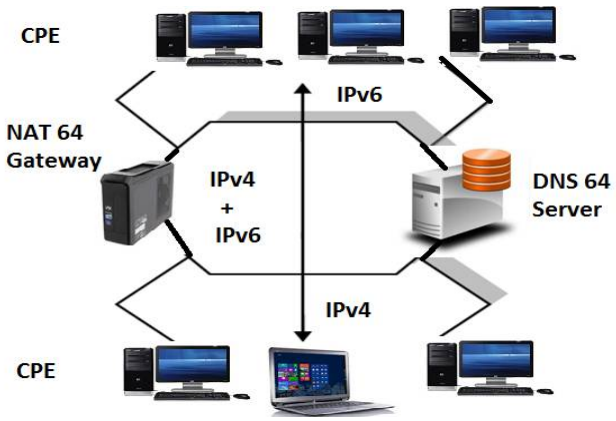


**Fig 6: NAT64 Tunneling Mechanism**

NAT 666 does not need the substitute of available CPE devices. It uses the proven NAT technique. It also does not need changing other network elements i.e. Domain Name Service. But then there could be a possible overlap between the users private address block and the private address block utilized between the CPE and the service supplier. This could lead to packets misrouting. The classic drawbacks of NAT666 technique, is masking of end subscribers IP address and breaking end-to-end interaction even more for application that embed IP addresses inside the packet payload, i.e. media applications, because it includes invoking the NAT technique twice for transmission. The packets routing between two different users behind the same LSN is also challenging and may need a change in firewall schemes. The NAT64 technique as represented in fig 4 is utilized for both the transition of coexistence of IPv6 and IPv4. It operates together with DNS64, necessarily a DNS translation facility, to enable client-server communication between an IPv4-only server and an IPv6-only client and vice versa. It permits for peer-to-peer communication that initiates from an end-node running either of the two protocols. NAT64 uses a pre-allocated IPv6 prefix to algorithmically interpret IPv4 addresses of IPv4 servers. The NAT64 is entirely transparent to end-subscribers because address translation happens at the service supplier network edge and it includes no change in client-end CPE devices. It also permits transition to IPv6 while preserving available IPv4-based infrastructure. It provides coexistence of IPv6-only and IPv4 only devices while assuring continuous communication between the two in the transition period.

## VII. 6RD MECHANISM

IPv6 rapid development is a automatically configuring, stateless, resilient, naturally scalable, point to multi point tunneling technique. IPv6 to IPv4 encapsulation is utilized in tunneling technique. The 6rd model is utilized to deploy IPv6 over the available IPv4 infrastructure of service suppliers. The technique relies upon algorithm mapping between IPv6 and IPv4 addresses allocated for utilization within the service supplier network. A 6rd mechanism [12] needs deploying one or more 6rd aware border relay routers and 6rd aware CPE. The CPE device encapsulates IPv6 packets, which are then taken over the service supplier's IPv4 network to border relay routers. The 6rd relay routers then encapsulates the packet and sends it natively to an IPv6 network as represented in fig 7.
The model enables service suppliers to provide IPv6 services alongside IPv4 services, while building minimal upgrades to their available IPv4 infrastructure. The model can be decommissioned upon completion of a service supplier's IPv4 network migration to a dual stack model. The two important components of 6rd model are: 1). Customer Equipment: IPv6 traffic coming from the end subscriber hosts is encapsulated in IPv4 also encapsulated and 6rd traffic achieved from the Internet through the BR router is de-capsulated. 2). Border Relay: router offers link between the Ipv6 network and CE routers. The disadvantage of 6rd is that, it needs upgrading CPE devices constantly. Service suppliers easily accommodate new subscribers with new equipment, but it may not be economical to upgrade available users. A 6rd prefix as represented in the fig 6 is chosen by the service provider for the usage of 6rd domain. There is exactly one 6rd prefix for a provided 6rd domain, as SP may deploy 6rd with a multiple 6rd domain or single 6rd domain. The IPv6 prefix [6] computed by CE for usage within the user site by integrating the 6rd prefix and the CE IPv4 address achieved by IPv4 configuration techniques. This prefix can be taken logically equivalent to an IPv6 delegated prefix. CE offers a range of prefixes to their sites.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 4, April 2016**

