Necessity to Migrate to IPv6

[1]Rahathullah Khan, [2]Hussain Fouad Sindi
[1&2]*Department of Information System*
King Abdul Aziz University, KSA
[1]mdrahathkhan26@yahoo.com, [2]u4sindi@gmail.com

Abstract

This paper describes the migration from the current Internet Protocol (IPv4) to the next generation of Internet Protocol (IPv6) and to adapt the new technologies which probably grows into our networks. We explain the need of implementations of IPv6 when one already is in existence and as well as focus on the awareness of different transition mechanism that makes the IPv4 and IPv6 to work simultaneous on the network. This provides an educational knowledge by showing the comparison of the current Internet protocol with the next generation internet protocol to learn into its technical depth with the addresses, the protocols and the processes.

1. Introduction

In this era of technology where everyone uses their IP enabled devices such as desktop, laptop, mobiles phones, tablet etc. to get connected on the network, the same time the network improvement becomes a very crucial. “The issues of global addressing determines the depletion of current Internet Protocol (IPv4) and deployment of the next generation of Internet protocol (IPv6) into various sectors such as private sector, public sector, government sector, technical and other educational institutions for the better performance and reliability, we had to improve the existing network” [3].

As discussed by the Federal CIO Council, “Internet Protocol (IP) is the language and set of rules that every computers use to talk to each other over the Internet” [13]. To solve this issue, the Internet needs to take a revolutionary step that will enable it to grow beyond its current limitations. The alteration need to be done by migrating to a newer Internet protocol which is known as Inter Protocol version 6 (IPv6) [14].

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) that is designed to overcome the Internet Protocol version 4 (IPv4). IPv6 which is popularly known as the Next Generation Internet Protocol (IPng) was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated IPv4 address exhaustion, and is described in Internet standard document RFC 2460.

In 1992, the Internet Engineering Task Force (IETF) recommended that internet number resources must be managed by subsidiary organizations at a regional level. Thus making a committee known as Regional Internet Registries (RIRs). These RIRs was responsible for the regional allocation and managing the role in cooperation with IANA (Internet Assigned Numbers Authority). There are five RIRs namely APNIC (Asia Pacific Network Information Centre), RIPE NCC (Reseaux IP Europeens Network Coordination Center), LACNIC (Latin America Caribbean Network Information Centre), ARIN (American Registry for Internet Numbers) and AfriNIC (African Network Information Centre). Figure1. Below shows the committee operated by IANA.

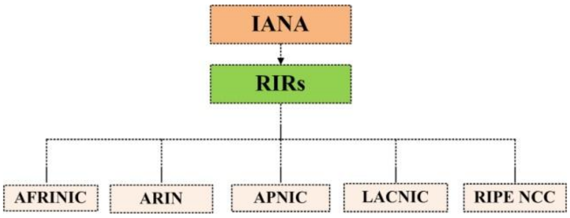

Figure1. IPv6 Registries

The table below shows the report of IANA Unallocated Address Pool Exhaustion generated on 10th Jan, 2012 [11].

Table.1 Unallocated Address pool exhaustion

RIR	Projected Exhaustion Date	Remaining Address in RIR pool (/8s)
APNIC	19-Apr-2011	1.2023
RIPENCC	22-Jul-2012	3..2110
ARIN	09-Jul-2013	5.6788
LACNIC	30-Jan-2014	3.8878
AFRINIC	02-Oct-2014	4.3534

The main difference between IPv4 and IPv6 points to their addressing formats. “IPv4 uses only 32 bits (4 bytes) for an Internet Protocol address, and can therefore support 2^{32} (4,294,967,296) addresses, where as IPv6 uses 128-bit (16 bytes) addresses, so the new address space supports 2^{128} addresses. This expansion allows for many more devices and users to connect on the internet as well as provides an extra flexibility in allocating addresses and efficiency for routing traffic" [12].

IPv6 has been developed based on the past experience we have with IPv4. It has been implemented and tested intensely up to the network layer. It takes everything that was amazing about IPv4 and added flexibility to extend it, to make it the network protocol of the future. IPv6 is capable of handling the Internet growth rate and to support the new types of services, especially in the area of mobility that we have to expect in the coming years.

IPv6 includes a transition mechanism which is designed to allow users to adopt and deploy IPv6 in a highly diffuse fashion and to provide direct interoperability between IPv4 and IPv6 hosts. The transition to a new version of the Internet Protocol must be incremental, with few interdependencies.

