# IPv4 versus IPv6 Security structure – A review using online sources

**Suleiman Abdullahi[1], Lawal Idris Bagiwa[2]**

[1]Department of Mathematics and Computer Sciences, Faculty of Natural and Applied Science, Al-Qalam University, Katsina, P.M.B. 2137 Dutsin-ma Road, Katsina State, Nigeria.
abduljby02@gmail.com

[2]Department of Computer Studies, College of Science and Technology, Hassan Usman Katsina Polytechnic P.M.B. 2052 Katsina State, Nigeria.
lbagiwa@yahoo.com

## Abstract

This paper was aimed at critically reviewing Journal Articles in order to make comparisons between Internet Protocol version 4 (IPv4) and Internet Protocol version 4 (IPv6) with emphasis on the issues related to security as well as to review the security challenges associated with IPv6 total implementation and total elimination of IPv4 in today's internet system.



## Introduction

**IPV4 - Internet Protocol version 4** (**IPv4**) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed.[1] IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).[2] IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery.[1] These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).[3]

The IPv4 address space is a 32 bit field.[8] There are 4,294,967,296 unique values, considered in this context as a sequence of 256 "/8s", where each "/8" corresponds to 16,777,216 unique address values.[11]

| Class | Most significant octet | No. of Networks | No. of users per network |
|---|---|---|---|
| A | 0XXXXXXX | $2^7 = 128$ | $2^{24}-2$ |
| B | 10XXXXXX | $2^{14} = 16,384$ | $2^{16}-2$ |
| C | 110XXXXX | $2^{21} = 2,097,152$ | $2^8-2$ |
| D | 1110XXXX | Multicast Address | |
| E | 11110XXX | Research Purpose | |

| Class | Start Address | End Address |
|---|---|---|
| A | 0.0.0.0 | 127.255.255.255 |
| B | 128.0.0.0 | 191.255.255.255 |
| C | 192.0.0.0 | 223.255.255.255 |

IANA reserved blocks for private internets

| Class | Start Address | End Address |
|---|---|---|
| A | 10.0.0.0 | 10.255.255.255 |
| B | 172.16.0.0 | 172.31.255.255 |
| C | 192.168.0.0 | 192.168.255.255 |

**IPV6 -** IPv6 is short for "Internet Protocol Version 6". IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4. In order to communicate over the Internet, computers and other devices must have sender and receiver addresses. These numeric addresses are known as Internet Protocol addresses. As the Internet and the number of people using it grows exponentially, so does the need for IP addresses. IPv6 is a standard developed by the Internet Engineering Task Force, an organization that develops Internet technologies. The IETF, anticipating the need for more IP addresses, created IPv6 to accommodate the growing number of users and devices accessing the Internet. [5]
IPv6 allows more users and devices to communicate on the Internet by using bigger numbers to create IP addresses. Under IPv4, every IP address is 32 bits long, which allows 4.3 billion unique addresses. An example IPv4 address is: 172.16.254.1[10]

In comparison, IPv6 addresses are 128 bits, which allow for approximately three hundred and forty trillion, trillion unique IP addresses. An example IPv6 address is:

2001:db8:ffff:1:201:02ff:fe03:0405 [3]

**IPv6 Address Prefix allocation Source: RFC: 1884[9]**

| Allocation Type | Format Prefix | Fraction of the address space |
|---|---|---|
| Reserved | 0000 0000 | 1/256 |
| Reserved for NSAP allocation | 0000 001 | 1/128 |
| Reserved for IPX allocation | 0000 010 | 1/128 |
| Provider-Based Unicast Address | 010 | 1/8 |
| Reserved for Geographic-Based Unicast Addresses | 100 | 1/8 |
| Link-local use addresses | 1111 1110 10 | 1/1024 |
| Site-local use addresses | 1111 1110 11 | 1/1024 |
| Multicast addresses | 1111 1111 | 1/256 |

