ANALYSIS THE CONNECTION PERFORMANCE BETWEEN IPv6 NETWORK AND IPv4 NETWORKS USING GNS3 AND JPerf

THESIS REPORT

To Fulfill The Requirements Of obtaining A Master Program Degree In Engineering In The Master Electrical Engineering

Arranged by:

MUSAB ALI SALEH EL NEFATI

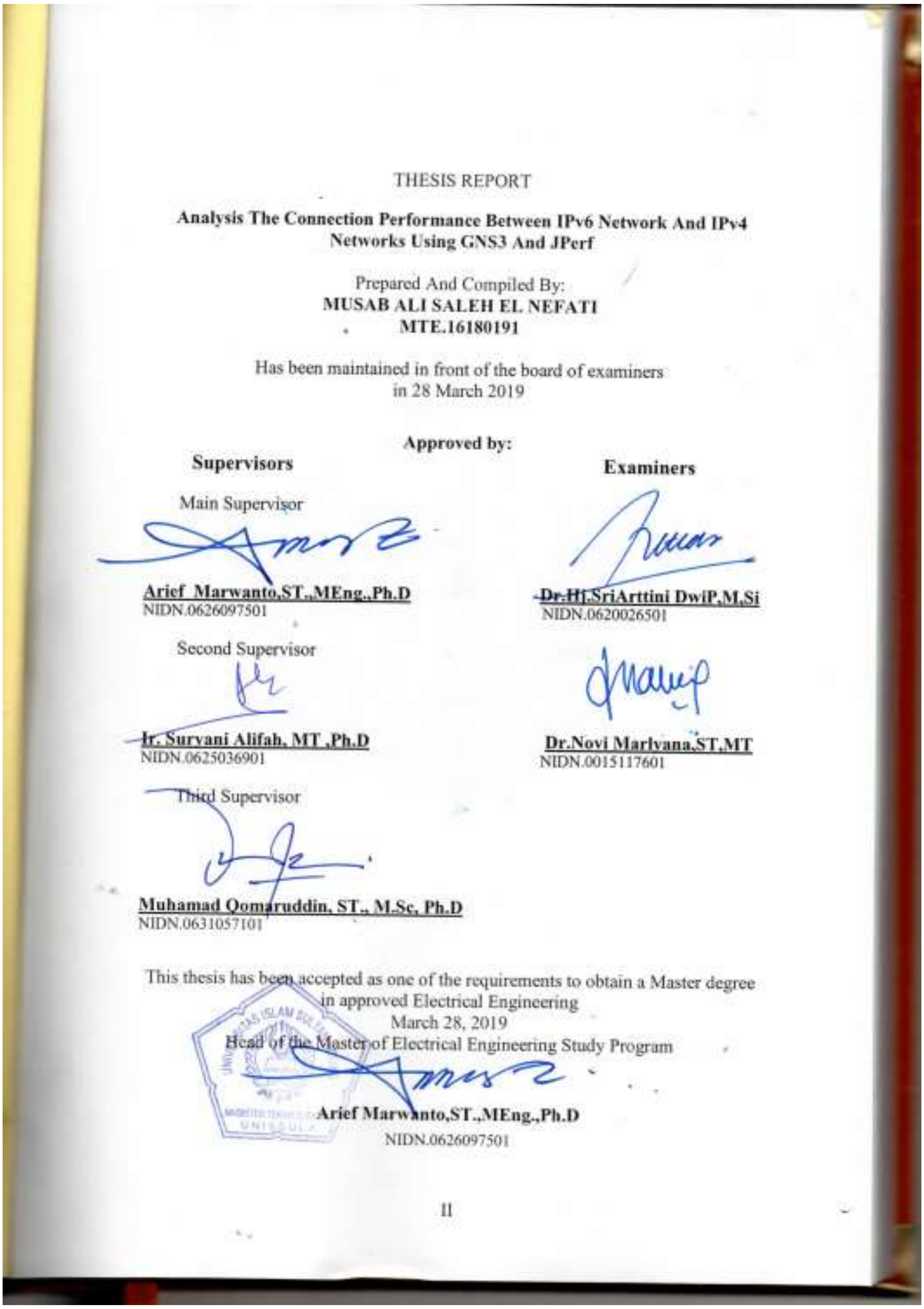
NIM: MTE.16180191

MAGISTER TEKNIK ELEKTRO

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM SULTAN AGUNG

SEMARANG
2019



THESIS REPORT

Analysis The Connection Performance Between IPv6 Network And IPv4 Networks Using GNS3 And JPerf

Prepared And Compiled By:
MUSAB ALI SALEH EL NEFATI
MTE.16180191

Has been maintained in front of the board of examiners
in 28 March 2019

Approved by:

Supervisors

Main Supervisor

Arief Marwanto,ST.,MEng.,Ph.D
NIDN.0626097501

Second Supervisor

Ir. Suryani Alifah, MT ,Ph.D
NIDN.0625036901

Third Supervisor

Muhamad Qomaruddin, ST., M.Sc, Ph.D
NIDN.0631057101

Examiners

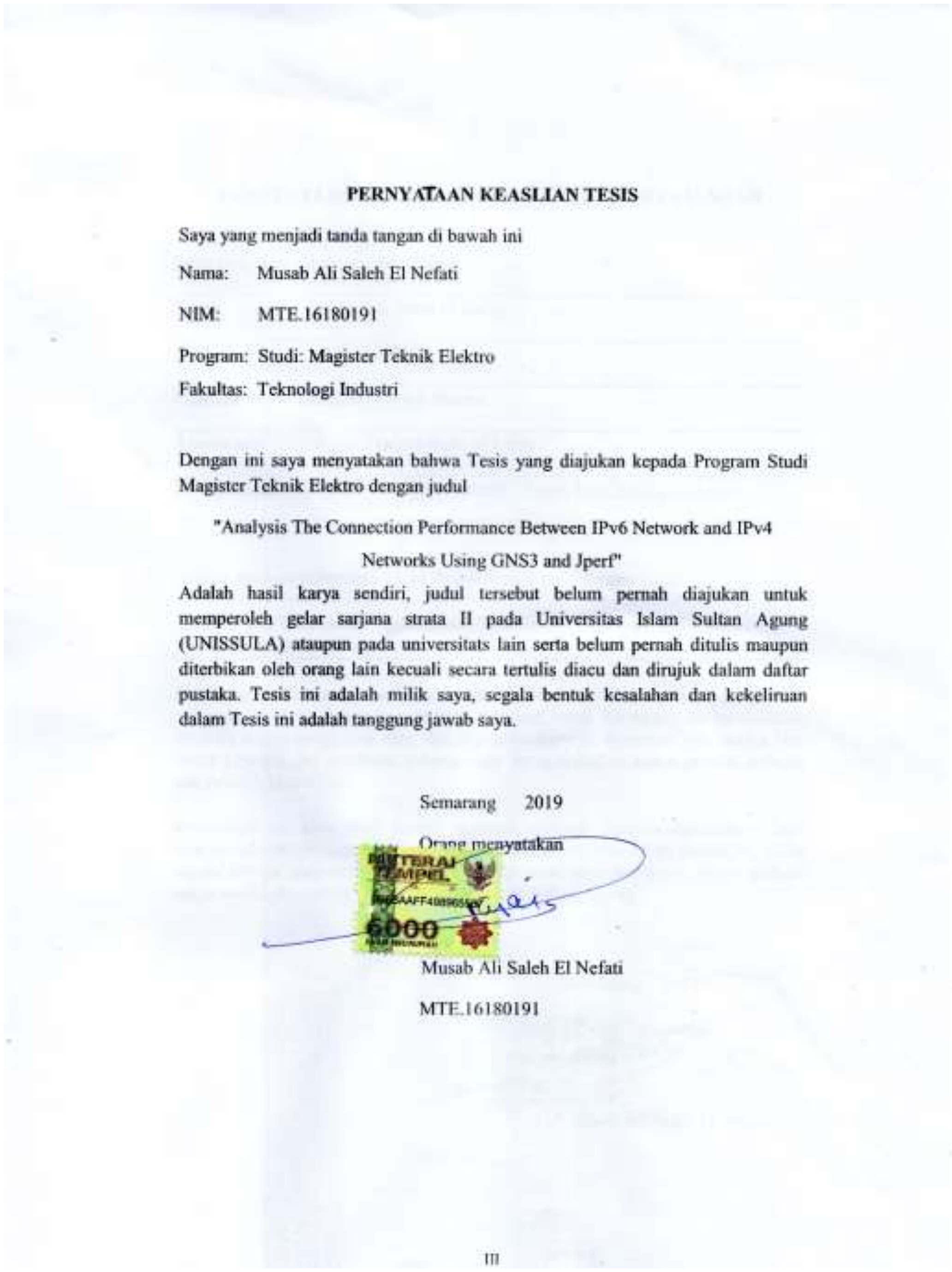
Dr.Hj.SriArttini DwiP,M.Si
NIDN.0620026501

Dr.Novi Marlyana,ST,MT
NIDN.0015117601

This thesis has been accepted as one of the requirements to obtain a Master degree
in approved Electrical Engineering
March 28, 2019
Head of the Master of Electrical Engineering Study Program

UNISSULA

Arief Marwanto,ST.,MEng.,Ph.D
NIDN.0626097501



PERNYATAAN KEASLIAN TESIS

Saya yang menjadi tanda tangan di bawah ini

Nama: Musab Ali Saleh El Nefati

NIM: MTE.16180191

Program: Studi: Magister Teknik Elektro

Fakultas: Teknologi Industri

Dengan ini saya menyatakan bahwa Tesis yang diajukan kepada Program Studi Magister Teknik Elektro dengan judul

"Analysis The Connection Performance Between IPv6 Network and IPv4 Networks Using GNS3 and Jperf"

Adalah hasil karya sendiri, judul tersebut belum pernah diajukan untuk memperoleh gelar sarjana strata II pada Universitas Islam Sultan Agung (UNISSULA) ataupun pada universitats lain serta belum pernah ditulis maupun diterbikan oleh orang lain kecuali secara tertulis diacu dan dirujuk dalam daftar pustaka. Tesis ini adalah milik saya, segala bentuk kesalahan dan kekeliruan dalam Tesis ini adalah tanggung jawab saya.

Semarang 2019

Orang menyatakan

METERAI TEMPEL

6000

Musab Ali Saleh El Nefati

MTE.16180191

KATA PENGANTAR

All praise and gratitude, the author prays to the presence of Allah SWT, because of the mercy and blessings of His author, I can complete this thesis, Allah willing, well. Solawat and greetings of the author always aim at the blessings of the Prophet Muhammad, His family, Sahabah, and his followers who always follow his teachings to the end of time.

This thesis is titled "Analysis of the Connection Performance Between IPv6 Network and IPv4 Networks Using GNS3 and Jperf "

He arranged for him to meet one of the conditions to achieve a Masters degree in the Master Program in Electrical Engineering, Faculty of Industrial Technology, Sultan Agung Islamic University, Semarang.

The author realizes that there are still many shortcomings and harmonies in writing this thesis. This is due to the limited knowledge and experience of the author, but thanks to all, encouragement, assistance and prayers from various parties, these obstacles can be resolved properly.

Therefore in this compactness the genius conveys the most loving to:

1. Arief Marwanto, ST, M.Eng ,, Ph.D as the main supervisor who has surprised many input, suggestions, took the time to help the author in the exploration of this thesis.
2. Ir. Suryani Alifah, MT, Ph.D as the second supervisor who has given input, advice, took time and convenience to the author in the preparation of this thesis
3. Muhamad Qomaruddin, ST, MSc, PhD as the third supervisor who has given input, advice, took time and convenience to the author in the preparation of this thesis
4. Dr. Hj Sri Arttini Dwi Prasctyowati, Dr.Novi Marlyana, ST, MT, who has been a examiner and gave many input and suggestions to the author.
5. All the lecturers in Master Electrecal Engineering Study Program of Sultan Agung Islamic University , which cannot be mentioned all by the author, have provided their knowledge and experience to the author, hopefully the knowledge that you provide is beneficial for all, hopefully you will always get reward from Allah SWT

6. Beloved father, beloved mother along with, my brothers ,sisters and my fiance all the big family who are always patient and unfamiliar I have given prayer, encouragement, motivation and enthusiasm when the author gets obstacles as long as the author starts studying until the completion of this study.

7. Friends of the 2018 Master of Electrical Engineering Study Program who always provide encouragement, motivation and enthusiasm as long as the author completes this thesis.

8. All Academicians of Sultan Agung Islamic University.

9. All Author's friends who can't be discharged, one by one, thank you for everything, so that the author can complete this thesis. In this shortness, the author uttered his apology as much as possible if the author has made many mistakes , both in terms of speech and behavior, all of that is purely from the author as an ordinary human who never escapes mistakes. Finally, the author hope that what is presented in this thesis can be useful for the development of science and technology. Hopefully all of this is blessed by Allah SWT. Amin.

Semarang, April 2019

Author

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

MOTTO

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيم

﴿ هُوَ الَّذِي جَعَلَ الشَّمْسَ ضِيَاءً وَالْقَمَرَ نُورًا وَقَدَّرَهُ مَنَازِلَ لِتَعْلَمُوا عَدَدَ السِّنِينَ وَالْحِسَابَ مَا خَلَقَ اللَّهُ ذَلِكَ إِلَّا بِالْحَقِّ يُفَصِّلُ الْآيَاتِ لِقَوْمٍ يَعْلَمُونَ ﴾
يونس{5}

صدق اللَّهُ العظيم

ABSTRACT

The IPv4 that is currently used is limited to handle new requests from IP addresses.To fix this problem IPv6 has been deployed. But the IPv4 can't be directly used , it should be get along with IPv6 . For the connection from IPv4 to IPv6 and opposite, there are three transition mechanisms. which are tunneling, translation and dual stack. In this research, the performances of these three mechanisms have been analyzed by GNS3 and JPerf in emulation system.the performance to get the results that shown of latency ,throughput and packet loss parameters for all the mechanisms as real time results.it can be seen that the Translation NAT-PT mechanism has the fast latency ,the tunneling has the best throughput and less packet loss and the dual stack keeps the moderating in all of the parameters .

Keywords: *IPv4; IPv6; Dual Stack; Tunneling; Translation.*

ABSTRAK

IPv4 yang saat ini digunakan terbatas untuk menangani permintaan baru dari alamat IP. Untuk memperbaiki masalah ini IPv6 telah digunakan. Tetapi IPv4 tidak bisa langsung digunakan, itu harus sesuai dengan IPv6. Untuk koneksi dari IPv4 ke IPv6 dan sebaliknya, ada tiga mekanisme transisi. yaitu Tunneling, Translation dan Dual Stack. Dalam penelitian ini, kinerja ketiga mekanisme ini telah dianalisis oleh GNS3 dan JPerf dalam sistem emulasi. Kinerja untuk mendapatkan hasil yang ditunjukkan dari parameter Latency, Throughput dan Packet loss untuk semua mekanisme sebagai hasil waktu nyata. Dapat dilihat bahwa mekanisme Terjemahan NAT-PT memiliki Latensi yang cepat, Tunneling memiliki Throughput terbaik dan kehilangan Packet yang lebih sedikit dan Dual stack menjaga moderasi di semua parameter.

