INTERNATIONAL JOURNAL OF NATURAL AND APPLIED SCIENCES (IJNAS), VOL. 5, NOS.1& 2 (2010); P. 59 – 66, 4FIGS.

Threat analysis on ipv4 to ipv6 migration

O. O. Elechi

ABSTRACT

The need for making use of the Internet is fast growing in peoples lives today. One of the major protocols of the Internet, the Internet Protocol (IP) of the network layer has posed concern for the major groups managing the Internet since the early 1990s. This protocol handles the addressing techniques on how people/nodes are reached which is more like telephone numbers. Because of the fast growing rate people request for these numbers, there is the fear that the available numbers might be exhausted in the very near feature. An advancement of the earlier protocol has been developed with several additional features in mind and groups of people have been seen to just be migrating to this new protocol. But some issues are still of concern which should be properly looked into to be able to migrate to what is actually a better protocol. Some of these issues have been tabled and weighed here for the various interested groups to have a feel of.

INTRODUCTION

The Internet has become very essential in the daily lives of every Tom Dick and Harry. Today kitchen ovens now come with Internet connectivity. The First School Leaving Certificate student in Nigeria has to have some basic form of computing and Internet browsing knowledge to be able to fill forms necessary to further his studies. The necessity of the Internet does not need much emphasis any longer in this our age yet people still spend time trying to discover avenues (loopholes) for their malicious purposes and sell their products or kill others'. Survival of the fittest!

The Internet came into being with a small population of people to be served in mind. Today the available address place in the current addressing scheme (IPv4 Internet Protocol version 4) (Postel, 1981) though has served well in the Internet's growth over the last decade, is now meant to serve the wide and fast growing necessity which is fast on the depletion. Several techniques like Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT) have been developed to increase the coverage of IPv4 which with the ultimate design makes use of 32 bit addressing which ordinarily should be able to assign 2^{32} locations. A new technology (IPv6) (Hinden , 1999) has been developed by some group of stake holders with the guidance of the Internet Engineering Task Force (IETF) to take care of the limited address locations available.

This scheme makes use of 128 bit addressing and hence should be capable of giving every molecule available on earth an address location. Obviously sounds very interesting for present and future needs. Some countries like Japan and China have almost completely switched to the use of IPv6. The design also had in mind to provide other features and capabilities with options for extensions, auto configuration, simplified format, improved security features etc.

Overnight migration would obviously be expensive for everyone making use of the Internet because not all their equipment are IPv6 compatible. Newer versions of operating systems quite alright have compatibility with IPv6, but when you talk of routers, switches and gateway equipment, you then realise you are talking money.

Moreover, the greatest threats of the Internet, viruses and worms have not been well proven to been taken care of by this new generation IP

This paper tries to present an analysis of threat and other migration issues that should be well looked into before the final migration is scheduled

INTERNET PROTOCOLS, IPV4 AND IPV6

IPv4

The Internet Protocol version 4 (IPv4) [RFC 791], a protocol of the network layer of the Open System for Interconnection (OSI) model Wack et al., 2002, is still the commonest Internet Protocol in use today. Up to now, several Internet service providers (ISPs) have refused to buy equipment compatible with later versions of the Internet Protocol.

*Corresponding author. Email: kachyelechi@yahoo.com
[1] Department of Computer Science Ebonyi State University Abakaliki - Nigeria

With the IPv4 addressing, each IP address is 32 bits (equivalently 4 bytes) long, which should then be able to give 2^{32} IP addresses usually written in the sol called dotted decimal notation. For example 201.151.122.30 should actually stand for 11001001 10010111 01111001 00011110 where each number separated by the dot(s) stands for each byte. Ideally every host, router or other communicate able device in the Internet must have a unique IP address.

