**National Research Journal of Information Technology & Information Science**
**Volume-1, Issue-1, Year-2014 PP: 17-25**

# IPv6-The Next Generation Internet Cyber Security

***Bhupinder kaur*, Shivani**, Varsha Rani******

***Assitant Professor, Hindu Kanya College, Kapurthala (PB), India.***

**Abstract**

In this paper we are going to describe the latest Internet Protocol IPv6- i.e. the "next generation" protocol by IETF to replace current version IPv4. IPv6 is implemented on all major operating systems in use, in commercial, business, and home consumer environments. IPv6 has a much larger address space than IPv4. This results from the use of a 128-bit address, where IPv4 uses only 32 bits. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the need for network address translation (NAT). The paper describes the major issues in the deployment of the IPv6 protocol. The various features and characteristics, security aspects, Quality of service, Compatibility with existing protocol i.e. IPv4 are also discussed

**Keywords-*ICMP, IGRP, IPv6, IPv4, IGMP, NAT, ISP, FTP, MTU, UDP,TCP***

**INTRODUCTION**

This paper describes the problems of the IPv4 Internet Protocol and how IPv6 addresses them. IPv6 is short for "Internet Protocol Version 6". IPv6 is the "next generation" protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 ("IPv4").

IPv6 addressing, the new IPv6 header and its extensions, the IPv6 replacements for the Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP), neighboring node interaction, IPv6 address auto configuration, and IPv6 routing. Most of today's Internet uses IPv4, which is now nearly twenty years old. IPv4 has been remarkably resilient in spite of its age, but it is beginning to have problems. Most importantly, there is a growing shortage of IPv4 addresses, which are needed by all new machines added to the Internet. Internet Protocol version 6 (IPv6) is the next-generation Internet Layer protocol for packet-switched Internet works and the Internet.

The 6Bone is the IPv6 backbone that was set up to assist in the evolution and deployment of IPv6 in the Internet. The 6Bone started as a concept in 1995 and was made concrete by a formation meeting at the March 1996 IETF meeting in Los Angeles. IPv4 is currently the dominant Internet Protocol version, and was the first to receive widespread use. Hexadecimal is used in IPv6 because it's easier to convert between hexadecimal and binary than it is to convert between decimal and binary. In December 1998, the Internet Engineering Task Force (IETF) designated IPv6 as the successor to version 4 by the publication of a Standards Track. IPv6 includes a transition mechanism, which is designed to allow users to adopt and deploy IPv6

Besides support for mobility, security was another requirement for the successor to today's Internet Protocol version. As a result, IPv6 protocol stacks are required to include IPsec. IPsec allows authentication, encryption, and compression of IP traffic. Except for application-level protocols like SSL or SSH, all IP traffic between two nodes can be handled without adjusting any applications. The benefit of this is that all applications on a machine can benefit from encryption and authentication, and that policies can be set on a per-host. IPv6 can be extended for new features by adding extension headers after the IPv6 header. Unlike the IPv4 headers, which can only support 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet.

**WHY IPV6 AFTER IPV4**

Indeed, IPv5 did exist. To understand why there is a jump from Version 4 to Version 6, we must review some Internet history.

The timeline stretches back to the early 1970s when the Advanced Research Projects Agency — now the Defense Advanced Research Projects Agency — began fleshing out its fledgling ARPAnet.

That eventually turned into NSFnet, a network the National Science Foundation operated primarily for government scientists. That, in turn, grew into the modern Internet.IP was first developed as a counterweight to TCP, which was the first complete set of protocols developed for ARPAnet. TCP is the transport layer of the Internet, layer four in the Open System Interconnection's seven-layer reference model. It manages network connections and data transport. IP is layer three, the component that enables addressing and routing, among other activities.

For several years, there was only TCP, which scientists were developing as a host-level, end-to-end protocol and a packaging and routing protocol. By the late 1970s, however, people realized they were trying to do too much with a single protocol. IP was created to handle packaging and routing functions.

The engineering world rarely discards anything, however. TCP development alone included two versions of the protocol. So by the time developers decided to split the work and create IP, the TCP line had already reached its third version. When the first complete set of TCP/IP protocols were announced in 1980, it was the fourth iteration, hence IPv4.

So IPv4 was actually the first standardized version of IP.

But as early as the 1970s, people realized the network would not be able to handle future requirements, so engineers created the Internet Stream (ST) Protocol to experiment with voice, video and distributed simulation via the network. Separate development of ST eventually led to ST2 in the 1990s. IBM, NeXT, Apple Computer and Sun Microsystems used that version in their commercial networking products.