.***Kata kunci:*** *IPv4; IPv6; Dual Stack; Tunneling; Translation*.

CHAPTER I
INTRODUCTION

1.1. Background

Each telecommunication device requires a connection to a calculation node, the connection between the calculation nodes requires a protocol, the number, the name, the origin of each packet, as each can define. The number of version 4 of the IP address, which is an update of the limited process of IP address requests. Internet bases (CIDR) are not protocol known as Internet Protocol version 4 (IPv4) that uses a cline wrapper without 32 bits: this protocol can cover around 4.3 million nodes in the world. The technology used is close to the IPv4 limit, which is the services and devices using 3G and 4G systems: Internet services (ISP) do not have enough IP to meet customer demand. Knowledge, problems, information, knowledge, knowledge, information and knowledge (VLSM), information and communication (CIDR), the existence of various problems in the field of translation. port addresses (PAT) and so on. However, all these technologies cannot recover the problem of not having an IP address. For this reason, the new version of IP can be important for manufacturers of the Internet's pace of development. Due to the limitations of IPv4 addresses, autonomous technologies have emerged: Internet Protocol version 6 (IPv6). IPv6, developed by IETF, is considered to be sufficiently efficient in terms of scalability, reliability, speed and security for IPv4. IPv6 is designed for the address space that is actually requested for Internet growth. IPv6 increases the IPv4-32 bit IP address layout to 128 bits [1]. In addition, the size for IPv4 is possible because it uses 128 bits, which encompasses all nodes, and any service must require IP both now and in the future.

Access the new generation IP to launch China, India and Japan. IPv6, 340 trillion, trillion, trillion nodes, IPv4 contains only 4.3 billion nodes. This will contribute to the construction of the necessary infrastructure for future development. IPv6 does not correspond to NAT as IPv4 because it provides security. IPv4 uses NAT as security, but its functionality is not primarily for security. Flow control gives high priority to some traffic to prevent congestion and connections with IPv6 will be end-to-end. In addition, IPv6 headers are simpler than IPv4. Growing, but with a higher-performing reflection, contains less space on which the data is processed. Failure to do with IPv6 is CRC because the package has been checked in the lower layer and therefore it is not necessary to check the upside errors. As a result, the processing time is reduced.

Switching from IPv4 to IPv6 requires a uniform method of disconnections and errors in the network. This requires a significant management of the main nodes, devices and systems for new IP generation. However, IPv6 addresses still work with IPv4 addresses; This means that IPv6 networks will join future IPv4 networks. However, IPv4 does not support the new network criteria. The current IPv4 network is large and complex, because IPv4 cannot be changed with IPv6. Switching from one technology to another is very difficult, because IPv4 and IPv6 are not the same set of communications. Three well-known transition mechanisms are known as Dual Stack, tunneling and translation [2].

A comprehensive study of the IPv4 transition to IPv6 has been carried out. When comparing Dual Stack, Tunneling, and Translation mechanisms, it has been found that Dual Stack provides better efficiency in terms of throughput and UDP results. Dual Stack is capable of implementing IPv4 and IPv6 on the same device, unlike Tunneling and also does not require additional address translators, such as when dealing with network translations. But Dual Stack costs are more because it is necessary to support IPv4 and IPv6 addresses.

Tunneling mechanisms generally tend to cause excessive load on ISPs and are more difficult to implement when compared to the other two mechanisms. Translation mechanisms on the other hand tend to have less feasibility and also require a separate device called Network Address Translator (NAT) to do address translation. To improve the efficiency of the Tunneling mechanism, techniques for IPv6 header compression have been applied. In this process the size of the header of an IPv6 packet decreases mostly from about 40 bytes of IPv6 headers to 6 bytes to provide better network results. The Dual

Stack and Tunneling mechanism can be implemented using the RIP and OSPF routing protocols. By implementing the RIP and OSPF protocols can make it easier for devices on the network to find a better routing path. Based on information collected from changes in dynamic link status, modifications can be made in the network in the event of a failure. In finding the best routing path, it is also possible to simultaneously reduce traversal costs.

1.2. Problem Statement

Based on the description in the background above, the formulation of the problem of the research is the performance of Dual Stack, Tunneling and Translation between IPv6 Network and IPv4 Network using emulation system more than simulation system are analyzed:

1. How the performance of dual stack, tunneling, and translation are analyzed?
2. How the performance of dual stack, tunneling, and translation in emulation system?

1.3. Objectives of the Research

As stated before, three eminent transitional components are widely known as Dual Stack, Tunneling and translation using emulation system more than simulation system. The purpose of this research is:

1. To analyze the mechanism dual stack, tunneling, and translation performance mechanism between IPv6 Network and IPv4 Network which is analyzed using GNS3 and JPerf.
2. To analyze the performance of dual stack, tunneling, and translation performance mechanism between IPv6 Network and IPv4 Network which is analyzed using GNS3 and JPerf in emulation system.

1.4. Thesis Contribution

By analyzes the performance in dual stack, tunneling, and translation, deeply understanding of comparative perform between IPv6 Network and IPv4 Network are describes.

1.5. Limitation of Works

Limitation of a problem is used to avoid the existence of irregularities and broadening the subject matter so that the research is more directed and facilitates discussion so that the research objectives will be achieved. Some of the limitations of the problem in this study are as follows:

Analyze dual stack, tunneling, and translation performance mechanism between IPv6 Network and IPv4 Network which is analyzed using GNS3 and JPerf in emulation system.

1.6. Research Originality

The difference between this research and the previous studies is that the previous studies used simulation tools that produce unreal results such as Packet Tracer and Opnet tools, but in this research were use emulation tools. These tools produce real time results at variance the tools which used in previous studies.

1.7. Outline Thesis Organization

To understand this thesis in order to obtain an overview of its contents, it is compiled by outlining in systematics as follows:

CHAPTER I INTRODUCTION

This chapter contains background, problem statements, objectives of the research, purpose of the research, thesis contributions, scope of works and outline thesis organization.

CHAPTER II LITERATURE REVIEW AND THEORY

This chapter contains literature review and theory about dual stack, tunneling, IPv4, and IPv6.

CHAPTER III RESEARCH METHODOLOGY

This chapter contains of general research model, proposed system model, performance analysis, simulation process, and summary.

CHAPTER IV RESULTS AND DISCUSSION

This chapter contains a discussion of the performance mechanism of Dual Stack, Tunneling and Translation between IPv6 Network and IPv4 Network

CHAPTER V CONCLUSION

This chapter is a conclusion of the discussion of the problems obtained from the research, besides that in this chapter also contains suggestions that are expected to be useful for the community.

CHAPTER II
LITERATURE REVIEW AND THEORY

2.1. Literature Review

Several studies related to the replacement of IPv4 and IPv6 networks have been investigated, which increases the demand of the Internet, which represents a big problem due to the exhaustion of existing IPv4 networks (Internet Protocol version 4). To overcome this situation, you must use version 6 of IP in the coming years. But IPv4 networks will not be excluded, but will also coexist with IPv6 networks. For the transition from IPv4 to IPv6 and vice versa, three transition mechanisms are used. They are Dual Stack, Tunneling and Translation. In this study, the IPv6 header, security and routing format has also focused on simulation software Packet Tracer simulation[3].

Other studies discussing IPv4 address space will disappear so that a transition to IPv6 is needed, which allows a wider address space but has limitations that inhibit its growth. IPv6 resolves problems that exist in previous versions of the protocol and provides new opportunities too. However, due to increased overhead costs in IPv6 and their interaction with the operating system that Hosts this communication protocol, there may be network performance problems. This study focuses on considerations that affect network performance analysis for IPv4 and IPv6-based networks for Ubuntu 10.0.4 open source Linux-based Operating Systems are used above virtual infrastructure. Ubuntu is configured with two versions of IP and empirically evaluated for performance differences. Performance-related metrics such as throughput, delay, and jitter are measured in the implementation of test-beds[4].

IPv6 is very popular among companies, organizations and Internet service providers (ISP) due to the limitations of IPv4. To avoid sudden changes from IPv4 to IPv6, three mechanisms are used to provide a seamless transition from IPv4 to IPv6 with minimal effects on the network. This mechanism is Dual Stack, tunnel and translation. This study will provide information on IPv4 and IPv6 and will evaluate IPv6's automatic and manual transition strategies comparing their performance to show how transition strategies affect network behavior. This experiment is executed using OPNET Modeler, which simulates networks that contain wide area networks (WAN), local area networks (LAN), Hosts and servers whose results are presented in graphs and tables, with a more detailed explanation. This experiment uses different measures, such as performance, latency (delay), queue delay, and TCP delays.[5]

Next generation internet protocol, known as IP Next Generation (IPNG), and later as IPv6, has been developed by the Internet Engineering Task Force (IETF) to replace the current Internet Protocol (also known as IPv4). Integration of IPv6 into the current network, several transition mechanisms have been proposed by the IETF IPng Transition Working Group. This study examines and empirically evaluates two transition mechanisms, namely 6-over-4, and IPv6 in IPv4 tunneling, because they are related to IPv6 performance. The results of this study explore the impact of this approach on the performance of end-to-end user applications using metrics such as throughput, latency, Host CPU utilization, TCP connection time, and the number of TCP connections per second that clients can create with remote servers. All experiments were carried out using two dual stack (IPv4 / IPv6) routers and two end-stations running Windows 2000, loaded with multiple IPv4 / IPv6 stacks[2].

Research conducted by Punithavathani and Sankaranarayanan (2009) shows that IPv4 and IPv6 are incompatible protocols. When both versions of IP are available and Internet users want to be connected without any restrictions, a transition mechanism is needed. During the time of migration from IPv4 to IPv6 networks, a number of transition mechanisms have been proposed by the IETF to ensure a smooth, gradual and independent transition. The IPv4 / IPv6 transition always occurs in the process of deploying IPv6-based services on the IPv4 Internet. The Next Generation Transition Working Group IETF (NGtrans) has proposed many transition mechanisms to enable the integration of IPv6 facilities into the current Network. This works especially addresses the performance of various tunneling transition mechanisms used in different networks. The effect of this mechanism on end-to-end application performance is explored using metrics such as transmission latency, throughput, CPU utilization and packet loss. Latency and throughput measured from the ipv6 to ipv4 mechanism are better than the tunnel and tunnel mechanisms that are configured, the ipv6 to ipv4 mechanism must work harder (greater overhead) for each packet sent, and therefore must run on more CPUs high utilization of edge routers. Larger packages have a higher loss rate, for all three tunneling mechanisms[6].

Other research shows that the IPv6 analysis transition mechanism, dual protocol stack, tunneling mechanism 6 to 4, and ISATAP tunnel network performance in general, results show that dual network IPv6 protocol stack has better performance than IPv4 dual stack protocol, and mechanism 6 to 4 and the ISATAP mechanism[7].

The period of coexistence between IPv4 and IPv6 networks, it is important to examine the effect of using IPv6 transition techniques on application performance. Evaluate certain user application performance for three transition techniques: dual-stack, 6to4 automatic and manual tunneling. Experimental assets have been carried out using the OPNET network simulator to evaluate the performance of five applications: web browsing, file transfer, voice, email and database access to transition techniques and compare application performance over pure IPv4 and IPv6 networks. The final results show variations in application performance between dual-stack, 6to4 automatic tunneling, and 6to4 tunneling manuals. The Formost application, dual-stack performs better than tunneling with respect to response time. In some cases, tunneling is performed better than dual stack related to other performance parameters, such as throughput and Jitter[8].

The actual transition from IPv4 to IPv6 requires network administrators to be aware of the next generation protocol and related risk issues. Because of the scale and complexity of today's internet architecture how to protect from existing investments and reduce the negative influence on users and provider services during the transition from IPv4 to IPv6 is a topic of the future that is very important for the advanced version of internet architecture. Research comparing IPv6 transition mechanism methods such as Dual Stack, Tunneling problems such as IPv6 automatic tunneling and manually configured tunneling considerations, IPv6 transition scenarios, IPv6 transition security issues, highlighting IPv6 and IPv4 threat reviews with automatic tunneling and consideration of tunneling configurations. Based on the results of this study propose a transition threat model for automatic tunneling and configuration tunneling that can be followed by University of Mysore (UoM), to estimate tunneling automatic and manually configured tunneling threat issues. Furthermore, there are different tunneling mechanisms such as: IPv6 through IPv4 GRE Tunnel, Tunnel broker, Automatic IPv4 - Compatible Tunnel and Automatic 6-to-4 Tunnel and also describes many common threats known to IPv6 and then compares and distinguishes how threats this is similar, can affect IPv6 network[9].

Research that investigates dual stack and tunneling technology while also looking at security risks from IPv6 and transition technologies. The IPv6 transition depends on the transition mechanism to complete a successful migration. Therefore both the stack mechanism and double tunneling are important elements that need to be investigated further. Both of these transition mechanisms allow IPv4 and IPv6 devices to work on the same network in the various ways described above, but leave behind severe vulnerabilities. As in the network, there are security implications that must be investigated. The mechanism of IPv6, dual-stack and tunneling has the risk. The two most common attacks that can be seen in the IPv6 protocol, dual stack and tunneling technology are DoS attacks and spoofing; However, there are many other attacks that apply to every technology. The dual stack implementation and tunnel scenario allows us to understand the various complexities involved in each mechanism while also briefly investigating the associated security risks. Taking into account this security risk, we carried out several simple attacks to simulate the ease with which it could attack the network. The performance analysis carried out clearly shows that the mechanism for tunneling causes a few performance problems[10].

Research that compares the efficiency of translation between IPv4-IPv6 translators and original connections. By testing three open-source software packages: Ntd (NAT-PT implementation), Ecdysis (NAT64 implementation), and Apache HTTP proxy, by sending HTTP over TCP via an IPv6 packet to travel through each translator to be translated into IPv4, with replies coming back from the IPv4 network through translators. This study shows that Ecdysis NAT64 is quite efficient in practice, except perhaps for networks that have a significant number of large outgoing packets and multiple simultaneous connections. With small networks, NAT64 works relatively efficiently compared to other translation techniques. If only the original IPv6 connection is available and no other IPv4-IPv6 coexistence technique can be used[11].

IPv4 has demonstrated its capabilities in terms of reliability, security and fast data transfer. Because IP is limited to 4.3 billion with IPv4, new techniques such as NAT and IPv6 seem to solve IP problems and provide a much more sophisticated experience. However, the transition from IPv4 to IPv6 takes time. Therefore, there is something that is more necessary for transitional techniques to play their part in establishing a smooth communication between two versions of IP. Dual Stack, tunneling, translation are three well-known transition techniques available today. When the three techniques are compared, Dual Stack and tunneling provide 100% efficiency in data transfer when tested on a small network of 10 routers, each router has its own loop or network. But in Dual Stack, RTT or latency are high compared to tunneling and translation due to the complexity of the router. Compared to the dual stack, the performance of IPv6 is better than the Ipv4 package. Although the dual stack is flexible and very efficient, you can see better results when using a limited number of dual-stack routers. Get an Ace and fit better in a small topology. Tunneling is the best technique when the network is very broad and the data must be transferred between the IP versions of the same network through other IP networks. The highest performance is observed in tunnels due to the simplicity involved in data transfer. Translation techniques that work in a similar way to NAT are true when only IPv4 nodes wish to communicate only with Ipv6 nodes or vice versa.

