Seminar Report
on

IPv6 : Next Generation IP

Presented by
N Ranjith Kumar
04IT6003

School of Information Technology
Indian Institute of Technology-Kharagpur

Table of Contents

1. Abstract:

The need for a new Internet Protocol is well understood and accepted in the networking industry. Requirements for more address space, simpler address design and handling at the IP layer, better QoS(Quality of service) support, greater security, and an increasing number of media types and Internet-capable devices have all contributed to drive the development of Internet Protocol version 6 (IPv6).

IPv4, the current version of the Internet Protocol deployed worldwide, has proven remarkably robust, easy to implement, and interoperable with a wide range of protocols and applications. Though substantially unchanged since it was first specified in the early 1980s, IPv4 has supported the scaling of the Internet to its current global proportions. However, the ongoing explosive growth of the Internet and Internet services has exposed deficiencies in IPv4 at the Internet's current scale and complexity. IPv6 was developed specifically to address these deficiencies, enabling further Internet growth and development.

In this seminar, I would like to specify the basics of IPv6, its deployment, and strategies for managing the transition from IPv4 to IPv6, its approach, development and advances in Ipv6.

2. Introduction:

Today's internet operates over one common network layer datagram protocol, Internet Protocol version 4 or IPv4. Virtually all interner communication services have been using the same basic IPv4 packet format over 25years, providing that IPv4 was extremely well designed and in a sense is an unprececedented success in an otherwise rapidly changing world of computer networks. However for more than 10years reaserches have been discussing the need for an improved version of Ip, originally called next-generation IP(Ipng), now called IP version 6(IPv6). The fact that IPv4 has been so tremendously successful and widely deployed makes it very diificuilt for any successor protocol to enter the secene. It obvios that marginal improvements over IPv4 would not justify the strong impact and therefore huge cost that the introduction of a new layer protocol. Hence in the early '90s a new design addressing most of the recognized weaknesses of IPv4 was started with in the Internet Engineering Task Force(IETF). The result was IPv6 offers is increased address space. Ultimately, this will lead to network simplification , fisrt through less need to maintain routing state within the network and second through reduced need for address translation; hence, it will improve the scalability of the internet. Due to early unbalanced IP address allocation policies, the need for more address space is not yet so pressing in the western world. However, already today some geographic regions, especially levels of Network Address Translator(NATs) to provide Internet access for those who need it. This problem will dramatically worsen in two phases.

Phase-1

First phase is the introduction of third-generation(3G) mobile communication. If every mobile terminal requires a permanent IPv4 address, we will quickly exhaust the remaining 20-30 percent of IPv4 address. This is true that 2G and 3G network provides make use of private/or temporary address through the use of NATs and protocols like DHCP, and that NATs to some extent enhance the privacy of mobile user; on the other hand, it also greatly increases network complexity and hinder easy reachabilty for mobile terminals. This is not a critical problem for web surfing, but is a huge barrier to the widespread introduction of peer-to-peer application.

Phase-2

The second phase will be the introduction of truly ubiquitous Networking. When every appliance or sensor needs an IP address, the demand for address space will grow dramatically. At that time the seemingly huge 128-bit address space of IPv6 may be just adequate.

Since the introduction of a new network layer protocol with new packet and header formats is a complex and costly process, IPv6 contains many other enhacements towards better mobility support, integrated security and multicast, a new routing mode called any cast , we may as well flow labels to ease quality of service management. Once the IP layer needs to be changed, we may as well include all features deemed useful for the future. The next change may be another 25 years out.

A significant obstacle to the success of IPv6 is application transitioning. Although support IPv6 in new applications is relatively straightforward, realizing a dual v4/v6 capability for every old application is not. The volume of legacy applications and tools, as well as their life span, is just too big . Hence, the introduction of IPv6 as a new network layer will be a gradual process, lasting many

years. On the other hand, there is no single killer application demonstrating the superiority of IPv6 from a service point of view. Advantages may become obvious only when looking large scale (i.e., millions of nodes); they may never become convincing in small trails with a few hundred computer . Network management tools exploiting of a new IPv6 capabilities in large networks are one family of IPv6 applications desperately needed. Demonstrating the benefit of IPv6 for peer-to-peer applications like voice over IP or distributing gaming could stimulate user demand. However, as of today little is happening in this domain, leading to a situation where IPv6 deployment is delayed due to lack of end user demand. The fact is the at the IPv6 provides important and useful changes that are critical to the long-standing of IP packet technologies.
1.How to introduce the IPv6 into existing networks
2. How to take advantage of its new features.

3. IP Version 6 Addressing Architecture

This defines the addressing architecture of the IP Version 6 protocol [IPv6]. It includes the IPv6 addressing model, text representations of IPv6 address, definition of IPv6 unicast address, anycast address, and multicast address, and an IPv6 nodes required address.

