Degree project

Migration from Internet Protocol Version 4 To Internet Protocol Version 6

Author: Amjad Mithani
Supervisor: Ola Flygt
Date: 2014-11-24
Course Code: 4DV01E, 15 credits
Level: Master
Department of Computer Science
Abstract

IPv4 has played it big role in spreading Internet and Internet based applications for more than 20 years. Now it will hand over the stage to its more powerful successor IPv6. IP is an important component of the TCP/IP protocol suit and the Internet is built on it.

IPv6 is a new generation protocol suite which has been proposed by the Internet Engineering Task Force (IETF) which uses the 128-bit address instead of IPv4 32-bit address. Moving to the next generation of Internet Protocol became an issue to solve many problems in the current generation.

Unfortunately IPv4 and IPv6 are incompatible with each other. It is necessary to create smooth transition mechanisms that a transition mechanism is required during the time of migration from IPv4 to IPv6 networks. This paper aims to supplement this by presenting the design and implementation of IPv4 to IPv6 Transition Scenarios. This paper very clearly illustrates the transition of IPv4-to-IPv6 Transition mechanisms along with how to execute IPv6 commands.

Keywords: IPv4, IPv6, TCP/IP Prot, Internet Engineering Task Force, Transition.
Acknowledgement

This research thesis would not have been possible without the kind support and help of many individuals. I would like to offer special thanks to my supervisor, lecturer Ola Flygt at Linnaeus University, School of Computer Science, Physics and Mathematics, for his guidance and constant supervision as well as for providing necessary information regarding the project and also for his support in completing this research project.

I would like to express my very great appreciation to Borge Nielsen for his valuable and constructive suggestions during lab at school Teknikum in Växjö. His willingness to give his time so generously has been very much appreciated.

I would also like to thank the staff of the school Teknikum in Växjö for giving me permission to visit their school and allow me to access the material in CISCO lab during tests for my project.

And finally, thanks to my parents, brothers and friends. They always supported me and encouraged me with their best wishes for the successful completion of this project.
**Contents**

1 INTRODUCTION .................................................................................................................. 1
   1.1 NEED OF IPv6 ................................................................................................................ 1
   1.2 PROBLEM STATEMENT .................................................................................................. 1
   1.3 RESEARCH CHALLENGES ............................................................................................. 1
   1.4 THESIS PURPOSE AND RESEARCH METHODOLOGY ............................................. 2
   1.5 ETHICAL ASPECTS ......................................................................................................... 2
   1.6 THE INTENDED AUDIENCE .......................................................................................... 2
   1.7 LIMITATIONS ................................................................................................................ 2
   1.8 OUTLINE ....................................................................................................................... 2

2. BACKGROUND ...................................................................................................................... 3
   2.1 INTERNET PROTOCOL VERSION 4 (IPv4) ..................................................................... 3
      2.1.1 Limited IPv4 Address Space .................................................................................. 3
   2.2 INTERNET PROTOCOL VERSION 6 (IPv6) ..................................................................... 4
   2.3 POTENTIAL ISSUES ...................................................................................................... 4
      2.3.1 Steps of Adoption .................................................................................................. 5
      2.3.2 Consumer Demand ............................................................................................... 5
      2.3.3 No Flag Date ......................................................................................................... 5
      2.3.4 Ubiquitous Communications ............................................................................... 5
      2.3.5 VoIP/Multimedia Services .................................................................................. 5
      2.3.6 Social Networks .................................................................................................. 6
      2.3.7 Sensor Networks .................................................................................................. 6

3. IPV6 ..................................................................................................................................... 7
   3.1 REASONS OF CHANGING IPv4 ................................................................................... 7
      3.1.1 Scarcity of IPv4 Address Space ............................................................................ 7
      3.1.2 Multimedia Traffic Handling ............................................................................... 7
      3.1.3 Mobility ............................................................................................................... 8
      3.1.4 Packet Handling .................................................................................................. 8
   3.2 IPv4 HEADER v/s IPv6 HEADER .................................................................................. 9
   3.3 CHALLENGES IN IPv6 DEPLOYMENT ................................................................. 10
      3.3.1 Limited Availability of IPv6 Resources on Internet ............................................. 10
      3.3.2 Unavailability of IPv6 Capable Applications ...................................................... 10
      3.3.3 Inherent Problem in Path MTU Discovery Process ............................................. 10
      3.3.4 Complexity in Mobile IPv6 Architecture ............................................................. 10
      3.3.5 Network Compatibility .......................................................................................... 11
      3.3.6 Compatibility Issues in Hardware ....................................................................... 11
      3.3.7 Compatibility Issue in Software .......................................................................... 11
      3.3.8 Improper IPv6 Implementation ............................................................................ 11
   3.4 ADDRESSING THE CHALLENGES ........................................................................... 11
      3.4.1 Encouragement from Government and Statutory Bodies .................................... 11
      3.4.2 No Experimentation on Production Network ....................................................... 11
      3.4.3 Co-existence of Both by Dual Stacking ............................................................... 12
   3.5 NETWORK ADDRESS TRANSLATION – PORT TRANSLATION ................................ 12
   3.6 TUNNELS ...................................................................................................................... 13
   3.7 METHODS BY WHICH SUCH TUNNELS CAN BE IMPLEMENTED ................................. 14
      3.7.1 Static Point to Point Tunnels .............................................................................. 14
      3.7.2 Dynamic Multpoint Tunnels ............................................................................... 14
         a. Automatic 6to4 tunnels ......................................................................................... 14
         b. Inter-site Automatic Tunneling Address Protocol .............................................. 14
4. IMPLEMENTATION OF IPV6 ......................................................................................... 16
  4.1 DIFFERENT TRANSITION TECHNOLOGIES USED TO CONDUCT EXPERIMENTS ...................................................... 16
  4.2 CASE 1 - IPV6 NETWORK TO IPV4 INTERNET, 6TO4 ............................................................................................................. 16
  4.3 CASE 2 - IPV4 INTERNET TO IPV6 NETWORK, 6TO4 ............................................................................................................. 17
  4.4 CASE 3 - IPV6 INTERNET TO IPV4 NETWORK, 4TO6 ............................................................................................................. 18
  4.5 CASE 4 - IPV6 NETWORK TO IPV4 NETWORK, 6TO4 ............................................................................................................. 19
  4.6 CASE 5 - IPV4 NETWORK TO IPV6 NETWORK, 4TO6 ............................................................................................................. 20
  4.6 CASE 6 - IPV6 TUNNEL OVER IPV4 INTERNET, MANUAL MODE .......................................................................................... 21
  4.7 CASE 7 - IPV6 TUNNEL OVER IPV4 INTERNET, AUTOMATIC MODE .................................................................................. 22
  4.8 CASE 8 - IPV6 NETWORK TO IPV4 INTERNET, NAT-PT .......................................................................................................... 23
  4.10 CASE 9 - IPV4 INTERNET TO IPV6 NETWORK, NAT-PT ...................................................................................................... 24
  4.11 CASE 10 - IPV4/IPV6 DUAL STACK NETWORK ................................................................................................................ 25
  4.12 CASE 11 - POINT-TO-POINT .................................................................................................................................................. 26
  4.13 CASE 12 - POINT TO MULTIPoint AUTOMATIC 6TO4 ........................................................................................................ 27
  4.14 CASE 13 - POINT TO MULTIPoint AUTOMATIC ISATAP .................................................................................................... 28
  4.15 CASE 14 - IPV4 TO IPV6 NAT .................................................................................................................................................. 29
  4.16 THEORETICAL EXPLANATION OF SIMULATION RESULTS .............................................................................................. 30

5. CONCLUSION & THE FUTURE WORK ........................................................................... 33
  5.1 PROPOSED SOLUTIONS TO THE RESEARCH QUESTIONS .................................................................................................. 33
  5.2 CONCLUSION ........................................................................................................................................................................... 33
  5.2 FUTURE WORK ......................................................................................................................................................................... 34

REFERENCES ....................................................................................................................... 36

APPENDIX .............................................................................................................................. 1
  A. IPV6 NETWORK TO IPV4 INTERNET, 6TO4 .................................................................................................................... 1
  B. IPV4 INTERNET TO IPV6 NETWORK, 6TO4 .................................................................................................................... 4
  C. IPV6 INTERNET TO IPV4 NETWORK, 4TO6 .................................................................................................................... 7
  D. IPV6 NETWORK TO IPV4 NETWORK, 6TO4 .................................................................................................................... 9
  E. IPV4 NETWORK TO IPV6 NETWORK, 4TO6 .................................................................................................................... 12
  F. IPV6 TUNNEL OVER IPV4 INTERNET, MANUAL MODE .................................................................................................. 14
  G. IPV6 TUNNEL OVER IPV4 INTERNET, AUTOMATIC MODE ............................................................................................. 17
  H. IPV6 NETWORK TO IPV4 INTERNET, NAT-PT ................................................................................................................ 20
  I. IPV4 INTERNET TO IPV6 NETWORK, NAT-PT ................................................................................................................ 23
  J. IPV4/IPV6 DUAL STACK NETWORK .................................................................................................................................. 25
  K. POINT-TO-POINT: ................................................................................................................................................................. 28
  L. POINT TO MULTIPoint AUTOMATIC 6TO4 ..................................................................................................................... 30
  M. POINT TO MULTIPoint AUTOMATIC ISATAP ................................................................................................................ 33
  N. IPV4 TO IPV6 NAT ................................................................................................................................................................. 37
List of Figures

Figure 2.1 : Internet Domain Survey Host Count.................................................4

Figure 3.1 IPv6 Mobility with Home Agent, Mobile Node and Correspondent Node [29]........8

Figure 3.2 IPv4 and IPv6 header comparison (Courtesy Cisco Systems).................................9

Figure 3.3 Co-existence of both by dual stacking .....................................................12

Figure 3.4 NAT-PT (Courtesy Cisco Systems)................................................................13

Figure 3.5 Tunneling (Courtesy Cisco Systems).............................................................13

Figure 4.2 IPv6 network to IPv4 Internet.....................................................................17

Figure 4.3 IPv4 Internet to IPv6 network.....................................................................18

Figure 4.4 IPv6 Internet to IPv4 network, 4to6.............................................................19

Figure 4.5 IPv6 network to IPv4 network, 6to4 .............................................................20

Figure 4.6 IPv4 network to IPv6 network, 4to6 .............................................................21

Figure 4.7 IPv6 tunnel over IPv4 Internet, manual mode ..............................................22

Figure 4.8 IPv6 tunnel over IPv4 Internet, automatic mode ..........................................23

Figure 4.9 IPv6 network to IPv4 Internet, NAT-PT.....................................................24

Figure 4.10 IPv4 Internet to IPv6 network, NAT-PT....................................................25

