



LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

TRANSITION FROM IPv4 TO IPv6

Best Transition Method for Large Enterprise Networks

LAHTI UNIVERSITY OF APPLIED
SCIENCES

Degree Programme in Business

Information Technology

Thesis

Spring 2012

Nguyen, Phu Minh Nguyen

Nguyen, Quynh Anh

Lahti University of Applied Sciences

Degree Programme in Business Information Technology

NGUYEN, PHU MINH NGUYEN: Transition from Ipv4 to Ipv6
NGUYEN, QUYNH ANH: Best Method for Large Enterprise
Networks

Bachelor's Thesis of Degree Programme in Business Information Technology, 97
pages, 25 pages of appendices

Spring 2012

ABSTRACT

On 8 June, 2011, over 1000 top websites in the world took part in an event called "World IPv6 Day". As IPv4 are running out, the need for changing to IP next generation, IPv6 is obvious. This study aims at finding the best method of transition from IPv4 to IPv6 for large enterprise networks.

This study analyzed experiences of several large enterprises that had deployed IPv6. Key factors on the success and failure of IPv6 deployment were synthesized from findings from those enterprises.

This research utilizes qualitative approach and inductive reasoning along with design science approach. Seven guidelines of design science method are followed strictly for better end results. Open-ended interviews will be data collection methods of the study. Documents, such as articles, books, and websites also provide lots of information. Content analysis helps the authors to look directly into context of documents to find the core meaning. The content of this study was examined on two scales: technical side and managerial side.

Findings upon data collected reveal several significant factors which affect IPv6 implementation project. Hence, a solution, the most applicable transition method was concluded. This method was then tested on a virtual environment simulating a large network model. It was proven to be working.

Keywords: internet protocol, IP, IPv4, transition, transition method, IPv6, large enterprise, network, IPv6 readiness

*This thesis is dedicated to my beloved family, **Nguyễn Phú Thọ, Nguyễn Thị Tùng,** and **Nguyễn Phú Quỳnh Như,** who gave birth to me at the first place, raised me up and always give me care and love to the fullest. I would not be where I am now without their endless love, huge encouragement and unconditional support. Last but not least, I would like to thank my girlfriend, **Đỗ Thị Minh Châu,** for her loving care and wholehearted support, as well as patience while I am doing my thesis.*

Nguyen Phu Minh Nguyen

To my beloved parents, family and friends, who are always beside me.

Nguyen Quynh Anh

ACKNOWLEDGEMENTS

*We would like to express our appreciation to all those who gave us the possibility to complete this Bachelors degree thesis. First and foremost we are deeply indebted to our supervisor, **Professor Torsti Rantapuska**, who has supported us throughout our thesis with his patience and knowledge whilst allowing us the room to work in our own way. Furthermore, we would like to offer our sincerest gratitude to **Professor Keith O' hiobhaird**, whose guidance and constructive feedback helped us to improve the linguistic and academic quality of our thesis. In addition, our sincere thanks go to all of our friends and participants in the interviews for their supportive advice and helpful information.*

Finally, we would like to thank Lahti University of Applied Sciences, where we acquired all the professional knowledge and academic support for our thesis.

Nguyen Phu Minh Nguyen & Nguyen Quynh Anh

TABLE OF CONTENTS

1	INTRODUCTION	1
2	RESEARCH METHOD	4
2.1	Question and Objectives	4
2.2	Research approach and Strategy: Design Science	5
2.2.1	Guideline 1: Design as an Artifact	6
2.2.2	Guideline 2: Problem Relevance	7
2.2.3	Guideline 3: Design Evaluation	7
2.2.4	Guideline 4: Research Contributions	8
2.2.5	Guideline 5: Research Rigor	9
2.2.6	Guideline 6: Design as a Search Process	9
2.2.7	Guideline 7: Communication of Research	9
2.3	Research Method	10
2.4	Scope and Limitation	11
2.5	Validity and Reliability	11
3	DATA FRAMEWORK	12
3.1	Data Collection	12
3.2	Data Analysis	13
4	INTERNET PROTOCOL	15
4.1	Overview	15
4.1.1	OSI Model	16
4.1.2	Network Address Translation	20
4.2	Features of IPv4	22
4.3	Features of IPv6	31
4.3.1	Introduction to IPv6	31
4.3.2	IPv6 New Features	33
4.4	IPv4 and IPv6 Comparison	38
5	BUSINESS NETWORK ANALYSIS	43
5.1	Research Data	43
5.1.1	Interviews Data	43
5.1.2	Documents Data	45
5.2	Network Infrastructure	46
5.3	Management Issues	51

5.3.1	Motivations	52
5.3.2	Hesitations	54
6	EVALUATION OF CURRENT TRANSITION METHODS	56
6.1	Method 1 - Dual Stack IPv4/IPv6 Devices	57
6.2	Method 2 – Translation	60
6.3	Method 3 – Tunneling	65
6.4	Conclusion	71
7	RECOMMENDATION OF IPV6 TRANSITION FOR ENTERPRISES	73
7.1.1	Business Side	74
7.1.2	Technical Side	76
7.1.3	Stages of Readiness	78
8	IPV6 IMPLEMENTATION	82
8.1	Introduction	82
8.2	Enterprise Network Design	82
8.3	Addressing Plan	88
8.4	Implementation Performance	90
8.4.1	Dynamic Host Configuration Protocol (DHCP)	90
8.4.2	Open Shortest Path First (OSPF)	91
8.4.3	Border Gateway Protocol (BGP)	91
8.4.4	Virtual Private Network (VPN)	91
8.4.5	Security Establishment	92
9	CONCLUSIONS	93
9.1	Overview	93
9.2	Research result	94
9.3	Recommendations	95
9.4	Methodology	96
9.5	Limitation and Further Study	97
	REFERENCES	98
	APPENDICES	107

LIST OF ABBREVIATIONS

ALG	Application Level Gateway
ARP	Address Resolution Protocol
ASA	Adaptive Security Appliance
BGP	Border Gateway Protocol
CEO	Chief Executive Officer
CIO	Chief Information Officer
CPT	Cisco Packet Tracer
CPU	Central Processing Unit
CTO	Chief Technology Officer
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DSTM	Dual Stack Transition Mechanism
FTP	File Transfer Protocol
IANA	Internet Assigned Number Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IOS	Internetwork Operating System
IP	Internet Protocol

IPng	IP-The next Generation
IPsec	IP security
IPv4	IP version 4
IPv6	IP version 6
IS	Information System
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
ICMPv6	Internet Control Message Protocol for IPv6
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
OSI	Open Systems Interconnection
OSPF	Open Shortest Path
PC	Personal ComputerFirst
PIX	Private Internet eXchange
POP3	Post Office Protocol version 3
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service

RFCs	Request For Comments
RIRs	Regional Internet Registries
SIIT	Stateless IP/ICMP Translator
SME	Small to medium-sized enterprise
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
STD	Standard
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web

LIST OF FIGURES

FIGURE 1. Organizational design and information systems design activities (Hevner, et al. 2004).....	5
FIGURE 2. Data analysis.....	13
FIGURE 3. Network address translation (Cisco, Cisco IOS Network address translation 2004).....	20
FIGURE 4. Static NAT (Tyson 2001)	21
FIGURE 5. Dynamic NAT (Tyson 2001).....	22
FIGURE 6. Overloading NAT (Tyson 2001).....	22
FIGURE 7. Subnetting (Lowe 2005)	28
FIGURE 8. Subnet mask (Lowe 2005).....	29
FIGURE 9. IPv4 free pool allocation (ARIN 2010)	30
FIGURE 10. IPv6 neighbor discovery protocol	37
FIGURE 11. Virtual Local Area Network (VLAN).....	47
FIGURE 12. Network Address Translation (Odom, Healy and Donohue 2009)..	48
FIGURE 13. Virtual Private Network.....	50
FIGURE 14. Different transition technologies (Subramanian 2003).....	56
FIGURE 15. The structure of Dual stack model (Oracle Corporation 2001).....	59
FIGURE 16. IPv4 – IPv6 dual stack operation (Cisco, The ABCs of IP version 6 2010).....	60
FIGURE 17. Translation method model (Microsoft, Technet 2012).....	60
FIGURE 18. SIIT Model (Vienna University of Technology 2012)	62
FIGURE 19. Deployment of IPv6 using NAT-PT (Cisco, The ABCs of IP version 6 2010)	63
FIGURE 20. Bump in the Stack model (TechWeb 2009)	64
FIGURE 21. Tunneling transition method (H3C 2003)	65
FIGURE 22. 6over 4 model (Microsoft 2011)	66
FIGURE 23. DSTM model (Wedel 2008).....	67
FIGURE 24. 6to4 Automatic Tunneling model	68
FIGURE 25. Teredo method (Microsoft 2011).....	69
FIGURE 26. Tunnel Broker model (Netnam Ltd. 2011).....	70
FIGURE 27. Headquarter network structure model.....	84
FIGURE 28. Branch 1 network structure model	85

FIGURE 29. VPN users	86
FIGURE 30. The whole network structure model	87
FIGURE 31. Ping from client computer to database server	112
FIGURE 32. Ping from DHCP server to client laptop	113
FIGURE 33. Ping from client computer to database server with Ipv6.....	116
FIGURE 34. Ping from client computer to database server with IPv6	117
FIGURE 35. DHCPv4 Configuration	118
FIGURE 36. Ping from PC on ISP3's router to Web server in Headquarter	124
FIGURE 37. Ping from VPN laptop to Database server in headquarter.....	126
FIGURE 38. Show IPSec.....	128
FIGURE 39. Ping from PC of ISP3's router to Mail server using IPv4	129
FIGURE 40. Ping from PC of ISP2's router to Database server using IPv6.....	129
FIGURE 41. Pre-configured model.....	130
FIGURE 42. Configured model.....	131

LIST OF TABLES

TABLE 1. Seven layers of OSI model (adapted from Balchunas 2007; OSI n.d.)	18
TABLE 2. Internet protocols in the range of OSI model layers (Ford, et al. 1999)	19
TABLE 3. IPv4 header (Ford, et al. 1999)	23
TABLE 4. IPv4 format	25
TABLE 5. IPv4 classes (Microsoft 2011; Mitchell n.d.)	26
TABLE 6. IPv6 header	32
TABLE 7. General format of IPv6	34
TABLE 8. Management issues	51
TABLE 9. Dual Stack (Nokia n.d.)	57
TABLE 10. Summary of three methods	71
TABLE 11. Rank description	80

1 INTRODUCTION

Since the birth of Internet in 1960s (Cerf 1993), it has completely change the way of communications forever. With its capabilities, the Internet has already become a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers regardless of geographic location (Leiner, et al. 2009). Nevertheless, there is still no model which valuing companies' Internet efforts correctly, even though the Internet's phenomenal impact on business and its reach across all sectors are uncountable. (Afuah and Tucci 2001). Besides, according to its nature in the structure of Internet, the TCP/IP has also played an important role in the global expansion of communications. As a result, the more users join the Internet, the better it would be to spread knowledge in every field around the world. However, this is also the problem as the IP address is not unlimited and the Internet community is witnessing the exhaust of IPv4 not year by year but day by day, which calls for a proper solution. The first group of Internet users that would be affected is internet service providers (ISPs), large enterprises, companies, etc. The reason is that they hold the most number of IPv4 for operation and management and before the IPv4 runs out, they will need an appropriate act to handle the exhaustion, and otherwise, the collapse of the worldwide Internet is foreseeable (Huston 2008).

This study is conducted to answer the question which is the best method for large enterprise networks to transit from IPv4 to IPv6. Currently, there have been many papers, documents, or reports about IPv4 exhaustion; the invention of IPv6 and the way administrators can apply IPv6 to existing networks, known as transition. However, there are still few or nearly no documents for applying the transition from IPv4 to IPv6 in a large enterprise networks with many different geographic branches around the world. Therefore, with this thesis, we would like to give our suggestion on a solution for a complete implementation of IPv6 into large enterprise network with no influence on its current operation. Furthermore, this thesis does not only focus on the technical aspects but also the management side. It would provide an insight into the importance of IPv6 transition, as well as a careful analysis on its influence to the enterprise network and its operation. For all the information above, this thesis could be used as a source of reference for

network administrators, board of directors, information executives, or students and network researchers who have an interest in the network communication and would like to join the community of IPv6.

Therefore, with the topic “Transition from IPv4 to IPv6: The best method for large enterprise networks”, we will have two main parts: the theoretical and the practical. For the first part, we would propose the research question, our approaches with the qualitative method, and also the data collection. In addition, we would give an introduction about computer network, internet protocol, especially all the main features of IPv4 and IPv6 to indicate the differences between them. And for the second part, we would like to apply the Design-Science method to analyze the current network infrastructure, IPv6 readiness in large enterprises to acknowledge the reasons and willingness for changing to IPv6. Moreover, this method is also be deployed in the IPv6 implementation for its effectiveness and risks.

Firstly, for the theoretical part, in Chapter 1, we would like to express the background and aims, along with the goal and scope of the thesis. Besides, a study is the combination of both theory and practice via change and reflection in a problematic situation within a framework. It is a process consisting of researchers and practitioners working together on a certain cycle of activities, including problem diagnosis, action intervention, and reflective learning (Lee 1999; Davis and Olson 1985). Therefore, Chapter 2 and 3 would handle mainly the research methods and data framework consisting of research questions and objectives, research approach and strategy, scope and limitation, validity and reliability, data collection and analysis. Chapter 4 also contains information about the Internet Protocol, known as IP. In this part, we would provide an insight into the network model with layers, the structure and features of both IPv4 and IPv6, and the difference between the old and new address format.

Secondly, for the empirical part, in Chapter 5, we would perform a business network analysis to understand the current network infrastructure in large enterprises. Chapter 6 grabs a thorough view on the IPv6 readiness and suggestion for the current infrastructure to be ready for the IPv6 implementation. Then Chapter 7 would contain the evaluation of current transition methods, which

becomes the base for choosing the right and suitable IPv6 implementation. The Chapter 8 is the place where we perform the practical implementation into real networks and test our methods for large enterprise networks with the network model as required from the design science method. As we all have known information systems and the organizations they support are complex, artificial, and purposefully designed. They are composed of people, structures, technologies, and work systems. Design science, as the other side of the IS research cycle, creates and evaluates IT artifacts intended to solve identified organizational problems. Such artifacts are represented in a structured form that may vary from software, formal logic and rigorous mathematics to informal natural language descriptions (Lee 1999; Davis and Olson 1985). Those artifacts are broadly defined as constructs, models, methods, and instantiations to meet with the business strategy, information technology strategy, organizational infrastructure and information system infrastructure. Finally, the conclusion in chapter 9 would include an overview of the thesis, innovations and limitations of the methods, as well as the result analysis from the implementation.

2 RESEARCH METHOD

This chapter provides the research question and research methodology of our study. Research approach will be presented in detail so that readers will comprehend our research model.

2.1 Question and Objectives

The most important and also initial step of a thesis is to define the research question. Based on the nature of that question, proper methods will be applied to find the expected answers. The research question of this thesis is: “*Transition from IPv4 to IPv6: What is the best method for large enterprise networks?*”

These following actions are taken to find the answers:

- Conducting a thorough literature review
- Interviewing some specific large companies which have deployed IPv6
- Analyzing their experiences and attitudes towards IPv6 deployment
- Analyzing and comparing some transition methods to find the best one
- Building a network model and testing the method
- Concluding the result (inductive)

The results from above actions are main objectives of this thesis, which include:

- Acquiring thorough understanding about IP as well as definitions, ideas, and arguments IPv6 transition methods.
- Getting better understanding of IPv6 deployment in real life project and experiences from companies who had deployed IPv6.
- Proposing the best method for transitions from IPv6 to IPv4 for large enterprise networks.

The type of this study’s research question is “solution” which means to find a way to solve a problem. Therefore, the purpose of this paper is to define and test the most applicable method for large enterprise network to transit their current IPv4 network to IPv6.

2.2 Research approach and Strategy: Design Science

Design science, as the other side of the IS research cycle, creates and evaluates IT artifacts intended to solve identified organizational problems. Such artifacts are represented in a structured form that may vary from software, formal logic and rigorous mathematics to informal natural language descriptions (Lee 1999; Davis and Olson 1985). Those artifacts are broadly defined as constructs, models, methods, and instantiations to meet with the business strategy, information technology strategy, organizational infrastructure and information system infrastructure.

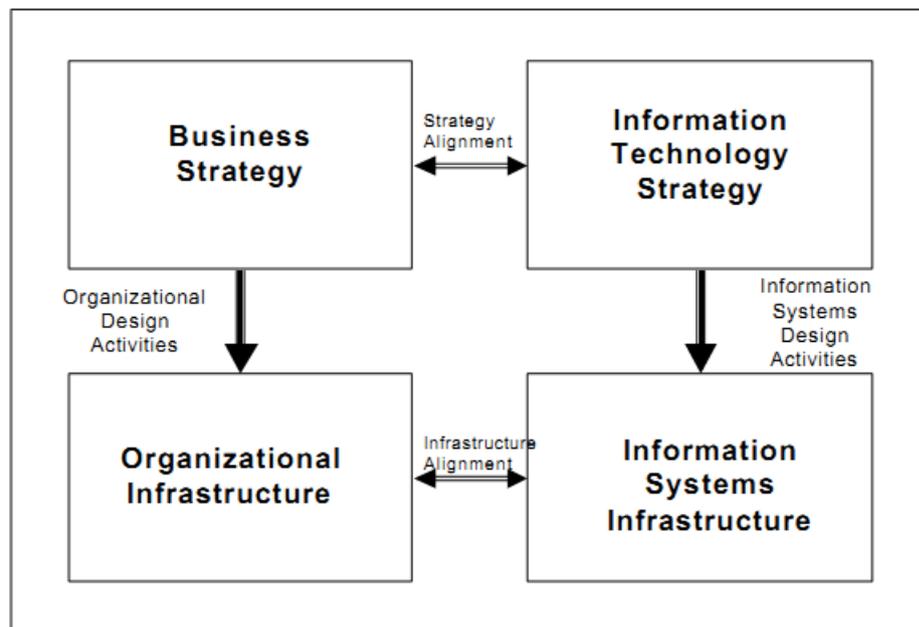


FIGURE 1. Organizational design and information systems design activities (Hevner, et al. 2004)

Therefore, the reason for using design science method is that it is a problem solving process. The fundamental principle of design-science research combines seven guidelines whose knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact. That is, design-science research requires the creation of an innovative, purposeful artifact

(Guideline 1) for a specified problem domain (Guideline 2). Because the artifact is "purposeful," it must yield utility for the specified problem. Hence, thorough evaluation of the artifact is crucial (Guideline 3). Novelty is similarly crucial since the artifact must be "innovative," solving a heretofore unsolved problem or solving a known problem in a more effective or efficient manner (Guideline 4). In this way, design-science research is differentiated from the practice of design. The artifact itself must be rigorously defined, formally represented, coherent, and internally consistent (Guideline 5). The process by which it is created, and often the artifact itself, incorporates or enables a search process whereby a problem space is constructed and a mechanism posed or enacted to find an effective solution (Guideline 6). Finally, the results of the design-science research must be communicated effectively (Guideline 7) both to a technical audience (researchers who will extend them and practitioners who will implement them) and to a managerial audience (researchers who will study them in context and practitioners who will decide if they should be implemented within their organizations) (Lee 1999; Davis and Olson 1985).

2.2.1 Guideline 1: Design as an Artifact

The result of design-science research in IS is, by definition, a purposeful IT artifact created to address an important organizational problem. It must be described effectively, enabling its implementation and application in an appropriate domain. For this reason, models for the three main methods used in the transition from IPv4 to IPv6 will be created. However, this will not be applied for small and medium companies but we aim for large businesses with over 250 employees along with a large network. This would help defining the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, and use of new implemented Ipv6 information systems. On the other hand, it also demonstrates feasibility both of the design process and of the designed product.

2.2.2 Guideline 2: Problem Relevance

The objective of research in information systems is to acquire knowledge and understanding that enable the development and implementation of technology-based solutions to heretofore unsolved and important business problems. Design science approaches this goal through the construction of innovative artifacts aimed at changing the phenomena that occur (Venkatesh 2000 according to Hevner, et al. 2004).

From our point of view, business organizations are goal-oriented entities existing in an economic and social setting. The design of organizational and inter-organizational information systems plays a major role in enabling effective business processes to achieve these goals. Because organizations spend billions of dollars annually on IT, only too often to conclude that those dollars were wasted (Keil 1995; Keil et al. 1998; Keil and Robey 1999 according to Hevner, et al. 2004). To deal with this matter, a survey will be conducted carefully and strictly with selected enterprises possessing large networks. At first, a questionnaire will be sent to get the results about the current network, IT expenditure, the success and failure of IPv6 deployment, affected factors and so on. These cases will be analyzed thoroughly to opt out the best method for the transition. From the analysis, a design will be simulated according to the specific condition to produce the best result which suits all networks.

2.2.3 Guideline 3: Design Evaluation

The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods (Hevner, et al. 2004). The business environment establishes the requirements upon which the evaluation of the artifact is based. This environment includes the technical infrastructure which itself is incrementally built by the implementation of new IT artifacts. Thus, evaluation includes the integration of the artifact within the technical infrastructure of the business environment. A design artifact is complete and effective when it satisfies the requirements and constraints of the problem it was

meant to solve. To fulfill this requirement, a test will be conducted thoroughly before and after implementation to check all the new features and also the integration with the old network. It would consist of many things such as: network performance, quality of services, compatibility, common services which are WWW, DNS, DHCP, routing, security, mail exchange, VPN, VoIP, etc... These kinds of test are summarized in the following table.

2.2.4 Guideline 4: Research Contributions

Effective design-science research must provide clear contributions in the areas of the design artifact, design construction knowledge (i.e., foundations), and/or design evaluation knowledge (i.e., methodologies). One or more of these contributions must be found in a given research project (Hevner, et al. 2004).

The Design Artifact - The artifact must enable the solution of heretofore unsolved problems. From this thesis, our artifact would be the new design model for the transition from IPv4 to IPv6 to obtain the best results.

Foundations - The creative development of our method of transition IPv4 to IPv6 would extend and improve the existing foundations in the network knowledge base.

However, we would also set the criteria for assessing contribution focus on representational fidelity and implement ability. This new information system themselves is the model of the IPv6 business network. This design must be "implementable". Beyond these, however, the design science research must demonstrate a clear contribution to the business environment, solving an important, previously unsolved problem.

2.2.5 Guideline 5: Research Rigor

Design-science research demands that the research applies rigorous methods. This research's main purpose is finding the best method to transit IPv4 system to IPv6 for large-scale network. Various organizations have defined and tested many methodologies. Our research focus on transition technique that come in one of three forms: *dual stacks*, *tunneling*, and *translation*. These transition mechanisms have been proposed by IEFT (Internet Engineering Task Force). (Daniel G.Waddington 2002, 139). According to the questionnaire conducted in this research on some large organizations network, the testing models will be built based on those transition methodologies stated above. Artifact model is going to be constructed on the basic of those three existing mechanism.

2.2.6 Guideline 6: Design as a Search Process

Design-science is a process searching for the best solutions for realistic problems (Hevner, et al. 2004). Our research identifies three main transition mechanisms from IPv4 to IPv6, which are: *dual stacks*, *tunneling*, and *translation*. The research will focus on the design of best transition method that based on those mechanisms. First, the research is going to find out the business needs and attributes of current network infrastructure and then to design a solution to satisfy the requirements. Cost and benefits of the proposed solutions will be discussed thoroughly.

2.2.7 Guideline 7: Communication of Research

Design-science research should be presented in a way that both technology-oriented audience and management-oriented audience can take advantages of. Our research on transition of IPv4 to IPv6 will present an artifact and technical issues related for building it. Critical factors that have influences on the implementation

will also be stated in our paper. Testing and evaluation process is going to be documented properly for further development purposes.

On the other hand, the research is based on the needs of realistic organizations. Cost and benefits of the solution provided by this paper will be discussed to help the decision-making process. Management-oriented audience can find information on resources needed as well as possibility to apply the artifact on their own context.

2.3 Research Method

Quantitative methods are often used to process random sampling data into numbers and statistics (Lichtman 2006). Quantitative research concerns with testing hypotheses, considers cause and effect, and calculates the size of a phenomenon of interest (Johnson and Christensen 2008). The end-results are usually statistical report including both descriptive and inferential statistics. Descriptive method summarizes and presents data in an informative way while inferential method generalizes about a population based on a sample. As such nature of quantitative method, data collection often includes closed-ended questionnaire, surveys that classify various experiences into categories, recording numerical data through observing events etc... (University of Wisconsin-Eau Claire n.d.)

On the other hand, the purpose of qualitative method is to understand and interpret processes underneath an observed event and evaluate people's perception involved in the event (InSites 2007). It concerns people, objects, words, images not numbers and statistics. In qualitative research, personal feelings and experiences are analyzed. Qualitative research is often used to construct a new theory from the data collected. For that reason, qualitative data collection methods are interviews with open-ended questions, observation, and document review. (University of Wisconsin-Eau Claire n.d.) This paper aims to study the current network conditions of some large enterprises as well as their attitude toward the transition from IPv4 to IPv6. Thus, qualitative research method is applied to this thesis. As observation was unable to be carried out, interviews and document review were done as data collection method in this paper.

2.4 Scope and Limitation

The scope of this thesis mainly discusses the most applicable transition method from IPv6 to IPv4 for enterprises with large network. The presentation of the method includes literature review, advantages, and configurations as well as simplified model of the method. As this thesis aims at large network, large enterprises with big network traffic may find it more useful than small and medium sized network. There are some transition procedures which may not be suitable for small and medium sized networks due to their complexity. Therefore, this thesis is most applicable and limited to large network.

2.5 Validity and Reliability

Presently, there are various definitions of validity and reliability in qualitative research method from perspectives of many different researchers. In this thesis, the understanding of validity and reliability will be considered and measured by the idea of trustworthiness according to Mishler (2000). Lincoln & Guba (1985) explained it as being able to establish confidence in the findings. Moreover, Johnson (1997) stated that reliability and validity can also be understood as “defensible”. (Golafshani 2003). Multiple perspectives from various sources should be compared and tested before the conclusion to strengthen the results and enhance “trustworthiness” (Yin 2011, 20).

This study relies on a variety of sources, which are from technical papers of leading telecommunication companies. Conclusion is drawn in reference to those data.

All the enterprises chosen had carried out IPv6 deployment. Those enterprises chosen are all large network enterprises which falls into class B to class A according to IP classes which means large network. All the interviewees are people who were in charge of or involved in IPv6 deployment in their companies. All data sources are listed in reference and can be verified.

Data collected will be analyzed by proper methods in the right procedures so that the study remains stability, reproducibility and accuracy. It means that data can be analyzed and classified in the same way over a period of time. (Palmquist n.d.)

3 DATA FRAMEWORK

3.1 Data Collection

We all know that multiple sources are more reliable than single reference. They enhance the validity and reliability of the thesis. This thesis research collected data by interviews with several specific organizations and document review. Document review or document analysis is the procedure of examining and evaluating published documents systematically in both printed and electronic form. As well as other qualitative data collection methods, data must be evaluated and explained in order to develop knowledge and evidence, which can support the research. (Corbin and Strauss 2008). In addition, documents forms are varied. They consist of books, newspapers, journal articles, advertisements, agendas, memos of meetings, letters, maps and charts, press releases, program proposals, applications forms, radio and TV transcripts, reports of organization, surveys, etc... (Bowen 2009). The procedure of analyzing includes searching, choosing, interpreting, and synthesizing data. Data taken from the documents can be quotations or extraction are organized and analyzed throughout content of the research. (Labuschagne 2003). This research paper contained extensive technical information which was synthesized from various sources, especially documents from leading networking organizations such as Cisco and Microsoft.

Interview is a commonly used research method. In qualitative research, researchers try to understand not only the fact of the subjects but also the meaning of their experience. The process of interviewing is to find out different point of view, problems, solutions, and attitudes of interviewees within the main theme of the research. (Rubin and Rubin 1995). There are several types of interview such as closed interview, standardized interview, and conversational interview. In this thesis, standardized, opened – ended interviews was conducted with people in charge of IPv6 deployment and network maintenance staffs to find out their different practical experiences on this subject. The questions are made so that answers are open-ended; which means participants can fully express their points of views and experiences (Turner 2010). The same questions were provided to the interviewees to make the process of analyzing and comparing more easily. (Israel,

et al. 2005, 308). Due to graphical difficulties, all the interviews were done via emails and telephone. The questionnaire can be found in the Appendix 1.

