Chapter 2

IPv6 and Internet Migration

2.1 Introduction

Internet Protocol Version 4 (IPv4) which was developed almost three decades ago is the mostly prevalent protocol version in use today. The IPv4 protocol enabled the hosts to send packets to another hosts having a unique address. However, it was never designed to scale millions and billions of hosts online. The rapid explosion of the internet and existence of high speed wireless and broadband networks have contributed towards depletion of IPv4 (Shah & Parvez, 2014). The IPv4 protocol created more than three decades ago with approximately an address space of 4 billion cannot cater to the needs of modern internet. The IPv4 32 bit address space got drained out soon and posed a serious problem on the growth of internetworks.

In late 80's, it was realized that address conservation methods like CIDR (classless inter-domain routing) and NAT (network address translation) need to be devised and implemented. But by the year 1992, CIDR (classless inter-domain routing) model was implemented and the number of connected hosts exceeded more than 100,000 (Rekhter & Li,1993 ; Fuller, Li ,Yu & Varadhan, 1993).Thus these short term solutions did not seem to help considering the number of devices that were getting connected to the internet daily. Also as the protocol was developed long time back, the features related to mobility, security and QoS (Quality of Service) were handled by additional protocols which cannot be integrated within the protocol. For example Internet Protocol Security (IPSec) is a protocol suit which provides network security by encrypting and protecting the data being sent. Internet Protocol Security (IPSec) provides security for IPv4 packets, but Internet Protocol Security (IPSec) is not built-in and use of IPSec in IPv4 has compatibility issues with NAT (Seo & Kent, 2005). Looking at IPv4, standards do exist for real time data delivery, known as QoS (Quality of Service) but the traffic load relies on just 8 bit TOS (type of service) field and identification of the payload data. The TOS in IPv4 has limited domain and with the passage of time has been redefined with different interpretations. Also payload identification is not possible when IPv4 packet is encrypted using a TCP or UDP port.

IETF in 1991 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 (Bradner & Mankin, 1993) was released for the Next Generation Internet Protocol which was followed by the release of several RFC's related to IPv6. Thus address scarcity and needs of the modern internet led to the development of IPv6, a new version of IP which was a result of a long term research that came into being in 1994. The IPv6 protocol is proposed to solve the long term problems of IPv4 (Rekhter & Li,1993).

In the initial stage, a migration from IPv4 to IPv4 was visualized (Gilligan & Nordmark, 2000) which will help IPv6 hosts to maintain connectivity and reachability with IPv4 hosts. When a complete migration to IPv6 will be obtained, an IPv4 decimate phase would be initiated. However, as of September 2015, the transition to IPv6 has not been completed. In fact it's still in its infancy as only 7 % of IPv6 has been adopted worldwide (Google, 2015).It's worth to mention here that transition to IPv6 will be a 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, the IANA (Internet Assigned Numbers Authority) allocated the last chunk of IPv4 addresses on Feb 3, 2011 to the Regional Internet Registries announcing end of IPv4 addresses (Shah & Parvez, 2014). Thus adopting IPv6 makes an unblemished choice of replacement for IPv4.

The architecture and header structure of IPv6 is different from IPv4.The differences are in six major areas:

- *Larger addressing space (128 bits)*
- *Stateless Automatic configuration.*
- *Simplified Packet Routing.*
- *Simplified Header.*
- *Improved security features (IPSec Support)*
- *Real-time support and multimedia services.*

To Implement IPv6 network, over 30 RFC's have been published since 1994. Adopting the protocol requires changes to dozens of network protocols like DNS, PPP, NAT, DHCP etc associated with IPv4 because those protocols were developed keeping IPv4 in mind which uses 32 bit addresses.

Since IPv6 uses 128 bit addresses, the incompatibility problem for protocols naturally exists. IETF therefore suggested that IPv4 and IPv6 protocols need to co-exist for a substantial amount of time until complete migration takes place.

2.2 Internet Protocol Version 6 (IPv6)

Internet Protocol version 6 (IPv6) is the next version of the internet protocol intended to succeed the previous version IPv4. IPv6 also known IP Next Generation IPng was designed to take an evolutionary step forward by IETF after realization that current IP address space was running out. IPv6 comes with a 128 bit address scheme and an address space of 2^{128} (approximately 3.4×10^{38}) addresses, enough to cover nearly every connected device on earth with a global unique address (Dunn, 2002). Such a large address space allows for every device and user in the world to connect to the internet. It also eliminates the use of NAT in IPv6 and improves connectivity, reliability and flexibility in the network. The design objectives of IPv6 were to support larger address space, security in the protocol and real time multimedia transmission. IPSec support has become a mandatory requirement in IPv6 unlike in IPv4 where it was optional. Payload identification (used in QoS) has been replaced by Flow Label field in IPv6 packet. The concept of fragmentation has been removed. The checksum and options has been replaced by extension headers in IPv6. Also IPv6 does not require manual configuration or DHCP because the system participates in "stateless" auto configuration which is one of the design goals of IPv6. Finally the packet header size has also been changed from 20 byte in IPv4 to 40 byte in IPv6 (Shah & Parvez,2014).

