IP version 6

Abdulla S. Mamuwala; University of Alabama Birmingham; Birmingham, AL

Keywords: IPv4, IPv6, Address capability, automatic configuring network devices, network security, real time performance, multicasting

ABSTRACT
Every computer on the Internet has a unique identifying number called an IP address. IPv4 is the IP system widely in use today. But IPv4 has a limited address space. Taking into account the ever-increasing network of computers, IPv4 in the near future will have to be replaced by a new IP addressing scheme. This new IP addressing scheme, which will replace IPv4, is called IPv6 (IP version 6). This paper discusses the reasons for replacing IPv4 with IPv6, how IPv6 overcomes the drawbacks of IPv4, and some of the special features of IPv6.

1. INTRODUCTION
The Internet from its humble start around 1973, connecting about 250 sites and 750 computers has seen an almost exponential growth since then. Now it connects more than 60 million users throughout the globe. Approaching the 21st century, the Internet will be used in ways, unimaginable by us today.

The Internet will not only connect computers but also electronic devices such as PDA’s, mobile phones, and even home appliances such as coffee makers and toasters. Therefore, devices both at work and at play will be connected to the Internet.

Every computer on the Internet has a unique identifying number called an IP address. The IP (Internet Protocol) system widely in use today is called IPv4 (IP version 4). IPv4 has certain disadvantages. The primary disadvantage is the limited address space available with IPv4.

Therefore, we require a new IP system, which will overcome the shortcomings of IPv4. This new IP system we are talking about, is called IPv6 (IP version 6). IPv6 is a standard set down by the Internet Engineering Task Force (IETF). IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

The Internet Engineering Steering Group (IESG) approved IPv6 or IPng, the Next-Generation Internet Protocol, on November 17, 1994 as a Proposed Standard [1]. Since that time a huge number of end-user organizations, standards groups, and network vendors have been working together on the specification and testing of early IPv6 implementations.

The new IP is based on a very simple philosophy: The Internet would have not been so successful in the past years if IPv4 had contained any major flaw. IPv4 was a very good design, and IPv6 should indeed keep most of its characteristics. In fact it could have been sufficient to simply increase the size of the addresses and to keep everything else unchanged. However 10 years of experience brought lessons. IPv6 is built on this additional knowledge. It is not a simple derivative of IPv4, but a definitive improvement [1].

2. ADDRESSING SCHEME OF IPv4
IPv4 uses a 32-bit field for addressing computers connected to the Internet. At the binary level we deal with only 0’s or 1’s. Therefore, the total number of computers on the Internet that can be allocated IP addresses using IPv4 is $2^{32}$ that will result in about 4.2 billion computers. Considering the fact that, China alone has a population of approximately 1.2 billion, in the near future, when the Internet will become accessible to more people than it is today, IPv4 will fail to provide IP addresses to all the devices connected to the Internet. In fact the demand for IP addresses will run far beyond the capacity of addresses that IPv4 can provide. A typical IPv4 address can be represented as 194.153.12.232.

The above IP address is composed of four one-byte fields of binary values separated by a decimal point. IPv4 address consists of two parts, a network number and a host or a machine number.

IPv4 is based on network and host number assignment. These numbers identify the network or host connection and not the actual network or computer. IPv4 divides its address assignment into three main classes A, B and C. Class A addresses assign the first 7 bits to the network and the remaining 24 bits to a host. Theses addresses are reserved for organizations that have up to 16,777,216 hosts, and there can be at most 128 of these networks. Class B assigns the first 14 bits to a network and the remaining 16 bits to a host. These addresses are reserved for organizations that have up to 65,536 hosts, and there can be at most 16,384 networks. Class C addresses assign the first 21 bits to a network and the remaining 7 bits to a host. These addresses are reserved for organizations that have fewer than 256 hosts, and there can be a maximum of 2,097,152 networks.

The addresses class determines the network mask of the address. A network mask is nothing but a 32-bit Internet address that has all the bits in the host number set to zero. Hosts and routers use the network mask to route Internet packets.

