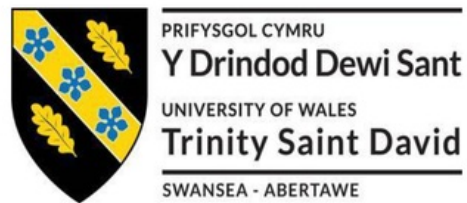


Project Report

by Ivan Carl Lagman

FILE	17639_IVAN_CARL_LAGMAN_PROJECT_REPORT_78196_18059934 18.D OCX (2.23M)		
TIME SUBMITTED	21-APR-2016 11:34 AM	WORD COUNT	13599
SUBMISSION ID	56187412	CHARACTER COUNT	77555



A STUDY BASED ON THE COMPARISON OF THE PERFORMANCE OF IPV4 AND IPV6

By: Ivan Carl Lagman

Supervisor: Dr Kapilan Radhakrishnan

Second Marker: Dr Carlene Campbell

Project submitted as part of the requirements for the award of BSc
(Hons) Computer Networks

April 2016

Declaration of Originality

I, Ivan Carl Lagman declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed:

Date:

Form of Consent

I, Ivan Carl Lagman hereby consent that my Project, submitted in candidature for the B.Sc.(Hons) Computer Networks degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed:

Date:

Copyright Acknowledgement

I acknowledge that the copyright of this project report, and any product developed as part of the project, belong to University of Wales Trinity Saint David, Swansea.

Abstract/Synopsis

In this paper, the main objective is to compare IPv4 and IPv6 in different criteria in order to recognise in which protocol is the most suitable to use under a situation. Additionally, this performance comparison is accomplished by comparing the two protocols using a network simulation tool (Riverbed OPNET). OPNET is network simulation software that allows network engineer to simulate the performance of any type of a network.

The network topology consists of devices such as routers, switches, workstations and servers. Each device contains multiple different configurations in order to help provide information for metrics such as Ethernet delay, packet loss and traffic received/sent.

Overall, the project design met the overall aims and objectives to compare the performance of IPv4 and IPv6 by using a simulation tool. To review, the version of internet protocol is identified in which to use for a specific purpose, IPv6 comes out as the most successful in all of the experiments; this paper looks to convince the audience that IPv6 should be used for applications when it comes to network design. Equally important, this paper provides and demonstrates evidence that IPv6 is available to migrate to now or in a few years' time.

Table of Contents

Declaration of Originality	1
Form of Consent	1
Copyright Acknowledgement	2
Abstract/Synopsis	3
List of Figures.....	5
List of Tables.....	7
Acknowledgements	8
Chapter 1 - INTRODUCTION	9
1.1 Introduction	9
1.2 Aims	10
1.3 Objectives	10
1.4 Structure of Project	10
Chapter 2 – RESEARCH & REVIEW OF LITERATURE	12
2.1 Introduction	12
2.2 What is the history of IPv4 and IPv6	12
2.3 Introduction to IPV6.....	22
.....	25
2.4 Deployment of IPv6.....	26
2.5 IPv6 Transition	28
.....	33
.....	40
2.6 Conclusion	40
Chapter 3 – RESEARCH METHODOLOGY	42
3.1 Introduction	42
3.2 Research Overview	42
3.2.1 Research Process	43
3.2.2 Research Philosophy.....	43
3.2.3 Research Methodologies	44
3.2.4 Data Collection	44
3.3 Research Deliverables	45
3.4 Conclusion.....	45
Chapter 4– DESIGN AND IMPLEMENTATION	47
4.1 Introduction	47

4.2 Design	47
Network Topology	49
4.3 Implementation.....	49
4.4 Conclusion	50
Chapter 5 –RESULTS AND DISCUSSIONS	51
5.1 Introduction	51
5.2 Results and discussion	51
5.3 Conclusion	55
6.1 Summary.....	57
6.2 Fulfilling the aims and objectives	57
6.3 Conclusion	57
6.4 Recommendations for further research.....	58
Chapter 7 – REFLECTIONS	59
Chapter 8 - REFERENCES	61
Gantt chart	65
Glossary	66

List of Figures

- Figure 1 – RIR IPv4 Address Run-Down-Model
- Figure 2: Network Topology
- Figure 3: Network Simulation Results
- Figure 4: TCP Throughput of Windows Operating Systems
- Figure 5: Median Round Trip Time (ms) with hop distance 10 and 20 for IPv4 and IPv6
- Figure 6: Ratio of IPv4 and IPv6 for seven metrics over the five years
- Figure 7: Active clients (4a, 4b), flow peak (4c, 4d) and detail (4e, 4f) performance for Facebook and Gmail on World IPv6 Day
- Figure 8: IPv4 and IPv6 Architecture
- Figure 9: average Ethernet delay for both protocols
- Figure 10: HTTP traffic received packets per second
- Figure 11: Processing delay of intra-communication (a) at Customer Edge (b) at Provider Relay
- Figure 12: Research Overview

- Figure 13: The Research Onion Model
- Figure 14: The Waterfall Model
- Figure 15: Project network topology
- Figure 16: Project average Ethernet delay for IPv4 and IPv6
- Figure 17: Project average FTP traffic sent/received per second
- Figure 18: Project average number of hops
- Figure 20: Project average HTTP traffic received per second
- Figure 21: Project average HTTP Traffic sent bytes per second

List of Tables

- Table 1 - Bit Allocation for the Class A Address Space
- Table 2 - Bit Allocation for the Class B Address Space
- Table 3 - Bit Allocation for the Class C Address Space
- Table 4 - Bit Allocation for the Class D Address Space
- Table 5: IP Address Ranges by each class with Subnet Masks
- Table 6 : IPv4 Addresses and IPv6 Equivalents
- Table 7: Comparing the IPv4 and IPv6 headers
- Table 8: Facts and Metrics of each version of internet protocol
- Table 9: World Internet Usage and Population Statistics as of March 2011
- Table 10: Classful Unicast IP Address
- Table 11: Transition methods to use for migration from IPv4 to IPv6
- Table 12: Transition mechanisms strengths and weaknesses

Acknowledgements

Firstly, I would like to thank all my family, friends and lecturers for continuously motivating me to put in hard work in my project. Secondly, I would like to express my gratitude to my project supervisor Kapilan Radhakrishnan for his guidance, understanding and pushing me farther than I thought I could go. Finally, I would like to express my thanks to my girlfriend for accompanying me to the library and constantly pushing me to work on my project.

Chapter 1 - INTRODUCTION

1.1 Introduction

Internet Protocol was designed in 1970 and was introduced in the networking industry in 1981. Internet protocol plays a large part of the development of networking and the internet. In 1970's, IETF (Internet Engineering Task Force) were working on Internet protocol and they firstly invented the old version of Internet Protocol. IPv1, IPv2 and IPv3 were used for the development of IPv4. They were never used for public and remained as experimental versions. [1][2]

At the time of the deployment of IPV4, it consists of 4,294,967,296 unique addresses available for public use. This was thought to be more than enough, however, it has become evident that the number of available address is being exhausted. This was one of the main reasons for the deployment and development of IPV6.[3]. In 1991, IETF had decided that IPv4 had outlive its design. This group responsibility was to find a new IP protocol to solve the problems of IPv4.[4]

In 1999, the IETF introduced IPv6 which is the new version of the internet protocol. [5] IPv6 has many improvements to overcome the problems of IPv4. IPv6 fulfils the increasingly complex requirements hierarchical addressing that is not supported in IPv4The main advantage that IPV6 has over IPV6 is its larger address space. [6][4]

The main aim of the experimental project is to compare the two protocols, this can be accomplished by using a software like OPNET. Use of OPNET will allow for help in producing valuable results which can led to use in concluding the differences between the two protocols. Furthermore, each section of this topic will be explored through the experimental project concluding valuable and correct information.

Additionally, in this report will consists of many different areas of this experimental project that are categorised into different chapters. These chapters

consists of introduction, figures, tables, evaluation and analysis results. Each of these chapters plays a large contribution in the completion of this project.

1.2 Aims

The aim of this project is to compare the different aspects of IPv4 and IPv6. This includes aspects such as: Performance, Reliability, Major Differences, Header or Address Format, Security and when to choose IPv4 or IPv6.

1.3 Objectives

The objectives of this project is to compare the two protocols. The objectives are:

- To gain understanding in the topic to be able to distinguish the main the differences between the two versions of IPv4 and IPv6
- To perform a background research on this topic, in order to able to identify the advantages and limitations of each protocol
- To evaluate the results gained from the experimental task which leads to being able identify which protocol to choose when it comes to network design or for any other experimental network purposes

1.4 Structure of Project

The project is structured accordingly in multiple chapters; firstly it will focused discuss closely into the theoretical stages of the project which will meet the aims and objectives of the project. Secondly, it will focus on the design stages of the project discussing the requirements and components that was obtained from the research conducted and covering the research methodology used which will help in the project design and implementation. Thirdly, the final stage will be focusing on testing and evaluating the simulation scenarios in order to analyse the results to determine the differences between the two protocols. Finally, there are also other chapters such as appendices, references, bibliography and glossary.

Chapter one illustrates a summary overview of the entire project. It details the main aims and objectives that once it has been accomplished will bring success to this research study.

Chapter two concentrates on the review of literature on this topic. It discusses the all the research information that has been obtained in order to support this project.

Chapter three focuses on the methodology methods that was used in this project such as the waterfall and the onion model. It focuses on the different research methodologies, strategies, approaches, reliability and validity of the project.

Chapter four details the design and implementation of the project. It concentrates closely on the stages in completing the simulation design. Also, it displays the tools, techniques and network components used in the network architecture.

Chapter five explains the conclusion of the data that was produced from the software simulation design. Additionally, this results data was compared to the results of the journal papers in the same topic as this project.

Chapter six explores the overall project conclusion and discusses any suggestions that would be useful to for future improvements in this project.

Chapter seven and eight consists of the reflection, references, appendix that was used for this research project. These chapters emphasises the reflections produced from completing the project software design and displays the references used to help in completing the literature review. Also, any sources that are classed as other materials such as glossary and Gantt chart.

Chapter 2 – RESEARCH & REVIEW OF LITERATURE

2.1 Introduction

Internet Protocol (IP) is a set of rules that defines how a computer transfer data to another computer. Internet Protocol is situated on the network layer of the OSI model and also located on internet layer of the TCP/IP model. On a network, each device and computer are given a unique IP address. IP assigns unique address to the devices across the entire network, it encapsulates the data into datagrams and sends the datagram to its destination. [1][7][8]

The aim of this experimental project is to gain sufficient amount of knowledge on the background and the current affairs of IPv4 and IPv6. Also, once sufficient knowledge is gathered, this valid information will be use in the experimental design of this project.

2.2 What is the history of IPv4 and IPv6

IPV4

IPV4 stands for Internet Protocol version 4; it was introduced in the early 1980's. At the time, the rise of the Internet has grown rapidly therefore there was a high demand of IPv4 addresses that were needed. IPV4 was the first version of Internet protocol; it was designed at 1970s and consists of approximately over four billion IP addresses. In modern day networking, IPV4 is the most commonly used protocol which is responsible for all the traffic on the Internet.[9] [10]

Classes of Addresses

IPv4 divides the network address space into five address classes. Each class are embedded in the first four bits of the network address which defines either the

different network size e.g. number of hosts for unicast addresses (Class A, B and C) or multicast network (Class D). The fifth class E address is reserved by the IETF for its own research purposes. The five address which are:

- Class A – It was designed to support the network scenarios with large entities requiring a large number of hosts address. In general, only the first octet is used for the network address. The three remaining octets to use to be able to identify any potential hosts to that specific network.

Table 1 : Bit Allocation for the Class A Address Space [11]

	First Octet	Second Octet	Third Octet	Fourth Octet
Usage	Network	Hosts	Host	Host
Required Binary Values	0-----	-----	-----	-----

- Class B – It was conceived as a middle ground between the two classes (A and C). The architects of the network address space followed their design of using the network octet boundaries. When in a fact, Class A network address was defined with just a single octet, a class B network address was treated to half of the four octets in an IP address.

Table 2: Bit Allocation for the Class B Address Space [11]

	First Octet	Second Octet	Third Octet	Fourth Octet
Usage	Network	Network	Host	Host
Required Binary Values	10-----	-----	-----	-----

- Class C – Class C address space provide a large number of network addresses, even though each one can endure only a limited number of host addresses. Class C network address uses three octets in length, leaving just one octet to use in identifying hosts in the specified network.

