American Journal of Scientific Research
ISSN 1450-223X Issue 33(2011), pp. 117-126

http://www.eurojournals.com/ajsr.htm

Transition Techniques of the Future Internet Protocol-IPv6

Ibikunle Frank. A.
Electrical & Information Engineering Dept
Covenant University, Ota, Nigeria

Oshin Babasanjo
Electrical & Information Engineering Dept
Covenant University, Ota, Nigeria

Abstract

In the 1970's the Internet Protocol (IP) was designed after much decision on it. Thirty years after its deployment and usage, the resulting design (i.e., IPv4) has been more than sufficient even though certain techniques had to be implemented to further reduce the rapid depletion of the IPv4 address space due to the exponential growth of the internet. However, the techniques implemented to further reduce the rapid depletion of IPv4 were only just temporary and have serious limitations. It should no longer be news that the transition from IPv4 to the new internet protocol (IPv6) will have to happen now. The transition techniques to achieve this transition process and the benefits that will accrue from having such an addressing scheme are the ultimate objective of this work. The paper clearly iterated that for successful transition to take place, organizations must first begin to run IPv4 and IPv6 in parallel. The vulnerable impacts of the transition and the appropriate solutions were explained.

Keywords: Network Security, IPv6, IPv4, Next Generation Network

1. Introduction

The Internet Protocol is a network-layer protocol in the OSI model that contains addressing information and some control information that enable packets to be routed in a network [4]. IP is the primary network-layer protocol in the TCP/IP protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP is equally well suited for both LAN and WAN communications. Internet Protocol has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through a network; and providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes. The IP addressing scheme is integral to the process of routing IP datagrams through an internetwork. Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for sub-networks. Each computer (known as host) on a TCP/IP network is assigned a unique logical address (32-bit in IPv4) that is divided into two main parts: the network number and the host number. The network number identifies a network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned

by the local network administrator. It is to be noted that IPv4 was designed with no security feature in mind, since it assumed that security should be provided by the end nodes. This is because in IPv4, IPSec which is a security feature is optional, unlike in the new internet protocol IPv6 where IPSec is a mandatory feature.

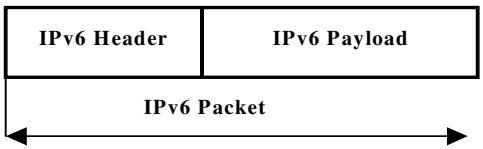
The sustainability of the IPv4 address space was really an impressive achievement for engineering and the engineers and this was sustained up until 2011 when the last set of IPv4 addresses were allocated [1]. Even though the various techniques implemented was a big plus to engineering, it was still not enough to cater for the enormous growth of the internet and the devices connected to it. It was observed that there will come a time the available IPv4 addresses will be exhausted, and this led to the recommendation of IPv6 on July 25, 1994 in RFC 1752 by IETF. Thus, the implementation of the new internet protocol is a big step in the right direction as it provides more addresses space, that is, 128 bit address system as against the 32 bit address system of IPv4. The address system of IPv4 in theory provides for only about 4 billion addresses [RFC1715] [2]. The new internet protocol provides enough addresses for about 340 un-decillion or 3.4×10^{38} addresses. IPv6 will support the deployment of new applications over the internet and it will open up broad fields of technology development [2, 3].

This paper enumerates the technical features, the business benefits, advantages of the new internet protocol and the security issues of both IPv4 and IPv6. The work explores the transition process from IPv4 to IPv6. The developed mechanisms to enable a seamless migration from IPv4 to IPv6 were examined. Finally, some deployment issues and strategies to prepare an adoption plan for deploying the IPv6 in an enterprise are given.

