Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Communicating between IPv4 and IPv6

Abhilash Bisht, Narjis Hasan, Palak Mehra
ECE, Lovely Professional University
India

Abstract— In this document, we have discussed the need of deployment of IPv6 to meet the increasing demands of IP addresses with the advent of technology. We analyse trends in the growth of the evolving IPv6 Internet. We find that the IPv6 network is maturing, albeit slowly. IPv4 and IPv6 networks both will exist during the transition period, while the two are not compatible in nature. While most core Internet transit providers have deployed IPv6, edge networks are lagging. This paper contains the transition of Internet Protocol from Version 4 (IPv4) to Version 6 (IPv6). Keeping in mind the coexistence of the two versions, we discuss the methods of communication between them.

Keywords— IPv4, IPv6, dual stack, address translation, tunnelling.

I. INTRODUCTION

In the 1970's, the Department of Defence developed the Transmission Control Protocol (TCP), to provide both Network and Transport layer functions. When this proved to be an inflexible solution, those functions were separated - with the Internet Protocol (IP) providing Network layer services, and TCP providing Transport layer services. Together, TCP and IP provide the core functionality for the TCP/IP or Internet protocol suite.

IP provides two fundamental Network layer services:

1) *Logical addressing* – provides a unique address that identifies both the host, and the network that host exists on.
2) *Routing* – determines the best path to a particular destination network and then routes data accordingly.

The Internet operates by transferring data between hosts in packets that are routed across networks as specified by routing protocols. These packets require an addressing scheme, such as IPv4 or IPv6, to specify their source and destination addresses. Each host, computer or other device on the Internet requires an IP address in order to communicate. IP was originally defined in RFC 760, and has been revised several times. IP Version 4 (IPv4) was the first version to experience widespread deployment, and is defined in RFC 791.

Prior to implementation of IPv4, engineers and scientists working on ARPANET debated on the length of an IP address. The debate was between 32-bit and 128-bit address lengths. The decision was to use a 32-bit length for the IPv4 address, but never foresaw the need for more than 4.3 billion address [1]. Thus, internet was born. On the 3rd of February 2011, the Internet Corporation for Assigned Names and Numbers (ICANN) handed out the last block of the IPv4 addresses [2].

The resulting scarcity of IPv4 address blocks led to gradual depletion of IPv4 address space. In order to save and reuse the address blocks, service providers (SP) resorted to mechanisms like Variable Length Subnet Mask (VLSM), Classless Inter-domain Routing (CIDR), private IP addresses in internal networks and multiple layers of Network Address Translation (NAT). The more ideal approach to solve the issue of address scarcity facing the networking industry was to move towards the IPv6 addressing scheme.

Although version 4 has a forward compatibility with version 6, IPv6 has no built-in backwards compatibility with IPv4, which means IPv6 networks cannot communicate with IPv4 in nature. Essentially IPv6 has created a parallel, independent network that coexist with its counterpart IPv4. If an IPv4 network wants to further support IPv6 communication, it has to carry out dedicated addressing and routing for IPv6, and update the network devices to enable IPv6. [4]Therefore IPv4 network will probably last for a long time. On the other hand, the continuous demands for new IP addresses are driving IPv6 towards a large-scale deployment. Therefore, IPv4 and IPv6 will coexist for a long period, and the transition process will be gradual.

II. IPv4

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) and it is the first version of the Protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet. IPv4 is still by far the most widely deployed Internet Layer protocol. It uses a 32 bit addressing and allows for 4,294,967,296 unique addresses [3]. IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP) [8].