We will recall that the Internet is network of networks. In the Internet, each network has an address so also does each host. IPv4 makes use of three classes of addressing for general purpose addressing, classes A, B and C (Fig 1). Class A uses the first byte for network address and the last three bytes for host addressing making it possible to have ideally 2^{24} hosts each in each 2^{8} networks. Class B makes use of the first two bytes for network addressing and the remaining two for host addressing making it possible to have 2^{16} hosts each in each 2^{16} networks, while class C makes use of the first three bytes for network addressing and the last byte for host addressing making it possible to have 2^{8} hosts each in each 2^{24} networks.

In actual sense, the first bit in a class A address must be 0, so as to be used to be identified as a class A address thereby reducing the number of possible number of networks to 2^{7}. In class B the first two bytes are 10 and in class C the first three bytes are 110.

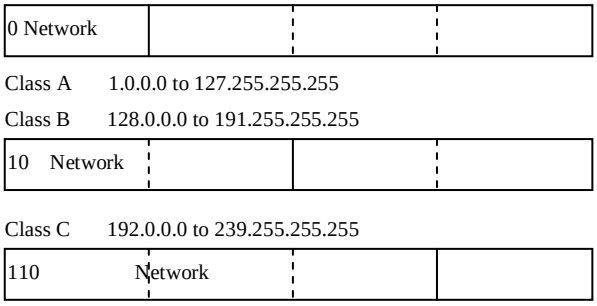

Fig 1. Classful addressing with address ranges (Kurose and Ross 2001)

Hence a class C address can be 223.1.7.0/24 where the ”/24” notation referred to as the network mask tells you that the first 24 bits is the network address. Each organisation then knowing the number of host it requires can then choose the class of addressing to go for.

These classes of addressing known as **classfull addressing** are no longer obeyed formally in the architecture of IPv4. This is because an organisation for example might need just two more IP addresses in excess of what is obtainable in Class B addressing and then go for a class A address which will then lead to large amount of waste of the scarce IP addresses. By 1996, the American Registry for Internet Numbers (ARIN) reported the complete exhaustion of the Class A addresses.

In 1993 then, the Internet Engineering Task Force (IETF), a community concerned with the development and operation of the Internet and its architecture, standardized the **Classless Interdomain Routing (CIDR)** [RFC 1519], where any number of leftmost bits can be used as the network address with the network mask well specified as with the example shown above. This greatly led to a drop in the rate of depletion of the available IP address. Further to that, an organisation (ISP for example) can still divide (create **subnets**) from the remaining rightmost bits to create its own internal networks within its network. Also with a technique known as IP masquerading, an organisation can have a single gateway router have a gateway router with two interfaces, one bearing an IP address (referred to as the public IP address) which is gotten from the service provider and the other bearing one of the internally generated IP addresses (referred to as the private IP address), which is assigned to the hosts in the Local Area Network (LAN). The hosts in the LAN are oblivious of the fact that the IP address which it is using is not visible in the public Internet. When any of these hosts try to make an Internet connection, the request on getting to the router is “apprehended” and a fresh packet generated bearing the source IP address as the routers address, and the response on arrival is redirected back to the originating internal host

With this second technique as well, it is obvious that IPv4 has gone a long way in saving its scarce IP addresses. This second technique is now commonly used by most LANs especially where the internal host is used for just browsing purposes and not going to serve as a public server.

IPv4 Datagram format

The IPv4 datagram format is shown in Fig.2 of which the fields are explained afterwards.

