Role and Issues of IPV4 and IPV6

Taniya Jain[1], Vedansh Gupta[2], Mahendra singh Sagar[3]

[1]*Student, CCSIT, TMU, Moradabad*

[2]*Student, CCSIT, TMU, Moradabad*

[3]*Asst. prof, CCSIT, TMU, Moradabad*

1jain916440@gmail.coom

2vedanshgupta144@gmail.com

[3]third.author@third.com

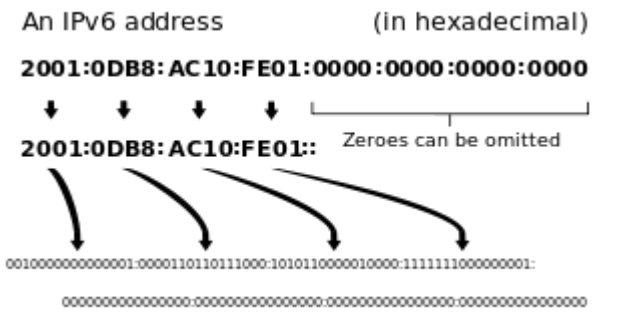
Abstract— **This paper has the role and issues about IPV4 and IPV6. In this paper author asked about the brief introduction of IPV4 and IPV6 header and multicasting. While discussing about IPV6 author also discussed about the hexadecimal address format representation. Further the working of MEDIA, HUB, SWITCH, ROUTER, GATRWAY and HOST addressing are discussed this paper. When we choose and abut some networking terms like gateway, host etc. Here the advantage of IPV6 are also discuss and comparison about IPV4 and IPV6.**

Keywords— **IPV4, IPV6, protocols, gateway ,host ,switch ,address**

I. INTRODUCTION

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 stands for Internet Protocol version 6 also known as IPNG (IP next generation) is the second version of the Internet Protocol to be used generally across the virtual world. The first version was IPv4. IPNG was designed to take an evolutionary step from IPv4. It was not a design goal to take a radical step away from IPv4. Functions
which work in IPv4 were kept in IPNG. Functions which didn't work were removed. The Internet operates by transferring data between hosts in packets that are routed across networks as specified by routing protocols. These packets require an addressing scheme, such as IPv4 or IPv6, to specify their source and destination addresses. Each host, computer or other device on the Internet requires an IP address in order to communicate. The growth of the Internet has created a need for more addresses than are possible with IPv4. Like IPv4, IPv6 is an internet-layer protocol for packet switched internetworking and provides end-to-end datagram transmission across multiple IP networks. While IPv4 allows 32 bits for an IP address, and therefore has 232 (4 294 967 296) possible addresses, IPv6 uses 128-bit addresses, for an address space of 2128 (approximately 3.4×1038) addresses. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

Main features



IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks, closely adhering to the design principles developed in the previous version of the protocol, Internet Protocol Version 4 (IPv4). IPv6 was first formally described in Internet standard document RFC 1883, published in December 1995. That RFC was obsolete and replaced by RFC 2460, published in December 1998. In July 2017 this specification was obsolete and replaced by RFC 8200.

In addition to offering more addresses, IPv6 also implements features not present in IPv4. It simplifies aspects of address assignment (stateless address auto configuration), network renumbering, and router announcements when changing network connectivity providers. It simplifies processing of packets in routers by placing the responsibility for packet fragmentation into the end points. The IPv6 subnet size is standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link layer addressing information (MAC address). Network security was a design requirement of the IPv6 architecture, and included the original specification.

II. WHAT IS NETWORK?

A Network in the world of computers is said to be a collection of interconnected hosts, via some shared media which can be wired or wireless. A computer network enables its hosts to share and exchange data and information over the media. Network can be a Local Area Network spanned across an office or Metro Area Network spanned across a city or Wide Area Network which can be spanned across cities and provinces.