ST2, which offered connection-based communications and guaranteed quality of service, was considered a great advance over IP and was formally designated IPv5.

By the time that happened, however, the idea of the next generation of the Internet, or IPng, had already started to percolate. IPng work began in 1994. Instead of moving smoothly through the ST2-based IPv5 to this next-generation Internet, people working on the upgrades decided to improve IPv4 and add everything they thought would be needed for the future Internet. That meant skipping from IPv4 to IPv6.

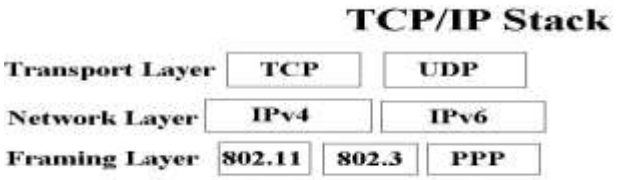
**THE IPV6 ADDRESS SPACE**

- •128-bit address space
- –2128possible addresses
- –340,282,366,920,938,463,463,374,607,431,768,211,456 addresses (3.4 x 1038)
- –6.65 x 1023addresses per square metre of Earth's surface
- •128 bits were chosen to allow multiple levels of hierarchy and flexibility in designing hierarchical addressing and routing
- •Typical unicast IPv6 address:
- –64 bits for subnet ID, 64 bits for interface ID

**PRINCIPLE& WORKING**

IPv6 has a much larger address space than IPv4. This results from the use of a 128-bit address, where IPv4 uses only 32 bits. The new address space thus supports $2^{128}$ (about $3.4\times10^{38}$) addresses. This expansion provides

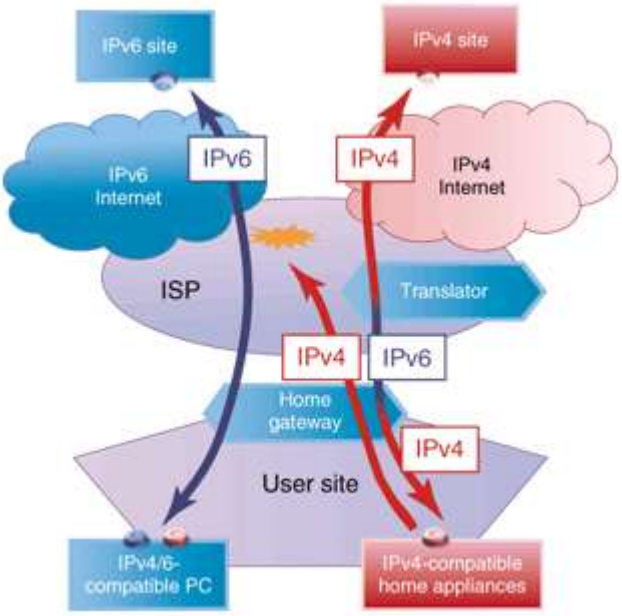
flexibility in allocating addresses and routing traffic and eliminates the need for network address translation (NAT). NAT gained widespread deployment as an effort to alleviate IPv4 address exhaustion.




IPv6 also implements new features that simplify aspects of address assignment (stateless address auto configuration) and network renumbering (prefix and router announcements) when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address). The IPv6 Working Group is focused both on understanding how IPv6 will enable Internet2 to achieve its goals and on promoting and coordinating the deployment of IPv6 throughout the Internet2 infrastructure. The Internet2 IPv6 Working Group aims to make IPv6 an effective tool for the Internet2 community and, in so doing, to contribute to the IPv6 work in the broader Internet by exercising, proliferating, and improving IPv6 infrastructure and software in the Internet2 context.

**TECHNICAL SPECIFICATION**

In order to send a packet that is too large to fit in the MTU of the Path to its destination, a source node may divide the packet into Fragments and send each fragment as a separate packet, to be reassembled at the receiver. For every packet that is to be fragmented, the source node generates an Identification value. The Identification must be different than that of any other fragmented packet sent recently* with the same Source Address and Destination Address. If a Routing header is present, the Destination Address of concern is that of the final destination.



