Heartian Journal of Pure and Applied Sciences,
March 2014, Vol. 3(1) p.p. 3-10

A study on Need of Transition from IPv4 to IPv6

***Regitha M R and Varghese Paul[1]**

Department of Computer Science, Sacred Heart College, Thevara

[1]Department of Information Technology, Cochin University of Science and Technology, Thrikkakara

Abstract

Rapid growth of Internet usage creates challenges to Internet management groups, stake holders and service providers. During 80's, Internet Protocol addressing was designed which is called IPv4 (Internet Protocol Version 4). It uses 32-bit address scheme, in which it can accommodate about 4 billion unique addresses. The number of usable addresses is actually much lower than the above. There are several problems such as impending exhaustion of the IPv4 address space, configuration and complexities and poor security at the IP level. To overcome these concerns, in the early 90's, IETF (Internet Engineering Task Force), began developing a new IP protocol namely IPv6 (Internet Protocol version 6) or Next Generation IP or IPng. Since IPv6 addresses are 128 bits long, the theoretical address space if all addresses were used is 2^{128} addresses. This number, when expanded out, is 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456, which is normally expressed in scientific notation as about 3.4×10^{38} addresses. That's about 340 trillion, trillion, trillion addresses. It will not only eliminate the shortcomings of IPv4, but also unlock new features and services. This paper highlights the limitations of IPv4, features of IPv6, need of transition from IPv4 to IPv6 and various transition methods of 4to6.

Key Words: Internet Protocol, Internet Engineering Task Force, Network Address Translation, Dual Stack, Tunneling, Translation.

Introduction

The scarcity of ipv4 address blocks leads to gradual depletion of ipv4 address space. In order to save and reuse the address blocks, service providers (sp) resort to mechanisms like multiple layers of network address translation (nat) (1). The more ideal approach to solve the issue of address scarcity facing the networking industry is to move towards the ipv6 addressing scheme. Ipv6 provides other additional improvements. First, it provides increased efficiency in routing. Second, it provides faster packet processing. Third, it supports multicast thereby overpowering the hassles of broadcasting packets. Fourth, it avoids nat, therefore, proves to be more robust.

Ipv6 is a packet switched network layer protocol that enables data communications. It involves the sending and receiving of data in packets between two nodes in a network. It was intended to replace the widely used ipv4 that is considered the backbone of the modern internet. Ipv6 is often referred to as the "next generation internet" because of its expanded capabilities

*Correspondent author
E-Mail: regitha.baiju@gmail.com
Tel:9846150145

and its growth through recent large scale deployments. In 2004, japan and korea were acknowledged as having the first public deployments of ipv6.

The limitations of ipv4

The main limitations of ipv4 are scarcity of ipv4 address, security related issues, quality of service and address configuration related issues. Ipv4 was published in 1981 and the initial design did not anticipate the expansion of internet, hence it created a lot of issues which proved that it needed changes. The following are the limitations of ipv4(2).

Limited address space

Organizations in the united states hold most public ipv4 address space worldwide. This limited address space has forced the wide deployment of network address translators, which can share one public ipv4 address among several privately addressed computers. Nats have the side effect of acting as a barrier for server, listener, and peer-to-peer applications running on computers that are located behind the nat. Although there are workarounds for nat issues, they only add complexity to what should be an end-to-end addressable global network.

Flat routing infrastructure

In the early Internet, address prefixes were not allocated to create a summarizable, hierarchical routing infrastructure. Instead, individual address prefixes were assigned and each address prefix became a new route in the routing tables of the Internet backbone routers. Today's Internet is a mixture of flat and hierarchical routing, but there are still more than 85,000 routes in the routing tables of Internet backbone routers. Figure 1 explains the structure of IPv4.