A computer network can be as simple as two PCs connected together via a single copper cable or it can be grown up to the complexity where every computer in this world is connected to every other, called the Internet. A network then includes more and more ,components to reach its ultimate goal of data exchange. Below is a brief description of the components involved in computer network:

Hosts - Hosts are said to be situated at ultimate end of the network, i.e. a host is a source of information and another host will be the destination. Information flows end to end between hosts. A host can be a user's PC, an internet Server, a database server etc.

Media - If wired, then it can be copper cable, fiber optic cable, and coaxial cable. If wireless, it can be free-to-air radio frequency or some special wireless band. Wireless frequencies can be used to interconnect remote sites too.

Hub - A hub is a multiport repeater and it is used to connect hosts in a LAN segment. Because of low throughputs hubs are now rarely used. Hub works on Layer-1 (Physical Layer) of OSI Model.

Switch - A Switch is a multiport bridge and is used to connect hosts in a LAN segment. Switches are much faster than Hubs and operate on wire speed. Switch works on Layer-2 (Data Link Layer), but Layer-3 (Network Layer) switches are also available.

Router - A router is Layer-3 (Network Layer) device which makes routing Decisions for the data/information sent for some remote destination. Routers Make the core of any interconnected network and the Internet.

Gateways - A software or combination of software and hardware put together, works for exchanging data among networks which are using different protocols for sharing data.

Host Addressing- Communication between hosts can happen only if they can identify each other on the network. In a single collision domain (where every packet sent on the segment by one host is heard by every other host) hosts can communicate directly via MAC address. MAC address is a factory coded 48-bits hardware address which can also uniquely identify a host. But if a host wants to communicate with a remote host, i.e. not in the same segment or logically not connected, then some means of addressing is required to identify the remote host uniquely. A logical address is given to all hosts connected to Internet and this logical address is called Internet Protocol Address.

III. Internet Protocol Version 4 (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 based upon their logical addresses and to route data among them over the underlying network.

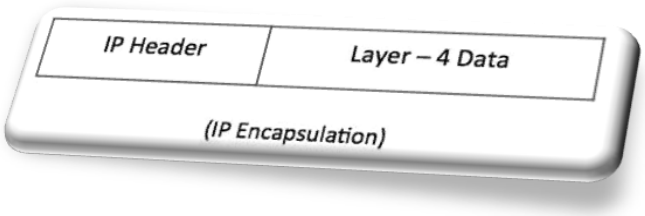
IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address.

The Problem of IPv4 and its Limitations The initial design of the IPv4 did not anticipate the growth of internet and this created many issues which brought forth the idea for the change of the numbering system of IPv4. The limitations of the IPv4 are highlighted below;

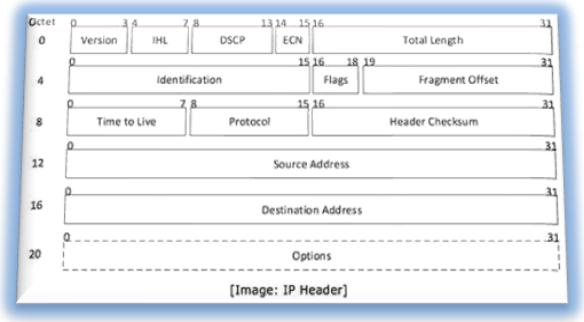
a) *Scarcity of IPv4 Addresses:* Because of the scarcity of IPv4 addresses, many users/ organizations implemented the Network Address Translation (NAT) to map multiple private IPv4 addresses to a single public IPv4 address. More workstations and devices which are connected to the internet also demand the need for more addresses and the current statistics prove that public IPv4 address space will be depleted in due time. This has therefore made the scarcity of IPv4 addressing system a major limitation.

b) *Security:* As stated earlier that the initial design did not anticipate some issues, security threats was also not anticipated at that time.

c) *Quality of Service:* Service quality relies on the 8 bits of the IPv4 type of service field and the identification of the payload. This service has limited functionality and payload identification is not possible when the IPv4 datagram packet payload is encrypted.



d) *Address Configuration Issues*:
Configuring IP addresses should be simplified and clarified as networks and internets are expanding and lots of computers and new invented devices are using IP.



