# The State of IPv6 Deployment: A global Review

Stephen Ugwuanyi, Fouead Attaran, Syeed Hussaini, Ahmed Merehil

**Abstract**— Reports on the depletion of internet address space by the Internet Assigned Numbers Authority, IANA since 2011 has been a major concern for both the network users and Internet Service Providers, ISP. This situation has pushed organizations and professional bodies to finding better transition strategies to move from IPv4 to the new protocol IPv6; which is an incompatible protocol with the IPv4. This perhaps, is one of the reasons which have affected the realization of the proposition that the internet would be fully migrated to IPv6 in 1999 in the Request for Comments, RFC 5211. This paper is an overview of this new evolved Internet Protocol IP, with emphasis on determining the level of IPv6 deployment in the world in terms of programme and devices that are now IPv6 enabled. The challenges faced with the various adopted transition mechanisms while describing the best practices in the deployment and gives an insight into the question if the IPv6 is now the backbone protocol of the world internet.

**Index Terms**—Architecture, Depletion, Deployment, Internet, Network, Protocol, Transition.

## 1 Introduction

INTERNET Protocol (IP) is the principal protocol in the communication suite of the internet. IP operate on the Network Layer of Open Systems Interconnection (OSI) and on the Internet Layer of Transmission Control Protocol/Internet Protocol TCP/IP model [1]. TCP/IP is a protocol which has been adopted over the years because of its user's requirement in allocating addresses to every device for recognition and dispreading packets on the Internet. The first IP used broadly is Internet Protocol version 4 (IPv4) but it has encountered some problems with growth due to the increasing number of user on the Internet. The depletion of the IPv4 protocol started in February, 2011 as the Internet Assigned Numbers Authority (IANA) allocated the last blocks from the global IPv4 address pool to the Regional Internet Registries (RIRs) [2]. Internet Protocol version 6 (IPv6) is the next generation of Internet Protocol which has been used globally because it eliminates the most important problems of IPv4.

Due to the massive development in Internet infrastructure, IPv6 is an up-to-date protocol that can handle the demands for new IP addresses by devices newly connected to the Internet, which are not only personal computers, laptops or tablets, but also Internet of Things (IoT) and Machine-to-Machine (M2M) devices such as sensors [3]. The rate of deployment of IPv6, the successor to IPv4 has taken time but has started to take a hold within both carrier network providers and ISPs.


- *Stephen Ugwuanyi is a master degree holder in Commuication, Control and Digital Signal Processing in University of Strathclyde, Glasgow G1 1XQ, United Kingdom (email: Stephen.ugwuanyi.2015@uni.strath.ac.uk)*
- *Fouead Attaran is a master degree holder in Electrical and Electronic Engineering in University of Strathclyde, Glasgow G1 1XQ. United Kingdom (email: fouead.attaran.2015@uni.strath.ac.uk)*
- *Ahmed Merehil is a master degree holder in Electrical and Electronic Engineering in University of Strathclyde, Glasgow G1 1XQ. United Kingdom (email: ahmed.merehil.2015@uni.strath.ac.uk)*
- *Syeed Hussaini is a master degree holder in Commuication, Control and Digital Signal Processing in University of Strathclyde, Glasgow G1 1XQ, United Kingdom (email:syed.sabeer.hussaini.2015@uni.strath.ac.uk)*


However, it is not clear how far the migration or adoption of IPv6 has been and the impact such changes have had on the typical network user - if any. Telecommunications carriers in both developing and developed markets have promised Next Generation IP based Networks (NGN) and IPv6 has often been the cited platform to enable the change to NGN deployment. The aims and objectives of this paper, therefore are:

1. To investigate the internet protocol evolutions from IPv4 to IPv6.
2. To investigate the quality of service parameters (QoS) of IPv6 and their effectiveness in the communication system.
3. To highlight the importance of IPv6.
4. To investigate the level of deployment with regards to IPv6 roll out, the associated technical challenges, and the impact on the telecommunication industries both established and emerging.

This paper is structured into three sections. First, is the general overview of the internet protocols with emphasis on the architecture, and various standardizations processes in IPv6. The second part discussed the various transition methods developed and adopted over the years in the quest to move from IPv4 to IPv6. The advantages and disadvantages of the various methods were identified. The final section of this paper looks at the level of deployment of IPv6 enabled devices and software in the world. This helped to ascertained if the architecture of communication industries is now fully a world of this new, faster, and more scalable, secure IP networks or is it just marketing hype or somewhere in between. Recommendations that could improve the rate of IPv6 deployment were highlighted.

## 2 IPv6 Internet Protocol and Architecture

IPv6 also known as IPng which is an abbreviation for (Internet Protocol Next Generation), as it is considered the newest version of internet protocols, has been deployed alongside the IPv4 networks. IPv6 was designed as an upgrade to internet protocol, as well as to continue to coexist with IPv4 along the

transition period. This is because of the advantages that IPv6 has in updating the internet protocol. It is configured to allow the growth of the internet steadily, in a consideration of number of hosts to the network and the amount of data being transmitted. The diagram below shows the position of IPv6 in the internet protocol suite.

