Bachelor's thesis

Bachelor Of Engineering

Information Technology

2015

Bhuwan Chhetri

TRANSITION FROM IPV4 TO IPV6

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Networking

2015 | 52

Instructor: Väänänen Ossi

Bhuwan Chhetri

ABSTRACT

Most of the Internet Service Providers, and web companies are enabling IPv6 permanently for their customers and services. Since World IPv6 launch began on 6 June 2012, global IPv6 traffic has grown by 500%. If this trend continues, in less than four years, half of the Internet users will connect with IPv6.

The main purpose of the thesis is to discuss the progress of IPv6 over the depletion of IPv4 along with features including its advantages and disadvantages. It aims to discover the best solution for a transition method and factors affecting IPv6 implementation, which is solely based on the data collected from different sources. Transition techniques are presented in this thesis elaborated with configuration and challenges. The thesis concludes that using an option like dual stack is a good possible solution since the NAT (Network Address Translation) transition appears less user friendly and has been discouraged by network operators with elapse of time.

KEYWORDS:

ISPs, IPv6, IPv4, NAT, dual stack, transition

CONTENTS

FIGURES

TABLES

LIST OF ABBREVIATIONS (OR) SYMBOLS

IP	Internet Protocol
IPng	IP the next generation
IPv4	IP version 4
IPv6	IP version 6
ISP	Internet Service Provider
QOS	Quality of Service
NIC	Network Interface Card
TCP	Transmission Control Protocol
ISO	International Organization for Standardization
OSI	Open Systems Interconnection
UDP	User Datagram Protocol
HTTP	Hypertext Transfer Protocol
ECN	Explicit Congestion Notification
TTL	Time To Live
IETF	Internet Engineering Task Force

NAT	Network Address Translation
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IGMP	Internet Group Management Protocol
ICMP	Internet Control Message Protocol
L2TP	Layer Two Tunnel Protocol
MTU	Maximum Transmission Unit
PPP	Point-to-Point Protocol
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
VPN	Virtual Private Network
OSPF	Open Shortest Path First
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
RFC	Request for Comments
RARP	Reverse Address Resolution Protocol
ARP	Address Resolution Protocol

ICP	Internet Content Provider
CP	Content Provider
SP	Service Provider
HA	High Availability
CPE	Customer Premise Equipment

1 INTRODUCTION

The IPv6 transition mechanism is a technology, which is designed to permit hosts on an IPv4 network to communicate with the hosts on an IPv6 network. With the exceptional expansion of Internet users in recent years, densely populated countries, for example China and India, are running out of IPv4 addressees. The TCP/IP has also played an important role in the global expansion of communications. More users joining the Internet results in spreading the knowledge in every field throughout the world. However, there is problem of the limited IP addresses while we are on IPv4. It has been estimated that IPv4 addressed would run out by 2011, so IPv6 was designed to solve the problem.[10]

The purpose of this thesis is to discuss the transition method and factors, which affect the IPv6 implementation. It also analyzes the progress of IPv6 and transition problems that are faced by the Internet Service Providers during the deployment of IPv6 and how the problems can be minimized.

This thesis introduces Internet Protocol, brief introduction about the Open Systems Interconnection (OSI) model and Transmission Control Protocol /Internet Protocol (TCP/IP). Chapter 3 discusses the IPv4 and its feature while in chapter 4, IPv6 and features are discussed. Chapter 5 compares IPv4 and IPv6 in routing information as well virtual private network to identify its implementation differences. Chapter 6 provides a complete transition method for the transition of IPv4 to IPv6, which are commonly used by the ISP. Section 6.6 describes the future of IP addressing in brief. Chapter 7 analyzes the practical transition of IPv6 over IPv4.

2 INTERNET PROTOCOL

2.1 Overview

On the Internet, every computer has a unique address. This address is called IP, which stands for Internet Protocol. It defines the format of packets and provides an addressing system, which has two functions: identifying hosts and providing a logical location service.

The dominant version of Internet Protocol is IPv4 and the next generation is Internet Protocol Version 6 (IPv6). Now, one may wonder where the IPv5 is. After the IPv4, IPv5 was introduced to overcome the obstacles or problems of IPv4. Mainly, it was designed to provide Quality of Service (Qos) for streaming services. It was envisioned to be the connection-oriented complement to IPv4 but was never introduced for public use. The next generation of Internet Protocol is IPv6, which is also called IPng or IP next generation. The features of IPv4 and IPv6 will be discussed later.

Before we go further, it is important to discuss what a network is. A network is the group of two or more computers connected with each other to exchange data using cable or wireless. When connected to the network, a computer is online and when disconnected, it is offline. In a network we can exchange different resources like data, application, hardware and other information. For this exchange, we need the following hardware: cables, switch, routers, network interface card (NIC) etc. Other than hardware, we need a server computer and a client computer. A server computers shares scanners, printers and other network services that have Internet access. Client computers are all the other computers, which are in same network with the Server computer. They can access all the resources provided by the server. To connect to the network, the computer needs a NIC. The NIC in the computers physically connects to the network with the help of an Ethernet cable. The Ethernet cable does not connect to network but it only helps to connect to the switch while the switch connects to the network.

2.2 OSI Model

The Open Systems Interconnection (OSI) model defines how the communication between two users in the network happens. The OSI model is composed of seven layers, each one having their own functions. The International Organization developed this model for Standardization (ISO) in 1984. Now, every network is built on this OSI model. The main purpose of building this model is to understand the networks and how it works. Having different layers it makes easy to troubleshoot if we have any problems in the future. The different layers of the OSI model are independent of each other but provide service to the other layers that are connected. Again, these seven layers are divided into two parts: the four upper layers and lower three layers. The four upper layers are used when a message passes from or to a user. The three lower layers are used when a message passes through the host computer.

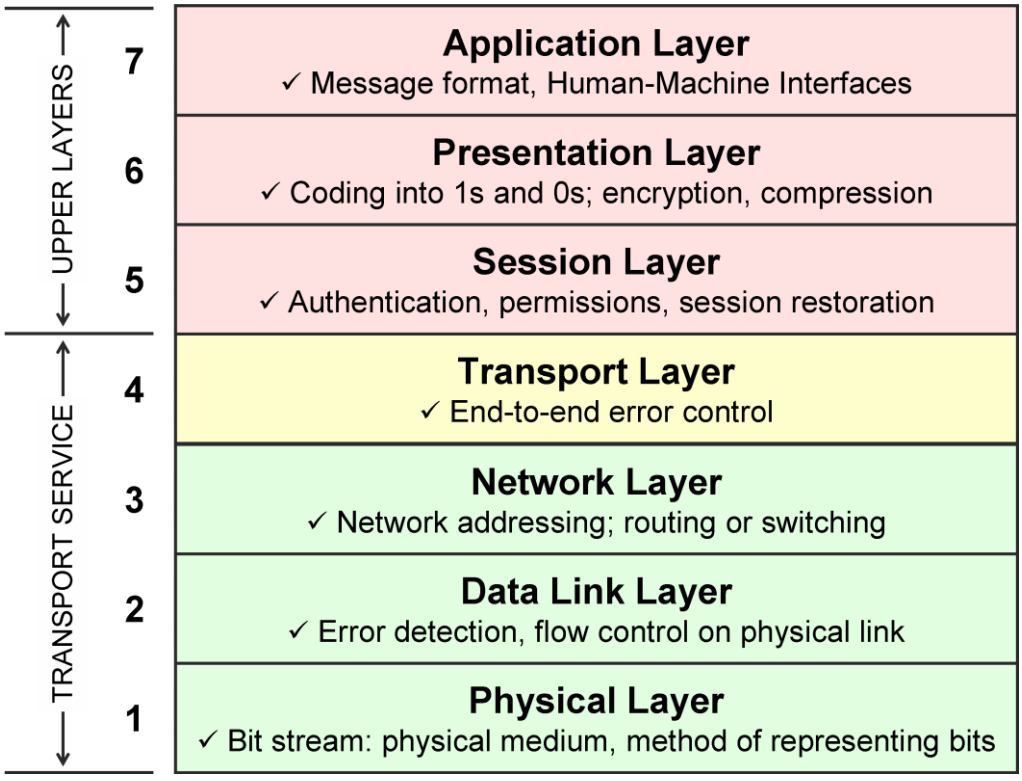


Figure 1. The 7 layers of OSI model [2].

There are seven layers in OSI model, which is shown in Figure 1. Each layer is described in detail below: - [2]

Physical layer: - It defines the physical equipment used for transferring the data across the network i.e. wires, computers, network cards, cables etc.

Data link layer: - This layer is used to control the signal that enter and leave the network cable. It deals with data framing and encapsulation.

Network layer: - It is concerned with the process of packet forwarding including routing through intermediate routers. It handles the addressing and routing of data based on logical addressing. Examples are apple talk DDP, IP, IPX.

Transport layer: - This layer is responsible for transferring the data from one point to point another without errors. Examples of the Transport layer are Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Sequenced Packet Exchange (SPX).

Session layer: - It manages, establishes, and terminates the connection between applications. It also deals with the session and connection coordination. Examples are NFS, NetBIOS names, RPC, SQL.

Presentation layer: - This layer converts data so that systems, which use different data formats, can exchange information. It is also called the syntax layer. Examples are encryption, ASCII, GIF, MIDI etc.

Application layer: - It represents the services that directly support applications such as software for file transfers, database access, emails and network games. It contains web-browser, FTP clients, email clients but does not include computer application software. Examples are WWW browsers, Telnet, HTTP, FTP, etc.

2.3 TCP/IP

TCP/IP is the network standard, which defines the Internet. The Internet Protocol (IP) standard explains how packets of information are exchanged over a set of networks. It has a packet addressing method that lets any computer forward a packet over the network to other computer, which is closer to the packet's recipient. TCP checks the packets that are sent through the network and requests for transmissions if errors

are found. TCP/IP was designed to solve the problems before the OSI model was introduced. [3]

TCP/IP has a network model as the OSI network model does but they are not the same.

