Review of IPv4 and IPv6 and various implementation methods of IPv6

Shraddha S. Jadhav[1], Beena R. Ballal[2]

[1] *B.E Student, Dept. of Electronics and Telecommunication, Vidyalankar Institute of Technology, Maharashtra, India*

[2] *Assistant Professor, Dept. of Electronics and Telecommunication, Vidyalankar Institute of Technology, Maharashtra, India*

---***---

Abstract - *Presently, approximately 25 billion people are connected worldwide, and these networks are connected through routers. IPv4 had some deficiencies like Address depletion problem, Lack of Encryption, and authentication of data features, which led to the development of IPng/IPv6. The development of IPV6 and deployment of the same is in process worldwide using various deployment techniques. These techniques enable the upgradation of networks to IPv6 deployed networks with little or no intervention of IPv4 services. Greater deployment efforts from a number of small networks could result in an increasing measure of global IPv6 deployment.*

***Keywords*—IPv4, IPv6, Routing, NAT, Protocols**

1. INTRODUCTION

The third layer of the Open System Interconnections model (OSI) is the Network layer, which is responsible for providing an IP address to packets, Routing, Inter-networking, and source to destination delivery. Also, it receives frames from the data link layer (second layer of OSI model) and delivers them to their intended destination based on the address contained within the frame. The Internet Protocols (IPs) provide the logical address to the network layer to trace the destination. IETF started to work on the successor of IPv4, in the early 1990s, which would solve address exhaustion problems. IPV6 also known as Next Generation IP or IPng, was designed and developed as a replacement for IPv4, in 1994 by IETF with its formal description under RFC 1883 published in 1995. IPV6 was a promising format for IP because of its advantages such as larger Address Space than IPv4 since it increases IP address size from 32 bits to 128 bits. It provides a better header format, dropping some header fields of IPv4. This simplifies and accelerates the routing process, new options to permit additional functionalities, provides support for more security by Encryption and Authentication of data, providing confidentiality and integrity to the packets. This paper documents the detailed comparison of IPv4 and IPv6 Protocols. Also reviews the various implantation methodologies of IPv6.

2. COMPARISON OF IPv4 AND IPv6

Functions that work in IPv4 were kept in IPng (next-generation IP i.e., IPv6) and which did not work were removed. IPv6 supports the same QoS (Quality of Service) features as IPv4, including the DiffServ indication, as well as a new 20- bit traffic flow field [1]. IPv4 has a variable header field length of 20-60 bytes whereas the IPv6 header is fixed size (40 bytes), which allow routers to process IPv6 packets faster resulting in traffic that can be forwarded at higher information rates, giving higher performance, and can be used for high bandwidth applications [2]. IPv4 uses manual configuration or Dynamic Host Configuration Protocol (DHCP) whereas IPv6 supports functionalities like auto configuration as well as plug and play [3]. IPv6 provides simpler encapsulation than IPv4 increasing routing efficiency. Few functions that IPv4 lacks, like IPsec security protocols, ESP (encapsulating security protocol), and AH (authentication header), are added to it for developing IPv6. Unlike IPv4, new generation protocol IPng uses multicast or anycast addresses.

An illustrative comparison based on the limitations of IPv4 and solutions to these limitations of IPv4 in the new generation protocol IPv6 is shown in the Table I.

TABLE -1: COMPARISON BASED ON FEATURES OF IPv4 AND IPv6 [3]

Sr No.	IPv4 drawbacks overcome by IPv6		
	Features of IPv4 (Limitations)	**IPv4 features explanation**	**Solution by IPv6**
1	IPv4 Address space	IPv4 has almost used up its address space of around 4 billion with 4, 294, 967, 296 addresses.	IPv6 eliminates the address exhaustion issue by replacing 4 octets of 8 bits and uses a hexadecimal number field. It provides an address size of 128 bits (16 bytes) and 2^{128} address blocks.
2	IPv4 Congestion in the	IPv4 uses its Broadcast functionality and	IPv6 reduces the network congestion and

Sr No.	IPv4 drawbacks overcome by IPv6		
	Features of IPv4 (Limitations)	IPv4 features explanation	Solution by IPv6
	Network	Integrated Header Format (IHF) for packet transmission. It transmits the packet before checking the address of the end point, this floods the whole network resulting in congestion.	overcrowding by packets sent as it uses Simple Header Format (SHF) that checks and identifies the destination of the packets before sending them.
3	IPv4 Packet Loss	The Time-To-Live (TTL) protocol in the IPv4 fragmented packet allocates a time frame for each packet that determines the timespan of each packet in the header, and it cannot be used for real-time applications as heavy data traffic may cause delay in transmission.	IPv6 routers make use of hop limit field which gives the number of links the packet can travel before getting discarded. This minimizes the chances of losing the packet during transmission.
4	IPv4 Security	The Internet Protocol Security (IPSec) on IPv4 is optional.	IPv6 supports IPSec and Authentication Header (AH) for encrypting and authenticating the packets transmitted between two end points. It provides secure transmission.
5	IPv4 Data Priority	IPv4 does not provide priority functionality for prioritizing the streaming data.	IPv6 uses Quality of Service (QoS) to prioritize the delay sensitive or heavy traffic packets being sent over the network.

