Towards IPv6 Migration and Challenges

Junaid Latief Shah
Department of Higher Education J&K

Asif Iqbal Khan
University of Kashmir

Towards IPv6 Migration and Challenges

Junaid Latief Shah, Department of Information Technology, Sri Pratap College, Cluster University Srinagar, Srinagar, India

Heena Farooq Bhat, Department of Computer Science, University of Kashmir, India

Asif Iqbal Khan, Department of Computer Science, University of Kashmir, India

ABSTRACT

The Internet, since its genesis in 1970's, has already become a global broadcasting potential for information dissemination and a channel for information collaboration and an interface between disparate users and their systems, separated by large geographical locations. The rate of growth of interconnected devices has been on exponential scale from the last decade. As of now, more than 5 billion devices are accessing the Internet. The Internet Protocol Version 4 (IPv4) which is a three decade old standard internetworking protocol using 32-bit address, fails to cater such a large number of hosts. In February 2011, the Internet Assigned Numbers Authority (IANA), the nodal agency for IP address allocation exhausted the central pool of IPv4 addresses completely. This rapid depletion of IP addresses was inevitable as a large number of devices are getting connected to internet. Also, inefficient utilization and remiss planning of IP address space acted as catalyst in the process of depletion. NAT, CIDR and Subnetting only serve as short interim solutions provided by IPv4. Moreover, IPv4 fails to scale up and bridge the security enhancements required by the modern Internet today. The only feasible option lies in unabridged transition to IPv6. Internet Protocol Version 6 (IPv6) provides an address space of 2^{128} i.e. trillions of addresses, making the IP address space potentially inexhaustible. Thus, adopting IPv6 makes a paragon choice of replacement for IPv4. This article reviews the next generation internet protocol IPv6 and explicates the discussion over the need for migrating to IPv6. The article also presents technical as well as non-technical challenges related to migration and presents overall statistics regarding IPv6 adoption around the world.

KEYWORDS

CIDR, IANA, IPv4, IPv6, NAT, RIR

1. INTRODUCTION

Internet Protocol Version 4 (IPv4) since its genesis has been pervasive even in today's operational networks. The IPv4 protocol enabled the hosts to send packets to other hosts having a unique address. However, it was never designed to scale millions and billions of hosts online. The contributing factor in address depletion has been exponential increase in internet ready devices and origin of broadband wireless networks (Chen & Liao, 2017). The three decade old protocol with a limited address space cannot scale up to the ever demanding needs of present day internet. This limited address space got exhausted and raised an alarming issue over the growth of internetworks.

DOI: 10.4018/IJTD.2019040105

In late 80's, IETF came up with the idea of using temporary internet patches like CIDR (classless inter-domain routing) and NAT (network address translation) for internet continuity. But in 1992, CIDR (classless inter-domain routing) design was put into operation and the number of internet nodes surpassed over 100,000 (Rekhter & Li, 1993; Fuller et al., 1993). Thus, these short term antidotes failed given the ever expanding nature of internet. Also, being an obsolete protocol, the distinctive attributes like mobility, security and QoS (Quality of Service) were supplemented by retrofitting such characteristics in IPv4. For example, Internet Protocol Security (IPsec) provides security for IPv4 packets at the network level using encryption mechanism. As IPsec is not an inherent component in IPv4, its implementation has compatibility issues with NAT (Kent & Seo, 2005). Although IPv4 ToS (type of service) and identification attributes provide support for real time data, but its implementation has a limited domain (only 8 bits).Also the term ToS has been polished over a number of times. IPv4 has also issues in payload identification when encryption is used on a TCP or UDP port address.

IETF in 1992 came to the conclusion that IPv4 was on the verge of exhaustion. The Internet Engineering Task Force (IETF) soon started the process of searching a more flexible solution by creating a temporary adhoc IP Next Generation (IPng) group to address the problems and issues of next internet protocol version. Consequently, a white paper solicitation was released for the Next Generation Internet Protocol which was followed by the release of several RFC's related to IPv6 (Bradner & Mankin, 1993). Thus, after an exhaustive research and owing to the problems of address depletion, a new version of IP known as IPv6 was proposed and designed (Rekhter & Li, 1993).

In the initial stage, a migration from IPv4 to IPv6 was visualized which will help IPv6 hosts to maintain connectivity and reachability with IPv4 hosts (Gilligan & Nordmark, 2000). When an entire transition occurs, IPv4 will automatically be wiped out. However, given the current statistics, the migration to IPv6 is still underway. In fact, it is still in its initial stages as only average 7% of world population is using IPv6 as per Google 2015 statistics. It's well understood that transition to IPv6 will be slow and gradual process overtime. The main rationale behind this being the massive deployment of NAT devices in enterprise and home networks which have acted as delaying catalyst in migration process. In fact, some people envisioned that the migration might even not occur. However as on Feb 3, 2011, the last block of IPv4 address space was allocated by the IANA (Internet Assigned Numbers Authority), thus declaring end of IPv4 addresses (Chen & Liao, 2017). Thus, adopting IPv6 makes an unblemished choice of replacement for IPv4.