2. The Future Internet Protocol (IPv6)

Like IPv4, IPv6 is a connectionless, unreliable datagram protocol used for routing packets between hosts [4]. IPv6 always makes a best-effort attempt to deliver a packet. An IPv6 packet might be lost, delivered out of sequence, duplicated, or delayed. IPv6 does not attempt to recover from these types of errors. The acknowledgment of packet delivery and the recovery of lost packets are done by a higher-layer protocol, such as TCP. From a packet-forwarding perspective, IPv6 operates just like IPv4. An IPv6 packet, also known as an *IPv6 datagram*, consists of an IPv6 header and an IPv6 payload, as shown in Figure 1.

Figure 1: IPv6 packet format



Taking a look at the IPv4 header in Figure 5 it can be seen that the field shaded in yellow were deleted from the header field in IPv6 [5].

Figure 2: IPv4 header

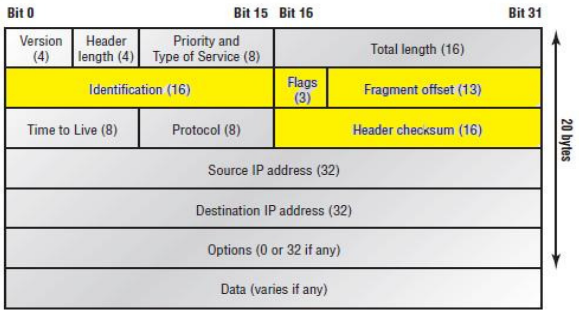
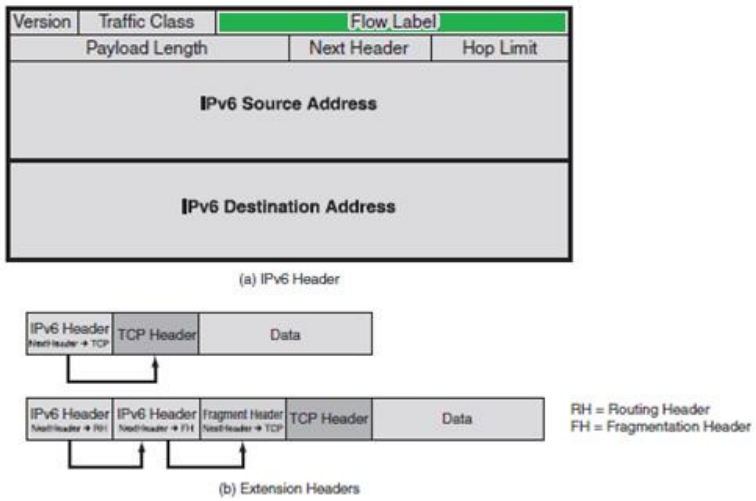


Figure 3, Depicts the header of IPv6, along with the extension header mechanism. It is to be noted that the area shaded in green is a new field in IPv6 [6]. IPv4 headers and IPv6 headers are not directly interoperable- hosts or routers must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats. This gives rise to a number of complexities in the migration process between the IPv4 and the IPv6 environments. However, techniques have been developed to handle these migrations.

Figure 3: IPv6 header



2.1. Benefits of IPv6

IPv6 is the new internet protocol that has been designed to have certain features that are better than the outgoing IPv4 addresses [6]. The functions that have been known to be working in IPv4 were retained and new features were added to improve functionality of the new internet protocol and thus led to the following benefits over the exhausted IPv4 address space [RFC 1752].

i. **Larger addresses:** From 32 bit address space in IPv4 to 128 bit address space. It enables all nodes to be addressable and reachable, removing the need for network address translation and restoring the end-to-end model for end-to-end capabilities such as security.
ii. **More levels of addressing hierarchy:** Multiple levels in the addressing hierarchy provide better aggregation of routes, easier allocation of addresses to downstream and scalability of the global routing table.
iii. **Auto configuration of nodes:** Auto-configuration is based on advertisements about the link addressing sent by the routers. Nodes insert their MAC address into the host part of the IPv6 address. It enables fast and reliable configuration of nodes, as well as easy renumbering.
iv. **Simpler and more efficient IP header:** Routers process the packets faster and more efficiently, which improves the forwarding performance.
v. **Mandatory IP security:** IPSec is mandatory in IPv6, which makes all nodes in a position to secure their traffic, if they have the necessary underlying key infrastructure.
vi. **Mobility Support:** the IPv6 protocol also provides a capability to support mobile devices. This feature allows for a device to have one unique IP address that permanently belongs to it regardless of location. As the mobile devices moves from one network to another, a new IPv6 address is created by incorporating the devices unique IP address and the network's designation number.