2. Overview and Limitation of IPv4

This paper describes the current version of Internet Protocol which is popularly known as Internet protocol version 4 (IPv4). IPv4 is the fourth version of TCP/IP suit which is widely in used from the past 25 years [1]. As this version (IPv4), did not participated in the growth of internet and had stood the test of scaling to a global utility of the size of internet today. IPv4 was not initially designed to support a very high number of network equipment which does not handle the address space requirements of the ever growing internet. As the reason for the exponential growth of internet, IPv4 is unable to satisfy the huge increase in number of users on the geographical needs of the internet expansion. As a result IPv4 address depletion is approaching quickly due to emerging applications such as internet enabled PDAs, home area network, mobile Ad-hoc network, IP wireless services etc required a new Internet Protocol.

This paper gets across the technologies that are used for the lifetime extension of IPv4 are listed below:

i. **Network Address Translation (NAT)**: NAT exists between the public and the private networks. Which means the host inside the private network is given the private addresses that are not reachable by the internet. It is useful only when communication is needed between the host in the private network and another host in the internet.

ii. **Classless inter-domain routing (CIDR):** It is the address scheme that uses aggregation strategies to minimize the size of top level internet routing table, where routers are grouped with the objective minimizing the quantity of information carried by the core routers. The main requirement for this scheme is use of routing protocols such as the Border Gateway Protocol version 4 and RIP version 2

iii. **Dynamic Host Configuration Protocol (DHCP):** DHCP is a TCP/IP protocol that enables assignment of temporary IP address to a host automatically when host connects to the network

This paper depicts the existence of these techniques seem likely to increased size of address space which fails to meet the following requirement:

i. Inadequacies in IP address space**.**
ii. Data security.
iii. Configuration complexity.
iv. Quality of Service (QoS)

We discussed the transition of IPv4 to the new version protocol to provide enhance features and to solve the IP address exhaustion problem that emerges to the Internet Protocol version6 (IPv6).

3. IPv6 Features and Benefits

We also illustrate the design of IPv6 to meet the requirement of the potentially huge internet expansion. With the feature like autoconfiguration and plug-and-play support technology, all other network enabled devices will be able to connect to the network without manual configuration as well as without bootstrap services as DHCP service. The existence of the IPv6 protocol shows the work of many different Internet Engineering Task Force (IETF) proposals, working in groups and represents their several years of efforts. IPv6 was designed to adapt the existing features of IPv4 and provide the following benefits to the network in IT professionals with the new services capabilities like:

i. Larger address space for global reachability and scalability. This states the extend of IP address space enough to offer a unique IP address to any new device which results in almost unlimited number of IP addresses.

ii. Simplified header format which is used for efficient packet handling. Where some of header fields have been removed as well as some new field have been added and modified the name in IPv6 to improve the efficiency. As the figure below gives the clear idea of this header format.

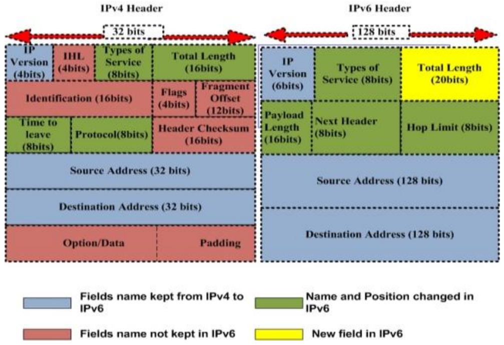

Figure 2.Header Format of IPv4 and IPv6

iii. The hierarchical network architecture is used to optimize the routing and to improve efficiency the efficiency of the network.

iv. In IPv6, ICMP protocol is revised and named it as ICMPv6 which includes new function to support autoconfiguration, neighbor discovery and multicasting.

v. Additionally IPv6 offers increased in number of Multicast addresses and will not use broadcast address leading to better performance on the network.

vi. The other important benefit of IPv6 is the Embedded Security that enables mandatory IP Security (IPsec) implementation which is optional in IPv4 making the network more secure.

vii. Improve support for IP Mobility [2].

4. How IPv4 differs from IPv6

As we, already discussed that IPv6 header is simpler and more efficient than the IPv4 header. The main difference of IPv4 header has 13 fields where as IPv6 header has only 8 fields with the fixed length. There are several improvements and updates over its predecessor (IPv4). It provides with a better features compared to IPv4 such as listed below:

i. **Great number of Addresses:** As IPv6 is the next generation Internet Protocol has 128 bits of address space, which is greater than IPv4 that can be used for many years.

ii. **Simple header format: T**his describe IPv6 headers field are lower than IPv4 which are optional to reduce the cost of packet handling and to keep the bandwidth cost low as possible.

iii. **Security and Authentication:** IPv6 provides an authentication on packets delivery and supports various security features by default.

iv. **Quality of Service (QOS):** In this service high priority packets arrived at their destination in such a way to provide quality. For example in video or audio streaming packets must arrive at destination closely as delay of a single packet that could make interference. The table below shows the difference between the current IPv4 and IPv6.