Table 3: Bit Allocation for the Class C Address Space [11]

	First Octet	Second Octet	Third Octet	Fourth Octet
--	-------------	--------------	-------------	--------------

Usage	Network	Network	Network	Host
Required Binary Values	110-----	-----	-----	-----

Class D – Class D address space is unique compared to the first three classes. Unlike the previous classes, this class does not follow to the convention of splitting the bit string into network and host address subcomponents. [11]

Table 4: Bit Allocation for the Class D Address Space

	First Octet	Second Octet	Third Octet	Fourth Octet
Usage	Multicast Group	Multicast Group	Multicast Group	Multicast Group
Required Binary Values	1110-----	-----	-----	-----

Class E – Class E address has been defined however is reserved by the IETF for its own research and experimental purposes. This address class begins at 240.0.0.0 and ends at the top of the address space of 255.255.255.x. [1]

Table 5: IP Address Ranges by each class with subnet mask

Class	Range
A (range/mask in dotted decimal)	0 .0.0.0 to 127.0.0.0/8 (255.0.0.0)
A (range in binary)	00000000 .00000000.00000000.00000000 to 01111111.00000000.00000000.00000000
A (mask in binary)	11111111.00000000.00000000.00000000/8
B (range/mask in dotted decimal)	128 .0.0.0 to 191.255.0.0/16 (255.255.0.0)
B (range in binary)	10000000 .00000000.00000000.00000000 to 10111111.11111111.00000000.00000000
B (mask in binary)	11111111 .11111111.00000000.00000000/16

C (range/mask in dotted decimal)	192 .0.0.0 to 223.255.255.0/24 (255.255.255.0)
C (range in binary)	11000000 .00000000.00000000.00000000 to 11011111.11111111.11111111.00000000
C (mask in binary)	11111111.11111111.11111111.00000000/24
D (range/mask in dotted decimal)	224 .0.0.0 to 239.255.255.255/32 (255.255.255.255)
D (range in binary)	11100000 .00000000.00000000.00000000 to 11101111.11111111.11111111.11111111
D (mask in binary)	11111111.11111111.11111111.11111111/32
E (range/mask in dotted decimal)	240 .0.0.0 to 255.255.255.255/32 (255.255.255.255)
E (range in binary)	11110000 .00000000.00000000.00000000 to 11111111.11111111.11111111.11111111
E (mask in binary)	11111111.11111111.11111111.11111111/32

Source: Ipv4 and Ipv6 attributes (2006) [12]

IPV6

IPV6 is the latest version of Internet Protocol and was designed to be the successor to IPv4. The IETF began development of a successor to IPv4 during the early 1990s. [13] In 1999, IPv6 was introduced, it provides a large amount of IP address available to the world and it is expected to handle the entire world's IP addressing needs into the future. [14] Moreover, it contains 340 undecillion IP address which is an extremely large amount in comparison to IPV4 and is sufficiently a lot to provide to the world needs for a few decades in the future. [15][16]

Routing Protocols

A routing protocol is a language that routers use as a way to communicate with each other so that they are able to inform each other the current status and the reachability of the network. [17] IPv4 and IPv6 both contain multiple and different routing protocols. Routing protocols are a set of rules that are used by routers in

order to dynamically learn about the different paths available to other networks and to transfer data between the networks. There are many protocols that are used in IPV4. They are:

1. RIP (Routing Information Protocol)

RIP is a standardised distance routing protocol which uses a method of distance as hop count metric. At the time it was developed, network traffic was not important as the routing tables were small enough therefore; RIP can only transmit full updates every thirty seconds. RIP has four basic timers which are:

- Update Timer, Invalid Timer, Hold Down Timer and Flush Timer [17]

2. OSPF (Open Shortest Path First)

OSPF is a standardised link-state routing protocol, it was designed to scale efficiently and to use in large enterprise networks. It has many advantages in comparison to other protocols i.e. it has not limitation when it comes to hops and also it supports VLSM (Variable Length Subnet Mask) whereas RIP cannot. [17]

3. EIGRP (Enhanced Internal Gateway Routing Protocol)

EIGRP is a dynamic routing protocol that evolved from IGRP which significant improvements of its successor. In 1993, EIGRP replaced IGRP to support IPv4 addresses that IGRP could not support. It is usually used in large-size networks, it updates only when the network topology changes, however it does not periodically update in comparison to other protocols such as RIP. [17]

4. BGP (Border Gateway Protocol)

BGP is the Internet's inter-domain routing protocol. [17]. It is the most scalable protocol out of all the routing protocols, it is the routing protocol for the Internet and for service providers in private networks.

In IPV6, the routing protocols are called slightly different in comparison to IPV4. There are many protocols that are used in IPV6. They are:

1. RIPng (Routing Information Protocol Next Generation)

In IPv6, the version of RIP is described in RFC 2080. It is called RIPng which indicate the name used for the next-generation of IP protocol. RIPng

supports function such as: Split Horizon and Poison reverse as its IPv4 counterpart. It also contains the same limitations, such as a maximum hop count of 15, and does adding to infinity for certain routing loops. [19]

2. EIGRP (Enhanced Internal Gateway Routing Protocol)

- a. EIGRP for IPv6 and for IPv4 have very similar features. They are both capable of implementing the diffusing update algorithm which was developed in 1980. Also, in IPv4, it uses MD5 authentication and similar support is provided for IPv6. They also contain major differences due to the design elements of IPv6 such as:

Automatic Summarisation

- i. It is enabled by default in IPv4; however, this function is disabled in IPv6 as it is a classless protocol

Split Horizon

- ii. IPv6 doesn't provide split horizon as it consists of multiple prefixes could exist on the same interface of a network device i.e. router [10]

3. OSPFv2 (Open Shortest Path First version 2)

In OSPFv2, it consists of basic mechanisms such as flooding, DR election, area support, SPF calculations. Also in OSPFv2, it runs on per-IP subnet basis in comparison to OSPFv3 where it runs on a per-link basis. There is no backward compatibility from OSPFv3 to OSPFv2. [10]

4. OSPFv3 (Open Shortest Path First version 3)

OSPFv3 is a link-state routing protocol for IPv4 and IPv6 which is the third version of OSPF. It is very different in comparison to OSPFv2, whereas for OSPFv3 each interface must be enabled using commands in interface configuration mode and a routing process does not need to be explicitly designed. [15]

What is the major difference?

In contrast to IPV4 and IPV6, the differences between can be categorised into five elements: addressing, routing, security, NAT, administrative workload and the support for mobile devices.[12] Also, there are many differences for IPv4 and IPv6 in in this section the equivalents is shown in the table below.

Table 6 : IPv4 Addresses and IPv6 Equivalents [5]

IPv4 Address	IPv6 Address
Internet Address Classes	Not applicable in IPv6
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IP Address	Global unicast addresses
Private IP addresses (10.0.0.0/8, 172.16.0.0/12. And 192.168.0.0/16)	Site-local addresses (FEC0::/10)
Auto configured addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)

The previous tables shows the differences of both IPv4 and IPv6 and IP addresses. Below is a table to display the differences of the header fields of both protocols.

Table 7: Comparing the IPv4 and IPv6 headers [5]

IPv4 Header Field	IPv6 Header Field
Version	Same field but with different version numbers.
Internet Header Length	Removed in IPv6. IPv6 does not include a Header Length field because the IPv6 header is always a fixed size of 40 bytes. Each extension header is either a fixed size or indicates its own size.
Type of Service	Replaced by the IPv6 Traffic Class field

IPv4 Header Field	IPv6 Header Field
Total Length	Replaced by the IPv6 Payload Length field, which only indicates the size of the payload.
Identification Fragmentation Flags Fragment Offset	Removed in IPv6. Fragmentation information is not included in the IPv6 header. It is contained in a Fragment extension header.
Time to Live	Replaced by the IPv6 Hop Limit field.
Protocol	Replaced by the IPv6 Next Header field.
Header Checksum	Removed in IPv6. In IPv6, bit-level error detection for the entire IPv6 packet is performed by the link layer.
Source Address	The field is the same except that IPv6 addresses are 128 bits in length.
Destination Address	The field is the same except that IPv6 addresses are 128 bits in length.
Options	Removed in IPv6. IPv4 options are replaced by IPv6 extension headers.

In the same way, the major differences between the two protocols is the number of IP addresses. IPv4 consists of 4,294,967,296 IP addresses, whereas IPv6 consists of 340,282,366,920,938,463,463,374,607,431,768,211,456 IP addresses. Below is a figure to display the facts and metrics of each version of internet protocol. [9]

Table 8: Facts and Metrics of each version of internet protocol

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,920,938,463,463,374,607,431,768,211,456$

Source: ARIN

The limitations of IPv4

Ever since IPv4 was introduced in the 1980's, it has been apparent that the number of available IPv4 address is being exhausted at a speed that it was not anticipated at the time in the design of the network. This was the main reason why the classful network was introduced, for the invention of Classless Inter-Domain Routing (CIDR) in 1993. [12]

The main primary reason for the exhausting is the continuous growth in the number of internet users, mobile devices which uses internet connection and always on devices such as ADSL modems. At this moment in history, this was the beginning to the development and invention of IPv6 as an alternative option. However, at the time it was estimate that 2010 will be the last year for IPv4, but some sources say they may last until 2012. [12]

Table 9: World Internet Usage and Population Statistics as of March 2011

World Region	Population (2011 Est)	Internet Users, Dec 31 2000	Internet Users, Latest Data	Penetration (% Population)	Growth, 2000 – 2011 (%)	Users, % of Table
Africa	1,037,524,058	4,154,400	118,609,620	11.4	2527.4	5.7
Asia	3,879,740,877	114,304,000	922,329,554	23.8	706.9	44.0
Europe	816,426,346	105,096,093	476,213,935	58.3	353.1	22.7

Middle East	216,258,843	3,284,800	68,553,666	31.7	1.987.0	3.3
North America	347,394,870	108,096,800	272,066,000	79.3	151.7	13.0
Latin America / Caribbean	597,283,165	18,068,919	215,939,400	36.2	1.037.4	10.3
Oceania / Australia	35,426,995	7,620,480	21,293,830	60.1	179.4	1.0
World Total	6,930,055,154	360,985,492	2,095,006,005	30.2	480.4	110.0

Source: Internet World Stats (2011) [13]

The number of people using the Internet has increased rapidly over the past few years. This is due to the remarkable growth of the wireless industry, including wireless and cellular networks such as: Wi-Fi (WLAN), 2G, and 3G, 4G LTE, WiMAX and Mobile Wireless (MBWA). It is still further rising of the number of mobile devices that needs to use the Internet. [13]

In modern day networking, North America was the one of the last continent in the world that have officially ran out of IPv4 address. In 2011, APNIC which allocates IPv4 address Asia-Pacific has declare that is has officially ran out of available addresses, RIPE, which supervises Europe, the Middle East and parts of Central Asia, was running out of addresses by 2012; LACNIC, which controls the Caribbean and Latin America declared it was out of addresses in 2014. Furthermore, the only continent that is left is AFRINIC, which manages Africa and is expected to run out of IPv4 address in 2019.[3].[21] Projections display that all five RIRs will run out of IPv4 addresses between 2015 and 2020. Below is a figure to display how the amount of remaining addresses in RIR pool has decreased in the past few years.

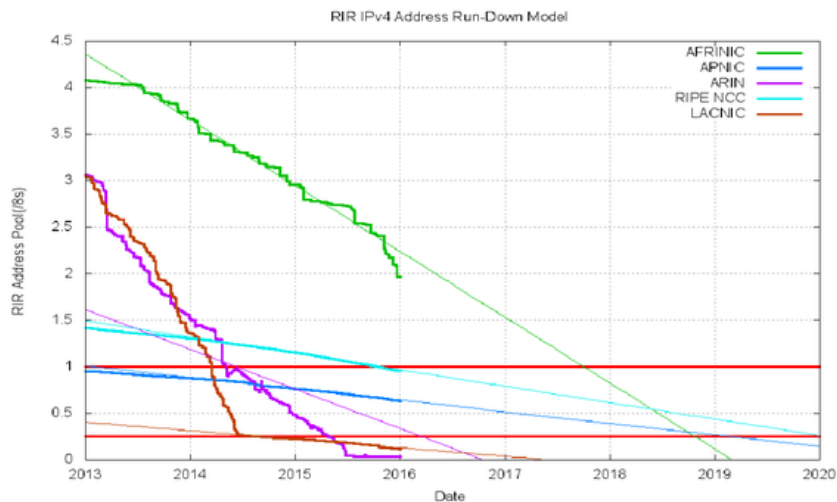


Figure 1 – RIR IPv4 Address Run-Down-Model [22]

Classless Inter-Domain Routing

In 1993, IETF introduced CIDR; which is a method that was developed to allow more allocation of IP address which helped reduce the problem of exhaustion of IP address and the growth of routing tables. The main goal behind the idea of CIDR is that blocks of multiple addresses can be combined to be able to create larger classless set of IP addresses, with more network hosts allowed. At the time, organisations/companies that was using ISP for their Internet connectivity have allocated of their provider's address space as required. [8]

In the early years, IPv4 network addresses were allocated using one of the three classes. They are: Class A, Class B and Class C as shown in the table below.

