International Journal of Modern Trends in Engineering and Research
www.ijmter.com

e-ISSN: 2349-9745
p-ISSN: 2393-8161

# Comparative study between IPV4 & IPV6

Krunal A Maheshwari

*Information Technology, G.H.Patel College of Engineering & Technology,kamaheshwari@yahoo.com ,*

**Abstract -** Nowadays IPv6 over IPv4 tunnels are widely used to form the global IPv6 Internet. This paper demonstrates the two tunnels and show when to immigrate from IPv4 to IPV6.Then the risks of immigration are discussed.

**Keywords –** IPv6, IPv4, IANA

## I. INTRODUCTION

Today IPv6 over IPv4 tunnels are widely used to connect large regional IPv6 networks, because it is relatively hard to construct an international or cross-continent native IPv6 network. This makes the characteristics of IPv6 over IPv4 tunnels very vital to the performance of the global IPv6 Internet.

Migrating from IPv4 to IPv6 in an instant is impossible because of the huge size of the Internet and of the great number of IPv4 users. Moreover, many organizations are becoming more and more dependent on the Internet for their daily work, and they therefore cannot tolerate downtime for the replacement of the IP protocol. As a result, there will not be one special day on which IPv4 will be turned off and IPv6 turned on because the two protocols can coexist without any problems. The migration from IPv4 to IPv6 must be implemented node by node by using auto configuration procedures to eliminate the need to configure IPv6 hosts manually. This way, users can immediately benefit from the many advantages of IPv6 while maintaining the possibility of communicating with IPv4 users or peripherals. Consequently, there is no reason to delay updating to IPv6.In this paper we are going to investigate the IPV6 and the IPV4 and when to decide to immigrate to IPV6.

## II. INTERNET PROTOCOL VERSION 4 (IPV4)

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet. IPv4 is still by far the most widely deployed Internet Layer protocol. It uses a 32 bit addressing and allows for 4,294,967,296 unique addresses.[2] Even though the name seems to imply that it's the fourth iteration of the key Internet Protocol, version 4 of IP was the first that was widely used in modern TCP/IP. IPv4, as it is sometimes called to differentiate it from the newer IPv6, is the Internet Protocol version in use on the Internet today, and an implementation of the protocol is running on hundreds of millions of computers. It provides the basic datagram delivery capabilities upon which all of TCP/IP functions, and it has proven its quality in use over a period of more than two decades.

Since the 1980s it has been apparent that the number of available IPv4 addresses is being exhausted at a rate that was not initially anticipated in the design of the network. This was the driving factor for the introduction of classful networks, for the creation of CIDR addressing. [3]

But despite these measures the IPV4 addresses are being consumed at an alarming rate and it is estimated that 2010 would be the last year for IPV4, some sources say they may last until 2012. Primary reason for IPV4 exhaustion is huge growth in number of internet users, mobile devices using Internet connection and always on devices such as ADSL modems and cable modems. This brings us to the development and adoption of IPV6 as an alternate solution.

## III. INTERNET PROTOCOL VERSION 6 (IPV6)

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic.

IPv6 stands for Internet Protocol version 6 also known as Ipng (IP next generation) is the second version of the Internet Protocol to be used generally across the virtual world. The first version was IPv4. IPng was designed to take an evolutionary step from IPv4. It was not a design goal to take a radical step away from IPv4. Functions which work in IPv4 were kept in IPng. Functions which didn't work were removed.

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 or IPv6, to specify their source and destination addresses. Each host, computer or other device on the Internet requires an IP address in order to communicate. The growth of the Internet has created a need for more addresses than are possible with IPv4.