TCP/IP is a four-layered standard. The four layers of TCP/IP are explained below:

Layer 4. Application Layer

It is the top most layer of TCP/IP model. The application layer is where the network and its application-layer protocol reside. Using the application protocol layers, packets of information are exchanged between hosts and remote users can communicate.

The application layer includes many protocols like DNS (Domain Naming System), HTTP protocol (which provides web document request and transfer), SMTP (which provides transfer of email message) and FTP (which provides transfer of files between two end systems). [4]

Layer 3. Transport Layer

It is the third layer of TCP/IP model, which resides in between the Transport Layer and the Application Layer. The Internet's transport layer transports application layer message between application endpoints.

The Transport Layer includes protocols like TCP (which provides connection-oriented services to its application) and UDP (which provides connectionless service to its application). [4]

Layer 2. Internet layer

The Internet layer is the second layer of the TCP/IP model. The Internet layer is between the Network Access layer and the Transport Layer. The Internet layer is responsible for moving data packets known as IP datagrams from one host to another. IP datagrams contain source and destination addresses, which are used to forward the datagrams between hosts and across network.

The Internet layer includes protocols like IP, ICMP, ARP, RARP and IGMP. [3]

Layer 1.Network Access Layer

The Network Access Layer is the first or lower layer of the TCP/IP model. The Network Access Layer explains how data is sent physically through the network including individual bits.
The Network Access Layer includes protocols like FDDI, X.25, Frame Relay, Ethernet, and Token Ring etc. [3]

2.4 Comparison of OSI Model and TCP/IP

Listed below are some of the major differences between the OSI model and the TCP/IP model with a diagrammatic comparison.

Table 1. Comparison of OSI Model and TCP/IP [5]

OSI (Open System Interconnection)	**TCP/IP (Transmission Control Protocol/Internet Protocol)**
It has seven layers.	It has four layers.
The transport layer guarantees delivery of packets.	The transport layer does not guarantee the delivery of packets.
OSI defines function of all the layers and provides layer functioning.	TCP/IP is not flexible with other layers as it is more based on protocols.
It has separate session and presentation layer.	It does not have separate session and presentation layer.
The Network layer provides both connection-oriented and connectionless service.	The Network layer provides connectionless service.
The OSI model is a generic, protocol-independent standard.	TCP/IP protocols are considered to be standards.
Protocols do not fit well into this model.	Protocols fit well in this model.

Table 1 provides a comparison between the OSI model and the TCP/IP model. It has attempted to present a practical comparison rather than a theoretical implementation. Besides this, the table also provides information on how the layers of these two models affect the performance and data communication including the frame encapsulation and defragmentation.

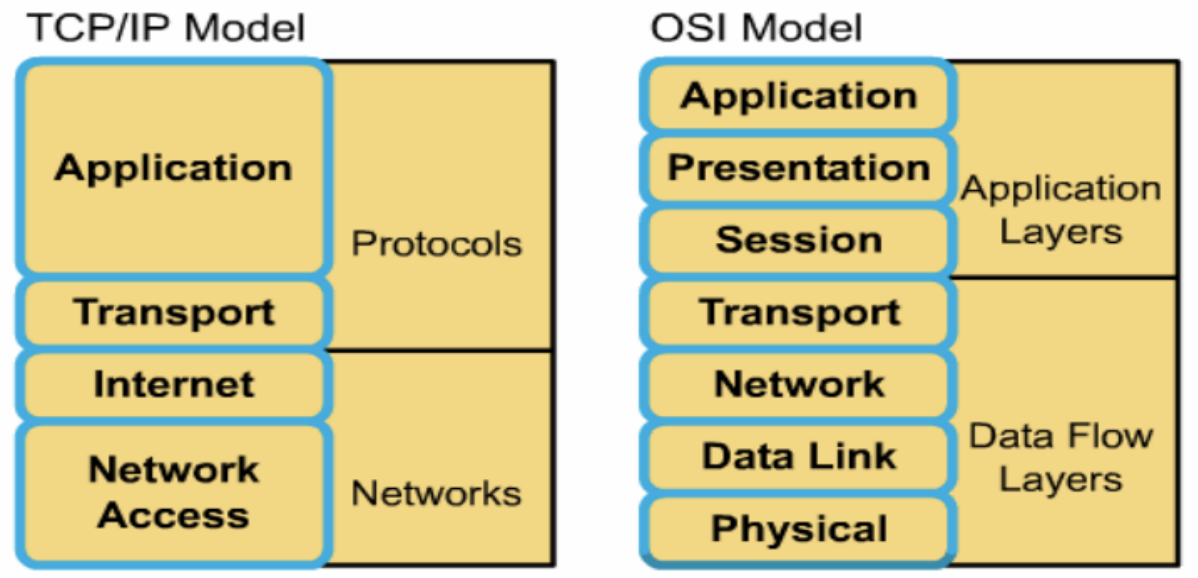


Figure 2. Comparison of TCP/IP and OSI Model [6]

Figure 2 provides the segments of model which could be considered as networks and Protocols layer as well as Application and Data Flow layers while there is flow of data traffic through various layers of TCI/IP and OSI model respectively. There are few similarities between these two models but the OSI model advances data communication as it increases hierarchy to application layer, resulting in improvement of performance and security.

3 IPV4

IPv4 is the first version of Protocol to use publicly although it is the 4th version of Internet Protocol. It was widely used in modern TCP/IP. It uses 32 bits of addresses and has the limit of 2^32 addresses. Due to the fast growth of Internet users, the IPv4 addresses have been in depletion.

3.1 Features of IPv4

An IP packet is composed of a header section and a data section. It has no data checksum or any other footer after the data section. There are 14 fields in the header and of which 13 are required. The 14th field is optional. [7]

<table>
<tr><td>Version</td><td>Header Length</td><td>Service Type</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td>Time To Live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Options +Padding</td></tr>
</table>

Figure 3. Contents of header of IPv4 packet

Detailed information about the header of IPv4 packet is segmented in Figure 3 to give an overview of its content while the frame is transmitted with IPv4 packet. More specifically, the IPv4 packet is embedded with a source and destination address with a frame length and communication expiry duration to give delivery acknowledgement while transmitting. The contents of the header of an IPv4 packet are explained below.

Version - It is the 4-bit version as there is a value of 4.
Internet Header Length (IHL) – The second field consisting of 4 bits is the Internet Header Length. The minimum value is 5.
Differentiated Services Code Point (DSCP) - It is known as type of service. It is defined by TFC 2474 and used for real time data streaming, for example VoIP.
Explicit Congestion Notification (ECN) - It allows end-to-end notification of network congestion without dropping any packets. It works well when supported by an underlying network.
Total length-This is the length of whole packets which include header and data both in bytes.
Identification – It is used to identify the original IP packet during transmission.
Flag - It has 3 bits. It helps to find out if the packets can be fragmented or not.
Fragment Offset - It is 13 bits long. It indicates the exact position of fragmenting the packets.
Time To Live (TTL) – It avoids looping in the network and helps to limit the packets that can cross the router.
Protocol - It defines the next layer protocol.
Header Checksum - This field is 16 bits long and is used to check if the received packets are error free.
Source Address - It is the address of the sender or the source.
Destination Address- It is the address of the receiver.
Option - It is used only when the value of IHL is greater than 5. These may contain values such as security, time stamp, record route etc.

IP addressing

IP address is an address which is unique and is used to identify the device in the network. It is composed of 32 binary bits. These 32 binary bits are broken into four octets, i.e., 8 bits each. Each octet is converted to a decimal and is separated by a dot. This is why we have IP addresses in dotted format, for example 82.50.69.83. The IP address Huber has two parts: a network number and a host number. The network number determines which network the host computer is located. The host number determines the exact host computer in that network. [8]

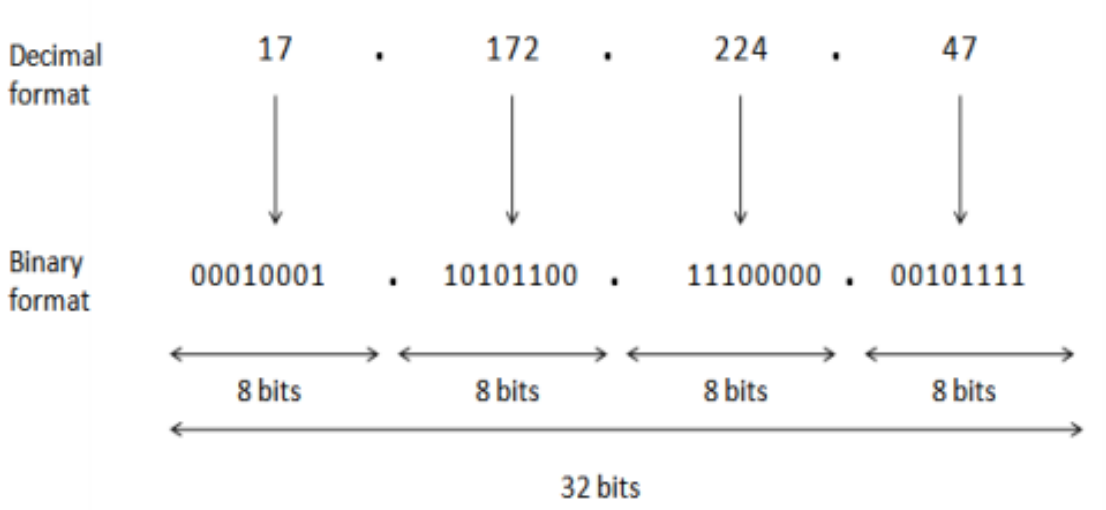


Figure 4. IPv4 format

The structural format of IPv4 is shown in Figure 4 where different octets are segmented to describe the binary content of each octet and its composited bit capacity. Moreover, the decimal and binary composition helps to observe each octet.

It is not easy to remember an address in binary form like 01010010.00110010.01000101.01010011 for 82.50.69.83. So to make it easy, a unique name is assigned by the Domain Name System (DNS).

Classification of Address

There are several classes of IP Address as the requirement of host per network. IPv4 is divided into 5 classes (A, B, C, D and E) and they are determined by the first octet of the IP address.