Because the efficiency of this technique is low, more NAT64 or NAT-PT routers can be used to obtain the best results[12].

Research that uses simplified SHIM6 based algorithm MI46 which integrates Tunnel Broker and 6to4 tunnel mechanism to form an optimized method to make IPv4 users use IPv6 applications. With the MI46 algorithm, we can overcome the shortcomings of the 6to4 tunnel mechanism, that is, the 6to4 address is difficult to aggregate when used as a common method for visiting IPv6 networks. Meanwhile, we are improving the Tunnel Broker mechanism. In situations where two or more dual-stack Hosts communicate with each other, the MI46 algorithm can effectively reduce the burden of the IPv6-relay gateway, and users can get a better experience. Therefore, we conclude that MI46 is a better solution for making IPv4 users use IPv6 applications than Tunnel Broker and 6to4 tunnel mechanisms[13].

One of the main challenges faced by the IPv6 community in the past few years is to determine the scenario in which the transition mechanism must be used and which one should be chosen with a particular scenario. The results of comparative evaluations were carried out on three main IPv6 interoperative mechanisms; NATPT, TRT, and DSTM show that while DSTM performs well both NAT-PT and TRT place significant overhead on the network[14].

Potential fatigue from IPv4 addresses starts IPv6 development. The new version of the Internet Protocol offers more networks and Host addresses, but the transition from now to the new version has been very slow. There are several reasons for the slow transition: complexity and uniformity are the pioneers. Thus for the time being, various transition mechanisms have been developed. Each mechanism has related benefits and weaknesses. In this study the two mechanisms, namely configurable tunnel and 6to4 transition mechanism, have been empirically evaluated for performance. Both mechanisms are implemented on two different Windows Server operating systems and performance related metrics such as throughput, delay, jitter and CPU usage of the transition end nodes are measured. The results obtained in the test-bed show that TCP/UDP throughput and jitter values of the two mechanisms are similar, but the delay and CPU readings are very different depending on the choice of transition mechanism and operating system[15].

IPv4 to IPv6 transition is an inevitable process when deploying IPv6 networks on this IPv4 Internet. Both protocols are expected to coexist for several years during the transition period. A number of transition techniques exist to deal with a variety of different network requirements. One of them is a tunneling mechanism. Tunneling means encapsulation of one protocol to another so that the encapsulated protocol is sent as a payload on the network. In this paper, a scheme is presented for tunneling IPv4 packets in an IPv6 package. This scheme will be useful in the future when most networks will be converted into IPv6 networks that involve minimum IPv4 routing. This technique, combined with a dual stack approach, allows IPv4 applications to run and interact with other IPv4 applications in the IPv4 and IPv6 network environments without modification and recompilation, and without NAT, or any proxy or application gateway[16].

The connectivity test between IPv4 and IPv6 networks with multiple stack transition methods produces communication for IPv4 and IPv6 protocols. In the transition mechanism, communication is only possible for IPv4 networks with the only IPv6 network. In the tunneling transition mechanism, a combination of IPv6 packages with IPv4 has been successfully performed. The three mechanisms are better suited to the scope of the network; each transition mechanism can be advantageous depending on the network situation. Because the Dual Stack mechanism is easy to implement in the early stages of migration from IPv4 to IPv6, this device must support both addressing protocols (IPv4 and IPv6), which make the routing table the desired enchance and process and take longer. The transition mechanism is a good choice when IPv4 - only networks that want to communicate with IPv6 networks only. On the other hand, the tunneling transition mechanism is chosen for networks where double sided networks are IPv6 networks and intermediate networks are IPv4 networks[17].

Other studies present experimental validation of network solutions that can support mobility to IPv4 Hosts and IPv6 Hosts in network scenarios where

IPv4-IPv6 connectivity is needed. The study shows that with a combination of configuration tunnels, 6to4, NAT-PT, and the appropriate TRT transition mechanism, it is possible to provide cellular services in a variety of transition scenarios. Cellular services are handled in the perspective of nomadic users who need the ability to communicate with other Hosts with their home addresses independently of the current network location[18].

Along with the commercialization of IPv6 on a global scale, the entire IPv6 industry chain will mature gradually. However, even after the implementation of IPv6 in the real world, a large number of older IPv4 devices and applications will not disappear overnight. Although there are solutions and tools developed to help facilitate the IPv4 / IPv6 transition, some of them are focused on handling the situation of cellular terminals that might move between different WIFI and 3G networks. With application software designed and implemented, IPv4 cellular terminals can reach IPv6 resources in an experimental environment. In addition, Host mobility has been taken into account, and cellular terminals can remain in IPv6 when they move from one network to another, as long as new IPv4 addresses assigned to them allow new tunnels to be established. Qualitative and quantitative tests have proven the practical significance and effectiveness of solutions[19].

The increasing demand for smart devices, the growth of fast internet users and the global ICT market are very competitive. From a different perspective, IPv6 infrastructure is relatively better than IP4. However, it still has several challenges in implementation due to interoperability issues between IPv4 and IPv6. So the two networks work together for a longer period of time as a transition period. A strategic plan for migrating to the next generation Internet Protocol version 6 for service providers is recommended. This outlines a business continuity plan with a smooth transition approach to IPv6-operated networks by providing broad ideas to voice and data service providers who are in the early stages of migrating their networks to IPv6. Basically service providers from developing countries are in the early stages of migration.

Therefore timely network migration cannot be avoided to continue and expand the business for better sustainability[20].

With the fatigue of IPv4 addressing space rapidly approaching, it has become a high priority for service providers, companies, IP equipment manufacturers, application developers, and governments to start implementing their own IPv6. Smooth migration from IPv4 to IPv6 is difficult to achieve. Therefore several mechanisms are needed to ensure smooth, gradual and independent changes to IPv6. Not only transitions, IPv6 integration is also needed in the existing network. Solutions (or mechanisms) can be divided into three categories: dual stack, tunneling and translation. Dual Stacking is the solution of choice in many scenarios. Dual Stacked devices can operate with IPv4 devices, IPv6 devices, and other Dual Stacked devices. Tunnels can be created where there are IPv6 islands separated by IPv4 seas, which are the norm during the initial stages of the transition to IPv6. To experiment and understand the roles IPv6 will play in the future, it is important for us to develop direct experience with IPv6 technology. Through efforts to create a Dual-Stack network using GNS3 it has enabled us to develop expertise and become technically competent with IPv6 technology in the academic environment[21].

Table 2.1. Previous Study

No	Authors	Subject to Analysis	Methodology	Results
1	[2]	Two transition mechanisms, namely 6-over-4, and IPv6 in IPv4 tunneling	All experiments were carried out using two dual stack routers (IPv4 / IPv6) and two end stations running	impact of this approach on the performance of end-to-end user applications using metrics such as throughput, latency, Host

			Windows 2000, which were loaded with several IPv4 / IPv6 stacks	CPU utilization, TCP connection time, and the number of TCP connections per second that clients can create with remote servers.
2	[3]	Performance analysis of Dual Stack, tunneling and translation mechanisms.	Performance analysis of dual stack, tunneling, and translation mechanisms using Packet Tracer simulations and simulation software.	Three mechanisms have different advantages and characteristics, with some disadvantages. The appropriate transition mechanism will be selected for networks based on various parameters such as network size, latest device availability, costs, security issues, and so on.
3	[4]	IPv4 and IPv6 performance analysis	Network performance analysis for IPv4 and IPv6 networks for Linux and open source ubuntu10.0.4 operating systems used over the virtual infrastructure.	The difference in performance between IPv4 and IPv6 for the benchmark is approximately 486 KB / second in KB and 0.11 MB. Small TCP window sizes will reduce the throughput for IPv4 and IPv6. The actual maximum IPv4 and IPv6 throughput for 100 Mbps links will not reach 100 Mbps maximum.
4	[5]	Automatic and manual IPv6 transition strategies by comparing the performance of Dual Stack, Tunnel and Translation.	Automatic and manual IPv6 transition strategies by comparing dual stack, tunnel, and translation performance using OPNET Modeler, which simulates	IPv6 has a higher throughput than the other four and the manuals are higher at 6 to 4 at 5 Mbps. 6to4 and manual policies require manual configuration to detect sources, and manual tunnels are required to

			networks that contain Wide Area Networks (WANs), Local Area Networks (LANs), Hosts, and servers.	detect the creation of a point-to-point mechanism.
5	[6]	IPv4 and IPv6 transition mechanisms.	End-to-end applications are explored using metrics such as transmission latency, throughput, CPU utilization and packet loss.	IPv4 and IPv6 are incompatible protocols. When both versions of IP are available and Internet users want to be connected without restrictions, a transition mechanism is needed. During the migration from IPv4 networks to IPv6, a number of transition mechanisms have been proposed by the IETF to ensure a smooth, gradual and independent transition. IPv4 / IPv6 transition always occurs in the process of using IPv6-based services on the IPv4 Internet.
6	[7]	IPv6 analysis transition mechanism, dual protocol stack, tunneling mechanism 6 to 4, and ISATAP tunnel network performance	PC1 and PC2 are tested transmitter and receiver running with Windows operation system. Due to limited resource, routers are simulated with high-performance PC.	Dual network IPv6 protocol stack has better performance than IPv4 dual stack protocol, and mechanism 6 to 4 and the ISATAP mechanism.
7	[8]	Evaluate certain user application performance for three transition techniques: dual-stack, 6to4 automatic	Experimental assets have been carried out using the OPNET network simulator to evaluate the performance of five applications: web browsing, file transfer, voice, email	Variations in application performance between dual-stack, 6to4 automatic tunneling, and 6to4 tunneling manuals. The Formost application, dual-stack performs better than tunneling with respect to response time.

		and manual tunneling.	and database access to transition techniques and compare application performance over pure IPv4 and IPv6 networks.	
8	[9]	Comparing IPv6 transition mechanism methods such as Dual Stack, Tunneling problems such as IPv6 automatic tunneling and manually configured tunneling considerations.	IPv6 transition scenarios, IPv6 transition security issues, highlighting IPv6 and IPv4 threat reviews with automatic tunneling and consideration of tunneling configurations.	There are different tunneling mechanisms such as: IPv6 through IPv4 GRE Tunnel, Tunnel broker, Automatic IPv4 – Compatible Tunnel and Automatic 6-to-4 Tunnel and also describes many common threats known to IPv6 and then compares and distinguishes how threats this is similar, can affect IPv6 network.
9	[10]	Investigates dual stack and tunneling technology while also looking at security risks from IPv6 and transition technologies.	Simple attacks to simulate the ease with which it could attack the network. The performance analysis carried out clearly shows that the mechanism for tunneling causes a few performance problems.	The mechanism of IPv6, dual-stack and tunneling has the risk. The two most common attacks that can be seen in the IPv6 protocol, dual stack and tunneling technology are DoS attacks and spoofing; However, there are many other attacks that apply to every technology.
10	[11]	Compares the efficiency of translation between IPv4-IPv6 translators and original connections.	By testing three open-source software packages: Ntd (NAT-PT implementation), Ecdysis (NAT64 implementation), and Apache HTTP proxy, by sending HTTP over TCP via an IPv6	Ecdysis NAT64 is quite efficient in practice, except perhaps for networks that have a significant number of large outgoing packets and multiple simultaneous connections. With small networks, NAT64 works

			packet to travel through each translator to be translated into IPv4, with replies coming back from the IPv4 network through translators.	relatively efficiently compared to other translation techniques.
11	[12]	Transition techniques to play their role to establish smooth communication between the two versions of IP.	Used NAT64 or NAT-PT to knows transition techniques to play their role to establish smooth communication.	Translation techniques that work similar to NAT, are right when only IPv4 nodes want to communicate with only Ipv6 nodes or vice versa. Because the efficiency of this technique is low, more numbers of NAT64 or NAT-PT routers can be used for the best results.
12	[13]	Optimized method to make IPv4 users use IPv6 applications.	Uses simplified SHIM6 based algorithm MI46 which integrates Tunnel Broker and 6to4 tunnel mechanism	With the MI46 algorithm, we can overcome the shortcomings of the 6to4 tunnel mechanism, that is, the 6to4 address is difficult to aggregate when used as a common method for visiting IPv6 networks.
13	[14]	Comparative evaluations were carried out on three main IPv6 interpretative mechanisms	Used NATPT, TRT, and DSTM to comparative evaluations.	DSTM performs well both NAT-PT and TRT place significant overhead on the network.
14	[15]	Configurable tunnel and 6to4 transition mechanism.	Both mechanisms are implemented on two different Windows Server operating systems and performance related metrics such as throughput, delay, jitter and CPU usage	Test-bed show that TCP/UDP throughput and jitter values of the two mechanisms are similar, but the delay and CPU readings are very different depending on the choice of transition mechanism and operating system.

			of the transition end nodes.	
15	[16]	Presented scheme tunneling IPv4 packets in an IPv6 package	Combined with a dual stack approach	IPv4 applications to run and interact with other IPv4 applications in the IPv4 and IPv6 network environments without modification and recompilation, and without NAT, or any proxy or application gateway.
16	[17]	The connectivity test between IPv4 and IPv6 networks.	Multiple stack transition methods produces communication for IPv4 and IPv6 protocols.	The three mechanisms are better suited to the scope of the network; each transition mechanism can be advantageous depending on the network situation.
17	[18]	Experimental validation of network solutions that can support mobility to IPv4 Hosts and IPv6 Hosts	Network scenarios where IPv4-IPv6 connectivity	Combination of configuration tunnels, 6to4, NAT-PT, and the appropriate TRT transition mechanism, it is possible to provide cellular services in a variety of transition scenarios. Cellular services are handled in the perspective of nomadic users who need the ability to communicate with other Hosts with their home addresses independently of the current network location.
18	[19]	IPv4 to IPv6 transition	Application software designed and implemented, IPv4 cellular terminals can reach IPv6 resources	Host mobility has been taken into account, and cellular terminals can remain in IPv6 when they move from one network to another, as long as new IPv4 addresses assigned to them allow new tunnels to be established. Qualitative

				and quantitative tests have proven the practical significance and effectiveness of solutions.
19	[20]	Business continuity plan with a smooth transition approach to IPv6-operated networks by providing broad.	A strategic plan for migrating to the next generation Internet Protocol version 6 for service providers	Service providers from developing countries are in the early stages of migration. Therefore timely network migration cannot be avoided to continue and expand the business for better sustainability.
20	[21]	Several mechanisms are needed to ensure smooth, gradual and independent changes to IPv6.	Dual stack, tunneling and translation investigated.	Dual stack devices can operate with IPv4 devices, IPv6 devices, and other Dual Stacked devices. Tunnels can be created where there are IPv6 islands separated by IPv4 seas, which are the norm during the initial stages of the transition to IPv6.

Based on previous research, all studies examined the IPv4 to IPv6 transition and the performance of dual stacking, tunneling, and translation. The difference between the research that researchers conducted with previous research is the method used by researchers whose researchers conducted research using emulation instead of using simulations, as did previous research.

