Computer Network - IP Address & Subnetting

Rajesh Kumar, Pinky Ramchandra Shinde

Abstract: The next-generation Internet Protocol, initially known as IP Next Generation (Ipng), and then later as IPv6, has been developed by the Internet Engineering Task Force (IETF) to replace the current Internet Protocol (also known as IPv4). which offers 2128 possible addresses To enable the integration of IPv6 into current networks, several transition mechanisms have been proposed by the IETF IPng Transition Working Group. This work examines and empirically evaluates two transition mechanisms, namely IPv6 to IPv4 tunneling and dual-stack mechanism, as they relate to the performance of IPv6. The primary focus of this paper is to compare and analyze IPv4 and IPv6 networks, study their characteristics and header formats. The paper also attempts to outline the key deployment issues and security-related challenges which are being faced and dealt with during the migration process.

Keywords— IP address, Subnet, IPV4, IPV6, Multicast Address, Unicast Address, 6-over-4, encapsulation, tunneling,

I. INTRODUCTION

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

The rapid explosion of the internet and existence of high speed wireless and broadband networks have contributed towards depletion of IPv4.The IPv4 protocol created more than three decades ago with approximately an address space of 4 billion cannot cater to the needs of modern internet. The IANA (Internet Assigned Numbers Authority) allocated the last chunk of IPv4 addresses on Feb 3, 2011 to the Regional Internet Registries announcing end of IPv4 addresses [1].

The address depletion has posed a serious problem on the growth of internetworks. The short term solutions like PPP/DHCP (address sharing), CIDR (classless inter-domain routing) and NAT (network address translation) do not seem to help considering the number of devices that are getting connected to the internet daily. Also as the protocol was developed long time back, the features related to mobility, security and QoS (Quality of Service) are handled by additional protocols which cannot be integrated within the protocol.

II. IP ADDRESS

As we know that an Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, Printer) participating in a computer network that uses the Internet Protocol for communication. There are 5 classes of IP address. "Class A" blocks (2^{24} addresses, approximately 16.7 million). "Class B" (2^{16}) and "C" blocks (2^{8}) were provided to smaller networks. Early network architecture permitted only these three sizes.

A. Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses. The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^{7}-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

B. Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is:

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

C. Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is:

11000000 – 11011111
192 – 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses.

Class C IP address format is:

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

D. Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

Revised Version Manuscript Received on May 02, 2016.

Rajesh Kumar, Senior Lecturer, Department of Computer Science and Engineering, Govt. Polytechnic College, Ujjain – 456001 (M.P.). India.

Ms. Pinky Ramchandra Shinde, Assistant Professor, Department of Computer, New Horizon Institute of Management Studies, Sector -13, Airoli, Navi Mumbai, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

11100000 – 11101111
224 – 239

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

E. Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

III. IPV4

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the
OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts 3. THE TCP/IP MODEL Ipv4 6 based upon their logical addresses and to route data among them over the underlying network. IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address. Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.

Internet Protocol version 4 (**IPv4**) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet, and was the first version deployed for production in the ARPANET in 1983. It still routes most Internet traffic today,[1] despite the ongoing deployment of a successor protocol, IPv6. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980). IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP). IPv4 uses 32-bit (four-byte) addresses, which limits the address space to 4294967296 (2^{32}) addresses. This limitation stimulated the development of IPv6 in the 1990s, which has been in commercial deployment since 2006.Because of the demand of the growing Internet, the small address space finally suffered exhaustion on February 3, 2011, after having been significantly delayed by classful network design, Classless Inter-Domain Routing, and network address translation (NAT). IPv4 reserves special address blocks for private networks (~18 million addresses) and multicast addresses (~270 million addresses).

IV. IPV6

Internet Protocol version 6 also known as IPng (IP next generation) is the latest version of the IP for the Internet. IPv6 comes with a 128 bit address scheme, enough to cover nearly every connected device on earth with a global unique address [4].IPv6 uses 128 bit addresses with an address space of 2_{128} (approximately $3.4\times10_{38}$) addresses. Such a large address space allows for every device and user in the world to connect to the internet. It also eliminates the use of NAT in IPv6 and improves connectivity, reliability and flexibility in the network. The design objectives of IPv6 were to support larger address space, security in the protocol and real time multimedia transmission. IPSec support has become a mandatory requirement in IPv6 unlike in IPv4 where it was optional. Payload identification (used in QoS) has been replaced by Flow Label field in IPv6 packet.

The concept of fragmentation has been removed. The checksum and options has been replaced by extension headers in IPv6.Also IPv6 does not require manual configuration or DHCP because the system participates in "stateless" auto configuration which is one of the design goals of IPv6.Finally the packet header size has also been changed from 20 byte in IPv4 to 40 byte in IPv6

A. IPv6 Header Structure

Figure 1 shows the difference between IPv6 and IPv4 headers.