3. IMPLEMENTATION OF IPv6

Though IPv6 provides many advantages over IPv4, it has still not been deployed completely by many ISPs as it needs full path participation. Therefore, different transition mechanisms have been implemented to avail the features of both IPv4 and IPv6. These protocols cannot be merged but can run in parallel using the transition mechanisms. Based on APNIC data at present only 31% of Internet users are IPv6 capable. The adoption rate of IPv6 varies from high number of users in India (76%) to above 50% number of users in five countries namely, Germany, Vietnam, Belgium, Greece, and Malaysia. Table II below gives an overview of change in number of users from 2021 to 2022 for top 10 economies.

TABLE -2: HIGHEST ABSOLUTE GROWTH OF USERS OVER 2021 [4]

Rank	IPv6 Users				
	2021	2022	Change	Users (est.)	Country
1	164,459,081	274,019,342	109,560,261	820,328,035	China
2	420,258,878	439,312,401	19,053,523	574,511,661	India
3	9,616,919	15,677,224	6,060,305	32,204,986	Saudi Arabia
4	783,660	6,587,084	5,803,424	113,054,932	Indonesia
5	34,839,061	38,584,943	3,745,882	89,811,643	Mexico
6	58,410,683	61,762,731	3,352,048	161,217,993	Brazil
7	23,995,676	26,879,572	2,883,896	53,010,341	Vietnam
8	4,140,135	6,647,417	2,507,282	34,549,112	Colombia
9	872,279	3,359,080	2,486,801	9,004,547	Guatemala
10	141,528	2,435,168	2,293,640	16,308,208	Chile

Major Operating System (OSs) are IPv6-capable. Therefore, deploying IPv6 at the user and edge site is easier, using methods allowing distinct IPv6 domains to communicate with each other by carrying IPv6 traffic over the existing IPv4 infrastructure before the network completely gets deployed with IPv6 backbone. The five key techniques for deploying IPv6 are:

1. Implementing IPv6 using tunneling method
2. Using Dual Stack Backbones
3. IPv6 over MPLS Backbone
4. Protocol Translation Mechanisms
5. Using Dedicated Data Links

3.1 Implementing IPv6 using tunneling method

In tunneling, routers between two IPv6 nodes need not be IPv6-capable, this decreases dependencies. The tunnel has two IPv4 routers connected with a virtual point-to-point link, routing IPv6 packets held by an IPv4 packet over the IPv4 network. Various tunneling technologies have been developed to support IPv4 over IPv6 tunnel as well as IPv6 over IPv4 tunnel. These technologies are generally categorized as configured or automatic tunnels, the latter tunnel type is predefined, and the former is created and torn down "on the fly" [5]. In configured tunnels, configuring tunnel endpoints is required to configure the devices to transmit packets based on the destination, and other tunnel configuration parameters like Maximum Transmission Unit (MTU). Whereas in Automatic tunnels, tunneling is based on information contained in the IPv6 packet, such as source or destination IP address. Tunneling of IPv6 packet over IPv4 packet is shown in Fig.1 below.

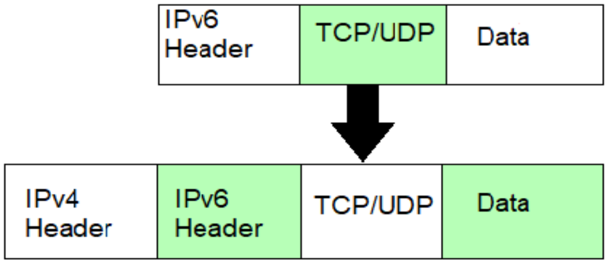

Fig -1: IPv6 over IPv4 Tunneling

The existing IPv4 infrastructure is used for routing IPv6 traffic with the help of a tunneling technique selected based on the mechanism used by the encapsulating node to determine the address of the tunnel end node. IPv6 datagrams can be tunneled using IPv6 or IPv4 hosts, and routers over regions of IPv4 routing topology by encapsulating them inside IPv4 packets. The resulting tunneled packet size is managed by the tunneling encapsulator endpoint, with respect to the tunnel's maximum transmission unit (MTU) or packet size and inform the source if the packet is too large for the tunnel.