2.2. Theory

2.2.1. Dual Stack

The dual stack is a general system and the core of the transition technique between IPv4 and IPv6 networks. As indicated above, the Dual Stack technique can be applied between IPv4 and IPv6 addresses, it must be defined in the same network interface, this means that we can use routers, but we must use a separate interface for both ipv6 addresses. In the implementation of Dual Stack, all network devices, such as workstations, servers, routers, etc. To implement the dual stack, all devices must be compatible with the IP version and the additional processing power and simultaneously handle both protocols. Dual IPv4 / IPv6 transitions are important mechanisms needed in many end Hosts and network equipment during the transition period. The IPv4 / IPv6 Dual Stack transition mechanism is needed on many Hosts and network equipment during the transition period. It is recommended that all Hosts before fully migrating to IPv6 must have a dual stack protocol that is the final node / system must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6. The final system / sender Host (Source Host) will identify which version package must be sent to the receiving Host must be determined by sending a request to DNS, for example if the DNS returns an IPv4 address then the source Host sends an IPv4 packet. If DNS returns an IPv6 address, the source Host will send IPv6 packets . from the Figure 2.1 a typical dual stack scenario has been shown [22].

The dual stack approach is considered one of the most straight forward transitions. This dual stack method assumes that both the Host / router provides support for both IPv4 protocols, IPv6 in its architecture and has the ability to send / receive IPv4 and IPv6 packets. It can also operate in one of three modes such as (1) When both the Host / Host source / stack is enabled IPv4, or (2) When both the Source / Destination Host is the IPv6 stack that is activated, or (3) One source Host / The recipient Host is an IPv4 / IPv6 stack that is activated. Dual stack is one that supports both IPv4 or IPv6 protocols, can be configured with IPv4 32 bit addresses or IPv6 128 bit addresses using mechanisms such as DHCP to obtain IPv4 addresses and use IPv6 mechanisms such as automatic configuration without status, or DHCPv6 to obtain addresses IPv6[22].

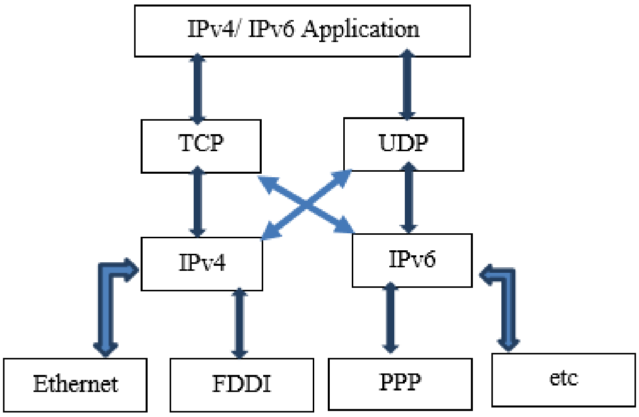


Figure 2.1 Dual Stack System [22]

According to Wu, et. al (2013), the Ethernet contains nodes and these nodes can support both protocols in parallel in the same infrastructure. Therefore, nodes can provide data transmission for IPv4 and IPv6. This technique is not suitable for large networks such as the Internet because it is difficult and expensive to close all nodes on such a large network. On the other hand, it is suitable for small networks, which require less management and are easily controlled. Double piles are considered to be the basis for creating two other techniques for the transition between IPv4 and IPv6[22].

2.2.2. Tunneling

By encapsulating IPv6 packets inside IPv4 packets, IPv6-capable hosts and IPv6-capable networks isolated from other IPv6-capable systems or the IPv6 internet at large can exchange IPv6 packets over IPv4-only infrastructure[23].

The tunnel is divided into two, namely manual or automatic. The connection to the manual is the point-to-point mode given by the direction of origin and destination of the tunnel by the operator, while the automatic connection is the point to the point where the source address is determined by the operator and the address of the operator is found. destination.

automatically The idea of the tunnel serves as a bridge to transfer packets between the same two networks through incompatible networks[24]. In other words, IPv6 will be part of IPv4, and IPv6 data will flow using the IPv4 infrastructure, which will send it to destination (IPv6) for processing; A tunnel is a virtual link between two points to transfer data [25].

a. Manual Tunneling

The manual tunneling provides connections between IPv6 networks over an IPv4 network as a static point-to-point tunnel. IPv4 and IPv6 are manually set as source and destination. This strategy provides a secure connection between two ends[26].

b. Automatic Tunnel

There are various types of automatic tunnels as follows.

1) tunnel Broker

The Dual Stack is important for tunnel intermediaries, so the tunnels that will be Hosted on IPv4 networks can only be built. Web servers are necessary to build tunnels because users must connect to a web server and apply certain authentication details (such as IP addresses, operating systems and IPv6 support software) and the playback will be in the form of short scripts; now the IPv4 to IPv6 tunnel is ready for use. The tunnel broker is considered an automatic configuration service and will configure the endpoints for the network side, the DNS server and the end user [27].

The tunnel broker contains different parts: the first is the tunnel broker (TB), which sends instructions between the server and the DNS. In addition, TB works as a monitor for tunnels, and if the tunnel is down you can use another tunnel that is already in the tunnel group. The second is the tunnel server (TS), which must have at least three IPv6, IPv4 unicast and any broadcast: it is used for routing, accessibility and endpoints for each user. Third, the Tunnel Group (TSG), which uses IPv4 casts to split the tunnel servers into tunneling server groups, all of which have the same broadcast broadcast IPcast address. This makes the tunnel work more efficiently because the requests of the users will be sent to the nearest tunnel and, if there is a problem with the connection, another tunnel will take over and generate a connection.

The fourth part is the DNS system, where each user has a domain name and the assignment is made by the DNS system. This requires the user to register to access the tunnel, and then the user will obtain an IPv6 address; In the end, the communication was carried out on a website such as http://gogo6.com/ using the HTTP protocol [28]. Figure 2.2 shows the mechanism of the corridor tunnel.

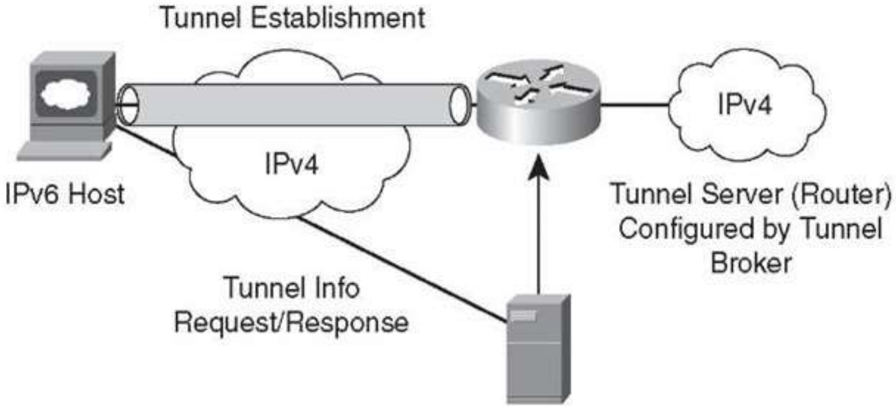

Tunnel Establishment
IPv4
IPv4
IPv6 Host
Tunnel Server (Router) Configured by Tunnel Broker
Tunnel Info Request/Response

Figure 2.2 Tunnel Broker Mechanism [27]

1) 6to4

6to4 is a technique that can connect IPv6 domains separated by IPv4 networks. The IPv4 network acts as a link between the IPv6 network. 6to4 is an automatic tunnel. It uses IPv4 infrastructure to transfer IPv6 packages. Therefore, IPv4 addresses are part of an IPv6 address during the transfer of packets until they reach the other side of the tunnel [27]. The IPv6 network is connected together using a 6to4 router with the 2002 prefix: IPv4 address ::/ 48. The IPv4 address (32 bits) is the 6to4 router address.

The purpose of IPv6 will extract the encapsulation address. In addition to connecting an IPv6 network with IPv6 Internet over an IPv4 network, the prefix is the same and the 6to4 router encapsulates the IPv4 destination for the 6to4 relay router, as shown in Figure 7, there are two IPv6 Hosts isolated by the IPv4 Network; tunneling used by IPv6 to send data via IPv4[25].

From the Figure 2.3, it is shown that two IPv6 hosts from two different networks are connecting each other through IPv4 network infrastructure.

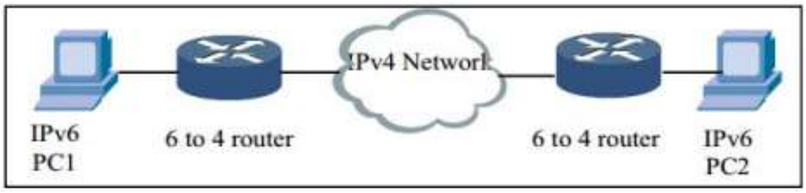


Figure 2.3 6to4 Mechanism[5]

2) 6 over 4

The 6over4 is an automatic technique for providing approaches to IPv6 nodes that are in a collection of IPv4 networks. These IPv6 nodes are not directly connected to each other; so this technique will create virtual links to provide a way for IPv6 nodes to communicate[25]. Virtual links are made by IPv4 Multicast; it is represented by Ethernet with IPv6 and Multicast with IPv4. Therefore, IPv4 infrastructure must be fully supported by IPv4 to provide virtual links to all IPv6 nodes. There are two important protocols to use with this technique, SLAAC and ND, the last one that causes security problems because ND messages may be attacked[22].

3) ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

ISATAP is another mechanism to enable communication between IPv6 and IPv4 using tunneling techniques. This is used to connect the local IPv6 address with the prefix fe80::5efe / 96, followed by 32 bit IPv4. ISATAP can build more than one gateway, which is used as a tunnel for IPv6 to access ISATAP Hosts[22].

ISTAP is an automatic tunnel and this is a point to point connection. This addressing depends on the embedding strategy; IPv6 addresses will be in an IPv4 address. ISATAP Tunnel is able to provide connections between IPv6 and IPv4 routers: at the start of the Host connection in ISTAP it will get an address called the local ISATAP address and will detect the next jump of the ISATAP router. As shown in Figure 2.4 The packages will then be sent by the tunnel after embedding the IPv6 address into the IPv4 address. At the destination, the IPv4 header will be deleted and the packet sent to the IPv6 server; there is a server that sends packets to the ISATAP network and finally the ISATAP router prepares the IPv6 packet to IPv4 and sends it to the ISATAP Host, which then deletes the IPv4 header and extracts the IPv6 packet[29].

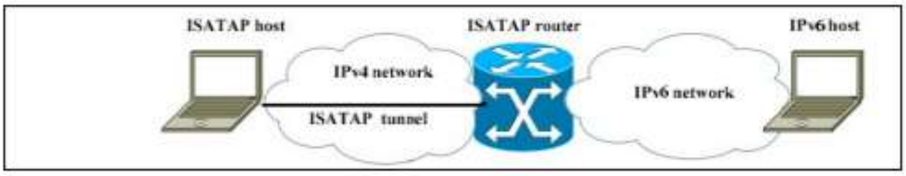


Figure 2.4. ISTAP Mechanism [29]

2.2.3. Translation

The translation mechanism changes the header format from IPv4 to IPv6 format and vice versa. This scheme translates packages from both addresses. Using this translation, IPv6 Hosts can only communicate with IPv4 Hosts only. The translation method consists of two types, such as stateless and stateful. Citizenship translation, packages are not interrelated with one another while translations with state are interrelated. Translation without state, there is no reference to translucent packages during the temporary conversion of translations related to the previous package[24].

a. SIIT (Stateless IP / ICMP Translation)

Translation is done with a header between IPv4 and IPv6. During translation information may be lost and NAT (network address translation) is needed; therefore this technique is not recommended [14]. The SIIT technique requires each IPv6 Host to have a specified IPv4 address. There are two types of addressing: one is known as an IPv4-translated address for an IPv6 Host, where the IPv6 address is generated by adding the prefix 0: ffff: 0: 0: 0/96 before the IPv4 address; the second type is known as IPv4-mapped address for IPv4 Hosts, and IPv6 is generated by adding :: ffff: 0: 0/96 before the IPv4 address.

Translation operation as follows: the IPv4 packet is translated to IPv6, the source will take the prefix :: ffff: 0: 0/96 and the destination will take the prefix 0: ffff: 0: 0: 0/96 and delete it from the original. DNS is very important in knowing the address; Local DNS servers help IPv6 Hosts learn IPv4 addresses that are mapped to get 'AAAA' records from 'A' using DNS64. In addition, IPv4 records are listed on IPv6 Hosts to answer heterogeneous questions and no security issues are added to the network with the SIIT technique; also DHCPv6 and SLAA can be used to assign IPv6 addresses to Hosts. This type is a translation without a state[22].

b. NAT-PT (Translation of Network Address - Protocol Translation)

Communication between native IPv6 and native IPv4 can be obtained using NAT-PT. This mechanism has an IPv4 global pool and a 96-bit IPv6 prefix. The translation will be made by assigning IPv6 with a collection of IPv4 addresses through the NAT-PT gateway. This mechanism does not require additional applications or relies on other mechanisms, such as dual stack, but requires interoperability with the core network for easy and fast management[27].

from the Figure 2.5 can be shown The translation will be made by assigning IPv6 with a collection of IPv4 addresses through the NAT-PT gateway

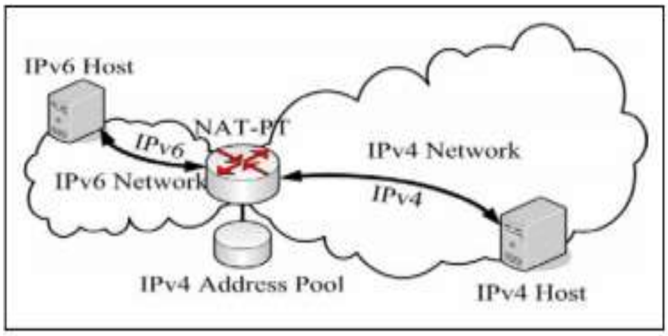


Figure 2.5 NAT-PT Mechanism [31]

Prefix :: / 96 will be used to generate a new address. To translate from IPv6 to IPv4, an IPv4 source will be created from an IPv6 source and a port is found by looking for it in the NAT binding table; Destination IPv4 is created by deleting the prefix. To translate from IPv4 to IPv6, the prefix will be added to the IPv4 source address to create an IPv6 source, and the destination address is created using the destination IPv4 address and the port appears in the NAT binding table. To avoid problems generated by building binding maps, heterogeneous addressing will use ALG DNS on the translator. This will help in converting A queries to AAAA in two ways to produce clear binding between IPv6 and IPv4 addressing IPv4 using a collection of addresses[22].

c. BIS (Bump in stack) and BIA (Bump in API)

Both BIA and BIS are state translations. These two mechanisms are used to solve problems when applications on IPv4 want to communicate with IPv6 Hosts remotely over an IPv6 network; this strategy relies on how to fool applications using IPv4 to assume that the remote Host is IPv4 too. This technique is built by software and entered into the Host. Security is weak enough for DOS attacks on DNS requests: by exhausting a collection of IPv4 addresses, the binding table will be full[22].

1) Bump in stack (BIS)

BIS uses packet-based translation: translations run operations by creating the source address of the Host and destination of the binding table with the IPv4 destination address. When the packet reaches the Host, the translator translates the packet to IPv4 and the source address is taken from the binding table with the IPv6 source address and destination of the Host IPv4 address, as shown in Figure 2.6 [22]. The translation between IPv4 and IPv6 is done by BIS double-stack injection for Hosts and IPv4 is detected to IPv6[31].