Before the interviews were conducted, emails concerning the issues were sent to all the appropriate organizations asking for permissions. Unfortunately, as always happening when conducting a research, not many have answered back or given permissions for the research. The list of organization who agreed to participate in this bachelor study is in Chapter 5.

3.2 Data Analysis

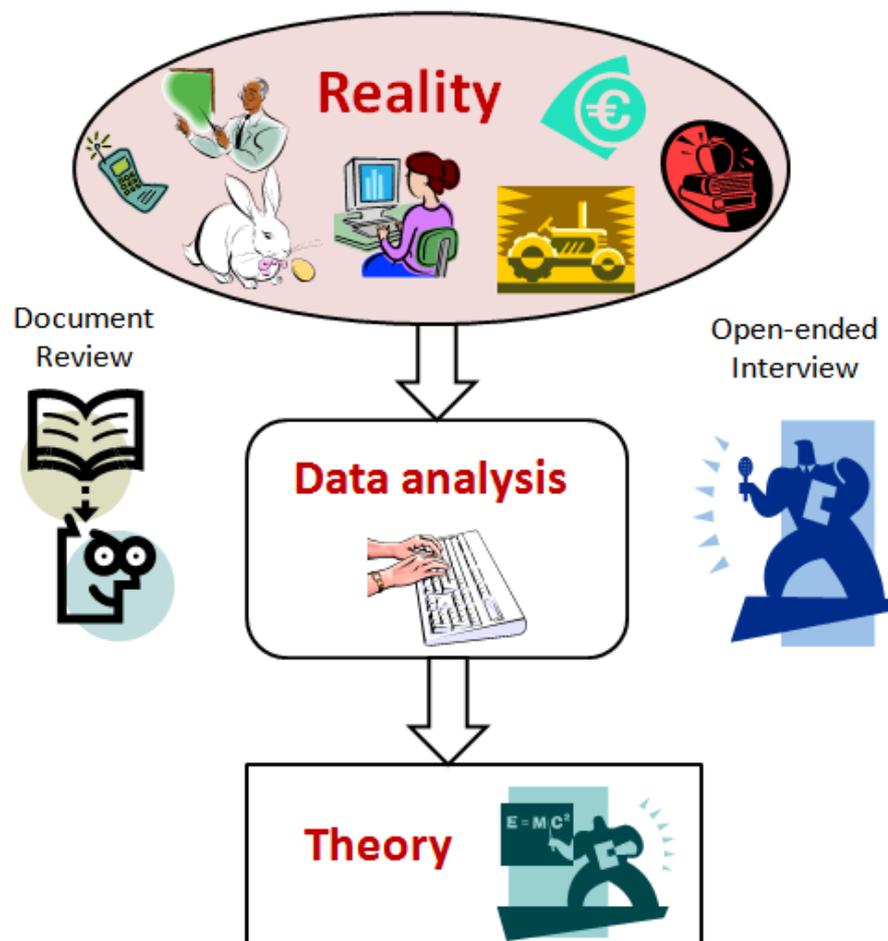


FIGURE 2. Data analysis

The process of analysis in this paper is inductive approach. As we can see from Figure 2 above, data collected from document review and interviews will be processed to draw a theory. Theory is concluded based on the data.

As we compare all the technical aspects of current transitions methods and from real-life experiences of interviewees, the best transition method, which can be applied to large enterprise network, can be found out. The process of transition that is best for enterprises will also be concluded based on the experiences of interview participants.

There are various methods for qualitative data analysis. In this thesis, the method “content analysis” is used. This method classifies themes and ideas taken from data into groups. This method is theory driven, which means that theory decides the subject we look for. There are some rules of content analysis but most important is that categories must be inclusive and mutually exclusive. (Weber 1990). By applying this method, differences, intensions and trends can be detected via looking directly at the texts and transcripts. Uses of content analysis enable behavioral responses of communicators or personal feelings to be described. (Palmquist n.d.).

We will look into the documents and interview transcripts to find out the main subject. Answers to the same question from different interviewees will be compared to search for mutual view, how the ideas related in different situations as well as different points of views. The same process is applied to data from document review. Important phrases or words are highlighted and coded. Therefore, a set of data groups will be formed. This procedure is done several times to avoid leaving vital information out.

4 INTERNET PROTOCOL

4.1 Overview

The first thing to know is the definition of a network. A network is a group of computers linked together via communication devices and transmission media. A computer is *online* when it is connected to a network, or *log on*. On the other hand, it is *offline* or *log off* when it is disconnected. A computer, which is connected to a computer network, is called a *node* (Lowe 2005, 36). The main purpose of connecting different computers together is that they can exchange *resources* i.e. hardware, applications, data, and information. All networks need specialized network hardware and applications to work. Hardware consists of cables, network interface card, network switch, routers, repeater etc. In general, all networks are built from these following parts:

Server computers are computers that share resources such as printers, scanners; disk storage, and network services i.e. Internet access. The servers normally run specialized network operating system and network service software.

Client computers are all the other computers on the network, which are not server. End users use client computers to request and access the resources on the network provided by server

If a computer wants to connect to the network, it needs a *NIC*, a Network Interface Card. This card enables computers to physically connect to the network via cable. It is also referred as Ethernet card or network adapter. This card is attached inside the computers.

Cables do not actually connect computers to each other. In fact, cables connect computers to a *switch*. The switch, in turn, connects the rest of network together. Switches can be connected together to make a larger network.

Finally, to make a network actually work, *network software* is required. For clients as well as servers, specialized software is installed in order to share the resources on the network. (Lowe 2005).

Presently, the world's largest computer network is the Internet.

“The Internet is a worldwide collection of networks that connects million of business, government, agencies, educational institutions, and individuals.” (Gary B.Shelly, 2012, pp. 10-12)

Each computer on the Internet must have a unique address, which marks it as different to other computers on the Internet. This special address is called IP, which stands for Internet Protocol. Network protocol administrates all communication activities. It defines order and format of messages transmitted among network devices along with the actions upon those transmissions. (Jim Kurose 2007). At this time, there are two version of IP address: IPv4 (Internet Protocol version 4) and IPv6 (Internet protocol version 6). A question may come up. What happened to IPv5? Raffi Krikorian from www.oreillynet.com had given us the answer. Back to the end of 1970's, a protocol for experimental transmission of voice, video, and distributed simulation called ST, the Internet Stream Protocol was made. It was implemented at places like IBM, Apple, and Sun. That protocol can be given the name version 5. Therefore, the next generation of IP is now IPv6. (Krikorian 2003). Nowadays, IPv4 addresses are so common that the term IP is understood as IPv4. Details features of IPv4 and IPv6 will be discussed later in this chapter.

4.1.1 OSI Model

Today, all of the networks are built based on the frame of Open Systems Interconnection (OSI) model. OSI was issued in 1984 by the International Organization for Standardization (ISO). It is a standard for international communication that explains seven abstract layers of networking framework for protocol. The OSI model describes the way messages should be transmitted between any two points in the network. The main purpose of this model is to make it easy to communicate between different hardware and software system

with different underlying architectures. Network protocols allow entities in a host to communicate with equivalent entities at the same layer in another host. Each layer interacts directly only to the layer under it and provides facilities just for the layer above it. (Ford, et al. 1999). The figure below explains seven layers of the OSI model.

TABLE 1. Seven layers of OSI model (adapted from Balchunas 2007; OSI n.d.)

APPLICATION 7	<ul style="list-style-type: none"> This layer provides the interface between the network and user applications. User interact directly to this layer. This layer does not include computer application software but contain web-browsers, email clients, FTP clients.
PRESENTATION 6	<ul style="list-style-type: none"> This layer controls the format of data being transmitted. It makes sure that data will be understood by other sending and receiving device as well as other layers. This layer also control the encryption and compression of data.
SESSION 5	<ul style="list-style-type: none"> This layer sets up, manages and terminates the communication session between computers.
TRANSPORT 4	<ul style="list-style-type: none"> This layer controls data segmentation, data flow and provides error checking recovery of data before and after transmission.
NETWORK 3	<ul style="list-style-type: none"> This layer concerns with the processes logical addressing and routing data across the network hierarchy.
DATA 2	<ul style="list-style-type: none"> This layer explains the logical way that data being transmitted reliably. It deals with the data framing and encapsulation.
PHYSICAL 1	<ul style="list-style-type: none"> This layer defines the physical network equipment transferring data across the network i.e. cables, wires, network cards etc.

Network protocols spread the entire OSI model. Table 2 shows some network protocols equivalent to each OSI layer.

TABLE 2. Internet protocols in the range of OSI model layers (Ford, et al. 1999)

OSI Reference Model	Internet Protocol Suite	
Application	FTP, Telnet, SMTP, SNMP	NFS
Presentation		XDR
Session		RPC
Transport	TCP, UDP	
Network	Routing Protocols	IP
Link	ARP, RARP	
Physical	Not Specified	

The IP is at layer 3 of OSI model, which is the Network layer. It contains addressing information and other information which allows data packets to be routed.

4.1.2 Network Address Translation

Network Address Translation, as known as NAT, is a technique that operates on the router to connect two networks together. NAT makes the router function as an agent between the private (or “inside”) and the public, the Internet (or “outside”) (Cisco, Cisco IOS Network address translation 2004). It means that a globally unique IP address can represent a whole group of computers (Tyson 2001).

Let’s imagine NAT as a receptionist in an office. An officer may instruct the receptionist not to forward all the messages sent to him but only from people he requests. Now, when someone calls the main number to the office, which is the only official number, the receptionist will check to make sure that officer is expecting the call from this person. Only then she will forward the caller to the officer. (Tyson 2001).

Similarly, the NAT device uses a single unique IP address to represent the inside network to the Internet. Inside the network, each computer can have any IP address. When a packet of data is sent, the NAT translate the private IP to public IP. It keeps track of the sending packets so that it knows who is expecting for the reply from which source then match up the right incoming packet to the right host. (Tyson 2001). Figure 3 below demonstrates above explanation.

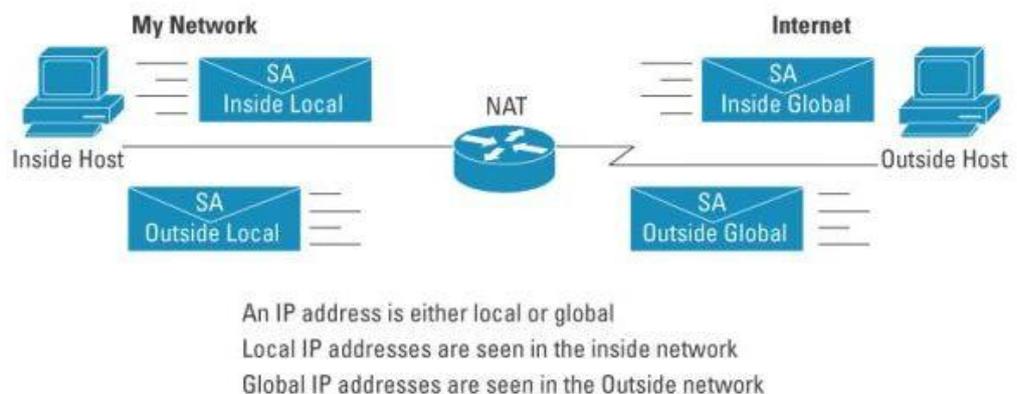


FIGURE 3. Network address translation (Cisco, Cisco IOS Network address translation 2004).

NAT works in several ways as described below.

Static NAT

As can be seen from Figure 4, in static NAT, the host with the IP address of 192.168.32.15 will always be translated to 213.18.123.112. In static NAT, an unregistered private IP address will be mapped to a registered public IP address on one-to-one scale. This technique comes in handy when outside network need to access a device.

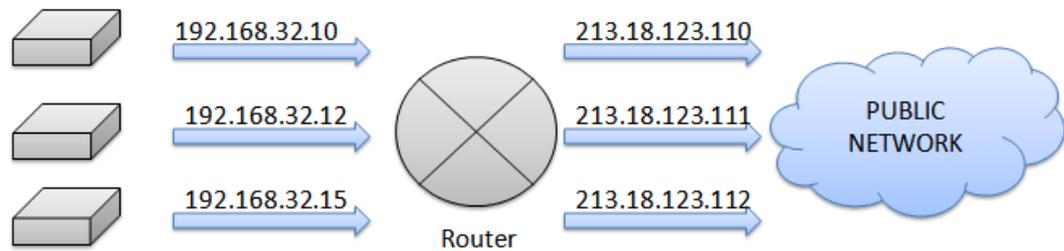


FIGURE 4. Static NAT (Tyson 2001)

Dynamic NAT

Figure 5 demonstrates that the host with the IP address 192.168.32.10 will be translated to the first available IP address in the range. In dynamic NAT, a private IP address will be assigned to an available registered public IP address from a range of registered addresses.

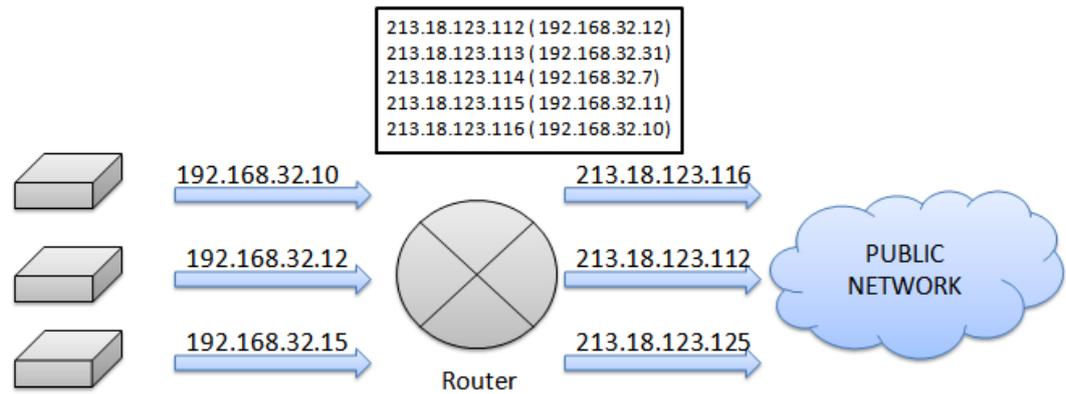


FIGURE 5. Dynamic NAT (Tyson 2001)

Overloading

In Figure 6, each host in the private network is translated to the same public IP address which is 213.18.123.100 but assigned to different ports. Overloading is a form of dynamic NAT which maps several private IP addresses to a same public IP address by assigning different port numbers. (Tyson 2001).

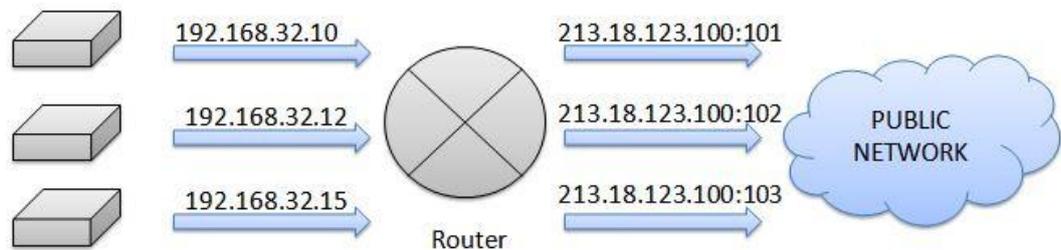


FIGURE 6. Overloading NAT (Tyson 2001)

4.2 Features of IPv4

IP is a standard protocol with STD number 5 that is documented in RFC 791 of IETF (Internet Engineering Task Force). Its main function is to deliver data packets between network devices. IP provides an unreliable, connectionless and

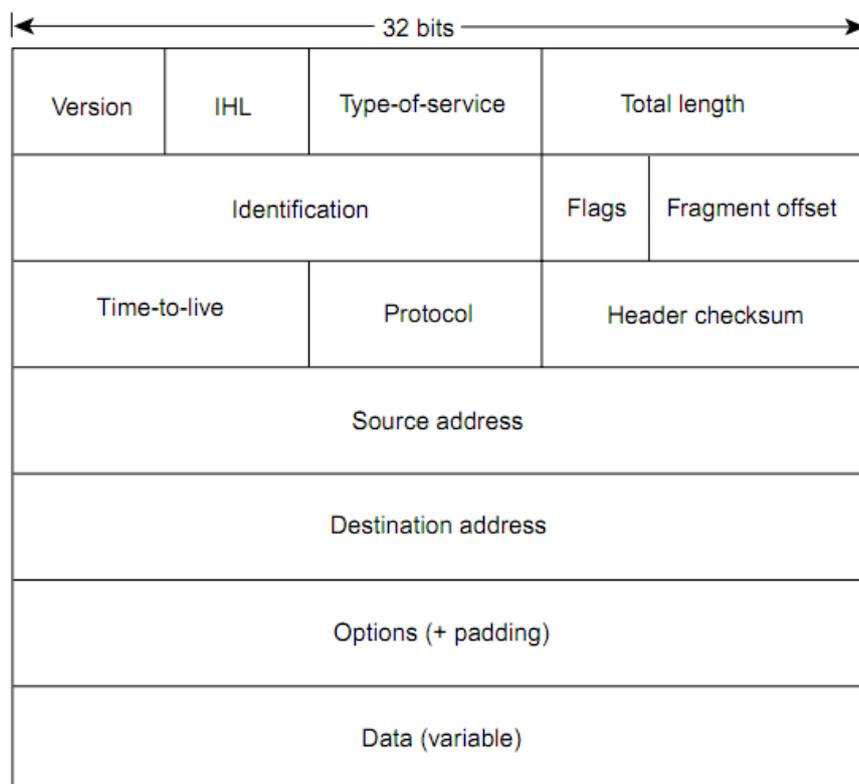
best-effort delivery of packet or also called datagrams through Internet. In addition, IP also provides fragmentation and reassembly of packets into original message. (Ford, et al. 1999)

An unreliable connectionless communication is a data transmission method in packet switching network, which transmit data packet in on direction without checking the existence or availability of the destination. In this method, each data packet has a header, which carries sufficient information to deliver the packet to its destination (Microsoft 2011).

Best-effort means that the data delivered can be repeated, lost, corrupted or broken. Data is not guaranteed to be delivered (Microsoft 2011).

IPv4 packet header format

TABLE 3. IPv4 header (Ford, et al. 1999)



Each field of the header is explained as following.

Version points out the IP version in use. The value of this field is 4 as the name IPv4.

IHL (IP Header Length) is the length of the header in 32 bits word and points to the beginning of the data. The minimum value of the header is 5.

Type of service indicates how the upper-layer protocol will treat and handle the data packet with different levels of priorities.

Total Length is the length of the entire packet including header and data. It is measured in octets/

Identification is a value that identifies the current packet which helps in assembling the fragment of the packet.

Flags field has 3 bits that allow the router to fragment packet or not.

Fragment Offset contains 13 bits indicates which packet a fragment belongs to.

Time-to-Live prevents the packet from looping forever. It shows the maximum allowed time that the packet stays in the internet.

Protocol specifies which next layer protocol will be used after the IP processing is done.

Header Checksum is on the header only. Some of the header's fields may change, therefore this is computed each time the header is processed.

Source Address marks the sender.

Destination Address indicates the receiver.

Options support some other options i.e. security.

Data includes information of next layer.

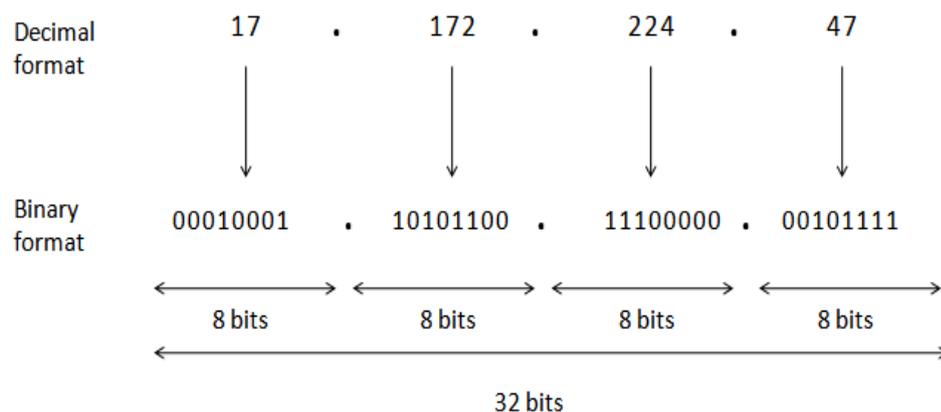
(Ford, et al. 1999; RFC791).

IP addressing

The process of routing data packets within the Internet requires the IP addressing scheme to let any two hosts to exchange information to each other. The IP address is a unique number assigned to each host on Internet. It is represented by a 32-bit binary value divided into four groups of eight bits (Ford, et al. 1999). This IP address number consists of two main parts: The *network number* and the *host number*. The *network number* identifies which network the host computer is located. The *host number* identifies a specific host computer on that network. (Ford, et al. 1999).

A typical IPv4 address is separated by dots and expressed in decimal format, which is known as *dotted decimal number* or *dotted decimal notation*. (Gary B.Shelly 2012, 110). In this format, each group of eight bits is called an *octet*, which will be represented by a corresponding decimal value. Each octet value ranges from 0 through 255. Table 4 below illustrates the basic format of an IPv4 address.

TABLE 4. IPv4 format



An IPv4 address such as 17.172.224.47 has its binary format as 00010001.10101100.11100000.00101111. It is not easy to remember such an

address; therefore, it is then assigned a unique name, which is resolved through the Domain Name System (DNS). The address above will be translated into `www.apple.com`, which users will type into an address bar to access the website.

Classifying IP address

IPv4 addresses are categorized into five classes for use of different network size: A, B, C, D and E. Classes A to C are used commercially while class D is used for *multicasting* and class E is for experimental purpose. Which part of the address is the *network number* decides the class. (Gary B. Shelly 2012). To determine which class an address belongs to, the first octet is used as in the following table.

TABLE 5. IPv4 classes (Microsoft 2011; Mitchell n.d.)

Class	Format	Starting bits	Address Range	No. Bits of Network /Host	Number of Networks	Number of Hosts	Purpose
A	N.H.H.H	0	0.0.0.0 to 127.255.255.255	7/24	126	16,777,214 ($2^{24}-2$)	Large organizations
B	N.N.H.H	10	128.0.0.0 to 191.255.255.255	14/16	16,384	65,543 ($2^{16}-2$)	Medium organizations
C	N.N.N.H	110	192.0.0.0 to 223.255.255.255	22/8	2,097,152	245 (2^8-2)	Small organizations
D	N/A	1110	224.0.0.0 to 239.255.255.255	N/A	N/A	N/A	Multicast groups (RFC 1112)
E	N/A	11110	240.0.0.0 to 255.255.255.255	N/A	N/A	N/A	Experimental

N = Network number, H = Host number

The number of hosts is minus by 2 in each range because IETF reserved some certain addresses for broadcasting, maintenance, and hosts etc (RFC5735).

Class A is normally used for large organizations with a big number of hosts while Class C is suitable for small networks. Small-medium sized enterprises networks must use Class B. The gap between Class C and Class B is rather larger. Many enterprises have more than 245 hosts but far less than 65,543 hosts. Moreover, the

number of SMEs is increasing rapidly and there are not enough IP addresses to provide them. The solution to this problem was solved through IP *subnetting*, which allows the administrator to divide the network into subnets (or sub networks).

Subnetting

Subnetting is a technique used to divide an IP network into several smaller subordinate networks that can be called *subnets*. A *subnet* is a subordinate network of a bigger Class A, B, or C network and under control of local administrators. The outside network views the entire big network as a single IP without knowing the detail of internal network structure. This technique helps network administrators to create a much more flexible and efficient network with more traffic capacity. Why it is said that subnetting provides extra flexibility for the network administrators? We already know that for typical IPv4 classes, there are merely three options for a network number length: 8 bits, 16 bits and 24 bits corresponding for Class A, B and C. That leaves three choice of the host number: 254, more than 65 thousand and 16 millions. As mentioned before, SMEs that fall into scale between 254 and 65 thousand find it difficult to have a right network without wasting or have a shortage of IP addresses. Subnetting allows a portion of host number of Class A, B or C to be used as sub network number, which makes it much more efficient use of IP addresses. On the other hand, for performance reason, subnetting is use to divided broadcast domain into smaller than even Class C so that not one single domain must carry all the network traffic. (Lowe 2005, 364). Figure 7 demonstrates an example of subnetting.

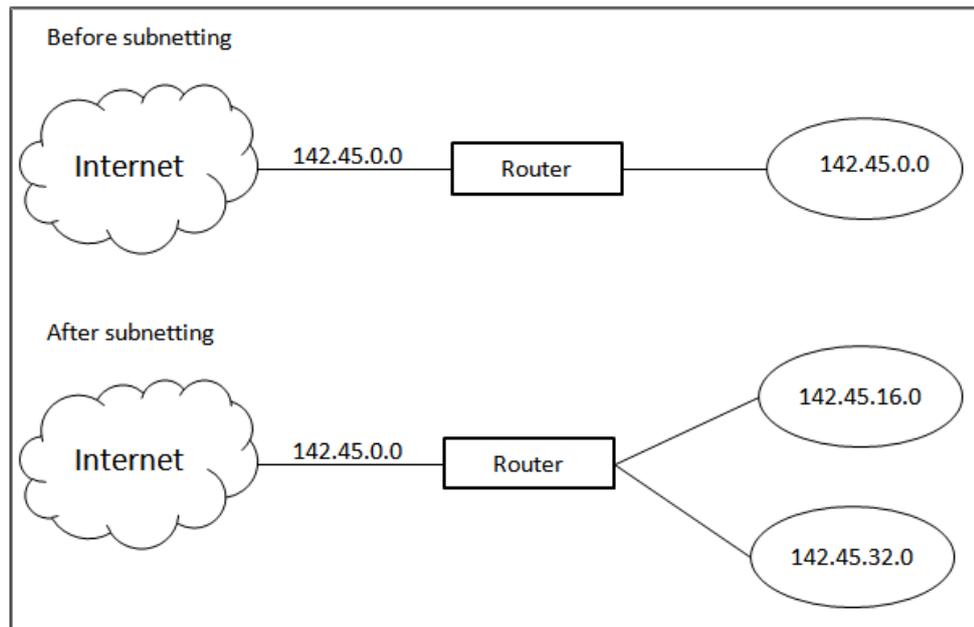


FIGURE 7. Subnetting (Lowe 2005)

The network is assigned the IP address 142.45.0.0 and a single broadcast domain will carry all the traffic of this network. After subnetting, the first part of network number was used to divide the network into 2 smaller ones, subnet 16 and subnet 32. The outside world still views the whole as a single 142.45.0.0. It considers a host at 142.45.32.46 belongs to 142.45.0.0. When a datagram is sent to that host, the router will determine which subnet it belongs to by check the subnet part of host number.

For “borrowing” from the host number, subnets can have any length of network number instead of standard 8 bits, 16 bits or 24 bits. For the router to know which part of host number was used for network number of subnets, a *subnet mask* is needed. Subnet mask is a 32-bits number that looks like an IP address but actually it has a completely different technical meaning. All the 1 in the binary format indicate the bits for network number, and all the 0 indicate the bits of the IP address that act as host number. (Lowe 2005, 364)

Figure 7 above has a 16-bit network with 4-bit subnet in addition will have a subnet mask like this:

11111111 . 11111111 . 11110000 . 00000000

This makes the actual network number of subnet 20 and host number 12 bits. The router will perform the AND operation to decide the network ID of an IP address as figure 8.

	142	.	45	.	32	.	46
IP address :	10001110		00101101		00100000		00101110
Subnet mask :	11111111		11111111		11110000		00000000
Network ID :	10001110		00101101		00100000		00000000
	142	.	45	.	32	.	0

FIGURE 8. Subnet mask (Lowe 2005)

Accordingly, the packet, which is sent to 142.45.32.46, will be routed to subnet 142.45.32.0

The subnet mask also normally represented in dotted decimal format.

