A Study on Comparison and Contrast between IPv6 and IPv4 Feature Sets

J. Hanumanthappa¹ and Manjaiah D.H²

Abstract--- This document provides an analysis and comparison of IPv4 and IPv6 under various circumstances. It is well understood that IPv6 has been designed to replace IPv4. We have done a feature-by-feature comparison and contrast of IPv6 versus IPv4 and found that IPv6 offers many unique opportunities for increasing a network architectures efficiency and agility. In some sense, there is a competition going on between these protocols, as they are not directly compatible, and network providers and users are being forced to determine whether to support one or both protocols for various network services. The new version of IP, (i.e. IPv6), constitutes an effort to overcome the inborn limitations of IPv4, in order for the new protocol to be able to respond to the new needs as they shape today in the Internet. This paper is aimed to discuss about various comparison issues when porting an IPv4 application to IPv6 with focus on issues that an application developer would face rather than a complete API reference. IPv4 is the incumbent and currently has the most widespread usage for conventional Internet applications. IPv6 is a large-scale re-design and re-engineering of IPv4, based on many lessons learned as the IPv4-based Internet grew and was used in unforeseen ways.

Keywords--- IPv4, IPv6, Multicast, Quality of service (QOS), Routing.

I. INTRODUCTION

The primary motivation for change arises from the limited address space. When IPv6 deployed on a large scale it has solved many current networking problems. When IP was defined, only a few computer networks has existed. Then the designers decided to use 32 bits for an IP address because doing so allowed the Internet to include over a million networks. However, the global Internet is growing exponentially, with the size doubling in less than a year. Currently, two versions of the Internet Protocol (IP) are in use on the Internet. In some sense, there is a competition going on between these protocols, as they are not directly compatible, and network providers and users are being forced to determine whether to support one or both protocols for various network services. IP version 4 (IPv4) is the incumbent and currently has the most widespread usage for conventional Internet applications. IP version 6 (IPv6) is a large-scale re-design and re-engineering of IPv4, based on many lessons learned as the IPv4-based Internet grew and was used in unforeseen ways.

Although it would seem obvious that IPv6 is a superior and valuable protocol to deploy, there is often considerable resistance to enabling IPv6 because Decision-makers have difficulty in seeing a business case for IPv6, unsure of how it can be less costly, more efficient, more productive, etc than the IPv4 status quo. Also, some analysts have propagated significant amounts of misinformation about IPv6 over the last several years. The primary motivation for the defining a new version of IP arises from the address space limitation—larger addresses are necessary to accommodate continued growth of Internet. The secondary motivation for the changes in IP has arisen from the new Internet applications. For example, an applications that deliver audio and video need to deliver data at regular intervals. In this paper we have also contrasted the various features of IPv4 and IPv6.

A. The serious problems of IPv4 are as follows

1. Insufficient number of unique “valid” addresses.
2. Routing tables at core are becoming unmanageably large.
3. Fixed length headers are not flexible enough for new functionality.
4. Packet size (and Practice of fragmentation) is inefficient.

B. The next-generation IPv6 has some advantages over IPv4 that can be summarized as follows

(i). Larger address space: An IPv6 address is 128 bits long. Compared with the 32-bit address of IPv4, this is a huge (2³²) increase in the address space.

(ii). IPv6 addressing: An IPv6 address consists of 16 bytes (octets). It is 128 bits long.

To make address more readable, IPv6 specifies hexadecimal colon notation. In notation 128 bits are divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation require four hexadecimal digits. Therefore address consists of 32 hexadecimal digits with

---

¹Hanumanthappa, J., Dos in Computer Science, University of Mysore, Manasagangotri, Mysore, Karnataka, INDIA (phone: +091-821-2419552; fax: +091-0821-2510789; Email: hanums_j@yahoo.com)
²Dr.Manjaiah.D.H., Reader, Mangalore University, Mangalagangotri, Mangalore, Karnataka, INDIA. (phone: +091 - 0824 - 2287670; fax: +091 - 0824 - 2287424 Email: ylm521@yahoo.co.in)
every four digits separated by a colon. Although the IP address, even in hexadecimal format, is very long, many of the digits are zeros. In this we can abbreviate the address. The leading zeros of a section can be omitted. Only the leading zeros can be dropped, not the trailing zeros. The below figure shows abbreviated IPv6 address.

