ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE

SCHOOL OF INFORMATION SCIENCE

IPV4 TO IPV6 MIGRATION FRAMEWORK: THE CASE OF BUNNA INTERNATIONAL BANK.

By

ABIY HABTAMU

SEPTEMBER, 2020

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE

SCHOOL OF INFORMATION SCIENCE

IPV4 TO IPV6 MIGRATION FRAMEWORK: THE CASE OF BUNNA INTERNATIONAL BANK.

A Thesis Submitted to School of Information Science of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information System

By: Abiy Habtamu

Advisor: Workshet Lamenew (Ph.D.)

September 2020

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE

SCHOOL OF INFORMATION SCIENCE

IPV4 TO IPV6 MIGRATION FRAMEWORK: THE CASE OF BUNNA INTERNATIONAL BANK.

By: Abiy Habtamu

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 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: _____

Abiy Habtamu

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

Advisor's Signature: _____

Workshet Lamenew (Ph.D.)

Acknowledgments

First of all, I would like to express and offer my special gratitude to Almighty God for giving me the strength, wisdom, and health to undertake this research study and complete it successfully.

I would like to express the deepest appreciation to my family for their strong and unforgettable support, their patience with me through all my study processes.

I would like also to transfer my deep gratitude to Dr. Workshet Lamenew, my research advisor, for his patient guidance, great encouragement, and valuable critiques for this study work. During my study, his assistance has a great role in providing me valuable support, criticism, and guidance to complete my study.

Finally, I give my deepest thankfulness to Bunna International Bank S.C staff members for your tangible assistance and valuable information during my study.

Abstract

Internet protocol (IP) is considered a core protocol for every communication that performs worldwide. The world is considered as a big village due to the radical enhancement of communication. Due to the scarcity of IP addresses, low performance, a decline of a security, and reduction of reliability, IPv4 is becoming a deprecated protocol, and IPv6 was created by IETF to resolve those problems.

Due to the incompatibility nature of the two protocols, IPv4 to IPv6 migration process has different factors for its success. An inadequate study has been done in previous research and it becomes an exciting domain for research. This study engaged Bunna International Bank S.C in the development of a migration framework by integrating different factors considered as a milestone for the transition process.

The study follows a design science approach and performs one iteration cycle during the framework development. Data were collected from respondents via interview, observation, and document analysis. Throughout the collection process, high and middle-level management and field expertise are consulted to give their perception of IPv4 and IPv6 technologies. IT senior managers gave invaluable organizational level information on the IPv4 to IPv6 migration process. Besides to expertise interview, an observation was also performed by the researcher. The researcher had an opportunity to visit the head office, branches, data center, and disaster recovery site infrastructure network. Moreover, document analysis was performed by visiting relevant documents that assist the migration process.

The proposed framework has pre-migration, migration, and post-migration phases. In each phase, a fragment of tasks is put that the organization should perform during the transition period. Additionally, the framework also introduces a hybrid migration model that fits the organizational infrastructure. Finally, the framework is simulated by the standard tool GNS3 and also evaluated by a domain expert using ISO/IEC 25010:2011 quality model. Thus, the result exposes that the proposed framework can assist in the transition of BIB's infrastructure from the legacy protocol (IPv4) to IPv6.

Keywords: *BIB, IPv4, IPv6, Framework*

Table of Content

List of Tables

List of Figures

List of Acronyms

AH	Authentication Header
ARP	Address Resolution Protocol
ARPANET	Advanced Research Project Agency Network
ATM:	Automated Teller Machine
B2B	Business to Business
CIO	Chief Information Officer
CPE	Customer-premise Equipment
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DC	Data Center
DR	Disaster Recovery Site
DoS	Denial-of-Service Attack
DSM	Dual-Stack Model
ESP	Encapsulating Security Payload
EIGRP	Enhanced Interior Gateway Routing Protocol
GNS3	Graphical Network Simulator-3
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IOS	Internetwork Operating System
ISO	International Standard Organization
ITISD	Information Technology Infrastructure and Security Directorate
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4

IPv6	Internet Protocol Version 6
IRTF	Internet Research Task Force
ISATAP	Inter-Site Automatic Tunnel Addressing Protocol
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Connection
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAT-PT	Network Address Translation – Protocol Translation.
NBE	National Bank of Ethiopia
NCP	Network Control Program
NFS	Network File System
NREN	National Research and Education Network
OPNET	Optimized Network Engineering Tools
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
POS	Point of Sale
QoS	Quality of Service
RAM	Random-Access Memory
RFC	Request for comments
RIR	Regional Internet Registries
RIP	Routing Information Protocol
SIIT	Stateless IPICMP Translation
SAN	Storage Area Network
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WAN	Wide Area Network

CHAPTER ONE

1. INTRODUCTION

The main purpose of this chapter is to introduce the background of IPv4, IPv6, and its migration. The chapter generally includes the research problem and its research questions, general and specific objectives of the study, scope and limitations of the study, and significance of the study. Finally, how this thesis is conducted is also presented.

1.1 Background of the Study

The Internet protocol (IP) is the method or protocol by which data is sent from one source of device to another using the Internet or Intranet. It is the protocol that governs all communication on the TCP/IP network (Dell, 2014). Its development commenced in 1973 and was based on NCP, the protocol in use on ARPANET at that time. TCP/IP protocol became the standard protocol for the entire Internet in 1983 and is currently referred to as IPv4. At that moment, engineers responsible for the development of IPv4 could not have anticipated the growth of the Internet could lead to a shortage of addresses. According to Samad, Abbasi, Memon, Aziz, and Rahman (2018), currently, devices in our world increasing radically due to technological progression, therefore, exhaustion of the IPv4 address has become a focal point for big organizations.

IPv4 (Internet Protocol Version 4) was initially defined by IETF 791 and RFC 791 and was published in 1981 (Samad et al., 2018). Its initial architecture did not expect the rapid growth of the Internet. Its addressing scheme uses 32-bit address space. This 32-bit address space is classified mainly into five subclasses. Class A, B, C, D, and E. This 32-bit address architecture allows 4,294,967,296 IPv4 addresses that seemed too many at the time but not with our current Internet demand. Nevertheless, NAT avoids this scarcity temporally by mapping one public IPv4 address to many private addresses in the hidden zone. NAT is now the de facto means for connecting networks to the Internet (Arifin, Abdullah, Berhan, & Budiarto, 2006). However, it not a desirable solution to future address shortage because it also degrades the enterprise's network performance. NAT-PT also has operational issues and is not considered a viable medium or long-term strategy for either coexistence of IPv4/IPv6 or transition (Baker, Li, & Yin, 2011).

IPv6 (Internet Protocol Version 6) has a much larger address space, architected with 128 bits (Arifin et al., 2006). This provides an extraordinarily large number of addresses: $3.4x10^{38}$ addresses. In simple terms $6.7x10^{23}$ addresses for every square meter of the Earth's surface. Due to its huge amount of address IPv6 protocol is promising with a shining future. Moreover, from different perspectives, IPv6 infrastructure is comparatively better than IPv4.

IPv4 (Internet Protocol Version 4) is an underlying protocol upon which the Internet is based and has several serious flaws. It includes limited address space, lack of security, and performance limitation (Dell, 2014; Samad et al., 2018). Different studies propose many transition mechanisms. Mackay, Edwards, Dunmore, Chown, and Carvalho (2003) puts transitioning from IPv4 to IPv6 tools operate either within a site or between sites communication across the Internet fall into one of three categories: Tunneling tools used to communicate different native IPv6 over IPv4 dominated Internet; Interoperation tools provide communication between IPv6 and IPv4 (Dual-Stack), and through the translation of IPv4 to IPv6 packets and vice versa.

IT (information technology) infrastructure is a set of IT components that are the foundation of an IT service. These components are typically referred to as physical components. Network infrastructure is one subset of IT infrastructure used for communications. BIB depends on the infrastructure to give the desired service. IPv4 is one of the major protocols of communication in its infrastructure for the past decades. Throughout its technological improvement, this protocol is replacing with a new version, which is IPv6. In developed countries moving to IPv6 has become accelerated because of its multi-dimensional advantages like scarcity of IP address, easy management, and enhanced security. In our county Ethiopia, Ethio-telecom has already become close to start this long-term process (Matebie, 2019).

Currently, Ethiopia has eighteen private and governmental banks governed by NBE. BIB is one of the private banks in the country. For its business sustainability, it deployed its core banking solution on top of its infrastructure. Related to that, it uses the IPv4 protocol for the daily transactions it performs.

Organizations that delay their IPv6 migration plan put themselves at risk and also lose their competitive advantage one way or another. BIB has numerous routers, switches, firewalls, and other infrastructure equipment to run the day to day business activities. However, the current

global security threats and IPv4's performance issue, it puts BIB at risk in both security and business effectiveness. Thus, migrating to IPv6 can grant BIB a better business future.

1.2 Problem Statement

The next-generation network layer protocol IPv6 is developed to overcome the problems of IPv4. It is based on QoS which supports auto-configuration, enhanced security and performance, and higher addresses space. Initially, IPv6 became a compulsion due to the shortage of IPv4 addresses and was considered as a father of IPv4 protocol. IPv4 cannot offer enough IP address with the current demand for Internet compared to IPv6. Ethio-telecom is the only ISP responsible for offering Internet access and other network communication to different organizations in Ethiopia. Throughout the company's technological improvement IPv4 has becoming exhaustively utilized. This leads the company to the scarcity of IPv4 addresses. According to Matebie (2019), the company plans to migrate within the coming two years. NAT temporally solves the issue caused by the lack of IP addresses in IPv4 to some extent and also saves public addresses provided by ISPs and the organizations are using private addresses for their Intranets. However, NAT does not support network layer security standard and it does not support the mapping of all upper-layer protocols, it embodies a drawback to configure end-to-end services, and has significant performance issue (Dawadi, Joshi, Khanal, & Pulchowk, 2015; Samad et al., 2018).

BIB (Bunna International Bank) is one of the private banks in Ethiopia and a client of Ethio-telecom. To satisfy its customers with fast and secure transactions through branches, ATMs, mobile and Internet banking, USSD, and POS services, it strongly relies on the infrastructure of Ethio-telecom. As a result of this, BIB should also prepare and start to think about adopting IPv6. For this migration process, BIB needs a framework that assists in the migration process.

Another big problem with staying on IPv4 is security. IPv4 also suffers from a lack of sufficient security (Dell, 2014). IPv4 is unable to provide authentication or provide standard encryption measures to packets transmitted across ISP's MPLS. Important communication traffic, such as between branches and DC or B2B transactions, somehow is not secured as compared to IPv6. In other words, no end-to-end communication security persists. IPSec protocol designed a suite that enables network security by protecting the data being sent over the Ethio-telecom. This protocol is not built-in in the IPv4 schema. There is a standard for IPv4 security such as IPSec. However,

some implementations of IPSec are proprietary and require a consumer to spend more money on a license fee to use this security suite on the client-side (Samad et al., 2018).

To avoid costly capital and possible failure of a business continuity plan, BIB must migrate to IPv6 sooner rather than later. As Aljawarneh (2005) thought, many organizations will look at their networks and not see a big problem with staying on IPv4. Today, migrating into IPv6 is not an individual's or organization's interest. This is, therefore, for all those reasons staying on IPv4 is too risky for BIB.

The term "*transition*" has carried the sense that IPv6 is going to replace IPv4 (Baker, Li, & Yin, 2011). The transition between IPv4 and IPv6 is a long and tidy process, enclose with different factors and impossible to switch the entire infrastructure over to IPv6 overnight. This requires the transition and inter-operation framework for a successful migration.

According to Samad et al. (2018), migration process challenges mainly involved a lack of fixed standards to implement IPv6 in an organization and it is not backward compatible with IPv4. Also, IPv6 designers don't have a transition plan and IPv4/IPv6 networks have become a complex issue (Govil, Govil, Kaur, & Kaur, 2008). Due to these facts, several transition mechanisms have been developed that can be used to make the transition to IPv6 smoothly. However, technologies are changing so quickly, and enormously, most of the studies are focused only on the technical aspect of IPv4 to IPv6 migration. They did not integrate other organizational factors that should be considered in the organizational transition process. Moreover, most previous works are focused on the national level. Thus, there is a lack of investigation on an organizational level and need sufficient effort for IPv4 to IPv6 transition.

Currently, studies also reveal that IPv6 migration is important and also mandatory for big organizations. Early studies are conducted at Ethio-telecom since it the only ISP in the country. Matebie (2019) conduct a study at Ethio-telecom that provides an understanding and analysis of IPv6 transition for application and system perspective, and also proposed a framework that can facilitate the transition process for the Ethio-telecom. On the other hand, Gizachew (2019) also has done another transition framework study on the same company with a network side. However, migrating only to Ethio-telecom is just halfway. Thus, BIB must also involve in IPv4 to IPv6 migration process. BIB is one of the customers of Ethio-telecom, and also has a different

infrastructure from Ethio-telecom. Transition techniques are very dependent on the infrastructure organizations do have, and as Mekonnen and Abdulkadir (2013) recommended, further studies to be carried on developing frameworks on migration process and assessment with different transaction mechanisms for the organization. Accordingly, no studies have been conducted in Ethiopia banking industries in IPv4 to IPv6 migration. Therefore, this study is conducted in BIB's context and will use as a milestone for its migration process.

Research questions

This study attempts to investigate and answer the following research questions

1. What are the factors that have an impact on the IPv4 to IPv6 migration process?
2. What transition technique is fit for BIB infrastructure?

1.3 Objective of the Research

1.3.1 General Objective

The general objective of this research is to design and propose IPv4 to IPv6 migration framework for BIB from the infrastructure perspective.

1.3.2 Specific Objectives

To achieve the above general objective, the following specific objectives are formulated.

- To review related literature in IPv6 adoption and migration techniques,
- To assess the current infrastructure status towards IPv6 migration,
- To assess a suitable transition technique for the bank and propose a framework, and
- To demonstrate and evaluate the proposed framework.

1.4 Scope and Limitation of the Study

In Ethiopia, studies are conducted in Ethio-telecom for IPv6 migration. However, the Ethiopian banking sector is untouched in previous studies. This study is conducted in BIB to migrate the bank into IPv6 focusing on its infrastructure. Besides the infrastructure, other applications, and systems that exist in the bank are excluded from this study. Thus, this study is an attempt to develop a high-level framework based on the infrastructure that exists in the bank and aimed to facilitate its migration process by proposing a suitable transition model. The scope also covers the framework demonstration and evaluation.

1.5 Significance of the Study

Since IP is one of the powerful protocols in communication history, making IPv4 to IPv6 migration or transition can be considered a very complex and risky task. To make a simple justification, consider the Internet, it highly depends on this protocol in day to day activities. Overall, any communication generally depends on this protocol. When we come to BIB, it is majorly infused by this technology. Bank's communication from DC to branches, ATMs, Internet banking, and other services are served by IPv4 protocol. The bank will be beneficiary by a successful transition to the IPv6 protocol.

This study mainly helps BIB to migrate from legacy Internet protocol (IPv4) to IPv6 in an effective way. As the researcher stated above, the study ultimately provides a framework that uses as a milestone for the migration from IPv4 to IPv6 transition process for BIB. Thus, BIB will be beneficiary by using a framework as a guide tool whenever it is starting its migration.

This study also motivates more studies for other scholars to conduct a transition framework in other business sectors and can be used as an input for future studies on related topics since the migration to IPv6 is become a mandatory issue for big organizations and enterprises.

1.6 Organization of the Thesis

This study is organized into seven chapters. Chapter one contains the arrangement of the thesis and makes the reader familiar with the thesis. It contains background to the study, statement of the problem, the purpose of the study, research questions, significance of the study, and scope of the study are discussed.

Chapter two focused on review relevant literature to create a theoretical foundation for the research. It includes an intensive literature review in IPv4 and IPv6 protocols architecture, the benefit of IPv6 over IPv4, and current migration techniques and frameworks. It also includes factors and challenges in IPv6 adoption. Moreover, it contains a long-term IPv6 implementation in the organization. Finally, the chapter concluded with a review of related works focused on the area.

The third chapter discussed a methodology and research design that a researcher applied to the study by considering the objective of the study. It comprises a research approach, data collection technique, and analysis method.

The infrastructure survey is presented in chapter four. The researcher performed an infrastructure assessment in the organization toward IPv6. DC, DR, head office, and branches are part of the assessment. Accordingly, the researcher came up with the architecture of the infrastructure and its capability to adopt IPv6.

In chapter five, data were collected using interviews, observation, and document analysis. The interview was held to obtain different views from domain expertise. As per the collected data, thematic analysis was made and the finding from the analysis was discussed in each section.

Chapter six deals with the development of the IPv4 to IPv6 migration framework and evaluation of the proposed framework. The proposed framework was formulated based on the discussion and findings performed in chapter five. Consequently, the framework was demonstrated and evaluated using the GNS3 tool and ISO/IEC 25010:2011 quality standard respectively.

The final chapter, chapter six where the researcher concluded its study findings and puts its recommendation. A researcher also puts future work for other researchers to look at it.

CHAPTER TWO

2. LITERATURE REVIEW

2.1 Overview

The literature review is an essential part of this research as it contains scholarly papers and books, which include the current knowledge, findings, as well as theoretical and methodological contributions to IPv4 to IPv6 migration. In this chapter, the researcher reviews scholarly published articles and books to understand the concept and theories, and to identify what a real research gap.

2.2 Internet Protocol (IP)

Internet protocol (IP) is the technique or method by which data or payload is sent from one source of a computer to another destination using the Internet; A set of rules that allows communication between two or more devices or hosts on a network. Isaac (2017) specified the technical pattern of the packets and addressing of the communication device on the network. Each computer participates in the network of the Internet known as hosts. It is the main network protocol in the Internet model (Alam, Habib, & Mazumder, 2011). Chukwuemeka and Bakon (2016) also define IP, the movement of packets from source to destination; to provide internetworking network devices. In the OSI model, the network layer is responsible for the delivery of individual packets from a certain source to a destination host.

Saklani and Dimri (2013) in 1991, the IETF decided that the current version of IP, called IPv4, had outlived its design. It intended to interconnect few hosts and was never expected to grow to the size of the Internet has become today. The new version of IP, called IPv6 was the result of a long and tumultuous process that came to a head in 1994 when the IETG gave a clear direction for IPv6. It does so by creating a new version of the protocol which serves the function of IPv4, but without the same limitations for IPv4.

TCP (Transmission Control Protocol) became the core control component of this communication. TCP model interoperates connection-oriented links and datagram services between hosts, and formally known as TCP/IP or Internet protocol suite (Alam, Habib, & Mazumder, 2011).

2.2.1 IPv4 Addressing

Defined in RFC 791, IPv4 is the first version of the protocol to be deployed on ARPANET in 1983, which then became the Internet (Cooper & Yen, 2005). IPv4 includes 32 bits of addresses in the header for address space. It has 4,294,967,296 addresses that seemed sufficient for the imaginable number of computing devices at the time. This traditional 32-bit addressing architecture has four octets and each of eight bits, for example, 255.255.255.255 refers to a broadcast address.

Isaac (2017) in IPv4 address architecture, there are five major classes are existed. Class A address has a large number of nodes and is intended for a large organization that can support 16 million hosts and 127 subnets. The high order bit in a class A IPv4 address is always set to 0. The zero in the first octets is joined with the remaining seven bits to complete the network ID (first octet). The remaining 24 bits (three octets) belong to the host ID. Thus, the actual maximum usable number of nodes for this class is 16,777,214.

A Class B address is designed for a medium organization that needs a medium number of hosts. It can offer 65,000 hosts and 16,000 subnets. The two high order bits in a class B IPv4 address are always set to binary 1 0. The 1 0 in the first two octets is joined with the remaining 14 bits to complete the network ID. The remaining 16 bits which belong to the last remaining octets represent the host ID.

Class C address is appropriate for small organizations that have 254 hosts but they can chunk their networks up to 2 million subnets. The three high order bits in a Class C address are always set to binary 1 1 0 with the remaining 21 bits to complete the network ID. The remaining 8 bits in the last octet represent the host ID.

The IPv4 class D addresses are used for reserved for multicast addresses. The four high-order bits are always set to 1 1 1 0 in the first four octets which is 28 bits represents network ID, then the remaining bits are used as a host ID. The last class in IPv4 addressing is class E, reserved for the experimental purpose of the future. The high-order bits in a class E address are set to 11110. Both classes can represent 2^{28} total addresses in the class.

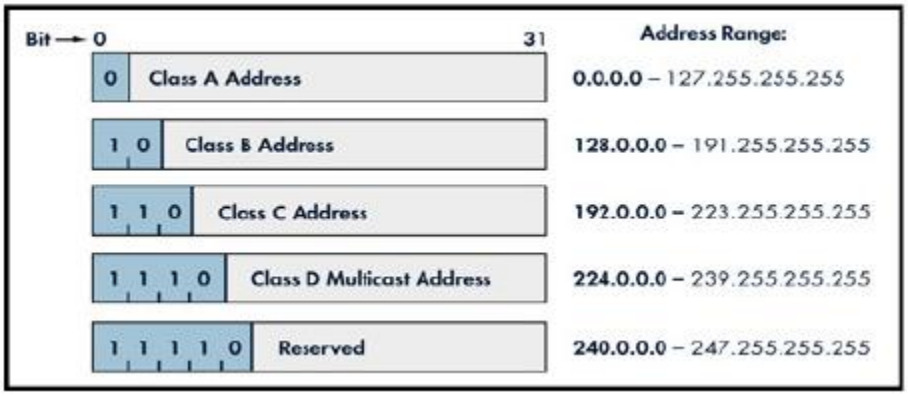

Figure 2 - 1: IPv4 addressing, adopted from (Albkerat & Issac, 2014)

2.2.2 IPv4 Header

An IPv4 header is a prefix to a packet that contains information about the version and some appropriate information for the packet. Figure 2-2 shows an IP header. This will give an idea of what IP protocol has to through every time user data is sent from the source and is to be sent to a remote network.

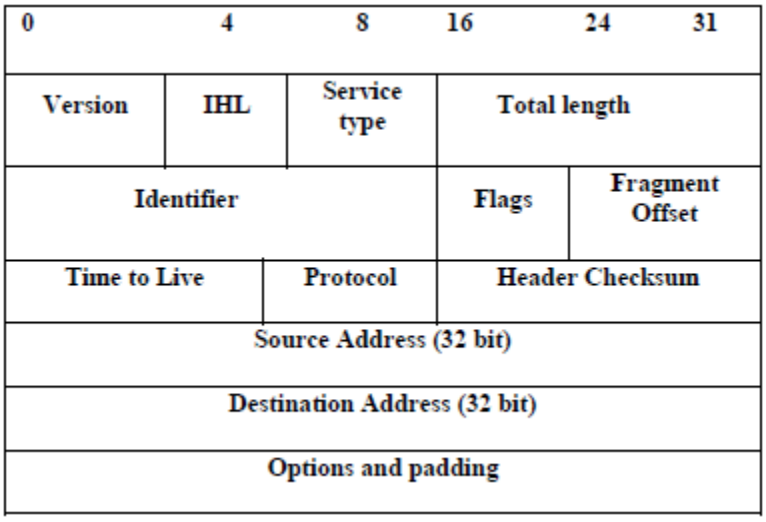

Figure 2 - 2: IPv4 header, adopted from (Albkerat & Issac, 2014)

The following fields make up the IPv4 header:

Version: IP version number.

Header length: Header length in 32-bit words.

Total length: Measurement of the packet including header and data.

Identification: Unique IP-packet value.

Flags: Specifies whether fragmentation should occur.

Fragment Offset: offers breaking up and reassembly if the packet is too large to put in a frame.

Time to Live: The time to live is set into a packet when it is initially generated.

Protocol: Port of the upper-layer protocol, like ARP and ICMP.

Header Checksum: Cyclic redundancy check (CRC) on the header only.

Source IP Address: 32-bit IP address for a source node.

Destination IP Address: 32-bit IP address for the destination host.

Options and Padding: used for network testing, debugging, security, and more.

2.2.3 IPv6 Addressing

Internet protocol version 6 (IPV6) is a new version of the Internet Protocol (Cooper & Yen, 2005). It is designed as a successor to IPv4 [RFC-791]. It has a large address space that provides more than enough globally unique IP addresses for every network device on our planet - 128 bits long. Its address consists of 16 bytes or octets. To make this address more efficient to manipulate it specifies hexadecimal colon notation. Thus, 128 bits are divided into eight sections of 2 bytes in length. It is written similarly with IPv4 style dotted notation, without sort notation an IPv6 address will appear as follow:

65535.65535.65535.65535.65535.65535.65535.65535

128 bits of IPv6 address equally divided between the routing prefix and the interface identifier. The routing prefix of a global unicast address is a globally unique prefix identifying the subnet the

interface belongs to, while the 64 bits of the IPv6 address represent the – also universally unique –EUI-64 identifier of the network interface.

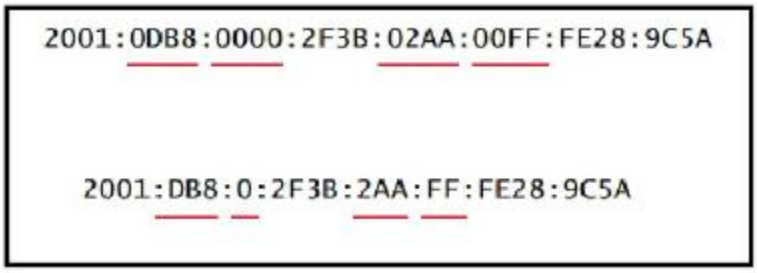

Figure 2 - 3: IPv6 addressing, adopted from (Albkerat & Issac, 2014)

Internet protocol version 6 (IPv6) addresses are assigned to interfaces, not to nodes (Chauhan & Sharma, 2014). IPv6 unicast, anycast, and multicast types of addresses. Unlike IPv4, IPv6 does not have a broadcast address; this function is being replaced by a multicast address.

- **Unicast:** This address is an identifier for a single interface and is delivered to the interface identified by that interface. Load sharing over multiple physical interfaces can be obtained by assigning a unicast address or a set of unicast addresses to multiple physical interfaces if the implementation treats the multiple interfaces as a single interface.
- **Anycast:** This address is an identifier for a set of interfaces. However, a packet sent to this address is delivered to only one of the interfaces identified by that address, possibly the nearest one.
- **Multicast:** This address is an identifier for a set of interfaces. A packet sent to a multicast address is delivered to all interfaces recognized by that address. Nikkel (2007) also defines several multicast addresses that exist for various purposes. Some examples of multicast addresses are:
  - FF02:0:0:0:0:0:0:1 All Nodes Address
  - FF02:0:0:0:0:0:0:2 All Routers Address
  - FF05:0:0:0:0:0:1:3 All-DHCP-servers
  - FF01:0:0:0:0:0:0:FB mDNSv6

A crucial feature in IPv6 addressing is auto-configuration in a network (Stevens et al. 2005). It creates a link-local address, verifies its uniqueness on a link auto-configuration increases the self-efficiency of network devices by taking a considerable amount of management functions and without relying on the central or additional configuration servers (Shah & Parvez, 2015). The auto-configuration technique has both stateful address and stateless address. The stateless transition uses local information and non-local information that is advertised by routers to produce addresses. Routers advertise prefixes that recognize the subnet related to a link. Hosts make an interface identifier that uniquely identifies an interface on a subnet. On the other hand, in stateful auto-configuration, hosts obtain interface addresses or configuration information and parameters from a server. A server keeps a database that checks which addresses have been given to which hosts. Global unicast subnet prefixes are assigned by the Internet Assigned Numbers Authority (IANA) through their Regional Internet Registries (RIRs). The standard policy of RIRs is to assign 32-bits prefixes to ISPs, allowing ISPs to structure their topology with the remaining bits of the prefix. The remaining bits of the prefix, 32-bit for default policy applied, allow assigning prefixes to subscribers in an efficient and aggregately way.

2.2.4 IPv6 Header

The new version protocol IPv6 is better than IPv4 in terms of complexity and efficiency. Like of IPv4 header, it contains information about the IPv6 packet. Figure 2-4 shows the composition of the IPv6 header.

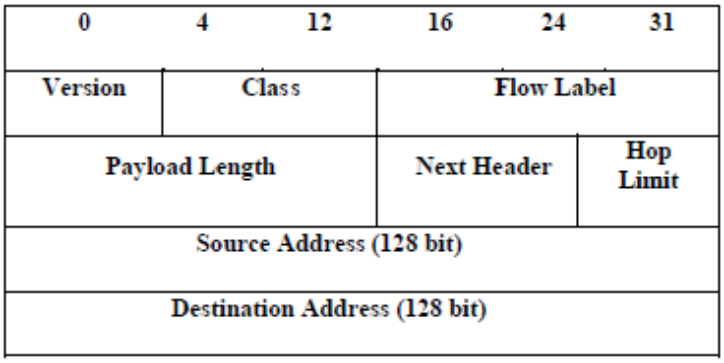

Figure 2 - 4: IPv6 header, adopted from (Chauhan& Sharma, 2014)

Version: It represents the version of Internet Protocol, i.e. IPv6, represented in 4 bits.

Class: Used to identify the type of service is offered for the packet.

Flow Label: The source tag sequence to help the router detect a particular packet belongs to a specific flow of information.

Payload Length: Used to identify the router about information for a particular packet contains in its payload.

Next Header: This field usually states the transport layer protocol used by a packet.

Hop Limit: The value is decremented by one at each forwarding node and the packet is discarded if it becomes 0.

Source Address: The actual IPv6 address of the sending node or host.

Destination Address: The actual IPv6 address to the destination node(s) or host(s).

2.3 Network Address Translation (NAT)

Network address translation (NAT) is a protocol by which a single device connects to the Internet with a public IP address shares that connection through the use of a private address, by hiding those devices behind the private address (Cooper & Yen, 2005). Devices configured with private IP addresses are commonly referred to as non-routable addresses, while public addresses offered by ISP are typically known as routable addresses (routable throughout the globe).

The exhaustion of IPv4 addresses causes inadequate design capacity of the original Internet infrastructure. One of the short-term solutions is proposed by the IPv4 engineers for the exhaustion of address was NAT (Ahmad & Yaacob, 2012). The idea behind this protocol, it just allows multiple nodes to share on or more public IP addresses. The original aim for NAT was to slow the exhaustion of available IP address space by allowing many private IP addresses to be characterized by some smaller number of public IP addresses.

Network Address Translation (NAT) has several advantages. It conserves legally recorded addresses, reduces address overlap rate in a different organization, increases flexibility when connecting to the Internet. It also eliminates address renumbering as network changes. However,

the advantages are limited only to the use of the IPv4 address protocol. Besides those advantages, it has its limitations. NAT has a loss of end-to-end IP traceability and certain applications will not work with NAT enabled in the organization.

2.4 IPv4 and IPv6 Comparison

The next-generation IPv6 has come up with some advantages over the legacy protocol IPv4 (Alam, Habib & Mazumder, 2011). It was designed to support +340 undecillion IPv6 addresses compared with 4.3 billion IPv4 addresses. IPv6 allocates enough addresses to every user and device so that every IP device has a truly unique address (Nizar & Ali, 2012). IPv4 uses 32-bit (4-bytes) addresses to uniquely recognize hosts within the Internet. IPv6 uses 128-bit (16-bytes) addresses to uniquely recognize hosts within the Internet.

Network Address Translation (NAT) has become a very common technique to deal with the shortage of IPv4 addresses. Even though, NAT doesn't work very well for many Internet applications, ranging from old dependable, such as NFS and DNS, to newer applications such as group conferencing (Nizar & Ali, 2012). Since the IP address space exhaustion is resolved by IPv6, NAT is unnecessary in IPv6 connectivity, therefore, IPv6 has no NAT during its design (Isaac, 2017). IPv6 by itself will re-establish transparency and end-to-end traffic across the Internet.

The IPv6 requirement mandates that IPv6-enabled hosts must support the IP security protocol (IPSec). IPv6 hosts are more secure than IPv4 nodes. It also includes security features, such as payload encryption and authentication source to destination communication (end-to-end security). As Isaac (2017) said, IPv4 does not have enough security because IPSec is optional, while IPv6 has built-in security which has IPSec.

Quality of service (QoS) refers to technology that maintains data traffic to reduce packet loss, latency, and jitter. It supports to provide better support for real-time traffic by labeled flows in IPv6 specification. Al-zobbi (2014) also believed, QoS reduces the routing time and increase network performance. IPv6 header has a static size of 40-byte. This size will increase the router's efficiency and decrease the routing delay time. In IPv4, routers spend more time to look up the IP header length field; Header length field is not available in IPv6, because the IPv6 header is a fixed size, while IPv4 is a variable size of 20-60 bytes. The header length field in IPv6 is no longer

needed due to the fixed header size. Tomar and Rawat (2017) also, support IPv6's routing performance; it has features of no header checksum calculation and no IP packet fragmentation at intermediate routers, which makes it better than IPv4 from a routing point of view. Generally, QoS can be measured quantitatively in different parameter, some of which are the following:

- **Packet Loss**: when a certain link becomes congested and routers and switches are starting to drop packets.
- **Jitter**: as a result of network congestion, timing drift, and router changes.
- **Latency**: time to travel packets from certain sources to a certain destination.
- **Bandwidth**: the maximum amount of data transmitted from one point to another in a given amount of time.

IPv6 has no such disadvantages. The only disadvantage is that its network bit is quite longer (Isaac, 2017). This gives rise to complexity and hinders a clear understanding of its technology. IPv6 supports auto-configuration as well as plug and play functionality. On the other hand, IPv4 just only supports manual configuration or DHCP. In the mobile phone, IPv4 only support from 1G to 3G phones, this range is extended in IPv6 up to 4G and above. In IPv6 transmission, unlike IPv4, it only uses a multicast group rather than broadcast addresses. For example, IPv6 multicast addresses use the prefix ff00::/8 and IPv4 broadcast address uses 255.255.255.255.

Generally, IPv6 is better than IPv4 by its numerous features. Table 2-1 shows the main difference between the two protocols.