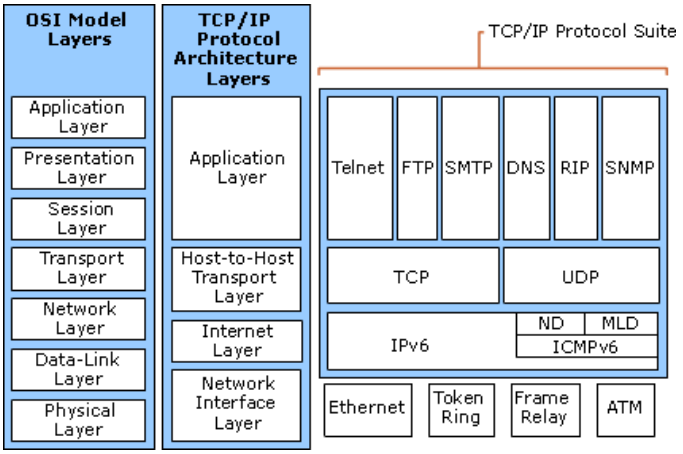


Fig. 1. Position of IPv6 in TCP/IP protocol suite [3]

IPv6 has been in the developmental process but became very important recently because of the depletion of IPv4. The motivation for IPv6 is the concern about the capacity for the IPv4 addresses being deployed every day and to be run out soon. Therefore, the increment of addresses by IPv6 is one of main benefits along other intriguing technical improvements in IPv6 to enhance the capability of IP in totality

### 2.1 Analysing IPv6 Network Architecture

The overall accomplishment of the Internet has brought about a blast of new clients and applications, and this development has set new requests upon the system base and upon system directors. In the mid-1990s, the IETF started to outline IPv6 with the goal of enhancing IPv4 to meet these new requests. The areas focused for development includes:

#### 1. Address Space Depletion

The consumption of IP locations has been anticipated for a long time and numerous patches and expansions have been added to IPv4 to reduce and delay the approaching emergency. Among those expansions are Variable-Length Subnet Covering (VLSM), Classless Inter- Domain Routing (CIDR), Network Address Translation (NAT), Port Address Translation (PAT), and private location spaces.

#### 2. Network Performance

The Internet has outgrown numerous elements in IPv4 that now hampers system execution. Among these some elements are header checksums, Maximum Transmission Unit, MTU size, and parcel discontinuity. IPv6 is streamlined to reduce convention overhead.

#### 3. Security

IPv4 was not outlined because of security. It was viewed as the obligation of higher layers in the Open Systems Interconnect (OSI) model. IPv6 gives incorporated security backing to encryption and validation. Plug and Play configuring hubs in an IPv4 system has been dependably entangled. Numerous setup assignments are physically escalated and not commonsense in vast systems. A valid example is the renumbering of a system when another internet administration supplier is chosen. The development of portable registering has likewise added to the workload of system directors.

## 3 IPV6 STANDARDISATION

The internet is fundamentally based on the existence of open, non-proprietary standards. They are key in allowing devices, services, and applications to work together across a wide and dispersed availability of networks. Today, one of the **biggest** mark indicators of success of these standards is how they are developed. The protocol which is expected to become the de facto standard for both local and global connectivity is expected to incorporate extra features, including increased processing speed, and an enhanced security and quality of service parameters [5]. However, the fast spreading use of the internet and new services such as mobile IP, IP telephony, and IP capable mobile telephony may eventually require the total replacement of IPv4 with IPv6 [6].

The development of this protocol lies on the Internet Engineering Task Force (IETF), a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the internet architecture and the smooth operation of the internet. Some of the core groups behind the development of the standards are the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), and the Internet Architecture Board (IAB) [7]. The standardisation efforts for this protocol began decades ago by a division of IETF, IPng Work Group, formally known as the IP next generation, through Request for Comments (RFCs) proposals [8].

The focus of the group was to simplify the IPv6 architecture, increase the address scale and, to create a simple transition plan, simplified configuration, and make it more secured in providing classless services. After examining several proposals, the IETF settled on IPv6, recommended in January 1995 in RFC 1752, sometimes also referred to as the Next Generation Internet Protocol [1]. Since then, several organizations, such as the IPv6 Forum, have been working towards its widespread implementation. By 2004, IPv6 was widely available from industry and supported by most new network equipment. Currently, the standardisation issues has been moved towards the issues of migration from IPv4 to IPv6 [9].

Other standardisation efforts includes the government policies by international organisations such as ITU, European Commission, Czech Telecommunication Office (CTU) to support interoperability of eGovernment services by overcoming technical challenges and supporting IPv6 [9]. The IPv6 forum of the European Telecommunication Standards Institute ETSI and the ITU at the Cohosts Global IPv6 Transition Test Event promoted the transition and adoption of IPv6 worldwide by the network equipment vendors, specialists in interworking and network interconnection, as well as Internet Service Providers (ISPs) [10].

However, this policy is yet to be fully embraced in the whole continent per the Government Enabled with IPv6 (GEN6) research conducted in the African continent. The survey "clearly demonstrate that IPv6 support on the content provider's site is being blatantly disregarded" [9].

## 4 IPV6 SUPPORT CAPABILITIES

The improvement made in specifying IPv6 protocol relative to IPv4 came with powerful new capabilities. These includes the additional security for packet filtering and intrusion management, increased address space, mobility support, improved multicasting, and updated explicit routing capabilities in IPv6 network infrastructure. The following are the major support capabilities in IPv6.

### 4.1 Security

The IPv6 security was developed to support interoperable encryption based security. IPv6 incorporates security into its architecture by introducing two optional extension headers: The Encrypted Security Payload (ESP) header and Authentication Header (AH). The two headers can be used separately or together to support many types of security functions.

Authentication Header (AH) is the heart of the Authentication process. The header is the integrity check value (ICV) field. The ICV is computed by the source and computed again by the destination for verification. This procedure provides both connectionless integrity and data origin authentication. Connectionless integrity detects modifications to the payload. Data origin authentication verifies the identity of the source of the data. The AH also contains a sequence number field that can be used to detect packet replay attacks, which tie up receiving system resources. By examining the sequence numbers, we can spot the arrival of duplicate IP packets.