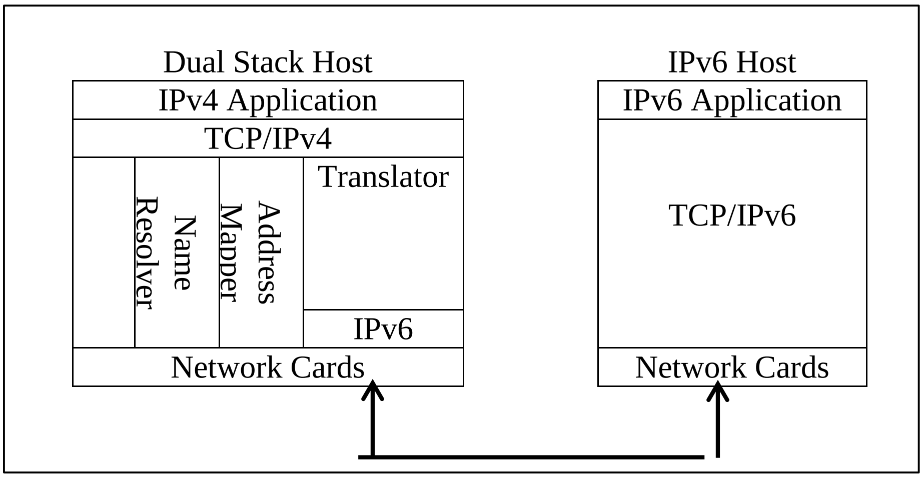


Figure 2.6 BIS Mechanism [22]

2) Bump in API (BIA)

BIA is similar to BIS; with the BIA translator translated between the IPv4 API and the IPv6 API. Name resolvers and mapper addresses are the same as in BIS, and the mapper function is responsible for translation. The translation will be done without an IP header so that security will not break between end and end.

2.2.4. IPv4

IPv4 is considered as the core of internet addressing, because it allows data transmission using TCP / IP. In previous years, this protocol proved its stability and reliability in working in an internet environment to provide connections for millions of nodes.IPv4 was launched in the 1980s. After a short period of time, this protocol began to run out; this causes the use of routing between class domains (CIDR). However, this does not provide a long-term solution because of rapid internet use. Some sources estimate that it will run out in 2010 or 2012, which is the main reason for developing a new version that can accommodate more consumers.

IPv4 contains 32 bits. This can include 4.3 billion addresses. The address is represented as 192.168.2.1. Each can be from 0 to 255, can theoretically address up to 4 billion computer Hosts or more precisely 4,294,967,296 Hosts worldwide, the number of Hosts is obtained from 256 (obtained from 8 bits) in the 4th rank (because there are 4 octets) so the maximum value of the IP version 4 address is 255.255.255.255 where the value is calculated from zero so that the value of the Host value that can be accommodated is 256x256x256x256 = 4,294,967,296 Hosts, if the Host exceeds the quota then IP version 6 or IPv6 is made. In general, IPv4 contains five classes. Each class provides different restrictions for address numbers for networks and Hosts.

The IP address of version 4 is divided into several classes, seen from the first octet, as shown in the table. Actually the difference between the IP class version 4 is the binary pattern found in the first octet (mainly the initial / high-order bits), but to be easier to remember, it will be remembered faster by using decimal representations.

Table 2.2. Divided of IP Address of Version 4 [22]

Class	**First Octet (Decimal)**	**First Octet (Binner)**	**Used by**
Class A	1-127	0xxx xxxx	Address unicast for large scale networks
Class B	128-191	10xx xxxx	Address unicast for medium to large scale networks
Class C	192-223	110x xxxx	Address unicast for small scale networks
Class D	224-239	1110 xxxx	Multicast address (not unicast address)

Class E	240-255	1111 xxxx	is conserved, generally used as an experimental address; (not a unicast address)

From the Table 2.2 can be known the following:

a. Class A

Class A addresses are given for large-scale networks. The highest bit sequence number in the class A IP address is always set to 0 (zero). The next seven bits — to complete the first octet — will make a network identifier. The remaining 24 bits (or the last three octets) represent the Host identifier. This allows class A to have up to 126 networks, and 16,777,214 Hosts per network. The address with the initial octet 127 is not permitted, because it is used for the Inter process Communication (IPC) mechanism in the machine in question.

b. Class B

Class B addresses are reserved for medium to large scale networks. The first two bits in the first octet of the class B IP address are always set to binary number 10. The next 14 bits (to complete the first two octets), will make a network identifier. The remaining 16 bits (the last two octets) represent the Host identifier. Class B can have 16,384 networks, and 65,534 Hosts for each network.

c. Class C

Class C IP addresses are used for small-scale networks. The first three bits in the first octet of class C address are always set to binary value 110. The next 21 bits (to complete the first three octets) will form a network identifier. The remaining 8 bits (as the last octet) will represent the Host identifier. This allows the creation of a total of 2,097,152 networks, and 254 Hosts for each network.

d. Class D

Class D IP addresses are provided only for multicast IP addresses, but differ from the three classes above. The first four bits in IP class D are always set to binary numbers 1110. The remaining 28 bits are used as addresses that can be used to identify Hosts. To be clear about this address, see the IPv4 Multicast Address section.

e. Class E

Class E IP addresses are provided as "experimental" or experimental addresses and are reserved for future use. The first four bits are always set to binary 1111 numbers. The remaining 28 bits are used as addresses that can be used to identify Hosts.

2.2.5. IPv6

IPv6 Internet Protocol was developed as a future network layer protocol to come, to overcome the shortage of IPv4 address space. IPv6 is the sixth version of the IP address. The IPv6 protocol address is 128-bit long. To represent a 128-bit address, IPv6 uses a total of 8 fields consisting of 4 hexadecimal values separated by colons represented like (:). So that it allows 2 ^ 128 = 3,4 × 1038 addresses[32]. This is a very large number of addresses, then IPV4. This new IPv6 address will meet Internet requests and ensure to meet needs. Basically, there are 3 types of IP addressing version 6, namely:

a. Unicast address

This identifies the signal in the network interface where IP provides a packet sent to a unicast address to a particular Host to the internet.

b. Anycast address

In this addressing system, the IP address is assigned to the group interface and can be a different node. This is also used as an identification Host on the internet. If a multicast address, sending a packet to anycast address only reaches one of the interfaces on the closest Host. Conversely, anycast address cannot identify when the address is in the same format as the unicast address and it is only different that with some sense for this reason it can be said that the unicast address function is like that of anycast address.

in the Figure 2.7 can be seen the explanation of the three Types of IP Address Version 6

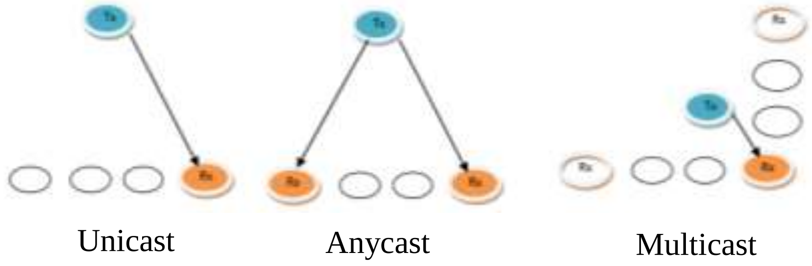


Figure 2.7 The Three Types of IP Addressing Version 6 [32]

c. Multicast address

Multicast addresses identify multiple interfaces on the internet. Packages sent to all interfaces set can join the corresponding multicast group using multicast addresses. It is known that IPv6 does not have a broadcast address, but the broadcast here is entered by multicast addressing using the multicast group "ff02 :: 1". To reduce the IPv6 protocol interface barrier using the local link-multicast group.

Some of the benefits of the IPv6 protocol are given below:

a. Very large address space (2128).
b. Allows extension.
c. The header format is simpler than IPv4.
d. Supports increased mobility and increased security than IPv4.
e. IPv6 addresses support automatic configuration modes that provide greater management flexibility than larger networks.

In Figure 2.8 we can see that the IPv6 addresses basically use 128 bits for IP addressing and 128 bits are separated by eight groups, each group has sixteen bits and they are separated by colons ":". For example, "2000: db80: 0448: 5a73: 0000: 0000: 0000: 0001" here it can be seen that each letter is used in lowercase letters, suggested by the IETF. The zero block can be simplified using a double colon "::". So the address given is like 2000: db80: 448: 5a73 :: 1. The network address range is written in Classless Inter Domain Routing (CIDR) notation. The network is represented by the first address in the block, backslash (/) and the decimal value equals the size in the prefix bit.

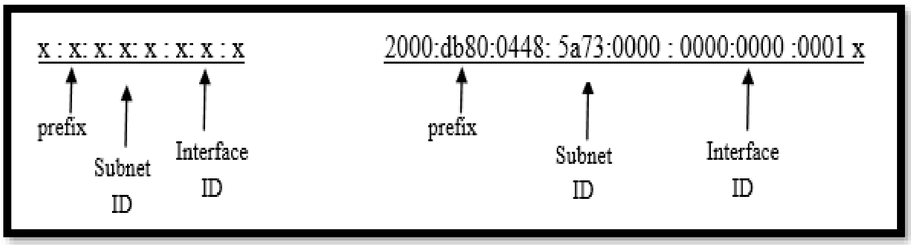

x : x: x: x: x : x: x : x
prefix
Subnet ID
Interface ID
2000:db80:0448: 5a73:0000 : 0000:0000 :0001 x
prefix
Subnet ID
Interface ID

Figure 2.8. IPv6 addresses basically use 128 bits [32]

2.2.6. Jperf and GNS3

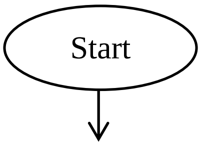
JPerf is a simple framework for writing and running automated performance and scalability tests. It's like network monitoring but its work to analysis the performance, its can be analysis the Measure throughput and latency and packet loss as real way[35].

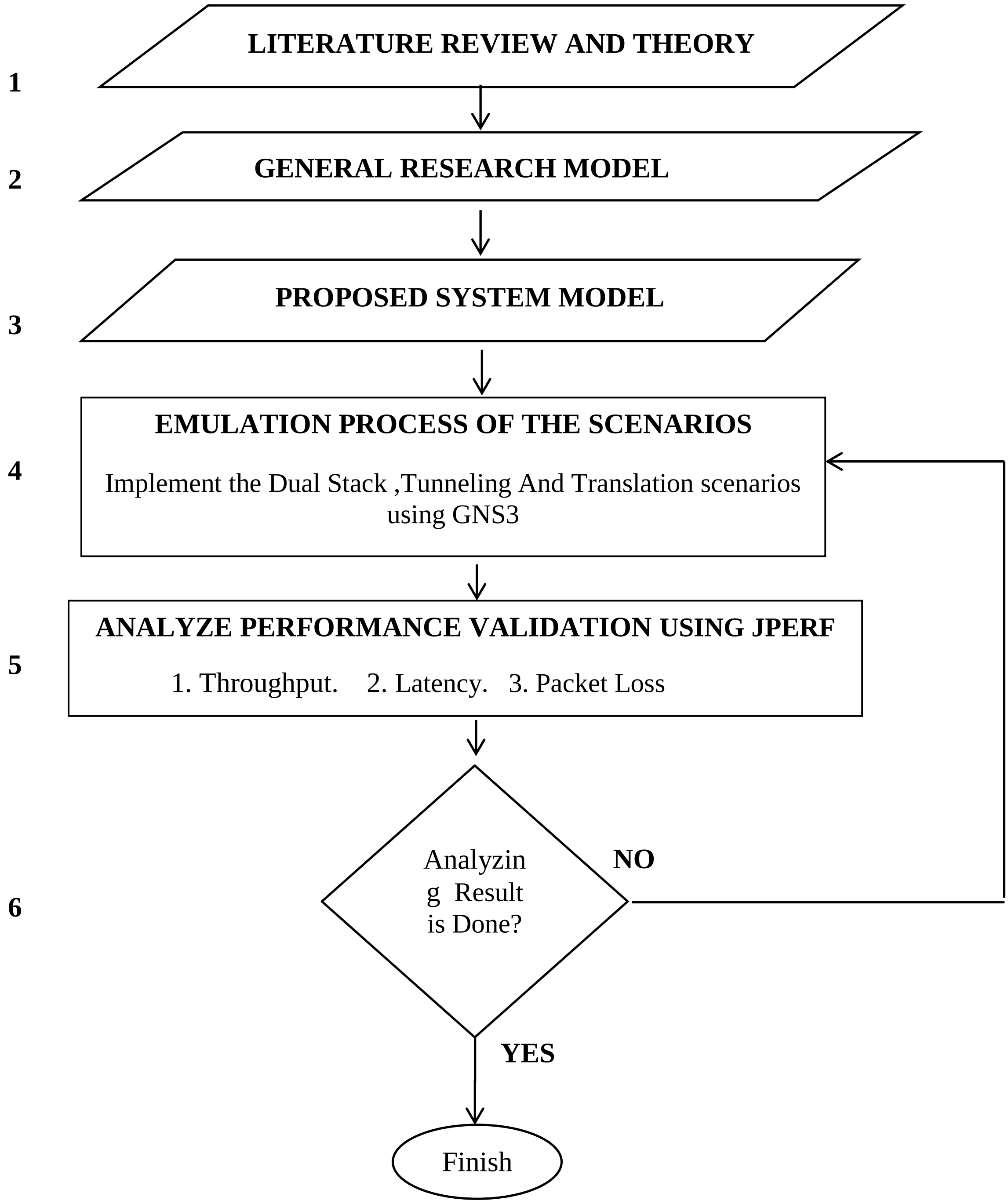
GNS3 When building a new enterprise network, it can be useful to emulate the network by GNS3 (Graphical Network Simulation) before going to do it real . this emulation allows for better testing and troubleshooting, as well as creating different models to find the one that is most effective for the company's needs.

Whereas the cost of network equipments can be prohibitive, since the network engineers are essentially limited to the equipment they have on hand, and don't have the budget to invest in additional hardware to experiment with different configurations. Thankfully, there are other options. With a tool like GNS3, it's possible to create a virtual network right on a PC and experiment with different configurations there rather than on actual hardware[36].