Figure 4.11 IPv4/IPv6 Dual Stack Network.................................................................26

Figure 4.12 Point-to-point .........................................................................................27

Figure 4.13 Point to Multipoint Automatic 6to4............................................................28

Figure 4.14 Point to Multipoint Automatic ISATAP ....................................................29

Figure 4.15 IPv4 to IPv6 NAT ....................................................................................30
# List of Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>Third Generation</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
</tr>
<tr>
<td>BSD</td>
<td>Berkeley Software Distribution</td>
</tr>
<tr>
<td>CISCO</td>
<td>Computer Information System Company</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DF</td>
<td>Data Frame</td>
</tr>
<tr>
<td>EUI</td>
<td>End-User Interface</td>
</tr>
<tr>
<td>GNS</td>
<td>Graphical Network Simulator</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation, &amp; Air Conditioning</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Message</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPTV</td>
<td>Internet Protocol Television</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol Version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>ISATAP</td>
<td>Intra-Site Automatic Tunnel Addressing Protocol</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NAT-PT</td>
<td>Network Address Translation – Port Translation</td>
</tr>
<tr>
<td>NCP</td>
<td>Network Control Protocol</td>
</tr>
<tr>
<td>NGN</td>
<td>Next Generation Network(s)</td>
</tr>
<tr>
<td>NT</td>
<td>New Technology</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First (a routing protocol)</td>
</tr>
<tr>
<td>PMTUD</td>
<td>Path Maximum Transmission Unit Discovery</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VoD</td>
<td>Voice and Data</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol</td>
</tr>
</tbody>
</table>
1 Introduction
This chapter introduces the need for the Internet Protocol Version 6 (IPv6), states the problem definition and identifies the thesis goals.

1.1 Need of IPv6
IPv6 has numerous mechanisms over its forerunner, counting a superior and more miscellaneous address space, built in extensibility, and the influence to upkeep a more vigorous safety standard. Intrinsically, it assists as an influential groundwork for the formation of new and better-quality net-centric set of products and services. Even though the previous years will not go down in the records of past as ground-breaking for the Data Age, advanced supposed did not stop. It just stimulated into fester mode. This list is by no means comprehensive, but it does highpoint a numeral of very gifted expertise where IPv6 will be a building block. [19].

1.2 Problem Statement
It is already known that IPv4 has limited address space. In the future more address space will be needed for new portable devices in homes and in offices. The numbers of Internet users are increasing day by day. Till now billions of devices are connected to the Internet. As we know that migration process for the implementation of IPv6 is under development since the year 1990. Although thousands of organizations have received IPv6 resources, fully IPv6 adaption has been slower than anticipated. Computer Information System Company (CISCO) forecasts that as the number of users are increasing rapidly so in the near future connected devices will be double. IPv6 will support the larger address space on larger scale and provide better quality service. Using both routing protocols sending and receiving data could be successful with the help of tunnels. It might be possible to use different technologies to transmit the data, so different technologies will be used, for that purpose we will conduct some test based on different scenarios, to help us to migrate from IPv4 to IPv6 [27].

1.3 Research Challenges
In this report five important challenges are presented and proposed solutions in order to deliver reliable services by considering the above problem statement.
1. Why are we moving to IPv6 protocol and why IPv4 is going away?
2. What is beneficial about IPv6 and what are the main IPv6 improvements?
3. What changes do we need to do to be able to send and receive data belonging to both protocols simultaneously?
4. How does it work to communicate between two networks where one is using IPv4 and the other is using IPv6?
5. What possible transition technologies are there between IPv4 and IPv6 and how do they work?
1.4 Thesis Purpose and Research Methodology

The goal is to gain the theoretical knowledge and to do the research and help the individuals and organizations in moving from IPv4 to IPv6. The aim is to identify the challenges and problems and provide the easier solutions to help individuals not to depend on IPv4 but moving to IPv6.

As this project require the technical knowledge to provide the possible solutions from moving IPv4 to IPv6. Using the available resources which will more focused on IPv4 and IPv6, will clarify the problems, benefits and challenges that we are facing nowadays.

In the simulation part, experimental work using a Graphical Network Simulator (GNS) network emulator will be carried out, this tool provides friendly user interface rather than other existing emulators. Different scenarios will be designed by using GNS3. Later tests and configuration will be done and based on that results will be provided. This thesis will be based extensively on literature study and lab tests. In addition technology text books, articles and different forums from Information and Communication Technology (ICT) and Institute of Electrical and Electronics Engineers (IEEE) journals are used to get knowledge.

1.5 Ethical Aspects

Irrespective of the more fanciful possibilities of future Internet use, the need for IP addresses is related to providing fair access to the Internet. The shortage of IP addresses clearly arises as an ethical and societal issue in considering the scope for increasing the participation by people in developing countries. The technical security issues arising relate to the inherent or eventual capabilities of IPv6 to provide a secure environment for end-to-end transmission, on one hand, and the expansion of possible risks owing to the new uses to which IPv6-enabled devices will be put, on the other.

1.6 The Intended Audience

This thesis is intended for advanced network users who are willing to migrate from IPv4 to IPv6. Those who are already aware of the IPv4.

1.7 Limitations

Basic networking terms will not be covered in this thesis so reading this report will require technical knowledge of networks [32] [33]. Because of limited availability of the resources the problems identified and scenarios presented are tested in a lab, and it requires good technical knowledge to setup the lab environment. Security threats and protection will not be covered in this thesis because of the limited time and do not have any group member.

1.8 Outline

In the 1st chapter the need of IPv6 is presented. Problem statement is also presented in this chapter. Thesis purpose and research methodology, intended audience and limitations of thesis are also described. 2nd chapter represents the background of the research work. 3rd chapter provides information about IPv6 in depth. 4th chapter represents different scenarios based on problems identified and implemented the scenarios. 5th chapter represents the solution, and gather the results and evaluate and came up with conclusion and future work.
2. Background
This chapter represents the information about Internet Protocol Version 4 and Internet Protocol Version 6. In addition, some of the potential issues occur during migration are also described.

2.1 Internet Protocol Version 4 (IPv4)
Each computer system connected with Internet has an IP address. Till now version IPv4 over IPv6 is the only protocol which is mostly used over the Internet. All the medias are dependent on IPv4. The IPv4 has 4294967296 different addresses that is $2^{32}$.

Following table shows the classes of IPv4 [24].

<table>
<thead>
<tr>
<th>Classes</th>
<th>High Order Bits</th>
<th>Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td>0.0.0.0</td>
<td>127.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>10</td>
<td>128.0.0.0</td>
<td>191.255.255.255</td>
</tr>
<tr>
<td>C</td>
<td>110</td>
<td>192.0.0.0</td>
<td>223.255.255.255</td>
</tr>
<tr>
<td>D</td>
<td>1110</td>
<td>224.0.0.0</td>
<td>239.255.255.255</td>
</tr>
<tr>
<td>E</td>
<td>11110</td>
<td>240.0.0.0</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

Table 2.1: IPv4 Classes

As in the Table 2.1 there are 4 classes: First the IP address of class A which is in the range of (0.0.0.0 - 127.255.255.255) and then comes class B (128.0.0.0 - 191.255.255.255) and then C (192.0.0.0 - 223.255.255.255). These three classes of IP addresses used for commercial purpose. And class D which is (224.0.0.0 - 239.255.255.255) used for multicasting. And finally comes class D which is (240.0.0.0 - 255.255.255.255) used for research purpose.

2.1.1 Limited IPv4 Address Space
As described in section 2.1 that IPv4 contains many addresses. Hosts on the Internet are rapidly increasing each year which leads to the serious loss of IPv4 and will be used IPv6. Figuer 2.1 shows the Internet Domain Survey Host Count [25].
Figure 2.1: Internet Domain Survey Host Count

Figure 2.1 shows the time-period on x-axis and where as on the y-axis number of the hosts. In the figure the numbers of hosts are rapidly increasing from time to time. In year 2000 the numbers of hosts were 100,000,000 whereas in year 2006 it is 500,000,000 it shows the exponential growth of hosts. As we see IPv4 is in high demand every year as the numbers of hosts are increasing. At some time it will be bound to short of IPv4 address space [28].

2.2 Internet Protocol Version 6 (IPv6)

IPv6 is sometimes described as enhancement or modification of IPv4. But practically it is a different protocol that is developed to replace the existing IPv4 protocol from Transmission Control Protocol (TCP/ IP) protocol stack. There are some similarities between the two protocols, but the differences are more than the similarities. Details concerning this will be given in section 3.2. Though some fields are common like source and destination address etc but the fields are different in size and format. The new IPv6 address has 128 bits represented by blocks of hexadecimal representation while IPv4 addresses are 32 bit long binary field represented as 4 octets in decimal format [2].

Internet Protocol version 6 is basically the improvements of IPv4 and designed to overcome the deficiency in IPV4 [26]. Internet Protocol version 6 provides many features and provides the better performance and improvement.

2.3 Potential Issues

Migration from IPv4 to IPv6 does not only have to face technical issues there are many other issues as well. Here are some issues listed which can impact on our transition to IPv6 [17]. To discuss these issues is very important because we are going to build networks in future which will be based on IPv6. Requirements on networks are extremely different than 15 years ago. Today we are bulding networks that should work for many years in future. Following issues encounters influence deliberations in diverse ways.

1. Steps of Adoption
2. Consumer Demand
3. No Flag Date
4. Ubiquitous Communications
5. Voice over Internet Protocol (VoIP)/Multimedia Services
6. Social Networks
7. Sensor Networks

2.3.1 Steps of Adoption
Migration to IPv6 started slowly because initially the connectivity was limited, less material was available, backbone services were not plentiful, there was lack of IPv6 exchange points and IPv4 devices were embedded.

Before 2010 there was only very little portion of IPv6. Organizations are transforming to IPv6 but not leaving IPv4 at all, they want to keep both Internet protocols at the same time to support all their devices. IPv6 is growing but very slowly as it growing from very low base, it will take time to adopt it completely. A noteworthy barricade in its acceptance is negative network effect, which means that it causes many problems while setting up device to work with IPv6 [17].

2.3.2 Consumer Demand
IPv6 has never been consumer choice. They just need Internet regardless of the concern which Internet protocol is running. All the public Internet services are coming to them via Internet protocol version 4 so they do not think there is a need of a migration into version 6. All the devices which consumers usually use at their home are IPv4 enabled like their cameras, game consoles and TVs if in this situation service providers’ shift to IPv6 then it would not be acceptable for consumers because they never wanted to work their equipment improperly [17].

2.3.3 No Flag Date
There is no deadline indicated by which the conversion must be successful especially after the earlier changeover from Network Control Protocol (NCP) to IPv4. There is no resolution or law to decide any deadline for this transition. If it exists then it would be the core key to migrate successfully on new version [17]. Various specialists forecast that the conversion will be prolonged, possibly for measured areas, for the only projects that can have network effect have already migrated to IPv6.

