Journal of Advanced Computer Science & Technology, *6 (1) (2017) 1-12*

Journal of Advanced Computer Science & Technology

Website: www.sciencepubco.com/index.php/JACST
doi: 10.14419/jacst.v6i1.6714
Research paper

The magic of internet protocol

Khaldoun Batiha

Business Networking &Systems Management, Philadelphia University, Jordan
E-mail: kh_batiha&Philadelphia.edu.jo

Abstract

As the developing use of web and intranet keep on expanding colossally, the issue to suit more clients and gadgets has been risen. Subsequently, a location range must be required to oblige the hurry. Sadly, IPv4 address region and alternatives are insufficient to meet this new necessity. A fresh out of the box new Protocol is expected to satisfy the developing interest. IPv6 is the best response to the above issues. We should have an early on study on IPv6 convention. IPv6 convention offers verity of advantages that incorporates a more extensive location region and upgraded choices and changes that are not beforehand be found in the IPv4. IPv6 in contrast with IPv4 have a wide address range, simple documentations for representation of a location, enhanced administrations and alternatives, upgraded header, propelled highlights, new choices and bolster, auto setup highlight, new convention bolster, Network Security, Virus and Worms Security, Support for different Operating frameworks and stage including Microsoft windows, Linux and MAC.

Keywords: *Protocol; Tunneling; Network-Topology; Packet; Address Consumption; Address Pool; IPV6 SERVICES; Ipv6 Prefix Representation; Ipv6 Header; Attacks.*

1. Introduction

This paper is not only a comparison between the options and advancements of IPv6 protocol and IPv4 protocol but also describes that why this protocol, we would like to set-apart from the net before it actually capable of being accomplished. The paper not only describe the substantiation of the options of IPv6 that are not available for IPv4 but also project the very importance of IPv6 and propose a plan that will lead to the proper implementation of this protocol in the web to achieve new targets, which were previously not attainable with IPv4.

In conjunction with the above, it also discuss the victimization of IPv4 due to depletion of unapportion IP Address within the net. This victimization is mentioned in two different studies held in two different times. The outcome of both studies regarding the unallocated address pool predicts that when it will exhaust, IPv4 addresses do not remain accessible. However the problem can be fairly solved forever with the implementation of IPv6 protocol. By implementing IPv6 protocol, we ought not to improve or jump to a different protocol in the future as it might be used up of unallocated address pool of IPv6.

We also discuss here that how we can implement the advancements of IPv6 protocol. We will also discuss the topics including Auto Configuration, Twin Stack System and Tunneling. We will also try to find out that would it be economical to implement this new protocol or can we implement it into the existing infrastructure.

2. Context

Internet Protocol Address or Simply IP is a protocol exists in Network-Layer which practices to expel the Datagram i.e. blocks of knowledge, which encapsulates data from the higher layers of the network and aims to delivered the data blocks to its destination. Scientific headers are attached to the transport layer (A higher Layer) to form the encapsulation. In data communication over net, the datagram could be altered before reaching its destination and can be lost, delayed or duplicated. These encapsulation of datagrams helps to avoid any such circumstances [1] [2].

IP is responsible for addressing network and hosts in the Network-Topology. IPv4 is most widely used type of Internet Protocol that consists of a 32-bit long address. This 32 bit data is divided into four memory units. These memory units are also known as octets. Each unit consists of 0-255 Decimal range of memory. The all four unit represents the network half and host with scientific header (i.e. network address). The representation is also known as dotted decimal notation and looks like 192.168.1.1 [1].

IPv4 address is divided into 5 different classes. This division in classes is also known as classful network architecture mode of Internet Protocol. There are 5 different classes in classful addressing mode.

Class A: Ranges from 0-127 (Unit Octet)
Class B: Ranges from 128-191 (Unit Octet)
Class C: Ranges from 192-233 (Unit Octet)
Class D: Ranges from 224-239 (Unit Octet)
Class E: Ranges from 240-254 (Unit Octet)

Class A, B and C represents the number of hosts for unicast addresses, Class D shows multicast network and Class E has been reserved for future or for any experimental mode. In class A, first octet shows network half and remaining 3 represents host half. Primary two represents for network half and remaining two shows host half in class B. In Class C, the only last octet is used for host half and all first three octets are for network half [15].

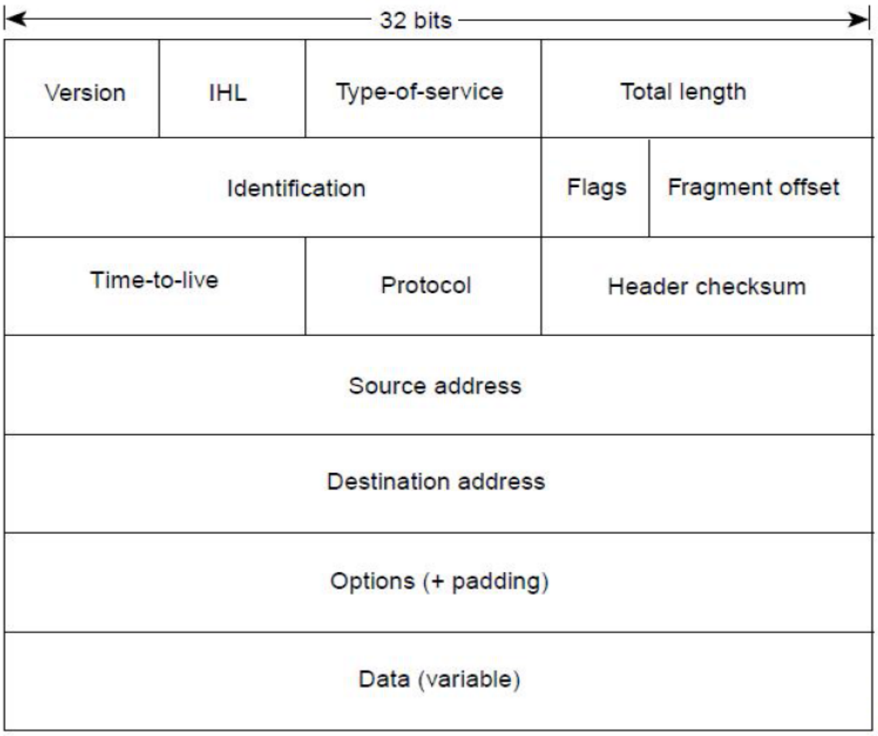

Fig. 1: Fourteen Fields Comprise an IP Packet [2].

Let's discuss the IP packet field [2]:
Version: Version represents the Internet Protocol Version.
IP Header-Length (IHL): The IHL shows the length of knowledge blocks (i.e. Datagram) in 32-bit.
Type-of-service: Indicates the varied level of importance of assigned Datagram which would be handled in an Upper Layer Protocol.
Total Length: It shows the length of information, header and IP packets. The total length specifies in bytes.
Identification: the datagram segments can be identified by this field. It helps to identify the datagram with a whole number.
Flags: The flags represent the fragmentation management and consist of 3-bit field. The 3-bit field consists of one higher order and two lower order bits. The higher order bit is don't care bit whereas middle order bit specifies the position of the last fragmented packets. The lower order flag bit indicates the frequency of the fragmented packets.
Fragment Offset: The first datagram is constructed by the destination side or receiver with the help of fragment offset. It indicated the relative start-position of fragment's information with in the original data blocks.
Time-To-Live: It refers to a regularly decremented counter during datagram reconstruction, down to zero. At zero the datagram is cast aside. It prevents the process to loop endlessly.
Protocol: After the completion of Internet Protocol processing, Upper Layer protocol receives incoming packets.
Header Checksum: Checks the header of IP.
Source Address: Indicates the sender address.
Destination Address: As name implies, it indicates the receiving end address.

