College of Natural & Computational Sciences

School of Information Science

IPV6 Migration Framework for EthioTelecom.

By

NAHOM GIZACHEW

March 2019

Addis Ababa, Ethiopia

College of Natural & Computational Sciences

School of Information Science

IPV6 Migration Framework for EthioTelecom.

By

NAHOM GIZACHEW

Advisor: Workshet Lamenew (Ph.D)

March 2019

Addis Ababa, Ethiopia

College of Natural & Computational Sciences

School of Information Science

IPV6 Migration Framework for EthioTelecom

By: NAHOM GIZACHEW

Name and signature of Members of the Examining Board

Workshet Lamenew (Ph.D) Advisor	_____ Signature	_____ Date
Dereje Teferi (Ph.D) Examiner	_____ Signature	_____ Date
Wondwossen Mulugeta (Ph.D) Examiner	_____ Signature	_____ Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

I declare that the thesis is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature: _____

Nahom Gizachew Teka

This thesis has been submitted for examination with my approval as university advisor.

Advisor's Signature: _____

Workshet Lamenew (Ph.D)

Dedication

I dedicate this thesis to my family: You are everything I am today, I owe it all to you. I would like to thank you for all you have done for me.

Acknowledgments

I would like to start by thanking God for letting me have the strength when I needed one and paving the way to the finish.

My sister, who has always been by my side in the good and bad moments, helping me in whatever she can, I would like to give her my utmostacknowledgment. Also my advisor Dr. Workshet, who have been helpful and very patient with me through all the process, this would have never happened without him.

I would also like to pass my thanks to my family who has given me the moral and guidance to when I was doing this research.

Also, I am very grateful for all my friends who were there for me in providing necessary technical knowledge and information necessary sparing their valuable time.

I also would like to express my best gratitude to all that helped me while I was doing this paper and helping me with whatever you can.

Finally, I want to pass my deep heartfelt thanks to all members of AAU information science department instructors for their patience, helpful information care, and support during my study.

Thanks all for your encouragement and help!

Abstract

The internet is growing and advancing, and it's not slowing down. This growth requires a stable backbone to have a seamless communication. To support this ever-growing demand for internet and ubiquity of communication and the depletion of the current IP version IPv6 was born. IETF developed this new version of IP to resolve some issues of IPv4 like scalability, performance, and reliability.

Even though IPV6 was developed a while ago, its application was late mainly because of NAT and other services that let IPV4 continue in the current Internet. But now the new Internet is getting born, for instance Internet of Things (IoT) and other advanced technologies need a more efficient way of communicating so it will not be long before IPV6 takes over. To this end, attempts have begun to transit from IPV4 to IPV6.

However, time and different networks structure, usage and the deep integration of IPV4 makes it hard to automatically transition to IPV6, it may take time and resource to make full transit from IPV4 to IPV6 as the two protocols are not compatible. Even though attempts are done in IPV6 migration, scholars observed that the transition needs a framework that will help in migrating IPV4 to IPV6 with a minimum complication while allowing a room for both to exist until IPV4 network fully transit.

The current ISP in Ethiopia, Ethio Telecom, has an IPV4 only core network. So this research is an attempt to propose a framework that would enable the core network of the ISP to avail and be able to handle IPV6 enabled services. The research follows design science as a methodology, because design science allows as to come up with an artifact and evaluate this artifact in real world situation and to collect data questionnaire was selected. Configurations and designing logical networks are done to demonstrate the framework in a real scenario. GNS3 and NS3 are used to simulate and collect appropriate data. The routing and other configuration done were also be used to evaluate how the new framework is in regards to performance. After evaluating by simulating the framework, the research has found that the framework can be

implemented and also the performance in the services which were selected for the test run smoothly.

The framework which is proposed in this thesis is very important for providing a stepping stone for the migration process of IPV4 based networks and ISP's. Transitioning the core of a major ISP very hard, it needs time and consderation on all sides because of the outcomes could be devastating if not dealt with care. So this thesis proposes a framework that could reduce the complexity and pave the path for transitioning to IPV6.

Keywords: ISP, Internet, IPv6, IPv4, Framework

Contents

Table of Figures

Content of Tables

List of Acronym

Acronym	Definition
AAAA	Authentication, Authorization, and Accounting
ACM	Association for Computing Machinery
ADSL	Asymmetric digital subscriber line
ALG	Application-level gateway
API	Application Programing interface
ARP	Address Resolution Protocol
BIA	Business Impact Analysis
BIS	Business Information System
CAIDA	Center for Applied Internet Data Analysis
CPE	Customer-premises equipment
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain name server
DOD	Department of Defense
DSM	Dynamic spectrum management
DSRM	Directory Services Restore Mode
FTP	File transfer protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICT	Information Communication technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior gateway protocol
IP	Internet protocol
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISP	Internet service provider
LAN	Local Area network

LLC	Logical link control
MIB	Management information base
MPLS	Multiprotocol Label Switching
NAT	Network address translation
NOC	Network operations center
OSPF	Open shortest path first
RFC	Request for Comments
RIP	Routing Information Protocol
SIIT	Stateless IP/ICMP Translation
SNMP	Simple Network Management Protocol
TCP	Transport control protocol
UDP	User datagram protocol
WAN	Wide area network
WSN	Wireless sensor network

Chapter One

1.1. Introduction

As a communication protocol, IP provides an identification and location system for computers both on the Internet and local network. Internet Protocol version 4 (IPv4) has been used successfully for the past years. Currently, IPv4 still routes most Internet traffic. However, due to the predictable exhaustion of IPv4 addresses, the transition to IPv6 is imperative, because IPv6 can provide a larger available address space and embedded security [1] [2].

IPv6, the new protocol for the internet commonly known as, Internet 2,is relatively a new concept for the world when it was introduced to people when networks started running out of the currently being used IPv4. With admirable foresight, the Internet Engineering Task Force (IETF) initiated the concept, design, and development of a suite of protocols and standards now known as Internet Protocol Version 6 (IPv6) in early 1994 as a worthy tool to phase out and supplant IPv4 over the coming years [3].

The IPv6 proposed standard was published in December 1998, but it certainly takes a long period of time to implement and test a standard. Until it's finally shipped in products it can pass several years. In the case of IPv6, it was also necessary to deploy pilot networks to test it in real environments. Operators needed time as well to learn how to work with the new technology. All in all, it's fair to say that the decade that followed the publishing of RFC 2460 ("Internet Protocol, Version 6 (IPv6)"), was a period of time for experimenting, testing, and learning [4]

IPv6 has both abundant address resources and steady communication performance by providing better IP header format using the base OSI model, so it becomes the ideal solution for the point-to-point communication between Wireless sensor networks (WSN) and the Internet. The new protocol aims to effectively support the ever-expanding Internet usage functionality, and also address security concerns [5].

IPv6 uses a128-bit address size compared with the 32-bit system used in IPv4 and will allow for as many as $3.4x10^{38}$ possible addresses, enough to cover every inhabitant on planet earth several times over. The 128-bit system also provides for multiple levels of hierarchy and flexibility in hierarchical addressing and routing, a feature that IPv4-based Internet lacked [6].

The reasons that led the Internet community to seek the development of the new version of the IP address is listed below [2]:

- Lack of addresses.
- Performance-manageability
- Security, and
- Automatic address assignment

Having a large number of address space is not enough now, the current technologies and the way they are moving force us to have more features, like Security and speed with maximum agility. An address that could fit anywhere with less modification and more adaptive behavior is what the world is moving for; thus IPV6. IPV6 brings the ability to manage quality of a network also allows for a better flexibility when it comes to QoS while doing this IPV6 also provides an in built security using IPSec as its back bone. IPV6 address assignment also brings in a new concept which tries to minimize the time and resource used while assigning an address to a node in a network. IPV6 has a concept that a node could get its IP from a close by network device which is using IPV6 [7].

So if the world is moving in this direction what happens to the old network, it can't be stripped down and converted to the new network overnight? It needs a way to overcome the challenges that will arise from trying to convert to the new space.

These challenges become even more complex when on an Internet Service Provider (ISP) level. ISP has many types of connection for account less number of service they provide on top of that they connect residence, companies and mobiles users. These services now are not limited to data connection only because now using internet you can do many things, so ISP's also thought about Quality of Service (QoS) is another challenge to consider.

ISP are the backbone of a countries development. They help in connecting the country to the world. Financial centers, Educational Institutes, NGO's, and much more depend on the ISP which is giving the service. Now consider the above factors and having to do all these with one ISP this makes things even more complicated.

ISPs that are one for their country have to deal with the above factor, and Ethio telecom is no different. Ethio telecom is an ISP in Ethiopia that connects and handles ISP related communications. In doing so it utilizes IPV4 primarily for doing its major tasks.

This research focus on Ethio Telecom's challenges and the solution towards moving to the new protocol IPV6 and finding or suggesting a possible solution to the challenges found or discovered. It also tries to assess the level of IPV6 usage in the existing network and how deep has it been used. Currently, most Ethio telecom services are running using IPV4.

A brief recap of the major events in the development of the new protocol is given below:

Basic protocol (RFC 2460) published in 1998

	Basic socket API (RFC 2553) and DHCPv6 (RFC 3315) published in 2003.
	Mobile IPv6 (RFC 3775) published in 2004
	Flow label specifications (RFC 3697) added 2004
	Address architecture (RFC 4291) stable, minor revision in 2006
	Node requirements (RFC 4294) published 2006

Table 1 IPV6 History [8]

The private and public addressing in the IPV4 world has now been replaced with the fact that we have abundant addresses we can allocate to everyone. There is no need to say this is a private and this is a public address. It is known that IPv4 has classes and each class has its own public and private address except for the class D and E, which are reserved for another purpose. Similar to IPV4, IPV6 has somewhat class like division which is used for Subnetting purpose and reservation for specific uses of the IP schema. Anycast addressing, Link-local addressing Multicast addressing are examples. This study also discusses briefly on how IPv6 is formatted, how it is allocated in different forms of the addressing schema.

So how do we manage IPV6 and how is the allocation set? IANA (Internet Assigned Number Authority) is responsible for doing the allocation and assignment how each block of the IPV6 address will be used and for what purpose. Keep in mind that since there is no broadcasting in

IPV6 which leads to there is no broadcast address and everyone has one unique IP address which in turn put that everyone is connected to IP addresses need to be carefully allocated. To add to the fact that IPV6 is a better protocol it also has security embedded in it.

For more information refer to Annex 1 as a guide for the current IPV4 and IPV6 addressing layout of the world. This will put perspective of how IPV6 is much more superior to IPV4 and why the need to transit is required and inevitable.

1.2. Background to the research

This research is a step to identify the challenges that arise when an ISP decides to shift from one addressing protocol to the other (IPV4 to IPV6). After identifying these challenges the research will also try to propose a framework that could be used to minimize the effect of the challenges.

IPV4 being the most widely used addressing technology currently and IPV6 not being backward compatible creates a space where organizations have to decide when and how to move from IPV4. Given the current shortcomings of IPV4 not to transition or at least implement coexistence might be a hard choice. Having said that it's not easy just to up and convert to the new protocol, there multiple factors to be considered starting from the simplest to the complex issues that might arise due to transition.

These factors are even magnified in the case of ISP's. The case of Ethio Telecom is not that different from other ISP's. ISP's by their nature are setup to provide service, in doing so they have to make sure the consistency of the service that they provide is reliable. So approaches to change and transition needs to be carefully laid out and planned in advance. And when it comes to new areas like IPV6 all sides need to be check before fully converting.

Many transition works has been done internationally and there are some local works as well, showing the many aspects of IPV6 and why we need to transition. They also have tried to point out the tools and ways of transitioning, to minimize the complication that may occur during this time. Coming to local works, very little has been done in regards to IPV6 to a point only one can be found documented. It was done by Banchalem Admassu, where she tried to show the use of 6PE in transition an IPV4 edge router in Ethio Telecom network. The research which was done by Banchalem was restricted to the edge of a network while not considering the core and the customer side of the network [9].

The researches which were done on IPV6 and how to transition to it is very little in regards to Ethio telecom, and this opens up a room for hesitation and uncertainties. So to reduce these uncertainties this research tries fill the gap by showing the challenges that may arise and the solution to overcome them by providing a framework.

One other thing to consider is the level of transition, is how deep the transition will go to before allowing the coexistence. Ethio telecom have different gateways, different service types, and infrastructure setup. Knowing where to do the transition or coexistence on the specific location and which technology to use is very important.

The other factor that needs to be considered is that Ethio Telecom don't stand alone since it's a service-oriented organization it will need to communicate with the world, so this need should be considered as well. Internal network and also the External networks that Ethio telecom will have to route while providing services.

1.3. Statement of the Problem

The world is moving fast, always growing and struggling to find new ways to improve and mature the current ICT based technologies. IPv6 is one of its fruits, although it has been there for a while it has not been utilized as it should have been. But recent developments in the Internet and the new technologies has forced the world to consider IPV6.

IPv4 has served us well for the last 35 years. But in a world of already exhausted address space, its future seems uncertain. IPV4 tried to survive using different methods to extend its lifetime by utilizing NAT, double NAT and other methods, but everyone knew it wouldn't last forever. However, most ISPs didn't start deploying IPv6 networks actively until the address pool got almost depleted [10].

Using address translation methods comes with their own problems; latency, high requirement for resource, and also there are services that could not be used in a NAT environment. Due to the mentioned factors IPV6 is the ideal solution which was proposed by IETF. But while transitioning to IPV6 there are factors to consider:

- Is current network prepared for the move?

    - IPV4 was running for a long time, most network where following the best practice to deploy IPV4 and the services that utilized it. So is the current network layout or configuration ready for the transition, keep in mind IPV6 is not backward compatible.
- What devices are there and how do they support the new protocol?
    - Devices which are running in the current network as well as devices which connect to the network need to be considered as well. Does they support IPV6?
- What benefits do we expect from the new protocol?
    - Changing or moving to IPV6 is a major decision that needs to be taken, in doing so the benefits that IPV6 provides need to be put forth clearly.

1.4. Research questions

1. What are the challenges in moving from IPV4 to IPV6 in regards to Ethio Telecom?
2. What would be the most suitable transition method that can be adapted by Ethio Telecom?
3. Can a framework be designed and implemented for the transition purpose?

1.5. Objectives

1.5.1. General Objective

The objective of the research is to create IPV6 migration framework to meet the challenges in moving from IPV4 to IPV6 in the context of an ISP Ethio Telecom.

1.5.2. Specific Objective

The specific objectives of this research include

- ✓ Review relevant literature to understand the options for IPV6 migration
- ✓ Understand current IPv6 transition methods in the context of Ethio Telecom.
- ✓ Investigate the IPV6 migration practices and identify the challenges of IPV6 migration for Ethio Telecom.
- ✓ Propose a framework for the technical aspect of how to meet the challenges of moving to IPV6.
- ✓ Evaluate the framework.

1.6. The significance of the study

In a world that has a vibrant IT environment which resulted in the adoption of IPv6, a way of understanding the underlying and practical implications of the current IPv4 technologies, platform and usage are necessary. This study will make both practical and academic contributions to the domain area by attempting to highlight the factors associated with IPv6 migration. It will aid multinational organizations and ISPs focus on what issues must be dealt with before complete migration to the relatively newer IPv6 technologies. Furthermore, this research will improve and give a stepping stone for future researchers when handling IPV6 within certain organizational contexts. IPV4 is the current protocol and it still is in use for some ISPs, but migration to IPv6 is inevitable due to the vigorous world of IT. Even though there are ways we can use both versions at the same time, at the expense of speed and stability, the fact remains IPv4 will soon be obsolete. Thus this study can be of use to any IT organization interested in operating in a stable IT platform by studying the challenges that hamper the successful migration of IPv4 to IPv6.

1.7. The scope of the study

The scope of this research is limited to designing a framework for a technical side that could be utilized for starting an IPV6 address migration process and helps to see the different challenges while having a way to address them. The technical part which this research is concerned of is the routing and tunneling part of the network where external contact happens. This could be contacts from other ISP, Clients or third party networks. The scope also covers the framework designing and evaluation. AS mentioned in the topic the context of the research is on Ethiopia's IPS which is Ethio telecom.

The paper will be answering the research stated above based on the three views, these views are:

1. Clients or Customers of Ethio Telecom
2. Other ISPs that Etho Telecom uses
3. The internal network of Ethio Telecom

1.8. Ethical Concerns

The data collected from the users and the ISP will only serve the academic interests of the student and will maintain confidentiality and anonymity of the responders. Privacy and legal matters of the study will be respected and applied by the researcher. The researcher will make sure to use a recommendation letter from the Addis Ababa University written, in regards to the research, to the ISP and Selected end Users. All works of other authors used for the purposes of this study will be properly cited and referenced in the final section of the study.

1.9. Structure of the Thesis

This research is organized as follows.

Chapter 1: Includes Introduction which gives a highlight on the different version protocols it uses, Statement of the problem, objectives, significance and scope of the study.

Chapter 2: This chapter is about the different literatures from different sources that helps is finding the gaps as well as supports the paper. It also put forth the different terminologies, current trends and what other have done.

Chapter 3: This chapter covers the methodology used in the research. Which methodology was selected and the sampling technique, data collection instruments, procedures etc. Design science has been selected as the methodology to be used for this specific research.

Chapter 4: is all about the current Ethio Teleocm network, how it is setup. It also show the different layers of connection the network has like Aggregate Layer. This chapter also discusses about the current transition methods used while transitioning of IPV4 to IPV6.

Chapter 5: This chapter is all about the framework design and the process taken to design it.

Chapter 6: This is the chapter which evaluates the framework which was designed and researchers result.

Chapter 7: This is the last which concludes the paper and giving direction for future work.

Chapter Two

2. Literature Review

Many of the papers in this research has conveyed the Constraints and Various Transition Mechanisms on how they can improve today's network in moving to the future network while maintaining connectivity between each and every device currently connected to the net.

Google has announced that over 10% of users access Google through IPv6 [8]. CAIDA has shown that from January 2014 to January 2015, the number of IPv6 access increased by 23% and the number of links between them increased by 29% [11].

Existing studies have addressed that IPv6-centric next-generation networks are widely deployed and applied. With the development of IPv6, applications such as video conference, IPTV, VoIP, and online games will become more and more prevalent inIPv6 networks [11], so keeping network availability as well as good performance is crucial. Investigating the best ways to transition to IPv6 network is the basis of guaranteeing the network with a good performance. Therefore, many studies have been performed to analyze IPV4-IPv6 networks, as well as figure out the differences between IPv4 and IPv6.However, our understanding of the IPv6 network cannot catchup with the speed of its development. So a deep understanding of the current IPV4 network could set a base in going through the transition.

The transition between the IPv4 Internet of today and the IPv6 Internet of the future will be a long process the fact that both protocols must coexist for some time. Figure 2 will show the transition phases. A mechanism for ensuring smooth, stepwise and independent changeover to IPv6 services is required. Such a mechanism must help the seamless coexistence of IPv4 and IPv6 nodes during the transition period. IETF has created the Ngtrans Group to facilitate the smooth transition from IPv4 to IPv6 services. The various transition strategies can be broadly divided into three categories, dual stack, tunneling, and other translation mechanisms. [5]

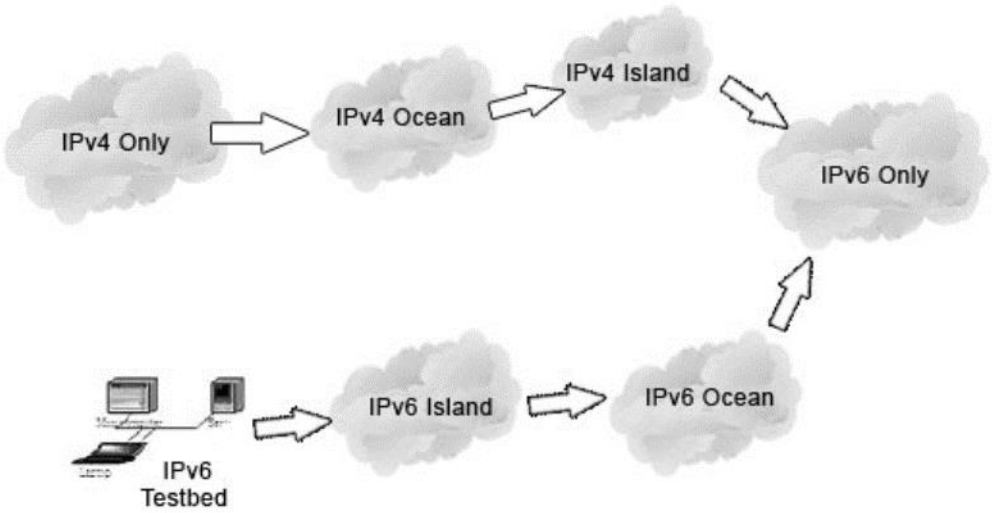

Figure 1 IPv4/IPv6 Transition Phases [5]

IPV6 has both abundant address resources and steady communication performance, so it becomes the ideal solution for most networks today, but it's is also a technology that comes with expense as all new technologies. IPV6 need equipment's that support it, so no backward compatibility is one issue especially for countries that are slow in adopting new technologies and don't have the resource to invest more on new and upcoming technologies. Keeping this in mind finding the best way to fit all of IPV6 in a single run could be hard and not feasible.