2.3.4 Ubiquitous Communications
There is a rapid growth of mobile service due to the interlinked facilities from the cellular networks. Therefore, there is an increasing need for constant infrastructure and protocol that maintains mobility and can grip a wide quantity of devices. Therefore, it allows the communication from node to node with having IPv6 address it does not need any special device and no matter how the nodes are connected [19].

2.3.5 VoIP/Multimedia Services
VoIP has been making exceptional advancement from a technology acceptance viewpoint. A move from H.323 to Session Initiation Protocol (SIP) has permitted more vigorous VoIP employments with a superior level of straightforwardness and expandability. Moreover, the kind of circulation in VoIP services happening above the network is far more varied, counting data, voice, and video. The capability to access content on any kind of platform is very appealing to customers, mainly those who are extremely mobile. IPv6, with amplified address space, a great multicast space capability, and an attraction for SIP, assists as a reasonable platform for the growth of these facilities [19].
2.3.6 Social Networks
The way of interacting with your family and friend has been changed a lot from written letters, to phone calls, to e-mails, to SMS and Instant Messages (IM). Because this is the age on technology and without technology we cannot move forward. That advancement lingers these days. The aptitude to transmission photographs, conduct discussions in isolated Peer to Peer (P2P), show private info on the Internet, find compatible societies, or play collaborating sports needs an Internet that is flexible, supports ad-hoc networks, and can be protected. IPv6, with its self-configuring abilities and provision for Internet Protocol Security (IPSec) at the IP stack layer will be a unstable tool to permit this setting [19].

2.3.7 Sensor Networks
Sensor Network is a new concept in market. They can be seen in engineering apparatus, substantial machines, safety systems, and Heating, Ventilation, and Air Conditioning (HVAC) systems. This new concept is based on collecting all these techs on one platform. The usage of intensive care systems to notice poison and radiation in water systems, air percolation system, or at airdrome or transport stations around the biosphere has considerably amplified.

To deploy and manage this large number of systems there is extra need of security and protection systems as well. IPv6 offers a very established and malleable platform that supports flexibility, ad-hoc networking [20].
3. IPv6
The best feature in IPv6 is about address space. It allows us to provide services with reliability. IPv4 address is lot more complex, because it tries to do more, for example fragmentation, fragmentation is not doubt by IPv6 header. IPv6 used 128-bit addresses compared to the IPv4 where as IPv4 uses 32-bit addresses and Network Address Translation will not be necessary and it will provide easier communication. IPv6 provides unrestrained address richness. Internet protocol version 6 offers auto configuration proficiencies. They are small-scale, quicker and more controllable, particularly for more connections.

IPv6 bit in IPv6 provides more unique IP addresses for every connected device globally. Direct addressing is probable because of huge address space; the requirement for Network Address Translation (NAT) devices is successfully reduced. Addresses in IPv6 provide scalability to improve internet than addresses provided by IPv4.

IPv6 provides interoperability and flexibility which are extensively embedded in network devices. IPSEC is built into the IPv6 protocol, functional with appropriate key structure. Thus providing improved security features. [18]

3.1 Reasons of Changing IPv4
There are four important reasons based on my knowledge and researches of changing IPv4 to IPv6 are following:

1. Scarcity of IPv4 Address Space
2. Multimedia Traffic Handling
3. Mobility
4. Packet Handling

3.1.1 Scarcity of IPv4 Address Space
The IPv4 address space has $2^{32}$ addresses. But in reality a large number of such addresses are unusable for various reasons like sub-netting, oversized allocation, unplanned address roll out etc. Moreover the telecom service providers are gradually shifting from circuit switch to pure packet switched network. Big Telco’s have already deployed Next Generation Network (NGN) to support different services for communication like VoIP, Third Generation (3G), Voice and Data (VoD), Internet Protocol Television (IPTV). New technologies are coming every year and they will require number of IP addresses. IPv6 with a very large address space ($2^{128}$) is capable of catering unique address to all the present host and future for many coming years [5].

University of Venezuela has approximately 8000 connected nodes in the network which suffered from various problems due to NAT. Sluggish performance, network bottleneck and difficult scalability was nightmare for University network administrators. The university decided to expand their network and migrate to IPv6 which resulted elimination of all such problems [12].

3.1.2 Multimedia Traffic Handling
Unicast, multicast and broadcast is supported by IPv4 whereas each has limited significance in today’s age of technology. Network traffic issue is mainly caused by broadcast. IPv4 is not suitable for effectively handle the demands of future multimedia
based clients and applications. Multimedia application provides better communication services using IPv4 [5].

3.1.3 Mobility
Today’s consumer demands more mobility with their mobile devices and applications. So mobility in IPv6 supports faster handover and better communication. Mobile IP routing may have some limitation but are complex to implement and manage [5].

As we know this is the age of technology and technology is changing day by day. The main advantage of mobility is in IPv6 that the device discovers the address and of neighbours and execute configuration automatically. As in Figure 3.1 we create the link between the mobile-node and correspondent home agent, to minimize the third party addresses required on foreign network [23].

![IPv6 Mobility with Home Agent, Mobile Node and Correspondent Node](image)

*Figure 3.1: IPv6 Mobility with Home Agent, Mobile Node and Correspondent Node [29]*

Figure 3.1 shows that Correspondent Node and Mobile Node linked with Home Agent which maintains an association between the nodes of the different network through the IP addresses where as the IP Host that Maintains Network connectivity of the home agent on the foreign network.

3.1.4 Packet Handling
IPv6 has dynamic path Maximum Transmission Unit (MTU) discovery so the frames are sized by the source router according the minimum MTU of links en-route. These eliminates the need of Central Processing Unit (CPU) exhaustive fragmentation and assembly process in the intermediate routes making the packet handling fast and smooth [6].
3.2 IPv4 Header v/s IPv6 Header
IPv4 header has more fields in comparison with IPv6. The total difference between these two headers is 20 bytes it is because of the destination address in header of IPv6. Below is the headers shown for both IPv4 and IPv6 [3] [26].

![IPv4 Header Diagram](image1)

![IPv6 Header Diagram](image2)

**Figure 3.2: IPv4 and IPv6 header comparison (Courtesy Cisco Systems)**

From Figure 3.2 we can see that though some of the fields are common but IPv6 has removed some of the earlier fields like Header Length, Identification (Fragment ID), Fragmentation Flags, Fragment Offset, Header Checksum, and Options. The Payload Length field does not include the length of the standard packet header. Some new fields like Flow Label, next header have been introduced [1].

Apart from the basic header a new concept of extension header has also been introduced. Those headers are added only when extra bit of information is required. Thus reduces the overhead for normal operation.

IPv6 allows inclusion of following extension header types (in orders)
- IPv6 basic header
- Hop-by-Hop Options header
- Destination Options header (for options to be processed by more than just final recipient)
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header
- Destination Options header (for options to be processed only by final recipient) [4]
So the header structure is considerably different and thus the way an IPv6 packet is processed by layer 3 (and above) of any node is also different. Though all the new equipment like routers, switches and operating systems like Win XP (and later versions of Windows), Mac and Free Berkeley Software Distribution (BSD) are made IPv6 compatible by the vendors/developers but old systems may require software/firmware upgrade.

3.3 Challenges in IPv6 Deployment

There are many challenges you could face while migration from IPv4 to IPv6. Some challenges are presented in depth are given below:

3.3.1 Limited Availability of IPv6 Resources on Internet

The Internet services are mainly based on IPv4 and it is still running on it. But the IPv6 based servers and contents are not as widely available as IPv4 versions. Some of the big organizations have introduced service on IPv6 but as add on service. Most of the organization has very limited or no focus to introduce IPv6 based content. As IPv6 hosts can not access IPv4 content there will be very little drive to change to IPv6 by the end users until and unless reasonable volume of resources are available [5][8].

3.3.2 Unavailability of IPv6 Capable Applications

IPv6 is implemented in network layer and all the layers from and above it must be compatible with IPv6. For example there is no concept of fragmentation in IPv6 and the MTU is determined by source by using Path MTU Discovery Path Maximum Transmission Unit Discovery (PMTUD). Now if for some reason this process fails there may be a possibility of packet drop in the network. The application which initiated the communication should be capable of recognizing this failure and take necessary action. Thus the IPv6 based application should be different than IPv4. But numbers of such applications are limited as on date [9].

3.3.3 Inherent Problem in Path MTU Discovery Process

The concept of fragmentation is not present in IPv6; the source determines minimum MTU in the path that is supported. In the beginning it sends a packet with the MTU size of its own interface and with Data Frame (DF) bit set. If any transit router cannot forward the packet it drops it with an Internet Control Message Protocol (ICMP) error message to the source. The source reduces the size of the next packet and the process goes on till the source is successfully capable of sending packet to the destination. The weakness of this process is dependency on ICMP. Most of the administrator prefers to restrict ICMP messages in router for serious security reasons. In such case the ICMP error generated s part of PMTUD by the transit router will not reach the source and the process will fail [11].

3.3.4 Complexity in Mobile IPv6 Architecture

The mobile IPv6 allows users to roam from one location to other without losing its network address. This is specifically useful for mobile broadband deployment. But the architecture of the process itself has some drawbacks. The communication of mobile nodes migrating to other location is routed through a home agent (practically a router); this may result sub-optimal routing. Moreover as the home agents act as proxy for the mobile nodes when number of such nodes are large it may cause serious scalability issue and performance degradation [10].
3.3.5 Network Compatibility
It has already been described that IPv4 and IPv6 have major differences and those are not compatible. So an IPv6 node cannot transmit over native IPv4 network and vice versa. An organization even after getting IPv6 prefixes from the regional registry may become an isolate IPv6 island if its upstream ISPs core network does not support IPv6 [2].

3.3.6 Compatibility Issues in Hardware
As described earlier almost all the equipment manufacturers and application developers are making their products IPv6 compatible. Even for the older platforms software and firmware updates are released to make those IPv6 compatible. But they are not extending such fixes for end-of-life products.

Moreover some of the old routers and switches that used hardware based accelerators need complete change of the chips and thus complete replacement of such items for all practical purpose [1].

The older VoIP phones do not support IPv6 and their firmware cannot be changed also and thus requires complete replacement [1].

3.3.7 Compatibility Issue in Software
All the operating systems of Microsoft beyond Windows XP and other operating systems like Free BSD and MAC supports TCPv6/IPv6 protocol stack. So no additional application is required. But some of the organizations may still use Windows New Technology (NT) based servers. IPv6 can be implemented in such cases but it is not well scalable [1].