Secondly, the Encrypted Security Payload (ESP) Header IPv6 can provide confidentiality by encrypting the payload. The IPV6 ESP header contains a security parameter index (SPI) field that refers to a security association telling the destination how the payload is encrypted. ESP headers may be used end-to-end or for tunneling. When tunneling, the original IPv6 header and payload are both encrypted and jacketed by outer IPv6 and ESP headers. Near the destination, a security gateway strips away the outer headers and decrypts the original header and payload. This encapsulation provides limited traffic flow confidentiality because a traffic analyzer may see the outer headers but not the inner encrypted header and payload. Security vulnerabilities is common to both IPv4 and IPv6. IPv6 address space of 128 bit as compared to a 32-bit address space in IPv4 makes IPv6 routers no longer perform packet fragmentation and reassembly by the communicating devices.

IPv6 has security as its major design criteria and with standards based in IPv6 protocols allowing secured network using TCP, ICMP, IPsec, SEND etc. to support additional extensions such as authentication, data integrity, and data confidentiality in IPv6. Examples of such security capabilities include the use of Internet Protocol (IPsec), High Assurance Internet Encryptor (HAIPE), Secure Neighbour Discovery (SEND), cryptographically generated addresses (CGA), special purpose addresses, port filtering, firewalling, and Network Behaviour Anomaly Detection (NBAD) [11].

### 4.2 Mobility

Handover is the most important function of mobility management. In heterogeneous networks overlapping areas, seamless handover means not only the continuous data transmission but also the selection of the appropriate target access network and handover strategy at appropriate time. Therefore, the handover control function should be able to adapt itself to dynamic network environments and various QoS requirements. The stateless address auto-configuration capability was introduced to automatically configure IPv6 addresses on new network reduces the administrative burden of manual configuration. These implies that the use of Internet Control Message Protocol (ICMP) was now required [12].

### 4.3 Addressing Scheme

The Internet has grown from a research based closed network to a social network used by everyone today and has become the largest economy in the world [12]. IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. And a new type of address called an "anycast address" is defined, used to send a packet to any one of a group of nodes.

The massive address space of IPv6 means that every networked element can have a globally unique address, enabling seamless end-to-end secure communication without Network Address Translation (NAT). Removing NAT simplifies the network design, and improves the reliability, functionality, and manageability of the network. The responsibility for managing the IP resources today is delegated from a global level authority namely the Internet Assigned Numbers Authority (IANA) through regional organizations namely the RIRs and ultimately to individual ISPs [13].

### 4.4 Header Format Simplification

Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header. Improved support for extensions and options changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

### 4.5 Flow Labeling Capacity

A new capability is added to enable the labeling of packets belonging to traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.

## 5 IPV6 QUALITY OF SERVICE (QOS)

The quality of service depends on several services that are provided by the network while sending packets between a source and destination nodes [14]. There are different metrics proposed to measure the QoS provided on a network. Most

are defined by the working group IP performance metrics, which include variables such as the amount of data that can be transmitted in a time unit (bandwidth), amount of data transmitted per second (throughput), cost, probability of loss delay, and delay variation (jitter) which measures the delay experienced between the packets that come across the same route network and others [15].

The delay could be propagation delay; the time taken to pass a bit through a link, processing delay; the elapsed time to process a packet in a node and queuing Delay; the time-out for a packet in the queue before being transmitted. The packet loss and average delay is lower in IPv6 as shown in table1.

Table 1. Quality statistics for IPv4 and IPv6 experiments [14]

| | Packet Lost | Average Jitter | Max. Jitter | Average Time |
|---|---|---|---|---|
| IPv4 | 32% | 101 | 137 | 220 |
| IPv6 | 13% | 16 | 103 | 30 |

Other metrics includes the flow label and the traffic class. Flow label field in the IPv6 header which has the size of 20 bits is used to identify the packets routed across the network. However, it is still under supervision and subject to change as the requirements for flow support in the internet become clearer. Some types of hosts or routers do not support the flow label field function. These hosts or routers are required to set the field to zero. Flow label field in IPv6 solves the problem of violation of layer in which a router needs access to the transport-layer protocol or application to process the packets instead of using only the data from the network layer [16]. The 8-bit traffic class field in IPv6 is used by source or a router to identify the difference between the classes or priorities of IPv6 packets. The nodes use the traffic class field in the IPv6 header to make this identification. The routers that forward the packets also use the traffic class field for the same purpose.

The following general requirements apply to the traffic class field: The service interface to the IPv6 service inside a node must supply the value of the traffic class bits for an upper layer protocol, the traffic class bits must be in packets that are originated by that upper layer protocol. The traffic class bits in a received packet might not be the same value that is sent by the packet's source. Therefore, the upper layer protocol must not assume that the values are the same. The reasons for the development of the new version of the internet protocol were the exhaustion of the address space, the growth of the backbone routing table, security issues, IP options size limitation, and routing performance.

### 5.1 More efficient address space allocation

IPv6 has $2^{128}$ bits different IP addresses available for possible network devices to be connected in the network. IPv6 address uses the last 64 bits to describe the host ID for a system on a network and the last 64 bits of the address to distinguish hosts from one another on the same subnet. Whether using the link-local, site-local, or globally routable unicast address format, the last 64 bits on a machine will remain the same. This is because IPv6 uses the Layer 2 Media Access Control (MAC) address as the host ID for a machine (the Layer 2 MAC address is the address that is burned into all Layer 2 hardware, such as Ethernet cards and other Network Interface Cards).

Since MAC addresses are only 48 bits long. This limits the number of addresses that can be used because there will rarely be 264 addresses in use on a typical Ethernet LAN. Some address space gets wasted. However, if the 64 bits used for host ID is removed and the first three bits is used to designate globally routable unicast addresses, then 261 possible addresses (2.31E+018) will be achieved. So even without using all the addresses that IPv6 has available, IPv6 still the scaling ability to take the internet well beyond the future of IPv4. Clearly, IPv6 frees up our ability to use addressing efficiently without having to worry about running out of addresses.