2. INTERNET PROTOCOL VERSION 6 (IPV6)

Internet Protocol version 6 (IPv6) or IP next generation is the successor of IPv4. The protocol is viewed as a decisive step forward by IETF after foreseeing the depletion of IPv4 address space. IPv6 supports an 128 bit address format and supplements an address space of 2^{128} (approximately 3.4×10^{38}) addresses, i.e. more than sufficient to cover theoretically every internet ready device on earth with a global unique address (Dunn,2002). The huge address space also provides flexibility for every node in the world to remain connected to the internet. The protocol also abolishes the requirement for NAT and enhances connectivity, reliability and flexibility of the network. The major objectives of IPv6 were to dispense huge address space, enhance security element in the protocol and support for real time traffic. IPv6 treats IPsec as an intrinsic element unlike that in IPv4 where it was retrofitted and optional. A new field Flow Label has been introduced to support Payload identification (used in QoS) in IPv6 packet. The idea of fragmentation has been dropped. The extension headers part takes care of the checksum and option in IPv6. Also, IPv6 introduces "stateless" auto configuration which is one of the design goals and thus eliminates the cumbersome manual configuration of IP or DHCP. Lastly the size of packet header has been increased from 20 byte in IPv4 to 40 byte in IPv6 (Chen & Liao, 2017).

2.1. Header Structure

As specified in (Deering & Hinden, 2017), IPv6 has a fixed size header of 40 bytes. Because some fields from the IPv4 header have been removed in IPv6, it has been made simpler and flexible. The fields that are removed include IP header length, header checksum, flags, fragmentation offset and identification fields. The extension header field replaces the options field in IPv6. The main motive behind redesigning the header was to improve performance in header processing by nodes. The IPv6 header is shown in the Figure 1.

- **Version:** Specifies the version of the IP protocol;
- **Traffic class:** Meant for type-of-service (ToS) and priority of the packet. The purpose of this field is to handle real time transmission;
- **Flow Label:** Used for special handling of data packets. All packets packets belonging to a particular flow carry the same label;
- **Payload Length:** Carries the length of IPv6 data payload;
- **Next Header:** Carries information regarding next extension header to examine;
- **Hop Limit:** Used as a counter for data packets. Serves same purpose as TTL in IPv4;
- **Source and Destination Address:** Specifies the source and destination IP address of hosts.

2.2. Addressing Types

The IPv6 address is 128 bits or 16 byte long which is four times more than the older version i.e. IPv4. IPv6 address is usually written with the help of 32 hexadecimal digits. These digits are arranged into 8 groups and each group consists of 4 hexadecimal digits. These groups are separated from one another with the help of colons (**:**). An example of IPv6 address is shown as:

2001:2713:1ce1:0216:020a:53ff:fe73:41a3

Normally IPv6 address has the format as shown in Figure 2:

- **Global Routing Prefix (48 bits):** Defines the range of addresses assigned which uniquely identifies a site connected to the Internet. This is usually assigned by ISP's;

Figure 1. IPv6 header structure

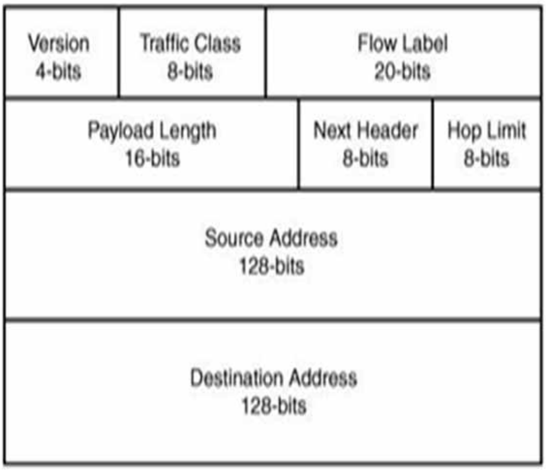
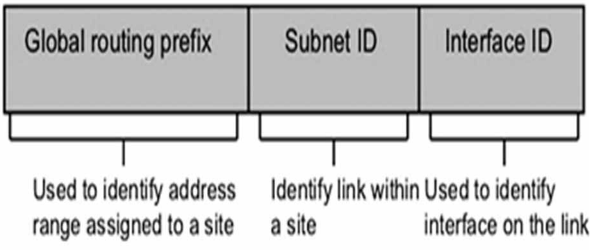


Figure 2. IPv6 address format


Global routing prefix
Subnet ID
Interface ID
Used to identify address range assigned to a site
Identify link within a site
Used to identify interface on the link

- **Subnet ID (16 bits):** Identifies the subnet within the network. It is designed to be structurally hierarchical by site admins;
- **Interface Identifier (64 bits):** Identifies an interface within the link. It is usually constructed from the link layer address of the node or through some random number generation algorithm.

Similar to IPv4's CIDR format, an IPv6 address can be written in CIDR format to determine the number of leftmost bits that identify the network prefix or a specific type of address. Usually, ISP's assign /48 block of address range to corporations leaving out 80 bits to be distributed between other two chunks. When it's known that only one subnet is needed, a /64 prefix can be allocated in that case. When it's known that one and only one device is connecting, a /128 prefix can be allocated.

Zero compression or address compression scheme is also possible which makes reading and writing of IPv6 addresses easier. The key is that one of the three leading (not trailing) zeroes in a hex grouping can be dropped.

