IJCTA, 9(27), 2016, pp. 303-311 ISSN: 0974-5572

IPv6–The Future Internet Protocol (A Sensible and Comparative Technical Study with IPv4)

S. Manimozhi* and J. Gnana Jayanthi**

ABSTRACT

Today, the two most important Internet Protocols such as Internet Protocol version 4 (IPv4) and Internet Protocol version6 (IPv6) are designed and developed with a lot of various upgrading proposals by Request For Comments (RFC). The IPv4 is defined by Internet Engineering Task Force (IETF) RFC 791. IPv4 lacks in address space parceling for the current population. This issue has been solved by the Next Generation Protocol called IPv6. To standardize, IPv6 protocol has been repeatedly enhanced and modified for its scalability, routing, security and for many other areas. However, both IPv4 and IPv6 are not interoperable. Hence this paper highlights the several significant features in comparison with its earlier version protocol in use. The paper aims to help the companies and enterprises to realize the business benefits of IPv6 and move to the immediate deployment of IPv6.

Keywords: IPv6 Address and Configuration, IPv6 Addressing, IPv6 Routing, IPv6 Mobility, IPv6 QoS, IPv6 Security, IPv6 Transition Mechanisms, IPv6 Global Usage Status, IPv6 Research Projects.

1. INTRODUCTION

One of the core protocols which is widely used in the Internet is the Internet Protocol version 4 (IPv4), has been developed around 1970s. This IPv4 protocol, capable of providing more than 4 billion unique addresses, creates much of the traffic in the Internet and this is due to the commercialization of the IPv4 Internet [1]. Presently, only 220.922/8 of address blocks are available for use in the public IPv4 Internet. The recent status of the total IPv4 address space is indicated in the figure, Figure 1.

Initial design of IPv4 did not anticipate the escalation in the Internet growth and therefore created a lot of issues. Of many issues, the two major issues in IPv4 are (i) ROuting and (ii) ADdressing (ROAD). The Internet authority community forecasted late in 1980s that there might be addresses depletion in IPv4 [2]. Next to IPv4, STream (ST) protocol, version 5 of the Internet Protocol version was proposed. But, it doesn't satisfy the essential needs. Then, the purpose of Simple Internet Protocol (SIP) has been identified as an alternative to IPv4 protocol. SIP was carefully revised and referred to as IPng. IETF renamed this new protocol, IPng, as Internet Protocol version 6 (IPv6) defined by RFC 1736 in the year 1995. The IETF, first published the basic IPv6 protocol in 1998. It has since seen a number of enhancements, such as the addition of mobile IPv6 specifications in 2004 [3].

This paper is structured as follows. Section 2 analyzes the technical features of IPv6 in comparison with IPv4 in terms of addressing architectures, configuration, headers, routing, neighbor discovery, mobility, security and quality of service. IPv4 to IPv6 Transition Mechanisms such as Dual Stack mechanism, Tunneling mechanism and Network Address Translation mechanisms are summarized in the section 3. This paper is concluded in section 4.

* Research Scholar, Department of Computer Science, Bharathiyar University, Coimbatore, Tamilnadu, *Email: manimozhi.subramanian@gmail.com*

** Assistant Professor, Department of Computer Science, Rajah Serfoji Govt. College, (Autonomous), Thanjavur, Tamilnadu, *Email: jgnanamtcy@gmail.com*