2.2.1 Header Structure

As specified in (Hinden & Deering, 1995), 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 options field has been replaced by extension header field. The main motive behind redesigning the header was to improve performance in header processing by nodes. The IPv6 header is shown in the figure 2.1.

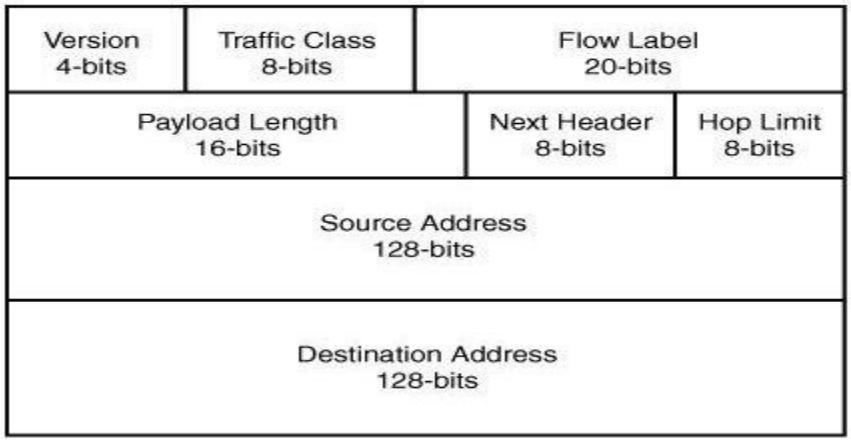

Figure 2.1 IPv6 Header Structure

Version: It describes the current version of the IP protocol. Its value is 6 for IPv6.

Traffic class: Previously in IPv4, defined as the type-of-service (ToS), the traffic class field defines the class-of-service priority of the packet. This field is used to handle real time data and multimedia. Its length is 8 bits. Priority ranges from 0 (lowest) to 7 (highest).

Flow Label: It is used by the source to label all packets belonging to a particular flow. The flow is a unique combination of the source address and the value of a non zero flow label. Multiple flows may exist between destination and source nodes. The routers treat packets belonging to a particular flow in a similar way .Its length is 20 bits.

Payload Length: This field specifies the length of the IPv6 payload. Its Length is 16 bits.

Next Header: This field shows the next extension header to examine. Its Length is 8 bits.

Hop Limit: Also known as TTL in IPv4, the value in this field gets decremented each time packet passes through a router. When the value approaches zero without making up to its intended destination, the packet gets discarded. The maximum allowed value in IPv6 is 255 hops. The length of this field is 8 bits.

Source and Destination Address: This field specifies the 128 bit source and destination IP addresses.

2.2.2 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 2.2

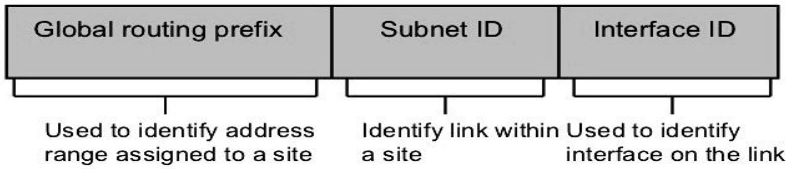

Figure 2.2 IPv6 address format

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

Subnet ID (16 bits) identifies the subnet within the network. It is designed to be structurally hierarchical by site admin's.

Interface Identifier (64 bits) identifies an interface within the link. It is usually constructed from the Mac address of the node or through some random number generation algorithm.

Similar to IPv4's CIDR format, an IPv6 address can be written in IPv6 address/prefix length form 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 parts. A /64 prefix can be allocated when it is known that one and only one subnet is needed. A /128 prefix can be allocated when it is absolutely known that one and only one device is connecting.

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 three types of addresses for IPv6,

Unicast Addresses identifies a single unique interface on the network. The packet sent to this address is delivered to the interface identified by it. Unicast addresses can be of type Global Unicast, Site Local Unicast and Link Local Unicast.