Moreover, an address containing all-zero portions may be substituted by a double colon which can be done only once:

e.g. 0000:0000:0000:0000:0000:0000:0000:0001/128 becomes :: 1/128

The concept of an address scope has been introduced lately in the design of IPv6.By definition; four different types of scopes are possible for an IPv6 address. They are:

- **Interface Local Scope:** Which is restricted to a single interface. e.g. A loopback address i.e. :: 1;
- **Link Local Scope:** Which is restricted to a given link on a LAN. Link Local addresses are formed by prefixing a well-known prefix FE80::/64 to the 64 bit interface identifier;
- **Unique Local Address:** Which pertains to all networks within an organization i.e. routable within a corporate network. ULA substitutes for deprecated site local address having a prefix of FEC0::/10;
- **Global Scope:** Applies to whole internet and is routable universally.

RFC 4291 defines the following IPv6 address types:

- **Unicast Addresses:** Distinguishes a single unique node on the link. The data packet transmitted to this address is transported to the node recognized by it. Three categories of Unicast addresses include Global Unicast, Site Local Unicast and Link Local Unicast;
- **Anycast Address:** Recognizes a group of nodes on the link; however, a data packet transmitted to this address is delivered only to the nearest node decided by the calculations of the routing protocol;

- **Multicast Address:** Recognizes a group of nodes determined by a multicast group address. The data packet transmitted to this address is received by all the member nodes of the group.

In addition to the above-mentioned addresses, IPv6 also defines some special addresses which are used for specific purposes:

- **Unspecified Address (::/128):** This address consists of all zeroes and may be used by a source node soliciting for an address (e.g. DHCPv6) during the boot process or in case of auto configuration. This address should never be statically or dynamically assigned to an interface and it should not be used a destination address as this address is usually not forwarded by the routers on the network;
- **Loopback Address (::1/128):** This address is normally useful in testing and diagnosis of the IP network. This address retransmits packets to itself;
- **IPv4 compatible IPv6 address:** These addresses play their role in tunneling IPv6 packets over IPv4 network hardware;
- **IPv4 mapped IPv6 address:** This is used to represent the address of IPv4 only nodes as an IPv6 address.

The format is **::** FFFF/96 + 32 bit IPv4 address.

2.3. Extension Headers

IPv6 introduces extension headers which are used to handle optional fields. The Extension Headers if present are implemented as chain of headers and are appended at the end of the base header each indentified by a unique next header value. RFC 2460 supports the following six extension headers:

1. Hop by Hop Option (Next Header value 0)
2. Routing Header (Next Header value 43)
3. Fragmentation (Next Header value 44)
4. Authentication (Next Header value 51)
5. Encrypted Security Protocol (Next Header value 50)
6. Destination Option (Next Header value 60)

3. NEED FOR INTERNET MIGRATION

The migration to Next Generation Internet Protocol (IPv6) is inevitable because of the unanticipated increase in internet users and devices. As early as in 1995, the idea of migration was conceived which ultimately led to the evolution of IPv6.The IPv6 network migration is seen as an intricate daunting task impeding its evolution. Nevertheless, with emergence of new IPv6 migration techniques, its complete integration with current IP networks seems to be achievable in near future. Although IPv6 implementation is yet to attain a maturity level, its success will ultimately depend on its implementation in a broader perspective (Domzal, 2013). The IPv6 protocol boasts a 128-bit address space to allow for massively more addresses. IPv6 is designed to solve the long-term performance, reliability and scalability problems of IPv4.The following are the motivating factors and modern-day internet requirements that drive the migration to IPv6.

3.1. Lack of Address Space in IPv4

IPv6 offers an address space of 2^{128} (approximately 3.4×10^{38}) addresses, meaning that theoretically every square inch of earth will have an IP address. Such a huge address space diminishes the address scarcity issue of IPv4 and also abolishes the need of NAT in IPv6.

3.2. Real Time Multimedia Support

Quality of Service (QoS) in Real Time Multimedia is an important network performance parameter having significant impact on real time applications like VoIP, Interactive gaming and Video Streaming. The internet today has become the most important communication channel. Prior to the year 2000, it was primarily used for electronic mail, file transfer and network news (USENET). Traditionally all the network traffic was treated on equal priority basis. The IP's best effort service model had no guarantees for network performance parameters like delay, variation in delay, reliability, jitter etc. But today with the emergence of new real-time applications like VoIP and Video Streaming (Parra et al., 2011), factors like delay, jitter, bandwidth and packet loss play a pivotal role in network performance which were earlier insignificant. The QoS is often attributed to managing the network resources efficiently which are important for high performance of critical real-time applications (Forouzan, 2006). The internet today consists of lot of multimedia and interactive applications having specific requirements of delay and bandwidth which challenge the essential design goals of internet protocol and its best effort service model (Qadir & Siddiqi, 2011). Thus, QoS is an active area of research today. Managing QoS guarantees bandwidth for key applications and users. The transmission data rates, error probability can be measured and improved and in certain cases also guaranteed to some extent. The main advantage of QoS defined network is the ability to prioritize traffic to allow critical application flows to be serviced first before the application flow with lesser priority (Parra et al., 2011). IPv4 doesn't have any built-in mechanism for handling the multimedia and real-time application. The amount of jitter and delay is also higher in case of IPv4 because it does not differentiate between time sensitive data payloads like voice and video applications and those that are not sensitive to delay like file transfer. IPv6 braces QoS with the help of two fields i.e. Flow Label and Traffic Class. The flow label field is 20 bits and is drafted for specially handling flow of data. The unique flow is defined as combination of source address and non-zero flow label. The IPv6 routers treat packets equally belonging to a particular flow. The 8-bit traffic class field is used for prioritizing the data packets. This field can take different values ranging from priority level 0 to 7. The 6 most significant bits are used for defining differentiated services used for classification of packets. The next 2 bits are used for ECN (Explicit Congestion Notification).