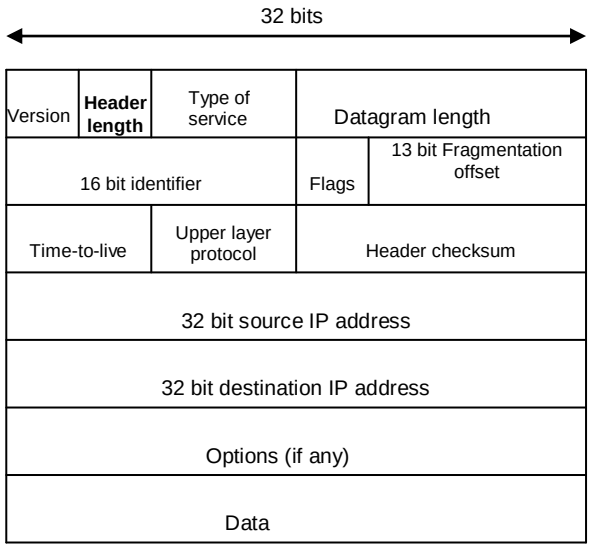

Fig 2. IPv4 datagram format

Version Number: This four bit field specifies the version of the Internet Protocol which the following datagram is built in.
Header Length: Though most times the option field is absent and of variable length, this value is used to know the actual length of the header and hence deduce where the actual data starts.

Type of Service: This specifies how the datagram should be handled and is of utmost importance in times of congestion to differentiate between data packets and control packets.

Datagram length: This specifies the length of the entire packet, main data and header.

Identifier, Flags, and Fragmentation offset: With IPv4, some datagram received from the upper layers might be too large and will have to be broken down into smaller chunks of packets, especially with the fact that the lower layer protocol in use might only be able to carry a certain amount of data at a time. These fields are then used for fragmentation and reassembly but only in end systems not in intermediate routers. IPv6 does not support fragmentation at intermediary nodes.

Time-to-live: This specifies the maximum amount of hops (routers) a datagram can make before it is discarded. It is used to ensure that a datagram does not circulate forever.

Protocol: this specifies the upper layer protocol the datagram will be handed over to on reaching the final destination.

Header Checksum: Each node uses this value to check for errors in the received datagram and discards it if present. Every two bytes in the header are summed using 1's complement and stored in this checksum field. It is recomputed at every router because certain values like the time-to-live changes at every router.

Source and destination IP address: these fields carry the 32 bit IP address of the originating host and final destination host.

Options: the inclusion of data in this field is actually optional. Some datagram require some certain options in handing while others do not. Those that carry these options are thought to have added to processing work of the router and because of this, the option field was not included in the IPv6 datagram format.

IPv6

The urge for the development of a successor of the IPv4 dates back to the early 1990s with the realization of the fast depletion of its available address. The development of the new version IPv6 had in mind to augment several drawback of its earlier version. It thus has these enhancements

Greater addressing capability: As has been mentioned earlier, this makes use of 128 bits each for source and destination addresses, making it possible to have up to 2^{128} address location unlike that of the much smaller IPv4 Arano (2004). This should give every molecule on earth an address.

Streamlined 40 byte header: Several fields have been removed in the IPv6 datagram header. Unlike the IPv4 header which had 13 fields, the IPv6 header has just 8 fields which should obviously lead to faster processing time of the IP datagram at various hops.

Priority determination: The IPv6 header has two fields, traffic class and flow label which are somehow used to assign various levels of priority to the datagram packets, which enables some datagram receive better or faster service than others Hopps (2003)

The format for the IPv6 datagram format is shown in Fig.3 and explained afterwards