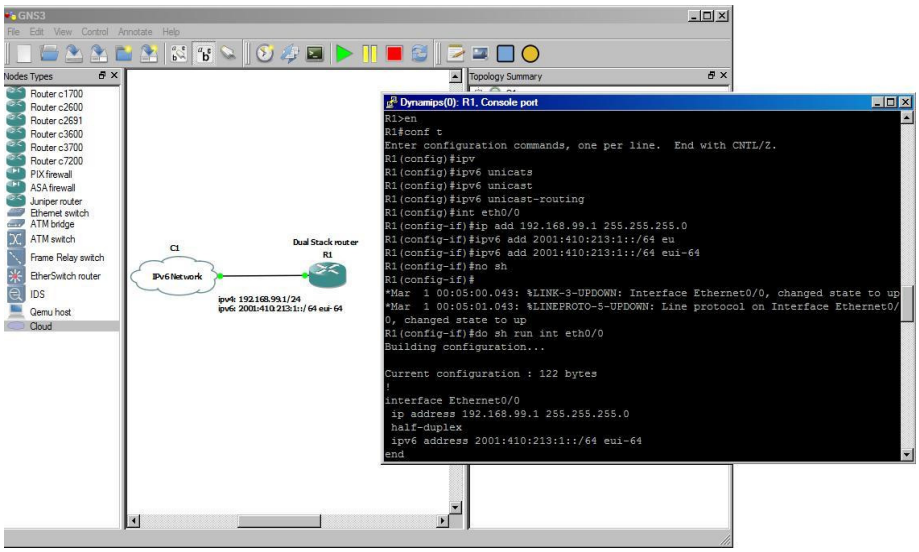
2.2. The Transition Process

In the past, various transition mechanisms have been brought up with each of them having their own advantages and disadvantages. What is most important is analysing your network to find out which transition method best suits your network [11]. There are three transition mechanisms that are in use. They are: Dual Stack, Tunnelling and Translation

2.2.1. Dual Stack [RFC 4213]

This is the most direct of all the transition processes in making IPv6 compatible with IPv4 nodes and it was described in RFC 4213 [6]. In this transition process, the node maintains both IPv4 and IPv6 stack. A network node that supports both internet protocols is called a dual stack node. Thus a dual stack node can have both IPv4 and IPv6 packets transmitted.

Figure 4: Configuration of dual stack on a Cisco router using GNS3



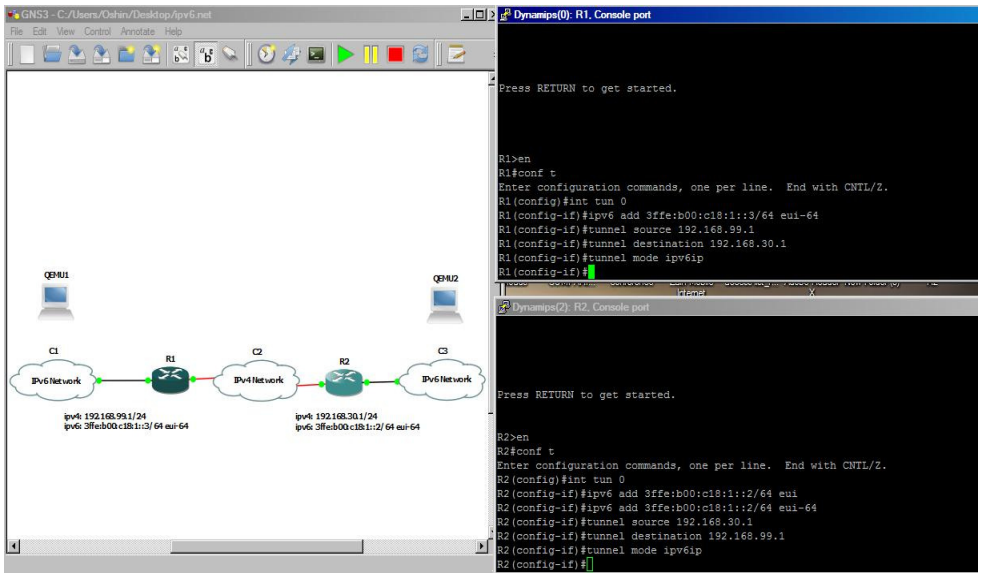
This type of transition process is a preferred method for application servers [7]. The choice of the IP version is based on name lookup and application preference. For an upper layer application supporting both IPv4 and IPv6, either TCP or UDP can be selected at the transport layer, while IPv6 stack is preferred at the network layer.