So most researchers propose for tunneling algorithms that could adapt the new and still support the old technologies. There are an over sixteen different transition technologies which have been currently identified and with the possibilities of interactions between different networks implementing different mechanisms to a complex picture of the mixed IPv4-IPv6 internet. [12]

IPv6 island network connecting to the IPv4 internet. Some of the techniques available are: [12]

- ✓ NAT-PT with SIIT
- ✓ Transport relay translators
- ✓ Socks64
- ✓ Shipworm

For a host to host communication there are some techniques like [12]

- ✓ DSTM
- ✓ BIS

- ✓ 6over4
- ✓ BIA

2.1. Operational Definitions

IPV6 is a fairly new concept and in barking on this new concept brings about new ideas and technologies with it. So in this section of the paper will try to point out important concepts and what they are all about.

Internet Protocol Address

IP or the Internet protocol is the main reason for this research so passing without discussing what it is and how it came to be we consider as "The sky might not be blue". So what is the internet protocol and how did it come to be. The articlefrom1980 of the United States of America Department of Defense explains IP as a protocol designed to let interconnected packet switched computer network systems or "Catenet" to communicate with each other [13] [14]. Up to now, this definition has not changed and IP since then has served what it was meant to the server with just some upgrades to what it can do. Going through different version, today the internet protocol has two versions working to interconnect systems. IPV4 uses 32bit addressing schema producing 2^{32}addresses which are just above four billion addresses. IPv6 is also called IPng (Internet Protocol next generation) and it is the newest version of the Internet Protocol reviewed by the IETF standards committees to replace the current version, IPv4. [8]

While increasing the pool of addresses is one of the most often-talked about the benefit of IPv6, there are other important technological changes in IPv6 that will improve the IP protocol:

- ✓ No more NAT (Network Address Translation)
- ✓ Auto-configuration
- ✓ No more private address collisions
- ✓ Better multicast routing
- ✓ Simpler header format
- ✓ Simplified, more efficient routing
- ✓ The true quality of service (QoS), also called "flow labeling"
- ✓ Built-in authentication and privacy support

- ✓ Flexible options and extensions
- ✓ Easier administration

Introduction to IPv6

IPv4 has demonstrated its features to be useful both in the implementation and operation. Furthermore, it plays an important part in every network, from a local area network to the worldwide Internet. Nevertheless, everything has two sides and IPv4 is not an exception. With the growth of population and the development of technology, the demand for IPv4 addresses becomes higher and higher day by day while the resource is running out. Although private addresses have been long used to compensate for this problem, it is just a temporary solution as the levitation of Internet-connected devices makes sure that the public IPv4 addresses will soon be exhausted. Furthermore, the rise of the Internet and its users require devices which play as backbone routers to manage and support a great amount of routing tables consisting of over 70,000 routes across the world [15].

However, every problem has in it the seeds of its own solution. In response to these matters, a new concept has been developed which is known as IPng (IP-The Next Generation) or IPv6 (Internet Protocol version 6) along with its protocols and support. Similar to IPv4, IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. With many of its additional features, the IPv6 is supposed to eventually replace the old IPv4 in every network without limitations. The main differences between IPv4 and IPv6 range from new addressing space to built-in security. The following sections discuss each of these new features in detail [2].

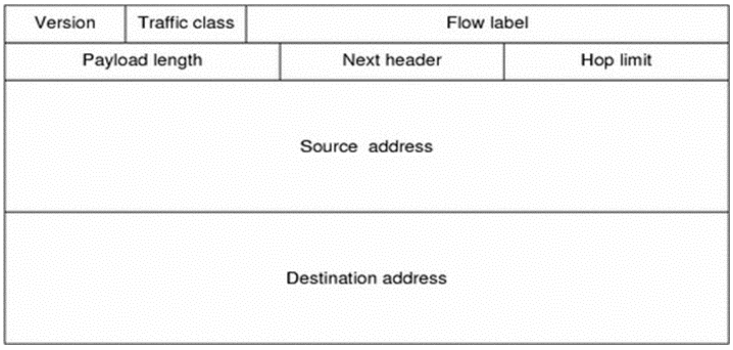

Table 2 IPv6 header [15]

"Version - Internet Protocol version number = 6.

Traffic Class - 8-bit traffic class field.

Flow Label - 20-bit flow label.

Payload Length-16-bit unsigned integer: Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets. (Note that any extension headers present are considered part of the payload, i.e., included in the length count.)

Next Header - 8-bit selector which identifies the type of header immediately following the IPv6 header. It uses the same values as the IPv4 Protocol field.

Hop Limit - 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.

Source Address - 128-bit address of the originator of the packet.

Destination Address - 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).” [15]

The new form of IPv6 header aims to reduce header overhead by relocating unimportant fields and optional fields to extension headers which are positioned right after the IPv6 header. As a result, this enables the simplified IPv6 header to be processed more efficiently at intermediate routers. However, the IPv6 protocol is incompatible with the IPv4 protocol. Therefore, a network connected device (host or router) needs to apply an implementation of both IPv4 and IPv6 in order to identify and process two kinds of header formats [16].

2.2. IPv6 New Features

Expanded address space

As we have mentioned above, the main reason for the invention of IPv6 is the shortage of IPv4 resources. Despite its usefulness and flexibility, IPv4 combines of 32 bits, which can only create a total of 2^{32} (4,294,967,296) addresses. Meanwhile, with new technologies, IPv6 contains 128 bits, and as calculated above, the new address space supports a number of 2^{128}

(340,282,366,920,938,000,000,000,000,000,000,000,000,000) addresses, which is 2^{96} times larger than IPv4 address resources. From those calculations, there has been a saying that “With IPv6, nearly every object in the world can obtain an address for its own”. As a result, this expanded

address range of IPv6 can be variously applied from the Internet backbone (interconnected networks, core routers) to individual subnets (hosts, end devices) within an organization. Furthermore, it also makes address-conservation techniques, such as NATs, become unnecessary, which gained widespread deployment as an effort to alleviate IPv4 address exhaustion [15].

Effective and organized infrastructure for addressing and routing

Along with the expanded address space comes the hierarchical address format. This is also a new and important aspect of IPv6. Unlike IPv4 hierarchical address consists of network, subnet, and host components, IPv6, supported with 128-bit addresses, provides globally unique and organized addressing known as prefixes (address classes in IPv4).

Advanced address configuration

In order to reduce complexity in the configuration of the host, IPv6 is equipped with new functions to uphold two ways of address configuration:

Stateful address configuration: a host receives IPv6 address along with optional configuration specifications from a server named DHCPv6 via a UDP link. However, in the circumstance that DHCPv6 server does not exist on that link, there will be some special nodes acting as relay agents to help transmit these request packets from the host to other DHCPv6 servers in the nearby link or forward to the next relay agent.

Stateless address configuration: with this mechanism, manual configuration of the hosts or additional servers is no longer needed. In addition, it helps to minimize the configuration of routers. It also gives way for a host to form its own addresses, known as link-local addresses, by utilizing local and advertised information from routers. This means hosts on the same link can automatically create themselves link-local addresses and communicate with each other with manual configuration or in the absence of a router [17].

Built-in security

Since the birth of the Internet up to today, security has always been an important issue when there is an increasing number of hackers, equipped with networking knowledge, trying to prove themselves. The Internet once was a network without intermediary gateways or routers or security (an end-to-end network). After that, as the network develops, there raises a question "How to ensure the safety of private data when transmitting on a public network?" Under the

circumstances, gateways, firewalls, and local network isolation have become available all over the world as a reply to this question. Despite these efforts, data privacy and security continues to be a prominent issue and no complete solution has been found. However, in conjunction with the invention of IPv6, whose main purpose is to overcome the IP address depletion, the most propitious answer for the data protection has been found, known as built-in security (IPSec) [18].

IPSec is a framework of open standards-setting network security policies for transmitting packets in a network. It is developed to function in the layers between the physical layers and the application layer. This ensures all data encapsulated in the packet to travel safely among stations such as routers. Therefore, in IPv6 structure contains a protocol suite requirement to support for IPSec, increase network security and contribute to interoperability among various IPv6 deployments. However, the IPSec in IPv6 is located in the extension headers, which makes the use of IPSec is optional. Consequently, security may be improved thanks to the built-in security in IPv6 protocol, the total protection still lies in the hands of human beings [19].

Better support for Quality of Service

Quality of Service (QoS) is an old term commonly used in modern networks. In IPv4 networks, it is known as "best level of effort" service. However, it has a weakness that IPv4-implemented networks are unable to tell the difference if data that are time-sensitive (streaming video or audio) or not (file transfer). In case a packet is lost when transmitting, the TCP identifies the loss and it will send a request for retransmission. However, this will also create an inevitable delay. As a result, when the video is streaming, a gap will occur such as there is neither sound nor picture [17].

Fortunately, in 128 bits of IPv6 are there some new features to increase assured service, enhance security, and improve reliability. The way of identifying and handling traffic is defined in new fields of IPv6. By applying a Flow Label field in the header, it enables packets belonging to a flow are recognized and handled specially. As the traffic is recognized in the header, QoS can be supported efficiently. With these enhancements, IPv6 supports applications to request handling with no delay across the WAN. This will help time-sensitive data to load with low latency via priority level:

- Level 0 - No specify priority
- Level 1 - Background traffic (news)
- Level 2 - Unattended data transfer (email)
- Level 3 - Reserved
- Level 4 - Attended bulk transfer (FTP)
- Level 5 - Reserved
- Level 6 - Interactive traffic (Telnet, Windowing)
- Level 7 - Control traffic (routing, network management)

However, although this method minimizes fragmentation and latency, it consumes more bandwidth for prompt arrival, which results in inefficient utilization.

Neighbor Discovery Protocol

Since the invention of IPv6 also comes the new Neighbor Discovery protocol, which manipulates messaging as the technique to manage the interaction of neighbor nodes on the same link, which is called Internet Control Message.

Protocol for IPv6 (ICMPv6). The list of major activities that the Neighbor Discovery protocol controls over the IPv6 local link includes router discovery for supporting hosts to find routers on the local link, address autoconfiguration for assigning automatically IPv6 addresses for interfaces, prefix discovery for discovering the known subnet prefixes to differentiate destinations, address resolution for determining the link-local address of a neighbor with only the destinations' IP address, next-hop determination for applying an algorithm to identify the IP address of a packet recipient one hop that is beyond the local link, neighbor unreachability detection for identifying if a neighbor is no longer reachable, duplicate address detection for determining if an address that the node wants to use is not already in use, and redirection for supporting routers to inform a host of a better first-hop node to use to reach a particular destination. [20]

As from those functions above, the Neighbor Discovery protocol for IPv6 is performing the functions of Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages and contributing additional functionality. [19] Neighbor Discovery uses the following ICMP message types for communication among nodes on a link:

- Router solicitation
- Router advertisement
- Neighbor solicitation
- Neighbor advertisement
- Redirection

Extensibility

In IPv6, new features can be extended by adding extension headers after the IPv6 header. Different from the IPv4 header, which leaves only 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet. [12]

For More info on IPV4 V6 please refer Annex 1 table IPv4 and IPv6 Comparison.

2.3. IPV6 transition Mechanisms

Bump-In-the-Stack Mechanism

BIS mechanism an RFC 2767 standard includes a TCP/IPV4 protocol module and a translator module, which consists of three bump components and is layered above an IPV6 module. The identified packets are translated into IPV6 packets and then forwarded to the IPV6 protocol module. The three bump components are the extension name resolver, which examines DNS lookups to determine whether the peer node is IPV6-only, which allocates a temporary IPV4 address to the IPV6peer and caches the address mapping, which translates packets between IPv4and IPv6 protocols. [3]

Network Address Translation-Protocol Translation

The NAT-PT mechanism is a Stateful IPV4/IPV6 translator. NAT-PT nodes are at the boundary between IPV6 and IPV4 networks. Each node maintains a pool of globally routable IPV4 addresses, which are dynamically assigned to IPV6 nodes when sessions are initiated across the

IPV6/IPV4 boundary. This mechanism allows native IPV6 nodes and applications to communicate with native IPV4 nodes and applications, and vice versa. [11] [3]

Dual stack mechanisms (DSM)

This mechanism is the deployment of a quite simple idea. Any host that desires to participate in both IPv4 and IPv6 networks has to maintain both stacks on its network interface(s). It enables a full IPv4 end-to-end communication between a dual-stack host within an IPv6 only network and an IPv4 only host. The DST mechanism is based on a tunneling mechanism using a dynamic tunnel interface combined with temporary IPv4 address assignment provided by a DHCPv6 server. DSTM is based on the usage of a DHCPv6 server, which temporarily assigns global IPv4 addresses to IPv6 hosts that wish to communicate with an IPv4 only host. The IPv4 packets are encapsulated intoIPv6 packets through a DTI interface and are transferred within the IPv6 network to the Border Router, which interconnects the IPv6 network with the IPv4 network. [2]

IPV6 Provider Edge routers (6PE)

6PE according to the RFC4798 standard, defines it as a versatile approach to interconnecting IPV6 islands over a Multiprotocol Label Switching (MPLS) core. This is independent of the control plane in the MPLS core is based on IPV4 or IPV6 routing and connectivity label bindings, it actually relies on IPV6 Provider Edge routers (6PE) being dual-stacked and both IPV6 and IPV4 enabled towards edge devices. [16] The other point on 6PE is that it does not use manual standard tunnels, it provides an alternative where all tunnels are established dynamically eliminating the need to configure and maintain tunnels. So 6PE is a technique that provides global IPv6 reachability over IPv4 MPLS. It allows one shared routing table for all other devices. 6PE allows IPv6 domains to communicate with one another over the IPv4 without an explicit tunnel setup, requiring only one IPv4 address per IPv6 domain.

Routing Protocols

Routing is the most important function on the internet which relies completely on IP addresses for the propagation of reachability information. And routing protocols help is achieving the above with standardizing and find the best routes for the communication using different algorithms.

With the transition towards IPv6 and in a mixed network scenario, existing routing protocols for both interior and exterior routing requires upgrade. The IGP protocols like OSPF, RIP and IS-IS have newer versions tailored in such a way they can operate on IPv6 addresses.

DNS Support

The existing DNS mechanism for IPV4 networks provides the name to address lookup and the reverse mapping from address to a name. The name servers now require to store the associated IPv6 address of a name (in addition to the IPV4address) as well as they should be able to perform the reverse lookup functionality.

The DNS records for IPV6 currently use the A6 format or the AAAA format (A6 has experimental status and AAAA is the preferred IETF supported mechanism). [12] Hence a DNS client requiring theIPv6 address of a host would request the server for the AAAA entry (not many servers supportA6) of that host. If the entry is found, it is used directly, otherwise, the entry corresponding to the IPV4 address is retrieved and mapped into an IPV6 address by using standard procedures. [2] [1]

Network Management

As new standards are being defined for the IPV6 protocol and all other related technologies, the corresponding SNMP MIB definitions for these are also being considered. Which in turn affects vendors dealing with network management because they have to implement the new MIBs. The standard transport mechanism for SNMP is over UDP which could run either over IPV4 or IPV6 with appropriate changes to the socket layer [2].

Standard SNMP management platforms like have basic support for IPV6 available and are also indicating roadmaps with full feature support for IPV6 [11]. Unless sufficient management tools are available, the commercial deployment of IPV6would be difficult since ISPs and enterprise network managers require the tools to configure and monitor IPV6 networks. The tools become very important especially in a mixed network scenario where the network manager will have to keep track of tunnels, routing issues, DNS configurations, and other services across IPV4, IPv6 and even both networks.

Mechanism Type	Implication on Application	IPv4 address Requirements	Hosts/site	Mechanism Comments
Dual stack	None	Permanent or pool of addresses allocated by a DHCP server	Site/host	Very simple to set up, available to every node supporting IPv6 stack
DSTM	None	The pool of addresses required Site/host for AIIH server	Site/host	Allows the host to run the end-to-end IPv4 application within an IPV6-only network. Allows IPv4/1Pv6 of the IPv6-only host application to communicate with either IPv4 or IPv6 end point without the need of specific ALG
6to4	Applications need to be ported to interface with the IPv6 stack	IPv4 address of border routers	Site/host	Allows automatic joining of IPv6 network separated by an IPv4-only network
Tunnel broker	Applications need to be ported to interface with the IPv6 stack	One for the dual-stackhost. At least one for the tunnel broker implementation	Site/host	Each IPv6 network needs to have a 6to4 border router
6over4	Applications need to be ported to interface with the IPv6 stack	One per host	Host	Allows an isolated IPv4 host within an IPv4only network, to reach an IPv6 wide network

NAT-PT	Applications including IP addresses in the packet payload need the availability of a dedicated ALG into the NAT-PT router	Pool of IPv4 addresses needed	Site	Allows automatic joining of IPv6 network separated by an IPv4-only network

Table 3 Different IPV6 Transition Methods [5] [1] [21]

The above are the transition methods which this research has identified after reviewing different works. All of the methods have their own advantages and drawbacks as discussed above. This shows one cannot just pick and use any of the methods and of any kind of situation. For this research Dual stack has been chosen to be used as part of the frame work. The reason why Dual stack has been chosen is because of the nature of it, Dual stack has no effect to the current application running and it ability to be deployed with a minimum effect on the network. Also dual stack supports both version of protocols and allows flexibility while and after deploying it.

To support this the research has evaluated the current transition methods.

2.4. Evaluation of Current IPv6 Transition Methods

The transition from IPv4 to IPv6 is not something that's going to happen overnight it involves a lot of changes in network structures with the use of IP addresses. Although many kinds of transition mechanisms have been proposed to help with this process, the implementation of IPv6 is never said to be easy and simple, even for experienced administrators [15]. As a result, the most difficult problem to make decisions for is which method can be used for the implementation process to achieve a smooth and seamless transition. So, to do this below are different methods that this research evaluated and shows at the end why Dual stack is chosen to be part of the framework being proposed.

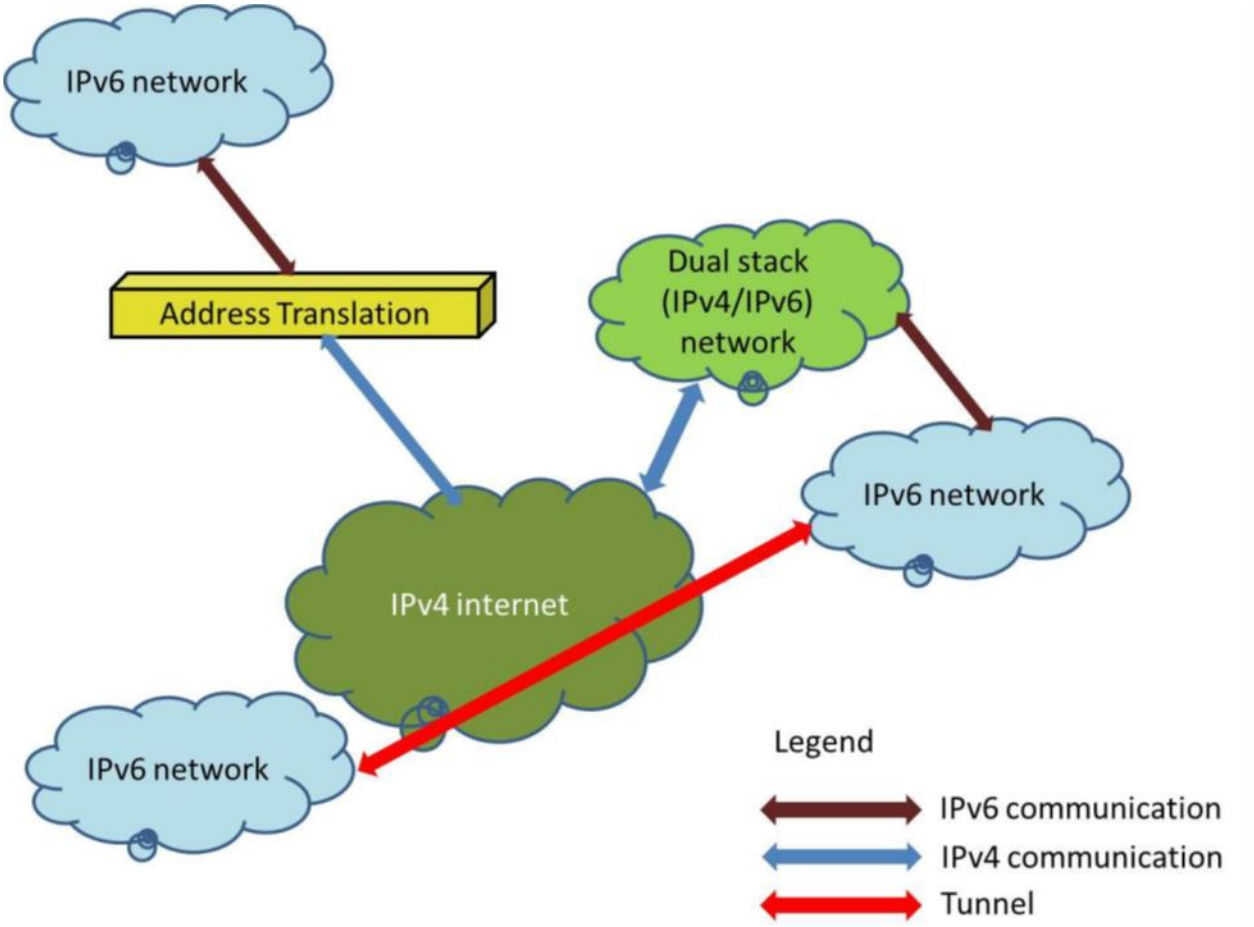

Figure 2 Different transition technologies [5]

On the above figure, we can see that there could be a lot of technologies that could be used in the translation of IPV4 IPV6 networks. Over sixteen transition techniques have been used and tested for the communications between different networks to ensure IPv4 and IPv6 interoperability

[15]. “One size does not fit all and a network can apply different transition mechanisms together to support a complete distributed system” [15].