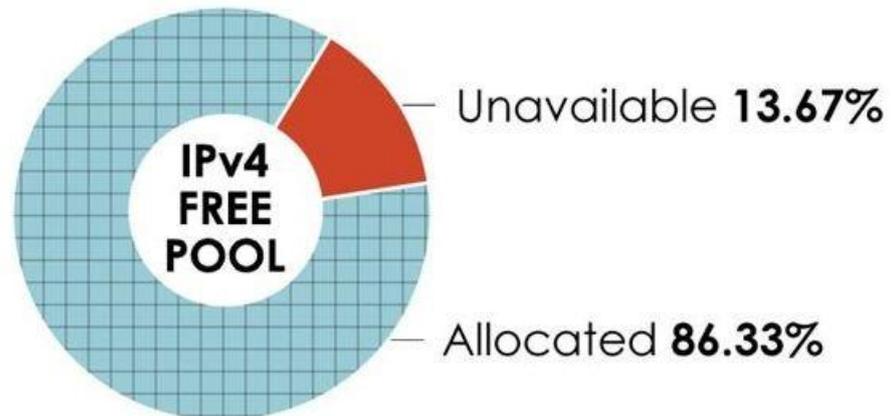
11111111 . 11111111 . 11110000 . 00000000
 255 . 255 . 240 . 0

(Lowe 2005; Ford, et al. 1999).

IPv4 space utilization

IP addresses are 32-bit binary numbers. Each number can be 0 or 1. Thus, the total possible number of IP addresses can be 2^{32} , which equals 4,294,967,296 unique values. Nevertheless, the actual usable value is about 3 billion as some of the addresses are reserved for special purposes. (Gary B. Shelly, 2012, p. 110)

IPv4 addresses are managed through the Internet Assigned Number Authority (IANA) who distributes large address block for five Regional Internet Registries (RIRs) according to geographical territories. Until recent, the pool of free IPv4 is now nearly running out.



* as of 3 February 2011

FIGURE 9. IPv4 free pool allocation (ARIN 2010)

Figure 9 indicates that by the time of 3rd February 2011, IANA assigned each RIR its last block of /8 IPv4 addresses. It means that the free pool of IPv4 actually has reached 0%. As the wheel must go on, Ip next Generation, which is Ipv6 is the solution to the future of the Internet. The address size is increased from 32-bit number to 128-bit number and represented in hexadecimal notation. The number of address jumps to $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$. IPv6 deployment has begun. (ARIN 2010).

4.3 Features of IPv6

In this sub chapter, the main features of IPv6 will be presented.

4.3.1 Introduction to IPv6

As from above, IPv4 has demonstrated its features to be useful both in the implementation and operation. Furthermore, it plays an important part in every network, from a local area network to the worldwide Internet. Nevertheless, everything has two sides and IPv4 is not an exception. With the growth of population and the development of technology, the demand for IPv4 addresses becomes higher and higher day by day while the resource is running out. Although private addresses have been long used to compensate for this problem, it is just a temporary solution as the levitation of Internet-connected devices makes sure that the public IPv4 addresses will soon be exhausted. Furthermore, the rise of Internet and its users requires devices which play as backbone routers to manage and support a great amount of routing tables consisting of over 70,000 routes across the world (Davies, 2002).

However, every problem has in it the seeds of its own solution. In response to these matters, a new concept has been developed which is known as IPng (IP-The Next Generation) or IPv6 (Internet Protocol version 6) along with its protocols and support. Similar to IPv4, IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. With many of its additional features, the IPv6 is supposed to eventually replace the old IPv4 in every network without limitations (Deering & Hinden, 1998). The main differences between IPv4 and IPv6 range from new addressing space to built-in security. The following sections discuss each of these new features in detail.

Streamlined header format

TABLE 6. IPv6 header

Version	Traffic class	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			

Version - 4-bit Internet Protocol version number = 6.

Traffic Class - 8-bit traffic class field.

Flow Label - 20-bit flow label.

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

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

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

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

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

The new form of IPv6 header aims to reduce header overhead by relocating unimportant fields and option fields to extension headers which are positioned right after the IPv6 header. As a result, this enables the simplified IPv6 header to be processed more efficiently at intermediate routers. However, the IPv6 protocol is incompatible with the IPv4 protocol. Therefore, a network connected device (host or router) needs to apply an implementation of both IPv4 and IPv6 in order to identify and process two kinds of header formats (Hagen, 2006).

4.3.2 IPv6 New Features

Expanded address space

As we have mentioned above, the main reason for the invention of IPv6 is the shortage of IPv4 resources. Despite its usefulness and flexibility, IPv4 combines of 32 bits, which can only create a total of 2^{32} (4,294,967,296) addresses. Meanwhile, with new technologies, IPv6 contains 128 bits, and as calculated above, the new address space supports a number of 2^{128} (340,282,366,920,938,000,000,000,000,000,000,000,000,000) addresses, which is 2^{96} times larger than IPv4 address resources. From those calculations, there has been a saying that “With IPv6, nearly every object in the world can obtain an address for its own”. As a result, this expanded address range of IPv6 can be variously applied from the Internet backbone (interconnected networks, core routers) to individual subnets (hosts, end devices) within an organization. Furthermore, it also makes address-conservation techniques, such as NATs, become unnecessary, which gained widespread deployment as an effort to alleviate IPv4 address exhaustion (Microsoft, 2005).

Effective and organized infrastructure for addressing and routing

Along with the expanded address space comes the hierarchical address format. This is also a new and important aspect of IPv6. Unlike IPv4 hierarchical address

consists of network, subnet, and host components, IPv6, supported with 128-bit addresses, provides globally unique and organized addressing known as prefixes (address classes in IPv4).

TABLE 7. General format of IPv6

Global routing prefix	Subnet ID	Interface ID
n bits	m bits	128-(n+m) bits

Global routing prefix: a value (typically hierarchically structured) assigned to a site

Subnet ID: an identifier of a link within the site

Interface ID: a unique identifier for a network device on a given link (usually automatically assigned).

Within the IPv6 contains a range of global addresses, whose purpose is to form an effective, organized, and downsized infrastructure for routing that discusses the conventional development of multiple levels from Internet service providers. Appropriately, backbone routers contain routing tables which are much smaller in the IPv6 Internet. (IBM, 2008)

Advanced address configuration

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

Stateful address configuration: a host receives IPv6 address along with optional configuration specifications from a server named DHCPv6 via a UDP link.

However, in the circumstance that DHCPv6 server does not exist on that link, there will be some special nodes acting as relay agents to help transmit these

request packets from the host to other DHCPv6 servers in the nearby link or forward to the next relay agent.

Stateless address configuration: with this mechanism, manual configuration of the hosts or additional servers is no longer needed. In addition, it helps to minimize the configuration of routers. It also gives way for a host to form its own addresses, known as link-local addresses, by utilizing local and advertised information from routers. This means hosts on the same link can automatically create themselves link-local addresses and communicate with each other with manual configuration or in the absence of a router (Cisco, 2010).

Built-in security

Since the birth of Internet up to today, security has always been an important issue when there are an increasing number of hackers, equipped with networking knowledge, trying to prove themselves. The Internet once was a network without intermediary gateways or routers or security (an end-to-end network). After that, as the network develops, there raises a question “How to ensure the safety of private data when transmitting on a public network?”. Under the circumstances, gateways, firewalls, and local network isolation have become available all over the world as a reply to this question. Despite these efforts, data privacy and security continues to be a prominent issue and no complete solution has been found. However, in conjunction with the invention of IPv6, whose main purpose is to overcome the IP address depletion, the most propitious answer for the data protection has been found, known as built-in security (IPSec) (RFC 1825 - Security Architecture for the Internet Protocol).

IPSec is a framework of open standards setting network security policies for transmitting packets in a network. It is developed to function in the layers between the physical layers and the application layer. This ensures all data encapsulated in the packet to travel safely among stations such as routers. Therefore, in IPv6 structure contains a protocol suite requirement to support for IPSec, increase network security and contribute to interoperability among various IPv6 deployments. However, the IPSec in IPv6 is located in the extension headers,

which makes the use of IPSec is optional. Consequently, security may be improved thanks to the built-in security in IPv6 protocol, the total protection still lies in the hands of human beings (Arora & Desai, 2008).

Better support for Quality of Service

Quality of Service (QoS) is an old term commonly used in modern networks. In IPv4 networks, it is known as "best level of effort" service. However, it has a weakness that IPv4-implemented networks are unable to tell the difference if data that are time-sensitive (streaming video or audio) or not (file transfer). In case a packet is lost when transmitting, the TCP identifies the loss and it will send a request for retransmission. However, this will also create an inevitable delay. As a result, when the video is streaming, a gap will occur such as there is neither sound nor picture. (Armitage 2000).

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

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

- Level 7 - Control traffic (routing, network management)

However, although this method minimizes fragmentation and latency, it consumes more bandwidth for prompt arrival, which results in inefficient utilization (Oracle, 2010).

Neighbor Discovery Protocol

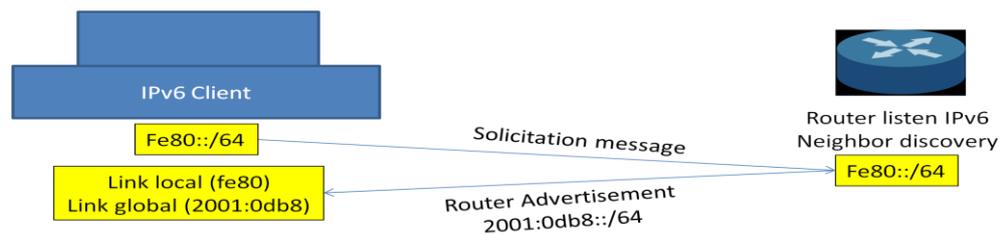


FIGURE 10. IPv6 neighbor discovery protocol

Since the invention of IPv6 also comes the new Neighbor Discovery protocol, which manipulates messaging as the technique to manage the interaction of neighbor nodes on the same link, which is called Internet Control Message Protocol for IPv6 (ICMPv6). The list of major activities that the Neighbor Discovery protocol controls over the IPv6 local link includes router discovery for supporting hosts to find routers on the local link, address auto configuration for assigning automatically IPv6 addresses for interfaces, prefix discovery for discovering the known subnet prefixes to differentiate destinations, address resolution for determining the link-local address of a neighbor with only the destinations' IP address, next-hop determination for applying an algorithm to identify the IP address of a packet recipient one hop that is beyond the local link, neighbor unreachability detection for identifying if a neighbor is no longer reachable, duplicate address detection for determining if an address that the node wants to use is not already in use, and redirection for supporting routers to inform a host of a better first-hop node to use to reach a particular destination (RFC4861).

As from those functions above, the Neighbor Discovery protocol for IPv6 is performing the functions of Address Resolution Protocol (ARP), ICMPv4 Router

Discovery, and ICMPv4 Redirect messages and contributing additional functionality (Narten, 1999). Neighbor Discovery uses the following ICMP message types for communication among nodes on a link:

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

Extensibility

In IPv6, new features can be extended by adding extension headers after the IPv6 header. Different from the IPv4 header, which leaves only 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet (RFC4861).

4.4 IPv4 and IPv6 Comparison

Description	IPv4	IPv6
Address	<p>32 bits long (4 bytes).</p> <p>Consist of a network and a host portion, based on address class.</p> <p>Different address classes are constructed: A, B, C, D, or E depending on initial few bits.</p> <p>The total number of IPv4 addresses is 4 294 967 296.</p> <p>The configuration of IPv4 is</p>	<p>128 bits long (16 bytes).</p> <p>Basic architecture is 64 bits for the network number and 64 bits for the host number.</p> <p>The host portion of an IPv6 address (or part of it) will be derived from a MAC address or other interface identifier.</p> <p>The total number of IPv6</p>

Description	IPv4	IPv6
	<p>nnn.nnn.nnn.nnn, where $0 \leq nnn \leq 255$, and each n is a decimal digit.</p> <p>For example: 192.168.1.1</p>	<p>addresses is 3,40282E+38</p> <p>The configuration of IPv6 is xxxx:xxxx:xxxx:xxxx:xxxx:x xxx:xxxx:xxxx, where each x is a hexadecimal digit, representing 4 bits.</p> <p>For example: fe80:0:0:0:200:f8ff:fe21:67cf</p>
Address mask	Used to assign network from host portion.	Not used
Address Resolution Protocol	Used by IPv4 to find a physical address (MAC or link address), associated with an IPv4 address.	No ARP as IPv6 contains these functions within itself for stateless auto-configuration and neighbor discovery using ICMPv6.
Address types	Unicast Multicast Broadcast	Unicast Multicast Anycast
Configuration	IP addresses and routes must be established while configuring a new system to communicate with other systems.	IPv6 interfaces are self-configuring using IPv6 stateless auto-configuration to communicate with other IPv6 systems that are local and remote.
Domain Name	Applications receive host names (www.google.fi) and use DNS to	Same for IPv6. Support for IPv6 exists using AAAA

Description	IPv4	IPv6
System (DNS)	<p>get IP address (173.194.32.18).</p> <p>Applications also receive IP addresses and use DNS to get host names.</p> <p>For IPv4, the domain for reverse lookups is in-addr.arpa.</p>	<p>(quad A) record type and reverse lookup (IP-to-name).</p> <p>Applications may elect to accept IPv6 addresses from DNS (or not) and then use IPv6 to communicate (or not).</p> <p>For IPv6, the domain used for reverse lookups is ip6.arpa or ip6.int (if not found)</p>
Dynamic Host Configuration Protocol (DHCP)	Used to dynamically obtain an IP address and other configuration information.	DHCP does not support IPv6.
File Transfer Protocol (FTP)	Used to send and receive files across networks.	Does not support IPv6.
Internet Control Message Protocol (ICMP)	Used to communicate network information.	The same for IPv6 (ICMPv6) with some new attributes to support neighbor discovery and related functions.
IP header	Variable length of 20-60 bytes, based on IP options present.	<p>Fixed length of 40 bytes</p> <p>No IP header options.</p> <p>Simpler than the IPv4 header.</p>

Description	IPv4	IPv6
IP header options	Many options that might associate with an IP header (before any transport header).	No options but support some extension headers: hop-by-hop, routing, fragment, and destination.
LAN connection	Used by an IP interface to get to the physical network. Many types exist; for example, token ring, and Ethernet. Sometimes referred to as the physical interface, link, or line.	IPv6 can be used with any Ethernet adapters and is also supported over virtual Ethernet between logical partitions.
Maximum Transmission Unit (MTU)	The maximum number of bytes that a particular link type (Ethernet or modem) supports.	Use a MTU of 1280 bytes. The layers need to fragment and defragment the packets to send over a link with less than 1280 MTU.
Network Address Translation (NAT)	Basic firewall functions in TCP/IP.	IPv6 does not require NAT as the expanded address space of IPv6 eradicates the address shortage problem.
Packet filtering	Basic firewall functions in TCP/IP	Does not support IPv6.
Packet forwarding	TCP/IP can be built to forward IPv4 packets when they are transmitting on different networks.	IPv6 packets are not forwarded.
Ports	TCP and UDP have separate port spaces in the range from 1	The same as IPv4. However, as these are in a new address

Description	IPv4	IPv6
	to 65535.	family, there are now four separate port spaces.
Private and public addresses	<p>All IPv4 addresses are public, except for three address ranges:</p> <p>In class A - 10.*.*.* (10/8)</p> <p>In class B - 172.16.0.0 to 172.31.255.255 (172.16/12)</p> <p>In class C - 192.168.*.* (192.168/16).</p> <p>Private addresses are used within organizations and cannot be routed across the Internet.</p>	<p>IPv6 addresses are either public or temporary. However, temporary addresses, which are used to shield the identity of a client when it commences communication (for privacy), can be globally routed.</p> <p>Temporary addresses have a limited lifetime and generally identical to public addresses.</p>
Route	<p>A mapping of a set of IP addresses to a physical interface and a next-hop IP address to forward IP packets using the line. IPv4 routes are associated with an IPv4 interface.</p>	<p>The same as IPv4 but IPv6 routes are associated to a physical interface as because source address selection functions differently for IPv6 than for IPv4.</p>
Virtual private network (VPN)	<p>Used to extend a secure and private network over an existing public network.</p>	<p>Does not support IPv6. (IBM 2008)</p>

5 BUSINESS NETWORK ANALYSIS

5.1 Research Data

This section provides data collected in this thesis.

5.1.1 Interviews Data

The questions of our interviews can be found in Appendix 1. Here are some key responses from interviewees who agreed to participate.

Seppo Syrjanen, Data network specialist from IT Center of University of Helsinki.

“We have 18,000 computers (Windows, Linux, Mac), 50,000 users, 2000 servers. The main purpose for IPv6 deployment project is testing and preparing for future. There are no problems with IPv6 yet. IPv6 is only used on some test networks and AD Domain controllers. The method of transition was routing. The transition of IPv6 is a long gradual process that will take time and efforts. IPv6 of our system is not ready at the moment; it will be a couple of year until www.helsinki.fi can have an IPv6 address. There is no external budget for IPv6; it will be done in part of basic operations.”

Aleksi Suhonen, Internetworking Consulting – Axu TM Oy

“Our business is involved in a lot of online transaction. The budget for IP expenditure of our company is 4000 EUR/year. The reasons for deploying IPv6 are ease of server numbering, future proofing, and gathering user experiences for consulting purposes. We expected that IP expenditure would drop once we finally get rid of IPv4. We applied Dual-Stack and now testing NAT64 on a few IPv6-only devices. It was tough to get native IPv6 transit at first. User education must be prepared before the implementation”

Anna Niemi, Traffic Specialist, Vertaa.fi Oy

“Although we have some deployment of IPv6, unfortunately our network issues are handled by a company in the Netherlands, ASP4ALL. We have no intention to deploy IPv6 on our own or at the moment.”

Nguyen Dac Thuan, Networking Manager of FPT Telecom Corporation.

“We have more than 5000 users and our business is involved in lots of online transactions. The main reason for deploying IPv6 was testing. We applied Dual-Stack as transition method because we purchased devices that can run both IPv4 and IPv6 from Cisco. The main problem was to configure software designed for our system. Other problem was training our staffs about IPv6. Our IPv6 project got a lot of support from top executives. We will be very happy to have a complete solution to IPv6 deployment.”

Nguyen Ho Phi Long, Cisco Certified System Instructor at Nhatnghe Network Training Center

“Currently, there are around 600 desktops and laptops in the center with 100 servers, which are all contributed for education. This means we do many online business and training. The IPv6 is mainly deployed to cope with the standard requirements from Cisco Training Program. It was very hard at the beginning but now everything is running smoothly. As we are a training center, we use all possible transition methods for educating people. When we complete IPv6 deployment, we think there will be some advantages. The main problem was the high cost of IPv6 devices and the knowledge of our staffs about IPv6. Fortunately, we get much support from our superiors with a budget of 6000Eur per

year. We are also looking for a solution to deploy IPv6 to the rest of our network.”

5.1.2 Documents Data

Requests For Comments (RFCs) is a document system invented by Steve Crocker in 1969 to keep the record as well as improve technology being used on the ARPAnet. An RFC describes a research or applications on networking technology or define a new one.

RFCs can be written by anyone who wishes to provide ideas or a new way to enhance the network. After an RFC is submitted via RFC Editor-page or emails, it will be evaluated by a group of engineers, which is the Internet Engineering Task Force (IETF). Engineers and developers of IETF will check then assign a number to each RFC. Thus, the number is also a unique name for each RFC. For instance, the first RFC is called RFC 1, and RFC 1 always refers to the first RFC about host software invented in 1969. Some of RFCs are published as Internet Standards (STD). Once published, an RFC can never be modified. A modification will be published as a new RFC with new number. (Blank 2004).

TCP/IP was developed by the RFC method of development. In this thesis, we consulted RFCs as our data on technical issues. RFCs are the most updated and trustable papers on networking technology. A set of RFC, which will be used in this thesis, is stated in Appendix 2 with citations provided by IETF at RFC Index Page (<http://www.ietf.org/download/rfc-index.txt>)

Besides RFCs, a set of journal papers on networking technology is also used as technical data in this study.

- IPv4/IPv6 Translation Technology

Nakajima, Masaki, and Nobumasu Kobayashi. "IPv4/IPv6 Translation Technology." *FUJITSU sci. Tech. J.*, 2004: 159-169.

- Transitioning from IPv4 to IPv6 - A Technical Overview

Mackay, Michael, and Christopher Edwards. "Transitioning from IPv4 to IPv6 - A Technical Overview." Lancaster: Computing Department, Faculty of Applied Sciences, Lancaster University.

- Cisco – LISP White Paper Series - Enterprise IPv6 Transition Strategy Using the Locator/ID Separation Protocol

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/ps10800/white_paper_c11-629044.pdf

- The development of IPv6 in an IPv4 world as transition strategies

Subramanian, Saisree. *IPv6 Transition strategies*. November 2003

5.2 Network Infrastructure

Developed technologies have created more new functions for the enterprise networks but they also bring as many risks as well. Therefore, large enterprises are enhancing computer networks and also adopting new technologies to support a single network infrastructure which has the ability to provide all the required services such as higher security, maximum data transmission, scalability, routing protocols and so on. In addition, this must be achieved with the lowest cost and efforts to connect business partners, suppliers and employees scattered across regions. As the requirement for these applications are escalating, it has become standards for implementing an enterprise communication network to ensure the provided solutions for real time operation, data transfer speed, and reliability. Based on the interview with Mr. Seppo Syrjanen, Data network specialist of IT center, the University of Helsinki is currently in possession of 18000 computers and 2000 servers with 50000 users located in different areas. As a result, this network has the needs to meet and support various kinds of request from clients continuously all day and night. Therefore, it requires a stable, scalable and reliable network backbone infrastructure to manage online operations effectively, which normally consists of the following components:

Virtual Local Area Network

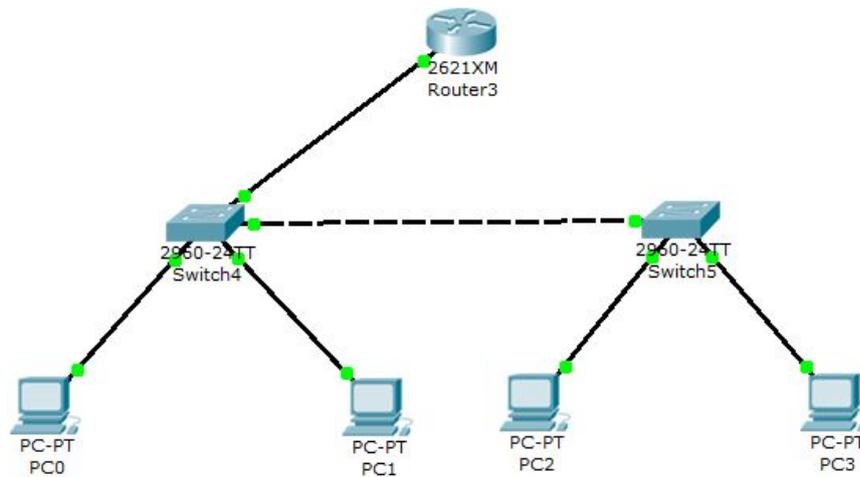


FIGURE 11. Virtual Local Area Network (VLAN)

The figure above indicates a model of a VLAN. A large enterprise often is comprised of many small and medium companies and departments. However, if each company uses a different network, the communication among departments is not assured. Therefore, instead of running a different network, each company is assigned to a unique Virtual Local Area Network (VLAN) and subnet within the single physical network. Normally, it is a function of routers to create broadcast domains but with VLAN, a switch can also create the broadcast domain as well. Furthermore, according to Mr. Nguyen Ho Phi Long, Network Instructor at Nhatnghe Training Center, VLAN is suitable for large networks with a lot of broadcast traffic, especially, when the LAN already has more than 200 devices or more security is required or users run the same application such as VoIP phones. This helps to ensure the highest level of security and confidentiality for enterprise communications.

Network Address Translation (NAT)

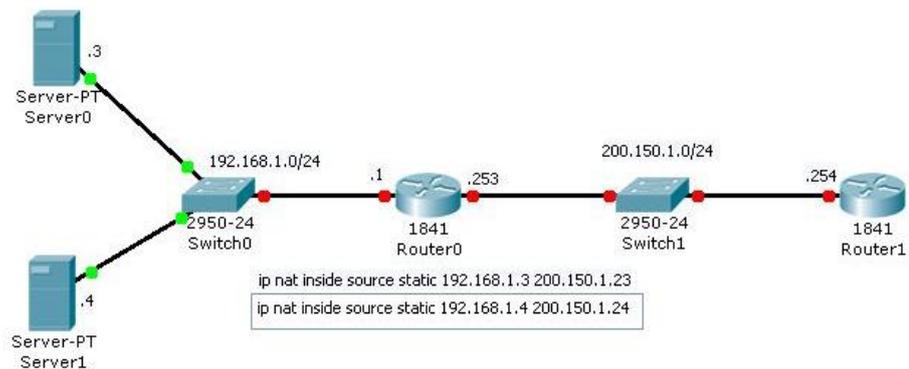


FIGURE 12. Network Address Translation (Odom, Healy and Donohue 2009).

In an enterprise computer network, it is ordinary to conceal an entire IP address space, comprising of private IP addresses, behind a single IP address or a small group of IP addresses in another public address space, which is known as Network Address Translation (NAT). This is the process which aims to alter information in IP packet headers when being transmitted through a router. Most computer systems set NAT to work in order to enable multiple hosts on private networks to access the Internet using a single public IP address. However, NAT is also known to create enormous disadvantages for the Internet connectivity performance, which demands careful implementation. For an enterprise network, all clients will use private addressing internally and external access is achieved using Network Address Translation (NAT) (RFC3022 2001).

Demilitarized Zone (DMZ)

In large enterprise networks, DMZ acts as an extra layer of security for local area networks (LANs). In other words, it is a secure zone between the internal networks (trusted) and the external networks (untrusted). In case the system is attacked, along with firewall, it will protect the whole internal network. For this reason, security methods must be added such as stopping unnecessary services, applying necessary services with minimized privileges, deleting any useless

accounts, and ensuring DMZ to be running with the latest security updates and patches. This is also called a Data Management Zone which provides secure services for internal users by servers such as web server contains and delivers websites of enterprises to customers and suppliers, email server supports SMTP and POP3 or IMAP to maintain and control the email system within the organizations, FTP server supports FTP service to transfer files among hosts within the system, application server contains a software framework providing environment to support the construction of applications, DHCP server assigns IP addresses to client computers, which is often used in enterprise networks to reduce configuration efforts, etc. (RFC2647 1999).

Firewall

According to Mr. Nguyen Ho Phi Long, Network instructor at Nhatnghe training center, nearly in every network nowadays, there is always at least one firewall inside. It can be a system consisting of router, proxy, or gateway to establish security rules for access control between two networks. In that way, the internal network is protected against threats from the outside. A firewall can be either a hardware device or a software program installed on a secure computer. In a large enterprise network, there are two kinds of firewall implementations: distributed firewall and centralized firewall.

Virtual Private Network (VPN)

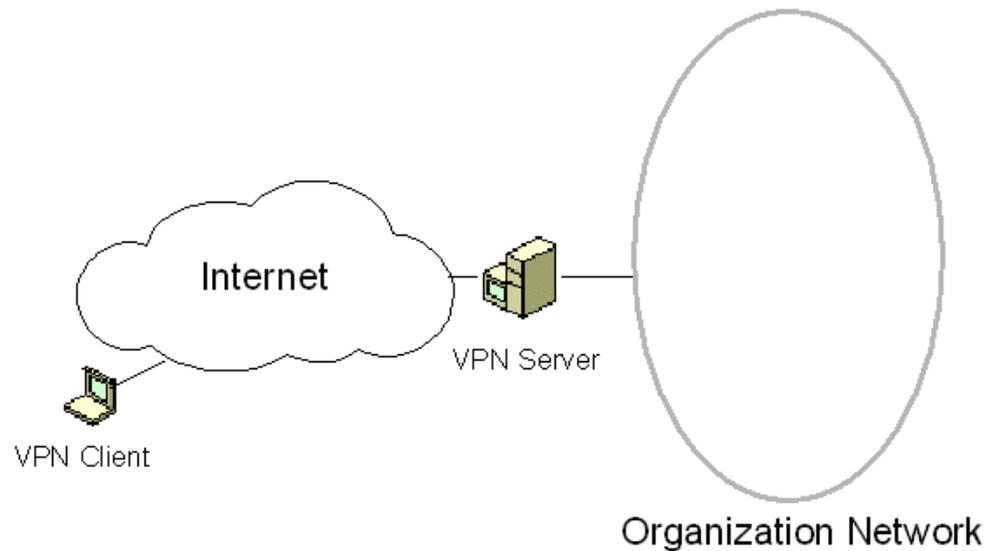


FIGURE 13. Virtual Private Network

Each enterprise has a large number of employees and this will lead to a situation that when they stay far away from the offices, they also need to access company data which can only expose to internal networks. For this reason, many large enterprise networks have arranged to adopt a VPN connection to allow clients access internal machines securely from the public networks. This acts as a private network configured inside a public network (Internet) to easily manage facilities of large networks. Based on the interview with Aleksu Suhonen, Internetworking consultant at Axu TM Oy, VPNs are widely used by enterprises to create wide area networks to provide site-to-site connections to branch offices and to allow mobile users to access their company networks. There are many kinds of VPN that are being used:

- Internet VPNs: Several protocols are used to provide security over the Internet such as SSL, IPsec, L2TP and PPTP.
- Frame Relay VPNs: Carriers offer point-to-point and multipoint VPNs using frame relay. Customer equipment converts packets to frame relay packets.