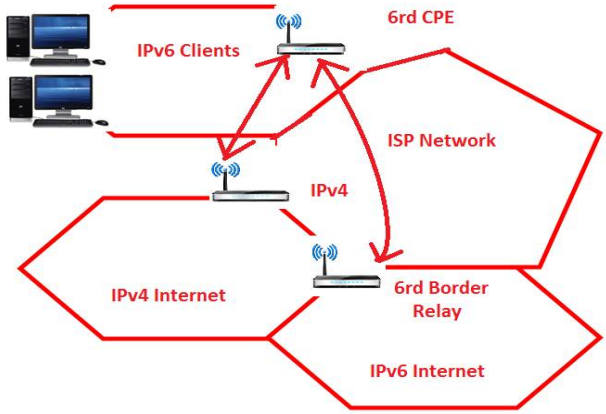


**Fig 7: IPv6 6rd Mechanism**

## VIII. CONCLUSION

This paper covers the different transition techniques that were utilized for the transition between IPv6 networks to IPv4 networks and vice versa. The total review confirms the efficient way of transition is IPv6 Rapid Development method. The work to bring out the most efficient method as compared to IPv6 Rapid Development is on process as it leads to large overhead and it is not appropriate for huge mobile networks. For further work, the performance of the work to be introduced can be measured utilizing NS2 simulator. Moreover, the problem of IPv4 addressing in Ipv6 network may be taken into consideration for further research.

## REFERENCES

[1] Grosse, E. and Lakshman, Y. "Network processors applied to IPv4/IPv6 transition", IEEE Network, Vol. 17(4), pp.35-39, 2003.
[2] Ali, A. "Comparison study between IPv4 & IPv6", International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue No. 3, pp.314-317, 2009.
[3] Batiha, K. "Improving IPv6 Addressing Type and Size", International Journal of Computer Networks & Communications (IJCNC), Vol. 5, Issue 4, pp.41-51, 2013.
[4] I. Parra, J. "Comparison of IPv4 and IPv6 Networks Including Concepts for Deployment and Interworking", INFOTECH Seminar Advanced Communication Services (ACS), pp.1-13, 2012.
[5] Sailan, M., Hassan, R. and Patel, A. ,"A comparative review of IPv4 and IPv6 for research test bed", In Proceedings of International Conference on Electrical Engineering and Informatics (ICEEI '09), Malaysia, pp.427-433, 2009.
[6] Ahmad, N. and Yaacob, A. " IPSec over Heterogeneous IPv4 and IPv6Networks: Issues and Implementation", International Journal of Computer Networks & Communications (IJCNC), Vol. 4(5), pp. 57-72, 2012.
[7] Arafat, M., Ahmed, F. and Sobhan, M."On the Migration of a Large Scale Network from IPv4 to IPv6 Environment", International Journal of Computer Networks & Communications (IJCNC), 6(2), pp.111-126, 2014.
[8] Wu, P., Cui, Y., Wu, J., Liu, J. and Metz, C. "Transition from IPv4 to IPv6: A state-of-the-art survey", IEEE Communications Surveys & Tutorials, 15(3), pp.1407—1424, 2013.
[9] Wu, Y. and Zhou, X." Research on the IPv6 performance analysis based on dual-protocol stack and Tunnel transition", Proceedings of the 6th International Conference on Computer Science & Education (ICCSE), pp.1091—1093, 2011.
[10] Chen, J., Chang, Y. and Lin, C." Performance investigation of IPv4/IPv6 transition Mechanisms", Proceedings of the 6th International Conference on Advanced Communication Technology, pp.545—550, 2004.
[11] Narayanan, A., Mohideen, M. and Raja, M. "IPv6 Tunnelling Over IPV4", International Journal of Computer Science Issues (IJCSI), 9(2), pp.599-604, 2012.
[12] Xiaodong, Z. "Research on the Next-generation Internet transition technology", In Proceedings of Second International Symposium on Computational Intelligence and Design (SCID '09), pp.380-382, 2009.
[13] A. Law, W. Kelton, and W. Kelton, "Simulation modelin and analysis". McGraw-Hill New York, vol. 2, 1999.
[14] Y. Wang, S. Ye, and X. Li, "Understanding Current IPv6 Performance: A Measurement Study," in 10th IEEE Symposium on Computer Communications, Jun. 2005.
[15] X. Zhou, R. E. Kooij, H. Uijterwaal, and P. van Mieghem, "Estimation of Perceived Quality of Service for Applications on IPv6 Networks," in ACM PM2HW2N'06, Oct. 2006.
[16] D. P. Pezaros, D. Hutchison, F. J. Garcia, R. D. Gardner, and J. S. Sventek, "Service Quality Measurements for IPv6 Inter-networks," in 12th IEEE IWQoS, Jun. 2004.
[17] T.-Y. Wu, H.-C. Chao, T.-G. Tsuei, and Y.-F. Li, "A Measurement Study of Network Efficiency for TWAREN IPv6 Backbone," International Journal of Network Management, vol. 15, no. 6, pp. 411–419, Nov. 2005.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 4, April 2016**