C. Better header format: IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

D. New options: Changes in the way IP header options are encoded allow for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

E. Allowance for resource allocation: IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

F. Support for resource allocation: In IPv6, the type-of-service field has been removed, but a mechanism called flow label has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video. IPv6 enables addressing architectures that scale well in terms of the number of nodes and subnetworks, the size of subnet works, and the degree of change within subnet works this includes typically-encountered cases where IPv4 becomes difficult to use robustly. Global routing tables in IPv6 are potentially much simpler than their IPv4 counterparts, and thus require lower memory and computational resources. In resource-constrained environments, IPv6 requires less processing than IPv4, which can result in reduced power demands and latencies, especially for routers.

G. Support for more security: The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

H. Flow Labeling Capability: A new capability is added to enable the labeling of packets belonging to particular traffic “flows” for which the sender requests special handling, such as non-default quality of service or “real-time” service.

II. COMPARISON AND CONTRAST BETWEEN IPV6 AND IPV4 FEATURE ISSUES

While IPv4 and IPv6 are similar in much of their basic framework, there are also many differences.

From first glance, there are obviously differences in the addresses between IPv4 and IPv6. The graphic below shows an IP address for both versions of IP. IPv4 Address Example: 125.12.3.65, IPv6 Address Example: 2145:00D5:2F3B:0000:0000:00FF:EF00:98F3.

Removing zeros can also reduce the IPv6 address. Zeros can be removed when they are leading in and within any 16-bit block. The address from the previous example could be reduced using this to the following representation. Note that in the example the block of EF00 does not lose its zeros because they are at the end of the block.

IPv6 Address with Leading Zeros Removed: 2145:D5:2F3B:0:FF:EF00:98F3

Compressing zeros can further reduce IPv6 addresses. A contiguous block of zeros within a 16-bit block can be removed. The blocks of zeros are then represented by double colons:: For example, the IPv6 Multicast address of FF02:0000:0000:0000:0000:0000:0000:0002 can be reduced to FF02::2 using compression.

IPv6 Address with Compressed and Removed Zeros: 2145:D5:2F3B::FF:EF00:98F3

IPv6 performs pretty much the same functions as IPv4, but in a more reliable manner, with larger addresses and more flexible and efficient packet headers. Today the internet has grown to be a million-network, which is something with startling consequences. For instance, one of the most publicized consequences of this growth has been the depletion of the internet address space. Initially, the Internet’s address space consisted of \(2^{32}\) addresses about 4 billion addresses. Today, however, that amount is insufficient, even more if we consider emerging new technologies such as 3G/4G wireless devices and other wireless appliances [1]. However many issues to be considering while comparing the IPv4 with IPv6.

A. Addressing:

The most obvious difference between IPv6 and IPv4 is that IPv6 addresses are 128 bits [1], whereas IPv4 addresses are only 32 bits [2]. This increase in the raw number of bits means that there is a factor of \(2^{96}\) more addresses available.
in IPv6 than in IPv4. Due to the way that the address spaces are sub netted, scoped, and defined for multicast, private/experimental use, and other factors, the actual contrast is less direct than this simple factor. In IPv4 the addresses are 32 bit addresses represented by using three notations. 1. Dotted-decimal notation, 2. Hexadecimal notation, 3. Binary notation. In Dotted-decimal notation the IP address is represented as 10.1.3.7, whereas in Hexadecimal notation the one IP address is represented as 0x810B0BEF, whereas in Binary notation the one IP address is represented as 1000 0111 0000 1011 0000 1011 1110 11111.

B. IPv6 addressing: An IPv6 address consists of 16 bytes (octets). It is 128 bits long. An IPv4 address has 32 bits, whereas an IPv6 address contains 128 bits. The 128 bits in an IPv6 address are split between the network and host addresses. There are 64 bits for the network address and 64 bits for the host address. Due to the larger address space, the number of available addresses jumps from 4,294,967,296 in IPv4 to 340,282,366,920,938,463,463,374,607,431,768,211,456 (or 3.4x10^38) in IPv6. IPv6 addresses are also assigned using a different format. IPv4 uses a dotted decimal and IPv6 uses a colon-hex format. The larger address space allows for clearer addressing and routing. It also allows for multiple interfaces per host and multiple addresses per interface.