### 5.2 End to end addressing

IPv4 used the class full IP assignment rules. This was followed by method based on the principles of Classless Inter-Domain Routing (CIDR). IPv6 is a new method that is meant to redesign the de-aggregation problems associated with each of these by splitting the IPv6 address into a set of definite scopes in which IPv6 addresses are delegated. The format, Prefix is used to show that an address is globally routable, unicast, or another type of address, and is always set to the same value. This allows a routing system to quickly discern whether a packet is globally routable, unicast or some other type.

### 5.3 Fragmentation only by the source host

In IPv6 header file, there are a few control fields which were added to perform the fragmentation, by using the flags. It is useful in understanding the number of the packet fragmentation and which the last fragment of the data flow is. The fragment offset indicates the fragment position in the original datagrams. The flag field has the responsibility to identify each unique and original fragment of the datagram.

### 5.4 Routers calculation of header checksum (speed up)

The checksum field in IPv4 header file was removed in IPv6. This is because the early networks were slow and unreliable connections, thus computing the checksum at each hop was necessary for ensuring data integrity. While today's network links are much faster and reliable, that only the hosts performs checksum not the routers.

### 5.5 Multicasting instead of broadcasting

To use multicast instead of broadcast in IPv6, multicast group is an arbitrary group of receivers that want to receive a data stream. The environment of multicast contains the senders and receivers, where every host can send to any specific group, while only the members of that group could receive the message.

### 5.6 Built-in security mechanism

One of the reasons of developing IPv6 was security. IPv6 added security features into network architecture by presenting two optional spread headers: The Authentication Header (AH) and the Encrypted Security Payload (ESP) header. These two headers can be used together or separately to support many

types of security functions.

### 5.7 Internet Control Message protocol (ICMPv6)

Internet Control Message Protocol (ICMPv6) is an integral part of IPv6 which performs error reporting and diagnostic functions. It also has the framework to add any implementation for future work. Neighbor Discovery Protocol (NDP) is a node discovery protocol in IPv6 which replaces and enhances functions of ARP.

### 5.8 Auto configuration

IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbour discovery protocol via ICMP router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains internet layer configuration parameters [17]. Routers present a special case of requirements for address configuration, as they often are sources of auto configuration information, such as router and prefix advertisements.

### 5.9 Modeler header structure

IPv6 header is simpler and more streamlined than the IPv4 header. The new header has only six fields and two addresses, while an IPv4 header contains ten fixed fields, two addresses, and a variable-length options field. The disadvantages include;

1. Difficult to remember the IP addresses
2. Creating a smooth transition from IPv4 to IPv6
3. IPv6 is not available to machines that run IPv4
4. Consumers costs in having to replace an IPv4 machine
5. Time to convert to IPv6.

### 7.3 Transition Strategies

Translation enables conversion of protocol semantics and syntax between IPv4 and IPv6 allowing hosts of different IP versions in different network to communicate with one another. The transition between today's IPv4 internet and the future IPv6 is in progress but not straightforward and needs guidelines to simplify and standardize transition between the two versions.

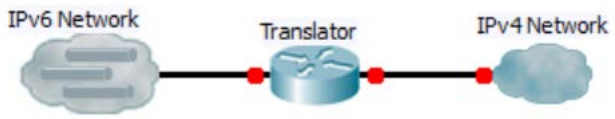


Fig. 2. IPv6 to IPv4 Network

As shown in figure 2, the translation process converts the IPv4 header into an IPv6 header when it receives an IPv4 packet destined to an IPv6 network. The transition of the internet protocol from IPv4 to IPv6 has been a major concern for the IETF. Series of strategies for IPv6 transition solutions have been proposed of which many are yet to be deployed for an evaluation to determine their seen success in real world [18]. However, the drive for IPv6 transition solutions are still continuously being worked out with management as one of the major differences among them. This has resulted to non-realization of the set date for an IPv6 world.

However, it is not all that feasible to just switch everything over to IPv6 without some type of transition. This paper recognizes transition as a major problem in moving from IPv4 to Ipv6 [17]. IPv6 transition mechanisms are the technology that facilitates the transition of internet from its initial and current IPv4 infrastructure to the successor addressing and routing system of IPv6. As IPv4 and IPv6 networks are not directly interoperable, these technologies are designed to permit hosts on either network to participate in networking with the other network. To meet its technical criteria, IPv6 must have a straight forward transition plan from the current IPv4. Internet Engineering Task Force (IETF) conducts working groups and discussions through the IETF Internet Drafts (ID) and Request for Comments (RFC) processes to develop these transition technologies towards that goal [17]. These will help to overcome the issues of scalability and other problems where IPv6 is the only access networks deployed while the majority of internet services remain in IPv4.

### 5.10 Dual-Stack

In this method, the way of communication is simultaneously done between IPv6 and IPv4 despite which protocol is used, then the traffic has reached the node or the router would respond immediately. This technique uses the IPv6 and IPv4 in parallel inside the same stack. The choice is given by the policy of the administrator, as to the type of the service is demanded, and which network is needed. This technique does not change the packet header and it does not create an encapsulation between the IPv6 and IPv4, and this is known as Native Dual Stack [2].

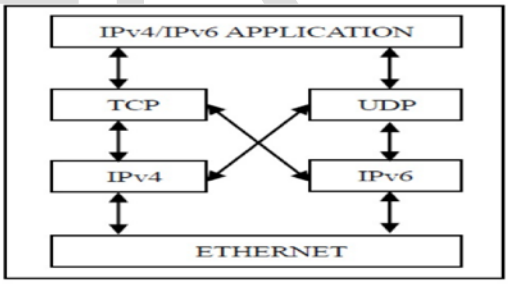


Fig. 3. Dual-Stacks

Regarding to [3], the internet has many nodes that support the service of both protocols combination ability between IPv6 and IPv4 in parallel within the same nodes infrastructure so that the node can provide the transfer of packets and their data for IPv4 and IPv6 protocols. Yet this method is not well fitted to the bigger networks due to the difficulty and expensive coverage to every node in the networks. In addition, it is very suitable to small networks, which have less management and very easy to control and deploy.