Next, the addressing scheme of IPv6 will be discussed, and it will be shown how it overcomes the address space limitations of IPv4.

3. ADDRESSING SCHEME OF IPv6
IPv6 uses a 128-bit field for addressing devices connected
to the Internet. Therefore, the total number of devices on the Internet that can be allocated IP addresses using IPv6 are about $3 \times 10^{38}$. That gives us more than $6 \times 10^{23}$ addresses for every square meter of the earth’s surface. Hence, the address space limitations experienced while using IPv4 are overcome by using IPv6. There are three forms of representing the IPv6 address.

3.1. Preferred form:
The preferred form can be represented as X:X:X:X:X where X stands for the hexadecimal values of the eight 16-bit pieces of the address. For example, IPv6 in the preferred form can be represented in the following form. FEED:FOOD:DEED:7765:5564:BEEB:6545:FEED. Here, a colon separates each section and four hexadecimal numbers represent each 16-bit section.

3.2. Compressed form:
The compressed form uses double colons (::) to represent multiple groups of 16 bit zeroes. An address can use a double colon only once. For example, 1080:0:0:0:8:800:200C:417A:: this IP address in the compressed form would then be represented as 1080::8:800:200C:417A.

3.3. Mixed Form:
The Mixed form is represented as X:X:X:X:X:D,D,D,D. The Xs are in the IPv6 format whereas the Ds are in the IPv4 format. The above format is used in a mixed environment of IPv4 & IPv6 nodes.

4. THE IPV6 HEADER AND ITS ADVANTAGES AS COMPARED TO IPV4

<table>
<thead>
<tr>
<th>Version</th>
<th>DS byte</th>
<th>Flow label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload length</td>
<td>Next header</td>
<td>Hop limit</td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 1**-Format of IPv6 Header [1]

The explanation of the header field shown in figure 1 is as follows:

- Version (4 bit): This field indicates the protocol version, will thus contain the number 6.
- DS byte (8 bit): This field is used by the source and the routers to establish which packets belong to the same traffic class and thus set up the different priorities to which the packets belong.
- Flow label (20 bit): Label for data flow.
- Payload length (16 bit): Indicates the length of the data field.
- Next header (8 bit): Identifies the type of header immediately following the IPv6 header.
- Hop limit (8 bit): This field is decremented by one at each node, when the count reaches zero the packet is discarded.
- Source address (128 bit): Contains the address of the source of the packet.
- Destination address (128 bit): The address of the intended recipient of the packet.

In comparison to the IPv4 header the IPv6 header is less complicated. In IPv6 the checksum is computed at the layer 2 itself, therefore we can eliminate the checksum field altogether. But there is a drawback to this too, if the checksum is eliminated the packets become vulnerable to the errors that the routers can make while processing the packets. However, the networks remain fairly safe because the packets will be discarded if they contain invalid fields, say for example the destination field does not exist.

The hop limit field gives the maximum number of hops the packet will take before reaching the destination address. In IPv4 this function is performed by the TTL field, which is given in seconds. In order attain simplicity in IPv4 also the routers convert the seconds into hops and then reconvert back to seconds. This kind of change also ensures advantage on the bandwidth side. This is because the hop limit is 8 bits therefore the maximum number of hops that the packet can make form node to node is 255 [2].

The IPv4 header length is variable therefore we have to specify the IPv4 header length and the length of the packet. In IPv6 the header length is fixed to 40 byte as a result we only need to specify the length of the data field, also the payload length is 16 bits long, so the size of the packets cannot increase 64 kb. The limited size has many advantage, to mention a few, overhead will be less, the queuing time will be reduced, etc...IPv6 also incorporates the flow label field, which is used to identify the data requiring special handling for real-time applications.

In IPv6 we have 6 extension headers to specify options more efficiently as compared to the IPv4 options field, which is dropped in IPv6 header. The extension headers are placed immediately after the IPv6 header. This arrangement has an advantage because the processing time is saved for the routers that do not have to process these extension headers [1].