Table 10: Classful Unicast IP Address

Address Class	First Octet Range	Number of Possible Networks	Number of Hosts per Network
Class A	0 to 127	128 (2 are reserved)	16,777,214
Class B	128 to 191	16,384	65,534
Class C	192 to 223	2,097,152	254

Source: IP Addressing Fundamentals (2011) [13]

2.3 Introduction to IPV6

Why was IPV6 invented?

IPv4 allows systems to communicate and forms the foundation of the Internet as seen today, however, IPv4 has many limitations. In 1999, the IETF introduced a successor to IPv4; IPv6 it is a new version of the internet protocol. [5]. It is a technology that was developed in order to overcome these limitations. Even though it has many similarities to IPv4, IPv6 satisfies the increasingly complex requirements hierarchical addressing that IPv4 does not support. [22] Also, IPv6 provides better improvements to network topologies such as peer to peer and client/server. [23] The main advantage that IPV6 has over IPV6 is its larger address space and a better performance. [4]

IPv6 is a greater improvement of IPv4 that consists of features that better match the current and predictable network demands, these are the features:

- **Larger Address Space**

IPv6 address size are 128 bits in comparison to IPv4's 32 bits. This large amount of address space provides many advantages such as improved flexibility and global reachability, easier multihoming to ISP (Internet Service Providers).

- **Support for mobility and security**

Mobile and security is supported which helps guarantee compliance with mobile IP and IPsec standards.

- **Elimination of public-to-private NAT-** The larger address space allows for end to end communication without having to use NAT

- **Simplified header for improved router efficiency**

A simple header provides many benefits, such as improve routing efficiency for performance, scalability, flexibility, simpler and more efficient extension header mechanisms. [22][24]

Advantages of using IPv6

Moreover, as IPv6 contains a large number of address space, it greatly benefits ISPs as they will have more than enough IP address to allocate every customer in order that every device has an IP address on their home network. [12] In addition, another benefit of using IPv6 is that it eliminates the need for NAT which

outcomes in a better connectivity in peer to peer networks. Also, IPv6 promotes interoperability between different IPv6 implementations. [13].

IPv6 also includes IPsec which adds overhead which help reduce the network performance. The increased header size and IPsec Ipv6 would also increase bandwidth utilisation, increase latency and be able to reduce network throughput for IPv6 traffic. [19]

Furthermore, IPv6 consist of many tools that is useful to help with the transition from IPv4 to IPv6, also including NAT and tunnelling. [27] NAT provides a mechanism to translate an IPv4 address to an IPv6 address or vice version, also IPv4 can be tunnel over IPv6. Tunnelling encapsulates the IPv6 packet into an IPv4 packet in order that it can be used and transferred over an IPv4 network. [13]

IPv6 Security

In modern day networking, the usage of the Internet is highly increasing day by day, therefore there is higher risk in hacking and data leakage to occur which leaves security as a major concern. IPv6 consists of two security schemes into its protocol which are: IP Authentication Header (RFC 1826) and IP Encapsulating Security Payload (ESP, described in RFC 1827). [28]. When IPv4 was invented, it lacked security mechanisms, this lead to IPsec being retrofitted with additional components and features to provide as a security measure for IPv6. [29]

IPv6 provides capabilities that makes it more superior than IPv4 such as a streamlined packet format, compatible with source routing, also an integrated authentication and provides a method of encryption to further improve the quality of security. [5]

IPv4 and IPv6 QoS Mechanisms

In this paper, metrics and levels in QoS was used to plan three simulation scenarios which produce valuable results such as traffic stage, average delay and average delay for the clients. The software OPNET was used in order to simulate the network scenarios. Below are the figures that display the network topology and the simulation results. [30]

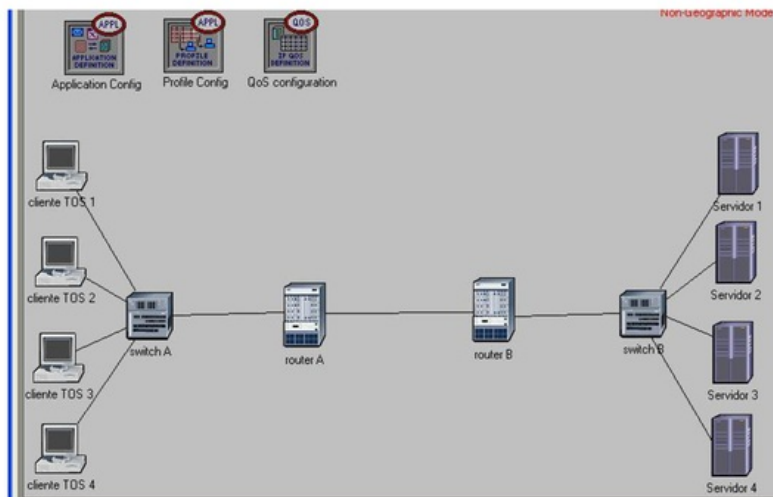


Figure 2: Network Topology [30]

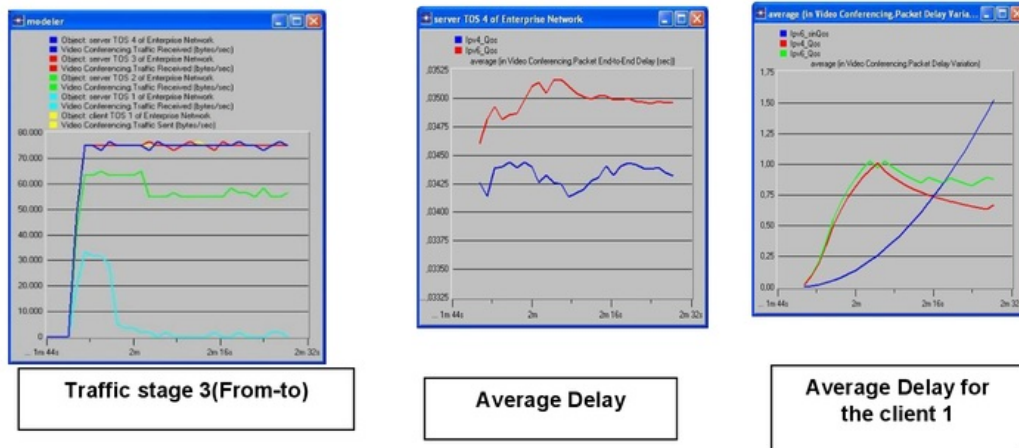


Figure 3: Network Simulation Results [30]

2.4 Deployment of IPv6

Security Threats

Deploying IPv6, it is important to consider that it will contain many potential threats therefore; deployment should be cautiously thought of. There are many different ways administrators can help make their network secure when they begin to use IPv6 prior to the implementation of IPv6.

- Administrators should take sufficient time to develop and learn an in-depth knowledge of the different aspects of IPv6. IPv4 and IPv6 are different in many ways such as dual-stack and IPv6 only. These needs to be understood to the same level that IPv4 was in the past
- Administrators should begin their IPv6 networks gradually. Firstly, the IPv6 traffic coming in and out of the network should be blocked. Next, making the different sections of the network available to the organisation's requirements, also by informing employees that are specific sections that are available
- Administrators can also help maintain the IPv6 world more secure by carefully choosing the range of IP address that they make available to end users. A range that is too large will most likely to be unnecessary and can make it more easier for end users to abuse the amount of IP addresses [31]

Challenges

Only a small percentage of today's Internet (10%) has accessed Google using IPv6 connectivity. Many organisations have deployed IPV6 to make it a reality to the public. However, each type of organisation faces its own challenges in deploying IPv6. Mobile network providers, residential ISPs are amongst the organisations facing the largest challenges in IPv6 deployment. The main factor of the challenge for both mobile network providers and ISP is their large and continuous amount of growing end users, which causes a large demand for IP addresses and their reliance on the equipment manufacturers to implement IPv6 support before they are able to deploy. Content providers are mainly focused on

reaching as many Internet users as possible, they must accommodate IPv6 alongside IPv4 even in before of its extensive use across the world.

Dual stack is the approach that allows support and compatibility for both IPv4 and IPv6. In order for this technique to occur routers and hosts have to implement both IPv4 and IPv6 routing protocols. [32]. This technique/nodes are also known as IPv4 compatible IPv6 address nodes. The dual-stack technique enables the coexistence of both IPv4 and IPv6 applications depending on an IP layer routing.

Security threats similar in IPv4 and IPv6 network

IPv4 and IPv6 have many differences between them, they still have some aspects that are similar to each other. Some of the attacks have not fundamentally changed by the arrival of IPv6. In regardless of security enhancements included in IPv6, IPv6 network are still vulnerable to the different types of viruses and attacks. Some security threats still exists, therefore there are different types of security attacks could potentially damage IPv6 networks. Along with that, some types of attacks that occur in IPv4 networks did not also fundamentally change by the arrival of IPv6; which means that they can affect both IPv4 and IPv6 networks. There are few types' security threats that are similar in both protocols.

Sniffing Attacks

A great example of an attack that harms both IPv4 and IPv6 networks is a sniffing attack. The sniffing attacks include capture networks packets, if the packets are not correctly encrypted, the data within the packet can be captured using a sniffer. This attack can be avoided by using the IPsec security architecture, which is also used in IPv4 as an option and in IPv6 as a requirement.

Application Layer Attacks

Today, application layer attacks are one of the most common attacks in networking. There are many types of application attacks such as CGI attacks and different types of viruses and worms. On the other hand, transition to IPv6 will neither prevent networks and system to suffer from these attacks nor alleviate their consequences since both protocols (IPv4 and IPv6) are located at the network layer and these types of attacks are happened at the application layer of the OSI model. [33]

Flooding Attacks (DoS Attack)

A security attack that occurs often in an IPv4 network is a flooding attack. A flooding attack is when an attacker attempts to prevent legitimate users from accessing internet services or information. A great example would be a computer user typing in a URL on the Internet which would then send a request on the computer server to view the web page but the attacker has the ability to overload the server and deny the user access to the website. This type of security threats can also harm the IPv6 networks, as the principles of the flooding attack remain the same throughout. [33]

Rogue Devices

In a typical network, rogue devices are placed into network that are not authorised by the network administrator. This type of attacks are common in IPv4 networks and are not changed in IPv6. In order to avoid this attack, IPsec security architecture should be used in a proper way in IPv6, authentication for devices could reduce this attack. [33]

Man-in-the-middle-attacks (MITM attack)

A man in the middle attacks is when the hacker secretly intercepts and relays messages between two end users who believe they are communicating directly with each other. This involves in intercepting a public key message exchange that is transferred during the communication and retransmits the message while replacing the requested key to their own. [33]

2.5 IPv6 Transition

The transition between IPv4 and IPv6 protocols is very important, or else the world risks the failure of the success of the Internet. Fundamentally, IPv6 was developed and implemented as an improvement to IPv4, however the differences between the two protocols are significantly effective. The lack of interoperability means that IPv4 hosts and routers will not be in a place to directly handle IPv6 or vice versa. Although, there are many nature difficulties ahead, effective transitions plans and transition mechanism are needed in order that it covers the complete range of communication demands. Additionally, companies/organisations must invest in the

development of the transition plans so that their products operate correctly and remain relevant. [32]

In order to maintain a smooth and steady transition from Ipv4 to IPv6. It is imperative that network operators and engineers executes an action plan to follow, which indicates the following common methods for a smooth migration.

Table 11: Transition methods to use for migration from IPv4 to IPv6

Transition Method	Description
Dual Stacking	Devices like PCs and Routers run both IPv4 and IPv6 hence have two sets of addresses.
Manual tunnelling of IPv6-to IPv4	In manual tunnelling of IPv6 packets are tunnelled across an IPv4 network by encapsulating them in IPv4 packets requiring routers configuring with dual stacks.
Dynamic IPv6 to IPv4 tunnelling	Dynamic tunnelling of IPv6 to IPv4 allows IPv6 localities to connect to other IPv6 localities across an IPv4 backbone, such as the web automatically. This method applies a matchless IPv6 prefix to each locality without having to retrieve IPv6 addressing information from address registries or ISPs.
Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)	ISATA uses virtual links to connect IPv6 within a site which primarily uses IPv4. Boundary routers between the addressing types must be configured with dual stacks.
Teredo tunnelling	Teredo tunnelling has the hosts perform the tunnelling instead of using routers to tunnel packets which requires the hosts to be configured with dual stacks. It is often used to move packets through an IPv4 address translation tool.
NAT Proxying & Translation(NATPT)	Has an address translation device translated addresses between an IPv6 and IPv4 network or vice versa.