Configuration

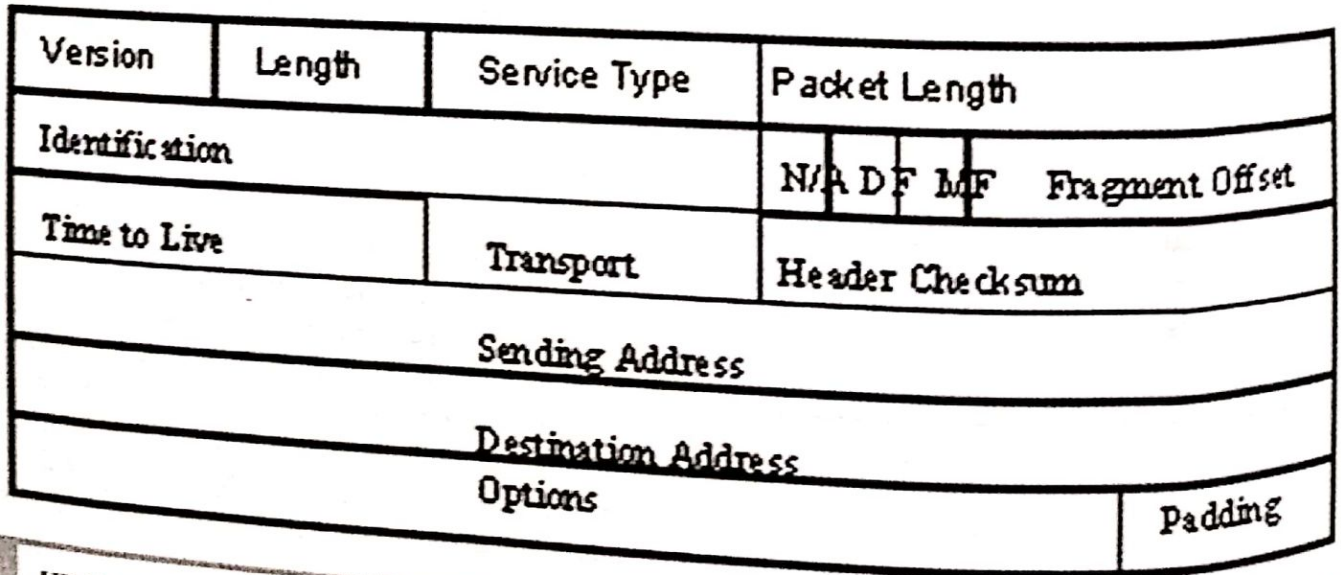
Ipv4 must be configured, either manually or through the Dynamic Host Configuration Protocol (DHCP). DHCP allows ipv4 configuration administration to scale to large networks, but DHCP infrastructure must be configured manually.

Security

Security for IPv4 is specified by the use of Internet Protocol security (IPsec). However, IPsec is optional for IPv4 implementations. Because an application cannot rely on IPsec being present to secure traffic, an application might resort to other security standards or a proprietary security scheme. The need for built-in security is even more important today, when we face an increasingly hostile environment on the Internet.

Prioritized delivery

Prioritized packet delivery, such as special handling parameters for low delay and low variance in delay for voice or video traffic, is possible with IPv4. However, it relies on a new interpretation of the IPv4 Type of Service (ToS)



field, which is not supported for all the devices on the network. Additionally, identification of the packet flow must be done using an upper layer protocol identifier such as a TCP or User Datagram Protocol (UDP) port. This additional processing of the packet by intermediate routers makes forwarding less efficient.

Mobility

Mobility is a new requirement for Internet-connected devices, in which a node can change its address as it changes its physical attachment to the Internet and still maintain existing connections. Although there is a specification for IPv4 mobility, due to a lack of infrastructure, communications with an IPv4 mobile node are inefficient.

IPv6 Packet Header and Fields

Increasing the IP address pool was a major factor in the development of IPv6(3). The biggest benefit of IPv6 is that it will replace the IPv4 32-bit address scheme with a much longer 128-bit address scheme. IPv6 also offers additional technical advantages such simplified headers in 8 fields (instead of the 13 fields in IPv4) as well as improved security with the addition of two new extension headers (authentication header and encapsulating security header).The IPv6 header has been designed to be simple and easy to process. This enables IPv6 devices the ability to spend the majority of their time dealing with the data contained within the packet and not the packet header itself. The Figure 2 shows IPv6 packet header structure.

Version

The size of the Version field is 4 bits. The Version field shows the version of IP and is set to 6.

Traffic Class

The size of Traffic Class field is 8 bits. Traffic Class field is similar to the IPv4 ToS field. The Traffic Class field indicates the IPv6 packet's class or priority.