- Virtual IP VPNs: Carriers offer multipoint networks that accept only IP packets from the customer and run over an IP core. These virtual private routed networks (VPRNs) connect the customer's IP router to the provider's IP router and require some coordination.
- Ethernet VPNs from Carriers: Carriers offer services that encapsulate Ethernet frames and deliver them across their network to an Ethernet connection on the other end.

5.3 Management Issues

In this part, management issues of organizations on deploying IPv6 will be analyzed. According to responses from the interviews as well as some document and bloggers of telecommunication, data can be categorized into groups as following table.

TABLE 8. Management issues

Categories		Participants' responses and issues
Motivations	Technical features	More addressing space Testing Preparing for the shortage of IPv4 in the future
	Profit issues	Long – term cost saving
	Supports from top executives	Yes
Hesitations	Technical features	Old system's compatibilities
	Profit issues	Training costs No instant advantages
	Supports from top executives	Don't want change while business is running well

5.3.1 Motivations

IPv4 exhaustion is obvious and it causes future addressing problems. Our interviews also revealed IPv4 exhaustion as the most common reason stated. As we know that IPv4 free pool is out, new Internet connections are rising fast in developing countries. Once those remaining IPv4 addresses are out, new connections will be provided with IPv6. If enterprises do not prepare for such parallel existence of IPv4 and IPv6, they may lose a number of customers who cannot access them on Internet.

From the interviews with heads of IT departments, the idea that addressing is the main reason for IPv6 to be created and address space boosting is the only improvement of IPv6 is pretty popular. In fact, the advances of IPv6 include update the protocol, addressing space as well as other aspects. Let's take a look at some important technical features that IPv6 is designed to archive according to Mr. Nguyen Ho Phi Long, Cisco Certified System Instructor at Nhatnghe Network Training Center:

More address space - This feature is the most well-known about IPv6. It provide up to $2^{128} = 3.4 \times 10^{38}$. It gets rid of NAT, technology for the lack of IPv4. It allows every device to have a permanent unique public address.

Better Management and Administration - Stateless auto configuration that means much less manual-configuration of IP address, even with DHC.

Improve routing performance - New header format of IPv6 remove routers from the fragmentation process, which means more efficient performance from routers.

Better multicasting/Media - IPv6 has built-in features for multicast and unicast groups. IPv4 had an option for multicasting but the support for it has been delaying.

Efficient mobility - As IPv4 was developed at the time when there was no mobile IP concept which leads to the need of Mobile IP. IPv6 provides mobility support by eliminating triangular routing.

Better security - IPsec, a framework from IETF, in IPv6 helps to advance the security implementation. By using IPsec, devices can acquire data privately, data verification and data integrity at the network layer.

As inferred from the interview with Aleksu Suhonen, Internetworking Consulting of Axu TM Oy, the most important aspect to an enterprise is *cost saving*. Technical features above may not sound very interesting to them. On cost-saving scale, the transition to IPv6 may offer many benefits for large enterprises. It promises to bring better routing performance, improve security and auto-configuration, which generate lower implementation cost, and daily maintenance basic cost. Therefore, it may save long-term IT cost for enterprises. Here are some approaches that enterprises that plan to adopt IPv6 should consider.

Firstly, IPv6 should be integrated into the product lifecycle replacement. The initial step of adopting IPv6 is to examine the existing information system infrastructure. Some hardware doesn't support IPv6 while software can be changed and upgraded. The next step is to specify IPv6 conformity with the RFPs. Then enterprises can reduce cost of IPv6 transition by including it to the product procurement plan of the current IT budget. IT staffs may consider the purchase of IPv6 supporting products while planning their regular procurement plan. In addition, IPv6 training cost should also be integrated into the IT budget; this cost may be considerably high during IPv6 adoption. These actions not only aim to prevent unexpected or unnecessary costs but also make the transition process smoother.

According to the interview with Mr. Nguyen Dac Thuan, Networking Manager of FPT Telecom, a leading telecommunication company in Vietnam, FPT has been purchasing IPv6 support devices, especially devices of Cisco. The company is aware clearly of the integration process in order to prepare for future. However, the training of staffs was not planned well; therefore it cost more than expected.

Transition technologies are also important factors of IPv6 transition process. There are several common techniques which will be discussed further in chapter 6 of this paper. To lower the cost and the associated operative effect of IPv6 adoption, it can be done by deploying IPv6 components in a fashion starting at the network bounds and evenly moving "inwards towards the core". (Das 2008).

Moreover, “the early bird gets the worm”, IPv6 is a certain future that it may bring opportunities to early service provider. Since many enterprises are new to IPv6, service provider can be a consultant in decision making while making some profit. Chip Popoviciu, technical leader with Cisco and co-author of the book *Global IPv6 Strategies*, emphasized the value that early adoption can get. Service providers can sell various services if they can play a role in helping enterprises deploy IPv6.

IPv6 day, organized in 2010, had indicated the participation of a various organizations. For some organizations, the reasons for deploying IPv6 include *testing*. According to Mr. Seppo Syrjanen, Data Network Specialist from IT Center of University of Helsinki, universities and especially equipments vendors who offer hardware and software products would like to make sure they are capable of communicating between IPv4 networks and IPv6 devices. Demand for IPv6 devices may be low at present but surely it will rise up in near future. To be prepared for it, IPv6 support should be integrated into product life cycle soon. Some organizations deploy IPv6 to test their present system so that it will be compatible with both IPv4 and IPv6.

5.3.2 Hesitations

IPv6 has been in the game for quite a while, but we have not seen any quick and eager movement toward the transition from IPv4 to IPv6. What are the reasons for such hesitations of enterprises?

In the successful IPv6 deployment list of Finnish organizations (derived from <http://www.vyncke.org/ipv6status/detailed.php?country=fi>), we see companies like Vertta, who let their service provider do IPv6 deployment for testing. This company didn't quite know about IPv6 transition. They left that process for their service provider.

Ethan Banks, a network engineer and host on Packet Pushers, an independent podcast on data networking, had shared his view on this issue. He said that his

company does not need IPv6 to do business or reach a new market while there are no important resources that is only reachable via IPv6 nor customers available only through IPv6. He also indicated that without a ready service provider along with transition solution, enterprises seem to be indifferent toward IPv6. (Banks 2011). For that reasons, without excellent service provider in the market, customers will not be ready to deploy IPv6. There is a saying that “Don't fix it if it hasn't broken yet”, then why bother changing while the business is going on well.

On the other hand, there is no backwards compatibility in transition to IPv6. Microsoft has no intention to implement IPv6 for older Window OS such as Windows 98 or Windows Millennium Edition or Windows 2000 (Microsoft 2008). Therefore, there are some concerns with the cost of replacing a variety of application, which needs to be IPv6 compatible. However, most of the networking software support IPv6 comes as an upgrades based on old software version, thus there is not much extra cost, even no. Nevertheless, specific software tailored for company is much more different. If an enterprise wishes to transit all software to IPv6 compatible and eliminate IPv4, it may come up with huge costs. It also costs a lot of time and efforts of applications developer to change the applications according to information from the interview with Mr. Nguyen Dac Thuan from FPT Telecom.

In conclusion, customers' awareness of IPv6 transition wasn't so high. Enterprises currently have not much ideas on what involve in the transition i.e. computers, network devices, infrastructures. They need a plan before they “hit the IPv6 wall unexpectedly”. (Middleton 2011).

6 EVALUATION OF CURRENT TRANSITION METHODS

The transition from IPv4 to IPv6 is not a one-day step and involves a lot of changes in network structures with the use of IP addresses. For the future success of IPv6, the next step in deploying IPv6 is to vote for the most suitable transition methods and their management. Although many kinds of transition mechanisms have been invented to help with the process, the implementation of IPv6 is never said to be easy and simple, even for experienced administrators. As a result, the most difficult problem to make decisions for is which method will be chosen for the implementation process to achieve a smooth and seamless transition (Raicu and Zeadally 2003).

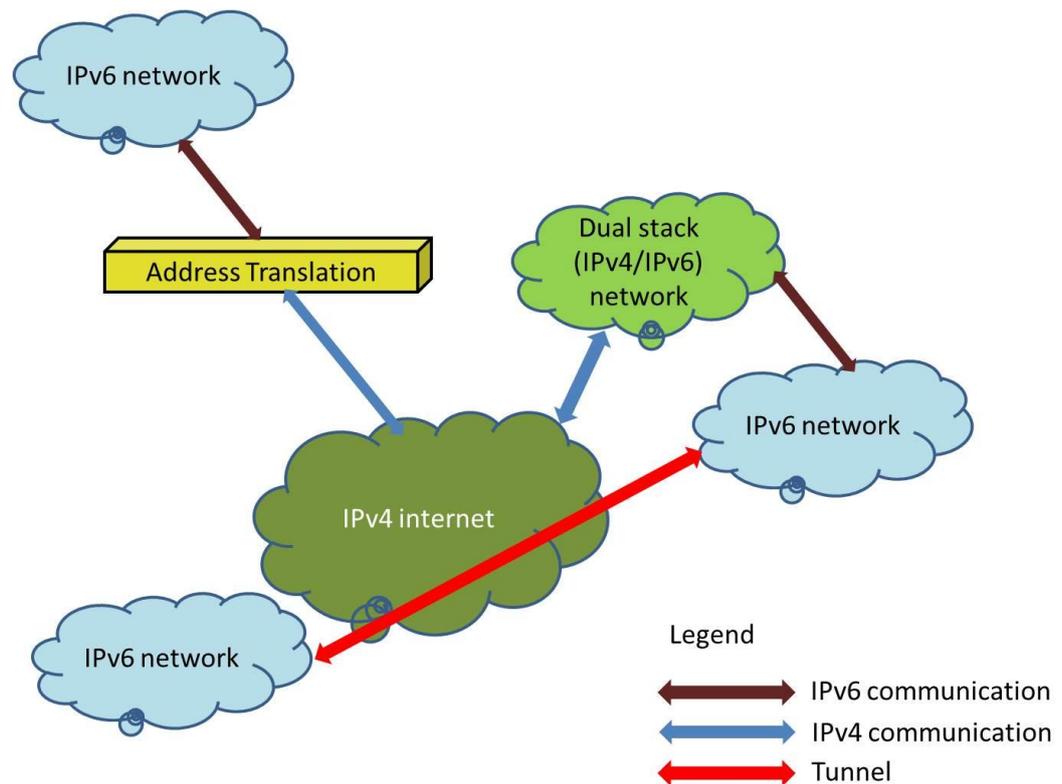


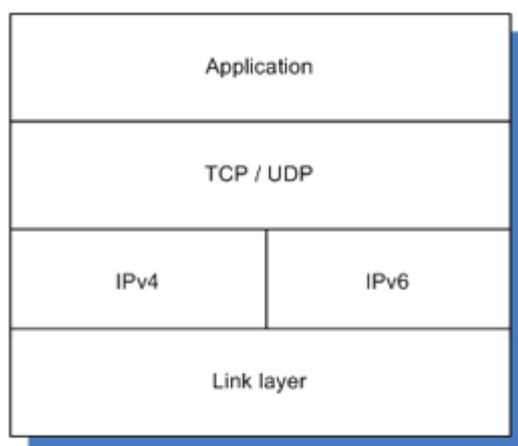
FIGURE 14. Different transition technologies (Subramanian 2003)

According to the above picture, there are different kinds of technologies which can be applied such as dual stack, tunneling mechanisms, and translation techniques. Over sixteen transition techniques have been used and tested for the communications between different networks to ensure IPv4 and IPv6 interoperability. Therefore, to make decision on the best suited transition methods, it is really important to have an overview of the current IPv4 networks. In addition, enterprises must analyze needed functionalities, scalability, and securities in the corporation. Besides, “one size does not fit all” and a network can be applied different transition mechanisms together to support a complete distributed system.

In this section, based on the information from the research and literature review, we would present an overview of some major transition methods as well as relevant matter to opt out the best methods for large enterprise networks. Each technique possesses individual attributes and plays an important part in the transition process. In general, we can classify various transition techniques into three categories with respect to connectivity and necessary elements for the implementation

6.1 Method 1 - Dual Stack IPv4/IPv6 Devices

TABLE 9. Dual Stack (Nokia n.d.)



From the table above, the dual stack happens in the network layer, which contains both IPv4 and IPv6. Stack means, “A stack is a type of data structure -- a means of storing information in a computer. When a new object is entered in a stack, it is placed on top of all the previously entered objects. In other words, the stack data structure is just like a stack of cards, papers, credit card mailings, or any other real-world objects you can think of. The term "stack" can also be short for a network protocol stack. In networking, connections between computers are made through a series of smaller connections. These connections, or layers, act like the stack data structure, in that they are built and disposed of in the same way”. (TechTerms n.d.).

However, like any market regulations, the acceptance of any new technology lies in the way it integrates into the current infrastructure with no serious breakdown of service. A large enterprise network includes many IPv4 networks and thousands of IPv4 nodes. Therefore, the transition from IPv4 to IPv6 does not require upgrades on all nodes at the same time; IPv4 and IPv6 will coexist for some time. As a result, enterprises can apply dual stack method to transit to IPv6.

The dual stack method is literally to use two IPv4 and IPv6 stacks for operating simultaneously, which enables devices to run on either protocol, according to available services, network availability, and administrative policies. This can be achieved in both end systems and network devices. As a result, IPv4 enabled programs use IPv4 stack and this goes the same for IPv6. The IP header version field would play an important role in receiving and sending packets. In other words, this kind of IPv6 transition is the encapsulation of IPv6 within IPv4. The complete transition can be managed by DNS, for example, in the circumstance that a dual-stacked device queries the name of a destination and DNS gives it an IPv4 address (a DNS A Record), it sends IPv4 packets, or in case DNS responds with an IPv6 address (a DNS AAAA Record), it sends IPv6 packets. This mechanism is currently the best choice for the transition as many operating systems have applied dual IP protocol stacks (Cho, Luckie and Huffaker 2004).

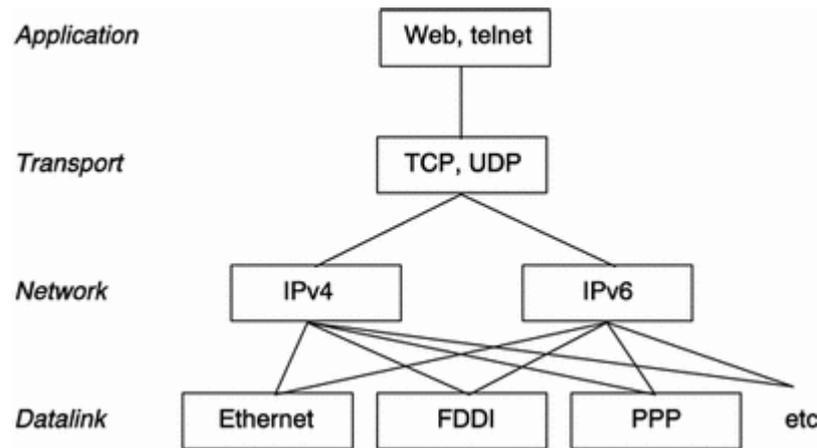


FIGURE 15. The structure of Dual stack model (Oracle Corporation 2001).

As presented in Figure 15, the dual stack method is implemented in the network layer for both IPv4 and IPv6. Before transferring the packet to the next layer, the network layer will choose which one to use based on the information from the datalink layer. Large enterprise networks that are decided to transit to IPv6 can apply the dual stack method as the basic strategy, which involves the device configuration to be able to utilize IPv4 and IPv6 at the same time on the core routers, perimeter routers, firewalls, server-farm routers, and desktop access routers. Depending on the response to DNS requests, applications can choose which protocol to use and this choice can be made in consonance with the type of IP traffic. Furthermore, hosts can attain both available IPv4 content and IPv6 content. Accordingly, dual stack mechanism presents a flexible transition strategy. However, despite its greatest flexibility, there are still some concerned issues with this method such as every dual-stack device still requires an IPv4 address; two routing tables must be maintained in every dual-stacked router; as two stacks must be run at the same time, additional memory and CPU power will be required; moreover, every network requires its own routing protocol; supplementary security concepts and rules must be set within firewalls to be suited to each stack; a DNS with the ability to resolve both IPv4 and IPv6 addresses is required; finally, all programs must be able to choose the communication over either IPv4 or IPv6, and separate network management commands are required (Hirorai and Yoshifuji 2006). For example, based on the figure below, the client computer at first sends a DNS lookup request for the website `www.a.com`. Then, the DNS

server will reply with an IPv4 and an IPv6 address of the website. Finally, the client computer will use that information to send request to the router via either IPv4 or IPv6 network and the web server will reply the client by allowing to load the website.

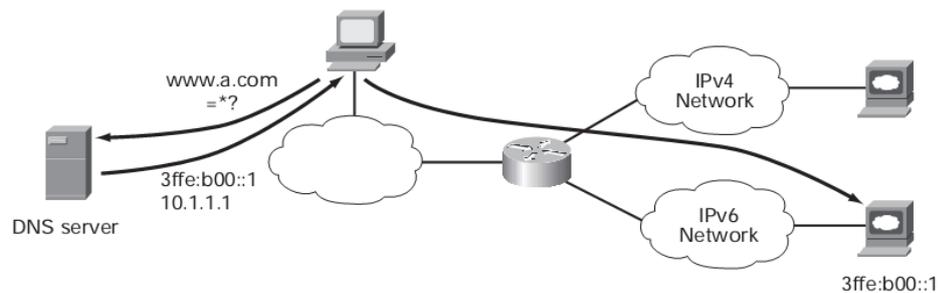


FIGURE 16. IPv4 – IPv6 dual stack operation (Cisco, The ABCs of IP version 6 2010)

6.2 Method 2 – Translation

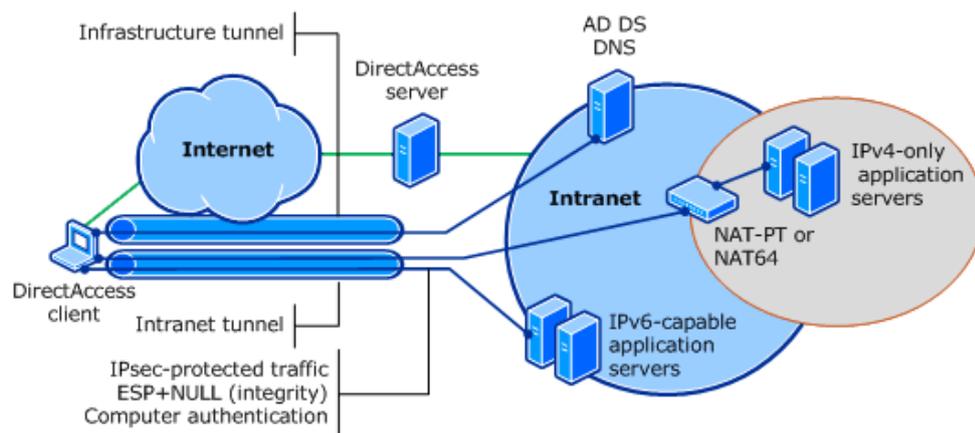


FIGURE 17. Translation method model (Microsoft, Technet 2012)

Together with IPv6 deployment strategies into large enterprise networks, the figure above indicates that there are various translation mechanisms (NAT-PT, application level gateways (ALG)) also applied to enable the communication between IPv4-only applications and IPv6-only applications. The meaning of translation is to convert directly protocols from IPv4 to IPv6 or vice versa, which might result in transforming those two protocol headers and payload. This mechanism can be established at layers in protocol stack, consisting of network, transport, and application layers. The translation method has many mechanisms, which can be either stateless or stateful. While stateless means that the translator can perform every conversion separately with no reference to previous packets, stateful is the vice versa, which maintains some form of state in regard to previous packets. The translation process can be conducted in either end systems or network devices (Nakajima and Kobayashi 2004).

The fundamental part of translation mechanism in transition process is the conversion of IP and ICMP packets. All translation methods, which are used to establish communication between IPv6-only and IPv4-only hosts, for instance, NAT-PT or BIS, apply an algorithm known as Stateless IP/ICMP Translator (SIIT). The function of this algorithm is to translate packet-by-packet the headers in the IP packet between IPv4 and IPv6, and also addresses in the headers among IPv4, IPv4-translated or IPv4-mapped IPv6 addresses. However, this does not mean IPv6 hosts can get an IPv4 address or route packets, but this assumes that each IPv6 host can have a temporary assigned IPv4 address (Nakajima and Kobayashi 2004).

Stateless IP/ICMP Translation (SIIT)

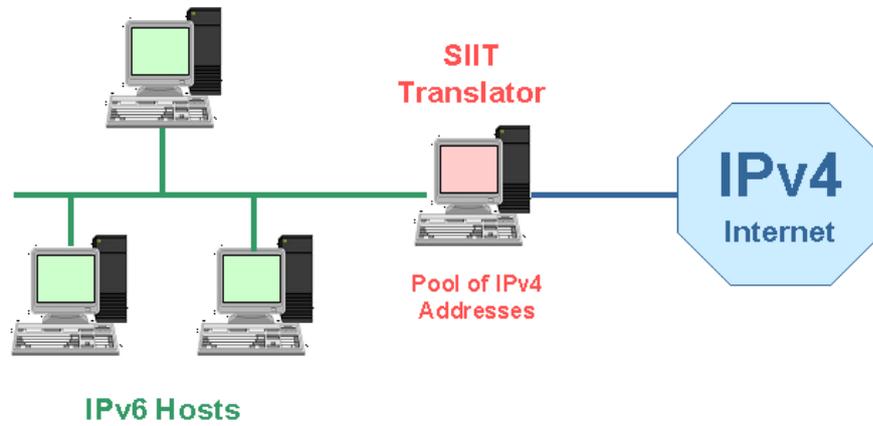


FIGURE 18. SIIT Model (Vienna University of Technology 2012)

The above figure indicates an algorithm that designates a two-way translation between IPv4 and IPv6 packet headers or between ICMPv4 and ICMPv6 messages. The interpretation has been arranged so that UDP and TCP header checksums are not influenced during the process. More importantly, SIIT is currently used as the backbone for NAT-PT and BIS (RFC2765 2000).

Network Address Translation-Protocol Translation (NAT-PT)

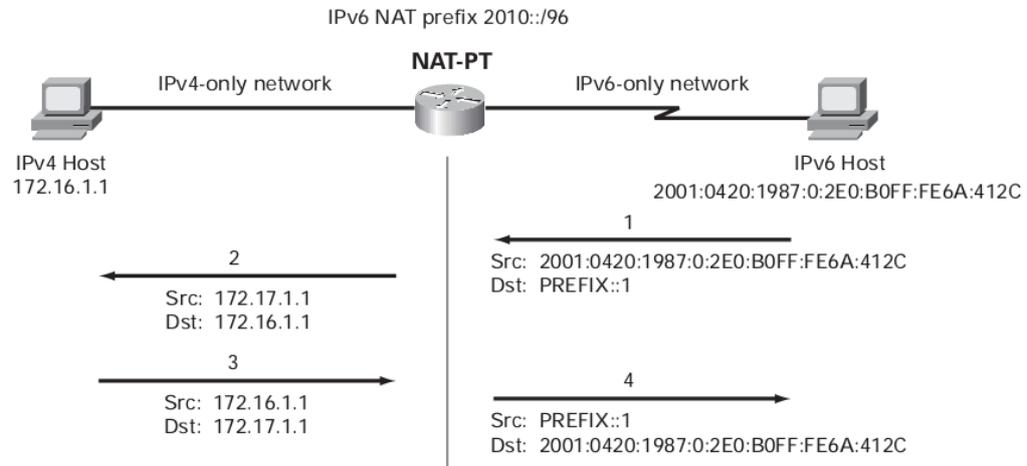


FIGURE 19. Deployment of IPv6 using NAT-PT (Cisco, *The ABCs of IP version 6* 2010)

From the figure above, the router is used as a translation communicator between an IPv4-only network and an IPv6-only network. NAT-PT is considered as a stateful translator functioning in the network layer with the SIIT algorithm. The main role of a NAT-PT device, such as routers or servers, is to support numerous IPv6 nodes by assigning a temporary IPv4 address for each, which permits native IPv6 hosts and applications to communicate with native IPv4 hosts and applications. In general, it acts as a communication proxy with IPv4 peers. Proxy means “a server that stands between an external network (such as Internet) and an organization's internal (private) networks and serves as a firewall. It prevents external users from directly accessing the internal information resources, or even knowing their location. All external requests for information are intercepted by the proxy server and checked for their validity, and only authorized requests are passed on to the internal server” (BusinessDictionary n.d.). However, this mechanism still possesses limitations similar to IPv4 NAT such as point of failure, decreased performance of an application level gateway (ALG), reduction in the overall value and utility of the network. NAT-PT also prevents the ability to implement security at the IP layer (RFC2766 2000).

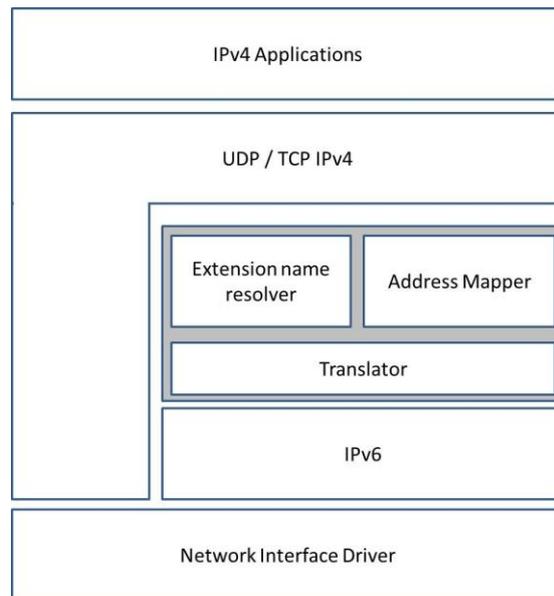
Bump in the Stack

FIGURE 20. Bump in the Stack model (TechWeb 2009)

The BIS method means there are three more fields inserted into the structure of layers as indicated in Figure 20. There will be three additional components, name resolver extension, address mapper, and translator, and are layers between the application and network layers. The BIS method is specially designed for communication between IPv4 applications on an IPv4-only host and IPv6-only hosts. The term bump is used to describe extra modules in a TCP/IP stack. Firstly, the extension name resolver uses DNS lookups to see if the node supports only IPv6. Secondly, the address mapper will allocate a temporary IPv4 address for the IPv6 node and save that in the address mapping caches. Thirdly, the translator translates packets between IPv4 and IPv6. In the circumstances that a program needs to transmit data from and to a host, which supports only IPv6, those layers will play their roles to map an IPv6 address into the IPv4 address of the IPv4 host. Nevertheless, those temporary IPv4 addresses are only apparent in the end system and normally come from a private address space. Therefore, BIS is only suitable to programs that include no address-dependent fields in application layer protocols. One more thing is that this method can only be implemented on end systems. The reason for this limitation is that it is easier for translation processes

to solve application to network interoperability problems but it would be harder to control on a larger scale (RFC2767 2000).