This section will try to point out the framework which will be proposed here based on the information from the research and literature review, will try to include some major transition methods as well as a relevant matter to opt out the best methods for large enterprise networks. Each technique possesses individual attributes and plays an important part in the transition process.

Dual Stack IPv4/IPv6

Dual stack happens in the network layer, which contains both IPv4 and IPv6.According to [15], “*A stack is a type of data structure -- a means of storing information in a computer. When a new object is entered in a stack, it is placed on top of all the previously entered objects. In other words, the stack data structure is just like a stack of cards, papers, or any other real-world objects you can think of. In networking, connections between computers are made through a series of smaller connections. These connections, or layers, act like the stack data structure, in that they are built and disposed of in the same way*”.

However, like any market regulations, the acceptance of any new technology lies in the way it integrates into the current infrastructure with no serious breakdown of service. An ISP network includes many IPv4 networks and thousands of IPv4 nodes. Therefore, the transition from IPv4 to IPv6 should go gradually rather than shift all nodes at the same time; IPv4 and IPv6 will coexist for some time. As a result using dual-stack method to transit could be best suited for such cases.

The dual-stack method is literally to use two IPv4 and IPv6 stacks for operating simultaneously, which enables devices to run on either protocol, according to available services, network availability, and administrative policies. This can be achieved by both end systems and network devices. As a result, IPv4 enabled programs to use IPv4 stack and this goes the same for IPv6. The IP header version field would play an important role in receiving and sending packets. In other words, this kind of IPv6 transition is the encapsulation of IPv6 within IPv4. The complete transition can be managed by DNS, for example, in the circumstance that a dual-stacked device queries the name of a destination and DNS gives it an IPv4 address, it sends IPv4 packets, or in

case DNS responds with an IPv6 address, it sends IPv6 packets. This mechanism is currently the best choice for the transition as many operating systems have applied dual IP protocol stacks [22].

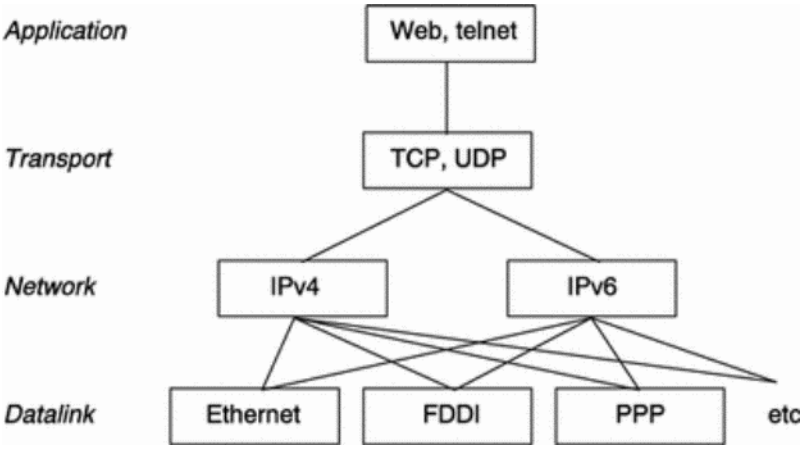

Figure 3 The structure of Dual stack model [17]

As presented in above figure 7, the dual stack method is implemented in the network layer for both IPv4 and IPv6. Before transferring the packet to the next layer, the network layer will choose which one to use based on the information from the datalink layer. Large enterprise networks that are decided to transit to IPv6 can apply the dual stack method as the basic strategy, which involves the device configuration to be able to utilize IPv4 and IPv6 at the same time on the core routers, perimeter routers, firewalls, server-farm routers, and desktop access routers. Depending on the response to DNS requests, applications can choose which protocol to use and this choice can be made in consonance with the type of IP traffic. Furthermore, hosts can attain both available IPv4 content and IPv6 content. Accordingly, the dual-stack mechanism presents a flexible transition strategy [23].

However, despite its greatest flexibility, there are still some concerned issues with this method such as every dual-stack device still requires an IPv4 address; two routing tables must be maintained in every dual-stacked router; as two stacks must be run at the same time, additional memory and CPU power will be required; moreover, every network requires its own routing protocol; supplementary security concepts and rules must be set within firewalls to be suited to each stack; a DNS with the ability to resolve both IPv4 and IPv6 addresses is required; finally, all programs must be able to choose the communication over either IPv4 or IPv6, and separate

network management commands are required [22]. For example, based on figure 8 below, the client computer at first sends a DNS lookup request for the website www.a.com. Then, the DNS server will reply with an IPv4 and an IPv6 address of the website. Finally, the client computer will use that information to send a request to the router via either IPv4 or IPv6 network and the web server will reply the client by allowing to load the website.

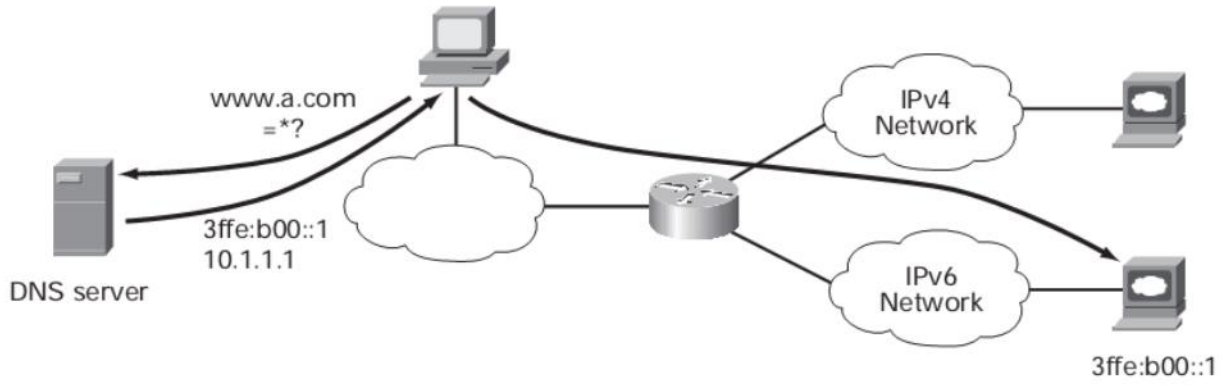

Figure 4 IPv4 – IPv6 dual stack operation [17]

Translation

Together with IPv6 deployment strategies into large enterprise networks, figure 8below indicates that there are various translation mechanisms (NAT-PT, application level gateways (ALG)) also applied to enable the communication between IPv4-only applications and IPv6-only applications. The meaning of translation is to convert directly protocols from IPv4 to IPv6 or vice versa, which might result in transforming those two protocol headers and payload. This mechanism can be established at layers in the protocol stack, consisting of network, transport, and application layers. The translation method has many mechanisms, which can be either stateless or stateful. While stateless means that the translator can perform every conversion separately with no reference to previous packets, stateful is the vice versa, which maintains some form of state in regard to previous packets. The translation process can be conducted in either end systems or network devices [24].

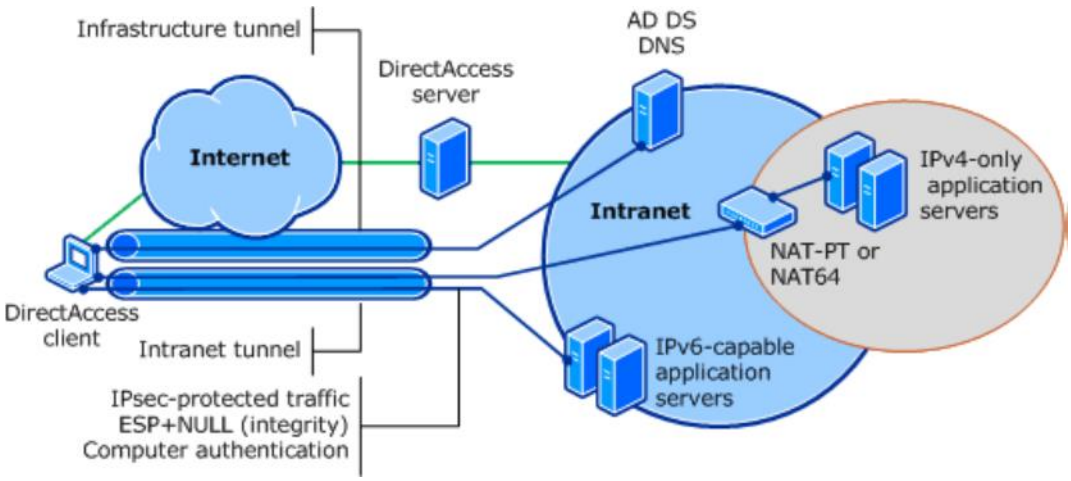

Figure 5 Translation method model [15]

The fundamental part of the translation mechanism in the transition process is the conversion of IP and ICMP packets. All translation methods, which are used to establish communication between IPv6-only and IPv4-only hosts, for instance, NAT-PT or BIS, apply an algorithm known as Stateless IP/ICMP Translator (SIIT). The function of this algorithm is to translate packet-by-packet the headers in the IP packet between IPv4 and IPv6, and also addresses in the headers among IPv4, IPv4-translated or IPv4-mapped IPv6 addresses. However, this does not mean IPv6 hosts can get an IPv4 address or route packets, but this assumes that each IPv6 host can have a temporary assigned IPv4 address [1].

The fundamental part of the translation mechanism in the transition process is the conversion of IP and ICMP packets. All translation methods, which are used to establish communication betweenIPv6-only and IPv4-only hosts, for instance, NAT-PT or BIS, apply an algorithm known as Stateless IP/ICMP Translator (SIIT). The function of this algorithm is to translate packet-by-packet the headers in the IP packet between IPv4 and IPv6, and also addresses in the headers amongIPv4, IPv4-translated or IPv4-mapped IPv6 addresses. However, this does not mean IPv6 hosts can get an IPv4 address or route packets, but this assumes that each IPv6 host can have a temporary assigned IPv4 address [11].

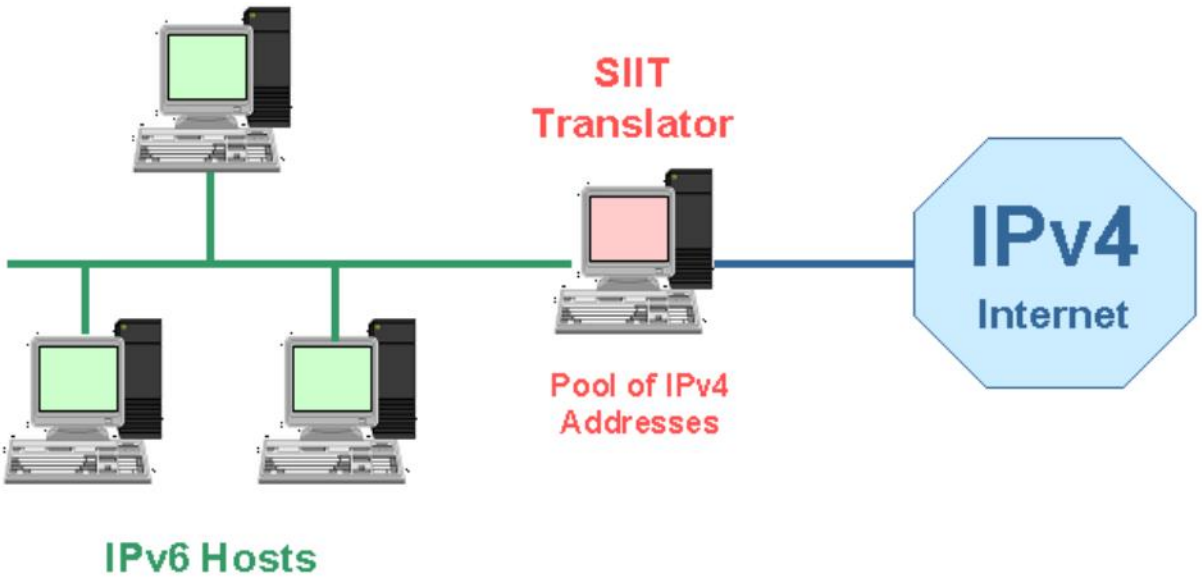

Figure 6 Stateless IP/ICMP Translation (SIIT) [2]

The above figure 10 indicates an algorithm that designates a two-way translation between IPv4 and IPv6 packet headers or between ICMPv4 and ICMPv6 messages. The interpretation has been arranged so that UDP and TCP header checksums are not influenced during the process. More importantly, SIIT is currently used as the backbone for NAT-PT and BIS [25].

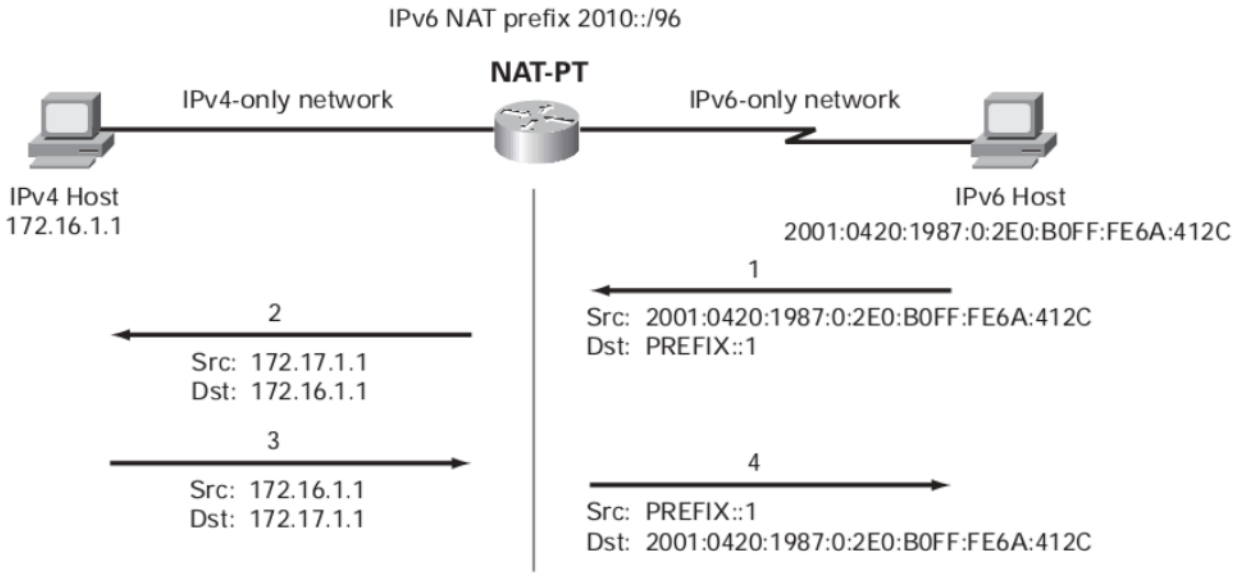

Figure 7 Network Address Translation-Protocol Translation (NAT-PT) [1]

From the figure above, the router is used as a translation communicator between an IPv4-only network and an IPv6-only network. NAT-PT is considered as a stateful translator functioning in the network layer with the SIIT algorithm. The main role of a NAT-PT device, such as routers or servers, is to support numerous IPv6 nodes by assigning a temporary IPv4 address for each, which permits native IPv6 hosts and applications to communicate with native IPv4 hosts and applications. In general, it acts as a communication proxy with IPv4 peers. According to [15] "A *server that stands between an external network (such as the Internet) and an organization's internal (private) networks and serves as a firewall. It prevents external users from directly accessing the internal information resources, or even knowing their location. All external requests for information are intercepted by the proxy server and checked for their validity, and only authorized requests are passed on to the internal server*". However, this mechanism still possesses limitations similar to IPv4 NAT such as point of failure, decreased performance of an application level gateway (ALG), a reduction in the overall value and utility of the network. NAT-PT also prevents the ability to implement security at the IP layer [1] [26].

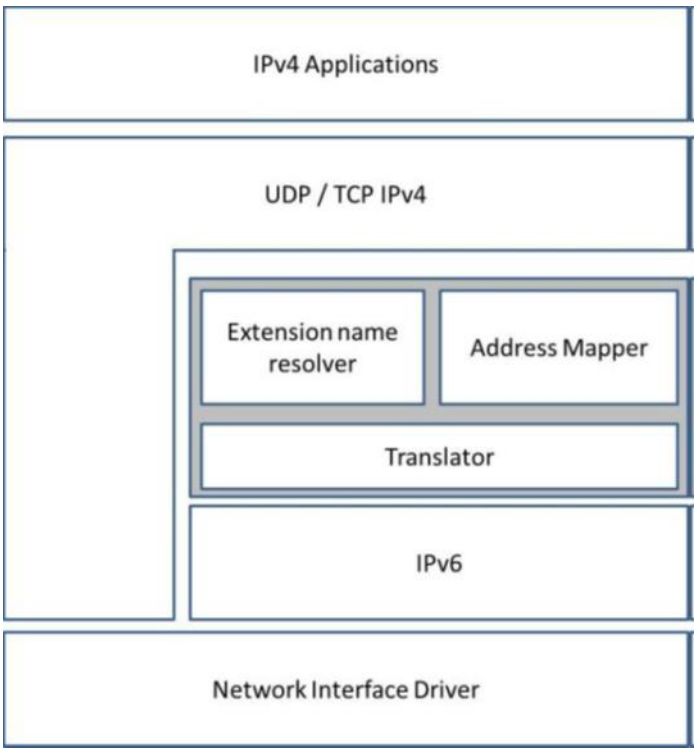

Figure 8 Bump in the Stack model [15]

The BIS method means there are three more fields inserted into the structure of layers as indicated in Figure 12 above. There will be three additional components, name resolver extension, address mapper, and translator, and are layers between the application and network layers. The BIS method is specially designed for communication between IPv4 applications on an IPv4-only host and IPv6-only hosts. The term bump is used to describe extra modules in a TCP/IP stack. Firstly, the extension name resolver uses DNS lookups to see if the node supports only IPv6. Secondly, the address mapper will allocate a temporary IPv4 address for the IPv6 node and save that in the address mapping caches. Thirdly, the translator translates packets between IPv4 and IPv6. In the circumstances that a program needs to transmit data from and to a host, which supports only IPv6, those layers will play their roles to map an IPv6 address into the IPv4 address of the IPv4 host. Nevertheless, those temporary IPv4 addresses are only apparent in the end system and normally come from a private address space. Therefore, BIS is only suitable for programs that include no address-dependent fields in application layer protocols. One more thing is that this method can only be implemented on end systems. The reason for this limitation is that it is easier for translation processes to solve application to network interoperability problems but it would be harder to control on a larger scale [27].

Those are three representatives for the translation mechanism, which are currently used in the IPv6 transition. With this method, we can easily connect devices in networks. Furthermore, it requires neither modifications to nodes nor additional applications to be established on networks. Only some adjustments need to be made on the boundary routers. However, nothing is perfect and this translation is also not an exception. Although it has some benefits, the disadvantages it possesses are also taken into consideration. At first, the first drawback of the NAT techniques is that the end-to-end security is not supported. Secondly, due to the function of NAT, routers would become the single point of failure, which means if anything occurs to routers, the whole networks could collapse. Finally, the level of complexity in IP addresses would be increased, which can cause the loss of information in the process [1].

Tunneling

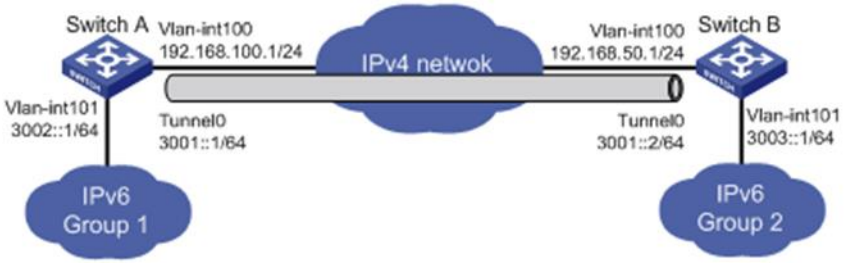

Figure 9 Tunneling transition method [3]

The last method discussed for IPv6 transition process is tunneling as presented in Figure 13. This is used to transfer data between compatible networking nodes over incompatible networks. There are two ordinary scenarios to apply tunneling technique: the allowance of end systems to apply off link transition devices in a distributed network and the act of enabling edge devices in networks to inter-connect over incompatible networks.

Technically speaking, the tunneling technique utilizes a protocol whose function is to encapsulate the payload between two nodes or end systems. This encapsulation is carried out at the tunnel entrance and the payload will be de-capsulated at the tunnel exit. This process is known as the definition of the tunnel. Therefore, the main issue in deploying tunnel is to configure tunnel endpoints, determine positions for applying encapsulation. Based on our research, this mechanism is generally attained via manual or tool-based parameter entry, existing services like DNS or DHCP, or by taking into use the embedment of information into IP addresses or applying an IPV6 anycast address [15]. Network devices can achieve the two processes of encapsulation and de-capsulation at tunnel endpoints. In general, tunneling mechanism is a simple deployment with point-to-point configuration. Nevertheless, tunnels can also be implemented hierarchically and sequentially. The hierarchical structure is applied in the circumstances that there are transition tunnels operating alongside with security or QoS tunnels. The sequential structure can be established in an end-to-end path, from end systems to local gateways, and beyond. As a result, these two establishments always increase requirements for processing and packet delay [28]. Up to date, there exist different tunneling methods such as 6to4, ISATAP, Teredo, DSTM, and 6over4. Tunnels may be manually configured or automatically configured [24].