The extension headers must be in a specific sequence which known as the “header chain”. The header chain is as follows:

- IPv6 header
- Hop by hop option header
- Destination option header
- Routing header
- Fragmentation header
- Authentication header
- Encrypted security payload header
- Destination option header
- Upper layer header

5. SPECIAL FEATURES OF IPV6

Some of the special features of IPv6 are discussed below.
5.1. Autoconfiguration

Autoconfiguration implies that a computer or any machine can automatically figure out the parameters that it needs to use to connect to the Internet. This is particularly advantageous in situations when a person is not trained to deal with computer networks. We can only expect him to remove the machine from the box, plug it in using various connectors. The same situation can be applicable to a network administrator, when he has to build a network overnight.

Capability of IPv6 to provide a large number of IP addresses can be used to create multi-level hierarchies of address allocation. The hierarchical approach will make automatic configuration much more practical then what it sounds today.

The number of devices connected to the Internet is ever increasing this will increase the number of end-to-end paths as the square of allocated addresses. Hence, increasing the number of intermediate routes by a greater factor. The situation discussed above implies that automatic routing is essential, because we do not expect every individual to have the knowledge of configuring his or her computer.

Major Corporate networks and Internet service providers face the problem of manually configuring large number of hosts connected to their networks. IPv6’s auto configuration automatically configures a new device and allows it to communicate with the network. Thereby eliminating the manual configuration problems faced in IPv4.

5.2. Security

When we are connected to the Internet, data is not sent in one continuous stream, but it is cut into slices. Such a slice of data is called a ‘packet’. A lot of packets will create the final information. Hackers, who want to tap in, or in other words gain access to the packets, use what is known as a packet sniffer. A packet sniffer can be thought of as a sort of wiretap device. A device that can "plug" into computer networks and eavesdrops on the network traffic. Thereby, hackers can easily crack passwords, which have given rise to password sniffing, followed by spoofing of addresses and stealing of connections. IP spoofing is nothing but imitating the IP address of a host or a router. This will allow the hacker to gain access to the protected information. From the above discussion we can conclude that Internet is vulnerable to attacks and requires, security features.

IPv6 is designed with key security features, which gives it an added advantage over IPv4. IPv4 will instead have to be redesigned in order to incorporate the same security features that IPv6 possess. The two security features in IPv6 are the authentication header and the encrypted security payload.

The authentication header provides authentication. Authentication is a procedure by which a receiver of a packet is assured that the source from which the packets originate is the one from which they are intended to come from. Authentication also assures that there is no manipulation of the packet, which is received. The second security feature encrypted security payload, ensures that only authorized receivers read the content of the packet.

Both authentication and encryption demand that the receiving and sending stations agree on key, like an authentication or encryption algorithm, and on a set of secondary parameters such as such as the lifetime of the key or the details of the algorithms utilization. This type of agreements will establish a security association between the senders and receivers. That is the receiver receives the packets it will only be able to decrypt it if it can link them with the context of security association. The IPv6 authenticated and encrypted packets all convey a Security Parameter Index (SPI)[2].

5.2.1. Authentication Header

Authentication header is one of the general extension headers that have been defined for IPv6. The authentication header is inserted between the IPv6 header and the end-to-end payload. A TCP packet will contain an IPv6 header, an authentication header, and the TCP packet itself, but many other ways of inserting the authentication header are available. The authentication header by no means will alter the functionality of TCP, or any other end-to-end protocol such as UCP or ICMP. In fact the end-to-end protocols will reject any packets that are not properly authenticated.

<table>
<thead>
<tr>
<th>Next Header</th>
<th>Payload Len</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Security Parameter Index (SPI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sequence Number Field</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication Data Variable</td>
</tr>
</tbody>
</table>

![Figure 2-Format of the Authentication Header](1)

The authentication header as shown in figure 2 has a very simple syntax. It starts with a 96-bit header that compromises the number of the next header in the daisy chain, the length of the authentication payload, 16 reserved bits that should be left to zero, the 32-bit SPI of the security association, and a 32-bit sequence number. This fixed set of parameters is followed by the authentication data, encoded as a variable number of 32-bit words following the SPI. It will be set for example, to 4 if the authentication data is 96-bits long.