Features	IPv4	IPv6
Address length	32 bits	128 bits
The checksum in the IP header	Included	No Checksum
Quality of Service (QoS)	Differentiated services	Use traffic classless and flow labels
Packet fragmentation	Done by routers	Done only by the source node
IPSec support	Optional	Mandatory
IP configuration	Manual or DHCP	Auto-configuration or DHCP
Broadcast address	Available	Not- available
NAT protocol	Support	Not-support

Table 2 - 1: Differences between IPv4 and IPv6

2.5 Benefits of IPv6 Protocol over IPv4 Protocol

The first benefit of IPv6 is address space. It offers a large address that allows some 340 trillion, trillion, and trillion addresses (Chauhan & Sharma, 2014). The current 4 billion IPv4 addresses are significantly exhausted. IPv6 is designed to support +340 undecillion IP addresses compared with 4.3 billion IPv4 addresses. If we estimate everybody in this world (7.6 billion) will require 3 IP addresses per person, then we can estimate the total required IP addresses for all the people around the world, which is 7.6 billion x 3 = 22.8 billion IP addresses. If we assume these peoples use IPv6, we still have (+340 undecillion-22.8 billion) IP addresses. Generally, IPv6 address space has more than enough to represent every device that will exist on our planet.

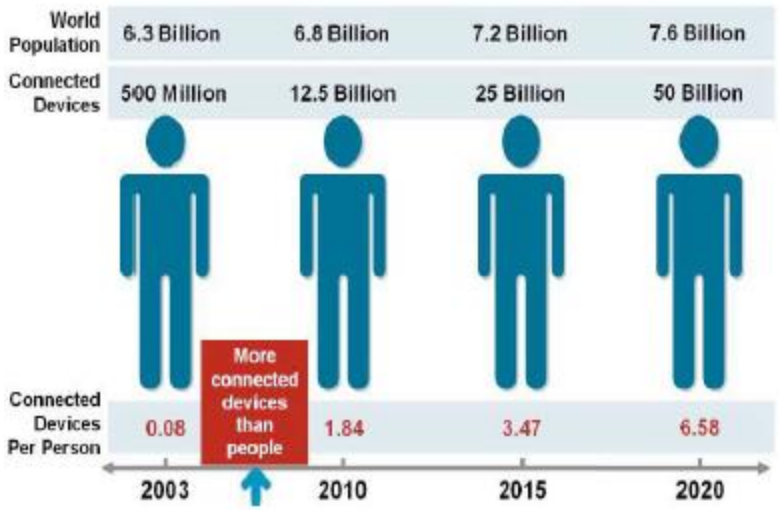

Figure 2 - 5: Demand of IP address, adopted from (Hasab, Abu, Babiker, & Mustafa, 2014)

IPv6 enhances routing efficiency by reducing the size of routing tables and makes routing more efficient by allows us to aggregate network address into a single prefix and announce this one prefix to the other IPv6 networks. IPv6 also simplified packet header makes packet processing more efficient. It allows an extension for new options by introducing a new header format as discussed above. Now with this format processing, IPv6 packets are much simpler and fast. IPv6 extension headers are not processed by every router except the hop by hop option and the checksum field is also eliminated from the header, thus making processing simpler and efficient (Chauhan & Sharma, 2014).

Internet Protocol Version 4 (IPv4) broadcast address is replaced with a multicast address in IPv6. This multicast address feature allows bandwidth-intensive packets flow to be sent to multiple destinations in a parallel fashion. Thus, it saves network bandwidth. This new feature adds a filed in IPv6 header, named "*Flow Label*" (Isaac, 2017).

Internet Protocol Version 6 (IPv6) simplified network configuration for network administrators. Address auto-configuration is built-in IPv6. A host can generate its IP address by appending its MAC address within the prefix of the local link address send from the router. Chauhan and Sharma (2014) state, IPv6 offers three types of auto-configuration; stateful auto-configuration, stateless auto-configuration, and both. The stateful technique is used when a network requires more serious control or an exact address assignment. It is the equivalent to the use of DHCP in IPv4. On the other hand, the stateless auto-configuration process allows a node to generate its link-local, site-

local, and global addresses using a combination of local information and information advertised by routers with no configuration on the host. Therefore, the management of a network becomes easy for network administrators.

Network address translation (NAT) is eliminated on the IPv6 protocol. NAT can be implemented in a router, firewall, or proxy server which interconnects a group of hosts to another network. It can be used to enable several hosts to share one or more IP addresses. Primary it was invented due to the lack of IP addresses in IPv4 addressing schema and it was intended to be a good short-term solution. However, thanks to IPv6, today there are sufficient IP addresses offer by this protocol.

Internet Protocol Version 6 (IPv6) provides end-to-end connectivity at the IP layer is maintained. This is performed by IPSec, which provides confidentiality, authentication, and data integrity. IPSec is built-in, which means that a secure network will be easier to build and deploy in the IPv6 world (Saklani & Dimri, 2013). IPv6 provides access control limits access to people to have an authorization, authentication certifies that the person who sends the data is who the person claims to be, and confidentiality ensures that any data carried over a public network, including password, is encrypted to make it very hard for anyone to see the exchanged data (Cooper & Yen, 2005).

Caicedo (2014) stated IPSec defines two types of security headers: Authentication Header (AH) and Encapsulating Security Payload (ESP). The AH provides integrity-protection and the ESP header can provide integrity-protection plus protection supported by encryption. Moreover, Internet Key Exchange (IKE) protocol uses nodes involved in an information exchange can establish a set of symmetric secret keys for encryption and protect the integrity of the packets they send to each other.

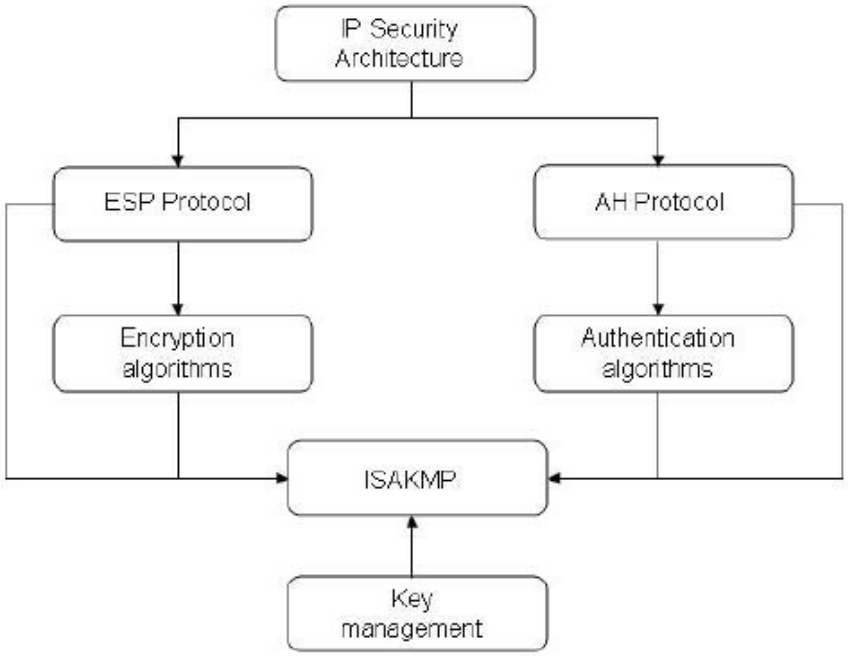

Figure 2 - 6: IPSec architecture, adopted from (Caicedo, 2014)

Another benefit of IPv6 is QoS. In IPv4, service quality relies on the 8 bits of IPv4 in the service field (Chukwuemeka & Bakon, 2016). Even if this service is available in IPv4, Type of service (TOS) field and the identification of the payload, it is not possible when IPv4 payload identification (uses a TCP or UDP port) and IPv4 datagram packet payload is encrypted (Kanth, 2016). IPv6‘s unique features, like no header checksum calculation and no IP packet fragmentation at intermediate routers, can enhance the QoS at the end-user (Tomar & Rawat, 2017). This means that some networks may also have different paths for IPv4 and IPv6 services. Hence, may have different hop counts and MTU. A path with a smaller hop count and larger MTU value is IPv6 network may also enhance the QoS for the end-user and may also experience lesser congestion. Cooper and Yen (2005) pointed out IPv6 QoS, another common technique to enhance the services is flow and traffic labeling in payload transmission. By using traffic class and flow label field, IPv6 allows nodes to distinguish certain packets far possible special treatment by a router. These payloads may carry-sensitive or real-time customer transaction data that needs to benefit from special processing. These kinds of traffics are identified by the corporate router by a flow label and packets are placed into a special queue for fast processing.

2.6 IPv4 to IPv6 Transition Techniques

Migrating from IPv4 to IPv6 is an immediate need and difficult because of the huge size of the Internet and the great number of IPv4 users (Saklani & Dimri, 2013). Thus, this process needs a prolonged period to avoid downtime of the organization. Since organizations are becoming more and more dependent on the Internet for their daily activity, and they are not in opposition to tolerate downtime for the replacement of the IP protocol. This implies that transition schemes must be put in place for graceful migration from IPv4 to IPv6 networks. Currently, the main approaches to transitioning from IPv4 to IPv6 are:

- Dual-stack mechanisms,
- Traffic tunneling, and
- Translation mechanisms.

2.6.1 Dual-Stack

The first transition technique is referred to as Dual-Stack. The organization must create an IPv6 network parallel to the existing or legacy IPv4 network (Dhamale & Singh, 2018). In Dual-Stack architecture, all the components of the network system should support both the IPv4 and IPv6 protocols (Chauhan & Sharma, 2014). As the name implies, Dual-Stack involves the implementation of stacks in both IPv4 and IPv6 clients and allows a client in a native IPv6 network to communicate with an IPv4 host in an IPv4 network (Yousafzai, Othman, & Hassan, 2015). Therefore, an application using the network must choose either IPv4 or IPv6, by selecting the correct address based on the type of IP traffic and particular requirements of the communication. Thus, it is preferred for the network with a mixture of IPv4 and IPv6 applications that require both the protocols. To do so, routers must upgrade to IPv6 and it also requires the dual management of IPv4 and IPv6 routing tables. According to Muzhir, Ani, and Haddad (2012), the Dual-Stack transition technique contains two protocol stacks that function similarly and allow network hosts to communicate either via IPv4 or IPv6. They can be implemented in both the end system and network node, which means the network hardware runs IPv4 and IPv6 simultaneously. To forward IPv6 packets to the various destinations, the network designer can use one of the following approaches:

- **Native IPv6**: configure IPv6 on most or all routers, on most or all production interfaces, making all routers use a Dual-Stack.

- **IPv6 tunnels**: configure some routers with IPv6, other without IPv6, and tunnel the IPv6 packets over the IPv4 network by encapsulating IPv6 packets inside IPv4 packets.

Dual-Stack Model (DSM) is the most versatile way to deploy IPv6 in existing IPv4 environments (Kanth, 2016). IPv6 and IPv4 are allowed along with the related features required to make IPv6 routable, highly available, and secure. In some cases, IPv6 is not enabled on some device interfaces because of the existence of legacy applications for which not supported in IPv6. The main drawback of this model is that network device upgrades might be required when the existing devices are not IPv6-capable. Not only this, the IPv6 traffic experiences higher latency, lower throughput, or more lost packets than IPv4 traffic but applications will still communicate over IPv6 at the expense of network performance (poor IPv6 network performance).

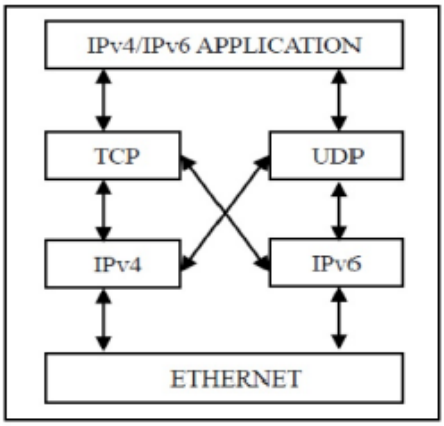

Figure 2 - 7: Dual-Stack, adopted from (Albkerat & Issac, 2014)

A common Dual-Stack migration strategy is to make the transition from the core to the edge (Gold, 2011). This usually includes allowing two TCP/IP protocol stacks on routers and firewalls. After the network maintenances IPv6 and IPv4 protocols, the process will enable Dual-Protocol stacks on the servers and then the edge computers. Security becomes worrying when routers are communicating with other non-authenticated routers. Sharma (2010) also recommended focusing on host security on a Dual-Stack device, network designers should aware that applications can be subject to attack on both IPv6 and IPv4. Therefore, any host controls like firewalls and IDS should be configured to block traffic from both IP versions.

The strongest arguments coming from Albkerat and Issac (2014) on Dual-Stack implementation are for large networks. As the authors believed, Dual-Stack is not suitable for large networks like the Internet because it is difficult and expensive to cover all the nodes in such huge networks. Thus, it is suitable for small networks, which needless management and is easy to control.

2.6.2 Traffic Tunneling

Tunneling is a technique by which the existing IPv4 backbone can be used to transmit IPv6 traffic and vice versa (Chauhan & Sharma, 2014). The tunneling protocol carries the tunneled protocol and introduces carrying one protocol inside another. Tunnels take IPv6 packets and encapsulate them in IPv4 packets to be sent across the IPv4 network that didn't upgrade to the new protocol (Chukwuemeka & Bakon, 2016). The basic principles behind the tunneling techniques are packet encapsulation and packet de-capsulation (Yousafzai et al., 2015). Encapsulation is used when an IPv4 header transfers IPv6 packets from source to destination in the IPv4 network. In contrast, de-capsulation is used when the IPv6/IPv4 host or router receives an IPv4 datagram that is addressed to one of its IPv4 addresses or a multicast group address.

According to Muzhir et al. (2012), the encapsulation approach enables the connectivity between IPv6 islands by tunneling one protocol over another. In other words, tunneling techniques are encapsulating IPv6 packets within IPv4 packets and passing them through the native IPv4 domains. The tunnel is widely used in nowadays networks. This technology only requires both ends of the tunnel equipment to support both protocols, and each tunnel should be established between two endpoints.

Tunneling could be either manual or automatic. As Gold (2011) explained, manual tunneling requires configuration at both ends of the tunnel (source and destination), whereas dynamic tunneling is created automatically. Manual tunnels are manually configured but the configuration is required at both ends of the tunnel and the administrator will always know how his or her tunnel is created (Bendale, Naykude, & Nikam, 2015). From a management and security perspective, manual tunnels are good for implementation but from a configuration perspective, they are a little bit more tedious to work with it. Dynamic tunneling techniques simplify maintenance related to statically configured tunnels. Static tunnels make traffic information obtainable for each endpoint, providing additional security against injected traffic. Dynamic tunnels are not easy to track who is

communicating over the transient tunnels. Generally, in traffic tunneling techniques, there is a situation in which traffic will be encapsulated, and usually many firewalls won't inspect the traffic if it is in a tunnel. Related to this, static IPv6 in IPv4 tunneling is desirable because explicit allows and disallows are in the policy on the edge routers (Sharma, 2010).

2.6.2.1 Tunnel Broker

The Dual-Stack is important for a tunnel broker so that a tunnel for the hosts in the IPv4 network only can be built (Albkerat & Issac, 2014). Additionally, the webserver is required to build the tunnel because the user should be connected to a web server and applies certain authentication details (such as the IP address, operating system, and IPv6 support software) and the reply will be a short script. Then, the IPv4 to IPv6 tunnel is ready to use.

The service operates in IPv6 tunnel broker is, first the user contacts the tunnel broker and performs the registration procedure (Punithavathani & Sankaranarayanan, 2009). After user recording, the user again contacts the tunnel broker for authentication and offering configuration information. During the authentication, the broker verifies the user authority to get the service. The third step is the broker will configure the network side end-point and finally, the tunnel will be active and the user will be connected to IPv6 networks. To get this service, IPv4 connectivity between the user and the service provider is required.

According to Narayanan, Mohideen, and Raja (2012), this tunnel broker or an organizer uses four sub-systems to make the system operational. Those are the following:

- **Tunnel Server (TS)**: is a point where the users get connected to the IPv6 network. Tunnels are set up between the tunnel servers and the users. It monitors the attached users.
- **Tunnel Server Group (TSG)**: responsible for assigning IPv4 anycast address.
- **DNS System**: responsible for providing mappings from IPv6 addresses to the domain names.

2.6.2.2 6 to 4

A 6 to 4 tunneling mechanism allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks. This transition technique is a flexible mechanism that enables the communication between IPv6 islands over the IPv4 Internet (Chown, 2002). 6 to 4 uses the IPv4 network to transfer the IPv6 packet. Thus, the IPv4 network acts as a link between the IPv6 networks (Albkerat & Issac, 2014). It is usually applied almost totally in border router or device, without explicit host modifications except for a default address selection (see figure 2 - 8). Its usage is expected to be most common during the medium-term phase of the transition process to IPv6 when there are many IPv6. This is very useful when an organization wants to enable the IPv6 protocol can use the prefix 2002::/16 without needing to request production address space (under 2001::16) from its associated NREN or the RIPENCC.

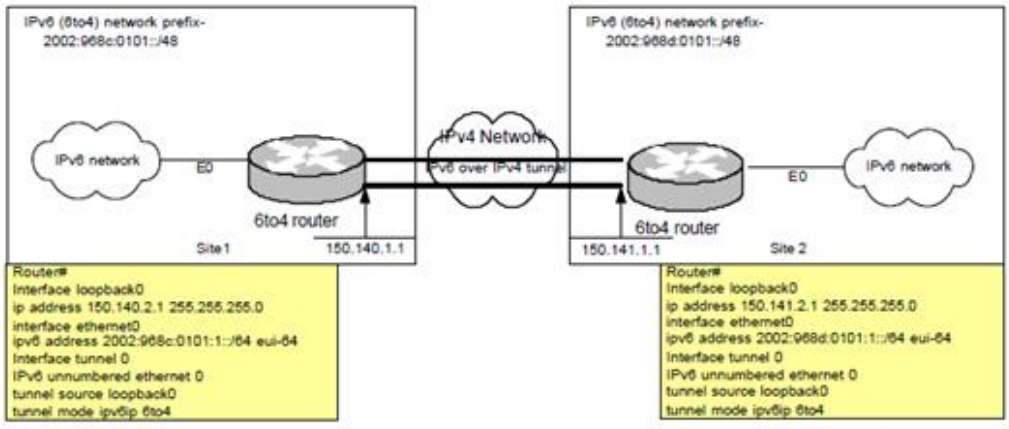

Figure 2 - 8: The usage of the 6 to 4 mechanism, adopted from (Chown, 2002)

As we can see from the figure 2 - 8, in order to Site 1 and Site2 to communicate with their IPv6 world beyond the other 6 to 4 sites, organizations must deploy a 6 to 4 relay router either on their premises or use and external (public) 6 to 4 relay service.

2.6.2.3 6 over 4

This automatic technique is for providing an approach of IPv6 nodes that exist within a pool of IPv4 networks. IPv6 nodes are not directly connected, so this technique will create a virtual link to provide a way for the IPv6 need to communicate (Albkerat & Issac, 2014).

The purpose of this method is to allow isolated IPv6 hosts, located on a physical link that has no directly connected IPv6 router, to become fully functional IPv6 hosts by implementing an IPv4

multicast address as their virtual local link. The multicast addresses are a fully interconnected set of IPv4 subnets, within the same local multicast scope, on which at least two IPv6 nodes are conforming to this requirement. 6 over 4 requires no configuration, but IPv4 multicasting must be enabled and all host stacks included must have a 6 over 4 implementations.

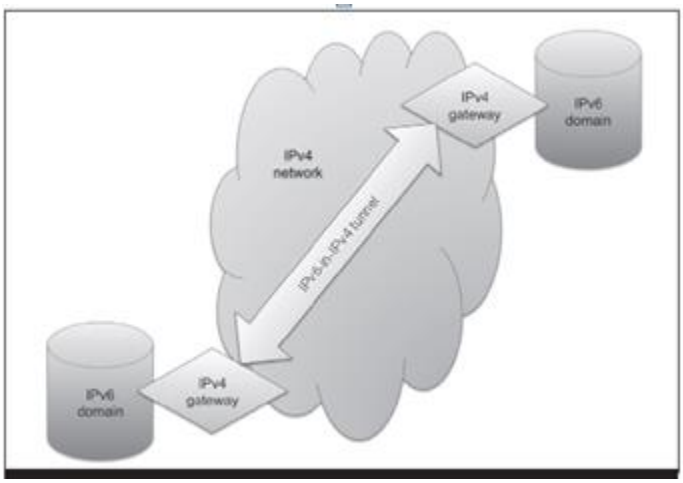

Figure 2 - 9: Tunnelling IPv6 traffic over the IPv4 network, adopted from (Gold, 2011)

2.6.2.4 ISATAP (Inter-Site Automatic Tunnel Addressing Protocol)

ISATAP (Inter-Site Automatic Tunnel Addressing Protocol) is used to link the local IPv6 addresses with the prefix fe80::5efe/96, which is followed by the IPv4 32 bits (Albkerat & Issac, 2014). It is an automatic tunnel and it is a point to point connection. It is mainly used to provide IPv6 connectivity between IPv6/IPv4 hosts across an IPv4 network. Further, this technology is used within private organizations, as the addresses use not routable on the Internet.

ISATAP (Inter-Site Automatic Tunnel Addressing Protocol) use to identify the IPv4 address of the remote site for tunneling IPv6 packets. As a result, a network administrator can create dynamic multipoint tunnels using ISTAP, in general, a concept much like the multipoint tunnels created using automatic 6 to 4 tunnels.

The host using the standard addresses auto-configuration mechanism automatically configures ISATAP tunneling. The ISATAP router is accountable for resolving IPv6 to an IPv4 address. And, the host communicates with the ISATAP router by using IPv4. The router provides the host with information about the IPv6 network prefixes, and default gateway (see Figure 2 - 10).

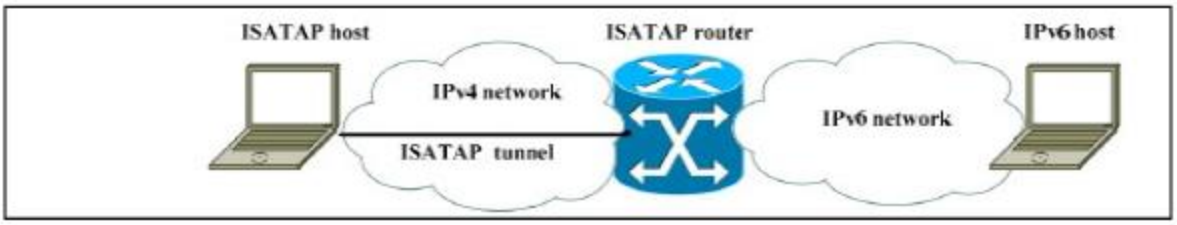

Figure 2 - 10: ISATAP mechanism, adopted from (Albkerat & Issac, 2014)

2.6.3 Translation Mechanism

The translator is a device capable of translating traffic from IPv4 to IPv6 or vice versa (Chauhan & Sharma, 2014). This transition technique intends to remove the need for the Dual-Stack transition technique by translating traffic from native IPv4 devices to operate within an IPv6 infrastructure. It performs header and address translation between IPv4 and IPv6 protocols. As declared by Dhamale and Singh (2018), the concept of address translation is also similar to NAT. As NAT maps private addresses to public addresses, the translator translates IPv4 addresses to IPv6 addresses.

The advantage of this technique is IPv4 users can use this translation technology with no or little change in the existing infrastructure to connect with the IPv6 network and vice versa (Karthikeyan & Chandra, 2016). The overall goal of the translation is to translate packets with IPv6 addresses to the client with IPv4 addresses. So, the native IPv6 hosts can talk to the native IPv4 hosts. Translation can occur at several layers of TCP/IP including network, transport, and application layers (Arafat, Sobhan, & Ahmed, 2014). Translations alter or carry conversion of IP packets between IPv6/IPv4 which often results in attribute or information loss, unlike tunneling which doesn't modify the tunneled datagram. This method has two mechanisms, which can be either stateless or stateful. While stateless means that the translator performs every traffic separately with no reference to the previous one. Stateful maintains some form of state about previous individual traffic. The translation process can take place in either end systems or network devices. From a security perspective, translation techniques also have their holes. It suffers from spoofing and DoS attacks (Sharma, 2010).

2.6.3.1 SIIT (Stateless IPICMP Translation)

The translation is performed with the header between IPv4 and IPv6. It requires each IPv4 host to have an assigned IPv4 address. This technique allows the native IPv6 host to talk to the native IPv4 hosts. The translation is on the IP packet header. This method requires one temporary IPv4 address per host; it becomes a problem if the organization is faced with a shortage of IP addresses. The temporary IPv4 address range will be used as a native IPv4 address is translated IPv6 address. The packets will travel through a stateless IP/ICMP translator that will translate the packet header between IPv4 and IPv6. Meanwhile, in the opinion of Albkerat and Issac (2014), SIIT is not recommended using, because during the translation the information might be lost and NAT protocol is also required.

2.6.3.2 NAT-PT (Network Address Translation – Protocol Translation)

This technique has a pool of global IPv4 and IPv6 prefixes with a length of 96 bits. The translation will be created by assigning the IPv6 with the IPv4 address pool through the NAT-PT gateway (Albkerat & Issac, 2014). It does not require an extra application or depend on another mechanism, such as Dual-Stack, but it requires interoperability with the core network for easy and fast management. Each host populates a pool of globally routable IPv4 addresses, which are automatically assigned to IPv6 hosts when sessions are initiated across the IPv6/IPv4 boundary (Punithavathani & Sankaranarayanan, 2009). This technique allows only IPv6 networks and applications to communicate with IPv4 only hosts and applications. The prefix ::/96 will be used to produce a new address.

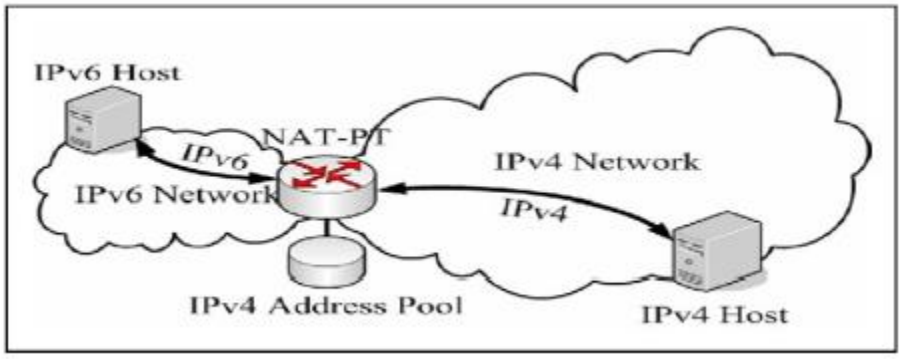

Figure 2 - 11: NAT-PT Transition mechanisms, adopted from (Albkerat & Issac, 2014)

2.7 Comparison of Transition Technologies

According to Albkerat and Issac (2014) analysis, network performance varies across different mechanisms. The CPU utilization of manual tunneling and 6 to 4 is higher than Dual-Stack because the transition technology generates more effort to encapsulate and decapsulate traffic packets. On the other hand, Dual-Stack has less delay with TCP, but with a 6 to 4 and manual tunnel, the delay is higher because the packets are not transferred directly as usual. On the other hand, the tunnel broker technique has a low administration cost (Bouras, Ganos, & Karaliotas, 2003). Authors like Hasab, Abu, Babiker, and Mustafa (2014) also tried to see Dual-Stack and tunnel from a security perspective. Dual-Stack is less secure than tunneling. Meanwhile, Dual-Stack runs both IPv4 and IPv6 independent of each other and has complex management while tunnels carry one protocol inside another and easy to implement over existing IPv4 infrastructure.

Using the Dual-Stack backbone has the benefit of using native IPv4/IPv6 service, however, it uses decline a router performance and needs heavy effort for the migration (Bouras et al., 2003). The partial Dual-Stack as a backbone in the migration process has fewer routers stress and enhances their performance. Unlike full Dual-Stack, partial Dual-Stack has flexibility in different migration phases.

Another performance analysis was performed by Yagoub, Yosif, Babiker, Mustafa, and Hamied (2014) using GNS3 using latency and packet loss parameters for a tunnel, NAT-PT, and Dual-Stack. There is a higher latency in NAT-PT follows Dual-Stack and LANs tunnel. Therefore, the tunneling technique is the best in terms of latency and packet loss. Quintero, Sans, and Gamess (2016) also, expose ISATAP and 6 to 4 have similar network performance, encouraging network administrators to choose the one that better suits their needs, or to mix both technologies if required.

Generally, table 2 - 2 shows the advantage and disadvantages of Dual-Stack, translation, and tunneling migration techniques.

Migration technique	Advantages	Disadvantages
Dual-Stack	Easy to implement	Use two routing tables. Thus, hard to manage.
	Low Cost	High memory and CPU utilization
Translation	Solve network interoperability problem	Harder to control on a large-scale network
Tunneling	Configure tunnel endpoints only	Face another problem of NATs
	Simple to implement and no additional management	Take more CPU power and hard for troubleshooting

Table 2 - 2: Advantages and disadvantages of migration techniques

2.8 Challenges and Factors to IPv6 Migration

2.8.1 Security Challenges

Many efforts have been done on evaluating the security implication of the IPv4 to IPv6 migration techniques for Dual-Stack, tunneling, and translation. The existence of these transition technologies creates a situation in which network designers need to understand the security implications of the transition technologies and select the appropriate transition technology for their network (Sharma, 2010). In tunneling technology, the network designer mostly does not consider IPv6 tunneling when defining a security policy. Because of this, unauthorized traffic could traverse the firewall in tunnels. Moreover, as noted in many transition studies done Sharma (2010), automatic tunneling mechanisms are susceptible to packet forgery and DoS attacks. To minimize these attacks, static IPv6 in IPv4 tunneling is a perfect solution because explicit allows and denies

are in the IP policy on the edge routers. The administrator by itself establishes a trust relationship between tunnel endpoints and continues to implement an inbound and outbound security policy.

The translation mechanism also suffers in spoofing and DoS issues as native IPv4 translation technologies. Network designers should also aware that applications can be subject to attack on both IPv6 and IPv4 on Dual-Stack devices. Thus, firewalls and IDSs should block traffic from both IP versions when a necessary block is required. During the transition process, network designers should have a security and knowledge plan (Khudhair & Mohammed, 2017). Designers should have training consists of major topics like organizational benefits associated with IPv6, its technical requirements, expected risks, and attacks, safety, and security consideration over IPv4 to IPv6 transition mechanisms. Sharma (2010) solidifies the importance of awareness of security threats in the transition process, "*without adequate training and attention on the part of network operators to the new consideration with IPv6 security, it will be very difficult to ensure a smooth transition to IPv6*."

2.8.2 Technical Deployment Challenges

Deploying IPv6 has introduced different challenges in different implementation projects. The first challenge would be primarily considered when we think to deploy IPv6 is a technical issue. According to Saklani and Dimri (2013), different implementation technical challenges are identified. The key migration challenges are as follow:

- **IPv6 and IPv4 hosts must interoperate**: Especially using the Dual-Stack transition technique, core network devices should support both IPv6 and IPv4 protocols. This becomes a problem when legacy devices that do not support IPv6 exit in network infrastructure.
- **Possibility of Progressive and no Traumatic Transition**: Network administrators and end-users usually think that migration is easy to implement. Due to this, IPv4 hosts, routers, and other devices can be updated to IPv6, one at a time, without requiring other hosts or routers to be updated simultaneously. A phased approach to migrate a few users at a time may be a good idea with adequate testing, otherwise, if there is a problem, many users may be affected.

- **Addressing Complexity**: In the process of migration network devices are updated to IPv6, it can also continue to use IPv4 addresses. Using both addressing schemas ends up in complex management and troubleshooting. Shevenell (2005) argues on managing IPv4 devices in an IPv6 network becomes significant and needs attention when the core part of the network becomes the upgrade to IPv6.

2.8.3 Factors affecting IPv6 Adoption

As Main, Politechnic, Zakaria, and Robiah (2014) pointed out, majorly there are two factors organization to migrate to IPv6:

- Physical Factor, and
- Human factor.

2.8.3.1 Physical Factor

Deployment Status

Planning is an important part and a process of thinking about and organizing activities need to achieve the migration process successfully. If an organization needs to deploy or migrate to IPv6, the organization first must start a plan towards IPv6. This activity includes training, inventory work, budget, and ensure long-term investment in its infrastructure. Planning is just the first element and stage in the deployment of IPv6 in the organization.

The other phase in IPv6 deployment is implementation. It includes a network audit, selection of network components, network management, planning, and execution (real implementation). It incorporates elements of understanding of new standards and levels of implementation. It also integrated the element of testing in the implementation phase to clarify the deployment status.

Cost

Infrastructure upgrades need a high investment. Since IPv6 and IPv4 are two different protocols it might need extra infrastructure while deploying IPv6 in the organization. Moreover, the cost of overhauling the existing IPv4 infrastructure is high for most network operators and service providers as well as any organization. Though upgrading from IPv4 to IPv6 requires more cost but still needs to minimize the cost by investing in IPv6 compliance devices for future use.

The other significant cost is in the migration process is during deployment operation. An organization that has a plan to migrate needs to provide a significant budget used for planning, designing, testing, training, and deployment operation costs.

Cost estimation of IPv6 transition is important and can help IPv6 migration faster. A good example of this is Arifin et al. (2006), a study conducted in University Sains Malaysia, the cost of migration from IPv4 to IPv6 includes two aspects. The first aspect is the economic cost which is the real cost of hardware, software, and training, and another cost that the sudden cost that takes place in the system. The second aspect is the technical assessment which will discuss some components of the economic cost but from a technical point of view.