Having had a clear view of the highlighted points regarding issues of IPv4 addresses it is clear to say that since the number of users on the internet is continually increasing very fast, but the address structure of the IPv4 header is fixed which is a leading problem now as the number of addresses is becoming less and less. Another aspect is regarding the development of new applications like Multi-Media and Video conferencing, new features of IP are needed. The following facts will be considered to be demonstrated in the new IP numbering system.

Ÿ Scalable Multicast
Ÿ Provider Selection
Ÿ Mobility Plug-and-Play
Ÿ Real time flow

ipv4 packet formate

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.

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

Version: Version no. of Internet Protocol used (e.g. IPv4).

*IHL***:** Internet Header Length; Length of entire IP header.

*DSCP***:** Differentiated Services Code Point; this is Type of Service.

ECN: Explicit Congestion Notification; It carries information about the congestion seen in the route.

Total Length: Length of entire IP Packet (including IP header and IP Payload).

*Identification***:** If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.

Flags: As required by the network resources, if IP Packet is too large to handle, these 'flags' tell if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.

*Fragment Offset***:** This offset tells the exact position of the fragment in the original IP Packet.

Time to Live: To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.

Protocol: Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.

*Header Checksum***:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.

Source Address: 32-bit address of the Sender (or source) of the packet.

Destination Address: 32-bit address of the Receiver (or destination) of the packet.

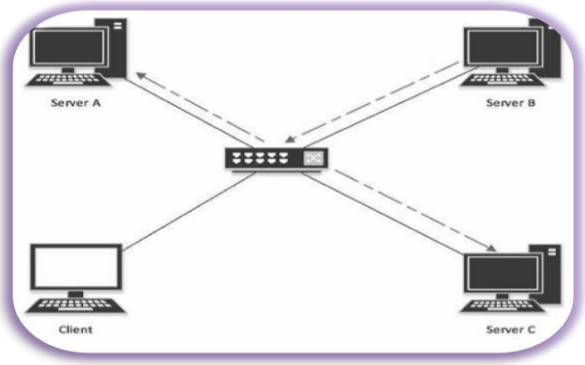
Options: This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

Ipv4 addresing

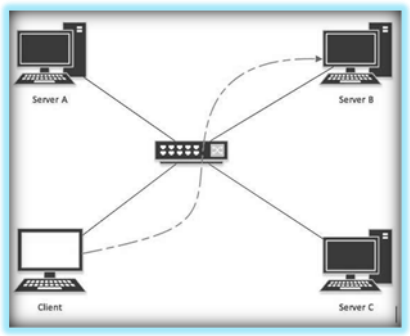
IPv4 supports three different types of addressing modes.

Unicast Addressing Mode

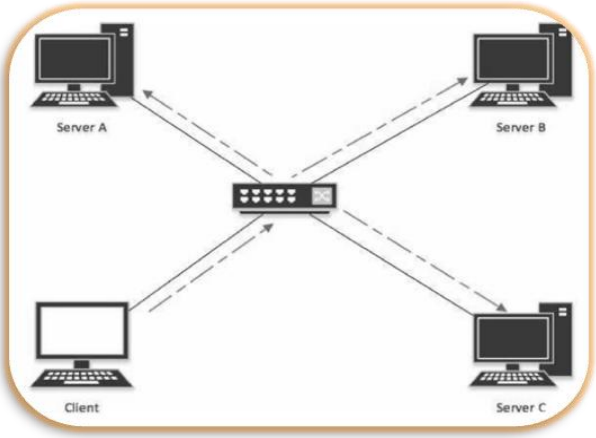
In this mode, data is sent only to one destined host. The Destination Address field



