Issues in IPv4 to IPv6 Migration

[1]Saurabh Dey, [2]Shilpa. N

International School of Information Management,
University of Mysore, Manasagangotri,
Mysore – 570006, India

{[1]saurabh@isim, [2]shilpa}@isim.net.in

Abstract: **This paper contains concepts of IP addresses and the migration of IPv6 from IPv4. Till date the most commonly and widely used protocol is IPv4 for internetwork and intra network communication in both wired and wireless environment. But due to the advancement of Internet usage the availability of IP addresses are in danger. The IP addresses in IPv4 are distributed and used in such a way, that, the possibility of getting new public IP address for an organization is very difficult. In this global competitive era, organizations are established frequently and hence there is a demand for technological communications in the existing business network. The scarcity of IPv4 addresses is limiting the expansion of internetwork, so IPv6 came into existence which is considered as the ultimate solution to the problem related to IPv4. But there is always a problem in migration of technology and/or platforms. IPv6 migration is needed but the issues related to this migration must be taken into consideration.**

Keyword: **IPv6, IPv4, IP address, public IP, migration issues**

I. Introduction

Internet Technologies is an integral part of daily life. People talk about Internet, Bluetooth, Wi-Fi, 2G, 3G, EDGE, WiMAX, RFID etc. as a part of their daily gossip. A person, who says that, he wants a Bluetooth enabled cell phone, may not know the exact working principle of Bluetooth service or technology. But, the only thing he knows is that, how to switch on a Bluetooth device and how to transfer a file from one cell phone to the other. In other words, advancement of Internet Technologies has made life easy in such a way, that a lay man can also use the services without knowing all the internal details, the architecture, data transfer rate, etc.

The communication technology is growing very fast to provide superior quality service in affordable cost. New devices are introduced which are user friendly, interactive, having higher data transfer rate, better information security and privacy, reliable end-to-end communication, etc. An example of communication technology is Internet Technology or data communication which can be defined as "communication between collection of autonomous computers or similar kind of devices in presence of some medium and set of rules for exchanging information". Data communication among computers is possible if the respective addresses of the computers are known to each other. This concept is similar to traditional postal service. Generally for data communication, six different types of addresses are needed. They are source port address, destination port address, source IP address, destination IP address, source MAC address and destination MAC address. This paper has given a brief introduction to different types of addresses, mainly emphasized on IP addresses and discussed the migration issues from IPv4 to IPv6.

II. Addresses in Data Communication

This section has introduced a simple wired data communication technique between two nodes or computers which are connected in an Ethernet network. Suppose a node (node **A**) wants to transfer a data to another node (node **D**) then, the source node must know the address of the destination node.

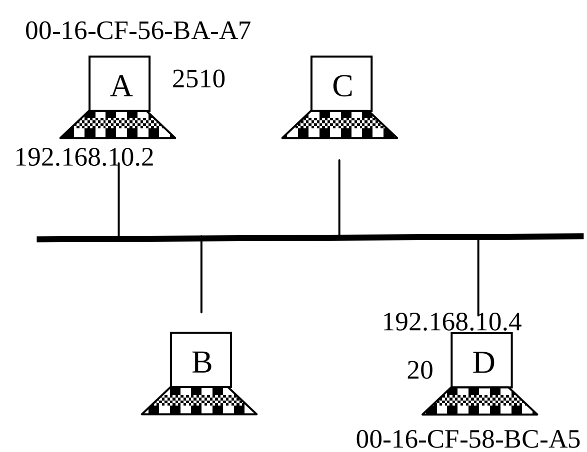

Figure 1: Ethernet Network
Source: An Ethernet Network in ISiM, University of Mysore

Each node contains a port address, a MAC address and an IP address for sending or receiving data. Brief descriptions of the addresses are given below:

A. Port Address:

A port address is a number which identifies a port in a node. Specific applications have specific port numbers, so data can be forwarded to the proper port. The Port number is used by Transport Layer protocols of the Internet Protocol suite such as TCP and UDP. A Port number is a 16 bit integer (unsigned) ranging from 0 to 65535. Port numbers below 1024 are used for standard applications such as Port 80 for HTTP, Port 25 for SMTP etc [1]. The Port number forms one part of the SOCKET address. In *Figure 1* the Port address of the source node **A** is 2510 which is sending a FTP request to destination node **D** having Port address 20 (standard Port address for FTP). Response from **D** to **A** will arrive on Port 2510 in **A**.