3.1. IPv6 Header format

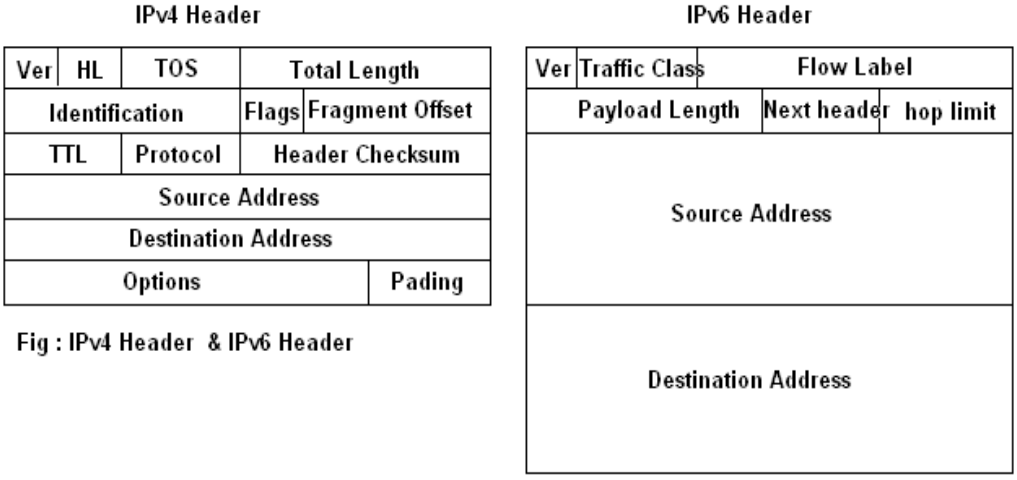

Fig : IPv4 Header & IPv6 Header

3.2. IPv6 Addressing

IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces. There are three types of addresses:

3.2.1.Unicast: An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

***3.2.2.Anycast*:** An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance).

***3.2.3Multicast*:** An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

There are no broadcast addresses in IPv6, their function being superseded by multicast addresses. In IPv6, all zeros and all ones are legal values for any field,unless specifically excluded. Specifically, prefixes may contain zero-valued fields or end in zeros.

3.3.Addressing Model :

IPv6 Addresses of all types are assigned to interfaces, not nodes.Since each interface belongs to a single node, any of that node's Interfaces' unicast addresses may be used as an identifier for the node.

An IPv6 unicast address refers to a single interface. A single interface may be assigned multiple IPv6 addresses of any type (unicast, anycast, and multicast). There are two exceptions to this model. These are:

1) A single address may be assigned to multiple physical interfaces if the implementation treats the multiple physical interfaces as one interface when presenting it to the internet layer. This is useful for load-sharing over multiple physical interfaces.

2) Routers may have unnumbered interfaces (i.e., no IPv6 address assigned to the interface) on point-to-point links to eliminate the necessity to manually configure and advertise the addresses. Addresses are not needed for point-to-point interfaces on routers if those interfaces are not to be used as the origins or destinations of any IPv6 datagrams.

IPv6 continues the IPv4 model that a subnet is associated with one link. Multiple subnets may be assigned to the same link.

3.4.Text Representation of Addresses

There are three conventional forms for representing IPv6 addresses as text strings:

1) The preferred form is x:x:x:x:x:x:x:x, where the 'x's are the hexadecimal values of the eight 16-bit pieces of the address.
   Examples:

   FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
   1080:0:0:0:8:800:200C:417A

Note that it is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field (except for the case described in 2.).

2) Due to the method of allocating certain styles of IPv6 addresses, it will be common for addresses to contain long strings of zero bits. In order to make writing addresses containing zero bits easier a special syntax is available to

compress the zeros. The use of "::" indicates multiple groups of 16-bits of zeros. The "::" can only appear once in an address. The "::" can also be used to compress the leading and/or trailing zeros in an address.

For example the following addresses:

1080:0:0:0:8:800:200C:417A	A unicast address
FF01:0:0:0:0:0:0:43	A multicast address
0:0:0:0:0:0:0:1	The loopback address
0:0:0:0:0:0:0:0	The unspecified addresses

may be represented as:

1080::8:800:200C:417A	A unicast address
FF01::43	A multicast address
::1	The loopback address
::	The unspecified addresses

3) An alternative form that is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes is x:x:x:x:x:x:d.d.d.d, where the 'x's are the hexadecimal values of the six high-order 16-bit pieces of the address, and the 'd's are the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation).

Examples:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

or in compressed form:

::13.1.68.3

::FFFF:129.144.52.38

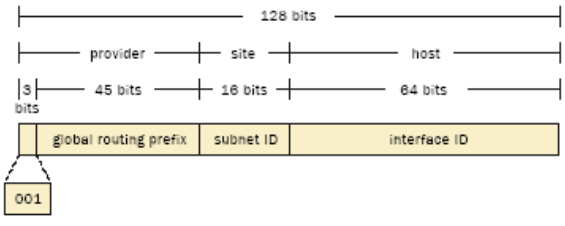

Figure . Global unicast address format.

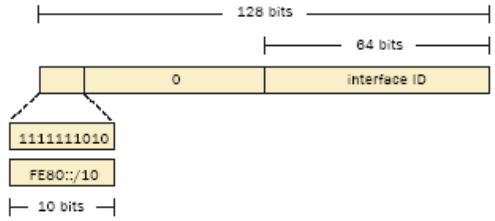

Figure . Link-local unicast address format.