5.2.2. Encrypted Security Payload (ESP)

The authentication header does not transform or alter the data by any means. The data is still vulnerable to a sniffer’s attack. By using the encrypted security payload confidentiality is achieved. ESP is always the last header in the chain of IPv6 extension headers. That is it is the last on that is visible when the encryption is applied. The Generic Format of the Encrypted Security Payload is shown in Figure3.

<table>
<thead>
<tr>
<th>32-bit SPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit Sequence number</td>
</tr>
<tr>
<td>Encrypted Data and Parameters</td>
</tr>
<tr>
<td>Authentication Data</td>
</tr>
</tbody>
</table>

![Figure 3-Generic Format of the Encrypted Security Payload](2)
The ESP header has been redesigned during the 1997 revision of the Internet security standards to include a sequence number and an authentication checksum. The sequence number of the ESP is exactly similar to that of the AH. It protects receivers against replay attacks. The authentication checksum, carried after the encrypted data, protects the receivers against a class of attacks that operate by mangling or truncating the encrypted data. The algorithm used to combine the checksum is a parameter of the security association. In all cases checksum protects the sequence number and the encrypted data.

5.3. Real-Time Performance

Steve Deering published the very first draft of the SIP protocol in the fall of 1992. An initial assumption of SIP was alignment on 64-bit boundaries. The initial version of SIP had two 64 bit addresses for source and destination and some secondary fields such as packet length, payload type, or hop count. Now these secondary bits did not require 64 bits, and Steve was left with about 32 extra bits. These 32 extra bits were used for a flow identifier that could be used to identify real time flows, to allocate resources and priorities through some reservation protocol. After about two years of research and refinements, this resulted in the definitions of the flow label and class of IPv6.

The IPv6 specification defines flows. The definition, however, is carefully worded not to imply any imply any specific property. “A flow is a sequence of packets sent from a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers.” In fact, the definition of flow comes implicitly from the definition of flow label itself. A flow is the set of packets that comes from the same source to the same destination and bears the same flow label.

Response time and quality of service have been a major problem as far as adoption of TCP/IP (Transfer Control Protocol) for real-time and near real-time applications such as telephony, video, e-commerce etc., are concerned. By making use of the IPv6’s packet prioritization feature TCP/IP now becomes the protocol of choice for these applications [3]. Packet prioritization is nothing, but simply, assigning priority levels to the packets. This feature assures that lower priority packets do not interrupt real-time data flow.

For example, IP telephony and videoconferencing applications have special requirements compared to other network services. Because they are real time services they demand consistent performance from the network, whereas applications such as email and file transfer can tolerate a network slowdown quite well. Therefore packets, which deal with IP telephony and video-conferencing applications, are given a higher priority [3].

5.4. Multicasting

The increase in the number of multimedia-enabled desktop computers has given rise to a new class of multimedia applications that operate in networked environments. These network multimedia applications take advantage of the existing network infrastructure to deliver video and audio applications to end-users. Most notable are the video conferencing and video server applications. With these applications, video and audio streams are transferred over the network between peers or between clients and servers.

Multicasting capability was introduced in IPv4 in 1998 with the definition of class D addresses and the Internet Group Management Protocol (IGMP) [3]. The developers of IPv6 while developing this protocol insured that they incorporate multicasting capability on all IPv6 nodes, they also made sure that all routers could route multicast packets.

The general format for a multicast address includes an octet with a multicast prefix 11111111, followed by four bits of flags, four bits of scope, and a group identifier. Format is shown diagrammatically in Figure 3.