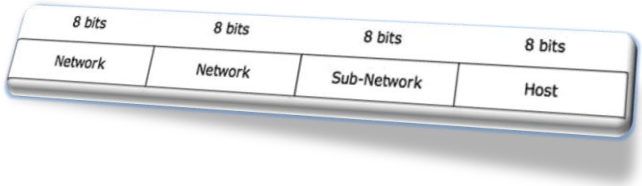
Contains 32-bit IP address of the destination host. Here the client sends data to the Targeted server:



Broadcast Addressing Mode In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e. 255.255.255.255.
When a host sees this packet on the network it is bound to process it. Here the client sends a packet, which is entertained by all the Servers:



Multicast Addressing Mode This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.
Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the Hosts in that network.
Hierarchical Addressing Scheme IPv4 uses hierarchical addressing scheme. An IP address, which is 32-bits in length, is divided into two or three parts as depicted:

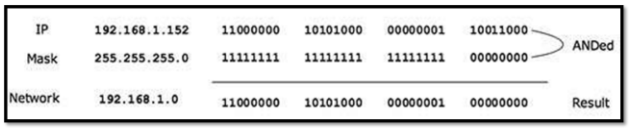


A single IP address can contain information about the network and its sub-network and ultimately the host. This scheme enables the IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts.

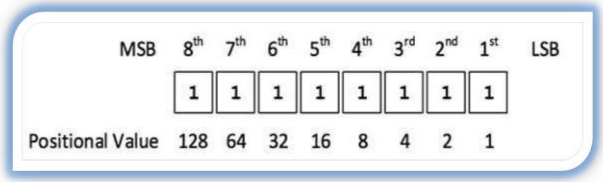
128	64	32	16	8	4	2	1	Value
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	1	1	3
0	0	0	0	0	1	0	0	4
0	0	0	0	0	1	0	1	5
0	0	0	0	0	1	1	0	6
0	0	0	0	0	1	1	1	7
0	0	0	0	1	0	0	0	8
0	0	0	0	1	0	0	1	9
0	0	0	0	1	0	1	0	10
0	0	0	1	0	0	0	0	16
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	1	0	0	100
0	1	1	1	1	1	1	1	127
1	0	0	0	0	0	0	0	128
1	0	1	0	1	0	0	0	168
1	1	0	0	0	0	0	0	192
1	1	1	1	1	1	1	1	255

Subnet Mask
The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet

Mask is also 32 bits long. If the IP address in binary is ANDED with its Subnet Mask, the result yields the Network address.
For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then:



This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.
Binary Representation
The positional value method is the simplest form of converting binary from decimal value. IP address is 32-bit value which is divided into 4 octets. A binary octet contains 8 bits and the value of each bit can be determined by the position of bit value '1' in the octet.

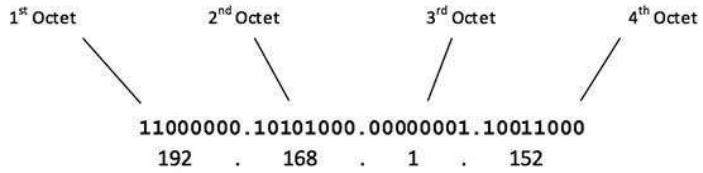


Positional value of bits is determined by 2 raised to power (position – 1), that is the value of a bit 1 at position 6 is 26-1 that is 25 that is 32. The total value of the octet is determined by adding up the positional value of bits. The value of 11000000 is 128+64 = 192. Some examples are shown in the table below:

ADDRESS CLASS

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.
The Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



The number of networks and the number of hosts per class can be derived by this formula:

Number of networks = 2^network_bits

Number of Hosts/Network = 2^host_bits – 2

IV. *INTERNET PROTOCOL VERSION 6 (IPV6)*

It is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4. Pv6 became a Draft Standard in December 1998, and became an Internet Standard on 14 July 2017.

IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks, closely adhering to the design principles developed in the previous version of the protocol, Internet Protocol Version 4 (IPv4). IPv6 was first formally described in Internet standard document RFC 1883, published in December 1995. That RFC was obsolete and replaced by RFC 2460, published in December

1998. In July 2017 this specification was obsolete and replaced by RFC 8200.

WHEN TO CHOOSE IPV6?

As long IPv4 networks do what you need them to do, let them run. But when an IPv4 network hits the limits for some reason, choose IPv6. IPv6 is mature enough to be used in corporate and commercial networks, as many case studies and deployments worldwide show. High investments in new IPv4 setups, fixes, or complex configurations for IPv4 (especially NATs) should be

avoided if possible because they are investments in a technology that will slowly be phased out. When you reach the point where this becomes necessary, evaluate IPv6. Whatever you invest in IPv6 is an investment in future technology Here's the list of indicators that it may be time for you to consider or integrate IPv6:-

*Your IPv4 network or NAT implementation needs

to be fixed or extended.

- You are running out of address space.
- You want to prepare your network for applications that are based on advanced features of IPv6.
- You need end-to-end security for a large number of users and you do not have the address space, or you struggle with a NAT implementation.
- Your hardware or applications reach the end of their lifecycle and must be replaced. Make sure you buy products that support IPv6, even if you don't enable it right away.

THE MIGRATION FROM IPV4 TO IPV6

The years from 1997 to 2000 will be characterized by the adoption of IPv6 by ISPs and users. During 1997, user could still have problems related to the newness of products, but starting from 1998, IPv6 will be part of mass-produced protocols distributed on routers, on workstations, and on PCs. At that point, organizations will begin to migrate, less or more gradually, to IPv6. The key goals of the migration are as follow:

- IPv6 and IPv4 hosts must interoperate.
- The use of IPv6 hosts and routers must be distributed over the Internet in a simple and progressive way, with a little interdependence.
- Network administrators and end users must think that the migration is easy to understand and implement. A set of mechanisms called SIT (Simple Internet Transition) has been implemented; it includes protocols and management rules to simplify the migration. The main characteristics of SIT are the following:
- Possibility of a progressive and nontraumatic transition: IPv4 hosts and routers can be updated to IPv6, one at a time, without requiring other hosts or routers to be updated simultaneously.
- Minimum requirements for updating: The only requirement for updating hosts to IPv6 is the availability of a DNS server to manage IPv6 addresses. No requirements are needed for routers.
- Addressing simplicity: When a router or a host is updated to IPv6, it can also continue to use IPv4 addresses.

IPv6 Subnetting

Subnetting is a way for users to take an assigned IP address space and partition it to meet their specific needs. For example, if an organization has two office locations, one large and one small, the IP address space can be subnetted so that the hosts getthe addresses they need, and traffic can be efficiently handled internally without concerning the global public Internet. Subnetting today in

IPv4 and IPv6 is done by prefixes, but again IPv6 has its own rules.

As an example of how an IPv6 address would be subnetted, assume that the ISP has provided a 48-bit prefix to the user. Consider the address and prefix 2001:0867:5309/48 for instance. Because each four hexadecimal digits are 16 bits, and the last 64 bits are usually the interface identifier (the "host" portion of the address in IPv4), this leaves 16 bits for subnetting.

The 16 subnet bits allow for 28 or 256 subnets. In each subnet, all address possibilities are allowed except for all zeros, which is reserved in IPv6 for subnet router anycast messages. Assume the subnet bits, assigned locally, for a certain subnet are 9abc.

This subnet would allow 264-1 addresses in the range:

2001:0867:53099abc:0000:0000:0000:0001 to 2001:0867:53099abc:ffff:ffff:ffff:ff ff

So, when subnetted, an IPv6 address consists of three parts:

The global routing prefix (2001:0867:5309/48 in this example)

The subnet identifier (9abc in this example)

The interface identifier or "host address" (the remaining 64 bits in this example)

A Need for IPv6?