Source: 2013 [34]

Tunnelling enables the communication between IPv4 and IPv6 networks and users. This mechanism is based upon the process of encapsulation and de-capsulation. The stages of encapsulating and de-capsulating packets within the frame for local forwarding leaves vulnerabilities on the network for hackers to exploit and gain unauthorised access to the network. There are two types of tunnelling, they are:

- Automatic Tunnelling – This process involves transferring IPv6 packets to the destination node and configured tunnels this results in delivering to a pre-configured tunnel end node
- Configured Tunnelling – This process includes the source data for the IPv4 packet to be checked. This provides the process to IP spoofing and inserting the packet at the tunnel end node avoiding firewalls and bypassing filtering checks

Additionally, it is important that network administrators are aware of the strengths and weaknesses of each transition technique. Table 12 displays the advantages and disadvantages of each transition mechanism.

Table 12: Transition mechanisms strengths and weaknesses

Transition Mechanism	Strengths	Weaknesses
Dual-Stack	Deals with the issues of the most address selection and DNS resolution. Allows backwards compatibility (IPv4 support) and simple to deploy. Most famous and available on the most platforms.	Increase the cost of routing processes. Additional Memory and CPU. Network security requirements became more difficult.
Translation	Easy to be implemented on "one-off" basis. Works with a private address space, the nodes that are (NAT) configured. Non mentioned change will be done in the infrastructure of the existing network, thus keeping IPv4 business in work.	Complicated to be administered. Requires a considerable amount of configuration that will slow down packet flow. Some security risks especially with (NAT).
Tunnelling	Simple to be deployed. Allows the IPv6 packets to be transported over an	Must be manually configured in some cases. Possible problems with delay

Transition Mechanism	Strengths	Weaknesses
	IPv4 network.	and inactivity. Single Point of Failure (Tunnel endpoint). Additional CPU load to perform the Encapsulation/de-capsulation.

Source: 2014 [32]

Disadvantages of migrating to IPv6

In networking, there are many reasons why any migration to IPv6 should go or not go ahead, this can be determined by listing the pros and cons of the project. This is an overview list of the reasons why the transition to IPv6 should not go ahead. They are:

- A difficulty in time scheduling
 - For businesses the return on investment is uncertain
 - Interoperability with software packages and hardware equipment
 - Users are resilient to change protocols
 - Experience with new proposed protocol is limited
 - Equipment upgrades are uncertain in worth
- [35]

IPV6 Addressing Types

IPv6 supports three types of addressing. They are:

- Unicast – A source interface sends the packets to only one destination interface with a unique IP address. Also, a packet sent to a unicast address will be transferred to the interface that is identified by that address.
- Multicast – The packets may be sent for a set of destination interfaces belonging to different nodes. Also, a packet sent to a multicast address will be transferred to the interface that is identified by that address.
- Anycast – A source interface sends the packets to only one interface which is typically the closest one to the source interface. [6]

IPv4 and IPv6 Performance

Performance in LTE network

As the depletion of IPv4 addresses continues, network vendors and service providers have started to speed up the deployment of IPv6 into their networks. As it is very difficult to transition all their networks to IPv6 at once which leads to both internet protocols coexisting for a few more years in the future. In wireless networking, multiple transition techniques have been developed in order to support coherent transition from IPv4 to IPv6. These techniques are listed and discussed below:

- **Dual-stack** – Dual-stack devices consists of IPv4 and IPv6 stacks, they can maintain the same network topology as the IPv4 network and is very simple to deploy. Although, it still requires IPv4 addresses and some routers may have restricted capabilities to support and use IPv6 networks[8]
- **Tunnelling** – In order to send IPv6 packets of an IPv4 backbone network, a dual-stack edge router has to encapsulate the packets into IPv4 packets and transmits it to the IPv4 backbone network. To have a dual stack, it does not require any modifications to the backbone network and only edge routers are required.
- **Address Translation** – A NAT (network address translator) is located between IPv4 and IPv6 networks, in order to create a bridge in between those two networks. Address translation can be executed on the network layer (Layer 3) and above layers. On the layer 3, the IPv4 header is replaced to IPv6 header and vice versa.(e.g. 464XLAT) On the application layer, the IP address included in the application header is translated (i.e. DNS64) [36]

Performance of Wireless networks under several operating systems

In this conference paper, a test-bed survey was established in order to compare the IPv4 and IPv6 stacks alongside a set of six performance metrics. Also performed was a comparison of two IPv6 designs running Windows 2000 and Solaris 8 using similar hardware configurations.

Additionally, in two Microsoft OS, Windows XP and Windows Server 2003 are configured with IPv4 and IPv6 analytically analysed for differences and performance. Along with that, in two operating systems, Windows Vista and Linux Ubuntu are configured again with the two versions of Internet Protocol. Performance metrics such as network throughput, delay, jitter and CPU usage analytically measured on a test-bed designed. Furthermore, the results show that performance depends not only on the IP version and the network traffic type, but also on the selection of the operating system. [37]

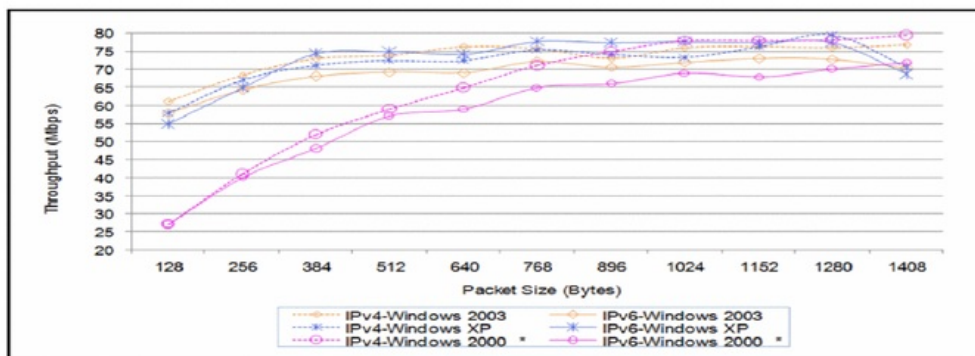


Figure 4: TCP Throughput of Windows Operating Systems [37]

IPv6 Adoption Performance

One of the most essential metric of IPv6 adoption is performance which can be categorised into different areas depending on the evaluation perspective. Below is a figure to show the work performed in comparing IPv4 and IPv6 performance with a hop distance of 10 and 20 for several years. [38]

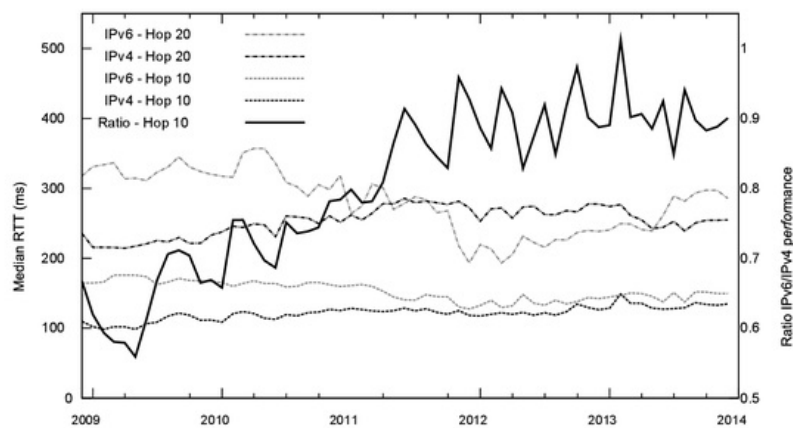


Figure 5: Median Round Trip Time (ms) with hop distance 10 and 20 for IPv4 and IPv6 [38]

Furthermore, another comparison of the two protocols was tested which was the five-ratios of IPv6 relative to IPv4 for seven metrics of their choosing. [38]

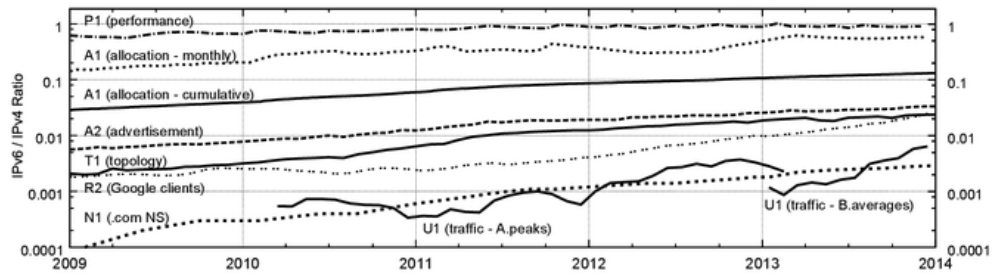


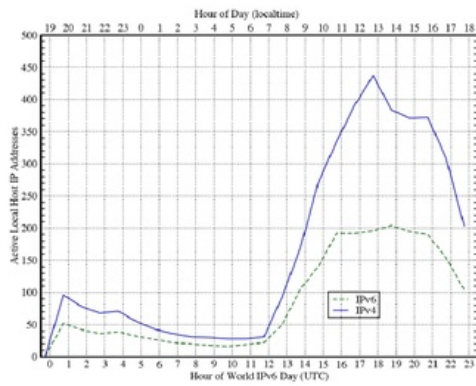
Figure 6: Ratio of IPv4 and IPv6 for seven metrics over the five years [38]

Performance of Internet Services on IPv6

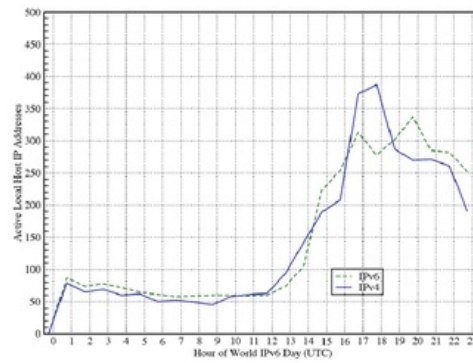
In this paper, a performance assessment framework was developed in order to assess the performance of Internet services over IPv6 on World IPv6 day which took place on June 8 2011. Two of most popular internet service, Facebook and Google Mail (Gmail) was selected to be monitored during the event of World IPv6 day. [39]

A) Facebook Active Client IP
Addresses

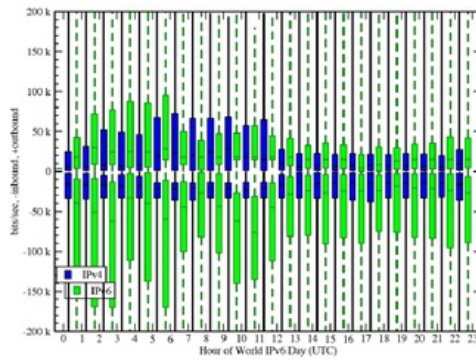
(B) Gmail Active Client IP
Addresses



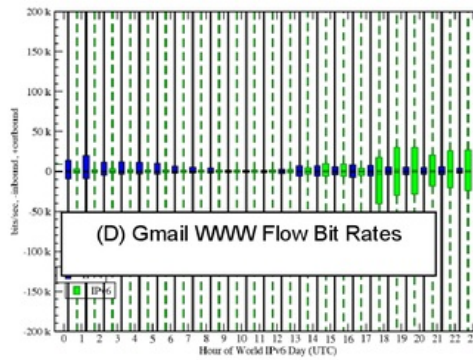
C) Facebook WWW Flow Bit Rates



(D) Gmail WWW Flow Bit Rates



(e) Facebook WWW Flow Bit Rates (detail)



(f) Gmail WWW Flow Bit Rates (detail)

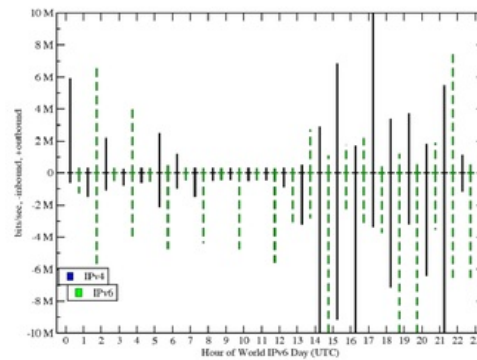
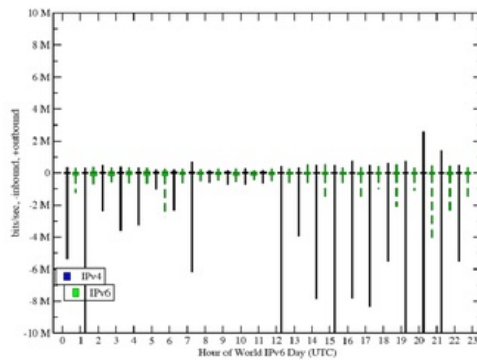


Figure 7: Active clients (4a, 4b), flow peak (4c, 4d) and detail (4e, 4f) performance for Facebook

Facebook Active Client IP Addresses (A)

In Figure 7 A, the number of active local hosts IP addresses for IPv4 and IPv6 that are active on Facebook is displayed on the graph. In the graph, the horizontal axis is labelled and displays the local time (UTC) each hour of the event of World IPv6 Day. Specifically, the lowest level of traffic activity is at the 06:00 and the highest level of traffic is at 12:00 noon, with the activity slowly decreasing towards the end of the event at about 17:00.