Table 2. Comparison of IPv4 and IPv6

IPv4	IPv6
1. Sources and destination addresses are 32 bits in length.	**1. Sources and destination addresses are 128 bits in length.**
2. IPSec support is optional	**2. IPSec support is required.**
3. No identification of packet flow for QoS handling by routers is present within the IPv4 header	**3. Packet flow identification for QoS handling by routers is present within the IPv6 is using the Flow label field.**
4. Header includes a checksum.	**4. Header does not include a checksum.**
5. Header includes options.	**5. All optional data is moved to IPv6 extension headers.**
6. Must be configured either manually or through DHCP for IPv4.	**6. Does not require manual configuration or DHCP for IPv6**
7. Broadcast addresses are used to send traffic to all nodes on a subnet.	**7. There are no IPv6 broadcast addresses. Instead a link-local scope all-nodes multicast address is used.**

5. IPv6 Addressing

This paper educates one to learn and recognize the IPv6 address syntax. The basic principle we need to remember is that the computer communicates through IP rather than the name. IPv6 addresses are written in the following format as given below:

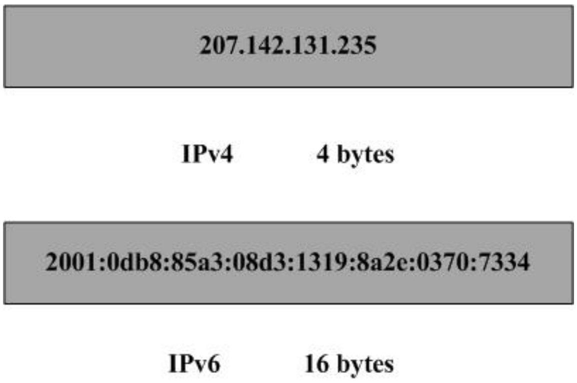

Figure 3.IPv6 address syntax

Unlike the IPv4 addresses, which are 32 bits long, written in decimal and separated by periods, IPv6 addresses are 128 bits long, written in hexadecimal. The most importantly these octets are separated by colons (:).

For example the IP address in IPv6 will look like in this form: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

Here the colons are separated by 16-bits field. The leading zeros can be omitted in each field when you find 0003 which can be written :3: as given in the above example.

Also a double colon (::) can be used in an address to replace multiple fields of zeros. For example: fe80:0:0:0:200:f8ff:fe21:67cf which can be written as fe80::200:f8ff:fe21:67cf

5.1. Types of IPv6 Address

This paper also discriminates between the different IPv6 address types. Generally IPv6 addresses are categorized into the following types.

5.1.1. Unicast

This address uniquely identifies an interface identifier (IID) of an IPv6 node. A Packet sent to a Unicast address is delivered to the single interface identifier by that address. This Unicast address can be divided into different types of addresses which include:

i. **Global unicast** addresses, are the conventional, publicly routable address, just like conventional IPv4 publicly routable addresses which split into 2 parts of 64 bits each one is network identifier and the other will be interface identifier.

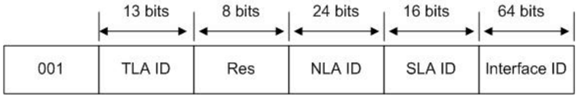

Figure.4 Structure of Global Unicast Address

ii. **Link-local** addresses are similar to the private, non-routable addresses in IPv4 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). They are not meant to be routed, but confined to a single network segment. Link-local addresses mean you can easily throw together a temporary LAN, such as for conferences or meetings, or set up a permanent small LAN the easy way.

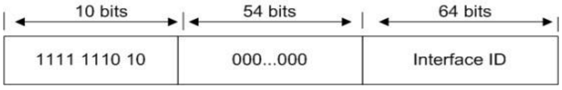

Figure.5 Structure of Link-Local Address

iii. **Unique local** addresses are also meant for private addressing, with the addition of being unique, so that joining two subnets does not cause address collisions.

iv. **Special addresses** are the loopback addresses, IPv4-address mapped spaces, and 6-to-4 addresses for crossing from an IPv4 network to an IPv6 network.

5.1.2. Multicast

This address identifies the group of IPv6 interfaces. A packet sent to a multicast address is processed by all members of the multicast group.

5.1.3. Anycast

This address is assigned to multiple interfaces on a multiple node. A packet sent to an Anycast address is being delivered to only one of these interfaces mostly to the nearest one [15].