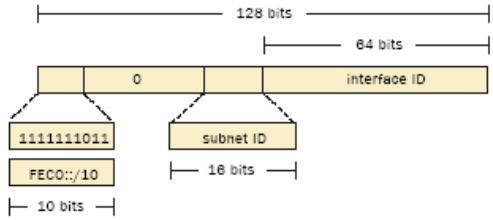

Figure . Site-local unicast address format.

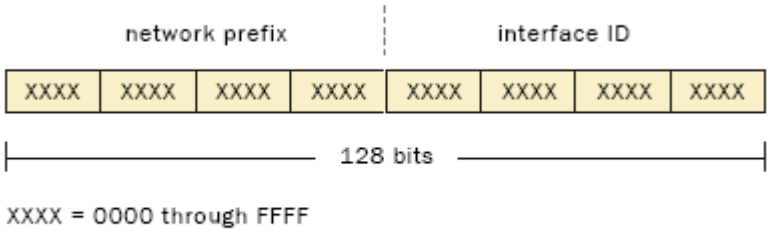

Figure . IPv6 address format.

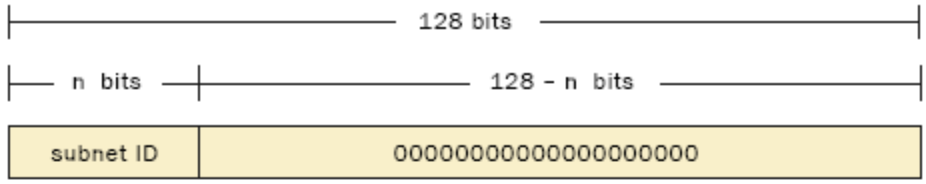

Figure . Anycast address format.

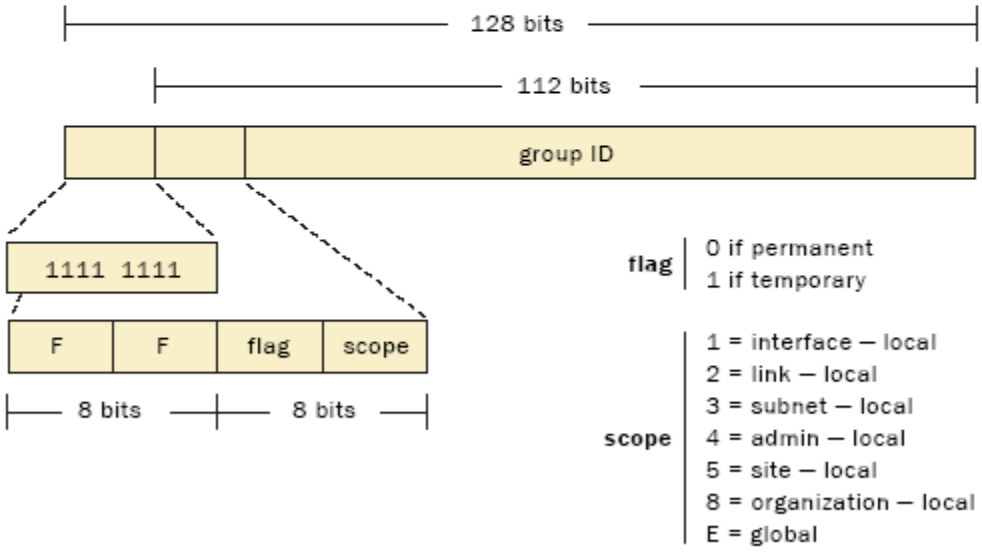

Figure . Multicast address format.

4. Goals of IPv6 address space management

4.1. Goals

IPv6 address space is a public resource that must be managed in a prudent manner with regards to the long-term interests of the internet. Responsible address space management involves balancing a set of sometimes competing goals. The following are the goals relevant to IPv6 address policy.

4.2. Uniqueness

Every assignment and/or allocation of address space must guarantee uniqueness worldwide. This is an absolute requirement for ensuring that every public host on the Internet can be uniquely identified.

4.3. Registration

Internet address space must be registered in a registry database accessible to appropriate members of the Internet community. This is necessary to ensure the uniqueness of each Internet address and to provide reference information for Internet troubleshooting at all levels, ranging from all RIRs and IRs to end users.

The goal of registration should be applied within the context of reasonable privacy considerations and applicable laws.

4.4. Aggregation

Wherever possible, address space should be distributed in a hierarchical manner, according to the topology of network infrastructure. This is necessary to permit the aggregation of routing information by ISPs, and to limit the expansion of Internet routing tables.

This goal is particularly important in IPv6 addressing, where the size of the total address pool creates significant implications for both internal and external routing.

IPv6 address policies should seek to avoid fragmentation of address ranges.

Further, RIRs should apply practices that maximize the potential for subsequent allocations to be made contiguous with past allocations currently held. However, there can be no guarantee of contiguous allocation.

4.5. Conservation

Although IPv6 provides an extremely large pool of address space, address policies should avoid unnecessarily wasteful practices. Requests for address space should be supported by appropriate documentation and stockpiling of unused addresses should be avoided.

4.6. Fairness

All policies and practices relating to the use of public address space should apply fairly and equitably to all existing and potential members of the Internet community, regardless of their location, nationality, size or any other factor.

4.7. Minimized Overhead

It is desirable to minimize the overhead associated with obtaining address space. Overhead includes the need to go back to RIRs for additional space too frequently, the overhead associated with managing address space that grows through a number of small successive incremental expansions rather than through fewer, but larger, expansions.