Even if the implementation of IPv6 will involve some investment since it is new technology and it will run using the current network infrastructure which is IPv4. The key features that IPv6 offered will enable them to save costs, especially in the long run. The important cost components are:

- **Network and Hardware Costs**: consists of IPv6 router which is forwarding IPv6 packets and IPv6 firewalls which is also an important security mechanism, and it is functioning as packet filtering. Other network hardware such as interface cards, switches, and hosts are included.
- **Network Software**: includes the software cost for upgrading some network devices that will require working with IPv6.
- **Training Cost**: it is one of the most significant and changeable costs due to the need of keeping the network administrators up to the standard and also to keep the track of the upgraded hardware and software technology. The big challenge for the implementation of IPv6 is a lack of understanding of the benefit of IPv6; this is because of insufficient training on this protocol (Bouras et al., 2003).
- **Other Costs**: related to the implementation of IPv6, other IPv6 management and security costs are come up to enhance the implemented project.

Main et al. (2014) Support costs for infrastructure upgrades and deployment operations are mandatory. Upgrading infrastructure from IPv4 to IPv6 requires high costs. This is directly related to the deployment operation. According to Nguyen, Minh, and Anh (2012), the organization plans to initiate the IPv6 address transition needs to provide the significant budget used for planning, design, testing, training, and deployment costs.

Equipment

Considering infrastructure equipment is important in the preparation for the migration process. Especially network equipment (routers, switches, and firewalls) have a great role since they provide connectivity between different applications. Their compatibility with the IPv6 protocol is the key issue. There might exist a lot of legacy hardware should be upgraded or replaced during the migration process.

2.8.3.2 Human Factor

Motivation

The first important ingredient for the human factor is motivation. It contains factors makes motivate the organization to migrate to the new IPv6 protocol. As we saw earlier (refer to section 2.4) IPv6 has numerous advantages over IPv4. Those advantages mostly motivate the organization to start the migration process. Besides the advantages of IPv6, the key motivation behind IPv6 was the shortage of IPv4 address space. IPv4 is nearly exhausted and needs to be replaced by a newer version of IPv6.

Training

Internet Protocol Version 6 (IPv6) is the next version for IP and is considered a new technology. Therefore, training on this new technology is needed for an organization that has a plan for a migration. One of the big barriers to the adoption of IPv6 is a lack of adequate training for the IT staff members. IT staffs training is important if their knowledge is not sufficient for IPv6 migration and IPv6 by itself is more complex than the existing protocol (IPv4).

Knowledge

Besides IPv6 training, implementation knowledge in deployment strategy is needed by technical staff as a preparation to migrate. Technical IT staff needs to always keep up-to-date on IPv6 activities to gain knowledge on the latest deployment strategy. Main et al. (2014) also support the knowledge factor in deployment strategy, insufficient knowledge of the organization's migration strategy is an obstacle for the migration process.

Practical knowledge and experience are crucial factors and are also considered as the biggest challenges to adopt IPv6. For instance, configuring and managing IPv6 in different vendor devices also considered a problem if IT staff have sufficient skills. Staff members always need to develop their technical knowledge with the current state of technology.

2.9 IPv6 Strategies and Deployment

IPv6 implementation by itself is a long-term process with different challenges. To avoid common obstacles IPv6 implementation has five basic steps (Saklani & Dimri, 2013). IPv6 assessment of existing infrastructure is the first step to grasp basic information about the organizational network architecture. This step is very important for the second step, which is IPv6 address planning. Even though, IPv6 does not have a shortage of IP address like IPv4, addressing the plan not going to be an easy task for the network designer. IPv6 addressing is very much different from that of IPv4. The third step is looking at best practices for peer organizations how they deployed IPv6. Sharing their experience help the organization to solve a common problem inappropriate time interval. The fourth step is to come up with a good IPv6 security policy. This policy is useful to reduce the vulnerability of the organization through the migration process. The final step is to design and implement the migration paths. Those paths may defer from organization to organization and depend on the infrastructure they do have.

The other important task is setting up a typical IPv6 environment to able to test with IPv6 carefully. Because IPv6 is a very complex protocol and it differs from IPv4 in many areas. This separate test environment is also used for additional testing like new features embedded in IPv6. Moreover, it can be used for different IPv6 workshops and training purposes. After all documenting knowledge and experiences should be considered within the project team members.

Different organizations, such as ITU, IETF, Cisco, IEEE, and IPv6 forums proposed different adoption strategies (Chiniah, 2014). IPv6 implementation plan consists of two main components, namely, business planning and technical planning. In business planning, the organizations are identifying business motivation for the deployment of IPv6 and relate business aims to IPv6 interoperability. As such organizations should be well aware of the benefits, costs, and risks associated with the adoption of IPv6. The technical planning involves the process of finding out the hardware and software that requires an upgrade to support IPv6. It is a technical aspect of the organization's IT infrastructure towards IPv6 interoperability. This process might need only an IOS upgrade or replace the legacy device.

In the study conducted in Sri Lankan ISP networks, deployment of IPv6 is also classified into three phases: the preparation phase, transition phase, and post-transition phase (Jayasanka, 2015). The established approach was applied and effectively tested in IPv6 migration of Lanka communication (Pvt) Ltd backbone network. The preparation phase is highly focused on the finding of preliminary study and cost-effective methods. The preparation phase includes upgrade existing infrastructure, identify serious equipment, prioritize devices and applications, and find out list cost solutions for an infrastructure upgrade. Previously, cost challenges proposed by Arifin et al. (2006) for the migration were reduced in this developed approach due to the identification of critical network devices, firmware upgrade, prioritizing the upgrade, and well-organized millstones identified in the preparation phase. Also, consider this stage as the planning phase for IPv6 deployment, and contains how to create a migration process (Khudhair & Mohammed, 2017). Every network has its specification; therefore, a specific migration plan must be created for each case. As Khudhair and Mohammed (2017) say, to come up with this specification, a survey of the prevailing network facilities or equipment has a crucial role. Isolate the devices in the organization have to be upgrade or change. On the other hand, the transition phases more of the implementation of IPv6 planed in the preparation phase. It contains network configure migration mechanism and IPv6 addresses, configure AAA records needed for DNS, configure address translation in both IPV6 only and IPv4 only customer networks, and apply security configuration on firewalls. The final phase was the post-transition phase. In this phase, it applied to smooth options to reduce operational overhead. Since it is a fresh implement and a new technology, experts need to follow day to day operations.

2.10 Related Works

For the past decade, IPv6 development and migration issues have been addressed by several researchers, practitioners, and academicians. Related to this, several transition techniques, frameworks, and adoption plans and techniques were proposed. In this section, the researcher will discuss some relevant related works done by different authors.

Gizachew (2019) developed a migration framework that can be used to migrate IPv4 to IPv6 for Ethio-telecom. The study was conducted with a network infrastructure perspective. The proposed framework was adopted from Y.Cui with modification. It was modified based on the study finding in the research. The main challenges identified by the researcher are, device compatibility, legacy running in the network, network downtime management, and expertise. As a methodology, the researcher used a design science approach and structured interviews and questionnaires. The proposed framework also demonstrated using GNS3 and NS3 simulator tools. Overall, the framework is grounded on flow-based packet forwarding technology. The current study conduct in BIB is different from previous by its data analysis and framework components integrated into three phases. Data are collected using an interview from selected domain expertise to perform thematic analysis. The framework is not limited to technical migration for the company. It also integrates organizational-level factors that influence the migration process.

Matebie (2019) as well as developed a migration framework from IPv4 to IPv6 for Ethio-telecom. Unlike Gizachew (2019) the main intention of this study was to provide IPv6 transition for legacy applications and systems. The proposed framework aimed to use to facilitate the IPv4 to IPv6 application and system's transition in the context of the Ethio-telecom information system division. A design science research approach used with multiple data collection methods: semi-structured interviews and survey questionnaires. According to the researcher document analysis and observation were also conducted to identify the gaps and needs, based on which the requirements of the framework are formulated. Finally, the proposed framework is evaluated by domain expertise.

A descriptive study titled "*Framework for IPv4/IPv6 Translation*" discussed the NAT-PT translation technique (Baker, Li, & Yin, 2011). As discussed in the migration technique, this translation technique is categorized as automatic tunneling. According to the authors, the NAT-PT translation protocol is deprecated by RFC 4966. NAT-PT is not considered a viable medium or

long-term strategy for either coexistence or transition. A study noted that using NAT-PT as a general-purpose solution is bad for middle and large enterprises. Moreover, the authors offered a deep discussion on different transition technology; Dual-Stack, tunneling, and translator.

Another qualitative approach and inductive reasoning along with the design science approach are conducted by (Nguyen, Minh, & Anh, 2012). This study aimed to come up with the best transition approach from IPv4 to IPv6 for large enterprise networks. The study analyzed the experiences of several large enterprises that had deployed IPv6. The study analyzed the experiences of several large enterprises that have deployed IPv6, and the study finding reveals several significant factors that affected the IPv6 implementation project. The plan for the implementation of IPv6 has a vital role in the successful deployment of IPv6. A proper budget must be considered in advance including planning, design, testing, deployment, personnel training, and operational costs. Also, the study recommended that the human factor has a great role in IPv6 deployment. Project team members must be people who understand the internal network structure because they will decide which method of transition to apply. Choosing the right method will avoid many troubles for administration and the administrator must be the one who knows about IPv6.

A general overview of the migration technique is discussed by (Yousafzai et al., 2015). After its intensive discussion, the authors also come up with a holistic long-term migration technique by introducing a real testbed implementation scenario for a campus network. In their study, they performed the preparation, implementation, testing, and analysis of an IPv6 infrastructure testbed. Moreover, they also proposed major pre-activities for the design and implementation of an IPv6 network within a campus network. Their research methodology consists of four major phases:

- **Preparation**: In this phase, a survey was performed to check the existing network devices for IPv6 testbed support. Some infrastructure equipment could support IPv6, and others were upgraded to support IPv6.
- I**mplementation**: IPv6 addresses were assigned to the client computers and network devices. The IPv6 testbed infrastructure equipment included a Cisco router, Cisco switch, D-Link router, and computers.
- **Testing**: the researchers tested the network connectivity of the IPv6 testbed. First, they tested the IPv6 addresses that had been assigned to the network devices and client computers in their IPv6 testbed network. Following that, they measured the IPv6

connection bandwidth speed. Finally, they examined the validation and browsing of IPv6 websites.

- **Analysis of result**: they analyzed the result from the connectivity test to verify the setup of the IPv6 testbed by running such as ping.

An experimental study performed by Albkerat and Issac (2014) is trying to shed the light on IPv4 and IPv6 and assess the automatic and manual transition strategies of the IPv6 by comparing their performance to show how the transition strategy affected network behaviors. The experiment was performed using the OPNET tool that illustrates a network infrastructure. The experiment based on throughput, latency (delay), queuing delay, and TCP delay as a parameter. As a result, CPU utilization for manual and 6to4 is higher than IPv6, IPv4, and Dual-Stack because the transition technology generates more effort to encapsulate and de-capsulate. The Dual-Stack transition model found less delay with TCP. 6to4 and manual transition techniques, the delay is higher because the packets are not transferred directly as a Dual-Stack model. The throughputs of the four network simulations were analyzed using three different data rates: 1, 2, and 5 Mbps. The results show that IPv6 has a higher throughput than the other four, and for manual, it is higher than 6to4 to 5 Mbps. The 6to4 and manual strategies required manual configurations to detect the source, and the manual tunnel is required to have the destination detected build the point to point mechanism.

A case study in the Google enterprise network describes how IPv6 deployed incorporate network in a relatively short time with a small core team that carried most of the network, the challenges faced during the different implementation phases, and the network design used for IPv6 connectivity (Babiker, Nikolova, & Chittimaneni, n.d.). As a methodology the authors use four principles:

- **Think globally and try to enable IPv6 every-where**: in every office, on every host, and every service and application they run or use inside our corporate network.
- **Work iteratively**: plan, implement, and iterate launching small pieces rather than try to complete everything at once.
- **Implement reliably**: Every IPv6 implementation had to be as reliable and capable as the IPv4 ones, or else no one would use and rely on the new protocol connectivity.

- **Don't add downtime**: Fold the IPv6 deployments into our normal upgrade cycles, to avoid additional network outages.

As lessons learned from this deployment technique, since lots of providers still do not offer Dual-Stack support the CPE (customer-premises equipment), they had to use manually built GRE over IPSec tunnels to provide IPv6 connectivity for distributed offices and locations. Creating tunnels causes changes in the MTU of the packets. This often causes extra load on the router's CPU and memory, and all possible fragmentation and reassembly add extra latency. Another big problem was dealing with the end host OS immature IPv6 support. For instance, some of them preferred IPv4 over IPv6 connectivity by default. Some other devices do not turn on IPv6 by default, which makes the users of this OS incapable of testing and giving feedback for the IPv6 deployment. Regarding the organizational lessons, the IPv6 migration potentially touches everything, and so migrating just the network or just a single service or application or platform does not make sense by itself.

No.	Author	Title	Objective	Methodology	Finding
1.	(Kanth, 2016)	Comparative performance test on IPv6 migration technique: Tunneling	List out the existing protocol IPv4 and to uphold the need for IPv6 transition and experimentation in Tunnel-Transition performance by packet loss, latency, and throughput.	Experimental	Examine the feasibility of the transition by carrying out various experiments (based on packet loss, latency, and throughput) on transition strategies used while migrating to IPv6 (Dual-Stack and Tunneling).
2.	(Dell, 2018)	On the Dual-Stack transition to IPv6: A forlorn hope?	To the analysis of the Dual-Stack transition mechanism by which IPv6 diffusion.	Experimental	The Dual-Stack migration technique is unlikely to work, leaving the Internet with no workable

					means of achieving a transition to IPv6.
3.	(Thalmann & Harris, n.d.)	Internet protocol version 6 network migration and performance analysis	To review the IPv6 feature, a methodology, and performance measurements to aid and simplify migration and optimization concerns for IPv6 networks.	Design science	Structured migration methodology to aid the network migratory in choosing and implementing optima migration mechanisms.
4.	(Dhamale & Singh, 2018)	Migration from IPv4 to IPv6	To find out an answer to reduce delays in IPv6 implementation and propose a suitable transition mechanism for migrating from IPv4 to IPv6.	Experimental	Dual-Stack is a viable solution for an ISP to migrate gradually to IPv6. It offers the possibility for hosts to reach content in both networks because of its ability to run two protocols at the same time. Tunneling is not appropriate for an ISP because the protocol increases the latency in the network.
5.	(Hilles & Faniran, 2017)	Evaluating IPv4 to IPv6 transitions for a small enterprise in Nigeria	To give a deep understanding of the IPv6, and migration techniques. And also, to evaluate the ways to	Quantitative	Transition happens effectively in the organization. The best way without affecting the daily actions is a slow transition, by

			migrate from IPv4 infrastructure to IPv6.		running IPv4 and IPv6 simultaneously on an infrastructure.
6.	(Arifin et al., 2006)	An economical IPv4-to-IPv6 transition model: A case study for university network	To be a model or a useful guide for IPv6 migration in USM (UniversitiSains Malaysia) network as well as for other universities' network.	Quantitative	Cost assessment of IPv6 transition can assistance the IPv6 migration process. The overall transition cost estimation in USM is low. The highest cost occurs for labor, unpredictable, and management costs. The cost for hardware is low since USM just upgrade their cost switches and routers.
7.	(Jayasanka, 2015)	An approach for stable migration of IPv4 to IPv6 in SRI LANKAN ISP networks	To propose an elegant framework for migration of IPv4 to IPv6 in Sri Lankan ISP networks.	Quantitative	The developed method was applied and positively tested in IPv6 migration of Lanka Communication (Pvt) Ltd backbone network. By applying this transition technique, it was likely to advance the LankaCom backbone network to provide services to any customer who requests

					a native IPv6 network. The cost for this transition process was decreased due to the identification of serious devices, firmware upgrades, ordering the upgrades, and well-organized millstones. By using a framework, the migration was done without loosing the end to end connectivity via the backbone network for both IPv4 and IPv6 networks.
8.	(Yagoub et al., 2014)	Evaluation and comparisons of migration techniques from IPv4 to IPv6 using the GNS3 simulator.	To evaluate three transition mechanisms (Dual-Stack, tunneling, and translator) using latency and packet loss as a parameter.	Experimental	The tunneling migration is the best in ways of latency, packet loss, and RRT.

Table 2 - 3: Summary of related works

2.11 Chapter Summary

In this chapter, a researcher reviewed important points regarding IPv6 migration. The researcher introduced the two IP protocols (IPv4 and IPv6) and their basic difference in terms of IP address, packet structure, and their features. Also, a researcher tried to see the basic benefits of IPv6 over IPv4.

Globally, there are three categories of IPv4 to IPv6 migration techniques: Dual-Stack, Traffic tunneling, and Translator. Each technique has its advantage and disadvantage and it is not an easy task to select an appropriate technique and implement a selected technique for enterprises. Related to that, IPv6 migration has several challenges in terms of security, technical issue, and costs. Additionally, we tried to see factors and challenges affecting the migration process in the organizations.

CHAPTER THREE

3. RESEARCH DESIGN AND METHODOLOGY

3.1 Overview

In this chapter, the researcher intends to describe the research design and methodology used to achieve an appropriate result. Mainly, it covers and discusses the research methodology and approach, data collection techniques, data source, population size and sampling, and quality of the research.

3.2 Research Method

A research methodology is a process used to collect preliminary data for analysis and end up with a valuable output. It is the systematic and theoretical analysis of the methods applied to a field of study (Petra & Lietz, 2010). The research methodology is a hypothetical analysis of the main part of the methods and principles related to a branch of knowledge. It is the general research strategy that outlines how research is to be undertaken, and among other things, identifies the methods to be used in it.

The important part of the process of research is to select the appropriate methodology for the study (Igwenagu, 2016). There are several criteria for the classification of research types these include a method of research and the goal of research. Research methods depend on the type of research and the nature of the research.

Design science methodology majorly offers specific rules for evaluation and integration within a research process (Bisandu, 2019). Thus, this study aimed to develop a transition framework from IPv4 to IPv6 that can be evaluated and demonstrated. The following section will cover research design, approach, data collection methods, data source, data analysis and finally evaluating the proposed framework (artifact).

3.3 Research Design

Design science creates and evaluates IT artifact intended to solve the identified organizational problem, and build new or innovative artifacts for problem-solving or improvement attainment. The design science research process has six steps: problem identification and motivation, objectives for a solution, design and development, demonstration, evaluation, and communication (Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, & Samir Chatterjee, 2007).

The design science research methodology is a very good ground as a method in Information Science and Computer Science because it is a method that associate with human, organizational social kind of problem-solving through artifact development (Bisandu, 2019).

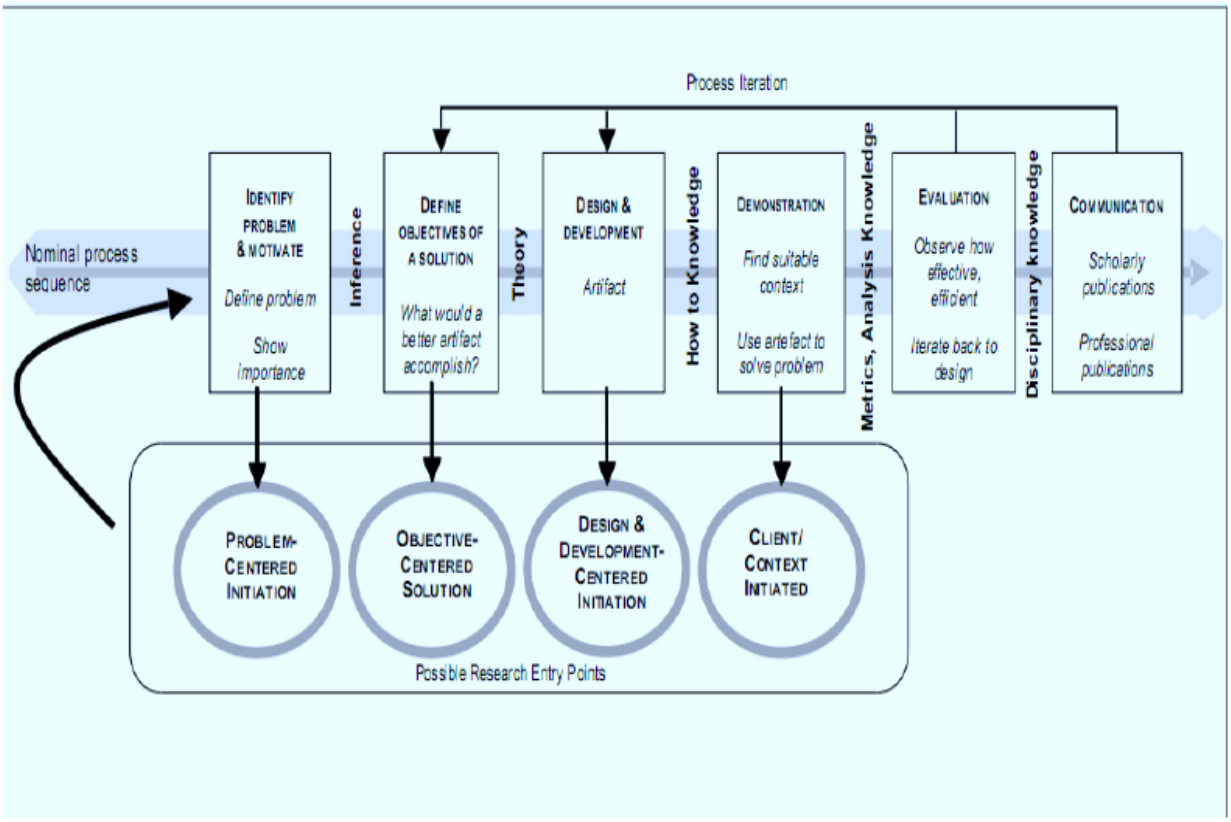

Figure 3 - 1: The design science research process, adopted from (Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, & Samir Chatterjee, 2007)

3.4 Problem Identification and Motivation

Ethio-telecom is the only ISP in Ethiopia and it on the way to transition to IPv6. Since BIB depends on Ethio-telecom infrastructure, the transition progress is a good motivation for BIB to prepare for this transition. A transition from IPv4 to IPv6 is a long-term process and needs a framework that guides for a successful migration.

In many countries, strong organizations are common to adopt IPv6 in their infrastructure. However, it has many challenges during the adoption process. The crucial factor for this problem is organizations don't have a transition framework that guides through the process. Moreover, the backward incompatibility issue of IPv6 to IPv4 and the dependency of the migration process on an organization's infrastructure lead to the need for an intensive investigation for the successful migration process. Thus, this process needs to be guided with a framework.

3.5 Objective of a Solution

As a solution, this study aimed to develop a migration framework that helps BIB to transit from IPv4 to IPv6 based on its infrastructure. To achieve this objective, the researcher collected relevant data via interview, document analysis, and observation.

3.6 Design and Development

Problems are identified from prior literature, and then the new artifact is being developed to solve those problems. Artifact, in this case, is a framework that helps or guide BIB to transit from IPv4 to IPv6. Additionally, the researcher also come up with a transition model that is suitable for the organizational infrastructure.

3.6.1 Data Source and Sampling

As Tongco (2007) argued, purposive sampling is used in specific skills, knowledge, or practices; comparisons between practices. The researcher used a purposive sampling technique for the interview. To develop a migration framework, expertise inputs are much valuable. Ten interviews are planned to collect sufficient information (see Table 3 - 1). The respondents are asked to offer descriptions of their experiences and knowledge regarding IPv4 and IPv6 from their organization's perspective. Those interviewees contributed to the research finding and answering questions posed by the researcher.

No. of participants	Participants Pseudonym	Position
1	InfraDir	Infrastructure and Security Director
1	InfraDivMgr	Infrastructure and Support Division Manager
1	ITSecDivMgr	IT Security Division Manager
2	NetEng	Network and Hardware Engineer
2	SenNetDatAdmin	Senior Network and Data Center Administrator
2	SenInfraExp	Senior Infrastructure and Support Expert
1	SenInfraSec	Senior Infrastructure Security Expert

Table 3 - 1: Organization of interview respondents.

3.6.2 Data Collection Method and Analysis

Data gathering is crucial in research, as the data is meant to contribute a better understanding of a theoretical framework (Etikan, Musa, & Alkassim, 2015). To achieve the ultimate objective of this study, the researcher used multiple data sources: primary and secondary data sources. From a primary data source, semi-structured interviews and observations are conducted. From the secondary data source, scholarly published articles, books, configuration files, and BIB's documents are included as a data source. Thereafter, a thematic analysis approach was performed to extract important concepts and finding for the study.

3.6.2.1 Primary Data Collection

Primary data considered as one way to measure and collect practical and personal experiences. Interview and direct observation are an example to collect this type of data. The researcher used two techniques to collect its primary data: Semi-structured interviews and observation.

Interviews

The researcher used interviews for individuals who agreed to participate in the research. Data are collected using semi-structured interviews intended to conclude senior domain expertise and middle-level management. For instance, infrastructure and support division managers gave

relevant information about their network infrastructure how looks like and the technology they have used. Senior managers like infrastructure and security directors gave information about the long term and short-term planning concerning IPv6 implementation by considering security threats. The interview question was adopted from (Kaur, 2015). It was modified as per the need for this study. Interviews were all face-to-face with a time range of 40 - 60 minutes per respondent. After conducted one interview and took notes for each participant, the process of writing a complete transcript from the note was performed. Therefore, the loss of information is avoided.

Instrument development

The first part of the interview guide is about to grasp some important information about the respondent. The respondents are expected to describe their working experience and current working environment with their responsibility. This helps the researcher to understand the depth of their knowledge, skills, and experience in the domain.

The second part of the interview guide is focused on infrastructure equipment that exists in the organization. This part was added by the researcher in the interview guide. The main aim of this part is to assess infrastructure equipment that exists in the organization towards to IPv6 protocol and create an overview of the current infrastructure. Moreover, the infrastructure assessment helps the researcher to demonstrate the proposed transition technique in the study and also to measure the capability of the infrastructure to adopt IPv6.

The third part of the interview guide is all about the motivation of the organization to deploy IPv6 in its infrastructure and it is also added by the researcher in the interview guide. In this part, the researcher aims to collect different motivations explained and discussed by respondents to align with organizational benefits get from deploying IPv6 over IPv4 protocol.

The company's current status and its planning process is another part of the interview guide. This helps the researcher how organizational planning is performed before adopting IPv6 in the organization. This is also assisted by the workflow exit in the organization while deciding on IPv6 adoption in the organization.

Collecting factors affecting the migration process from IPv4 to IPv6 also an important part of the interview guide. Those questions aim to select and identify the factors that have an influence on the IPv4 to IPv6 migration process in the organization. Therefore, it has a vital role in the development of the framework.

Cost constraints related to the migration process, the effect and extent of staff experience and knowledge, and the role of training in the adoption process also another important point in the interview guide. Besides that, security concern in the migration process has a vital role in the migration process (Khudhair & Mohammed, 2017). Thus, security and IT policies related questions are incorporated in the interview guide by the researcher.

Finally, the interview guide focused on selecting appropriate transition techniques for the organizational infrastructure. Respondents have a good opportunity to describe and justify by proposing appropriate transition techniques from well-known transition mechanisms.

Observation

The researcher used a structured observation method in DC, DR, branches, and head office. It has been approved by the BIB's Infrastructure and Security Director. During the observation process, the researcher had one chance of visitation for each domain. Each visitation took more than an hour. This is considered adequate for the study and helps the researcher to have direct access to research phenomena.

The goal of observation in this study is to grasp the current status of BIB regarding IPv6. How the DC and DR are structured and how infrastructure components are connected, how branches and head office infrastructures are linked to DC, and how they look like. Furthermore, it helps to triangulate data collected from the document and expertise interview.

3.6.2.2 Secondary Data Collection

By using secondary data collection, it is possible to use data collected earlier by other researchers or for other purposes. This includes published articles, organizational records, and documents kept routinely by the organization.

Literature Review

A literature review has been conducted as discussed in chapter two. A researcher first went to review other literature related to the study area. It includes the current knowledge of IPv6 including a substantive finding by other authors. Using literature, the researcher grasped data that shows the current knowledge in the IPv4, IPv6, and their migration. This helps to know the current stage or state of technology. The researcher tried to identified IPv4 to IPv6 transition techniques and what they can capable to do. The researcher also tried to look up the best experience shared by a medium and big organization when they deployed IPv6 in their infrastructure. Using this secondary source, it has been also tried to extract factors to adopt IPv6, IPv6 adoption strategies, and three major transition methods with their advantage and disadvantage.

Document Analysis

The second data source from secondary data for this study is BIB's document and configuration files. Previously as the researcher mentioned data was collected using observation in DC, DR, branches, and head-office. To support those observations, important documents are reviewed on the architectures and designs of those sites, and protocol used.

The other vital documents are reviewed on IT policies and procedures in BIB. Those documents gave for the researcher BIB's long-term achievement regarding IT projects and support the interview questions performed by the researcher.

Besides the observation, DC, DR, and branches infrastructure design and layout are put on as a form of a document. These documents show how infrastructure components are interconnected with each other and help to strengthen data obtained during observation. Proportional to physical IT infrastructure architecture, there are logical designs. Most of the logical designs are put as configuration files for production servers and network components. The researcher also visited those configuration files to understand the logical structure of sites and IP related protocols used. However, for organizational security reasons, those pieces of information are not attached to this study.

3.6.3 Quality of the Research Design

Data triangulation was performed by collecting data from different sources. It used more than one method to collect data on the same topic. The researcher used four methods to collect data on its study: literature, document analysis, observation, and interview. This helps the researcher to capture different dimensions of data to the same study. This is helpful to perform triangulation and reached a final result discussed in the phenomenon. The reason for taking the data from those different sources is to achieve an in-depth understanding of the collected data, and the researcher is capable of confirmed that there is no misunderstanding or misinterpretation of the respondent's ideas.

Pilot Testing

As Igwenagu (2016) pointed out, it is common for the researcher may find out that the available information is so scanty that embarking on the study might result in a waste of money and efforts without necessarily achieving the objective. The study is rich in interviews and offers detailed information in understanding the participant's experiences. Therefore, performing pilot testing on interviews is an important part to test the questions and to gain some experience in interviewing for the researcher. Thus, it becomes desirable then to carry out the preliminary study before the main study.

According to Majid, Othman, Mohamad, Lim, and Yusof (2017) pilot testing has five steps: determine interview questions, have the initial interview questions reviewed by experts, selecting the participants, piloting for interviews and report the modification made on it. In the first step, the researcher established open-ended questions related to IPv4 to IPv6 migration. Those questions are reviewed by domain-expertise and language expertise. Domain expertise gave relevant information regarding the generic concept of IPv4/IPv6 and correct irrelevant language usage. The questions are modified accordingly gained by expertise recommendation. Three participants are selected from a total of ten participants. The three participants are selected purposively considered as an expert founded in managerial and senior level in BIB. The pilot study was conducted on three selected respondents between May 4, 2020 to May 7, 2020. Each interview took 20 minutes. During the test, the researcher grasps some experience in conducting the semi-structured interview and some inputs from expertise to the interview questions.

3.7 Demonstration

Once the transition framework has been developed; a demonstration is performed to measure the efficiency to solve problems. This step is an important part of a design science approach since many participants are afraid of using new technology. Running a demonstration using a simulation tool makes it easy to understand the capability and manageability of the IPv6 protocol for the study participants. The other important thing about this demonstration is to give the overall picture of the framework before the real implementation of the production or their testbed. Therefore, research participant expertise grasps major configuration rules in the IPv6 world.

The demonstration is done using the GNS3 experimental tool to simulate the framework. It is open-source software that can be downloaded and used for free. Thus, it has no limitation on the number of devices supported and it can simulate and run a real image of devices. This simulation tool does not need an external resource. It supports Windows 7 and above, Mac OS (version 10.9) and above, and Linux operating system. The researcher used the Windows 10 operating system to run a framework demonstration.

3.9 Evaluation

The evaluation was performed by domain experts to improve the framework. The researcher tried to measure how the framework assists IPv4 to IPv6 migration process in BIB. This activity involves comparing the objective of the study to the actual observation result from the framework in the demonstration. Additionally, evaluation is supported by performing a satisfaction survey to expertise. This satisfaction is supported by using an ISO/IEC 25010:2011 quality requirement and evaluation.

3.9 Communication

After the researcher developed a framework, the final output explained the idea and thought process behind the work. In this process, Senior IT management, Network Engineers, Network and Data Center Administrators, and other infrastructure experts in BIB are included. Moreover, this section also includes a thesis report and presentation to the Department of Information Science. Finally, the study article will be published in the journal for the rest of the community.

3.10 Ethical Concerns

The researcher considered various ethical concerns while performing this study. These ethical issues are mainly based on the materials and sources used as references are properly acknowledged, and confidentiality of the respondents, documents, configuration files are kept and used only for academic purposes of the study.

3.11 Chapter Summary

In this chapter, the research methodology used for this study was presented. Accordingly, as a research strategy and study area, a case study is selected. The research approach employed was design science. In its research method, data were collected using articles, semi-structured interviews, document analysis, and observation. Thematic analysis is performed for data collected using interviews from the identified respondents. Eventually, a proposed framework was evaluated and demonstrated using the ISO/IEC 25010:2011 and GNS3 simulation tool.

CHAPTER FOUR

4. INFRASTRUCTURE SURVEY

4.1 Overview

As Yousafzai et al. (2015) suggested, the survey of the existing network infrastructure is an important task before starting the real migration plan and implementation. Survey the current infrastructure has a vital role to develop a migration framework as well as to select a transition technique (Main et al., 2014). The researcher performed its infrastructure survey in BIB's network architecture to get a holistic view of the organization. When we talk about BIB's network architecture, it is all about the design of a communication network and its peripherals. It is a structure for the specification of a network's physical components, functional organization, and operational principles and procedures. In this section, the researcher is tried to investigate BIB's infrastructure before start the data analysis obtained from respondents. Physical components, network layout and topologies, and connections between branches and head-office to the data center are included. Thereafter, the willingness of BIB's infrastructure to adopt IPv6 in terms of the technical approach is evaluated. This survey is conducted using observation, document analysis, and expert interviews.