**IP addressing architecture**

An IP address is a binary number, which identifies any user's computer directly connected to the Internet. An IPv4 address consists of 32 bits, but it is usually represented by a group of four numbers (8 bits hexadecimal), from 0 to 255 ranges and separated by full stops. An example of this representation is showed below:

124.32.43.4

Several domain names can also be linked to the same IP address, in effect similar to having more than one name for the same person. The format of the IPv4 header is showed in figure 2:

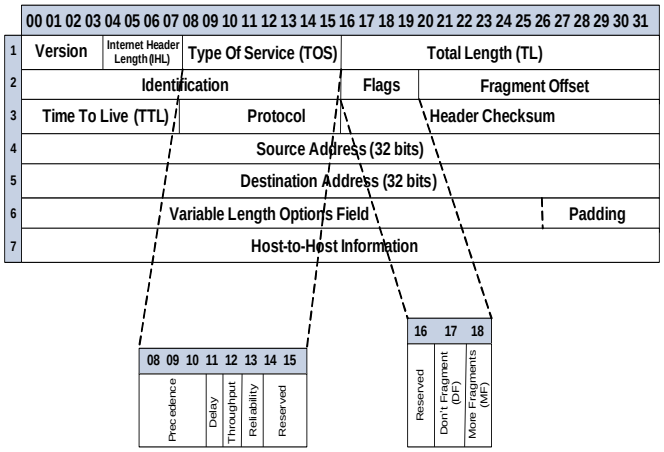



Figure 2: IPv4 Structure

The most recognized change from IPv4 to IPv6 is the length of network addresses. The IPv6 addresses have 128 bits length. The 128 bits provide approximately $3.4x10^{38}$ separate values. An IPv6 address consists of eight numbers in the hexadecimal format, from 0 to 65535 (decimal) ranges and separated by a colon ":". An example of this new representation is showed following:

FECA:0000:234A:0043:AB45:FFFF:9A3E:000B

In other to compare with the IPv4 header next figure 3 shows the IPv6 format header:

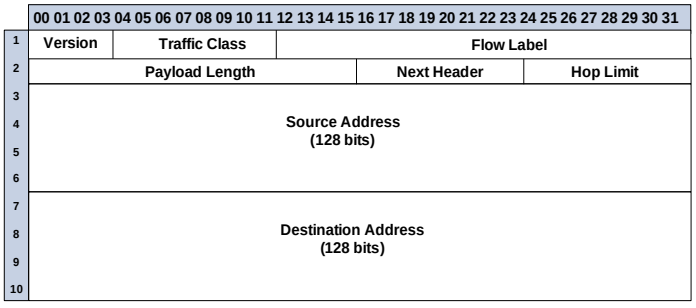



**Figure 3: IPv6 Structure**

**SERVICES AND EQUIPMENT'S**

The "converging" new generation communication networks are using and planning to use an IP based network infrastructure with multi-functional end-devices, always on, always reachable peer-to-peer, with mobility, quality of service and end-to-end security. Even non telecom industries such as music, radio and television will be supported in the IP environment. There are applications that need or will benefit from IPv6 such:
Mobile broadband IP;
Mobile IP broadcast;
Peer to peer VoIP;
Digital radio;
iTV and IPTV;
Grids;
P2P multiplayer games;
RFID;
Control networks;
Remote manufacturing systems;
Sensor networks;
Microsoft (native support of IPv6 in the next version of Windows – Longhorn).

There are also a few technologies that will support the migration to IPv6 like:

Powerline Communication;
Wi-Fi;
Wi-Max;
ZigBee;
Unlicensed Mobile Access (UMA).
Migration
The current IP-based network will gradually migrate from IPv4 to IPv6. Signalling interworking will need to be supported between the IPv6 network and the existing IPv4 network. Mapping of signalling between IPv6 and IPv4 is required. From the deployment point of view, there are three stages of evolution scenarios:
First stage (stage 1): IPv4 ocean and IPv6 island;
Second stage (stage 2): IPv6 ocean and IPv4 island;
Third stage (stage 3): IPv6 ocean and IPv6 island.

There are several migration mechanisms from the IPv4 protocol to IPv6 protocol. The most discussed techniques are:

**A. Dual stack** – to allow IPv4 and IPv6 to coexist in the same devices and networks.

**Dual Stack Technique**
In this method it is proposed to implement two protocols stacks in the same device. The protocol stack used for each link depends on the device used at the other end of the link.

**B. Tunnelling** – to avoid order dependencies when upgrading hosts, routers or regions.

**Tunnelling Techniques**
Tunnelling techniques are used in two phases in the migration to a fully IPv6 network. In the first phase the core of the network uses the IPv4 protocol and there are only small islands IPv6. Figure 5 shows this phase. The IPv6 protocol is encapsulated in IPv4 tunnels.

**C. Translation** – to allow IPv6 only devices to communicate with IPv4 only devices.

**Translation Techniques**
This technique uses a device, the NATPT (Network Address Translation – Protocol Translation) that translates in both directions between IPv4 and IPv6 at the boundary between an IPv4 network and an IPv6 network. Figure 7 shows this arrangement.