4.8. Conflict of goals

The goals described above will often conflict with each other, or with the needs of individual IRs or end users. All IRs evaluating requests for allocations and assignments must make judgments, seeking to balance the needs of the applicant with the needs of the Internet community as a whole.

In IPv6 address policy, the goal of aggregation is considered to be the most important.

5. IPv6 Policy Principles

To address the goals described in the previous section, the policies in this document discuss and follow the basic principles described below.

5.1. Address space not to be considered property

It is contrary to the goals of this document and is not in the interests of the Internet community as a whole for address space to be considered freehold property.

The policies in this document are based upon the understanding that globally-unique IPv6 unicast address space is licensed for use rather than owned. Specifically, IP addresses will be allocated and assigned on a license basis, with licenses subject to renewal on a periodic basis. The granting of a license is subject to specific conditions applied at the start or renewal of the license.

RIRs will generally renew licenses automatically, provided requesting organizations are making a good-faith effort at meeting the criteria under which they qualified for or were granted an allocation or assignment. However, in those cases where a requesting organization is not using the address space as intended, or is showing bad faith in following through on the associated obligation, RIRs reserve the right to not renew the license.

Note that when a license is renewed, the new license will be evaluated under and governed by the applicable IPv6 address policies in place at the time of renewal, which may differ from the policy in place at the time of the original allocation or assignment.

5.2. Routability not guaranteed

There is no guarantee that any address allocation or assignment will be globally routable.

However, RIRs must apply procedures that reduce the possibility of fragmented address space which may lead to a loss of routability.

5.3. Minimum Allocation

RIRs will apply a minimum size for IPv6 allocations, to facilitate prefix-based filtering.

The minimum allocation size for IPv6 address space is /32.

5.4. Consideration of IPv4 Infrastructure

Where an existing IPv4 service provider requests IPv6 space for eventual transition of existing services to IPv6, the number of present IPv4 customers may be used to justify a larger request than would be justified if based solely on the IPv6 infrastructure.

6. Benefits of IPv6

Aside from the increased address space,IPv6 offers a number of other key design improvements over IPv4.

6.1. Improved efficiency in routing and packet handling

IPv6's very large addressing space and network prefixes (Figure 1) allow the allocation of large address blocks to ISPs and other organizations. This enables an ISP or enterprise organization to aggregate the prefixes of all its customers (or internal users) into a single prefix and announce this one prefix to the IPv6 Internet. Within the IPv6 address space, the implementation of a multi-leveled address hierarchy provides more efficient and scalable routing. This hierarchical addressing structure reduces the size of the routing tables Internet routers must store and maintain. Though the IPv6 header is larger, its format is simpler than that of the IPv4 header. The IPv6 header removes the IPv4 fields for Header Length (IHL), Identification, Flags, Fragment Offset, Header Checksum, and Padding, which speeds processing of the basic IPv6 header. Also, all fields in the IPv6 header are 64-bit aligned, taking advantage of the current generation of 64-bit processors.

6.2. Support for autoconfiguration and plug and play

The need for plug-and-play autoconfiguration and address renumbering has become increasingly important to accommodate mobile services (data and voice) and Internetcapable appliances. IPv6's built-in address autoconfiguration feature enables a large number of IP hosts to easily discover the network and obtain new, globally unique IPv6 addresses. This allows plug-and-play deployment of Internet-enabled devices such as cell phones, wireless devices, and home appliances. The autoconfiguration feature also makes it simpler and easier to renumber an existing

network. This enables network operators to manage the transition from one provider to another more easily.

6.3. Support for embedded IPSec

Optional in IPv4, IPSec is a mandatory part of the IPv6 protocol suite. IPv6 provides security extension headers, making it easier to implement encryption, authentication, and virtual private networks (VPNs). By providing globally unique addresses and embedded security, IPv6 can provide end-to-end security services such as access control, confidentiality, and data integrity with less impact on network performance.

6.4. Enhanced support for Mobile IP and mobile computing devices

Mobile IP, defined in an IETF standard, allows mobile devices to move around without breaking their existing connections — an increasingly important network feature. Unlike IPv4, IPv6 mobility uses built-in autoconfiguration to obtain the Care-Of-Address, eliminating the need for a Foreign Agent. In addition, the binding process allows the Correspondent Node to communicate directly with the Mobile Node, avoiding the overhead of triangular routing required in IPv4. The result is a much more efficient Mobile IP architecture in IPv6.

6.5. Elimination of the need for network address translation (NAT)

NAT was introduced as a mechanism to share and reuse the same address space among different network segments. While it has temporarily eased the problem of IPv4 address shortage, it has also placed a burden on network devices and applications to deal with address translation. IPv6's increased address space eliminates the need for address translation, and with it, the problems and costs associated with NAT deployment.

6.6. Support for widely deployed routing protocols.

IPv6 maintains and extends support for existing Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). For example, OSPFv3, IS-ISv6, RIPng and MBGP4+ have been well defined to support IPv6.

6.7. Increased number of multicast addresses, and support for multicast

IPv6 multicast completely replaces IPv4 broadcast functionality, by handling IPv4 broadcast functions such as router discovery and router solicitation requests. Multicast saves network bandwidth and improves network efficiency.