There are five methods of tunneling IPv6 traffic:

1. Manual IPv6 tunnels
2. Automatic IPv4-Compatible tunnels
3. Generic Routing Encapsulation (GRE)
4. Automatic 6to4 tunnels
5. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels

The major limitations of all tunneling mechanisms are a single point of failure, crossing the firewall is not possible, and the need for up-gradation and changing of CPEs [6]. Tunneling can be preferred over NAT-PT or Translation mechanisms because of higher throughput of 23.27 kb/sec, Bandwidth of 51.2 kb/sec and Average Round Trip Time of 5ms. These observations based on a study done by Sheetal Singalar in [7] proves tunneling to be a better migration technique than translation but less desirable than dual stack.

3.2 Using Dual Stack Backbones

It allows migration of networks, end nodes, and applications by running IPv4 and IPv6 independently, coexisting in a dual IP layer backbone for routing. A dual stack is a protocol stack containing both IPv4 and IPv6 having an identical stack remainder. This allows the same applications and transport protocols like TCP, UDP, etc to run over version 4 and 6 protocols [5].

In dual stack, configured on a single interface or multiple interfaces, the transmission decision is made by the device depending on the traffic at the destination address. The packet sent reaches the destination over a dual-channel provided by dual-stack.

This simple strategy allows the same end system to support different applications not supporting the new generation protocol stack to coexist with the upgraded applications. Also, it enables the upgraded nodes to interoperate with IPv4-only by using IPv4 and vice versa by selecting and configuring suitable routing protocols for both the IP versions [8]. Dual Stack protocols are shown in Fig. 2. The Dual-stack backbone assigns addresses to endpoints based on protocol enabled by the network administrator either DHCPv4 or DHCPv6 [6]. The dual stack has two routing tables and provides the least Round-Trip Time of 2ms and high throughput of 64 kb/sec [7]. But increased resource requirement for providing high bandwidth is a limitation of this approach [9].

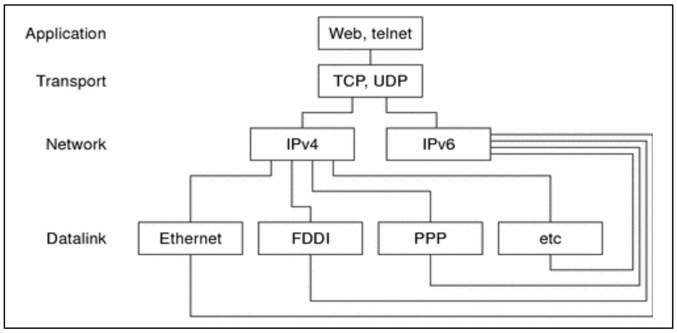

Fig -2: Dual-stack protocols through the OSI layer [5]

3.3 IPv6 over MPLS Backbone

Multi-Protocol Label Switching (MPLS) allows to tunnel IP, Ethernet, IPv6, PPP, Frame relay, etc. In the MPLS backbone, IPv6 nodes communicate with each other using packets which are forwarded based on the labels, used for identifying the destination, over an IPv4 MPLS infrastructure. The main drivers for deploying an MPLS based forwarding mechanism for IPv4 include Layer 2 and Layer 3 Virtual Private Networks, and Traffic Engineering and Fast Reroute [10]. IPv6 Provider Edge (6PE), and IPv6 VPN Provider Edge (6VPE) over MPLS, allow the service providers running an MPLS over IPv4 infrastructure offering IPv6 services with minor changes in the architecture. 6PE and 6VPE techniques were evaluated by Alex Leonel Yautibug Coro [11] for three parameters jitter, delay, and average packet size. The study concluded that 6PE technique was better than 6VPE for transmission and reception of streaming data by a difference of 8%.

3.4 Protocol Translation Mechanisms

Protocol Translation Mechanisms allow IPv4-only or IPv6-only devices to communicate directly with IPv6-only or IPv4-only devices, via some bi- directional protocol translation process. This often involves replacing and/or modifying the addresses/port numbers in packet headers. It performs the translation job by maintaining the IPv4 protocol suite inside the enterprise and translating the address of source and destination to the equivalent IPv6 addresses of the packets sent over the IP network. Another approach would be where an enterprise has transitioned to IPv6 internally but uses their limited public IPv4 addresses on the outside of a protocol translator. In this case, the internal IPv6 will be translated to external IPv4 for transmission of packets over the Internet. Translation-based mechanisms do not support multicast and embedded addresses. Also, they have difficulty translating APIs and cannot combine with secure DNS [6]. The IETF v6Ops Working Group considers the following IPv6 to IPv4 translation methods-

- NAT-Protocol Translation (NAT-PT)
- TCP-UDP relay
- Bump-in-the-Stack (BIS)
- SOCKS-based gateway

3.4.1 Network Address Translation Protocol Translation

NAT technology is used to translates a private address in an internal network into a legal public address to prolong IPv4 availability. It allows IPv4-only hosts to communicate with IPv6-only hosts and vice versa. It combines address mapping, protocol translation (SIIT), and a DNS_ALG supporting a bi-directional communication between IPv4 and IPv6 hosts. Though NATs promote reuse of the private address space, they often violate the fundamental design principle of the Internet which states to have all nodes a unique, globally reachable address. Thereby, preventing true end-to-end connectivity for all types of networking applications [2]. NAT-PT has high latency for all traffics due to additional overhead and provides low throughput [9]. Therefore, it is an undesirable migration technique.