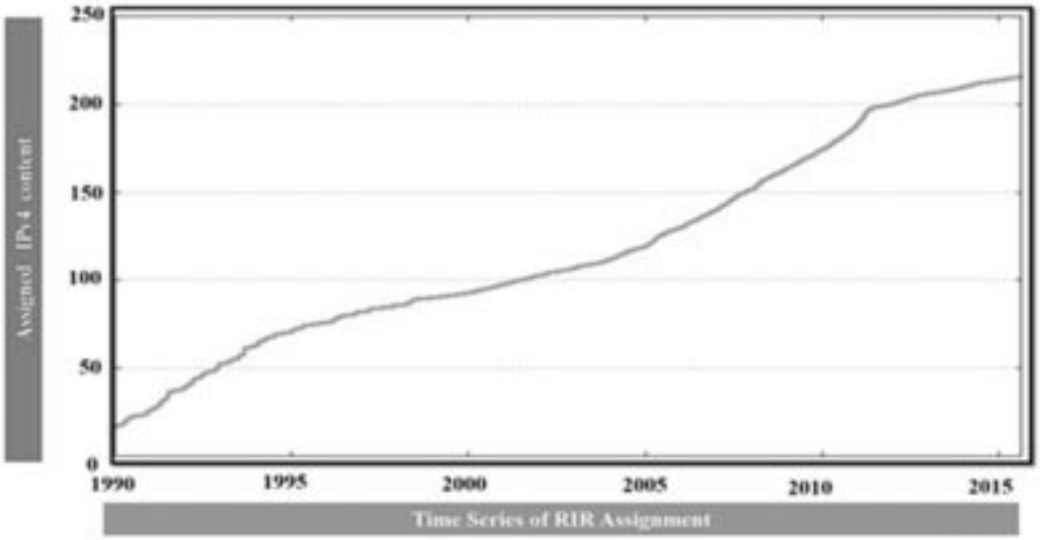

Figure 1: IPv4 Remaining Address Space Current Status

2. IPV6 TECHNICAL FEATURES

Of the several significant key features of the next generation protocol, IPv6, is its pool of addresses with a simplified address header format, address auto-configuration with not requiring Network Address Translation (NAT) and private address collisions. In IPv6 multicast routing is, simplified providing efficient routing and discovery methodologies, true Quality of Service (QoS), improved security with built-in authentication and privacy support, flexible options and extensions, easier administration without the need of Dynamic Host Configuration Protocol (DHCP), better provisions for ad-hoc networking for devices and smooth transition from the existing IPv4 protocol. These features are precisely summarized below.

2.1. IPv6 Address Size

IPv6 with 128 bits in address length is capable of providing 2^{128} unique addresses which are exactly 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 unique addresses and represented as eight groups of four hexadecimal digits with the groups being separated by colons (:) having 16 binary bits each, whereas IPv4 with 32 bits in address length is capable of providing 2^{32} unique addresses which are exactly 4,294,967,296 unique addresses; and represented four groups of dotted decimal number with groups separated by dots (.) having 8 binary bits each, in the range 0 to 255 [4].

2.2. IPv6 Address Class

IPv4 addresses are grouped and identified as Classful and Classless addresses. Classful address are categorized as Class A, Class B, Class C, Class D and Class E. Classless address is defined by Classless Inter-Domain

Table 1
Address Classes in IPv4

S.No	*Address Category*	*Address Prefix (bits)*	*Leading Bits*	*Total Address*	*Start Address*	*End Address*
1	Class A	1-126	0	2,147,483,648 (231)	0.0.0.0	127.255.255.255
2	Class B	128-191	10	1,073,741,824 (230)	128.0.0.0	191.255.255.255
3	Class C	192-223	110	536,870,912 (229)	192.0.0.0	223.255.255.255
4	Class D	224-239	1110	268,435,456 (228)	224.0.0.0	239.255.255.255
5	Class E	240-255	1111	268,435,456 (228)	240.0.0.0	255.255.255.255

Routing (CIDR) - an IPv4 address prefix in which 21 bits are fixed, leaving 11 bits for host IDs and Address categories are listed in Table.1. However in IPv6, the addresses are Classless addresses [5, 6, 7].

2.3. IPv6 Addresses based on the Routing

Based on the types of communications or routing the information, the IPv6 addresses are classified as (i) Unicast addresses (identifies a single interface), (ii) Multicast addresses (identifies multiple interfaces) and (iii) Anycast addresses (identifies multiple interfaces wherein the packets addressed to an anycast address are delivered to the nearest interface that is identified by the address). Further, IPv6 unicast addresses are classified as (i) Aggregatable global unicast addresses; (ii) Link-local addresses; (iii) Site-local addresses; (iv) Special addresses; (v) Compatibility addresses and (vi) NSAP addresses. There is no broadcast address in IPv6 [6, 8]. However, IPv4 offers unicast addresses, multicast addresses and broadcast address. The address types in IPv4 and IPv6 are listed in table, Table.2.