7. IPv6 Operation

7.1. Neighbor discovery

The neighbor discovery protocol enables IPv6 nodes and routers to determine the link-layer address of a neighbor on the same network, and to find and track neighbors. The IPv6 neighbor discovery process uses IPv6 ICMP (ICMPv6) messages and solicited-node multicast addresses to determine the link-layer address of a

neighbor on the same network, verify the reachability of a neighbor, and keep track of neighbor routers. When a node wants to determine the linklayer address of another node on the same local link, a neighbor solicitation message is sent on the local link, carrying the sender's own link-layer address. After receiving the neighbor solicitation message, the destination node replies by sending a neighbor advertisement message with its own link-layer address on the local link. After the neighbor advertisement is received, the source and destination nodes can communicate. Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link.

7.2. Router discovery

To discover the routers on the local link,the IPv6 router discovery process uses router advertisement and solicitation messages. Router advertisements messages are sent out periodically on each configured interface of an IPv6 router, and also in response to router solicitation messages from IPv6 nodes on the link. When a host does not have a configured unicast address, it sends a router solicitation message, enabling the host to autoconfigure itself quickly without having to wait for the next scheduled router advertisement message. A router advertisement contains or determines:

- The type of autoconfiguration a node should use – stateless or stateful.
- The Hop limit value a node should place in the IPv6 header.
- The network prefix a node should use to form the unicast address.
- The lifetime information of the included network prefix.
- The maximum transmission unit (MTU) size a node should use in sending packets.
- Whether the originating router should be used as default router.

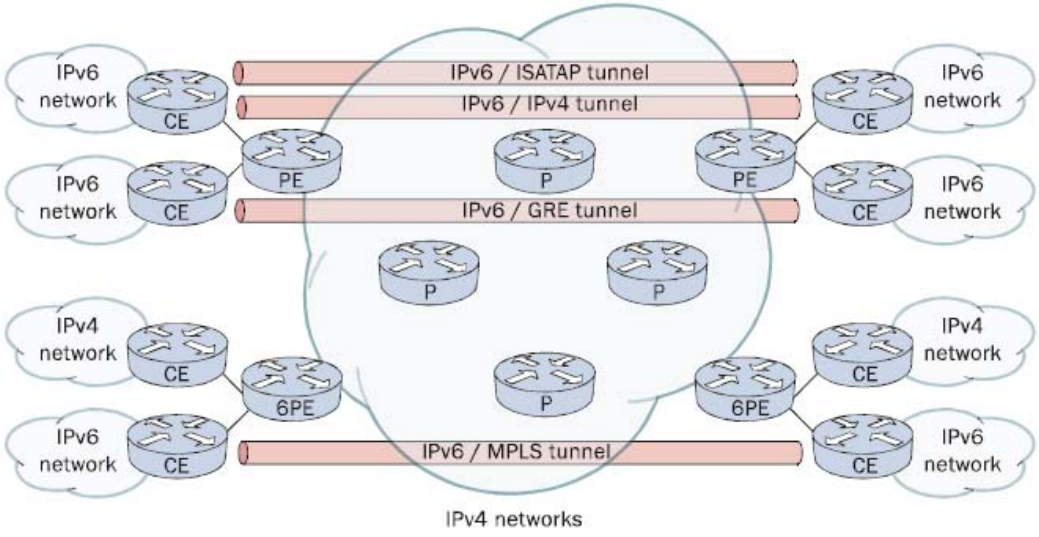

Figure 9. IPv6 tunnel mechanisms.

7.3. Stateless autoconfiguration and renumbering of IPv6 nodes

Stateless autoconfiguration enables serverless basic configuration of IPv6 nodes and easy renumbering. Stateless autoconfiguration uses the network prefix information in

the router advertisement messages as the /64 of prefix of the node address. The remaining 64 bits address is obtained by the MAC address assigned to the Ethernet interface combined with additional bits in EUI-64 format. For instance, a node with Ethernet interface address 0003B61A2061, combined with network prefix 2001:0001:1EEF:0000/64 provided by router advertisement, will have an IPv6 address as 2001:0001:1EEF:0000:0003:B6FF:FE1A: 2061. Renumbering of IPv6 nodes is possible through router advertisement messages, which contain both the old and new prefix.A decrease in the lifetime value of the old prefix alerts the nodes to use the new prefix, while still keeping their current connections intact with the old prefix. During this period, nodes have two unicast addresses in use. When the old prefix is no longer usable, the router advertisements will include only the new prefix.

7.4. Path Maximum Transfer Unit (MTU)

IPv6 routers do not handle fragmentation of packets, which is done, when necessary, by the originating or source node of the packet. IPv6 uses ICMP error reports to determine whether the packet size matches the MTU size along the delivery path. When a node reports “packet too big” via an ICMP error report, the source node will reduce the size of the transmit packet. The process is repeated until there is no “packet too big” error along the delivery path. This allows a node to dynamically discover and adjust to differences in the MTU size of every link along a given data path.