3.3. Mobile IP

Mobility is one of the dominant features of IPv6 which is well suited for mobile computing environments. Mobile IP allows devices to move from one network to another and still maintain existing connections. Although Mobile IPv6 is mainly targeted for mobile devices, it is equally applicable for wired environments. In a fixed IPv6 network mobile nodes cannot maintain connection with the previous connected link while moving to other networks. Thus, mobility is important to enable nodes to move from one IP subnet to another, i.e. Mobile IP facilitates node movement from one Ethernet segment to another as well as it accommodates node movement from an Ethernet segment to a wireless LAN, provided nodes IP address remains constant after such a transition (Zhang et al., 2009).

3.4. End to End Security Model

The support for IPsec in IPv4 was optional. IPsec was retrofitted in IPv4 as a security measure for securing the integrity and confidentiality of data packets. In IPv4; IPsec was used to provide security between two border gateway routers due to limitations imposed by NAT, however in IPv6 there is no need for NAT. Thus, in IPv6; IPsec can be used for accelerating and securing end-to-end communication (Akour, 2016). IPv6 treats IPsec as an inbuilt component rather than as additional component.

3.5. Improved Routing

Routing Deals with the mechanism of delivering packets from intended source to its destination. Routing process has had a significant change in IPv6.The legacy routing protocols like RIP, OSPF, BGP, ISIS have been retained in IPv6.The simpler header structure of the IPv6 packet and new hierarchical structure has made the routing tables lighter with fewer entries. Improved routing results in faster convergence of data packets. IPv6 also offer improved multicasting capability wherein the data packets are sent to several clients.

4. CHALLENGES TO MIGRATION

Migration to IPv6 is seen as a daunting task due to its incompatibility with IPv4. Initially the integration between the two heterogeneous environments will be fragile. Although the rudimentary building blocks for transition like Dual Stack, Tunneling and Translation are available, but they don't seem to fork out issues of network migration. Economic as well as infrastructural considerations also play a pivotal role in overall resolution. The major roadblocks impacting IPv4 to IPv6 migration are incompatibility between hardware and software, issues with left over legacy IPv4 applications, limited user experience with IPv6 and hesitation to accept new protocol and uncertainty about business returns on investment (Govil et al., 2008). An important factor in IPv6 success is porting of legacy IPv4 applications which is relatively simple but will take substantial amount of time due to vast installed base of IPv4. It's also probable that some legacy applications may never get docked to IPv6. Also, it may happen that migration to IPv6 will downgrade the performance of network. The infrastructural cost to handle coexistence and support to both the protocols will also be high till migration process completes. For an organization migrating to IPv6, a number of key requirements are listed below (Chen & Liao, 2017):

1. The operation of legacy IPv4 applications should not be hampered by router supporting encapsulation (e.g. tunnels);
2. The performance of IPv6 should be at par with the IPv4 service (e.g. with similar line data speed and characteristics);
3. The introduction of new protocol or flaw in any transition mechanism used cannot bargain security of the network;
4. Economic costs associated with introduction of IPv6 infrastructure must be framed carefully.

Migration to IPv6 environments is expected to be fairly complex. Initially, internetworking between the two environments will be critical. Existing IPv4 endpoints or nodes will need to run dual stack nodes or convert to IPv6 systems. Fortunately, the new protocol supports IPv4 compatible IPv6 addresses. Tunneling is a method that will support transition in the beginning (Chen & Liao, 2017). From the surplus literature available, the roadblocks or bottlenecks to migration can broadly be classified into two categories: Technical and Non-Technical Issues.

4.1. Technical Issues

Transitioning to IPv6 from IPv4 deployments is a demanding task. For onward and upward transition to IPv6, network hardware, security setup and ISP's must be designed and managed in such a way that provides simultaneous support to both IPv4 and IPv6 (Chen & Liao, 2017). A number of challenges and security issues have to be dealt with. For example; if the configuration is not correct, the security features of the network are at threat. Configuration process has to be carried out extra carefully. Also, in IPv6, it can't be predicted how fast convergence will occur, if there are routing loops or if the routing tables aren't properly managed since IPv6 routing protocols have not been tested as thoroughly as the IPv4 routing protocols. The routers and backbone links are imposed with extra burden because of multiple IPv4 and IPv6 routes due to which transactions may take longer to complete. The routers doing the conversion may become congested. Security issues like Distributed Denial of Service (DDoS) attacks are also possible in the transition phase due to multicast transfer.