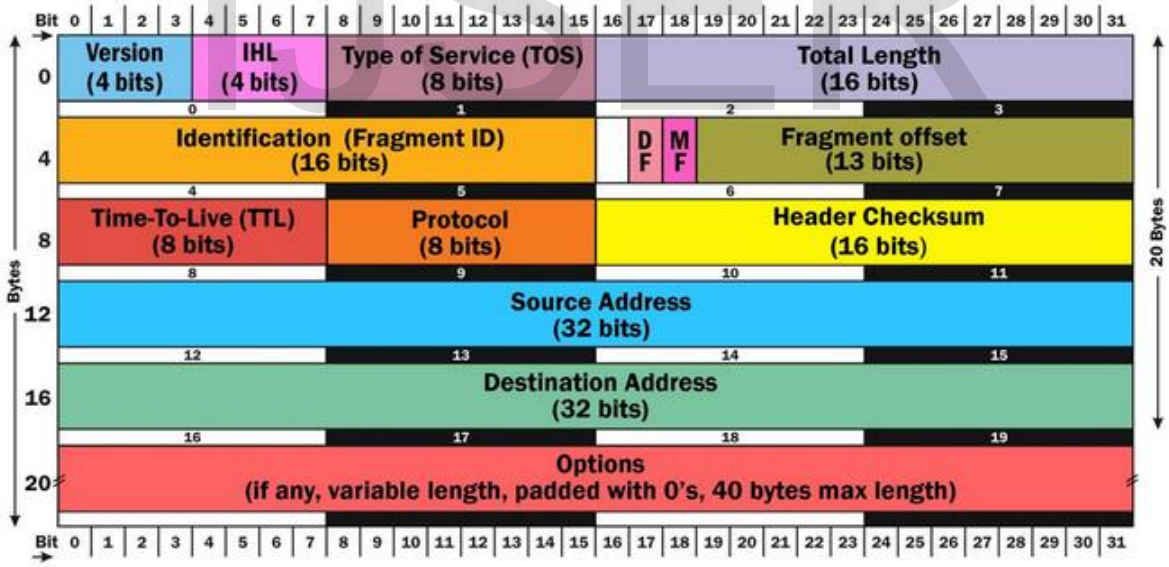
In IPv6, the address space is expanded from 32 bits to 128 bits that gives maximum of 2128 or about 3.403*1038 unique addresses. IPv6 has much larger address in comparison with IPv4. IPv6 is designed in such a way that it can provide unique addresses to everyone in this planet.[6]

The new features introduced with the IPv6 protocol can be summarized as follows:
1. A new header format
2. A much larger address space (128-bit in IPv6, compared to the 32-bit address space in IPv4)[2]
3. An efficient and hierarchical addressing and routing infrastructure [1]
4. Both stateless and stateful address configuration IPv6 Security v1.1 6
5. IP Security
6. Better Quality of Service (QoS) support [3]
7. A new protocol for neighboring node interaction
8. Extensibility [1]

**New header format**

The new header format in IPV6 was designed to be in fixed length(40 byte), even though some field from IPV4 has either been removed, renamed or moved to the new optional IPV6 extension header.[6]

**IPV4 Header**



## IPV6 Header

**Source: [9]**


The changes from IPv4 Packet Header to IPv6 Packet Header are as follows:

IPv4 **Version** field - same size (4 bits), same name, same function, in IPv6 Packet Header.

IPv4 **IHL** (Internet Header Length) field - ***discarded*** since IPv6 Packet Header is fixed length (40 bytes).

IPv4 **Type of Service** field - same size (8 bits), ***new name*** (**Traffic Class**), same function in IPv6 Packet Header.

IPv4 **Total Length** field - same size (16 bits), ***new name*** (**Payload Length**), now does not include length of the Packet Header, so new Payload Length = old Total Length - 40.