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

6.3 Method 3 – Tunneling

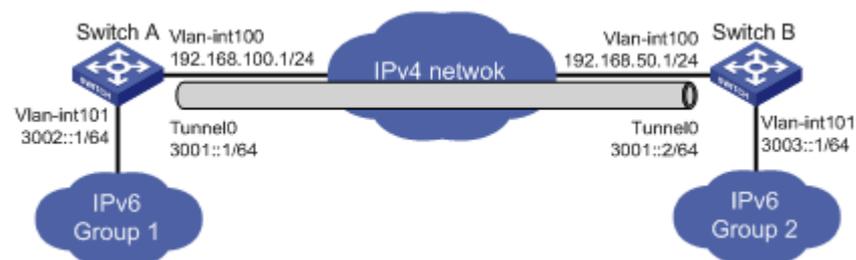


FIGURE 21. Tunneling transition method (H3C 2003)

The last category for IPv6 transition process is tunneling as presented in Figure 21. This is used to transfer data between compatible networking nodes over incompatible networks. There are two ordinary scenarios to apply tunneling: the allowance of end systems to apply offlink transition devices in a distributed network and the act of enabling edge devices in networks to inter-connect over

incompatible networks. Technically speaking, the tunneling technique utilizes a protocol whose function is to encapsulate the payload between two nodes or end systems. This encapsulation is carried out at the tunnel entrance and the payload will be de-capsulated at the tunnel exit. This process is known as the definition of tunnel. Therefore, the main issue in deploying tunnel is to configure tunnel endpoints, determine positions for applying encapsulation. Based on our research, this mechanism are generally attained via manual or tool-based parameter entry, existing services like DNS or DHCP, or by taking into use the embedment of information into IP addresses or applying an IPv6 anycast address. (Bi, Wu and Leng 2007). Network devices can achieve the two processes of encapsulation and de-capsulation at tunnel endpoints. In general, tunneling mechanism is a simple deployment with point-to-point configuration. Nevertheless, tunnels can also be implemented hierarchically and sequentially. Hierarchical structure is applied in the circumstances that there are transition tunnels operating alongside with security or QoS tunnels. Sequential structure can be established in an end-to-end path, from end systems to local gateways, and beyond. As a result, these two establishments always increase requirements for processing and packet delay. Up to date, there exist different tunneling methods such as 6to4, ISATAP, Teredo, DSTM, and 6over4. Tunnels may be manually configured or automatically configured. (Qing-weil and Lin 2007).

6over4

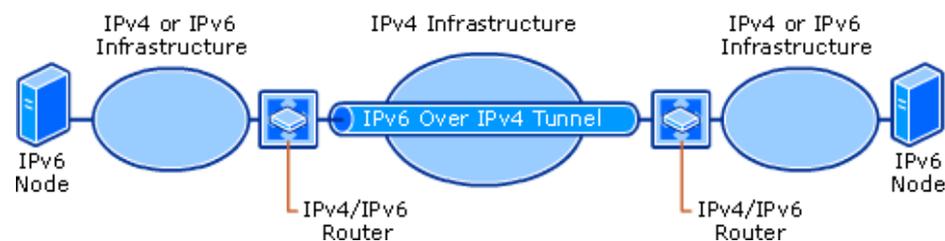


FIGURE 22. 6over 4 model (Microsoft 2011)

The figure above illustrates the 6over4 method that inserts IPv4 addresses into IPv6 address link layer identifier part and defines Neighbor Discovery (ND) over IPv4 by using organization-local multicast. In this method, the multicast enables IPv4 network to perform as a virtual LAN and the IPv6 target address will be resolved on this network to get the destination IPv4 address for the tunnel endpoint. This mechanism accommodates all features of IPv6 such as end-to-end security, multicast and stateless auto-configuration. It also bears resemblances to the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) method. (Bouras, Karaliotas and Ganos 2003).

Dual Stack Transition Mechanism (DSTM)

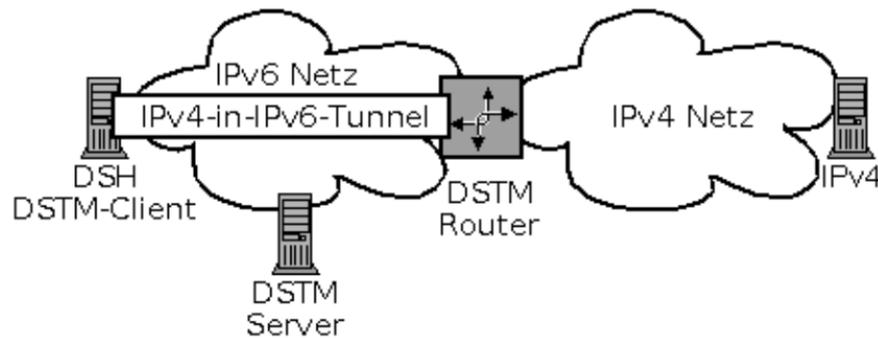


FIGURE 23. DSTM model (Wedel 2008)

The DSTM mechanism, which is expressed in Figure 23, allows temporary IPv4 addresses to be allocated for end systems with dual stack enabled with connection to networks that support IPv6 only. The general idea is that IPv4 packets will be tunneled to pass through IPv6 network to get to the global IPv4 Internet. In the event that a DSTM end system starts sessions, a DHCPv6 server which has been modified to acquire a temporary IPv4 address and the address of DSTM border router, to which packets are later tunneled. On the other hand, in case a node supporting only IPv4 initiates sessions, the request sent to DNS for the lookup process would be directed to an adjusted DNS server in the DSTM domain, at which a temporary IPv4 address will be appointed for the end system. As a result,

incoming packets are tunneled to this IPv4 address (Bouras, Karaliotas and Ganos 2003).

6to4 Automatic Tunneling

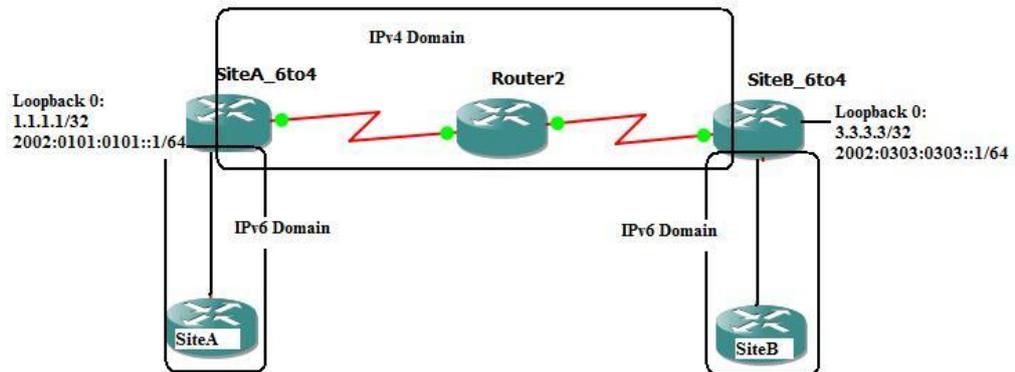


FIGURE 24. 6to4 Automatic Tunneling model

Automatic means that tunnel configuration is carried out with no additional management. As shown in Figure 24, this method is considered as the most popular choice in the field of automatic tunneling technique. When in operation, this mechanism will have IPv6 traffic tunneled upon IPv4 networks within isolated 6to4 networks. A special prefix containing the IPv4 address of its 6to4 gateway is supposed to be present in each 6to4 network, which enables tunnel endpoint addresses are acquired easily and requires no IPv6 administrative work. Then connection from 6to4 network to the rest of the IPv6 network is established via a dual stack local gateway and a dual stack relay router. Therefore, every IPv6 packet is directed to the gateway. These kinds of tunnels would transfer the traffic to appropriate gateway with suitable IPv4 address. (RFC6343 2011).

Teredo

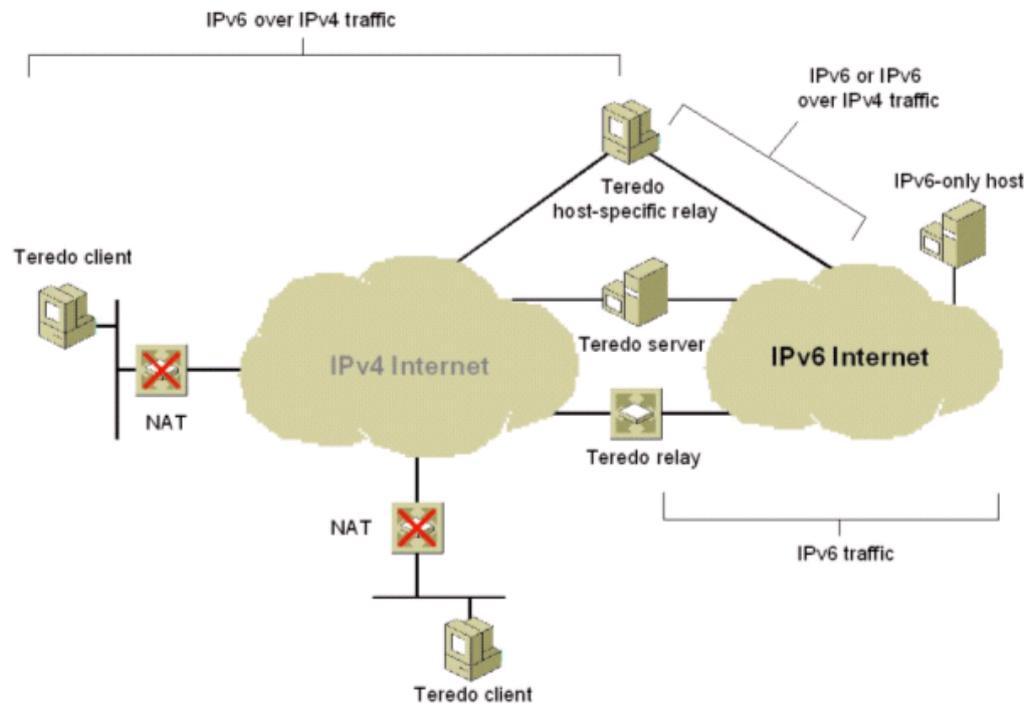


FIGURE 25. Teredo method (Microsoft 2011)

Teredo mechanism is a technique for assigning addresses and providing tunneling services automatically to allow IPv6 connectivity across IPv4 Internet. This method is supposed to be the solution for the lack of 6to4 functionality by supporting the tunnel for IPv6 packets between hosts within sites while 6to4 method only allows providing tunnels for IPv6 packets between edge devices. Based on our research, currently networks, which are applying IPv6, face another problem of NATs. Because of its nature, IPv4- encapsulated IPv6 packets have the header set to 41, which prevents them to pass through typical NATs. Accordingly, because UDP messages can be translated universally by NATs and can traverse multiple layers of NATs, Teredo encapsulates the IPv6 packet as an IPv4 UDP message, provided that NAT supports UDP port translation, it supports Teredo. (Huang, Quincy and Lin 2005).

Tunnel Broker

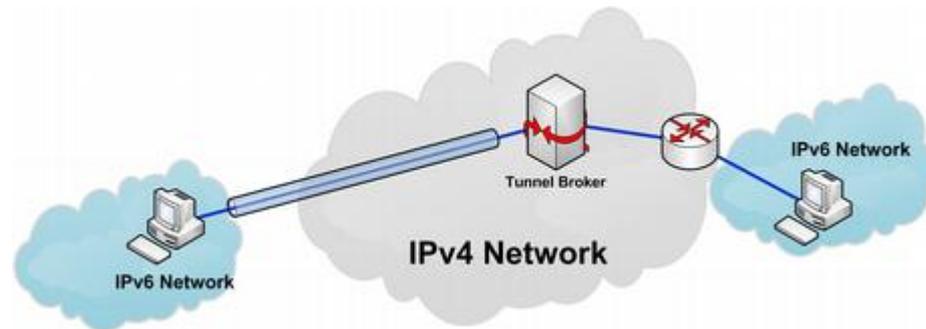


FIGURE 26. Tunnel Broker model (Netnam Ltd. 2011)

This is another approach to IPv6 with the support of dedicated servers, known as Tunnel Brokers as illustrated in Figure 27, to answer automatically tunnel requests from users, which is believed to increase IPv6 growth with connected hosts and to support access to IPv6 networks. Besides, this method makes it easy for IPv6 ISPs to manage access control by applying own policies on network usage. This is where users make connection for registering and activating tunnels. Then, dedicated servers or Tunnel Brokers control the management of tunnels with activities such as creation, modification and deletion for users. In addition, to support networks on a larger scale, this method can distribute the workload to some tunnel servers by delivering orders to concerned tunnel server when there is a need to manage a tunnel. Finally, connections between tunnel brokers and servers can occur with IPv4 or IPv6. (Chen, et al. 2002).

Generally, the tunneling mechanism allows us to connect isolated IPv6 nodes and networks whether or not the ISP has been upgraded to IPv6. Moreover, it also takes advantage of emerging IPv6 services while remaining connected to the IPv4 world. However, its encapsulation and de-capsulation take more time and CPU power, and add more complications to troubleshooting and network management as well. One more thing is that those tunnel endpoints can be single points of failure and they can be vulnerable to security attacks. (Waddington and Chang 2002).

6.4 Summary of three methods

Below is the summary table containing the advantages and disadvantages for three main methods above.

TABLE 10. Summary of three methods

	Advantages	Disadvantages
Tunneling	<ul style="list-style-type: none"> - Configure tunnel endpoints only - Simple deployment - No additional management 	<ul style="list-style-type: none"> - Face another problem of NATs - Take more time and CPU power - Harder to troubleshooting and network management - Have single points of failure - Vulnerable to security attacks
Translation	<ul style="list-style-type: none"> - The router is used as a translation communicator - Solve network interoperability problems 	<ul style="list-style-type: none"> - Limitations similar to IPv4 NAT - Reduction in the overall value and utility of the network. - Harder to control on a larger scale - Complexity increases in IP addresses
Dual stack	<ul style="list-style-type: none"> - Easy to implement - Low cost - Greatest flexibility - Already supported in all OSs and devices 	<ul style="list-style-type: none"> - Two routing tables - Additional memory and CPU power - Two firewall sets of policies

6.5 Conclusion

Based on the above overview of all mechanisms and current practices in researched enterprise networks, nearly all deployments of IPv6 in enterprise networks apply dual stack mechanism as it gives us a way to know more about IPv6 as well as to improve practical experience with a new address family, which plays an important role in the success of transition implementation. Therefore, in this thesis, we choose the dual stack mechanism to build a model for large enterprise networks.

7 RECOMMENDATION OF IPV6 TRANSITION FOR ENTERPRISES

“Readiness is a state of preparedness of persons, systems, or organizations to meet a situation and carry out a planned sequence of actions. Readiness is based on thoroughness of the planning, adequacy and training of the personnel, and supply and reserve of support services or systems” (BusinessDictionary n.d.).

In expression of IPv6, this means being ready for the implementation of IPv6 into a network when business requirements arise.

The University of Helsinki, Axu TM Oy, and FPT Telecom Corporation have already taken initial steps to implement IPv6 into the network system based answers gathered from the research. Although these efforts are now just meant for testing, the message from the international community is clear. The transition from IPv4 to IPv6 will become a must for enterprises, especially ones that currently provide online services based on IP addresses. They must be able to handle large requests from internal and external customers who are applying their emails or web or other services to everyday working lives over the Internet. As a result, this creates new demands for services to be approachable via both IPv4 and IPv6, which means organizations, enterprises or even governments who wish to continue online operations must right now consider the pros and cons of the usage of IPv6 and analyze future needs to integrate IPv6 into the whole system. It is impossible to predict exactly when IPv6 will become mandatory for most companies. However, in accordance with Mr. Seppo Syrjanen, Data Network Specialist from IT Center of University of Helsinki, although IPv6 adoption is a need for current companies to prepare for the future, aside from the exhaustion of IPv4 address for stakeholders to take into consideration, it is not an easy and single step that can be achieved in a short time but this requires a great amount of thorough planning and preparation to develop and adjust an IPv6 business case. Therefore, it is not when IPv4 addresses come to the point of complete exhaustion, IPv6 has already been considered as purely strategic because this is not only to establish global connectivity of enterprise networks for the future, but also to guarantee growth as well.

In this part, based on information from the interviews with large companies and enterprises, we would like to categorize different preparation activities that can be applied as a plan in this IPv6 implementation. This part would become a great asset to assure that a common method is ready to make plans and to check IPv6 readiness when it falls into place for each enterprise network. It is an outline of phases which have both technical infrastructure and business readiness taken into account for an enterprise to initiate the transition to IPv6.

7.1.1 Business Side

Phase 1: The determination of business grounds and demands to implement IPv6

An enterprise must have strong and reasonable desires to initiate the IPv6 transition project. They need to realize business requirements, motives and mark the features of IPv6 to those particular objectives. Five main conditions that need to be acutely considered are business operations after the depletion of IPv4 addresses, support for a great amount of network devices, enterprise policies for IPv6 transition, requests from customer, partners, suppliers, and the global-scaled trade Mr. Nguyen Dac Thuan, Networking Manager of FPT Telecom.

Phase 2: The analysis of profits, expenses, and risks

Enterprises need to assess the impacts of IPv6 transition and which kinds of benefits it brings to the business. Specifically, they need to perform thorough analysis to decide which certain line of business or programs can be benefited from IPv6 transition. In addition, from the interview with Aleksu Suhonen, Internetworking Consultant at Axu TM Oy, there are other relevant subjects that also need to be taken into serious consideration such as enhancement of new services as well as the maintenance of existing services, development of network efficiency and cost savings (the elimination of NAT or other work-around

methods), the high performance of large enterprise network, simple configuration of online operations, and the supply of tactical advantages.

Mr. Nguyen Ho Phi Long, Cisco Certified System Instructor at Nhatnghe Network Training Center, has said that costs estimation is the most important part in every project and it can decide the progress of the implementation. Therefore, once enterprises would like to initiate the IPv6 transition, they also need to be prepared for the budget that can be used for planning, design (infrastructure upgrades if needed), implementation testing, deployment, personnel training as well as operational costs.

Risk in definition is “a probability or threat of a damage, injury, liability, loss, or other negative occurrence that is caused by external or internal vulnerabilities, and that may be neutralized through preemptive action” (BusinessDictionary n.d.). In this IPv6 transition, risk includes business, legal, privacy, security, reliability, interoperability and technical risks. Only when we can identify risks and the impact it may affect, will we be able to apply action plans to prevent or reduce the influence on the whole project. These plans should put emphasis on major program activities, specific solutions, and impacts.

Phase 3: The settlement of a supervised group (SG) for administration of IPv6 transition project

According to Mr. Nguyen Dac Thuan, Networking Manager of FPT Telecom, the supervised group will temporarily act as a centralized management office (CMO) to make plans, administer, and control the progress of IPv6 transition throughout the entire enterprise. Furthermore, the SG will arrange sufficient resources such as staffing, training, and budget to support the IPv6 project successfully. This type of CMO is particularly crucial in large organized enterprises. Specifically, the SG will be responsible for recruiting suitable members to the group for different roles and responsibilities; gaining authority rights within the enterprise to support financial matters for the transition project and set policies to become the priority in case of shortage of resources; organizing an administration structure to guarantee the success implementation of IPv6 transition. The SG will be the

leader to set the milestones and targets for the working team and control the progress through successful results.

7.1.2 Technical Side

Phase 4: The assessment of all assets of current network infrastructure

From the interviews with Head of IT center from Nhatnghe Network Training Center, the University of Helsinki, we suggest that before starting to implement the IPv6 transition project, the enterprises need to carry out a complete analysis of current networks to get an overview of components that may need to be changed or upgraded to be suitable for transition to IPv6 such as address allocation, networks services (IP, wireless, VoIP, DNS, DHCP, NTP...), network management, applications, operational systems and support.

Phase 5: The establishment of architecture for IPv6 project

When implementing the transition from IPv4 to IPv6, there must be an overall IPv6 architecture for various impacted areas. It should be standard based and support IPv4 to perform a smooth transition. Moreover, this architecture should also expect new networks and services as well as foreseeable traffic growth after the implementation. There are some concerned major areas such as IPv6 addressing plan, IPv6 routing, IPv6 interconnection, IPv6 foreseeable traffic, IPv6 enabled systems, IPv6 deployment plan, transition mechanism (dual stack, tunneling, and translation), network services, security, management, scalability & reliability, and service level agreements (RFC2373 1998).

Phase 6: The outline of a specific structure on the influence of IPv6 project

The IPv6 project, once established, will place influence on every platform and service in the network. As a result, IPv6 capability and its influence will be decided according to enterprises' standard for each platform and service, which consists of commercial and industry standards. This includes the required resources (devices, personnel, budget, etc.) and the communication between system integrator and vendor, said by Mr. Nguyen Dac Thuan, Networking Manager of FPT Telecom.

Phase 7: The development of an IPv6 project plan

In this phase, the SG is required to gather all information and resources to design a final plan for IPv6 transition in the enterprise network. Because of its importance, this plan is required to contain a schedule of small projects to be implemented along with dependencies and priority. Furthermore, in accordance with Mr. Nguyen Ho Phi Long, Cisco Certified System Instructor at Nhatnghe Network Training Center, there should be a testing environment for members to gain experience with new IPv6 features and also to demonstrate the architecture, plans, policies... One more thing is that the SG should perform trials on the real enterprise network as well as operational processes to ensure that all devices and services acquired or developed are IPv6 capable.

Phase 8: The provision of a personnel-training program

This IPv6 transition project involves either business or technical aspects and this also means the attendance of many users from the board of directors to ordinary staff to maintain IPv6 readiness. As a result, training is required to update knowledge and skills for users to familiarize with the new system (RFC4057 2005). However, based on the position of users in the enterprise, there will be many types of training programs to be suitable for all. Based on the information from the interview with Mr. Nguyen Dac Thuan, Networking Manager of FPT Telecom, we divide the training into four categories:

General training program aims to give normal users primary information about IPv6 and its related issues. This training also includes a summary of IPv6 technologies, a basic knowledge of IPv6 technology, and also business factors or IPv6 capable services.

Engineer training program is to give detailed information about IPv6 technologies and this is suitable for staff members who are responsible for analyzing, planning, designing, testing and deploying IPv6.

Operational training program presents specific IPv6 education to employees who take care of the support for an IPv6 network.

Special training program includes advanced information in certain technology area, which is suitable for technical specialists or experts in a certain technology area such as security, mobile, etc.

7.1.3 Stages of Readiness

In this part, based on the information from literature review and interviews, we have combined that information to create a checking tool for enterprises to assess IPv6 readiness level in the network. Based on the result from this tool, the board of directors can have an overview of the current network and make decisions or plans according to the result. The stages of IPv6 readiness can be arranged into six ranks, which represent the work to be achieved before implementing IPv6:

Rank 1: The enterprise has no intention to implement IPv6.

At this stage, enterprises have no business requirements and decide not to integrate IPv6 into the system as they analyze that the expenditure for IPv4 shortage is lower than the effort and budget spent for transition to IPv6 while IPv4 exhaustion will not place influence on their business.

Rank 2: The enterprise has taken IPv6 into consideration but is still unprepared to initiate it.

At this stage, enterprises may hire IT experts to advise on the IPv6 project or methods to prevent IPv4 address exhaustion. Moreover, there may be discussions within the executive group (CIO, CEO, CTO...) to collect information in relation with IPv6 project such as business and technical requirements as well as cost and risk for transiting to IPv6.

Rank 3: The enterprise has an IPv6 program in place and is determining important issues.

At this stage, enterprises may establish a business case and a budget for the IPv6 migration. A supervised group is also formed to control and manage the progress of IPv6 implementation. The members and roles of the IPv6 Transition Group should be identified. Furthermore, a thorough analysis of current network infrastructure should be done to check the IPv6 capabilities. There will also be a deployment and testing plan as well as training programs for staff.

Rank 4: The enterprise possesses an IPv6 project associated by a final plan.

At this stage, enterprises may already have a sponsored IPv6 project which includes a detailed report of current infrastructure and a tested architecture design of IPv6 implementation.

Rank 5: The enterprise is in possession of an IPv6 project without any unresolved crucial issues.

At this stage, enterprises, supported by all detailed documents such as an IPv6 deployment plan, training plan, architecture design, may actively put into practice those plans and design to perform the first testing on the real networks.

Rank 6: The enterprise has successfully accomplished the IPv6 transition project.

At this stage, enterprises have deployed IPv6 into the system and finished the testing part. Furthermore, the training programs are also provided for every user. Last but not least, the system is ready to communicate with other IPv6 networks from customers, partners, and suppliers.

Below is the table to describe the phases that is suitable for each rank.

TABLE 11. Rank description

Phase	Description	Rank					
		1	2	3	4	5	6
1	The determination of business grounds and demands to implement IPv6		X	X	X	X	X
2	The analysis of profits, expenses, and risks		X	X	X	X	X
3	The settlement of a supervised group (SG) for administration of IPv6 transition project			X	X	X	X
4	The assessment of all assets of current network infrastructure				X	X	X
5	The establishment of an architecture for IPv6 project				X	X	X
6	The outline of a specific structure on the influence of IPv6 project					X	X
7	The development of an IPv6 project plan						X
8	The provision of a personnel training program						X

In general, it is necessary for enterprises to thoroughly analyze and implement an IPv6 transition with clear instructions to serve expectations. However, because of the specific expectations may change from time to time, and they can be different by various enterprises, a complete approach with careful planning and preparation as listed in this part, accompanied by the details for each phase will allow the IPv6 implementation project to be achieved successfully, which will open a new path for each enterprise to be ready for the next generation of communication networks.

8 IPV6 IMPLEMENTATION

8.1 Introduction

In this part, we will start to implement the IPv6 in the current IPv4 based system. To support the transition process, we will use a program, Cisco Packet Tracer (CPT), which is a powerful network simulation software using the core program from Cisco. Therefore, with the support of CPT, we can create a visual model of a network by the drag-and-drop methods. CPT is used to simulate network devices such as switches, routers, and servers... with a virtual IOS for operation and management. This includes designing network models ranging from simple to complex level based on practical requirements, simulating IOS platforms for routers, IPS, PIX firewall, ASA firewall of Cisco, simulating packet-switching devices such as Ethernet, ATM, Frame Relay switch, etc. (Janitor, Jakab and Knieward 2010).

In addition to the simulation program, we also build an artifact, a network model of an enterprise to implement the transition from IPv4 to IPv6. In this model, we will apply the dual stack mechanism to transit to IPv6.

8.2 Enterprise Network Design

Our model has three main areas. At first, the headquarters model (Figure 27), a center of operations or administration in an enterprise, consists of four groups:

Group 1: The Demilitarized Zone (DMZ) would contain all the most important servers in an enterprise such as web server, database server, file server, exchange server... Each of them stores all confidential information, which can only be accessed by authorized personnel and they will provide information and data for users inside and outside the network. However, due to the nature of services, these servers are usually exposed to untrusted networks. Therefore, in the DMZ, network administrators will apply all the latest patches, technology, and security to protect the network from hackers and other threats.

Group 2: This group is named “The Intrusion Prevention”, which is the combination of authentication server, VPN server, and intrusion prevention servers, responsible for checking logged in users as well as protecting the whole network from attacks or penetration.

Group 3: Known as “The Service Provision”, this group contains DHCP server, FTP server, DNS server, etc., providing necessary services throughout the system.

Group 4: Within this “Client Zone” group is the place for all client computers, laptops, mobile phones, etc., to connect to the network in the enterprise.