Table 2
Address Types of IPv4 and IPv6

S No	*Address Type*	*IPv4*	*IPv6*
1	Multicast Address	Multicast address space at 224.0.0.0/4	Multicast address space at FF00::/8
2	Broadcast Address	Has broadcast addresses for all devices	No such concept in IPv6 (uses multicast groups)
3	Unspecified Address	Uses 0.0.0.0 as unspecified address	Uses :: as unspecified address
4	Loopback Address	Uses 127.0.0.1 as loopback address	Uses ::1 as loopback address 0:0:0:0:0:0:0:1 (or ::1)
5	Global / Public Address	Supports globally unique "public" addresses	Supports globally unique unicast addresses
6	Local / Private Address	Uses 10.0.0.0/8, 172.16.0.0/16, and 192.168.0.0/16 as "private" addresses	Uses FD00::/8 as unique local addresses

2.4. -IPv6 Address Configuration

In IPv4, the address of a host, network mask and default gateway are to be configured manually with DHCP by a Network Administrator. The standardized IPv6 protocol has proven for auto-dynamic assignment of IPv6 addresses to the hosts. "Stateful Auto-Configuration" and "Stateless Auto-Configuration" are the two types of Auto-Configuration in IPv6 [9].

2.4.1. Stateful Address Auto-Configuration

Similar to the IPv4 – DHCP address configuration, IPv6 addresses are generated by using Dynamic Host Configuration Protocol version 6 (DHCPv6) without an external support, for installation and administration of nodes over IPv6 network.

2.4.2. Stateless Address Auto Configuration (SLAAC)

Stateless Address Auto Configuration (SLAAC) is the process of creating host address based on its hardware (Medium Access Control (MAC)) address. In SLAAC, an IPv6 node should connect with other IPv6 node through one IPv6 router. It allows each host to determine its address from the contents of received user advertisements. It makes use of the Institute of Electrical and Electronics Engineers (IEEE) Extended Unique Identifier (EUI-64) standard to define the Network Identity (NID) address.

2.5. IPv6 Header Format

An IP header is a prefix to an IP packet which contains the information of IP version, source IP, destination IP, time-to-live, etc. The format of IPv4 and IPv6 are different as shown in the following figures Figure 2. and