For integration between IPv4 and IPv6, the basic internet migration techniques as proposed by IETF include Dual Stack, Tunneling and Header Translation (Gilligan & Nordmark, 2000).

Dual Stack Technique although provides a workaround for migration, but it also requires huge amount of memory for sustaining two protocol stacks and two routing tables. Also, the implementation of two protocol stacks requires the occupancy of high computational power in nodes raising high infrastructure costs. Tunneling suffers from the drawback of packet header encapsulation and decapsulation which can cause potential processing overheads. Since IPv6 is designed for faster processing, these bottlenecks in migration phase are intolerable.

Header translation technique is less secure and does have potential flaws. Due to loss of information during translation, this technique is not preferred. Thus, all the migration techniques discussed above have their own merits and demerits. The comparative analysis of these techniques can be found in (Lencse & Kadobayashi, 2017).

Security has been the prime concern in deployment of IPv6 (Waddington & Chang, 2002). Since IPsec and other security protocols designed are supported in IPv4 and IPv6, however not all existing IPv4 systems implement these mechanisms. The redesign or remodeling of these security architectures could be costly in large scale deployment environments like IPv4. The choice of deploying a new IPv6 architecture (where IPsec is mandatory) seems to be more strategic and effective in the long term than incorporating these capabilities onto the IPv4 infrastructure (Domzal, 2013). However, since IPv6 implementation is brimming, network administrators may be oblivious of malicious IPv6 traffic that has tunneled into their networks. The implemented security algorithms examine only outer part of tunneled datagram's, which could be within permitted tolerance however ignoring the data content inside. If this traffic manages to decapsulate itself at the other end of tunnel inside the secured network successfully, then it is likely to be very critical since inside a network itself, defense security mechanism is comparably low (Waddington & Chang, 2002). Deploying IPsec in concurrence with IP translation mechanism like NAT-PT and TRT that include packet modification will render packet as inauthentic (Wu et al., 2013). It also breaks IPsec end-to-end security architecture.

DNS in IPv6 has been changed and TCP/IP protocol suite must be redesigned to support the new address format (Che & Lewis, 2010). A DNS specification for IPv6 called as AAAA and A6 records was proposed by IETF in RFC 2874. A6 records plot 128-bit IPv6 address to domain names besides mapping IPv6 address prefixes to partial domain names. Therefore, for resolution of IPv6 address or addresses from domain names, the DNS server must acquire an unabridged string of A6 records (Wu et al., 2013).

Routing protocols have also been changed in IPv6. Most interior and exterior routing protocols are direct extensions of IPv4 routing protocols. The protocols that are changed include RIPv6, OSPFv6, IDRP, BGP4, DHCPv6 etc.

Interoperability between hardware and software is another issue impeding the adoption of IPv6. During the early years of computing, windows 2003 and XP were in use which did not support IPv6 and therefore discouraged its deployment. These legacy operating systems need adaptations and modifications to work with the new IP protocol. Also, applications need to be ported to run over IPv6. This can be done easily if the application strictly segregates application layer from the communication layer. However, if the application uses complex middleware and customized Application Programming Interfaces (API's), the porting will be somewhat difficult to achieve. The up gradation of software may involve recompiling it with using different API's. The compatibility issues that might arise may be resolved later.

In totality, it can be argued that in present scenario, limited number of IPv6 security tools, policies and expertise is available. The adoption rate is greatly affected by the fact that large proportion of network professionals might be hesitant to embrace the new technology because of the phobia that it might disrupt existing services.

4.2. Non-Technical Issues

Non-technical or non-functional issues also play a major role in obstructing the early adoption of IPv6 (Govil et al., 2008). Every new technology that comes into the market is benefitted when we have a proper vendor support for it. When the development of IPv6 started, Windows 95 and NT were already dominant in the market. Both of these popular operating systems did not support IPv6. Additionally the routers and other available network hardware did not support the new protocol. Thus, when an organization would like to migrate to IPv6, all the underlying hardware and software would require changing. Since 2000, most of the hardware and software companies like Cisco, Microsoft and Nokia have been delivering products that are IPv6 compatible. Since then, the support for IPv6 is available on majority of operating systems.

With new technology comes the cost of implementation (Mackay et al., 2003). Migrating to IPv6 involves huge money investment which is a key factor in deciding whether to embrace the new protocol or not. Small enterprises may be hesitant to migrate depending on the age of their equipment that they use and how sustainable their infrastructure is. Private companies may show displeasure in the amount of money that needs to be spent on technological migration especially when a short-term solution like NAT is available. Today however the cost of hardware and software is small. A small software upgrade may be done by installing a patch in the operating system to support IPv6.

The implementation of new forefront technology like IPv6 is also encouraged by government's support, funding and policy. A government can take up the initiative and grant funding for early implementation of IPv6. A good example is of the Japanese government that launched the 'e-Japan priority policy program'. This program boosts the transition to IPv6 on large scale. Also, the IPv6 promotion council of Japan has been made functional to achieve following targets: to unite globally in embracing and development of IPv6; to generate required human resource for deployment and encourage new private business models involved in polishing IPv6 services.

The new technology education is another important factor affecting the acceptance of IPv6. Learning about the protocol is necessary for everyone that it will affect. The IPv6 migration will have an impact on everyone. There could be problem of skill shortage while migrating to IPv6.