2.2.2. Tunnelling [RFC 3056]

Tunnelling provides a way of using the existing IPv4 routing infrastructure to carry IPv6 traffic and was described in RFC 3056. This is because the key to a successful IPv6 transition is the compatibility with the existing IPv4 hosts and routers. This can be done by tunnelling the IPv6 datagram over regions of IPv4 routing topology by encapsulating them within IPv4 packets [8]. Tunnelling can be used in a variety of ways, such as: Router-to-Router, Host-to-Router, Host-to-Host and Router-to-Host. Tunnelling techniques are also classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel. In router-to-router or host-to-router methods, the IPv6 packet is tunnelled to a router. In host-to-host or router-to-host methods, the IPv6 packet is tunnelled all the way to its final destination.

There are two types of tunnels in IPv6: Automatic tunnels which are configured by using IPv4 address information embedded in an IPv6 address, and the configured tunnels which must be configured manually. These tunnels are used when using IPv6 addresses that do not have any embedded IPv4 information. The IPv6 and IPv4 addresses of the endpoints of the tunnel must be specified.

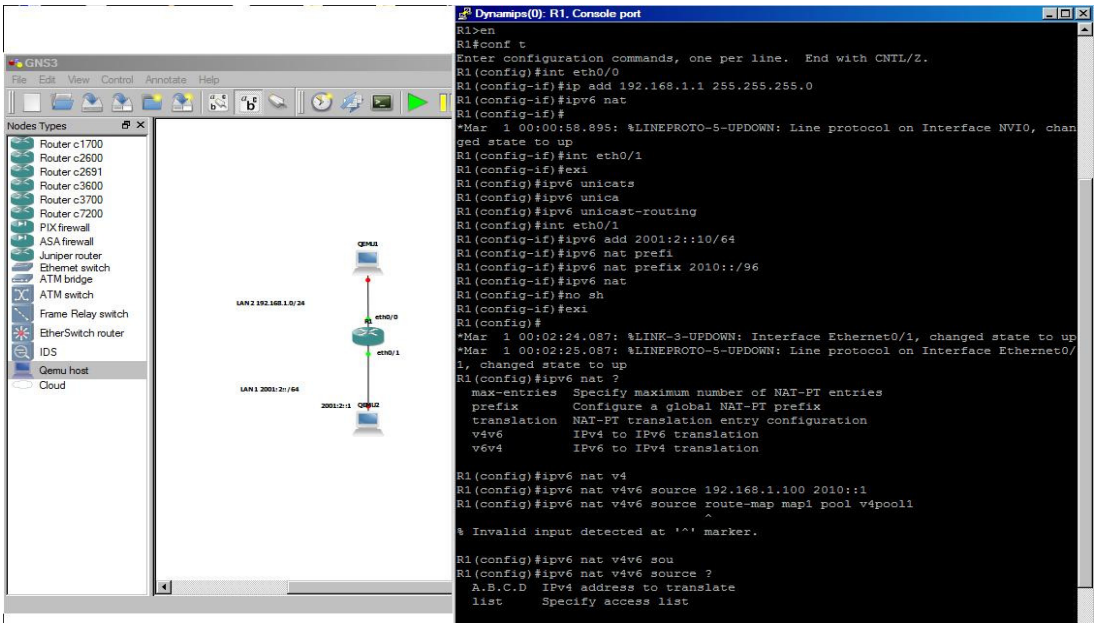
Figure 5: Configuration of tunnelling on a Router using GNS3