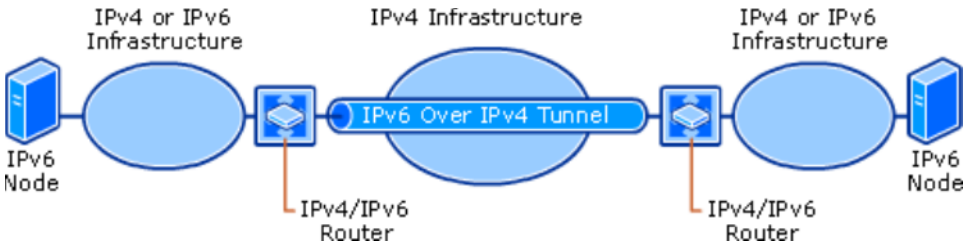

Figure 10 6over 4 model (Microsoft) [21]

The figure above illustrates the 6over4 method that inserts IPv4 addresses into IPv6 address link layer identifier part and defines Neighbor Discovery (ND) over IPv4 by using organization-local multicast. In this method, the multicast enables the IPv4 network to perform as a virtual LAN and the IPv6 target address will be resolved on this network to get the destination IPv4 address for the tunnel endpoint. This mechanism accommodates all features of IPv6 such as end-to-end security, multicast and stateless auto-configuration [21].

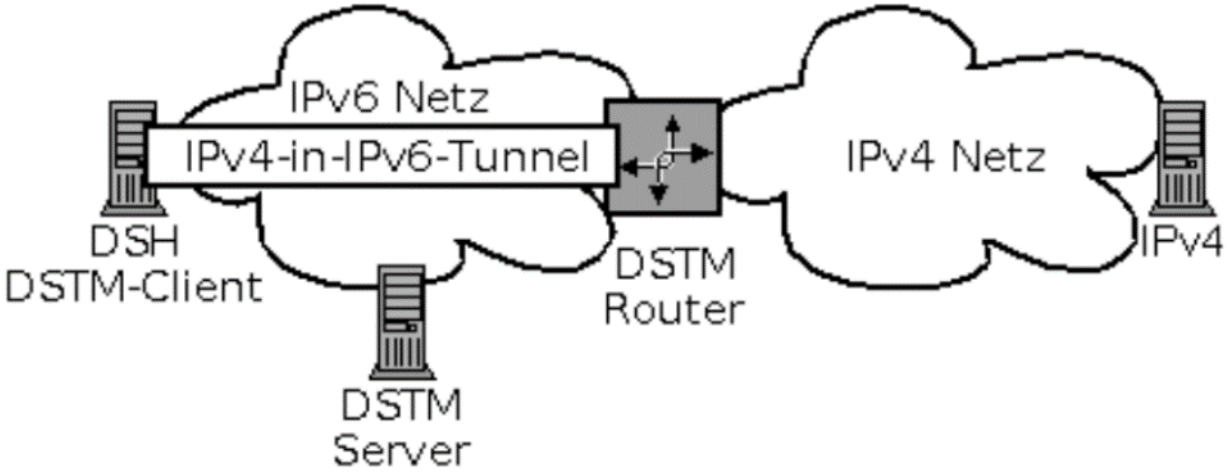

Figure 11 Dual Stack Transition Mechanism (DSTM) [2]

The DSTM mechanism, which is expressed in Figure 15, allows temporary IPV4 addresses to be allocated for end systems with dual-stack enabled with a connection to networks that support IPV6 only. The general idea is that IPV4 packets will be tunneled to pass through IPV6 network to get to the global IPV4 Internet. In the event that a DSTM end system starts sessions, a DHCPv6 server which has been modified to acquire a temporary IPV4 address and the address of DSTM border router, to which packets are later tunneled. On the other hand, in case a node supporting only IPV4 initiates sessions, the request sent to DNS for the lookup process would be

directed to an adjusted DNS server in the DSTM domain, at which a temporary IPV4 address will be appointed for the end system. As a result, incoming packets are tunneled to this IPV4 address [11].

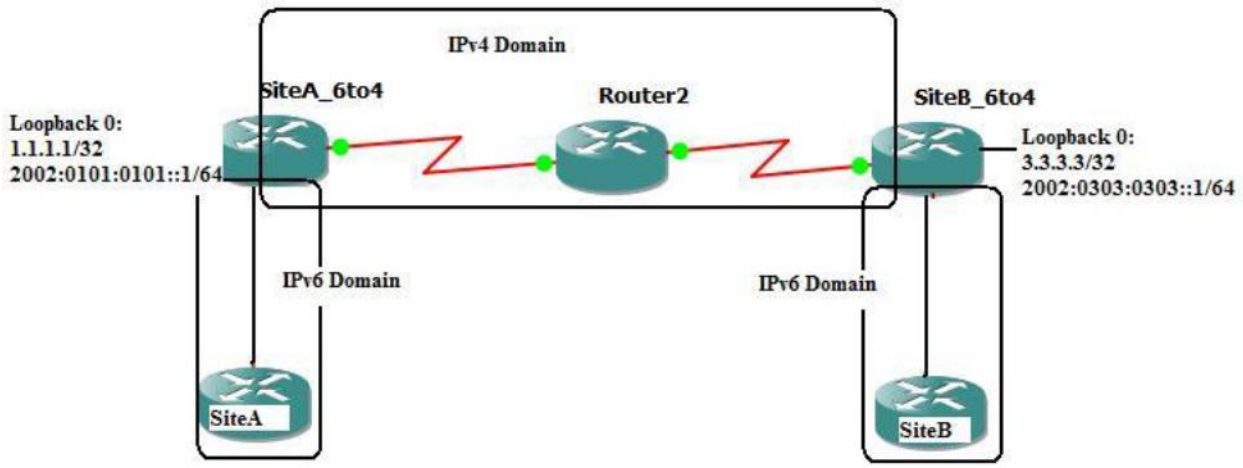

Figure 12 6to4 Automatic Tunneling Model [17]

Automatic means that tunnel configuration is carried out with no additional management. As shown in Figure 16, this method is considered the most popular choice in the field of automatic tunneling technique. When in operation, this mechanism will have IPv6 traffic tunneled upon IPv4 networks within isolated 6to4 networks. A special prefix containing the IPv4 address of its 6to4 gateway is supposed to be present in each 6to4 network, which enables tunnel endpoint addresses are acquired easily and requires no IPv6 administrative work. Then connection from 6to4 network to the rest of the IPv6 network is established via a dual-stack local gateway and a dual stack relay router. Therefore, every IPv6 packet is directed to the gateway. These kinds of tunnels would transfer the traffic to the appropriate gateway with suitable IPv4 address [4].

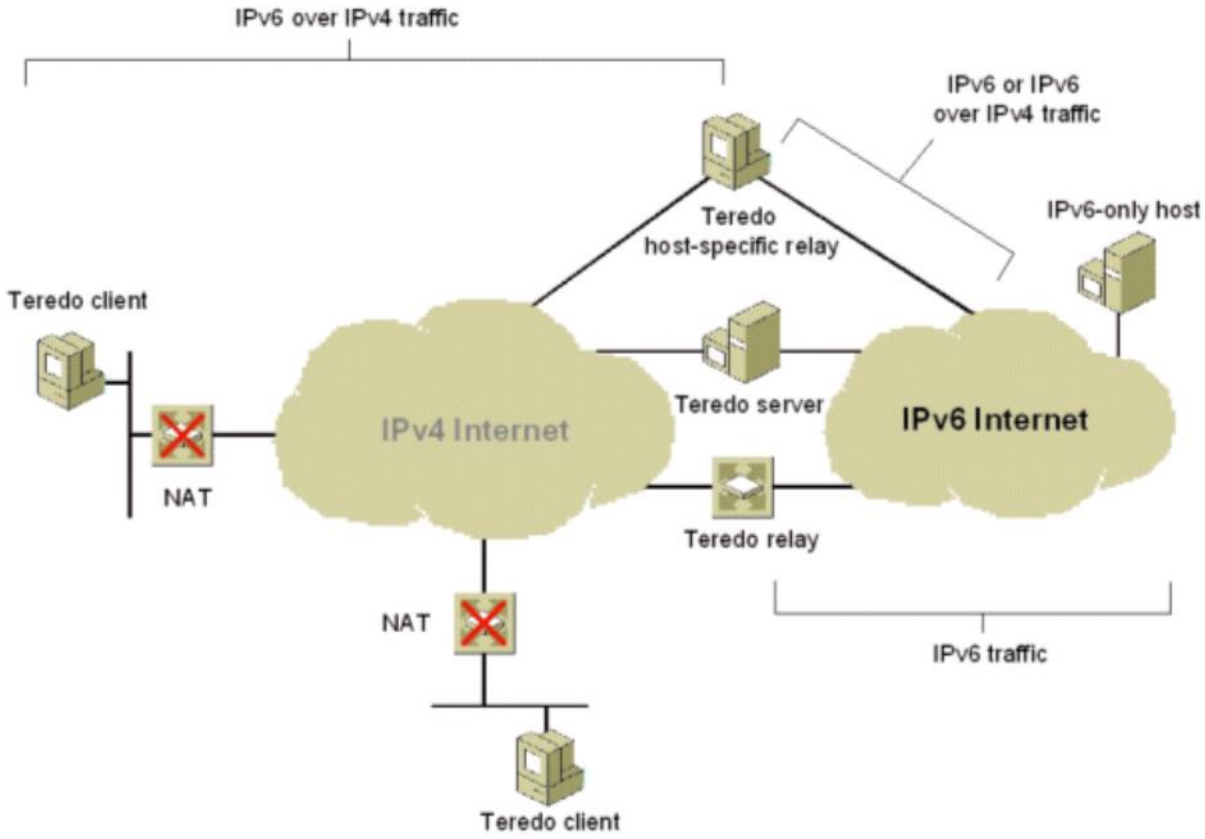

Figure 13 Teredo method [15]

Teredo mechanism is a technique for assigning addresses and providing tunneling services automatically to allow IPv6 connectivity across the IPv4 Internet. This method is supposed to be the solution for the lack of 6to4 functionality by supporting the tunnel for IPV6 packets between hosts within sites while 6to4 method only allows providing tunnels for IPV6 packets between edge devices. Based on different research, networks which are applying IPV6, face another problem with NATs. Because of its nature, IPV4- encapsulated IPV6 packets have the header set to 41, which prevents them to pass through typical NATs. Accordingly, because UDP messages can be translated universally by NATs and can traverse multiple layers of NATs, Teredo encapsulates the IPV6 packet as anIPV4 UDP message, provided that NAT supports UDP port translation, it supports Teredo [24].

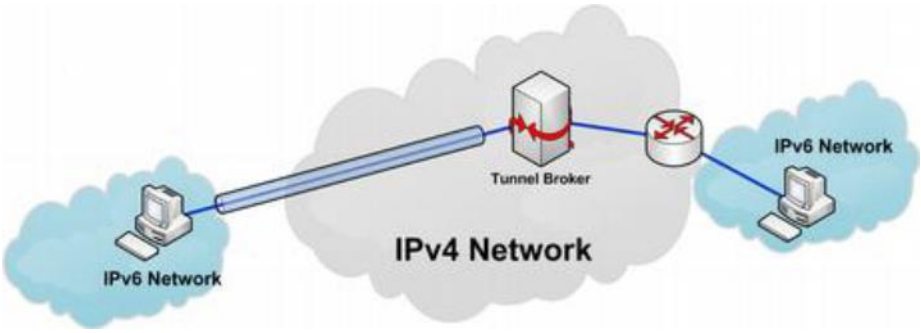

Figure 14 Tunnel Broker model [15]

This is another approach to IPV6 with the support of dedicated servers, known as Tunnel Brokers as illustrated in Figure 18, to answer automatically tunnel requests from users, which is believed to increase IPV6 growth with connected hosts and to support access to IPV6 networks. This method makes it easy for IPV6 ISPs to manage access control by applying own policies on network usage. This is where users make the connection for registering and activating tunnels. Then, dedicated servers or Tunnel Brokers control the management of tunnels with activities such as creation, modification, and deletion for users. In addition, to support networks on a larger scale, this method can distribute the workload to some tunnel servers by delivering orders to concerned tunnel server when there is a need to manage a tunnel. Finally, connections between tunnel brokers and servers can occur with IPV4 or IPV6 [16].

Generally, the tunneling mechanism allows us to connect isolated IPV6 nodes and networks whether or not the ISP has been upgraded to IPV6. Moreover, it also takes advantage of emerging IPV6 services while remaining connected to the IPV4 world. However, its encapsulation and de-capsulation take more time and CPU power and add more complications to troubleshooting and network management as well. One more thing is that those tunnel endpoints can be single points of failure and they can be vulnerable to security attacks [2].

	Advantages	Disadvantages
Tunneling	- Configure tunnel endpoints only - Simple deployment - No additional management	- Face another problem of NATs - Take more time and CPU power - Harder to troubleshooting and network management - Having less points of failure - Vulnerable to security attacks
Translation	- The router is used as a Translation communicator - Solve network interoperability problems	- Limitations similar to IPv4NAT - Reduction in the overall value and utility of the network. - Harder to control on a larger scale - Complexity increases in IP addresses
Dual Stack	- Easy to implement - Low cost - Greatest flexibility - Already supported in all OS sand devices	- Two routing tables - Additional memory and CPU power - Two firewall sets of policies

Table 4 Summary of three methods

2.5. Pervious Works on IPV6

Even though the smooth transition between IPV4 and IPV6 has been a topic for a long time, there are few local research papers done on this topic. These research papers focused on finding the best approach to moving to IPV6 while still keeping IPV4. Local work on this subject is very rare, rare in the fact that there is only one research found while doing this research. This research paper was done by Banchalem Admasu which tries to find a suitable technology for transitioning from IPV4 to IPV6 of Ethio telecom Edge network.

Banchalem's work was on finding the best tunneling protocol that fit Ethio Telecom. She compared the different transitions methods available as well. She also tried to put forth the best method suitable for Edge to communicate over an IPV4 network. She tried to simulate and test the applicability of 6PE tunneling transition method, 6PE allows router to connect over IPV4 enabled MPLS network [9]. ISP's when performing such a transition they have to consider the service they are giving, the service they utilize and also their internal network, each having their own challenges and complications.

6PE is a good method when it comes to connecting edge router over IPV4 enabled MPLS network but 6PE doesn't cover all network type nor it was designed to do so [29]. So while Banchalem's work is a big step in the transitioning process but her work only cover edge routers and their communication over MPLS network. This will leave a gap from the customer side or client side of Ethio Telecom connection. The CPE's connections the core network of Ethio Telecom has been ignored on her work.

The various tunneling methods used in different networks were proposed by these researchers along with a comparison to the fully migrated Network. The results found suggest that a fully migrated network performs better in speed and coherent communication between devices. Current papers suggested that full migration is yet to come. This is due to the size of the internet, how each device on the internet are connected and the different device types and the internal protocol utilized for connection within and outside of the net.

Y. Cui [30] proposed a framework for transitioning of IPV4 based network to IPV6. The framework proposed works in encapsulating and de encapsulating the network data flow. The algorithm which was used in this framework was called "Flow-based Forwarding". The

algorithm encapsulation process happened while data is being transferred by allowing a controller to seat between the nodes that needed to communicate.

Wang Xiaonan and Zhong Shan also wrote about finding a framework that could solve routing problems in the wireless sensor network. These types of networks are becoming popular and one of the reasons these networks were designed was to have them running with very low power consumption and relay data easily. These networks are similar to wireless ad-hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly sometimes they are called dust networks [31]. They proposed a framework that could support these kinds of networks and also evaluated the framework proposed in regards to performance and packet loss.

R. Gilligan al. [19] Studied the Transition Mechanisms for IPv6 Hosts and Routers and proposed a DE encapsulation algorithm. This algorithm was then standardized by IETF and become an RFC standard 2893 on August 2000. The algorithm takes in an IPV4 request and encapsulate it in a way that IPV6 enable device could see it as a request coming from an IPV6 host. This study opened up a lot of door for the framework that was proposed by Y. Cui.

The other major concept rarely observed by most papers is the concept of Network Address Translation (NAT). NAT is the one entity that let IPV4 exist up to this day. The other way of tunneling is using NAT which allows translation on both sides in creating or modifying bindings or session state while performing the translation. The translation of this type of network is not done symmetric or one to one mapping because of the address space difference between the protocols [1].

The new version of Internet protocol IPv6 has been treated as an issue in aspects of transition mechanisms, co-existing with the old version of Internet Protocol and the changes it brought along when deployed in a network. Different case studies, as well as researches, have been conducted in the area.

Dutta and Singh [32] studied the sustainability of IPv4 to IPv6 transition with empirical evaluation with two transition mechanisms over a local area network, namely dual stack and tunneling. They performed the evaluations over testbeds using throughput analysis and latency analysis. Tests were performed using the GNS3 program run on a reliable ICMPv6 Internet

layer. The results obtained showed that Dual Stack mechanism was found to have lower latency in all of the packet size tests. The consistency of latency was also found to be better in comparison to Tunnel mechanism but also Tunnel mechanism was found to have lower throughout values than Dual Stack. The results also showed that no significant deviations were found in CPU usage for both Dual Stack and Tunnel mechanisms though it was expected that Tunnel mechanism would have slightly higher CPU usage. The authors didn't address other transition mechanisms and proposed QoS over IP-based networks could be done as future work.

Bali [10] discussed IPV4 and IPV6 both manual and automatic transition strategies. The author also compared the performances to show how these transition strategies affect network behavior using interviews and concluded that native Dual-Stack is the technology that companies should consider for their deployment. It keeps both IPv4 and IPv6 running at the same time. When the network is fully transitioned to IPv6, operators can stop supporting IPv4.

Shah [33] evaluated three most commonly used transition mechanisms, namely Dual-Stack, Automatic 6to4 Tunneling and Manual 6in4 Tunneling using TCP delay, Link Throughput and Response Time as the key performance metrics. The result shows that using automatic tunnels (6to4) outperforms Dual-Stack and Manual 6in4 Tunneling. The author compared also the result with the native IPv6 environment. Results have shown that IPv6 only network produces a higher throughput and provides a minimum delay compared to transitioning networks. This also means that IPv6 has faster packet processing and forwarding capability than transitioning networks. The worst performance is shown by manual tunneling and Dual-Stack scenarios.

Savita and Monalisa [34] study different transition strategies like Dual-stack, Manual Tunnel, Generic Routing Encapsulation (GRE), Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) and 6to4 tunnel using Round-trip-time (RTT), Jitter and throughput as the key performance metrics for network with address allocation and router configuration with Open Shortest Path First (OSPF) routing protocol. The result shows that automatic tunnels (6to4 and ISATAP) outperform manual tunnels. They recommend using automatic tunnels for the applications which are sensitive to jitter, throughout and RTT.

Albkerat and Issac [7] examined the performance of five different network topologies which are IPv4, IPv6, Dual-Stack, 6to4 tunnel, and manual tunnel. To provide appropriate results, the

network performance is analyzed across various mechanisms. More delay is observed with 6to4 and manual tunnels since the packets are not transferred directly in comparison to Dual-Stack which shows less delay. Four different network simulations are examined with three dissimilar data rates: 1, 2 and 3 Mbps. The obtained results show that pure IPv6 throughput is higher than the others. Manual tunneling gives better throughput than 6to4 up to 5 Mbps.

Chen and Zhang [35] studied the design of Three-dimensional Interchange Network Based on IPv4/IPv6 Network. They have experimented with several existing and new IPv4/IPv6 interchange technology, combined with the actual situation of the campus network. This system puts forward mixed network and IPv6 network communication rapid solution. The scheme has run IPv6 speed quickly, with low investment. As a result, they have concluded that the schema is an important mode of the next generation of Internet development process.

Arafatet al. [36] Analyzed the performance of routing protocols in dual stack networks using GNS3 and wire shark simulators. After the experiment, it is found that a minor degradation within the throughput of the TCP, delay jitter, a lower packet loss rate, and a rather longer round-trip time occurred in a reallarge-scaledual-stack network. So they concluded that dual stack is the better technique to migrate to IPv6 network in comparison to tunneling and NAT techniques.

Ram et al. [37] investigated Service Provider IPv4 to IPv6 Network Migration Strategies. They examined the network transition steps after highlighting the migration strategies for Service Providers (SP) with different transition technologies. They have also explained different scenarios for the transition and discussed each scenario briefly. After the analysis, a strategic plan for migration to next generation to IPv6 for service providers is recommended which elaborates the business continuity plan with a smooth transitioning approach to IPv6 operable network by giving a broad idea to those voice and data service providers who are in the beginning stage of their network migration to IPv6.

Mirwais et al. [38] investigated the transition scenarios of IPv6 Migration within a Campus Network. They designed and implemented an IPv6 test-bed network, and prepared guidelines for smooth migration from IPv4 to IPv6. They also checked the physical connectivity of the IPv6 test-bed network with PTM and ISP. The test was performed by pinging both the PTM IPv6

router and the ISP IPv6 router. The results showed that the network configuration was replying properly with no packet loss.

Additionally, the bandwidth speed of the existing IPv6 Internet was tested and they realized a transfer rate consistent with available IPv6 throughput. Finally, they concluded that their step-by-step guidelines should be considered when extending the current IPv6 test-bed network in the future.