Gmail Active Client IP Addresses (B)

In Figure 7 B, the number of active local hosts IP addresses for IPv4 and IPv6 that are active on Gmail is displayed on the graph. In the graph, the horizontal axis is labelled and displays the local time (UTC) with the hour of the event of World IPv6 Day. The figure displays very similar amount of traffic in comparison to Figure 7A, this illustration shows that there is less activity with the amount of clients using Gmail. The reason for this is because the audience are more likely to check their Facebook to either check in or to share a post about the event.

Facebook WWW Flow Bit Rates (C)

In Figure 7 C, the graph presents the inbound and outbound flow rates, displayed with the local time of the event each hour. The figure also displays that the inbound rates from Facebook via IPv4 substantially exceeds the rates via IPv6. The reasons for this is because this service data is transferred to the client hosts' web browser.

Gmail WWW Flow Bit Rates (D)

In Figure 7 D, the graph demonstrates the inbound and outbound flow rates. Moreover, the figure displays that the inbound and outbound rates are approximately equal. Also, the graph provides details that in the hours of 1, 3,5,7,9 (UTC) shows that IPv6 exceeds the IPv4 rate.

Facebook WWW Flow Bit Rates (detail) (E)

In Figure 7e, the graph also displays the inbound and outbound flow rates. In this figure, it provides information that flow rates of Facebook are lower than 200kbits per second.

Gmail WWW Flow Bit Rates (detail) (F)

In Figure 7 F, the graph shows the inbound and outbound flow rates. Also, the figure demonstrates that the high activity of the local daytime, IPv4 and IPv6 performance seems approximately equal until after 17:00 when the IPv6 flows consists of a faster rates than IPv4 flow rates.

Performance comparison of IPv4 and IPv6 using OPNET

In this paper, it compares the performance of the two versions of protocol using the software OPNET. Many network parameters/metrics was investigated and compared such as: Ethernet delay, packet loss, jitter, response time and point to point utilisation. [23]

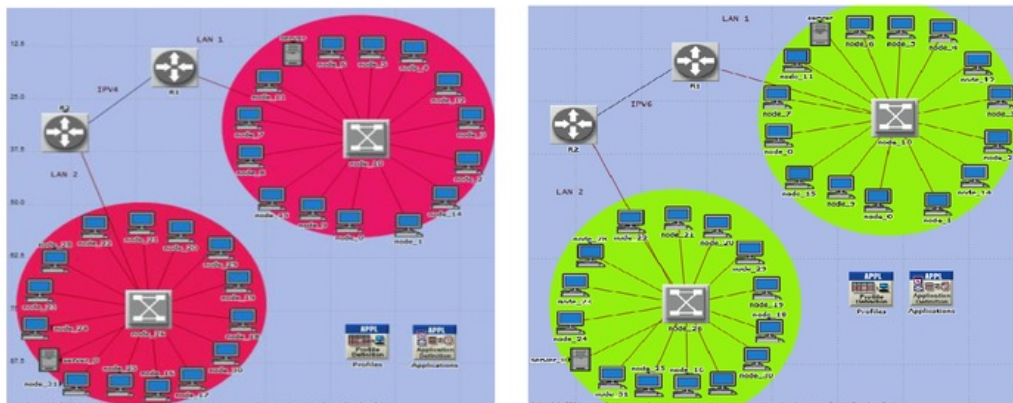


Figure 8: IPv4 and IPv6 Architecture [23]

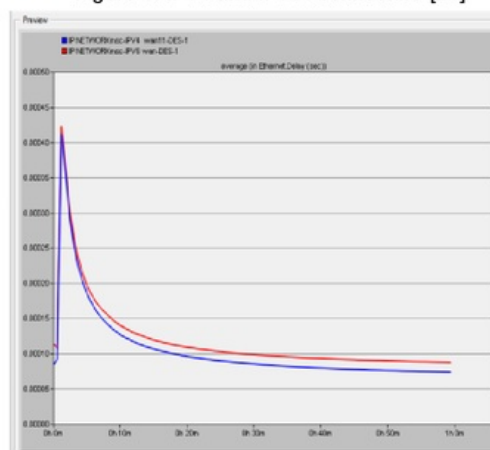


Figure 9: average Ethernet delay for both protocols [23]

In Figure 9, this graph is useful to use in the literature review, as it will provide as an asset in order to compare the results to the results and discussion chapter. This line graph provides evidence that IPv6 Ethernet delay is much faster than IPv4's. The reason for this is because the IPv6 header format was designed to support a large number of addresses and fast routing processes. As such, performing routing configurations in IPv6 should be faster due to the way its header format is designed.

Performance evaluation and comparisons of IPv4 and IPv6 using OPNET

In this paper, it compares the performance of the two versions of protocol using the software OPNET. Many network parameters/metrics was investigated and compared such as: packet dropped, Ethernet delay and http traffic received. [7]

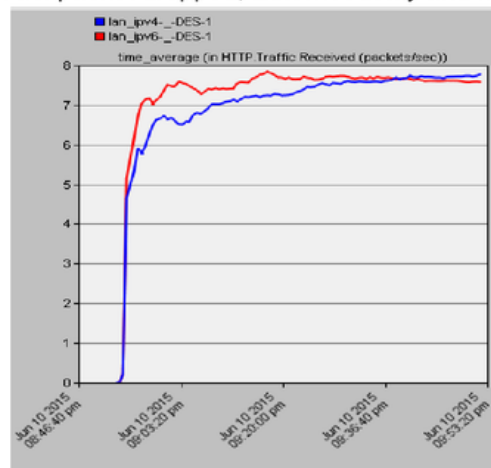


Figure 10: HTTP traffic received packets per second [7]

Figure 10 demonstrates the HTTP packets received per second using the configurations of IPv4 and IPv6. This is also another useful paper that is included

in the literature review, it can provide as a useful source (metric) to compare using IPv4 and IPv6 configurations.

When to choose IPv6

In modern day technology, there is a large increase in applications supporting the new protocol IPv6. This leads to end-users being influenced to migrate to the new internet protocol. When an IPv4 network reaches its limitation for any reason, it is time to choose IPv6. Ipv6 is developed sufficiently to be used in commercial networks, as shown in many case studies and deployments performed worldwide. Previously, high investments were provided in new IPv4 setup, repairs and complex configurations for IPv4. When the IPv4 network has reached its limits, it is important to consider evaluating IPv6 for end users' purposes. [28]

There are many reasons that may cause the end users to start considering to use IPv6:

- No more available IP address to use
- IPv4 network or NAT configurations needs to be repaired or extended
- Prepare the users' network for applications and software's that are established on the advanced features of IPv6
- Require an end-to-end security for a large number of users and there is no more address space available

Ipv6 Reliability

Reliability is one of the most important aspect for choosing to transition to IPv6. In this paper, it closely examines the transition mechanism of IPv4-in-IPv6 tunnelling which will be executed in a form of simulation scenarios. Four transition scenarios was developed in order to be evaluated such as 4over6, DS-lite, 4rd: NAT Centralization, and 4rd: NAT Distribution. [40]

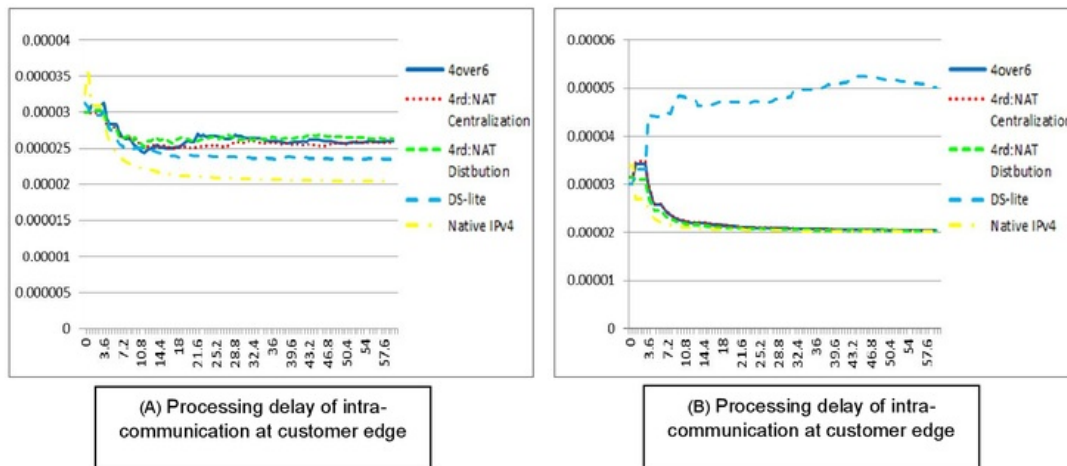


Figure 11: Processing delay of intra-communication [40]

In Figure 11 a, the graph shows processing delay on the equipment for initiating the communication tunnel for the traffic transition on the client's network, also known as the Customer Edge (CE).

In figure 11 b, the graph exhibits the metrics 4over6 and 4rd NAT distribution and centralisation have a delay in processing similar to the Native IPv6 as it can identify the tunnel-endpoint to the destination node.

2.6 Conclusion

To conclude, in this chapter each section from the research gained on this topic IPv4 and IPv6 has been thoroughly discussed and explained. To summarise, IPv4 is officially exhausted and depleted. Four of the regions (RIR) have declared that they are out of IP addresses. The only region that is still currently running is the Africa region (AFRNIC). Only 10% of the global population has accessed Google using IPv6 connectivity (January 2016).

IPv6 is the new protocol that was designed to fulfil the requirements of the world's population that consists of a high demand of IP address for their devices such as (Smartphones, Tablets, PDA's and laptops). IPv6 is suggested to be use when IPv4 is officially depleted all around the world. All the IPv6 characteristics and advantages are suitable sufficiently for the world to migrate to such as: IP address

space, built in security IPsec, distributes interoperability and mobile capabilities and finally IPv6 is easier to manage and more cost effective.

Chapter 3 – RESEARCH METHODOLOGY

3.1 Introduction

This chapter focuses on the projects' research methodology, in order to fulfil the aims and objectives the following experimental and theoretical research stages were acquired as the methodology of the research project. Most of the theoretical stages were mentioned in the literature review from the previous chapter.

3.2 Research Overview

In this section, it provides an overview of the entire project research processes.

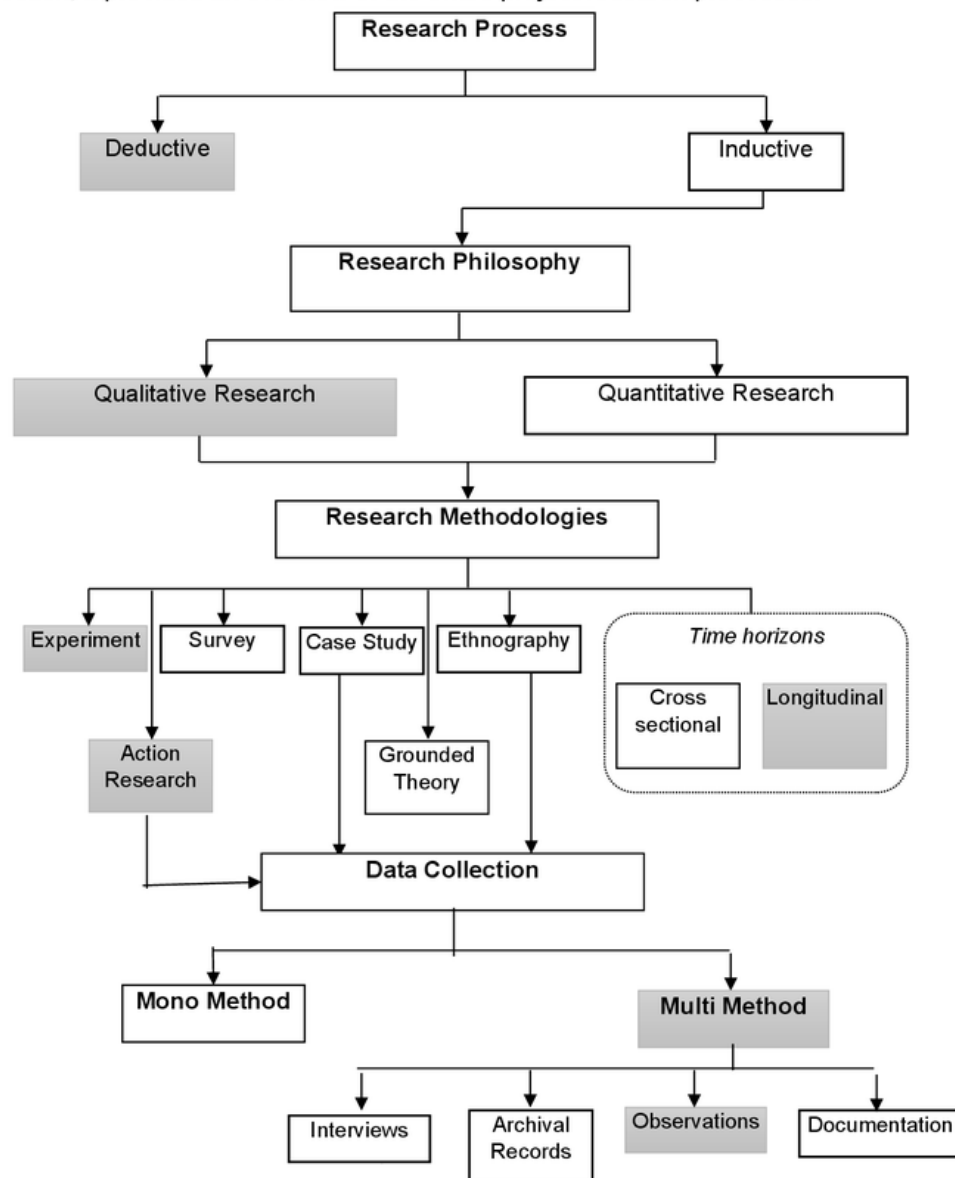


Figure 12: Research Overview

Above is the figure to display the research overview of this project. This illustrates the each of the research process for each stage of the projects' research methodology.