III. THE NEED OF IPV6

The rapid diffusion of the internet and the deployment of the high speed broadband networks have posed the problem of inadequate IPv4 addresses. Moreover this lack has been made worse by the progress made towards the ubiquitous network society, in which various types of information equipment, mobile computers and electrical information appliances work on the internet. The numbering space for IPv4 is very limited taking all the present and future applications of Internet into consideration. Already at the beginning of the 1990s, there was concern regarding the coming depletion of IP numbers. Some 20 years later, the last publicly available IPv4 addresses were allocated by IANA in February 2011, but still IPv6 has been only developed very slowly [4]. These are some limitations of IPv4 which force the need of IPv6,

1) Insufficient IP address space
2) Address prefix allocation
3) Data security

IPv6 is designed to solve the problems of IPv4. It does so by creating a new version of the protocol which serves the function of IPv4, but without the same limitations. Changing IP means changing dozens of Internet protocols and conventions, ranging from how IP addresses are stored in DNS (domain name system) and applications, to how datagrams are sent and routed over Ethernet, PPP, Token Ring, FDDI, and every other medium, to how programmers call network functions.

Some of the major advantages of IPv6 are:

1) *Larger IP address space*: IPv6 has 128-bit address space or 4 times more address bits compared to IPv4's 32-bit address space. This large address space will provide enough address space for many decades to come. In real terms, every residential or commercial customer will be able to receive more address space from TWC than the entire IPv4 address space contains – several billion IP addresses!
2) *Better security*: IPv6 includes security in the underlying protocol. For example, encryption of packets (ESP: Encapsulated Security Payload) and authentication of the sender of packets (AH: Authentication Header).
3) *Consideration to real time*: To implement better support for real-time traffic (such as videoconference), IPv6 includes a flow label mechanism so routers can more easily recognize where to send information.
4) *Plug and play:* IPv6 includes plug and play, which is easier for novice users to connect their machines to the network. Essentially, configuration will happen automatically.
5) *Better optimization*: IPv6 takes the best of what made IPv4 successful and gets rid of minor flaws and unused features

Fig 1. Ratio of IPv6/IPv4 in terms of routing table entries

IV. DIFFERENCES BETWEEN IPV4 AND IPV6

There are major differences between IPv4 and IPv6. In IPv6, ICMP is a crucial component. Besides the basic ICMP messages found in IPv4, IPv6 incorporates numerous new ICMP messages. ARP functionality in IPv4 has effectively been replaced with Neighbour Discovery (ICMP Types 135 & 136) and Router Discovery (ICMP Types 133 & 134) messages. One of the changes that is less obvious to the normal user is the IPv6 packet header. The basic IPv6 header has been streamlined to only contain the following fields: *Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address and Destination Address*. Routers can process this streamlined header more efficiently. The Flow Label is designed to allow a router to efficiently identify packets that belong to the same flow or connection.

TABLE I
COMPARISON OF IPV4 AND IPV6

Comparison of IPv4 and IPv6	
IPv4	**IPv6**
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
Uses broadcast addresses to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, multicast scoped addresses are used.
Fragmentation is supported at originating hosts and intermediate routers.	Fragmentation is not supported at routers. It is only supported at the originating host.
IP header includes a checksum.	IP header does not include a checksum.
IP header includes options.	All optional data is moved to IPv6 extension headers.
IPSec support is optional.	IPSec support is required in a full IPv6 implementation.
No identification of payload for QoS handling by routers is present within the IPv4 header.	Payload identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	Uses ICMPv6 Router Solicitation and Router Advertisement to determine the IPv6 address of the best default gateway and is a required function.
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	Uses multicast Neighbour Solicitation messages for address resolution.
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	Uses Multicast Listener Discovery (MLD) messages to manage local subnet group membership.
Addresses must be configured either manually or through DHCP. (DHCP is not supported in z/OS Communications Server.)	Addresses can be automatically assigned using stateless address auto configuration, assigned using DHCPv6, or manually configured. (DHCPv6 is not supported in z/OS Communications Server.)
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA or IP6.INT DNS domain to map IPv6 addresses to host names.
For QoS, IPv4 supports both differentiated and integrated services.	Differentiated and integrated services are both supported. In addition, IPv6 provides a flow label that can be used for more granular treatment of packets.