IPv4 **Identification (Fragment ID)** field - twice as big (32 bits), same name, same function, ***moved to Fragmentation Extension Header.***

IPv4 **DF** flag - ***discarded***, effectively always 1 (set) in IPv6.

IPv4 **MF** flag -same size (1 bit), same name, same function, ***moved to Fragmentation Extension Header***.

IPv4 **Fragment Offset** field - same size (13 bits), same name, same function, ***moved to Fragmentation Extension Header***.

IPv4 **Time-To-Live (TTL)** field - same size (8 bits), ***new name*** (**Hop Limit**), same function in IPv6 Packet Header.

IPv4 **Protocol** field - same size (8 bits), ***new name*** (**Next Header**), same function, in IPv6 Packet Header. There is a new set of possible values (some are the same as in the Protocol field in the IPv4 Packet Header, such as values for TCP, UDP and SCTP).

IPv4 **Header Checksum** field - ***discarded***, considered to be superfluous.

IPv4 **Source Address** field - ***new size*** (128 bits instead of 32), same name, same function, in IPv6 Packet Header.

IPv4 **Destination Address** field - ***new size*** (128 bits instead of 32), same name, same function, in IPv6 Packet Header.

IPv4 **Options** field - ***discarded*** (virtually never used in IPv4 Packet Header) - now Packet Header is fixed length (40 bytes) instead of 20 bytes + length of options field.[9]

Note: the order of the fields was also moved around some from the IPv4 Packet Header, to make fields line up better on 32 bit boundaries.

The enhancements in IPv6 provide better security in certain areas, but some of these areas are still open to exploitation by attackers.

## 2 Security Issues related to both IPV4 and IPV6

**Internet Protocol Security(IPSec)** Short for ***IP Sec****urity,* a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement Virtual Private Networks (VPNs). IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (*payload*) of each packet, but leaves the header untouched. [6]



In this review, the paper dwelled much on the IPV6 Security (IPV6Sec).

**IPV6Sec**

Under this feature there is need for one to look into the following:

**Address Space:**

The most obvious distinguishing feature of IPv6 is its use of much larger addresses. The size of an address in IPv6 is 128 bits, a bit-string that is four times longer than the 32-bit IPv4 address. A 32-bit address space allows for 232, or 4,294,967,296, possible addresses. [6] A 128-bit address space allows for 2128, or 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses.[3]

**IPSec and IPv6 Vulnerability**

A number of factors may also limit the possible security benefits of IPv6 deployment in the near term. For example, although the expanded IPv6 address space may eliminate address and port scanning-based network attacks, network administrators may also lose the ability to perform brute-force address scans for the purposes of security auditing and testing [7]. Many popular IPv4 security analysis tools are fundamentally based upon address scanning [6]. Thus finding and identifying misconfigured or compromised hosts that are deliberately “hiding” on an IPv6 subnet may be as difficult as attacking them from the outside[7].

***Tracking the identity of the user*** - In today's IPv4-based Internet, each time the user connects, a different IPv4 address might be obtained.[4] Because of this, the identity of users on the Internet is often unknown. So, it is difficult to track a dial-up user's traffic on the Internet on the basis of

IP address.[2] For IPv6-based dial-up connections, the user is assigned a 64-bit prefix after the connection is made through router discovery and stateless address auto-configuration. If the interface identifier is always based on the EUI-64 address, it is possible to identify the traffic of a specific node regardless of the prefix, making it easy to track a specific user and their use of the Internet.[1]

***IPv6 Address Spoofing (MAC Address Spoofing) Vulnerability -*** Because IPv6 address depends on MAC address which in a sense the MAC address is a computer's true name on a LAN.[8] Person might want to change the MAC address of a NIC for many reasons, maybe To get past MAC address filtering on a router, Sniffing other connections on the network, to keep their burned in MAC address out of IDS and security logs or to pull off a denial of service attack.[4] Unfortunately, this is privacy risk, because anyone who has your MAC address also has your IP address.[3]