Anycast Address identifies a group of interfaces on the network; however a packet sent to this address is delivered only to the nearest node determined by the metrics of the routing protocol.

Multicast Address identifies a group of interfaces identified by a multicast group address. The packet sent to this address is delivered to all the members 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 used to send packets to itself. It is normally useful in troubleshooting and testing the IP network.

IPv4 compatible IPv6 address This type of address is used to tunnel IPv6 packets over an IPv4 infrastructure. The IPv4 address is embedded in the lower 32 bits of an IPv6 address .i.e. Format is **::**/96+32 bit IPv4 address.

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.

2.2.3 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:

Hop by Hop Option (Next Header value 0): This option is used when the source passes the information to all the routers visited by a datagram. Only 3 options are currently defined so far: Pad-1, Pad-n, Jumbo payload. Pad-1 option having length 1 byte is designed for alignment purposes. Pad-n option is similar to pad-1 except it's used when 2 or more bytes are used for alignment purposes. Jumbo payload refers to a payload length more than 65,535 bytes.

Routing Header (Next Header value 43): It involves the concept of strict source route and loose source route as in IPv4. Strict source route is used by the source for predetermined route for the datagram as it travels through the internet. The sender can make a choice about route with a specific type of service such as minimum delay or max throughput. It may also choose a route that is safer and more reliable for the sender's purpose. If a datagram chooses a strict source route, all the defined routers in the option are to be visited by the datagram. Loose source route is similar to the strict source route but a bit flexible. Along with each router in the list that must be visited, the datagram can visit other routers as well which are not in the list.

Fragmentation (Next Header value 44): Its same concept as in IPv4 however with a little difference. In IPv4, the source or a router fragments the datagram if the size of the datagram is larger than the supported MTU of the network over which the datagram has to travel. In IPv6, the original source can only fragment. A source then finds the smallest value of MTU supported by any network on the path by using a technique for path MTU discovery. Using this gained knowledge, the source then re-fragments the datagram.

Authentication (Next Header value 51): This header carries out the validation of the message sender and ensures that the integrity of data is maintained.

Encrypted Security Protocol (Next Header value 50): This header provides confidentiality and guards against eavesdropping.

Destination Option (Next Header value 60): It's used when the source passes the information to the intended destination only. The routers in-between are not permitted to access to this information.

2.3 Need For Migration

The migration to Next Generation Internet Protocol (IPv6) is inevitable because of the unanticipated increase in internet access user base and requirements of the modern day internet. The need for the migration was realized as early as in 1995 which 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 (Parvez & Peer, 2012). The IPv6 protocol boasts a 128 bit address space to allow for massively more addresses i.e. four times that of an IPv4 address. 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.

- *Lack of address Space in IPv4*

IPv6 comes with a massive 128 bit addresses with an address space of 2^{128} (approximately 3.4×10^{38}) addresses. This means 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.

- *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 (Domzal,2013), 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 (Parra, Rios & Rubio, 2011) which are important for high performance of critical real time applications. 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 (Forouzan, 2006) and its best effort service model. 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 (Shah & Parvez,2014).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 on the other hand implements QoS with the

help of two fields i.e. Flow Label and Traffic Class. The 20 bit flow label field is designed to provide special handling for a flow of data. The flow is a unique combination of non zero flow label and source address. The IPv6 routers service the packets in similar fashion 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).

- *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 network. 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, as long as the mobile node's IP address remains the same after such a movement (Qadir & Siddiqi,2011). To accomplish this, connections to mobile nodes are made with a specific address that is always assigned to the mobile node, and through which the mobile node is always reachable. Mobile IPv6 provides Transport layer connection survivability when a node moves from one link to another by performing address maintenance for mobile nodes at the Internet layer.

- *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 (Zhang et al, 2009). IPv6 treats IPSec as an inbuilt component rather than as additional component.

- *Improved Routing*

Routing Deals with the mechanism of delivering packets from intended source to its destination. Routing process has underwent 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.

2.4 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 (Oxley, 2014). 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. Its 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 (Parvez & Peer, 2012) are listed below:

- The operation of legacy IPv4 applications should not be hampered by router supporting encapsulation (e.g. tunnels).

- The performance of IPv6 should be at par with the IPv4 service (e.g. with similar line data speed and characteristics).
- The introduction of new protocol or flaw in any transition mechanism used cannot bargain security of the network.
- 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, which is an IPv6 address format that employs embedded IPv4 addresses. Tunneling is a mechanism that will play a major role in the beginning**.** (Parvez & Peer, 2012)

From the surplus literature available, the roadblocks or bottlenecks to migration can broadly be classified into two categories: Technical and Non-Technical Issues.