C. Hierarchical addressing: We will use Unicast, broadcast, and multi cast addresses in IPv4. In IPv6 there are three major types of addresses: unicast, multicast, and any cast addresses. Unicast addresses are assigned to a single IPv6 node. Multicast addresses are assigned to multiples nodes within a single multicast group. Packets sent to a multicast address must be delivered to all members of the same multicast group. On the other hand, although any cast addresses are assigned to groups of nodes, they do not need to be delivered to all members of the group—it is sufficient that one node receives the packets. Additionally, IPv6 defines a new routing infrastructure that provides for more efficient and smaller routing tables. The IPv6 address space supports three types of address: Unicast, Multicast and Any cast. IPv6 Multicast addressing absorbs the role of IPv4’s broadcast addresses, which is no longer present. The biggest change is the introduction of the any cast address. Any cast addressing allows multiple nodes to be assigned the same any cast Address. When packets are sent to this address routing decides which node is closest to the source and routes the traffic to it. Anycast addresses could be useful in setting up mirror websites, with different physical locations being accessible through the same Anycast address. A user trying to access this site would then be routed to the closest site, resulting in a better experience. Addressing enhancements result in reduced administrative overhead. The teaming of IPv6 Neighbor Discovery and address auto configuration allows hosts to operate in any location without any special support. Renumbering is made easier, resulting in less manual attention by support and network administrators. Renumbering also makes transition from ISP to ISP or network segment to segment much easier and potentially seamless. Stateless and Stateful address configuration assist in making IP configuration and planning easier. Stateless configuration works without a DHCP server, while Stateful is a configuration that has a DHCP server present.

Address Auto configuration allows for a node to make use of router discovery to determine router addresses, network configuration parameters, on-link prefixes and additional addresses. What makes Address Auto configuration so impressive is that while it requires a multicast capable interface, it is possible without the use of DHCP. Through proper configuration and planning, this can reduce the overhead caused by DHCP management in large organizations and ISP’s.

With a new addressing scheme comes a new way of handling name resolution through DNS. The DNS changes required to support IPv6 are specified in RFC 1886. As part of the interim transition from IPv4 to IPv6, it is possible to register an IPv6 address on a DNS server as an IPv4 address. This is important if a consumer’s ISP has not moved to IPv6 for DNS and the consumer would prefer to use IPv6 DNS. The figure below shows a WHOIS lookup in which the domain has an IPv6 address and is found through IPv4 DNS. This example shows a WHOIS registration record from the registrar Network Solutions. The initial resolution with Network Solutions is an IPv4 address, the DNS server from which the record was retrieved.

(i).Unicast addresses: Aside from a few blocks set aside for local-use, multicast, or other specific functions, the majority of the IPv4’s 32-bit address space is designated for global unicast addresses [3]. Unicast addresses identify a single interface within the scope of a particular type of unicast address. The scope of an address is the region of the IPv6 network over which the address is unique. With the appropriate unicast routing topology, packets addressed to a unicast address are delivered only to a single interface. In the IPv4 addressing architecture, IANA delegates Regional Internet Registries (RIRs) /8 address blocks (8-bit network identifiers, also historically called “class A” address blocks), which the RIRs can then divide into variable-length blocks for further assignment to ISPs or other registries [6, 7]. In this regime, the maximum address block that a site can ever be given is a /8, which leaves only 24 bits for sub netting and addressing within the organization. Historically, large or complex organizations have required multiple /8s. For instance, at least 7 /8s belong to the US Department of Defense. Considering there
are only 256 such blocks, the IPv4 address space can be seen as severely limited in its ability to provide unique addresses to the elements of large organizations worldwide. To compound matters, even using multiple /8s is a poor solution, since there is no guarantee that the blocks will be numerically continuous, and if they are not, then both the local numbering scheme may be awkward, and multiple global routing table entries will be stored and propagated for the same site. In recent years, many IPv4 users have circumvented these issues by using Network Address Translators (Nat’s), although this practice is known to be fraught with problems of its own. Unicast address is a one address on a single interface and also it is delivery to a single interface.

The following are types of unicast IPv6 addresses:

- **Unspecified address**: 0:0:0:0:0:0:0:1 or the application layer. The IPv6 loop back address is an integer type IN6ADDR_LOOPBACK. The IPv6 loopback address is an in6_addr structure defined in <netinet/in.h>. For example:

```
struct in6_addr loopbackaddr = IN6ADDR_LOOPBACK_INIT;
```

The symbolic constant named IN6ADDR_LOOPBACK_INIT is defined in <netinet/in.h>. Use it only when declaring a sockaddr_in6 struct.