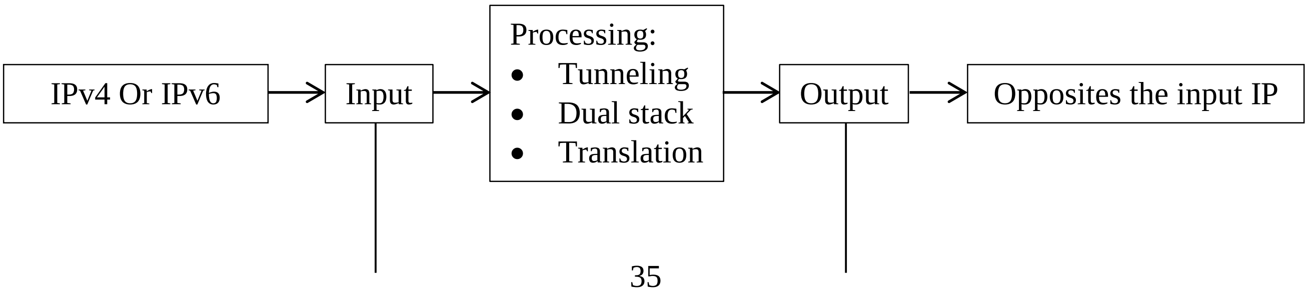
CHAPTER III
RESEARCH METHODOLOGY

3.1. Research Design




1
LITERATURE REVIEW AND THEORY
2
GENERAL RESEARCH MODEL
3
PROPOSED SYSTEM MODEL
4
EMULATION PROCESS OF THE SCENARIOS
Implement the Dual Stack ,Tunneling And Translation scenarios using GNS3
5
ANALYZE PERFORMANCE VALIDATION USING JPERF
1. Throughput. 2. Latency. 3. Packet Loss
6
Analyzin g Result is Done?
NO
YES
Finish

3.2. General Research Model



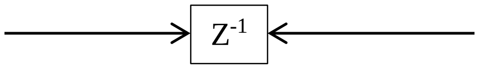


Figure 3.1.Transition IPv4 to IPv6

From the figure 3.1 can understand the general research model. The input data will be IPv4 or IPv6 and For the connection between IPv4 to IPv6 and The opposite, there are three transition mechanisms for that. They are Tunneling, Translation and Dual Stack. Then the output will be opposites the input IP.

The transition between IPv4 Internet and IPv6 Internet will be a long process as long as the two protocols coexist. The picture above shows the phase of the transition from IPv4 to IPv6. A mechanism to ensure a smooth, gradual and independent transition to IPv6 services is needed. Such a mechanism must help the coexistence of IPv4 and IPv6 nodes that are smooth during the transition period. IETF (Internet Engineering Task Force) has created the Ngtrans Group to facilitate the smooth transition from IPv4 services to IPv6. Various transition strategies can be divided into three categories, including dual stack, tunneling and translation mechanisms[33]. The dual-stack mechanism includes two protocol stacks that operate in parallel and allow network nodes to communicate either through IPv4 or IPv6[34]. Tunneling, from a transition perspective, allows incompatible networks to be bridged, and is usually applied point-to-point or sequentially. The basic function of translation in IPv4 / IPv6 transitions is to translate IP packets. In this works, real time emulator software is used to perform dual stack, tunneling and translation.

3.3. Proposed System Model

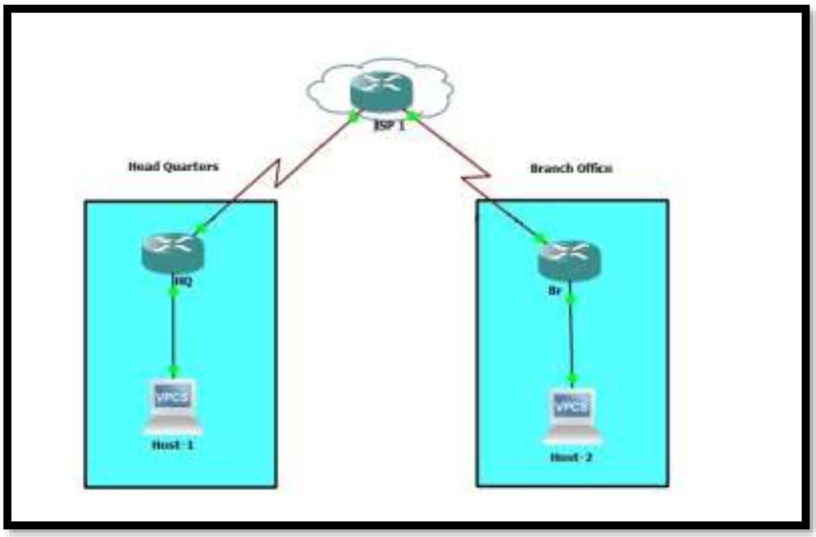


Figure 3.2 Proposed System Model

The transition between IPv4 Internet and IPv6 Internet will using three routers and two hosts as what shown in Figure 3.2 .Various transition strategies can be divided into three scenarios, all of these scenarios will be running with dual stack, tunneling and translation mechanisms all one by one via GNS3 tool. and analyzed the latency ,throughput and packet loss on all the transition scenarios using Jperf.

3.4. Performance Analysis

GNS3 is a graphical network simulator program that can simulate a more complex network topology compared to other simulators. This program can be run on operating systems, such as Window professional or Linux Ubuntu. GNS3 provides complete and accurate simulations, so that it relates to:

1. Dynamips, a Cisco IOS emulator.
2. Dynagen, a text-based front-end for Dynamips.
3. Qemu, a generic and open source emulator and virtualizer engine.
4. VirtualBox, a free and powerful virtualization software

The working principle of GNS3 is to emulate Cisco IOS on the computer, so that the PC can function like a router or even a switch, by activating functions from the Ethernet Switch Card.

The advantages of GNS3 are:

1. Allows full access to Cisco IOS
2. Enables a more real design topology with interactions to other systems such as the OS in VirtualBox, the Host computer (the place where GNS3 is installed) or the connection to the internet.

The disadvantages of GNS3 are:

1. Multilayer switches are not provided as default devices and also the operating system used on these devices. So it takes a module and also Cisco IOS to be able to use multilayer switches.
2. Requires relatively high computer resources

JPERF is an Internet Performance application (IPERF) front-end application to generate multicast traffic. JPERF is a java GUI based on the Iperf network measurement tool. The network topology consists of 7 virtual computers defined as VMWARE virtual machines with 10GB HDD and 1GB RAM per virtual machine and connected to a virtual hub via 100MB Fast Ethernet. Four virtual hubs connected to a virtual router via 100MB Fast Ethernet. Six virtual Cisco 2800 routers are connected between them via a serial link. The end-to-end connection is realized using a server as a source for streaming UDP media, then received by the client via IPv6 and IPv4 multicast networks using GNS3.

3.5. Emulation Process

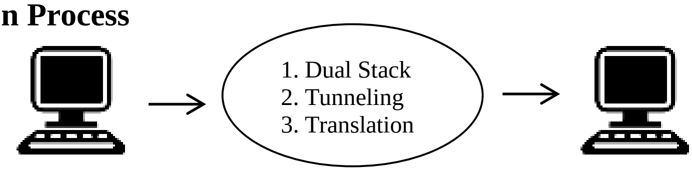


Figure 3.3 Emulation Process

Transition between IPv4 Internet and IPv6 The internet will be a long process as long as both protocols exist. The figure 3.3 above shows the phase of the transition from IPv4 to IPv6. Mechanisms are needed to ensure smooth, gradual and independent transitions to IPv6 services. Various transition strategies can be divided into three categories, including dual stack, tunneling and translation mechanisms. The dual-stack mechanism includes two protocol stacks that operate in parallel and allow network nodes to communicate either through IPv4 or IPv6 tunneling. From a transition perspective, it allows incompatible networks to be bridged, and is usually applied point-to-point or sequentially. The basic function of translation in IPv4 / IPv6 transitions is to translate IP packets. In this work, real-time emulator software is used to perform dual stack, tunneling, and translation.

Implementation agreements have been concluded between the head office and the branches of an enterprise through a with public IP Address network (Internet Service Provider). Two model samples were tested in the laboratory to assess the complexity, advantages and disadvantages of each method. The implementation work is carried out according to three scenarios by applying three methods such as the 6to4 manual tunnel , Dual Stack and Translation.

- MethodScenario 1: 6to4 manually tunneling .
- MethodScenario 2: Dual stack.
- MethodScenario 3: Translation

Behind the choice of these three special methods, it is easy to implement the existing material in a some company rather than throw the budget on new network devices and the other equipments . The base topology has been established with three routers as can see in figure(3.2) Headquarters (H Q), Internet Service Providers (IS P) and Branches (B r). and two clients devices Computer1 and Computer2 are used. The itemized connectivity process was explained in all the scenarios. In the three connectivity scenarios are the same. The equipment that will be used are:

- Router: Cisco Router 2800 Series with Router operating system IOS 12.4 (4) T8.

- Client: using windows operating system with a IP.

1. Scenario 1

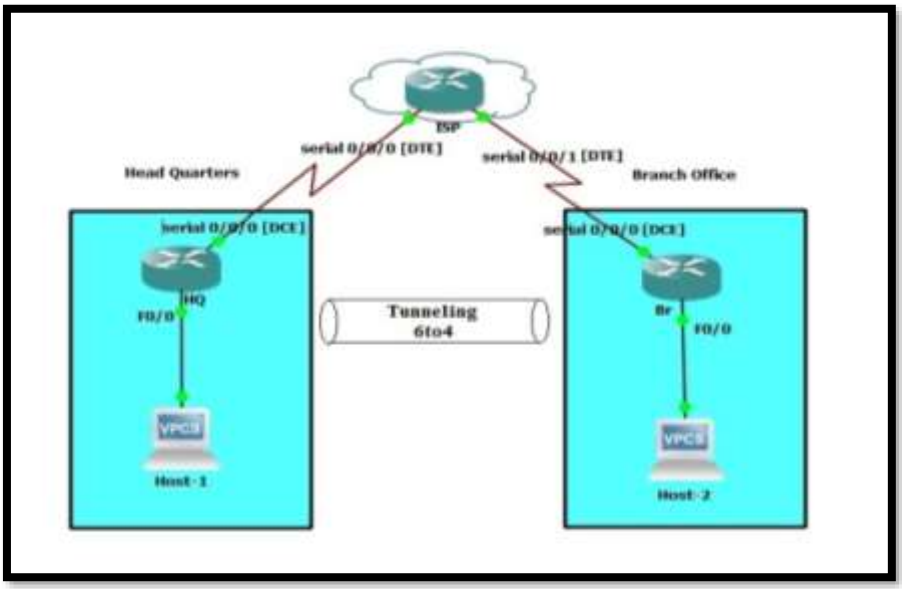


Figure 3.4 TunnelingTopology

a. Physical connection

As what shown in the figure 3.4 The network will be built between [H Q] and [B R] branches through an ISP. In Scenario 1, prepare a network, three routers, and two clients to use. Host-1 will be connected to the [H Q] FA interface with an straight Ethernet cable. The [H Q] interface serial [DCE] [0/0/0] will be connected to the ISP [DTE] [0/0/0] serial interface using a serial cable. The serial interface ISP [DTE] [0/0/1] is connected to the serial interface [B R] [DCE] [0/0/0] using a serial cable. The [B R] interface is connected to HOST-2 with a FA straight Ethernet cable. This ensures physical connectivity between [H Q] and the BR.

b. IP Address Scheme

Table 3.1.Host-1 and Host-2 IP Address [34]

Host	IPv6 address	Gateway IPv6
Host-1	FEC0:87:1:3::2/64	FEC0:87:1:3::1/64
Host-2	FEC0:87:1:4::2/64	FEC0:87:1:4::1/64

Table 3.2. Headquarters’, ISP and Branch IP Addresses [34]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	FastEthernet 0/0	--	FEC0:87:1:3::1/64
	Serial Interface 0/0/0	192.168.11.1/30	--
	Loop back0	190.168.5.1/24	FEC0::11:1/128
	Tunnel0	--	FEC0::12:1/128
ISP	Loop back0	190.168.6.1/24	--
	Serial Interface 0/0/0	192.168.11.2/30	--
	Serial Interface 0/0/1	192.168.12.1/30	--
Branch	Loop back0	190.168.7.1/24	FEC0::13:1/128
	Serial Interface 0/0/0	192.168.12.2/30	--
	FastEthernet 0/0	--	FEC0:87:1:4::1/64
	Tunnel0	--	FEC0::4:4/128

c. Establishment of routing

Routing of communication protocols from HOST-1 to HOST-2, performed on all routers. This routing protocol uses two types of protocols on the network. Thus, BGP as the External Gateway Protocol (EGP) for public networks such as the ISP network and the Inner Gateway Protocol (IGP) is OSPFv3 for private networks such as LAN connections. OSPFv3 is a status binding protocol that speeds up the merge of the wide network routes and preserve a copy of the tables of the routing that support IPv6 routing primarily.BGP is a vector-based steering convention, generally utilized as an EGP convention on the Internet. Two IP conventions are utilized in this situation, for example, IPv4 for open networks and IPv6 for close networks . Open systems are utilized between home office to ISP and among ISP and Br. close networks are utilized to set up an association between HOST-1's central command and HOST-2's base Router . with the [H Q] Router , OSPFv3 is arranged for IPv6 and BGP networks for IPv4 systems. Since the ISP switch is on a public open network BGP is configured. On the [B R] router, OSPFv3 is configured for IPv6 and BGP networks for IPv4 networks. Routing protocols are established on all routers, but the incompatibility between IPv4 and IPv6 does not allow the connection between Host-1 and Host -2.

In the first Scenario, an IPv6 packet from Host-1 is created to the send point as Host-2 and already sent to [H Q] . The [H Q] router is the first point of the tunnel that encapsulates IPv6 packets in IPv4. It is sent via ISP by IPv4 routes to the final point in the tunnel. The final point of the tunnel is the [B R] router that will separate IPv6 packet from IPv4 packets and send it to Host-2.