3.2.1 Research Process

The aims of this research process is to develop multiple network simulation scenarios in order to identify which protocol can be used for network design purposes.

3.2.2 Research Philosophy

In this project, the research onion model is used in order to follow the different stages of the data collection methods. This particular research model is one of the best methods in presenting how different research strategies and philosophies can be connected to each stage, each stage is presented into different layers. Below is an image which displays the different layers of the research model.

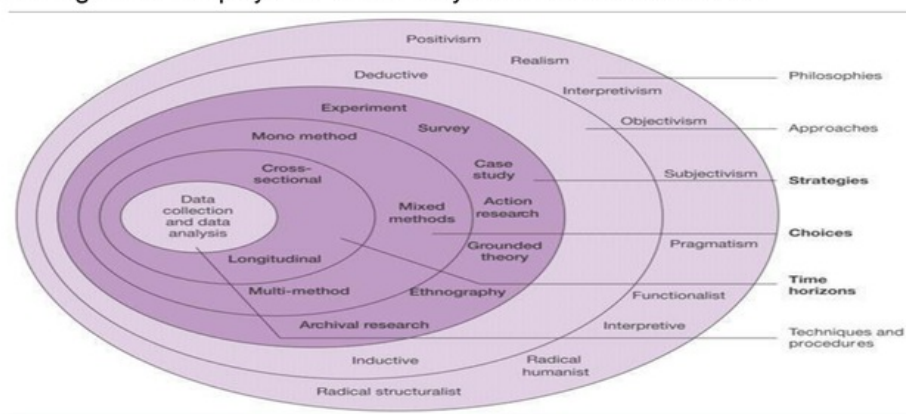


Figure 13: The Research Onion Model [41]

The philosophy that is most useful to this project is positivism as it is an experimental project. This philosophy is the most suitable for this project as it meets the aims and objectives. It is very useful as it is usually used in experimental projects and the data is collected will benefit the network designer with the simulation exercises.

The strategy that is selected to use for this project is the experiment strategy. This strategy is very useful as it uses a framework and uses an experiment testing process in order to see if the software feature performs in what is predicted. In this project, a simulation experiment test can be carried out on the performance of each of the protocol (IPv4 and IPv6) with different routing protocol configured for a simulation scenario such as delay, hop count and the performance of the topology.

3.2.3 Research Methodologies

In this project, the research methodology that is chosen to use the Waterfall model. A research methodology is a framework which is used to plan and design a project. It gives the reader a clear idea of what research methods and processes is going to be use in their research in order to achieve the research aims and objectives. Below is an image which displays the waterfall mode.

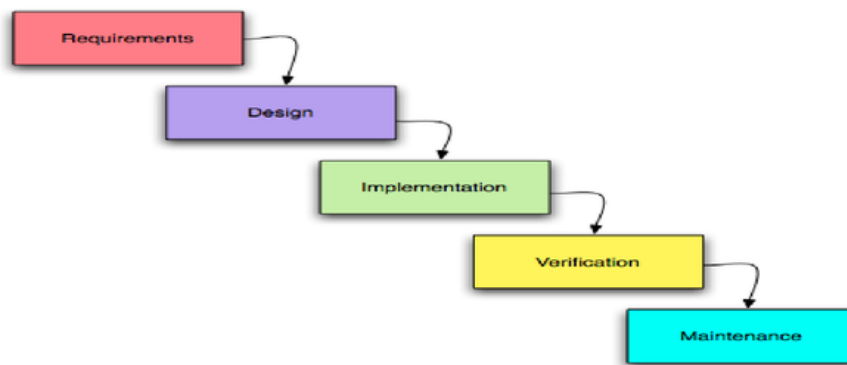


Figure 14: The Waterfall Model [42]

3.2.4 Data Collection

In this project, the data collection method that is chosen to use document review, it examines closely into the different past papers and documents that has been officially released by different organisations and companies.

There are many advantages when it comes to using this method such as:

- Reviewing past papers and documents provides the background and history of the topic

- Past papers are easily accessible from different database which also saves time and money for collecting data
- Information obtained from the documents is valid and reliable as it is collected from official resources

3.3 Research Deliverables

In this project, there are many different outcomes and deliverables that are expected when the experimental design is completed. The main outcome of this experiment is a fully network topology that displays results of multiple configured networks for each version of the Internet Protocol. This experimental project produces valuable information that can be used to determine in which protocol to use for different networking scenario purposes via routing protocol configurations.

The results and bar graphs are shown to help network engineers understand which routing protocols works well in each version of Internet protocol. The testing stages will include numerous simulation scenarios of a variety of different sizes of network, devices, configurations, features and structure in order that strengths and weakness are identified. Additionally, this makes the testing process fair on both protocol as each individual area is carefully evaluated into so that when it comes to analysing the results, the protocol can be clearly identified to use for certain network and routing protocol configurations. Furthermore, the results gained from this project will be compared to the previous papers that have been conducted over the previous on this topic.

Reliability and Validity

More importantly, it is imperative that all the data that the project produces and uses is obtain from a reliable source. In this project, all the sources that was used in completing the literature review was obtained from databases such as IEEE, ACM and Science Direct.

In addition, the validity of the data is also important, in this project the information gathered from the simulation design is a 100% valid as it is obtained from the software OPNET. Also, the entire work produced for this project design was produced from the network designer/analysis.

3.4 Conclusion

This chapter focuses on the research methodology, deliverables, strategy and processes. It explains each stage of the research process for this project. Also, it examines the research models that are used and the process within it that was used in order to complete this project.

Chapter 4– DESIGN AND IMPLEMENTATION

4.1 Introduction

This chapter discusses the different stages on the software design and implementation of the project. Along with that, this chapter will explain the different tools and stages that was used in order to design the network architecture for this project. Also, it will justify why and what devices where chosen to use in this design process.

The project consists of three different test-architectures. The first architecture is designed with IPv4 configurations, the second architecture is designed with IPv6 configurations and the last architecture is designed with both versions of IP configuration with security features. Another essential point, each scenario is configured with different configurations in order to execute a comparison between the two protocols.

4.2 Design

In this project, the OPNET simulation software (Riverbed 17.5 version) was used in order to compare the performance of IPv4 and IPv6. There are multiple performance metrics that was specifically used in order to compare the different features and the differences of each of the protocol such as: network delay, packets received, packet loss and bandwidth utilisation.

Network Components

In this simulation design, the network components that was used in the network topology, that was running on OPNET are twenty workstations, two switches and three routers outside the LAN network. Subsequently, the application definition parameters was configured for this scenario which was http and ftp. Along with that, the profile and application definitions was configured with applications such as http and ftp for this scenario.

This section discusses the following network components that are used in the network architectures:

- **Profile Config** – This feature was used to create user profiles and to generate traffic across the network

- **Application Config** - This feature was used to choose in which different applications and parameters to use in the network. The application name was used while designing the user profiles for the simulation design
- **Router Type** – ethernet2_slip8_gtwy_int, these routers were configured with RIP for the IPv4 scenario and RIPng for the IPv6 scenario, these routers were used to act as a gateway router, as all the three routers connect the two LAN together.
- **Switch Type** – ethernet32_switch, this type of switch was used in order to accommodate the amount of node devices in each LAN also if there are any future improvements this amount of ports is sufficient to be used
- **Workstation** – ethernet_wkstn, this workstation with client-server applications which is configured with FTP and HTTP
- **Server** – ethernet_server, this server is configured with client-server applications such as FTP and HTTP, this server was chosen in order to act as an Ethernet server in a local area network
- **Link Types**
 - **100BaseT** – This data link is used to connect hosts to routers or hosts to switches. This link is also capable at operating a connection at 100 Mbps
 - **PPP-DS3** – This link is used to connect routers to each other. It is capable of providing multiple connection speeds such as 10 Mbps, 100 Mbps, and 1 Gbps at one Ethernet connection, this was use to connect the routers in order to provide sufficient speed for the simulation

The objective of this experimental software design is to compare the two protocols by using two scenarios of a WAN network consisting of two LAN networks. Each scenario has three routers, two are connected to the switch and another router to connect the two routers; which allows the two LANs to connect to each other using the ppp-ds3 link. Figure 15 displays the two network architectures for this experimental project.

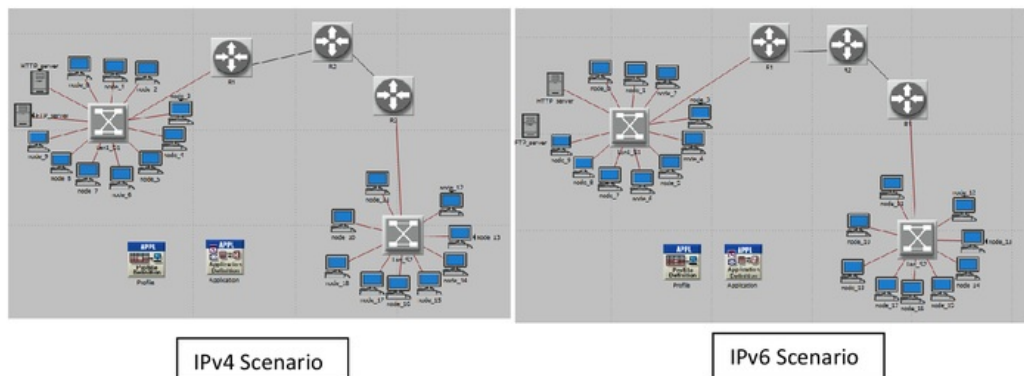


Figure 15: Project Network Topology

Network Topology

In this project, a star topology has been chosen to use in whilst designing the network scenarios. A star topology has many benefits to the network such as if one connection fails the rest of the network isn't affected, it is easy to install and add a device to a network.

Furthermore, this topology helps the network designer, in terms of that it is easier to troubleshoot for any faults or problems. Apart from that, it is also easy to remove any device that is connected to the network such as a printer, a server or a PC.

4.3 Implementation

Moreover, there are many tools that was used in order to fully complete this scenario design. Below is a list of the tools in OPNET:

- Simulation window – gathers and displays the simulation results
- Project window - displays and explains the network topology and link connections
- Node model – displays the interface of a network component

Another essential point, in each experiment scenario that was executed there were many results that was produced for this project. Each scenario has many different results, each result is based upon the metrics and parameters that was chosen.

In each scenario, the amount of nodes and devices remained exactly the same. The major difference with the configurations are the IP addressing and the routing protocol configurations. The client to server applications was configured with heavy browsing and high load on both scenarios and local network. This type of technique was chosen to use in order to solve how well the two versions of internet protocol would perform with that amount of traffic.

Another essential point, another tool that was used in order to show a difference between the scenarios if the IP configurations. In order to complete this step, the first scenario was designed using this method, Protocols>IPv4>Auto-Assign IPv4 Addresses. Next, the second scenario was configured using this method, Protocols >IPv6>Auto-Assign IPv6 Addresses.

4.4 Conclusion

In this chapter, it details the how was the software scenario was designed and implemented in order to undertake a performance simulation scenario of each protocol (IPv4 and IPv6). Network metrics such as Ethernet delay, ftp packet sent/received and http packet sent/received was compared with the same configurations in each version of protocol. Each result that was produced in this design is discussed and explained.