Like IPv4, IPv6 is an internet-layer protocol for packet switched internetworking and provides end-to-end datagram transmission across multiple IP networks. While IPv4 allows 32 bits for an IP address, and therefore has 232 (4 294 967 296) possible addresses, IPv6 uses 128-bit addresses, for an address space of 2128 (approximately 3.4×1038) addresses. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

## IV. LIMITATIONS OF IPV4

Since the 1980s it has been apparent that the number of available IPv4 addresses is being exhausted at a rate that was not initially anticipated in the design of the network. This was the driving factor for the introduction of classful networks, for the creation of CIDR addressing. [3]

But despite these measures the IPV4 addresses are being consumed at an alarming rate and it is estimated that 2010 would be the last year for IPV4, some sources say they may last until 2012. Primary reason for IPV4 exhaustion is huge growth in number of internet users, mobile devices using Internet connection and always on devices such as ADSL modems and cable modems. This brings us to the development and adoption of IPV6 as an alternate solution.

## V. HOW TO OVERCOME PROBLEMS OF IPv4 BY IPv6?

With such a huge address space, ISPs will have sufficient IP addresses to allocate enough addresses to every customer so that every IP device has a truly unique address – whether it's behind a firewall or not. NAT (network address translation) has become a very common technique to deal with the shortage of IP addresses. Unfortunately, NAT doesn't work very well for many Internet applications, ranging from old dependable, such as NFS and DNS, to newer applications such as group conferencing.

NAT has also been an impediment for business-to-business direct network connections, requiring baroque and elaborate address translators to make everything work reliably, scaling poorly, and offering a highly vulnerable single point of failure.

One of the goals of IPv6′s address space expansion is to make NAT unnecessary, improving total connectivity, reliability, and flexibility. IPv6 will re-establish transparency and end-to-end traffic across the Internet. The new IPv6 addresses are large and cumbersome to deal with, so IPv6 reduces the number of people who have to read and write them.

Another aspect of VPNs built into IPv6 is QoS (Quality of Service). IPv6 supports the same QoS features as IPv4, including the DiffServ indication, as well as a new 20-bit traffic flow field. Although the use of this part of IPv6 is not defined, it is provided as a solid base to build QoS protocols. The fifth major goal of IPv6 is VPNs, virtual private networks. The new IPSec security protocols, ESP (encapsulating security protocol) and AH (authentication header) are add-ons to IPv4. IPv6 builds-in and requires these protocols, which will mean that secure networks will be easier to build and deploy in an IPv6 world.

## VI. WHEN TO CHOOSE IPV6?

As long IPv4 networks do what you need them to do, let them run. But when an IPv4 network hits the limits for some reason, choose IPv6. IPv6 is mature enough to be used in corporate and commercial networks, as many case studies and deployments worldwide show. High investments in new IPv4 setups, fixes, or complex configurations for IPv4 (especially NATs) should be avoided if possible because they are investments in a technology that will slowly be phased out. When you reach the point where this becomes necessary, evaluate IPv6. Whatever you invest in IPv6 is an investment in future technology

Here's the list of indicators that it may be time for you to consider or integrate IPv6:

- Your IPv4 network or NAT implementation needs to be fixed or extended.
- You are running out of address space.
- You want to prepare your network for applications that are based on advanced features of IPv6.
- You need end-to-end security for a large number of users and you do not have the address space, or you struggle with a NAT implementation.
- Your hardware or applications reach the end of their lifecycle and must be replaced. Make sure you buy products that support IPv6, even if you don't enable it right away.

## VII. THE MIGRATION FROM IPV4 TO IPV6

The years from 1997 to 2000 will be characterized by the adoption of IPv6 by ISPs and users. During 1997, users could still have problems related to the newness of products, but starting from 1998, IPv6 will be part of mass-produced protocols distributed on routers, on workstations, and on PCs. At that point, organizations will begin to migrate, less or more gradually, to IPv6 [4].The key goals of the migration are as follow:

- IPv6 and IPv4 hosts must interoperate.
- The use of IPv6 hosts and routers must be distributed over the Internet in a simple and progressive way, with a little interdependence.
- Network administrators and end users must think that the migration is easy to understand and implement.