3.3.8 Improper IPv6 Implementation
IPv4 based networks are in place for years and network administrators take utmost care to “tune” the network to provide optimum service (like setting Quality of Service (QoS)) etc. But many of the administrators deploy IPv6 in experimental basis with default settings and values. They do not tune the network, which as a result causes poor network performance and frustrations amongst the end users. This may keep the end-users away from IPv6 [14].

3.4 Addressing the Challenges
Following are some challenges described:

3.4.1 Encouragement from Government and Statutory Bodies
Government and other statutory bodies may encourage developers and researchers of IPv6 based applications by giving awards and prizes. Special tax exemptions may be given to the software companies. Service Tax, VAT etc may be removed from IPv6 based software. These will encourage from developers to end users to adapt it [9].

3.4.2 No Experimentation on Production Network
The administrators should have separate lab set up for IPv6 before it is deployed in production network. IPv6 should be implemented and gone live after proper validation and testing. The parameters like QoS and other optimisation which are done in IPv4 network should also be done in IPv6 networks to avoid improper behaviour of network.
3.4.3 Co-existence of Both by Dual Stacking
In dual stacking both IPv4 and V6 are enabled in a single node/ network and the only one is used per case basis. For example a dual-stacked web server has both IPv4 and V6 address. It provides service to an IPv6 client by IPv6 address and legacy clients by IPv4 address. Similarly a dual stack router routes an IPv4 address based on IPv4 routing table and for IPv6 it does so based on IPv6 routing table.

Dual-stack is a good migration strategy when the existing data centre and network is planning to introduce IPv6 gradually. The enterprise may dual-stack its infrastructure and then gradually may withdraw IPv4 over time [2].

![Dual Stacking Diagram]

*Figure 3.3: Co-existence of both by dual stacking*

Figure 3.3 show that the dual-stack-node employment is a common provisional appliance where all devices and equipment like workplaces, servers and routers, etc. support both versions of Internet protocol IPv4 and IPv6. All the applications, networks and devices in any organization or workplace can interconnect using either version.

This provisional mechanism is moderately easy to device. Both versions of Internet protocols exist altogether and there is no problem for any device or application because they have both versions with them. The only drawback of this approach is that these devices, equipment and networks have to support both versions so there is need of an extra power like CPU usage etc [23].

3.5 Network Address Translation – Port Translation
Network Address Translation – Port Translation (NAT-PT) has been used widely for private to public IP translation. But the same may be used as a temporary measure to allow an IPv6 only node to communicate with all IPv4 only node [2].
Figure 3.4: NAT-PT (Courtesy Cisco Systems)

Figure 3.4 shows the translation approach, which basically translates the packets from one Internet protocol to another as shown in the above figure, IPv4 to IPv6. The benefit of this methodology is that it permits communication between all devices without bothering which version they support. The drawback of using this approach is that translator reads the header of every packet before processing and it needs extra power. Formation of the translator is tiresome. The only point of failure in this situation is translator [23].

3.6 Tunnels

Tunnels are logical paths to connect to remote IPv6 islands over an IPv4 transport network. In cases where the enterprise is IPv6 ready but its upstream service provider does not support IPv6 it becomes like an isolated region.

In such scenarios like in the diagram given in Figure 3.5 shows that tunnels can be created to connect two or more IPv6 sites over existing IPv4 transport network. The IPv6 packets before leaving the network are encapsulated inside a normal IPv4 packet. The packet is then routed as a normal IPv4 packet as the transit nodes are unaware that it has an IPv6 payload inside. At the boundary of the destination network the IPv4 headers and tailors are de-capsulated and original IPv6 packet is delivered to the intended IPv6 destination [2] [7].

Tunneling uses encapsulation to transmit IPv6 traffic in IPv4 packets and IPv4 traffic in IPv6 packets. This permits for an incomplete changeover where only some portion of any network is migrated to IPv6 while other parts remain unchanged. The benefit of using this strategy is that in situation where your old devices are not capable of dealing with IPv6
in case when they have not enough power can use the same old infrastructure or to save money cannot migrate as a whole. The drawback of tunneling is that it includes monotonous configuration. To encapsulate and expand tunneling need to have extra power on ends. Tunnels can generate routing inadequacies if they are not organized to counterpart the essential routing topology. The other disadvantage is tunnels may cause of security problems, as packets that were formerly evident are now compressed. And if want to troubleshoot any problem that it gets very difficult because of less visibility on the ends [23].

3.7 Methods by Which Such Tunnels Can Be Implemented
There are two methods by which Tunnels can be implemented are given below:

3.7.1 Static Point to Point Tunnels
This is best suited when there would be regular and considerable amount of traffic between sites. It also has the advantage of using any IPv6 capable routing protocol (e.g. Open Shortest Path First (a routing protocol) (OSPF) version-3, RIPnG) over the tunnels. The configuration is easy and straightforward where the administrators explicitly configure what source and destination IPv4 address is to be written in the encapsulating IPv4 header [2].

3.7.2 Dynamic Multipoint Tunnels
Dynamic routing protocol is best suited for sites that are expected to see infrequent IPv6 traffic. The deployment is not as simple as static point-to-point. The administrator has to properly choose the IPv6 prefixes of each site so that the existing IPv4 address is embedded (in hex representation) in IPv6 addresses. When the boundary router of the source network gets the IPv6 packet it checks the destination IPv6 address. And as the destination IPv6 addresses holds the IPv4 address of the destination (embedded as hex representation in a fixed position of the IPv6 address) the router calculates what should be the IPv4 source and destination address of the encapsulating header. And then the packet is routed as a normal IPv4 packet to the destination.

a. Automatic 6to4 tunnels
A special address class 2002::/16 are sub-netted to derive 2002:XXXX::/48 prefixes for each site. Where xxxx is the border router IP address of the specific site converted to hexadecimal. This call for a bit of planning and calculation of site prefixes before one can roll-out this method.

When the source border router receives a packet destined for 2002:XXXX::/48 prefix it quickly converts the XXXX bits to IPv4 address format to find the destination IPv4 address so that it can be encapsulation and routed as a general IPv4 packet [2].

b. Inter-site Automatic Tunneling Address Protocol
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) does not restrict the use of any reserved class inside the enterprise network. The ISATAP tunnels interface must have a routed IPv4 address (i.e. All the border and transit routers must have a route to it) and the IPv6 interface configuration is done by End-User Interface (EUI)-64 auto configuration. When the tunnel mode is configured as ISATAP the router automatically derives its own
IPv6 address as 64-bit link-local or global unicast prefix + 0000:5EFE + <IPv4 of ISATAP link>. With 0000:5EFE as the ISATAP identifier [2] [7].

c. Teredo
All the other Tunneling techniques described in this paper aims to connect between enterprise network sites. The tunnels are created and maintained between routers. But these mechanisms will not allow any home user to connect to IPv6 resources over IPv4 network. For example if a home user want to connect to IPv6 resource over his IPv4 Asymmetric Digital Subscriber Line (ADSL) or cable connections any of the described tunneling method will not help.

Teredo allows an ipv4 client to build a tunnel up to Teredo Server over User Datagram Protocol (UDP). The server supplies IPv6 address to the Teredo client and the communication can take place through that UDP tunnel by using the IPv6 address via Teredo relay [13].
Implementation of IPv6
Different scenarios have been studied for migration from IPv4 to IPv6 using the network tools, and many tests conducted which are stated below. The main purpose of conducting tests was migration from IPv4 to IPv6. Conducting tests play very important role in practical lives to identify the solutions for the problems or challenges in migration. This implementation will help the small and large organization in migration from IPv4 to IPv6. During the tests different problems have been described and presented the best solution with the results.

4.2 Different transition technologies used to conduct experiments
There are number of technologies to make the transition from IPv4 to IPv6. In this chapter different transition technologies implemented to make change from IPv4 to IPv6. Intra-Site Automatic Tunnel Addressing Protocol is used inside the private network. If you are planning to access the internet you can use the system like 6 to 4. 6 to 4 is a transition protocol designed to help the migrate to IPv6. Whereas Teredo is used when company used NAT device. The protocol relies on external servers which many ISP’s placed on the internet to help with the transition. ISATAP intended to be used in private networks only. It can not be used on the internet. To use both versions of protocol need to install ISATAP router between the newtowrks. 6 to 4 is designed as a transition protocol to help the adopting of IPv6. It is not developed for long term solution. 6 to 4 allows existing IPv4 networks to be used to tunnel IPv6 traffic. These transition technologies have been developed. These are needed because IPv6 has a different header than IPv4.

One day IPv6 will become the default protocol used on the internet but until that happens we will use IPv4 with IPv6. During migration, organization may face shrinking budgets, smaller teams and tighter deadlines, which are often, force them to cut corners. Migration does not mean simply moving data. It can always be done by doing tests and experiments using different tools and technologies. There are different network simulators available. GNS3 is one of the network simulator used to carry out for simulation for complex networks. GNS3 is an excellent tool to test the real world scenarios for migration process and it can be used on multiple operating systems like Windows, Linux, and MacOS X. I have done experiments using GNS3 where I can virtually create networks using different setting for configuration based on scenario. First of all configurations, which is the core of GNS3. We can configure GNS3 in different ways using the setting of an application. For example to check that the path to working directory is valid. Make sure to configure the path to the IOS image directory in setting. We will go to test setting to test the connection. To conduct experiment we need to creat virtual networks by dragging and dropping the routers/servers/switches using GNS3. Configurations properly need to be done to run the test. We used different commands based on each scenario to get results. Here are the some experiments conducted using GNS3.

4.2 Case 1 - IPv6 network to IPv4 Internet, 6to4
ABC Company is newly started company and have designed new network. Network consultants provided them IPv6 solution keeping in future consideration and to avoid any upgrades in near future as the technology is currently already introduced. However no ISP is providing IPv6 Internet yet and provides only IPv4 Internet connections. Now our
challenge is to allow our network with the IPv4 Internet. For configuration details and tests, see appendix A.

As both IPv6 network and IPv4 Internet is connecting to our Gateway router we can configure v6tov4 NAT translation. Our configuration will be done on Gateway router which will translate IPv6 addresses to IPv4 address.

4.3 Case 2 - IPv4 Internet to IPv6 network, 6to4
ABC Company has IPv6 network and IPv4 Internet connection. Now company wants to allow access to application server to some employees from home. So our challenge is that abc.com server should be accessible from the IPv4 Internet. For configuration details and tests, see appendix B.
As both IPv6 network and IPv4 Internet is connecting to our Gateway router we can configure v6tov4 NAT translation. Our configuration will be done on Gateway router which will translate IPv4 addresses to IPv6 address.