[18] K. Cho, M. Luckie, and B. Huffaker, "Identifying IPv6 Network Problems in the Dual-Stack World," in ACM SigComm Network Troubleshooting Workshop, Sep. 2004.
[19] S. Zeadally and L. Raicu, "Evaluating IPv6 on Windows and Solaris," IEEE Internet Comput., vol. 7, no. 3, pp. 51–57, May/Jun. 2003.
[20] R. Sargent, "Verification and validation of simulation models," in Proceedings of the 37th conference on Winter simulation. Winter Simulation Conference, pp. 130– 143, 2005.
[21] A. Law, "Statistical analysis of simulation output data: the practical state of the art," in Simulation Conference, 2007 Winter. IEEE, pp. 77–83,2008.
[22] OPNET, Modeler Release, 14th ed. [Online]. Available: http://www.opnet.com/solutions/network_rd/modeler.html.
[23] K. Salah, P. Calyam, and M. Buhari, "Assessing readiness of IP networks to support desktop videoconferencing using OPNET," Journal of Network and Computer Applications, vol. 31, no. 4, pp. 921–943, 2008.
[24] J. Moy, "OSPF Version 2," RFC 2328 (Standard), Internet Engineering Task Force, Apr. 1998, updated by RFC 5709. [Online]. Available: http://www.ietf.org/rfc/rfc2328.txt.
[25] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," RFC 5340 (Proposed Standard), Internet Engineering Task Force, [Online]. Available: http://www.ietf.org/rfc/rfc5340.txt, July 2008.
[26] P. Chimento and J. Ishac, "Defining Network Capacity," RFC 5136 (Informational), Internet Engineering Task Force, [Online]. Available: http://www.ietf.org/rfc/rfc5136.txt, Feb. 2008.
[27] K. Salah, P. Calyam, and M. Buhari, "Assessing readiness of IP networks to support desktop videoconferencing using OPNET," Journal of Network and Computer Applications vol. 31, no. 4, pp. 921–943, 2008.
[28] O. Balci, "Principles and techniques of simulation validation, verification, and testing," in Simulatio Conference Proceedings, 1995. Winter. IEEE, pp 147–154, 2002.
[29] K. Pawlikowski, H. Jeong, J. Lee et al., "On credibility o simulation studies of telecommunication networks," IEE Communications Magazine, vol. 40, no. 1, pp. 132–139, 2002.