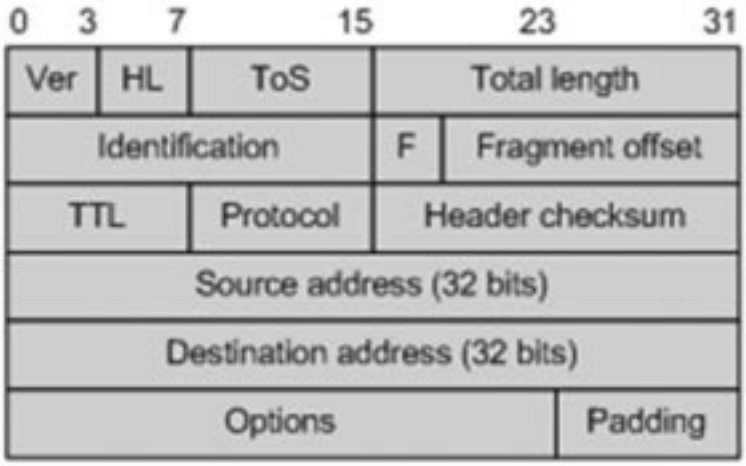

Figure 2: IPv4 Header Format

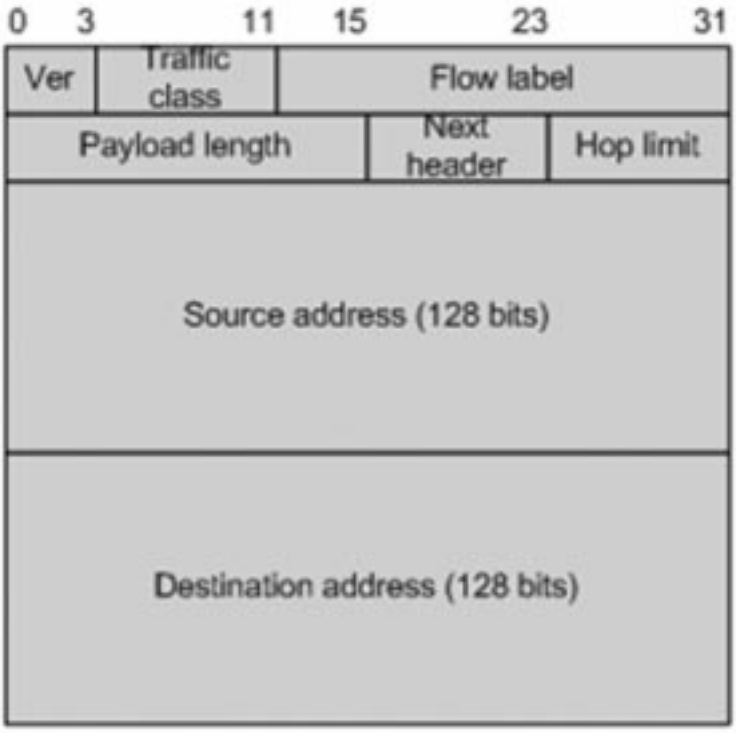

Figure 3: IPv6 Header Format

Figure 3. respectively. An IPv6 header contains new features when compared to IPv4 header. IPv6 header format is optimized to use 64 bits [4, 6, 8, 10, and 11]. The IPv6 header has been simplified to 8 than that of IPv4 with 14 fields. While IPv6 addressing is 4 times as large as IPv4, the header size of IPv6 twice as larger than IPv4 header size.

The IPv6 header was designed to maximize the efficiency and minimize header overheads. To provide some new features, some of the fields in IPv4 have been replaced in IPv6 and some more have been removed as listed in the following table, Table 3.

2.6. IPv6 Routing

The routing process is done by using different routing algorithms and it is not explicitly defined to its processor. The routing protocols are classified as Interior Routing Protocol (IRP) and Exterior Routing Protocol (ERP). IRP is used to route information within an autonomous system for routes information among routers inside its boundary

Table 3
Difference between IPv4 and IPv6 Header Format

S. No	*Field Name*	*IPv4*	*IPv6*
1.	Version	Yes	Yes
2.	Header Length	Yes	No
3.	Type of Service	Yes	Replaced by the TRAFFIC CLASS field.
4.	Total Length	Yes	Replaced by PAYLOAD LENGTH field.
5.	Identification	Yes	No
6.	Flags	Yes	No
7.	Fragment Offset	Yes	No
8.	Time to Live	Yes	Replaced by the HOP LIMIT field
9.	Protocol	Yes	Replaced by the NEXT HEADER field
10.	Header Checksum	Yes	No
11.	Source IP Address	Yes	Field increased from 32 bits to 128 bits
12.	Destination IP Address	Yes	Field increased from 32 bits to 128 bits
13.	Options	Yes	No
14.	Padding	Yes	No

Table 4
IPv4 and IPv6 Routing Protocols

S. No.	*Types of Routing Protocols*	*Name of the Protocols*	*Internet Protocols*			
			IPv4	*Algorithm*	*IPv6*	*Algorithm*
1.	Interior Gateway Protocol	Routing Information Protocol	RIPv1 RIPv2	Distance Vector Distance Vector	RIPng	Distance Vector
		Open Shortest Path First	OSPF v2	Shortest Path	OSPFv3	Shortest Path
		Intermediate System to Intermediate System	IS-ISv4	Link State	IS-ISv6	Link State
2.	Exterior Gateway Protocol	Border Gateway Protocol	BGP	Path Vector	BGPv4	Distance Vector

and ERP is used to routes information between two different autonomous systems. The most important routing algorithms are used to route the packets like Distance Vector Routing algorithm and Link-State Routing algorithm [12]. The most important used routing protocols in IPv4 and IPv6 are listed in Table 4.