Table 2. Describing 5 classes of IPv4 and their area of purpose

Class	**Format**	**Address range**	**No of networks**	**No of hosts**	**Area of use**
A	N.H.H.H	0.0.0.0 - 127.255.255.255	126	16,777,214	Large organization
B	N.H.H.H	128.0.0.0 – 191.255.255.255	16,384	65,543	Medium organization
C	N.H.H.H	192.0.0.0 – 223.255.255.255	2,097,152	245	Small organization
D	N/A	224.0.0.0 – 239.255.255.255	N/A	N/A	Multicast groups
E	N/A	240.0.0.0 – 255.255.255.255	N/A	N/A	Experimental

N= Network number, H = host number

In Table 2, the different classes of IP addresses of version 4 are shown based on format and range of IP addresses. It also adds the subnet masks applied to each class along with application of the respective classes. Basically, IPv4 it has been categorized in four classes, which are detailed in above table.

4 IPV6

The Internet Engineering Task Force (IETF) is in charge for defining Internet Protocols standards. When they developed IPv4, many issues were not taken into consideration, such as address and security issues. Later on, in the early 1990s IETF decided that to overcome the issues related to IPv4, they needed new versions of IP and IPng was created which is now known as IPv6. IPv6 offers many functions, which were not introduced in IPv4. Some of the improvements were increased address size, integrity communications, built in security. With many of these new features, IPv4 is supposed to be replaced by IPv6 in every network without any limitations. At the end of 1998, IPv6 was fully standardized. [1]

Above we have discussed the features of IPv4 and now we will be introducing the features of IPv6.

IPv6 header: -

<table>
<tr><td>Version</td><td>Traffic Class</td><td colspan="2">Flow Label</td></tr>
<tr><td colspan="2">Payload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="4">Source Address</td></tr>
<tr><td colspan="4">Destination Address</td></tr>
</table>

Version – It specifies the Internet Protocol version 6.
Traffic Class – It holds two values consisting of six and two. Six-bit values are used for differentiated services to classify the packets. Two-bit values are used for explicit congestion notification (ECN).
Flow Label – The 20-bit flow label was created for giving real-time application. The flow label is used to detect spoofed packets.
Payload Length – The 16-bit payload length contains the length of the data fields in bits.

Next Header – The 8-bit selector specifies the transport layer protocol and specifies the type of next header.
Hop Limit – The 8-bit unassigned integer is decremented by 1, and when counter reaches 0 packet is discarded.
Source Address –The 128-bit source address indicates the originator.
Destination Address – The 128-bits source address indicates the recipient of the packet.

4.1 Features of IPv6

The features of IPv6 are listed below:

New Packet Format and Header – The new IPv6 packet format assists to minimize packet header processing by routers. Operating nonessential and optional fields to extension headers that are placed after the IPv6 header attains this. Since IPv4 and IPv6 packets are significantly different, the two protocols are not able to exchange the information.

Larger Address Space – In comparison to IPv4, IPv6 uses four times more bits in the address. IPv4 uses 32 bits while IPv6 uses 128 bits. Due to the larger address space in the absence of NAT, there is less complexity in the network and this makes it simpler. Next, we can use a unique address for our every device in home and office.

Auto Configuration – There are two types of auto configuration in IPv6. IPv6 supports both stateful and stateless auto configuration of every other host device.
Stateful auto-configuration – This configuration is done manually for the installation and administration of nodes over a network. DHCPv6 works in the client server model and optionally provides IPv6 addresses and other configurations.

Stateless auto-configuration – This configuration is suitable for individuals and small organizations. It can get automatically an IPv6 address and is not automatically registered in the DNS. The server should be manually configured.

Security – IPSec security is built in IPv6, which is difficult to add in IPv4. IPsec is mandatory in IPv6. It provides security in the network level or to the application, which are running on the IPv6 network, for example, sending/receiving data over Internet, web server etc.
IPsec employs the Authentication Header and Encapsulating Security Payload Header to provide security. The AH and ESP Header can be used according to our desire security. The AH and ESP header can be used in the tunnel mode and transport mode.

-“tunnel mode”- This is the most commonly used method to encrypt traffic between secure IPSec gateways such as in between the Cisco router and PIX Firewall. It is also used to connect an end-to-end station running IPSec software. This is applied to the entire IP packet.

-“transport mode” – This is used between end stations supporting IPSec, or between an end–station and a gateway. This is assigned to the transport layer in the form of IPv6 header, authentication Header or Encapsulating.

5 COMPARISON OF IPV4 AND IPV6

It is important to note that IPv6 is much more than an extension of IPv4 addressing. IPv6 offers many enchantments over IPv4, and Table 3 provides a detailed comparison of IPv4 and IPv6 along with its differences in application of real world. It also compares routing information as well virtual private network to identify its implementation differences.

Table 3. Comparisons of IPv4 and IPv6 [9]

Description	IPv4	IPv6
Address	32 bits long (4 bytes). Composed of network and host portion, depends upon the address class. Form of the address is nnn.nnn.nnn.nnn, where 0<=nnn<=255,and each n is decimal digit. For ex:- 192.168.255.255	128 bits long (16 bytes). 64 bits is for the network number and 64 bits for host. Form of the address is xxxx:xxxx:xxxx:xxxx:xxxx:xxxxx: xxxx:xxxx, where x is hexadecimal number. For ex:- FE80:0000:0000:0000:0202:B3 FF:FE1E:8329
Address types	Spilt into 3 basic types unicast, multicast and broadcast address.	Split into 3 basic types unicast, multicast and anycast address.
Configuration	Need to be configured like IP address and routes.	Configuration is optional.
Domain Name System (DNS)	Application accept host names and then use DNS to get IP address, using socket API gethostbyname( ). Domain for reverse lookup is in –addr.arpa.	Same support for IPv6. Support for IPv6 exits using AAAA (quad A) record type and reverse lookup (IP-to-name). An application may elect to accept IPv6 address from DNS (or not) and then use IPv6 to

		communicate (or not). A new getaddrinfo( ) API is used. Domain used for reverse llokup is ip6.arpa and not found then ip6.int is used.
Dynamic Host Configuration Protocol (DHCP)	Used to dynamically obtain an IP address and other configuration information.	DHCP does not support.
File Transfer Protocol (FTP)	Allows transferring files across the networks.	FTP does not support.
Internet Group Management Protocol (IGMP)	Used to find the hosts which want traffic for particular multicast group,	MLD does what IGMP in IPv4, but uses ICMPv6 by adding a few MLD-specific ICMPv6 type values.
Internet Control Message Protocol (ICMP)	Used to communicate network information.	Similar is used while Internet Control Message Protocol Version 6 (ICMPv6) some new attributes.
IP header	Variable length of 20-60 bytes depending on IP options presents.	Fixed length of 40 bytes.
IP header options	More options might accompany an IP header.	No IP header options. IPv6 adds optional extension headers.
IP header Type of Service byte	Used by QoS and differentiated services to designate a traffic class.	Different codes used to designate an IPv6 traffic class. Currently IPv6 does not support TOS.
LAN connection	Used by an IP interface to get to the physical network. Many type exits for example token ring and Ethernet.	Can be used with any Ethernet adapters and is also supported over virtual Ethernet between logical partitions.
Layer Two Tunnel Protocol (L2TP)	Thought as virtual PPP and works over any supported	Does not support.

	line type.	
Maximum transmission unit (MTU)	Maximum transmission unit of a link is the maximum number of bytes that a particular link types such (Ethernet, modem) supports. For IPv4, 576 is the typical minimum.	Has a lower boundary limit on MTU of 120 bytes.
Netstat	Tool to look at the status of TCP/IP connections, interface or routes.	Same support for IPv6.
Network address translation (NAT)	Basic firewall functions integrated into TCP/IP.	Does not support as it solves the problem of shortage of address.
Packet filtering	It is the basic firewall functions, configured by the System i Navigator.	Does not support in IPv6.
Packet forwarding	The i5/OS TCP/IP can be configured to forward IP packets.	It has limited support for IPv6.
Point to Point Protocol (PPP)	Supports dialup interface over various modem and line types.	PPP does not support IPv6.
Private and public address	All IPv4 address are public, except for three address ranges which have been made private by IETF RFC 1918:10.*.*.* (10/8) , 172.16.0.0 through 172.31.255.255 (172.16/12) , and 192.168.*.* (192.168/16). Private address domains are	Temporary address can be globally routed and have limited lifetime and generally are indistinguishable from public address.

	commonly used by organization and cannot be routed throughout the Internet.	
Renumbering	It is done by manual reconfigurations with the help of DHCP.	It is important architectural element of IPv6 and is automatic within /48 prefix.
Route	Destination address is forwarded to the next hop using line. Default route is *DFTROUTE	IPv6 routes are bound to physical interface rather than an interface. Route is associated with physical layer as the source address selection is completely different from IPv4.
Routing Information Protocol (RIP)	This protocol is supported by the routed daemon.	Does not support.
Simple Network Management Protocol (SNMP)	It is protocol for system management.	Does not support.
Virtual Private Network (VPN)	Using IPsec it allows to extend a secure private network over an existing public network.	Same support for IPv6.

6 TRANSITION FROM IPV4 TO IPV6

There is not complete transition from IPv4 to IPv6 because IPv6 is not backward compatible. However, there are some technologies, which can convert IPv4 to IPv6. The technologies that can convert IPv4 to IPv6 are described as below step by step.

6.1 Dual Stack

In this method, both IPV4 and IPv6 protocols are available in the same network node and that is why it can connect to remote servers with both technologies (IPv4, IPv6). [10]
This technology ensures that only IPv4 node is upgraded. This technology is based on name lookup and application selection.