***Large address space -*** Port scanning technique allows “black-hats” to listen to specific services (ports) that could be associated to well-known vulnerabilities. [11]

***Multiple address vulnerability -***As IPV6 assigns multiple address to an interface which challenges the filtering rules in the firewalls access control lists,[1] a firewall will need to learn all the addresses dynamically.[8]

***Multicast Security vulnerability*** - IPV6 uses multicast for neighbor discovery, Dynamic Host Configuration Protocol and traditional multimedia applications.[7] If an attacker could send traffic to these multicast groups and all the systems that are part of these groups respond, that would give the attacker information that could be used for further attacks.[11]

***Extension Header Vulnerability*** - Because the protocol specifications have not constrained the usage of extension headers, they could potentially cause problems if used maliciously.[6]

***Fragmentation Security Vulnerability*** - In IPv6, fragmentation is never performed by the intermediary routers but by the end nodes themselves and This process can be used by attackers to either hide their attacks or to attack a node.[3][7]

**Security Improvements Over IPv4**

***Makes Port Scanning Harder***

When they start, attackers usually employ port scanning as a reconnaissance technique to gather as much information as possible about a victim’s network.[6] It is estimated that the entire IPv4 based Internet can be scanned in about 10 hours with enough bandwidth [2], given that IPv4 addresses are only 32 bits wide.[1] IPv6 dramatically increases this limit by expanding the number of bits in address fields to 128 bits.[8] By itself, such a massive address space creates a significant barrier for attackers wanting to conduct comprehensive port scanning.[10]

However, it should be noted that the port scanning reconnaissance technique used in IPv6 is basically the same as in IPv4, apart from the larger IP address space.[7] Therefore, current best practices used with IPv4, such as filtering internal-use IPv6 addresses in border routers, and filtering un-used services at the firewall, should be continued in IPv6 networks.[2]

***Cryptographically Generated Address (CGA)***

In IPv6, it is possible to bind a public signature key to an IPv6 address. The resulting IPv6 address is called a Cryptographically Generated Address (CGA)[1]. This provides additional security protection for the IPv6 neighborhood router discovery mechanism, and allows the user to provide a "proof of ownership" for a particular IPv6 address. This is a key differentiator from IPv4, as it is impossible to retrofit this functionality to IPv4 with the current 32-bit address space constraint. [7]

CGA offers three main advantages:
1. It makes spoofing attacks against, and stealing of, IPv6 addresses much harder.
2. It allows for messages signed with the owner's private key.
3. It does not require any upgrade or modification to overall network infrastructure. [1]

***Replacing ARP by Neighbor Discovery (ND) Protocol***

In the IPv4 protocol, a layer two (L2) address is not statically bound to a layer three (L3) IP address. Therefore, it can run on top of any L2 media without making significant change to the protocol. Connection between L2 and L3 addresses is established with a protocol named Address Resolution Protocol (ARP), which dynamically establishes mapping between L2 and L3 addresses on the local network segment.[3][10] ARP has its own security vulnerabilities (such as ARP Spoofing).[7] In the IPv6 protocol, there is no need for ARP because the interface identifier (ID) portion of L3 IPv6 address is directly derived from a device-specific L2 address (MAC Address).[2] The L3 IPv6 address, together with its locally derived interface ID portion, is then used at the global level across the whole IPv6 network. As a result, the security issues related to ARP no longer apply to IPv6. A new protocol called Neighbor Discovery (ND) Protocol for IPv6 is defined in RFC 4861[1] as a replacement to ARP.



## 3 IP ADDRESSING STRUCTURE

The IP addressing structure defines the architecture of a network. A well-planned addressing structure will reduce potential risks associated with new features provided by IPv6.[3]
The following areas should be considered when designing an IPv6 network.