3. IPV4 address area accessible

As we discussed earlier that in this paper we will study the two main studies regarding the prediction of exhaustion of IPv4 address area accessible.

3.1. Initial study

3.1.1. IPv4 addresses

As we know that IPv4 area consists of 32-bit field. This 32-bit field makes four 0-255 decimal value octets. There are varieties of address block areas that are reserved for special uses, they are 35.078 address blocks area unit made up of sixteen /8 blocks earmarked for particular usage in class D protocol. Sixteen (/8) blocks reserved future usage and 1/8 block (0.0.0.0/8) for native recognition. One /8 block embarked for loop back (127.0.0.0/8), and a /8 block earmarked for personal usage (10.0.0.0/8).
There are also few small size address blocks that are earmarked for variety of special purposes. As shown in figure1unassigned addresses that are controlled and managed by The Internet Assigned Numbers Authority (IANA) and approachable publically are sixteen /8 blocks whereas the assigned addresses to The Regional web Registries (RIRs) is 204.922 blocks [3].

3.1.2. Distribution of IPv4 address area unit

The Internet Assigned Numbers Authority IANA manages unallocated class A, B and C address area i.e. unicast address area. In context with the agreement between IANA and The Regional web Registries (RIRs), IANA then passes this address area to The Regional Web Registries. The address area unit then to be passed to the Internet Service Providers (ISPs) and Web Registries. The function of IANA is to exclusively allocate the unit of /8 address blocks under the agreement with RIRs and hence it does not responsible for the end-user / ISP address allocation [3].

3.1.3. The address consumption model

The full model of address consumption is constituted by aggregating many parts. Let's see the two main elements in the formation of address consumption model.
First Element: It shows the span of the publicized address.
Second Element: It projects the unadvertised address span.
These two elements are together called the Whole Address Demand.
The regional web registries is extrinsic to cater the whole address demand with the demands of unallocated pool by IANA so that it transforms the current model to the general address consumption level model as in Fig.3.[3]

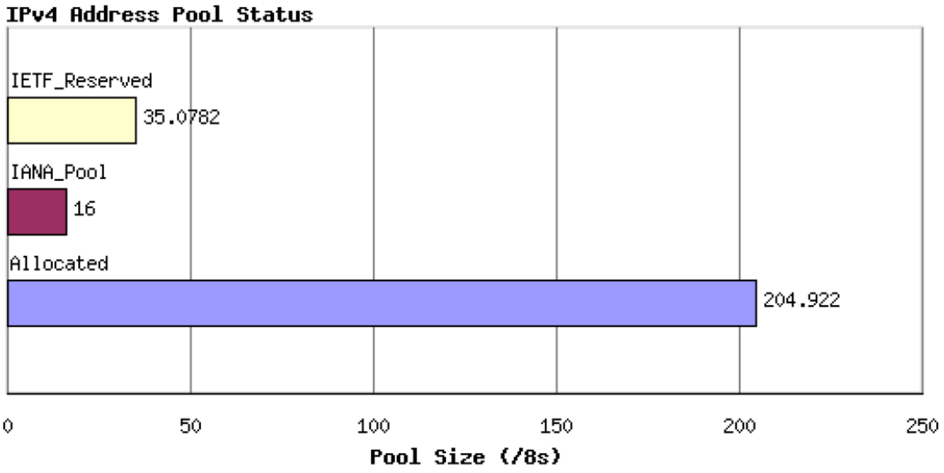

Fig. 2: [3] Pool Size.

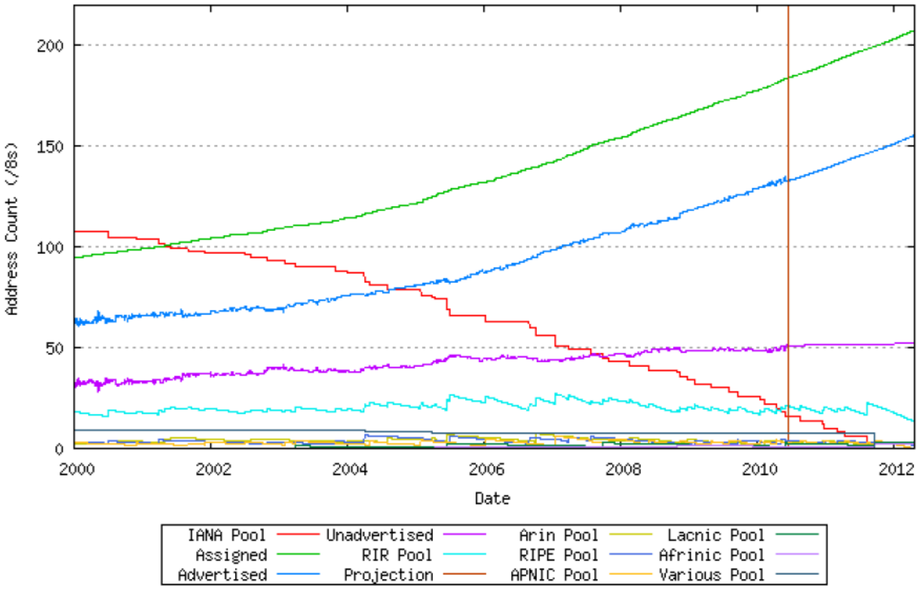

Fig. 3: Overall Address Consumption Model.

The date of exhaustion of IPv4 Unallocated address pool is to be foreseen as 17th April 2012. In addition to that this model also predicts the prediction of IANA unallocated address pool and the predicted date is 9th of August 2011 [3].

3.2. Second study

3.2.1. Address utilization of internet protocol IPv4

The Internet Engineering Task Force has reserved the address area of 20.09 of 256/8 network blocks or to use in multicast class 16 /8 blocks area unit has been reserved, close to 86 of whole IPv4 or 220 /8 blocks address accessible area for general purpose usage.

This address area allocation has been reserved till March 2005 which covers 146 /8 address blocks equivalent to some 66 of useable area. It also feat Seventy Four /8 blocks among the unallocated address pool, handled by Internet Assigned Numbers Authority i.e. IANA.

Therefore our method through the available Address Area comprises the tendency to area 2/3 unit area.

Address area model demand can be now derived by examining the continuous expansion of the global web's routing system and that is why we are capable now to make some probationary prediction to the duration of services of IPv4 address area.

The address consumption frequency has been increased over the time. On average, 4 /8 address blocks consumption has been upraised to 6 /8 blocks from 2002 to 2005. In other words, the remaining 74 /8 blocks spans till 2017 and that is a short time period.

See (Fig.4).If you foretell the model in another way, it is clear that with the continue expansion of internet over time, the frequency of increasing the address consumption is 5 /8 address block each year. This model of gradually raising the address consumption will surely exhaust the accessible address area till 2012. This is certainly a very short period of time [4].

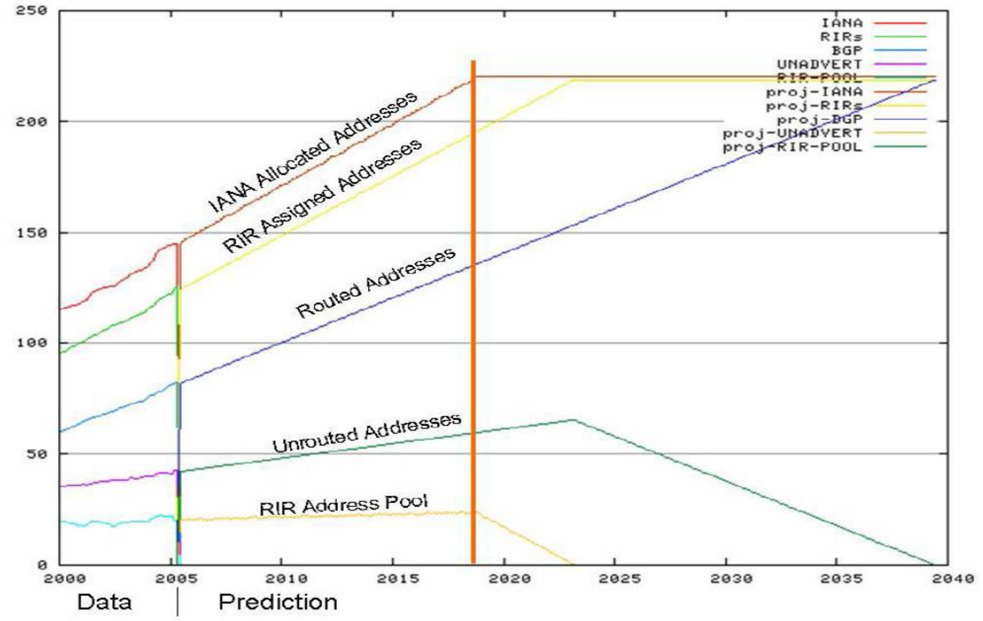

Fig. 4: Address Blocks Would.