5. GUIDELINES FOR MIGRATION

Transition Mechanisms must meet the following guidelines in the real world (Bi et al., 2007):

- **Scalability:** Plays an important role in determining the deployment of a transition mechanism. For example; transition technique like NAT-PT can administer few connections very well but with increase in internet ready devices, the operational and state sustenance loads also grow proportionally which lead to performance slump and system unavailability;
- **Security:** The transition mechanisms should not introduce security leaks and vulnerabilities in the network. This involves care full planning before deployment of the mechanism;
- **Performance:** The performance parameter directly hinges upon the scalability factor. By adopting a certain transition mechanism, the performance of the network should not degrade. For example; tunneling encapsulation/decapsulation has a direct impact on delay factor and also packet sizes;
- **Functionality:** While deploying certain transition mechanisms, some of the IPv6 features cannot be fully utilized and whether to operate them depends on the scenario present. For example; SIIT is unable to translate IPv4 options or IPv6 extension headers. Also, other mechanisms face arduous issues while translating multicast addresses. (Unless there is some bridge or gateway);
- **Requirement:** The worked mechanisms should be chosen by the requirements of configure method, IP addresses, applications etc.;

- **Ease of Use:** Transitioning and tool configuration should be abstracted from end user. The internal configurations should be hidden from applications end users;
- **Ease of Management:** To deploy a transition mechanism should not bring too much burden of management, and the network during IPv6 transition should be manageable.

6. IPV6 DEPLOYMENT AROUND THE WORLD

The 6Bone started in 1996 was the legacy IPv6 network and by the year 2004 had achieved a milestone of 1000 hosts in more than 50 countries (Frankel et al., 2010). Initially, it was used as a test network by IETF working groups. There is varied global deployment of IPv6 in each continent. The International IPv6 forum is the committee responsible for coordination of worldwide IPv6 activities. The International Task Force (e.g. North American IPv6 Task Force, European Task Force and various task forces in Asia and other parts of world) coordinate the regional task force activities. The Regional Task Forces bear the responsibility of coordinating activities in their particular regions. Google has been the frontrunner in reporting statistics regarding the IPv6 adoption. It regularly collects statistics about the IPv6 adoption on the internet by measuring the availability of IPv6 connectivity among Google users.

The Table 1 shows the data as reported by (Google, 2015) on 24th September 2015.The table reveals the percentage of adoption of IPv6 among the leading countries around the world.

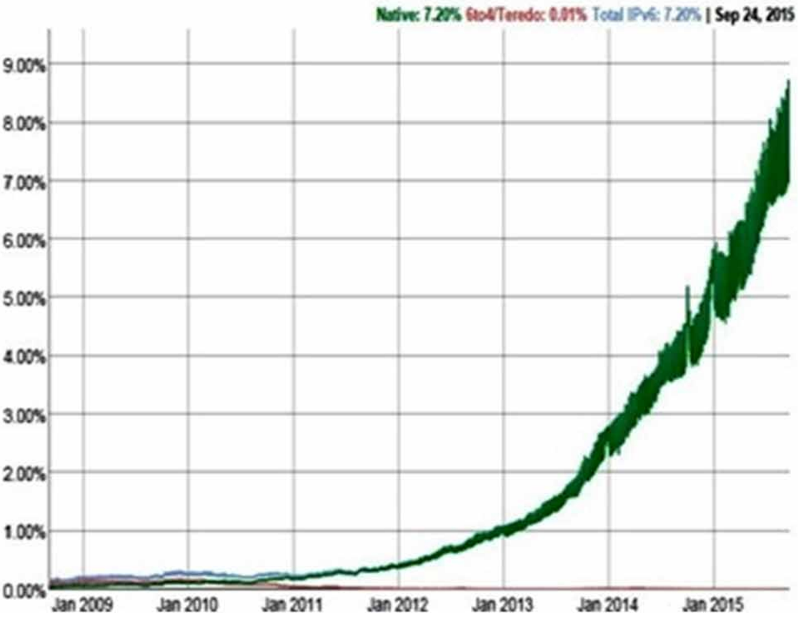
In Asia, the growing population and internet growth rate have contributed towards embracing the new protocol. IPv6 is already in use in some countries like Japan and China. In 2002, Japan was the frontrunner towards IPv6 development when they launched ‘e-Japan priority policy program’. This was followed by unprecedented support from tech giants like Sony who announced IPv6 support in all their devices (Karpilovsky et al., 2009). More statistics can be seen in Figure 3.

In 2001, China initiated the China Next Generation Internet (CNGI) project which was supported by China’s five major telecommunication operators. From initial phase, IPv6 Mobility was built into the CNGI. In 2005, the CNGI operation and deployment tests consisted of a total of 61 projects under

Table 1. IPv6 adoption rate

Country	%age	Country	%age
US	23.04	Russia	0.76
Canada	6.84	Italy	0.17
Brazil	6.41	Finland	7.67
Japan	8.81	Peru	15.77
Greece	18.8	China	1.76
Malaysia	8.58	France	6.45
Norway	8.02	Estonia	9.11
Portugal	20.58	Germany	22.4
UK	2.64	Belgium	42.17
India	0.47	Romania	6.63
Argentina	2.22	Mexico	0.33
Ecuador	13.66	New Zealand	6.5
Poland	1.33	Cambodia	0.33
Chile	0.01	Spain	0.14

Figure 3. Google user IPv6 adoption statistics from Sept 2015



the supervision of China's 100 top technology organizations and universities (Karpilovsky et al., 2009). The deployment of Metropolitan Area Networks (MANs) is being made operational in each city, with IPv6 dispensing a key role in this development. IPv6 finds application in other industries, such as the military, meteorology, seismology, intelligence architecture, and digital home networking.

