ISSN:0975-9646

Comparative Analysis of IPV4 and IPV6

Samson Isaac

Department of Engineering,
University of East London,
Malaysia.

Abstract-In the recent years, more devices and organizations tend to be becoming more reliant on the internet. The Internet protocol (IP) has become a driving force that allows this device to be connected to the internet. It also provides a suitable way of identifying such device connected to the Network.
In this paper, we will be more concern with the reviewing the comparative analysis of IPV4 and IPV6

Keywords: IP, IPV4, IPV6, IPsec, Internet, Network

INTRODUCTION

The network layer protocol can be defined as a set of rules that allow communication between two or more device (nodes) on that network. Without the network layer protocol, the device will only be connected to each other but no communication will take place. The most common of this protocol is the internet protocol (IP) that specified the technical pattern of the packet and the addressing of the communicating device on the network.
In the recent years, internet protocol version 4(IPV4) become the first type of IP before the arrival of the Internet Protocol Version 6 (IPV6).

IPV4 OVERVIEW

The Internet Protocol version 4 (IPV4) is one of the initial Internet Protocol (IP) that was formed by the IEFT (Internet Engineering Task Force) in the 1980's but was fully deployed in 1981. This became the first protocol of the Transmission Control Protocol/Internet Protocol used. There are some basic features that help to describe IPV4 one of such is addressing

1. IPV4 Addressing Space and Format

IPV4 uses 32-bit addressing techniques system and a representation of 2^{32} addressing which in total has an equivalent of 4 billion (4,294,967,296) unique addresses.

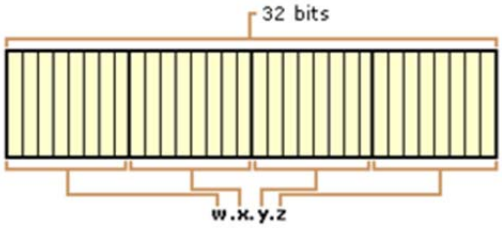

Figure 1.0 IP4 Address

Also, this IPV4 is categories into five classes namely Class A, Class B, Class C, Class D and Class E. Each of these classes has its own bit length the will help to identify the range of the address. Table 1 below shows the range of the different classes of the IPV4.

Table 1

ADDRESS CLASS	RANGE OF ADDRESS	FIRST ID FOR THE NETWORK	LAST ID FOR THE NETWORK
CLASS A	1 - 126	1.0.0.0	126.0.0.0
CLASS B	128 - 191	128.0.0.0	191.255.0.0
CLASS C	192 - 223	192.0.0.0	223.255.255.0
CLASS D	224 - 234	224.0.0.0	234.255.255.255
CLASS E	240 - 255	240.0.0.0	255.255.255.255

IPV4 make use of 127.0.0.0 address as an internal loopback IP address (reserved IP) to check itself on the network in cases of system failure or routing error check. IPV4 apply a four octet of 8 bits for representation in binary for example 192.168.80.3 in binary format is 11000000.101010000.01010000.00000011.

IPV4 Class A

The Class A IPV4 addresses are utilized on networks that has a very large number of hosts. The high order bit in a class A address is always set to zero (0). The zero in the first octet is joined with the remaining 7 (seven) bits to complete the Network ID. The remaining 24 bits which belong to the last three octets represent the Host ID. This allows for 126 networks and 16,777,214 hosts per network. The figure 1.1 Shows the detailed structure of class A addresses.

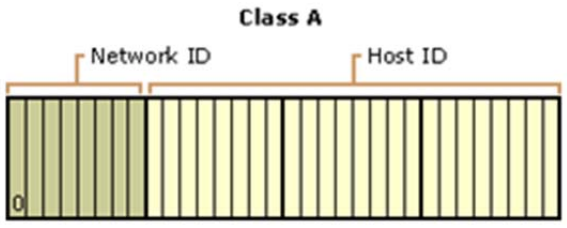

Figure 1.1 Class A IP Addresses

IPV4 Class B

The Class B IPV4 addresses are utilized on networks that have medium-sized to large-sized networks. The two high order bits in a class B address are always set to binary 1 0. The 1 0 in the first two octets is joined with the remaining 14 (fourteen) bits to complete the Network ID. The remaining 16 bits which belong to the last two octets represent the Host ID. This allows for 16,384 networks and 65,534 hosts per network. The figure 1.2 Shows the detailed structure of class B addresses.