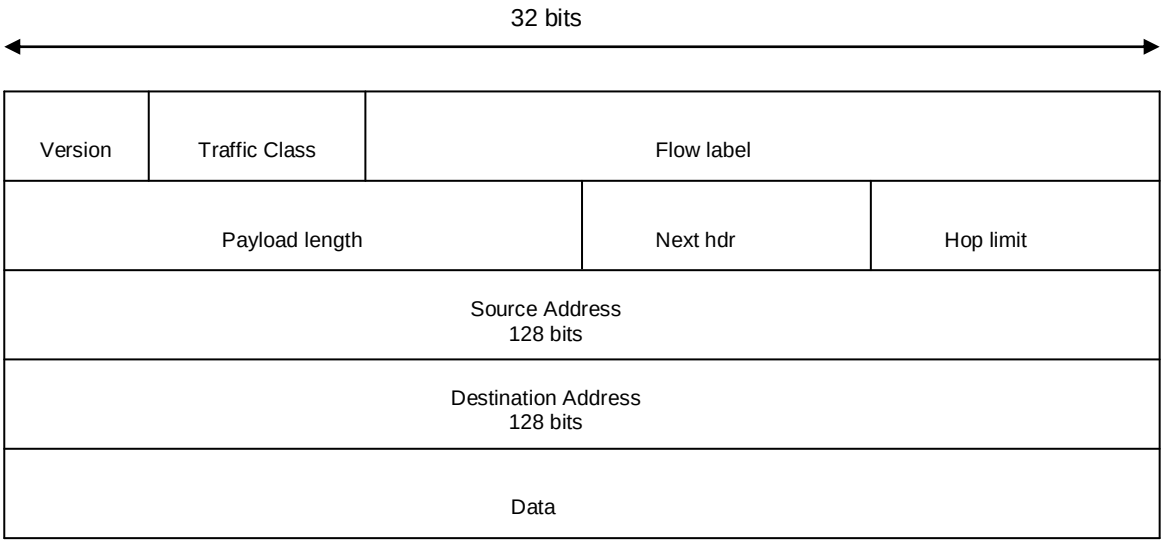

Fig 3. IPv6 datagram format

Version: Similar to that of IPv4 which is used to identify the version of the packet format. It is also four bits length.

Traffic Class and Flow label: Eight plus twenty bits field used to prioritise packets or group of packets. Within some certain groups (flow) as well, packets can be prioritised.

Payload length: This is a sixteen bit field showing the total number of bytes in the IPv6 datagram after the header.

Next header: This tells the upper layer protocol that the datagram will be handed over to at the destination end when the IPv6 header is stripped off (UDP or TCP).

Hop limit: Similar to time-to-live of IPv4. It states the maximum number of nodes the datagram can traverse in the network and then it is dropped on getting to that number. This is achieved by reducing the number in this field by one on traversing a node and finally dropped when it gets to zero to avoid the datagram circulating forever.

Source and Destination addresses: This is the 128 bit each source and destination IP addresses of the originating and destination hosts respectively

Data: The payload portion of the datagram which is handed to the upper layer protocol at the destination end.

THREATS TO IPV4 TO IPV6

This section outlines the various forms of threat and a comparison is made for the two protocols considered.

Reconnaissance: This usually is the first form of attack where the adversary tries to probe a network from layer two upwards to deduce the topography and figure out the various activities going on in the network. They can scan with tools like ping, traceroute, firewalk, and then port scans which would lead to the deductions of the deduce applications and operating systems running (Convery and Miller, 2003).

Header Manipulation and Fragmentation: This is a technique used to bypass network firewalls and Intrusion Detection Systems (IDS). Usually a fragmented data does not contain all its information so you cannot actually tell whether it is a valid data or not. It's been stated above that fragmentation is very necessary in IPv4 especially when a channel cannot carry a certain amount of Protocol Data Unit (PDU) size. Most IDS these days try to go a long way in reassembling fragmented data in order to figure out the type of data it is.

Spoofing: This is the situation whereby the adversary modifies its source IP address and port number to carry the network internal address so as to appear as data generated from the internal network. A common technique is injection false Simple Network Management Protocol messages. This situation makes it difficult for several adversaries to be tracked down and is still in massive usage.

DHCP and ARP attacks: DHCP stands for Dynamic Host Configuration Protocol which is an extension of BOOTP defined in RFC 1542 is on tools used by hosts in a LAN for initialisation such as to setup it's DNS (Domain Name System) and gateway addresses. The adversary tries to make the end hosts communicate with wrong systems in order to gain more access to the system. This it does by getting

involved with the initial communication on initialisation and responding to the hosts with these wrong information.