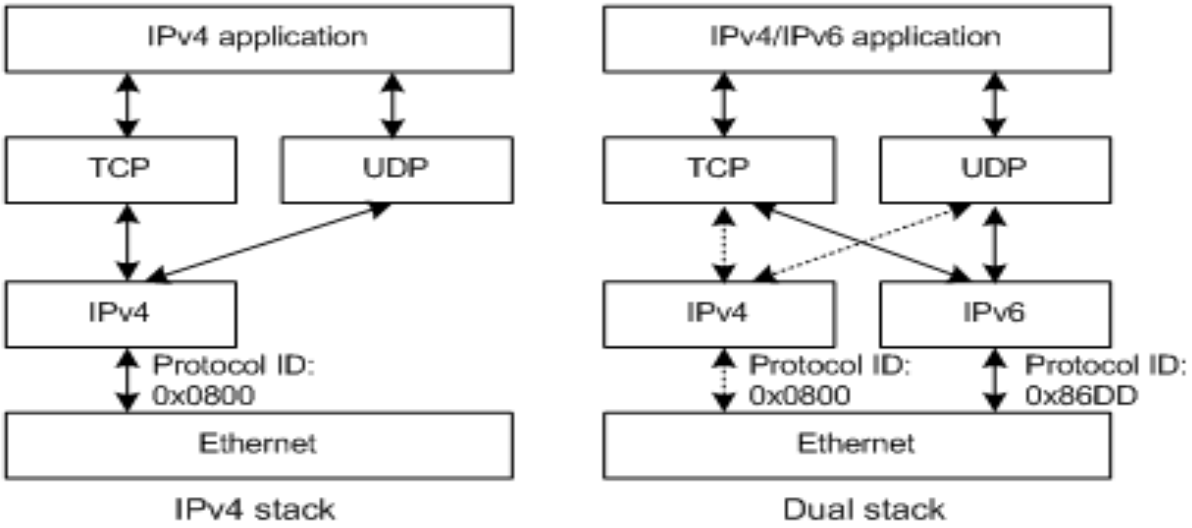
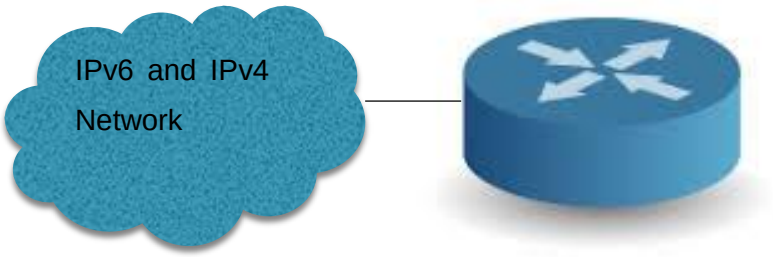


Figure 5. IPv4 application using the IPv4 stack /application using both IPv4 and IPv6 stacks [10]

Protocols in the world of Ethernet are implemented differently based on their IP version. Some could apply to IPv4 while others to IPv6. The diagrammatic sketch providing this information is shown in Figure 5.

6.1.1 Configuration [11]

Dual-Stack Router




```
router#
ipv6 unicast-routing

interface Ethernet0
ip address 192.168.99.1
255.255.255.0
ipv6 address
2001:db8:213:1::1/64
```

IPv4 : 192.168.99.1
IPv6:2001:db8:213:1::1/64

6.1.2 Challenges

Dual stack can connect with both IPv4 and IPv6 technologies. Challenges faced during the deployment of dual stack method are outlined as below:

- IPv4 and IPv6 have different software requirement to run. For example, IPv4 runs with OSPFv2 and IPv6 runs with OSPFv3.
- In Dual stack Exchange, the device is configured in only one stack and most forward to dual stack devices, for example, routers and then back to the same segment using the other stacks and this results in insufficient bandwidth. To implement dual stack, IPv6 needs to be activated in all network elements and this will cost on redesign of the existing networks.

6.2 Tunneling

For minimizing the transitions, all the routers on the way between the two IPv6 nodes do need to support IPv6. This method of transition is called tunneling. Primarily IPv6 packets are placed inside IPv4 packets then the packets are routed through the IPv4 routers.

One of the objections to integrating IPv6 into the current IPv4 networks is the ability to transport IPv6 packets over IPv4 –only networks. Tunneling or in IPv6 known as overlay tunnel can be used. IPv6 packets are encapsulated through the overlay tunnel in IPv4 packets for delivery across IPv4 infrastructure. The main disadvantage of tunneling is that it does not let communication between users of new protocols and old protocols without dual stack hosts.

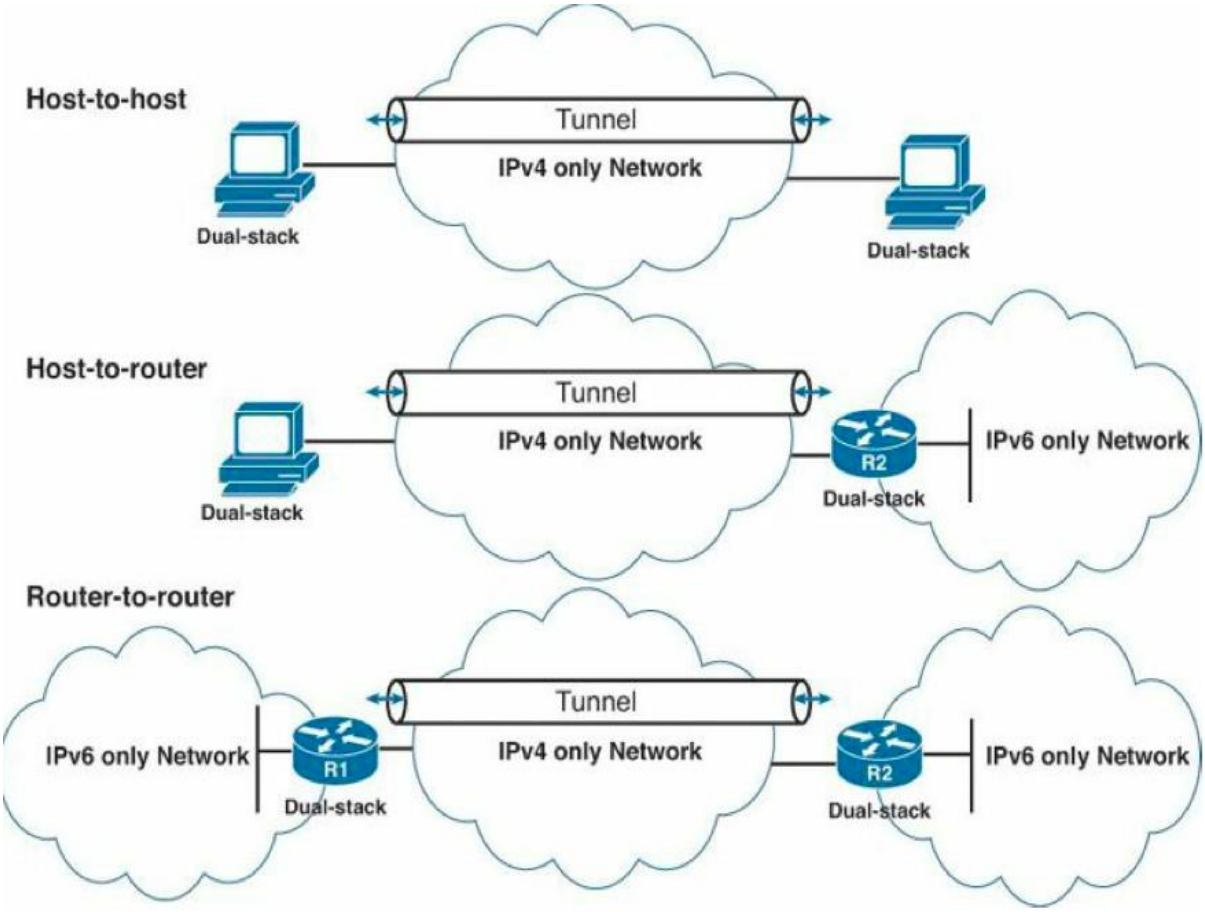


Figure 6. IPv6 tunneling involving different scenarios [10]

Tunneling can involve any combinations of routers depending upon the end-points (entry and exit points) of the tunnels. There are three scenarios: - host-to-host, host-to-router and router-to-router which are shown in Figure 6.

There are two types of protocols in a tunnel, namely transport protocol and passenger protocol.

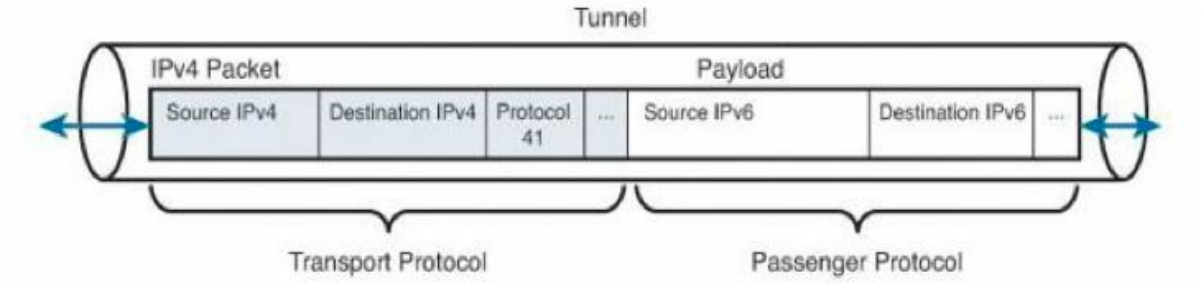


Figure 7. Tunnel consisting of protocols [10]

Transport Protocol: IPv4 is the transport protocol where the tunnel is created. In the IPv4 header, protocol 41 shows that the encapsulated data portion is an IPv6 packet. Passenger Protocol: IPv6 is the passenger protocol. Protocols are encapsulated in the tunnel and carried over the tunnel.