V. **IPv6**

IPv6 stands for Internet Protocol version 6 also known IPng (IP next generation) is the second version of the Internet Protocol to be used generally across the virtual world. IPng was not a design goal to take a radical step away from IPv4 but was designed to take an evolutionary step from IPv4. Functions which work in IPv4 were kept in IPng. Functions which didn't work were removed. Like IPv4, IPv6 is an internet-layer protocol for packet switched internetworking and provides end-to-end datagram transmission across multiple IP networks. IPv6 uses 128-bit addresses, for an address space of 2128 (approximately 3.4×1038) addresses. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion [3]. Features of IPv6 include:

1) *Address structure improvements*: Globally unique addresses with more levels of addressing hierarchy, to reduce the size of routing tables; auto-configuration of addresses by hosts; improved scalability of multicast routing, by adding a "scope" field to multicast addresses; a new type of address, the "anycast address", which is used to send a packet to any one of a group of devices.
1) Removal of the need for packet fragmentation en-route, by dynamic determination of the largest packet size that is supported by every link in the path. A link's MTU (Maximum Transmission Unit) must be at least 1280 bytes, compared with 576 bytes for IPv4.

2) Traffic Class, which allows a packet to be labelled with an appropriate priority. If the network becomes congested, the lowest priority packets are dropped.
3) Flow labels, which indicate to intermediate routers that packets are part of a flow, and that this flow requires a particular type of service. This feature enables, for example, real-time processing of data streams. It also increases routing speed because the forwarding router need only check the flow label, not the rest of the header. The handling indicated by the flow label can be done by the IPv6 Hop-by-Hop header, or by a separate protocol such as RSVP.
4) Mandatory authentication and data integrity protocols, through IPsec. IPsec is optional in IPv4.

VI. COMMUNICATING BETWEEN IPV6 AND IPV4

The need of the hour is to enable IPv6 capabilities on all existing networks. However, IPv4 networks cannot upgrade to IPv6 networks immediately. This is partially due to the perception of the technical immaturity of IPv6 as compared to IPv4. Also, service providers are highly risk-adverse and are not receptive to new changes so instantly, keeping in mind the change in infrastructure required. The technical incompatibilities to convert all the network devices to understand IPv6 instantly is another issue that had to be considered. These factors led to look for alternatives that support co-existence of IPv4 and IPv6 addressing schemes in networks [5].

A set of mechanisms called SIT (Simple Internet Transition) has been implemented; it includes protocols and management rules to simplify the migration. The main characteristics of SIT are the following:

1) *Possibility of a progressive and non-traumatic transition:* IPv4 hosts and routers can be updated to IPv6, one at a time, without requiring other hosts or routers to be updated simultaneously.
2) *Minimum requirements for updating*: The only requirement for updating hosts to IPv6 is the availability of a DNS server to manage IPv6 addresses. No requirements are needed for routers.
3) *Addressing simplicity:* When a router or a host is updated to IPv6, it can also continue to use IPv4 address.
4) *Low initial cost:* No preparatory work is necessary to begin the migration to IPv6.

Mechanisms used by SIT include the following [6]:

1) A structure of IPv6 addresses that allows the derivation of IPv6 addresses from IPv4 addresses.
2) The availability of the dual stack on hosts and on routers during the transition—that is, the presence of both IPv4 and IPv6 stacks at the same time.
3) A technique to encapsulate IPv6 packets inside IPv4 packets (tunnelling) to allow IPv6 packets to traverse clouds not yet updated to IPv6.
4) An optional technique that consists of translating IPv6 headers into IPv4 headers and vice versa to allow, in an advanced phase of the migration, IPv4-only nodes to communicate with IPv6-only nodes.

VII. DUAL STACK

This is the most common type of migration strategy because it allows the devices to communicate using either IPv4 or IPv6. Dual stacking allows the upgradation of devices and applications on the network one at a time.

The Dual Stack implementation consists of a network topology that provides the ability to route and forward IPv4 and IPv6 packets. This functionality can be at just the customer's environment, on the SP's network core, its edges, or some other combination. The dual stack approach can be deployed across the entire network or in regional areas but in order for the dual stack approach to work, protocol continuity for packets in transit must be met [5].

