# IPv6: TRANSITION METHODS AND ADVANTAGES

**A.M. Jayasekara[1], N.U. Wickamasinghe[1], W.H.M.S.P. Wijetunge[1], W.G.C.W. Kumara[2*]**

[1*] Undergraduate Student, Department of Mechatronics Engineering, Faculty of Engineering, South Asian Institute of Technology and Medicine (SAITM), Sri Lanka
[2*] Corresponding Author, Senior Lecturer, Department of Mechatronics Engineering, Faculty of Engineering, South Asian Institute of Technology and Medicine (SAITM), Sri Lanka,
Email: **chinthaka.w@saitm.edu.lk**

## ABSTRACT

By 2014, expected number of devices that are connected to the internet is estimated as – 50 billion and that is 12 times more devices than currently widely used IP addressing format IPv4 can support ($2^{32}$ – 4.3 billion IP addresses) and Internet Corporation for Assigned Names and Numbers (ICANN), the organization responsible for IP addressing has already admitted that they are currently out of IPv4 addresses [1]. As a result today we often have tens of thousands people using one IP address; which results in potential network breakdowns, decrease in Value Added Services (VAS) as well as security issues. Therefore, the only proper solution for this is switching to a more spacious method of IP addressing – that is IPv6 ($2^{128}$ - 340 undecillion addresses or 340 trillion groups of one trillion networks each - each network can handle a trillion devices) or Internet Protocol version 6.

Although most of the developed countries and large-scale companies are already using IPv6 small countries such as Sri Lanka are still using IPv4, [2] and IPv6 facilities by using various methods of conversion of IPv4 to IPv6 without implementing IPv6. The reasons for still using IPv4 instead of IPv6 are that, it is new the society lacks IPv6 expertise as well as the lack of awareness among the users. However, by analyzing the methods used by IPv6 enabled parties to change from IPv4 to IPv6, and looking at the positives we get from implementing IPv6 it is rewarding to transfer from IPv4 to IPv6. From which we have an ability to develop networks that provide less gatekeepers with added security and IPv6 global addressing allow speed and simplicity.

From the results of our research, we can say that changing from IPv4 to IPv6 is now much easier task than when it was first introduced, because compatibility with IPv6 networking is mainly a software or firmware issue and most personal computers running recent operating system versions are now IPv6-ready as well as most popular applications with network capabilities are too, and most others could be easily upgraded with support from the developers. Moreover, for the hardware, Low-level equipment like network adapters and network switches may not be affected by the change, since they transmit link-layer frames without inspecting the contents. So by implementing IPv6 instead of the IPv4 will be an investment for the development of the internet as well as allowing $2^{128}$ (340 Undecilion) users into internet instead of previous $2^{32}$ (4.3 billion) users.

***Key words*:** IPv4, IPv6, Internet, Transition methods

## 1. INTRODUCTION

The Internet operates by transferring data between hosts in packets that are routed across networks as specified by routing protocols. These packets require an addressing scheme, such as IPv4 and IPV6, to specify their source and destination address. Each host, computer or other device on the Internet require an IP address in order to communicate. Internet Protocol version 6 or IPV6 is the Internet's next generation protocol, designed to replace the current Internet Protocol, IP Version 4 or IPV4 which is predominately deployed and extensively used throughout the world. IPV6 is a standard, developed by the Internet Engineering Task Force (IETF), an organization that develops internet standards. The IEFT, anticipating the need for more IP addresses, create IPV6 to accommodate the growing number of users and the devices accessing the Internet. The exhaustion of available IPV4 address space was the primary reason for the development of the new protocol IPV6. The IEFT have added many new features and improvements to IPv4, in order to develop the new protocol. IPV6 is designed to meet the requirements of the potentially huge internet expansion. It will return to the global environment where the addressing rules of the network are transparent to the applications again. Through auto configuration and plug and play support, network devices will be able to connect to the network without manual configuration and without any bootstraps services. IPV6 succeed in doing this by providing some benefits for the IT and network professionals. First, the Internet Protocol version 6 (IPv6) has a larger address space which is a 128-bit identifier. This will result on almost unlimited number of IP address (approximately three hundred and forty trillion, trillion unique IP addresses.) and hierarchical network architecture for routing efficiency. Because of this, the ability to provide global address for each network device enables end-to-end reachability. In addition, Network management would be simpler. There are three types of IPv6 addresses: unicast, anycast, and multicast.