IETF IPv6 WG began in early 90s, to solve addressing growth issues, but CIDR, NAT, were developed IPv4 32 bit address = 4 billion hosts ~40% of the IPv4 address space is still unused which is different from unallocated The rising of Internet connected device and appliance will eventually deplete the IPv4 address space

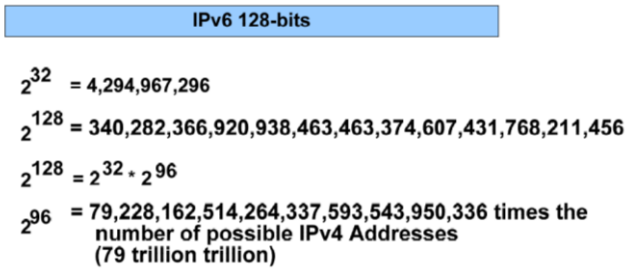
IP is everywhere Data, voice, audio and video integration is a reality Regional registries apply a strict allocation control

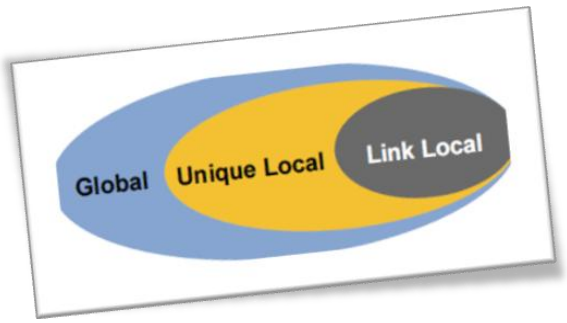
So, only compelling reason: More IP addresses.

IPv6 Header New Field—Flow Label (RFC3697)

Flow classifiers had been based on 5-tuple: Source/destination address, protocol type and port numbers of Transport Some of these fields may be unavailable due to fragmentation, IPv6 Header 20-Bit Flow Label Field to Identify Specific Flows Needing Special QoS encryption or locating them past extension headers With flow label, each source chooses its own flow label values; routers use source address flow label to identify distinct flows Flow label value of 0 used when no special QoS requested (the common case today)

Ipv6 addressing:

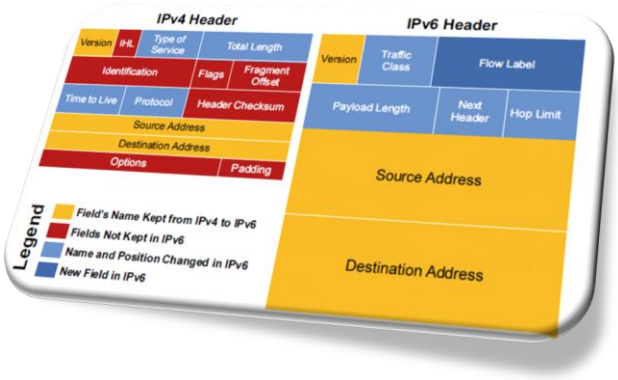




V. Types of IPv6 Addresses

Unicast Address of a single interface. One-to-one delivery to single interface Multicast Address of a set of interfaces. One-to-many delivery to all interfaces in the set Any cast Address of a set of interfaces. One-to-one-of many delivery to a single interface in the set

that is closest No more broadcast addresses IPv6 Address Allocation Process Lowest-Order 64-bit field of unicast address may be assigned in several different ways:
Auto-configured from a 64-bit EUI-64, or expanded from a 48-bit MAC address
(e.g., Ethernet address)
Auto-generated pseudo-random number (to address privacy concerns) Assigned via DHCP Manually configured IPv4 and IPv6 Header Comparison