For example: struct in6_addr loopbackaddr = IN6ADDR_LOOPBACK_INIT

A. D. Unspecified address (This host on this network address):- This is an address in which the prefix part as well as suffix part are zero. In other words the entire address consists of zeros. It is used only to indicate the absence of an address, this type of address cannot be assigned to a node. This type of address is used by a host at bootstrap time when it does not know its ip address. We can use this type of address as a source address. The unspecified address can’t be used as a destination address. The IPv6 unspecified address, 0:0:0:0:0:0:0 or ::, is equivalent to the IPv4 unspecified address of 0.0.0.0.

B. E. Concept of Class full v/s Classless addressing: The IPv4 is broadly divided into Class-A, Class-B, Class-C, Class-D, and Class-E types, where as IPv6 Classless is addressing.

C. F. Concept of Netid and Host id: The Netid is also called as Prefix part. It is a portion of an IP address that defines a network. Where as Host id is a portion of an IP address which identifies a host or router on the network. It is also called as suffix section. We will use prefix and suffix in Class-A, Class-B as well as Class-C addresses in IPv4. The Netid in Class-A is 8 bits and Hostid is 24 bits, where as in Class-B the Net id is 16 bits and Host id also 16 bits, and in Class-C the Netid is 24 bits and Hostid is 8 bits. The netid and Hostid in IPv6 are totally different from IPv4. The first 64 bits address space of an IPv6 address is considered as Netid and another 64 bits address space is considered as a Hostid. The below figure represents a Netid and Hostid in IPv4.

<table>
<thead>
<tr>
<th>Class A</th>
<th>byte 1</th>
<th>byte 2</th>
<th>byte 3</th>
<th>byte 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>p Netid</td>
<td>Hostid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class B</td>
<td>0</td>
<td>Netid</td>
<td>Hostid</td>
<td></td>
</tr>
<tr>
<td>Class C</td>
<td>1 1 0 0</td>
<td>Netid</td>
<td>Hostid</td>
<td></td>
</tr>
<tr>
<td>Class D</td>
<td>1 1 1 0</td>
<td>Multicast address</td>
<td>Hostid</td>
<td></td>
</tr>
<tr>
<td>Class E</td>
<td>1 1 1 1</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

D. G. Address allocation: Usually in IPv4, addresses were allocated by network class. As address space is depleted, smaller allocations using Classless Inter-Domain Routing
(CIDR) are made. Allocation has not been balanced among institutions and nations; where as in IPv6 Allocation is in the earliest stages. The Internet Engineering Task Force (IETF) and Internet Architecture Board (IAB) have recommended that essentially every organization, home, or entity be allocated a /48 subnet prefix length. This would leave 16 bits for the organization to do sub netting. The address space is large enough to give every person in the world their own /48 subnet prefix length.

H. Address lifetime: In IPv4 Generally, not an applicable concept, except for addresses assigned using DHCP, where as in IPv6 IPv6 addresses have two lifetimes: preferred and valid, with the preferred lifetime always <= valid. After the preferred lifetime expires, the address is not to be used as a source IP address for new connections if an equally.

IPv6 brings major changes to the IP header. IPv6’s header is far more flexible and contains fewer fields, with the number of fields dropping from 13 to 8. Fewer header fields result in a cleaner header format and Quality of Service (QoS) that was not present in IPv4. IP option fields in headers have been replaced by a set of optional extensions.

The efficiency of IPv6’s header can be seen by comparing the IPv4 header. IPv4’s header is far more flexible and contains fewer fields, with IP option fields in headers replaced by a set of optional extensions. The IPv6’s header can be seen by comparing the address to header size. Even though the IPv6 address is four times as large as the IPv4 address, the header is only twice as large. Priority traffic, such as real time audio or video, can be distinguished from lower priority traffic through a priority field. The images below show the difference in the headers. Red designates fields in the IPv4 header that are no longer present in the IPv6 header.

| IPv4 Header |
|-----------------|-----------------|-----------------|
| 0 | 4 | 8 | 16 | 24 | 31 |
| Version | IHL | Service type | Total length |
| Identifier | Flags | Fragment Offset |
| Time to Live | Protocol | Header Checksum |
| Source Address (32 bit) |
| Destination Address (32 bit) |
| Options and padding |

| IPv6 Header |
|-----------------|-----------------|-----------------|
| 0 | 4 | 12 | 16 | 24 | 31 |
| Version | Class | Flow Label |
| Payload Length | Next Header | Hop Limit |
| Source Address (128 bit) |
| Destination Address (128 bit) |