4.2 Data Center Survey

4.2.1 Data Center Architecture and Design

BIB's DC is home to the computational power, communication, storage of data, and application. This infrastructure is the biggest asset of BIB and a focal point in its IT architecture. A careful design of the data center infrastructure is important and even has a direct impact on its performance, resiliency, and scalability so that it needs to be carefully considered.

Data obtained from SenNetDatAdmin and design document shows, BIB's data-center network design is based on two layers' approach: core/distribute and access layers.

According to him: *"…The data center is considered as a tier-three data center. However, it has two layers: collapsed distribution/core, and access layers."*

Core-layer: This layer provides the high-level-speed packet switching backplane for all flows going in and out of the DC (see Figure 4 - 1). It provides connectivity to multiple aggregation

modules and provides resilient layer 3 switches that provide no single point of failure. It also supplies a high-speed connection to the access layers, servers, and edge routers. Redundancy is implemented to ensure a highly available and reliable to the backbone.

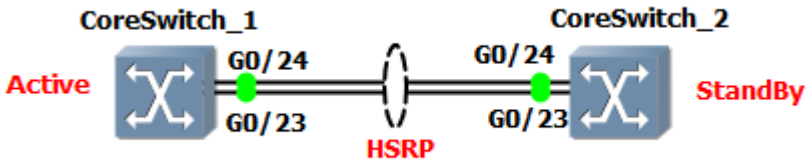

Figure 4 - 1: Core switches architecture

As we can see from Figure 4 - 1 G0/24 and G0/23 are aggregated (ether-channel ports) links that are dedicated to the purpose of the two core switches for clustering. This cluster used the HSRP protocol. This ether-channel port is connected using 10 Gbit UTP cables to listen to their heart-bit and those core switches are directly connected to the production servers using SAN switches (Sparc T8-4). The Core-application solution the so-called "*Finacle*" is deployed on those servers and offered high connectivity by this layer. When we come to the DR site, one core-switch is dedicated to a core layer (see Figure 4 - 2).

As a whole, the following are actions performed in this layer:

- Implemented IPv4 access-list, IPv4 packets filtering and queuing,
- Deployed IPv4 Security and network policies,
- Routing between VLANs and another workgroup, and
- Defined broadcast and multicast domains.

Access-layer:

The access-layers founded within a BIB's DC and DR sites are performing and monitor data exchanges between the nodes and the core-layer. It defines how a certain host accesses or join the rest of the network.

It also interfaced with IT-users from different workgroups and provides uplinks to the core layer. DC and DR design document shows, devices that exist in this layer are layer-two switches (See Figure 4 - 2), nothing do with IP protocol at all. This layer allows authorized IT-users to access

the rest of the infrastructure components in DC and DR using the MAC addresses. The main users are IT-user's workstations.

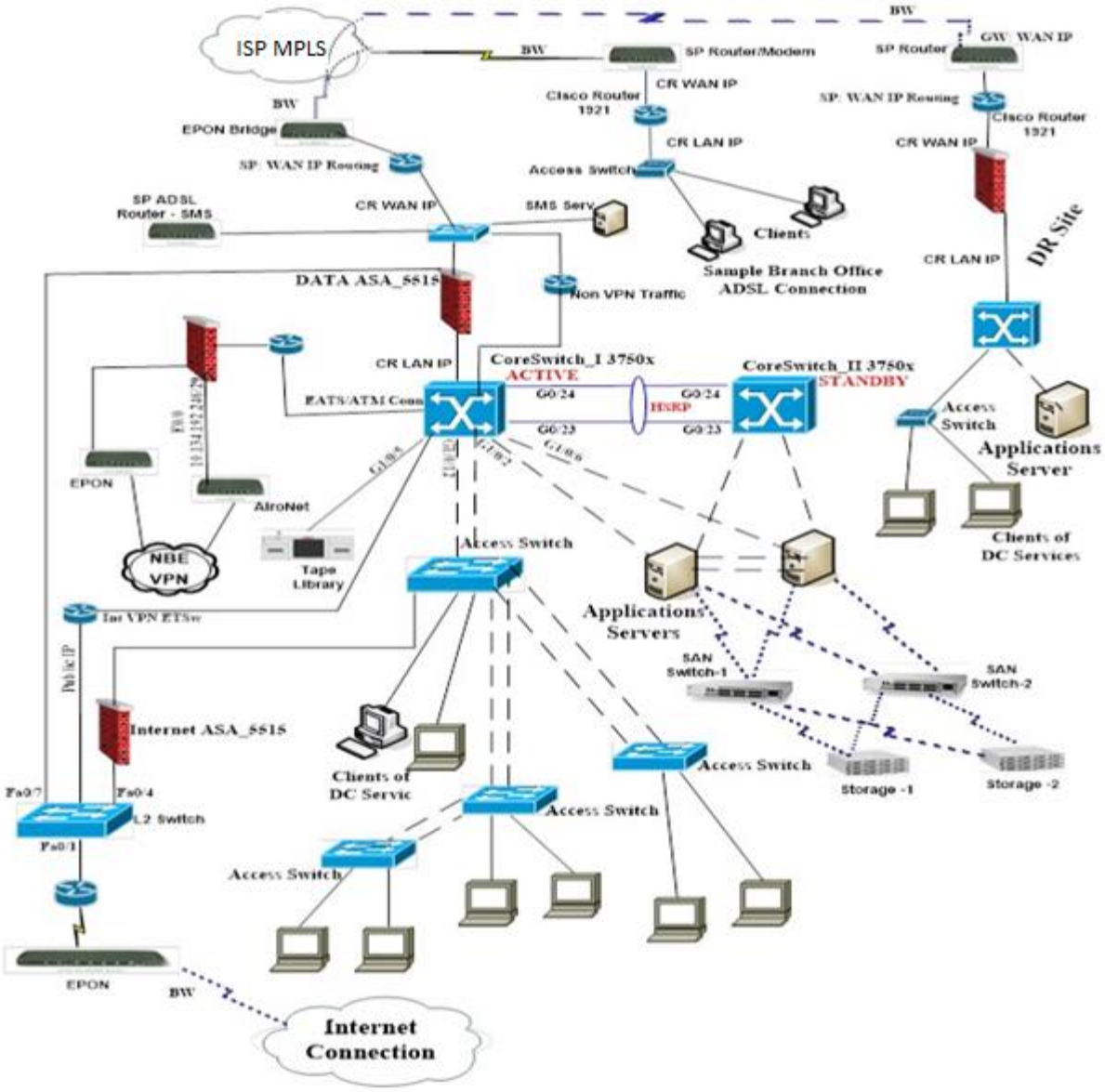

Figure 4 - 2: BIB's Data Centre and Disaster Recovery Sites Design

4.2.2 Connecting Device

A connecting device commonly refers to as networking devices and has different roles to play in a computer network. They also work in different segments of the network performing different works. In BIB's DC different connecting device are categorized as below:

- **Routers**: BIB used Cisco edge 1900 routers at the edge of the DC and DR.
- **EPON (Ether Passive Optical Network)**: provided by the ISP, capable to support fiber transmission and routing used for connecting the DC to 230+ branches.
- **GPON**: an optical device used to connect DC to the rest of the branches by using fiber technology.
- **SAN switches**: a type of fiber switch used to connect servers and pools of storage exists in the storage device.
- **Firewalls**: Control transaction traffic performed by core application, filtering Internet traffic generated by the end-users, and used to guard the DC and DR.
- **Layer 2 Switch**: a device used to transfer traffic or frames using MAC addresses in a local area network (LAN).
- **Layer 3 switches**: It performs high-speed packet transferring by combines the functionality of a switch and a router.

NetEng: *"… Our network equipment is from Cisco. They need a small change or upgrading their IOS to support IPv6. With my best experience, ISP equipment is also capable to configure with IPv6 protocol. Even though, they are owned and configured by ISP…"*

4.2.3 Computing Device

The computing devices are any electronic equipment controlled by a CPU, including desktops, laptops, and servers. The organization uses different models as computing devices in both the DC and DR sites. They can be classified into five categories:

- **Application servers**: Servers to run the application in BIB.
- **Web servers**: Web-logic is used as a web server presented virtual machines.
- **Database Servers**: Virtual machines provide raw data for core-application.
- **Tape Libraries**: is a high capacity storage system used for storing and retrieving BIB's customer data.

- **Storages**: Used by the servers that are used to store, access, and manage digital data shared over a network.
- **Hardware load-balancer (HLD)**: used to share out traffic across application servers on the subnet.

InfraDivMgr confirmed storage devices support IPv6 protocol by said "*.... Oracle is our vendor for production servers, tape libraries, and storage. Besides their huge computing capability, they also support IPv6 protocol ...*"

SenInfraExp: *"... Like other operating systems, Solaris 11 can support IPv6 on Sparc-T8 servers."*

4.3 Branch and Head-office Survey

BIB's infrastructure is not limited to DC and DR. It has also an infrastructure on branches and head-office. In this survey, the researcher first takes a look at the branch's infrastructure, subsequently, head-office will be continued.

4.3.1 Branches Infrastructure

Herewith, the researcher is tried to put the overall architecture in branches. Figure 4 - 3 shows a topology of how the network devices and computers are connected. The edge-router is responsible for filtering traffic comes from inbound and outbound using a standard access-list and made some route between private and public IPv4 address. With an average, each branch has five hosts, one unmanaged switch, and the one edge-router. The edge-router connected one interface to BIB's LAN, another to WAN provided by ISP. Thus, traffic generated from local BIB's LAN is routed to ISP public IP address and vice-versa. The following are infrastructure components that exist in each branch.

- **ADSL (Asymmetric Digital Subscriber Line)**: provided form ISP to connect all branches with the DC, uses copper as transmission media.
- **Edge-Routers**: BIB use Cisco edge 1900 series routers interfaced with ISP's ADSL.
- **Unmanaged Switch**: allow devices to connected without network administrator configuration and perform a frame switch.
- **Hosts**: User's computers and printers used by BIB's staff members.

- **ATM (Automatic Teller Machine):** allows people to take out their money from BIB's account by using their card.
- **POS Machine (Point of Sale Terminal):** electronic equipment used to facilitate card payments in different locations.

SenInfraExp: "*BIB has more than 50 ATMs and 34 POS machines distributed throughout our county. All ATMs are supported by both IPv4 and IPv6 protocols. Even though, POS machines are only supported IPv4 protocol. "*

SenNetDatAdmin elaborates unmanaged switch exists in infrastructure as "*... We used unmanaged switches from Cisco and 3com vendors in each branch. Since they are unmanaged and layer two devices, they cannot support both IPv4 and IPv6 address schema. However, it is not the problem at all, BIB considered one branch as one subnet."*

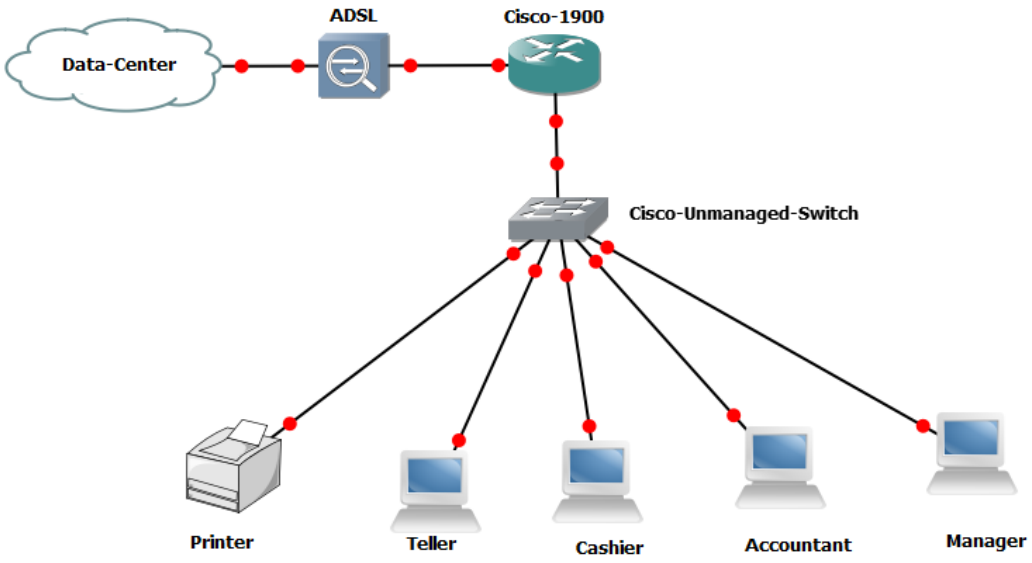

Figure 4 - 3: BIB's Branch Network Design

4.3.2 Head office Survey

4.3.2.1 Head office Infrastructure

Unlike branches, head office network architecture has physically isolated LANs. As we can see from figure 4 - 4, there are two major users, applications and Internet users. The application users are users dedicated only to use core-application solutions (Finacle) and other homemade applications, whereas, Internet users perform some activities related to the business on the Internet. This reduces external attacks that might come from the external domain.

Similar to branches, edge routers are responsible to perform NAT, and traffic filtering using an access-list. Traffic passing through the edge router is inspected and filtered by the firewall attempting to pass through it. Also, unwanted traffic forbidden by BIB's security policy generated from end-users is blocked.

NetEng tries to reflect the similarities of head office and branch infrastructure as: *"Head-office network structure is more or less similar to branches except for its layer-three switch that gave high packet routing and switching …. "*

Two application servers are directly connected to the core-switch and accessible by the users located in each VLAN. Overall, six VLANs are architected based on the organizational department. Communications between those VLANs are performed by a layer-three switch using inter-VLAN switching technology. The core-banking solution is accessed from the head-office passed through Ethio-telecom MPLS.

SenInfraExp: *"… SMS and HRMS systems are frequently accessed by human resource and Finance directorates. They exist in two separate servers in the head-office mini-data center."*

The edge router is directly connected to the core-switch responsible for making a route to the ISP infrastructure. The core-switch is dedicated to performing VLANs and inter-VLAN switching to enhance network performance. Six layer-two switches act like an access-switch and two application servers are connected to it. As we can see from figure 4 - 4, there are six VLANs designed per department.

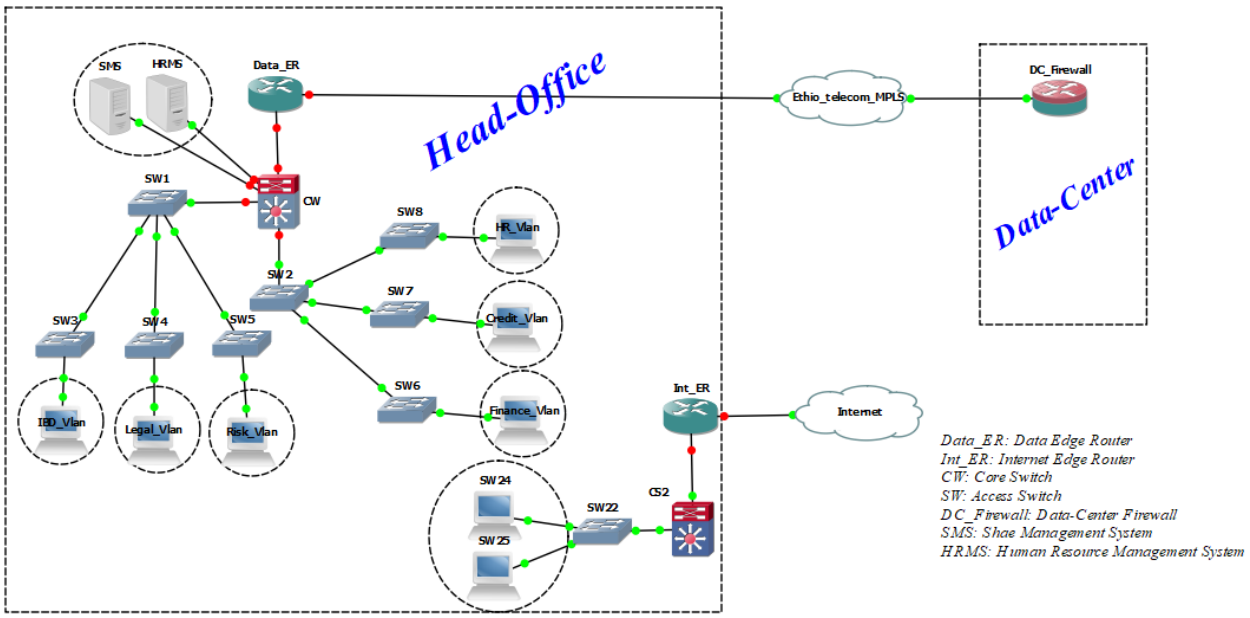

Figure 4 - 4: BIB's Head-Office Network Design

Since it is a production network, static routes are configured when some particular subnet tries to navigate to another. The network administrator defines and specifies the traffic flow from source to destination and vice versa. This method enhances the performance of the network and security.

Generally, BIB has a combination of computing and network devices in its DC, DR, branches, and head-office sites. In the current state, most infrastructure equipment supports both IPv4 and IPv6. Table 4-1 shows detailed information on those devices.

No.	Infrastructure Equipment	Sites	Quantity	Support IPv6
1.	FortiGate 900D	DC & HO	2	yes
2.	Edge-Router	DC, DR & HO	6	yes
3.	ASA 5515-x Firewall	DC &DR	3	yes
4.	Tape Library	DC	1	yes
5.	ZFS Storage Server	DC & DR	3	yes
6.	HP Proliant DL380P Gen 8	DC	1	yes
7.	SAN Switch	DC & DR	3	yes
8.	Sparc T5-2 Servers	DC	3	yes
9.	Sparc T8-4 Servers	DC&DR	3	yes
10.	F5 hardware Load Balancer	DC	1	yes
11.	Core Switches	DC, DR & HO	5	yes
12.	POS machines	BR	34	No
13.	Layer-two Switch (Unmanaged)	BR	250	No
14.	Layer-two Switch (managed)	DC, DR & HO	25	yes
15	User computers	HO & BR	1500	yes

Table 4 - 1: Summary of BIB's infrastructure equipment.

4.4 Chapter Summary

In this survey, we have seen the general overview of DC, DR, and head-office and branches' infrastructure structure. DC has mainly two layers: core and access layers. On those layers, we also identified computing and connecting devices that were assumed affected by IPv6. Unlike DC branches and head-office infrastructure is not classified by layer. However, they have many numbers of infrastructure devices compared to DC and DR. Generally, the survey result show that most devices have capable to support IPv6 except POS machines and unmanaged access switches. Thus, overall BIB's infrastructure has a technical capability and to adopt IPv6.

CHAPTER FIVE

5. DATA PRESENTATION, ANALYSIS, AND DISCUSSION

5.1 Overview

In this chapter, the researcher performed data analysis and interpretation that of data collected through interviews, document analysis, and observation. The interpretation helps to find the motivation to migrate from IPv4 to IPv6 in BIB, after that, the main factors that should be considered for this migration process have been identified. Finally, from well-known transition techniques, the researcher proposed the best transition model that is fit for BIB.

5.2 Data Presentation

The researcher performed basic themes before analyzing, interpreting, and discussing the data. As the researcher planned earlier, data is collected from articles, expert interviews, observation, and document analysis. This makes the analysis process effective for the researcher. The semi-structured interview questions made the respondent flexible for their answers. Data collection from interviews is performed by taking notes and categorizing the information related to each other for analysis. Finally, the interpretations are used to produce the final report by the researcher.

The researcher identified to interview the infrastructure and security director, infrastructure and support division manager, IT security division manager, senior infrastructure and support experts, senior network and data center administrators, senior infrastructure security experts, and hardware and network engineers. The researcher believes those experts have detail knowledge and experience within the domain and aimed to offer detailed information on the sector.

Besides the collected data from BIB's respondents, the researcher also revised files related to configuration and other relevant related documents. Additionally, the researcher observed the current BIB's infrastructure.

5.3 Case Study Analysis and Findings

In this section, the cases for IPv4 to IPv6 migration process components are discussed in detail that is derived from data collected by interview, document analysis, and observation to achieve the research objectives and answer the research question specified in chapter one.

5.3.1 Motivation to migrate from IPv4 to IPv6

According to the respondent's feedback, migration from IPv4 to IPv6 had three motivations. Those motivations are external forces, technological advancement, and competitive advantages. In this section, those motivations are presented.

5.3.1.1 External forces

External forces are considered as an outside driving force that motivates BIB to move from IPv4 to IPv6. Ethio-telecom has a great role and impact on the migration process at the national level. However, its role is not always necessary for an organization to adopt IPv6. Remarkably, there are two types of IPv6 adoption approach: top-down and bottom-up. The top-down approach recommends that first, the ISP will migrate its infrastructure to IPv6 then it will allocate its services and IP address to the rest of the organization that exists in the country. Throughout its long-term strategy, organizations will be sucked into ISP's IPv6 infrastructure. Unlike the top-down, the bottom-up approach follows the reverse one. Organizations can adopt IPv6 before the ISP. This happens when organizations become mature and strong enough with their infrastructure to adopt IPv6 before the ISP. The ISP's MPLS infrastructure stays on the IPv4 protocol and transmits the IPv4 payload. By using different transition techniques ISP's infrastructure can be pass while the organization communicates with each other. Finally, most of the organizations become IPv6 based infrastructure and overwhelm the ISP MPLS. Thus, ISP will force to adopt IPv6 on its infrastructure.

Most of the respondents have argued Ethio-telecom has a great motivation in IPv6 adoption for BIB. According to InfraDir: "*Ethio-telecom is expecting to shift its service from IPv4 to IPv6 soon. It is a matter of time. At that moment, every organization including BIB will be forced to adopt IPv6. It will start to offer IPv6 addresses rather than IPv4 addresses.*"

InfraDivMgr commented: "*Since Ethio-telecom has a strong argument to move from IPv4 to IPv6, so we do have to do the same.*"

SenNetDatAdmin also put his idea: *"Since Ethio-telecom is the only ISP exist in our country, its infrastructure migration will consequence a serious impact if we are not ready for the transition.*"

Even though most of the respondents believed that Ethio-telecom had a great motivation for the IPv6 migration, data collected from Network Engineers reflects the fact that ISP's role is minimum in the IPv6 migration process in BIB.

NetEng stated: "*In developed countries, the bottom-up adoption mechanism is a common migration approach. Organizations are strong enough and give attention to adopting new technologies. We don't have any special reason to ignore IPv6 adoption in our organization."*

The migration process is not just a short-term process. It needs iterative development in its adoption process. To do so, BIB needs to be in a position to navigate its infrastructure to IPv6. Using IPv6 addresses, BIB will start to implement in its infrastructure partially. First, it will try to connect its DC and DR with the rest of the branches. Branches are now the main focal point for the customers. Throughout the gradual process, each section will be migrating to IPv6.

5.3.1.2 Technological advancement

As several pieces of literature mentioned, the main reason for the birth of IPv6 is the shortage of IP addresses. IPv6 has a lot of advantages at the side given that the huge amount of IP addresses. Those advantages are mature enough in BIB to adopt IPv6. Data collected from the interviewees and articles exposed the fact that IPv4 has become a depreciated protocol. For instance, according to RFC: 6814, many IPv4 options have become obsolete in production or real-time practice. However, those options have not been formally deprecated. Deprecated features in IPv4 protocols are stream ID, extended Internet protocol, traceroute, ENCODE, VISA, address extension, selectively directed broadcast, dynamic packet state, and upstream multicast packet.

Considering the above fact, IPv4 has served the communication world for many decades with its disadvantages and it is also becoming a historic protocol. However, it doesn't mean that IPv4 is outdated and not supported by RFC. RFC still publishes some of the IPv4 updates when it is necessary until IPv6 overtakes the whole communication. This protocol can be used with its drawback when the network administrator understands the risks and the consequences come on performance and security in an organizational network.

Most of the infrastructure equipment from different vendors becomes to support IPv6. In chapter four, the researcher's assessment of BIB infrastructure also shows the majority of devices have supported this protocol. This shows the IPv6 technology turns into well famous and aimed to

overcome IPv4 technology. As one Network Engineer commented that, there is less attention on IPv6 technology.

He commented: *"Organizations including BIB are not common in adopting IPv6. They think it is worthless unless they run out of IPv4 addresses. They remain in IPv4 protocol unless they are pushed by a government or regulatory body.*"

Technology by its nature is dynamic and its advancement is always in progress. Data from most participants shows that the advancement of technology is reflected in infrastructure equipment and equipment vendors gave a huge emphasis on IPv6 technology.

SenNetDatAdmin explained how vendors gave attention to IPv6 technology by saying "*Since I have been working as a Cisco trainer, Cisco expands its training and certification exams enormously to IPv6 protocol. This implies the protocol becomes well-known and expertise needs to give attention to the technology*."

SenInfraExp: "*Technologies are changes radically through time. Most of the vendors including Cisco and Oracle are capable to support IPv6."*

Articles like Zakari et al. (2019) justified IPv6 has more network performance than IPv4. Moreover, most of the respondents confirmed that IPv6 has more efficiency in routing and packet processing. It also supports new services and enhanced security.

NetEng "*I believe IPv6 comes up with a better performance in routing and packet processing than IPv4.*"

SenInfraSec *"Security is an important concern in communication. IPv6 minimizes the security risk that comes from cyber-attack."*

Starting from vendors to training centers IPv6 adoption is accelerated. This new technology is becoming a compulsory protocol in communication. This technology comes up with much advancement over the legacy protocol. Since it is important in communication, it is adopted in many computing, communication, storage devices, and other infrastructure types of equipment. The technological advancement and benefits get from this advancement inspire BIB to adopt or migrate to the IPv6 protocol.

5.3.1.3 Competitive advantage

Implementing or moving to IPv6 provides competitive advantages for BIB. As we discussed in chapter three, IPv6 by itself comes up with a lot of advantages over IPv4. Thus, it has technological advancement, packets are more efficient routing and processing in this protocol, and traffic congestion is significantly reduced in the infrastructure. This has a huge role in the day to today bank's transaction. With the current competitive business environment, customer satisfaction is a crucial factor. Only accessibility of the bank's service to the customer is not enough nowadays. Customers need their money at any time and place whenever they need the service. InfraDir also justified this by saying: "… *Operational excellence is put as a term to achieve the bank's long-term strategy*"

NetEng explained the performance of IPv6 over IPv4 by saying: "*In theoretical and in technical speaking, IPv6 reduces the size of the routing table that makes the routers to find a specific path with a short period. This what we called summarization in IPv4 protocol. It aggregates two or more subnets are taken together to one super-net to reduce the routing table in routers*."

SenNetDatAdmin: "*IPv6 eliminates IP-level checksum in its structure. This reduces to recalculate at every hop. Our routers should be busy with their primary functionality.*"

SenInfraExp mentioned a big concept on IPv4 vs IPv6 broadcast capability: "*IPv4 is famous for its broadcast capability. It sucks your network bandwidth if your infrastructure is designed improperly. Multicast features of IPv6 reduce bandwidth usage by getting rid of the broadcast idea."*

The SenInfraSec has reflected IPv6 end-to-end connection: *"NAT is eliminated and true end-to-end connectivity at the IP layer is restored."*

InfraDivMgr: *"NAT also slowing down your network and has a problem with its usage in the long run in the organization. I believe the organization will be beneficial to invest in IPv6."*

The ITSecDivMgr also explained why IPv6 is more secure than IPv4: "*One of the best flavors of IPv6 is IPSec. It provides confidentiality, authentication, and data integrity. This helps us to secure the payload end-to-end transmission.*"

Customers worry about how secure is their money. There is much in the news about different threats and attacks performed in the financial sector. Customer confidence in BIB is a critical juncture. IPv4 has an absence of end-to-end connection and a lack of security (Oxley, 2014). One of the potential threats identified in the banking sector is a cyber-threat. Cyber-security is very important to secure the bank's transaction and protect customer's assets. Besides that, channel banking like mobile, Internet, and agent banking has become important for the customer, and also BIB gives attention to those services. Stabilizing and securing infrastructure enhance BIB's operational excellence to achieve its long-term strategy. Moreover, it provides competitive advantages over others.

5.3.2 Factor Affecting for Migration Process

Migration from IPv4 to IPv6 is a long way process especially for large organizations like BIB. During this process, many factors should be considered for the success and failure of a migration process. Considering those factors is a crucial thing for the successful adoption of IPv6 in the organizational infrastructure and ingredient for the migration framework proposed by the researcher. In this section, we will see those all factors identified in the study, which are an individual factor, organizational factor, physical factor, and security factor to implement IPv6.

5.3.2.1 Individual factor

The individual factor is a factor that is directly related to the capacity of employees that exists in the organization. This capacity is expressed in terms of knowledge, skills, and training. An employee's quality has a direct impact on the success and failure of the IPv6 migration process in BIB. IPv6 technology needs a technical capability to implement IPv6, and how to operate once it is deployed. Furthermore, IPv6 is a new technology and needs some domain expertise before migrating to IPv6 in an organization.

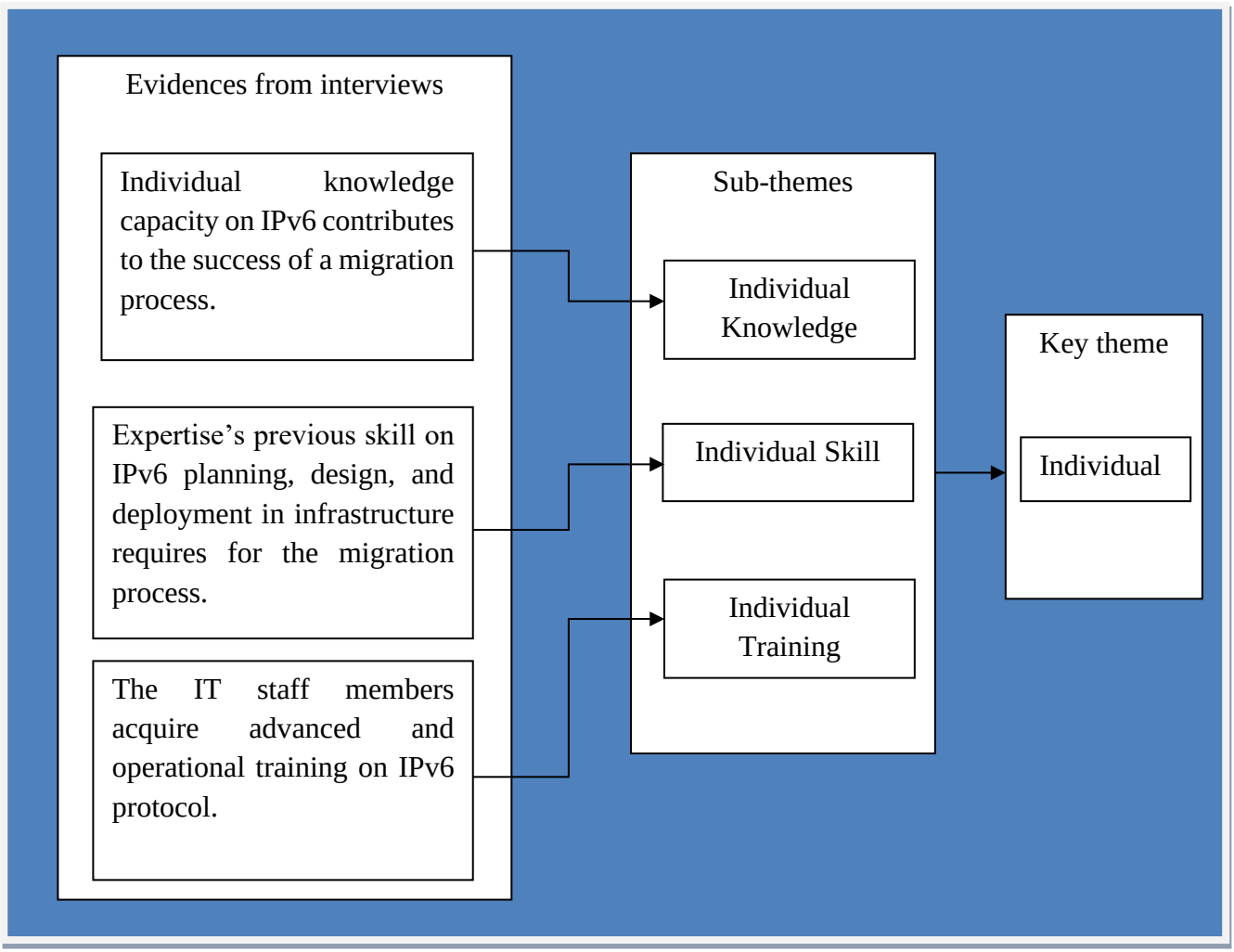

Figure 5 - 1 The individual factor for the migration process.

Knowledge and skills

BIB has employees who have more knowledge of IPv6 protocol. Knowledge in this study is expressed as the basic principle, concepts, and information regarding IPv6 that can be easily expressed in reality. This knowledge is theories of IPv6 supported by books, media, encyclopedias, academic institutions, and other sources. Skills, on the other hand, it is an opportunity to change IPv6 knowledge in practice. In this case, the effect is tangible or noticeable in the organization. It is the ability to use the knowledge and applying it in a certain context that is useful. A good example of this is, a network engineer working on the organization may have good background

knowledge about IPv6 but might not necessarily have good skills. Data from the interviewee also show that the gap between the two sub-factors.

SenInfraExp mentioned that he has a high knowledge of IPv6: "*IPv6 is not a new concept for me. I knew since I graduated from university and I would like to believe I do have good knowledge of IPv6. However, I don't have much skill in IPv6."*

One of the interviewees from the managers' group said: "*Our employees are mature enough in both IPv4 and IPv6 knowledge. Skill on IPv6 needs a day to day interaction and activities on the protocol. Since we are using native IPv4, it is hard to say that our employees are rich in IPv6 skills."*

According to SenNetDatAdmin: "*I don't have any real experience on IPv6 protocol. I'm just developing myself in a simulation environment. I believe IPv6's skill will be mature if you do have a chance to deploy on certain infrastructure."*

The respondent from network engineers exposed the lack of skill in IPv6: "*I never had an opportunity to participate in any project related to IPv6.*"

Data collected from all respondents show that BIB staff has sufficient knowledgeable IT employees on the IPv6 protocol, but not mature in skill. Knowledgeable staffs have the potential to use their knowledge to practice rather than non-knowledgeable employees. However, there is also a lack of IPv6 expertise. Expertise should have both knowledge and skills within his/her work experience. Skills come from real experience took from IPv6 project or production environment. IPv6 experts have a great role in IPv6 adoption because they have both theoretical knowledge and practical skill in this new domain.