2.7. IPv6 Neighbor Discovery Protocol

IPv4 uses the process of resolving 32 bits IPv4 address into a 48 bits physical address (MAC Address) through Address Resolution Protocol (ARP) [13]. Likewise IPv4 protocol uses the processes of the Router Discovery and Redirect message through the Internet Control Message Protocol (ICMP). The processes of resolving into MAC address, Router Discovery and Redirect message are all combined into a single protocol called Neighbor Discovery Protocol (ND) in IPv6 protocol [14]. Also ND provides additional functionality to identify the relationships between different neighboring devices in an IPv6 network [15].

2.8. IPv6 Mobility

Mobile Internet (MIP / MIPv4) protocol provides a node's mobility from its home network into another network (referred as foreign network) by acquiring a new IP address, called a Care-of Address (CoA). Further, MIP

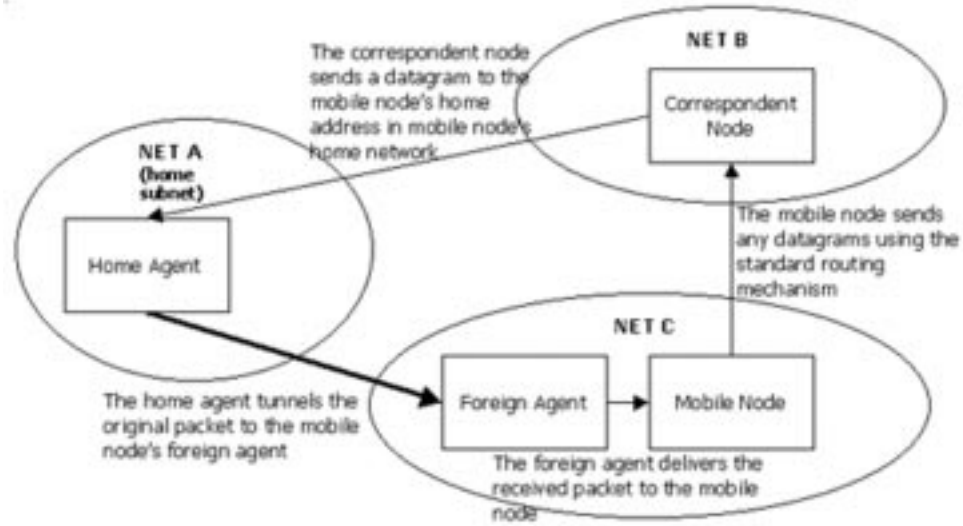

Figure 4: Data delivery in MIP protocol

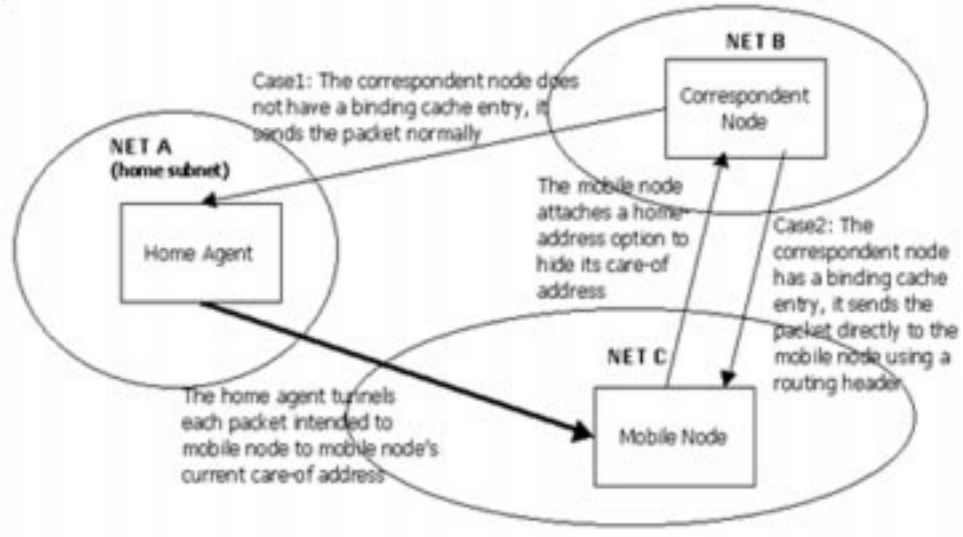

Figure 5: Data delivery in MIPv6

involves two kinds of mobility agents to achieve the transparent mobility, called (i) the home agent and (ii) the foreign agent. At least one home agent is required to be present in the home subnet of the mobile node. Even though mobility of an IPv4 node to another IPv4 network is possible, there arises a problem of triangular communication between Home Agent, Foreign Agent and Destination Agent through a tunnel [16], as shown in figure, Figure 4.

This triangular routing in MIP is resolved in IPv6 mobility and it is the integral part of IPv6. IPv6 mobility enables a mobile node to move from one link to another link without changing the mobile node's IP address. Henceforth, MIPv6 provides the mechanisms to allow mobile nodes to change their locations and addresses without losing the existing connections [2, 4, 6, 15] as shown in figure, Figure 5.

2.9. IPv6 Security

In IPv4 the security issues are implemented using Internet Protocol Security (IPSec) [17]. The data in network is protected by using authenticating and encrypting methodologies. In IPv4, IPSec is an optional field and security concept is implemented in end to end layer. IPSec utilizes the Authentication Header (AH) and Encapsulating Security Payload Header (ESP) [18]. IPv6 provides end-to-end encryption by using integrity

checking process in all compatible devices and systems. The process of IPSec is same for both IPv4 and IPv6 but in IPv6, IPsec is an integral part and it can be utilized for the entire routing. The security issues are same in IPv4 and IPv6 but IPv6 has more security problems when compared to IPv4. So, there is a need to implement separate IPv6 security mechanisms.