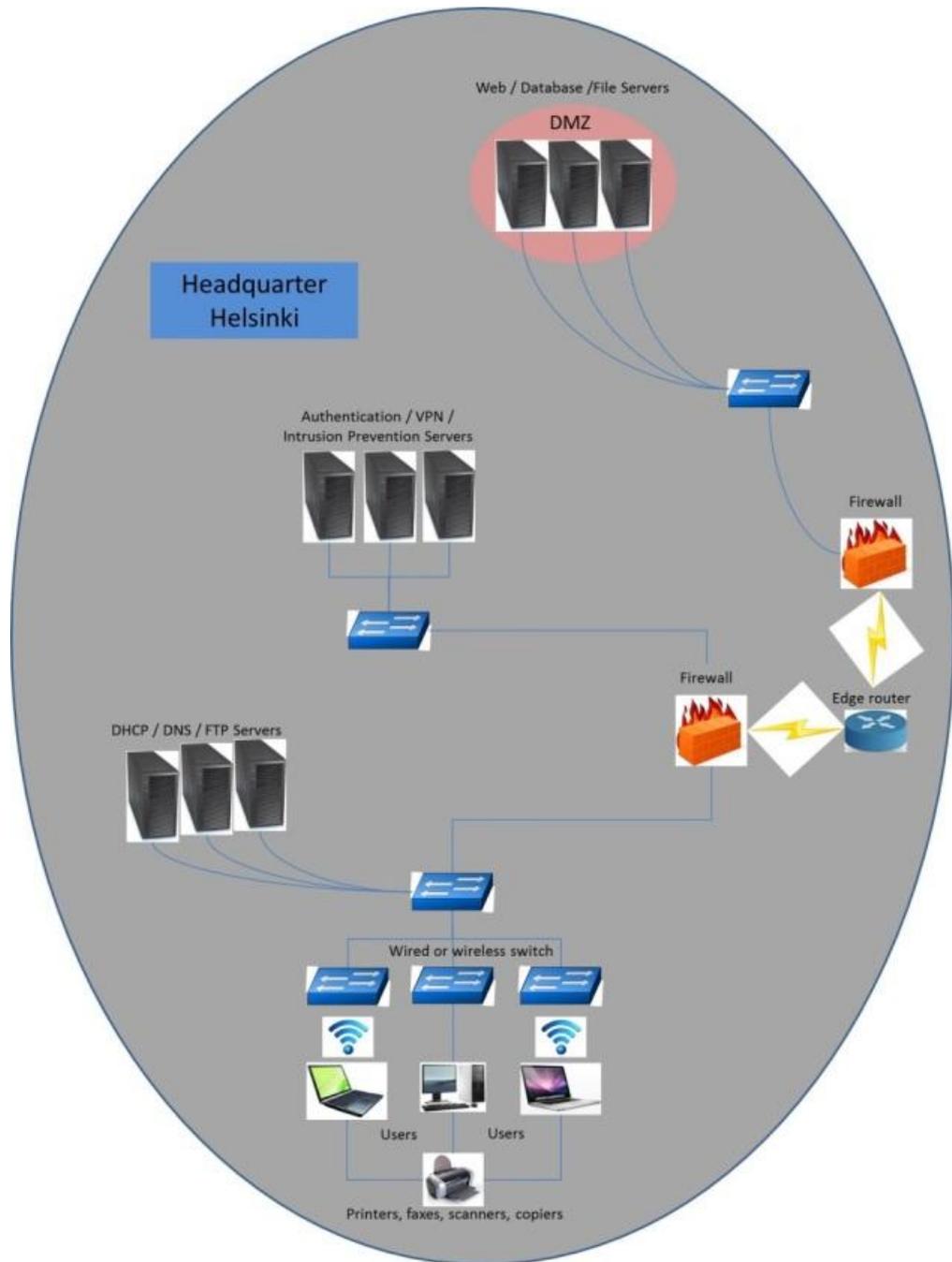


FIGURE 27. Headquarter network structure model

Secondly, a branch is a division of the business that can be located in various geographic areas. Therefore, the network model of each branch is similar to the headquarter model only without the DMZ.

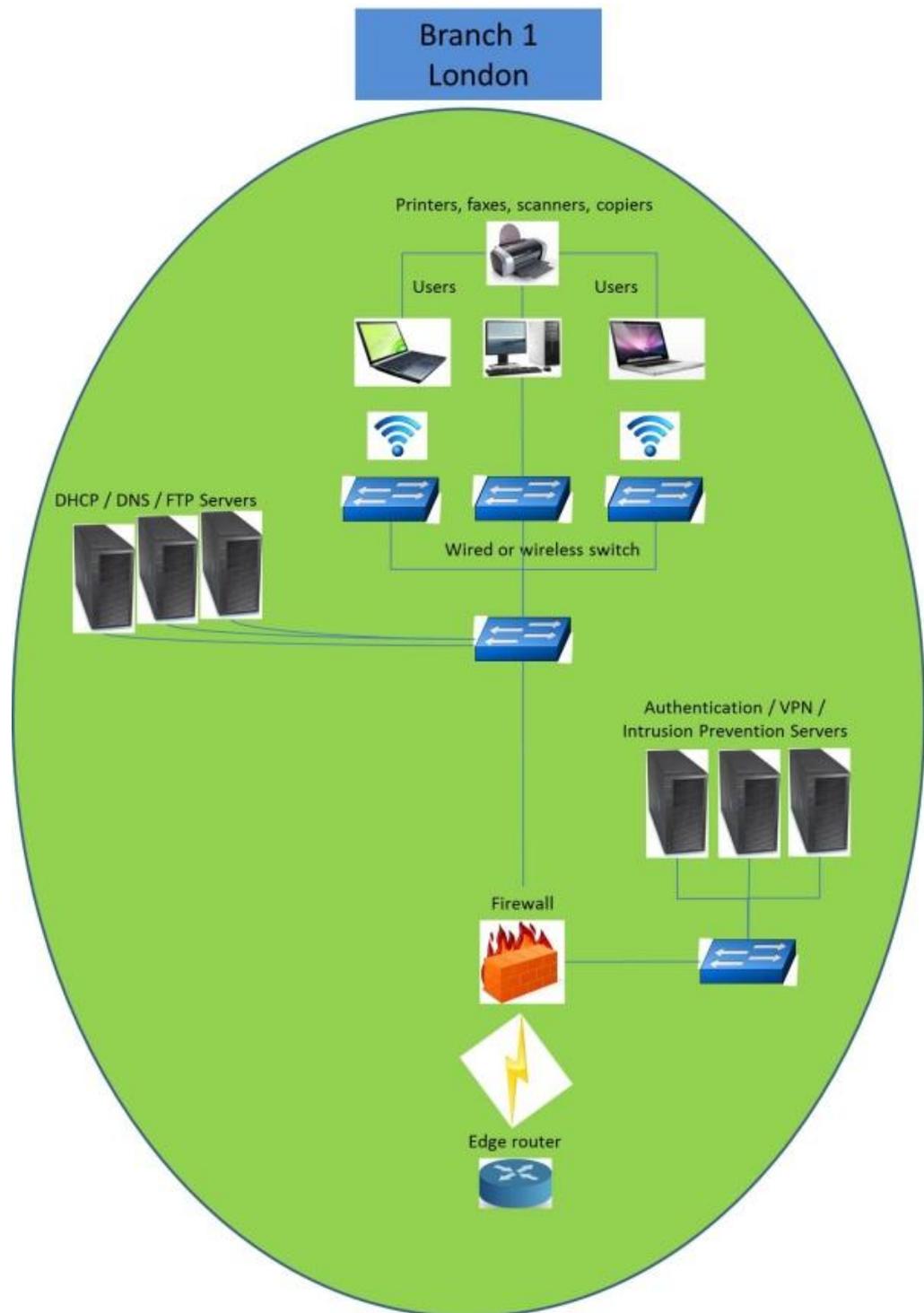


FIGURE 28. Branch 1 network structure model

Thirdly, the group of ISP routers with VPN users who perform the work outside the enterprise network still needs to get access to data from protected servers inside the network.

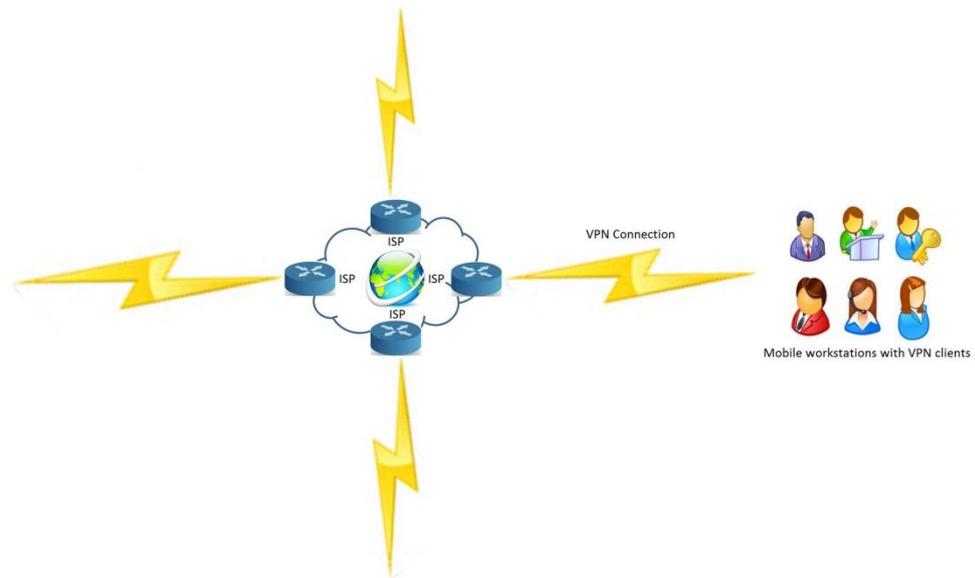


FIGURE 29. VPN users

And finally, the total enterprise network model is presented in Figure 30 below.

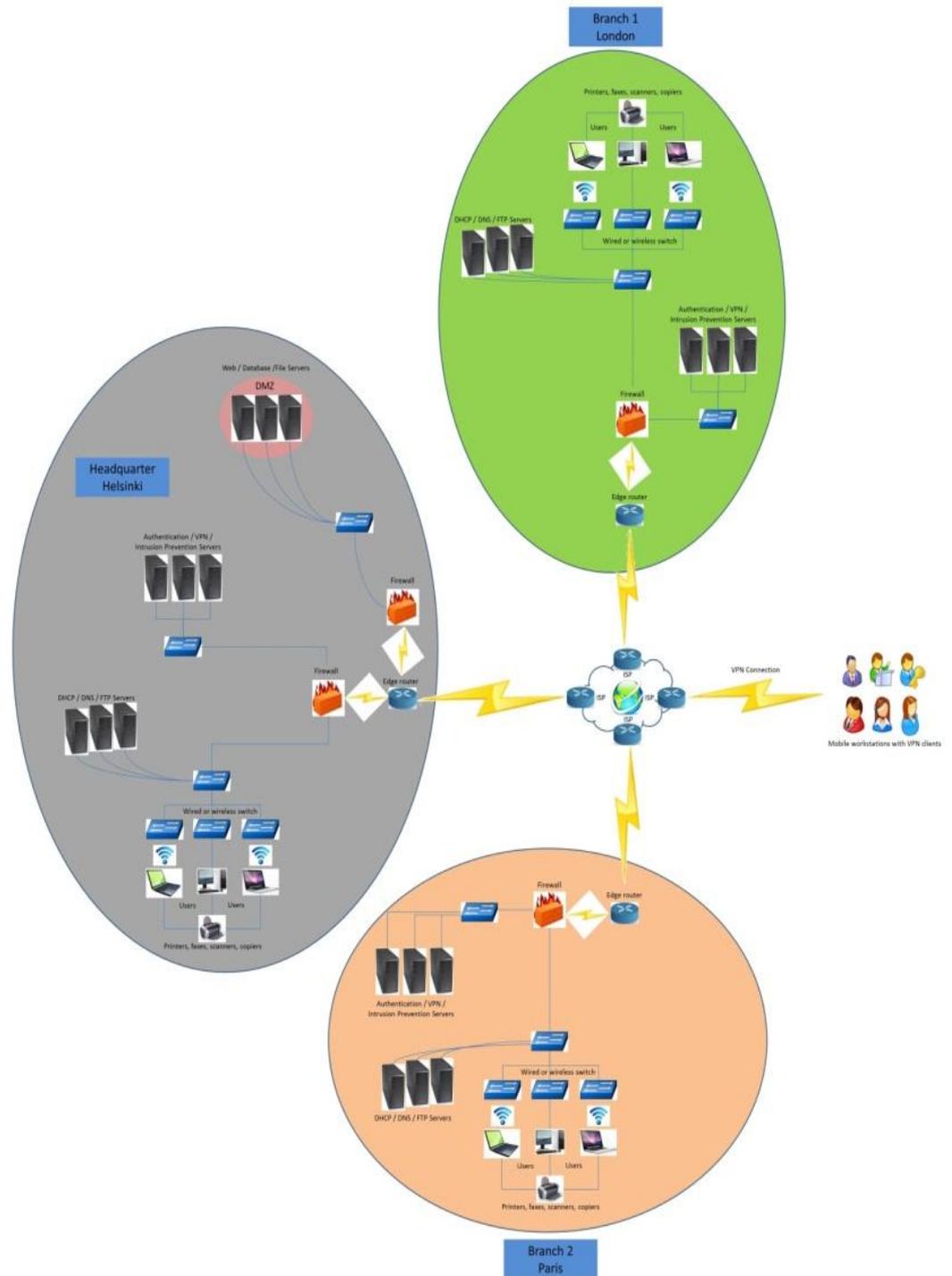


FIGURE 30. The whole network structure model

8.3 Addressing Plan

Although the model includes one headquarters, two branches, and VPN group, in the scope of the implementation, we only set addressing plans for the headquarters, edge routers and ISP routers to simulate the network. For the other two branches, the practice can be applied similarly.

There are two kinds of addresses: static and dynamic. Statically public addresses are often assigned for main computers, servers, and routers to make it stable so that other end devices can establish connection to perform various activities such as accessing data storage, uploading information, downloading file, etc. Dynamic addresses are distributed for client devices to join the enterprise network.

Therefore, in our network model, we also set the static and public addressing plan for headquarter as listed below:

Group 1 (DMZ):

	IPv4	IPv6
Database server	194.195.196.1/16	2001:ABCD::C2C3:C401/32
Web server	194.195.196.2/16	2001:ABCD::C2C3:C402/32
Mail server	194.195.196.3/16	2001:ABCD::C2C3:C403/32

Group 2 (Authentication):

	IPv4	IPv6
Authentication server	10.12.13.1/8	FEC0:1234::5/48
Firewall server	10.12.13.2/8	FEC0:1234::6/48
VPN server	10.12.13.3/8	FEC0:1234::7/48

Group 3 (Service):

	IPv4	IPv6
DNS server	10.12.13.4/8	FEC0:1234::2/48
DHCPv4 server	10.12.13.5/8	FEC0:1234::3/48
FTP server	10.12.13.6/8	FEC0:1234::4/48

Group 4 (Client):

DHCPv4 Pool	DHCPv6 Pool
10.20.0.1/8 – 10.255.255.254/8	FEC0:1234::1/48 – FEC0:1234::FFFE/48

Headquarter Router:

	Network	Gateway
DMZ	Net 194.195.0.0/16	194.195.1.1/16
	Net 2001:ABCD::/32	2001:ABCD::C2C3:0101/32
Client Zone	Net 10.0.0.0/8	10.0.0.1/8
	Net FEC0:1234::/64	FEC0:1234::1/64
Internet Zone	Net 130.131.0.0/16	130.131.0.1/16
	Net 2001::/16	2001::C2C3:0001/64

London Router

	Network	Gateway
Internet Zone	Net 11.12.13.0/16	11.12.13.2/16
	Net 2001:1234::/32	2001:1234::B0C:0D02/32

Paris Router

	Network	Gateway
Internet Zone	Net 128.0.0.0/16	128.0.0.2/16
	Net 2001:D4D5::/32	2001:D4D5::1234:0001/32

8.4 Implementation Performance

8.4.1 Dynamic Host Configuration Protocol (DHCP)

DHCP is used to assign IP addresses automatically for end devices, such as laptops, desktops, and mobile phones when joining the network. In our model, as we apply the dual stack method, there would be one DHCPv4 for IPv4 distribution and one DHCPv6 for IPv6 assignment. Therefore, there will be a server in the “Service Provision” group to provide IPv4 for all devices in the “Client Zone” group and it will be configured as in Appendix 2. For the IPv6, although IPv6 resource is very large, we will apply the IPv6 unicast site-local address for the local clients to ensure security and better management. However, due to the limitation of the simulator program, the edge router will act as the DHCPv6 for the distribution of IPv6 to client devices and the configuration can be found in Appendix 3.

8.4.2 Open Shortest Path First (OSPF)

There are different distinct networks within a large system such as network for servers, network for clients, and network for security. As a result, a routing protocol is required to connect these networks together so that a user from client network can communicate with servers to get access to private information.

Among many routing protocols, we choose the OSPF, which known as a routing protocol for IP that operates mainly as a link-state protocol and it is very suitable for large enterprise networks because of its capability and interoperability. As in the enterprise network model, according to the dual stack transition, we would create and maintain two routing tables for IPv4 and IPv6 as in Appendix 3.

8.4.3 Border Gateway Protocol (BGP)

In order to build our model, we need to set up the Internet to enable the communications between the headquarters and branches. Therefore, we apply the BGP routing protocol, which is mainly used for core routers among autonomous system around the world. Most ISPs use this protocol to communicate with each other. The configuration of BGP for the simulation of Internet can be found in Appendix 3.

8.4.4 Virtual Private Network (VPN)

VPN is a private network that is used by nearly almost every large company to make it convenient for mobile employees but still ensure data safety via the Internet. As a result, we also simulate this group of users in our network model according to the Appendix 3.

8.4.5 Security Establishment

The most important matter in large networks is security, especially with the new IPv6 implementation. The security is achieved during the implementation process in the infrastructure to protect the system safe when using both IPv4 and IPv6. These acts can include setting usernames and passwords, applying network policies, encrypting data when sent and received, creating access list for better control and management. See Appendix 3 for more detail.

9 CONCLUSIONS

9.1 Overview

This part presents the whole thesis structure for better understanding of the study.

Chapter 1 introduced the topic of this study that was the method of transition from IPv4 to IPv6 that is best for large network enterprises.

Chapter 2 presented the research question, research objectives and research methods. The main purpose of this study was to find out the most practical transition method for enterprises with large network. This research question type is “solution” which requires a problem solving process. Therefore, design science method was applied. Hence, 7 guidelines of design science were followed strictly.

Chapter 3 concerned data collection method and data analysis. Since qualitative approach was used, qualitative data collection methods such as interviews with open-ended questions and document review were conducted. Content analysis was chosen as data analysis method since we analyzed a lot of technical papers on current transition methods. We need direct understanding of these papers as to what they said, what they instructed. Content analysis helped us to understand what is the nature of the text itself. It also helps with analyzing interview transcripts.

Chapter 4 was the literature review of IP, IPv4 and IPv6. The basic concept of IPs and their features were presented thoroughly in this chapter.

Chapter 5 analyzed data that had been collected via documents and interviews. Data were categorized into groups based on technical or managerial content. This chapter discussed network infrastructure of large enterprise networks and management issues on transition from IPv4 to IPv6.

Chapter 6 evaluated the three most current applicable methods of transition that were dual stack, translation and tunneling. These methods were evaluated according to data analyzed in chapter 5 to conclude the most suitable method that was dual stack.

Chapter 7 suggested several matters to consider when deploying IPv6 on both management scale and technical scale to make it efficient and profitable.

In chapter 8, an artifact was built to test the method. A model of an enterprise large network would be built in a virtual environment via simulation software. The chosen method was tested. This chapter contained detailed technical steps on how to apply dual stack method.

9.2 Research result

The first objective was to understand current IPv6 transition methods based on knowledge about IP in general as well as IPv4 and IPv6 in particular. The authors learned that global IPv4 free pool was completely exhausted now; the transition to IPv6 would be a must for near future. There are three transition methods that were most applied i.e. dual stack, translation and tunneling. Each of them has its own advantages and disadvantages.

The second objective was to analyze real life experiences of enterprises that had deployed IPv6. We learned that the reasons for starting IPv6 could be:

- Preparing for IPv4 shortage coming in near future
- Testing the transition process
- Better features
- Getting support from top executives on the project

On the other hand, some enterprises were not interested in IPv6 transition for the following reasons:

- Business is still going on well
- Training costs
- No instant advantages
- No solution from service providers
- No backward compatibilities

For those above reasons, dual stack seems to be the best method. It is flexible because it utilizes both IPv4 and IPv6 at the same time on routers and easy to handle. Translation method makes the network vulnerable, as the whole networks will collapse if something bad happens to the routers in the transition process. Tunneling adds more complications to network management and has troubles with security attacks, which will not make executives happy.

9.3 Recommendations

Understand the situation. Most companies are running well with IPv4. Although global free pool of IPv4 is exhausted, regional ISP still has a certain amount of IPv4 to provide. They won't have troubles until several years. What will come then? Developing countries with increasing numbers of new computers and devices connecting to the Internet will need their IPs, which will be IPv6. These countries are new markets which large international companies are aiming at. Being slow to adopt new technology will lead to losing access to these potential customers. Besides, IPv6 has new features that promise to bring better management and administration as well as improve security. Moreover, service providers who can offer enterprises services in transition obviously can make profit out of it.

Be prepared. In every project, the most vital part is to plan the implementation process. Proper budget must be considered in advance including planning, design, testing, deployment, personnel training and operational costs. Assessment of current network structure to outline architecture for an IPv6 project is important. Once the project is decided, IPv6 must be integrated into IT procurement. Even if it is decided not to deploy IPv6, still IPv6 support products should be integrated into product lifecycle replacement. The reason is that the network will still be able to communicate with IPv6 from the outside world and it makes the transition process much more fluent in case the organization needs to deploy IPv6 later on. Software or a system tailored for specific organization should be considered an IPv6 matter, as it is very difficult to change in the future. “*Prior preparation prevents poor performance*” (James Baker).

Pay attention to human factor. The human factor includes staffs of project teams and the operational administrator. Project team members must be people who really understand internal network structure because they will decide which method of transition to apply. Choosing the right method will avoid many troubles for administration. The operational administrator must be the one who has knowledge of IPv6. As mentioned before, in the case of FPT Telecom in Vietnam, after IPv6 deployment, the administrator didn't really know IPv6, which increased the cost of staff training and decreased effectiveness of the project.

9.4 Methodology

The thesis followed seven guidelines of design science method. It was an inductive study looking for a solution to a problem. The interviews in this study were conducted with people who are involved in IPv6 deployment projects in large network enterprises in Vietnam and Finland. Therefore, they can answer the questionnaire with their practical experiences.

Additionally, document review was essential for this study since this thesis concerned a lot of technical issues and evaluated situations based on existing techniques, which were documented in various published sources. It was

important to study documents on technical experiences of previous projects as well as new technology coming.

Content analysis was the right choice for analyzing those documents and interviews' transcripts.

9.5 Limitation and Further Study

The first limitation of this study is that, there were only 4 large network enterprises interviewed. The authors tried to contact as many large enterprises in Finland and Vietnam who had deployed IPv6 as possible. Unfortunately, very few answered back and helped. Half of enterprises that answered back had successfully carried out IPv6 project while the other half had failed. Therefore, the authors could analyze reasons for the success as well as failure to find out the best method.

This study was limited to large enterprises that had a network size of over 1000 computers. Consequently, the research results may not be true for smaller network.

Finally, there are various areas for further study based on this thesis. Firstly, a study with a larger sample or more cases could be done for better results. Another topic could be transition method for small and medium network enterprises. Or it is possible to find the critical factors for the failure of IPv6 deployment in general or large network size enterprises in particular (or small and medium sized ones). Additionally, further study on IPv6 for mobile devices can be considered.

REFERENCES

- Afuah, Allan, and Christopher L. Tucci. *Internet Business Models and Strategies: Text and Cases*. Irwin/McGraw-Hill, 2001.
- Alan R. Hevner, Salvatore T. March, Jinsoo Park, Sudha Ram. *Design Science in Information System Research*. MIS Quarterly.
- ARIN. *American Registry for Internet Numbers*. 11 30, 2010.
https://www.arin.net/knowledge/v4_deplete_v6_adopt.ppt (accessed October 23, 2011).
- Armitage, Grenville. *Quality of Service in IP Networks*. Sams, 2000.
- Arora, Pankaj, and Kiren Desai. *Security Features of IPv6*. San Jose University, 2008.
- Balchunas, Aaron. *Router Alley*. 2007. <http://www.routeralley.com/ra/docs/osi.pdf> (accessed December 6, 2011).
- Banks, Ethan. *Packet Pusher*. September 29, 2011. <http://packetpushers.net/the-reason-enterprises-arent-deploying-ipv6/> (accessed December 8, 2011).
- Bi, Jun, Jianping Wu, and Xiaoxiang Leng. "IPv4/IPv6 Transition Technologies and Univer6 Architecture." *IJCSNS International Journal of Computer Science and Network Security*, 2007: VOL.7 No.1.
- Blank, Tekijät Andrew G. *TCP/IP Foundations*. SYBEX Inc., 2004.
- Bouras, C., A. Karaliotas, and P. Ganos. "The development of IPv6 in an IPv4 world as transition strategies." *Internet Research*, Vol. 13 Iss: 2, 2003: 86-93.
- Bowen, Glenn. "Document Analysis as a Qualitative Research Method." *Qualitative Research Journal*, 2009: vol. 9, no. 2.
- BusinessDictionary. *BusinessDictionary*.
<http://www.businessdictionary.com/definition/readiness.html> (accessed November 5, 2011).

Cerf, Vincent. "How the Internet Came to Be." 1993.

Chen, Maokel, Xin Liu, Cheng Yan, and Hui Huang. "IPv6 Tunnel Broker Design and Implementation." Beijing, March 11, 2002.

Cho, Kenjiro, Matthew Luckie, and Bradley Huffaker. "Identifying IPv6 network problems in the dual-stack world." SIGCOMM 2004, September 2004.

Cisco. "Cisco IOS Network address translation." CISCO. 2004.

http://www.cisco.com/en/US/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.pdf (accessed November 15, 2011).

Cisco. *IPv6 Addressing Guide*. 2010 йил 1-12.

Cisco. *The ABCs of IP version 6*. February 20, 2010.

Corbin, Juliet M., and Anselm L. Strauss. *Basic of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage Publications, Inc., 2008.

Daniel G. Waddington, Fangzhe Chang. "Realizing the Transition to IPv6." *IEEE Communications Magazine*, 2002: 139.

Das, Kaushik. *IPv6*. 2008. <http://ipv6.com/index.htm> (accessed December 3, 2011).

Davies, Joe. *Microsoft Technet*. August 15, 2002. <http://technet.microsoft.com> (accessed September 20, 2011).

Davis, G, and M Olson. *Management Information Systems: Conceptual Foundations Structure and Development, Second Ed*. Boston: McGraw-Hill, Inc., 1985.

Deering, S., and R. Hinden. *Internet Protocol Version 6 Specification*. The Internet Society, 1998.

Ford, Merilee, H. Kim Lew, Steve Spanier, and Tim Stevenson. *Internetworking Technology Overview, Second Edition*. Cisco Systems, Inc., 1999.

Gary B. Shelly, Misty E. Vermaat. *Discovering Computers: Your Interactive Guide to the Digital World*. United States of America: COURSE TECHNOLOGY, CENGAGE Learning, 2012.

Golafshani, Nahid. "Understanding reliability and validity in qualitative research." *The Qualitative Report*. Toronto, Canada: <http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf>, December 2003.

H3C. *H3C Technologies Co., Limited*. 2003. http://www.h3c.com/portal/res/201108/15/20110815_1239983_image005_722543_1285_0.png (accessed October 19, 2011).

Hagen, Silvia. *IPv6 Essentials*. O'Reilly Media, Inc., 2006.

Henderson, J, and N Venkatraman. "Strategic Alignment: Leveraging Information Technology for Transforming Organizations." *IBM Systems Journal*, 1993.

Hevner, Alan R., Salvatore T. March, Jinsoo Park, and Sudha Ram. "Design Science in Information Systems Research." *MIS Quarterly*, 2004.

Hirorai, R., and H. Yoshifuji. "Problems on IPv4 - IPv6 network transition." IntecNetCore, Inc., February 13, 2006.

Huang, Shiang-Ming, Wu Quincy, and Yi-Bing Lin. "Tunneling IPv6 through NAT with Teredo mechanism." Taiwan: National Chiao Tung University, April 25, 2005.

Huston, Geoff. "The Changing Foundation of the Internet: Confronting IPv4 Address Exhaustion." *The ISP Column: A monthly column on things Internet*, October 2008.

IBM. *IBM Corporation*. 2008. <http://www.ibm.com/us/en/> (accessed 10 12, 2011).

InSites. "CLIP - Communities of Learning, Inquiry, and Practice." *InSites*. 5 2007. http://www.insites.org/CLIP_v1_site/downloads/PDFs/TipsQualQuanMthds.4B.8-07.pdf (accessed November 21, 2011).

InternetProtocols. *FabCentral*.

<http://fab.cba.mit.edu/classes/MIT/961.04/people/neil/ip.pdf> (accessed December 5, 2011).

Israel, Barbara A., Eugenia Eng, Amy J. Achulz, and Edith A. Parker. *Methods in Community-Based Participatory Research for Health*. John Wiley & Sons, Inc., 2005.

Janitor, J., F. Jakab, and K. Knieward. "Visual Learning Tools for Teaching/Learning Computer Networks: Cisco Networking Academy and Packet Tracer." *Networking and Services (ICN), 2010 Sith International Conference*, 2010: 351-355.

Jim Kurose, Keith Ross. *Computer Networking: A top Down Approach, 5th edition*. Addison-Wesley, 2007.

Johnson, B, and L Christensen. *Educational research: Quantitative, qualitative, and mixed approaches*. California: Thousand Oaks, CA: Sage Publications, 2008.