2.2.3. Translation [RFC 2765 and RFC 2766]

Translation is the tool of last resort. These schemes are inherently complex. They need to be used anytime dual stack is not an option, such as in a case where there are simple workstations that cannot be upgraded, or nodes that are accessing the network through a NAT port [10]. Stateless IP/ICMP Translation Algorithm (SIIT) describes such a process that can be used in separate applications such as NAT-PT (Network Address Translation-Protocol Translation).

Figure 6: Configuration of NAT on a Router using GNS3



The goal is to provide transparent routing for nodes in IPv6 networks to communicate with nodes in IPv4 networks and vice versa. The NAT gateway uses a pool of globally unique IPv4 addresses and binds them to IPv6 addresses. No changes to the end nodes are necessary [6].

The translation mechanisms described in RFC 2766 [10] should be used only if no other transition mechanism is possible and dual-stack operation should be avoided for certain reasons. This mechanism has a number of disadvantages. For instance, it does not take full advantage of the

advanced capabilities that IPv6 offers. But it is a choice when, for a certain time, access to IPv4-only networks and applications is needed

3. Stages of IPv6 Deployment

3.1. Implement IPv6 on your External Facing Internet Presence

Since there will be an introduction of IPv6 only clients in the coming months and years, namely new mobile devices, it is only imperative that organizations should support IPv6 on their external facing web sites, mail servers and other application. There are two options to achieve this task, either to implement Dual-stack or Translation. It is to be noted that the use of the translation method introduces a number of operational concerns. All traffic will need to traverse the protocol translation (PT) device creating a potential performance bottleneck.

3.2. Migrate the Core Backbone and WAN to Dual-Stack

The organization should consider deploying IPv6 internally on their switches and routers to achieve parity with other organizations as they do same. This means that all organizations are advised to switch over to dual-stack deployment of all internal switching and routing. WAN optimization equipment, firewall, and the infrastructure and security components impacting the WAN must also be IPv6 compatible.

3.3. Migrate the Intranet to IPv6

With the core backbone infrastructure in place, organizations should enable local IPv6 access to the intranet. This could be done with the IPv6 to IPv4 translation but for the various operational complications, the preferred deployment route is dual stack again.

3.4. Implement IPv6 Internet Access

The availability of IPv6 sites is growing. A couple of years back, just a little more than 3 Autonomous Systems announced IPv6 routes. Today, there are about less than 1,000 IPv6 routes in the Internet routing table and less than 100 new IPv6 Internet routes a year [12]. Today, websites such as google.com, facebook.com and youtube.com all have IPv6 web presence.

3.5. Enable Native IPv6 Access to the End Client

With the core of the infrastructure in place, organizations can then push IPv6 access to the edge of their network. The way IPv6 addresses are assigned and managed should be put into total consideration.

4. Security Issues

This section takes an overview of known limitations of IPv4, and a brief look at the security features and issues of IPv6.

4.1. IPv4 Security Issues

IPv4 was designed with no security in mind, because of its end-to-end model. IPv4 assumes that security should be provided by the end nodes [13]. For instance, if an application such as e-mail requires encryption services, it should be the responsibility of such application at the end nodes to provide such services. Today, the original Internet continues to be completely transparent and no security framework provides for resilient against threats such as:

i. *Denial of service attacks (DOS)*: This is a type of attack in which certain services are flooded with a large amount of illegitimate requests which render the targeted server unreachable by legitimate users. An example of DOS attack that results from an architectural vulnerability of IPv4 is the broadcast flooding attack or Smurf attack [14]
ii. *Malicious code distribution*: viruses and worms can use compromised hosts to infect remote systems. IPv4's small address space can facilitate malicious code distribution [14].
iii. *Man-in-the-middle attacks*: IPv4 lacks proper authentication mechanisms which may facilitate men-in-the-middle attacks. Additionally, ARP poisoning and ICMP redirects can also be used to perpetrate this type of attacks [14, 15].
iv. *Fragmentation attacks*: This type of attacks exploits the way certain operating systems handle large IPv4 packets. An example of this type of attack is the *ping of death* attack. In a *ping of death* attack the target system is flooded with fragmented ICMP *ping* packets. With each fragment, the size of the reassembled *ping* packet grows beyond the packet size limit of IPv4, therefore crashing the target system [14].
v. *Port scanning and other reconnaissance attacks*: In this type of attacks a whole section of a network is scanned to find potential targets with open services. Unfortunately, IPv4's address space is so small that scanning a whole class C network can take a little more than 4 minutes [16].
vi. *ARP poisoning and ICMP redirect*: In IPv4 networks, the Address Resolution Protocol (ARP) is responsible for mapping a host's IP address with its physical or MAC address. This information is stored by each host in a special memory location known as the ARP table. Each time a connection with an unknown host is needed, an ARP request is sent out on the network. Then, either the unknown host responds broadcasting its own IP address or a router does it with the appropriate information. *ARP poisoning* occurs when forged ARP responses are broadcasted with incorrect mapping information that could force packets to be sent to the wrong destination. A similar approach is used by ICMP redirect attacks [14].

However, many techniques have been developed to overcome some of the IPv4 security limitations. Though Network Address Translation (NAT) and Network Address Port Translation (NAPT) were introduced to facilitate the re-use and preservation of a rapidly depleting IPv4 address space, these techniques can also provide for certain level of protection against some of the mentioned threats. The introduction of IPSec also facilitated the use of encryption communication, although its implementation is optional and continues to be the sole responsibility of the end nodes.

4.2. IPV6 Security Improvements

It is important to acknowledge the fact that IPv6 is not necessarily more secure than IPv4, but its approach to security is only marginally better than IPv4 [17]. The following sub-sections summarize some IPv6's improvements that provide for better network security.

4.2.1. Large Address Space

Port scanning is said to be one of the best known techniques in use today. Port scanning allows "black-hats" to listen to specific ports that could be associated to well-known vulnerabilities [16]. In IPv4 networks, port scanning is a relatively simple task. Most IPv4 segments are Class C, with 8 bits allocated for host addressing. Scanning a typical IPv4 subnet, at a rate of one host per second, translates into:

2^8 hosts * 1 second/ 1 host * 1 minute/ 60 seconds = 4.267minutes.

In IPv6 networks, the landscape is radically different. IPv6 subnets use 64 bits for allocating host addresses. Consequently, a typical IPv6 subnet requires:

2^{64} hosts * 1 sec/ 1 host * 1 year/ 31,536,000 sec = 584,942,417,355 years

Scanning such a large address space is almost an impossible task [15]. However, it is not absolutely impossible [17].

4.2.2. IPSec

IPv4 offers IPSec capability. However, IPv4's support for IPSec is optional. By contrast, the RFC4301 mandates for IPv6 to use IPSec in all nodes [15, 18]. IPSec is a set of cryptographic protocols that provides secure data communication. IPSec uses two wire-level protocols namely;

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

The first protocol provides authentication and data integrity. The second protocol provides authentication, data integrity, and confidentiality [18]. In IPv6 networks both the AH header and the ESP header are defined as extension headers. Additionally, IPSec provides for a third suite of protocols for protocol negotiation and key exchange management known as the Internet Key Exchange (IKE). This protocol suite provides the initial functionality needed to establish and negotiating security parameters between endpoints. Additionally, it keeps track of this information to guarantee that communication continues to be secure up to the end.