Flow Label

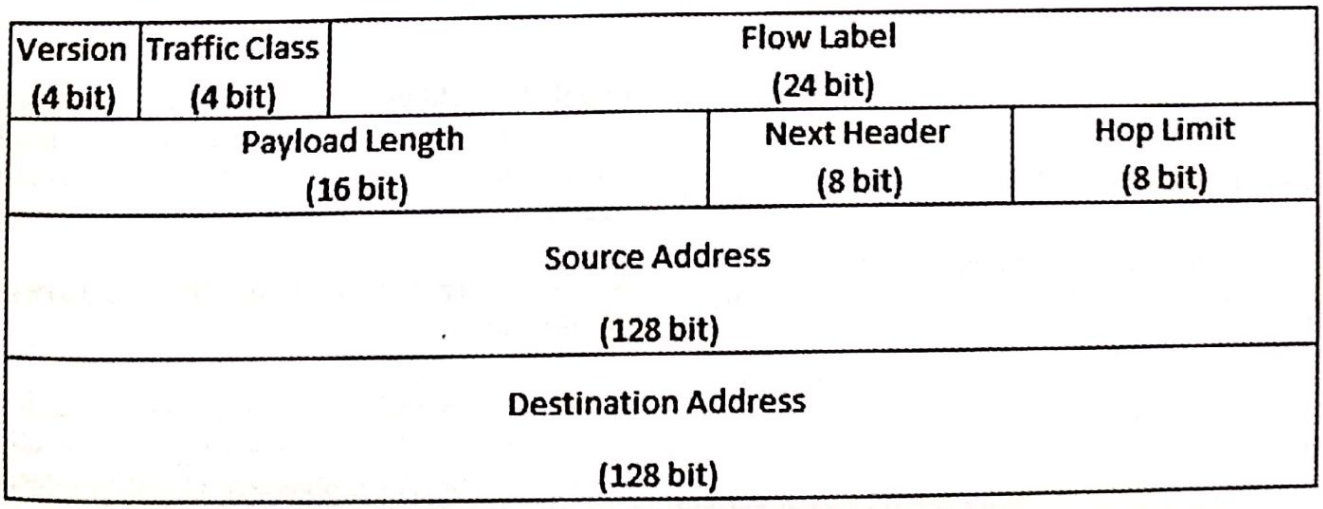
The size of Flow Label field is 20 bits. The Flow Label field provides additional support for real-time datagram delivery and quality of service features. The purpose of Flow Label field is to indicate that this packet belongs to a specific sequence of packets between a source and destination and can be used to prioritized delivery of packets for services like voice.

Payload Length

The size of the Payload Length field is 16 bits. This field shows the length of the IPv6 payload, including the extension headers and the upper layer protocol data.

Next Header

The size of the Next Header field is 8 bits. This field shows either the type of the first extension (if any extension header is available)



or the protocol in the upper layer such as TCP, UDP, or ICMPv6.

Hop Limit

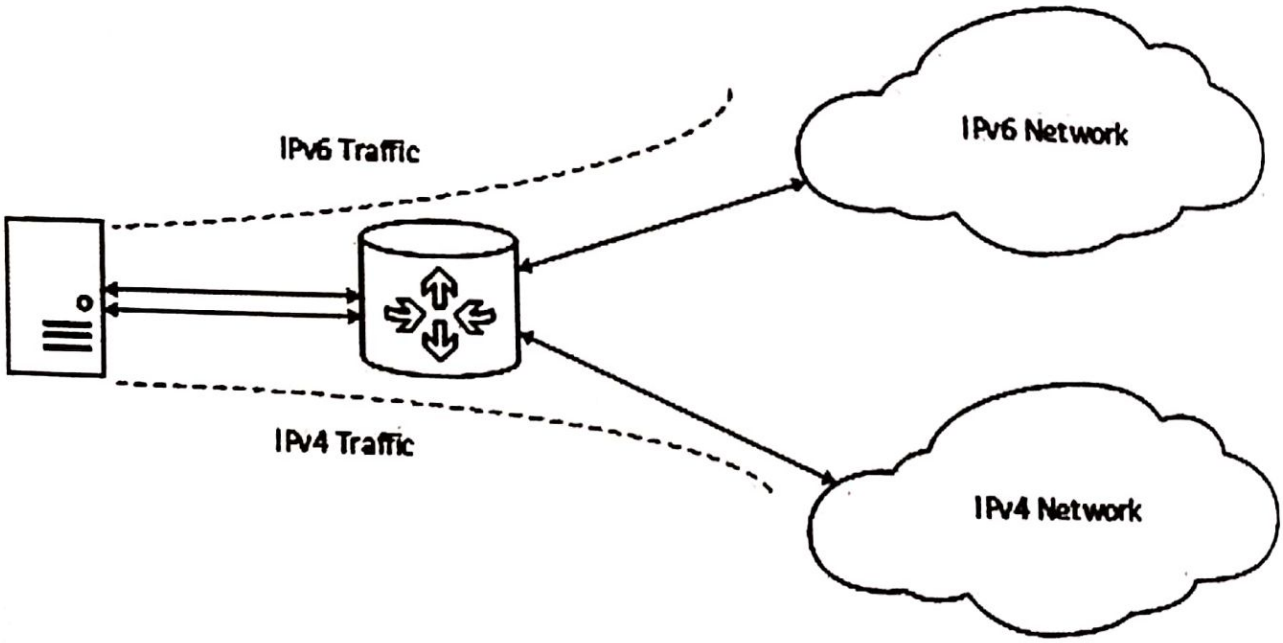
The size of the Hop Limit field is 8 bits. This field shows the maximum number of routers the IPv6 packet can travel. This Hop Limit field is similar to IPv4 Time to Live (TtL) field.