3.4.2 TCP-UDP relay

TCP-UDP relay mechanism works by setting up separate connections for IPv4 and IPv6 hosts at the transport layer and runs on a dedicated server. Then transfers the information between two. No changes are needed to IPv4 and IPv6 hosts.

3.4.3 Bump-in-the-Stack (BIS)

The BIS mechanism integrates three components, namely “extension name resolver”, an “address mapper” and a “translator module”, into the network operating system. These three components are based on SIIT Algorithm. IPv4 host communicates with IPv6-only host using extra layers for mapping an IPv6 address into an IPv4 address. BIS uses transition protocol between TCP/IP module and Network card driver for snooping data flow and translating the packets either to IPv6 or IPv4 [6].

3.4.4 SOCKS-based gateway

SOCKS is an Internet protocol that operates at layer 5 of the OSI model and is used for exchanging network packets through a proxy server between a client and server. At the application layer, the SOCK-based IPv4/IPv6 gateway relays the two “terminated” IPv4 and IPv6 connections. It advances the native SOCKS and connection relay mechanisms.

4. CONCLUSION

IPv6 provides higher QoS, and security as compared to IPv4. Different migration techniques are applied to networks based on various performance metrics. A dual-stack backbone providing low jitter and delay is a superior mechanism. But, tunneling can be used in situations where dual stack cannot be implemented. Though NAT was widely used as a solution for the extinction of IPv4 addresses, it has several drawbacks like low throughput, bandwidth, and high RTT. The transition of IPv6 deployment is inevitable as the whole world is facing the same issue of IPv4 address blocks shortage. Meeting the needs of a new market, IPv6 is a durable solution to the growing internet challenges, providing several flexible transition mechanisms. More efforts are required to seek significant levels of IPv6 deployment in major industrialized nations.

REFERENCES

[1] Amer Nizar Abu Ali, "Comparison study between IPV4 & IPV6," IJCSI International Journal of Computer Science, vol. 9, pp. 314-317, May 2012.

[2] J Deka Ganesh Chandra, Margaret Kathing, and Das Prashanta Kumar, "A Comparative Study on IPv4 and IPv6," Proc. - 2013 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2013, pp. 286-289, June 2013.

[3] Samson Isaac, "Comparative Analysis of IPV4 and IPV6," (IJCSIT) International Journal of Computer, vol. 7(2), pp. 675-678, 2016.

[4] Geoff Huston, "Another Year of the Transition to IPv6," 2022, [online] Available: https://blog.apnic.net/2022/02/21/another-year-of-the-transition-to-ipv6/.

[5] Sun Microsystems IPv6 Administration Guide(2003), "Making the Transition From IPv4 to IPv6," [online] Available: https://docs.oracle.com/cd/E19683-01/817-0573/817-0573.pdf.

[6] Ala Hamersheh and Yazan AbdAlaziz, "Transition to IPv6 Protocol, Where We Are?," Proc. IEEE Int. Conf. Comput. Inf. Sci. (ICCIS), vol. 24, pp. 2291-2304, April 2019.

[7] Sheetal Singalar and R M Banakar, "Performance Analysis of IPv4 to IPv6 Transition Mechanisms," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-6, 2018.

[8] Mallik Tatipamula, Patrick Grossetete and Hiroshi Esaki, "IPv6 Integration and Coexistence Strategies for Next-Generation Networks," IEEE Communications Magazine, vol. 42, pp. 88-96, January 2004.

[9] Luke Smith, Mark Jacobi and Samir Al-Khayatt, "Evaluation of IPv6 transition mechanisms using QoS service policies," 2018 11th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), pp. 1-5, 2018.

[10] Wim Verrydt and Ciprian Popoviciu, "Study of IPv6 Multicast Deployment in MPLS Netw," 2006 International Multi-Conference on Computing in the Global Information Technology - (ICCGI'06), 2006.

[11] Alex Leonel Yautibug Coro, Diego Avila-Pesantez and Alberto Arellano-Aucancela, "Evaluation of 6PE and 6VPE techniques in MPLS-VPN networks for video streaming," 2021 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT), December 2021.