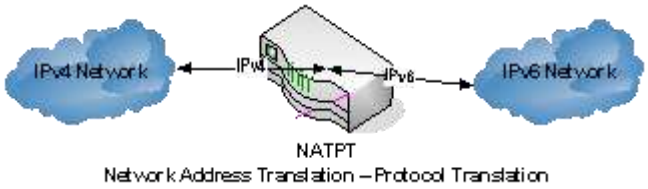



Figure : The arrangement with Network Address Translation – Protocol Translation

**APPLICATIONS**

***A. IPv6 implementation for system***
There is software available for most operating systems in common use today. Find your favorite OS on our list of IPv6 implementations. We also have a collection of "how to install" documents for various systems.

***B. Applications run over IPv6***
Many common Internet applications already work with IPv6, and more are being ported..

**COMPARISON**
IPv6 is a conservative extension of IPv4. Most transport- and application-layer protocols need little or no change to operate over IPv6; exceptions are application protocols that embed network-layer addresses, such as FTP or NTPv3. IPv6 and IPv4 are two completely separate protocols. IPv6 is not backwards compatible with IPv4, and IPv4 hosts and routers will not be able to deal directly with IPv6 traffic (and vice versa).

IPv6 specifies a new packet format, designed to minimize packet-header processing. Since the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable. In addition to address scopes, IPv6 introduces the concept of "scope zones". Each address can only belong to one zone corresponding to its scope. A "link zone" (link-local zone) consists of all network interfaces connected on one link. Addresses maintain their uniqueness only inside a given scope zone. The most common way to talk to a host is by talking to it directly using its unicast address. In IPv4, the unicast address is the "normal" IP address assigned to a single host, with all address bits assigned. The broadcast address used to address all hosts in the same IP subnet has the network bits set to the network address, and all host bits set to "1" (which can be easily done using the netmask and some bit operations). Multicast addresses are used to reach a number of hosts in the same multicast group, which can be machines spread across the Internet.

**FEATURES**

***A. New header format***
The IPv6 header has a new format that is designed to minimize header overhead. This is achieved by moving both nonessential fields and option fields to extension headers that are placed after the IPv6 header. The streamlined IPv6 header provides more efficient processing at intermediate routers.

IPv4 headers and IPv6 headers are not interoperable and the IPv6 protocol is not backward compatible with the IPv4 protocol. A host or router must use an implementation of both IPv4 and IPv6 in order to recognize and

process both header formats. The new IPv6 header is only twice as large as the IPv4 header, even though IPv6 addresses are four times as large as IPv4 addresses.

Efficient and hierarchical addressing and routing infrastructure

IPv6 global addresses used on the IPv6 portion of the Internet are designed to create an efficient, hierarchical, and summarizable routing infrastructure that addresses the common occurrence of multiple levels of Internet service providers. On the IPv6 Internet, backbone routers have much smaller routing tables.

***B. Stateless and Stateful address configuration***

To simplify host configuration, IPv6 supports both stateful address configuration, such as address configuration in the presence of a DHCP server, and stateless address configuration (address configuration in the absence of a DHCP server). With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (link-local addresses) and with addresses that are derived from prefixes advertised by local routers. Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

***C. Built-in security***

Support for IPSec is an IPv6 protocol suite requirement. This requirement provides a standards-based solution for network security needs and promotes interoperability between different IPv6 implementations

***D. Better support for quality of service (QoS)***

New fields in the IPv6 header define how traffic is handled and identified. Traffic identification, by using a Flow Label field in the IPv6 header, allows routers to identify and provide special handling for packets that belong to a flow. A flow is a series of packets between a source and destination. Because the traffic is identified in the IPv6 header, support for QoS can be easily achieved even when the packet payload is encrypted with IPSec.

New protocol for neighboring node interaction

The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of neighboring nodes (that is, nodes on the same link). Neighbor Discovery replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages ExtensibilityIPv6 can be extended for new features by adding extension headers after the IPv6 header. Unlike the IPv4 header, which can only support 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet.with efficient multicast and unicast messages and provides additional functionality.

**ADVANTAGES**

***A. Larger address space***

IPv6 has 128-bit (16-byte) source and destination addresses. Although 128 bits can provide over 3.4×1038 possible combinations, the large address space of IPv6 has been designed to allow for multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within an organization.