Source Address

The size of the Source Address field is 128 bits. The Source Address field shows the IPv6 address of the source of the packet.

Destination Address

The size of the Destination Address field is 128 bits. The Destination Address field shows the IPv6 address of the destination of the packet.



The Features of IPv6

The most obvious improvement in IPv6 over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features. Some of the features are given below(4).

New Packet Format and Header

IPv6 specifies a new packet format. It helps to minimize packet header processing by routers. This is achieved by moving both nonessential and optional fields to extension headers that are placed after the IPv6 header. Since IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable.

Large Address Space

IPv4 has 32 bit (4-byte) address space, but IPv6 has 128-bit (16-byte) address space. The very large IPv6 address space supports a total of 3.4×10^{38} addresses. This large address space allows a better, systematic, hierarchical allocation of addresses and efficient route aggregation.

Stateful and Stateless IPv6 address configuration

In IPv6, stateful or stateless configuration is possible. Hosts on a link can automatically configure with IPv6 addresses called link-local

addresses and with addresses derived from prefixes advertised by local routers. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters. The router which is available in the link responds to the request from the host with a router advertisement packet that contains network - layer configuration parameters. Hosts can configure link-local addresses automatically and communicate each other without manual configuration even there is no router available.

Multicast

The three types of communication available in IPv4 are unicast, multicast and broadcast. Unicast is one-to-one communication; multicast is one-to-many communication and broadcast is one-to-all communication. The transmission of a packet to all hosts was performed by using special broadcast addresses in IPv4. Broadcast communication is not available in IPv6 and therefore does not define broadcast addresses.

Integrated Internet Protocol Security (IPSec)

It is a set of Internet standards that uses cryp tographic security services to provide Confidentiality, Authentication, Data integrity. The support for IPSec was optional in IPv4 but it is an integral part of the base protocol suite in IPv6.

Neighbor Discovery Protocol (NDP)

It is a protocol available IPv6 which is based on Internet Control Message Protocol Version 6 (ICMPv6) messages that manage the interaction nodes on the same link. There is no Address Resolution Protocol (ARP) for IPv6 and the role of the ARP is replaced by NDP.

Extensibility

The features of IPv6 can be extended by adding extension headers after IPv6 header. The size IPv6 extension headers is constrained only by the size of the IPv6 packet, unlike 40 bytes of options of IPv4.

Jumbogram

A "Jumbogram" is an IPv6 packet containing a payload larger than 65,535 octets (5). The regular IPv6 header has a 16-bit Payload Length field and, therefore, supports payloads up to 65,535 octets long. However, the Jumbo Payload option uses an IPv6 hop-by-hop option, which carries a 32-bit length field, in order to allow transmission of IPv6 packets with payloads between 65,536 and 4,294,967,295 octets (2^{32}-1) in length.