THE TRANSITION MECHANISMS

### 7.1 Dual stack

In dual stack, network nodes are equipped with IPV4 and IPV6 protocol stacks, one for IPV4 and one for IPV6 depending on the application or protocol they are using they just use one protocol stack with the other. Most of the operating systems support this. This is the most widely used IPV4 to IPV6 transition mechanism because it does not require any tunnelling or translation.

Generally it is achievable to configure the dual stack to use only one of the protocols among IPV4 and IPV6 while disabling the other. Dual stack is capable of working with both the network nodes (workstations or servers) and the routers

In a network, dual stack (IPV4/IPV6) has to be implemented in all the routers to work effectively. This solution can only work if these two addressing schemes are running in parallel because there is no communication between the IPv4 network nodes and the IPv6 network nodes; applications must be capable of supporting both modes. The dual stack mechanism is used frequently today, but requires that all network nodes must have an adequate amount of processing power and memory to maintain two different Internet Protocol stacks and dual management is also essential.

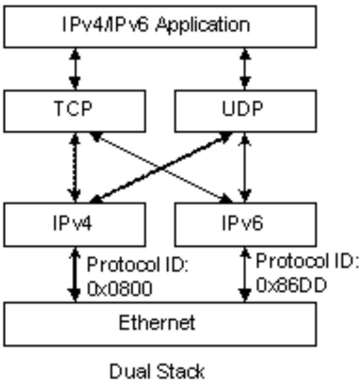


*Figure 1. Dual stack*

### 7.2 Tunneling

The term tunneling means when one network protocol encapsulates another protocol. By using tunnels we can carry a packet over an incompatible destination network. Here as an IPv6 migration strategy the purpose of tunneling is to interconnect IPv6 network hosts via IPv4 backbone using IPv6 tunnels . Overlay tunnels are the techniques that may be used to establish the connection between isolated IPv6 networks. Though, the use of tunneling strategies must not be considered as a concluding IPv6 network architecture, to a certain extent, it is a temporary solution until Dual stack and Native IPv6 can be completely implemented. Main reasons for using tunneling strategies lie into the below mentioned categories:

- Tunneling strategies provide an inexpensive means for connecting IPv6 networks. Only the endpoints i.e. border routers need to be upgraded to support both IPv4 and IPv6 protocols.
- Tunneling strategies allow communication establishment between IPv6 networks over a network that is IPv4 only or still not ready to deploy IPv6.

The IPv6 tunnel is shown in Figure 2. There are 4 types of tunnels supported by GNS3 which are discussed subsequently.