Virus: This remains the greatest problem to network stability today. Basically no end/human user system can operate in the Internet today with out some form of antivirus, Slade (2006) It has proven itself today to be the most cause of alarm in the network industry especially with that, which can be termed its younger and stronger brother – the worm

IPv4 best practices

With the use of firewall in most establishments or organisations, most people today find their business in the Internet stable and reliable. It is said that IPv6 is designed with better security features in mind, but with features available with most firewall systems, it is more like that there is not yet really any improvement in IPv6. Fig. 4 shows a typical design of an IPv4 network with a firewall installed to handle security features. In some scenarios, you find the functionalities of the edge router and the firewall being combined in one system

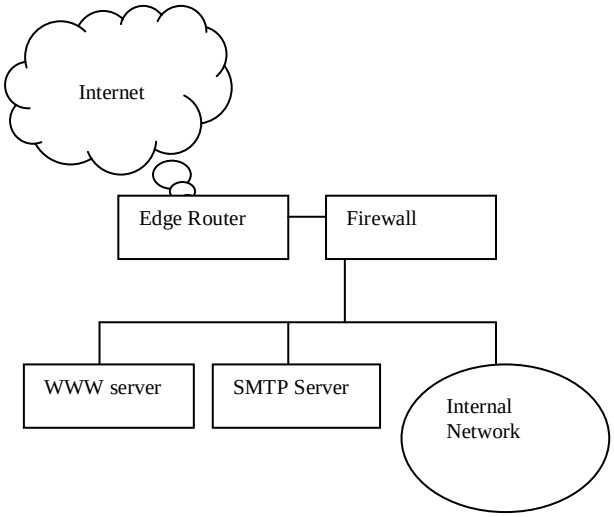

Fig 4. Common IPv4 network

You find from Fig. 4 that the security can be enforced in the firewall and the edge router. Other features can as well be deployed like intrusion detection, application proxies, etc. Usually most firewalls operate with a list of user defined rules set to handle data from layer two protocol upwards. Specifying rules for the lower layer protocols are easier and gets more cumbersome as you climb up the protocol stack. This is where your might say that IPv6 has an advantage with the insistence in use of IPsec enabling some form of end host firewall but we should not forget that intrusion tunneling is easier achieved with IPsec especially with out-of-order and overlapped fragments. An incoming protocol data unit into the firewall system is checked against the list of rules and if matched with a rule, an action specified against that rule is carried out. Most people set a default rule to drop a data that does not match any of the defined rules. Other common techniques normally adapted are listed below

- Logging: A successful hacking activity can be traced if logging is enabled. System administration can forward a log to collection sites that track and identity attackers that have scanned IP address.
- Port hiding: When a computer has this functionality on, and another computer tries to connect to it on one of its blocked port, it does not send any form of reply, thereby hiding the existence of such port and decreasing the vulnerability of the system. Even the IP address of the system as well can be hidden. This happens when the system does not answer to any form of other systems initiated request, but usually from the outside world
- Automatic lockout: Unlike dial-up, broadband connection has an always-on nature. Even with inactivity of users, the Internet connection is open for hackers and viruses at all times Tanenbaum, (1996). The automatic lockout feature turns off the Internet connection after a settable timeout.
- Connection Notification: Some firewall systems can be configured to notify the administrator when a new process is trying to access the Internet. The administrator then checks it out and allows or disallows it and might as well make that rule permanent in order not to be bothered in future when the same process wants to access the Internet.
- Spoofing denial: Most hackers and viruses try to penetrate a firewall by specifying one of the internal network's IP address as their own IP address. This can be checked by denying any data coming from the external interface of the firewall wall system and having internal source address.

Similarities in IPv4 and IPv6 attacks

In reconnaissance, because of the wider range of numbers in IPv6 networks and subnets, the scanning takes a longer time to complete but the technique is basically the same. But with

the new multicast and site specific addresses in IPv6, it makes it easy to find certain set of edge systems like servers and routers to attack.