MIP / MIPv4 introduce three authentication extension headers that are used to authenticate the registration requests and replies between the following parties: mobile node-home agent, mobile node-foreign agent and home agent-foreign agent. Unlike in MIPv4, the low level security mechanisms are not part of the protocol specification in mobile IPv6. Instead, MIPv6 relies on IPSec to provide the necessary mechanisms for authentication and encryption. MIPv4 is that due to use of IPSec, MIPv6 also supports data encryption in addition to authentication. MIPv6 protocol specifies that all packets carrying binding update or binding acknowledgement destination options must be authenticated using AH or ESP. Both of the headers provide sender authentication, data integrity protection, and replay protection. The functionality of AH closely matches the MIPv4 security mechanisms but reliance on standard security mechanism makes implementing MIPv6 easier and in a way MIPv6 less prone to implementation or specification errors.

2.10. IPv6 Quality-of-Service (QoS)

IPv4 QoS is defined through the use of the *type of service* and *IP precedence bits* in the IP header. *Differentiated service* provides in a greater number of IPv4 networks because of the increasing penetration of Voice over IP (VoIP) and other quality of service-sensitive technologies. In IPv6, a similar IP header field, known as *traffic class*, enables originating nodes or forwarding routers to determine the priority of various IPv6 packets from various priority levels and flow label field - which is designed to request specific treatment for a sequence or flow of packets and slates to be used in an identical manner to the current differentiated service bits. QoS features supported for IPv6 environments include packet classification, queuing, traffic shaping, Weighted Random Early Detection (WRED), class-based packet marking, and policing of IPv6 packets [19]. QoS has been comprehensively integrated into IPv6 for better resolution of the various qualities of service.

3. IPV4 TO IPV6 TRANSITION MECHANISMS

The complete transition from IPv4 to IPv6 is possible only if (i) IPv6 is backward compatible with IPv4; (ii) Existing IPv4-only equipments (routers, bridges, switches, servers, client nodes etc.) are to be replaced with IPv4/ IPv6 compatible equipments or IPv6-only equipment; and (iii) whether the existing hardware chipset and the existing software version support IPv6. Of all, since IPv6 is not backward compatible with IPv4, there is a need for other new technologies. IPv4 can still work along with the newer version called IPv6, without any additional changes. However, to provide a communication between IPv4 mobile nodes with IPv6 mobile nodes, three new transition mechanisms were introduced called (i) Dual Stack mechanism, (ii) Tunneling mechanism, and (iii) Network Address Translation mechanism.