4. IPV6 services and options

Internet Engineering Task Force (IETF) has outlined the Internet Protocol Version 6 (IPv6 Protocol) in the publication with the online customary description, RFC 2460, in the year 1998. IPv6 is an Online Protocol Layer for (PSN) Packet Switching Networks. This online protocol means to replace the pre dominant but continuously exhausted Internet Protocol Version 4 i.e. IPv4.

This Version 6 Internet Protocol collectively implements two features that change the following.

Stateless address Auto Configuration: It changes the aspect of address assignment.

Prefix and Router Announcements: It changes Network Renumbering.

The host symbol portion of an address has been up scale to 64-bits to make the process automatic and easier to make the Host Symbol from the Media Access Control Address or MAC Address and this has become the basics of standardization of Subnet of Internet Protocol IPv6 [6].

4.1. IPv6 address

The first main differentiation between IPv4 Vs IPv6 is that the Internet Protocol Address Area Unit of IPv4 is of 32 bits but the same parameter has been upscale to 128 bits in IPv6. This increased size of Internet Protocol Address area unit to 128 bits also has some drawbacks. The worth mentioned here is the overhead of victimization of 128 bits for every Supply & Destination address is far greater than the victimization of 32 bits in IPv4 in a datagram header. The reason for such victimization size is flexibility [9].

4.1.1. Internet protocol address ipv6 prefix representation& address-notation

As IPv4 address area unit comprises of 32-bits, it is easy to represent the IPv4 with the North American notation standards and that is why the IPv4 uses dotted mathematical notations. The case is different when it comes to IPv6 Protocol. As the size is huge i.e. 128-bits, it is impractical to adopt the same dotted mathematical notation.

Example: The IPv6 address looks like the following if we follow the same methodology as we use in IPv4; 128.91.45.157.220.40.0.0.0.0.252.87.212.200.31.255 [9].

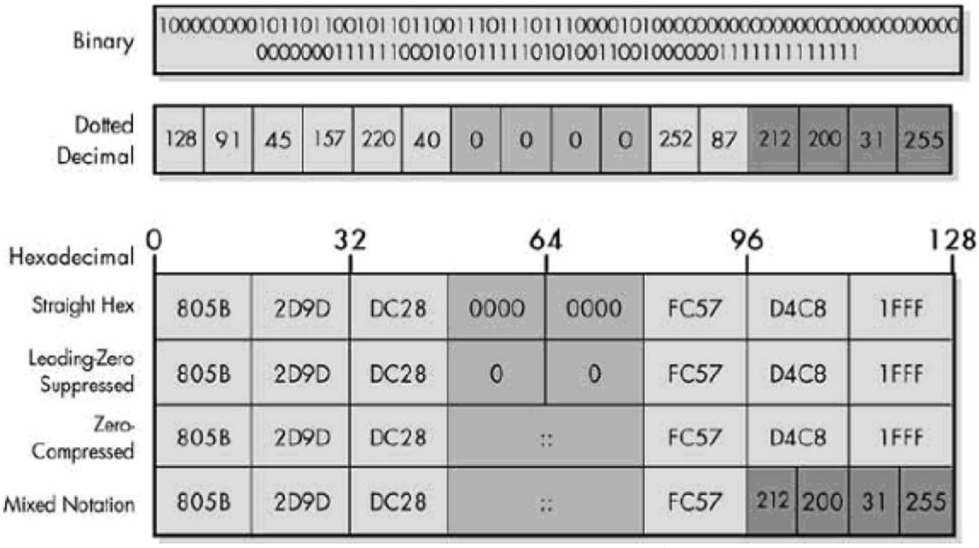

Fig. 5: Binary Y, Decimal and Hexadecimal Representation of the IPv6 Addresses.

4.1.2. IPv6 address positional representation system notation

IPv6 uses Positional System Notation to represent the Network Protocol Address which expresses representation in replacement of Decimal to create addresses shorter than Decimal. There is couple of advantages of Positional Notation System. First, it is possible to represent an address in fewer characters. Second is that the conversion of Positional Notation to Binary and Binary to Positional is much easier and quick to that of Binary to Decimal and Decimal to Binary.

The method has some disadvantage too. The prominent demerit of this system is that individuals face troubles when they come across the positional notation and find hard to work with as they are not use to that. IPv6 addresses area unit is also known as Colon Hex Decimal Notation. It is because that it comprises with 8Sixteen bit words positioned by colons.

The Colon Hex Decimal Notation of IPv6 looks like the following;

805A:2D9D: DC28:0000:0000:FC57:D4C8:1FFC

The above notation can be rewritten by following the rule that the leading zeros can be suppressed in order to shorten the size of the notation. By suppressing the leading zeros, the above notation can be re written as;

805A: 2D9D: DC28: 0:0: FC57: D4C8: 1FFC

In addition to above, there is another way to more shorten some of the IPv4 addresses. The technique is known as Zero Compression. In Zero Compression tactic, an string of continuous zeros in the address is substituted by Double-Colons.

Example:

FF10:4501:0:0:0:0:0:31

The above notation can be shortened by zero compression technique and the final notation will look like this; FF10:4501:: 31

There is another alternative to the above Notation System for IPv6 and i.e. Mixed Notation. In Mixed Notation, the address of IPv4 can be embedded into the Colon Hex Decimal Notation. The primary 96-bits remain as in the basic Colon Hex Decimal Notation and the remaining 32-bits are replaced by the Dotted Decimal Notation, which is used in IPv4.

Example:

This Colon Hex Decimal 805A:2D9D:DC28:0:0:FC58:D4C8:1FFF can be represented in Mixed-Notation as 805A:2D9D: DC28:: FC58:212.200.31.255 [9].

4.1.3. IPv6 address prefix length representation

The address area of IPv6 is mainly divided into the diversified Network ID bits along with different kinds of Host ID bits.

Prefix: The network symbol is called the Prefix.

Prefix Length: The range of bits in network symbol is called Prefix Length.

The prefix is defined at the end of IP address by adding a “Slash”. Hence the range after the Slash refers to Prefix Length. To understand it further let’s assumes the following sample Network Address.

805B:2D9D: DC28:: FC57:D4C8: 1FFF

For instance the initial 48 bits are used for Network ID i.e. Prefix, the Network Address can be represented like805B:2D9D: DC28:: FC57: D4C8:1FFF / 48

In IPv4, the Prefix there are represented by Dotted Decimal Notation and known as Subnet Mask. In contrast to IPv4, IPv6 does not use the Subnet Mask but instead it completely depends on Prefix Length [9].

4.1.4. The equivalent of IPv4 address in IPv6

Table1 Illustrate the IPv6 equivalent of IPv4 addresses and address ideas.

5. IPv6 header

5.1. IPv6 header

5.1.1. The format of ipv6 header

The format of IPv6 Header comprises with a new arrangement that is created to accommodate the Header-Overhead bits to a lower limit. It moves non-essential fields

To extension header that are located once in IPv6 Header.