As with IPv4, IPv6 firewall and IDSs try to go a long way with fragment reassembly. Even when you have out-of-order fragments, the system tries to place them in the correct order before allowing it to pass or drop it. With IPv6, fragmentation is not allowed in intermediary nodes and RFC 2460 does not give room for MTU smaller than 1280 octets. However, if overlapping packets are allowed to bypass the security device that poises the problem. Most administrators now drop the packet less than 1280 except if it is the last byte in the chain

Spoofing techniques are the same in IPv4 and IPv6 except that with IPv6, there is a greater array of numbers to play with. As stated earlier, you can setup your firewall rules to detect spoofed addresses and stop them from entering your network. Today, with the RFC 2827 technique, service providers can also check to ensure that spoofed data are not generated internally by their own subnets or customers. Especially where DHCP is in place and with the auto-configuration capability of IPv6, administrators now try to make use of layer addressing in screening data.

Viruses and Worms obviously have the same techniques in both IP versions. The designers of IPv6 systems also make room for the use of antivirus software like in IPv4. But with increased address space in IPv6, viruses and worms that scan for IP addresses in networks will find it difficult to succeed in this new version because of the large array of addresses to scan. However, all the techniques for antivirus in IPv4 is also deployed in IPv6.

MIGRATION ISSUES

There are several known techniques for migrating to a full fledged IPv6 network out of which two are widely know and used today. The two and a few others are highlighted below

Dual stack: This technique requires gradually introducing IPv4/IPv6 compatible equipment into the network from some ends, which will then be gradually replacing the IPv4 devices. These nodes speak both IPv4 and IPv6 hence can interoperate with devices that can speak only IPv6 or IPv4.

Tunneling: In this scenario, two networks or nodes that are IPv6 can communicate over an IPv4 network. The IPv6 packets are encapsulated in an IPv4 packet and passed through an IPv4 network. On getting to the IPv6 section, the IPv4 section is stripped of and then the packet is continued to be treated as IPv6 packet which is what it originally is. It is more like having several IPv6 islands connected through IPv4 networks. Though tunnelling has its drawbacks like slow throughput and administrators configuring tunnel endpoints, it is still the most adapted technique in use today.

6to4: This is meant to allow host on IPv4 networks communicate with IPv6 node with very minimal manual configuration, Emigh (2002) . Here you have a gateway router which is IPv4/IPv6 compliant and give the IPv4 border an address recognisable by IPv6 which is just prefixing the IPv4 32 bit address with "2002, "

Translation: When an IPv4 system need to communicate with an IPv6 system, some form of translation is required. This is usually done by the edge router rewriting the IP headers or using a Transmission Control Protocol (TCP) relay. This technique is often advised to be avoided and instead use an IPv4 to speak to IPv4 and IPv6 to speak to IPv6.

These techniques appear to be moving gradually and successfully but some countries have said that they will completely move over to IPv6 within a dead line without bearing in mind other factors and necessary improvement required for the successful transition. In fact, some other stake holders are even against the transition saying IPv4 is very successful and enough with the advent of CIDR and NAT. Today some web sites gather pools of peoples' opinion/votes of their preference or support on IPv4 or IPv6. Below are some issues that need serious consideration of the deployment of IPv6.

Hardware cost: The deployment of IPv6 will obviously need replacement of lots of host, routers, servers and lots of other computing equipment. It is very clear that not all these equipment are IPv6 compatible. We are also aware that most of these equipment before the expiration of their useful life normally have newer models with mode advanced and greater capabilities, but it is also possible that most of these equipment might have just been procured, or its useful life has not been utilized or might even have been as spare in a store all these while.

Software cost: It is well known that the firmware of most equipment is upgradeable. Most manufacturing companies today release the later version of the firmware of their products online. But you should not expect Windows XP which is the oldest version of Windows that supports IPv6 to

run on a 386 processor for instance. The Windows XP package is as well not even gotten free of charge. You will find out that there are a lot of hosts, routers and other terminal equipment which will need their software to be changed to be IPv6 compatible.