4.4 Case 3 - IPv6 Internet to IPv4 network, 4to6
ABC Company has a factory in remote area where no Internet service was offered before. However they were managing IPv4 network locally and server data was being sent to company owner through CDs/DVDs. Now a new ISP has started services there but offers only IPv6 Internet connection. Company wants to get connection initially on trial basis but don’t want to upgrade its network to IPv6 until they satisfied with the ISP. Now the challenge is to integrate the IPv6 Internet with their IPv4 network so abc.com server can be accessible by company owner through Internet. For configuration details and tests, see appendix C.
4.5 Case 4 - IPv6 network to IPv4 network, 6to4

ABC Company recently upgraded its head office network from IPv4 to IPv6 but didn’t upgraded Server Farm because servers are widely accessible on Internet and couldn’t be downed for upgrade during current year. Our challenge is allow Head Office users to communicate with servers located in server farm. For configuration details and tests, see appendix D.
Figure 4.5: IPv6 network to IPv4 network, 6to4

4.6 Case 5 - IPv4 network to IPv6 network, 4to6
ABC company recently upgraded its head office network from IPv4 to IPv6 but have not upgraded branch office yet and planning to upgrade in couple of month due to costing issue. Meanwhile communication Branch Office user must requires access to Head Office servers which is very critical and can’t be stopped. Our challenge is allow Head Office users to communicate with servers located at head office. For configuration details and tests, see appendix E.
4.7 Case 6 - IPv6 tunnel over IPv4 Internet, manual mode
ABC Company has upgraded its network from IPv4 to IPv6 on both sites Head Office and Branch Office. However ISP is still providing only IPv4 Internet connection and doesn’t support IPv6. Branch office must be able to communicate with Head Office server. For configuration details and tests, see appendix F.
Figure 4.7: IPv6 tunnel over IPv4 Internet, manual mode

4.8 Case 7 - IPv6 tunnel over IPv4 Internet, automatic mode
ABC Company has upgraded its network from IPv4 to IPv6 on both sites Head Office and Branch Office. However ISP is still providing only IPv4 Internet connection and doesn’t support IPv6. Branch office must be able to communicate with Head Office server. For configuration details and tests, see appendix G.
4.9 Case 8 - IPv6 network to IPv4 Internet, NAT-PT

ABC Company is newly started company and have designed new network. Network consultants provided them IPv6 solution keeping in future consideration and to avoid any upgrades in near future as the technology is currently already introduced. However no ISP is providing IPv6 Internet yet and provides only IPv4 Internet connections. Now our challenge is to allow our network with the IPv4 Internet. For configuration details and tests, see appendix H.
4.10 Case 9 - IPv4 Internet to IPv6 network, NAT-PT

ABC Company has IPv6 network and IPv4 Internet connection. Now company wants to allow access to application server to some employees from home. So our challenge is that abc.com server should be accessible from the IPv4 Internet. For configuration details and tests, see appendix I.
4.11 Case 10 - IPv4/IPv6 Dual Stack Network

ABC Company at its factory just upgraded network from IPv4 to IPv6. However now it is identified that Factory Machines do not support IPv6 which was somehow skipped by the consultant during planning. Factory machines send processing data to the Application server which is then used by other network users for reporting and other needs. At this stage company don’t want to revert back to IPv4. Our challenge is to allow both IPv4 factory machines and IPv6 network users to communicate with Application server. For configuration details and tests, see appendix J.
4.12 Case 11 - Point-to-point
ABCD organization has two sites, site 1 and site 2 which are IPv6 ready as in figure. The company does not want to have a dual stack network but inter connection between both site is essential. The service providers to which the sites are connected support only IPv4. So our challenge is to implement end-to-end IPv6 communication between site1 and site2 over IPv4 network. For configuration details and tests, see appendix K.
4.13 Case 12 - Point to Multipoint Automatic 6to4

ABCD organization has three sites site 1, site 2 and site 3 which are IPv6 ready as in figure 2. The company does not want to have a dual stack network but interconnection between both sites is essential and the traffic is in frequent. The service providers to which the sites are connected support only IPv4. So our challenge is to implement end-to-end IPv6 communication between site 1, site 2 and site 3 over IPv4 network. For configuration details and tests, see appendix L.
4.14 Case 13 - Point to Multipoint Automatic ISATAP

ABCD organization has three sites site 1, site 2 and site 3 which are IPv6 ready as in figure 4.2. The company does not want to have a dual stack network but inter connection between both sites is essential and the traffic is in frequent. The service providers to which the sites are connected support only IPv4. So our challenge is to implement end-to-end IPv6 communication between site 1, site 2 and site 3 over IPv4 network. For configuration details and tests, see appendix M.
4.15 Case 14 - IPv4 to IPv6 NAT
ABCD organization has some IP phones in their network, which does not support IPv6, and there is no way these devices can be replaced. The unified communication server of ABCD however is a native IPv6 host. And thus there is no way the IPv4 clients can communicate to this server. Our aim is to make this communication possible. For configuration details and tests, see appendix N.
4.16 Theoretical Explanation of Simulation Results

This paragraph reviews the configurations that have been done. Case #14 that is described in section 4.15 and in Appendix N, will be used as an example. In this case it is described that the communication is possible in any organization where IPv6 is not supported in the network. In order to do this experiment and test, first case is, ping from 192.168.0.1 (IPv4 device) to 2001::2 (IPv6 Server) before the NAT is implemented. The IPv4 device ping the IPv6 server, but does not get success, because the IPv4 device is not capable and compatible with IPv6 server. The ping to the virtual IP also failed because the translation is still not implemented. Second case is, ping from 192.168.0.1 (IPv4 device) to 10.0.0.1 (translated IPv4 address of IPv6 server) after NAT is implemented. The IPv4 device sent echo reply to the virtual IP of IPv6 server and the packet reaches NAT router, it finds the destination address is 10.0.0.1, so it converts the IPv4 encapsulation to the IPv6 encapsulation and add IPv6 address of the server 2001::1 in the destination address field. In this case router uses its own IPv6 address of the outgoing interface as source address (2001::1), whereas on other hand server does not recognize that the echo request is sent by an IPv4 hosts and sends echo reply to 2001::1. The NAT router now changes the encapsulation from IPv6 to IPv4, so it changes the destination address to 192.168.0.1, source address to 10.0.0.1 and forwards the packet to IPv4 device. Thus communication between an IPv4 and IPv6 end points takes place.

We will build point-to-point static GRE tunnel between two sites and IPv6 communication will take place over thins tunnel. In this case native IPv6 packets will be encapsulated inside IPv4 packet and will be travelling through the IPv4 core network until reaches the tunnel end point. The tunnel end point will de-capsulate the IPv4 packet to bring out the IPv6 packet. The core network will be unaware about this IPv6 payload and route the packet as a normal IPv4 packet.

In section 4.2 and 4.3 I build point-to-multipoint 6to4 automatic tunnel between two sites and IPv6 communication will take place over thins tunnel. In this case special prefix 2002::/16 are used to site addressing. Each site id allotted a special /48 subnet in the format
2002: first two octets of tunnel source ip for the site converted to hex format; last two octets converted to hex/48.

The site administrator may now further create /64 subnets for various interfaces.
For example tunnel source of site 3 is 3.3.3.3 (loopback 0)
So the prefix allotted to site 3 is 2002:0303:0303::/48
We have assigned the subnet 2002:0303:0303::/64 to the loopback 1 interface for testing
Similarly 2002:0101:0101::/48 and 2002:0202:0202::/48 are assigned to site 1 and site 2 respectively. It allows IPv4 networks to tunnel IPv6 traffic.

In section 4.4 and 4.5 should be configured same way as done in section 4.1 and section 4.2. Now if one IPv6 packet is to be sent to 2002:0202:0202::/48 from any other router it can quickly found the destination IPv4 address from the special IPv6 address i.e. 2.2.2.2. And native IPv6 packets will be encapsulated inside IPv4 packet with destination address 2.2.2.2 and will be travelling through the IPv4 core network until reaches the tunnel end point. The tunnel end point will de-capsulate the IPv4 packet to bring out the IPv6 packet. The core network will be unaware about this IPv6 payload and route the packet as a normal IPv4 packet.

Suppose one echo packet from site 1 is to be sent to 2012::1 i.e. site 2. From the routing table it is found that the next hop address is 2010:::5EFE:202:202 for this destination and the next hop is reachable over tunnel 0 interface. At this point the ISATAP logic triggers source router quickly converts and last 32 bits of next hop IPv6 address to dotted decimal IPv4 address format and quickly founds the destination ipv4 address i.e. 2.2.2.2. And native IPv6 packets will be encapsulated inside IPv4 packet with destination address 2.2.2.2 and will be travelling through the IPv4 core network until reaches the tunnel end point. The tunnel end point will de-capsulate the IPv4 packet to bring out the IPv6 packet. The core network will be unaware about this IPv6 payload and route the packet as a normal IPv4 packet.

In section 4.6 it allows IPv4 networks to tunnel IPv6 traffic. To do this a public IPv6 is used and theses address start with 2002:WWXX:YYZZ:SubnetID:InterfaceID. We will not establish tunnels between two sites.

In section 4.7 the same logic also holds for the return path i.e. echo-reply and thus we can successfully ping from site 1 to site 2. We establish the tunnels between two sites.

In section 4.8 similarly when ping is sent from site 1 to site 3 i.e. 2013::1 the logic encapsulates it with IPv4 destination address of 3.3.3.3 and communication then travel 6 to 4 router and enters in IPv6 Networks.

In section 4.9 and section 4.10 we will put a layer 3 device (a router or multilayer switch) between the IPv4 client and IPv6 server and use Network Address Translation in it to convert the IPv6 address to an IPv6 address and vice versa. The IPv4 client will not be aware of the IPv6 address of the destination, rather it will send the packets to the translated IPv4 address. The NAT device will receive the packet and remove the IPv4 header. The payload will then be encapsulated in IPv6 header and destination address will be set as the corresponding IPv6 address from the NAT table. The revere from IPv6 to IPv4 is analogous.

In section 4.11 Dual Stack is used to provide IPv4 connectivity with the use of IPv6. In this IPv4 interface is used for connecting to the webserver. The source automatically determines the destination IPv4 address of the packet and writes it to the destination addresses field of the encapsulating IPv4 header. Similarly when ping is sent from site 1 to site 3 i.e. 2002:0303:0303::1 the logic encapsulates it with IPv6 destination address of 3.3.3.3 and so on.
In section 4.12 I have configured a point to point tunnel between router 1 and router 2 and are able to successfully ping the IPv6 loopback address of both ends this time. Though the core network is still IPv6 incapable but now our IPv6 packets are encapsulated inside IPv4 packet. So the core network sees these echo requests as a normal IPv4 packet and routes those till the destination. Similarly it also transports the echo-reply sent from destination to source as normal IPv4 packet. At both the ends the IPv4 encapsulation is stripped off and actual IPv6 payload is brought out. For this reason we are able to successfully communicate on IPv6 over a native IPv4 core network.