3.1. Dual Stack mechanism

A router / a server is installed with both protocols, IPv4 and IPv6 addresses configured on its interfaces to allow both IPv4 and IPv6 communication to take place between IPv4 node and IPv6 node without changing their respective IP versions. The following figure, Figure.6 depicts the dual stack mechanism.

3.2. Tunneling mechanism

When IPv4 communications are taking place and if there is an IPv6 network in between the corresponding IPv4 networks, a tunnel is created in the IPv6 network to encapsulate IPv4 packets in IPv6 network and this process is depicted in the following figure, Figure 7.

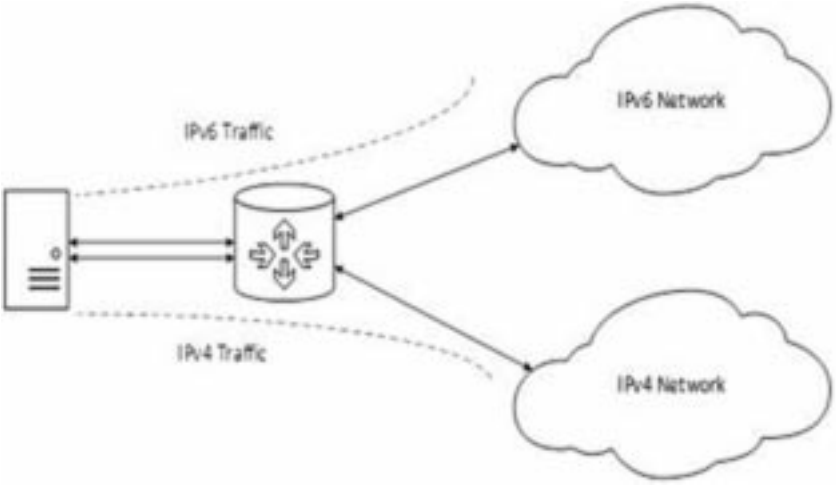

Figure 6: Dual Stack Mechanism

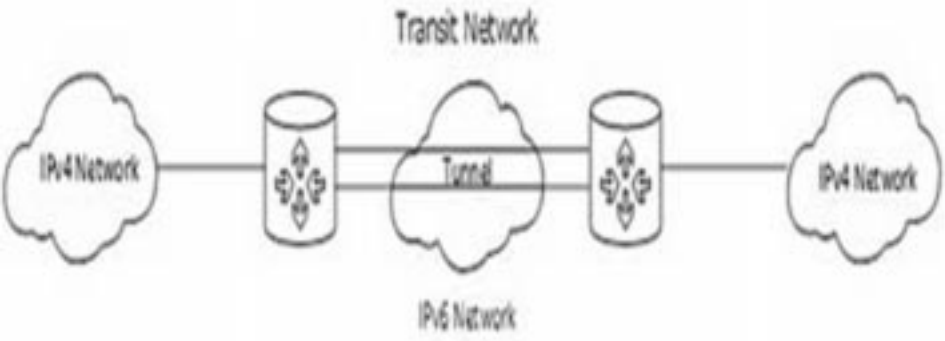

Figure 7: Tunneling Mechanism

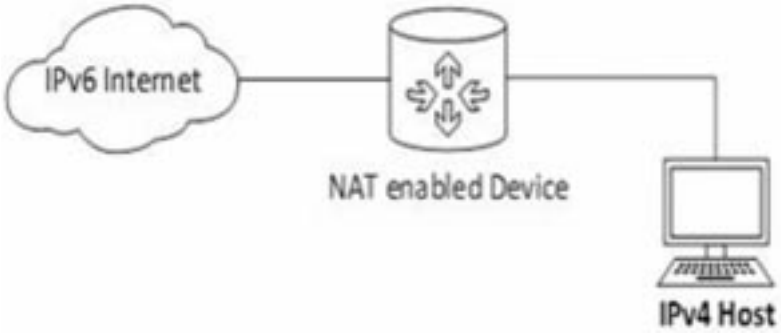

Figure 8: NAT-PT Mechanism

3.3. Network Address Translation – Protocol Translation (NAT-PT) mechanism

When IPv4 node from IPv4 network initiate a communication with IPv6 node in a IPv6 network, the IPv6 server in the IPv6 network cannot understand the IPv4 address. Hence a Network Address Translation – Protocol Translation NAT-PT device is enabled in the IPv6 network. This NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet [20]. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa and this process is depicted in the figure, Figure 8.