Training: To be able to make good use of new equipment or software, you have to be trained on how to use it. Lot of these companies will have to train their staffs or themselves to either continue in business or just to remain aware of their environment.

Other Protocols: The Internet comprises of lots of protocols that are for various uses in the Internet itself today. Some of these protocols have some involvements in the network layer while others do not. Those that interact with the network layer are not all IPv6 compliant. It is very possible that the protocols to replace all functionalities of these ones that not IPv6 compliant are not yet available, Perlman 2000

Undefined issues

There are several issues yet undefined in the new version of IP, IPv6 which has poised a great concern to network administrators especially with the fact that IPv6 is not backward compatible with IPv4 as with most cases of Information Technology (IT) solutions. CIDR and NAT have proven to be very successful in IPv4 but there are no straight out issues on network performance and network reliability that IPv6 have poised over these technologies.

IPsec which is a security specification designed to maintain the confidentiality of data is functionally the same in the two versions available. The only difference is that it is optional in IPv4 while IPv6 insists on it. But with the absence of IPsec, are there any other security features included in this our new version? Can the address authentication mechanism of IPsec deter spoofing attacks?

You find out that NAT devices not always function only as NAT devices. They can include routing functions, firewalls and IDS. The routing function makes it possible to allow for peer to peer connections. With the elimination of these middle devices can the IPv6 network function with as much stability as the IPv4?

CONCLUSION

As has been explained above, IPv6 offers a much greater address space than can be gotten with IPv4. You also find out that IPv4 gives additional functionalities that has not been measured in its new counterpart IPv6. With the development of NAT, you find out that most time the edge router bearing two IP addresses (private and public) act as not just the gateway but a firewall for the internal network. There is so much enthusiasm on moving into the new version that is not backward compatible and all functionalities of the old version have not been well explored in this new IP version. There are websites you will visit today and they take pools of peoples support for IPv4 or IPv6 showing that the trust for IPv6 is not yet strong in people or they are not yet well convinced. The major security advantage of IPv6 is its insistence of the use of IPsec which is optional in IPv4. But with the diagram shown in fig 4 most people have protected their IPv4 network comfortably even without any trace of IPsec. With the NAT and CIDR technologies, there is still time to give room for explorations on IPv6 to certify whether it is okay as it is and then specifically spell out various of these undefined issues stated in the last section above

REFERENCES

Arano T (2004). IPv6 Migration Issues (http://gac.icann.org/web/meetings/mtg19/IPv6MigrationIssues_TakashiArano.pdf)

Convery and Miller (2003). IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0) (http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf)

Emigh J. (2002). IPv6: Migration Issues Loom for NetworkAdministrators (http://suraj.lums.edu.pk/~cs678s04/2004%20Projects/Mids/Group06.pdf)

Hinden R. (1999). IP Next Generation (IP ng) (http://playground.sun.com/pub/ipng/html/ipng-main.html)

Hopps, C. (2003). Routing IPv6 with IS-IS (http://www.ietf.org.internet-drafts/draft-ietf-isis-ipv6-05.txt)

Kurose, J. F. and Ross, K. W. (2001). Computer Networking: A Top-Down Approach Featuring the Internet, Addison Wesley Longman, Inc

Perlman, R. (2000). Interconnections Second Edition: Bridges, Routers, Switch, and Internetworking protocols. Addison Wesley Longman

Postel J., (1981). [RFC 791] Internet protocol: DARPA Internet program Protocol Specification (http://www.rfc-editor.org/rfc/rfc791.txt)

Slade R., (2006). Robert Slade's Computer Virus History. Computer Knowledge Website (http://www.cknow.com/vtutor/RobertSladesComputerVirus.html)

Tanenbaum, A. S. (1996). Computer Networks, Prentice-Hall, Inc

Wack J., Cutlet K., Pole J., (2002). Guidelines on firewalls and firewall policy. National Institute of Standards and Technology 800-41, 5-12