TRansition Methods of IPv4-IPv6

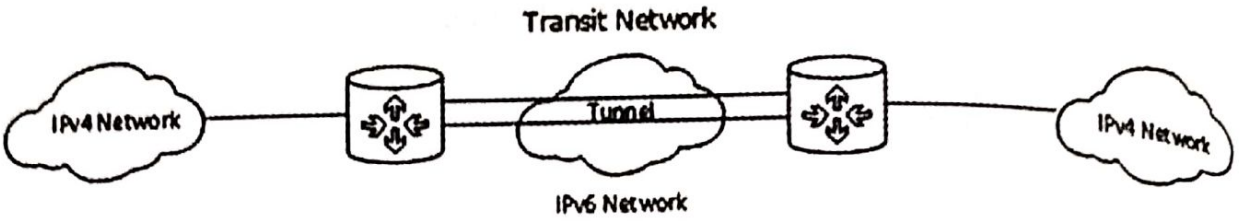
The IETF standards committee, the IPv6 Operations Working Group is responsible for developing the guidelines for the operation of a shared IPv4 and IPv6 Internet. The group also provides operational guidance on how to deploy IPv6 into existing IPv4 only networks as well as into new network installations. There are three transition methods from IPv4 to IPv6.

Dual Stacking

In the common method, dual stacking, a device runs both protocol stacks: IPv4 and IPv6 (6). Dual stacking can be accomplished on the same interface or different interfaces of the device. In the Figure 3; shows an example of dual stacking on a router, where Network A has a mixture of devices configured for the two different protocols, and the router configured in a dual stack mode. Older IPv4-only applications can still work while they are migrated to IPv6 by supporting newer APIs to handle IPv6 addresses and DNS lookups with IPv6 addresses.

Manual IPv6 Tunnels

A manually created IPv6 tunnel is configured between two routers that each must support both IPv4 and IPv6. 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 and for the purposes of IPv6 tunneling operates and is configured very much the same as manual tunnels. GRE itself is able to be used to tunnel over a diverse number of network layer protocols other than IPv4

6to4 Tunnels:

As the name suggests a 6to4 tunnel allows IPv6 to be tunneled via IPv4. Unlike the previously discussed tunneling methods, the 6to4 method is automatically set up using the 2002::/16 IPv6 address space(8). 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 but allows the implementer to use the IPv6 block that was assigned to it.

IPv4 Compatible Tunnels

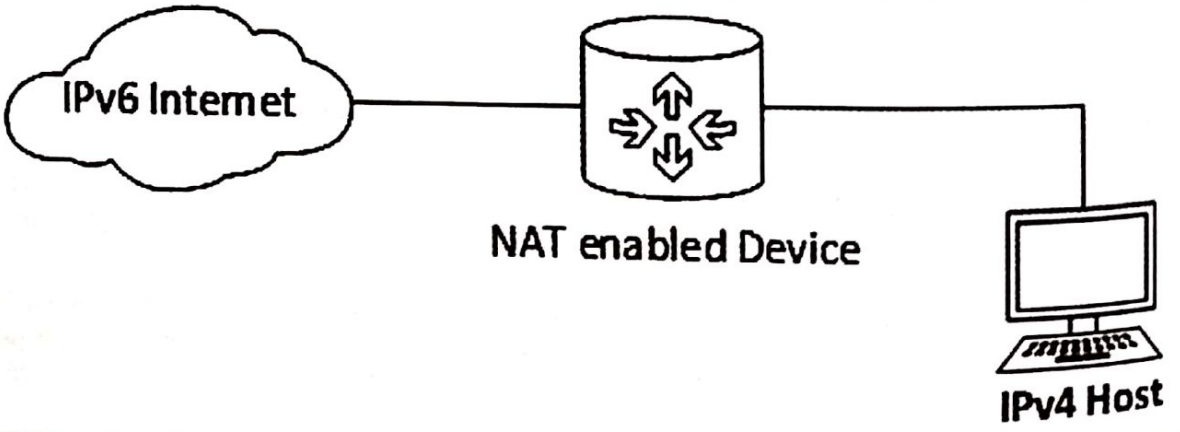
The IPv4 Compatible tunneling method is very similar to 6to4 tunneling; both provide a mechanism to tunnel IPv6 over IPv4. The major difference is how the IPv4 address is embedded inside the IPv6 address that is used by the edge device.