**Numbering plan and hierarchical addressing**

The numbering plan describes how the organization segregates its IPv6 allocation, for example, if an organization is granted with a 16 subnet bits (/48) address block, this will allow to support 65,000 subnets. A good numbering plan can simplify access control lists and firewall rules in security operations, and identify ownership of sites, links and interfaces easily. Organizations should carefully plan and create a site hierarchy by consider subnet methods as follows:

- Sequentially numbering subnets
- VLAN number
- IPv4 subnet number
- Physical location of network
- Functional unit of an organization (Accounts, Operation, etc) [1][10][11]

**Unauthorized IPv6 Clients**

IPv6 support is available for most modern operating systems or equipment; it can be easy and sometime unnoticeable to user where the IPv6 protocol is enabled. Due to the extended capabilities of IPv6, as well as the possibility of an IPv6 host having a number of global IPv6 addresses, it potentially provides an environment that make network level access easier for attacker if the access controls are not properly deployed. To reduce the risk, the following measures could be considered:

- Locate and disable any IPv6 enabled equipment
- Detect and block IPv6 or IPv6 tunnel traffic at network perimeter
- Include IPv6 usage policies in the organization's security plan [3][8]

**Common Attacks in Both IPv4 and IPv6**

IPv6 cannot solve all security problems. Basically it cannot prevent attacks on layers above the network layer in the network protocol stack. Possible attacks that IPv6 cannot address include:

**Application layer attacks:** Attacks performed at the application layer (OSI Layer 7) such as buffer overflow, viruses and malicious codes, web application attacks, and so on. [7] Brute-force attacks and password guessing attacks on authentication modules.

**Rogue devices:** Devices introduced into the network that is not authorized. A device may be a single PC, but it could be a switch, router, DNS server, DHCP server or even a wireless access point. [6]

**Denial of Service:** The problem of denial of service attacks is still present with IPv6.

Attacks using social networking techniques such as email spamming, phishing, etc

- Due to export laws, the strength of the encryption algorithms to be used to ensure global Inter-operability is limited.
- IPSec relies on a public-key infrastructure (PKI) that has not yet been fully standardized.
- There is some additional work needed in the IKE area and in improving protection against Denial of Service/Flooding attacks.[6]

## 4 IPv6 Transition

Transitioning tools allow IPv4 applications to connect to IPv6 services, and IPv6 applications to connect to IPv4 services. However, attackers might exploit this if the security issues have not been fully addressed.

There are a variety of IPv6 transition technologies, such as 6to4 (defined in RFC 3056[9]), Simple Internet Transition [3] (SIT) tunnels, and IPv6 over UDP (such as Teredo[9]). IPv6 traffic can enter networks via these methods while administrators are not aware that networks are vulnerable to IPv6 exploits. In addition, many firewalls permit UDP traffic, allowing IPv6 over UDP to get through firewalls without the knowledge of administrators. Attackers might also use 6to4 tunnels to evade intrusion detection or prevention systems. Some firewall products are only capable of filtering IPv4 traffic and not IPv6 traffic. Attackers can exploit this loophole and hence compromise the network by using IPv6 packets. [1][7]

**Migration issue**

There are number of issues to be considered before migrating from IPV4 to IPV6, these include: **Infrastructure** -The TCP/IP suite must be redesigned to support the new address format. e.g. the DNS has defined AAAA resource record for IPv6 (128 bit) but it has defined A resource record for IPv4 (32 bit).[1]

**Tunneling**- Without changing the applications, IPv6 can be implemented in an existing network by using IPv6 over IPv4 tunneling for connecting the IPv4 nodes to the backbone network. But tunneling has very less throughput.[1]

**Financial**- Migrating from IPv4 to IPv6 means, purchasing new network devices (which supports IPv6) such as switches, routers etc. which is a kind of additional investment.[3]

**Security**- The IPv6 is not used in wide scale till now and it is not tested properly. So no one is very sure about the security level of IPv6. [2]