The extension header of IPv6 is also efficiently processes at intermediate routers [8].

Table 1: IPv4 Addressing Concepts and Their IPv6 Equivalents [8].

IPv4 Address	IPv6 Address
Internet address classes	Not applicable in IPv6
Multicast addresses (224.0.0.0 /4)	IPv6 multicast addresses (FF00 ::/8)
Broadcast addresses	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is::1
Public IP addresses	Global unicast addresses
Private IP addresses (10. 0 .0 .0/8, 172. 16. 0.0/12, and 192.168 .0. 0/16)	Site-local addresses (FEC0:: /10)
Auto configured addresses (169.254.0.0/16)	Link-local addresses (FE80::/ 64)
Text representation Dotted decimal notation	Text representation: Colon hexadecimal format with suppression of leading zeros and zero compression. IPv4-compatible addresses are expressed in dotted decimal notation
Network bits representation: Subnit mask on dotted decimal notation or prefix length	Network bits representation: Prefix length notation only
DNS name resolution: IPv4 host address (A) resource record	DNS name resolution: IPv6 host address (AAAA) resource record
DNS reverse resolution :IN-ADDR .ARPA domain	DNS reverse resolution: IP6 ARPA domain

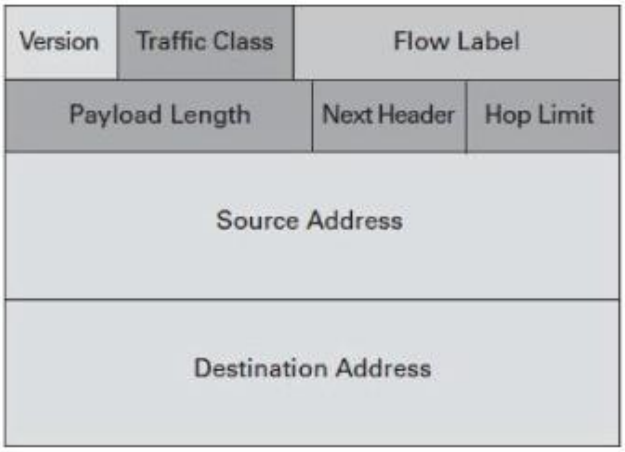

Fig. 6: IPv6 Header format

Version: Internet protocol version number.
Traffic Class: Type of service should be delivered to the packet and the Explicit Congestion Notification.
Flow Label (Prioritized Delivery): There are fields in the IPv6 Header that outline the Traffic. The field is a Traffic recognition field allowing to add a Flow-Label with in the Header of IPv6 that allow the routers to treat differently for packets in the flow, the stream of packets between the supply and destination node. Hence, the Traffic is known in IPv6 header and that make the prioritize delivery to be happened as soon as packet payload is ciphered. This is used by the supply node to label packet stream of to the like flow. The flow is unambiguously combined by the supply address and non-zero flow label. This is how a Twenty Four bit Flow Label inside the IPv6 Header is functioning for the improved accompaniment for prioritized delivery [8].
Payload Length: The payload length is a 16-bit field in the header that contains the length, in octets, of the data field following the IPv6 [7].
Next Header: The Eight Bit Next-Header field is placed in the primary portion of the Payload i.e. Information field of IPv6 and used to identify the type of header [7].

Hop Limit: This is an 8-bit field. The hop is decremented at every node that advancing a packet. When the hop counts Zero after decrements, that means the packet is now been cast-off [7].
Source Address: Packets originating node address is placed in the Source Address. The source address is a 128-bit supply Address field [7].
Destination Address: The destination field is also 128-bit long Address field that contains the receiving-end address [7].

5.1.2. Extension header

There are some optional fields in the header of IPv4 that are used for selected processing of data. Usually, we do not use these optional fields and these fields set the performance of routers down. IPv6 uses the Extension Header instead of these ex gratia field.
The majority of the data packets usually process easily and therefore the main IPv6 Header area unit is enough. But the packets which need extra data packets in the network layer will encapsulate this data in Extension Header, placed with IPv6 Header.
The issue with IPv4 extra field is that every intermediate router in the network has to be checked to identify its existence in the network and once identified, to process them. This surly degrade the performance while forwarding the IPv4 packets. In IPv6, the Delivery and Forwarding choices affects extension header only. The Extension Header is solely responsible to process every single intermediate router in the network. This speeds up the IPv6 Header Processing and enhancing the forwarding performance [7].

5.1.3. Comparing the ipv4 and ipv6 headers

Table 2: IPv4 Header Fields and Corresponding IPv6 Equivalents [8].

IPv4 Header Field	IPv6 Header Field
Version	Same field but with different version numbers.
Internet Header Length	Removed in IPv6. IPv6 does not include a Header Length field because the IPv6 header is always a fixed size of 40 bytes. Each extension header is either a fixed size or Indicates its own size
Type of Service	Replaced by the IPv6 Traffic Class field
Total Length	Replaced by the IPv6 Payload Length field, which only indicates the size of the payload
Identification Fragmentation Flags Fragment Offset	Removed in IPv6. Fragmentation Information is not included in the IPv6 header. It is contained in a Fragment extension header
Time to Live	Replaced by the IPv6 Hop Limit field
Protocol	Replaced by the 1Pv6 Next Header field
Header Checksum	Removed in IPv6. In IPv6, bit-level error detection for the entire IPv6 packet is performed by the Ink layer.
Source Address	The field is the same except that IPv6 addresses are 128 bits in length
Destination Address	The field is the same except that IPv6 addresses are 128 bits in length
Options	Removed in IPv6. IPv4 options are replaced by IPv6 extension headers

5.1.4. Network address translation support in ipv6

The NAT (Network Address Translation) is an operation that is a perfect example of how does a good idea at one time can have some unforeseen consequences. The idea behind NAT is that NAT device is used to translate the one globally known Real or Public IPv4 into the large number of Private IP addresses. This is used where a large number of private computers can share single public address to access internet or other services and this is its immediate benefit. The NAT interrupt and breaks the Protocols which is required for incoming connections to carry IP addresses. This operation hides the real IP of the Host Computer which makes the communication significantly complicated. This is one simple reason that IPv6 users speaks on the Dark Side of the NAT as typically there were a myth that NAT can also be used as Security feature anytime. This is a very important to look into thoughtfully that once work out on an IPv6 transition plan of action, as no one desires to loose NAT's comprehended benefits. IPv6 supports all the comprehended advantages of NAT area unit [5].

5.1.5. IPV6 auto configuration

One of the very useful features of IPv6 is that it supports node Plug and Play. It means that it offers Plug and Play Auto Configuration of node connected to IPv6 Network without any intervention of human.

This is advantageous in a Stateless or Server-less Network where the node has been automatically configured by sending a neighbor solicitation message (Neighbor Discover Protocol). The feature is achievable in addition to DHCPv6, the State-full-Address autoconfiguration that's just like IPv4 DHCP. But the Plug and Play Auto Configuration in IPv6 is an enhanced and much better version [5].

5.1.6. IPV6 quality of service (QoS)

As discussed earlier that IPv6 offers a Twenty bit field in the Header which is called Flow Label. The Flow Label is positioned in the header for employing Quality of Service. It allows to label the packets of constant flow at supply node and hence the better delivery priority.

IPv6 Quality of Service (QoS) is somehow the same as that of its IPv4 counterpart. It faces the same challenges as it follows in inherit model of IPv4. For the time being the presence of Flow Label does not vindicate the claim that IPv6 has a better Quality of Service [5].

5.1.7. IPV6 multicast

As name implies that multicast is the class facility that allows transmitting one packet to multiple destinations. IPv6 does not follow out the broadcast as in IPv4. In IPv4, a packet can be send to all hosts that linked up. IPv6 cause a packet to the host-link to multicast-cluster. It thus deficient the impression of IPv4 broadcasting addresses.