Training

The lack of IPv6 training has a huge impact on IPv6 migration. Lack of staff training can limit the knowledge of IPv6 as well as the migration process. Since technologies are change and update frequently, giving the training is an important aspect for the organization to sustain staff knowledge. Organization staffs with matured with knowledge and supported with training have a great ability to adapt and implement new technology in the organization.

According to most of the respondents, the organization is struggled to recruit staff with IPv6 knowledge and experience. Even though, less effort is performed on employee training programs. Some of the training is irrelevant to IT staffs to develop their knowledge and only focus on the current state of infrastructure rather than introducing the new technologies. For example, giving the basic difference between IPv4 and IPv6 to IT staff is not fruitful for the production environment. It becomes better to give standard implementation, technical specification, and security consideration in IPv6 technology. It will be preferable to cover up real-time challenges on IPv6 manipulation.

InfraDir gave his believes on the importance of short-term training for staff and he stated: "*We are not in a good position to give advanced technologies and workshops offered by different vendors. Most of the pieces of training are helpful to manage the current infrastructure of the bank. Thus, with our current training plan, it will be difficult to implement IPv6 on our infrastructure. The role of training is a crucial factor in the success of IPv6 deployment.*"

On the other hand, documents from the IT infrastructure and security staff training policy enumerates and stipulates that all IT infrastructure and security staff shall be adequately trained and certified before they are allowed to take responsibility for the execution of their allotted tasks and responsibilities.

NetEng: "*I took online training and exams presented by different instructors on IPv4 vs IPv6 to build my technical knowledge and skill. I believe it is not much enough for IPv6 implementation for our organization.*"

Even though some short-term training is important for IT staff, respondents from the security division argue advanced training is important for individual IT staff. This helps the organization to enhance its security team.

He commented: *"IT infrastructure security responsibilities shall be carried out by appropriately trained individuals. Security by its nature needs detailed knowledge and skills on the domain. To resist attacks comes external during the transition and after the transition, IT-security staff should be strong enough in their knowledge by giving them appropriate training."*

SenInfraSec also supports the importance of advanced training on IPv6: *"Training should be an advanced level of IPv6 protocol and its features assisting with a hands-on lab."*

Most of the respondents did not have a chance to attend training or a workshop on IPv6. As BIB is a technologically dependent company, its staff should be supported in training and workshop to make strong enough in their knowledge and skills. Also, the company should consider and give more emphasis on giving advanced training for the internal staff with the appropriate budget and time as put on the company's training policy. For instance, the third objective of the Bank's ITISD policy also exposed that, IT infrastructure and security is responsible and shall be carried out by appropriately trained individuals. Moreover, ITISD staff management policy reflects that the bank must ensure that a sufficient number of adequately skilled and qualified staff must available to ensure reliable and uninterrupted business operation of the bank's business-critical information technology. Since IT staffs knows infrastructure structure and layout in a better way, training and workshop addressing them enhance the chance of the company to implement and operate IPv6 smoothly.

5.3.2.2 Organizational factor

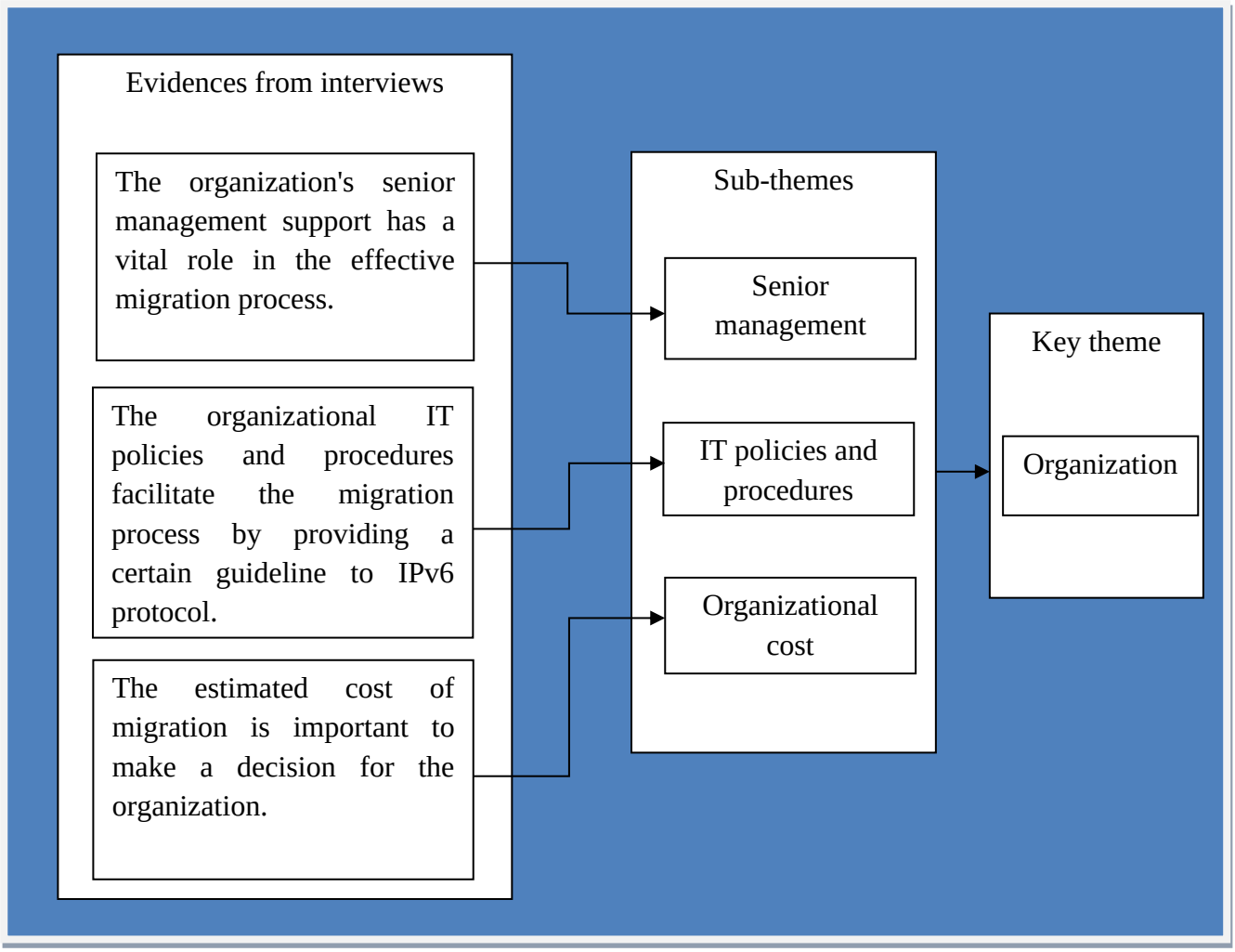

Figure 5 - 2 The Organizational factor for the migration process.

Senior management support

Senior management had a great role in important decision making in the bank, especially non-IT senior management. One of the decisions made by those managements is recognition of project initiatives and releasing appropriate funds for initiatives that need the approval of senior management. The big challenge identified by respondents is how to convince non-IT senior management to support this migration process. As we discussed before, migration operation has a long-term project behavior so that it needs formal senior management recognition, budget, and time. This is also supported by ITISD policy, and puts explicitly as "*IT infrastructure security*

activities must be integrated into other management activities of the bank, including strategic planning, capital planning, and enterprise architecture."

The ITSecDivMgr explained how IPv6 challenges in other non-IT senior management: "*We feel migrating to IPv6 needs more effort and follow up. It is hard to make to believe other management to support IPv6 adoption. Non-IT management only cares their environment is running smoothly in the current time.*"

In the same way, InfraDir also discussed non-IT senior management is one sub-factor organizational factor. According to his idea: "*Most of the non-IT management are lacks of deep understanding of technologies and how it useful for the business. Since IPv6 is not mature in our country, there is no company considered as a role model. It is hard to convince senior management how IPv6 is significant for the bank's long-term achievement.*"

In line with this InfraDivMgr shared his best experience in convincing non-IT senior management in other projects: "*I remember there were so many financial problems faced to change the production servers to upgrade the core banking solution. The senior management was hard to release funds in IT projects. It is hard to convince them in terms of investment."*

SenNetDatAdmin in his part added: "*Migration process needs more investment so that it is not an easy task to approve by Non-IT senior management.*

Organizational strategy, policies, and procedures

As Saklani and Dimri (2013) argue, IPv6 adoption is a long-term process in the organization. To execute this long-term process, it should be supported with organizational strategy. An organizational strategy is the collection of long-term and short-term processes or actions a bank intends to take to achieve long-term and short-term goals. The sum of these actions makes up a company's strategic plan. Strategic planning is an umbrella that is used to help summarize planning, performance measurement, and program budgeting (Fairholm, 2009).

When we say policies, they are just rules and guidelines established by BIB to reach its long-term goals put on its strategy documents. That police are executed through procedures. Procedures are just specific methods employed to state the bank policies in action in the day-to-day activities of the organization. For instance, BIB has a strong ITISD policy that relies on IT infrastructure to run

the daily operations and deliver products and services. With increasing reliance on IT infrastructure, growing complexity of IT infrastructure. Constantly changing information security threat and risk environment, information security has become a mission-essential function.

Data collected from interviewees and document analysis show that BIB has not yet incorporated IPv6 adoption in its policy and procedures. It also has not any IPv6 strategic plan put in both long-term and short-term plans.

The IT managers said: "*The bank did not have any policies and procedures to adopt IPv6 in its infrastructure.*"

However, InfraDir explained the period to review the bank's policy as follows: "*The policy document shall be reviewed in a period of every two years after the original approval date and/or when additional policy or amendment requires for meeting and adopting the information technology change."*

Cost

All informants identified planning, training, and deploying IPv6 needs high cost for IPv6 adoption in the organization. From those, training had more cost to in the IPv6 migration process. For instance, IT technical staff needs more training on IPv6 on how to plan, design, and configure IPv6 in the current infrastructure. Cost anticipation for IPv6 adoption is an important aspect during the migration. As Arifin, Abdullah, Berhan, and Budiarto (2006) suggested, there are two aspects: economical and technical. The economical aspect of the migration process is to deal with the real cost of hardware, software (IOS), and training for IT staff. The technical aspect is about the real implementation of IPv6 by IT technical staff.

Mostly, current infrastructure may be changed to fulfill the IPv6 design and best practice to come up with an effective design. This leads the organization to invest more in infrastructure equipment and IOS upgrade that fit IPv6 specification. As Main, Politechnic, Zakaria, and Robiah (2014) pointed out, infrastructure upgrade has a high cost in the migration process. However, as most of the respondents argued and the researcher's observation shows, hardware replacement and IOS upgrade is not a necessary task for the organization and also as such not a big economical factor

that exposes the organization to spend more money on it. Thus, related costs expect from replacing infrastructure equipment and IOS upgrades will be significantly low.

The SenNetDatAdmin justified hardware replacement and IOS upgrade is not important for the migration. According to him:" *Maybe I can say that most of the equipment that exists in our data-center is support IPv6. We don't need extra cost or investment in the equipment."*

All respondents argue training has a huge cost for the organization. Giving training for individuals that containing hands-on lab practice is difficult for the organization. To get real practical training with a real environment from vendors costs a lot of money. Domain expertise and instructors are not available in the country. Of course, join-venture companies are working with foreign companies that offer a full course with real scenario support. However, the bank is not supporting a huge amount of cost for the staff. The SenInfraExp validated its importance as the following responses: *"Training offered from vendors like Cisco and Oracle are very expensive to afford by the bank."*

Generally, BIB has two types of cost aspects to adopt IPv6 in its infrastructure that needs more focus: Economical and technical. From economical IT staff training should give attention to IPv6 technologies. This includes advanced planning, designing, and implementation of IPv6 in the organization by considering the current IPv4 infrastructure. After the staff is mature in technology, the technical cost will follow. The technical cost is related to the implementation cost. It contains a cost from starting to the end of IPv6 deployment.

5.3.2.3 Physical factor

Infrastructure Upgrade

Change by its nature is hard and difficult to manage if it is not followed properly by domain expertise. Business interruption is unacceptable with the current high business competitiveness and dangers the organization to lose its customers. Like the rest of the organization, BIB wants to stay competitive in today's business area in the country. To avoid such risk, BIB drafts a change control for its infrastructure and security to govern and administer the IT infrastructure and security service and operations of the bank. Data from the interviewee and observation on configuration files reflect that infrastructure upgrade for the adoption of IPv6 is likely low.

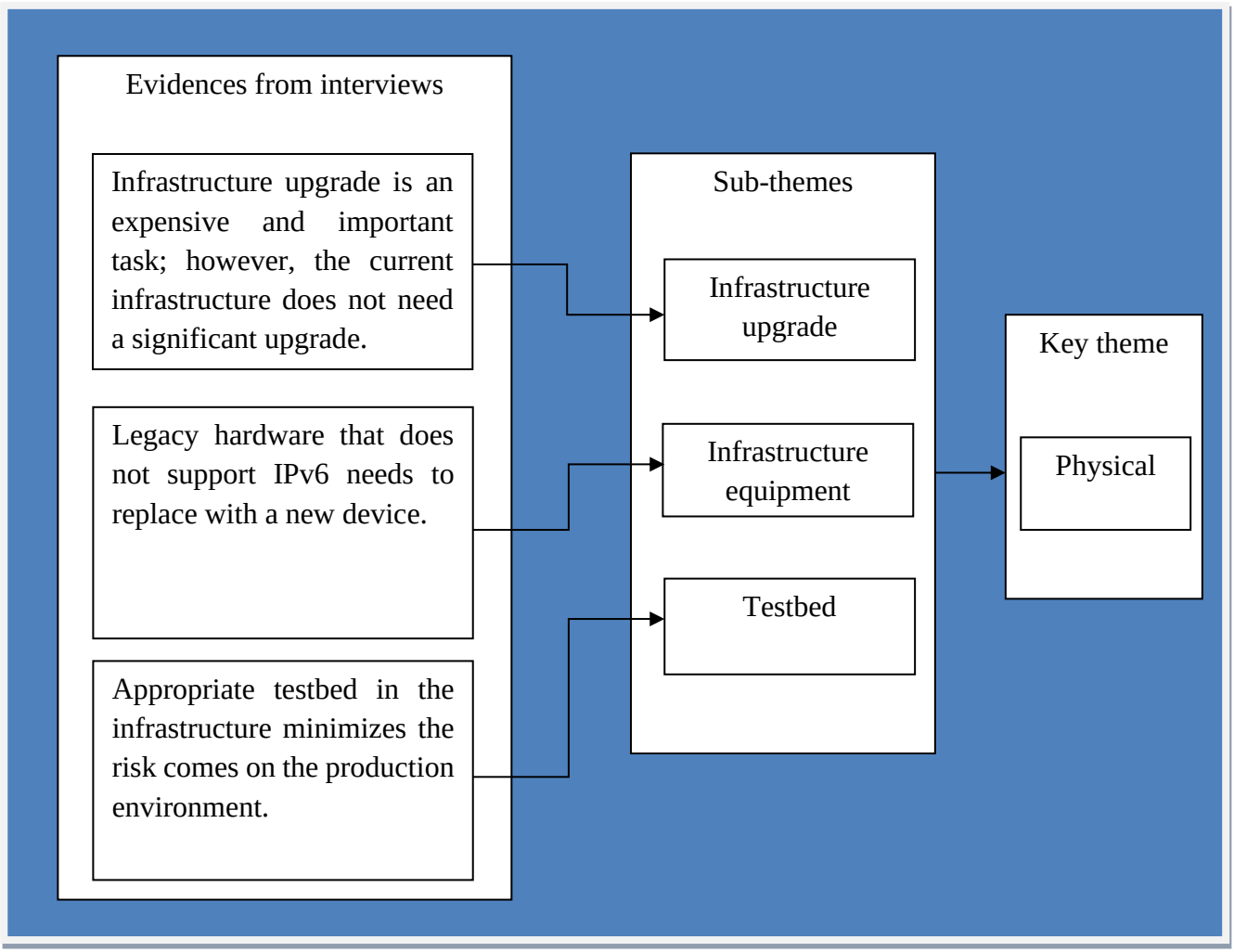

Figure 5 - 3 The physical factor for the migration process.

The SenNetDatAdmin gave their response as "*Infrastructure upgrade is not such important for our company. All most of all network devices, including servers, can support IPv6. Moreover, most of the IOS versions on network devices support dynamic routing in IPv6 protocol.*"

Particularly, the respondent from SenInfraExp said that "*Investment in infrastructure upgrade is a very expensive task for our company. The infrastructure upgrade is important and needs more investment for IPv6 deployment. Fortunately, our infrastructure doesn't need many upgrades for the IPv6 adoption.*"

Infrastructure upgrades need a high investment for BIB. When we say high investment, in terms of cost for skilled manpower to redesign and configure a new infrastructure. Nowadays, IT types of equipment are very expensive and challenge BIB to afford it. There is also a big challenge to

get a fund from the company and convincing higher-level management how it is important of changing IT equipment for the success of IPv6 migration and business return get from it. As researchers performed in chapter four, a proper inventory will minimize the cost of the infrastructure upgrade. All DC, DR, and office infrastructure types of equipment including their IOS are supported IPv6 protocol (refer to chapter four). Thus, IPv6 can be implemented on the existing infrastructure.

Infrastructure equipment

Migration to IPv6 protocol has a great influence on infrastructure equipment and a lot of legacy hardware is expected that doesn't have compatibility with this protocol. We can classify them into three sections based on their support on IP protocol: Native IPv4, both IPv4 and IPv6, and Native IPv6. Native IPv4 device is commonly called legacy devices that support only IPv4 protocol. Those devices need replacement with proportional new devices that support IPv6. According to most respondent's argument and observation results shows, all infrastructure equipment that exists in BIB are supports IPv6, except POS machines and unmanaged switches.

SenInfraExp: *"All computing machines are in the position to support IPv6."*

NetEng: *"All network devices support IPv6 and IPv4."*

The native IPv6 devices are referred to as new devices that only support IPv6 protocol. Since IPv4 protocol becomes a depreciate protocol and IPv6 consider as a promising communication protocol, there is some device that eradicates IPv4 protocol from their standards. Fortunately, BIB had not such IT equipment in its infrastructure (refer to chapter four).

Testbed

The testbed is an important part of IPv6 adoption. It is a collection of IT equipment aimed to simulate the real infrastructure that exists in the company. Since IPv6 is a new technology in BIB, there is a need to conduct rigorous, transparent, and replicable testing on it before directly dive into the production environment. Data collected from respondents and literature recommended organizations should have a structured testbed for IPv6 before fully adopting IPv6. This helps BIB to minimize the risk during the migration process.

The NetEng and SenNetDatAdmin supported the benefit of testbed as "*BIB has a good habit in change management. Any change that affects the production environment always the first test in a test environment before it is implemented in a production environment.*"

SenInfraExp also believed risk will minimize by using testbed in the organization. According to him: *"Testbed reduces the risk and enhances the success of the migration process. It also helps to assess security threats during the transition period."*

ITSecDivMgr: *"It provides us to see new security threats and perform a penetration test on IPv6 infrastructure."*

Document analysis results also expose that; BIB has a strong policy on change management. Changes are interrupted by the current production environment directly or indirectly. Those changes should first test in a test environment to analyze their consequence. IPv6 adoption changes the logical structure of the infrastructure in BIB so that the testbed has a grand role in the successful migration process.

5.3.2.4 Security factor

Infrastructure vulnerability

During the transition process, it is common to face security threats and the probability of the existing security bridges is pretty much high. Since transition by its nature both IPv4 and IPv6 protocols are running simultaneously or one each after for a certain period. Therefore, it is hard to manage attacks from both protocols.

The manager from the security team gave his recommendation: "*We should consider both IPv4 and IPv6 attacks and threats. For this matter, we need to think about expertise on both protocols to defend our infrastructure from external attacks.*"

SenInfraSec also shares his idea: "*Using two protocols in parallel increases the vulnerability in the transition process. Related to that, we need to modify IT policies and procedures to achieve our security goal."*

NetEng: "*There will be also high management issues when using two protocols simultaneously."*

The other vulnerability option starts with selecting the appropriate transition technique for the organization and deploying it on infrastructure. Every transition technique has its advantage and disadvantage in different types of attacks. Identifying a proper transition technique is important to minimize external and internal attacks.

SenInfraSec commented as "*A hybrid technique is preferable because we can get more advantage from different migration techniques and helps to firm organizational security during the migration era. It will not be an easy task for attackers to penetrate the infrastructure when the current infrastructure migrates to IPv6.*"

SenNetDatAdmin also added that: "*Using more than one technique enhances the security; however, it has administration overhead for network engineers to troubleshoot and manage in their day to day activity.*"

Even if using a fusion migration technique has extra administration overhead for network administration, it enhances the security level and reduces attack in the migration process. Attack attempts on one transition technique will not be sufficient to penetrate the network infrastructure. Thus, using a fusion of migration techniques offers a multi-dimensional security advantage for the infrastructure.

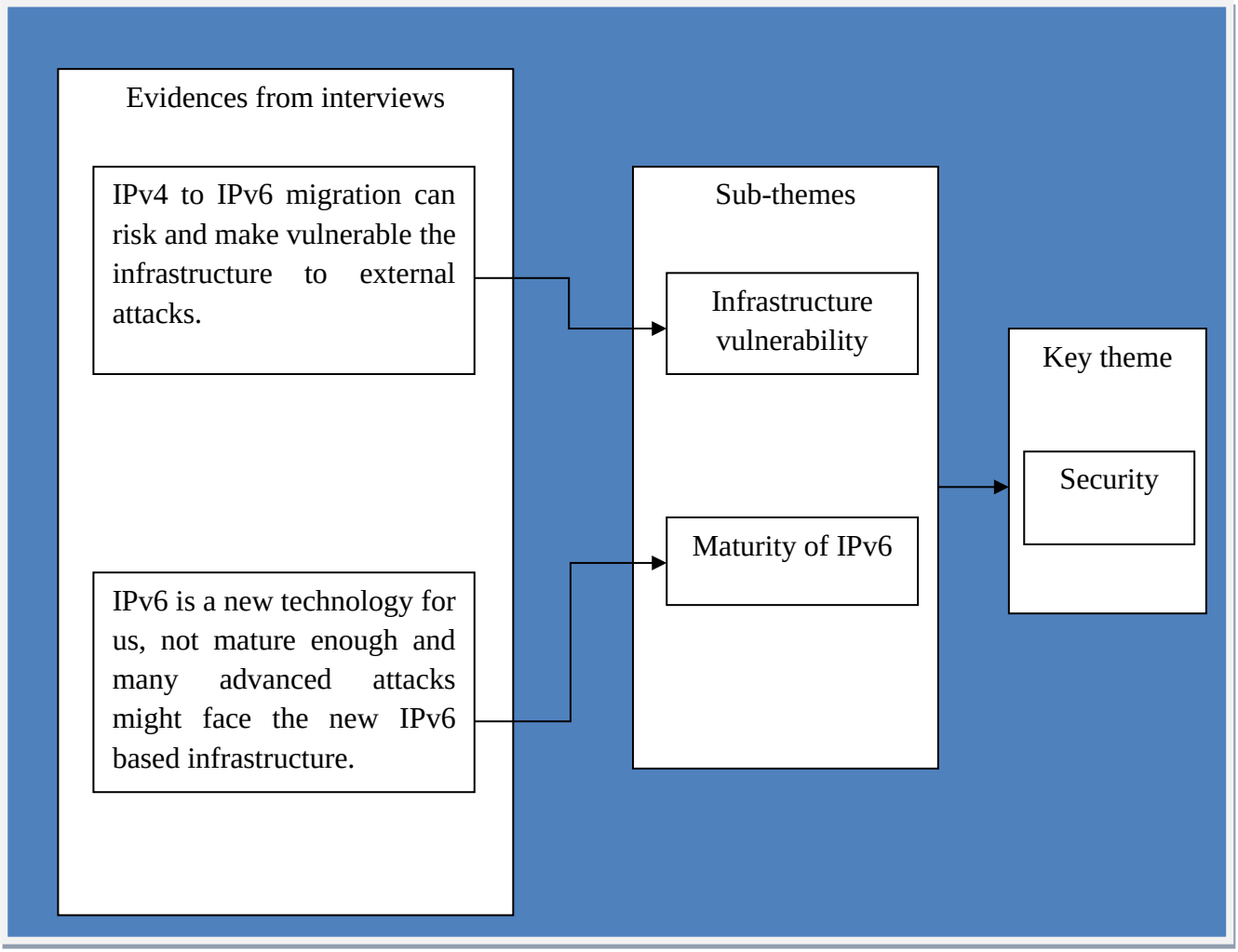

Figure 5 - 4 Security factor for the migration process.

Maturity of IPv6

IPv6 is less mature in implementation, especially in our country. There is no empirical evidence that shows the types of attacks performed in IPv6. Even if IPv6 comes with a stronger security rule than IPv4, there are a lot of modern attacks that exist for IPv6. Familiar with IPv6 attacks and threats should not be considered as an easy duty for security expertise. Related to that, BIB's security teams shall ensure network access control and monitoring mechanism in place to protect the bank's mission-critical network infrastructure services from malicious external entities.

SenInfraSec: *"Since IPv6 is a new technology, it is less mature in what type of attack it might face. So that many, attacks and threats may happen in our infrastructure beyond our expectation."*

ITSecDivMgr gave his comment on the advanced attack as: *"Since it comes up with enhanced security, attackers may come up with advanced technology to bridge IPv6 security. It might not be tolerated by our expertise."*

5.3.3 Best transition technique

In chapter two we have seen different transition technologies mainly classified as Dual-Stack, Tunneling, and Translation techniques. As most authors argued as selecting appropriate translation techniques for an organization is a challenging task and often depends on organizational infrastructure. Data collected from BIB's expertise, observation, and document analysis reflect on a hybrid of Dual-Stack and Tunneling techniques.

Dual-stack

A Dual-Stack transition technique contains both IPv4 and IPv6 protocols and makes them communicate with each other in network equipment, especially on routers. For nodes, they have both IPv4 and IPv6 addresses associated with each NIC; so those nodes are communicating with both IPv4 and IPv6 networks without any problem. All respondents believed that Dual-Stack one of the promising options in the transition process for BIB core infrastructure.

According to SenNetDatAdmin: "*Dual-Stack has good flexibility to deploy IPv6 on the current infrastructure. It supports both protocols simultaneously. However, if we implement a Dual-Stack in hosts, it will not be economical and its manageability issue becomes so difficult.*"

As we have seen in chapter four, one of the prominent layers in BIB DC is a core-layer. If we trace any traffic that comes to DC, it always passed through this layer. This implies that whether native IPv6 or IPv4 traffics will be route on the core-layer. Dhamale and Singh (2018) also argued that Dual-Stack will be effective and economical for the organization if it is implemented on the core-layer devices to help the legacy IPv4 network to communicate an IPv6 network.

SenInfraExp also elaborates on the advantage of Dual-stack as: "*Native IPv4 applications and devices that are late to migrate can run over IPv6-only network without any further modification.*"

SenNetDatAdmin: "*IPv6 implementation needs more time to adopt and the two protocols have different format and behavior. Engaging both protocols in our infrastructure seems a good approach for a certain time for a backbone network.*"

Dual-Stack will act as the focal point and a backbone in the migration process. Native IPv4 and IPv6 networks mostly exist in this process. Traffic from both protocols should be routed and users must get services without any interruption. This helps the designer to work out the incompatibility between IPv4 and IPv6 protocols.

Tunneling

Tunneling refers to the process of establishing a virtual tunnel between two or more routers located in different geographical locations. This tunnel can be used on those routers to communicate privately by excluding third parties' networks or MPLS. The concept of tunneling is mostly confused with encryption. In the tunneling process, the payload will not encrypt, rather it will encapsulate (Cui et al., 2013). Encapsulation IPv6 packet into to IPv4 packet on one side will de-capsulate the original IPv6 packet on the other side, forwarding it to the final destination. All respondents came up with an argument on using tunneling techniques for organizational branches if Ethio-telecom is late to migrate to IPv6.

SenInfraSec proposed a tunneling technique for the bank's branch to communicate to DC. According to him: "*We do have more than 230 branches distributed all over the country and connected to our data center through Ethio-telecom MPLS. We can publish our private tunnels over the ISP infrastructure. This helps us to enhance our security and pass the ISP's MPLS infrastructure without any problem.*"

NetEng also solidifies SenInfraSec ideas as: "*As much as I'd like to believe that, branches should be a native IPv6 domain and tunneling becomes a promising migration technique.*"

When we see from the design perspective, all branches need a router assumed to peer to the DC firewall. Tunneling IPv6 over IPv4 configuration will be performed on routers and firewalls. All IT equipment that exists in branches remains in the native IPv6 domain. As such, tunneling allows a quicker migration for BIB.

Translation Mechanism

A translation method is used to provide a way to translate the IPv4 packet to the IPv6 packet and vice versa. Unlike tunneling, the traffic is not encapsulating the IP header, rather it will convert the IP header to the appropriate format. For instance, a host with IPv4 address might send a request to an IPv6 only server which is not understanding the legacy protocol to communicate. In this case, and the intermediate device needed to make a payload modification or remove the IPv4 packet header and adds an IPv6 packet header and vice versa. Most of the respondents do not argue on this transition mechanism for the migration process for the organization.

SenNetDatAdmin: "*Our infrastructure did not have new devices that can only speak IPv6 protocol. We don't need to translate or convert an IP header to provide communication between IPv4 to IPv6 protocols*."

NetEng: "*It is unlikely to use a translator device between native IPv4 and IPv6 network. It needs a high processing capacity device and also it might degrade the performance of the network.*"

RFC 2766 also expose NAT-PT is moving to historic status and likely fade away over time. Since it performs address translation, applications that carry the IP address in the higher layer do not work. It also has a lack of end-to-end layer security and also cannot be deployed in combination with secure DNS. Baker, Li, and Yin (2011) also argue NAT-PT is not considered as a promising transition technique and bad for a medium and large organization. Moreover, there might be a packet loss during translating packets from one to another. Thus, it might have an impact on day-to-day business activities.

Generally, the following table shows the summary of the case study analysis and findings performed in this study.

1.	**Motivation to migrate from IPv4 to IPv6.**
	External force **Technological advancement** **Competitive advantages**
2.	Factor affecting the migration process (Research question 1).
	Individual factor *Knowledge and skills* *Training* **Organizational factor** *Senior management support* *Organizational strategy, policies, and procedures* *Cost* **Physical factor** *Infrastructure upgrade* *Infrastructure equipment* *Testbed* **Security factor** *Infrastructure vulnerability* *Maturity of IPv6*
3.	Best transition technique (Research question 2).
	A hybrid transition model *Dual-stack* *Tunneling*

Table 5 - 1: Summary of case study analysis and findings

5.4 Discussion

In this section, the researcher tied to put and present a compressive discussion based on the previous findings of the study. The discussions are articulated based on data obtained from interviews, document analysis, and observation. Research questions put in chapter one is also discussed and summarized in this section.

5.4.1 Motivation to migrate from IPv4 to IPv6

The first key motivation for BIB to migrate from IPv4 to IPv6 is an external force. The services provider company on the national level is Ethio-telecom. This company currently offers native IPv4 address blocks for its customer. As most of the respondents argue and believed this IPv4 range may not a promising solution for business communication for the future. According to them, there are many reasons behind this, and the important reason is the execution of IPv4 addresses. Due to this case, Ethio-telecom already started a migration process from IPv4 to IPv6. This migration process in the company also justified by (Matebie, 2019), and the author puts its conclusion the migration process will be soon because of the scarcity of IPv4 addresses.

Saying that the moment Ethio-telecom makes its migration, it will start to provide and force to use IPv6 address blocks rather than IPv4 for its customers. BIB is one of its customers, it should adopt IPv6 address blocks in its infrastructure. Adopting IPv6 in BIB's infrastructure is more advantageous for the company in the future. According to the respondents, when IPv6 protocol becoming the mandatory protocol for the communication by the service provider; BIB will not suffer its business environment at that moment if it is early to adopt it. In the future, adopting this new protocol is unavoidable and Ethio-telecom also may push organizations to use it since it is the only service provider.

The second key motivation for BIB to migrate from IPv4 to IPv6 is a technological advancement in worldwide. Data collected from literature and interview respondents shows that IPv6 has a more advantageous and advanced protocol than IPv4. IPv6 getting more mature and a promising protocol in RFC than IPv4, and it's becoming a depreciate protocol in RFC. Moreover, different vendors like Cisco, Oracle, Juniper, HP, Fortinet, and others are giving more attention to IPv6 than IPv4. Besides IT equipment advancement, network training centers also giving much inclusive training and support on IPv6. From both equipment vendors and training centers, IPv6 is getting a

more famous and well-known communication protocol through time which seems it surpass IPv4 in a short period.

As the researcher stated above, IPv6 technology advancement is getting more reliable in the industry even by RFC. Respondents show IPv6 technology advancement in three dimensions, those are efficiency in routing and packet processing, supporting new services, and enhancing security. An experimental study Chauhan and Sharma (2014) also supports that IPv6 has more routable in the router to process its packet than IPv4. It also supports new technology services and capabilities to support them compared to IPv4. IPv4 has to become a deflate protocol and it has not more updates compared to IPv6. Security enhancement also shows the gap between IPv4 and IPv6, it has more secure communication between devices than IPv4.

The third motivation for BIB to move from IPv4 to IPv6 is a competitive advantage. The advantage gets from IPv6 over IPv4 can make BIB more beneficial and increase its competitiveness. As we discussed earlier, technological advancement is one motivation for BIB, related to that it also provides a competitive advantage. To reiterate, most of the interviewed believe using IPv6 plays a great role in business competitiveness. For instance, packets are routed and processed more efficiently than IPv4, there will be a possibility to reduce traffic congestion in BIB infrastructure. The same thing in the security, the bank will be well confident in its day to day transaction. According to all respondents, IPv6 will decrease attacks for cyber much more than IPv4, especially from mobile, Internet, and agent banking services. Thus, customer satisfaction will be improved and it will have a good opportunity to penetrate the banking industry.