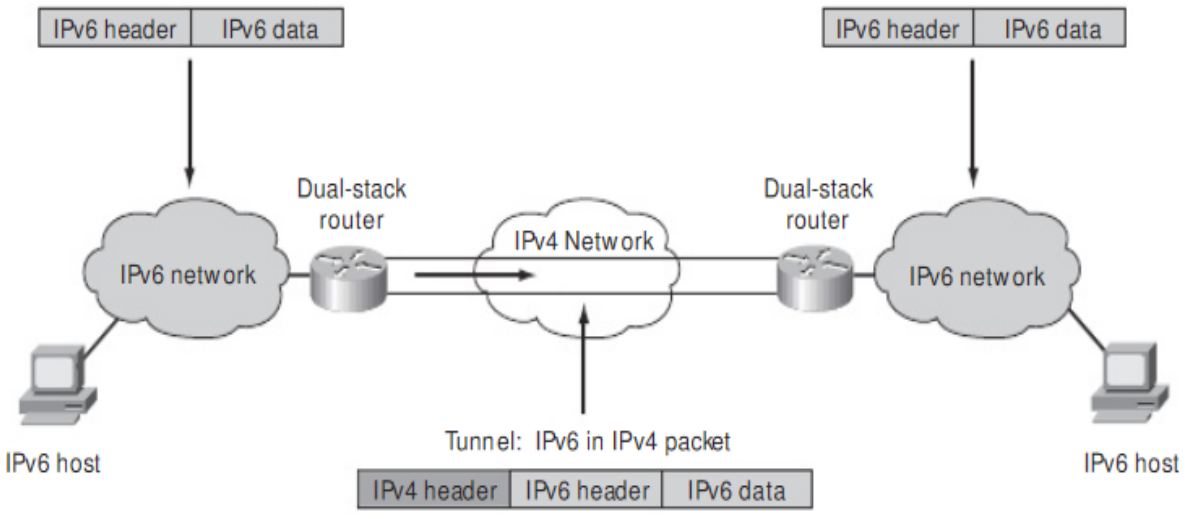


Figure 8. Use of IPv6 over IPv4 tunnels [10]

Table 4. Types of IPv6 tunnels [10]

Tunneling Type	**Tunnel mode command**	**Tunnel source**	**Tunnel destination**	**Interface Prefix or Address**	**Notes**
Manual	Ipv6ip	An IPv4 address or a reference to an interface on which IPv4 is configured. This can be the IPv4 address of the physical interface or a loopback interface.	An IPv4 address	An IPv6 address	Can carry IPv6 packets only.
GRE	gre ip		An IPv4 address	An IPv6 address	Can carry IPv6. Connectionless Network Service (CLNS), and many other types of packets. Note: IPv4 compatible uses the ::/96 prefix. Cisco recommends not to use this tunnel type
IPv4 compatible	Ipv6ip auto-tunnel		Not required. These are all point to multipoint tunneling types.	Not required. The interface address is generated as ::tunnel-source96.	
6to4	Ipv6ip 6to4		The IPv4 destination address is calculated in a per-packet	An IPv6 address	Site uses the address from the 2002::/16 prefix. Point to multipoint

			basic, using the IPv6 destination address.		tunnels that can be used to connect isolated IPv6 sites.
ISATP	Ipv6ip isatap		-	An IPv6 prefix in modified EUI-64 format. The IPv6 address is generated from the prefix and the tunnel source IPv4 address.	Point to point multipoint tunnels that can be used to connect systems within a site. Allows an individual dual-stack host within a site to communicate. Sites can use IPv6 unicast address.

6.2.1 Configuration

IETF defined several protocols and techniques for establishing tunnels between dual-stack nodes. Primarily, all the tunneling performs the same function: transports the IPv6 packet inside and IPv4 packet between the two end points of tunnel.

In the following Table 5, there is an example and the commands for configuring the manual tunnel between two end points.

Table 5. Configuration commands for manual tunneling [10]

Command	Description
Router(config)#**interface tunnel** tunnel-number	Enters interface configuration mode and states a tunnel interface and number

Router(config-if)# **ipv6-address** ipv6-prefix/prefix-length[eui-64]	States the IPv6 network set to the interface and enables IPV6 processing on the interface.
Router(config-if)# **tunnel source**{ip-address / interface-type interface number}	States the source IPv4 address and the number for the tunnel interface. The source IPv4 address must be reachable from the other side of the tunnel. The interface must be configured with an IPv4 address if interface is specified.
Router(config-if)# **tunnel destination** ip-address	States the destination IPv4 address or host for the tunnel interface
Router(config-if)# **tunnel mode ipv6ip**	States a manual IPv6 tunnel. Note: the tunnel mode ipv6ip command states IPV6 as the passenger protocol and IPv4 as both the encapsulation and transport protocol for the manual IPv6 tunnel.
Router(config-if)# **ipv6 route** ipv6-prefix/prefix length **tunnel** tunnel-number	Configures a static route for the IPv6 prefix using the tunnel number specified in the interface tunnel command.

6.2.2 Challenges

Table 5 provides a description for different commands used for configuration for 6to4 manual tunnel. A brief outline of the challenges faced by the 6to4 manual tunnel in the network are listed below:

- It has to be manually configured.
- There will be potential issues with delay and latency through the tunnel.
- Tunnel destination point is unknown.
- Extra (additional) CPU load is needed for encapsulation and de-capsulation.
- There is no built in security. [12]

6.3 6to4 Tunnels

Manual tunnels are easy to configure but they do not scale well when a large number of tunnels is necessary. IETF has defined a mechanism called 6to4 to automatically connect to multiple IPv6 networks over one configured tunnel. 6to4 tunnels are defined in RFC 3056 [10], connection of IPv6 Domains via IPv4 Clouds. This 6to4 is point-to-multipoint connection. The difference between 6to4 and a manual tunnel is that the manual tunnel has to configure statically the other end of the tunnel, the tunnel IPv4 destination address while the IPv4 destination address is automatically derived from the IPv6 destination of the packet.

A single 6to4 tunnel can be used to connect to any number of IPv6 networks, any number of tunnel destinations. Below is the figure describing the 6to4 tunnel.

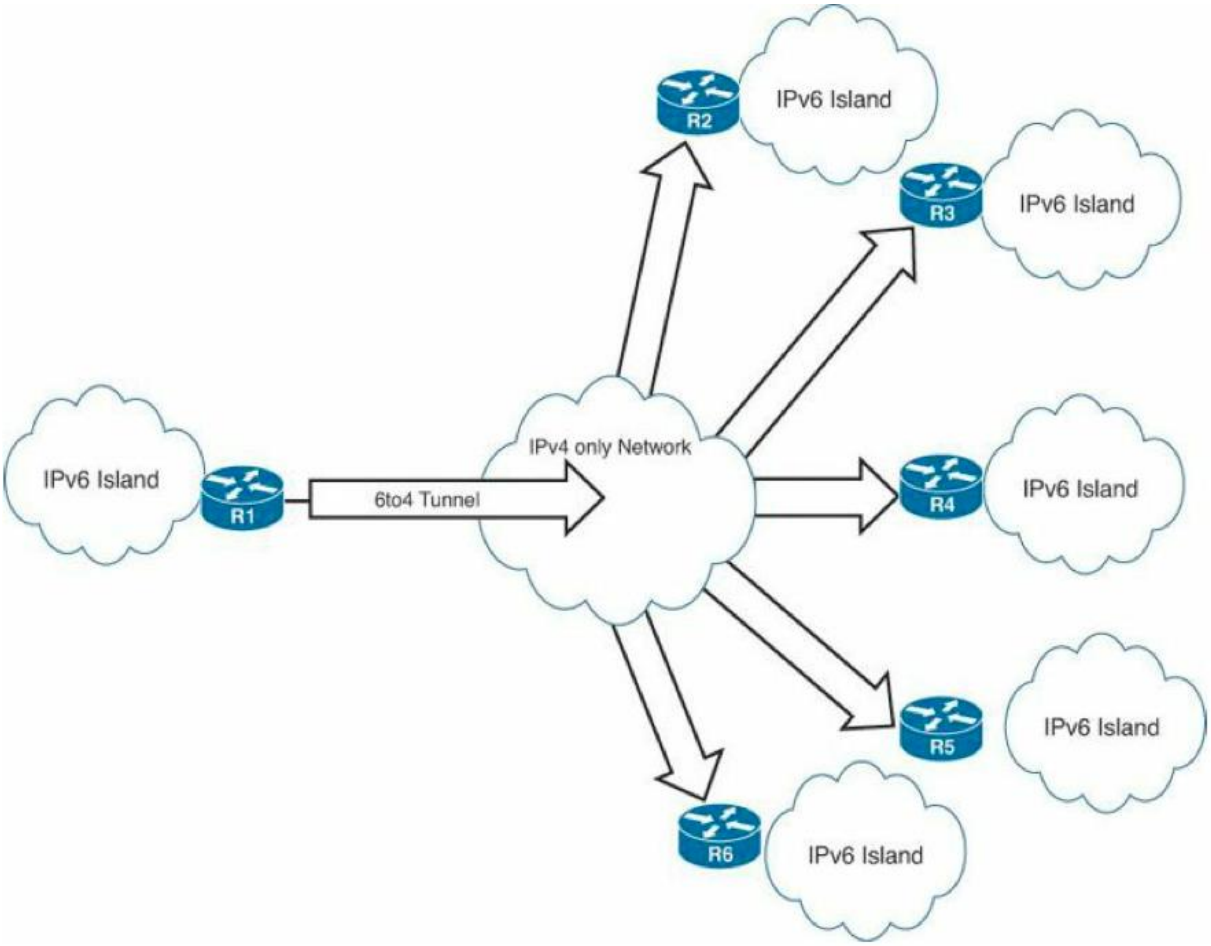


Figure 9. 6to4 tunnel [9]

6.3.1 Configuration

In the following Table 6, there is a description and the commands for configuring the 6to4 tunnel between two end points.

Table 6. Configuration commands for 6to4 tunnel [10]

Command	Description
Router(config)# **interface tunnel** tunnel-number	States a tunnel interface and number and enables configuration mode.
Router(config-if)# **ipv6-address** ipv6-prefix/prefix-length [eui-64]	States the IPv6 network set to the interface and enters IPv6 processing on the interface. The IPv6 enable command can be used to create a link-local address and enable IPv6 on the interface without specifying an IPv6 address.
Router(config-if)# **tunnel source**{ip-address /interface-type interface number}	States the source IPv4 address or the source interface type and number for the tunnel interface. The source IPv4 address must be reachable from the other side of the tunnel. If an interface is defined, the interface must be configured with an IPv4 address.
Router(config-if)# **tunnel mode ipv6ip 6to4**	States an IPv6 tunnel using a 6to4 address. Using the 6to4 technique IPv4 destination address will be determined.
Router(config-if)# **ipv6 route** ipv6-prefix/prefix-length **tunnel** tunnel-number	Configures a static route for the IPv6 to 6to4 prefix 2002::/16 to the specified tunnel interface. The tunnel number that is specified in the ipv6 route command should be same as the tunnel number in

	the interface tunnel command.