In Section 4.13 Suppose one echo packet from site 1 is to be sent to 2002:0202:0202:1::1 i.e. site 2. The source router quickly converts bits 17th through 32nd to dotted decimal IPv4 address format and quickly founds the destination ipv4 address from the special ipv6 address i.e. 2.2.2.2. And native IPv6 packets will be encapsulated inside IPv4 packet with destination address 2.2.2.2 and will be travelling through the IPv4 core network until reaches the tunnel end point. The tunnel end point will de-capulate the IPv4 packet to bring out the IPv6 packet. The core network will be unaware about this IPv6 payload and route the packet as a normal IPv4 packet.

In section 4.14 We have configured point to multipoint ISATAP tunnels in all sites and repeated the ping tests. This time all the sites are able to ping each other’s IPv6 loopback address. Even the core network is IPv4 only now the source can encapsulate the IPv6 packets inside the IPv4 packet and send it over the core network which transports it as normal IPv4 packet. The logic of automatic 6to4 and ISATAP is very much similar but there is a fundamental difference. For the former we need to use a specific reserved range i.e. 2002::/16 for site addressing but for lattes there is no such restriction.

In section 4.15 The IPv4Device sent echo reply to the virtual ip of IPv6 server. It is unaware that the server only has IPv6 address. When the packet reaches NAT Router the NAT router check the destination address is 10.0.0.1. So it converts the IPv4 encapsulation to the IPv6 encapsulation and adds the IPv6 address of the server 2001::1 in the destination address field. The router uses its own IPv6 address of the outgoing interface as source address (2001::1) in this case.
5. Conclusion and Future Work
This chapter represents the proposed solutions to the problems identified and researched. It also represents the conclusion and future work.

5.1 Proposed solutions to the research questions

1. Why are we moving to IPv6 protocol and why IPv4 is going away?
The greatest reason is they were running out of IPv4 address. We were talking about running out of IPv4 address since 1995, and in 1995 Network Address Translation were introduced to our network. NAT has extended the life about IPv4 addresses. But nowadays countries like China and South America expanding their economies they are beginning to deplete all IPv4 address. IPv4 was simply not be able to satisfy the increasing domains, it also fails to meet the today's needs True network and user mobility.

2. What is beneficial about IPv6 and what are the main IPv6 Improvements?
IPv6 will be able to much larger scale of devices to connect to the Internet which is important since the number of Internet enable devices are increasing per person automatically such as smart phones and laptops. In 2015 7.1 Billion mobile devices are expected to exist. IPv6 provides QoS which means better inter operability between different Medias including Telephony, TV, Radio and Internet. IPv6 provides Plug and Play automatic configuration which will require less user and administration and it is known as stateless address and auto configuration. IPv6 will supply larger address space and stability with almost unlimited amount of addresses. IPv6 provides hierarchical network architecture for routing efficiency making network management simpler as well as provides new and enhanced features.

3. What changes do we need to do to be able to send and receive data belonging to both protocols simultaneously?
The IPv6 routing is completely independent of IPv4 routing. Host or router is equipped with both IPv4 and IPv6 protocol stacks in the operating system. Add-on to your existing applications/servers i.e. your server needs both IPv4 and IPv6 addresses configured. IPv6 addresses could be mapped to IPv4 addresses using NAT.

4. How does it work to communicate between two networks where one is using IPv4 and the other is using IPv6?
There is no common protocol between the two but could be done by install an Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) between the networks. If the computer is on the IPv4 network wants to communicate with the computer on IPv6 network, computer first communicates to the ISATAP Router using IPv4, in order for host on IPv6 network to receive the communication the router must communicate IPv6 host in IPv6. To do this router use a link local address (FE80::0:5EFE:ww.xx:yy.zz), and link local address always start with FE80 and used for local traffic only, in the host part of the address 5EFE follow by the IPv4 address, e.g.: FE80::5EFE:10.0.30.120 -> FE80::5EFE:0A00:1E78.

5. What possible transition technologies are there between IPv4 and IPv6 and how do they work?
A Tredo is a NAT traversal technology for IPv6 traffic. It encapsulates IPv6 traffic into an IPv4 UDP message containing an IPv4 and UDP message that can easily transmitted by multi-layer NAT devices. IPv6 applications work better with Tredo across NAT.

Tredo is available for Windows server 2008, Windows Vista, Windows 7 and Windows XP. We can use Tredo when we have an IPv4 NAT device.

If we have situation like for example if the company wants to use IPv6 but does not want to upgrade the IPv4 NAT device, Tredo is need to be used.

Consider this network the clients on the network connect to the IPv4 to access the Internet, the NAT device has one public IP address, in order to connect IPv6 host, clients contacts Tredo server, the Tredo server gives the client IP address to the Tredo Relay, client creates the tunnel to the Tredo Relay, all the communication between client and Tredo Relay is in IPv4 which makes the communication compatible with the NAT device. The client then can use the tunnel to send it IPv6 traffic to its destination.

6to4 tunneling technology that provides IPv6 connectivity across the IPv4 network to the Internet. 6to4 adapter encapsulates IPv6 traffic in an IPv6 header. 6to4 adapter is created when there is no ISATAP router and public IP address assigned. No NAT support so Tredo is more used than 6to4.

It is designed as a transition protocol to help the adoption of IPv6; it is not developed to a long term solution. 6to4 allows existing IPv4 networks to be used to tunnel IPv6 traffic. For example there are two IPv6 networks and we want to communicate between them, and between them we have the Internet which is this time is mostly IPv4, to communicate between these 6to4 router is used to tunnel the IPv6 protocol over the Internet to do this a public IPv6 IP address is used (2002:WWXX.YYZZ:SubnetID:InterfaceID), these addresses are all start with 2002 followed by IPv4 address that is WWXX.YYZZ followed by SubnetID and InterfaceID.

5.2 Conclusion

Internet Protocol Version 4 is now at the end-edge. Even then all the users and companies are still using IPv4 and dependent on it. Internet Protocol Version 6 is more dominant on Internet Protocol Version 4.

IPv4 are having fixed length but IPv6 headers are flexible as a new concept of extension header has been introduced. Additional headers are used along with usual headers when required. The IPv6 address space is much bigger (2^{128}) in comparison to the IPv4 address space (2^{32}). This was one of the driving forces for development of IPv6. The biggest advantage in comparison with all other advantages of IPv6 is providing the larger number of addresses. One important thing from my research is that the full implementation of IPv6 is not an easy process, it will not work in a day or two or a year, according to research it will take around 10 years period to be completely dependent on IPv6. [31]

Different approaches have been used during the configuration and test. The advantage of different approach is, In Dual Stack: Allows applications to move over a timeframe that makes local business sense. In Tunneling: Allows traversing infrastructure components to avoid out-of-cycle upgrades. In Translation: Enables communication between IPv4-only and IPv6-only endpoints. And the disadvantage is: In Dual stack: Required a pool of IPv4 addresses, and operating parallel infrastructures. In Tunneling: Increased complexity along with reduced diagnostic ability. In Translation: Applications fail, as well as complexity of synchronizing namespaces.
6to4 transition technology is used to carry IPv6 traffic to Internet when no ISPTAP router is present and a public IPv4 address is assigned. ISATAP used to carry IPv6 traffic across an IPv4 link. Tredo used to carry IPv6 traffic across NAT to the Internet. 6to4 used to carry IPv6 traffic to the Internet when no ISPTAP router is present and a public IPv4 address is assigned.

5.3 Future work
For the future work, many things are still left to fully migrate from IPv4 to IPv6. More investigation and awareness is needed and more tests should do to check the different network services at different levels along with implementation of firewall is needed and tested.

The majority of the companies will convert to the new protocol for the next 2 to 6 years but the time to start thinking about and preparing for the transition is now. This transition will be a lengthy process and will require a planning and implementation strategy. A single transition may take up to 6 months, larger companies will face more of a challenge and global companies may find that their partners in Asia are already making the switch.

This is the age of Internet and mobile technology. In future communication will take place in many devices. They will communicate through each other by Internet like Vehicles, Fridge, Ovens Cameras and etc; will be assigned with unique IP address for its physical existence. In addition various sensors connected with Internet facilitated by IPv6 address space should be installed on apartments/buildings. These are the some areas that can be researched.
REFERENCES


[3] [Online] Cisco Systems;


[5] [Online] Siddharta Saha;


Available at: http://www.incognito.com/resources/articles/five-reasons-why-you-should-upgrade-to-ipv6.pdf


[34] [Online] Bruce Sinclair – IPv6 & Networking the Internet of Things [Link]
| A. IPV6 NETWORK TO IPV4 INTERNET, 6TO4 | 2 |
| B. IPV4 INTERNET TO IPV6 NETWORK, 6TO4 | 4 |
| C. IPV6 INTERNET TO IPV4 NETWORK, 4TO6 | 7 |
| D. IPV6 NETWORK TO IPV4 NETWORK, 6TO4 | 9 |
| E. IPV4 NETWORK TO IPV6 NETWORK, 4TO6 | 12 |
| F. IPV6 TUNNEL OVER IPV4 INTERNET, MANUAL MODE | 14 |
| G. IPV6 TUNNEL OVER IPV4 INTERNET, AUTOMATIC MODE | 17 |
| H. IPV6 NETWORK TO IPV4 INTERNET, NAT-PT | 20 |
| I. IPV4 INTERNET TO IPV6 NETWORK, NAT-PT | 23 |
| J. IPV4/IPV6 DUAL STACK NETWORK | 25 |
| J. POINT-TO-POINT | 28 |
| K. POINT TO MULTIPONT AUTOMATIC 6TO4 | 30 |
| M. POINT TO MULTIPONT AUTOMATIC ISATAP | 33 |
| N. IPV4 TO IPV6 NAT | 37 |
A. IPv6 network to IPv4 Internet, 6to4

Configuration Details and Tests

Configuration on Gateway

! version 12.4
! hostname Gateway
! ipv6 unicast-routing
! interface FastEthernet0/0
  ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
ipv6 nat
! interface FastEthernet0/1
  no ip address
duplex auto
speed auto
ipv6 address 2012::1/96
ipv6 enable
ipv6 nat
! ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
! ipv6 nat v4v6 source 8.8.8.8 2011::8
ipv6 nat v6v4 source list IPv6_list pool IPv4_pool
ipv6 nat v6v4 pool IPv4_pool 1.1.1.11 1.1.1.200 prefix-length 24
ipv6 nat prefix 2011::/96
! ipv6 access-list IPv6_list
  permit ipv6 any any
!