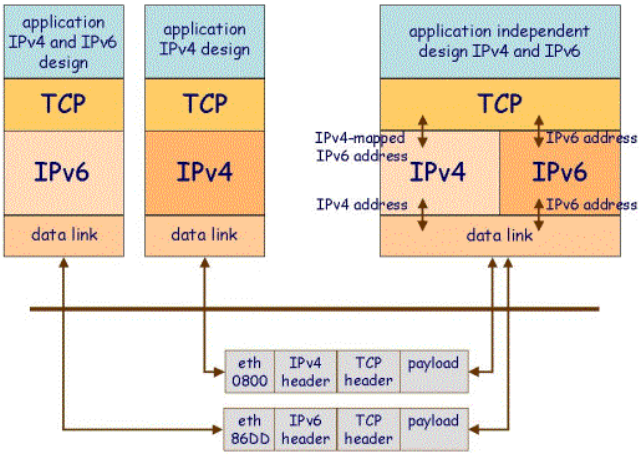

Fig 2. Dual Stack Visualisation

This is a temporary solution for easing the migration from IPv4 to IPv6. As more and more hosts and devices on the network are upgraded, more of communication will occur over IPv6 and the old IPv4 protocol stacks will no longer needed and can then be removed

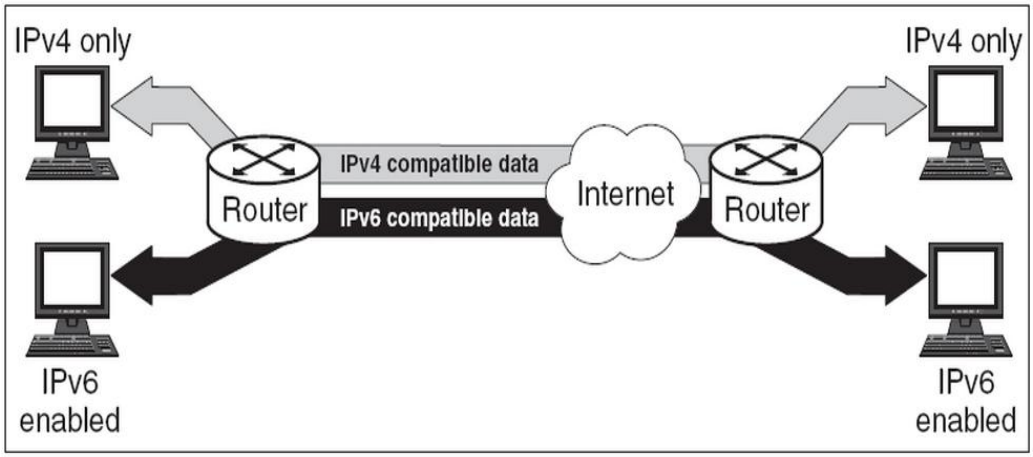

Fig 3. Example of a dual stack network

VIII. TRANSLATION TECHNOLOGIES

Translation technologies translate one protocol into another protocol. This facilitates interoperability between the protocols. Address Family Translation (AFT) facilitates communication between IPv6-only and IPv4-only hosts by performing IP header and address translation between the two address families. AFT is not a long term support strategy; it is a medium term coexistence strategy that can be used to facilitate a long term program of IPv6 transition by both enterprises and ISPs.