Unicast addresses are typically assigned to one and only one network interface; however, when multiple network interfaces are logically treated as a single interface, a single unicast address may be assigned to all of these network interfaces. Anycast and multicast addresses may be assigned to multiple network interfaces. IPv6 uses a variable length Format to distinguish between the multiple types of IPv6 addresses. The IPv6 addresses assigned to a network interface may be changed over its lifetime. An example IPv6 address is, 2001:db8:ffff:1:201:02ff:fe03:0405.

Second benefit would be IPV6 provide a simplified header format for efficient packet handling. Six of the twelve IPV4 header fields (IHL, Identification, Flags, Fragment Offset, Header checksum, Options and padding) have been removed in IPV6. Some IPV4 fields have been carried over with modified names and some new field to be added to improve the efficiency. Third, an hierarchical network architecture for routing efficiency which follows some of the IPV4 principles. Another important of the IPv6 is the embedded security with Mandatory IPsec (IP Security) Implementation. [3, 4]

## 2. METHODOLOGY

The research was conducted using a literature review using articles and other research material found on the Internet, as well as analyzing various statistical data and methods of implementations for IPv6.

## 3. RESULTS

There are three main methods that can be used when transitioning a network from IPv4 to IPv6; these include:

- Dual Stack - Running both IPv4 and IPv6 on the same devices
- Tunneling - Transporting IPv6 traffic through an IPv4 network transparently
- Translation – Converting IPv6traffic to IPv4 traffic for transport and vice versa.

### 3.1 Dual Stack

This is the simplest approach when transitioning to IPv6.It operates both Ipv4 and IPv6 simultaneously on the same infrastructure. The same router can be used. However, IPv6 is not supported on all of the IPv4 devices; in these situations, other methods must be considered.

### 3.2 Tunneling

Tunneling is a concept that encapsulates a given packet and then it is transported from the source to a destination transparently where it is capsulated and retransmitted. There are some different tunneling methods that exist for IPv6; most of them are integrated as part of networking devices manufactures certification tests. Following are the various methods of tunneling being used in the world today.

- **Manual IPv6 Tunnels**

A manually created IPv6 tunnel is configured between two routers, that each must support both IPv4 and IPv6. The primary use is for stable connections that require regular secure communication between two edge routers or between an end system and an edge router, or for connection to remote IPv6 networks. Incoming traffic that is destined for networks on the other side of the tunnel is encapsulated on the source router and tunneled through IPv4.

- **Generic Routing Encapsulation (GRE) IPv6 tunnels**

GRE is a protocol that was developed by Cisco. Its Purposes are same as the manual tunneling method to operate IPv6 tunneling and it is configured very much as manual tunnels. . GRE itself is able to be used to tunnel over a diverse number of network layer protocols other than IPv4. GRE tunnels can also be used to encapsulate traffic so that the traffic inside the tunnel is unaware of the network topology. GRE tunnel can be used to tunnel both IPv6 over IPv4 and IPv4 over IPv6. Same as the manual tunnel tunnels both the source and destination must be manually configured and each must support both IPv4 and IPv6.

- **6to4 Tunnels**

This is different from other tunneling methods. It is IPv6 to be tunneled via IPv4. 6to4 allows for automatic IPv6-to-IPv4 address translation, and treats the underlying IPv4 network as one big Non-Broadcast Multi-Access (NBMA) network, rather than a collection of independent point-to-point links. The IPv4 address for the edge routers is embedded in an IPv6 address that is created.