### 6.2 Tunnel

This method is used when there are two same networks with the same IP protocol and yet their connection is through another IP protocol connection. The tunneling strategy creates a virtual link to get to the required IP network. Tunneling method can be in two ways, either automatic or manual. Auto-

matic connection is a point-to-multipoint where the operator assign the source address as well as the destination address automatically. On the other hand, the manual connection is a point to point method, which in a way is to assign the source and destination address by the operator for the tunnel. The tunnel aspect works like a bridge between similar networks to transfer packets over incompatible network [4]. Moreover, the IPv6 will be part of IPv4 and the data of IPv6 will go through the infrastructure of IPv4. In totality, tunnel is a virtual connection between two points that transfer data, and process it [5].

Figure 7: Tuning mechanisms of IPv6.

### 6.3 Translation

This method is like the Network Address Translation (NAT), for changing from IPv4 to IPv6 under a condition of the source and destination type [1].

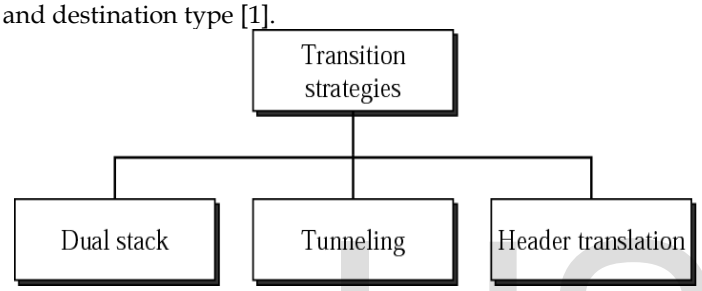


Fig. 8. Transition Strategy

Translation has the method of changing the payload and the header of the IP packet from the version 6 to version 4 and vice versa, and it has two methods of translation; stateless and state-full. Stateless operation has no reference from the last packet during conversation, while in state-full conversation, packet is attached [6].

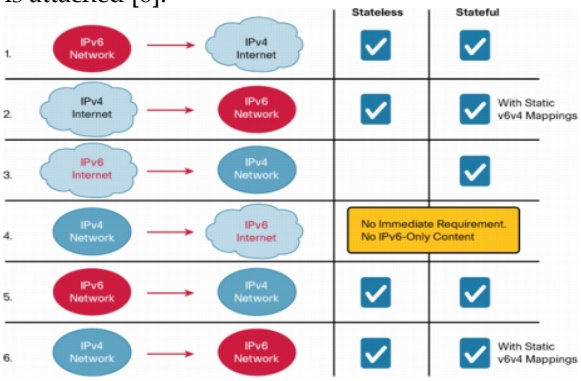


Fig. 9. Transition between IPv4 and IPv6

## 6 Chanllenges in Ipv6 Transition

The transition from IPv4 to IPv6 has been faced with many challenges. After decades of development by the IETF, the basic IPv6 protocol became mature enough to replace IPv4 [19]. However, due to the incompatibility of IPv6 packet headers with IPv4, network devices and host devices must be upgraded to support IPv6. The transition and evolution to IPv6 were expected to complete in three stages. The first stage started with the deployment of IPv6 from the IPv4-based network. Second was for IPv4 and IPv6 to coexist in one network and the third stage is where IPv6 plays a leading role on the network and the IPv4 network is gradually retired. The figure below is a detailed illustration of roadmap to transit from IPv4 to IPv6.

Figure 10: Roadmap from IPv4 to IPv6

The internet is currently in the second and third stage of the transition process as shown in the figure 11 below. Among these mechanisms, dual stack is the simplest and easiest to deploy, and the remaining two are applicable only to specific situations.

Figure 11: Approaches to IPv6 Transition

The transition mechanism requires the deployment of software and hardware components at both the last-mile and the edge networks. These different mechanisms and the associated equipment pose new challenges. They range from lack of a unified scheme that supports these mechanisms to it becoming more challenging when because there are many devices on the current IPv4 networks. The cost of replacing these huge amounts of resources and the fact that the system cannot tolerate any down time in the services irrespective of the type of services they provide remains a future challenge.

A unified and flexible approach is necessary for the success of IPv6 transition. Software Defined Network (SDN) approach enables the IPv6 Transition Services Module, ITSM to program SDN-enabled equipment to tunnel IPv6 traffic across an IPv4 data plane, by letting the controller to translate the commands issued by the ITSM into a form that can be executed. SDN-enabled equipment provides a perfect supporting mechanism for unifying the existing transition protocols to address the challenges of transitioning from IPv4 to IPv6 in a cost-effective manner. It demonstrates that low complexity, high flexibility and low cost are achievable in addition to incurring low complexity and low cost to network carriers. Also, this approach does not allow end users to upgrade their software or hardware equipment to transition from IPv4 to IPv6, if the network equipment is SDN compatible.

## 7 Deployment Level of Ipv6

The introduction of IPv6 to the networking protocol since early 90's opened up several questions within the networking industry with respect to its adaption rate and various transition mechanisms from IPv4 to IPv6. This study has shown that IPv6 is a more efficient, and future oriented protocol that will provides additional seamless services that were not part of its predecessor protocol, IPv4. The practices within the industries shows that IPv6 is a defacto standard at present and is currently being deployed in almost all the Internet architecture worldwide wide great disparity across the various continent.