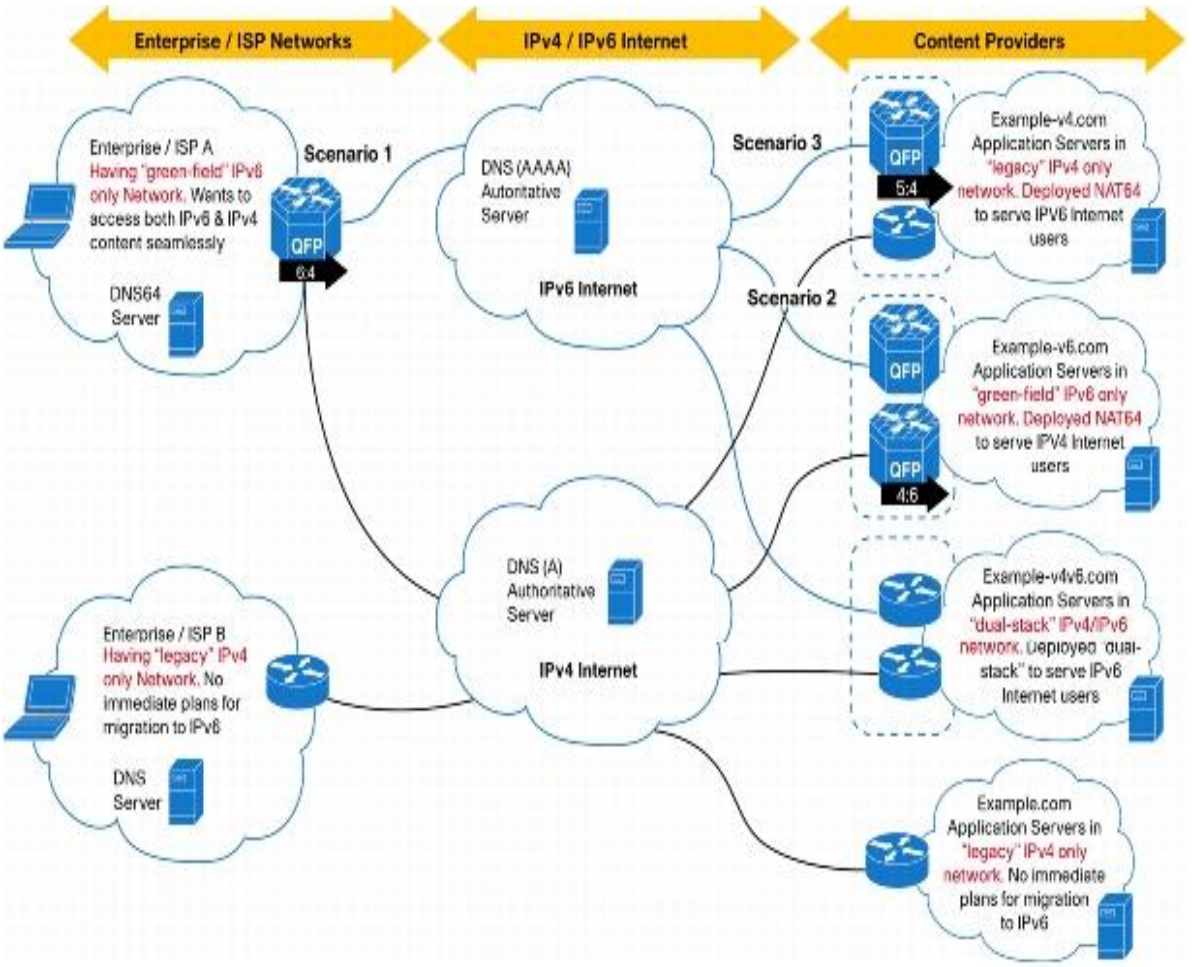

Fig 4. Scenarios for IPv6/IPv4 Translation

Translation offers two major advantages:

1) It provides a gradual migration to IPv6 by providing seamless internet experience to greenfiled IPv6-only users, accessing IPv4 internet services.
2) Existing content providers and content enablers can provide services transparently to IPv6 internet users by using translation technology, with little or no change in the existing network infrastructure, thus maintaining IPv4 business continuity [7].