- **IPv6 rapid deployment (6rd)**

The 6rd method was derived from the 6to4 method. It has a significant change that it operates entirely within the end user's ISP's network, which avoids the main weaknesses in original 6to4.

- **IPv4 Compatible Tunnels**

This method is also very similar to 6to4 tunneling method. Both methods provide a system to tunnel IPv6 over IPv4. The major difference is how the IPv4 address is embedded inside the IPv6 address that is used by the edge device.

- **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Tunnels**

This method is more like the other tunneling methods. ISATAP method transport IPv6 traffic over IPv4. However, unlike other methods the ISATAP method is intended to be used inside a site and not between two dual stacked edge devices.

### 3.3 Translation

This is completely different from the tunneling methods mentioned above. A translation method provides a way to translate IPv6 to IPv4 traffic and vice versa. In translation methods, traffic is not encapsulated but it is converted to the destination type. There are two main methods that are used to translate IPv6.

- **Network Address Translation Protocol Translation (NAT-PT)**

The NAT-PT method has the ability to configure a translation of an IPv4 network address into an IPv6 network address and vise versa either statically or dynamically. The operation is very similar to NAT implementations, but includes a protocol translation function. NAT-PT also ties in an Application Layer Gateway (ALG) functionality that converts Domain Name System (DNS) mappings between protocols.

- **NAT64**

NAT-PT is tied in ALG functionality is one of the main limitations. NAT64 and DNS64 both are developed at the same time, which are configured and implemented separately. NAT64 is a mechanism to allow IPv6 hosts to communicate with IPv4 servers. The endpoint for an IPv4 address and an IPv6 network segment of 32-bits is the NAT server. The IPv6 client embeds the IPv4 address it wishes to communicate with using these bits and sends its packets to the resulting address. Then a NAT-mapping is created between the IPv6 and IPv4 address, allowing them to communicate by the NAT64 server. [5, 6, 7]

## 4. CONCLUSION

After analyzing the methods of IPv6 transition we can identify following main three transition methods.

- Dual stack

Allow IPv4 and IPv6 to coexist in the same devices and networks.

- Tunneling

Allow the transport of IPv6 traffic over the existing IPv4 infrastructure.

- Translation

Allow IPv6 only nodes to communicate with IPv4 only nodes.

Dual Stack is useful in the earlier stages of IPv4 to IPv6 transition, and it is the simplest way of having IPv4 and IPv6 in the same network. However, the main disadvantage in dual stack method is that some network vendors and servers do not support IPv6 so some users might find themselves unable to connect to some web sites. Moreover, translation method comes handy when dealing with different types of protocols but when IPv4 uses NAT this is not a good option.

Tunneling techniques are used on top of an existing IPv4 infrastructure and uses IPv4 to route the IPv6 packets between IPv6 networks. So Tunneling is used by networks not yet capable of offering native IPv6 functionality.

Now, as available IPv4 addresses are almost over it is the time for ISPs, large and small companies and universities to start migrating to IPv6. Based on the results of this analysis of the available technologies a company/ university that is planning to migrate can select any available option based on their requirements and IT infrastructure.

## 5. REFERENCES

[1]. Internet Corporation for Assigned Names and Numbers (ICANN).

[2]. Steinar H. Gunderson, "Global IPv6 statistics: Measuring the current state of IPv6 for ordinary users", Réseaux IP Européens (RIPE).

[3]. A Layman's Guide to the IPv6 Transition, macobserver.com, http://www.macobserver.com/tmo/article/a_laymans_guide_to_the_ipv6_transition/.

[4]. ICANN, Beginner's Guide to Internet Protocol (IP) Addresses.

[5] IPv6 at APNIC community, http://www.apnic.net/community/ipv6-rogram.

[6]. IPv6 deployment support site, Internet community of online networking specialists (icons), http://icons.apnic.net/display/IPv6/Home.

[7]. American Registry for Internet Numbers, ARIN IPv6 wiki, http://getipv6.info/index.php/Main_Page.