B. MAC Address:

In computer networking, the MAC address is also known as physical address which is unique for individual network adapters. It operates in media access control sub layer of OSI reference model. The MAC address is a 48 bit address and the IEEE 802 standard format for printing the MAC address is two hexadecimal digits separated by hyphens (-). A particular device can be attached to any LAN in this world with an assurance that, the MAC address is unique. The first 24 bits correspond to the OUI which is assigned by IEEE. The remaining 24 bit is administered by the assignee [2]. In *Figure 1* the MAC address of the source node **A** is 00-16-CF-56-BA-A7 and the MAC address of node **D** is 00-16-CF-58-BC-A5. In data communication, the source MAC address and destination MAC address is needed for transmitting frame.

C. IP Address:

IP address is also known as logical address of a computer network. It is not a unique address like MAC address because it is not hard coded. IP address works in Network layer of the OSI reference model and needed for routing of network packets. It is a 32 bit address and the standard format is, four 8 bits that are separated by dot (.). An IP address performs two principal functions: host or network interface identification and location addressing. This IP address version is known as IPv4. Detail on IPv4 is discussed in later part. In *Figure 1* node **A** is assigned with an IP address 192.168.10.2 and node **D** is assigned with an IP address 192.168.10.4.

At the time of communication at source – **A**, address encapsulation is done. At the source the data is segmented and the Transport header is added which contains the port addresses (2510 and 20). After segmentation, in network layer - packet is formed and along with Transport Header the Network Header is added, this contains IP addresses (192.168.10.2 and 192.168.10.4). Then in data link layer frame is generated and with the upper layer headers, another header is added (frame header). It contains the physical addresses (00-16-CF-56-BA-A7 and 00-16-CF-58-BC-A5). Finally frame is converted into bits and transmitted to destination. At destination **D,** the decapsulation is done in reverse order and all the headers are removed and finally the data is received by the node.

III. IPv4 Summary

A. Address Space:

IPv4 uses 32 bit addresses which gives an address space of 2^{32} i.e. 4,294,967,296 many unique addresses. IPv4 reserves some of the addresses as private IP address, some as multicast address. It is represented in dotted decimal format (each octet is separated by a dot). In IPv4, the IP addresses are segmented into different classes to design fine grained sub network. These classes are distinguished based on the first three bits of the most significant octet. Each class has its own network boundary defined by the octets and the number of networks depends on the network boundary [3] [4]. The following table is an overview of the classes:

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

Table 1

For allocating IP addresses class A, B and C are used. The range is given below in dotted decimal format:

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

Table 2

The IPv4 sized class-full network architecture was successful in the early days, when each node was assigned with a unique IP address. But the rapid growth of internet, created a problem in the availability of IP addresses. Because allocating a “class A” address to an individual means, losing large number of unique host addresses that falls under that specific network. So class-less method was introduced (known as CIDR) for allocating IP addresses and routing of Internet Protocol packets. This concept enabled network users to create sub-network within an organizations with only one network address.

Then standardization is done for differentiating private and public IP addresses (RFC 1918) [5]. The public IP address is used for global communication and is unique. So it is not recommended to use public IP addresses inside a private network (network within an organization for internal communication). The private IP address ranges are given below:

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

Table 3: IANA reserved blocks for private internets

B. Packet Structure:

The packet consists of header section and data section. The header section consists of thirteen fields, of which twelve fields are in use and one is optional. The header format is given below in Figure 2:

Bit offset	0-3	4-7	8-15	16-18	19-31
0	Version	Header length	Differentiated Services	Total length	
32	Identification			Flags	Fragment offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	Options (if any)				
160 or 192+	Data				

The version is set to 4 for IPv4. The total length is in bytes and is the combined length of header and data. Identification field is a 16 bit number which together with the source address uniquely identify a packet. Flags are used to control whether routers are allowed to fragment the packets. Protocol indicates the type of transport packet whether it is TCP or UDP etc. Source address field and destination address field contain IP addresses of the source and destination respectively. Optional field is used, if IP header length is greater than 32 bit [6].