VI. Major advantages of IPv6 over IPv4?

1. Huge number of IP addresses IPv6 has 128 bit addresses when compared to 32 bit addresses of IPv4 which results in a very large increase in the availability of IP addresses and creates a lot of advantages
2. End to End Connectivity IPv6 eliminates the need for NAT which results in better connectivity in peer-peer networks.
3. Built-in Security IPv6 promotes interoperability between different IPv6 implementations.
4. More Efficient Routing : IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical. IPv6 allows ISPs to aggregate the prefixes of their customers' networks into a single prefix and announce this one prefix to the IPv6 Internet. In addition, in IPv6 networks, fragmentation is handled by the source device, rather than the router, using a protocol for discovery of the path's maximum transmission unit (MTU).
5. More Efficient Packet Processing : IPv6's simplified packet header makes packet processing more efficient. Compared with IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop. Getting rid of the IP-level checksum was possible because most link-layer technologies already contain checksum and error-control capabilities. In addition, most transport layers, which handle end-to-end connectivity, have a checksum that enables error detection.

VII. Conclusions

In this paper we compared IPv4 and IPv6 in address structure, headers fields, security, routing protocols, IP address configuration, function of different protocols, etc. IPv4 is the first version of protocol which has been used globally. When IPv4 was designed, it was estimated to be used for a long time, but the number of devices which are able to connect network is increasing, so that IPv4 faced some problems. In this study we found the main drawbacks of IPv4 and the major features of IPv6 that eliminates the drawbacks of IPv4. Address shortage is one of the important problems of IP, people use multiple devices like PC, laptop, PDA and phones thus the request for IP addresses is raising thus the number of IPv4 addresses is being a problem in future. IPv6 provides larger address space, the length of address in IPv4 is 32-bit, it is increased to 128-bit in IPv6. Mobility is another drawback of IPv4, if a mobile node changes its location, it will lose the current IP address and it should be established again. In contrast of IPv4, IPv6 enhances mobility. IPv6 allows mobile nodes to change their location without dropping the IP address. The security field (IPsec) in IPv4 is optional and all the responsibility of security belongs to the end nodes which is not safe. IPv6 header contains IPsec field, and it is required. This field is implemented by using AH, ESP and IKE. In IPv4, the configuration of IP is done by either manually or DHCP but IPv6 made configuration easy by using auto configuration. According to the previous considerations, IPv6 protocol will be better as compared to the IPv4 protocol. It has arrived as the next generation Internet Protocol and provides several functionalities to eliminate the limitations of IPv4.

REFERENCES

[1] S. L. Levin, and S. Schmidt. "IPv4 to IPv6: challenges, solutions, and lessons," Telecommunications Policy, 2014.

[2] O. Babatunde, and O. Al-Debagy, "A comparative review of internet protocol version 4 (IPv4) and internet protocol version 6 (IPv6)," arXiv preprint arXiv:1407.2717, 2014.

[3] C. E. Caicedo, J. B. D. Joshi, and S. R. Tuladhar. "IPv6 security challenges," IEEE Computer 42.2 ,2009: 36-42.

[4] "Differences between IPv4 and IPv6," omnisecu, [Online], Available: http://www.omnisecu.com/tcpip/ipv6/differences-between-ipv4-and-ipv6.php [Accessed By 21 June 2014].

[5] "Comparison of IPv4 and IPv6", ibm , [Online] 29 April 2007 , Available: http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_72/ rzai2/rzai2compipv4ipv6.htm [Accessed By 21 June 2014].

[6] "IPv6 – tutorial," Tutorialspoint, [Online] , Available: http://Www.Tutorialspoint.Com/Ipv6/ [Accessed By 15 August 2014].

[7] J. I. Parra, "Comparison of IPv4 and IPv6 networks including concepts for deployment and interworking," INFOTECH Seminar Advanced Communication Services (ACS), Institute of Communication Networks and Computer engineering. University of Stuugart, 2004.

[8] "Introduction to IP version 6," Microsoft , [Online] September 2003 , Available: http://Www.Microsoft.Com/En-In/Download/Details.Aspx?Id=21536 [Accessed By 6 August 2014].

[9] E. Durdağı, and A. Buldu, "IPV4/IPV6 security and threat comparisons," Procedia-Social and Behavioral Sciences 2.2 ,2010.