The other side of multicasting is that it works on one subnet but may not globally. This is because that most of the Network infrastructure presently do not have provision to route multicast packets.

IPv6 Multicast has some common options and protocols with IPv4 as well as has some improvements too. A corporation is employed a tiniest IPv6 International Routing Prefix once, special IPv6 Multicast teams to assign for the cross-domain / inner-domain application of multicast.

However in IPv4, it is even hard to implement even a single globally routable cross-domain multicast's group assignment for a corporation. In addition to new multicast solution, IPv6 also supports the Embedded Rendezvous Point (Embedded RP) or Source Specific Multicast (SSM) [5].

5.1.8. The component of multicast listener discovery

MLD or Multicast Listener Discovery is a component in IPv6 that is used by IPv6 to discover Multicast Listener on directly attached link. MLD is equivalent to IGMPv2 (Web Cluster Management Protocol) of IPv4.Both, MLD of IPv6 and IGMP of Ipv4 discover the Multicast addresses that have minimum one attender.

5.1.9. Neighbor discovery in ipv6

Neighbor Discovery also known as ND is a component in IPv6, comprises of content and processes to authenticate the neighboring nodes mutual relationship. Neighbor Discovery is the replacement of the ICMP Router Discovery in Internet Protocol Version 4 with the addition of improvements.

ND is employed by hosts:

- To detect neighboring routers.
- To detect addresses, address-prefixes& various configuration parameters.

ND is employed by routers:

- To advertise their existence, configuration of host's parameters, & on-link prefixes.
- To communicate to hosts of an improved next-hop address to forward packets for a selected destination.

ND is employed by nodes:

- To resolve the address of link-layer adjacent node to that an IPv6 packet is being advanced and ascertain once the link-layer address of an adjacent node has been modified.
- To ascertain that whether a neighbor continues to be accessible or not [8].

5.1.10. IPv6 MTU

IPv6 supports the link layer of 1280 bytes packet size. If the link-layer does not support 1280 bytes it should give a link-layer fragmentation and reconstruction.

For link-layers, which support a configurable MTU (Maximum Transmission Unit), it's advised that the design should be of an MTU of at least 1500 bytes (the LAN II encapsulation IPv6 MTU). The example of a ready to set maximum transmit unit is MRU i.e. the most Receive Unit of PPP (Point to Point Protocol).IPv6 also offers for Path MTU Discovery method victimization the Packet of ICMPv6, like IPv4, to huge message in "Path MTU Discovery."

With the Path MTU Discovery, IPv6 is able to transmit packets of sizes bigger than 1280 bytes. Payload of higher layer protocol will be fragmented by Supply host of IPv6 that area unit greater than the trail MTU by victimization the method and Fragment previously defined header. Usually the usage of fragmentation is discouraged as a node of IPv6 must be able to assemble a fragmented-packet of minimum 1500 bytes [8].

5.1.11. Fragmentation

Payloads of Supply nodes are fragmented in IPv6. IPv6 reconstruct the data using fragment extension header by doing the fragmentation of the payload at supply node, if the path MTU or the link is smaller than the submitted payload by higher layer protocol [8].

5.1.12. IPv6 simplified process by routers

IPv6 simplifies the process of packet forwarding. The modification or you can say the simplification is made to the packet header by the routers which also do the process more economical.

- The packet header used in IPv6 is way easier and simplified than the packet header in IPv4, with often used fields to apart options; which results double the scale of Option-Less IPv6 header to that of Option-Less IPv4, though the address in IPv6 unit area is as large as multiple of four to that of IPv4.

- Host area unit of IPv6 is needed to do either of the following things.
- It perform PMTU Discovery
- It sends packets smaller than1280 octets which is the IPv6 minimum MTU size.
- It performs end-end fragmentation.
- IPv6 routers do not perform fragmentation.
- There is no checksum (The error detection technique) in the header of IPv6; instead each link layer assures the integrity protection and the next layer checksum i.e. TCP, UDP etc.
- After header field modification, IPv6 routers do not re-compute the confirmation. The router should not calculate the time a packet needs to stay in the queue and that is why the field i.e. Time-To-Live in IPv4 is converted in to the Hop Limit [5].

5.1.13. Quality of IPv6

IETF (Internet Engineering Task Force) Protocol has been standardized for both IPv6 an IPv4 and is known as MIP (Mobile IP). In MIP, the IP quality is usually substitutable. When to considering the possible scope of gearing up for Mobile IP, Example; 3GPP or 3GPP2 (Third Generation Partnership Project) is the standard for handheld devices, it is witnessed that there are chances of up sizing the unit area addressing of Mobile devices. Hence IPv6 needs a large address area for this type of configuration.

In addition, to Mobile IPv6 allows the extension header of IPv6 that unit area is integral to the protocol. That is why, IPv6 protocol integrates the feature of IP mobility as requires by RFC 1752 that permits the rendering of path in optical manner amongst the mobile nodes and communication peer and other feature like this.

The market is integrating new products support standardization protocol like NEMO (For Network Quality) and previously discusses MIPv6. New business models and new communities of interest is also rapidly being the part of the business. These new deployments make the quality to easily integrate and to have provision for various new devices like Wireless Radio, Video Calling, VoIP and other multimode features in new handsets. With the use of IP Multimedia Subsystem (IMS) along with the improved standards and features of IPv6 brands can now quickly introduce advance products in the market [5].

6. Difference between ipv4 and ipv6 [16]

Let’s find out the variation between IPv4 and IPv6 protocols.
IPv4: Source and Destination Unit Area is of 4 bytes long i.e. 32-bits long.
IPv6: Source and Destination Unit Area is of 16 bytes long i.e. 128-bits long.
IPv4: IPsec support is optional.
IPv6: IPsec support is mandatory.
IPv4: Do not identify the flow of packets for Quality of Services.
IPv6: Packet flow identification is there in the header by implementing Flow Label for Quality of Service handling by routers.
IPv4: Every router is responsible for fragmentation.
IPv6: Fragmentation is done by the host not by the routers.
IPv4: Uses confirmation in the header.
IPv6: Does not use the confirmation in the header.
IPv4: Main header includes ex gratia information.
IPv6: Extension header includes the optional information.
IPv4: IP address to the link layer address has been resolved by the ARP (Address Resolution Protocol) which uses Broadcast Creative Person Request Frame.
IPv6: Multicast solicitation Messages replaces the Broadcast Creative Person Request Frame.
IPv4: IGMP, also known as Web Cluster Management Protocol. Its functionality is to handle local Subnet Cluster Membership.
IPv6: There is not IGMP in IPv6 instead it uses MLD, Multicast Attender Discovery Message.
IPv4: ICMP Router Discovery is utilized to see the IPv4 address of the simplest default entrance and is optional.
IPv6:ICMPv6 Router Solicitation and Router advertisement messages are employed and is mandatory.
IPv4: Uses Broadcast Address Area Unit to transmit Traffic to nodes connected.
IPv6: Does not use Broadcast Address instead it uses a Link Local Scope Multicast Address.

IPv4: is designed by DHCP or Manually.
IPv6: Does not use DHCP or Manual design.
IPv4: Uses pointer (PTR) Resource Records within the IN-ADDR.ARPA DNS domain to map out host IP address.
IPv6: Uses pointer (PTR) Resource Records within the IP6.ARPA DNS domain to map out host IP address.
IPv4: Supports 576-Bytes, possible fragmented, Packet Size.
IPv6: Supports 1280-Bytes, un-fragmented, Packet Size.