2.4.1 Technical Issues

Transitioning to IPv6 from IPv4 deployments is a demanding task. For onward and upward transition to IPv6, network infrastructure, security and data centers must be designed and managed in such a way that provides simultaneous support to both IPv4 and IPv6 (Shah & Parvez,2014). 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 (Govil et al, 2008).

Security has been the prime concern in deployment of IPv6 (Dunmore, 2005). 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 (Parvez & Peer, 2012). 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 (Dunmore, 2005). Deploying IPSec in concurrence with IP translation mechanism like NAT-PT and TRT that include packet modification will render packet as inauthentic (Waddington & Chang, 2002). It also breaks IPSec end-to-end security architecture.

DNS in IPv6 has been changed (Saurabh & Shilpa, 2011) and TCP/IP protocol suite must be redesigned to support the new address format. 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 (Waddington & Chang, 2002).

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.

2.4.2 Non-Technical Issues

Non Technical or Non functional issues also play a major role in obstructing the early adoption of IPv6 (Oxley, 2014) .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 (Che & Lewis, 2010). 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 has encouraged the adoption of IPv6 on priority basis. Also, the IPv6 promotion council of Japan has been set up with three objectives: to collaborate internationally in the deployment 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.

2.5 Guidelines for Migration

Transition Mechanisms must meet the following guidelines (Mackay et al, 2003; 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 connecting devices, the processing and state maintenance loads also grow proportionally which lead to performance slump and system un availability.
- *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 and etc.
- *Ease of Use:* Transition tool configuration should be hidden from the application's end user; if IPv6 is successfully deployed, end users are unlikely to notice the change.
- *Ease of Management:* To introduce a transition mechanism should not bring too much burden of management, and the network during IPv6 transition should be manageable.

2.6 IPv6 Deployment in world

The oldest know IPv6 network known as 6Bone was started in 1996 and by the year 2004 had connected more than 1000 hosts in 50 countries (Hagen, 2006). Initially IETF working groups used it as a test network. The global deployment of IPv6 varies with each continent. The worldwide IPv6 activities are coordinated by International IPv6 forum. The regional task force activities are coordinated by 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).The Regional Task Forces are responsible for coordinating activities in their 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.

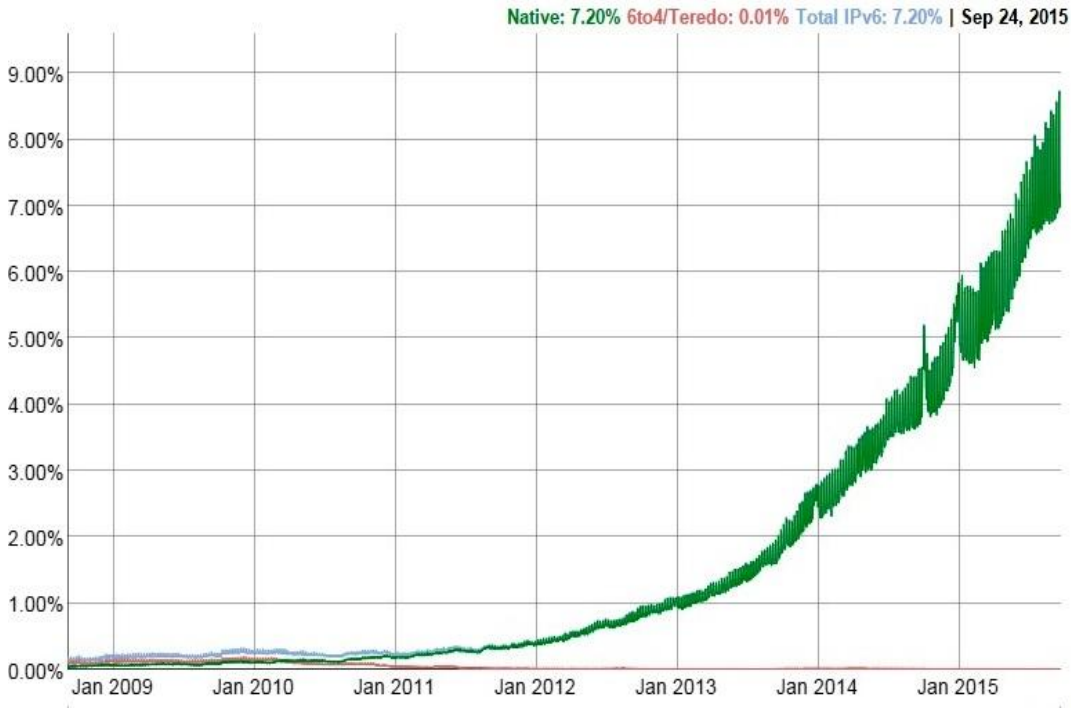

Figure 2.3 Google User IPv6 Adoption Statistics, from Sept 2015

The table 2.1 shows the as data reported by (Google, 2015) on 24th Sep, 2015.The table reveals the percentage of adoption of IPv6 among the leading countries around the world.