Lalitha [29] evaluated and explained the IPv4 to IPv6 Network Migration and Coexistence techniques including security threats and performance evaluation. To calculate the performance of the IPv4 and IPv6 protocols, all consideration has been made over bandwidth utilization, delay, throughput, and round trip time performance metrics. Different procedures have been adopted to calculate the performance of these protocol stacks. All the experiments are conducted within 60 seconds interval. From the experiment, they have concluded that bandwidth utilization is comparatively better in IPv6 than IPv4. Delay is less in IPv6 than IPv4. IPv6 will have better performance. However, its migration is not easy since it involves lots of cost hence replacement should be gradual.

Che and Lewis [39] evaluated the current deployment and migration status of IPv6 around the world as well as the reasons for the slow rate of progress, including the debate surrounding the demand for IPv6 technology. The issues relating to IPv4 to IPv6 migration are addressed and solutions are proposed along with decision-making guidelines. But the authors did not include IPv6's contribution to wireless and mobile networks. The authors focused on IPv6s deployment in Internet backbone and enterprise networks. Their findings aim to evaluate the needs and requirements of IPv6 in order to ascertain the extent to which it can be made commonplace. The authors briefly discussed and compared the pros and cons of IPv6 migration, different transition approaches, and different tunneling mechanisms. They used OPNET Modeler as a tool for performance evaluations.

Finally, the authors concluded that the migration to IPv6 is a necessity in the long term, but IPv6 is not just about IP address space, there are also some other significant advantages. They also stated that IPv6 will provide the entire Internet community with clear benefits, which will eventually become the mainstream.

Stevens et al. [40] experimented with the deployment of service aware access networks through IPv6 for some selected broadband access topologies. The authors introduced and evaluated an efficient IPv6 subnetting scheme, minimizing routing tables through hierarchical addressing. A solution for forcing non-local traffic to the correct ISP edge, in a multi-ISP environment was also another evaluated schema by the authors. For a functional evaluation of the data plane architecture presented, the authors used a small scale access network low-risk migration using legacy aggregation equipment which was constructed using common PC hardware running Linux. As a result of the conducted tests and evaluation results, the authors concluded that an IPv6 data plane could be used as the cornerstone of a future service-oriented access network, providing tools to cope with the issues in access networks. The authors also indicated that besides the data plane, operational access networks need an accurate Authentication, Authorization, and Accounting (AAA) scheme. Another concluding remark done by the authors is that a converged access network needs an adequate end-to-end QoS architecture, for which IPv6 can provide the necessary building blocks.

Sumara et al. [41] surveyed the theoretical concepts of IPv6 and also focus on IPv6 address format, routing and the three mechanisms of migration from IPv4 to IPv6 network: Dual Stack, Translation and Tunneling using network simulator as packet tracer. The researchers conducted Connectivity test successfully between IPv4 and IPv6 networks. Accordingly, they concluded that all three mechanisms are good according to the scope of the network; each transition mechanism can be beneficial depending on the situation of a network. The Dual Stack mechanism is easier to implement at the initial stage of migration from IPv4 to IPv6 but devices must support both addressing protocols (IPv4 and IPv6), which makes the routing tables to increase considerably and this routing takes longer times. The transition mechanism is a good choice when IPv4 only network wants to communicate with IPv6 only network. On the other side, the tunneling transition mechanism is chosen when end networks are IPv6 and intermediate networks are IPv4.

Hossain et al. [42]experimented with the three mechanisms of IPv4 to IPv6 transition by deploying and analyzing all the three. The researchers have found that the three mechanisms have distinct advantages and features with some disadvantages. The simulation results show that if latency, throughput, and packet loss are considered then the tunneling method is the best

choice while the NAT-PT is the worst. But the tunneling method has some security issues that will be solved by IPsec (IP security). So the researchers recommended using tunneling mode with IPSec for the transition purpose.

They have also explained that due to the limitation of Packet Tracer, their comparisons were also limited to few application layer services and also limited to the Cisco devices only.

Mohamed et al. [43] have evaluated the delay, packet loss and throughput performance on simulation and analytical methods. The network topology was configured in three scenarios as IPv4, IPv6, and tunnel (6to4). They have done statistical analysis to provide suitable results and to show that the network's performance varied and the throughputs of the three network simulations were analyzed. The researchers used The Optimized Network Engineering Tools (OPNET) Modeler as a simulator tool. Delay, throughput, and packet loss were considered as performance metrics in this research work. Results obtained showed that in 6to4 the delay is higher than IPv4 because the packets are not transferred directly. Regarding throughput, the results showed that IPv6 has high throughput compared to tunneling and IPv4 and finally in the results, it is shown that IPv6 has high packet loss compared to tunneling and IPv4.

Generally, all the works reviewed focused on the transition scenarios and how it can be implemented. One of the articles overviewed the implementation of the transitions mechanisms on ISPs and another article sets a campus network to deploy the mechanisms to test the performances. There is also a large area network case review but none of the articles were done on a specific ISP. In this thesis, the transition scenarios are supposed to be implemented on Ethio telecom which is the only service provider in Ethiopia. Deploying the transition mechanisms throughout Ethio telecom network requires analyzing the connectivity and protocols used in the existing network. Apart from that, it is mandatory to conduct tests on the proposed transition mechanisms in order to suggest which one is more suitable for Ethio telecom infrastructure and service delivery.

In the research works reviewed above, there is no pure IPv6 deployment scenario yet. The same is true for Ethio telecoms case also. By this time of the transition is difficult to have a fully IPv6 only network. Since all the web is not fully IPv6 enabled there will always be an interaction with only IPv4 enabled network elements but it is also not easy for an ISP to transit to fully IPv6 the

only network in terms of resource, infrastructure, skill as well as time.

Author	Topic and Year of Publication	Research Questions	Objectives	Methodologies	Research Gaps	Findings	Contribution
Banchalem Admasu	IPV4 to IPV6 Transition Ethio Tele (2017)	• How can we smoothly transfer to IPV6	Design, test and Evaluate the technical requirement for transition to IPV6	Site Survey and Interview for data collection, Design Implementation and test for requirement fulfillment	The author tried to address a full transition and only assessed base configuration change.	Found out that 6PE is can be an efficient way of transition to IPV6.	Found the gaps of the current infrastructure of the ISP.
Y. Cui	Unified IPv6 Transition Framework With Flow-based Forwarding (2014)	• Creating a framework for transition to IPV6.	Design and Evaluate a framework for transitioning	Design Science	Full conversion of a network was considered and also old CPE were ignored.	Designed a framework	Contributed to the RFC standard stack for IPV6 transitioning framework.
R. Gilligan al.	*IPv6 Transition Mechanisms (2000)*	• Creating an algorithm for encapsulation and de encapsulation of network flow based data	Create and algorithm	Design Science	Only restricted to algorithm design	Created a flow based algorithm for transitioning of IPV4 networks	Their algorithm was adapted by IETF and became an RFC standard.
Wang Xiaonan and Zhong Shan	A Routing Scheme for IPv6-Based All-IP	What are the factors affecting routing scheme's performance	The paper proposes a routing	Literature and Experiment	Finding the best routing protocol	Results show the correctness	• IPv6 address structure and the IPv6

	Wireless Sensor Networks (2012)	parameters including routing power consumption and delay.	scheme for IPv6-based all-IP wireless sensor networks.		schema.	and efficiency of the selected scheme.	address auto-configuration algorithm for all-IP WSN, • proposes a routing algorithm in the link layer for all-IP WSN, • the IPv6 stack performing the proposed routing algorithm is optimized
C. Bouras P. Ganos and A. Karaliotas	The deployment of IPv6 in an IPv4 world and transition strategies (2003)	transition mechanisms that can be deployed in order to facilitate the transition Process to the new version of the IP protocol.	Finding the best transition strategies for the IPV4 based networks	Literature and Experiment	The paper mostly discuss about small and medium networks while ISP side is not that much studied in depth.	Proposing the best mechanisms for transition in regards to dual-stack and tunneling	• Provided to room for further research • Mixture mechanisms and their effect in different special needs, architectures and technologies that are deployed in each network.
Nejc ŠKOBERNE And Mojca CIGLARIČ	Practical Evaluation of Stateful NAT64/DNS64 Translation (2011)	1. NAT64/DNS64 usability in the real world 2. Find out how Current Network protocols traverse Ecdysis, the first open source stateful NAT64 and DNS64	Evaluate and find protocols, among 18 of them HTTP, RDP, MSNP, and IMAP, and	Literature and Experiment	External network adaptation is not discussed.	NAT64/DNS 64 translation might not provide an experience comparable to native	Opened a door for the NAT64/DNS64 research. They have also put for different way of analyzing IPV6-IPV4 translation.

		implementation.	Discuss the shortcomings of such translations that might not be Apparent at first sight.			IPv6- or IPv4-only connectivity, especially since VoIP and IM applications are extensively used in home environments.	
D.Shalini Punithavathani	IPv4/IPv6 Transition Mechanisms	What factors affect the performance of the various tunneling transition mechanisms used in different networks	Analyzing different accepts of IPv4 – IPV6 transition Performa in regards to latency, Throughput and loss rate	Literature and Experiment	Only the performance loss side of the transition is studied while there are other factor that could have been considered, like management of the new network, communication of external network with the new network,	The 6to4-tunnel mechanism will be first choice because address allocation is simple and only one tunnel endpoint must to be configured.	How we can minimize the performance loss in transition of IPV4-IPV6

					vendor specific products and many more.		
Jivika Govil , Jivesh Govil , Navkeerat Kaur, Harkeerat Kaur	An Examination of IPv4 and IPv6 Networks : Constraints and Various Transition Mechanisms	What are the constraints, various techniques and standards require for high level compatibility, smooth transition and interoperation between IPv4 and IPv6.	Show how each transition mechanism will affect the transition process of IPv4 to IPV6	Literature and Experiment		Each Transition Mechanisms set out by the IETF has their own effect in performanc e in different networks. And also IPv6 solves internet scaling challenges, provides flexible transition mechanisms for the current internet, and meets the needs of such new markets as mobile.	Put forth the factors that affect transition or performance of networks. Also opened up a path for future works.
Yao-Chung Chang, Reen-	Performance Investigation of	What are the performance factors	Find out which	Literature and Experiment	Did not consider the	Different mechanisms	Cleared the confusions of

Cheng Wang, Han-Chieh Chao, Jiann-Liang Chen	IPv4/IPv6 Transition Mechanisms (2014)	when moving from IPV4 network to IPV6 network or vice versa	performance factors are affected when using different IETF setout Transition Mechanisms		duality effect that is when both protocols run on the same network.	have different advantages and disadvantages and may be appropriate for different transition scenarios.	when to use which Transition Mechanisms
Béla Almási, Szabolcs Szilágyi	Investigating the Performance of the MPT Multipath Communication Library in IPv4 and IPv6 (2016)	What are Network layer solution for using MPTCP	Show the MPT communication library's working mechanism and detailed numerical examples to show the MPT library aggregates the paths' throughput in IPv4 and IPv6 environments. To	Literature and Experiment		The MPT multipath environment can successfully aggregate the physical paths throughput capacity.	Demonstrated the effective throughput aggregation property of The MPT library in IPv6 and in mixed environments.

			investigate the throughput performance of the MPT tool using IPv4, IPv6 and mixed network environments.				
So this research tries to fill the gap on the point that when considering transitioning in ISP, the CPE core network the Core network operations are over seen. So this research will try to include the CPE's and core network in the framework being proposed.							

Chapter summary

After reviewing various literatures related with the study the review have found most of the research done consider transitioning to IPV6 totally, which show there is a gap in finding middle ground for the current IPV4 network and current services running on IPV4. Another gap found from the review is while evaluating performance the duality is missed and each protocol is judge with in a separate network of its own. So this research will try to put forth a framework that will help if finding a middle ground or a network that could run both protocols till the current IPV4 network completely transitions. The review also helped in deciding the methodology to be used in this research which is Design Science.

Chapter Three

3. Research Methods and Design

3.1. Introduction

This chapter explains the research methodologies used. The research methodologies which are used for this research are Design science and Qualitative research. This chapter also explains the different approaches and views in which the methodology is used as well why the specific methodology has been chosen to carry out the research.

The main methodology that has been used in the research is Design Science. Design Science research is a set of synthetic and analytical techniques and perspectives (complementing positivist, interpretive, and critical perspectives) for performing research in IS. Design science research involves two primary activities to improve and understand the behavior of aspects of Information Systems: 1. the creation of new knowledge through the design of novel or innovative artifacts (things or processes) and 2.the analysis of the artifact's use and/or performance with reflection and abstraction. The artifacts created in the design science research process include, but are not limited to, algorithms, human/computer interfaces, and system design methodologies or languages. [44]

The other methodology which has been utilized in this research is qualitative research. The research will follow different methods that will help to attain the goal set out in the objective.

3.2. Methodology

This study was conducted using the Design Science research methodology to address its general and specific objectives. It is a design science based research study that will try to find a framework that will best suit the ways in transitioning of IPV4 to IPV6 while still keeping IPV4 for networks that might not yet support IPV6. The study tested the proposed path using data collected from the test environment and simulating it on automatically generated network traffic. A Design science is chosen as a methodology because it takes in to account the activity, event or problem that contains a real or hypothetical situation and includes the complexities you would encounter in the workplace. So this will help to see how the complexities of real life influence the decisions or solution proposed [45].

3.3. Design Science

Design science researchers can be found in many disciplines and fields, notably Engineering and Computer Science, and there are a variety of approaches, methods, and techniques used in design science research. Within the field of Information Systems, an increasing number of observers are calling for a return to an exploration of the "IT" that underlies all IS research thus underlining the need for IS design science research [44].

Design science research is highly used in disciplines that are concerned with the creation of artifacts. Many Information system researchers pioneered design science but little Design science researches were conducted in more than a decades. Lack of a methodology to serve as a commonly accepted framework for DS research and of template for its presentation may have contributed to its slow adoption. The design science research methodology (DSRM) incorporates principles, practices, and procedures required to carry out such research and should meet three objectives: it is consistent with prior literature, it provides a nominal process model for doing DS research, and it provides a mental model for presenting and evaluating DS research in Information Systems. The more widely accepted and also used design science process includes six steps: problem identification and motivation, the definition of the objectives for a solution, design and development, demonstration, evaluation, and communication [44].

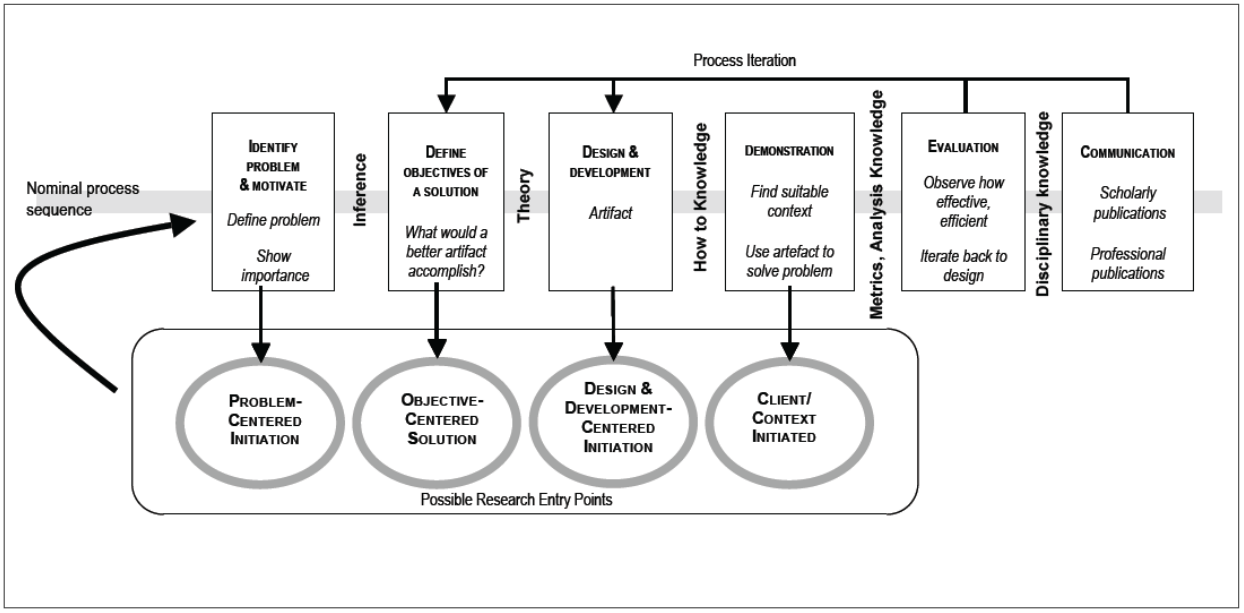

Figure 15Design Science Research Methodology (DSRM) Process Model [44]

3.3.1. Problem Identification and Motivation

3.3.1.1. Motivation

The main motivation for doing this research is that IPV6 is untapped or highly overseen technology in Ethiopia. IPV6 has been left alone in Ethiopia for some time now while other countries have been trying to include and use it. The way the world is going in the communication roam shows that the need to shift or use IPV6 partiality is inevitable. If the time is this close to using it then we should know at least the challenges and how to overcome them when the time arrives.

The other reason which goes hand in hand with the above is that the local researches done on IPV6 is very low to the point that only one paper is found at Addis Ababa University. This shows that the topic is very much open and still has a lot of points and problem to be addressed which can't be covered with one or two researchers.

3.3.1.2. Problem Identification

The initial step in design science is problem identification. Here is where the problem or in this case challenges will be identified and put forth. Ethio telecom being the only ISP for the country the services it gives needs to be up-to-date and maintain the standards that is required. IPV6 is the new path that is out there that ISP all over the world are moving towards [10]. This moving or transitioning of the Internet protocol will affect Ethio telecom and having to transition immediately will be a challenge. These challenges like routing, marinating duality till all IPV4 services are transitioned and the performance factor of having both protocols to run in the same network could have a major effect in the way Ethio telecom is providing its service. After the problems are clearly identified this paper showed the specific importance of the work to provide a solution for the challenges. This research will show a framework that can effectively and efficiently provide a way to minimize the challenge. In order to come up with the solution, the researcher followed qualitative data collection instruments.

3.4. Research Design

"RD is the entire process of research from conceptualizing a problem by writing research questions, and on to data collection, analysis, interpretation, and report writing." [45] Having a research design helps in having a clear path or view in the collection and analysis of data that will have a directed aim to generalize the findings and proposed solutions. All in all, it will help in providing steps or activities to take while collecting relevant data and the techniques to use while doing so. This will intern let the research have direction and consistency.

The research was conducted in steps that will let it have the most and best outcome possible. First, an extensive literature review of related work was done to show the lacking of transition mechanisms for the IP Versions. After finding the points or the facts that where lucking this part of the step was complete.

Next, the study is proceeded in using a case study on the ISP of Ethiopia (Ethio Telecom) because a case study will let the researcher know how to do analyses and describe each of the components related to the work. Then a survey was conducted using a written questionnaire adapted from previously validated instruments of similar work. In addition, the target sample of the study will be identified and a questioner will be distributed using an online platform. Unstructured interview with NOC and addressing technical personals will also be conducted.

Finally, the research will choose the data analysis tools and methods and the proposed transition method will be tested using the tools and techniques based on the generated network traffic on how it will react to each scenario. After choosing the appropriate tools, the collected data and analyzed data will be used to test the validity of the chosen transition method. This section will be completed by a series of justifiable interpretation of the findings and identification of future research prospects.

3.5. Data Collection

3.5.1. Questionnaire & Interview

Since this research is on networking aspects of ICT industry questionnaire and Interview are critical in doing research of this type. To fully understand what is there in the current set up to figure out what challenges may arise to do it. The interview will give a deep insight into what

lies in the specific networks that are being assessed and considered for the research. In this case security of the Ethio telecom has prevented from doing any site assessment and deep inspection of the network so using interview helped in getting necessary data that could have been retrieved through site assessment. The interview was designed based on an RFC standard that was used to collect data in regards to IPV6 in ISP. [46]

The questionnaire adapted has been modified to include question that were left out or were not included in the original document. The modification was done to include factor which where unique to Ethio telecom and also to cover the expertise part. The questionnaire was distributed for the selected samples using google docs. The questionnaire used has been attached in the Annex 2.

3.5.2. Document Analysis

Requests For Comments (RFCs) is a document system invented by Steve Crocken in 1969 to keep the record as well as improve technology being used on the ARPA net. An RFC describes a research or applications on networking technology or defines a new one [15].

RFC's are well refined and assessed by a group of engineers for that specific which the RFC is published for. RFC's have a unique number for each publication and RFC's are not modified their modification is published as another RFC, so this makes them be a good reference for technical information. This research will be using RFC to analyze and provide an explanation to technical data. Besides RFC the research also consults Journal paper, thesis done on the specific field, books and white papers from a trusted site (Cisco, Microsoft, and etc…).

3.5.3. Study Sample

The study has selected to use purposive sampling in order to collect data. This sampling was selected because it enables the researcher to collected targeted data or data collection from experts who are in direct relation with the topic being studied. Purposive sampling enables a researcher to use judgment to select samples that could enable to answer questions and to meet the objectives. So, this sampling was selected to gather appropriate data from 2 NOC and 3 IP department staffs of Ethio Telecom. The study also included devices which were deployed in Companies using ADSL or copper-based internet, and companies using the Fiber Based internet.

The result set from the questionnaire which was collected from the above sample shows that IPV6 is rarely used or considered and most of the services which are currently running are using IPV4. It's also observed that, most of the CPE devices doesn't support IPV6 specifically the ones which are used in providing ADSL services to customers or subscribers. There is also a gap in the current status of Ethio telecom in regards to IPV4 address allocation rate and time of depilation readiness.