TABLE III. TRANSLATION SCENARIOS AND THEIR APPLICABILITY

Scenarios for IPv6/IPv4 Translation	**Applicability**	**Example**
Scenario 1: An IPv6 network to the IPv4 Internet	Greenfield IPv6-only network wanting to transparently access both IPv6 and existing IPv4 content Initiated from IPv6 hosts and network	ISPs rolling out new services and networks for IPv6-only smartphones (third-generation [3G], Long-Term Evolution [LTE], etc.) handsets Enterprises deploying IPv6-only network
Scenario 2: The IPv4 Internet to an IPv6 network	Servers in greenfield IPv6-only network wanting to transparently serve both IPv4 and IPv6 users Initiated from IPv4 hosts and network	Upcoming or existing content providers rolling out services in IPv6-only environment
Scenario 3: The IPv6 Internet to an IPv4 network	Servers in existing IPv4-only network wanting to serve IPV6 Internet users Initiated from IPv6 hosts and network	Existing content providers migrating to IPv6 and thus wanting to offer services to IPv6 Internet users as part of coexistence strategy
Scenario 4: An IPv4 network to the IPv6 Internet	Not a viable case in the near future; this scenario will probably occur only sometime after the early stage of the IPv6/IPv4 transition	None
Scenario 5: An IPv6 network to an IPv4 network	Both an IPv4 network and an IPv6 network are within the same organization	Similar to scenario1, catering to Intranet instead of Internet
Scenario 6: An IPv4 network to an IPv6 network	Same as above	Similar to scenario2, catering to intranet instead of Internet
Scenario 7: The IPv6 Internet to the IPv4 Internet	Would suffer from poor throughput	None
Scenario 8: The IPv4 Internet to the IPv6 Internet	No viable translation technique to handle unlimited IPv6 address translation	None

IX. TUNNELLING

Tunnelling is used to achieve heterogeneous traversing, when there are two isolated hosts that wish to communicate over a network that does not support its protocol stack. Tunnelling allows new network technologies to be implemented while using the existing network infrastructure. One of the major issues inherent in the tunnelling approach, is the requirement to configure each tunnel endpoint [5].

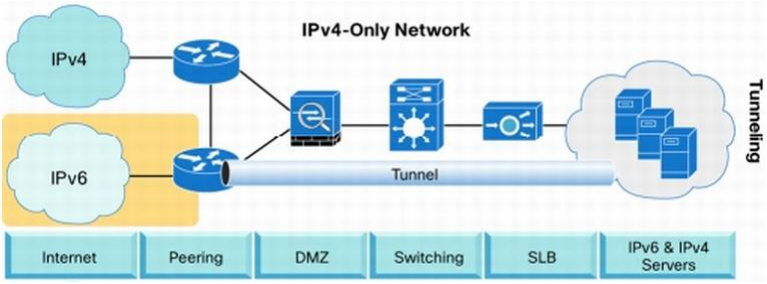

Fig 4. Illustration of Tunnelling

IPv6 tunnelling technologies have been widely explored. Examples of this technology are Teredo, ISATAP, 6to4, 6rd, 4to6 and DS-Lite.

The basic principle of tunnelling is shown in Figure 1. To deliver IPvY packets across the IPvX network in the middle, we deploy two tunnel endpoints on the border of the IPvX network.

When the ingress endpoint (Tunnel endpoint 1) receives an IPvY packet from the IPvY network, it encapsulates the IPvY packet with IPvX protocol header and puts the whole IPvY packet into the payload of the new IPvX packet. Then the IPvX packet is forwarded through the IPvX network.

When the egress endpoint (Tunnel endpoint 2) receives the encapsulated IPvX packet, it decapsulates the packet, extracts the original IPvY packet and forwards it to the IPvY network.

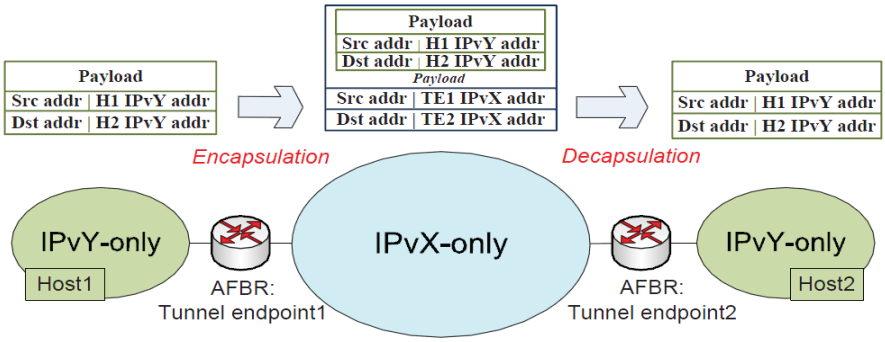

Fig 5. Basic principle of tunnelling

When performing the encapsulation, Endpoint 1 should fill in the IPvX destination address in the encapsulation header properly, which guarantees that the encapsulated packet will be forwarded to endpoint 2. Usually the IPvX address of endpoint 2 is figured out and used as the encapsulation destination address. Tunnelling is actually a generic technology; under the scope of IPv6 transition, tunnelling can achieve communications between IPv4 networks/hosts across an IPv6 network (IPv4-over-IPv6), and communications between IPv6 networks/hosts across an IPv4 network (IPv6-over-IPv4) [6].