Many technologies such as NAT and CIDR have been de-

veloped to facilitate the rapid deployment but have been faced with the economic aspect of the transition. The key players of this sector, the ISP, have resorted to using many sub-netting strategies to continue to provide various services while compromising the scalability of the industries. Most of the hardware and software are IPv6 enabled and the decision of what, when, and how to move from IPv4 to IPv6 still depends upon the type of the network, the network providers, and the Government regulation of a country or region.

The three basic aspects involved in the deployment of IPv6 are; the protocol, the products, and the adoption rate.

### 1. IPv6 Protocol

IPv6 has benefited a lot from the Internet Engineering Task Force (IETF). The core standards have been stable for many years and deployed in both research and operational contexts. This aspect mainly emphasizes on the core specifications which includes the development of architecture, addressing, packet size etc. In addition to the core specifications, IPv6 protocol includes a large number of individual standards like the new updates in the quality of service and the security standards. Thus, even though the core IPv6 specifications are stable, there would be a continuous research regarding IPv6-related specifications.

### 2. IPv6 Product

The core IPv6 specifications are becoming increasingly available as a standard part for the products. However, not all products are fully IPv6 capable at this time and some significant upgrade gaps remain in the devices, especially in low-end consumer equipment. Similarly, while many software applications and operating systems especially in open source code have already been updated for IPv6, not all products including some from major vendors are fully IPv6 ready. Therefore, to deploy IPv6, supports of the products play a crucial role.

### 3. IPv6 Adoption

The networks that were built up for the IPv4 must be adopted for IPv6. There is a strong growing experience in the deployment of IPv6 in research networks and R&D projects, while some production networks (primarily in Japan and Korea) have been running IPv6 for several years. Today in internet traffic, IPv6 remains small in comparison to IPv4. As seen in previous studies [4], in December 2008, despite IPv6 marking its 10th anniversary as a Standard Track protocol, IPv6 still lacked behind in the usage of addresses and the traffic in the publicly accessible internet which was still dominated by IPv4 [4].

A study by Google, reported in November 2008 [20] indicating that penetration was still less than one percent of internet traffic in any country. The leaders were Russia (0.76%), France (0.65%), Ukraine (0.64%), Norway (0.49%), and the United States (0.45%). Although Asia led in terms of absolute deployment numbers, the relative penetration was smaller (e.g., China: 0.24%). By 2011, all major operating systems in use on personal computers and server systems had production-quality IPv6 implementations. Cellular telephone systems present a large deployment field for Internet Protocol (IP) devices as mobile telephone service is making the transition from the third generaton to the the new generations technologies.

By March 2014, 448 (92.8%) of the 483-leading domain level in the internet, supported IPv6 to access their domain name servers, and 441 (91.3%) zones contained IPv6 access information and approximately 5.7 million domains (3.4%) had IPv6 address records in their zones. Of all networks in the global routing table, 17.4% had IPv6 protocol support [21].

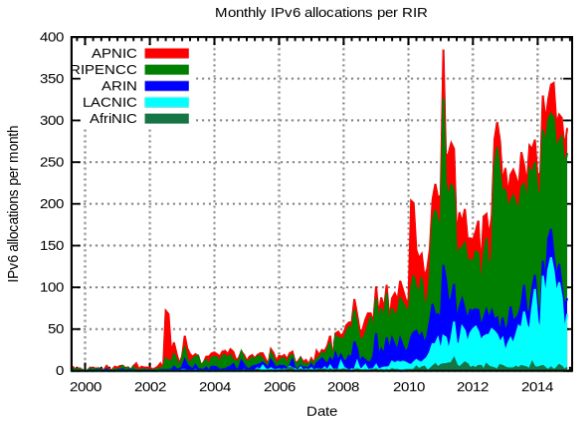


Figure 1: A graph of IPv6 allocation since 2008 [22]

At present Belgium tops the list in the IPv6 enabled users, USA comes after Switzerland in third position and United Kingdom ranks in 31st position worldwide [23]. World IPv6 Day was announced on January 12, 2011, this was a technical testing and publicity event in 2011 sponsored and organized by the Internet Society and several large content providers to test and promote public IPv6 deployment.

Internet Society: World IPv6 Launch on June 6, 2012, to bring permanent IPv6 deployment, there were more than 400 participants in the original World IPv6 Day included some of the most heavily accessed destinations on the Internet, content distribution networks as well as various Internet service and infrastructure providers such as Google, Facebook, Telmax, and BBC. The test primarily consisted of websites publishing AAAA records, which allow IPv6 capable hosts to connect using IPv6. Following the success of the original World IPv6 Day, the exercise was repeated on June 6, 2012 as the World IPv6 Launch, this time with the intention of leaving IPv6 permanently enabled on all participating sites.

IPv6 enabled users in UK from 2008 to present is nearly 2.48% of total UK population as suggested by the Google [23]. Several major UK Universities and Colleges such as Cambridge and Esher College upgraded their campus routing infrastructure to provide IPv6 unicast support to their users. Andrews & Arnold launched a native IPv6 service in October 2005 and offer IPv6 by default. The UK Government started to replace much of its Government Secured Intranet (a wide-area network) with a new Public Services Network (PSN). The aspiration was to deploy using IPv6 and support IPv4. The implementation is based on IPv4 but supplier's must can support IPv6 [24].

*Secure Deployment of IPv6:*

The main intention while in the process of level of deployment is to maintain the element called the functional parity with the present services and networks. This is a part which focuses on this

goal. Deployment's primary intention is to integrate IPv6 with an existing IPv4 environment while maintaining, if not enhancing, the existing level of security. This section can be characterised as: [25]

### *A.* *Security Risks*

Security risk is a section which gives important information of risks that organizations may face when moving from an IPv4 to IPv4/IPv6 and eventually IPv6 environment. The deployment of IPv6 is inevitable. Exhaustion of the IPv4 address space literal solution and the only long-term solution is to deploy IPv6. To deploy IPv6 transition of network is very important concern. IPv6 is not backwards compatible with IPv4, which means organizations must change their network infrastructure and systems to deploy IPv6. IPv6 has a huge impact in changing the whole network of organisations. Major vendors or organizations must start to think and understand about the transition technologies and the strategies of risk mitigation. This can be achieved by effective planning by respective organisations to make a smooth, secure and successful transition [27].