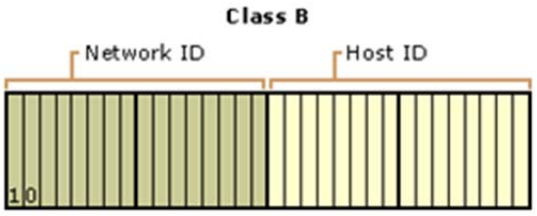

Figure 1.2 Class B IP Addresses

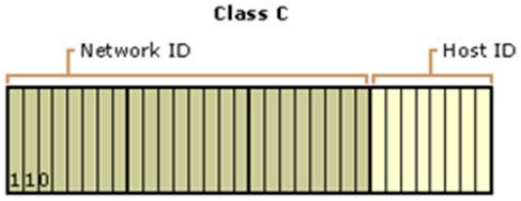

Figure 1.3 Class C IP Addresses

IPV4 Class C

The Class C IPV4 addresses are utilized on networks that have mostly small networks. The three high order bits in a class C address are always set to binary 1 1 0. The 1 1 0 in the first three octets is joined with the remaining 21 (twenty-one) bits to complete the Network ID. The remaining 8 bits which belong to the last octets represent the Host ID. Class C allows for 2,097,152 networks and 254 hosts per network The figure 1.3 Shows the detailed structure of class C addresses.

Table 2. Below shows the summary of address classes A, B, and C that can be used for host IP addresses

IPV4 Class D

The IPV4 Class D addresses are used as reserved for IP multicast addresses. The four high-order bits in a class D address are always set to binary 1 1 1 0. The 1 1 1 0 in the first four octets which is 28 (twenty-eight) bits represent Network ID. The remaining bits are used as Host ID. Microsoft supports class D addresses for applications to multicast data to multicast-capable hosts on an internetwork.

IPV4 Class E

The IPV4 Class E addresses are usually referred to as experimental address that is reserved for future use. Basically, Class E addresses are used for the purpose of Research and so on. The high-order bits in a class E address are set to 1111.

The IP addressing system is a system that contains a subnet mask that helps to differentiate the Network address and the Hosts address. For example, considering an IP address of 192.168.0.2 with subnet mask 255.255.255.0. We will discover that this network is a class C IP address and the last octet decimal which is "2" represent the Host

Table 2

IP address	Total Number of Bits For Network ID/Host ID	First octet of IP address	Number Of Network Bits Used To Identify Class	Usable Number Of Network Idd	Number Of Possible Networks IDs	Number Of Host IDs For Network ID
IPV4 Class A	8/24	0XXX XXXX	1	8-1 = 7	2^7-2 = 126	2^{24} -2 = 16,277,24
IPV4 Class B	16/16	10XX XXXX	2	16-2 14	2^{14} = 16,384	2^{16} – 2 = 65,534
IPV4 Class C	24/8	110X XXXX	3	24-3= 21	2^{21} = 2,097,152	2^8 -2 = 254

Limitation of IPV4

Features	Explanation
1. IPV4 ADDRESS SPACE AND FORMAT	IPV4 only have room for 4 billion address space since the addressing representation is 2^{32} which is equivalent to 4, 294, 967, 296 number of addresses and IP are usually static by configuration or Dynamic Host Configuration Protocol (DHCP), CIDR (Classless Internet Domain Routing), NAT (Network Address Translation) are used to manage and automatically assign dynamic IP.
2. IPV4 SECURITY	The internet Protocol Security (IPsec) support in IPV4 is optional as a result of this, packets are not verified and no encryption is made during the transmission of the packet.
3. IPV4 NETWORK CONGESTION	IPV4 uses the Integrated Header Format (IHF) which does not check the destination of the data before sending, as a result, flood the whole network with such data thereby resulting into congestion. This occurs as a result of the broadcast functionality of the IPV4
4. IPV4 LOSS OF PACKET	IPV4 router has fragment packet that contains what is referred to as Time-To-Live (TTL) protocol that allocate a time frame for each packet to live the header field and once the time frame elapsed the packet is drop which may lead to losing of such packet. It is not suitable for real-time data like video call, streaming video, voice over internet protocol (VOIP) and so on. Also heavy traffic data causes delay during transmission.
5. IPV4 DATA PRIORITY	IPV4 does not give much priority to delay sensitive packets like video streaming because IPV4 does not have the features that allow it to identify which type of data that has been transmitted. This means that IPV4 does not offer priority functionality during transmission. All of these and many more leads to the gradual migration from IPV4 to IPV6.