X. CONCLUSIONS AND FUTURE ASPECTS

Solution to the deficiency of IP addresses in version 4, IPv6 having 128 bit address length provides nearly an unlimited supply of addresses (340,282,366,920,938,463,463,374,607,43
1,768,211,456 to be exact). This provides roughly 50 octillion addresses per person alive on Earth today, or roughly 3.7 x 1021 addresses per square inch of the Earth's surface.

IPv6 is currently 0.9% of IPv4 in terms of routing table entries. Assuming future exponential growth of this ratio IPv6 will be at 80% of the IPv4 internet in 2026.

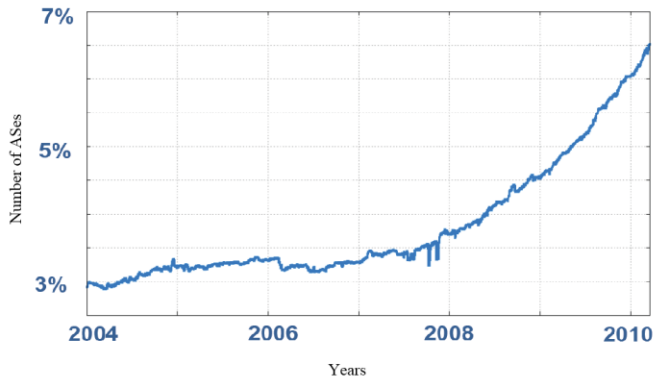

Fig 6. IPv6/IPv4 Ratio in terms of Autonomous Systems (ASes) that announce or transit IPv6 route

In terms of Autonomous Systems (ASes) that announce or transit IPv6 routes, IPv6 is currently 6.5% of IPv4. V6 will be at 80% of v4 internet in 2017. The 'size' of the IPv6 deployment in terms of end-to-end hosts IPv6 capability is around 1% of the total number of internet end-hosts at present. Tunneling of IPv6 in IPv6 represents around 10% of IPv6 sessions.

Through this paper we conclude that though IPv6 deployment is a necessity, it is still a gradual transition in spite of the various advantages associated with the new version. IPv4 and IPv6 will coexist for a long time hence the need for methods of communication between the new and old versions.

ACKNOWLEDGMENT

We would like to thank our mentor, Er. Gunjan Gandhi, *Asst. Professor, Department of Electronics and Communications Engineering, Lovely Professional University*, for his invaluable feedback which helped substantially in improving the quality of the paper.

REFERENCES

[1] T.A. Limoncelli. "Successful Strategies for IPv6 Rollouts. Really," Commun. Of the ACM, vol. 54, no. 4, pp. 44-50, Apr., 2011.

[2] S. Lawson. "Update: ICANN assigns its last IPv4 Addresses," Computerworld, February 03, 2011. http://www.computerworld.com/s/article/9207961/Update_ICANN_assigns_its_last_IPv4_addresses. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[3] Comparison study between IPV4 & IPV6,Amer Nizar Abu Ali,Philadelphia University, Jordan, CIS department

[4] Transition from IPv4 to IPv6,Reza Tadayoni, reza@cmi.aau.dk,Anders Henten, henten@cmi.aau.dk,Center for Communication, Media and Information technologies (CMI),Aalborg University Copenhagen

[5] "A Comparative Study of IPv4/IPv6 Co-existence Technologies", Jinesh Doshi, Rachid Chaoua, Saurabh Kumar, Sahana Mallya

[6] "Transition from IPv4 to IPv6: A State-of-the-Art Survey", Peng Wu, Yong Cui, Jianping Wu, Jiangchuan Liu, Chris Metz

[7] http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

[8] http://en.wikipedia.org/wiki/IPv4