6.3.2 Challenges

Table 6provides a description for different commands used for configuration for 6to4 tunnel. 6to4 tunnel can be used to connect to any number of IPv6 networks and any number of tunnel destinations. A brief outline of the challenges faced by the 6to4 tunnel in the network are listed below:

- ➢ This mechanism requires a globally unique IPv4 address and the NAT tunnel endpoint is not allowed.
- ➢ IPv4 packets to broadcast, multicast, and loopback address must not be sent through tunnel.
- ➢ This technique is suitable for sites but not for individual hosts. [12]

6.4 ISTAP

ISATAP stands for Intra-Site Automatic Tunnel Addressing Protocol. ISTAP tunnels are sketched for transporting IPv6 packets within sites but not between the sites, where IPv6 infrastructure is not available. It is similar to other automatic tunneling mechanisms. ISATAP uses a well-defined IPv6 address format consisting of any /64 unicast IPv6 prefix and a 64-bit interface ID that contains the last 32 bits of the IPv6 address.

Unlike (?) other tunneling methods, it can remain between any two dual stack devices: host-to-host, host-to-router or router-to-host. The main feature of ISATAP is to provide dual stack hosts with access to the IPv6 network over IPv4 only network.

It is considered a quick and temporary solution to give access to IPv6 resources.

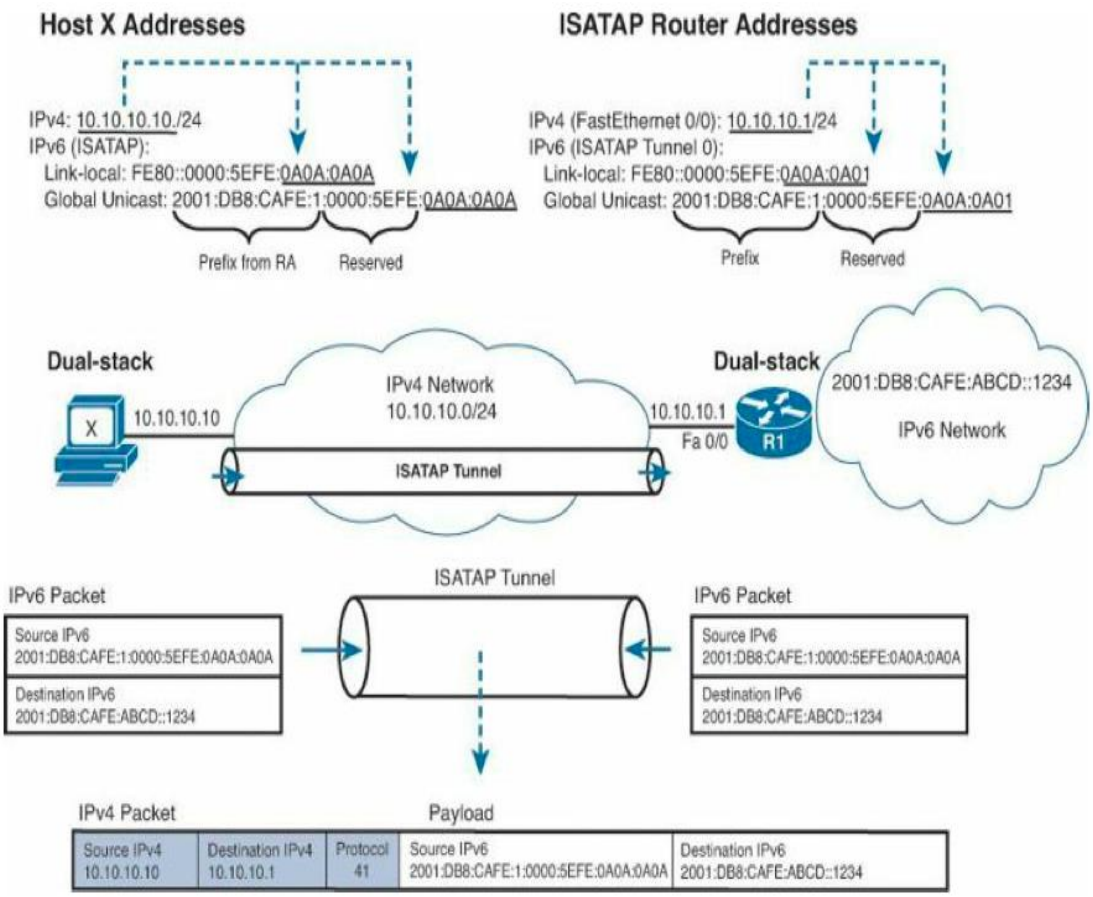


Figure 10. ISATAP Tunnel [10]

6.4.1 Configuration

In Table 7, there is a description and the commands for configuring an ISATAP tunnel between two end points.

Table 7. Configuration commands for an ISATAP tunnel [10]

Command	Description
Router(config)# **interface tunnel** tunnel-number	States a tunnel interface and number and enables a configuration mode
Router(config-if)# **ipv6-address** ipv6-prefix/prefix-length [**eui-64**]	States the IPv6 network assigned to the interface and enables IPv6 processing on the interface. Using the eui-64 option will create an IPv6 address using the ISATAP EUI-64 format.
Router(config-if)# **no ipv6 nd suppress-ra**	This commands re-enables the sending of IPv6 Router Advertisements to allow client auto configuration as sending of IPv6 Router Advertisements is disabled by default on tunnel interface. The command **no ipv6 nd ra suppress** can also be entered.
Router(config-if)# **tunnel source** {ip-address /interface-type interface number}	States the source IPv4 address or the source interface type and number for the tunnel interface. If an interface is defined, the interface should be configured with and IPv4 address.
Router(config-if)# **tunnel mode ipv6ip isatap**	States an IPv6 tunnel using an ISATAP address.

6.4.2 Challenges

Table 7 provides a description for different commands used for configuration in an ISATAP tunnel. These tunnels are designed for transporting IPv6 packets within sites but not between the sites. Small outlines of challenges faced by it in the network in order to check the incoming and outgoing network are mentioned below:

- This technique requires more setup than other methods.

- ➢ It has some security issues.
- ➢ It is designed for intra-site use not for the inter-site connectivity. [12]

6.5 Network Address Translation

Network Address Translation (NAT) method facilitates communication between IPv4-only and IPv6-only network by translating two different IP address families. This method translates IPv6 from IPv4 and gives consistent Internet experience to the users by accessing contents over the Internet, which have IPv4 services. Another important feature of this method is that existing Internet service providers can provide IPv6 services just by using translation features and that is why they do not have to upgrade their whole system to IPv6 to provide IPv6 services to the end users. [13] The two types of translation are

i) NAT64: Network Address Translation IPv6 to IPv4

ii) NAT-PT: Network Address Translation – Protocol Translation

NAT is a common procedure in IPv4, commonly used to translate between private (RFC 1918)[10] address and public IPv4 address space. NAT64 provides connection between IPv4-only networks and IPv6 only. It provides two major advantages over tunneling, provides a gradual and seamless migration to IPv6 and services transparently to IPv6 Internet users.

NAT64

NAT 64 is the technique or procedure for IPv4-to-IPv6 transition and IPv4-IPv6 coexistence. NAT64 is the replacement for the NAT-PT as documented in RFC 6144, Framework for IPv4/Ipv6 Translation. With DNS64, the fundamental goal of NAT64 is to allow an IPv6-only client to initiate communications to an IPv4-only server.

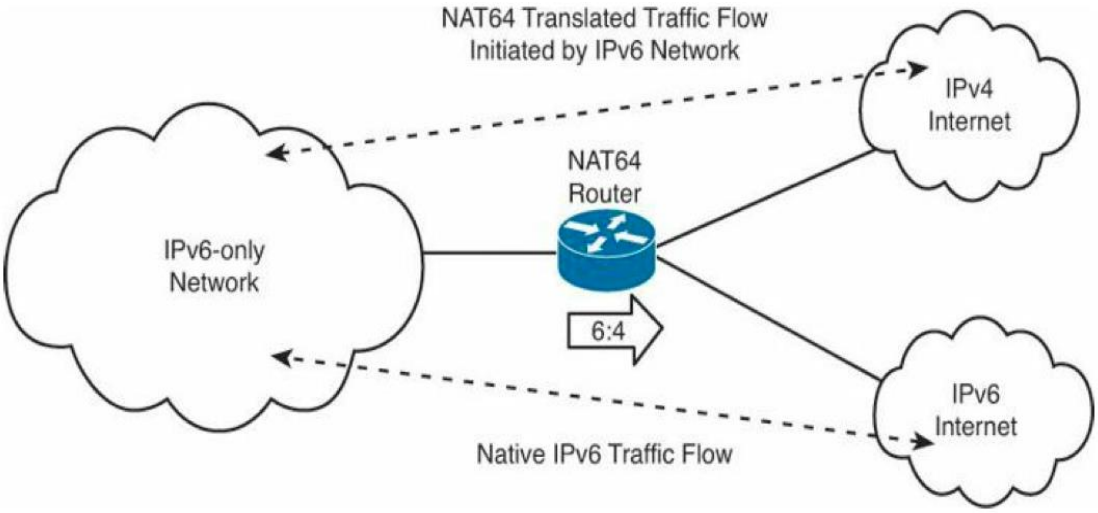


Figure 11. IPV6-only Network Accessing IPv4 and IPv6 Internet [10]

In Figure 11, the communication channel between IPv4 Internet and IPv6 Internet is presented, sketching the effect of protocol routing on router in Internet network.