IPV6 OVERVIEW

The Internet Protocol Version 6 (IPV6), which most times is referred to as IPng (Internet Protocol Next Generation) that was formed by the IEFT (Internet Engineering Task Force) in December 1998 but was fully deployed in 1999. IPV6 is a new technology on the existing IPV4. Although both protocols can work together in the same network and still function effectively.

IPV6 ADDRESSING

IPV6 uses a 128 bit addressing technique system and a representation of 2^{128} addressing which is equivalent to (340,282,366,920,938,463,463,374,607,431,768, 211,456) unique addresses. It became more significant to move from IPV4 to IPV6 because of the rapid growth in the number of devices such as Computers, Ipads, games consoles, smartphone, e.t.c that accesses the internet

OTHER SCHEMES AVAILABLE

Although before IPV6 was out to use other schemes existed like

1. **IPV4 NETWORK ADDRESS TRANSLATION**
   The IPV4 Network Address Translation (NAT) technology is a scheme that bridges the gap between end to end connection thereby acting as an intermediate between private and public network thereby allowing the public network to be connected to the private network and also private network to public network. The technology breaks the initial default standard of public-to-public and private-to-private network connection
2. **IPV4 Classless Internet Domain Routing (CIDR)**
   IPV4 Classless Inter Domain Routing (CIDR) is used to manage and automatically assign dynamic IP. The scheme helps to replace the former Class A, B and C of the IPV4 with the Classless Inter Domain Routing which allow one IP address to assign network to other IP addresses that are unique. The CIDR is like the normal IP address only that it has a splash and a number after the original IP address like 172.160.0.0/16. It is frequently refer to as Network IP Prefix.

SOLUTION TO THE IPV4 BY IPV6

Some of the solutions that IPV6 offer over IPv4 are described in terms of features and migration.

a. In Term of Feature

Features	Explanation
1. **IPV4 ADDRESS SPACE AND FORMAT**	IPV6 tends to use a hexadecimal number field to replace the four octets of 8 bits. It eliminates the Network Address Translation (NAT) which is used by the IPV4 to extend it address by increasing the address size from 32-bits (4 byte) which is almost about 4 billion address space to 128-bits (16 byte) that is large enough for every molecule in the solar system to use, which is approximately 3.4 x 10^{38} addresses. It makes use of auto-configuration (DHCPV6).
2. **IPV4 SECURITY**	IPV6 uses the Internet Protocol Security (IPsec) and also Authentication Header (AH) for the purpose of Authentication of packet and encapsulation of the packet during transmission.
3. **IPV4 NETWORK CONGESTION**	IPV6 uses a more Simpler Header Format (SHF) that makes it easier to check and identify the destination of the packets before sending the packets, as a result, reducing the flood of packets on the network.
4. **IPV4 LOSS OF PACKET**	IPV6 make used of Hop limit field instead of the Time-to-live (TTL). The router does not have fragment packet and also overhead intensive process that may lead to losing of the packet as while as a delay in IPV4.
5. **IPV4 DATA PRIORITY**	IPV6 gives more priority to delay sensitive packets from a bulk data that is being transmitted via the internet. IPV6 is able to achieve this through the built-in Quality of Service (QOS) that helps to give more priority to heavy traffic packets.

b. IN TERM OF MIGRATION

There four types of immigration method from IPV4 to IPV6

1. Dual Stack Method:

This method allows both the IPV4 and IPV6 to co-occur within the same network. The dual-stack method provides a dual channel that allows both the packet send to reach their destination. It forms a stack network that care for both the IPV4 and also IPV6. As shown in fig.1.4. This method is good for smaller networks but not appropriate for large network environment (Al-Debagy O., 2014).