In question reading the challenges that they may face while transitioning to IPV6 most of the answers reflected that there may be Lack of skills and expertise and Legacy systems which are running currently. Also the other major challenged that could be face during transition was the issue with current devices which are not able to support IPV6 majorly the CPE devices. Because these CPE devices are distributed to customers and changing all these devices could bear a major problem.

3.5.4. Study Instruments

Existing documents on the infrastructure of Ethio Telecom is used as one of the instruments. Ethio Telecom's website is one of the sources of the documents that are used for this research. The interview is also the other data collecting method along with Google forms. The other instruments which were used are NS-3, Edraw Max and GNS3 to implement, replicate, simulate and test the data that has been collected.

3.6. Define the Objective of the Solution

This is the second step in the design science research process model. In this stage the study aims to identify the requirements for developing a framework from transitioning IPV4 to IPV6. It tries to provide a way to show how the framework could be useful and minimize the challenges after identifying and pre-evaluating their relevance. Qualitative data is used to show how the proposed framework is expected to support solutions to the challenges that were not previously addressed or considered in other researches. After data collection, the data will be narrated and summarized. This involves analysis of the data and finally data interpretation. Qualitative data analysis method is used to analyze the data collected from interview and document analysis.

The analysis technique used in this study is thematic coding analysis technique in which the result of the data collected will be grouped based on the current categories of transition methods.

Finally generalization is made and presented accordingly for the qualitative data by way of narrating and interpreting the situations.

3.7. Design and Development

A feasible artifact is developed and implemented in this phase. A framework is a model artifact that provides a broad overview or skeleton of interlinked items which helps as a guide to achieve the specific objective. After all the above stages are completed the appropriate and suitable framework was developed using software tool Edraw-Max. The framework is developed based on RFC standards of pervious works and made a few modification to adapt the current challenges. Edraw Max was selected because of its rich features, adaptability and easy of deployment. The developed framework shows each component with its functionalities to solve the identified challenges of Ethio telecom in transitioning to IPV6. Each of the component of the framework is discussed in detail in the consecutive chapters. The developed migration framework is designed to Ethio Telecom or considering ISP but can be used for big organization with massive network infrastructure.

3.8. Demonstration

This is a phase where the researcher shows the artifact or framework developed to tackle the challenges of moving to IPV6. Simulation or experimental device will be used to farther prove the framework. GNS3 and Network simulator are chosen as a demonstration tool for this study. GNS3 was chosen because of its ability to simulate a real device router and its ability to run image of a device. This gives a better simulation because the researcher is able to get result as close possible as he/she would get on an actual device.

The other points that were demonstrated are the configuration and how the framework can easily be implemented. After completion of the demonstration the researcher shows that the existing network service are still in function and measuring the performance of the transitioned network. This is done by using both GUI based packet collection application as well as command line based application like CMD, putty and Wireshark.

All of the configuration, performance testing and application outputs can be found in Annex 3.

3.9. Evaluation

On this section the research tried to measure and evaluate how well the framework helps in reducing the challenges of moving to IPV6. Evaluation proves how the proposed framework is effective and efficient to solve the challenges of ISP in this case Ethio telecom. This activity can be done by comparing the objectives of a solution to actual observed results from the use of the framework. Since the framework is not being used in actual environment a simulation will be used. The simulation will have an IPV4 network and a corresponding IPV6 network. The IPV6 network will be a transitioned network of the IPV4 using the framework. Then using these networks the framework was evaluated in regards to the performance change and making sure that the existing services are still active and running.

Chapter Summary

All in all this chapter put forth the main methodology which was used that is Design science research methodology. This methodology was selected because of it agility when it comes to framework creation. Purposive sampling was used to collect data from the Ethio telecom through Questionnaires.

The next chapter will cover the current Ethio telecom network layout and the major services running on top of it.

Chapter Four

4. Ethio Telecom Current Network

4.1. Introduction

Ethio telecom is a sole service provider for voice, Internet and other data services for subscribers in Ethiopia. To keep providing a variety of services, Ethio telecom has initiated different projects to enhance and upgrade the services it provides. The general view of current network topology of Ethio telecom is shown in Figure 4. The figure shows Ethio telecom's network consists of access, aggregate and core layers before reaching out to the Internet. Each of these network having their own configuration and security in place. Each of these layers communicates through routers that act like a border for the layers and also help in providing visibility where it's needed. There is an explanation below of each layer of networks discussed with each one's specific architecture.

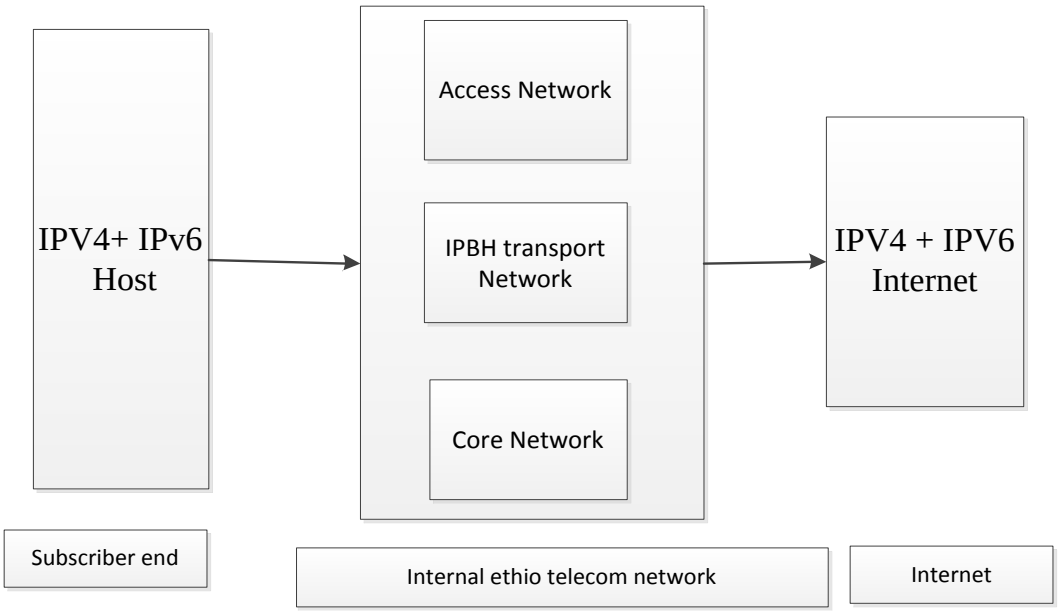

Figure 16 Ethio Telecom Current Network [9]

4.2. Access Network

This network segment provides access to broadband services and aggregates to subscribers of Ethio telecom. The subscriber traffic is handed over to the Service Provider at Layer 2 or 3. This layer is where layer two and layer three Switches, Digital Subscriber Line Access Multiplexer (DSLAM)'s, Multiservice Access Nodes (MSANs) and other access devices of any type will be placed here as well. It is the layer where subscriber's customer premises equipment (CPE) will be connected to as well. The devices in this layer have different nature, some of the major devices are mentioned below.

- ✓ DSLAM is a network device; usually, it receives signals from multiple customer DSL connections and puts the signals on high-speed backbone line using multiplexing techniques. DSLAM multiplexers connect DSL lines with some combination of Asynchronous Transfer Mode (ATM) and Frame Relay networks [9]. This is the main connection gateway for ADSL users of Ethio telecom.

- ✓ MSAN (multiservice access node) is an access layer equipment which uses Ethernet (or ATM) switching to forward traffic. It forwards all subscriber traffic upstream to an edge router that acts as the centralized control point and prevents direct subscriber-to-subscriber communication [9].

- ✓ MSAG is also another access device at the edge layer in the Soft Switch system. It performs conversion and processing of the access media stream. Based on Soft Switch standard adaptation layer protocol and transport layer protocol, MSAG enables service to access such as analog telephone set and broadband services. MSAG is used to connect the analog interface subscribers directly to the IP network, and performing voice/fax conversion between the subscriber side and the IP network side [9].

- ✓ Optical Line Terminal (OLT) is equipment where fiber optic cable will be terminated in central locations. It assigns time slots upstream. Optical Network Terminal (ONT) is a terminal device at customer premises equipment. This is issued by Ethio telecom for fiber

based internet users or subscribers. Most of these devices are used as a termination point for the fiber connection that is coming from Ethio Telecom and the start of the customer premises. The fiber which are terminated here are usually connected to a media converter or to any fiber enabled device. [9]

.

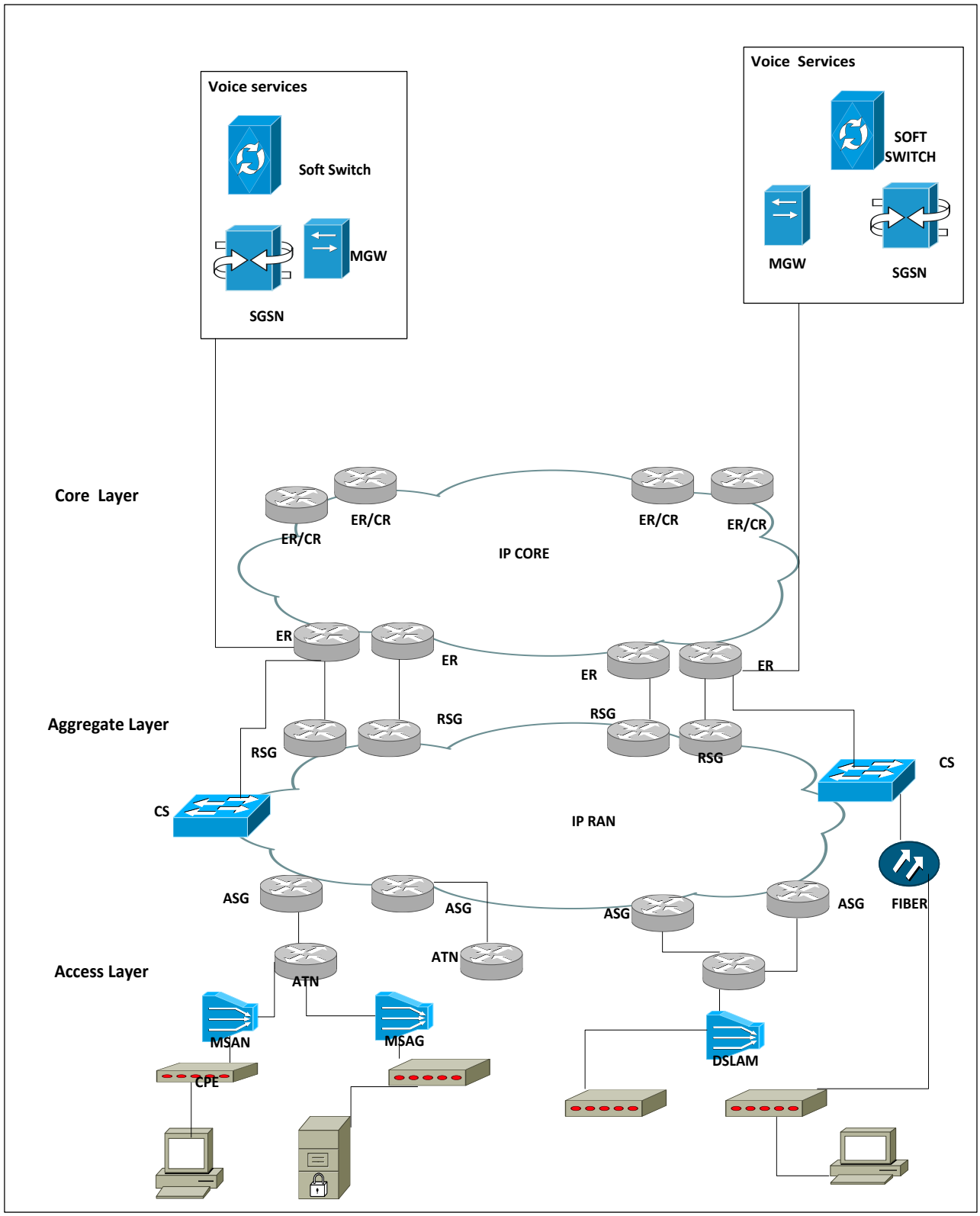

Figure 17 Current Ethio telecom network [9]

4.3. Aggregate Layer (IP Backhaul)

This is an IP based transport network between the access network and the core network. This network segment is a Radio Access Network which is used for transport as an IP aware backhaul transport network which consists of three layers of devices. Cell Site Gateways (CSGs), Aggregator site gateways (ASGs) and Radio Site Gateways (RSGs) are the three parts of this transport network segment. The CSGs are part of the access network, whereas the ASG and RSGs belong to the aggregate layer. In all parts of these layers, high capacity routers and layer three switches are deployed.

IP-RAN architecture is introduced into an existing Time Division Multiplex (TDM) based network environment without disrupting or redesigning the network. All radio nodes natively support IP over T1/E1 and Ethernet interfaces. As the network grows further, Ethio telecom can aggregate T1/E1 lines and leverage lower-cost optical transport. [9]

4.4. Core Network

This network provides Intranet and Internet IP connectivity for the subscribers. It is a layer where all the traffic converges and routed to the backbone and gateway routers. Traffic from all parts of the network and all types of services come to this layer of the network to be routed within and out of the Ethio telecom network. It signifies the highly functional communication facilities that interconnect primary nodes. The core network also delivers a route to exchange information among various sub-networks. [9]

This layer also functions as a backbone network. It has a set of pathways to which other large networks connect for long distance communication. Various networking technologies work together as connection points or nodes and are connected by different mediums for transporting data like optical fiber, traditional copper and even wireless technology like microwave and satellites.

When doing the transitioning the current network layout needs to be considered, how each of the above layers communicate and well as the connection points to each other. So from Figure 5 we can see that there are three layers are connected with Edge or border routers. These router are

currently running IPV4 with the ability to support IPV6. Even though these router support IPV6 we can't up and convert them because of the CPE and inter connection devices which are not supporting IPV6.

So based on these the framework which will be proposed considers the interconnection and the layout of the network. Also put forth that the conversion or transition of IPV6 should occur without affecting the current communication as well as the service running.

4.5. Internet Services by Ethio telecom

The network is just a road without the services that are running using this road. Ethio telecom provides different services to customers or subscribers. One of the major service that Ethio telecom provide is Internet access. This service is provided using Digital subscriber line (DSL), fiber to the home (FTTH), satellite and mobile broadband. They are categorized based on the characteristic of their transmission media. [9]

A summary of devices which are found from analysis from different documents of Ethio Telecom and A thesis done by Banchalem is shown below.

No	Device type	Owner /Vendor	Used in the Network as	IPv6 Compatibly
1	T8000	ZTE	Broadband access server	It supports: • IPv4/IPv6 routing protocol, • IPv4/Ipv6 multicast routing protocol, • MPLS L2/L3 VPN and IPv4-IPv6 transition technologies. • MPLS signaling protocol.

2	M6000	ZTE	Gateway router, Core router, Edge router	It supports: • IPv4/IPv6 dual-stack, • 6PE, • 6vPE, • It also supports the IPv4 and IPv6 dual protocol stack, • all the relevant migration technologies, such as the manual tunneling, auto tunneling, 6to4 tunneling and NAT-PT.
3	T160/ 164G	ZTE	Core switch	It supports Basic IPv6 capacities
4	CX600 X16/X8	Huawei	RSG	CX600 supports: • IPv6 user access, authentication, and rich NAT • Dual stack/DS-Lite, • Tunneling and translation. • It also supports Next Hop separation to optimize the IPv6 convergence time and larger IPv6 FIB to improve the scalability. All of these help to provide comprehensive solutions based on high performance for transition from IPv4 to IPv6.
5	ATN950B	Huawei	CSG	It supports basic IPv6 interface address
6	9806H	ZTE, Huawei	DSL Module	It supports basic IPv6 interface address
7	ZXA10-C300M	ZTE, Huawei	MSAN, MSAG	It supports basic IPv6 interface address

Table 5 Ethio Telecom Device List

Circle	**4G Data & Internet subscribers (in million)**	**3G Data & Internet subscribers (in million)**	**2G Data & Internet subscribers (in million)**	**Fixed broadband internet subscribers (in million)**	**Total subscribers per circle (in million)**
Addis Ababa	0.4	1.5	0.92	0.4	3.2

North and East	Not planned	1.941	2.21	132,000	4.283
South and West	Not planned	1.941	2.21	132,000	4.283
Total	-	-	-	-	11.786

Table 6 Ethio Telecom Subscriber Distribution

Chapter Summary

This chapter discussed about Ethio telecom network layout, the major services that Ethio telecom provides, how each of the layers operate and the list of devices that are currently running. This will be a major input for the next because the framework which was selected and modified was based on the current network of Ethio telecom as well as the services that are provided.

The next chapter will cover why Y. Cui's framework was selected and propose the changes to his framework.

Chapter Five

5.1 Why this Framework

Why Y, Chi's Framework? Based on the different Articles and RFC standards which have been reviewed Chi's Framework stand out because its allows us to see a full picture of the network being transitioned, with a minor modification of the framework Ethio Telecom network can be easily transitioned and also Chi's framework considers a layered network rather than consider the whole network as one. Also this framework has been designed considering ISP networks.

Based on the data collected by the questionnaire, Ethio Telecom has not started nay move to IPV6, Cui's framework which uses a flow-based packet forwarding technology allows the organization analyze and select the best transition method or use a combination of them.

5.2 The Framework

This framework makes use of the flow-based packet forwarding technology, which can simplify the implementation of both control plane and data plane operations of transition mechanisms. Having an integrated and flexible framework to implement and deploy using the above translation and tunneling mechanisms could be hard without a guide or path so the framework can benefit by reducing the cost of implementation, providing flexibility for deployment, and enabling transition mechanisms to coexist and cooperate in the common infrastructure. The framework is based on the Y. Cui of Unified IPv6 Transition Framework which was done considering the list of methods available and the fact that companies may be forced to use multiple of them.

This framework adopts a kind of flow-based packet forwarding technology, which can simplify the implementation of both control plane and data plane operations of transition mechanisms. The framework was designed to provide an integrated approach to implement the most popular transition mechanisms like NAT64, DS-Lite, Lightweight 4over6 and MAP-E. This framework helps in reducing the cost of implementing, deploying transition mechanisms, and enable these mechanisms to coexist in the common infrastructure. The common infrastructure is a keyword here since Ethio Telecom has one big network which runs all over the country and the fact that

they have not started any movement to IPV6 this kind of framework will be useful to show where and how to go about it. [30]

Currently, the framework assumes the ISP is IPV6 network and the customer is has a full IPV6 network which will connect to the ISP CPE switch. Then relayed out to the IPV6 internet through the BR switch. CPE Switch performs the flow-based packet forwarding function. It must support the software encapsulation functions. It must also support traditional NAPT44 and NAT64 translator function.

BR Switch also performs the flow-based packet forwarding function. It MUST support the software encapsulation/ decapsulation function specified in [RFC6333], [I-D.ietf-softwire-lw4over6] and [I-D.ietf-softwire-map]. Particularly, it MUST support the port-set matching for incoming IPv4 packets, which is defined in section 6.2of [I-D.ietf-softwire-lw4over6].The controller is responsible for controlling the performance of both CPE Switch and BR Switch. It must configure the forwarding rules in the flow tables maintained by the CPE Switch and BR Switch. It maintains the NAPT44 state and NAT64 state that is associated with the CPE Switch. It also maintains the NAPT44 state, MAP mapping rules, and Lightweight 4over6 binding table state that are associated with the BR Switch.

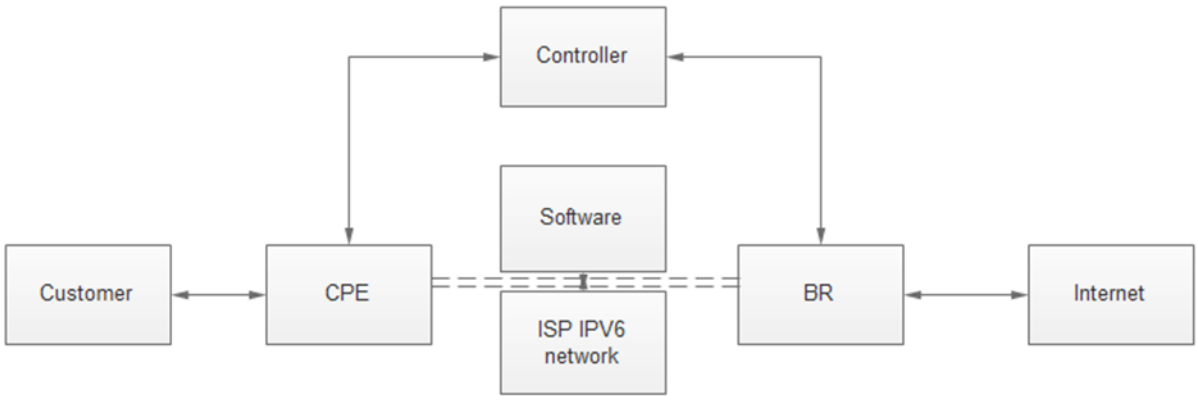

Figure 18 Unified IPv6 Transition Framework [30]

5.2.1. Control Plane Behavior

At least one software mechanism should be deployed in the system. Multiple software mechanisms can be deployed at the same time. This situation includes two cases: (1) mechanisms are implemented in different devices (e.g.DS-Lite B4 and Lightweight 4over6 LwB4 are implemented in different CPE Switches); (2) mechanisms are activated in the same devices. In the first case, Controller can distinguish the CPE Switches or BR Switches by their addresses; in the second case, CPE Switch and BR Switch can apply actions of different mechanisms to different flows according to the flow table. [30]

The end devices in the customer LAN can be provisioned with privateIPv4 addresses by a local DHCP server. They can also be provisioned with at least one global IPv6 address. CPE Switch and BR Switch MUST be provisioned with at least one IPv6address in the IPv6 ISP network. They MUST be configured with default forwarding rules by Controller. These default rules should cover actions such as forward-to-controller action and default encapsulation/ de capsulation action. Note that configuring default encapsulation/ de capsulation rules can be regarded as establishing a tunnel between CPE Switch and BR Switch if Lightweight 4over6 or MAP-E is deployed in the network. [30]

5.2.2. Data Plane Behavior

When receiving an incoming packet that doesn't have a match in the flow table (usually the initial packet of a new flow), CPE Switch and BR Switch MUST forward the packet to Controller. Controller MUST determine how to proceed the flow (e.g. whether to apply NAT/ NAT64translation and/ or softwareencapsulation/ decapsulation), and interpret the process into a set of forwarding rule configurations.