In India, IPv6 internet users make up only 0.08% of all the Internet users in India when compared to the 4% adoption rate globally. The Network & Technologies (NT) cell of DoT, GoI has released the "National IPv6 Deployment Roadmap Version II" in March 2013. The vision document lists the following main objectives:

1. To take the next step forward and lay down important milestones to facilitate substantial transition to IPv6 in the country in a phased and time bound manner;
2. IPv6 based innovative applications in areas like rural emergency healthcare, Tele-education, smart metering, smart grid, smart building, smart city, etc., have tremendous potential to boost the socio-economic development of the country.

In January 2014, to promote certification programs from IPv6 Forum, Criterion Networking Academy bagged the privilege of becoming first Indian organization to receive IPv6 Forum accreditation for silver and gold certified certification programs. After successful completion of certification programs offered by the academy, the candidates will acquire practical IPv6 knowledge and expertise and receive IPv6 Forum Certified Network Engineer certifications at Silver and Gold Engineer levels which they can include as part of their professional and academic credentials. In Europe, since 2000, the European Commission has led from the front and supported the deployment of IPv6.To boost the economic setup, the commission believes that IPv6 development will play a key role. The first ISP to offer IPv6 services at commercial level was Telia in Sweden. In 2002, Telia already affixed six different POPs (Points of Presence) across Europe. A number of ISP's do not support commercial operation of IPv6 as yet but the groundwork for initial deployment is already in progression and are in the process of starting their operations. IPv6 Internet backbones as well as

Internet Exchange Points (IEX) are expanding at gradual pace. To support IPv6, two major research projects partially funded by the European Commission include the 6net project and Euro6IX. The 6net was a three-year European project initiated to check whether IPv6 satisfy the demands of rapidly increasing global Internet. The project was formally over in 2005. The Euro6IX project was initiated by Internet Society Technologies (IST) with objective to support a rapid establishment of IPv6 in Europe. In early 2004, the German company Telekom made an assumption that by the end of year 2020, world telephone and mobile communication will entirely be IP-based. To meet this challenge, many of the telecom providers are working day and night in the background. IPv6 VoIP find number of implementations including car vendors. Renault in collaboration with cisco, for instance, has prepared a prototype model of IPv6-networked car. The car includes a Cisco router enabling mobile IPv6 implementation. This also enables the car to have an internal IPv6-based network that can be used for scanning, control, and sustenance; for weather and traffic updates, and road condition information; or by passengers to surf the web or watch digital TV with any IPv6-capable device. With the mobile IPv6 implementation, the Cisco router can switch networks to find the best possible signal depending on its position and as such the connected devices inside the car will continue accessing internet without any disruption.

The U.S. DoD's announced its migration to IPv6 network by the year 2008. Starting in 2003, DoD agencies had to include requirements for IPv6 enablement in all their IT purchases. Given that the U.S. DoD's IT spending budget is around 30 billion dollars a year (USD), this provides significant motivation for vendors. The NATO allies and other defense agencies across the globe have followed their policy. This significant thought will exponentially increase the IPv6 market not only in the United States, but all across the world.

7. CONCLUSION

The IPv4 to IPv6 migration is inevitable and IP exhaustion is yet to be conceived by organizations and companies as a predominant issue that requires substantial solutions. The major vendor organizations including government agencies are reluctant to put in the investment that is to be required in future. The contribution demands time and effort for hardware and as well as software up-gradation. This incurs cost, which is one of the blocking factors including restructuring networks and operating two protocol stacks (IPv4 and IPv6) simultaneously, enhancing network software and hardware, educating and instructing the human resource, and diagnosing network implementations for errors. However; given the tangible and substantial gains of IPv6 and attributes demanded by the modern secure internet, the deployment of IPv6 would be a better bet. In this paper, an attempt has been made to highlight the reasons for migration as well as taking into consideration the challenges that are more likely to arise. This analysis will help government as well as R&D organizations to carefully plan their network migration. Given the number of problems in the current internetwork, migration process may be the only solution viable in the long run.

REFERENCES

Akour, I. (2016). Between Transition from IPv4 and IPv6 Adaption: The Case of Jordanian Government. *International Journal Of Advanced Computer Science And Applications*, *7*(9), 248–252. doi:10.14569/IJACSA.2016.070936

Bi, J., Wu, J., & Leng, X. (2007). IPv4/IPv6 transition technologies and univer6 architecture. *International Journal of Computer Science and Network Security*, *7*(1), 232–243.

Blanchet, M. (2009). *Migrating to IPv6: a practical guide to implementing IPv6 in mobile and fixed networks*. John Wiley and Sons.