There are three components to NAT64: -

NAT64 prefix: Prefixes /32, /40, /48, /56, /64, or /96 are used with a converted IPv4 address to transport the packet over the IPv6-only networks. A Prefix can be a network–specific prefix (NSP) or a well-known prefix (WKP). An NSP refers to an organization and is generally a subnet from the organization's prefix. The WKP for NAT64 is 64:ff9b::/96. If NSP is not defined, NAT64 will use WKP to prepend the converted IPv4 address.

DNS64 server: The DNS64 server acts as a normal DNS server for IPv6 AAAA records but will try to detect an IPv4 A record when the AAAA record is not available. If an A record is detected, DNS64 changes the IPv4 A record into an IPv6 AAAA record using the NAT64 prefix. It gives the feeling to the IPv6-only host that it can communicate with a server using IPv6.

NAT64 router: The NAT64 router advertises the NAT64 prefix into the IPv6-only network along with operating the translation between the IPv6-only and IPv4-only network.

In Table 8, there is a description and the commands for configuring the router for NAT64.

Table 8. Basic commands used to configure the router for NAT64 [10]

Command	Description
Router(config)# **interface** type number	States an interface type and number and enable the configuration mode. This interface faces only IPv6-only network and only configured with an IPv6 address.
Router(config-if)# **ipv6 address** ipv6-address/prefix-length	States the IPv6 address and prefix length to be assigned.
Router(config-if)# **nat64 enable**	Enables NAT64 translation on the interface.
Router(config-if)# **interface** type number	States an interface type and number and enables configuration mode. This interface faces only IPv4-only network and only configured with an IPv4 address.
Router(config-if)# **ip address** ipv4-address subnet-mask	States the IPv4 address and subnet mask to be assigned to the interface.
Router(config-if)# **nat64 enable**	Enables NAT64 translation on the interface.
Router(config-if)# **nat64 prefix stateful** ipv6-prefix/prefix-length	Explains the prefix and a prefix length for stateful NAT64: Ipv6-prefix: this argument must be in the form documented in RFC 2373, where address is defined in hexadecimal using 16-bit values between colons. /prefix-length: length of the IPv6 prefix.

Router(config-if)# **nat64 v4 pool** pool-name start-address-range end-address-range	Enables NAT64 IPv4 configuration. pool: configures and IPv4 address pool. pool-name: name of the IPv4 address pool. start-address-range: starting address of the address pool range. end-address-range: ending address of the address pool range.
Router(config-if)# **nat64 v6v4 list** list-name **pool** pool-name [overload]	Translates an IPv6 source address to IPv4 source address and IPv4 destination address to an IPv6 destination address for NAT64: list: associates an IPv4 pool with the filtering mechanism, which decides when to apply an IPv6 address mapping. list name: the name of the IPv6 access list. pool: determines the NAT64 pool for dynamic mapping of addresses. pool-name: the name of the NAT64 pool. overload: enables NAT64 overload address translation(optional).
Router(config-if)# **ipv6 access-list** access-list-name	Explains an IPv6 ACL, and enters IPv6 access list configuration mode. The argument access-list-name defines the name of the IPv6 ACL.
Router(config-if)# **ipv6 permit** ipv6-address/ipv6-prefix-length	States the IPv6 address and prefix length to be translated.

NAT-PT: Network Address Translation – Protocol Translation

NAT-PT is similar to the NAT system utilized in IPv4 that is frequently used for converting private (RFC 1918) IPv4 address to public IPv4 address and vice versa. It is used to convert IPv4 address to IPv6 address and vice versa. This method should be used only when there are no other techniques to allow IPv6-only devices to communicate with IPv4-only devices.

The common types of NAT-PT are discussed below: -

Static NAT-PT

The static NAT-PT uses static translation order to map one IPv6 address to one IPv4 address. One-to-one mapping of the IPv6 and Ipv4 address is statically configured on the NAT-PT router. It is useful when applications or servers require connection to the stable IPv4 address.

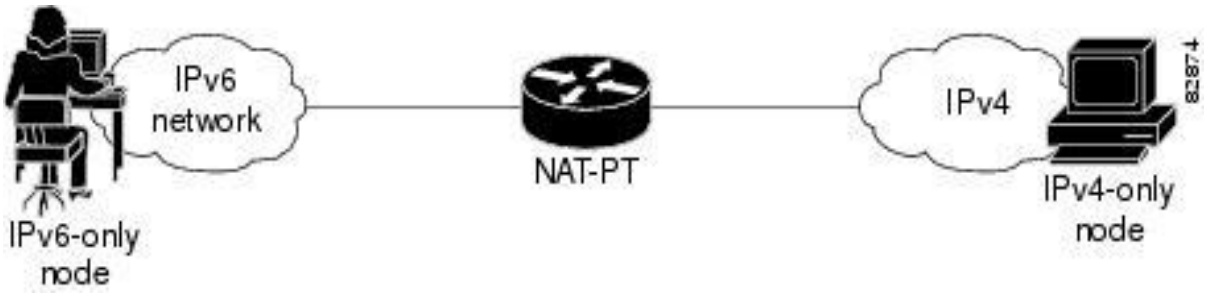


Figure 12. Dynamic NAT-PT Operation [14]

Dynamic NAT-PT

The dynamic NAT-PT translation technique needs at least one static mapping for the IPv4 Domain Name System (DNS) server. After the IPv6 to IPv4 network is settled, reply packets travelling from IPv4 to IPv6 use the formerly settled dynamic mapping to convert back from IPv4 to IPv6 and vice versa for an IPv4-only host.

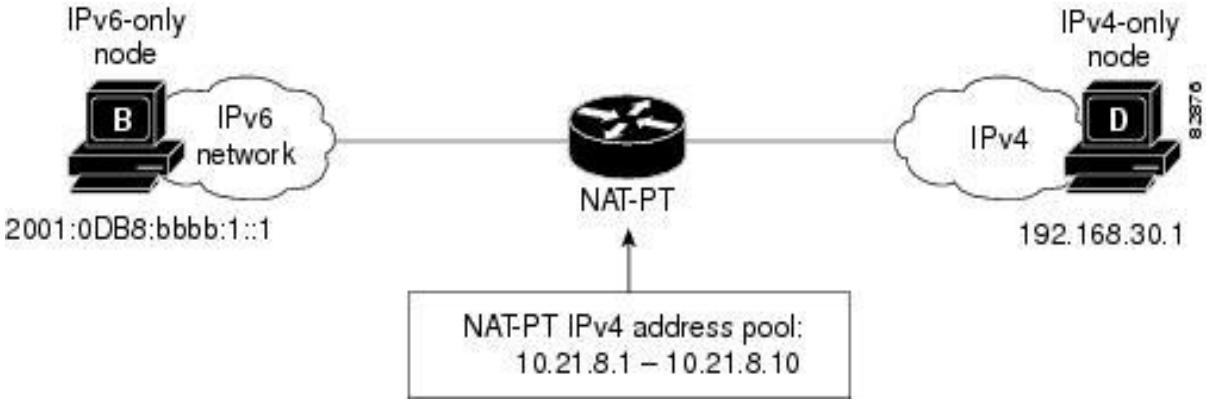


Figure 13. Dynamic NAT-PT Operation [14]

6.5.1 Configuration

InTable 9, there is a description and the commands for configuring static NAT-PT.

Table 9. Configuration commands for static NAT-PT [10]

Commands	Description
Router(config)# **interface** type number	States an interface type and number and enable the configuration mode. This interface faces only IPv6-only network and only configured with an IPv6 address.
Router(config-if)# **ipv6 address** ipv6-address/prefix-length	States the IPv6 address and prefix length to be referring to the interface.
Router(config-if)# **ipv6 nat**	Enables NAT-PT on the interface.
Router(config-if)# **interface** type number	States an interface type and number and enable the configuration mode. This interface faces only IPv4-only network and only configured with an IPv4 address.
Router(config-if)# **ip address** ipv4-address subnet-mask	States the IPv4 address and subnet mask to be referring to the interface.
Router(config-if)# **ipv6 nat**	Enables NAT-PT on the interface.

Router(config-if)# **ipv6 nat prefix** ipv6-prefix/prefix-length	Explains the IPv6 prefix to be used as the NAT-PT prefix for the IPv6 domain. The only prefix length supported is 96.
Router(config-if)# **ipv6 nat v4v6** source ipv4-address ipv6-address	Packets with the source ipv4-address will be converted to the source ipv6-address. The IPv6-address is the destination IPv6 address used by the IPv6 host to reach the IPv4 host.
Router(config-if)# **ipv6 nat v6v4** source ipv6-address ipv4-address	Packets with the source IPv6-address will be converted to the source IPv4-address. The IPv4-address is the destination IPv4 address used by the IPv4 host to reach the IPv6 host.

In Table 10, there are the configuration commands for dynamic NAT-PT with the description.

Table 10. Configuration commands for dynamic NAT-PT [10]

Commands	Description
Router(config)# **ipv6 access-list** ipv6-acl-name	Explains the IPv6 access list and enables the configuration mode in the router.
Router(config-ipv6-acl)# **permit** source-ipv6-address/prefix-length destination-ipv6-address/prefix-length)	Explains the range of IPv6 addresses allowed to be translated.
Router(config)# **ipv6 natv6v4** source list ipv6-acl-name pool ipv4-pool-name	Explains the dynamic mapping between the permitted IPv6 source address and the pool of IPv4 address. The IPv6-acl-name identifies the IPv6 ACL used to determine which IPv6 will be translated. The IPv4-pool-name selects the pool of IPv4 address to be used in the

	translation.
Router(config)# **ipv6 nat v6v4 pool** ipv4-pool-name ipv6-acl-name start-ipv4-address end-ipv4-address	Explains the pool of source IPv4 address used for translation.