<table>
<thead>
<tr>
<th>11111111</th>
<th>4-bit flag</th>
<th>4-bit Scop</th>
<th>112-bit Group ID</th>
</tr>
</thead>
</table>

**Figure 4**: Format of Multicast Addresses [3]

Out of the four bits of flag, only the fourth is defined in the IPv6 specifications. The three other bits are reserved and should be initialized to zero. The fourth bit is abbreviated as T for Transient. The global Internet numbering authority a permanent well known address, whereas a transient address is one that is not assigned a permanent address. This is what is typically used in the MBONE today.

The multicast function sends packets to all hosts that register to receive them. Multicasting makes it possible for a large number of users to receive data simultaneously, without wasting bandwidth broadcasting to the entire network. IPv6 can also limit the distribution of the packets to a specific location, region, company etc., thereby providing security and reducing bandwidth, all using its multicasting option.

5.5. Anycast

While multicasting has been happily tried by tens of thousands of IPv4 stations on the MBONE, anycasting was still a research project when the IPv6 specifications were written. The principle of anycasting in itself is very simple. Instead of sending one packet to a specific server, one sends the packet to a generic address that will be recognized by all the servers of a given type, and one trusts the routing system to deliver the packet to the nearest of these servers. One could use anycasting to find out the name of the nearest name server, the nearest file server, or the nearest time server.

There is no specific anycast format in IPv6. Anycast addresses are treated by hosts in exactly the same way as unicast addresses. The load is on the routing system, which has to maintain one route for each anycast address that is active in a given site. This is however conceptually very easy. In a distance vector protocol such as RIP, it is sufficient to add one entry per anycast address to the vector of destination. In a link state protocol such as OSPF, one should create a special type of link state record that describes the presence of an anycast group member near one of the routers.

One excepted usage of anycasting is fuzzy routing for example sending a packet at or through “one router of network X”. This is still under study because of the requirement to
define associated management mechanics. The IPv6 specification purposes, however a limited step in that direction by defining the subnet router anycast address:

<table>
<thead>
<tr>
<th>n bit Subnet Prefix</th>
<th>128-n bits 00000</th>
</tr>
</thead>
</table>

**Figure 5-Subnet Anycast Address [3]**

The idea is that if a given prefix identifies a subnet, for example, an Ethernet, the all the routers connected to that subnet should recognize the anycast address formed by appending to that prefix a null station identifier. This will allow stations to send packets to one of the subnet’s routers. This particular type of anycasting does not require any extension to the routing tables because there is already an entry for the subnet.

### 5.6. Unicast Addresses

The IPv6 unicast address is contiguous bit-wise maskable, and in this respect is similar to IPv4 addresses under CIDR. IPv6 supports three major types of unicast addresses:

- Provider-based unicast address: These addresses are assigned to the organizations by ISPs. These addresses offer globally unique Internet addresses to all of the organization members. Provider-based unicast addresses provide easy integration within the worldwide Internet community.
- Site-local-use addresses: This type of address can be assigned to network devices within an isolated intranet. The organization can join the Internet community at a later time without an adverse effect on the addressing structure.
- Link-local-use addresses: This type of address is used by individuals on a single communications link, such as a mobile laptop computer users connected through phone lines (voice or ISDN) or radio links [3].

### 5.7. Inter-domain Routing

Back in 1991, when the first efforts to define a new version of IP were started, we foresaw three possible "deaths of the Internet": the shortage of network numbers, the explosion of the routing tables, and the overall shortage of IP addresses; there is room for trillions of networks and hosts. But just making the address larger does not by any means solve the explosion of the routing tables.

In today’s Internet, if a router wants to compare the best routes toward all destinations, it must maintain an entry for each network of the Internet in its routing table. Most routers do not do this because their tables are already too large. They only maintain precise routing for a limited subset of the Internet, for example their business partners, and they use default routes to reach each other’s networks. But, the backbone routers in the transit networks of Internet providers cannot use such simplification. They must maintain complete tables. As a result, providers must continuously upgrade their configurations to cope with the growth of the Internet [3].

The solution to this explosion of the routing table is, however, well known: We must aggregate several routing entries. This supposes that we introduce some hierarchy for the addresses and that we deploy an inter-domain routing technology that enables us to take advantage of this hierarchy.