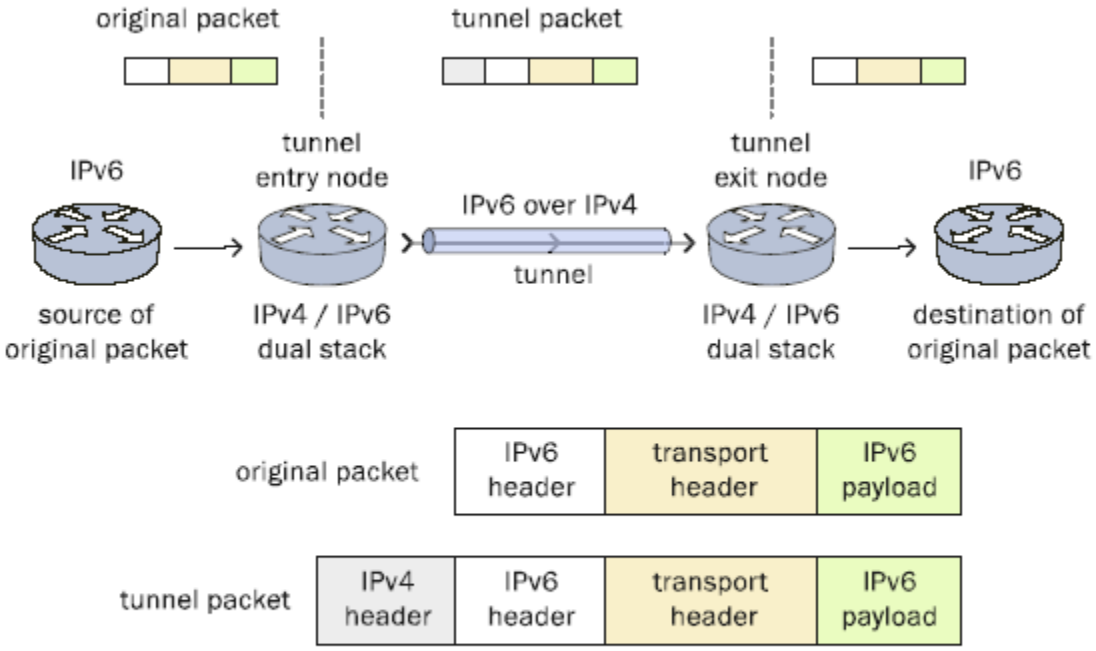

Figure 8. IPv6 over IPv4 tunneling.

7.5. DHCPv6 and Domain Name Server (DNS)

In addition to stateless autoconfiguration, IPv6 also supports stateful configuration with DHCPv6. The IPv6 node has an option to solicit an address via DHCP server

when a router is not found. The operation of DHCPv6 is mostly similar to that of DHCPv4; however, DHCPv6 uses multicast for many of its messages. IPv6 also introduces a new record type to accommodate IPv6 addresses in Domain Name Servers. The AAAA record, also known as “quad A”, has been recommended by the IETF for mapping a host name to an IPv6 address.

8. IPv6 Deployment

IPv6 provides many benefits over legacy IPv4 technology; however, all agree that any successful strategy for IPv6 deployment requires it to coexist with IPv4 for some extended period of time. A
number of strategies have been developed for managing this complex and prolonged transition from IPv4 to IPv6. The following subsections describe several of these strategies.

8.1. Dual-stack backbone

In dual-stack backbone deployment, all routers in the network maintain both IPv4 and IPv6 protocol stacks. Applications choose between using IPv4 or IPv6, with the application selecting the correct address based on the type of IP traffic and particular requirements of the communication. Today, dual-stack routing is the preferred deployment strategy for network infrastructures with a mixture of IPv4 and IPv6 applications that require both protocols. This strategy has several limitations, however: all routers in the network must be upgraded to IPv6; routers also require a dual addressing scheme, dual management of the IPv4 and IPv6 routing protocols and sufficient memory for both the IPv4 and IPv6 routing tables.

8.2. IPv6 over IPv4 tunneling

IPv6 over IPv4 tunneling encapsulates IPv6 traffic within IPv4 packets, to be sent over an IPv4 backbone (Figure 8). This enables “island” IPv6 end systems and routers to communicate through an existing IPv4 infrastructure. A variety of tunneling mechanisms are available for deploying IPv6 (Figure 9), as described in the following sections.

8.3. Manually configured tunnels.

As defined by RFC 2893, both end points of the tunnel need to be configured with appropriate IPv6 and IPv4 addresses. The edge routers sitting at the end points, usually a dual stack router, will forward the tunneled traffic based on the configuration. GRE (Generic Routing Encapsulation) tunnels. Defined to transport data over the IPv4 network, GRE allows one network protocol to be transmitted over another network protocol, by encapsulating the packets to be transmitted within GRE packets. GRE is an ideal mechanism to tunnel IPv6 traffic.

8.4. IPv4-compatible tunnels or 6over4 tunnels.

As defined in RFC 2893, these tunnel mechanisms automatically set up tunnels based on the IPv4-compatible IPv6 addresses. An IPv4-compatible IPv6 address defines the left-most 96 bits as
zero, followed by an IPv4 address embedded in the last 32 bits. For example, 0:0:0:0:0:0.64.23.45.21 is an IPv4-compatible address.

8.5. 6to4 tunnels.

As defined by RFC 3056, 6to4 tunneling uses an IPv4 address embedded in the IPv6 address to identify the end point of the tunnel and setup tunnel automatically (Figure 10).