Chapter 5 –RESULTS AND DISCUSSIONS

5.1 Introduction

This chapter details the review from the data results produced from the previous chapter. It explains any patterns between the previous work in the journal papers and the data results gained the simulation scenarios.

5.2 Results and discussion

Firstly, the simulation ran for approximately 1 hour (3600 secs) which established the appropriate duration simulation in order to gain the sufficient amount of data from the network's behaviour.

One of the most important metric that was selected in this scenario design was Ethernet delay. Each scenario contains valuable information on this metric, figure 15 displays the average Ethernet delay for IPv4 and IPv6. Each simulation scenario was simulated in the duration of one hour.

In figure 16, it is clearly shown that the IPv6 delay is higher than IPv4. Also, the result of this particular simulation was expected because IPv6 has a larger header field in comparison to IPv4; the packets are also not transferred directly. Furthermore, this result is also similar to Al-Gadi et al simulation results in their experiment. [23]

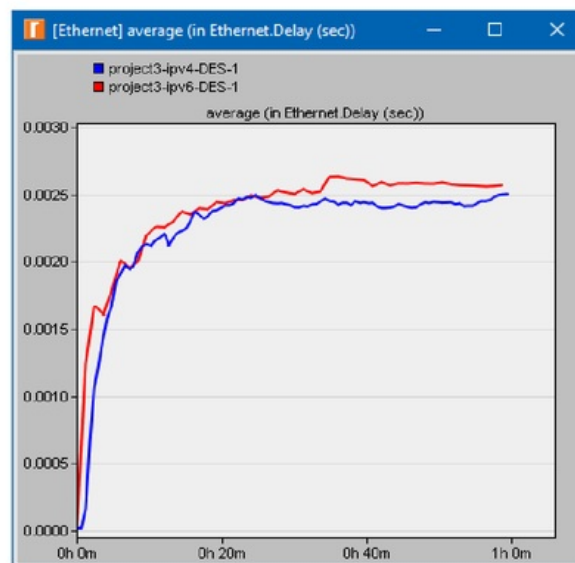


Figure 16: Project average Ethernet delay for IPv4 and IPv6

Secondly, the FTP server was configured with FTP configurations, the FTP server for each scenario is configured exactly the same. Each node in the network has an application destination of FTP in order to be able to send/receive packets from client to server or vice versa. Figure 17 displays that IPv6 sends and receives packet slightly faster than IPv4.

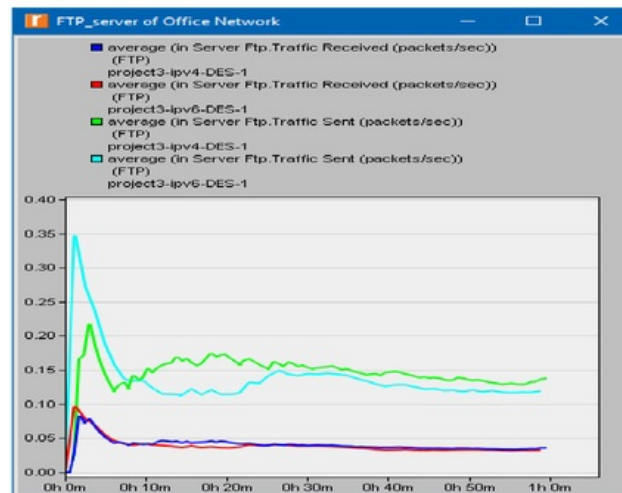
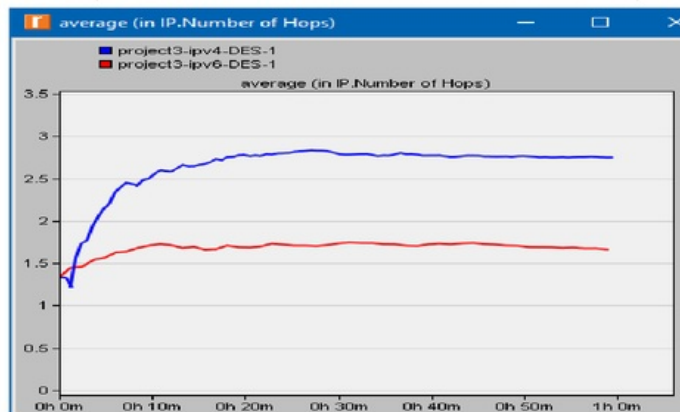


Figure 17: Project average FTP traffic sent/received per second

Also, the number of hops was also tested in each scenario. Figure 18 displays the details on the number of hops taken for each protocol. As clearly shown in the line graph, IPv4 average a high number of hops (approximately 2.5 hops) in comparison to IPv6 (1.4 hops). The network designer expected this as IPv6 requires fewer hops to reach the destination node. IPv6 requires few hops between hops.



network
[24]

Figure 18: Project average number of hops

HTTP object response time is the time it takes to response for each inline object from the HTML page. Figure 19 displays that IPv6 has a faster response compared to IPv4. HTTP server was configured for each scenario and is configured exactly the same except the IP addressing in the nodes. Each node has an application destination of HTTP in order to be able to send/receive packets from client to server or vice versa.

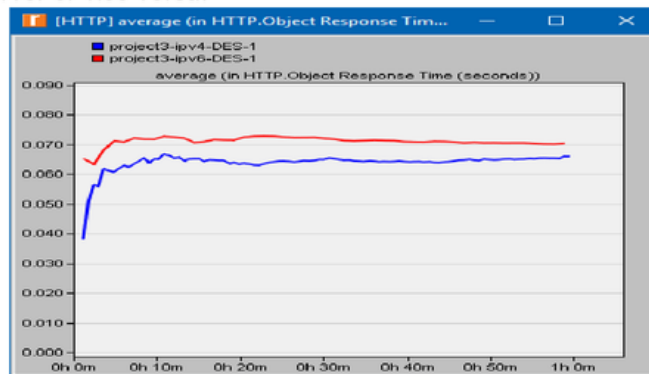


Figure 19: Project HTTP Object Response time

Figure 20 displays that IPv6 receives packets much faster than IPv4 with approximately about 10-12000 packets per second, this means that IPv6 is much faster than IPv4. At the start of the simulation, both protocols were fairly equal until approximately about five to ten minutes. Consequently, IPv6 greatly exceeds the amount of packets received until towards the end of the simulation.

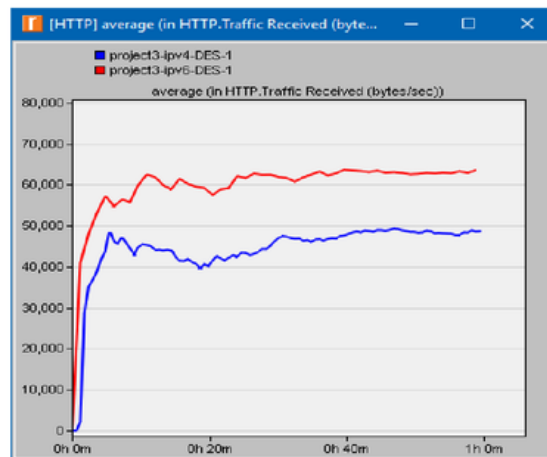


Figure 20: Project average HTTP traffic received bytes per second

Figure 21 displays that IPv6 has a higher average sent packets via the HTTP server. This graph is obviously very similar to figure 20 as that graph displays the average packets received bytes per second. As it shows, the traffic sent is the same as the received packets at the destination. This rules out the theory that there is a possibility of a packet loss throughout the process as the results are almost the same. Most of the past papers did not execute a comparison with packet loss, except Mahmoud et al where they covered packet loss comparisons of the protocols. [7] Furthermore, in this comparison of HTTP traffic, two sets of figures had to be provided because if they were demonstrated in the same figure, the traffic sent for the two protocols are too small to show.

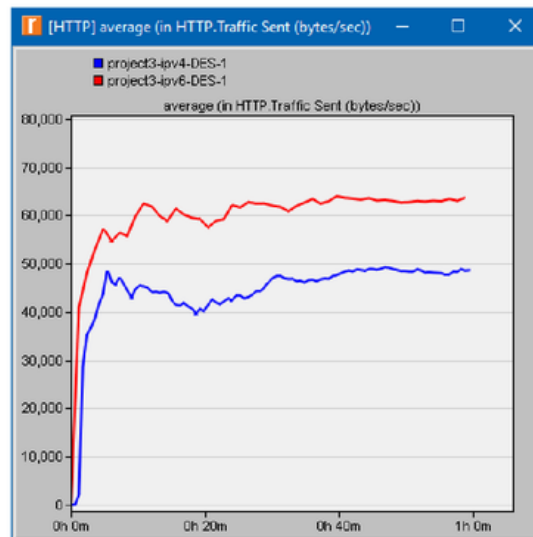


Figure 21: Project average HTTP Traffic sent bytes per second

Figure 22 displays the average IP traffic dropped for both the protocols. As shown, IPv4 IP traffic has dropped more traffic compared to IPv6, this figure clearly matches figure 17 showing the IP number of hops. IP traffic dropped packets per second is the numbers IP datagrams dropped by all the nodes across all the IP interfaces. There are few reasons why IP packet traffic is dropped such as exceeded maximum the number of hops and insufficient space in central

processor queue. In this case scenario, I believe that it comes to the reason of that IPv4 had to dropped the packets due to exceeding the amount of number of hops.

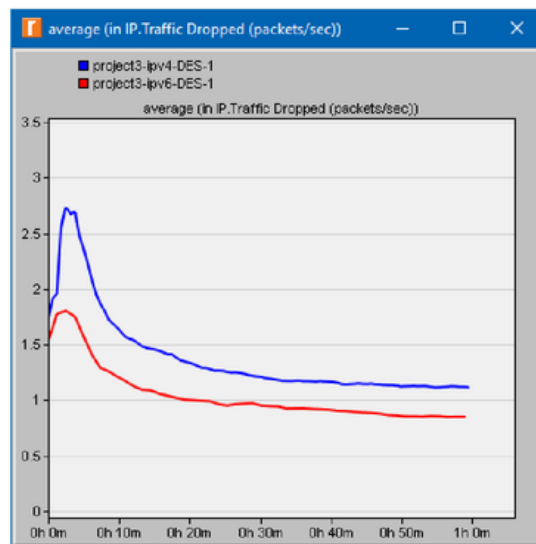


Figure 22: Project IP Traffic Dropped packet/sec

5.3 Conclusion

In conclusion, this chapter covered and discussed all the results and from the previous chapter. It compared the performance of the two protocols, the security architecture and risks/attacks, the header and address format and advantages and limitations of each protocol. The experiment results support some of the research data that was stated in the literature review. Accordingly, the analysis of IPv4 and IPv6 network scenario demonstrates that IPv6 is a much faster and is the superior protocol out of the two.

In the design and implementation chapter, it proved that IPv6 was certainly the best and superior protocol and should be considered to adopt to as IPv4 address space has become depleted. In this chapter, IPv6 was clearly shown that it was

the best protocol to use when it comes to designing a network with real-time applications and profile configurations.

Chapter 6 – CONCLUSIONS AND RECOMMENDATIONS

6.1 Summary

In this chapter, it provides an overall summary of the entire project. It briefly highlights and discusses the most important points of the previous chapters. Also, it covers how the design fulfilled the aims and objectives and what were the project outcomes.

6.2 Fulfilling the aims and objectives

To summarise, the results that was gained from the software design matched the research that was mentioned in the literature review. A lot of the results that was shown in the design chapters was very similar to the past papers that have been published in this topic.

The software design fulfilled the project aims and objectives that was set in place at the start of this project. The project also produce a background research on each element of the two Internet protocol versions which resulted in completing the objectives such as identifying the advantages and limitations of each protocol. The project was designed in the way from the information gained from the literature review for each protocol.

In this project, if it was to be undertaken again from the beginning, the network designer would have given more time in writing and researching the literature review therefore; more information could have been use in designing the experimental design.

6.3 Conclusion

To conclude, in this project report, an experimental design was carried out in order to compare the performance of the two versions of Internet protocol (IPv4 and IPv6); following the information such as structures, format and design ideas gained from the literature review. The software design consist of two scenarios configured with the same topology, however made up of different protocols and address configurations. From the literature review, it is clear that the world is ready to migrate to IPv6, however, IPv6 requires ISP to adopt to an expensive dual-stack network in order that IPv4 and IPv6 can communicate with each other. Also, ISP

have to deal with the problem of interoperability with application and hardware support whilst deploying IPv6 group of addresses to their customers.

From the results gained from the design and implementation chapter, it is very clear that IPv6 performed much better than IPv4 in the Ethernet delay, http traffic received and sent and ftp traffic received and sent. IPv6 should be used when dealing with real-time application configuration in comparison to IPv4.