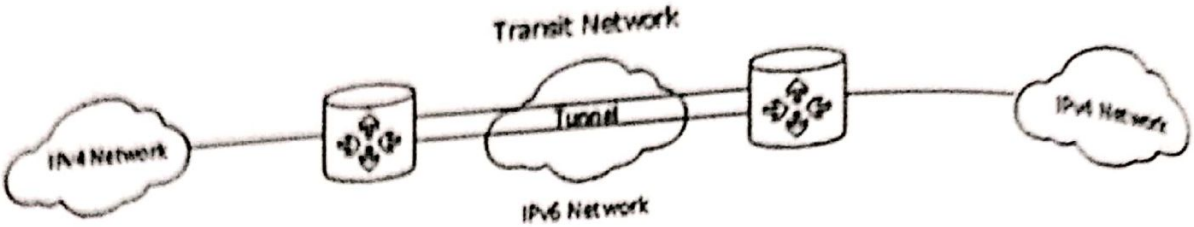
Translation

The concept behind this type of NAT and the newer technologies that support address translation between IPv4 and IPv6 networks is similar (9). IPv6 translation technologies differ from IPv6 tunneling technologies; this is because the translation technologies enable IPv4-only devices to speak to IPv6-only devices, which is not possible with any of the tunneling methods. There are two methods that are typically used with translated IPv6 networks. Figure 5 is an example of translation.

Network Address Translation—Protocol Translation (NAT-PT)

The NAT-PT method enables the ability to either statically or dynamically configure a translation of an IPv4 network address into an IPv6 network address and vice versa. Implementation of NAT operation 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.





Generic Routing Encapsulation (GRE) IPv6 tunnels

GRE is a protocol that was developed by Cisco and for the purposes of IPv6 tunneling operates and is configured very much the same as manual tunnels. GRE itself is able to be used to tunnel over a diverse number of network layer protocols other than IPv4

6to4 Tunnels:

As the name suggests a 6to4 tunnel allows IPv6 to be tunneled via IPv4. Unlike the previously discussed tunneling methods, the 6to4 method is automatically set up using the 2002::/16 IPv6 address space(8). 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 but allows the implementer to use the IPv6 block that was assigned to it.

IPv4 Compatible Tunnels

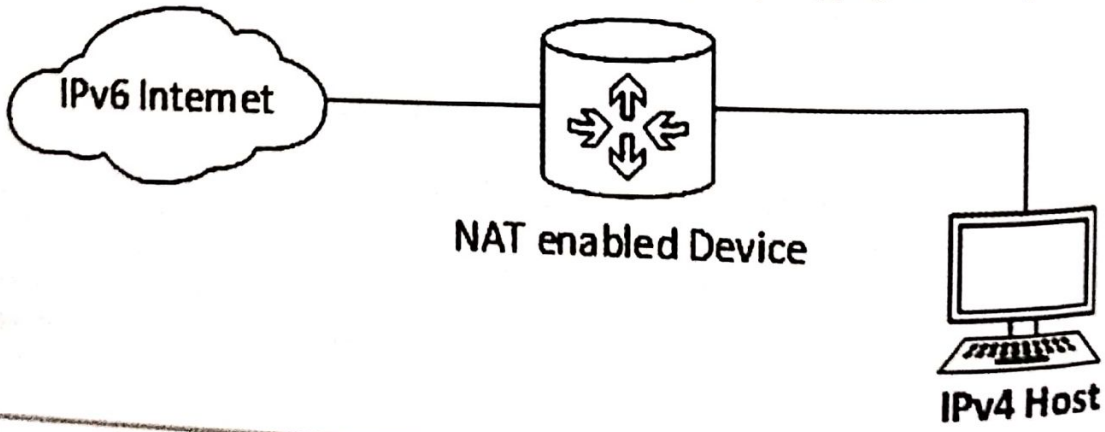
The IPv4 Compatible tunneling method is very similar to 6to4 tunneling; both provide a mechanism to tunnel IPv6 over IPv4. The major difference is how the IPv4 address is embedded inside the IPv6 address that is used by the edge device.

Translation

The concept behind this type of NAT and the newer technologies that support address translation between IPv4 and IPv6 networks is similar (9). IPv6 translation technologies differ from IPv6 tunneling technologies; this is because the translation technologies enable IPv4-only devices to speak to IPv6-only devices, which is not possible with any of the tunneling methods. There are two methods that are typically used with translated IPv6 networks. Figure 5 is an example of translation.