8.6. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunnels.

As defined in draft-ietfngtrans- isatap-16, ISATAP tunneling is very similar to 6to4 tunneling, but is designed for use in a local site or campus network. The ISATAP address contains the 64-bit network prefix, 0000:5EFE, and an IPv4 address identifying the address of the tunnel end point (Figure 11).

8.7. MPLS (Multi-Protocol Label Switching) tunnels.

Using MPLS technology, isolated IPv6 domains can communicate with each other over a MPLS IPv4 core network. Because MPLS forwarding is based on labels rather than the IP header itself, this implementation requires far fewer backbone infrastructure upgrades and less reconfiguration of core routers, providing a very cost-effective way to deploy IPv6. Additionally, MPLS's inherent VPN and traffic engineering services allow IPv6 networks to be combined into VPNs or extranets over an infrastructure supporting IPv4 VPNs and MPLS-TE.

9. IPv6 Challenges

Expectations for IPv6 are high: it is perceived as the protocol of the next generation Internet, replacing today's legacy IPv4-based networks. As described above, IPv6 deploys a new data plane to fix various addressing and efficiency problems with IPv4, and a new routing control plane to effectively make use of the new addresses. The impact of the new data and control planes on today's networks is significant. Failures or interruption are unacceptable in missioncritical networking environments. Network operators and service providers are facing tough questions – when and how to migrate to IPv6? To answer these questions with certainty, they need assurance that in their particular networks, IPv6 will provide:

- Rapid expansion needed for more users and devices.
- Smooth transition and coexistence with IPv4.
- Robust network failure recovery.

• Deliverable Quality of Service.
• Improved network security.

Network equipment manufacturers (NEMs) face the challenge of building routers to support both IPv6 and IPv4 networks, with two sets of control and data planes. This can add significant resource requirements to routers supporting dual stacks, impacting router performance and scalability. Additional transition mechanisms like tunneling and application/address translation add complexity to router design. For end users, IPv6 improves productivity by enabling network connectivity via a wider range of media and delivery mechanisms. But for general acceptance, the new IPv6 networks must demonstrate responsiveness at least equal to that of IPv4. In addition, while several end user environments and applications like Windows XP, Linux, and sendmail support IPv6 today, more applications are needed to enhance IPv6's overall acceptance.

10. Home Networking with IPv6 (Case Study)

The need for home networks is growing at a rapid rate. There are several factors driving this increase. In general, there are three main drivers of home networks today. These are the continual growth in the use of home PCs, the rapid introduction of smart devices, and the phenomenal growth of home-based businesses and telecommuting. In 1999, 43.1 million homes in the United States owned a PC. Of these, 9.4 million owned two PCs and 3 million owned 3 or more PCs. As the PC becomes more and more of a commodity, the number of homes with PCs will increase as will the number of homes containing multiple PCs. The owners of these machines will want to be able to share data, both with other machines in the home and with machines via the Internet.

The introduction of smart devices is giving consumers the flexibility of automating tasks.Devices such as Personal Digital Assistants (PDAs), smart phones, and set-top boxes are offering new capabilities and features. Smart devices will be able to control such systems as smart appliances (Internet refrigerator, microwave), electronics (home theater, stereo), and home security systems. In order to perform these tasks, the smart devices and the smart appliances will have to be network-capable and globally reachable. The home-based workforce is increasing at an incredible rate. In 1998, there were 13 million home-based businesses with a double-digit growth rate. From 1995 to 1997 the number of telecommuters in the United States grew by 30%. In 1998 alone, that number grew by another 40%. As the number of home-based workers increases, so will the need for home networks. Home-based businesses will want the capability of operating on the World Wide Web, accessing home resources while traveling, and sharing data with customers and co-workers. As these markets grow, the need for flexible home-networking tools increases. The home network will have to be robust, but simple. Much like the PC, users will want to be able to plug new devices into the network and have them work. If a customer has to maintain a complex system in the home, it will not be widely used. For these reasons, the Internet Protocol Version 6 (IPv6) will play a critical roll in the home networking market.

If widespread use of home networks is to be realized, the technology needed to build these networks must meet some important goals. These goals are meant to ensure that the non-technical user will be willing to use the technology. If the tools are too complicated, the market for home networks will be limited to those people

who are willing to invest time in learning new technology. The first goal is to have a network that requires a low amount of configuration and maintenance. If the user spends a large period of time setting up or maintaining the network, it will decrease the willingness to use the technology. If things are kept simple, widespread acceptance will be more likely. This should apply to both devices installed during the original network setup as well as the introduction of new devices into an existing home network. The next goal is to allow a wide range of devices to participate in the home network. These networks should not be limited to the devices that are network capable today. The technology used to for these networks should be flexible enough to allow for their use on a wide range of devices and appliances. Flexibility in the type of communication media is the next goal. The home networking market should not and will not be restricted to traditional copper wire networks. Home networking tools must support a wide spectrum of media. Possible media types are Ethernet, RF (Bluetooth), firewire (IEEE 1394), wireless (IEEE 802.11) and power-line. Regardless of the media, home-networking appliances should work the same. Finally, home-networking users will expect to be able to access their networks from remote locations. The home networking tools used must allow for secure access to the home networking user while still keeping unwanted intruders out.