Organisation may face some general risks and they are as follows:

- Immense use of IPv6 by the community of attackers.
- Unauthorized deployment of IPv6 on existing IPv4 production networks
- IPv4/IPv6 dual operations have high complexity.
- IPv6 network has some sort of vulnerabilities that may cause some of the risk.
- Immaturity of IPv6 security products and processes
- Inconsistent support by the organisations or vendors. [25]

### **B.** *Addressing Security*

Lot of organisations and administrators usually conclude the operational issue of IP addressing. The numbering plan can also affect the organization's security posture. Some of the primary organisations portray the addressing structure and the function of a network. These are some of the features that were employed in reducing the threats to security and privacy in IPv6 addressing:

- Management of addressing
- Extension sequences of privacy
- Consequence numbering strategy of RFC's.
- Matter of addressing of EUI-64 during security concern
- Design of the system to make security compatible [25].

*IPv6 Implementation*:

The transition deployment can be done by following two strategies and are

1. Pervasive IPv6 deployment
2. Sparse IPv6 deployment.

As far as pervasive approach is concerned, dual stack is a major impact where the organizations have huge role to play. They help in enterprising the dual nature of IPv4/Ipv6. This type of method is only impeccable only when the new devices have compatibility on both IPv4 and IPv6 networks. This si only possible when they are working properly in a efficient manner. After confirming that the services and translation mechanisms are functioning properly, IPv4 is disabled on all equipment, leaving an IPv6 dominant network [26].

IPv6 pervasive and sparse deployments are different from each and their differences can be stated as follows:

- Shorter life cycle is a main difference. The IPv6 pervasive deployment has a shorter lifecycle than an IPv6 sparse deployment.
- A mechanism of tunnelling is another difference where IPv6 sparse deployment has major impact of longer duration.

Implementation is the most difficult part which involves the strategy of the secure installation and configuration of IPv6 equipment, tunnels, and translation mechanisms. The deployment stage differs depending on which deployment scenario is used. In both scenarios, the strategies used have been different. The actual IPv6 implementation involves a phased deployment. The initial strategies are same in any type of the method of deployment. [26].

These are some of the steps that employ IPv6 pervasive deployment:

- Effective usage of IPv6 routing for the deployment of IPv6 connectivity externally.
- Proper usage of firewalls, policies etc. of IPv6 while configuring the devices in support with security plan, standards, and procedures.
- Feature of interior outing for IPv6 deployment.
- Having enabled hosts of IPv6.
- Deploying basic IPv6 services (DNS, DHCPv6, and NTPv6).
- Fine usage of the translation mechanisms for deploying IPv6.
- Monitoring the management strategies protocols such as IDPS, SNMP, authentication and netflow [25].

These are some of the steps that employ IPv6 sparse deployment:

- Proper usage of firewalls, policies etc. of IPv6 while configuring the devices in support with security plan, standards, and procedures.
- Having access to the basic IPv6 deployed services such as DNS, DHCPv6 etc.
- Effective usage of IPv6 routing for the deployment of IPv6 connectivity externally.

- Fine usage of the translation mechanisms for deploying IPv6.
- Deploying external IPv6 connectivity with exterior IPv6 routing.
- Enabling dual protocols on core routers. (This step can be performed at this point or after completing Step 5).
- Enabling management monitoring (SNMP, service monitoring, IDPS, authentication, statistical monitoring, and netflow). [25]

These are some of deployment strategies where care should be taken in the implementation and deployment process. Security risks are the new incompatible during the initial deployment of a new protocol such as IPv6, but whereas the other strategies like mitigation are effective and many of the residual risks are no different from those that challenge existing IPv4 networks [27].
The main feature of the IPv6 security is the IPsec and it should be deployed, wherever possible, to secure IPv6 networks. Transition technologies allow existing IPv4 networks to coexist and interoperate with IPv6 networks, systems, and services. These transition mechanisms cover a wide range of technologies and transition scenarios. Planning of the deployment is a crucial and the vendors or organizations must have a plan to deploy IPv6 in secure way with having an eye on lifecycle of equipment from inception to disposal [25].

In summary, IPv6 is ready for deployment, but additional effort is needed to make a successful implementation. The IETF, equipment vendors, application developers, network operators, government and end users all have roles to play in ensuring the successful wide-spread deployment of IPv6.

The core IPv6 specifications are becoming increasingly available as a standard part of products and service offerings. However, not all products are fully IPv6 capable now and some significant upgrade gaps remain, especially in low-end consumer equipment. However, despite a decade long development and implementation history as a Standards Track protocol, general worldwide deployment of IPv6 is increasing slowly. As of September 2013, about 4% of domain names and 16.2% of the networks on the Internet have IPv6 protocol support [20]. In summary, IPv6 is ready for deployment, but additional effort is needed to make its use pervasive. The equipment vendors, application developers, network operators and end users all have roles to play in ensuring the successful wide-spread deployment of IPv6.

## 8 Future of IPv6

### 1. New Protocol for Neighboring Node Interaction

The neighbour discovery protocol for IPv6 is a series of internet control message protocol for IPv6 (ICMPv6) message that manage the interaction of neighboring nodes. Neighbour discovery replace addresses resolution protocol (ARP), ICMPv4 router discovery, and ICMPv4 redirect message with efficient multicast and unicast message and provides additional functionality.