5.4.2 Factor Affecting for Migration Process

Individual factor

The second research question of the study is to identify and answer factors affecting the migration process from IPv4 to IPv6 in BIB. The first factor identified by the interviewers is an individual factor. This factor measures the IT employee capacity in terms of knowledge, skills, experience, and training. The participants noted that knowledge of IPv6 has a great role in the success of the IPv4 to IPv6 migration. Related to that, BIB employees have enough knowledge regarding the IPv6 protocol. On the other hand, BIB has a lack of expertise that has good skills in IPv6 protocol. An employee with a lack of skill has reduced the success of the migration process. According to

the respondent, most did not have any experience with the IPv6 protocol. Additionally, they also point out it will be a large risk to move to IPv6 without containing IPv6 expertise.

The other important key under individual factor is training. All respondents justified that IPv6 training is directly proportional to the success of IPv4 to IPv6 migration. Not only this but a lack of training also a negative impact on the development of knowledge in staff members. The finding is consistent with the result of Main, Politechnic, Zakaria, and Robiah (2014) who argue that training has a positive contribution to the success of IPv6 migration. Knowledgeable staff is need for IPv4 to IPv6 migration. Therefore, appropriate training enhances the development of staff knowledge. Additionally, they also confirmed that BIB staffs have limited training on IPv6. IPv6 technology by itself is a new technology and updates are including frequently. Training for IT staff members is a crucial thing in the success of IPv4 to IPv6 migration.

Organizational factor

The first key under organizational factor is senior management support on IPv4 to IPv6 migration process. To execute this migration process in the organization, first, it should be recognized and supported as an initiative in the organization. According to the majority of the respondents, this is a big challenge and has a big impact on the success of the migration process. The migration process needs more funds from the organization, senior management approval is a mandatory task. Related to that, convincing senior management needs more time and effort from the rest of the IT staff. Moreover, senior management support is also not noted in earlier studies and identified in the current researcher's finding.

Organizational strategy, policies, and procedures are the second key sub-factor under organizational factors. IPv4 to IPv6 migration is a long-term process, needs extended time, budget, and effort. To accomplish this task, it should be supported by organizational strategy, policies, and procedures. The result of this study also supports (Fairholm, 2009). Data from the interview and document analysis expose that BIB had not any policy and procedure to execute the migration process. This implies that the bank's IT policy and procedure should be revised to guide to move from IPv4 to IPv6. This has a great role in the success of the migration process. The participant

also pointed out that modifying IT policy and procedure were essential ingredients to ensure the migration process.

Cost expecting from the organization are classified as planning, testing, and deploying in the migration. Planning is related to hardware, software (IOS), and training costs. According to the researcher's assessment (in chapter four), this cost is minimal for upgrading devices. Another big cost identified by the respondent is the training cost. Offering advanced and operational staff training has more cost for the organization. The main reason for this is the lack of domain expertise and instructors in the country. Foreign trainers inquire more money to educate staff members and not affordable by the organization. The last cost comes from testing and deploying IPv6. This is included in the implementation phase of the migration process. It is also in line with the argument of Arifin et al. (2006) that classified the cost of migration from IPv4 to IPv6 as economical cost and technical cost.

Physical factor

The first key under the physical factor for IPv4 to IPv6 migration is an infrastructure upgrade. Data obtained from respondents and observation shows infrastructure upgrade is likely low. Moreover, they also argue it needs high investment, skilled manpower and it needs intensive plan and design. As all devices' firmware and operating systems are capable to support and compatibility with IPv6, upgrading the existing infrastructure is not as important to implement IPv6.

Replacement of infrastructure equipment is another important point. Legacy infrastructure equipment that is not compatible with IPv6 needs replacement. Main, Politechnic, Zakaria, & Robiah (2014) support considering replacing hardware that could not support IPv6 has an important role in the success of the migration process. Even though, all respondents reflect that all devices do not need replacement except POS machines and unmanaged switches.

The testbed is an important environment for the IPv6 migration process and has a positive impact. Since IPv4 to IPv6 migration is a revolutionary change in the infrastructure, all respondents believed and BIB’s policy document showed, change in infrastructure first needs to be tested in a test environment. This finding complements the work of Yousafzai et al. (2015) who has stressed

testbed has a vital role in minimizing the risk obtained by the migration process. Furthermore, it also minimizes business interruption in the transition period.

Security Factor

The first sub-factor under the security factor is infrastructure vulnerability. The infrastructure might be highly vulnerable in the transition period. Remarkably, two probabilities have been identified this vulnerability might exist. Running both IPv4 and IPv6 protocols simultaneously enhance infrastructure vulnerability. To avoid running both protocols on infrastructure is hard because the transition period is not performed for a short period. Expertise needs to perform hard code their security protocol to manage and defend against attacks that come from both protocols. The second probability is during selecting an appropriate transition technique. According to the respondents, and Taib and Budiarto (2007) show that using more than one technique is preferable and also minimizes the attack. Using a single technique is much easier than using more than one technique for attackers during the migration process.

The second key under the security factor is the maturity of IPv6. With the advancement of IP protocol, threats that come from the attacker also become enhanced. Make expertise familiar with those attacks and threats is an essential part of the success of the migration process. Perhaps, without a strong infrastructure security policy, the transition process will be at risk. As security teams are argued, expertise in the migration process is capable to manage different monitoring and defending tools to enhance infrastructure security. Moreover, the maturity of IPv6 is also not noted in earlier studies and identified in the current researcher's finding.

5.4.3 Transition technique

Data collected from interviews show that a hybrid transition model is a promising solution for the success of the migration process. The hybrid model is to deploy two or more independent transition techniques within the infrastructure (Taib & Budiarto, 2007). Flexibility and security are the key aspects of this hybrid technique. Dual-Stack and tunneling techniques are selected to formulate the hybrid transition model.

Dual-Stack deploys IPv4 and IPv6 in parallel mode. It's preferable of its scalability and easy to implement on the existing infrastructure. As a result, it is easier to maintain and troubleshooting. Moreover, it has two protocols, each protocol is running independently. It is preferable to the backbone network.

Tunneling techniques are selected to deploy for areas that do not currently support IPv6 in the infrastructure, which is the ISP. In the article review, we have seen different tunneling techniques and how they were helpful to communicate native IPv6 domains located in different geographical locations over IPv4 infrastructure. Branches, ATMs, POS machines need to access and communicate the DC. In this scenario, tunneling is identified as a good solution to pass Ethio-telecom MPLS.

The following table summarizes the discussion below.

No.	IPv4 to IPv6 Migration	Evidence was collected from interviews.
1.	Motivation to migrate from IPv4 to IPv6.	The motivation for BIB to migrate from IPv4 to IPv6 is an external force, technological advancement, and competitive advantage.
2.	Factor affecting for migration process (Research question 1).	The major factor identified for the migration process is an individual factor, organizational factor, physical factor, and security factor.
3.	Best transition technique (Research question 2).	A hybrid model is identified as the best transition technique for BIB infrastructure. The model is formulated from Dual-Stack and Tunneling transition technique.

Table 5 - 2: Summary of discussion

5.5 Chapter Summary

The chapter was focused on the data presentation, interpretation, and findings of the study. Data were collected using interviews, document analysis, and observation. Throughout the chapter, the researcher identified and discussed the motivations of BIB to migrate from IPv4 to IPv6 and factors affecting the migration process. Finally, the researcher proposed a hybrid transition model that assists BIB to transition from IPv4 to IPv6.

CHAPTER SIX

6. FRAMEWORK DEVELOPMENT AND DISCUSSION

6.1 Overview

The beauty of the design science approach is its rigor cycle for artifact development, evaluation, and demonstration of the developed artifact. In previous chapters, data collected from respondents, documents, and observations have been analyzed. Consequently, in this chapter, a framework is developed to meet the ultimate objective of this research. Jayasanka (2015) approach is used for the development of the framework. Moreover, this chapter also addressed a demonstration using a simulation tool called GNS3 to clarify the usability of the framework. Eventually, the framework is evaluated by domain experts to see if it is applicable, efficient, and effective.

6.3 Proposed Framework

Jayasanka (2015) proposed the migration process should have three phases: preparation, transition, and post-transition. The preparation phase is the first phase in the migration process where preparation for the implementation of IPv6 takes place. The second phase is the transition phase which is considered and defined for a transition for the company without affecting the company's working environment. The last phase is the post-transition phase contains a process to maintain the organization's operations.

The proposed framework has three parts: pre-migration, migration, and post-migration. Pre-migration is a first process that has readiness assessment, infrastructure equipment, infrastructure upgrade, planning, and staff training. The migration phase is the main phase that contains the deployment of IPv6 on the infrastructure. Then after, in post-migration, the new IPv6 based infrastructure will be supported in domain expertise.

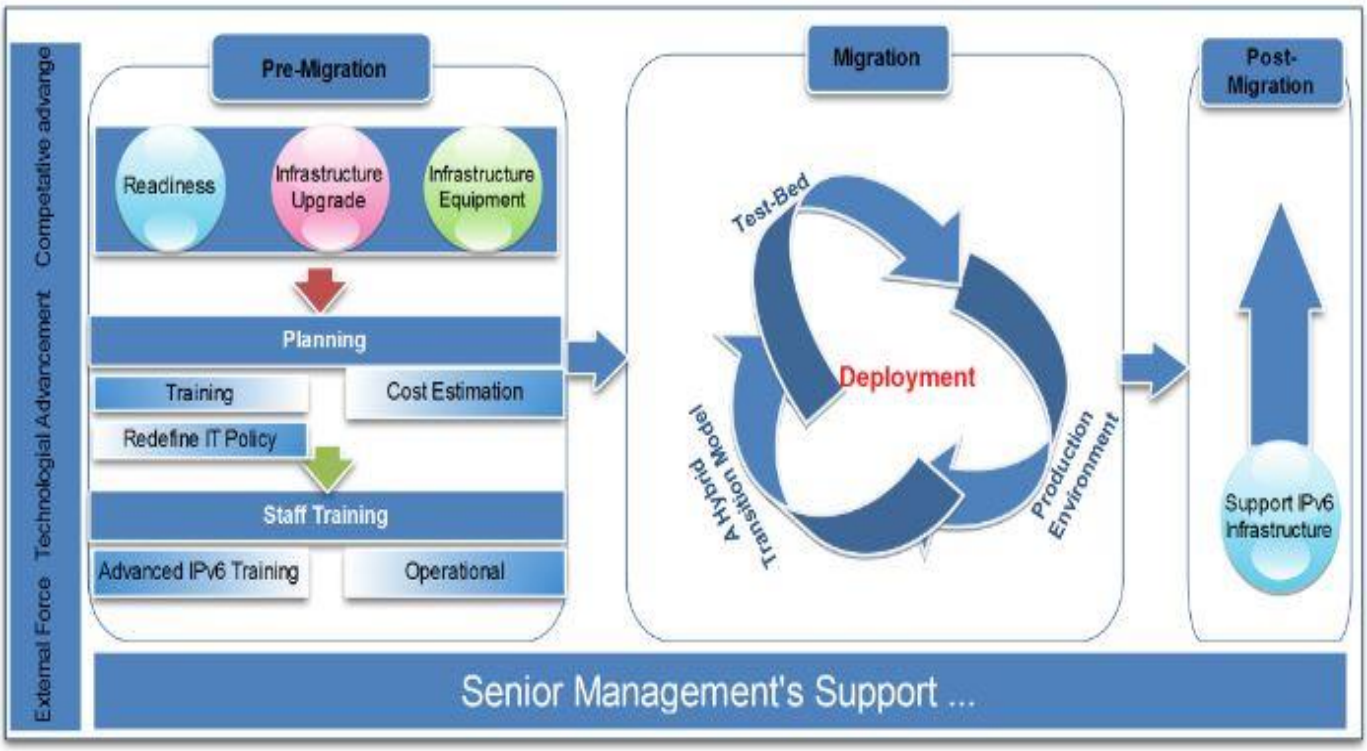

Figure 6 - 1: A proposed framework for IPv4 to IPv6 migration

Jayasanka VS Proposed framework

The proposed migration by Jayasanka (2015) came up with a framework designed for Sri Lankan ISP networks and mainly assist ISP's infrastructures to adopt IPv6. Moreover, components of the migration framework are focused on the technical perspective while implementing IPv6 on the ISP's infrastructure. As we discussed above, it has a preparation phase, transition phase, and post-transition phase.

The preparation phase in the framework dealt with upgrading on the existing hardware, identify critical infrastructure, prioritize device which helps to maintain the end to end connectivity during the transition phase, find out low-cost solutions for upgrades, and apply firmware solution instead of hardware solutions. The survey helped to identify hardware that supports IPv6 and needs to be replaced. Furthermore, staff training for the migration process is performed in this phase.

The transition phase defines steps and a list of tasks performed while IPv6 is deployed in ISP. Besides the IPv6 implementation, configure migration mechanism and IPv6 address, configure and records needs for DNS, configure address translation in both IPv6 only and IPv4 only customer networks, maintain load balancing and error logging, apply access control list and firewall rules for routers and firewalls, and supporting the company services were tasks considered in this phase.

The third and final phase considered in Jayasanka (2015) is the post-transition phase. In this phase, apply smoothing options to reduce operational overhead. This helps Lanka's communication (Pvt) infrastructure smooth without losing the end-to-end connectivity and perform stable service for its customer after the transition phase.

The proposed migration framework in this study intended to correlate organizational factors that influence the migration process in the organization and proposed appropriate transition techniques for the infrastructure. The proposed framework adopted the three migration phases from Jayasanka (2015) and come up with pre-migration, migration, and post-migration phases. In the pre-migration phase, infrastructure upgrades, infrastructure equipment, and cost estimation were also included in Jayasanka (2015) and in the current proposed framework. Meanwhile, readiness, redefine IT policy, and advanced and operational staff training was added to the proposed framework by the researcher.

The migration phase in the proposed framework also introduces a hybrid transition model for the organizational infrastructure which is not in Jayasanka (2015) framework. Like Jayasanka (2015), supporting IPv6 infrastructure is an important task after IPv6 implementation, therefore, it was put in the post-migration phase in the proposed framework.

Unlike Jayasanka (2015) framework, the proposed framework also integrated external force, technological advancement, and competitive advantage as a motivation for the organization to adopt IPv6. Moreover, Senior management’s support also has a vital role in the success of the migration process and is also considered as an additional component for the proposed framework in this study.

In the following section, the proposed framework phases and components will be discussed in detail.

6.2 Framework Development

As discussed in chapter four, BIB has its infrastructure to achieve its vision and mission. A framework is simple diagrams that organize its components in a usable way. The migration from IPv4 to IPv6 problem is much unstructured and has many factors that affect the process. The framework developed by different authors cannot be used for BIB as they are because of two main reasons. First, most of the frameworks are focused on the technical effectiveness of the migration process. The second reason is current frameworks are developed on the national level rather than the organizational level that should consider different organizational factors for the migration process. Due to those major reasons, those frameworks are considered a clumsy solution for BIB. Therefore, a framework needs to be developed as a compressive that integrated both technical and organizational factors for BIB. It also facilitates the migration process as a milestone.

Generally, considering the fact done in the previous chapters, the researcher followed the following steps to develop the proposed framework.

- Point out the main finding identified from data analysis,
- Identifying the main components of the framework,
- Develop a framework iteratively until the research requirement get saturated,
- The framework is elaborated and demonstrated for a particular domain, and
- The framework is evaluated by expertise to further modification.

6.4 Framework Components and Description

6.4.1 Pre-Migration phase

The pre-migration step is important to avoid common obstacles and challenges in the IPv6 transition. It contains readiness, infrastructure equipment, infrastructure upgrade, planning, and staff training. Those components are discussed in this sub-section.

Readiness Assessment, infrastructure equipment, and infrastructure upgrade

The first finding from data analysis and article review was migration from IPv4 to IPv6 incorporates a challenge due to a lack of proper inventory in the existing infrastructure. An inventory of the existing infrastructure should be intensively done. In this step, all available infrastructure equipment shall be surveyed. This includes a list of all infrastructure IPv4 addresses in the network, equipment firmware or IOS, and DNS mappings. The assessment of the current

infrastructure would verify if the existing infrastructure devices can support IPv6 (Yousafzai, Othman, & Hassan, 2015).

Legacy devices that do not support IPv6 shall be replaced with new devices (like POS machines and unmanaged switches). Identifying those devices will help the engineers to come up with good cost estimation, and helps to plan for a migration phase. Main, Politechnic, Zakaria, and Robiah (2014) infrastructure enhancement might need during deployment operation and cost will be involved during the migration process. Since hardware replacement is an expensive task, there is also a probability of legacy hardware can support IPv6 protocol by upgrading its firmware or IOS. There are some devices or model series that can be upgradable by their vendor. If that so, upgrading infrastructure equipment is a better option than replacing whole hardware. For instance, in BIB infrastructure there are some routers whose IOS supports IPv6 only on RIP and OSPF protocols. However, in the migration plan, if engineers believe EIGRP more efficient protocol for IPv6 than RIP and OSPF, upgrading IOS seems to be necessary.

During the assessment, it shall also evaluate the readiness in knowledge and skill of IT staff that will support the migration process. The role of IT staff is vital for the success of the migration process as well in the post-migration phase. In the migration phase, there will be intensive iterative tests and deployment of IPv6 in the testbed and the production environment respectively. This needs a high quality of technical skills and knowledge to achieve the process at a scheduled time. This implies that identifying low skilled and knowledgeable staff and prepares them for appropriate training is an important task to keep the quality of staff. The readiness of IT staff's skill and knowledge shall be evaluated and any training that is required and should be documented for the further planning process.

Cost Estimation

Cost estimation is classified as infrastructure cost, training cost, and implementation cost. Infrastructure costs related to infrastructure upgrades and replacing legacy hardware. Devices identified as not supporting IPv6 need to replace or upgrade. They might be routers, switches, firewalls, and servers that exist in the infrastructure. The first list of devices is identified and cost estimation for each device will be put by selecting suitable vendors.

Training is another big cost that invests in an employee's mind. This cost depends on the nature of training, type of training, and time interval it takes to complete the course. The nature of training can be incremental or one-time training. Incremental training mostly has more than one phase. One-time training is usually completed in a single phase. Operational training has also a high cost compared to theoretical pieces of training. It needs a hands-on lab or in a real environment, and it also needs more time and high cost. Training costs can also classify as a direct cost and indirect cost. Direct cost is a cost directly associated with purchasing IPv6 training and delivering the training. This depends on the time of training it will take and the infrastructure needs for the training. Indirect cost incurs other staff members to train those who have not direct association with IPv6 training but give indirect assistance for the migration process.

Training

Training is one of the most important aspects of improving staff knowledge. Adequate training is necessary to make BIB investment in the migration process. In this phase, one of the big tasks was assessing the readiness of staff knowledge on IPv6. Skills and knowledge measured in previous readiness assessments help to develop a good training plan for IT staff. Operational and advanced training shall be identified for IT staff. The training plan should have a crisp description of its role and scope undoubtedly to align with the objective of the IPv6 migration. The formulated training plan sets priorities and allocates resources based on BIB's budget.

The training that takes place close to the time of implementation shall be made part of the actual implementation plan. It shall have two types of training: advanced and operational. IPv6 advanced training covers all advanced IPv6 features, LAN, and WAN networks with different migration techniques. The migration process uses advanced migration technologies; advanced training is a crucial thing for the transition. Besides advanced training, operational training also has a vital role and advantage in the IPv6 transition. Developing staff's technical capabilities is a mandatory approach in this process. Real IPv6 deployment needs more technical skill than other theoretical capabilities. Therefore, operational training has a vital role in the migration process.

Well-trained employees are essential to the success of the migration process. They make fewer mistakes and, they feel responsible and confident in their job by providing visibility major knowledge. Training also increases their commitment, productivity, and personal confidence in

their day to day activities. Moreover, it has provided the potential to simulating their idea in a test environment.

Redefine IT Policy

IT (Information technology) policy is a set of guidelines for employees who work in IT-related assets. BIB has created IT policies to ensure or protect security threats and attacks for the organization based on IPv4 protocol. It also shapes the organization's staff members how to use and share data and information among themselves and to external parties. Threats are always developing, and compliance requirements are becoming drastically complex. This becomes more complex for BIB in the transition process. BIB shall review its IT policies to a comprehensive security program to cover challenges that might occur by both protocols. Without reviewed IT policies, it is hard to coordinate the migration program and other security programs across the organization.

For instance, updating ITISD policy and follow the procedure has a great role in diminishing security breaches during the transition period. This is because IPv6 is emerging with new threats, and coexistence with IPv4 also changes the security posture of the company. Thus, the organization should make the policy practical and enforceable before the attempt to start the migration process.

Sometimes policy can be broader than expected. To limit and see the big objective of the policy, the purpose shall be clear enough that reflects the new protocol. Since the IT policy is reviewable every two years as per the bank's rule, it can be reshaped if it is needed. Its objective also shall reflect confidentiality, integrity, and availability. Moreover, the document shall be continually updated with the evolving of the transition process requirements

Confidentiality protects information and data from unauthorized access and misuse from both IPv4 and IPv6 traffic. Most of the information in BIB has a high degree of sensitivity such as customer's private information and their transaction, therefore, the confidentiality of their data and information should be ensured. During the transition period, the organizational infrastructure vulnerabilities and attacks may enhance, therefore frequent attacks are expected. For instance, capturing and analyzing IPv4 and IPv6 traffic is an important procedure in IT security to reduce attacks.

Integrity deals to protect information from alteration during communication by an unauthorized party. For example, communication between branches and DC shall assurance in the accuracy and completeness of transaction information and secure from tampering. The policy shall have a strong procedure to address and countermeasures that can protect from cyber-attacks and frauds.

Besides protecting information and data asset of the organization, the policy also shall grant the availability of is information to the success of business competitiveness. It shall ensure to provide the needed information timely as well as uninterrupted access to the system. Threats have a different technique to harm the organizational infrastructure and denying authorized users to access the information system.

6.4.2 Migration phase

Deploying IPv6

Deploying IPv6 is considered as an implementation of IPv6 in the existing infrastructure. This is assumed that the infrastructure is ready to run the new protocol side by side with IPv4. It has three sub-sections: transition model, testbed, and production environment. A hybrid transition model formulated by Dual-Stack and Tunneling is developed. A migration has n phases that depend on the migration architecture plan by engineers. Each n^{th} phase is first implemented on the organization testbed before the production environment. Once the implementation passes the test procedure, it shall deploy in the production environment. This reduces service interruption for the customers in the migration process.

A Hybrid migration model

A hybrid model is developed as a transition technique that fit for BIB. The model employs two independent transition techniques: Dual-Stack and Tunneling. The model has much flexibility since it is a combination of two transition techniques. Dual-Stack is used in the area where the equipment supports IPv6 and IPv4 on the backbone of the network (distributed and aggregated layer). Dual-Stack is important for the organization to deploy IPv6 depending on the performance requirement from the transition technique (Sansa-Otim & Mile, 2013). Manual-tunneling is deployed for areas that do not currently support IPv6 (Ethio-telecom) and to connect geographically distributed sites (branches) to the data center. The reason manual-tunneling is selected from traffic tunneling techniques is to enhance security.

A hybrid migration model has the following advantages on the organizational infrastructure:

- Flexibility to deploy,
- Enhanced security, and
- No need for immediate hardware upgrade for the infrastructure.

Generally, it can be said the advantage get from this hybrid model is vital for the organization to migrate its infrastructure smoothly. The model will be verified in the demonstration section.

Test Bed

A testbed is an important environment for IPv6. Implementation takes place before deploying in a real environment. As participants indicated BIB has its testbed that is dedicated to testing new technologies. The test environment has a collection of routers, switches, firewalls, and servers. This test environment aims to see the impact of new technologies, services, and products to decrease the interruption of the business environment. The test environment is logically separate from the production environment. Thus, anything done on the test environment will not have any impact on the production environment.

Test performing on a testbed provides a good opportunity to see different transition techniques, their behaviors on the current infrastructure. Not only this, but it has also a crucial role in the enhancement of security for the IPv6 environment. For example, expertise is free to perform different IPv6 penetration tests and other security enhancements. Iterative testing with appropriate documentation helps expertise better implementation structure and security for the production environment.

Generally, deploying IPv6 on the testbed has the following advantages for the migration framework:

- Enhance expertise skill and knowledge on IPv6 and transition techniques,
- Prevent interruption of service to customers,
- Enhance expertise confidence to deploy on the production environment,
- Enhanced security and performance for the production environment, and
- Reduce the risk.

Therefore, it can be concluded that the importance of testbeds in the migration process is fundamental for the success of the process by avoiding business environment interruption, risk on the production environment, and enhancement of security.

6.4.3 Post-migration

Support IPv6 infrastructure

After successful migration from IPv4 to IPv6, the infrastructure needs strong and rigorous support to sustain the environment more stable. Trained IT staff and other staff members have a role in this phase. They are expected to exhaust their knowledge and skills to maintain the new infrastructure. For instance, network engineers should be dedicated to monitoring network traffic and measure the performance of the new IPv6 based infrastructure. They also should give an immediate response to incidents that might face by performing troubleshooting in a short time.

Security teams shall have also a tangible operation to assist the new infrastructure. IPv6 is a new protocol, new threats are expected. The security team shall anticipate types of IPv6 attacks and shall be ready for those attacks. This can be done by performing a rigorous penetration test and hard coding on security devices. Thus, the security team has the responsibility to secure the IPv6 infrastructure.

6.4.4 Top management

In a previous chapter, top management is considered as one of the critical success factors for the IPv4 to IPv6 migration process. Effective involvement and support practice of senior management significantly improves migration success. Senior executives perceive that organizational issues are also more important for the success of the migration process than technical issues.

The organization shall spend much effort and resources in supporting the migration process. Migration to the IPv6 process is considered a large-scale and complex project. Senior management support is the most important and critical factor for project success in the organization (Ahmed, 2016; Young & Jordan, 2008). Senior management support is considered to enhance the understanding and perception of a project among its users, and stimulate better outcome (Boonstra, 2011).

Another vital role of this component in the framework is organizational funding. BIB highly depends on senior management to release funds for IPv4 to IPv6 migration process. Senior

management, especially executive management support needed to ensure appropriate funding for the migration. To get a sufficient budget, IT management needs to reflect on the role of the migration process and have an impact on meeting the organizational strategic objective.

Senior management also helps to secure the migration process resource. Executive management has the power to get the right people assigned for the migration by revising the organizational structure. This is done by selecting appropriate expertise to assist the migration process from an external source which enhances the quality of staff. They also approve an advanced budget that needs for the migration process.

6.5 Simulation

One of the research questions for this study is to identify the transition technique that fits for BIB in the transition process. In the previous chapter, a hybrid model is identified as a migration technique. Once the IPv6 transition strategies are accepted and populated by high-level management, one of the big issues is how to implement it in the organization. GNS3 simulator is conducted for simulation and experimental purposes by configuring the Cisco router having an IOS version 7200. After clearly defining the IPv4 and IPv6 addressing format, the Dual-Stack is used fully in the core layer, and manual tunneling is also implemented through Ethio-telecom MPLS. At the side of static routing, an OSPF routing protocol is selected for routers. It is open-source and suitable for a Dual-Stack and HSRP. Generally, as figure 6 - 2 illustrates, this experiment has taken between a DC and a sample branch.

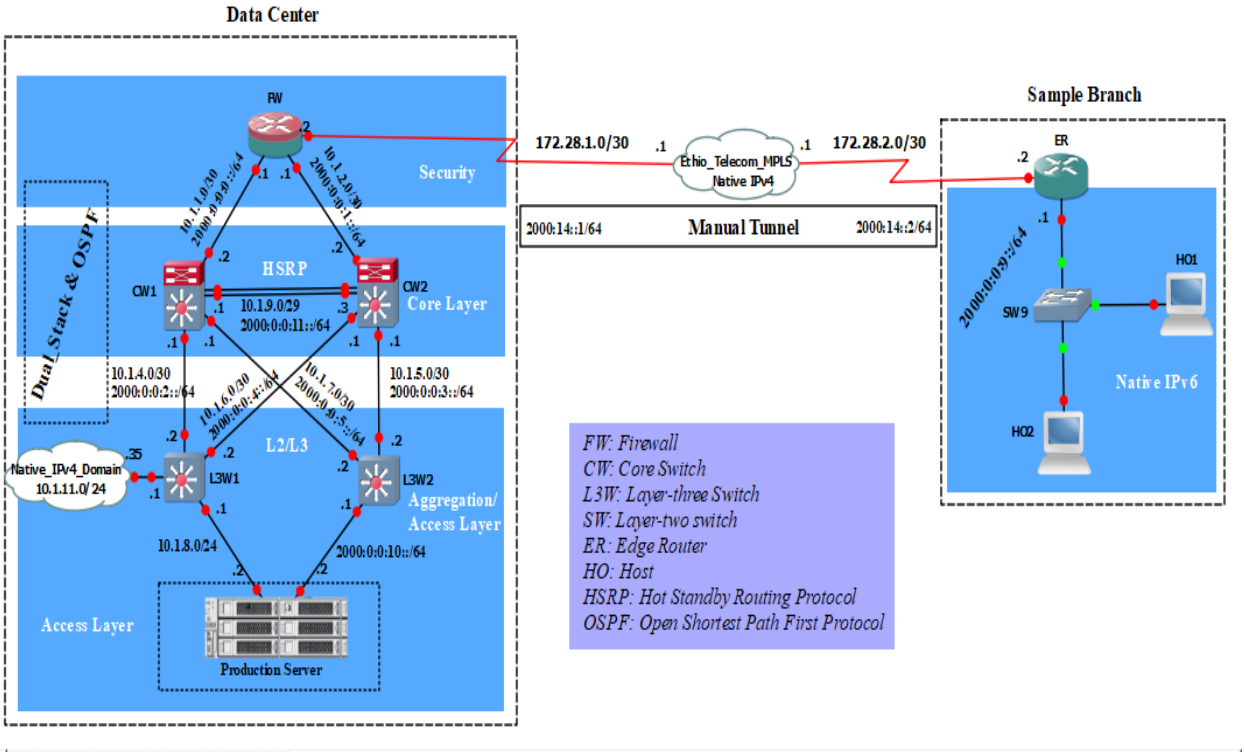

Figure 6 - 2: A hybrid transition model.

Core Layer

In chapter four, the researcher has identified the core layer is one of the major sections in the BIB data center. It is also referred to as the network backbone and responsible for transporting large amounts of data rapidly. For this experimental test, the researcher used two layer-three switches (CW1 and CW2) with high availability. It is a place where full Dual-Stack is implemented and their entire gigabit interfaces are configured with IPv4 and IPv6 simultaneously. Adjacent to a Dual-Stack, the OSPF routing protocol is configured with an area of 0 to facilitate the routing process.

Aggregation and Access layers

The aggregation layer ensures the highest possible performance between the core-layer and access-layer communication in DC. This avoids bottlenecks between devices in the network by aggregating multiple ports into a single connection. In this layer, L3W1 and L3W2 are configured

with static IPv4 and IPv6 addresses and participated partially in the Dual-Stack transition technique and also participated in OSPF routing protocol in area 0. A native IPv4 subnet connected on L3W1 is assumed and reserved for IPv4 users and devices delayed to migrate for different reasons that can access the production server (see figure 6 - 2).

The access layer is end-user devices such as production servers and desktop computers. Desktop computers and layer-two switches exist in the branch infrastructures are a native IPv6 network and aimed to access the production server in the BIB DC. In DC, the access layer is referred to as a production server with an assumption of containing all access switches in mind. As we can see from the diagram (see figure 6 - 2), the production server has a two-gigabit interface one for IPv4 and another for IPv6 users in the network. The purpose of giving two interfaces for IPv4 and IPv6 schema is to serve both native IPv4 and IPv6 domain concurrently.

Dual-Stack

The Dual-Stack transition technique is fully configured on the core layer and partially on an aggregated layer, where both IPv4 and IPv6 protocols are used simultaneously. Figure 6 - 2 illustrates the physical network designed for the simulation. FW, CW1, CW2, L3W1, and L3W2 are configured or assigned in both IPv4 and IPv6 addresses in their interface. They populate two separate routing tables for IPv4 and IPv6. Traffic generated from native IPv4 domains is routed through the IPv4 routing table and traffic generated from native IPv6 domains is routed through the IPv6 routing table. By doing this, devices are capable to entertain both protocols IPv4 and IPv6 traffic on the network. As we can see from the infrastructure design, native IPv6 domains like branches and native IPv4 domains have equal access to the production server. This makes users get a core-banking solution from IPv4 and IPv6 domains.

Each interface of core-switches (CW1 and CW2) is configured on both IPv4 and IPv6 protocols This makes them entertain each traffic that comes from those protocols and helps to establish their routing table (See figure 6 - 3 and figure 6 - 4).