Configuration on User1

! version 12.4
! hostname User1
! ipv6 host google.com 2011::8
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2012::11/96
!ipv6 route ::/0 2012::1
!
-----------------------------------------------------------------------
Configuration on User2
-----------------------------------------------------------------------
!
version 12.4
!
hostname User2
!
ipv6 host google.com 2011::8
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2012::12/96
!ipv6 route ::/0 2012::1
!
-----------------------------------------------------------------------
Configuration on Internet
-----------------------------------------------------------------------
!
version 12.4
!
hostname Internet
!
ip name-server 8.8.8.8
!
interface FastEthernet0/0
  ip address 1.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
  ip address 8.8.8.7 255.255.255.0
duplex auto
speed auto
!
ip dns server
!
Configuration on google.com

---

version 12.4

hostname google.com

ip host google.com 8.8.8.8

interface FastEthernet0/0
  ip address 8.8.8.8 255.255.255.0
duplex auto
  speed auto

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

ip dns server

- Ping google.com (8.8.8.8) from Gateway router
- Ping google.com (2011::8) from User1 and User2

---

B. IPv4 Internet to IPv6 network, 6to4

Configuration Details and Tests

Configuration on Gateway

---

version 12.4

hostname Gateway

ipv6 unicast-routing

interface FastEthernet0/0
  ip address 5.5.5.5 255.255.255.0
duplex auto
  speed auto
  ipv6 nat

interface FastEthernet0/1
  no ip address
duplex auto
speed auto
ipv6 address 2001::2/96
ipv6 nat

! ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!

ip access-list extended IPv4_list
   permit ip any any
!

ipv6 nat v4v6 source list IPv4_list pool IPv6_pool
ipv6 nat v4v6 pool IPv6_pool 2002::1 2002::1000 prefix-length 96
ipv6 nat v6v4 source 2001::1 5.5.5.10
ipv6 nat prefix 2002::/96
!

----------------------------------------------------------
------------
Configuration on User1
----------------------------------------------------------
!
version 12.4
!
hostname User1
!
ip name-server 5.5.5.6
!
interface FastEthernet0/0
   ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
----------------------------------------------------------
Configuration on User2
----------------------------------------------------------
!
version 12.4
!
hostname User2
!
ip name-server 5.5.5.6
!
ipv6 host google.com 2011::8
!
interface FastEthernet0/0
   ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
ipv6 address 2012::12/96
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ipv6 route ::/0 2012::1
!
-----------------------------------------------------------------------
Configuration on Internet
-----------------------------------------------------------------------
!
version 12.4
!
hostname Internet
!
ip host abc.com 5.5.5.10
!
interface FastEthernet0/0
 ip address 5.5.5.6 255.255.255.0
duplex auto
 speed auto
!
interface FastEthernet1/1
 no switchport
 ip address 1.1.1.3 255.255.255.0
!
interface FastEthernet1/2
 no switchport
 ip address 2.2.2.3 255.255.255.0
!
ip dns server
!
-----------------------------------------------------------------------
Configuration on abc.com
-----------------------------------------------------------------------
!
version 12.4
!
hostname abc.com
!
interface FastEthernet0/0
 no ip address
duplex auto
 speed auto
 ipv6 address 2001::1/96
!
ipv6 route ::/0 2001::2
!
• Ping abc.com (5.5.5.10) from User1
• Ping abc.com (5.5.5.10) from User2

C. IPv6 Internet to IPv4 network, 4to6

Configuration Details and Tests

Configuration on Gateway

version 12.4
hostname Gateway
ip host abc.com 192.168.1.1
ipv6 unicast-routing
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:3::1/64
ipv6 nat
interface FastEthernet0/1
ip address 192.168.1.2 255.255.255.0
duplex auto
speed auto
ipv6 nat
ipv6 route ::/0 2001:3::2
ipv6 nat v4v6 source 192.168.1.1 2011::8
ipv6 nat v6v4 source list IPv6_list interface FastEthernet0/1 overload
ipv6 nat prefix 2011::/96
ipv6 access-list IPv6_list
  permit ipv6 any any

Configuration on User1

version 12.4
hostname User1
ipv6 host abc.com 2011::8
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:1::11/64
!
ipv6 route ::/0 2001:1::1
!

Configuration on User2

! version 12.4
!
hostname User2
!
ipv6 host abc.com 2011::8
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:2::22/64
!
ipv6 route ::/0 2001:2::1
!

Configuration on Internet

! version 12.4
!
hostname Internet
!
ipv6 unicast-routing
ipv6 host abc.com 2011::8
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:3::2/64
!
interface FastEthernet1/1
  no switchport
  no ip address
  ipv6 address 2001:1::1/64
interface FastEthernet1/2
no switchport
no ip address
ipv6 address 2001:2::1/64
!
ipv6 route ::/0 2001:3::1
!
-----------------------------------------------------------------------
Configuration on abc.com
-----------------------------------------------------------------------
!
version 12.4
!
hostname abc.com
!
ip host abc.com 192.168.1.1
!
interface FastEthernet0/0
  ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
• Ping abc.com (2011::8) from User1
• Ping abc.com (2011::8) from User2

**D. IPv6 network to IPv4 network, 6to4**

Configuration Details and Tests

-----------------------------------------------------------------------
Configuration on Gateway
-----------------------------------------------------------------------
!
version 12.4
!
hostname Gateway
!
ip host abc.com 192.168.1.1
!
ipv6 unicast-routing
!
interface FastEthernet0/0
  ip address 192.168.2.2 255.255.255.0
duplex auto
speed auto
ipv6 nat
interface FastEthernet0/1
  no ip address
duplex auto
  speed auto
ipv6 address 2001::1/64
ipv6 nat
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ipv6 nat v4v6 source 192.168.1.1 2011::8
ipv6 nat v6v4 source list IPv6_list interface FastEthernet0/0 overload
ipv6 nat prefix 2011::/96
!
ipv6 access-list IPv6_list
  permit ipv6 any any

Configuration on User1

! version 12.4
! hostname User1
! ipv6 host abc.com 2011::8
! interface FastEthernet0/0
  no ip address
duplex auto
  speed auto
ipv6 address 2001::11/64
!
ipv6 route ::/0 2001::1

Configuration on User2

! version 12.4
! hostname User2
! ipv6 host abc.com 2011::8
! interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001::12/64
!
ipv6 route ::/0 2001::1
!

-----------------------------------------------------------------------
Configuration on Router
-----------------------------------------------------------------------
!
version 12.4
!
hostname Router
!
ip host abc.com 192.168.1.1
!
interface FastEthernet0/0
  ip address 192.168.2.1 255.255.255.0
duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 192.168.1.2 255.255.255.0
duplex auto
  speed auto
!

-----------------------------------------------------------------------
Configuration on abc.com
-----------------------------------------------------------------------
!
version 12.4
!
hostname abc.com
!
ip host abc.com 192.168.1.1
!
interface FastEthernet0/0
  ip address 192.168.1.1 255.255.255.0
duplex auto
  speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
• Ping abc.com (192.168.1.1) from Gateway router
• Ping abc.com (2011::8) from User1 and User2
E. IPv4 network to IPv6 network, 4to6

Configuration Details and Tests

Configuration on Gateway

```
! version 12.4
!
hostname Gateway
!
ip host abc.com 192.168.5.5
!
interface FastEthernet0/0
  ip address 192.168.5.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
  ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
```

Configuration on User1

```
!
version 12.4
!
hostname User1
!
ip host abc.com 192.168.5.5
!
interface FastEthernet0/0
  ip address 192.168.1.11 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
```

Configuration on User2

```
!
version 12.4
```
hostname User2

ip host abc.com 192.168.5.5

interface FastEthernet0/0
ip address 192.168.1.12 255.255.255.0
duplex auto
speed auto

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

-----------------------------------------------
Configuration on Router
-----------------------------------------------
!
version 12.4
!
hostname Router
!
ipv6 unicast-routing
ipv6 host abc.com 2001:1::1
!
interface FastEthernet0/0
ip address 192.168.5.1 255.255.255.0
duplex auto
speed auto
ipv6 nat
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address 2001:1::2/64
ipv6 nat
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

!
!
ip access-list extended IPv4_list
  permit ip any any
!
ipv6 nat v4v6 source list IPv4_list pool IPv6_pool
ipv6 nat v4v6 pool IPv6_pool 2002::1 2002::1000 prefix-length 96
ipv6 nat v6v4 source 2001:1::1 192.168.5.5
ipv6 nat prefix 2002::/96

-----------------------------------------------
Configuration on abc.com

version 12.4
hostname abc.com
ipv6 host abc.com 2001:1::1
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:1::1/64
ipv6 route ::/0 2001:1::2

• Ping abc.com (192.168.5.5) from Gateway router
• Ping abc.com (192.168.5.5) from User1 and User2

F. IPv6 tunnel over IPv4 Internet, manual mode

Configuration Details and Tests

Configurations on BO_Gateway

version 12.4
hostname BO_Gateway
ipv6 unicast-routing
ipv6 host abc.com 2001:1::1
interface Tunnel1
  no ip address
  ipv6 address 2001:102::2/64
tunnel source FastEthernet0/1
tunnel destination 1.1.1.1
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:2::1/64
!
interface FastEthernet0/1
  ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!
ipv6 route ::/0 2001:102::1
!
-----------------------------------------------------------------------
Configuration on User1
-----------------------------------------------------------------------
!
version 12.4
!
hostname User1
!
ipv6 host abc.com 2001:1::1
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:2::11/64
!
ipv6 route ::/0 2001:2::1
!
-----------------------------------------------------------------------
Configuration on User2
-----------------------------------------------------------------------
!
version 12.4
!
hostname User2
!
ipv6 host abc.com 2001:1::1
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:2::12/64
!
ipv6 route ::/0 2001:2::1
!
Configuration on HO_Gateway

! version 12.4
! hostname HO_Gateway
!
ipv6 unicast-routing
ipv6 host abc.com 2001:1::1
!
interface Tunnel1
 no ip address
 ipv6 address 2001:102::1/64
tunnel source FastEthernet0/0
tunnel destination 2.2.2.2
!
interface FastEthernet0/0
 ip address 1.1.1.1 255.255.255.0
duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
duplex auto
 speed auto
 ipv6 address 2001:1::2/64
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ipv6 route ::/0 2001:102::2
!