Bouras, C., Gkamas, A., Primpas, D., & Stamos, K. (2004, July). Quality of Service aspects in an IPv6 domain. In *2004 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'04)*, San Jose, CA (pp. 238-245).

Bradner, S., & Mankin, A. (1993). IP: Next generation (IPng) white paper solicitation (No. RFC 1550).

Che, X., & Lewis, D. (2010). Ipv6: current deployment and migration status. *International journal of research and reviews in computer science, 1*(2), 22.

Chen, Y. S., & Liao, S. Y. (2017). A Framework for Supporting Application Level Interoperability between IPv4 and IPv6. In *Advances in Intelligent Information Hiding and Multimedia Signal Processing* (pp. 271–278). Cham: Springer. doi:10.1007/978-3-319-50209-0_33

Deering, S., & Hinden, R. (2017). *Internet protocol, version 6 (IPv6) specification* (No. RFC 8200)..

Domzal, J. (2013, November). Flow-aware networking as an architecture for the IPv6 QoS Parallel Internet. In *Telecommunication Networks and Applications Conference (ATNAC), 2013 Australasian* (pp. 30-35). IEEE. doi:10.1109/ATNAC.2013.6705352

Dunn, T. (2002). Marketplace-the IPv6 transition. *IEEE Internet Computing*, *6*(3), 11–13. doi:10.1109/MIC.2002.1003125

Forouzan, A. B. (2006). *Data communications & networking (sie)*. Tata McGraw-Hill Education.

Frankel, S., Graveman, R., Pearce, J., & Rooks, M. (2010). Guidelines for the secure deployment of IPv6. *NIST Special Publication*, *800*, 119.

Fuller, V., Li, T., Yu, J., & Varadhan, K. (1993). Classless inter-domain routing (CIDR): an address assignment and aggregation strategy (No. RFC 1519).

Gilligan, R., & Nordmark, E. (2000). Transition mechanisms for IPv6 hosts and routers (No. RFC 2893).

Govil, J., Govil, J., Kaur, N., & Kaur, H. (2008, April). An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms. In IEEE Southeastcon 2008 (pp. 178-185). IEEE.

Hagen, S. (2006). *IPv6 essentials*. O'Reilly Media, Inc.

Jayanthi, J. G., & Rabara, S. A. (2010, July). Next generation internet protocol-Technical realms. In *2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)* (Vol. 9, pp. 394-399). IEEE. doi:10.1109/ICCSIT.2010.5564916

Karpilovsky, E., Gerber, A., Pei, D., Rexford, J., & Shaikh, A. (2009, April). Quantifying the extent of IPv6 deployment. In *International Conference on Passive and Active Network Measurement* (pp. 13-22). Springer. doi:10.1007/978-3-642-00975-4_2

Kent, S., & Seo, K. (2005). Security architecture for the internet protocol (No. RFC 4301). 10.1007/978-3-642-00975-4_2

Lencse, G., & Kadobayashi, Y. (2017, August). Survey of IPv6 transition technologies for security analysis. In *IEICE Technical Committee on Internet Architecture (IA),* Tokyo, Japan (pp. 19–24).

Mackay, M., Edwards, C., Dunmore, M., Chown, T., & Carvalho, G. (2003). A scenario-based review of IPv6 transition tools. *IEEE Internet Computing*, *7*(3), 27–35. doi:10.1109/MIC.2003.1200298

Nordmark, E., & Gilligan, R. (2005). *Basic transition mechanisms for IPv6 hosts and routers* (No. RFC 4213).

Parra, O. J. S., Rios, A. P., & Rubio, G. L. (2011, September). Quality of Service over IPV6 and IPV4. In *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)* (pp. 1-4). IEEE. doi:10.1109/wicom.2011.6040165

Qadir, S., & Siddiqi, M. U. (2011). Cryptographically generated addresses (CGAs): A survey and an analysis of performance for use in mobile environment. *IJCSNS Int. J. Comput. Sci. Netw. Secur*, *11*(2), 24–31.

Rekhter, Y., & Li, T. (1993). An architecture for IP address allocation with CIDR (No. RFC 1518).

Shah, J. L. (2015). Challenges Security Aspects and Solutions for Migrating from IPv4 to IPv6.

Waddington, D. G., & Chang, F. (2002). Realizing the transition to IPv6. *IEEE Communications Magazine*, *40*(6), 138–148. doi:10.1109/MCOM.2002.1007420

Wang, Y., Ye, S., & Li, X. (2005, June). Understanding current IPv6 performance: a measurement study. In *Proceedings. 10th IEEE Symposium on Computers and Communications ISCC 2005* (pp. 71-76). IEEE. doi:10.1109/ISCC.2005.151

Wu, P., Cui, Y., Wu, J., Liu, J., & Metz, C. (2013). Transition from IPv4 to IPv6: A state-of-the-art survey. *IEEE Communications Surveys and Tutorials*, *15*(3), 1407–1424. doi:10.1109/SURV.2012.110112.00200

Zhang, Y., Li, Z., Mei, S., Xiao, L., & Wang, M. (2009, November). A new approach for accelerating IPSec communication. In *2009 International Conference on Multimedia Information Networking and Security* (pp. 482-485). IEEE. doi:10.1109/MINES.2009.151