The planned solution for IPv6 is to use provider addresses, because these addresses have a good relation with the networks topology. Routes will be exchanged through the Inter-domain Routing Protocol (IDRP). Users that specific constraints will be able to build tunnels or use the routing header to build up transit routes that fit their policy requirements.

### 5.8. Making the Transition to IPv6 Networking

The change in the IP address will cause a change in the entire networking structure. Firstly, the IP layer needs to be completely changed from IPv4 to IPv6, and the new IP layer has to be tuned to run over the various L2 mechanisms, which are present today. Also the transport protocols have to be constructed which use IPv6 (TCP, UDP and other new transport protocols like SCTP). To effect the changes described it is not possible to jump to IPv6 from IPv4. The strategy would be to introduce a few IPv6 nodes into IPv4 network and then gradually increase them over time till the entire network becomes IPv6 [3].

[Diagram showing IPv4 to IPv6 transition]

It is obvious that the complete change over to IPv6 would be impossible because the existing IPv4 backbone would pose a great difficulty towards the complete adoption of IPv6. Therefore there is a requirement for the co-existence of the two networking technologies and internetworking requirements have emerged. The different transition technologies are given below:

- Tunneling mechanisms
- Configured tunnels
- Automatic tunnels
- 6to4
- ISATAP (Intra-Site Automatic Tunneling Addressing Protocol)
- Tunnel Broker
- NAT-PT with SIIT

Some important aspects of transition

- Routing Protocols: Routing is an important function to ensure reliable propagation of information. Considering that there will be a mixed IPv4 and IPv6 network requires an up gradation of the existing interior and exterior routing protocols. The IGP
protocols like OSPF, RIP and IS-IS have directly newer versions defined which operate on IPv6 addresses basic identifiers.

- DNS support: Currently existing DNS mechanisms provide the name to address lookup and reverse mapping from address to name. Now, the IPv6 addresses will also have to be stored with the IPv4 addresses by the name servers. Currently the DNS records for IPv6 use the A6 format or the AAAA format.

- Network Management: SNMP is the de-facto management protocol used in the current Internet. As new standards are being defined for IPv6 protocol and all other related technologies the related, the corresponding SNMP MIB definitions for these are also being made. The standard transport mechanism for SNMP is over UDP, which could run either over IPv4 or IPv6 with appropriate changes to the socket layer.

- Interaction between transition techniques: Since we are using multiple transition techniques the administrator of a local area network has to consider issues arising out of combination of techniques. For example DSTM and ISTAP have opposite functions and should not be used on the same host. The network administrator would require comprehensive tools to configure and manage a network where multiple transition techniques interact with each other [4].

6. CONCLUSION

Today ten’s of millions of IPv4-based systems are in use, converting them to IPv6 will be a major challenge, that to considering the fact, that most organizations that use IPv4 are not as yet running short of the address space available to them. Even though the cost of conversion from IPv4 to IPv6 might be enormous but facilities like auto configuration both for hosts and routers, are worth the cost of switching to IPv6 all on their own.

The transition to IPv6 is dependent on many factors such as the delivery of IPv6 products, the publication of IPv6 standards and the existence of a management infrastructure. Many implementations of IPv6 are already available, at least on experimental basis. IPv6 stacks can be obtained for several variations of the UNIX operating system, such as AIX, BSD/OS, DIGITAL UNIX, FreeBSD, HP-UX, Linux, NetBSD, SCO and Solaris [3].

In spite of the fact that in the initial stages of adopting IPv6, network administrators might be in a state of disarray, but the switch will have to come sooner rather than later, for IPv6 is a technology which cannot be neglected nor written off.

REFERENCES

BIOGRAPHY

Abdulla S.Mamuwala
Electrical & Computer Engineering
University of Alabama at Birmingham
Birmingham, AL 35294-1150 USA

e-mail: asm@uab.edu

Abdulla Mamuwala: is an Electrical Engineering student at the University of Alabama at Birmingham. He has completed his Bachelor’s Degree from the University of Bombay, India in August 2002.