Home networks are likely to follow the general trend of the Internet towards peer-to-peer based applications (e.g. VoIP) as opposed to the current client-server based (web surfing). In addition home networks are also likely to offer services to external users via the Internet (e.g. Web server, or remote control of home electrics/electronics). This is enabled with the increasing bandwidth available to home networks (cable modem, xDSL) and requires incoming connectivity i.e.: publicly addressable home networks.

The following devices have the stateless auto-configuration feature of IPv6 that allows devices to configure globally routable IPv6 address. All these devices are used in a single above considered home say desktop, washing machine, TV, DVD player, oven, scanner etc….

Device-1	FE80::2053:FF:50AB:3F50
Device-2	FE80::1030:23FF:FEAB:20
Device-3	FE80::ABBD:2044:BAD3:5020
Device-4	FE80::AC30:2352:2020:FEED
Device-5	FE80::9A37:25FF:FEED:BA80
	PREFIX = 2880:5E34::/64

In the above table , all of the IPv6 capable devices have configured local-use IPv6 address. These address allow the devices to communicate with one another on the local communication media. For many home network applications, these local-use address will be sufficient. In the case where global reachability is needed, the home gateway device can transmit an advertisement message that indicate the global IPv6 prefix assigned to the network.

In the next table , all of the devices have received the advertisement. The devices extract the IPv6 prefix information and use it to automalically generate their own global IPv6 address. These address can be used by the devices to communicate with any other network-capable device that is reachable via the service provider(s).

Device-1	FE80::2053:FF:50AB:3F50
	2880:5E34::2053:FF:50AB:3F50

Device-2	FE80::1030:23FF:FEAB:20
	2880:5E34::23FF:FEAB:20
Device-3	FE80::ABBD:2044:BAD3:5020
	2880:5E34::ABBD:2044:BAD3:5020
Device-4	FE80::AC30:2352:2020:FEED
	2880:5E34::AC30:2352:2020:FEED
Device-5	FE80::9A37:25FF:FEED:BA80
	PREFIX = 2880:5E34::/64

The major benefit of this functionality is that end-users will not have to now how to configure network information into each individual device. This feature will also help alleviate problems caused by configuration errors.

11. Conclusion

Though the benefits of IPv6 are well understood, the cost of overhauling the existing IPv4 infrastructure is prohibitive for many network operators and service providers. The current attitude toward IPv6 in the US market could be characterized as “IPv4 is working. Why change?” The real driving force for IPv6 will come from countries and regions whose only choice for global competitiveness in the next decade is to change to larger address space. The path to complete global IPv6 connectivity will be lengthy and full of challenges. Many transitional schemes and strategies will be used to ease the pains and minimize investment into IPv6 deployment.

Ipv6 will grow the way the internet did, with pockets of users connecting. However, the protocol will grow faster because the internet infrastructure is already in place. IPv6 will flourish only for certain applications, such as wireless telephony, or in certain markets, such as china. Otherwise, there will be no rush to adoption.

According to IBM, IPv6 is proceeding on schedule . “People have to look at this as a strategic issue”, said ”not as something that is going to be profitable in six months. It is something we have to do make the network grow worldwide for the next 100 years”

12. Acknowledgements

I would like to thank Dr. S. K .Ghosh, Dr. Debasis Samanta, for their review and comments on this document and made my presentation successful.

13. References

1. Internet Protocol Version 6(IPv6) – Conformance and Performance testing
   W. Agoura Road
   [ixia , www.ixiacom.com]
2. Guest editorial- IPv6: The basis for the Next Generation Internet
   Han-chieh chao , heinrich J. stuttgen , Daniel G. Waddington
   [IEEE Communication Magazine. Jan2004]
3. Is IPv6 Finally Gaining Ground ? - - -
   George Lawton [IEEE-Computer august-2001]
4. IPv6- Next Generation Internet Protocol
   [*EDS: eds.com*]

5. IPv6 Address Allocation and Assinment Policy
   [ARIN – American Registry for Internet Numbers:: 26 June 2002]
6. Evolutionary IPv6 *–Adam Stone*
   [IEEE Internet Computing , April –2004]
7. IPv6 Addressing Architecture
   R. Hinden and S. Deering
   [rfc-1884 , December 1995]
8. Home Networking with IPv6
   Brain Haberman, Nortel Networks, George Tsitsis , BT
9. IPv6: Basis for the Next-generation Networks
   Studty and Emulation of IPv6 Internet-Exchange- Based Addressing Models
   Davis Fernandez and Tomas de Miguel
   [IEEE Communication Magazine , January 2004]
10. IPv6 Home Network Domain Name Auto-Configuration for Intelligent Appliances
    Tin-Yu Wu, Chia-Chang Hsu, Han-Chieh Chao
    [Contributed paper Manuscript received by Feb24,2004 – IEEE]
11. A Look at a Native IPv6 Multicast
    Chris Metr and Mallik Tatipamula . Cisco Systems
    [IEEE Computer Society, July-2004, IEEE Internet Computing]

About Me……..,
N Ranjith Kumar (Mtech-IT)
nrk@sit.iitkgp.ernet.in,
http://sit.iitkgp.ernet.in/~nrk