The controller then passes these configurations to CPE Switch and BR Switch. CPE Switch and BR Switch then configure their flow table according to these configurations, continue to apply the corresponding actions to the packet, and forward it to the next step. When receiving the subsequent packets of the flow, CPE Switch and BR Switch will apply the same actions to them, according to the forwarding rules in the flow table. [30]

Switch	Flow type	Matched actions	Processing
CPE	Outbound IPv4	Encapsulation	Encapsulate V6 header
		NAT44 + Encapsulation	NAT44 encapsulate V6 header
	Outbound IPv6	NAT64 + Encapsulation	NAT64 encapsulate v6 header
	Inbound IPv6	De capsulation	De capsulate V6 header
		NAT44 + De capsulation	De capsulate V6 header to NAT44
		NAT64 + De capsulation	De capsulate V6 header to NAT64
BR	Outbound IPv6	NAT44 + De capsulation	De capsulate IPv6 header NAT44
		De capsulation	De capsulate IPv6 header
	Inbound IPv4	NAT44 + Encapsulation	NAT44 to encapsulate v6 header
		Encapsulation	Encapsulate v6 header

Table 7 Auto Processing of Flows [30]

After analysis of the data on the current network of Ethio Telecom and the data collected using questionnaire and explained in the methodology Study Sample section. The following challenges are identified.

In regards to devices most of the Customer End devices don't support IPV6 specially ones which are deployed to give ADSL service to customers.

On the core network, the services which are running are still IPV4 based and since IPV6 is not backward compatible these services running on IPV4 will need to be considered while transitioning. Also communication from different IP based applications need to be considered

against IPV6 Speed and performance while transitioning. Modification and downtime planning are also challenges that could affect the transition.

Expertise is another challenge that could be faced while doing the transitioning, IPV6 is new path it has its own sub netting, header structure and management perks. So having a trained and fast tracked expertise on and after transitioning of the network is a must.

So based on the above challenges and by using the framework proposed by Y. Cui, the framework have been modified to suit Ethio Telecom. The major points that led to the need to modify the framework are:

- ✓ Most if not all Ethio telecom copper-based internet users have an IPV4 only CPE which has no capability to switch from and to IPV6 networks. Retracting and deploying a new ones will not only take time but could also cause a major dissatisfaction of customers. So to counteract to this issue the CPE will still be the same and if there is any customer that may want to use IPV6 in their network they could implement a dual-stack that could let them easily interface with the CPE router.
- ✓ The ISP or Ethio Telecom is still running IPV4 network for its major addressing use, so rather than converting the ISP to V6, which will take time, a lot of resource and inconsistency in the network. So have the BR to be a Dual-stack and fully support IPV6 will minimize the problem and still have a decent network flow.
- ✓ Tunneling over the ISP, most of the customers use CPE devices that don't support IPV6 and to mitigate this we can either use a software-based tunneling which will be hard to do since the devices which are currently used are outdatedand have limited processing and memory. The second option will be until all CPE's have migrated or changed to the new and improved model, is to restrict tunneling to Fiber users were their network or edge router can support dual stack.
- ✓ On the software component, we can have it listen to application layer based IPV6 calls to load off the conversion to and from IPV4.

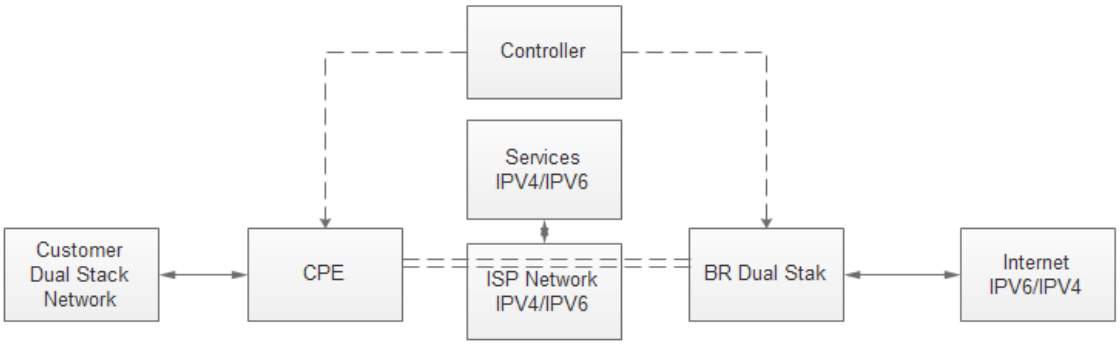

Figure 19 Proposed Framework

5.3 Modifications and Additions to the Framework

5.3.1. Customer Side of Connection

The customer side of the framework has to be changed to a Customer Dual stack network, because of the issue the Ethio telecom's most CPE devices doesn't support IPV6 and Y. Cui's framework rely's on the CPE's ability to do the translation using NAT64. But since the current CPE devices does not support this the customer side has been modified. This will reduce the need to change these CPE devices and also could save time and cost that is used to replace them. But in the meantime this will allow the customer to use IPV6 by just enabling dual stack. This way the customer could still use IPV6 and IPV6 service without having to change the CPE connecting it to the core network.

5.3.2. CPE

The CPE in the new modified framework stays as a normal CPE which could only support IPV4, but in time these devices could be changed to support IPV6.

5.3.3. Controller

The controller stays the same as the original framework, with the change to being an active participant in the network, to just being an optional part that if and when CPE's that support IPV6 are introduced in the network the controller will be responsible for controlling the performance of both CPE Switch and BR Switch. It will also configure the forwarding rules in the flow tables maintained by the CPE Switch and BR Switch. It maintains the NAPT44 state and NAT64 state that is associated with the CPE Switch. It also maintains the NAPT44 state,

MAP mapping rules, and Lightweight 4over6 binding table state that are associated with the BR Switch.

5.3.4. ISP Network

The ISP network was modified to support both IPV6 and IPV4 contrary to the original framework which only supports IPV6. This modification was made to have legacy services running on IPV4 will still continue to run till they have been replace or rolled out. And on the software part of the Core network the new framework changed the name from software to services running on IPV6/V4, because not only software are running but also other network related services could be running and as well these services could be running on either protocol.

5.3.5. Border Router

The border router was an IPV6 only router in the original framework, but since the border router communicates with the inside network, the Internet and any tunneled packets passing through the core network the BR cannot be a one protocol network or device. There is also the fact that the Internet is not an IPV4 only or IPV6 only network so in this regard the change in the naming of the inter section to Internet IPV4/IPV6.

Chapter Summary

This chapter was all about the framework that was proposed and why Y. Cui's framework was select to be modified. Also in this chapter were the proposed framework components and why the change or the modification was needed were discussed.

In next chapter will evaluate the proposed framework in regards to deployment, performance and current service continuity.

Chapter Six

Evaluation of the proposed framework

The proposed framework with no evaluation is a just a picture with a connected box. Evaluation is the systematic investigation of the merit, worth, or significance of the framework. Evaluation practice has changed dramatically new methods and approaches have been developed and it is now used for increasingly diverse projects and researches. To evaluate the above framework this research uses simulation tools to produce the existing two environment and see how the framework would help in the transition process. The tools which have been used here are Network Simulator - 3 (NS-3), GNS3, Cisco 2960 catalyst switches, and Cisco 2111X routers.

The above tools were selected because of their ability to simulate a real world device configuration and communication performance and also allow the researcher to measure the out puts. GNS3 will allow the researcher to adapt a real router configuration and also have a controlled environment to do the testing. NS-3 is also a tool that can be used to pass repetitive packet simultaneously allowing varied payload.

The GNS3 network model has been taken from an existing project done on top of Ethio telecom network, so to avoid repetition this research will adapt from that project and modify some aspects to tailor it to this paper.

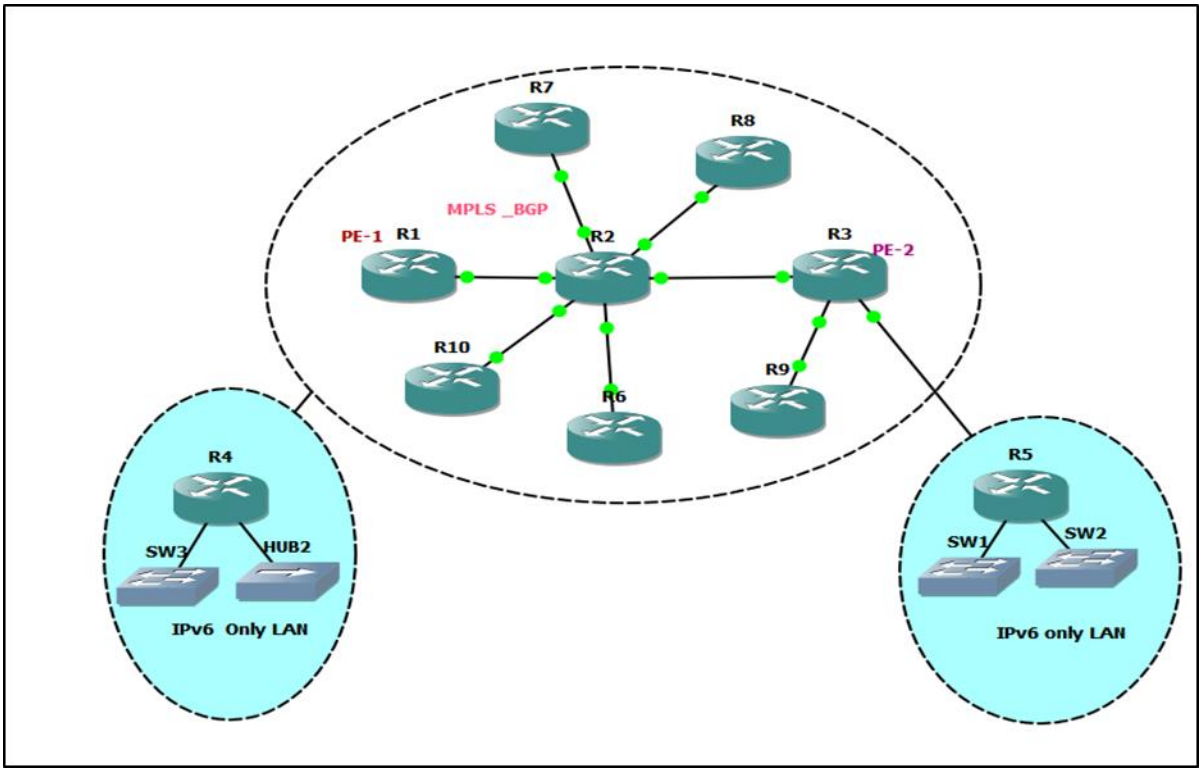

Figure 20 GNS3 Simulated network [9]

The configuration which has been done on the above simulation are discussed below.

The first one is setting up the topology with IPv4 addresses using OSPF routing and MPLS based BGP (MP-BGP) as a transport protocol. This setting enables label distribution protocols to be active and Labels will be forwarded together with routes. This is done for all routers shown in the topology as core devices.

Next is configuring IPv6 addresses on the two routers which are gateways of for two IPv6 only LANs (R4 &R5). These two routers running IPv6.

On the last network, the simulation is configuring MP-BGP on the PE routers to make label switching possible. In addition, enabling Cisco's feature Cisco Express Forwarding (CEF) enables IPv6 labels from both LANs to be learned and distributed with MP-BGP over the core routers.

OSPF routing protocol is configured to make each IPv4 router learn the route from another router within the core routers topology. All the routers created will be in the same OSFP number which simulates an IPv4 core network structure with OSPF routing protocol running in between. As Figure 20 demonstrates, routers R2, R6, R7, R8, R9, and R10 all run in IPv4 enabled network infrastructure. On the other hand, routers R1 and R3 run both IPv4 and IPv6 enabled network modes since these two are the PE (Provider End) routers which have dual stack configuration. So, R1 and R3 will be the routers that will learn all the labels from the core network they are connected to and from both IPv6 LANs.

IPv6 LAN routers R4 and R5 need to communicate with each other through the IPv4 network infrastructure. The labels from R4 should be learned and transported over the core network and reach to R5 and vice versa.

The purpose of this simulated setup is to align the framework proposed will produce an easy in transferring to IPV6 and compare the result with the previous network to see how the new network is performing.

Based on the above explanation the research simulated the framework on top of the GNS3 and modify the configuration to match the framework. To do that we are changing the right side of the network to be a dual-stack network while having both the IPV4 and IPV6 and the left to be as is while testing interchanging it to IPV4 and IPV6 to see the effect. To process the evaluation the network will be implemented or simulated one as it is and the other with the framework so as to compare the effect and see how the challenges are reduced. In Annex 4 you will find the configuration for the network routers. Below is discussed the effect of the framework in the performance of the network and services running.

To evaluate the framework as mentioned above this research used two networks one all IPV4 network while the other is the network moved using the framework. For this evaluation a selected number of service are used mainly because of time and resource available to do the test. The services selected for this test are MPLS and Routed data connection.

The first phase of the Evaluation is implementation can the framework be implemented or be used to transition the current simulated network. This has been done using GNS3 to simulate the conversion and based on the configuration seen on the below figure x from of the routers used

we can see that the routers were able to simulate dual stack and pinged each other for connection test. Showing that a transition could happen using the framework.

```
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FEC0:0:0:1::1/64
 mpls ip
!
interface FastEthernet1/1
 ip address 10.10.11.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 100
 router-id 10.10.10.1
 log-adjacency-changes
 network 10.10.10.1 0.0.0.0 area 0
 network 10.10.11.1 0.0.0.0 area 0
!
router bgp 123
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.10.10.3 remote-as 100
 neighbor 10.10.10.3 update-source Loopback0
 !
 address-family ipv6
 neighbor 10.10.10.3 activate
 neighbor 10.10.10.3 send-label
 redistribute connected
 redistribute static
 no synchronization
 exit-address-family
!
no ip http server
no ip http secure-server
!
ipv6 route FEC0:0:0:4::/64 FEC0:0:0:1::2
!
```

Figure 21 Configuration of Customer Side Router

```
ipv6 unicast-routing
ipv6 cef
mpls label protocol ldp
!
interface Loopback0
 ip address 10.10.10.3 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex half
!
interface FastEthernet1/0
 ip address 10.10.12.3 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet1/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FEC0::1/64
!
router ospf 100
 router-id 10.10.10.3
 log-adjacency-changes
 network 10.10.10.3 0.0.0.0 area 0
 network 10.10.12.3 0.0.0.0 area 0
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.10.10.1 remote-as 100
 neighbor 10.10.10.1 update-source Loopback0
 !
 address-family ipv6
 neighbor 10.10.10.1 activate
 neighbor 10.10.10.1 send-label
```

Figure 22 Configuration of BR Router

```
R5# ping ipv6 FECO:0:0:4::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FECO:0:0:4::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =48/98/128 ms
R5# traceroute ?
   WORD         Trace route to destination address or hostname
   appletalk    AppleTalk Trace
   clns                 ISO CLNS Trace
   ip           IP Trace
   ipv6         IPv6 Trace
   ipx          IPX Trace
   <cr>

R5# traceroute ipv6 FECO:0:0:4::1

Type escape sequence to abort.
Tracing the route to FECO:0:0:4::1

   1  FECO::1 68 msec 32 msec 36 msec
   2  *     *     *
   3  FECO:0:0:1::1 160 msec 108 msec 92 msec
   4  FECO:0:0:4::1 180 msec 96 msec 84 msec
R5#
```

Figure 23 Ping and Trace Route Results

After implementation a test of performance using varied payload was done on both network the following outcome was observed. This test was done on a 1000 ping by varying the payload and the average was taken for both latency and loss rate. Wireshark was used to sniff through the packet.

Full IPV4 Network					
Measure	**Payload 64**	**Payload 128**	**Payload 256**	**Payload 512**	**Payload 1024**
Latency	**1ms**	**1ms**	**1ms**	**4.23ms**	**8.32ms**
Loss Rate	**0**	**0**	**0**	**1**	**2**

Table 8 Full IPV4 Network

Framework Network					
Measure	**Payload 64**	**Payload 128**	**Payload 256**	**Payload 512**	**Payload 1024**
Latency	**1ms**	**1ms**	**1ms**	**1ms**	**6.41ms**
Loss Rate	**0**	**0**	**0**	**0**	**1**

Table 9 Framework based Network

In summary the above show that IPV6 is in fact working and the performance of IPV6 can also be seen in effect. Since we can see the consistence of data flow with the variation of payload.

Chapter Seven

7. Conclusion and Recommendation

7.1. Overview

The previous chapter was focused on analyzing data gathered from different data collection instruments and finally an appropriate framework was developed. The ultimate purpose of this chapter is to conclude and summarize the study and indicating future direction for fellow researchers.

7.2. Conclusion

The research was conducted to design a framework that can be used to migrate IPV4 to IPV6. Currently Ethio telecom, the ISP for Ethiopia is using an IPV4 based network in almost all of its service. This could be fine for the current situation but the world is moving on and IPV4's are becoming the past. As a result Ethio telecom will be forced to migrate or least be able to accommodate IPV6 service while still running IPV4.

This study is conducted to achieve the general objective "IPV6 migration framework to meet the challenges in moving from IPV4 to IPV6". To effectively achieve this objective specific objectives were set and different literatures related with the research from different sources were reviewed.

Based on the process that the research has undergone and an understanding of the current IPv6 transition methods based on knowledge about IP in general as well as IPv4 and IPv6 in particular. The researcher has learned that global IPV4 pool was is almost completely exhausted now and transitioning to IPv6 would be a must for near future. There are three transition methods that were most reviewed i.e. dual stack, translation and tunneling. Each of them with their own advantages and disadvantages.

The main objective of the paper was to come up with a framework that could be used by Ethio telecom, and the paper has put forth a framework that was deduced from a framework put forth by Y. Cui. The framework was modified based on the challenges identified while doing this research. The main challenges identified by this research are, device compatibility, legacy services running in the network, network downtime management and experstise. To slove this

challenges the framework was proposed. After simulating and evaluating of the framework the researcher has found with minimal modification the framework could be applied to migrate and prepare Ethio telecom network infrastructure for IPV6. The framework was evaluated based on service continuity and performance.

7.3. Recommendations

Based on the findings and the above conclusions the following recommendations are put forth.

1. The researcher recommends that Ethio telecom should start thinking about IPV6 and prepare for the inevitable.

2. Ethio telecom should assess and evaluate the readiness of all the devices including the CPE according to the research.

7.4. Limitation

- ✓ Accessibility of the full network data for site visit and observation has affect the research.
- ✓ Finding actual personnel's that were responsible for IP and IPV6 related works.
- ✓ Time, Money and better testing infrastructure has limited the evaluation of performance to a minimal network.

7.5. Suggestion for Future Research

This research is just a start to the massive world of IPV6, there is still many to be done be it in improving this framework to assessing the different aspects of the protocol. Below are a list of recommendations for future work that could benefit the IT and organizations society at large. This list has been complied based on the challenges faced and the different reviews of other works in the field. We can take as example the Security aspects, while doing this research security was not considered, and we now that security is one of the major consideration of an ISP. So before and while transition is being done security need to be considered and well over seen. Also the Soft factor, managing expertise needs to be consider as well this is because the expert who is doing the transition need to keep an updated stack of knowledge because of the ever changing technologies to wards IPV6.

So based on the literature reviews done and the path taken while doing this research the following future research topics are suggested.

- The security aspects of IPV6 while migrating from IPV4 could be investigated.
- Managing the soft factor of transition of IPV6.
- Evaluating the above framework based on different factors other than performance and with performance.
- Address management of IPV6
- Service delivery and IPV6

References

[1] Š. Nejc and C. Mojca, "Practical Evaluation of Stateful NAT64/DNS64 Translation," *Advances in Electrical and Computer Engineering,* vol. 11, no. 3, pp. 49-54, 2011.

[2] C. Bouras, P. Ganas and A. Karaliotas, "The deployment of IPv6 in an IPV4 world and transition strategies," *Internet Research: Electronic Networking Applications and Policy Volume 13 . Number 2,* pp. 86-93, 2003.

[3] C. Yao-Chung, W. Reen-Cheng, C. Han-Chieh and C. Jiann-Liang, "Performance Investigation of IPv4/IPv6 Transition Mechanisms," in *DOI: 10.1109/ICACT.2004.1292930 · Source: IEEE Xplore*, 2004.

[4] B. Carpenter, "RFC: Advisory Guidelines for 6to4 Deployment," Internet Engineering Task Force (IETF), 2011.

[5] D. Punithavathani, "IPv4/IPv6 Transition Mechanisms," *European Journal of Scientific Research,* vol. 34, no. 1, pp. 110-124, 2009.