- The length of header has been changed from 20 to 40 bytes
- IPv4 has 4 bytes for address (i.e. 32 bits) while as IPv6 has16 bytes (128 bits).
- The fields in the header has been reduced from 12(IPv4) to 8(IPv6).
- There is no options field in IPv6 header, however it uses "extension headers" that support greater functionalities

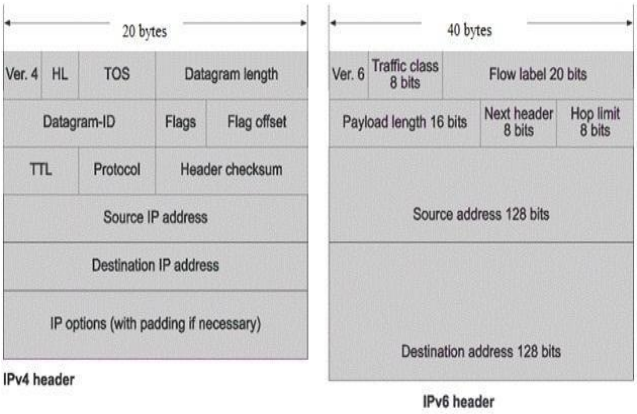

Figure 1-IPv4 and IPv6 Header comparison

B. IPv6 Extension Headers

The Extension header fields are listed below:

1) Hop by Hop Option: This option is used when the source passes the information to all the routers visited by a datagram. Only 3 options are currently defined so far: Pad-1, Pad-n, Jumbo payload.Pad-1 option having length 1 byte is designed for alignment purposes. Pad-n option is similar to pad-1 except it's used when 2 or more bytes are used for alignment purposes. Jumbo payload refers to a payload length more than 65,535 bytes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

2) Source Routing: It involves the concept of strict source route and loose source route as in IPv4.Strict source route is used by the source for predetermined route for the datagram as it travels through the internet. The sender can make a choice about route with a specific type of service such as minimum delay or max throughput. It may also choose a route that is more safer and more reliable for the sender's purpose. If a datagram chooses a strict source route, all the defined routers in the option are to be visited by the datagram. Loose source route is similar to the strict source route but a bit flexible. Along with each router in the list that must be visited, the datagram can visit other routers as well which are not in the list.

3) Fragmentation: Its same concept as in IPv4 however with a little difference. In IPv4, the source or a router fragments the datagram if the size of the datagram is larger than the supported MTU of the network over which the datagram has to travel. In IPv6, the original source can only fragment. A source then finds the smallest value of MTU supported by any network on the path by using a technique for path MTU discovery. Using this gained knowledge, the source then re-fragments the datagram..

4) Authentication: This header carries out the validation of the message sender and ensures that the integrity of data is maintained.

5) Encrypted Security Protocol: This header provides confidentiality and guards against eavesdropping

6) Destination Option: It's used when the source passes the information to the intended destination only. The routers in-between are not permitted to access to this information.

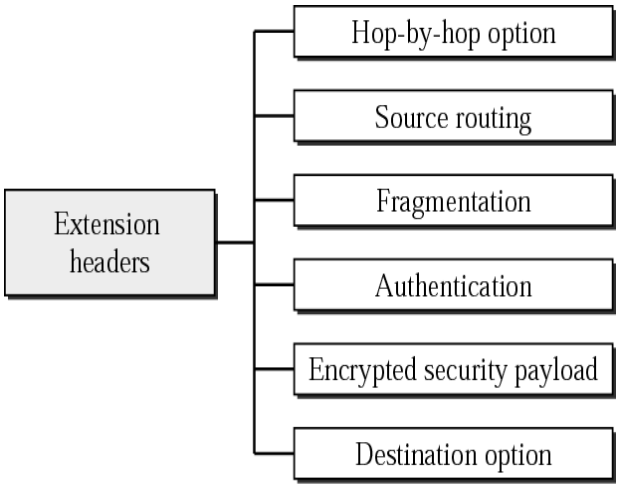

Figure 2: IPv6 Extension Headers

C. IPv4 to IPv6 Transition mechanisms

The transition between the IPv4 Internet today and the IPv6 Internet of the future will be a long process during both protocols coexists. Figure1 shows the transition plan. A mechanism for ensuring smooth stepwise and independent changeover to IPv6 services is required. Such a mechanism must help the seamless coexistence of IPv4 and IPv6 nodes during the transition period. IETF has created the Ngtrans Group to facilitate the smooth transition from IPv4 to IPv6 services [5]. The various transition strategies can be broadly divided into three categories, including dual stack, tunneling and translation mechanisms.