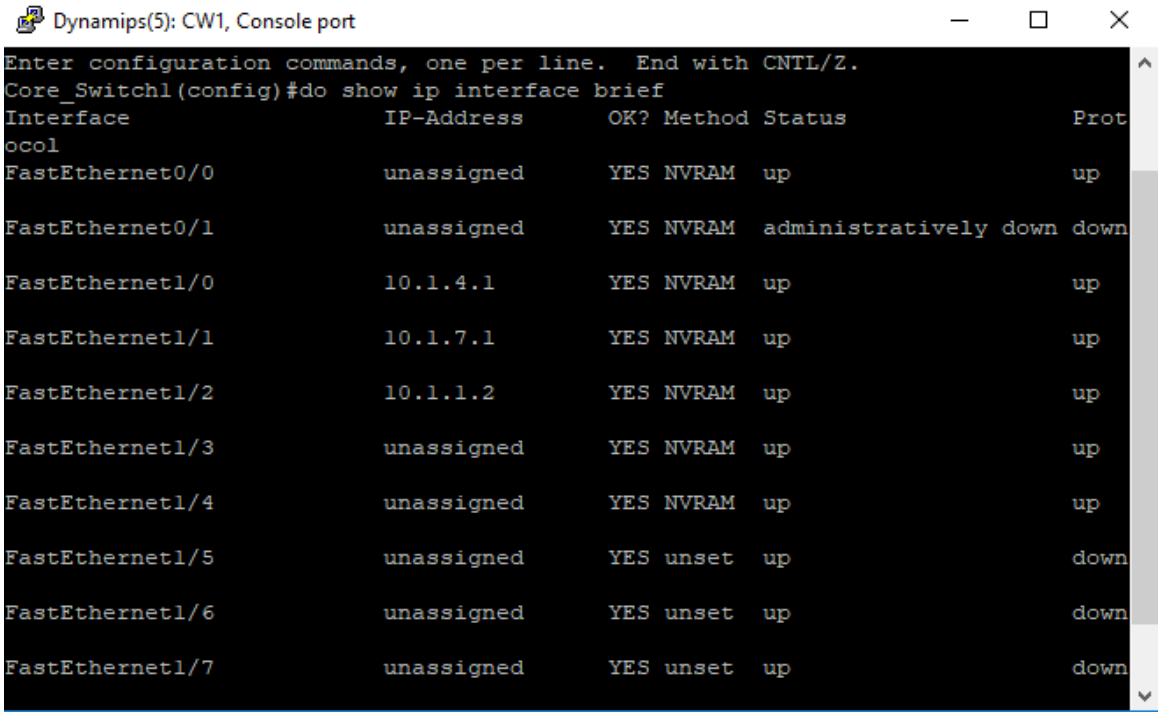

Figure 6 - 3: IPv4 interface status.

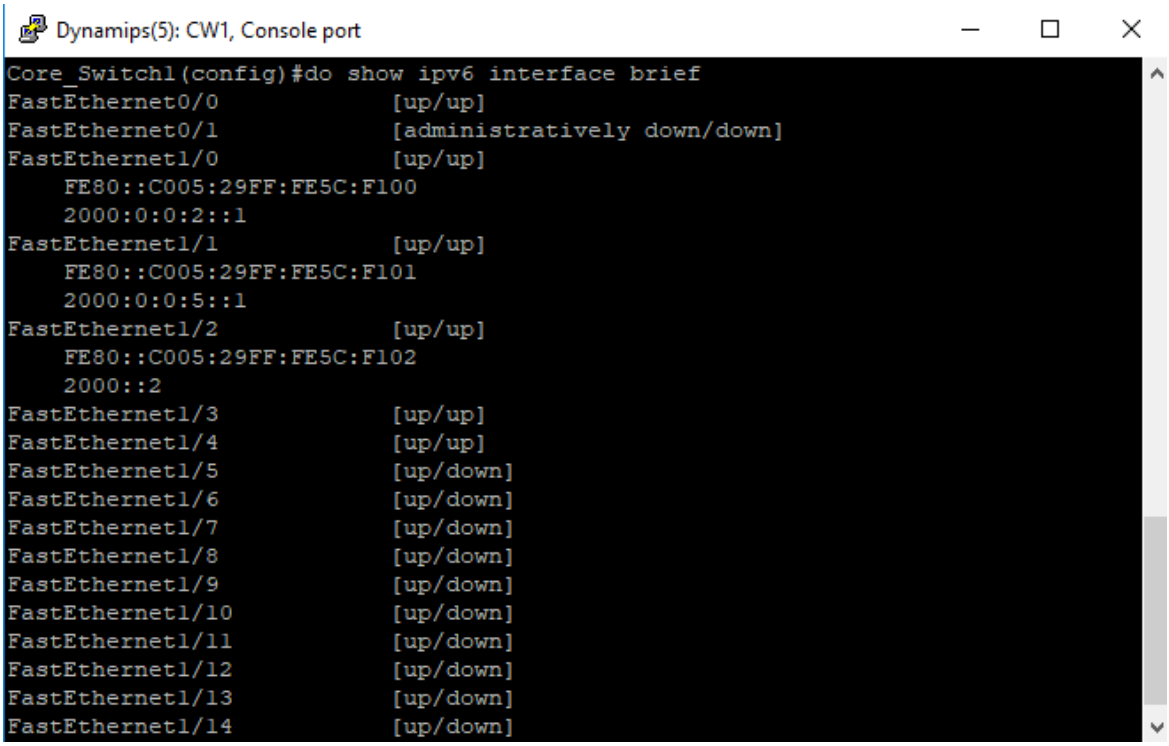

Figure 6 - 4: IPv6 interface status.

Figure 6 - 5 and Figure 6 - 6 show the routing table formulated by CW1. We can notice that both IPv4 and IPv6 are established their routing table to route their traffic separately. The reason for populating two different routing tables is the lack of backward compatibility of IPv6 to IPv4 (Samad et al., 2018).

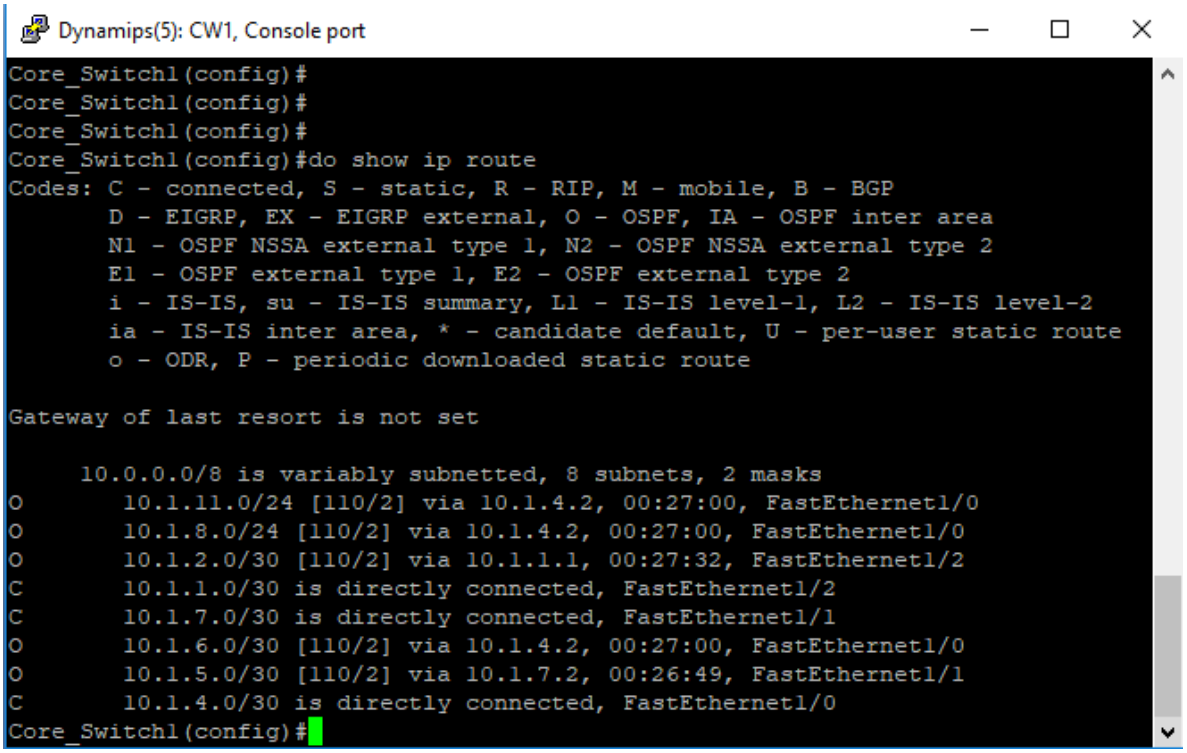

Figure 6 - 5: IPv4 routing table.

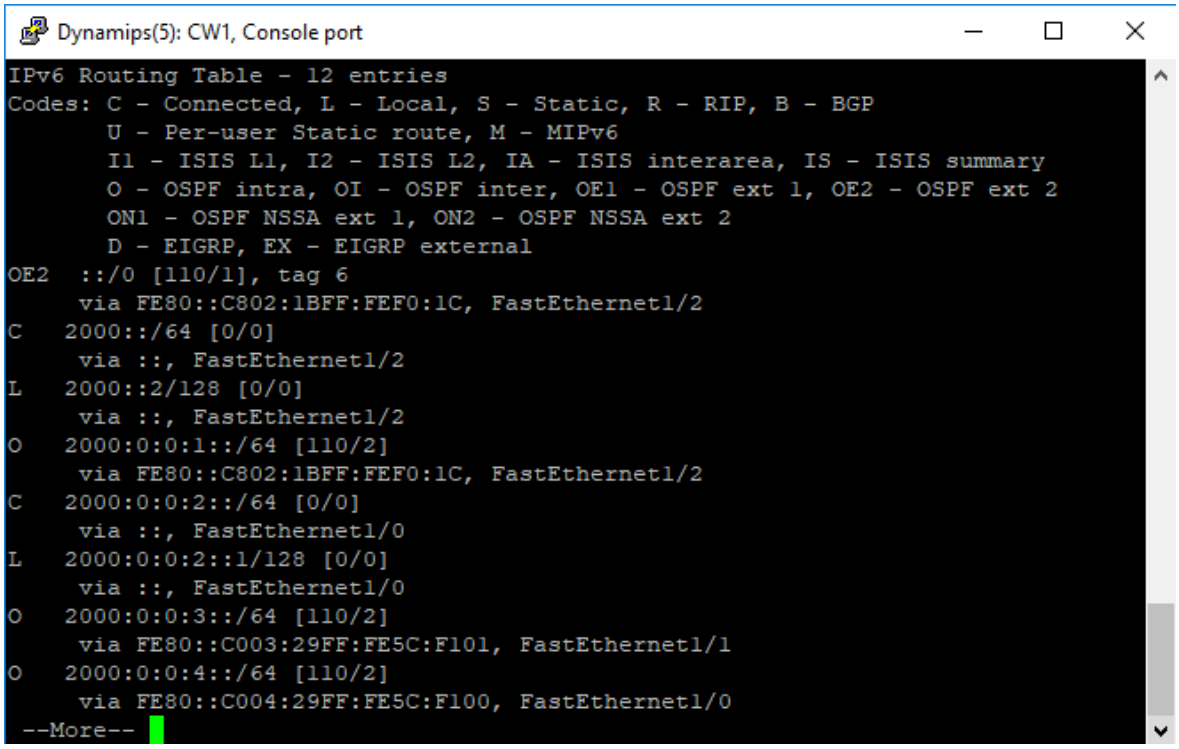

Figure 6 - 6: IPv6 routing table.

OSPF (Open Shortest Path First)

OSPF (Open Shortest Path First) is an open standard routing protocol that's implemented in both core-layer and aggregated layers. There are multiple routers and L3 switches. Using the OSPF protocol makes the routing process efficient and less congestive. It has two versions, OSPFv2 and OSPFv3. In the researcher's demonstration, both versions are used. As we have seen in the above section, the Dual-Stack is implemented and also seen two routing tables for IPv4 and IPv6. OSPFv2 only supports IPv4 protocol and is used to formulate the IPv4 routing table for the best path from source to destination. OSPFv3 supports IPv6 protocol. As figure 6 - 5 and 6 - 6 also illustrate the routing table for IPv4 and IPv6 formulated by the OSPF protocol. "O" represented a routing path formulated an OSPF protocol in both IPv4 and IPv6 routing tables.

Figure 6 - 7 (*show run | sec ospf*) also confirmed that both OSPFv2 and OSPFv3 are running in the Dual-Stack devices. OSPFv2 uses an area 0 and OSPFv3 uses an area 6 to advertise their subnets to their neighbor in the Dual-Stack process.

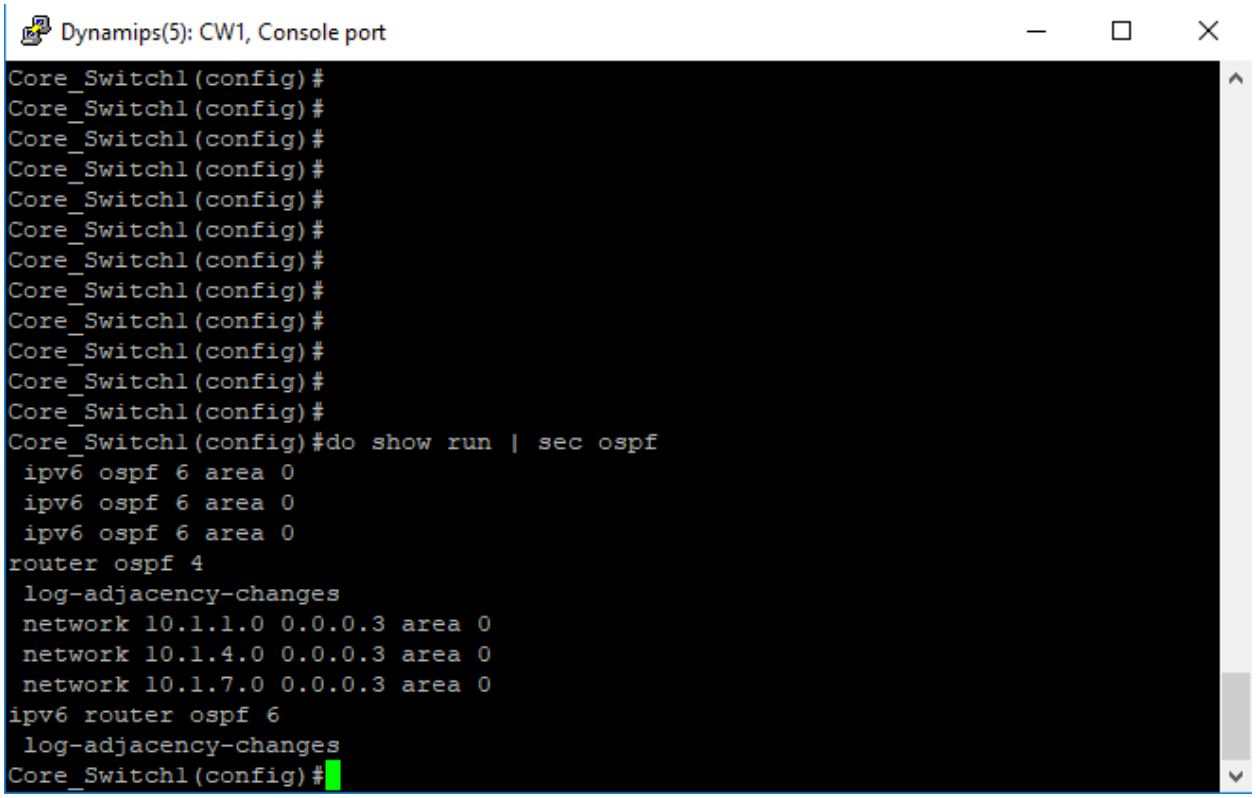

Figure 6 - 7: IPv4 and IPv6 OSPF area.

Manual Tunneling

After successfully configured major network devices in the DC infrastructure in IPv4 and IPv6, native IPv6 must communicate to the DC infrastructure. The Dual-Stack is in the position to communicate IPv4 and IPv6. DC infrastructure components can communicate with each other. One of the barriers considered is Ethio-telecom infrastructure. If this ISP is not migrated to IPv6 at an appropriate time, BIB needs tunneling strategies. By using tunneling strategies, the IPv6 traffic can be transmitted with the help of the IPv4 network which already exists. This is done by embedding the IPv6 packet inside the IPv4 packet header so that it can be routable in the existing Ethio-telecom IPv4 infrastructure. At the final stage, the IPv6 packet is extracted from the IPv4 header and the actual and secured IPv6 payload will be load into the router.

There are several tunneling strategies and classified as manual and automatic tunneling. Automatic tunneling strategies have potential security threats compared to manual tunneling strategies. A router has a chance to make a tunnel with a neighbor considered as hostile. Once they perform a tunnel, a hostile device has access to BIB's network and also can inject and advertise its routing

in the network. To avoid this security hole, the researcher preferred to use manual tunneling strategies. A network administrator establishes a tunnel on behalf of routers. In technical speaking, the administrator defines the source and destination of the tunnel and tells the router how to make a tunnel by defining a static argument.

Like Dual-Stack, manual tunneling uses both IPv4 and IPv6 addresses. The IPv4 address is assigned to the physical interface of the router (172.28.1.0/30), offered by the Ethio-telecom. Using this IPv4 address schema as a source and destination, a new virtual tunnel and interface are created in the DC firewall and branches edge router. Figure 6 - 8 and Figure 6 - 9 (*show ip int bri and show IPv6 int bri*) illustrates the two interfaces.

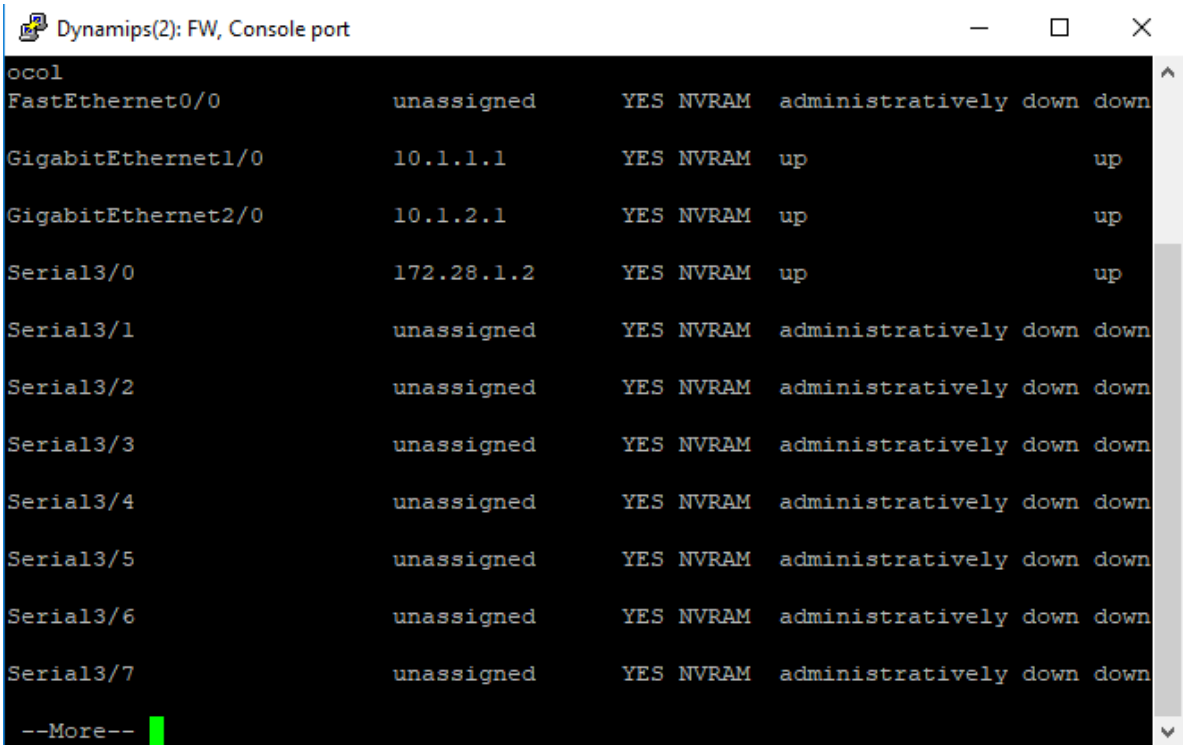

Figure 6 - 8: IPv4 configuration for physical interfaces.

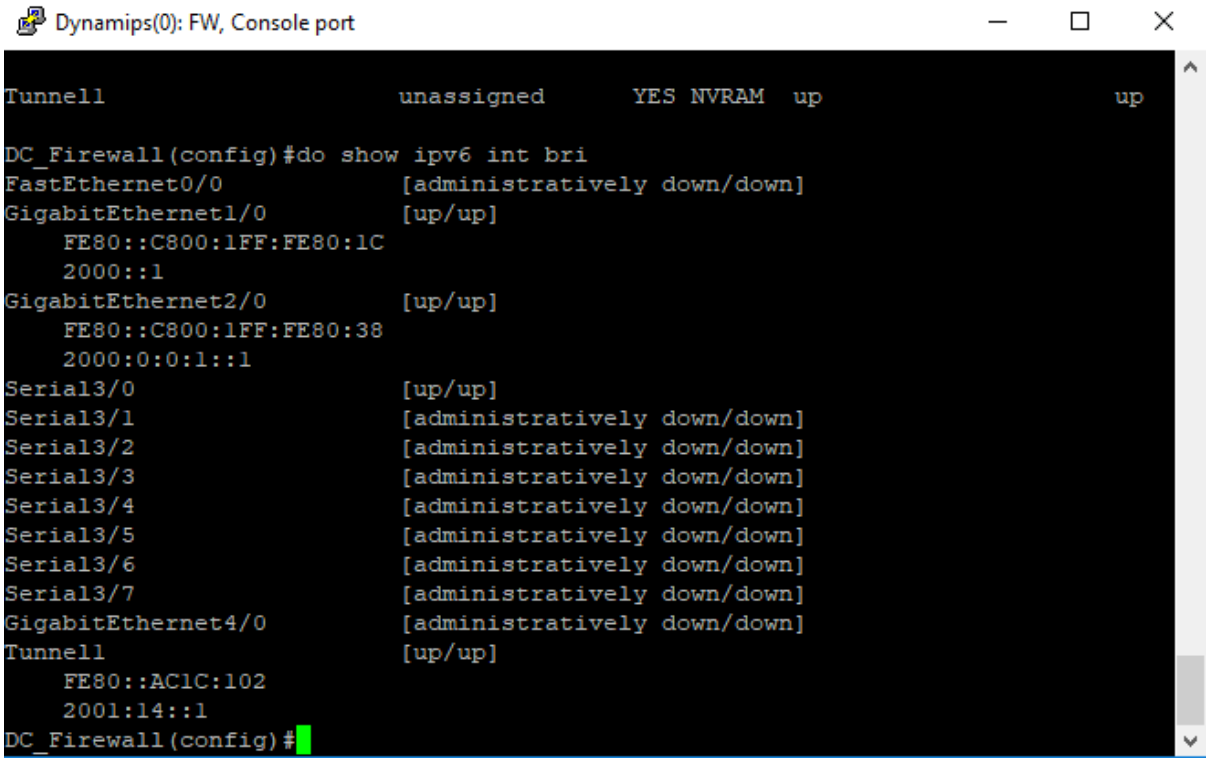

Figure 6 - 9: IPv6 configuration for physical interfaces.

Figure 6 - 10 (*show int tunnel 1*) shows detailed information about the tunnel between the DC firewall and the branch's edge router. It clearly shows that the tunnel uses the IPv4 address as a source and destination defined by the administrator to encapsulate the traffic inside of it. Moreover, it also shows that the tunnel protocol is using IPv6/IP.

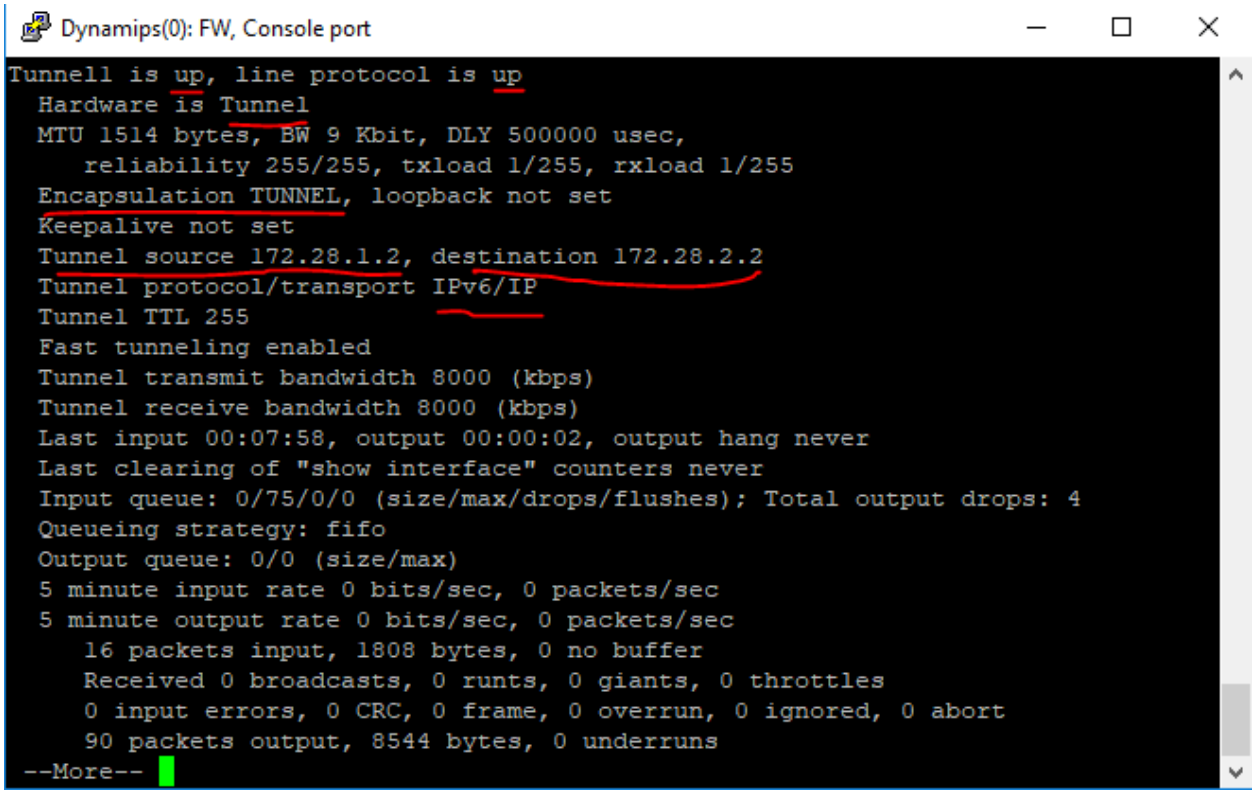

Figure 6 - 10: A manual tunnel configuration and its status.

The other good justification is showed in figure 6 - 11 (*show run | sec tunnel*). The manual tunneling technique is used by the administrator, which is "*ipv6ip*". It means to tell the router to encapsulate IPv6 traffic within IPv4 traffic. Without all settings we have seen so far, the router will not produce the peer with other routers dynamically.

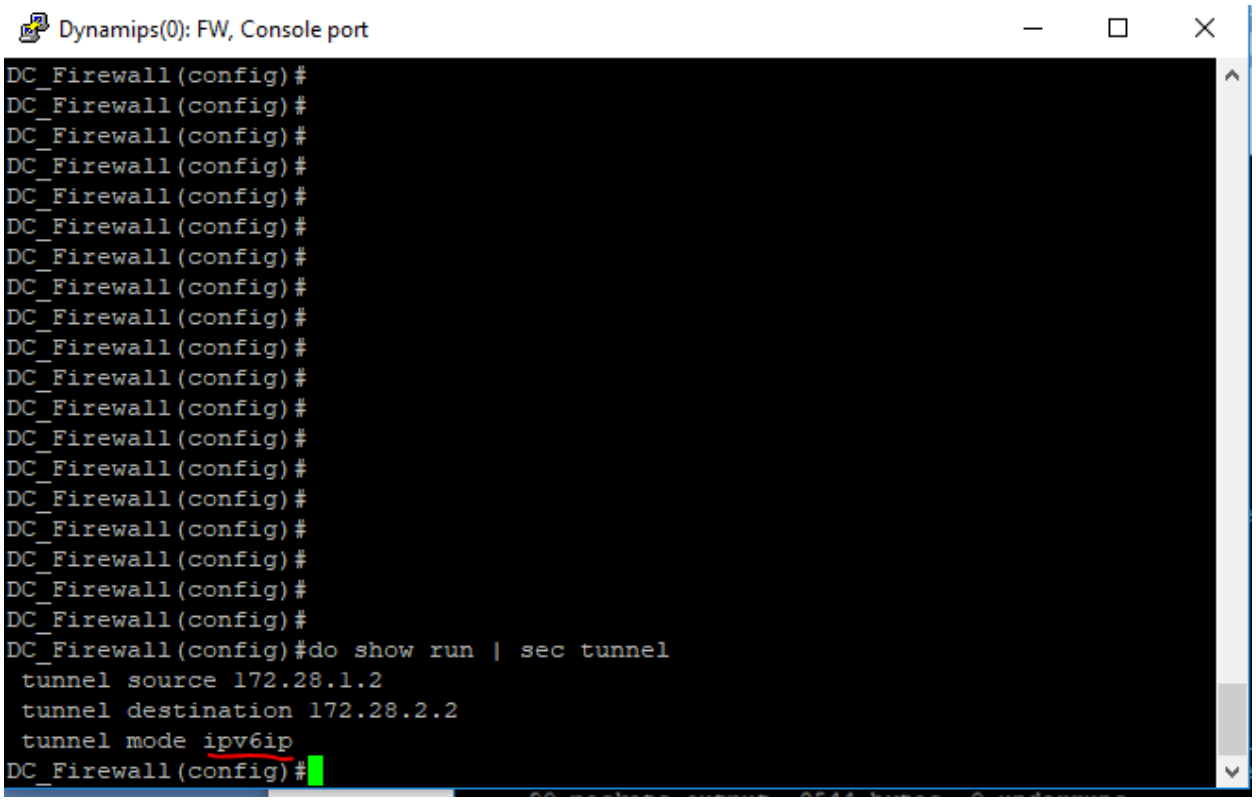

Figure 6 - 11: A manual tunnel configuration (ipv6ip).

To finalize this demonstration, the researcher did confirm the communication between IPv4 and IPv6 protocol as well as the accessibility of DC from the sample branch. To do so, the researcher executes a "*ping*" command from a sample branch edge router (native IPv6) and from the native IPv4 domain to a production server. Figure 6 - 12 and 6 - 13 confirmed that communication is done successfully.

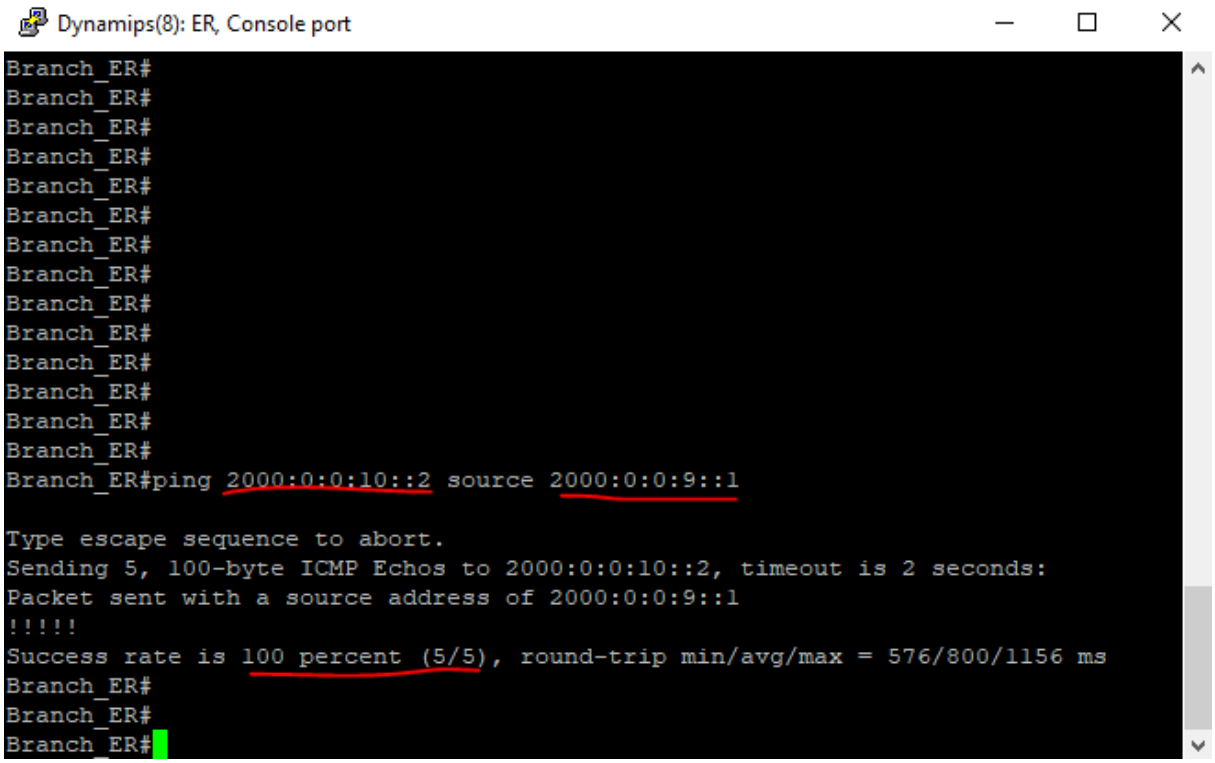

Figure 6 - 12: Connectivity checking between branch and DC.