I. Security:- Security is a key feature of IPv6. IPv6 is primarily focused on improved security, which makes it popular as data security becomes more and more of a hot topic in all areas of IT. There are many standardized and required security features within IPv6 without having to make changes to applications. Among the improved security features is packet signing to handle authentication. Data confidentiality through encryption helps aid security within IPv6. IPv6 includes an end to end security model that is designed to protect DHCP, DNS and IPv6 mobility. While IPv6’s improvement in security does not make IP invulnerable from attacks, it is certainly a positive and necessary addition.

J. Routing:- The IP routing experience differs with the implementation of IPv6. Smaller routing tables result in more efficient routing and less overhead through faster computation and aggregation. The routing structure makes use of a hierarchical structure that is also more efficient.

K. Neighbor Discovery:- Neighbor Discovery (ND), as specified in RFC2461, is an important piece of IPv6 because it replaces Address Resolution Protocol (ARP) and Internet Control Message Protocol Redirect. ND allows hosts to find neighboring routers, discover addresses, address prefixes and additional configuration information. For routers, ND can be used to broadcast the configuration parameters for hosts seeking connectivity as well as provide improved hop and addressing information for its hosts. The following data structures are defined in RFC2461 on examples for storing ND related information:

(i). Neighbor Cache: Address information is stored about individual neighbors that the host has sent traffic to recently.

(ii). Destination Cache: Address information is stored about destinations that traffic has been sent to recently.

(iii). Prefix List: Prefix lists are defined from information received from Router Advertisements. Default Router List: Keeps track of default routers based from Router Advertisement.

L. Mobility: Due to the way Mobile IPv4 operates (in its most efficient mode), using triangle routing, and packets will cross part of their path within a tunnel, and then another part regularly, with no tunnel. Thus, the IPv4 PCI size changes depending on where in the network it is measured when Mobile IPv4 is used. On the other hand, we will assume a Mobile IPv6 scenario where Route Optimization (RO) is supported, such that packets go directly to their destination without tunneling. This is a feature of IPv6 that has no analogue in IPv4. In a Mobile IPv6 with RO setting, though, different PCI components get placed on a packet depending on whether a mobile node (MN) is using a Care-of Address as a "from" address in outgoing packets, whether the Care-of Address is being used as a "to" address by a corresponding node (CN), or whether Care-of Addresses are used in both directions (between two MNs, both away from their "home" networks).
III. CONCLUSIONS

In conclusion, IPv6 offers many potential business case advantages over IPv4 and is currently possible to use successfully in production environments with readily available materials, possibly without even requiring hardware or software upgrades from currently used systems. Consumer upgrades are underway, but will take a long period of time. Consumer products will drive consumer upgrades. Mobile IP devices, home gaming systems and other consumer-focused products will begin to incorporate IPv6, bringing it into the home. IPv6 enables addressing architectures that scale well in terms of the number of nodes and sub networks, the size of sub networks, and the degree of change within sub networks; including practical cases where IPv4 becomes difficult to use robustly. Mobile IP devices are already connecting to 802.11 Hot Spots that run IPv6. ISP upgrades to IPv6 will likely be consumer driven. As some ISP’s begin to upgrade their networks to IPv6, users will see further IPv6 integration in their homes. Without doubt, IPv6 represents a considerable improvement if compared to the old IPv4 protocol stack. The new suite of protocols provides innumerable features that improve both the overall functionality as well as some specific security functions. Although IPv6 offers better security (larger address space and the use of encrypted communication), the protocol also raises new security challenges. Particular aspects of IPv6 that we have positively identified as advances over IPv4 include:

- IPv6 implementation and migration cannot and should not happen overnight. Major changes are required in all areas of industry to allow migration. Countries and companies, both large and small, must make the move to IPv6 before overall migration of the Internet backbones can happen. As organizations test and complete their migration to IPv6, we move closer to an IPv6 Internet. Some estimates state that IPv6 will not be fully implemented until 2030 or as late as 2040. While major steps are being made towards implementation of the new protocol, a completely IPv6 Internet is many decades away.

REFERENCES