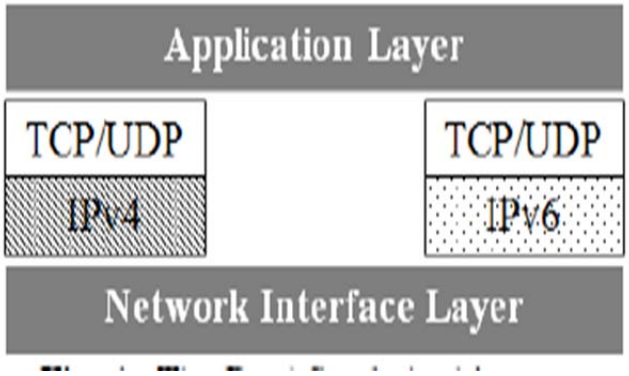

fig 1.4

2. Tunneling Method:

Tunneling method allows the IPV6 packet to use the IPV4 link through encapsulation of the packet. This happens in a situation where you cannot access the IPV6 site (Nizar A., 2012). Fig. 1.5 gives a detailed diagrammatic explanation. Tunneling provides a connection between different dual stack routers, hosts or both of them.

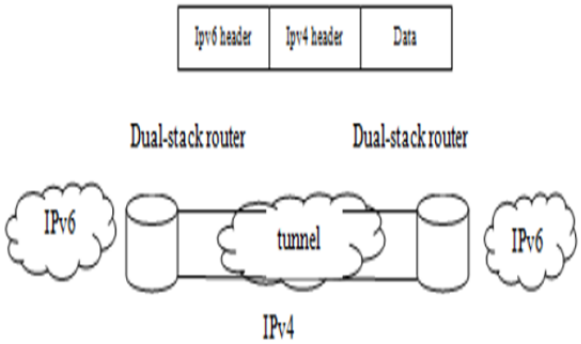

fig. 1.5

3. Translation and Proxying method:

This method allows the IPV6 nodes to communicate with IPV4 nodes so the both protocols can translate each Protocol traffic. This is a translation done using the NAT-P (Network Address Translation Protocols) as such the configuration of the translation is done either statically or dynamically to translate the IPV4 address to IPV6 and also IPV6 address to IPV4 (Babatunde O. , 2014).

4. The Simplicity of Addressing:

The simplicity of addressing allows automatic updating of the routers or host that allows the IPV6 to maintain the IPV4 address as in automatic tunneling where the connection is done between different dual stack routers or hosts or the both (Al-Debagy O., 2014).

TABLE 3: Shows Performance of both IPV4 and IPV6

FEATURES	IPV4	IPV6
1. ADDRESSING	IPv4 uses 32-bit (4 bytes) addressing space about 2^{32} addresses although some are used for special purposes like 10.0.0.0 and 127.0.0.0	IPv4 uses 128-bit (16 bytes) addressing space about 2^{128} addresses
2. HEADER	It has an integrated header field length of 20-60 bytes and also other header options	It has a simpler header format with length of 40 bytes without any header options
3. SECURITY	IPV4 does not have enough security because IPsec is optional	IPV6 has a built-in security which have IPsec
4. CONFIGURATION	It only supports manual configuration or Dynamic Host Configuration Protocol (DHCP)	It support auto-configuration as well as plug and play functionality
5. MOBILE SUPPORT	IPV4 support mobile IP that ranges from 1G to 3G phones	IPV6 support mobile IP that ranges from 4G and above phones
6. NETWORK ADDRESSING TRANSLATION (NAT)	NAT is used increased address limitation	It has no NAT during its design
7. TRANSMISSION	It has broadcast addresses for all devices	IPV6 only uses a multicast group
8. SUPPORT	Uses 0.0.0.0 as unspecified address	Uses :: as unspecified address
9. LOOPBACK	It uses 127.0.0.0 as loopback IP address	It uses :: 1 as loopback IP address

CONCLUSION

IPV6 has become the impending technology for the future of the Internet as such migrating from IPV4 to IPV6 may take more time because a gradual process and more techniques have to be put in place for this protocol to it co-exists and function effectively without affecting the business and organization using the protocols

The research paper gives a detailed explanation of how IPV4 and IPV6 differ and how both of them can co-occur within the same network and function properly without one interfering the other. Also telling us how IPV6 contains all the features that IPV4 has and the Add-ons of the IPV6.

REFERENCES

[1] Amer Nizar Abu Ali, “Comparison study between IPV4 & IPV6”, International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.

[2] Olabenjo Babatunde and Omar Al-Debagy, “ A Comparative review of internet protocol version 4 (IPV4) and internet protocol version 6 (IPV6) “, International Journal of Computer Trends and Technology (IJCTT), Vol 13, Issue 10, No 1, July 2014.