## 5 BEST PRACTICES

Below are some best practices for reference in building and maintaining secure IPv6 networks:
- Use standard, non-obvious static addresses for critical systems;
- Ensure adequate filtering capabilities for IPv6;
- Filter internal-use IPv6 addresses at border routers;
- Block all IPv6 traffic on IPv4-only networks;
- Filter unnecessary services at the firewall;
- Develop a granular ICMPv6 filtering policy and filter all unnecessary ICMP message types;
- Maintain host and application security with a consistent security policy for both IPv4 and IPv6;
- Use IPSec to authenticate and provide confidentiality to assets;
- Document the procedures for last-hop trace back; and
- Pay close attention to the security aspects of transition mechanisms. [1][2][6][10]



## References

[1] A., M. and Sameeha,, A. (2012). Look at IPV6 Security advantages over IPV4. *Network and Complex Systems*, [online] 2(4). Available at: http://www.iiste.org/Journals/index.php/NCS/article/view/2593/2608 [Accessed 1st Oct. 2020].

[2] Ali Saihood, A. (2013). Security Features In Ipv6. *International Journal of Scientific Research*, [online] 04(01). Available at: http://www.ijscr.com/article/v04i2013/I1V4%20(4).pdf [Accessed 4 Oct. 2020].

[3] Dawood, H. (2012). IPV6 Security Vulnerabilities. *International Journal of Information Security Science*, [online] 1(4). Available at: http://www.ijiss.org/ijiss/index.php/ijiss/article/view/16/100-105 [Accessed 13 Sep. 2020].

[4] Dey, S. and N., S. (2014). Issues in IPV4 to IPV6 Migration. *International Journal of Computer Applications in Engineering Science(IJCAES)*, [online] 1(1). Available at: http://www.caesjournals.org/uploads/IJCAES-CSE-2011-19.pdf [Accessed 13 Oct. 2014].

[5] Hamarsheh, A. and Goossens, M. (2011). Exploiting Local IPv4-only Access Networks to Deliver IPv6 Service to End-users. *INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS*, [online] 5(3). Available at: http://www.universitypress.org.uk/journals/cc/20-795.pdf [Accessed 25 Sept. 2020].

[6] Kumar Tripathi, A. and Srivastava,Harish Pal, A. (2014). Security Issues in Mobile IPv6. *International Journal of Computer Applications*. [online] Available at: http://research.ijcaonline.org/dristi/number1/dristi1004.pdf [Accessed 5th Oct. 2020].

[7] Narayanan,, A., Khaja Mohideen,, M. and Raja, M. (2012). IPv6 Tunneling Over IPV4. *International Journal of Computer Science Issues*, [online] 9(2). Available at: http://ijcsi.org/papers/IJCSI-9-2-2-599-604.pdf [Accessed 15 Aug. 2020].

[8] Nizar Abu Ali,, A. (2012). Comparison study between IPV4 & IPV6. *International Journal of Computer Science Issues*, [online] 9(3). Available at: http://ijcsi.org/papers/IJCSI-9-3-1-314-317.pdf [Accessed 20 Sept. 2020].

[9] RFC 1884 IP Version 6 Addressing Architecture. Category: Standards Track. (1995). [online] Available at: http://tools.ietf.org/pdf/rfc1884.pdf [Accessed 25 Sept. 2020].

[10] Wang, X. and Mu, Y. (2012). Asecure IPv6 address configuration scheme for aMANET. *Wiley Online Library*. [online] Available at: http://www.readcube.com/articles/10.1002/sec.611? [Accessed 1st Oct. 2020].

[11] Wang, X., Cheng, H. and Yao, Y. (2014). Mobility support for IPv6-based VANET. *International Journal of Parallel, Emergent and Distributed Systems*. [online] Available at: http://www.tandfonline.com/doi/abs/10.1080/17445760.2014.920841 [Accessed 3rd Oct. 2020].