6.5.2 Challenges

Table 10 provides a description for different commands used for configuration in static and dynamic NAT-PT. Mostly, it modifies restriction based on the updated configuration of network. It works with IPv6 access-list and allows/denies the network accordingly. Small outlines of challenges faced by NAT in the network in order to check the incoming and outgoing network are mentioned below:

- They are not expected to be used widely as they slow down packet flow.
- They do not allow the network to exploit specific capabilities of either protocol.
- They act as a redundant channel in the online communication over the Internet. [12]

6.6 Future of IP Addressing

Everyone one in the modern business world uses Internet and its rapid growth is the main reason behind the importance of Internet Protocol (IP) address. Every device must have a unique IP address to connect to the Internet in order to exchange data with another. Everyone uses IP addresses but only few understand them as they cannot be seen and are highly intangible. There is a great change happening as people are moving to adopt IPv6 and providers are trying to save their customers by moving to IPv6. If providers do not do so, they will soon be out of business as the IPv4 will be no longer in use. Providers should understand IPv6 and ensure they are prepared for the future, IPv4 and IPv6 are not compatible and devices using one or the other cannot communicate directly. Either providers should upgrade their devices or change to IPv6 by using transition techniques. One of the popular techniques is dual stacking as it supports both IPv4 and IPv6. IPv6 is the only long-term solution to

the depletion of IPv4 address pool. The depletion IPv4 address pool affects routing security. While distributing IPv4 addresses there was always pressure to preserve the free pool of IPv4 by making smaller allotment and aggregation. The astounding amount of available IPv6 address means that conservation is no longer pressing and large piles of blocks can be given out. [15]

Without IPv6 there will be limitation in use of technology in the coming years such as smartphones, which are gaining popularity in the recent years. With the increase of population and users of Internet, it is hard to settle with IPv4. Every Internet provider and company is moving to IPv6. Most of the countries, like China, the USA and India etc., have already moved their services to IPv6. For the continuous growth of Internet and spreading through the world, deployment of IPv6 is necessary.

7 ADVANTAGES AND DISADVATAGES OF PRACTICAL TRANSITION OF IPV6 OVER IPV4

ISPs and big companies need to take steps to ensure service continuity with transparency for their customers at all the times during transition and co-existence. It is most important that the transition to IPv6 is stable and non-interruptive to exiting services. The operators should have clear ideas how they will transition to IPv6 and know the risks and challenges ahead before they start the transition. Some operators may focus on green design while other may focus on IPv4 and IPv6 co-existence. Operators should have list of strategies and concepts what they are seeking for. IETF has been developing tools for more than a decade for transitioning to IPv6 but many operators have not yet begun yet. The reason behind that could be lacking IPv6 development in applications, hosts, CPEs, network equipment, and contents. Another reason could be lack of knowledge in applying technologies and techniques in the network without causing interruption in service. The transition problem faced by the providers include the following areas: Network, Connectivity, Applications, and network Management and Operation. [16]

a) Network problems

Address Architecture

IPv6 has much larger address space in comparison with IPv4. Due to the large IPv6 address space, special attention is needed when designing the IPv6 network since it differs from the fragmented and smaller IPv4 address design. Providers will need to plan in advance for IPv6 unlike IPv4, will provide them with an enormous address space, which needs cautious architectural consideration.

Connectivity

While starting transition to IPv6, the systems engineers should design a network to provide continuity of service to the customers. For this, dual stack is the natural approach but due to the depletion of IPv4 address and cost, providers may consider to upgrade part of their network to IPv6-only.

High Availability

High Availability (HA) is the major requirement for every service and network service. Providers have huge experience in running high availability in IPv4 using mature protocols, such as VRRP and OSPF Graceful Restart. Compared to IPv4, HA for IPv6 is less known. An application running on IPv6 may need to failover to IPv4 network due to network failure during transitioning. Some work needs to be done in this area to fix this problem. Besides, the new transition techniques require new HA models. If HA is supported, providers will normally deploy a transition method. [16]

b) Application Problems

During the transition process, IPv4 and IPv6 application will coexist in the network. Regardless of what technology providers choose to use, services should be provided to the customers. Providers should find out the best techniques for the transition without affecting the services they provide.

c) Network Management and Operation Problems

In paper, organizing an IPv6 network should be similar to organizing an IPv4 network. For example, SNMP works over IPv6 without modification. New technologies and techniques may be introduced during the transition process. These new technologies and techniques require new operation models.

The growth of Internet users has led to the shortage of usable IPv4 in the nearer future. Giant communication companies, like China Telecom, are practical examples for encouragement of IPv6, because of consequences caused due to the limited IPv4 addresses. Few technical issues arise due to the change of platform from IPv4 to IPv6 and these are outlined as follows: -

1. Limited availability of IPv4 addresses to China Telecom gave rise to the need to find a new way of identifying Internet gateways. This led to the transition to IPv6. [17]
2. Newly used IPv6 is uncommon in Internet websites and very few Internet Content Provider (ICP) look for the option of IPv6 when

expanding proprietary services because of the enormous code change and increasing manpower. Many business websites are always linking each other and creating a complex structure, which leads to many problems when one website migrates to IPv6 only. Content Provider/Service Providers (CP/SP) do not realize how urgent it is to migrate to IPv6, which is the main reason why ICP migration lacking motivation. [17]

3. Some specific terminals (for example, set top box) do not support IPv6 while the main operating systems do. [17]
4. China Telecom has two key problems while IPv6 transition, large-scale network and large number of subscribers. The transition involves multiples level and broad scope, which lead to huge costs in modification as with the large-scale network and various service platforms. [17]
5. The use of IPv6 becomes a reliable solution for companies like China Telecom and Internet-based companies for expanding the volume of subscribers.

8 CONCLUSION

The thesis discusses the approach of IPv6 over the limited IPv4 in Internet world where users have increased rapidly. It also compares the consequences and features of transition from IPv4 to IPv6. Transition methods with their configuration and challenges that come forward during each transition process, are also documented in this thesis. A practical approach of various transition methods led to the conclusion that dual stack remains more popular and practical with low cost in implementation and supported by wide range of devices. Transition methods, like tunneling and translation, are not optimally supported for the networks during a transition from IPv4 to IPv6 although these tools are provided by IETF to make the transition easier. Thus, dual stack seems the preferable method to begin adopting IPv6 with upgradable devices in order to securely manage the exiting IPv4 Infrastructure. This transition incurs minimal impact on customers, as they do not have to move IPv6 overnight and can deploy and migrate to IPv6 when they are ready.

The thesis also provides the comparison between IPv4 with IPv6, reflecting on the consequences arising due to transition from one to the other. IPv6 has newly introduced an Internet algorithm, taking a comparable elapse of time to complete the upgrade on the entire telecommunication platform, and working with zero stress under IPv4. The transition problems faced by the Internet service providers concern network, connectivity, applications, and network management and operation. Before the process of deployment, a study can be carried out so that the time and cost can be saved during the transition process. The deployment of IPv6 is the best way for the growth of Internet and users around so that there will be no any limitation to using the technology that are discovering.

REFERENCES

[1] What is IPv6? [ONLINE] Available at: http://IPv4.opus1.com/IPV6/whatisIPV6.html. [Accessed: 03 March 2015].

[2] Router-Switch. 2013. What is OSI Model & the Overall Explanation of ISO 7 Layers. [ONLINE] Available at: http://IPv4.cisco1900router.com/what-is-ios-model-the-overall-explanation-of-ios-7-layers.html. [Accessed: 04 March 2015].

[3] omnisecu. TCP/IP. [ONLINE] Available at: http://www.omnisecu.com/tcpip/tcpip-model.php. [Accessed: 07 July 2015].

[4] Kurose, J &Ross, K. 2010. Computer Networking. 5th ed. USA: Pearson

[5] Eazynotes. Comparasion between OSI and TCP/IP model. [ONLINE] Available at: http://www.eazynotes.com/notes/computer-networks/slides/comparison-between-osi-tcpip-model.pdf. [Accessed: 04 July 2015].

[6] tutorialslodge. 2014. OSI and TCP/IP Model. [ONLINE] Available at: http://tutorialslodge.com/osi-tcpip-model/. [Accessed: 10 July 2015].

[7] tcpipguide. Internet Protocol Version 4 (IP, IPv4). [ONLINE] Available at: http://IPv4.tcpipguide.com/free/t_InternetProtocolVersion4IPIPV4.htm. [Accessed: 20 May 2015].

[8] IPv4 Addressing. 2015. IPv4 Addressing. [ONLINE] Available at: https://technet.microsoft.com/en-us/library/dd379547(v=ws.10).aspx. [Accessed: 02 July 2015].

[9] IBM. Comparison of IPv4 and IPv6. [ONLINE] Available at: https://IPv4-01.ibm.com/support/knowledgecenter/ssw_ibm_i_72/rzai2/rzai2compIPV4IPV6.htm. [Accessed: 08 April 2015].

[10] Graziani. R. 2012. IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6. 1 Edition. Cisco Press.

[11] training.apnic.net. 1800. IPv4 to IPv6 Transition. [ONLINE] Available at: https://training.apnic.net/docs/eIP603_Transition.pdf. [Accessed: 12 July 2015].

[12] Sellers, C. 2009. IPv6 Transition Mechanisms and Strategies. [ONLINE] Available at: http://IPv4.rmv6tf.org/wp-content/uploads/2012/11/Chuck-Sellers-090421-IPV6-Transition-Mechanisms-Sellers1.pdf. [Accessed: 29 June 2015].

[13] Das, K. Network Address Translation (NAT) Pros & Cons. Network Address Translation (NAT) Pros & Cons, [Online]. Available at: http://IPv6.com/articles/nat/NAT-Pros-and-Cons.html [Accessed: 29 July 2015].

[14] Cisco. NAT-PT for IPv6. [ONLINE] Available at: http://IPv4.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html. [Accessed 28 July 2015].

[15] IP Addresses. 2013. IP Addresses. [ONLINE] Available at: http://www.itproportal.com/2013/07/02/ip-addresses-how-they-shaped-the-past-of-the-internet-and-what-they-will-influence-its-future/. [Accessed: 09 August 2015].

[16] IETF. 2010. Problem Statements of IPv6 Transition of ISP. [ONLINE] Available at: https://tools.ietf.org/html/draft-lee-v4v6tran-problem-02. [Accessed: 04 August 2015].

[17] Internet Engineering Task Force. 2011. Broadband Service Provider Use Case . [ONLINE] Available at: http://www.watersprings.org/pub/id/draft-tian-v4v6tran-broadband-sp-usecase-00.txt. [Accessed 11 July 2015].