6. Transition Mechanism

As we discussed that the internet is consists of more than thousands of network and millions of IPv4 nodes resulting in shortage of IPv4 address for all the IP enabled devices running on the internet. While it is also possible that the IPv6 only networks will be deploy rapidly in the near future. Therefore it would be more common for IPv4 and IPv6 to be worked together on the same network infrastructure. To facilitate this co-existence and the necessary integration tools are required during the migration period.

To achieve this, we adapt wide range of techniques which are identified and implemented. The three main categories are:

i. Dual-Stack techniques
ii. Tunneling techniques
iii. Translation techniques allow IPv6-only nodes to communicate with IPv4-only nodes.

6.1. DUAL STACK

In this technique the name itself explain the two protocols which can operate in parallel to coexist in the same devices and allow network mode to communicate either via IPv4 or IPv6.

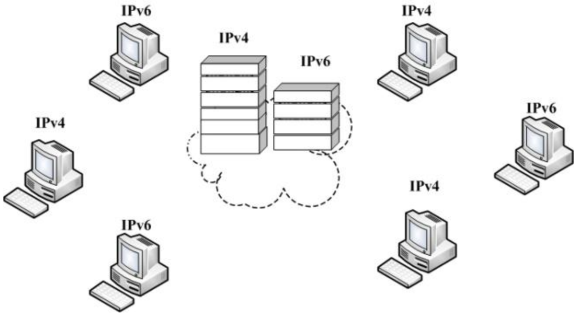

Figure.6 Dual Stack Infrastructure

The dual-stack protocol implementation in an operating system is a fundamental IPv4-to-IPv6 transition technology. It implements IPv4 and IPv6 protocol stacks either independently or in a hybrid form. The hybrid form is commonly implemented in modern operating systems supporting IPv6. Dual-stack hosts are described in RFC 4213. The modern hybrid dual-stack implementations of IPv4 and IPv6 allow programmers to write networking code that works transparently on IPv4 or IPv6. The software may use hybrid sockets designed to accept both IPv4 and IPv6 packets. When used in IPv4 communications, hybrid stacks use an IPv6 application programming interface and represent IPv4 addresses in a special address format, the IPv4-mapped IPv6 address. The structure of dual stack is show in the figure below [4].

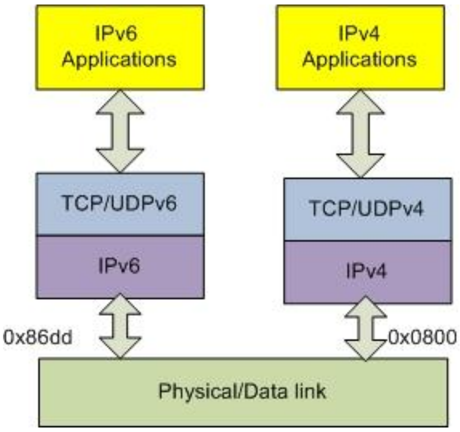

Figure.6 Structure of Dual Stack

6.2. TUNNELING

This paper illustrates the technique which allows the transport of IPv6 traffic over the existing IPv4 infrastructure. The mechanism used to reach IPv6 internet with an isolated host or network using the existing IPv4 infrastructure to carry IPv6 packets is known as Tunneling. It is the encapsulation of Ipv6 packets with an Ipv4 header so that Ipv6 packets can be sent over an IPv4 infrastructure. The Tunnel destination address is specified in the tunnel source configuration creating a P2P topology.

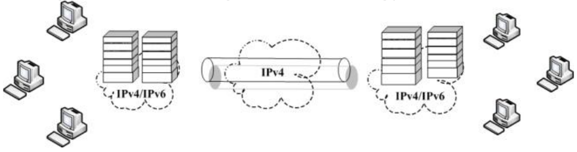

Figure.7 Structure of Tunneling

Thus this mechanism is very simple to deploy. The different types of tunneling mechanism are being classified into [5]:

6.2.1. 6-OVER-4

We discuss how IPv6 packets can be automatically encapsulated over an IPv4 network in which the IP multicast service is enabled so that IPv6 sees the entire network as a single LAN (Local Area Network). This solution poses scalability problems, and is hampered by the fact that the IP multicast the service which is not yet available on the Internet [6].

6.2.2. 6-to-4

We elaborate the method used for constructing IPv6 addresses automatically from IPv4 addresses which is an improvement over the use of IPv4-compatible addresses. This technique makes it extremely easy for IPv4 "islands" located in an IPv4 network to communicate with each other. However, a number of problems remain for communication between an isolated IPv6 network and the IPv6 Internet, which is developing on the basis of a unicast addressing approach other than that forecast by 6-to-4 [7].