[6] IEEE, "IEEE," [Online]. Available: www.ieee.org. [Accessed 15 December 2017].

[7] B. Albkerat and Issac, "Analysis of IPv6 Transition Technologies," *International Journal of Computer Networks & Communications (IJCNC),* vol. 6, no. 5, 2014.

[8] S. Services, "Resources," Association Management Solutions, LLC, 1992. [Online]. Available: http://www.ietf.org. [Accessed 15 December 2017].

[9] B. Admasu, "IPV4 to IPV6 Transition - EthioTele," Addis Ababa University, Addis Ababa, 2017.

[10] P. Bali, "A Detail Comprehensive Review on IPv4-to-IPv6Transition and Co-Existence Strategies," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 4, no. 4, 2015.

[11] L. Fuliang, W. Xingwei, P. Tian and Y. Jiahai, "A Case Study of IPv6 Network Performance: Packet Delay," *Hindawi,* vol. 2017, 2017.

[12] S. Saisree, *IPv6 Transition strategies White paper,* Wipro, 2003.

[13] Information Sciences Institute University of Southern California, "DOD STANDARD Internet protocol," Defense Advanced Research Projects Agency, Arlington, 1980.

[14] V. Cerf, "The Catenet Model for Internetworking," Information Processing Techniques Office,

Defense Advanced Research Projects Agency, 1978.

[15] Q. A. Nguyen, "TRANSITION FROM IPv4 TO IPv6 Best Transition Method for Large Enterprise Networks," *LAHTI UNIVERSITY OF APPLIED SCIENCES,* 2012.

[16] A. Béla and S. Szabolcs, "Investigating the Performance of the MPT Multipath Communication Library in IPv4 and IPv6," *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems,* vol. 5, no. 1, pp. 53-60, 2016.

[17] Cisco, "Design-Zone," CISCO, [Online]. Available: https://www.cisco.com. [Accessed 2 January 2017].

[18] R. Atkinson, "RFC: Security Architecture for the Internet Protocol," Naval Research Laboratory, 1995.

[19] Gilligan and Nordmark, *IPv6 Transition Mechanisms, RFC 2893,* IETF, 2000.

[20] T. Narten, E. Nordmark, W. Simpson and H. Soliman, "RFC: Neighbor Discovery for IP version 6 (IPv6)," Network Working Group, 2007.

[21] H. C. Paul and K. A. Bakon, "A STUDY ON IPv4 and IPv6: THE IMPORTANCE OF THEIR CO-EXISTENCE," *International Journal of Information System and Engineering,* vol. II, no. 2, pp. 97-106, 2016.

[22] L. Cho, B. Huffaker and L. Matthew, "Identifying IPv6 Network Problems in the Dual-Stack World," in *ACM SIGCOMM*, New York, 2004.

[23] H. Steffen and F. Benjamin, "A Comparison of Internet Protocol (IPv6) Security Guidelines," *Future Internet,* vol. 1, no. 6, pp. 1-60, 2014.

[24] G. Jivika, G. jivesh, K. Navkeerat and K. Harkeerat, "An Examination of IPv4 and IPv6 Networks: Constraints and Various Transition Mechanisms," IEEE, 2008.

[25] E. Nordmark, "RFC: Stateless IP/ICMP Translation Algorithm (SIIT)," Network Working Group, 2000.

[26] X. Wang and S. Zhong, "A Routing Scheme for IPv6-Based All-IP Wireless Sensor Networks," *International Journal of Distributed Sensor Networks,* vol. I, no. 750681, pp. 1-9, 2012.

[27] K. Tsuchiya, H. Higuchi and Y. Atarashi, "RFC: Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)," Network Working Group, 2000.

[28] J. L. Shah, "Next Generation Internet Protocol A Survey on Current Issues and Migration," *International Journal of Computer Science and Mobile Computing,* vol. 4, no. 1, pp. 490-496, 2015.

[29] K. L. Chandra, "IPv4 to IPv6 Network Migration and Coexistence," *International Research Journal of Engineering and Technology,* vol. 2, no. 2, pp. 1005-1009, 2015.

[30] Y. Cui, "Unified IPv6 Transition Framework With Flow-based Forwarding," Tsinghua University, Beijing, 2014.

[31] K. S. P. Brett A. Warneke, An Ultra-Low Energy Microcontroller for Smart Dust Wireless Sensor Networks, University of California, Berkeley, CA, 2004.

[32] C. Dutta and R. Singh, "Sustainable IPv4 to IPv6 Transition," *International Journal of Advanced Research,* vol. 2, no. 10, 2012.

[33] J. L. Shah, "Next Generation Internet Protocol A Survey on Current Issues and Migration," *International Journal of Computer Science and Mobile Computing,* vol. 4, no. 1, pp. 490-496, 2015.

[34] S.Savita and Monalisa, "Comparison analysis of various transition mechanisms from ipv4 to ipv6," *International Journal of Engineering and Computer Science ISSN,* vol. 2, no. 1, pp. 2006-2011, 2013.

[35] Y. Chen and Z. Zhang, "Design of Three-dimensional Interchange Network Based on IPv4/IPv6 Network," *Journal of Networks,* vol. 8, no. 3, 2013.

[36] Y. A. Muhammad, F. Ahmed and M. A. Sobhan, "On the Migration of a Large Scale Network from IPv4 to IPv6 Environment," *International Journal of Computer Networks & Communications (IJCNC),* vol. 6, no. 2, 2014.

[37] B. R. Dawadi, S. R. Joshi and A. R. Khanal, "Service Provider IPv4 to IPv6 Network Migration Strategies," *Journal of Emerging Trends in Computing and Information Sciences,* vol. 6, no. 10, 2015.

[38] M. Mirwais, N. Othman and R. Hassan, "Toward IPv6 Migration within a Campus Network," *Journal of Theoretical and Applied Information Technology,* vol. 77, no. 2, 2015.

[39] X. Che and D. Lewis, "IPv6 : Current Deployment and Migration Status," *International Journal of Research and Reviews in Computer Science (IJRRCS),* vol. 1, no. 2, 2010.

[40] T. Stevens, K. Vlaeminck, W. V. d. Meerssche, F. D. Turck, B. Dhoedt and P. Demeester, "Deployment of Service Aware Access Networks through IPv6," in *8th International Conference on Telecommunications - ConTEL 2005*, Zagreb, 2010.

[41] M. S. Sumara, P. A. Bavarva and S. A. Shrivastava, "Design Concept and Simulation of Migration from Present IPv4 Network to Future IPv6 Network Using Three Transition Mechanisms," *International Journal of Engineering Research & Technology (IJERT),* vol. 3, no. 4, 2014.

[42] M. A. Hossaina, D. Podderb, S. Jahanc and M. Hussaind, "Performance Analysis of Three Transition

Mechanisms between IPv6 Network and IPv4 Network: Dual Stack, Tunneling and Translation," *International Journal of Computer (IJC),* vol. 20, no. 1, pp. 217-228, 2016.

[43] A. Mohamed, A. K. Ahmed, D. A. B. A. Mustafa and D. G. E. Ibrahim, "Performance Evaluation of IPv4 Vs IPv6 and Tunneling Techniques Using Optimized Network Engineering Tools (OPNET)," *Journal of Computer Engineering (IOSR-JCE),* vol. 17, no. 1, pp. 72-75, 2015.

[44] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems,* vol. 24, no. 3, pp. 45-78, 2007.

[45] W. C. John, QUALITATIVE INQUIRY & RESEARCH DESIGN Choosing Among Five Approaches, Lincoln: SAGE Publications, 2007.

[46] S. Jiang and B. Carpenter, Interviewees, *QUESTIONNAIRE ON ISP IPv6 DEPLOYMENT.* [Interview]. 2010.

[47] A.B.Starman, "The Case Study as a type of Qualitative Research," *Journal of Contemporary Educational Studies,* vol. 1, pp. 8-43, 2013.

[48] N. W. Lawrence, Social Research Methods: Qualitative and Quantitative Approaches, Harlow: Pearson Education Limited, 2014.

[49] A. M. A. K. Ahmed, D. A. B. A. Mustafa and D. G. E. Ibrahim, "Performance Evaluation of IPv4 Vs IPv6 and Tunneling Techniques Using Optimized Network Engineering Tools (OPNET)," *Journal of Computer Engineering,* vol. 17, no. 1, pp. 72-75, 2015.

[50] A. M. A. K. Ahmed, D. A. B. A. Mustafa and D. G. E. Ibrahim, "Performance Evaluation of IPv4 Vs IPv6 and Tunneling Techniques Using Optimized Network Engineering Tools (OPNET)," *Journal of Computer Engineering,* vol. 17, no. 1, pp. 72-75, 2015.

[51] J. Ahmad and P. Palembang, "Performance Analysis for Migration Method IPv4 to IPv6 Using Dual-Stack Technique," in *The 5th ICIBA 2016, International Conference on Information Technology and Engineering Application*, Palembang-Indonesia, 2016.

[52] E. Telecom, "Services," [Online]. Available: http://www.ethiotelecom.et/services/. [Accessed 2 January 2018].

Annex 1

The table below is the current address space of the internet for IPV6 as stated by IETF.

Address(s)	Description	Reference	Date Registered	Last Reviewed
FF01:0:0:0:0:0:0:1	All Nodes Address	[RFC4291]		
FF01:0:0:0:0:0:0:2	All Routers Address	[RFC4291]		
FF01:0:0:0:0:0:0:C	variable scope allocation			
FF01:0:0:0:0:0:0:FB	mDNSv6	[RFC6762]	10/5/2005	
FF01:0:0:0:0:0:0:FC-FF01:0:0:0:0:0:0:FD	variable scope allocation			
FF01:0:0:0:0:0:0:100-FF01:0:0:0:0:0:0:15B	variable scope allocation			
FF01:0:0:0:0:0:0:160-FF01:0:0:0:0:0:0:16F	variable scope allocation			
FF01:0:0:0:0:0:0:175	variable scope allocation			
FF01:0:0:0:0:0:0:181-FF01:0:0:0:0:0:0:184	variable scope allocation			
FF01:0:0:0:0:0:0:18C	variable scope allocation			
FF01:0:0:0:0:0:0:201-FF01:0:0:0:0:0:0:202	variable scope allocation			
FF01:0:0:0:0:0:0:204-FF01:0:0:0:0:0:0:206	variable scope allocation			
FF01:0:0:0:0:0:0:2C0-FF01:0:0:0:0:0:0:2FF	variable scope allocation			
FF01:0:0:0:0:0:0:300	variable scope allocation			
FF01:0:0:0:0:0:0:3486	variable scope allocation			
FF01:0:0:0:0:0:0:BAC0	variable scope allocation			
FF01::1:1000/118	variable scope allocation			
FF01:0:0:0:0:0:2:0000-FF01:0:0:0:0:0:2:FFFF	variable scope allocation			
FF01::DB8:0:0/96	variable scope allocation			

IPv6 Prefix	Allocation	Reference	Notes
0000::/8	Reserved by IETF	[RFC4291]	[1]
0100::/8	Reserved by IETF	[RFC4291]	0100::/64
0200::/7	Reserved by IETF	[RFC4048]	Deprecated as of December 2004 [RFC4048]. Formerly an OSINSAP-mapped prefix set [RFC4548].
0400::/6	Reserved by IETF	[RFC4291]	
0800::/5	Reserved by IETF	[RFC4291]	
1000::/4	Reserved by IETF	[RFC4291]	
2000::/3	Global Unicast	[RFC4291]	[IANA registry ipv6-unicast-address-assignments].
4000::/3	Reserved by IETF	[RFC4291]	
6000::/3	Reserved by IETF	[RFC4291]	
8000::/3	Reserved by IETF	[RFC4291]	
a000::/3	Reserved by IETF	[RFC4291]	
c000::/3	Reserved by IETF	[RFC4291]	
e000::/4	Reserved by IETF	[RFC4291]	
f000::/5	Reserved by IETF	[RFC4291]	
f800::/6	Reserved by IETF	[RFC4291]	
fc00::/7	Unique Local Unicast	[RFC4193]	
fe00::/9	Reserved by IETF	[RFC4291]	
fe80::/10	Link-Scoped Unicast	[RFC4291]	
fec0::/10	Reserved by IETF	[RFC3879]	

Annex 2

Below you will find the questionnaire used in this research.

Questionnaire for IPV6 Research

Thank you for being part of this research and agreeing to fill out this questionnaire:

* Required

How well do you know IPV6 technology? *

- Very Good
- Good
- Fair
- Other: _____

Have your Company done any research related to IPV6

Your answer

What is your Company current status to wards IPV6 its initiatives in IPV6 migration.

Your answer

Approximate number of private/small office customers. *

Your answer

Approximate number of corporate customers (block of IPv4 addresses) *

Your answer

Do you offer IP multicast service? *

- ○ Yes
- ○ No

Access technologies used (ADSL,etc.)

Your answer _____

Do your customers use CPE that you supply?

- ○ Yes
- ○ No

Does the CPE that you provide support native IPv6?

- ○ Yes
- ○ No

When do you expect to run out of public IPv4 address space inside your own network?

Your answer

Do you run private (RFC1918) addresses and NAT within your network (i.e., a second layer of NAT inthe case of customers with their own NAT)?

- ○ Yes
- ○ No

When do you expect to run out of public IPv4 address space for customers?

Your answer

Do you offer private (RFC1918) addresses to your customers?

- ○ Yes
- ○ No
- ○ Maybe

Do you currently offer IPv6 as a regular service? *

- ○ Yes
- ○ No

If Yes, What percent of your customers currently use IPv6?

Your answer _____

Has your organization already deployed or are you ready for deployment of IPv6?

- ○ Yes, IPV6 is fully deployed
- ○ Yes, IPv6 is deployed in our core network(s) but not in access or other networks
- ○ We have an IPV6 deployment plan
- ○ Other: _____

If No, When do you plan to start IPv6 deployment?

Your answer _____

When do you plan to offer IPv6 as a special or beta-test service to customers?

Your answer _____

When do you plan to offer 1Pv6 as a regular service to all customers?

Your answer

If you where to deploy IPV6, what challenges or constraints may affect you from the below list?

- [ ] Lack of skills and expertise within our organization
- [ ] Lack of available training
- [ ] Our customers are not ready for IPv6
- [ ] Lack of applications that can run on IPv6
- [ ] Lack of devices that can run or support IPv6
- [ ] Legacy systems
- [ ] The cost of deploying IPv6 is too high
- [ ] Our upstream providers do not support IPv6
- [ ] There are no clear business/technical advantages or reasons to adopt IPv6
- [ ] The perceived risks of deploying IPv6 are high
- [ ] The risks of remaining with IPv4 are lower than deployment of IPv6 Option 11
- [ ] The risks of remaining with IPv4 are lower than deployment of IPv6
- [ ] Other: _____

Which basic IPv6 access method(s) apply?

- [ ] Dual stack routing backbone
- [ ] Separate IPv4 and IPv6 backbones
- [ ] 6to4 relay
- [ ] Teredo server
- [ ] Tunnel broker
- [ ] Other: _____

Please briefly explain the main reasons/issues behind your choice

Your answer _____

Which types of equipment in your network are unable to support IPv6?

Your answer _____

Can they be field-upgraded to support IPv6? *

- ○ Yes
- ○ No

Is any equipment 100% dedicated to IPv6? *

- ○ Yes
- ○ No

What length(s) of IPv6 prefix do you have or need from the registry?

Your answer

How are IPv6 prefixes delegated to CPEs? (Manual, PPPoE, RADIUS, DHCPv6, state less auto configuration /RA, etc...)

Your answer

Are your SMTP, POP3 and IMAP services dual-stack?

- ○ Yes
- ○ No

Are your HTTP services, including caching and webmail, dual-stack?

- ○ Yes
- ○ No

Are any other services dual-stack?

Your answer _____

Which of the following are dual-stack?

- [ ] Firewalls
- [ ] Intrusion detection
- [ ] Address management software
- [ ] Accounting software
- [ ] Monitoring software
- [ ] Network management tools
- [ ] Other: _____

Do you have customers who have explicitly refused to consider IPv6?

- ○ Yes No
- ○ Maybe
- ○

Any plans for Mobile IPv6 (or Nemo mobile networks)?

- ○ Yes
- ○ NO
- ○ Maybe

What features and tools are missing today for IPv6 deployment and operations?

Your answer

Any other comments about your IPv6 experience or plans?

Your answer

Thank you very much for your time.

SUBMIT

Annex 3

Below is the data collected from the questionnaires used in the research.

How well do you know IPV6 technology?	Have your Company done any research related to IPV6	What is your Company current status towards IPV6 its initiatives in IPV6 migrati	Approximate number of private/small office customers.	Approximate number of corporate customers (block of IPv4 address	Do you offer IP multicast service	Access technologies used (ADSL,etc.)	Do your customers use CPE that you supply	Does the CPE that you provide support native IPv6?	When do you expect to run out of public IPv4 address space inside your own network?	Do you run private (RFC1918) addresses and NAT within your	When do you expect to run out of public IPv4 address space for customers	Do you offer private (RFC1918) addresses to your customers?	Do you currently offer IPv6 as a regular service	If Yes, What percent of your customers currently use IPv6?	Has your organization already deployed or are you ready for deployment of IPv6?	If No, When do you plan to start IPv6 deployment?	When do you plan to offer IPv6 as a special or beta-test service to custom	When do you plan to offer IPv6 as a regular service to all customers?	If you where to deploy IPV6, what challenges or constraints may affect you from the below lis	Which basic IPv6 access method(s) apply	Please briefly explain the main reasons/issues behind your choice	Which types of equipment in your network are unable to support	Can they be field-upgraded to support IPv6?	Is any equipment 100% dedicated to IPv6?	What length(s) of IPv6 prefix do you have or need from the registry	How are IPv6 prefixes delegated to CPEs? (Manual, PPPoE, RADIUS, DHCPv	Are your SMTP, POP3 and IMAP services dual-stack?	Are your HTTP services, including caching and webmail, dual-stack?	Are any other services dual-stack?	Which of the following are dual-stack?	Do you have customers who have explicitly refused to consider IPv6?	Any plans for Mobile IPv6 (or Nemo mobile networks)?	What features and tools are missing today for IPv6 deployment and operati	Any other comments about your IPv6 experience or plans?
Good	no	at initial point	3000000	500000	Yes	ADSL, VDSL...	Yes	Yes	i don't know	No	Unknown	Yes	No		Not ready yet	i don't know	i don't know	i don't know	Lack of available training, Lack of devices that can run or support IPv6, Legacy systems				No	No										
Good	no	ongoing	3000000	500000	Yes	ADSL, VADSL, Fiber	Yes	No	I don't know	No	Unknown	Yes	No		Unkown		I don't Know		Lack of available training, Lack of devices that can run or support IPv6, Legacy systems				No	No										
Fair	No	Unkown	3000000	500000	Yes	ADSL, VADSL	No	No	Unknown	No	Uknown	Yes	No		No				Lack of skills and expertise within our organization, Lack of available training, Lack of applications that can run on IPv6, Lack of devices that can run or support IPv6, Legacy systems, The risks of remaining with IPv4 are lower than deployment of IPv6				No	No										
Good	No	I don't know	3000000	500000	Yes	ADSL, VADSL	Yes	No	Unknown	No	I don't Know	Yes	No		No	I don't know	I don't Know	I don't Know	Lack of skills and expertise within our organization, Lack of available training, Our customers are not ready for IPv6, Lack of applications that can run on IPv6, Lack of devices that can run or support IPv6, Legacy systems			CPE, Routers	No	No										
Good	No	Initial stage	3000000	500000	Yes	ADSL, VADSL	Yes	No	has not yet been considered	No		Yes	No		Unkown				Lack of available training, Lack of devices that can run or support IPv6, Legacy systems				No	No										

Annex 4

Here you will find the configuration that was used to simulate the network used for Evaluation.

```
Current configuration : 1471 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
no ip domain lookup
!
ipv6 unicast-routing
ipv6 cef
mpls label protocol ldp
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.255
```

```
!
interface FastEthernet0/0
 no ip address
 duplex half
!
interface FastEthernet1/0
 description ** Connection to R2 f1/0 **
 no ip address
 duplex auto
 speed auto
 ipv6 address FEC0:0:0:1::1/64
 mpls ip
!
interface FastEthernet1/1
 description ** Connection to R4 f1/0 **
 ip address 10.10.11.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 100
 router-id 10.10.10.1
 log-adjacency-changes
 network 10.10.10.1 0.0.0.0 area 0
 network 10.10.11.1 0.0.0.0 area 0
!
```

```
router bgp 123
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.10.10.3 remote-as 100
 neighbor 10.10.10.3 update-source Loopback0
 !
 address-family ipv6
 neighbor 10.10.10.3 activate
 neighbor 10.10.10.3 send-label
 redistribute connected
 redistribute static
 no synchronization
 exit-address-family
!
no ip http server
no ip http secure-server
!
ipv6 route FEC0:0:0:4::/64 FEC0:0:0:1::2
!
mpls ldp router-id Loopback0
!
control-plane
!
gatekeeper
 shutdown
```

```
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
End
!


!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
```

```
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
!
!
interface Tunnel0
 ip address 192.168.1.2 255.255.255.0
 tunnel source 61.55.122.9
 tunnel destination 72.1.55.19
!
interface FastEthernet0/0
 ip address 61.55.122.9 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 ip address 10.15.1.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Tunnel0
 network 10.15.1.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 61.155.122.1
```

```
ip route 0.0.0.0 0.0.0.0 61.55.122.1
ip route 72.1.55.0 255.255.255.0 61.55.122.1
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
End
```