Country Name	**IPv6 Adoption %age**	**Country Name**	**IPv6 Adoption %age**
United States	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
United Kingdom	2.64	Belgium	42.17
India	0.47	Romania	6.63

Table 2.1 IPv6 adoption Rate

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 (Frankel et al, 2010).

In China, the China Next Generation Internet (CNGI) project was started in 2001.China's five major telecommunication operators played a key role in this project. IPv6 Mobility was built into the CNGI from the beginning. The CNGI production deployment and application trials in 2005 consisted of a total of 61 projects undertaken by over 100 of China's top technology companies and universities (Hagen, 2006). Metropolitan Area Networks (MANs) are being deployed gradually in each city, with IPv6 playing an important part in this deployment. IPv6 is also being used 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 roadmap lists the following main objectives:

- 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.
- 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, Criterion Networking Academy became the first India based organization to receive IPv6 Forum accreditation for silver and gold certified certification programs from IPv6 Forum. By successfully completing IPv6 Forum certified programs offered by Criterion Networking Academy, IT professionals will be able to demonstrate that they have attained IPv6 knowledge and skills and receive IPv6 Forum Certified Network Engineer certifications at Silver and Gold Engineer levels and include them as part of their professional credentials.

In Europe, the European Commission has taken the lead and supported the introduction of IPv6 since 2000. The European Commission believes that IPv6 is essential for the competitiveness of

their economic area. Telia Sweden was one of the first ISPs to offer commercial IPv6 services. In 2002, Telia already offered six POPs (Points of Presence) in different locations in Europe. Most ISPs currently do not offer IPv6 services commercially, but in the background, many of them have prepared the introduction and will be able to react quickly to growing demand on the market. The numbers of IPv6 Internet backbones and Internet Exchange Points (IEX) are growing. In Europe, there are two major research projects partially funded by the European Commission: The 6net project and Euro6IX.The 6net was a three-year European project created to test whether IPv6 could cope with the demands of today's global Internet. The 6net project ended in 2005. The Internet Society Technologies (IST) initialized the Euro6IX project. Its goal was to support a rapid introduction of IPv6 in Europe.

The German company Telekom stated in early 2004 that they believe that by the year 2020, global telephone communication will be entirely IP-based. Many of the telecom providers are preparing for this challenge in the background. There are a number of VoIP implementations using IPv6. Car vendors will use IP as well. Renault, for instance, has a prototype of an IPv6-networked car that they co-developed with Cisco. It has a Cisco router built-in with a Mobile IPv6 implementation, so the car has an internal IPv6-based network that can be used for monitoring, control, and maintenance; for accessing weather, traffic, and road condition information; or by passengers to connect through wireless or Bluetooth 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 connection depending on its position. The systems and devices connected from inside the car will not lose their connections while the router is switching from one network to another.

The U.S. DoD's announced that it will migrate its network to IPv6 by 2008. Starting in 2003, all IT purchasing done by DoD agencies had to include requirements for IPv6 enablement. Given that the U.S. DoD's IT spending budget is around 30 billion dollars a year (USD), this provides significant motivation for vendors. Many other defense departments and NATO allies all over the globe have followed their example. This decision will accelerate the IPv6 market not only in the United States, but all over the world.

2.7 Summary

Migration Process from IPv4 to IPv6 is been often compared to the Y2K problem, demanding time and investment of resources. Companies are yet to recognize IPv4 number exhaustion as an alarming problem, and are not ready to put off the investment required into the future. In the future there may be risk of insufficient time and cost .The cost of migration to IPv6 could be a problem. Costs involved include renumbering networks and running two protocol stacks (IPv4 and IPv6) at the same time, upgrade to relevant software and hardware, training the manpower, and testing network implementations. However IPv6 does provide considerable benefits and features required by the modern secure internet. Given the number of problems in the current internetwork, migration process may be the only solution viable in the long run.