Although only a small percentage of possible addresses are currently allocated for use by hosts, there are plenty of addresses available for future use. With a much larger number of available addresses, address-conservation techniques, such as the deployment of NATs, are no longer necessary

***B .Multicast***

The ability to send a single packet to multiple destinations is part of the base specification in IPv6. This is unlike IPv4, where it is optional (but usually implemented) IPv6 does not implement broadcast, the ability to send a packet to all hosts on the attached link. The same effect can be achieved by sending a packet to the link-local all hosts multicast group. Most environments, however, do not currently have their network infrastructures

configured to route multicast packets; multicasting on single subnet will work, but global multicasting might not. IPv4 has a fixed size (40 bytes) of option parameters. In IPv6, options are implemented as additional extension headers after the IPv6 header, which limits their size only by the size of an entire packet. Security features for IPv6.The IPv6 protocol for Microsoft® Windows Server 2003 family incorporates Internet Protocol security (IPSec), which provides protection of IPv6 data as it is sent over the network. IP header format contains, version of the Internet protocol, traffic class, flow label, next header and hop limit source address and destination address.

***C. Jumbograms***

IPv4 limits packets to 64 KB of payload. IPv6 has optional support for packets over this limit, referred to as jumbograms, which can be as large as 4 GB. The use may improve performance over high-MTU networks. The presence of jumbograms is indicated by the Jumbo Payload Option header.

**Disadvantages**

IPV6 causes more CPU cycles on a router/switch and has a higher bandwidth overhead. A router has many tables such as the routing table, switching table which make the decisions on what routes go where and where to forward packets.Running IPv6 creates another stack of these tables separate from IPv4, so yes CPU and memory usage will increase. For a home user the increase would probably be marginal, but in an enterprise environment where you are actively participating in global routing etc then the extra resources required are very noticeable. This implementation of IPSec for IPv6 is not recommended for use in a production environment because it relies on static keying and has no provisions for updating keys upon sequence number reuse.

**Conclusion**

The main aim of this part of the paper was to present the basics of Internet Protocol and motivate the need for an upgraded version of this protocol. There are solutions available for achieving interoperability of the two protocols for every scenario. If the means of interoperating is chosen wisely, moving to IPv6 should not be too traumatic once the initial change is complete - no long-lasting efficiency penalties are necessary, and configuration need not be a huge burden.

**REFERENCES**

1. ISP Planet - Technology - Major Companies Give IPv6 Year-End Push, December 26, 2001, by Jim Thompson, http://ispplanet.com/technology/2001/ipv6_endyear.html
2. ISP Planet - Technology - Stop the IPv4 World, I Wanna Get Off, April 5, 2002, by Jim Thompson, http://www.ispplanet.com/technology/2002/ipv6_world_waits.html
3. Tech Encyclopedia, http://www.techweb.com/encyclopedia/
4. Internet Society (ISOC) - IPv6 and the Future of the Internet, Author: Brian Carpenter, 23 July 2001, http://www.isoc.org/briefings/001 October 2, 2002 8 of 9
5. IP Version 6 (IPv6), by Robert Hinden of Nokia, last updated on 16 January 2002, http://playground.sun.com/pub/ipng/html/ipng-main.html
6. The New Internet Protocol, William Stallings, http://www.csipv6.lancs.ac.uk/ipv6/documents/papers/stallings
7. IPv6 (IPng) - The Coming "Big Bang" in Cyberspace, Jim Bound, Al Cini, http://www.csipv6.lancs.ac.uk/ipv6/documents/papers/bound/IPNG.htm#For_More_Info
8. Interview: IPv6 Deployment Issues: Interview with Jim Bound (Compaq) and Latif Ladid (IPv6 forum president), July 1999, http://www.ipv6forum.com/navbar/technology/jbpminterview.htm
9. The Move to IPv6, Technical Paper, Alcatel, 02 2002, www.alcatel.com,search For IPv6, www.cid.alcatel.com/doctypes/techpaper/pdf/IPV6_tp.pdf
10. PAIX Engineering Interviews, Mr. Stephen Stuart, VP of Engineering and Mr. Brad Horak, Director of Engineering
11. ISP Planet - IPv6: The Future is Now, Jim Thompson, August 7, 2001, www.ispplanet.com/technology/2001/ipv6_nowagain.html
12. ISP Planet . Waiting, Waiting, and Waiting for IPv6, Jim Wagner, July 3, 2002, www.isp-planet.com/business/2002/ipv6_wait.html

13. .Latest IP version will be better geared to handle Net surge., eFE interview . C Mendiratta, Principal consultant, Cisco Systems, November 13, 2001, http://www.financialexpress.com/fe20011113/efetop5.html
14. What is the matter with IP Version 4?, 26th August 2002, http://www.itdirector.