### 2. Better Support in Terms of (QoS)

The addition of new fields in IPv6 header makes it possible to define how traffic is handled and identify by using the flow label field in the header. This makes it is possible to identify the traffic, which allows the router to identify and provides special handling for packets that belong to a flow and the series of packet between the source and destination which is the mean of flow. Because the traffic is identified in the IPv6 header, support for QoS can be easily achieved when the packet payload is encrypted with IPsec. Other futures of inheritance from IPv6 are Security encryption, header encryption, sender authentication and privacy.

## 10 Recommendations

The following recommendations if strictly adhered to will have a positive impact in making IPv6 the only protocol for the world internet.

1. Further deployment of IPv4 protocol should be discouraged in the less technological developed areas like the African continent. This will be achieved by encouraging government policies that would stop the movement of these obsolete IPv4 enabled devices from the developed countries to the developing countries.
2. We recommend an increase in the adoption of SDN. It will unify different IPv6 transition mechanisms and solve the deadlock problem in various transition mechanisms by allowing transparent upgrade in the infrastructure and services to support IPv6.
3. We also recommend that a unified approach should be adopted as many deployment models, transition strategies and too many standards makes it difficult for manufacturers to decide what method to implement.
4. There is need for an IPv6 training and education, monitoring and support to facilitate to reflect the industrial best practices in the deployment process.

## 11 Conclusion

The introduction of IPv6 to the networking protocol since early 90's opened up several questions within the networking industry with respect to its adaption rate and various transition mechanisms from IPv4 to IPv6. This study has shown that IPv6 is a more efficient, and future oriented protocol that will provides additional seamless services that were not part of its predecessor protocol, IPv4. The practices within the industries shows that IPv6 is a defacto standard at present and is currently being deployed in almost all the Internet architecture worldwide wide great disparity across the various continent.

Many technologies such as NAT and CIDR have been developed to facilitate the rapid deployment but have been faced with the economic aspect of the transition. The key players of this sector, the ISP, have resorted to using many sub-netting strategies to continue to provide various services while compromising the scalability of the industries.

Finally, it is concluded that, most of the hardware and

software are IPv6 enabled and the decision of what, when, and how to move from IPv4 to IPv6 still depends upon the type of the network, the network providers, and the Government regulation of a country or region. Transition from IPv4 to IPv6 is a planned process and major network players like Cisco and Google all over the world have already started the process. The current IPv6 web, email, DNS, and IPv6 enabled user's deployment status world-wide is below the expected level and has failed to meet up with initial proposed date, hence we can conclude that it is not an IPv6 world.

## ACKNOWLEDGMENT

The authors wish to thank Dr David McMillan for his support throughout the writing of this paper.

## REFERENCES

[1] J.S. Bridle, "Probabilistic Interpretation of Feedforward Classification Network Outputs, with Relationships to Statistical Pattern Recognition," *Neurocomputing – Algorithms, Architectures and Applications,* F. Fogelman-Soulie and J. Herault, eds., NATO ASI Series F68, Berlin: Springer-Verlag, pp. 227-236, 1989. (Book style with paper title and editor)

[2] W.-K. Chen, *Linear Networks and Systems.* Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

[3] H. Poor, "A Hypertext History of Multiuser Dimensions," *MUD History,* http://www.ccs.neu.edu/home/pb/mud-history.html. 1986. (URL link *include year)

[4] K. Elissa, "An Overview of Decision Theory," unpublished. (Unpublished manuscript)

[5] R. Nicole, "The Last Word on Decision Theory," *J. Computer Vision,* submitted for publication. (Pending publication)

[6] C. J. Kaufman, Rocky Mountain Research Laboratories, Boulder, Colo., personal communication, 1992. (Personal communication)

[7] D.S. Coming and O.G. Staadt, "Velocity-Aligned Discrete Oriented Polytopes for Dynamic Collision Detection," *IEEE Trans. Visualization and Computer Graphics*, vol. 14, no. 1, pp. 1-12, Jan/Feb 2008, doi:10.1109/TVCG.2007.70405. (IEEE Transactions)

[8] S.P. Bingulac, "On the Compatibility of Adaptive Controllers," *Proc. Fourth Ann. Allerton Conf. Circuits and Systems Theory*, pp. 8-16, 1994. (Conference proceedings)

[9] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representation," *Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS '07)*, pp. 57-64, Apr. 2007, doi:10.1109/SCIS.2007.367670**.** (Conference proceedings)

[10] J. Williams, "Narrow-Band Analyzer," PhD dissertation, Dept. of Electrical Eng., Harvard Univ., Cambridge, Mass., 1993. (Thesis or dissertation)

[11] E.E. Reber, R.L. Michell, and C.J. Carter, "Oxygen Absorption in the Earth's Atmosphere," Technical Report TR-0200 (420-46)-3, Aerospace Corp., Los Angeles, Calif., Nov. 1988. (Technical report with report number)

[12] L. Hubert and P. Arabie, "Comparing Partitions," *J. Classification,* vol. 2, no. 4, pp. 193-218, Apr. 1985. (Journal or magazine citation)

[13] R.J. Vidmar, "On the Use of Atmospheric Plasmas as Electromagnetic Reflectors," *IEEE Trans. Plasma Science*, vol. 21, no. 3, pp. 876-880, available at http://www.halcyon.com/pub/journals/21ps03-vidmar, Aug. 1992. (URL for Transaction, journal, or magzine)

[14] J.M.P. Martinez, R.B. Llavori, M.J.A. Cabo, and T.B. Pedersen, "Integrating Data Warehouses with Web Data: A Survey," *IEEE Trans. Knowledge and Data Eng.*, preprint, 21 Dec. 2007, doi:10.1109/TKDE.2007.190746. (PrePrint)