4.3. Security Issues in IPv6

The new IPv6 protocol stack represents a considerable advance in relation to the old IPv4 stack. However, despite its innumerable virtues, IPv6 still continues to be vulnerable. This section reviews some areas of IPv6 where security continues to be an important issue.

4.3.1. Dual-Stack Related Issues

At present, the Internet continues to be mostly IPv4 based. However, this will change soon as IPv4 addresses have been completely exhausted and more networks are migrated to the new protocol stack. Unfortunately, migrating millions of networks is going to take quite some time. In the meantime, some form of 6 to 4 dual-stack will supply the desired functionality. However, most of the issues are not a direct result of specific IPv6 design flaws but mostly a result of inappropriate configuration [19].

4.3.2. Header Manipulation Issues

The use of extension headers and IPSec can deter some common sources of attack based on header manipulation. However, the fact that extension headers must be processed by all stacks can be a source of trouble. A long chain of extension headers could be used to overwhelm certain nodes (e.g., firewalls) or masquerade an attack. Best practices recommend for filtering out traffic with unsupported services [15]. Spoofing continues to be a possibility in IPv6 networks. However, because of Neighbour Discovery (ND), spoofing is only possible by nodes on the same network segment. The same does not apply to 6 to4 transition networks. Although one approach to 6 to 4 transition is using some form of dual-stack functionality, another approach is using some type of tunnelling. Because tunnelling requires that a protocol is encapsulated in another, its use could be a source of security problems such as address spoofing [17].

4.3.3: Flooding Issues

Scanning for valid host addresses and services is considerably more difficult in IPv6 networks than it is in IPv4 networks. To effectively scan a whole IPv6 segment may take up to 580 billion year, because the address space uses 64 bits. However, the larger addressing space does not mean that IPv6 is totally invulnerable to this type of attack. Nor the lack of broadcast addresses makes IPv6 more secure. New features such as multicast addresses continue to be source of problems [20]. Smurf-type attacks are still possible on multicast traffic. Again, filtering out unnecessary traffic is the recommended best practice [15].

4.3.4. Mobility

This is a totally new feature of IPv6 that was not available in IPv4. Mobility is a very complex function that raises a considerable amount of concern when considering security. Mobility uses two types of addresses, the real address and the mobile address. The first is a typical IPv6 address contained in an extension header. The second is a temporary address contained in the IP header. Because of the characteristics of this networks (something more complicated if we consider wireless mobility), the temporary component of a mobile node address could be exposed to spoofing attacks on the home agent. Mobility requires special security measures and network administrators must be fully aware of them [15, 17].

5. Comparison of IPv4 and IPv6

Table 1: Comparison Analysis between the IPv4 and the new Internet Protocol (IPv6)

FEATURES	IPV4	IPV6
Address Resolution	Address Resolution Protocol (ARP) uses broadcast ARP request to resolve IP to MAC/Hardware address.	Multicast Neighbour Solicitation messages resolve IP address to MAC address.
Address Space	The address space available in IPv4 is 32 bits (4 bytes) in length.	The address space available in IPv6 is 128 bits (16 bytes) in length.
Internet Control Message Protocol (ICMP)	ICMP is used by IPv4 to communicate network information	Used similarly for IPv6; Internet Control Message Protocol version 6 provides some new attributes.
IP header	Variable length of 20-60 bytes, depending on IP options present.	Fixed length of 40 bytes. There are no IP header options. Generally, the IPv6 header is simpler than the IPv4 header.
Maximum Transmission Unit (MTU)	Maximum transmission unit of a link is the maximum number of bytes that a particular link type, such as Ethernet or modem, supports. For IPv4, 576 is the typical minimum.	IPv6 has an architected lower bound on MTU of 1280 bytes. That is, IPv6 will not fragment packets below this limit. To send IPv6 over a link with less than 1280 MTU, the link-layer must transparently fragment and defragment the IPv6 packets.
Multicast	Internet Group Management Protocol (IGMP) manages membership in local subnet groups.	Multicast Listener Discovery (MLD) message manages membership in local subnet groups.
Quality of Service (QoS)	Header does not identify packet flow for QoS handling by routers.	Header contains flow label field, which identifies packet flow for QoS handling by routers.
Routing Information Protocol (RIP)	RIP is a routing protocol supported by the routed daemon.	Currently, RIP does not support IPv6. IPv6 routing uses static routes.
Security Feature	IPSec is an optional feature in IPv4 and should be supported externally.	IPSec support is not optional in the implementation of IPv6.