6.2.3. IPV6 TUNNEL BROKER

It is an approach that involves using dedicated servers which automatically configure tunnels on behalf of users. This technique is particularly suitable for connections between small users and an IPv6 Service Provider. The IPv6 Tunnel Broker provides an automatic configuration service for IPv6 over IPv4 tunnels to users connected to the IPv4 Internet [8].

The tunnel broker manages tunnel requests from dual-stack clients and tunnel-broker servers, which connect to the intended IPv6 network. Dual-stack clients attempting to access an IPv6 network can optionally be directed via DNS name resolution to a tunnel broker web server for entry of authentication credentials to authorize use of the broker service.

6.3. TRANSLATION

We describe this mechanism which allows the IT professional to convert the packets from one protocol to another according to the requirement. The concept behind this approach is to allow communication between devices supporting any version. Translation approaches are generally recommended in an environment with IPv6-only nodes communicating with IPv4-only nodes. Several translation mechanisms are based on the SIIT (Stateless IP/ICMP Translation algorithm) algorithm and NAT-PT (Network Address Translation-Protocol Translation) mechanisms

6.3.1. STATELESS IP/ICMP TRANSLATION ALGORITHM

We discuss the SIIT algorithm used as a basis of the BIS (Bump in the Stack). BIS mechanism (RFC 2767) includes a TCP/IPv4 protocol module and a translator module, which consists of three bump components and is layered above an IPv6 module Packets from IPv4 applications flow into the TCP/IPv4 protocol module [9]. The identified packets are translated into IPv6 packets and then forwarded to the IPv6 protocol module. The three bump components are the extension name resolver, which examines DNS lookups to determine whether the peer node is IPv6-only; the address mapper, which allocates a temporary IPv4 address to the IPv6 peer and caches the address mapping; and the translator, which translates packets between IPv4 and IPv6 protocol.

6.3.2. NETWORK ADDRESS TRANSLATION-PROTOCOL TRANSLATION

This translation mechanism explains the translation done between IPv4 and IPv6 headers at the network layer. This allows the native IPv6-only hosts application to communicate with native IPv4-only host application. The NAT-PT mechanism is a stateful IPv4/IPv6 translator [10]. NAT-PT nodes are at the boundary between IPv6 and IPv4 networks. Each node maintains a pool of globally routable IPv4 addresses, which are dynamically assigned to IPv6 nodes when sessions are initiated across the Intranet. We also learned across the different mechanisms and solutions of transition. Planning and discussion are the only tools that can help to obtain smooth and better migration possible.

It is important to emphasize that migration success will depend, in addition to a great extent of the availability of software adapted to the new technology. This mechanism allows native IPv6 nodes and applications to communicate with native IPv4 nodes and applications, and vice versa. The NAT-PT mechanism is an interoperability solution that needs no modification or extra software, such as dual stacks, to be installed on any of the end user nodes, either the IPv4 or the IPv6 network. The mechanism implements the required interoperability functions within the core network, making interoperability between nodes easier to manage and faster to manifest

7. Conclusion

In this paper, we studied the Internet Protocol which is more extensively used throughout the world. This gives the review and awareness of the current internet protocol to the next generation protocol. The main aim for the development of new version of Internet Protocol happens due to the over exhaustion of available IPv4 address space. In addition, this also illustrates the comparative study between Internet Protocol version4 (IPv4) with the Internet Protocol version6 (IPv6). The discussion shows the importance of migration from IPv4 to IPv6 in the real networks using different transition techniques. This involves in adding many new features and necessary improvement to the current Internet Protocol version4 (IPv4).

8. References

[1] A Primer on IPv6, White paper, http://www.digi.com
[2] A white paper by 6WIND, “IPv6 Features and Benefits, March 2003
[3] Briefing paper Internet Society, “IPv6: Why and how government should be involved” in Jun, 2009.
[4] – [10] Han-Chieh Chao, “Performance Investigation of IPv4/IPv6 Transition Mechanisms”. http://hcc.dormv6.niu.edu.tw/~hccftp/journal30.pdf
[11] IPv4 address report http://www.potaroo.net/tools/ipv4/index.html
[12] IPv6 Introduction, http://en.wikipedia.org/wiki/IPv6
[13] IPv6 Transition guidance by Federal CIO Council, Architecture & Infrastructure in Feb 2006
[14] Ra’ed AlJa’afreh, ”Implementation of IPv4/IPv6 BDMS Transition Mechanism”, Second UKSIM European Symposium on Computer Modeling and Simulation.
[15] Silvia Hagen , “IPv6 Essentials”, published by O’REILLY