7. ICMP (Internet Control Message Protocol)

ICMP or Internet Control Message Protocol is a Network layer protocol that accounts error and processing different packets back to supply node. As name indicates that Internet Control Message Protocol generate multiple useful messages like below.
ICMP Messages:

- Destination Un-reachable
- Source Quench
- Redirect
- Timestamp
- Timestamp Reply
- Time Exceeded
- Router Advertisement
- Router Solicitation
- Address Mask Request
- Address Mask Reply

One thing here is important to understand that if there is ICMP message that could not be delivered for any reason, ICMP will not re attempt. This is useful to avoid the continuous flood that could be generated by the ICMP messages [2].

7.1. A comparison of ICMPv4 & ICMPv6 error messages

Table 3 shows a list of ordinarily used ICMPv4 error messages &its Accompanying ICMPv6 equivalents.

Table 3: ICMPv4 Error Messages and Their Corresponding ICMPv6 Equivalents [8].

ICMPv4 Message	ICMPv6 Equivalent
Destination Unreachable-Network unreachable (Type 3, Code 1)	Destination Unreachable-No route to destination (Type 1, Code 0)
Destination Unreachable-Host unreachable (Type 3, Code 1)	Destination Unreachable-Address unreachable (Type 1, Code 3)
Destination Unreachable-Protocol unreachable (Type 3, Code 2)	Parameter Problem-Unrecognized Next Header field (Type 4, Code I)
Destination Unreachable-Port unreachable (Type 3, Code 3)	Destination Unreachable-Port unreachable (Type 1, Code 4)
Destination Unreachable-Fragmentation needed and OF set (Type 3, Code 4)	Packet Too Big (Type 2, Code 0)
Destination Unreachable-Communication with destination host administratively prohibited (Type 3, Code 10)	Destination Unreachable-Communication with destination administratively prohibited (Type 1, Code 1)
Time Exceeded-TTL expired in transit (Type 11, Code 0)	Time Exceeded-Hop Limit exceeded (Type 3, Code 0)
Time Exceeded-Fragmentation timer expired (Type 11, Code 1)	Time Exceeded-Fragmentation timer exceeded (Type 3, Code 1)
Parameter Problem (Type 12, Code 0)	Parameter Problem (Type 4, Code 0 or Code 2)
Source Quench (Type 4, Code 0)	This message is not present in IPv6.
Redirect (Type 5, Code 0)	Neighbor Discovery Redirect message (Type 137, Code 0). For more information, see "Neighbor Discovery."

8. Package support in ipv6

IPv6 has an excellent package support. That means it supports almost all the major Operating Systems and Platforms available in the market. A patch, command or configuration setting is required to upgrade the support.

8.1. Microsoft windows

Microsoft Windows XP, Windows 2003 Server, Windows 7 and Windows 8 are all the supporting Operating Systems for IPv6. In Windows XP, all it needs a command “ipv6 install” to alter the LAN interfaces. A reboot is required after the command execution which surely interrupts current running connections and programs.
Microsoft Windows 2000 also support IPv6. An update is required to Microsoft Windows 2003 Service Pack1 or a newer version of service Pack is needed to install. The current update does not support Domain Name Server on IPv6 but support IPv6 addresses from Domain Name Server of Ipv4. This version supports full Ipv6 applications and stack [10].

8.2. Linux / UNIX

An easy activation and configuration is needed on many of the Linux / Unix Operating System Distribution to unlock the benefits of IPv6. A good thing is that the activation does not required the system reboot and hence there is no interruption for the programs and services. The new versions of these operating systems Kernel have IPv6 Firewall support.
Mandrake or Red Hat systems, which are the RPM-based distributions, are also required an additional Configuration Variable; “NETWORKING_IPv6=Yes” to the Internet Configuration File; “IPv6INIT=Yes” to the case-by-case interface file that cause the reboot of the network system. You can also manually start the IPv6 system instead a Network System. You can employ a UNIX Operating System as a router. In this case, when the UNIX is used for routing, "IPV6FORWARDING=yes” should be appended to the World Wide Web configuration file. While using UNIX as a router, you must add one extra parameter in addition to the previous one and i.e. to use
"IPV6TO4INIT=yes" in the Configuration File for interfacing.
Free BSD, Net BSD, Open BSD and other recent BSD distribution support IPv6 and Ipv6 Tunneling. Aix, HP / UX supports fully for Internet Protocol Version 6 IPv6. Solaris and Solaris x 86 also support IPv6 in version 8 and above 8.Solaris systems required solely the generation of "hostname6." files to change IPv6 LAN interface [10].

8.3. Other operating systems

Apple platform also fully support IPv6. Apple’s Macintosh OSX and later supports IPv6. Cisco and RUGGEDCOM which are the two major router manufacturers support IPv6 and have the provision in their router management software package as well as OSPF and BGP. Point to Point Protocol also can be employed by IPv6. IPv6 can be tunneled, connected or transported VPNs (Virtual Private Network), Serial Links & UDP Tunnels. In short, it is clear that IPv6 support variety of Packages, Operating Systems, Routers and Platforms [10].

9. Dual stack

IPv6 adaptation may become limited with a hurdle that the perceived quality of IPv6 web can be effected by the fact that if IPv6 infrastructure is poorly managed. To properly utilization of IPv6, many of the O.S IP like IPv6-IPv4, to be deployed to communicate with one another.
IPv6 was introduced, it came with the essential migration techniques to cover every conceivable IPv4 upgrade case, but many of the migration techniques were rejected by the technology community, and now there are few practical approaches which are being used today.
One such practical approach or technique which is widely used by the community is known as Dual Stack. In this technique both IPv4 and IPv6 runs on the same time. Supply node, destination node and routers/switches run both protocols. Initially the IPv6 is prioritized to run until the performance of communication is compromised, after that it automatically switched to IPv4 Protocol [11].

10. Tunneling

To implement IPv6 network successfully, a technique i.e. tunneling is used. Tunneling is a technique in which an isolated host or a network enduring IPv4 infrastructure to hold IPv6 packets. When an IPv6 packet exploits IPv6 domain & gets into the IPv4 domain, the packets are transmitted through the network by encapsulation into IPv4 packet. After the encapsulated IPv4 packets reach at the destination, it then off the IPv4 header area unit from IPv6 and then it continue on to an IPv6 domain [12][6].

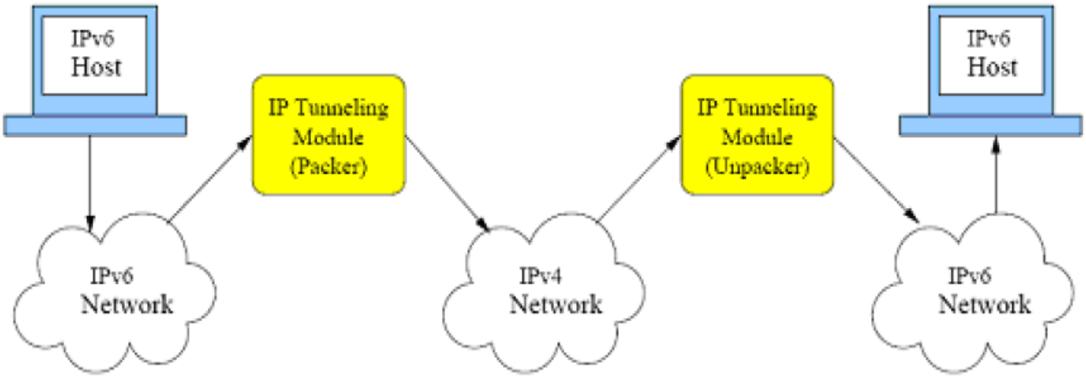

Fig. 7: Layout of Tunneling Modules between IPv6 and IPv4 Networks.

11. Security

Network Security is mandatory while designing any Network using any Protocol. When IPv6 was designed, Network security was taken into consideration during the planning phase and was integrated as a part of IPv6 design. Internet Protocol Security, also known as IPsec, was developed for IPv6. IPsec authenticates and encrypts IP packets during the communication. It also negotiates cryptographic keys during the session and authenticates the agents at the beginning of the session [13].