In IPv4, the availability of address space is exhausting rapidly. So now it is very difficult to allocate a public IP to newly registered individual or organization(s). IETF found a permanent solution to this problem and finally redesigned the Internet Protocol itself and named it as IPv6 [7].

IV. IPv6 SUMMARY

A. Address Space:

In IPv6, the address space is expanded from 32 bits to 128 bits that gives maximum of 2^{128} or about $3.403*10^{38}$ unique addresses. IPv6 has much larger address in comparison with IPv4. IPv6 is designed in such a way that it can provide unique addresses to everyone in this planet. This increase in address space not only allows expansion in allocating addresses, it also makes routing easier and cleaner due to hierarchical addressing. IPv6 addresses are written as eight groups of four hexadecimal digits separated by colon ":" e.g.

2023:0DC0:0000:82A3:0000:0000:0000:1487

For shortening this address, all the leading zeros can be omitted and one consecutive group of zeros can be replaced with (::). Only one group of zeros can be replaced by double colons. Thus the above mentioned address is same as

2023:0DC0:0:82A3::1487

It is given earlier, how the IPv4 address space is divided. In the similar fashion IPv6 address space is divided depending on the value of high order bits in the address. The high order bits and their fixed values are known as a Format Prefix. Following table shows IPv6 address space allocation by Format Prefix.

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

Table 4:IPv6 Address Prefix allocation
Source: RFC: 1884[8]

The remainder of the IPv6 address space is unassigned.

B. Packet Structure:

In IPv6 also the packet consists of header section and data section. The header section has eight fields. The IPv6 header format is given below in Figure 3:

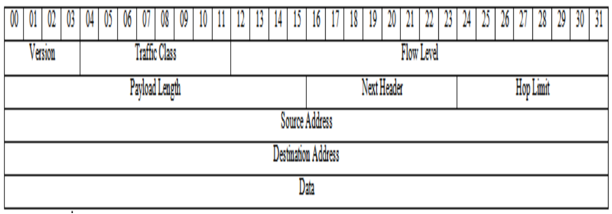

Figure 3: IPv6 Packet header format
Source: IPv6, Internet Protocol version 6 available at http://www.networksorcery.com/enp/protocol/ipv6.htm

The version field specifies IPv6 version number. Traffic class field is 8 bit which specifies Internet traffic priority delivery value. The 20 bit flow label specifies special router handling from source to destination for packet sequence. Payload length specifies the length of the date in the packet.

V. IPv6 Migration Issues

The migration is started from IPv4 to IPv6 but still many of the TCP/IP users have not seen any related software in their systems. Before launching the IPv6 protocol, network infrastructure must be upgraded in order to accommodate the supporting softwares and services. Most of the market leaders in the field of networking have started developing products and services that can support IPv6. Support for IPv6 in UNIX based system is already announced by most of the organizations such as IBM, Swedish Institute of Computer Science (SICS), and the U.S. Naval Research Laboratory etc. Many of the companies have announced for IPv6 support in different operating systems as well as application softwares - such as Apple announced support for IPv6 in MacOS, Novell announced to support it in NetWare, etc [9].

There are number of issues that must be taken into consideration while migrating from IPv4 to IPv6.

A. Infrastructure Issues:

The TCP/IP suite must be redesigned to support the new address format. e.g. the DNS has defined AAAA resource record for IPv6 (128 bit) but it has defined A resource record for IPv4 (32 bit). The other protocols must be redesigned to support IPv6 including DHCP, OSPF, RIP, BGP, ARP etc.

B. Tunnelling Issues:

Without changing the applications, IPv6 can be implemented in an existing network by using IPv6 over IPv4 tunnelling for connecting the IPv4 nodes to the backbone network. But tunnelling has very less throughput and it needs network managers to configure the tunnel end points information, which is a time consuming process.