4. CONCLUSION

IPv6 is now taking over the control of Internet to meet out the IPv4 address depletion. IPv6 commercial services are already started with about 3,100 companies including Google. This was a step towards encouraging Internet community to migrate to IPv6. IPv6 provides ample of address space and is designed to expand today's Internet

services. Based on the IPv4 address usage and allocation strategies, the Internet Analysts, based on the standard deviation method, predicted that, there will be a demand of 330 million IP addresses in 2017. IPv6 provides ample of address space and is designed to expand today's Internet services. Feature-rich IPv6 enabled Internet version 2 may deliver more than expected.

REFERENCES

[1] Olabenjo Babatunde1, Omar Al-Debag, "A Comparative Review Of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)", *International Journal of Computer Trends and Technology (IJCTT)* ,Volume 13 , No 1 , July 2014

[2] Geoff Huston, "IPv4 address report", August 2015.

[3] Japan Network Information Center (JPNIC), "Study Report on the IPv4 Address Space Exhaustion Issue (Phase I)", December 2007.

[4] Bradner.S, Mankin, A, "IP: Next Generation (IPng) White Paper Solicitation", RFC 1550, December 1993.

[5] https://technet. microsoft.com/en-us/library/bb726995.aspx, Published on November 02, 2004

[6] Bradner.S, Mankin.A,"The Recommendation for the IP Next Generation Protocol", RFC 1752. January 1995.

[7] http://www.iana.org/assignments/version-numbers/version-numbers.xhtml, last updated on 2007-06-27

[8] http://www.Lana org. Retrieved on 2016-02-12, last updated on 2016-3-6.

[9] Senthil Kumar.K, Rathina Gowri. S, "A survey of Next Generation Internet Protocol version 6" , *International Journal of Engineering Science Invention*,Volume 2, Issue 3, 23-28, March 2013.

[10] Saurabh Dey, Shilpa. N, "Issues in IPv4 to IPv6 Migration", *International Journal of Computer Applications in Engineering Sciences (IJCAES)*, **1(1)**, March 2011.

[11] Deering.S, Hinden.R., "Internet Protocol, Version 6 (IPv6) Specification", *Internet Engineering Task Force- Fremont*, USA RFC 2460, December 1998.

[12] David C. Plummer, "An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses", RFC 826 ,November 1982.

[13] Narten.T, Nordmark.E, Simpson.W,Soliman.H, "Neighbor Discovery for IP version 6 (IPv6) ", RFC 4861, September 2007.

[14] Prachi , Nikita Jora, "Mobile IP and Comparison between Mobile IPv4 and IPv6", *Journal of Network Communications and Emerging Technologies (JNCET)* , **2(1)**, May 2015.

[15] Frankel.S, Krishnan.S, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, February 2011.

[16] Mills.D, "Network Time Protocol (NTP) ", RFC 958, September 1985.

[17] Fayza Nada, "Performance analysis of mobile IPv4 andIPv6", *The International Arab Journal of Information Technology*, **4(2)**, April 2007.

[18] Masaki Nakajima, Nobumasu Kobayashi, "IPv4/IPv6 translation technology", *FUJITSU Sci.Tech.J*, June 2004.

[19] Nordmark.E, "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, Sun Microsystems, February 2000.

[20] Yoo. H.S, Cagalaban.G, Kim.S.H, "A Study on the Connectivity of IPv6 to IPv4 Domains and ItsSecurity Issues", *International Journal of Advanced Science and Technology*, **(10)**, 603-612, September 2009.