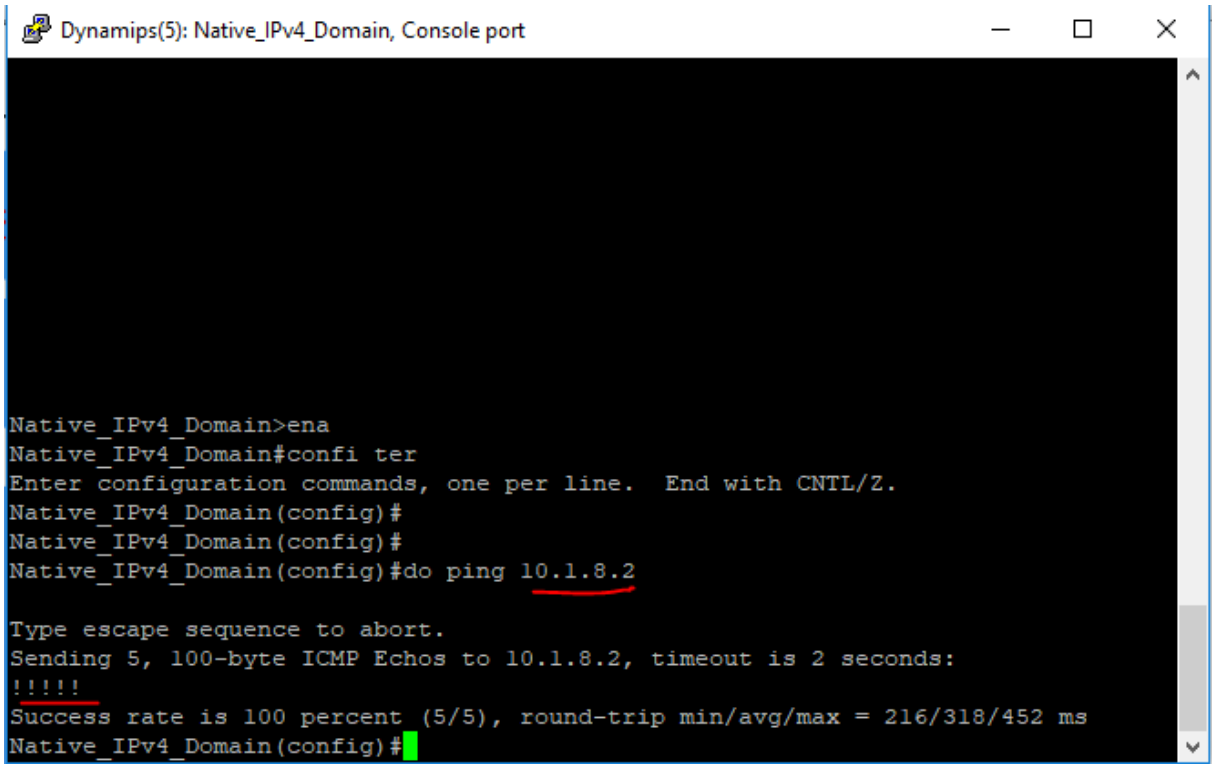

Figure 6 - 13: Connectivity checking between native IPv4 domains to a production server.

6.6 Evaluation

Evaluation occurs after the development of an IS artifact (Pries-Heje, Baskerville, & Venable, 2008). Evaluation is an empirical process or method that can be done in the same way as empirical research approaches. It is a core activity in conducting design science research and it should also measure the quality and efficacy of the artifact rigorously (Venable, Pries-heje, & Baskerville, 2012). Evaluation of a framework or an artifact is the development of criteria and the assessment of the artifact's performance. Moreover, the evaluation also has to determine how and why the proposed artifact worked.

Iteration in the development of the framework

Since the research approach is a design science, it gives flexibility in the development of the framework by the number of iterations. In this study, the researcher performed one iteration to come up with the desired output. This iteration was recycled to the design and development phase to change the framework architecture.

In the demonstration section, a framework has been demonstrated to the participants. According to their oral judgment and comment of the participants, positive comments and feedback have been noted. However, most of the respondents gave their comments on the migration phase that needs some improvement. The previously developed framework had a linear structure in the deployment of IPv6 on the organizational infrastructure (see figure 6 - 14).

Figure 6 - 14: Previous IPv6 deployment approach

A hybrid migration model was first tested on the testbed before it was directly implemented in the production environment. This helps expertise to know expected output while it is implemented in the production environment. However, the previous IPv6 implementation approach was limited by its lack of flexibility in the implementation because of its sequential nature. Thus, considering the participant comments and feedbacks, the framework development process iterates back to the redesign and development phase to come up with the recycled implementation approach (see figure 6 - 15).

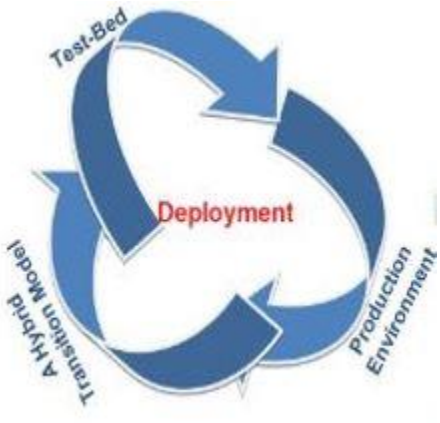

Figure 6 - 15: Modified IPv6 deployment approach

Unlike the previous IPv6 deployment approach, the modified approach has more flexibility and also has an N number of iterations in the process. The hybrid model can be iteratively tested and implemented in the testbed and production environment respectively.

Finally, the participant also got a chance to evaluate the final framework based on the ISO/IEC 25010:2011 quality model to accept their feedback for further development and assure the rigor of this study. The evaluation criteria have eight major components: Effectiveness, efficiency, satisfaction, usefulness, trust, freedom from risk, and context coverage, and flexibility.

Descriptive Statistics					
Evaluation Criteria	N	Min	Max	Mean	Std. Dev
1. Effectiveness **How do you rate the framework in terms of accuracy and completeness with which users achieve the IPv6 migration process?**	8	3.0	5.0	4.000	.5345
2. Efficiency **How do you evaluate the framework in terms expended with the accuracy and completeness with which users achieve the IPv6 migration process**	8	3.0	5.0	4.750	.7071
3. Satisfaction **How do you rate the framework in terms of the degree to which user needs are satisfied when a framework is used in BIB context of the use**	8	3.0	5.0	4.125	.6409
4. Usefulness **How do you rate the degree to which a user is satisfied with their perceived achievement of pragmatic goals, including the results of use and the consequences of use**	8	3.0	5.0	4.375	.7440
5. Trust **How do you rate the degree to which a user or other stockholders has confidence that a framework will behave as intended**	8	3.0	5.0	4.500	.7559
6. Freedom from risk **How do you rate the degree to which a framework mitigates the potential risk to economic status, human life, health, or the environment?**	8	2.0	5.0	4.250	1.1650
7. Context coverage	8	3.0	5.0	4.500	.7559

How do you rate the degree to which a framework can be used with effectiveness, efficiency, freedom from risk, and satisfaction in both specified contexts of use					
8. Flexibility	8	3.0	5.0	4.500	.7559
How do you rate the degree to which a framework can be used with effectiveness, efficiency, freedom from risk, and satisfaction in contexts beyond those initially specified in the requirements					
Valid N (listwise)	8				

Table 6 - 1: Mean and standard deviation of the framework evaluation

The evaluation framework result shows the framework has the highest mean value of 4.750 on efficiency which indicates that respondents highly agree on the framework efficiency in terms of expended with accuracy and completeness with the user's achievement IPv6 migration process. On the other hand, 4.000 is shown as a list of results on effectiveness. However, it implies respondents also agree on the framework's effectiveness.

Generally, mean values that are greater than 4.000 indicate respondents strongly agree with the criteria. Thus, the aggregate mean result is 4.375, which is strongly agrees with the overall framework quality. Besides the ISO model evaluation, the GNS3 tool demonstration also justified that a hybrid transition model has 100% end to end communication between DC and sample branch (see figure 6 – 12 and figure 6 - 13).

6.7 Chapter Summary

In this chapter, we have discussed the framework components and how they are developed. Thereafter, the hybrid transition model has been demonstrated using GNS3 to confirm the usability of the model. Finally, the overall framework also evaluated using ISO/IEC 25010:2011 quality model.

CHAPTER SEVEN

7. CONCLUSION AND RECOMMENDATION

7.1 Overview

In previous chapters, BIB's infrastructure is assessed. Data are collected with an interview, document analysis, and observation. Thematic analysis is performed to analyze the data. As a result, this chapter provides the conclusion and recommendation of this study. Depend on the finding of the study, the chapter proposes ideas for future work.

7.2 Conclusion

The ultimate goal of this study was to develop a framework that assists BIB's infrastructure to migrate from IPv4 to IPv6. To support this study, a literature review has been conducted on IPv4 vs IPv6 protocols, IPv4 to IPv6 transition techniques, challenges and factors to IPv6 migration, and IPv6 strategies and deployment. Moreover, the current infrastructure of the organization is assessed to assist the framework development.

A design science research approach is conducted as a research methodology. Data are collected using interviewees of domain expertise, document analysis, and direct observation. Thematic analysis has been used to analyze collected data. The developed framework is demonstrated to the respondent and a hybrid transition model also demonstrated using the GNS3 tool. Thereafter, the framework was also evaluated by ISO/IEC 25010:2011 standards.

A developed framework had three phases: pre-migration, migration, and post-migration phase. Pre-migration is the first phase of the migration process and it had readiness, infrastructure equipment, infrastructure upgrade, planning, and staff training as sub-components. The migration phase is the main phase in the migration process where a real migration takes place. In IPv6 deployment, a rigorous examination of IPv6 is performed on the testbed before applying to the production environment. Additionally, a hybrid migration model is also introduced. The model is a fusion of Dual-Stack and manual tunneling migration techniques. Dual-Stack is implemented on a core-layer or backbone of network infrastructure. The manual tunnel is used on site-to-site communication between DC and branches. The last phase in the framework is post-migration and

it is stressed the follow-up and support of new IPv6 infrastructure to keep going the organization business.

Besides the ultimate objective of this study, this study also tried to answer the research questions defined in chapter one.

1. What are the factors that have an impact on the IPv4 to IPv6 migration process?
   During the study, four major factors are exit in the migration process from IPv4 to IPv6. Those are individual factors, Organizational factors, physical factors, and security factors. Each factor had many sub-factors (please refer to chapter five).
2. What transition technique that fit for BIB infrastructure?
   A hybrid transition model is proposed in this study. The model is made up of well-known transition techniques: Dual-Stack and manual tunneling. The model is developed and demonstrated by considering BIB's current infrastructure (please refer to chapter six).

7.3 Recommendation for practice

BIB's infrastructure has a great role for different applications including a core-banking solution to maintain the organizational business. The migration of the current infrastructure to IPv6 is a complex task. The proposed framework offered by this study has a practical and general guideline for practitioners when the company transits its infrastructure from IPv4 to IPv6.

The hybrid transition model has Dual-stack and manual tunneling techniques. Considering applying two transition techniques has a vital advantage for the secured migration process. The IT policy and procedure need to be modified, following the new procedure and policy rigorously is an important task by staff members for the success of the migration process. Moreover, until the migration process is inclusive, the coexistence of IPv4 and IPv6 protocols is high and will work side by side. Thus, the company security architecture should be hard to avert attack comps from both protocols.

Data obtained from respondent expose that there is a lack of IPv6 training in the company. Since staff training has a great infuse on the migration process; the company should give well-formulated training for staff members before the IPv6 deployment. IPv6 training offer by the company should be at an advanced and operational level that build members knowledge and increase their technical

capabilities. Related to this, the company also should be willing to invest much in those training to assist the knowledge building on staff members.

There is also noted a lack of expertise on IPv6. This comes from staff members has lack skills in this protocol. The organization should consider and work on the enhancement of staff quality. Further investigation needs on the assessment of the quality of staff towards IPv6.

IPv6 deployment is considered a long-term project, thus planning is the most vital part of the migration process. The planning should consider design, test, implementation, training, and operational cost. Related to that detailed assessment of infrastructure or network architecture for IPv6 deployment is important.

Senior management should have awareness and a clear idea of the benefit get from this migration process. IT senior management should devote much to produce the awareness of IPv6 related to organizational business competitiveness to the rest of non-IT senior management. The migration process needs more budget, resources, and approval by top management. Both IT and non-IT senior management support is a crucial task in the migration process.

7.4 Limitation and future work

The study comes up with a migration framework that guides the organization's current infrastructure to IPv6 infrastructure. However, some limitations are mentioning to open for future studies.

The study is limited to BIB’s infrastructure is considered as the limitation of this study. The organization has different applications that rely on the infrastructure, future studies should see and consider the application perspective of the IPv6 adoption process parallel to the infrastructure.

The hybrid transition model proposed by the framework is also limited to BIB. It opens a wide way for other researchers to enhance the model or investigate other transition models by on other financial sector's infrastructure in the country.

Further studies conducting on the development and enhancement of a framework on other organizations exist in different business sectors can give a holistic view of the phenomenon or the transition process for the organizations.

Finally, security is becoming the most important point in the migration process. The technical security aspect of IPv4 to IPv6 migration could be investigated by other researchers by considering different transition techniques.

REFERENCES

Ahmad, N. M., & Yaacob, A. H. (2012). IPSec over heterogeneous IPv4 and IPv6 Networks : Issues and implementation. *International Journal of Computer Networks & Communication*, *4*(5), 57–72.

Ahmed, R. (2016). Top management support and project performance: An empirical study of public sector projects. *International Annual Conference of the American Society for Engineering Management, ASEM 2016*, (March). https://doi.org/10.2139/ssrn.3044377.

Al-zobbi, M. (2014). Comparison between IPv4 and IPv6 in adopting differentiated services. *International Journal of Scientific & Technology Research*, *3*(2), 237–242.

Albkerat, A., & Issac, B. (2014). Analysis of IPv6 transition technologies. *International Journal of Computer Networks & Communication, 6*(5), 19-38.

Arafat, M. Y., Sobhan, M. A., & Ahmed, F. (2014). Study on migration from IPv4 to IPv6 of a large scale network. *Canadian Center of Science and Education*, 8(3),67-83. https://doi.org/10.5539/mas.v8n3p67.

Arifin, A. H., Abdullah, D., Berhan, S. M., & Budiarto, R. (2006). An economical IPv4-to-IPv6 transition model: - A case study for university network. *International Journal of Computer Science and Network Security*, *6*(11), 170–178.

Babiker, H., Nikolova, I., & Chittimaneni, K. K. (n.d.). Deploying IPv6 in the Google enterprise network.

Baker, F., & Li, X., & Yin, K. (2011). Framework for IPv4/IPv6 translation. *Internet Engineering task force (IETF).*

Bendale, R., Naykude, S., & Nikam, N. (2015). IPv4 to IPv6 migration strategies. *International Journal of Engineering and Technical Research,* 3, 135–137.

Bisandu, D. B. (2019). Design science research methodology in computer science and information systems. *International Journal of Information Technology*, 1–7.

Bouras, C., Ganos, P., & Karaliotas, A. (2003). The deployment of IPv6 in an IPv4 world and transition strategies. *Internet Research: Electronic Networking Application and Policy, 13*(2), 86–93. https://doi.org/10.1108/10662240310469033.

Boonstra, A. (2011). How and why do top managers support or not support strategic IS projects? *Communications in Computer and Information Science*, *220 CCIS*(PART 2), 369–379. https://doi.org/10.1007/978-3-642-24355-4_37.

Caicedo, C. E. (2014). Security issues in IPv6 networks introduction.

Chauhan, D., & Sharma, S. (2014). A survey on next generation internet protocol: IPv6. *International Journal of Electronics and Electrical Engineering*, 2(2), *143-146.*

Chiniah, A. (2014). Assessment of IPv6 readiness and adoption strategy for Mauritius. *International Conference on Advanced in Engineering and Technology*, Singapore, March 29-30, http://dx.doi.org/10.15242/IIE.E0314230.

Chown, T. (2002). IPv4 to IPv6 migration scoping report for organizational (NREN) networks.

Chukwuemeka Paul, H., & Bakon, K. A. (2016). A study on IPv4 and IPv6: The importance of their co-existence. *International Journal of Information Systems and Engineering*, *4*(2), 97-106.https://doi.org/10.24924/ijise/2016.11/v4.iss2/97.106.

Cooper, M., & Yen, D. C. (2005). IPv6 : Business applications and implementation concerns. *Computer Standards & Interfaces,* 27–41. https://doi.org/10.1016/j.csi.2004.11.001.

Cui, Y., Dong, J., Wu, P., Wu, J., Metz, C., Lee, Y. L., & Durand, A. (2013). Tunnel-based IPv6 transition. *IEEE Internet Computing*, *17*(2), 62–68. https://doi.org/10.1109/MIC.2012.63.

Dawadi, B. R., Joshi, S. R., Khanal, A. R., & Pulchowk, C. C. (2015). Service provider IPv4 to IPv6 network migration strategies. *Journal of Emerging Trends in Computing and Information Sciences*, *6*(10), 4–10.

Dell, P. (2014). A comparison of attitudes to IPv6 in three countries. *Jurnal Sistem Informasi*, *1*(2), 87–100.

Dell, P. (2018). On the dual-stacking transition to IPv6 : A forlorn hope ? *Telecommunications Policy*, *42*(7), 575–581. https://doi.org/10.1016/j.telpol.2018.04.005.

Dhamale, D., & Singh, G. (2018). Migration from IPv4 to IPv6. *International Journal of Pure and Applied Mathematics*, *118*(24), 1–9.

Etikan, I., Musa, S., & Alkassim, R. (2015). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4.

Fairholm, M. R. (2009). Leadership and organizational strategy. *Innovation Journal*, *14*(1), 1–16.

Gizachew, N. (2019). IPv6 migration framework for Ethio Telecom. *Addis Ababa University*, *Addis Ababa*.

Gold, S. (2011). IPv6 migration and early action. *Network Security*, *2011*(3), 15–18. https://doi.org/10.1016/S1353-4858(11)70027-7.

Govil, J., Govil, J., Kaur, N., & Kaur, H. (2008). An examination of IPv4 and IPv6 networks: constraints and various transition mechanisms. *Conference Proceedings - IEEE SOUTHEASTCON*, 178–185. https://doi.org/10.1109/SECON.2008.4494282.

Hasab, N., Abu, E., Babiker, A., & Mustafa, A. N. (2014). IPv4 to IPv6 Migration. *International Journal of Engineering and Technical Research*, 2, 181–183.

Hilles, S. M. S., & Faniran, Q. (2017). Evaluating IPv4 to IPv6 transition for a small enterprise in Nigeria. *International Journal of Contemporary Computer Research*, *1*, 4–8.

Igwenagu, C. (2016). Fundamentals of research methodology and data collection. *LAP Lambert Academic Publishing*, (June), 4. Retrieved from https://www.researchgate.net/publication/303381524_Fundamentals_of_research_methodology_and_data_collection.

Isaac, S. (2017). Comparative analysis of IPV4 and IPV6. *International Journal of Computer and Information Technologies*, 7(2), 675–678.

Jayasanka, A. (2015). An approach for stable migration of IPv4 to IPv6 in Sri Lankan ISP. 0-4.

Kanth, R. (2016). Comparative performance test on IPv6 migration technique : Tunneling. *International Journal of Applied Engineering Research*, 10, 681-688.

Karthikeyan, N., & Chandra, K. (2016). Corporate migration from IPv4 to IPv6 using different transition mechanisms. *International Journal of Engineering Sciences & Research Technology*, 5(10), 802-808.

Kaur, A.(2015). How is digital infrastructure adopted and assimilated? The IPv6 story. *Auckland University of Technology*.

Khudhair, E. H., & Mohammed, I. J. (2017). A prototype and roadmap for transition to IPv6 with performance evaluation. *Research Journal of Applied Sciences, Engineering and Technology*, 14(8), 299-309. https://doi.org/10.19026/rjaset.14.4954.

Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, & Samir Chatterjee. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77.

Mackay, M., Edwards, C., Dunmore, M., Chown, T., & Carvalho, G. (2003). A scenario-based review of IPv6 transition tools. *IEEE Internet Computing*, *7*(3), 27–35. https://doi.org/10.1109/MIC.2003.1200298.

Main, A., Politechnic, M., Zakaria, N. A., & Robiah, Y. (2014). Organizational readiness element to develop readiness model for IPv6 migration. *Journal of Applied Science and Agriculture*. 9(18), 30-35.

Matebie, D. (2019). Designing a framework for IPv4 to IPv6 application and system transition: The case of Ethio Telecom. *Addis Ababa University*.

Mazumder, R., Alam, M., & Habib, A. (2011). Comparative sutdy of IPv4 and IPv6. *International journal of Mobile & Adhoc Network*, 1, 334-338.

Mekonnen, K., & Abdulkadir, T. (2013). IPv6 migration framework – case of institution in Ethiopia. *HiLCoE School of Computer Science and Technology*, 1(1), 100-103.

Muzhir, P., Ani, S. A.-, & Haddad, R. A. A. (2012). IPv4 / IPv6 transition. *International Journal of Engineering Science and Technology*, *4*(12), 4815–4822.

Majid, M. A. A., Othman, M., Mohamad, S. F., Lim, S. A. H., & Yusof, A. (2017). Piloting for interviews in qualitative research: operationalization and lessons learnt. *International Journal of Academic Research in Business and Social Sciences*, *7*(4). https://doi.org/10.6007/ijarbss/v7-i4/2916.

Narayanan, A. S., Mohideen, M. S. K., & Raja, M. C. (2012). IPv6 tunneling over IPv4. *International Journal of Computer Science Issues*, *9*(2), 599–604.

Nila, l.(2012).Transition from IPv4 to IPv6 best methods for large enterprise networks. *Lahti University of Applied Sciences*, 66.

Nikkel, B. J. (2007). An introduction to investigating IPv6 networks. *Digital Investigation 4*, 59–67. https://doi.org/10.1016/j.diin.2007.06.001.

Nizar, A., & Ali, A. (2012). Comparison study between IPv4 & IPv6. *International Journal of Computer Science*, *9*(3), 314–317.

Oxley, A. (2014). Issues affecting the adoption of IPv6. *International Conference on Computer and Information Sciences, ICCOINS 2014 - A Conference of World Engineering, Science and Technology Congress, ESTCON 2014 - Proceedings*, 1–6. https://doi.org/10.1109/ICCOINS.2014.6868375.

Petra, H., & Lietz. (2010) Research into questionnaire design – A summary of the literature. *International Journal of Market Research* Vol. 52 Iss.

Pries-Heje, J., Baskerville, R., & Venable, J. (2008). Strategies for design science research evaluation. *16th European Conference on Information Systems, ECIS 2008*.

Punithavathani, D. S., & Sankaranarayanan, K. (2009). IPv4/IPv6 transition mechanisms. *European Journal of Scientific Research*, *34*(1), 110–124.

Quintero, A., Sans, F., & Gamess, E. (2016). Performance Evaluation of IPv4 / IPv6 transition mechanisms. *l.J Computer Network and Information Security*, 2, 1–14. https://doi.org/10.5815/ijcnis.2016.02.01.

Saklani, A., & Dimri, S. C. (2013). Technical comparison between IPv4 & IPv6 and migration from IPv4 to IPv6. *International Journal of Science and Research*, *2*(7), 52–55.

Samad, F., Abbasi, A., Memon, Z. A., Aziz, A., & Rahman, A. (2018). The future of Internet: IPv6 fulfilling the routing needs in Internet of things. *International Journal of Future Generation Communication and Networking*, *11*(1), 13–22. https://doi.org/10.14257/ijfgcn.2018.11.1.02.

Shah, J. L., & Parvez, J. (2015). Optimizing security and address configuration in IPv6 SLAAC. *Procedia - Procedia Computer Science*, *54*, 177–185. https://doi.org/10.1016/j.procs.2015.06.020.

Sharma, V. (2010). IPv6 and IPv4 security challenge analysis and best practice Scenario. *International Journal of Advanced of Networking and Application*, *1*, 258–269.

Shevenell, M. (2005). Managing IPv6 Networks. 1-8.

Stevens, T., Vlaeminck, K., Meerssche, W. Van De, Turck, F. De, Dhoedt, B., & Demeester, P. (2005). Deployment of service aware access networks through IPv6. *8th International Conference on Telecommunication*, 7–14.

Sansa-Otim, J. S., & Mile, A. (2013). IPv4 to IPv6 transition strategies for enterprise networks in developing countries. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *119 LNICST* (February 2011), 94–104. https://doi.org/10.1007/978-3-642-41178-6_10.

Thalmann, A. J., & Harris, N. G. (n.d.). Internet protocol version 6 network migration and performance analysis. *The University of the witwatersrand, Johannesburg.*

Tomar, S. S., & Rawat, A. (2017). Study on QoS gains in migration from IPv4 to IPv6 Internet. *Information Technology and Computer Science*, *5*, 1–8. https://doi.org/10.5815/ijitcs.2017.05.01.

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Journal*, *5*, 147–158.

Taib, A. H. M., & Budiarto, R. (2007). Security mechanisms for the IPv4 to IPv6 transition. *2007 5th Student Conference on Research and Development, SCORED*, (December). https://doi.org/10.1109/SCORED.2007.4451365.

Van Der Pal, M. (2013). IPv6 preparation and deployment in datacenter infrastructure - A practical approach. *Journal of Telecommunications and Information Technology*, *2013*(1), 20–24.

Venable, J., Pries-heje, J., & Baskerville, R. (2012). A comprehensive framework for evaluation in design science research. *7th International Conference, DESRIST 2012, Las Vegas, NV, USA, May 14-15, 2012. Proceedings*, *7286*(2012), 423–438. https://doi.org/10.1007 978:3:642:29863:9:31.

Yagoub, G., Yosif, A., Babiker, A., Mustafa, A. N., & Hamied, M. A. (2014). Evaluation and comparisons of migration techniques from IPv4 To IPv6 using GNS3 Simulator. *Journal of Engineering, 04*(08), 51–57.

Yousafzai, M. M., Othman, N. O. R. E., & Hassan, R. (2015). Toward IPv4 to IPv6 migration within a campus network. *Journal of Theoretical and Applied Information Technology*, *77*(2), 209–217.

Young, R., & Jordan, E. (2008). Top management support: mantra or necessity? *International Journal of Project Management*, *26*(7), 713–725. https://doi.org/10.1016/j.ijproman.2008.06.001.

Zakari, A., Musa, M., Bekaroo, G., Bala, S. A., Hashem, I. A. T., & Hakak, S. (2019). IPv4 and IPv6 protocols: A comparative performance study. *ICSGRC 2019 - 2019 IEEE 10th Control and System Graduate Research Colloquium, Proceeding*, (August), 1–4. https://doi.org/10.1109/ICSGRC.2019.8837050.

APPENDICES

Appendix A: Semi-Structured Interview Outline

Source: Adopted with modification and addition from (Kaur, 2015)

1. Describe your role, experiences, and current responsibilities?
2. What is the company's current status towards IPv6 initiatives in IPv6 migration?
3. How large is your current infrastructure and how it looks like? (number of computer/network equipment/servers)
4. How about the equipment in the organization? Which equipment needs to replace or update?
5. What motivation will drive an organization to migrate from the current protocol to IPv6 protocol?
6. What is the company's status about the planning process to use IPv6 services?
7. Which factors affect deploying IPv6 and which one do you think needs to be prepared for the implementation?
8. Describe the organization's decision-making process behind adopting IPv6? What were the factors influencing the decision to adopt IPv6?
9. In your opinion, how will IPv6 affect the organization (operation/ IT support/etc)? Anything unexpected occurs? Why did it happen?
10. What barriers, if any, has the organization should encounter during IPv6 adoption planning/ implementation?
11. Do you think the organization facing cost constraints for IPv6 implementation? How?
12. What do you think is/will be the biggest cost of the organization's IPv6 adoption project: hardware, software, or human resources? Do you think IPv6 based network infrastructures are more cost-effective than IPv4?
13. Has the organization found it difficult to recruit staff with the knowledge and experience to implement IPv6? How?
14. Have you attended IPv6 training or education events with other organizations? How has that helped you in understanding IPv6 adoption?

15. Has training on IPv6 technology, security, and deployment on different infrastructure types of equipment have been provided? If that is so, to what extent?
16. Has an IPv6 strategy and IT security police been developed and updated to incorporate IPv6 requirements?
17. Do you think IPv6 would significantly increase data communication security in the organization? If that is so, to what extent?
18. In your opinion, which approach has the organization will use when adopting IPv6 (e.g. dual-stack)? How do you think will IPv6 be spread to the entire organization?
19. Do you have any recommendations, documentation that I can look at or comment on to accelerate IPv6 adoption in an organization?

Appendix B: Checklist for Document Analysis

1. Type of document: describes what type of document and content of the document. Is it configuration file, network design, policies, the procedure provided, and other for BIB?
2. The objective of the document: What is the purpose of the document and to whom it intended to guide?
3. Description of the document: When the document is written? Who drafts the document?

Appendix C: Checklist for Observation

1. Respondents working environment where infrastructure is implemented.
2. Visiting BIB's data center, disaster recovery sites, branches, and head office infrastructure.
3. Looking for the physical design of the network types of equipment.

Appendix D: Quality in Use Evaluation Model

Source: Adopted from ISO/IEC 25010:2011 'Quality in use model'.

Evaluation Criteria	Performance value				
	1	2	3	4	5
9. Effectiveness					
How do you rate the framework in terms of accuracy and completeness with which users achieve the IPv6 migration process?					
10. Efficiency					
How do you evaluate the framework in terms expended with the accuracy and completeness with which users achieve the IPv6 migration process					
11. Satisfaction					
How do you rate the framework in terms of the degree to which user needs are satisfied when a framework is used in BIB context of the use					
12. Usefulness					
How do you rate the degree to which a user is satisfied with their perceived achievement of pragmatic goals, including the results of use and the consequences of use					
13. Trust					
How do you rate the degree to which a user or other stockholders has confidence that a framework will behave as intended					
14. Freedom from risk					

How do you rate the degree to which a framework mitigates the potential risk to economic status, human life, health, or the environment?					
15. Context coverage					
How do you rate the degree to which a framework can be used with effectiveness, efficiency, freedom from risk, and satisfaction in both specified contexts of use					
16. Flexibility					
How do you rate the degree to which a framework can be used with effectiveness, efficiency, freedom from risk, and satisfaction in contexts beyond those initially specified in the requirements					

Appendix E: Configuration Files for Lab Experiment

== CW1 Configuration ==

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Core_Switch1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
ipv6 unicast-routing
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
vlan internal allocation policy ascending
!
interface FastEthernet0/0
 no ip address
 speed 100
 full-duplex
!
interface FastEthernet0/1
 no ip address
 shutdown
 speed 100
 full-duplex
!
interface FastEthernet1/0
 no switchport
 ip address 10.1.4.1 255.255.255.252
 ipv6 address 2000:0:0:2::1/64
 ipv6 ospf 6 area 0
!
interface FastEthernet1/1
 no switchport
 ip address 10.1.7.1 255.255.255.252
 ipv6 address 2000:0:0:5::1/64
 ipv6 ospf 6 area 0
!
interface FastEthernet1/2
```

```
 no switchport
 ip address 10.1.1.2 255.255.255.252
 ipv6 address 2000::2/64
 ipv6 ospf 6 area 0
!
interface FastEthernet1/3
 no switchport
 no ip address
!
interface FastEthernet1/4
 no switchport
 no ip address
!
interface FastEthernet1/5
!
interface FastEthernet1/6
!
interface FastEthernet1/7
!
interface FastEthernet1/8
!
interface FastEthernet1/9
!
interface FastEthernet1/10
!
interface FastEthernet1/11
!
interface FastEthernet1/12
!
interface FastEthernet1/13
!
interface FastEthernet1/14
!
interface FastEthernet1/15
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
!
router ospf 4
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.4.0 0.0.0.3 area 0
 network 10.1.7.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
```

```
!
ipv6 router ospf 6
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
End
```

== ER Configuration ==

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Branch_ER
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
interface Tunnel0
 no ip address
 ipv6 address 2000:14::2/64
 tunnel source 172.28.2.2
 tunnel destination 172.28.1.2
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Serial1/0
 ip address 172.28.2.2 255.255.255.252
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
```

```
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/4
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/5
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/6
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/7
 no ip address
 shutdown
 serial restart-delay 0
!
interface GigabitEthernet2/0
 no ip address
 negotiation auto
 ipv6 address 2000:0:0:9::/64
 ipv6 address 2000:0:0:9::1/64
!
ip forward-protocol nd
ip route 172.28.1.0 255.255.255.252
172.28.2.1
!
no ip http server
no ip http secure-server
!
ipv6 route ::/0 2000:14::1
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
End
```

== FW Configuration ==

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname DataCenter_FW
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
ipv6 cef
!
interface Tunnel0
 no ip address
 ipv6 address 2000:14::1/64
 ipv6 traffic-filter Branch_Access in
 ipv6 traffic-filter Branch_Tunnel out
 tunnel source 172.28.1.2
 tunnel destination 172.28.2.2
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 10.1.1.1 255.255.255.252
 negotiation auto
 ipv6 address 2000::1/64
 ipv6 ospf 6 area 0
!
interface GigabitEthernet2/0
 ip address 10.1.2.1 255.255.255.252
 negotiation auto
 ipv6 address 2000:0:0:1::1/64
 ipv6 ospf 6 area 0
!
interface Serial3/0
 ip address 172.28.1.2 255.255.255.252
 serial restart-delay 0
!
interface Serial3/1
 no ip address
```

```
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/4
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/5
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/6
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/7
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 4
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.2.0 0.0.0.0 area 0
 network 10.1.2.0 0.0.0.3 area 0
 default-information originate
!
ip forward-protocol nd
ip route 172.28.2.0 255.255.255.252
172.28.1.1
!
no ip http server
no ip http secure-server
!
ipv6 route ::/0 Serial3/0
ipv6 route ::/0 2000:14::2
ipv6 router ospf 6
 log-adjacency-changes
 default-information originate
!
ipv6 access-list Branch_Access
```

```
 permit ipv6 2000:0:0:9::/64 host
2000:0:0:10::2
 sequence 30 permit ipv6 2000:0:0:9::/64
2000::/64
 permit ipv6 2000:0:0:9::/64 2000:0:0:1::/64
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
End
```

Appendix F: University's Supportive Latter

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

Addis Ababa University
College of Natural Science
School of Information Science

Date: March 12, 2020
Ref No. SIS/65/2020/2012

To:- Bunna International Bank S.C
Addis Ababa

Subject:- Student Abiy Habtam

Dear Sir /Madam,

Student Abiy Habtam (ID.No GSE/4369/10) is graduate student at the School of Information System, Addis Ababa University. He is currently conducting a MSc. Thesis research under the title "IPV4 to IPV6 Migration Framework: The case of Bunna Interationa Bank".

I would like to thank you in advanced for all the assistance that you would provide to the student.

With Regards

Tibebe Beshah (PhD)
Head, School of Information Science

✉: 1176 Email: information_cci_cns@aau.edu.et ☎: +251-(11)-122-91-91