C. Financial Issues:

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

D. Security Issues:

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

VI. Abbreviations And Acronyms

Wi-Fi: Wireless Fidelity.
2G: Second generation wireless telephone technology.
3G: Third generation mobile phone technology.
EDGE: Enhanced Data rates for GSM Evolution.
WiMAX: Worldwide Interoperability for Microwave Access.
RFID: Radio-frequency identification.
IP: Internet Protocol.
IPv4: Internet Protocol version 4.
IPv6: Internet Protocol version 6.
MAC: Medium Access Control.
TCP: Transmission Control Protocol.
UDP: User Datagram Protocol.
HTTP: Hypertext Transfer Protocol.
SMTP: Simple Mail Transfer Protocol.
FTP: File Transfer Protocol.
OSI: Open System Interconnection.
IEEE: Institute of Electrical and Electronics Engineers.
LAN: Local Area Network.
OUI: Organizationally Unique Identifier.
CIDR: Classless Inter-Domain Routing.
IANA: Internet Assigned Numbers Authority.
IETF: Internet Engineering Task Force.
DNS: Domain Name System.
DHCP: Dynamic Host Configuration Protocol.
OSPF: Open Shortest Path First.
RIP: Routing Information Protocol.
BGP: Border Gateway Protocol.
ARP: Address Resolution Protocol.

VII. Conclusion

The migration from IPv4 to IPv6 is vital, because the present projection shows that IANA will run out of IPv4 available addresses within next few years. The IPv6 address space is sufficient for allocating addresses to all the devices available in earth. So there is no other alternative to this. But migrating to IPv6 has many issues; such as if IPv6 became a standard then organizations have to purchase new supporting systems (softwares and/or hardware), they can't continue with their existing resource such as a old routers that support only IPv4.

REFERENCES

[1] *List of TCP and UDP port numbers*, at http://en.wikipedia.org /wiki/List_of_TCP_and_UDP_port_numbers

[2] *802 IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*, available at http://standards.ieee.org /getieee802/download/802-2001.pdf

[3] *IP Address*, at http://en.wikipedia.org/wiki/IP_address

[4] *IP Address*, available at http://www.webopedia.com/TERM/I/ IP_address.html

[5] RFC 1918, *Network Working Group* - Request for Comments. at http://tools.ietf.org/html/rfc1918

[6] RFC: 791, *Internet Protocol, DARPA Internet Program, Protocol Specification*. September 1981, at http://www.ietf.org /rfc/rfc791.txt

[7] RFC 1883, *Internet Protocol, Version 6 (IPv6) Specification*. Request For Comments. The Internet Society. December 1995. at http://www.ietf.org/rfc/rfc1883.txt

[8] RFC 1884, *IP Version 6 Addressing Architecture*. Category: Standards Track. December 1995. at http://tools.ietf.org/rfc /rfc1884.txt

[9] Gary C. Kessler (February 1997) - *IPv6: The Next Generation Internet Protocol*, available at http://www.garykessler.net /library /ipv6_exp.html

[10] *IPv6: Migration Issues Loom for Network Administrators*, http:// www.enterprisenetworkingplanet.com/netsp/article.php /1365681/IPv6-Migration-Issues-Loom-for-Network-Administrators.htm

[11] Behrouz A. Forouzan -*Data Communication and Networking*

[12] *The Migration from IPv4 to IPv6*", Chapter 12. pp 227-240 at http://www.cu.ipv6tf.org/literatura/chap12.pdf

[13] Arbor Networks, *Tracking the IPv6 Migration*, at http://www.haakonringberg.com/work/papers/SR_IPv6_USFINAL.pdf

[14] Nalini Elkins, Inside Products, Inc. - *IPv6 Migration Issues* at http://www.rmv6tf.org/2010-IPv6-Summit-Presentations/IPv6 MigrationIssues-Nalini%20Elkins.pdf

[15] Cisco Systems - *IPv6 Migration Planning: Help for Getting There from Here* available at http://www.cu.ipv6tf.org /pdf/IPv6_Jan06.pdf

[16] Richard M. Roberts, *Introducing the IPv6 Standard* at http://www.rmroberts.com/FTP_files/IPv6StandardIntroduction.pdf