Johnson, B.R. "Examining the validity structure of qualitative research." *Education*, 1997: 282-292.

Jude, Mike. *SearchTelecom*. August 2010.

<http://searchtelecom.techtarget.com/feature/Without-killer-IPv6-services-in-the-mix-consumers-arent-IPv6-ready> (accessed December 8, 2011).

Keil, M. "Pulling the Plug: Software Project Management and the Problem of Project Escalation." *MIS Quarterly*, 1995: 421-447.

Keil, M, and M Robey. "Turning Around Troubled Software Projects: An Exploratory Study of Deescalation of Commitment to Failing Courses of Action." *Journal of Management Information Systems*, 1999: 63-87.

Keil, M, P.E Cule, K Lyytinen, and R.C Schmidt. "A Framework for Identifying Software Project Risks." *Communications of the ACM*, 1998: 76-83.

Kozierok, Charles M. *The TCP/IP Guide: A Comprehensive, illustrated internet protocols reference*. San Francisco: No Starch Press, 2005.

- Krikorian, Raffi. *O'Reilly - ONLamp.com*. June 12, 2003.
http://www.oreillynet.com/onlamp/blog/2003/06/what_ever_happened_to_ipv5.html (accessed 12 5, 2011).
- Labuschagne, Adri. "Qualitative Research - Airy Fairy or Fundamental." *The Qualitative Report*, March 2003.
- Lee, A. "Inaugural Editor's Comments." *MIS Quarterly*, March 1999: pp. v-xi.
- Leiner, Barry M., et al. "A Brief History of the Internet." *ACM SIGCOMM Computer Communication Review, Volume 39, Number 5*, October 2009: 22-31.
- Lichtman, M. *Qualitative research in education: A user's guide*. Thousand Oaks, CA: Sage Publication, 2006.
- Lincoln, Y.S, and E.G Guba. *Naturalistic inquiry*. Beverly Hill: CA: Sage Publications, Inc., 1985.
- Lowe, Doug. *Networking for Dummies, 7th Edition*. Indiana: Wiley Publishing, Inc., 2005.
- Mackay, Michael, and Christopher Edwards. "Transitioning from IPv4 to IPv6 - A Technical Overview." Lancaster: Computing Department, Faculty of Applied Sciences, Lancaster University.
- Microsoft. "Introduction to IP Version 6." Microsoft Corporation, January 2008.
- . *Microsoft Technet*. 01 21, 2005. <http://technet.microsoft.com/> (accessed 10 13, 2011).
- . *Technet*. January 1, 2012. <http://i.technet.microsoft.com/dynimg/IC348167.gif> (accessed January 22, 2012).
- . *TechNet Library*. 2011. [http://technet.microsoft.com/en-us/library/cc772973\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772973(WS.10).aspx) (accessed October 15, 2011).
- Middleton, James. *Telecoms*. July 13, 2011.
<http://www.telecoms.com/30695/ipv6-transition-stalled-by-lack-of-motivation/> (accessed 12 9, 2011).

Mitchell, Bradley. *About*.

<http://compnetworking.about.com/od/workingwithipaddresses/l/aa042400b.htm>
(accessed October 15, 2011).

Nakajima, Masaki, and Nobumasu Kobayashi. "IPv4/IPv6 Translation Technology." *FUJITSU sci. Tech. J.*, 2004: 159-169.

Narten, T. *Neighbor discovery and stateless autoconfiguration in IPv6*. IEEE Computer Society, 1999.

Netnam Ltd. *Tunnel Broker*. 2011.

http://tunnelbroker.netnam.vn/media/upload/tunnel_broker_medium.png
(accessed January 5, 2012).

Nokia. *Developer*.

http://library.developer.nokia.com/topic/S60_3rd_Edition_Cpp_Developers_Library/GUID-D81EAF75-EF8C-4B62-8866-439E29325E8A_d0e11389_href.png
(accessed December 10, 2011).

Odom, Wendell, Rus Healy, and Denise Donohue. *CCIE Routing and Switching Certification Guide*. Cisco Press, 2009.

Oracle. 2010. <http://www.oracle.com> (accessed 10 13, 2011).

Oracle Corporation. *Oracle*. 2001. <http://docs.oracle.com/cd/E19455-01/806-0916/images/dual.epsi.gif> (accessed December 19, 2011).

OSI. *Freesoft*. <http://www.freesoft.org/CIE/Topics/15.htm> (accessed December 6, 2011).

Palmquist, Mike. "ischool."

<http://www.ischool.utexas.edu/~palmquis/courses/content.html> (accessed December 3, 2011).

Penhoat, Joel, Olivier Le Grand, Orange Labs, Mikael Salaun, and Tayeb Lemlouma. *Definition and analysis of a Fixed Mobile Convergent architecture for enterprise VoIP services*. IGI Globle, 2011.

Qing-weil, Shen, and Zhang Lin. *Analysis of IPv4/IPv6 Transition Technology Based on Tunnel*. Anhui: Anhui Institute of Aechitecture and Industry, 2007.

Raicu, I., and S. Zeadally. "Evaluating IPv4 to IPv6 transition mechanisms." Dept. of Cumpnut. Sci., Purdue University, April 02, 2003.

RFC2373. *IETF*. July 1998. <http://tools.ietf.org/html/rfc2373> (accessed November 10, 2011).

RFC2647. *IETF*. August 1999. <http://www.ietf.org/rfc/rfc2647.txt> (accessed October 17, 2011).

RFC2765. "IETF." *IETF*. February 2000. <https://tools.ietf.org/html/rfc2765> (accessed December 18, 2011).

RFC2766. "IETF." *IETF*. February 2000. <https://tools.ietf.org/html/rfc2766> (accessed December 19, 2011).

RFC2767. *IETF*. February 2000. <https://tools.ietf.org/html/rfc2767> (accessed December 19, 2011).

RFC3022. "IETF." *IETF*. January 2001. <http://www.ietf.org/rfc/rfc3022.txt> (accessed October 17, 2011).

RFC4057. *IETF*. June 2005. <http://tools.ietf.org/html/rfc4057> (accessed November 10, 2011).

RFC4861. *IETF*. September 2007. <http://art.tools.ietf.org/html/rfc4861> (accessed October 17, 2011).

RFC5735. "IETF." *IETF*. January 2010. <http://tools.ietf.org/html/rfc5735> (accessed October 15, 2011).

RFC6343. *IETF*. August 2011. <https://tools.ietf.org/html/rfc6343> (accessed December 23, 2011).

RFC791. "IETF." *IETF*. September 1981. <http://tools.ietf.org/html/rfc791> (accessed November 19, 2011).

Rubin, Herbert, and Irene Rubin. *Qualitative Interviewing: The Art of Hearing Data*. Sage Publications, Inc., 1995.

Schwankert, Steven. *Sound the alarm, IPv6 execs say*. Aapril 16, 2008.

<http://www.infoworld.com/%5Bprimary-term-alias-prefix%5D/%5Bprimary-term%5D/sound-the-alarm-ipv6-exec-say-422> (accessed December 8, 2011).

Subramanian, Saisree. *IPv6 Transition strategies*. November 2003.

TCPIPGuide. *The TCP/IP Guide*. September 20, 2005.

http://www.tcpipguide.com/free/t_IPv6MotivationandOverview-3.htm (accessed November 16, 2011).

TechTerms. *TechTerms*. <http://www.techterms.com/definition/> (accessed December 12, 2011).

TechWeb. *The business technology network*. April 20, 2009.

<http://i.cmpnet.com/networksystemsdesignline/2006/o4/IPv6Figure4.gif> (accessed November 15, 2011).

Turner, Daniel W. "Qualitative Interview Design: A Practical Guide for Novice Investigators." *The Qualitative Report, Volume 15 Number 3*, 2010 йил May: 754-760.

Tyson, Jeff. *HowStuffWorks*. February 02, 2001.

<http://www.howstuffworks.com/nat.htm> (accessed November 14, 2011).

University of Wisconsin-Eau Claire. *University of Wisconsin-Eau Claire - People Pages*.

<http://people.uwec.edu/piercech/ResearchMethods/Data%20collection%20methods/DATA%20COLLECTION%20METHODS.htm> (accessed November 20, 2011).

Venkatesh, Viswanath. "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into Technology Acceptance Model." *Information Systems Research*, 2000: 342-365.

Vienna University of Technology. *Institute of Telecommunications*. January 10, 2012. <http://www.ibk.tuwien.ac.at/~ipv6/images/siit.png> (accessed January 22, 2012).

VoIP. *FCC - Federal Communications Commission*. February 01, 2010. <http://transition.fcc.gov/voip/> (accessed October 18, 2011).

Waddington, D.G., and Fangzhe Chang. "Realizing the transition to IPv6." *Communications Magazine*, Vol. 40 Iss: 6, 2002: 138-147.

Weber, Robert Philip. *Basic Content Analysis*. Sage Publications, Inc., 1990.

Wedel, Fachhochschule. *FHWedel University of Applied Sciences*. 2008. http://www.fh-wedel.de/~si/seminare/ws08/Ausarbeitung/08.ipv6/images/dstm_konzept.png (accessed December 23, 2011).

Yin, Robert K. *Qualitative Research from Start to Finish*. New York: The Guilford Press, 2011.

APPENDICES

APPENDIX 1: Questionnaire

1. Does your business involve in online operations (transaction, marketing, recruitment, communication)?
2. How much is the total IT expenditure in particular account (in percent) of your organization's total expenditure?
3. How large is your current computer network? (Number of computers/users/servers)
4. What are the main reasons for deploying IPv6 in the organization's network?
5. What is the expected budget that your organization would be willing to spend for the transmission from IPv4 to IPv6?
6. Which factors that initiated the IPv6 project?
7. What was the method of transmission chosen to be applied?
8. Are there any problems during the implementation? If possible, could you tell what they are?
9. Which factors needed to be prepared for the implementation?
10. If the implementation of IPv6 was successful, what is the most important factor? Are there any advantages that the organization gets after deploying IPv6?
11. If the implementation was failed, could you tell what the main reasons were?
Will your organization consider re-implementing IPv6?
12. Would you consider deploying IPv6 if there is a complete solution? What do you expect from this solution?

APPENDIX 2: List of RFCs used in this thesis

- RFC 2373 IP Version 6 Addressing Architecture. R. Hinden, S. Deering. July 1998. (Format: TXT=52526 bytes) (Obsoletes RFC1884) (Obsoleted by RFC3513) (Status: PROPOSED STANDARD)
- RFC2647 Benchmarking Terminology for Firewall Performance. D. Newman. August 1999. (Format: TXT=45374 bytes) (Status: INFORMATIONAL)
- RFC2765 Stateless IP/ICMP Translation Algorithm (SIIT). E. Nordmark. February 2000. (Format: TXT=59465 bytes) (Obsoleted by RFC6145)(Status: PROPOSED STANDARD)
- RFC2766 Network Address Translation - Protocol Translation (NAT-PT). G. Tsirtsis, P. Srisuresh. February 2000. (Format: TXT=49836 bytes) (Obsoleted by RFC4966) (Updated by RFC3152) (Status: HISTORIC)
- RFC2767 Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS). K. Tsuchiya, H. Higuchi, Y. Atarashi. February 2000. (Format: TXT=26402 bytes) (Status: INFORMATIONAL)
- RFC3022 Traditional IP Network Address Translator (Traditional NAT). P. Srisuresh, K. Egevang. January 2001. (Format: TXT=37675 bytes)(Obsoletes RFC1631) (Status: INFORMATIONAL)
- RFC4057 IPv6 Enterprise Network Scenarios. J. Bound, Ed.. June 2005. (Format: TXT=33454 bytes) (Status: INFORMATIONAL)

- RFC4861 Neighbor Discovery for IP version 6 (IPv6). T. Narten, E. Nordmark, W. Simpson, H. Soliman. September 2007. (Format: TXT=235106 bytes) (Obsoletes RFC2461) (Updated by RFC5942) (Status: DRAFF STANDARD)
- RFC5735 Special Use IPv4 Addresses. M. Cotton, L. Vegoda. January 2010. (Format: TXT=20369 bytes) (Obsoletes RFC3330) (Also BCP0153) (Status: BEST CURRENT PRACTICE)
- RFC6343 Advisory Guidelines for 6to4 Deployment. B. Carpenter. August 2011. (Format: TXT=51496 bytes) (Status: INFORMATIONAL)
- RFC791 Internet Protocol. J. Postel. September 1981. (Format: TXT=97779 bytes) (Obsoletes RFC0760) (Updated by RFC1349) (Also STD0005)(Status: STANDARD)

APPENDIX 3: Detail steps to configure network according to model built in chapter 8

OSPFv2 for IPv4

- Goal: Establishing OSPFv2 routing protocol for IPv4
- Detail steps:

```
R_Head>enable
R_Head#configure terminal
R_Head(config)# router ospf 1
R_Head(config-router)# network 10.0.0.0      0.0.0.255 area 0
R_Head(config-router)# network 194.195.0.0  0.0.0.0 area 0
R_Head(config-router)# network 130.131.0.0  0.0.255.255 area 0
```

- OSPFv2 verification:

```
R_Head#show ip ospf

  Routing Process "ospf 1" with ID 194.195.1.1

  Supports only single TOS(TOS0) routes

  Supports opaque LSA

  SPF schedule delay 5 secs, Hold time between two SPFs 10
secs

  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

  Number of external LSA 0. Checksum Sum 0x000000

  Number of opaque AS LSA 0. Checksum Sum 0x000000

  Number of DCbitless external and opaque AS LSA 0

  Number of DoNotAge external and opaque AS LSA 0

  Number of areas in this router is 1. 1 normal 0 stub 0
nssa

  External flood list length 0

    Area BACKBONE(0)

      Number of interfaces in this area is 3

      Area has no authentication

      SPF algorithm executed 2 times

      Area ranges are

      Number of LSA 1. Checksum Sum 0x00ca9d

      Number of opaque link LSA 0. Checksum Sum
0x000000

      Number of DCbitless LSA 0

      Number of indication LSA 0

      Number of DoNotAge LSA 0

      Flood list length 0
```

```
R_Head#show protocols
```

```
Global values:
```

```
Internet Protocol routing is enabled
```

```
FastEthernet0/0 is up, line protocol is up
```

```
Internet address is 10.0.0.1/8
```

```
FastEthernet0/1 is up, line protocol is up
```

```
Ethernet1/0 is up, line protocol is up
```

```
Internet address is 194.195.1.1/16
```

```
Ethernet1/1 is up, line protocol is up
```

```
Internet address is 130.131.0.1/16
```

```
Vlan1 is administratively down, line protocol is down
```

- Unit testing:
 - Ping from client computer to database server

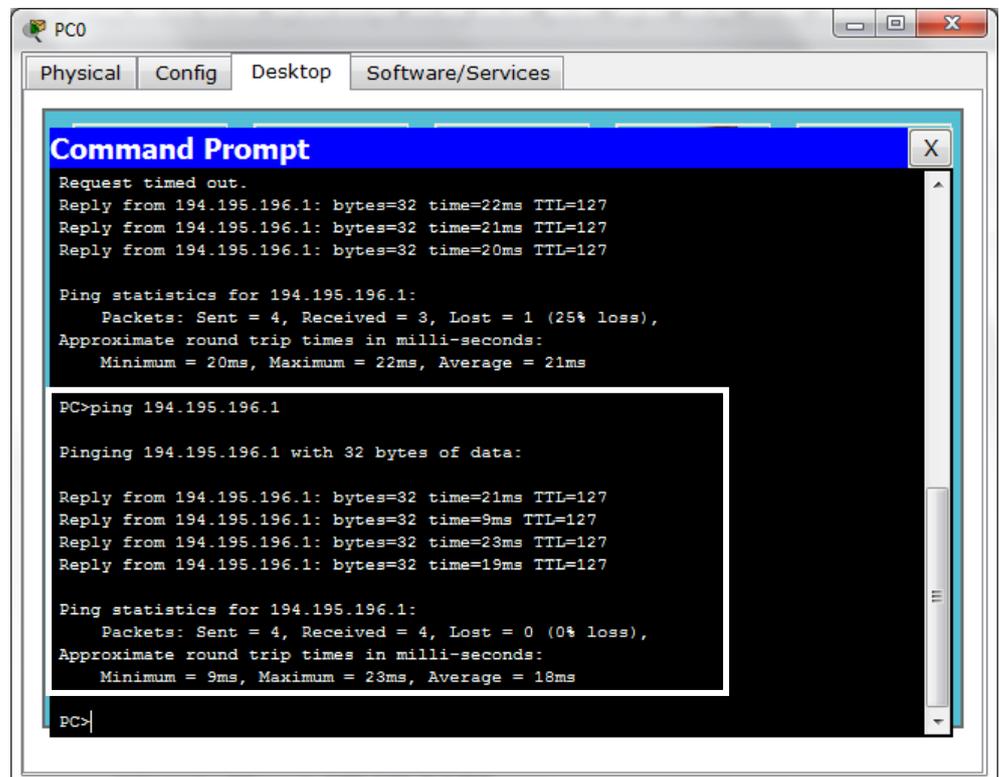


FIGURE 31. Ping from client computer to database server

- Ping from DHCP server to client laptop

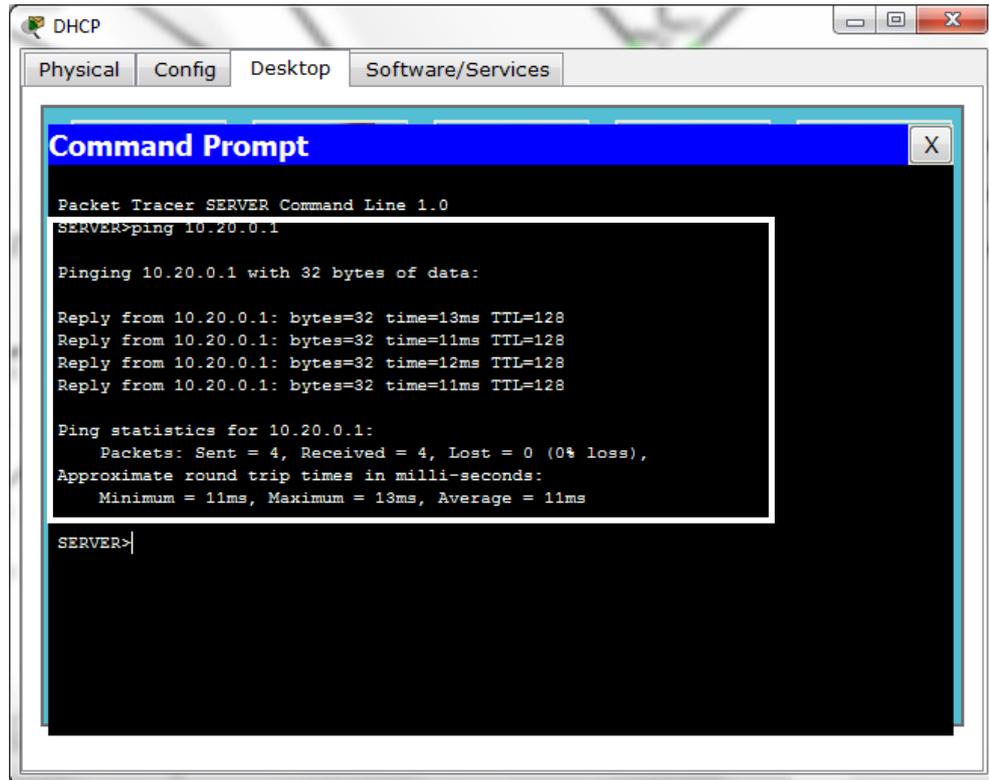


FIGURE 32. Ping from DHCP server to client laptop

From those results above, we have successfully implemented the OSPFv2 routing protocol for IPv4 to establish the internal communication among clients and servers.

OSPFv3 for IPv6

- Goal: Establishing OSPFv2 routing protocol for IPv4
- Detail steps:

```
R_Head>enable
R_Head#configure terminal
R_Head(config)#interface fastEthernet 0/0
R_Head(config-if)#ipv6 ospf 1 area 0
R_Head(config-if)#interface fastEthernet 0/1
R_Head(config-if)#ipv6 ospf 1 area 0
R_Head(config-if)#interface Ethernet 1/0
R_Head(config-if)#ipv6 ospf 1 area 0
R_Head(config-if)#interface Ethernet 1/1
R_Head(config-if)#ipv6 ospf 1 area 0
```

- OSPFv3 verification:

```
R_Head#show ipv6 route
```

```
IPv6 Routing Table - 5 entries
```

```
Codes: C - Connected, L - Local, S - Static, R -  
RIP, B - BGP
```

```
U - Per-user Static route, M - MIPv6
```

```
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS  
interarea, IS - ISIS summary
```

```
O - OSPF intra, OI - OSPF inter, OE1 - OSPF  
ext 1, OE2 - OSPF ext 2
```

```
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
D - EIGRP, EX - EIGRP external
```

```
C 2001:ABCD::/32 [0/0]
```

```
via ::, Ethernet1/0
```

```
L 2001:ABCD::C2C3:101/128 [0/0]
```

```
via ::, Ethernet1/0
```

```
C FEC0:1234::/64 [0/0]
```

```
via ::, FastEthernet0/0
```

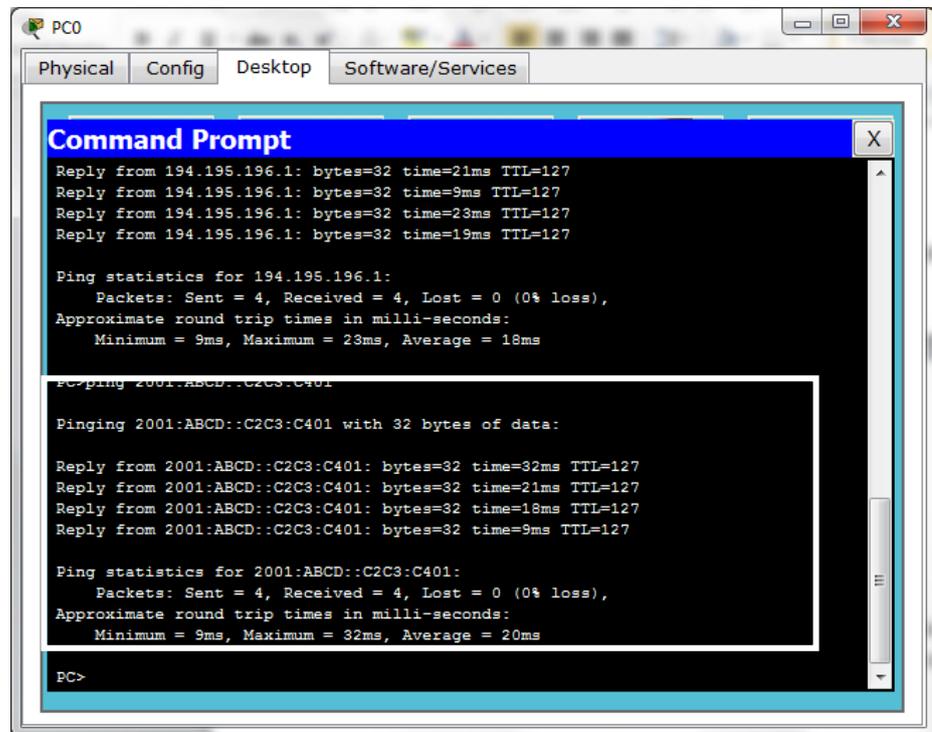
```
L FEC0:1234::1/128 [0/0]
```

```
via ::, FastEthernet0/0
```

```
L FF00::/8 [0/0]
```

```
via ::, Null0
```

- Unit testing:
 - Ping from client computer to database server with IPv6



```
PCO
Physical Config Desktop Software/Services

Command Prompt
Reply from 194.195.196.1: bytes=32 time=21ms TTL=127
Reply from 194.195.196.1: bytes=32 time=9ms TTL=127
Reply from 194.195.196.1: bytes=32 time=23ms TTL=127
Reply from 194.195.196.1: bytes=32 time=19ms TTL=127

Ping statistics for 194.195.196.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 23ms, Average = 18ms

PC>ping 2001:ABCD::C2C3:C401

Pinging 2001:ABCD::C2C3:C401 with 32 bytes of data:

Reply from 2001:ABCD::C2C3:C401: bytes=32 time=32ms TTL=127
Reply from 2001:ABCD::C2C3:C401: bytes=32 time=21ms TTL=127
Reply from 2001:ABCD::C2C3:C401: bytes=32 time=18ms TTL=127
Reply from 2001:ABCD::C2C3:C401: bytes=32 time=9ms TTL=127

Ping statistics for 2001:ABCD::C2C3:C401:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 32ms, Average = 20ms

PC>
```

FIGURE 33. Ping from client computer to database server with Ipv6

- Ping from client computer to database server with IPv6

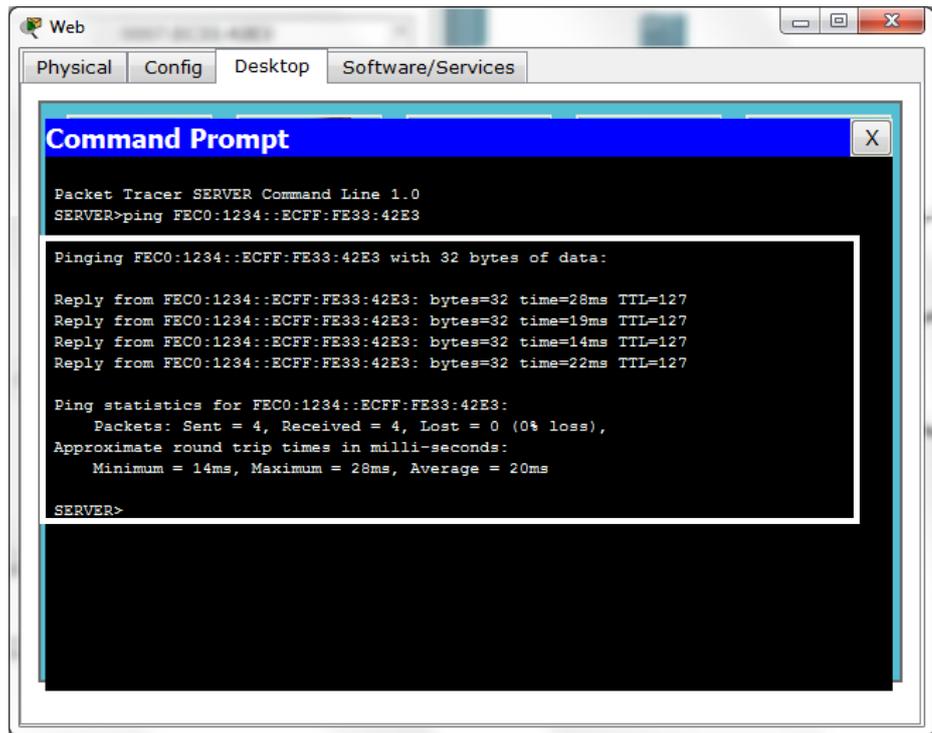


FIGURE 34. Ping from client computer to database server with IPv6

Based on the test results and the routing table in the verification part, we have achieved the goal of establishing OSPFv3 for IPv6 on each interface.