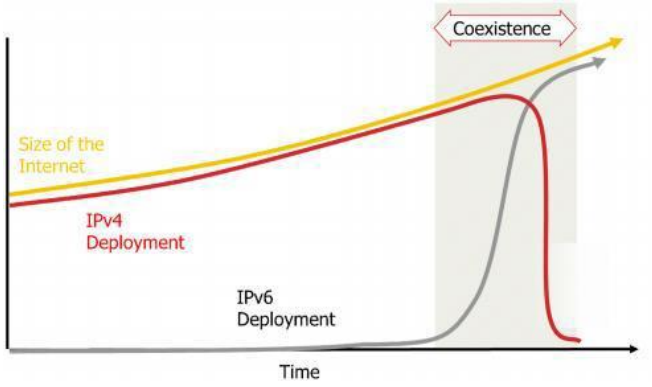

Figure 3: IPv4/IPv6 transition Plan

V. IPV4 Vs IPV6

	IPv4	IPv6
Address	32 bits (4 bytes) 12:34:56:78	128 bits (16 bytes) 1234:5678:9abc:def0: 1234:5678:9abc:def0
Packet size	576 bytes required, fragmentation optional	1280 bytes required without fragmentation
Packet fragmentation	Routers and sending hosts	Sending hosts only
Packet header	Does not identify packet flow for QoS handling	Contains Flow Label field that specifies packet flow for QoS handling
	Includes a checksum	Does not include a checksum
	Includes options up to 40 bytes	Extension headers used for optional data
DNS records	Address (A) records, maps host names	Address (AAAA) records, maps host names
	Pointer (PTR) records, IN-ADDR.ARPA DNS domain	Pointer (PTR) records, IP6.ARPA DNS domain
Address configuration	Manual or via DHCP	Stateless address autoconfiguration (SLAAC) using Internet Control Message Protocol version 6 (ICMPv6) or DHCPv6
IP to MAC resolution	broadcast ARP	Multicast Neighbor Solicitation
Local subnet group management	Internet Group Management Protocol (IGMP)	Multicast Listener Discovery (MLD)
Broadcast	Yes	No
Multicast	Yes	Yes
IPSec	optional, external	required

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

VI. SUBNETTING

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class. CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

1. Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly. For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2^1=2) with (2^{23}-2) 8388606 Hosts per Subnet. The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

2. Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and (2^{16}-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

3. Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator have 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

in order to allocate department-wise IP addresses as mentioned in the example.

Step - 1

Make a list of Subnets possible.

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step – 2

Sort the requirements of IPs in descending order (Highest to Lowest).

Sales 100

Purchase 50

Accounts 25

Management 5

Step – 3

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step – 4

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step – 5

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step – 6

Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

By using VLSM, the administrator can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which was not possible if he has used CIDR.

VII. CONCLUSION AND FUTURE WORK

A major issue that has been ignored in this paper is *security*. We assumes that each node trusts every other node, but if this is

Not the case then the following situations can arise:

- A node requests IP addresses for nodes that do not exist. In this way a node can acquire all the IP addresses denying others to participate in the network.
- A node assigns IP addresses to other nodes without following the given protocol. This can lead to IP address con_icts which might be dif_cult to resolve.
- A node selectively gives wrong information to other nodes. The synchronization process in our protocol depends on reliable broadcast. Since no such broadcast exists in a mobile distributed environment, one can question the robustness of the protocol.

Migration Process from IPv4 to IPv6 is been often compared to the Y2K problem, demanding time and investment of resources. Companies are yet to recognize IPv4 number exhaustion as an alarming problem, and are not ready to put off the investment required into the future. In the future there may be risk of insufficient time and cost [10]. The cost of migration to IPv6 could be a problem. Costs involved include renumbering networks and running two protocol stacks (IPv4 and IPv6) at the same time, upgrade to relevant software and hardware, training the manpower, and testing network implementations. However IPv6 does provide considerable benefits and features required by the modern secure internet. Given the number of problems in the current internetwork, migration process may be the only solution viable in the long run.

REFERENCES

1. http://inetcore.com/project/ipv4ec/index_en.html.
2. http://www.omnisecu.com/tcpip/ipv6/differences-between-ipv4-and-ipv6.php.
3. "IPv6 Headers", Online: http://www.cu.ipv6tf.org/literatura/chap3.pdf, chapter 3, pp. 40-55, Des 12 1997.
4. T. Dunn, "The IPv6 Transition," IEEE Internet Computing, Vol.6, No.3, May/June 2002, pp.11-13
5. IPv6 users' site: http://www.ipv6.org.
6. http://www.juniper.net/techpubs/en_US/junose14.2/information-products/topic-collections/swconfig-ip ipv6/index.html? topic-64529.html.
7. http://ipv6security.wikia.com/wiki/Ipv6_header
8. IETF IPv6 Transition Working Group, http://www.6bone.net/ngtrans.
9. http://en.wikipedia.org.
10. http://www.cybertelecom.org/dns/ipv6_transition.htm.
11. RFC 4213, Basic Transition Mechanisms for IPv6 Hosts and Routers.
12. http://www.gao.gov/new.items/d05471.pdf.
13. RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture .
14. RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers.
15. RFC 3596: DNS Extensions to Support IP Version 6 .
16. www.linecity.de/INFOTECH_ACS_SS04/acs4_top_4.pdf.
17. Ali, AmerNizar Abu. "Comparison study between IPV4 & IPV6." (2012).
18. Dutta, Chiranjit, and Ranjeet Singh. "Sustainable IPv4 to IPv6 Transition."*International Journal* 2.10 (2012).
19. Doshi, Jinesh, et al. "A Comparative Study of IPv4/IPv6 Co-existence Technologies."

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.