2. Scenario 2 (Dual stack)

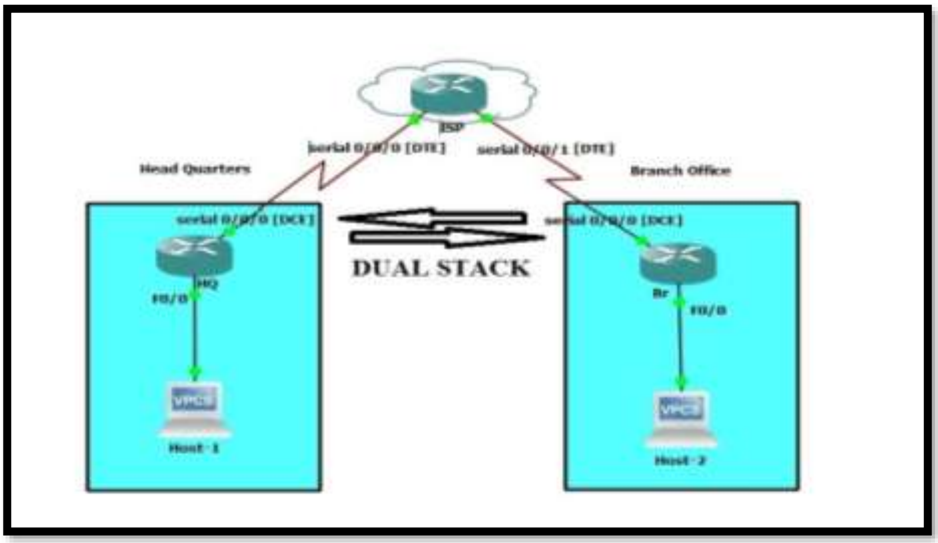


Figure 3.5 Dual Stack Topology

a. Physical connection

As what shown in the figure 3.5 The physical settings of second Scenario have done by the same method as the first Scenario. three routers and two clients are used. Host-1 connected to the FA0 / 0 [H Q] interface with a straight Ethernet cable. The [H Q] 0/0/0 series interface [DCE] is connected to the ISP 0/0/0 [DTE] serial interface with a serial cable. The serial interface ISP 0/0/1 [DTE] is connected to the serial interface [Br] 0/0/0 [DCE] using a serial cable. The [B r] FA0 / 0 interface is connected to HOST-2 with a straight Ethernet cable. This ensures physical connectivity between headquarters and the branch.

b. IP Address Scheme

Table 3.3. Host-1 and Host-2 IP Address [34]

Host	Criteria	IPv4 address	IPv6 address
Host-1	NIC Ethernet	192.168.14.10/24	FEC0:87:1:3::2/64
	Gateway	192.168.14.1/24	FEC0:87:1:3::1/64
Host-2	NIC Ethernet	192.168.13.20/24	FEC0:87:1:4::2/64
	Gateway	192.168.13.1/24	FEC0:87:1:4::1/64

Table 3.4. Headquarters, ISP and Branch IP Addresses [34]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	FastEthernet 0/0	192.168.14.1/24	FEC0:87:1:3::1/64
	Serial Interface 0/0/0	192.168.11.1/30	2001:2:11::1/112
	Loop back0	190.168.5.1/24	FEC0::11:1/128
ISP	Loop back0	190.168.6.1/24	FEC0::12:1/128
	Serial Interface 0/0/0	192.168.11.2/30	2001:2:11::2/112
	Serial Interface 0/0/1	192.168.12.1/30	2001:22:11::1/112
Branch	Loop back0	190.168.7.1/24	FEC0::13:1/128
	Serial Interface 0/0/0	192.168.12.2/30	2001:22:11::2/112
	FastEthernet 0/0	192.168.13.1/24	FEC0:87:1:4::1/64

c. Establish routing

In the second Scenario, the both versions of the IP protocols are used on the all routers. Two protocols (IPv4 and IPv6) work together, so all the routers must have duo routing protocols to uphold that infrastructure. The routing protocol OSPFv3 can support IPv4 and IPv6 on single node but is classified into duo routing tables on each node. SPFv3 is configured on each router ([H Q] , ISP, Br) for the both IP versions addresses. This allows the mechanism of dual stack routing between the nodes. The Dual Stack transition is used to uphold each network IP protocol. The node of Dual Stack can send and communicate together with IPv6 and IPv4 traffic.

3. Scenario 3 (Translation)

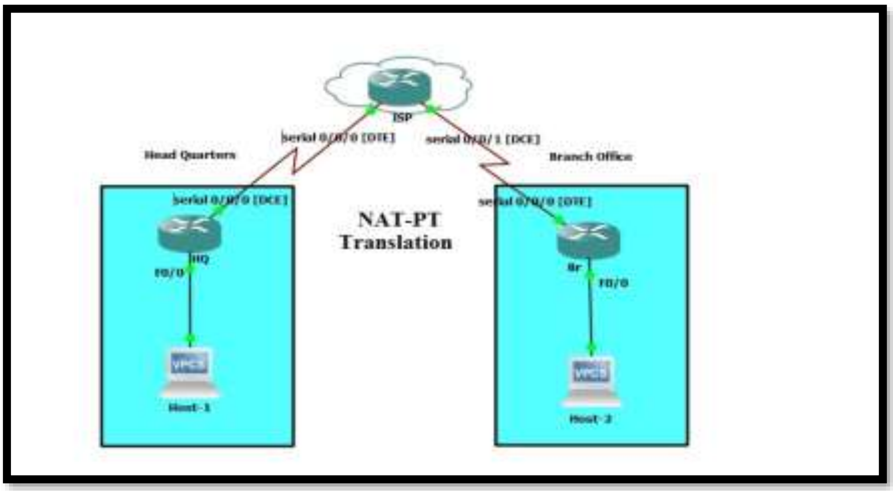


Figure 3.6 NAT-PT Topology

a. Physical connection

As the Figure 3.6 The network will be built between [H Q] and [B R] branches through an ISP. In Scenario 3, prepare a network, three routers, and two clients (Hosts) to use. Host-1 will be connected to the Ethernet interface FA 0/0 [H Q] with a straight Ethernet cable. The [H Q] Se0/0/0 interface series [DCE] will be connected to the ISP Se0/0/0 [DTE] serial interface using a serial cable. The serial interface ISP Se0/0/1 [DCE] is connected to the serial interface [B R] Se0/0/0 [DTE] using a cable serial. The [B R] FA 0/0 interface is connected to HOST-2 with a straight Ethernet cable.

d. IP Address

Table 3.5. Host-1 and Host-2 IP Address [34]

Host	Criteria	IPv4 address	IPv6 address
Host-1	Ethernet	192.168.13.10/24	--
	Gateway	192.168.13.1/24	--
Host-2	Ethernet	--	FEC0:87:1:4::2/64
	Gateway address	--	FEC0:87:1:4::1/64

Table 3.6. Headquarters', ISP and Branch IP Addresses [34]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	FastEthernet 0/0	192.168.13.1/24	--
	Serial 0/0/0	192.168.11.1/30	--
ISP	Serial 0/0/0	192.168.11.2/30	--
	Serial 0/0/1	--	2001:2:22::1/112
	IPv6 NAT v4v6 source	192.168.11.3	2001::960B:202
	IPv6 NAT v6v4 source	150.11.3.1	FEC0::13:1/128
	ipv6 nat prefix		2009::/96
Branch	Loopback 0		FEC0::13:1/128
	Serial 0/0/0	--	2001:2:22::2/112
	FastEthernet 0/0	--	FEC0:87:1:4::1/64

In the third Scenario, an IPv6 packet from Host-1 is created to the point as Host-2 and sent to [H Q] . The [H Q] router is the first point of the send traffic that encapsulates IPv4 packets in IPv6. It is sent via ISP via IPv6 routes at the final point of the destination . The final point of the send traffic is the [B R] router that separates IPv4 packets from IPv6 packets and sends them to HOST-2 using OSPFv3

3.6.Performance Validation

The empirical results for performance validation from this study used a tool called Jperf. The parameters to be measured in this study are:

- Response Time and packet receive by Ping test: Response time is an alternating time has taken by the packet data of IP from the source to the target point to the source.
- Analysis of the Latency.
- Analysis of the Throughput.
- Analysis of the Packet-loss.

3.7. Summary

The transition between IPv4 Internet and IPv6 can be divided into three categories, including dual stack, tunneling and translation mechanisms. In this research to analyzed the transition strategy IPv4 to IPv6 will use GNS3 and JPERF. From this research the performance mechanism in dual stack, tunneling, and translation will understanding of comparative perform between IPv6 and IPv4 network.

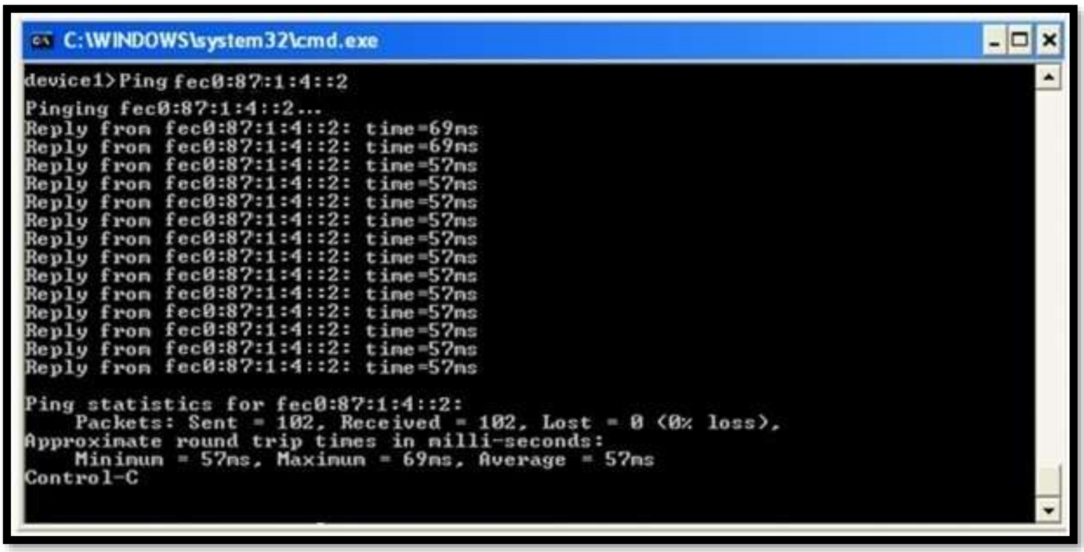
CHAPTER IV

RESULT AND DISCUSSION

4.1. Testing Result

4.1.1. Ping and Trace route test for 6to4 Tunnel (Scenario 1)

The Figures 4.1 & 4.2 shown the ping test and trace route commands to test the connections between two nodes of a network Host-1 to Host-2 (IPv6:FEC0:87:1:4::2) to determine latency and packet loss over of 100 packages the following:

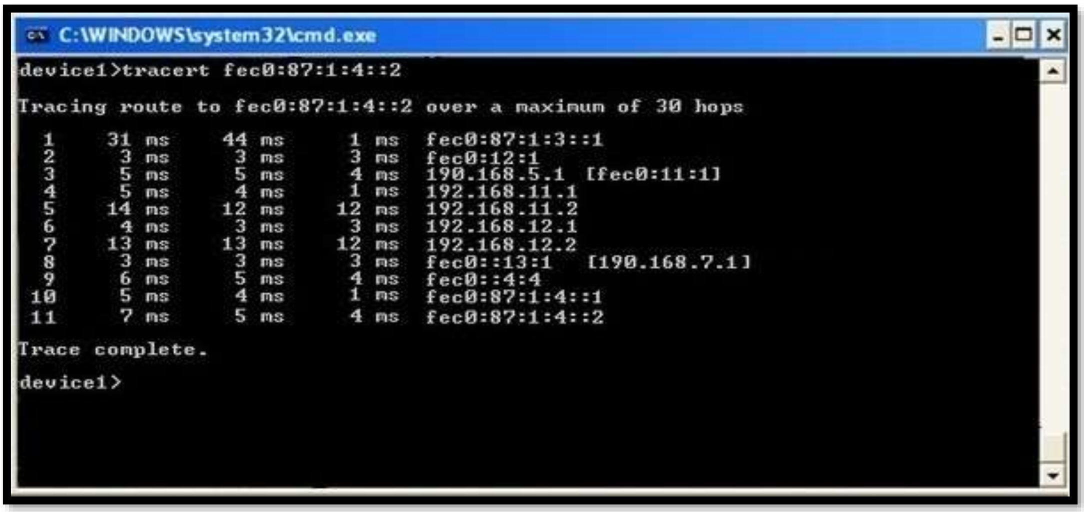


C:\WINDOWS\system32\cmd.exe

```
device1>Ping fec0:87:1:4::2
Pinging fec0:87:1:4::2...
Reply from fec0:87:1:4::2: time=69ms
Reply from fec0:87:1:4::2: time=69ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms

Ping statistics for fec0:87:1:4::2:
    Packets: Sent = 102, Received = 102, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 69ms, Average = 57ms
Control-C
```

Figure 4.1. Ping Test Result



C:\WINDOWS\system32\cmd.exe

```
device1>tracert fec0:87:1:4::2

Tracing route to fec0:87:1:4::2 over a maximum of 30 hops

  1    31 ms    44 ms     1 ms  fec0:87:1:3::1
  2     3 ms     3 ms     3 ms  fec0:12:1
  3     5 ms     5 ms     4 ms  190.168.5.1  [fec0:11:1]
  4     5 ms     4 ms     1 ms  192.168.11.1
  5    14 ms    12 ms    12 ms  192.168.11.2
  6     4 ms     3 ms     3 ms  192.168.12.1
  7    13 ms    13 ms    12 ms  192.168.12.2
  8     3 ms     3 ms     3 ms  fec0::13:1   [190.168.7.1]
  9     6 ms     5 ms     4 ms  fec0::4:4
 10     5 ms     4 ms     1 ms  fec0:87:1:4::1
 11     7 ms     5 ms     4 ms  fec0:87:1:4::2

Trace complete.

device1>
```

Figure 4.2. Traceroute Test Result of Tunneling

Table 4.1. Ping Test Result

Host-1	Host-2
Packets Sent	102
Packets Received	102
Loss	0

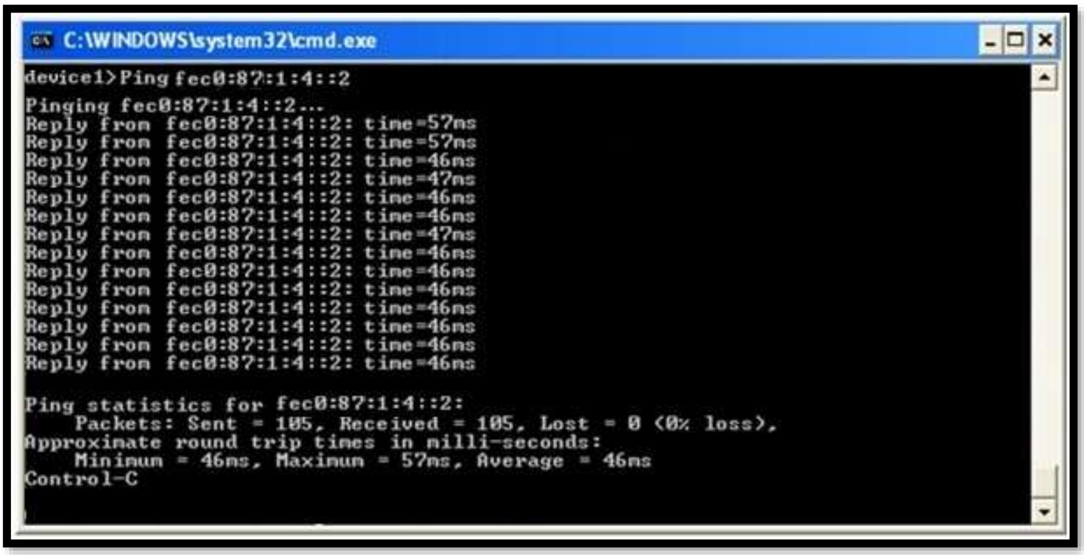
Table 4.2. Latency Test Result

Level	Latency MS
Minimum	57
Maximum	69
Average	57

Here per a ping testing which in figure (4.1) we got the results in the table (4.1) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 102 packets and received 102 packets so there is no Packet loss, but for the latency can see from the table (4.2) the time of the mechanism the highest time is 69ms and the lowest time is 57ms then the average is 57ms.