11.1. Security improvements in ipv6

Below are a few IPv6's up gradation to leverage higher network security.

11.1.1. Massive address area

Port-Scanning is the simplest and most widely used security technique today. It permits the "black-hats" to focus on to particular ports (services) that might be linked up to well-known insecurities. IPv4 segments are of category C. it means that 8-bits are used for host addressing. If someone wants to break-in in IPv4, it would scan IPv4 Subnet. If for example; it takes 1 sec to scan one host then it would need 4.25 minutes. But in IPv6, host area addressing consists of 64-bits. It means 584,942,417,355 years needed to scan ports at the speed of one host per second, which is impossible. So the massive Address Space available for the host addressing secure IPv6 Networks with ease [13].

11.1.2. IPSec

IPv4 has optional support of IPsec, Internet Protocol Security Protocol. As mentioned earlier that IPsec authenticates and encrypts IP packets during the communication. It also negotiates cryptographic keys, Encapsulating Security Payload (ESP),during the session and authenticates the agents Header (AH) at the beginning of the session.

ESP gives authentication, information integrity, and confidentiality and AH provides authentication and information integrity [13].

11.1.3. ND & Auto-Configuration of Address

NDP or Neighbor Discovery Protocol is IPv6 protocol that operates in the link layer of RFC 112. NDP is used for the following purpose.

- Address Auto Configuration for nodes
- Discovery of other nodes on network
- Determining the link addresses of other nodes
- Duplicate address spotting
- Finding available routers
- Finding available Domain Name servers
- Address prefix detection
- Maintaining reachability information about the paths to other active adjacent nodes [13].

11.2. Attacks

11.2.1. Reconnaissance

This is a hacking technique in which the hacker tries to explore the max amount as attainable of the target Network. The hacker uses many techniques and active strategies like scanning ports and data mining through internet or from public documents. There are two different considerations while the antagonist makes his strategy. One consideration IS for IPv4 and one is for IPv6 [14].

IPv4: There are number of consideration while he tries to break the Network Security. In IPv4, Ping Sweeps, Port Scanning and Vulnerability Scanning is widely known techniques.

IPv6: The considerations here are different from the one in IPv4.

1) The Port Scanning or Ping Sweep, due to its address area unit size is far harder to complete in a limited time in IPv6.
2) The other consideration for IPv6 is that the new Multicast addresses make the antagonist to search for set of various new key systems like NTP Server or Network Time Protocol, Routers and various other. It means the hacker can spot the key resources in IPv6 due to its support of new Multicast addresses to attack. Example: DHCP Server (FF05::3) or a Router (FF05::2) has a site particular address [14].

11.2.2. Access of unauthorized user

The set of host in the IP protocol stack is not limited. Attackers manipulate this fact to find out the property to upper-layer protocols and applications on Network devices and endpoint hosts. Let's see the IPv4 and IPv6 considerations. IPv4:IPv4 integrates Access Management Technology inside the system and at the end point of the Network. It means IPv4 have limited authorized access point.

The defending system uses ACLs, a network access control list, at the IP layer in order to permit only the approved host to send packets. Access Control List is integrated in the Networking devices like Firewalls and end nodes like Host Firewalls [14].

IPv6: The new addressing system is different from its IPv4 counterpart. It enables the ability of an adaptor in a node to have multiple IP address. Example: The multiple IPv6 addresses on the native subnet (link native - FE80:: /10), in an organization (site native – FC00::/16 or FD00::/16 unfinished social unit decision),on internet at massive scale (global unicast addresses – aggregates of prefix binary 001).

The Network security designer limits the access to the end nodes of IPv6 address and routing with the utilization of address ranges along with routing system [14].

11.2.3. Fragmentation & header manipulation

This is the class of hacking attack in which attacker tries to manipulate two IPv6 functions.

1) Attacker use fragmentation to invade the network security devices including NIDS or State-full Firewalls.
2) Attackers manipulate other headers to directly attack network infrastructure.

Let's see what to consider in IPv4 andIPv6.

IPv4: In order to bypass access control on devices such as Routers and Firewalls, fragmentation is used. Fragmentation conjointly has been customary modify attacks so as to bypass network security monitoring product like NIDS.

IPv6: One of the common strategies of attackers for fragmentation attacks is to overlap fragments to modify attacks from IPv4 Network Security devices [14].

11.2.4. Layer 3 spoofing

Layer 3 spoofing or IP Address Spoofing or Simply IP Spoofing is a technique in which attacker creates packets with the IP address which is forged and hence he conceal the source identity and impersonating another computing system.

IPv4: The layer 3 based IP Address Spoofing attacks are very common these days. They are so common that spoofing happens on daily basis. In Spoofing, attackers create spam, worm or virus attacks which are harder to find out.

There is a method of filtering to avoid Spoofing as specified in RFC 2827. The method is called Ingress Filtering, a technique to identify the packets that they are originate from the network and hence to avoid forged identity. Unfortunately, the Ingress Filtering is only enforced in the Network section of the address and not the Host part.

Therefore in a subnet of 24-bit 192.0.2.0/24, Ingress Filtering only allows identifying the Traffic origin from 192.0.3.0 and cannot stop spoofing to the entire host in 192.0.2.0/24 subnet associated to a broadcast domain.

IPv6: Layer 3 Spoofing in IPv6 is discouraged due to the fact that it has the collective nature of IPv6 Addresses globally. Hence in IPv6, RFC 2827 Ingress Filtering is integrated into the ISPs or Internet Service Providers. This strategy works as the ISPs are responsible to identify that at least their own customers are not involving in IP Spoofing [14].

11.2.5 Creative Person and DHCP Attacks:

This attack communicates the attacker to the compromised device or to be designed with incorrect network data like DNS server IP Addresses, and so on.

IPv4: A rogue DHCP server is not under the control of Network Administrator. Network devices such as Modem or a Router in a network are used by a common user intentionally or unintentionally to attack network like Man-in-the-Middle. In Man-in-the-Middle attack, the fact that DHCP server aims to reply the user request even before it validate DHCP server is used to compromise the Network security. DHCP messages are often spoofed that allow attacker to consume all accessible on server DHCP messages.

ARP Attack or ARP Spoofing is a technique in which hacker forge Address Resolution Protocol messages over local Area Network. In this way attacker links its MAC Address to the IP Address of an authorized computer on the network, IP-MAC binding.

IPv6: Unfortunately in IPv6, there is no inherent network security for DHCP Attacks. Dedicated DHCP servers don't seem to be common in IPv6 and don't seem to be even generally accessible in trendy server in operation systems.

It is an unfortunate that stateless auto-configuration messages are generally spoofed.ICMPv6, Neighbor Discovery, replaces the creative common in IPv6 [14].

11.2.6. Broadcast amplification attacks (SMURF)

Broadcast Amplification Attack or generally SMURF Attack is type of Denial-of-Service Attack in which massive number of ICMP packets (Internet Control Message Protocol) with the target user source IP is then IP Broadcast Address to the network. A number of devices will respond to this message. If the number of devices that respond to that message are fairly large then it dead-slow the speed of the victim's computer.

IPv4: This common attack attributes an easy mitigation methodology in IPv4 networks. There are two fixes.

1) Make a configuration to every single host and router to not be responsive on ICMP requests.
2) Make a configuration to discourage the routers not to forward packets to directed to broadcast addresses.

IPv6:IPv6 already set off the thought of an IP-directed broadcast from the protocol & specific language that derived to the protocol design to extenuate attacks. With regards to Broadcast Amplification Attacks (SMURF) attack, RFC 2463 states

"An ICMPv6 message shouldn't be generated as a response to a packet with an IPv6 multicast destination address, a link-layer multicast address, or a link-layer broadcast address"[14], (RFC 2463 section 2.2)

11.2.7. Routing attacks

In any network, attackers enforce routing attacks to redirect flow of traffic. Let's see the IPv4 and Ipv6 consideration regarding Routing Attacks.