DHCP IPv4

In the DHCP server, we configure address pool as depicted in the below picture:

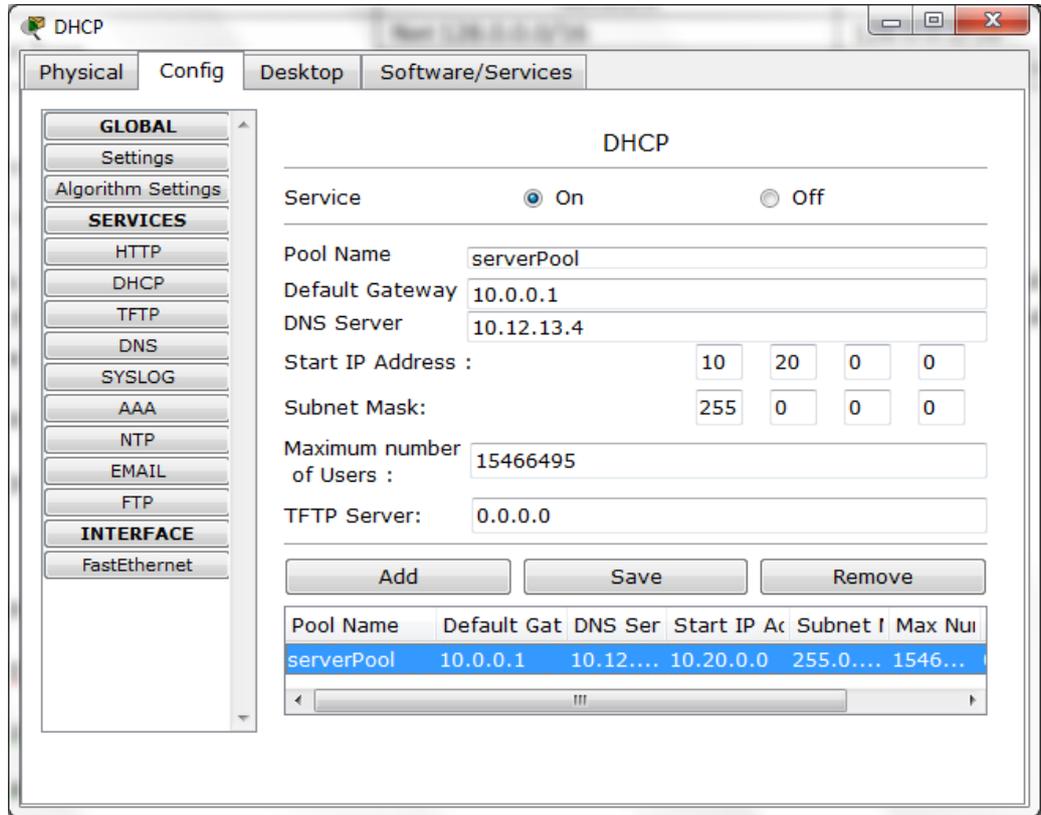


FIGURE 35. DHCPv4 Configuration

DHCP IPv6

- Goal: Configuring IPv6 address pool
- Detail steps:

```
Router#configure terminal
Router (config)#hostname R_Head
R_Head (config)#ipv6 unicast-routing
R_Head (config)#ipv6 dhcp pool head
R_Head (config-dhcp)#prefix-delegation pool head-pool1
lifetime 1800 600
R_Head (config-dhcp)#dns-server FEC0:1234::2
R_Head (config-dhcp)#domain-name enterprise.com
R_Head (config-dhcp)#exit
R_Head (config)#interface fastethernet0/0
R_Head (config-if)#ip address 10.0.0.1 255.0.0.0
R_Head (config-if)#ipv6 address FEC0:1234::1/64
R_Head (config-if)#ipv6 enable
R_Head (config-if)#ipv6 dhcp server head
R_Head (config-if)#exit
R_Head (config)#ipv6 local pool head-pool1 FEC0:1234::/40
48
```

- DHCPv6 Verification:

```
R_Head#show ipv6 dhcp pool
```

```
Results as following
```

```
    DHCPv6 pool: dhcpv6
```

```
    Prefix pool: dhcpv6-pool1
```

```
                                preferred lifetime 1800, valid  
lifetime 600
```

```
    DNS server: FEC0:1234::2
```

```
    Domain name: enterprise.com
```

```
    Active clients: 0
```

```
R_Head#show running-config

Building configuration...

Current configuration : 711 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R_Head
!
ipv6 unicast-routing
!
ipv6 dhcp pool dhcpv6
  prefix-delegation pool dhcpv6-pool1 lifetime 1800 600
  dns-server FEC0:1234::2
  domain-name enterprise.com
!
ipv6 local pool dhcpv6-pool1 FEC0:1234::/40 48
!
interface FastEthernet0/0
  ip address 10.0.0.1 255.0.0.0
  duplex auto
  speed auto
  ipv6 address FEC0:1234::2/64
  ipv6 dhcp server dhcpv6
```

Based on the results in verification step, we have successfully set up the IPv6 address pool ranging from FEC0:1234::1/48 – FEC0:1234::FFFE/48 through the interface fast Ethernet 0/0 with the IPv6 address FEC0:1234::2/64.

Border Gateway Protocol (BGP)

- Goal: Establish BGP routing protocols for 4 ISP routers to simulate the Internet.
- Detail steps to establish BGP
 - ISP1's router:

```
ISP1>enable
ISP1#configure terminal
ISP1(config)#router bgp 100
ISP1(config-router)#bgp log-neighbor-changes
ISP1(config-router)#neighbor 14.15.16.2 remote-as 200
ISP1(config-router)#neighbor 140.130.120.2 remote-as 300
ISP1(config-router)#network 130.131.0.0 mask 255.255.0.0
```

- ISP2's router:

```
ISP2>enable
ISP2#configure terminal
ISP2(config)#router bgp 200
ISP2(config-router)#bgp log-neighbor-changes
ISP2(config-router)#neighbor 14.15.16.1 remote-as 100
ISP2(config-router)#neighbor 129.130.131.2 remote-as 400
ISP2(config-router)#network 11.0.0.0 mask 255.0.0.0
```

- ISP3's router:

```
ISP3>enable
ISP3#configure terminal
ISP3(config)#router bgp 300
ISP3(config-router)#bgp log-neighbor-changes
ISP3(config-router)#neighbor 140.130.120.1 remote-as 100
ISP3(config-router)#neighbor 200.201.202.1 remote-as 400
ISP3(config-router)#network 128.0.0.0 mask 255.255.0.0
```

- ISP4's router:

```
ISP4>enable
ISP4#configure terminal
ISP4(config)#router bgp 400
ISP4(config-router)#bgp log-neighbor-changes
ISP4(config-router)#neighbor 129.130.131.1 remote-as 200
ISP4(config-router)#neighbor 200.201.202.2 remote-as 300
ISP4(config-router)#network 99.0.0.0 mask 255.0.0.0
```

- Unit testing:
 - Ping from PC on ISP3's router to Web server in Headquarter

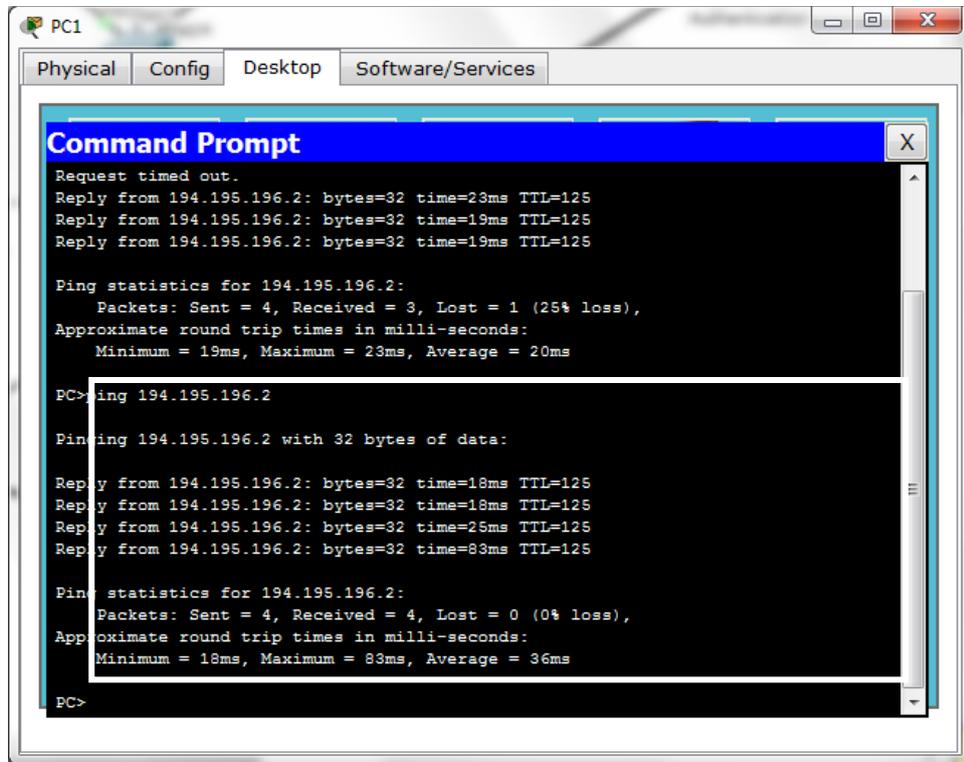


FIGURE 36. Ping from PC on ISP3's router to Web server in Headquarter

Virtual Private Network (VPN)

- Goal: Establish VPN for remote users
- Detail steps:
 - Headquarter Router:

```
R_Head(config)#crypto isakmp enable
R_Head (config)#crypto isakmp policy 1
R_Head (config-isakmp)#authentication pre-share
R_Head (config-isakmp)#encryption aes
R_Head (config-isakmp)#hash sha
R_Head (config-isakmp)#group 2
R_Head (config-isakmp)#exit
R_Head (config)#crypto isakmp key 1010 address 130.131.0.2
0.0.0.0
R_Head (config)#crypto ipsec transform-set vpnhead esp-aes esp-
sha-hmac
R_Head (config)#crypto ipsec security-association lifetime
seconds 86400
R_Head (config)#ip access-list extended aclhead
R_Head (config-ext-nacl)#permit ip 12.0.0.0 0.0.255.255 10.0.0.0
0.0.255.255
R_Head (config-ext-nacl)#exit
R_Head (config)#crypto map vpnmaphead 100 ipsec
R_Head (config-crypto-map)#match address aclhead
R_Head (config-crypto-map)#set peer 130.131.0.2
R_Head (config-crypto-map)#set pfs group2
R_Head (config-crypto-map)#set transform-set
R_Head (config-crypto-map)#exit
R_Head (config)#interface fastethernet 0/0.
R_Head (config-if)#crypto map vpnmaphead
```

- Unit testing:
 - Ping from VPN laptop to Database server in headquarter

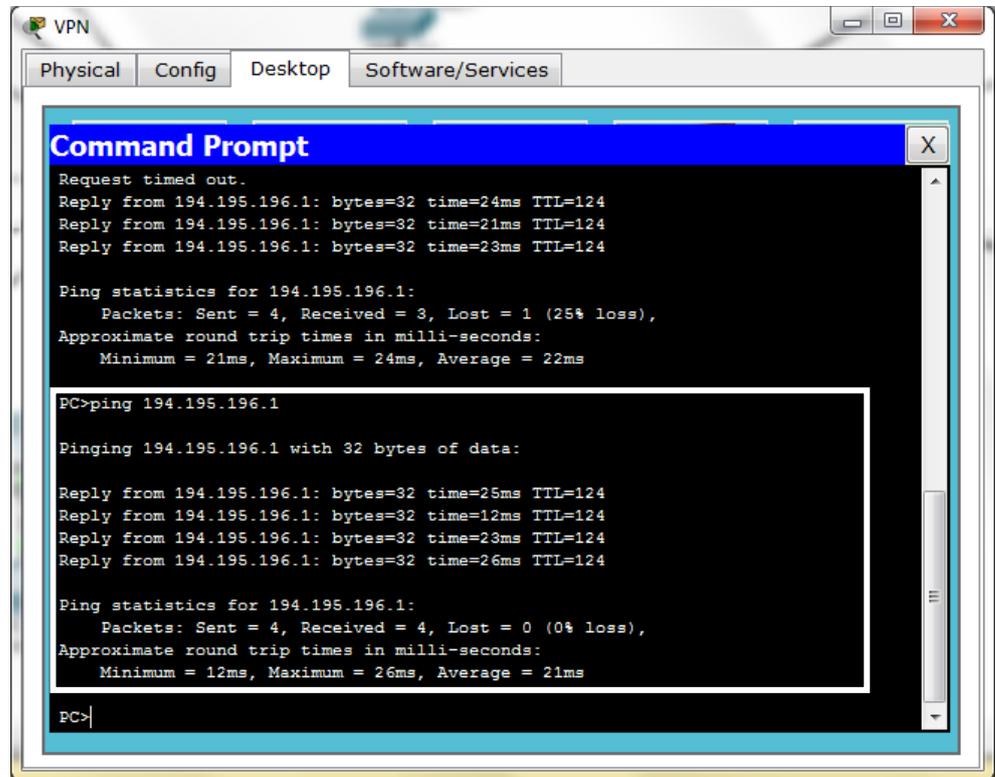


FIGURE 37. Ping from VPN laptop to Database server in headquarter

- Goal: - Set passwords for routers on all opening lines such as console, telnet, and auxiliary.
 - Configure encryption with IPsec
 - Set IPv4 and IPv6 access list for traffic filtering.
- Detail steps:
 - Set password for privileged mode

```

R_Head(config)#enable password test

R_Head (config)#enable secret vinita

```

- Set password for console line mode

```
R_Head (config)#line console 0  
  
R_Head (config-line)#password console  
  
R_Head (config-line)#login
```

- Set vty password for telnet line

```
R_Head (config)#line vty 0 4  
  
R_Head (config-line)#password telnet  
  
R_Head (config-line)#login
```

- Set password for auxiliary line mode

```
R_Head (config)#line aux 0  
  
R_Head (config-line)#password aux  
  
R_Head (config-line)#login
```

- Configure encryption with IPSec

```
R_Head(config)#crypto ipsec transform-set sechead  
esp-aes 128 esp-md5-hmac
```

- Set IPv4 extended access list to prevent ICMP (DOS attack) from the internet

```
R_Head (config)#access-list 104 deny icmp any any  
  
R_Head (config)#interface Ethernet 1/1  
  
R_Head (config-if)#ip access-group 104 in
```

- Set IPv6 access list to prevent ICMP (DOS attack) from the internet

```
R_Head(config)#ipv6 access-list icmpstop  
R_Head(config-ipv6-acl)# deny icmp any any  
R_Head(config)#interface Ethernet 1/1  
R_Head(config-if)# ipv6 traffic-filter icmpstop in
```

- Security verification:
 - Show IPSec

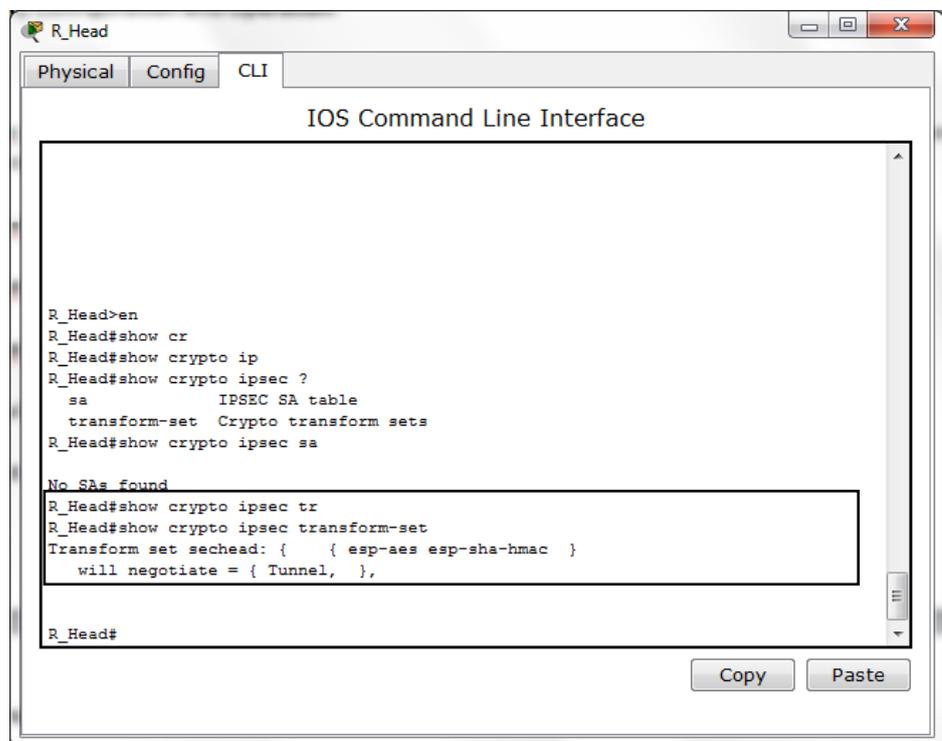


FIGURE 38. Show IPSec

- Ping from PC of ISP3's router to Mail server using IPv4

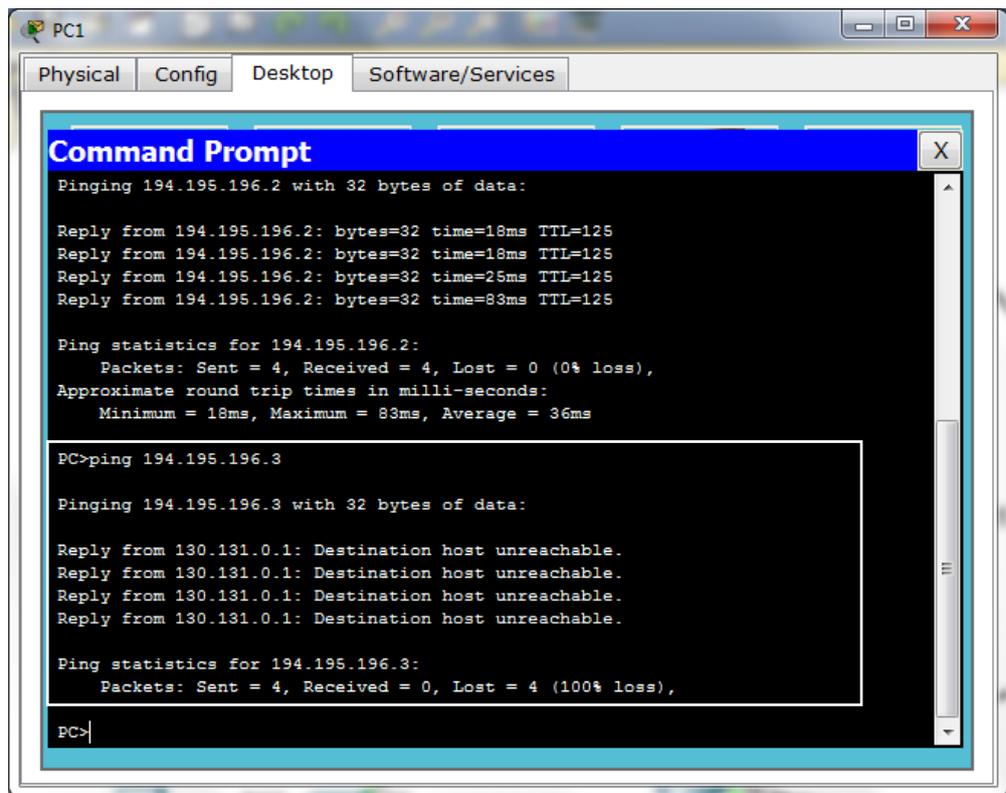


FIGURE 39. Ping from PC of ISP3's router to Mail server using IPv4

- Ping from PC of ISP2's router to Database server using IPv6

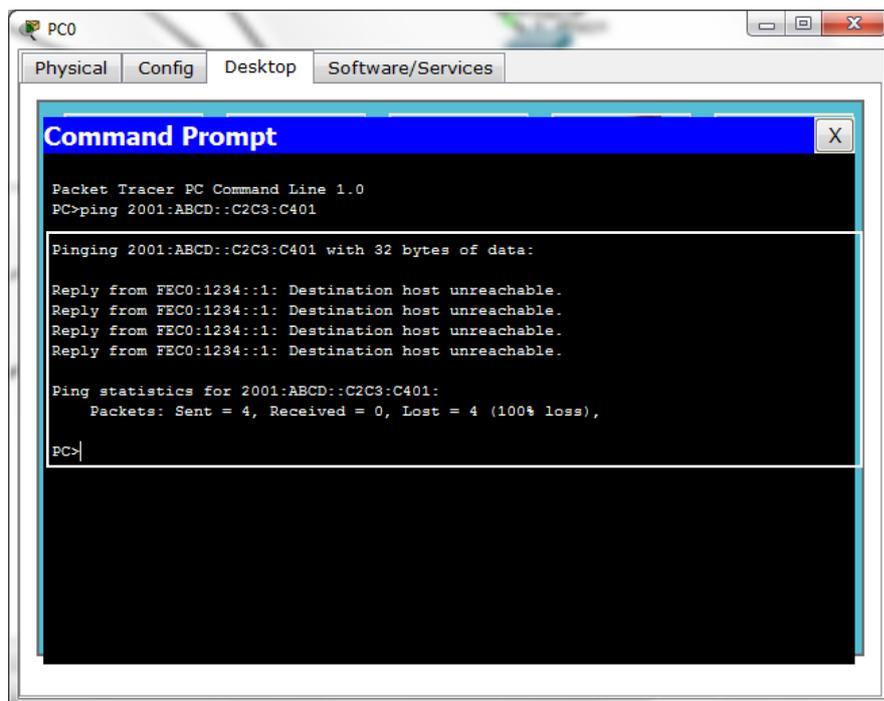


FIGURE 40. Ping from PC of ISP2's router to Database server using IPv6

The final completed network model

Figure 41 is the pre-configured model of the whole network. As we can see all the red dots means the routers have not been established correctly.

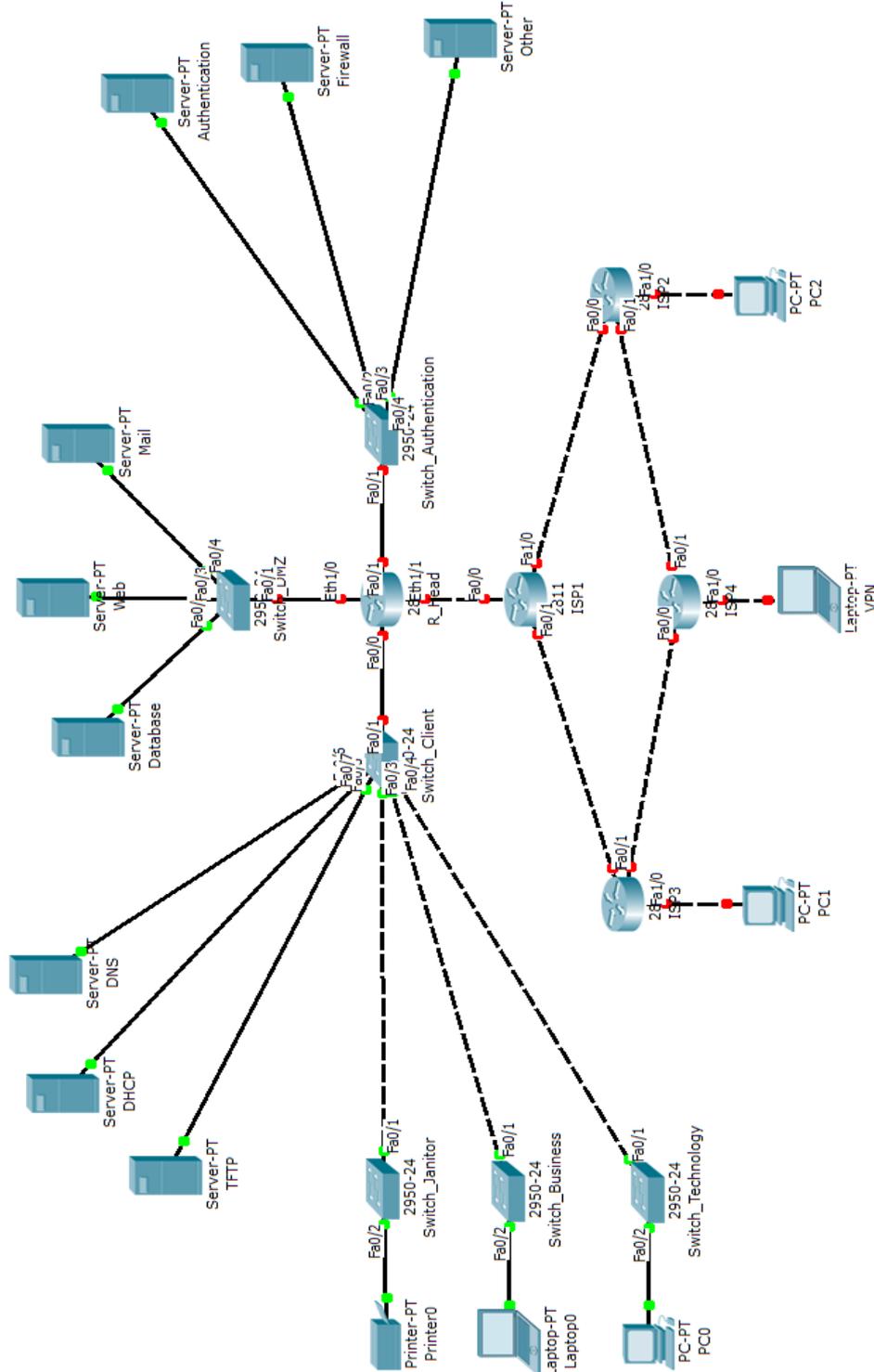


FIGURE 41. Pre-configured model

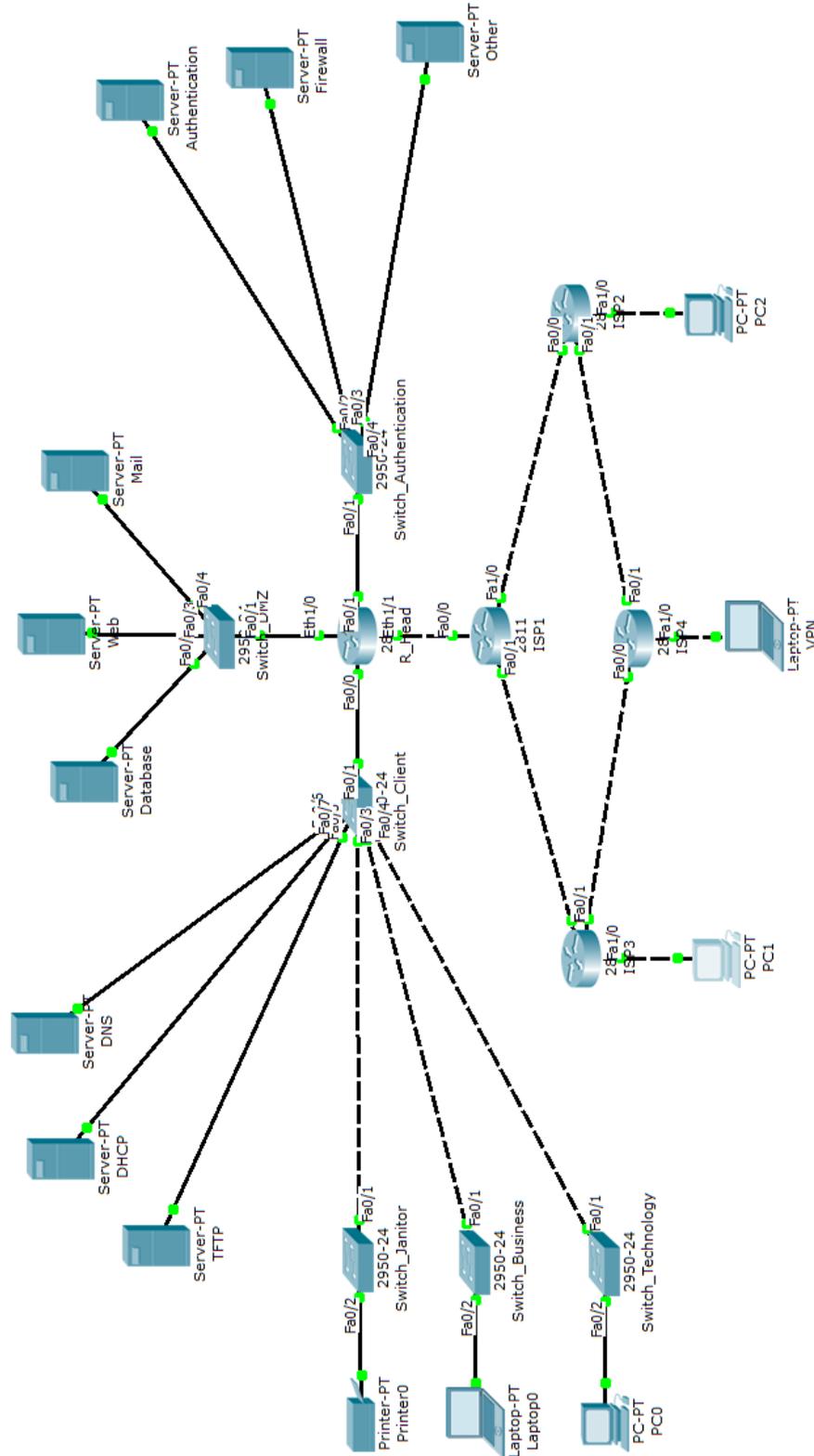


FIGURE 42. Configured model

Figure 42 is the configured and final model of the whole network. Based on the green dots, the model has been configured and ready to be used.