6. Conclusion

With the exhaustion of IPv4, it is clear that concerted action on IPv6 deployment is necessary to ensure the stability of the Internet and its continued growth. Failure to deploy IPv6 as a replacement for IPv4 addresses will be the biggest threat to face the Internet. Without the widespread adoption of IPv6 in the next few years, there is a very real threat to the integrity, stability and interoperability of the Internet. It is therefore vital that all Internet stakeholders, from governments and vendors to ISPs and telecoms, to work together to safeguard the growth and innovation that has made the Internet the success story that it has become. Many early adopters have deployed IPv6 in their networks. For those who have not, there is the very real risk of escalating costs and of losing out to competitors who planned ahead and were able to deploy IPv6 strategically.

Also, IPv6 represents a considerable improvement when compared to IPv4 protocol stack. The new suite of protocols provides innumerable features that improve both the overall functionality as well as some specific security functions. Although IPv6 offers better security (larger address space and the use of encrypted communication), the protocol also raises new security challenges. Ultimately, the new protocol creates as many new security problems as it solves old ones. And if that is not enough, the transition from the old protocol stack to the new one may present even more challenges. Further work is ongoing on the issues that might arise from the full implementation of IPv6 to individual privacy.

References

[1] Cisco Certified Network Associate by Todd Lammle, 6th Edition

[2] Deploying IPv6 Networks by Ciprian Popoviclu, Patrick Grossetete, Eric Levi-Abegnoli, Cisco Press, February 2006

[3] IPv6 Forum, the New Internet: Internet for Everyone. (www.ipv6forum.com)

[4] Raicu and S. Zeadally, "Impact of IPv6 on End-user Applications," Proceedings of the 10th International Conference on Telecommunications, Vol.2, February 2003, pp.973-980

[5] Voice over IPv6 architecture for next generation VOIP networks by Daniel Minoh, pg 12

[6] IPv6 essentials "Integrating IPv6 into your Network" by O'Reilly, pg 181

[7] Cisco Certified Routing and Switching Guide, by Anthony Bruno pg 269

[8] Migrating to IPv6, "A practical guide to implementing IPv6 in mobile and fixed Networks" by Marc Blanchet.

[9] IPv4 running out of address space http://www.informationweek.com

[10] RFC search http://www.rfc-editor.org/rfcsearch.html

[11] D. Waddington and F. Chang, "Realizing the Transition to IPv6," IEEE Communications Magazine, Vol.40, No.6, June 2002, pp.138-147.

[12] IPv6 "Potential Routing table Size" by Jason Schiller.

[13] Bradner, S; "The end-to-end security", IEEE security and privacy. Vol, no 6, pp 76-79, March 2006.

[14] Campbell, P, Calvat, B; Boswell, S. Security + guide to network security fundamentals,

[15] Popoviciu, C; Levy-Avegnoli, E; Grossetete, P; deploying IPv6 networks, Cisco press, Indianapolis, IN, 2006.

[16] Ford M, "New internet security and privacy models enabled by IPv6". 2005

[17] Szigeti, S; Risztic, P; "Will IPv6 bring better security?" proceedings 30th envomicro conf, 2004.

[18] Kent, S, Seo, K; "Security architecture for the internet protocol" RFC 4301, 2005 http://trols.ietf.org/html/4301

[19] Hiromi, R, Yoshifuji, H "Problems on IPv4 and IPv6 network transition" proceedings of the international symposium on applications and the internet workshop, saint 2005.

[20] Vives, A, Palet, J; "IPv6 distributed security problem statement" the 2005 symposium on applications and the internet workshops.