IPv4: In IPv4, routing attacks in the network are often avoided by implementing cryptography for the authentication of the routing messages between the peers. The most widely used practice here is MD5. MD5, Message Digest Rule 5, is cryptographic technique which generates 128 bits or 16 bytes hash value or 32 bit hexadecimal number. MD5 uses that key and pre-share it between the routing peer to authenticate the data integrity.

IPv6: Border Gateway Protocol (BGP) or Distance-Vector Protocol was extended to hold IPv6 routing data in RFC 2545. The BGP allows network administrator to set rules for routing decisions and network path. As such, BGP continues to believe transmission control protocol MD5 for authentication.

The Intermediate System-to-Intermediate System (IS-IS) protocol was covered to support IPv6.The Intermediate System-to-Intermediate System determines the best routes for datagrams through packet-switched networks to exchange the information between the computers in a network.

Initially IS-IS is used to authenticate LSPs or Link-State Packets, However, the easy word authentication wasn't encrypted.

RFC 3567 include a crypto graphical Authentication, like Message Digest rule, to IS-IS, and can still be able to defend IPv6 traffic.

The authentication field of header unit area has been removed in Open shortest Path (OSPFv3). Interior gateway protocol or RIP Next-Generation (RIPng) has

Routing data Protocol Next-Generation (RIPng) has collectively removed the certification from the specification. Both RIPng and OSPF produce authentication and integrity of routing data exchange by believing in Encapsulating Security Payload (ESP), AH and Internet Security Protocol (IPsec).

The protocol like "The Generalized TTL Security Mechanism" is used to extra secure the IP networks. This security mechanism can be applied to the specific Protocols of IPv6 so that if the Hop-Limit field within the header is deployed to shield a protocol stack [14].

11.2.8. Viruses and worms

One of the most severe security vulnerabilities are of from Viruses, Worms, Trojans and Bots. These are the computer programs which are designed by the attackers to compromise the network security. Viruses, Worms, Trojans and Bots are all part of a software class known as Malware. Malware is a malicious code which is used to steal, destroy, interrupt or infect the data in a computer or a network.

IPv4: Virus and worm can together harm the host and network transport and can accumulate burden to mail servers and routers on a network.

IPv6: In IPv6, Viruses are mostly of email based. These viruses can infect data and interrupt communication. Below is the main difference in all 4 malware component.

- Virus: A malicious program that can replicate itself and need a host.
- Worm: A malicious program that can replicate itself and works independently.
- Trojan: A malicious program that a user can recognize as a legitimate program.

These malwares uses various styles to break and compromise the security of a network like a worm can be used to search the vulnerable hosts in the network by scanning.

Attacker decides that what type of malware and technique he should use for the specific attack. Example: SQL Slammer-Type worm is not efficient as it does not able to search the hosts to infect [14].

12. Conclusion

We have explained that how an IPv6 protocol is the solution to many of the issues which were predicted due to the enormous increase in the internet usage. We have also discussed the new options available with the IPv6 protocol which were not available in IPv4 or the features which were available in IPv4 but have been enhanced in IPv6.

Also we have shown variety of enhancement in IPv6 and how the enhanced feature is better than its previous version. The improvements include but not limited to packet header, addressing schema, security issues, QoS, packet fragmentation and ICMP error messages.

Besides advantages, we have also discussed the limitations of Internet Protocol Version 6 like some security enhancements and Victimization (to hold IPv6 packet and the way servers ought to influence IPv4 and IPv6 stack within the same time). We have also presented the solution to the limitations like we have discussed about IPv6 Tunneling over IPv4 and the dual stack system.

In a section above, a comparison between IPv4 and IPv6 has been explained. The comparison that includes address area, fragmentation, IPsec, QoS, IGMP, ICMP, DHCP, PTR etc. and at the end we have seen that there is no major security modification from IPv4 to IPv6.

References

[1] “The ABCs of IP (Internet Protocol)” Online: http://www.esmagazine.com/ES/Home/Files/PDFs/Contemporary-Controls.pdf, November 2006.

[2] Cisco, “Internetworking Technology Overview”, Chapter 30, Online: http://fab.cba.mit.edu/classes/MIT/961.04/people/neil/ip.pdf, June 1999.

[3] Geoff Huston, “IPv4 Address Report”, Online: http://www.potaroo.net/tools/ipv4/index.html, 15- June-2010.

[4] Geoff Huston APNIC, “IPv4 Address Utilization”, Online: http://www.potaroo.net/papers/2005- 03-ipv4.pdf, March 2005.

[5] Patrick Grossetete, Ciprian P. Popoviciu, Fred Wettling, Fred Wettling, "Global IPv6 Strategies: From Business Analysis to Operational Planning" Online: http://media.techtarget.com/searchNetworking/downloads/IPv4_or_IPv6.pdf, 1st Edition, chapter 2, pp. 18-53, May 15, 2008.

[6] “IPv6" From Wikipedia, Online: http://en.wikipedia.org/wiki/IPv6, 18 September 2010.

[7] "IPv6 Headers", Online: http://www.cu.ipv6tf.org/literatura/chap3.pdf, chapter 3, pp. 40-55, Des 12 1997.

[8] Microsoft Corporation, Windows server 2008, "Introduction to IP version 6", Online: http://download.microsoft.com/download/e/9/b/e9bd20d3-cc8d-4162-aa60- 3aa3abc2b2e9/IPv6.doc, Jan 2008.

[9] Charles M. Kozierok, "TCP/IP GUID A COMPREHENSIVE, ILLUSTRATED INTERNET PROTOCOLS REFERENCE", online: http://nostarch.com/download/tcpip_ch25.pdf, chapter 25, pp.373-381, October 2005.

[10] Michael H. Warfield Senior Researcher and Fellow, X-Force Internet Security Systems, "Security Implications of IPv6", Online: http://documents.iss.net/9A18A7C3-C47C-4C27-96F5-A9855C2265FD/FinalDownload/DownloadId-00C126912550109A76A0FBC92403BECC/9A18A7C3-C47C-4C27-96F5- A9855C2265FD/whitepapers/IPv6.pdf, 2003.

[11] Kenjiro Cho Sony CSL/WIDE Project kjc@csl.sony.co.jp, Matthew Luckie U.Waikato/NLANR/CAIDA mjl@wand.net.nz, Bradley Huffaker CAIDA/SDSC/UCSD bhuffake@caida.org, "Identifying IPv6 Network Problems in the DualStack World ", Online: http://www.wand.net.nz/~mluckie/pubs/dualstack.pdf.

[12] James M. Moscola, David Lim, Alan Tetley Department of Computer Science, Washington University, Campus Box 1045, One Brookings Drive, Saint Louis, MO 63130, "IPv6 Tunneling Over an IPv4 Network", Online: http://www.arl.wustl.edu/~jmoscola/papers/moscola_iptunnel.pdf, December 13, 2001.

[13] Samuel Sotillo East Carolina University ss0526@ecu.edu, "IPv6 Security Issues", Online: http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf, 2006.

[14] Sean Convery (sean@cisco.com), Darrin Miller (dmiller@cisco.com), “IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)”, 2004.

[15] Doglase E. Comer, Department of Computer seines, Purdue University, West Lafayette, “Internetworking with TCP/IP Principles, Protocols and Architectures”, Fourth Edition, Volume 1, chapter 7, pp. 95-107, 2000.

[16] Amer N.AbuAli, Ismail Ghazi Shayeb, Khaldoun Batiha, Haifa Yabu Aliudos,The Benefits of Using Internet Protocol Version 6 (IPV6), International Review on Computers and Software - November 2010.