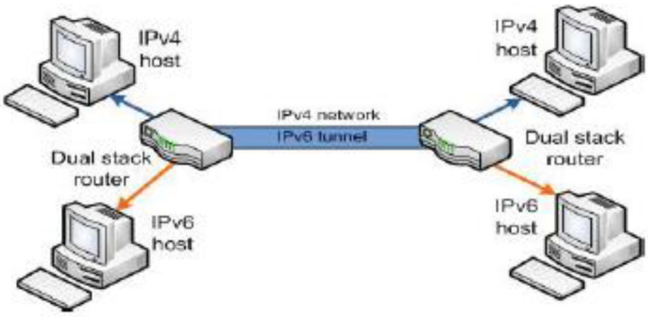


*Figure 2. IPv6 tunnel*

### 7.2.1 Manual tunnel

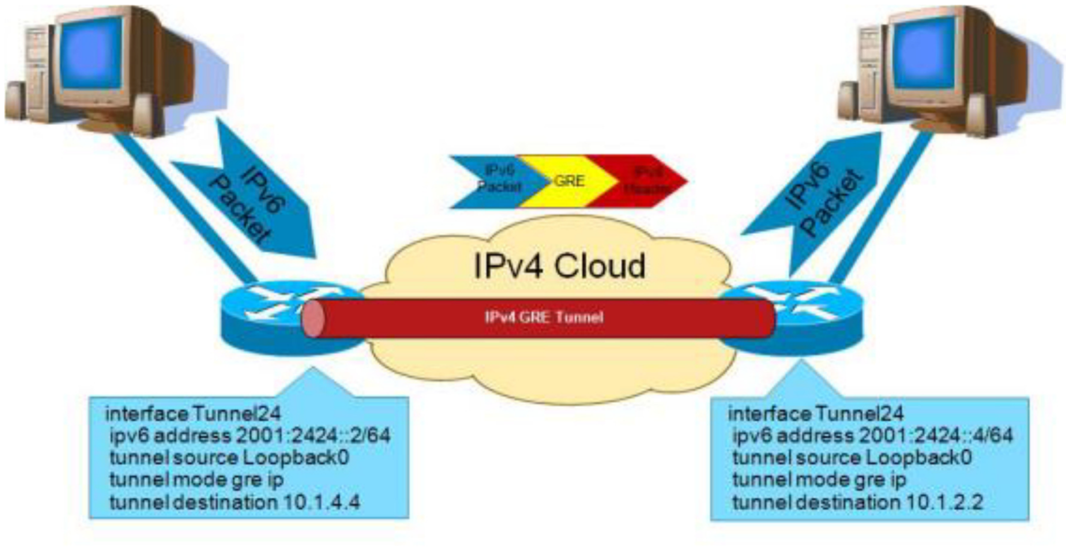
It constructs a permanent virtual connection, connecting two IPv6 networks that are associated over an IPv4 backbone. Manual tunnel is a point-to-point static tunnel. The source and destination of the tunnel has IPv4 addresses and they are dual-stacked, and tunnel interface is configured with an IPv6 address. IPv6 packets travel over the IPv4 environment [5].

Because the manual tunnel needs to be manually configured, it is not scalable and has high maintenance if a network change is required. Therefore, the more tunnel endpoints required, the greater the management overhead

### 7.2.2 GRE tunnel

GRE (Generic Routing Encapsulation) tunnel is a different type of Manual tunnel with tunnel source and tunnel destination both are configured for GRE manually shown in Figure 3. The source and destination of the tunnel has IPv4 addresses and they are dual-stacked, and tunnel interface is configured with an IPv6 address.

e-ISSN: 2349-9745
p-ISSN: 2393-8161



```
interface Tunnel24
 ipv6 address 2001:2424::2/64
 tunnel source Loopback0
 tunnel mode gre ip
 tunnel destination 10.1.4.4
```

```
interface Tunnel24
 ipv6 address 2001:2424::4/64
 tunnel source Loopback0
 tunnel mode gre ip
 tunnel destination 10.1.2.2
```

*Figure 3. GRE-IPv4 tunnel*

The GRE tunnel have an IPv6 packet embedded inside the GRE header and then inside the IPv4 header. GRE tunnel is also a point to point tunnel [5]. It has the same drawback of less scalability and greater management overhead as manual tunnel since it is also a type of manual tunnel.

## VIII. CONCLUSION

The Dual Stack mechanism is widely used for migration from IPv4 to IPv6.We need more power and memory to handle two different protocols. While using tunneling mechanism, we have a drawback of less scalability and greater management.so dual stack is better than tunneling in some cases.

## REFERENCES

[1] "IPv6 Headers", Online: http://www.cu.ipv6tf.org/literatura/chap3.pdf, chapter 3, pp. 40-55, Des 12 1997.
[2] S. Deering, R. Hinden, Internet Protocol Version 6 (RFC2460), 1998
[3] Ipv4/Ipv6 Translation Technology, Masaki Nakajima, Nobumasu Kobayashi , 2004
[4] E. Nordmark and R. Gilligan. (2005). “Basic Transition Mechanisms for IPv6 Hosts and Routers”. RFC 4213.
[5] Parisa Grayeli (Jan 2013), “Performance modelling and analysis of IPv6 Transition Mechanisms over MPLs”.