Network Address Translation—Protocol Translation (NAT-PT)

The NAT-PT method enables the ability to either statically or dynamically configure a translation of an IPv4 network address into an IPv6 network address and vice versa. Implementation of NAT operation 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

One of the main limitations to NAT-PT was that it tied in ALG functionality; this was considered a hindrance to deployment. With NAT64 also came DNS64, both of which are configured and implemented separately; when these were defined and accepted the use of NAT-PT was depreciated. NAT64 offers both a stateless and stateful option when deploying, the latter that keeps track of bindings and enables 1-to-N functionality. Communication has been compromised. This is because IPv4's lack of suitable authentication mechanisms. Many techniques or method had been developed to overcome the abovementioned security issues. For instance, the use of 'IPSec' to aid the use of encrypted communication between hosts, but this is still optional and continues to be the main responsibility of the end hosts.

The Comparison of Ipv6 Transition Methods

Table1 describes the advantages and disadvantages of three transition methods of IPv4-IPv6. By this comparison, we found Dual stack is best method of transition.

Method	Advantages	Disadvantages
Dual stack	• Easy to implement • Low cost • Greatest flexibility • Already supported in all OSs and devices	• Two routing tables • Additional memory and CPU power • Two firewall sets of policies
Tunneling	• Configure tunnel endpoints only • Simple deployment • No additional management	• Face another problem of NATs • Take more time and CPU power • Harder to troubleshooting and network management • Have single points of failure • Vulnerable to security attacks
Translation	• The router is used as a translation communicator • Solve network interoperability problems	• Limitations similar to IPv4 NAT • Reduction in the overall value and utility of the network. • Harder to control on a larger scale • Complexity increases in IP addresses

Table 1: Summary about three transition methods

Discussion

The industry faces a challenging transition while it moves carefully from its current IPv4-capable routers, switches, servers, and applications to IPv6-ready devices. Service providers whether they are providing content, hosting services, cloud services, or Internet access cannot add or accommodate new customers unless their services are equally accessible to both IPv4 and IPv6 users. The most cost effective and sensible migration strategy is to build on existing infrastructure using transition technologies to selectively add new IPv6 services as needed. Dual Stack operation, 6-to-4 tunneling and 6-to-4 translation are the key elements of IPv4 to IPv6 transition mechanisms. Implementations of these elements in IPv6 products are dependent on deployment and architectural factors.

This paper discussed the brief introduction of limitations of IPv4, header format and new features of IPv6, transition techniques of IPv4 to IPv6. IPv6 is there to replace IPv4, but even though IPv6 addresses have been available since 1996, the development of IPv6 has been very slow. The reasons are multiple but can be summarized in the hysteresis and path dependence in the system, which is caused by the many different kinds of switching costs associated with a transition. At present, IPv6

traffic is well below 1% of total Internet traffic. Based on this study we concluded that the transition to IPv6 network should be carefully planned. We need to carefully study the requirement for the transition and address the security related issues on the implementation.

References

1. http://journal.info.unlp.edu.ar/journal/journal33/papers/JCST-Aug12-3.pdf

2. "IPv6 Internals", The Internet Protocol Journal - Volume 9, Number 3, Iljitsch van Beijnum http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-3/ipv6_internals.html

3. http://cs.nmu.edu/~randy/Classes/CS442/Notes/IPv6_Header.html

4. http://technet.microsoft.com/en-us/library/cc780593(v=ws.10).aspx

5. https://www.os3.nl/_media/2011-2012/courses/lia yannick_scheelen_jeffrey_bosma_-_ipv6_jumbograms.pdf

6. http://www.juniper.net/techpubs/en_US/junos/topics/concept/ipv6-dual-stack-understanding.html

7. "IPv6 Tunneling Technology Configuration", by Sean Wilkins, Article is provided courtesy of Cisco Press on Jun 26, 2013. http://www.ciscopress.com/articles/article.asp?p=2104948

8. "6to4 IPv6 Tunneling", by stretch | Monday, March 15, 2010 at 12:29 a.m. UTC http://packetlife.net/blog/2010/mar/15/6to4-ipv6-tunneling/

9. Implementation and Evaluation of Protocols Translating Methods for IPv4 to IPv6 Transition, Cristian