6.4 Recommendations for further research

Suggestions for further work

In order to help people that are undertaking research using the network simulation tool (OPNET) in this topic. More research on the following elements will be useful for further research in this topic:

- Study can be extended into how the simulation tool OPNET operates
- Study can be extended into any software alternatives
- Study can be extended into the different aspects of the topic to help present more information to follow for the design and implementation stage
- Some resources were inaccessible due to requirement of payment

In this research study, there are many video tutorials that are available, however, many of these tutorials is restricted with the language barrier. It would be helpful to have more detailed tutorials available online to follow. Learning how to use the simulation tool occupied a lot of the network designer's time. It is highly suggested that a lot of research needs to be undertaken into using the software, before learning to use the software for design purposes, the different network topologies, configurations, tools, applications, profile and protocols.

Chapter 7 – REFLECTIONS

To review, I felt that whilst undertaking this project, I learnt a large number of important points about the topic and myself as a person. Firstly, even though I had the basic fundamental knowledge of IPv4 and IPv6, I was surprised of the fact the amount of research that has been performed in this topic which made easier for me to find the sources to reference for my literature review. I learnt that understanding how IPv4 and IPv6 operates has a large impact in the success of modern day computing. Furthermore, whilst creating and writing the literature review I learnt how the Internet Protocol evolved from decade to decade and the fact that IETF had tested three versions before finally releasing IPv4. Also, at the time of the deployment of IPv4, they believed that the amount of IP address was more than enough to accommodate the global population, however, IETF realised in the 90s the impending shortage of address space as a major limiting factor to the continued usage of the Internet.

This resulted in the development and deployment of a new version of Internet protocol which is IPv6. IPv6 was designed in order to accommodate the large amount of address space due to the rapid rise of IP address demand in the 90s. IETF simply added more IP address in IPv6 in comparison to IPv4 with 340 undecillion addresses. This new protocol also consisted a security architecture, allowed support for mobility and security, elimination of public-to-private NAT and contained a simplified header format in order for a more improved router efficiency.

Usually, it will take me a few weeks and constant review of the software tutorials and lessons in order for me to be competent in how to use the programme particularly in programming. Moreover, I was surprised of how quickly I adapted to become very comfortable in using the software OPNET for this project. I learnt how to operate the software's different tools and techniques by putting in a lot of time to test and explore the software.

Throughout the design and implementation stage, I realised it will take a long time and a lot hard work in order to understand most of the elements and tools that are used to help design the scenarios. During this time, I found a few tutorials,

manuals and troubleshooting guides to read and to learn how implement the guide into the software. Regardless of finding it difficult in learning how to operate OPNET, I enjoyed the challenge learning the different aspects and elements of the software. I believe that this is one of the major reasons why I had produce this amount of work on the design and implementation chapter. This was accomplished by playing about with the software, attempting what each button, tool and statistics would execute and demonstrate.

Additionally, as person I learnt that I can produce a good quality of work when I put hard-work and passion into the work. Also, whilst undertaking this project it helped me improve my time-management skills, as I had to solve the balance in managing my time to complete the project whilst having a part-time job. Apart from that, I had to also plan time aside to complete or to revise for exams and assignments during the course of the year.

I could have done this project much better by doing a lot more research in how the simulation tool OPNET operates, I wouldn't have had to spend a lot of time learning all the different tools and techniques just to design the two scenarios. Also, it took me quite a few attempts on how to get the software to save the work properly without it forcing itself to lose the configurations and to get the software to prompt me to back up the project whilst in activity for a few minutes.

Chapter 8 - REFERENCES

Below are a list of all the sources and resources that was used as references in this project report. These references help support the work that has been completed in this project.

- [1] A. Shiranzaei, "Internet Protocol Versions – A Review," vol. 202002, pp. 11–15, 2015.
- [2] A. Y. Korkusuz, "Introduction to IPv6 and Benefits of IPv6," 2012.
- [3] I. Van Beijnum, "It's official: North America out of new IPv4 addresses," 2015. [Online]. Available: <http://arstechnica.co.uk/information-technology/2015/07/us-exhausts-new-ipv4-addresses-waitlist-begins/>. [Accessed: 29-Oct-2015].
- [4] A. Ali, "Comparison study between IPV4 & IPV6," *Int. J. Comput. Sci. Issues*, vol. 9, no. 3, pp. 314–317, 2012.
- [5] M. Ahmad, "A comparative study on the performance of IPv4 and Ipv6," 2006.
- [6] K. Batiha, "I MPROVING IP V 6 A DDRESSING T YPES AND S IZE," vol. 5, no. 4, pp. 41–51, 2013.
- [7] A. Ibrahim, Y. Mahmoud, A. Babiker, and A. N. Mustafa, "Performance Evaluation and Comparisons For IPv4 & IPv6 Using OPNET Simulator," vol. 4, no. 8, pp. 2013–2015, 2015.
- [8] R. Uk, "IPV6 ROLLOUT IN THE UK A BIS Departmental Report," no. November, 2010.
- [9] A. Arin, "IPv4 and IPv6," p. 768, 1999.
- [10] M. Blanchet, "Migrating to IPv6," *Networks*, pp. 1–20, 2006.
- [11] M. Sportack, *IP Addressing Fundamentals*. Indianapolis: Cisco Press, 2003.
- [12] Cisco, "IP Addressing : IPv4 Addressing Configuration Guide , Cisco IOS XE Release 3S," no. 6387.
- [13] R. Graziani, "IPv6 Fundamentals," in *A Straightforward Approach to Understanding IPv6*, Indianapolis: Cisco Press, 2013, p. 8.

- [14] "Internet Protocol Version 6 - IPv6 Explained," *Oribt-computer-solutions*, 2015. [Online]. Available: <http://www.oribt-computer-solutions.com/internet-protocol-version-6-ipv6/>. [Accessed: 10-Nov-2015].
- [15] D. Goldman, "The Internet now has 340 trillion trillion trillion addresses," 2012. [Online]. Available: <http://money.cnn.com/2012/06/06/technology/ipv6/>. [Accessed: 25-Apr-2015].
- [16] A. S. Survey, P. Wu, Y. Cui, J. Wu, J. Liu, and C. Metz, "Transition from IPv4 to IPv6 :," vol. 15, no. 3, pp. 1407–1424, 2013.
- [17] J. Deng and K. Sun, "Comparison of RIP , OSPF and EIGRP Routing Protocols based on OPNET," 2014.
- [18] G. Huston, M. Rossi, and G. Armitage, "Securing BGP — A Literature Survey," *IEEE Commun. Surv. Tutorials*, vol. 13, no. 2, pp. 199–222, 2011.
- [19] C. Popoviciu, E. L. Abegnoli, and P. Grossetete, "Deploying IPv6 Networks," Cisco Press, 2008, p. 155.
- [20] F. F. Information, "IPv6 Routing : OSPFv3 Prerequisites for IPv6 Routing : OSPFv3 Restrictions for IPv6 Routing : OSPFv3 Information About IPv6 Routing : OSPFv3," vol. 3, pp. 1–14.
- [21] P. Richter, M. Allman, R. Bush, V. Paxson, and U. C. B. Icsi, "A Primer on IPv4 Scarcity," 1981.
- [22] D. Teare, *Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide*. 2010.
- [23] G. Yagoub, A. Yosif, A. Babiker, A. N. Mustafa, A. Yagoub, and A. Yosif, "Comparison Between Ipv4 And Ipv6 Using Opnet Simulator," vol. 04, no. 08, pp. 44–50, 2014.
- [24] "IPv4 vs. IPv6: How the Upgrade Improves Routing Efficiency." [Online]. Available: <http://www.telehouse.com/2015/08/ipv4-vs-ipv6-how-the-upgrade-improves-routing-efficiency/>.
- [25] P. Venkata, P. Reddy, K. Mohammed, I. Ali, B. Sandeep, and T. Ravi, "Importance and Benefits of IPV6 over IPV4 : A Study," vol. 2, no. 12, pp. 1–

2, 2012.

- [26] R. K. Murugesan, S. Ramadass, and R. Budiarto, "Improving the performance of IPv6 packet transmission over LAN," in *2009 IEEE Symposium on Industrial Electronics and Applications, ISIEA 2009 - Proceedings*, 2009, vol. 1, no. Isiea, pp. 182–187.
- [27] Y. Cui, Y. Chen, J. Liu, Y. Lee, J. Wu, and X. Wang, "State Management in IPv4 to IPv6 Transition," no. December, pp. 48–53, 2015.
- [28] M. Gupta, "IPv4 vs. IPV6 - The Next Generation Internet," 2010.
- [29] J. L. Shah, "Impact of IPSec on Real Time Applications in IPv6 and 6to4 Tunneled Migration Network," pp. 0–5, 2015.
- [30] O. J. S. Parra and A. P. Rios, "IPv6 and IPV4 QoS Mechanisms," pp. 5–7, 2011.
- [31] A. Turiel, "IPv6 : new technology ," *Netw. Secur.*, vol. 2011, no. 8, pp. 13–15, 2011.
- [32] A. S. Ahmed, R. Hassan, and N. E. Othman, "Security Threats for IPv6 Transition Strategies : A Review," pp. 83–88, 2014.
- [33] E. D. Ö and A. Buldu, "IPV4 / IPV6 security and threat comparisons," vol. 2, pp. 5285–5291, 2010.
- [34] D. G. Chandra, M. Kathing, and D. P. Kumar, "A Comparative Study on IPv4 and IPv6," *Commun. Syst. Netw. Technol. (CSNT), 2013 Int. Conf.*, pp. 286–289, 2013.
- [35] S. V Limkar, R. K. Jha, and S. Pimpalkar, "IPv6 : Issues and Solution for Next Millennium of Internet," no. Icwet, pp. 953–954, 2011.
- [36] J. Hyun, J. Li, H. Kim, J. Yoo, and J. W. Hong, "IPv4 and IPv6 Performance Comparison in IPv6 LTE Network," pp. 145–150, 2015.
- [37] H. M. A. Fahmy, "Performance Comparison of Wireless Networks over IPv6 and IPv4 Under Several Operating Systems," pp. 670–673, 2013.
- [38] J. Czyz, M. Allman, S. Iekel-johnson, E. Osterweil, and M. Bailey, "Measuring IPv6 Adoption," pp. 87–98, 2012.

- [39] D. Plonka and P. Barford, "Assessing Performance of Internet Services on IPv6."
- [40] N. Chuangchunsong, "Performance Evaluation of IPv4 / IPv6 Transition Mechanisms : IPv4-in-IPv6 Tunneling Techniques," pp. 238–243, 2014.
- [41] "No Title," 2015. [Online]. Available: <https://www.citethisforme.com/topic-ideas/business-marketing/Marketing and SERVQUAL model-6788992>.
- [42] D. Hughey, "The Traditional Waterfall Approach." [Online]. Available: <http://www.umsl.edu/~hugheyd/is6840/waterfall.html>.

Gantt chart

Below displays the original Gantt chart that was designed at the start of the project.

Task Name	Duration	Start	Finish
Project Introduction	2 days	Mon 05/10/15	Tue 06/10/15
Project Aims and Objectives	2 days	Mon 05/10/15	Tue 06/10/15
Literature Review	76 days	Mon 05/10/15	Sun 17/01/16
Research Methodology	6 days	Fri 22/01/16	Fri 29/01/16
Design & Implementation	22 days	Fri 29/01/16	Sun 28/02/16
Testing and Evaluation	20 days	Mon 29/02/16	Fri 25/03/16
Conclusion and Recommendations	10 days	Fri 25/03/16	Thu 07/04/16

Below displays the actual Gantt that was constantly updated during the completion the project.

Task Name	Duration	Start	Finish
Project Introduction	10 days	Mon 05/10/15	Fri 16/10/15
Project Aims and Objectives	10 days	Mon 05/10/15	Fri 16/10/15
Literature Review	116 days	Mon 05/10/15	Mon 14/03/16
Research Methodology	15 days	Mon 07/03/16	Fri 25/03/16
Design & Implementation	21 days	Fri 11/03/16	Fri 08/04/16
Testing and Evaluation	2 days	Fri 08/04/16	Mon 11/04/16
Conclusion and Recommendations	3 days	Mon 11/04/16	Wed 13/04/16

Glossary

Below is a list of the technical terms that was used in this research study. They are:

IETF – Internet Engineering Task Force, a large international group of network designers, engineers, operators and vendors that is mainly responsible for the evolution of the Internet.

IP – Internet Protocol, is a protocol that defines how a computer transfer data to another computer.

IPsec – Internet Protocol Security, is a set of protocols that provides security features to Internet Protocol.

NAT – Network Address Translation is a technique where a network device, assigns a public address to a workstation or a group of computer inside a private network.