Configuration on abc.com

! version 12.4
! hostname abc.com
!
ipv6 host abc.com 2001:1::1
!
interface FastEthernet0/0
 no ip address
duplex auto
 speed auto
 ipv6 address 2001:1::1/64
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ipv6 route ::/0 2001:102::2
Configuration on IPv4_Internet

version 12.4
hostname IPv4_Internet
interface FastEthernet0/0
  ip address 1.1.1.3 255.255.255.0
duplex auto
  speed auto
interface FastEthernet0/1
  ip address 2.2.2.3 255.255.255.0
duplex auto
  speed auto

• Ping abc.com (2001:1::1) from Gateway router
• Ping abc.com (2001:1::1) from User1 and User2

G. IPv6 tunnel over IPv4 Internet, automatic mode

Configuration Details and Tests

Configuration on BO_Gateway

version 12.4
hostname BO_Gateway
ipv6 unicast-routing
ipv6 host abc.com 2001:1::1
interface Tunnel1
  no ip address
  no ip redirects
tunnel source FastEthernet0/1
tunnel mode ipv6ip auto-tunnel
interface FastEthernet0/0
  no ip address
duplex auto
  speed auto
ipv6 address 2001:2::1/64
!
interface FastEthernet0/1
ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!
ipv6 route ::/0 ::1.1.1.1
!
-----------------------------------------------------------------------
Configuration on User1

-----------------------------------------------------------------------
!
version 12.4
!
hostname User1
!
ipv6 host abc.com 2001:1::1
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:2::11/64
!
ipv6 route ::/0 2001:2::1
!
-----------------------------------------------------------------------
Configuration on User2

-----------------------------------------------------------------------
!
!
version 12.4
!
hostname User2
!
ipv6 host abc.com 2001:1::1
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2001:2::12/64
!
ipv6 route ::/0 2001:2::1
!
Configuration on HO_Gateway

! version 12.4
! hostname HO_Gateway
! ipv6 unicast-routing
ipv6 host abc.com 2001:1::1
!
interface Tunnel1
 no ip address
 no ip redirects
 tunnel source FastEthernet0/0
 tunnel mode ipv6ip auto-tunnel
!
interface FastEthernet0/0
 ip address 1.1.1.1 255.255.255.0
duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
duplex auto
 speed auto
 ipv6 address 2001:1::2/64
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ipv6 route ::/0 ::2.2.2.2
!

Configuration on abc.com

! version 12.4
!
hostname abc.com
!
ipv6 host abc.com 2001:1::1
!
interface FastEthernet0/0
 no ip address
duplex auto
 speed auto
 ipv6 address 2001:1::1/64
!
ipv6 route ::/0 2001:1::2
!

Configuration on IPv4_Internet

! version 12.4
! hostname IPv4_Internet
! interface FastEthernet0/0
ip address 1.1.1.3 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 2.2.2.3 255.255.255.0
duplex auto
speed auto
!

• Ping abc.com (2001:1::1) from HO_Gateway router
• Ping abc.com (2001:1::1) from User1 and User2

H. IPv6 network to IPv4 Internet, NAT-PT

Configuration Details and Tests:

Configuration on Gateway

! version 12.4
! hostname Gateway
! ip name-server 8.8.8.8
! ipv6 unicast-routing
!
interface FastEthernet0/0
ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
ipv6 nat
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address 2012::1/96
ipv6 enable
ipv6 nat
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip dns server
!
ipv6 nat v4v6 source 8.8.8.8 2011::8
ipv6 nat v6v4 source list IPv6_list interface FastEthernet0/0 overload
ipv6 nat prefix 2011::/96 v4-mapped IPv6_list
!
ipv6 access-list IPv6_list
  permit ipv6 any any
!
-----------------------------------------------------------------------
Configuration on User1
-----------------------------------------------------------------------
!
version 12.4
!
hostname User1
!
ipv6 host google.com 2011::8
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2012::11/96
!
ipv6 route ::/0 2012::1
!
-----------------------------------------------------------------------
Configuration on User2
-----------------------------------------------------------------------
!
version 12.4
!
hostname User2
!
ipv6 host google.com 2011::8
!
interface FastEthernet0/0
  no ip address
duplex auto
speed auto
ipv6 address 2012::12/96
!
ipv6 route ::/0 2012::1
!
-----------------------------------------------------------------------
Configuration on Internet
-----------------------------------------------------------------------
!
version 12.4
!
hostname Internet
!
ip name-server 8.8.8.8
!
interface FastEthernet0/0
  ip address 1.1.1.2 255.255.255.0
duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 8.8.8.7 255.255.255.0
duplex auto
  speed auto
!
ip dns server
!
-----------------------------------------------------------------------
Configuration on google.com
-----------------------------------------------------------------------
!
version 12.4
!
hostname google.com
!
ip domain name google.com
ip host google.com 8.8.8.8
!
interface FastEthernet0/0
  ip address 8.8.8.8 255.255.255.0
duplex auto
  speed auto
!
ip route 0.0.0.0 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip dns server
!
• Ping google.com (8.8.8.8) from Gateway router
• Ping google.com (2011::8) from User1 and User2

I. IPv4 Internet to IPv6 network, NAT-PT

Configuration Details and Tests

Configuration on Gateway

```
! version 12.4
! hostname Gateway
! ipv6 unicast-routing
! interface FastEthernet0/0
  ip address 5.5.5.5 255.255.255.0
duplex auto
speed auto
ipv6 nat
!
interface FastEthernet0/1
  no ip address
duplex auto
speed auto
ipv6 address 2001::2/96
ipv6 nat
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip access-list extended IPv4_list
  permit ip any any
!
ipv6 nat v4v6 source list IPv4_list pool IPv6_pool
ipv6 nat v4v6 pool IPv6_pool 2002::1 2002::1000 prefix-length 96
ipv6 nat v6v4 source 2001::1 5.5.5.10
ipv6 nat prefix 2002::/96
!
```

Configuration on User1

```
! version 12.4
! hostname User1
!```
ip name-server 5.5.5.6
!
interface FastEthernet0/0
 ip address 1.1.1.1 255.255.255.0
duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
-----------------------------------------------------------------------
Configuration on User2
-----------------------------------------------------------------------
!
version 12.4
!
hostname User2
!
ip name-server 5.5.5.6
!
ipv6 host google.com 2011::8
!
interface FastEthernet0/0
 ip address 2.2.2.2 255.255.255.0
duplex auto
 speed auto
 ipv6 address 2012::12/96
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ipv6 route ::/0 2012::1
!
-----------------------------------------------------------------------
Configuration on Internet
-----------------------------------------------------------------------
!
version 12.4
!
hostname Internet
!
ip host abc.com 5.5.5.10
!
interface FastEthernet0/0
 ip address 5.5.5.6 255.255.255.0
duplex auto
 speed auto
!
interface FastEthernet1/1
 no switchport
ip address 1.1.1.3 255.255.255.0
!
interface FastEthernet1/2
  no switchport
  ip address 2.2.2.3 255.255.255.0
!
ip dns server
!
-----------------------------------------------------------------------
Configuration on abc.com
-----------------------------------------------------------------------
!
version 12.4
!
hostname abc.com
!
interface FastEthernet0/0
  no ip address
duplex auto
  speed auto
  ipv6 address 2001::1/96
!
ipv6 route ::/0 2001::2
!

  Ping abc.com (5.5.5.10) from User1
  Ping abc.com (5.5.5.10) from User2

J. IPv4/IPv6 Dual Stack Network

Configuration Details and Test
-----------------------------------------------------------------------
Configuration on DualStack router
-----------------------------------------------------------------------
!
version 12.4
!
hostname DualStack
!
ipv6 unicast-routing
!
interface FastEthernet1/0
  no switchport
  ip address 1.1.1.2 255.255.255.0
  ipv6 address 2001:1::2/64
!
interface FastEthernet1/1
  no switchport
no ip address
ipv6 address 2001:2::1/64
!
interface FastEthernet1/2
no switchport
ip address 2.2.2.1 255.255.255.0
!
ip route 3.3.3.0 255.255.255.0 FastEthernet1/2
!
ipv6 route ::/0 2001:2::2
!
-----------------------------------------------------------------------
Configuration on Application server
-----------------------------------------------------------------------
!
version 12.4
!
hostname Application
!
interface FastEthernet0/0
ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
ipv6 address 2001:1::1/64
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ipv6 route ::/0 2001:1::2
!
-----------------------------------------------------------------------
Configuration on R1 router
-----------------------------------------------------------------------
!
version 12.4
!
hostname R1
!
ipv6 unicast-routing
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:3::1/64
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address 2001:2::2/64
!
ipv6 route ::/0 2001:2::1
!

-----------------------------------------------------------------------

Configuration on User
-----------------------------------------------------------------------

!
version 12.4
!
hostname User
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:3::2/64
!
ipv6 route ::/0 2001:3::1
!

-----------------------------------------------------------------------

Configuration on R2 router
-----------------------------------------------------------------------

!
version 12.4
!
hostname R2
!
interface FastEthernet0/0
ip address 3.3.3.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!

-----------------------------------------------------------------------

Configuration on Factory_Machine
-----------------------------------------------------------------------

!
version 12.4
!
hostname Factory_Machine

interface FastEthernet0/0
  ip address 3.3.3.2 255.255.255.0
duplex auto
speed auto

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

• Ping Application server (2001:1::1) from User
• Ping Application server (1.1.1.1) from Factory_Machine

K. Point-to-point:

Configuration and Testing
L. Point to Multipoint Automatic 6to4

Configuration and Testing
Dynamips(1): Router1, Console port

site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#
site1#

site1#ping 2002:1002:0:0:0:1:1:1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:1002:0:0:1:1:1, timeout is 2 seconds:

....
Success rate is 0 percent (0/5)

site1#
site1#

site1#ping 2002:1003:1:1:1:1:1:1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:1003:1:1:1:1:1, timeout is 2 seconds:

....
Success rate is 0 percent (0/5)

site1#
site1#

Dynamips(2): Router1, Console port

site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#
site2#


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:1001:1:1:1:1, timeout is 2 seconds:

....
Success rate is 0 percent (0/5)

site2#
site2#


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:1001:1:1:1:1, timeout is 2 seconds:

....
Success rate is 0 percent (0/5)

site2#
site2#
site1# ping 2002:0202:0202:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:0202:0202:1::1, timeout is 2 seconds:

!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/159/232 ms

site1# ping 2002:0202:0202:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:0202:0202:1::1, timeout is 2 seconds:

!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 112/147/180 ms

site1#
M. Point to Multipoint Automatic ISATAP
Type escape sequence to abort.
Reading 5, 100-byte ICMP Echo to 2019::1, timeout is 2 seconds:
......
Success rate is 0 percent [0/5]

Type escape sequence to abort.
Reading 5, 100-byte ICMP Echo to 2018::1, timeout is 2 seconds:
......
Success rate is 0 percent [0/5]

Type escape sequence to abort.
Reading 5, 100-byte ICMP Echo to 2018::1, timeout is 2 seconds:
......
Success rate is 0 percent [0/5]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2011:1, timeout is 6 seconds:

Success rate is 0 percent (0/5)

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2012:1, timeout is 6 seconds:

Success rate is 0 percent (0/5)
N. IPv4 to IPv6 NAT

Configuration and Testing
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:

Packet loss is 0 percent (0/5), round-trip min/avg/max = 16/40/72 ms