4.1.2. Ping and Trace route test for dual stack (Scenario 2)

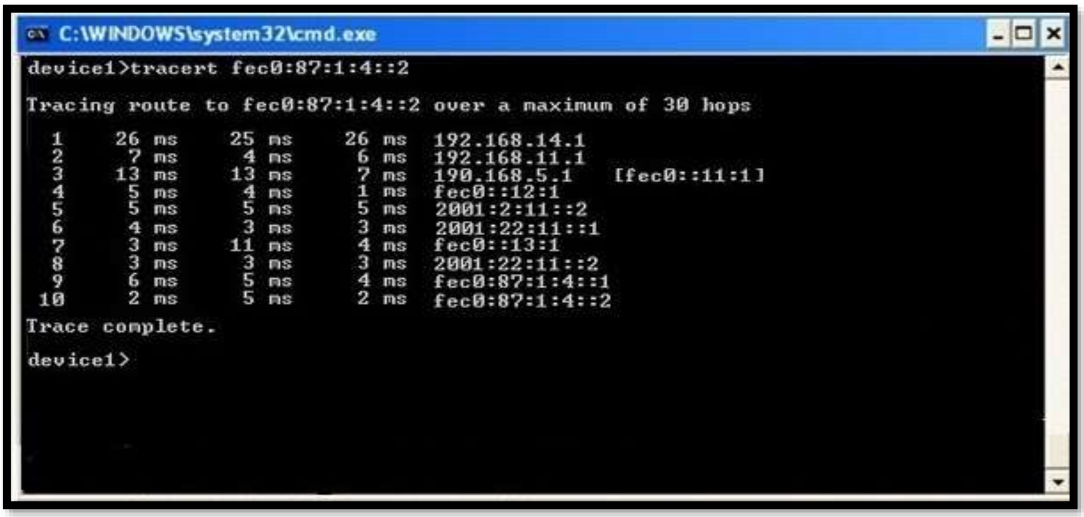
The Figures 4.3 & 4.4 below shown the ping test and trace route commands to test the connections in the second scenario among Host-1 to Host-2 (FEC0:87:1:4::2) to determine the latency and the loss of packets made for more than 100 packages.



```
device1>Ping fec0:87:1:4::2
Pinging fec0:87:1:4::2...
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=47ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=47ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms

Ping statistics for fec0:87:1:4::2:
    Packets: Sent = 105, Received = 105, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 57ms, Average = 46ms
Control-C
```

Figure 4.3. Ping Test Result



```
device1>tracert fec0:87:1:4::2

Tracing route to fec0:87:1:4::2 over a maximum of 30 hops

  1    26 ms    25 ms    26 ms  192.168.14.1
  2     7 ms     4 ms     6 ms  192.168.11.1
  3    13 ms    13 ms     7 ms  190.168.5.1    [fec0::11:1]
  4     5 ms     4 ms     1 ms  fec0::12:1
  5     5 ms     5 ms     5 ms  2001:2:11::2
  6     4 ms     3 ms     3 ms  2001:22:11::1
  7     3 ms    11 ms     4 ms  fec0::13:1
  8     3 ms     3 ms     3 ms  2001:22:11::2
  9     6 ms     5 ms     4 ms  fec0:87:1:4::1
 10     2 ms     5 ms     2 ms  fec0:87:1:4::2
Trace complete.

device1>
```

Figure 4.4. Traceroute Test Result of Dual Stack

Table 4.3. Ping Test Result

Source	Destination
Packets Sent	105
Packets Received	105
Loss	0

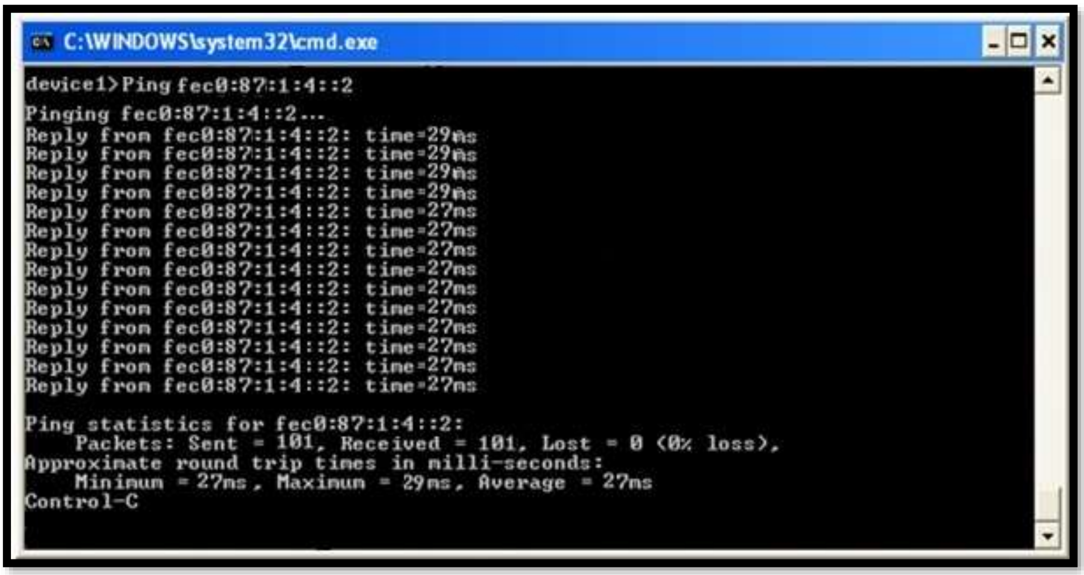
Table 4.4. Latency Result

Level	Latency MS
Minimum	46
Maximum	57
Average	46

here per a ping testing which in figure (4.3) we got the results in the table (4.3) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 105 packets and received 105 packets so there is no Packet loss, but for the latency can see from the table (4.4) the time of the mechanism the highest time is 57ms and the lowest time is 57ms then the average is 46ms.

4.1.3. Ping and Trace route test for Translation NAT-PT (Scenario 3)

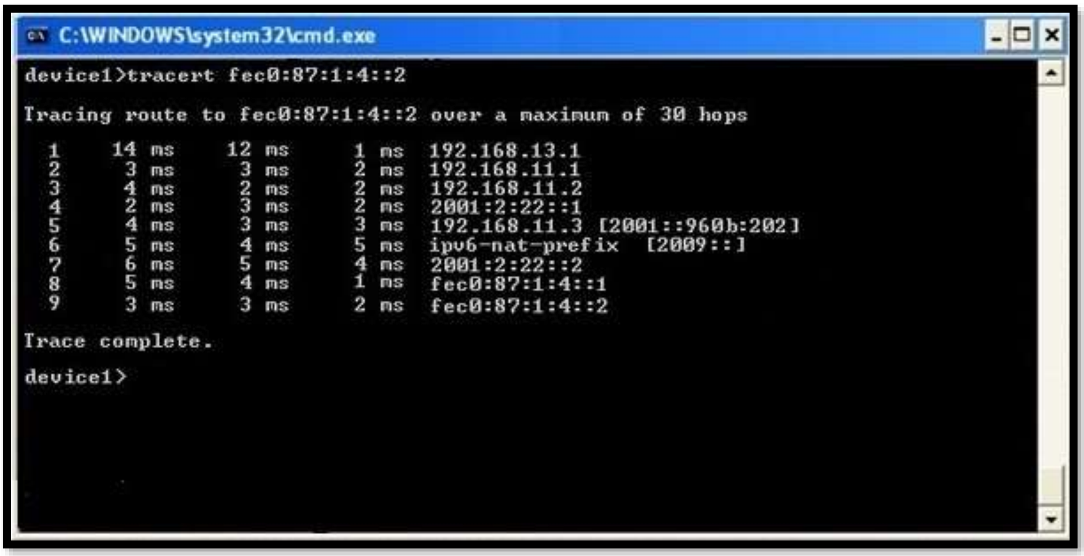
The Figures 4.5 & 4.6 shown the ping test and trace route commands to test the connections in the third scenario among Host-1 to Host-2 (IPv6:FEC0:87:1:4::2) to determine the latency and the loss of packets made for more than 100 packages.



```
device1>Ping fec0:87:1:4::2
Pinging fec0:87:1:4::2...
Reply from fec0:87:1:4::2: time=29ms
Reply from fec0:87:1:4::2: time=29ms
Reply from fec0:87:1:4::2: time=29ms
Reply from fec0:87:1:4::2: time=29ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms

Ping statistics for fec0:87:1:4::2:
    Packets: Sent = 101, Received = 101, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms , Maximum = 29ms, Average = 27ms
Control-C
```

Figure 4.5. Ping Test Result



```
device1>tracert fec0:87:1:4::2

Tracing route to fec0:87:1:4::2 over a maximum of 30 hops

  1    14 ms    12 ms     1 ms  192.168.13.1
  2     3 ms     3 ms     2 ms  192.168.11.1
  3     4 ms     2 ms     2 ms  192.168.11.2
  4     2 ms     3 ms     2 ms  2001:2:22::1
  5     4 ms     3 ms     3 ms  192.168.11.3 [2001::960b:202]
  6     5 ms     4 ms     5 ms  ipv6-nat-prefix  [2009::]
  7     6 ms     5 ms     4 ms  2001:2:22::2
  8     5 ms     4 ms     1 ms  fec0:87:1:4::1
  9     3 ms     3 ms     2 ms  fec0:87:1:4::2

Trace complete.

device1>
```

Figure 4.6. Traceroute Test Result of Translation NAT-PT

Table 4.5. Ping Test Result

Source Host-1	Destination HOST-2
Packets Sent	101
Packets Received	101
Loss	0

Table 4.6. Latency Result

Level	Latency MS
Minimum	27
Maximum	29
Average	27

Here per a ping testing which in figure (4.5) we got the results in the table (4.5) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 101 packets and received 101 packets so there is no Packet loss, but for the latency can see from the table (4.6) the time of the mechanism the highest time is 29ms and the lowest time is 27ms then the average is 27ms.

4.2. Jperf Results

4.2.1. Latency Analysis of the transition mechanisms

This test are performed on the behavior of the TCP latency in the all scenarios, HOST-2 as sender, and HOST-1 as the receiver listening to the client and The client generates ICMP (TCP) traffic using the Jperf tool.

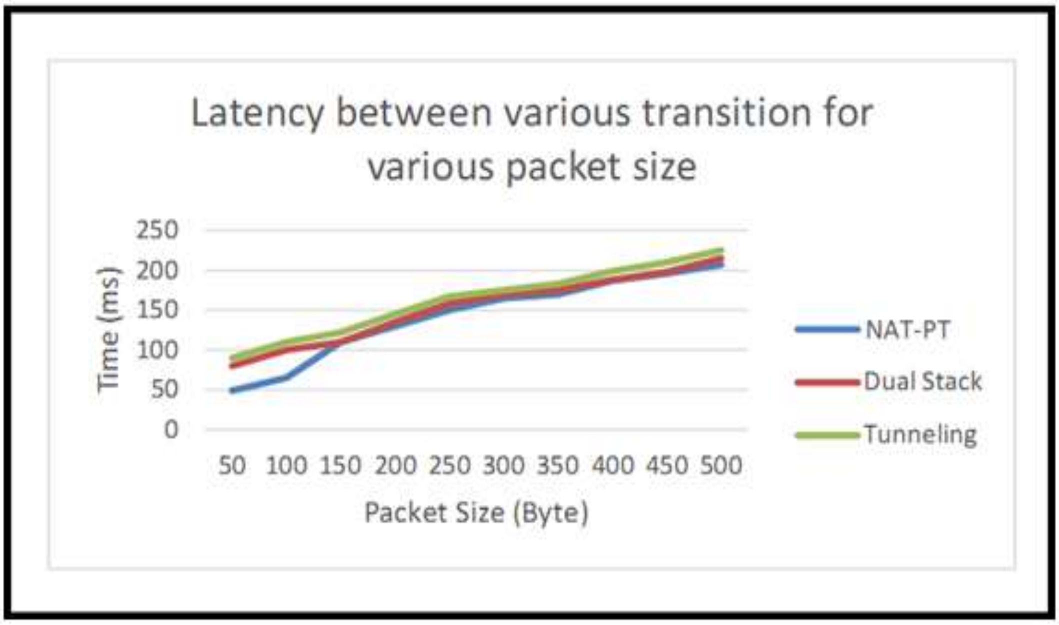


Figure 4.7 Latency Analysis of the transition mechanisms

As can be seen from figure (4.7). the latency can be appear on the packet size (500) Bytes the time of transfer can be achieved in (200) msec in Translation Mechanism (NAT-PT), in dual stack can be seen that the time also with (500) Bytes can be achieved (210) msec, then the tunneling mechanism the time can be in (220) msec with same packet size bytes

4.2.2. Analysis of the Throughput

This test are performed on the behavior of the TCP Throughput vs Packet size in the all scenarios, HOST-2 as sender , and HOST-1 as receiver ICMP (TCP) traffic using the Jperf tool.

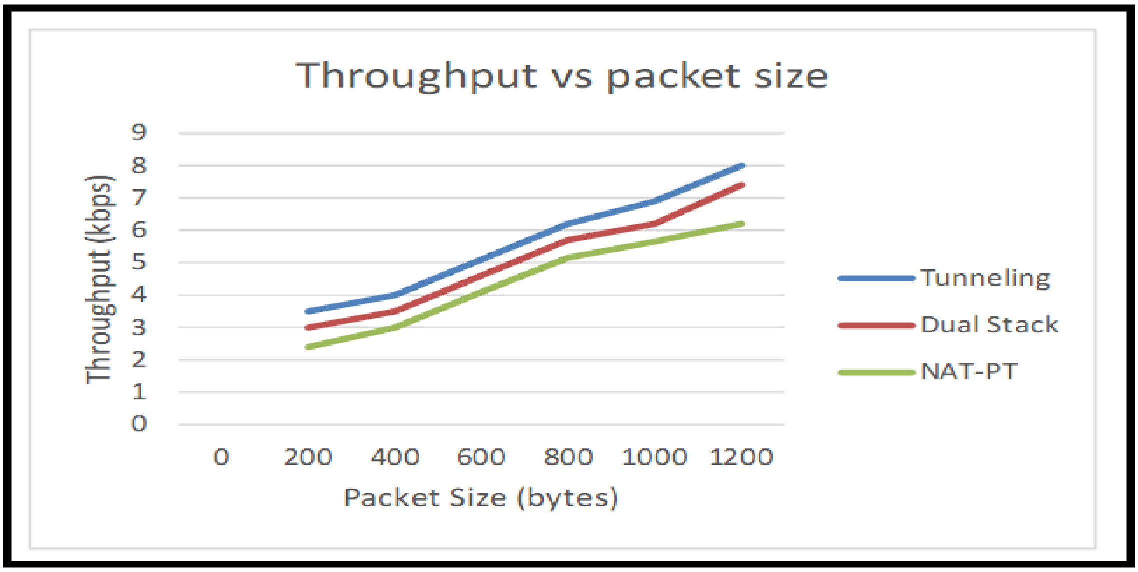


Figure 4.8 Analysis of the Throughput

As can be seen from figure (4.8). the packet size (1200) Bytes and the reason of using this high packet size is to make the result appear more, because if that using was be with low packet size the result will be as not appear with clear way as it is low packet size .

From the figure can be seen the carves of the three mechanisms shown the Throughput its can be achieved in Kbytes just under (6.2) Kbytes/sec in Translation Mechanism (NAT-PT) , in dual stack can be seen that the throughput increase is on the packet size (1200) Bytes can be achieved (7.2) kbytes/sec ,then the tunneling mechanism the throughput also seems to increase that can be seen on the same packet size (1200) Bytes throughput can be achieved in (8) Kbytes/sec.

4.2.3. Analysis of the Packet loss

This test are performed on the behavior of the TCP Packet loss in the all scenarios, HOST-2 as client, and HOST-1 as the server listening to the client and The client generates ICMP (TCP) traffic using the Jperf tool.

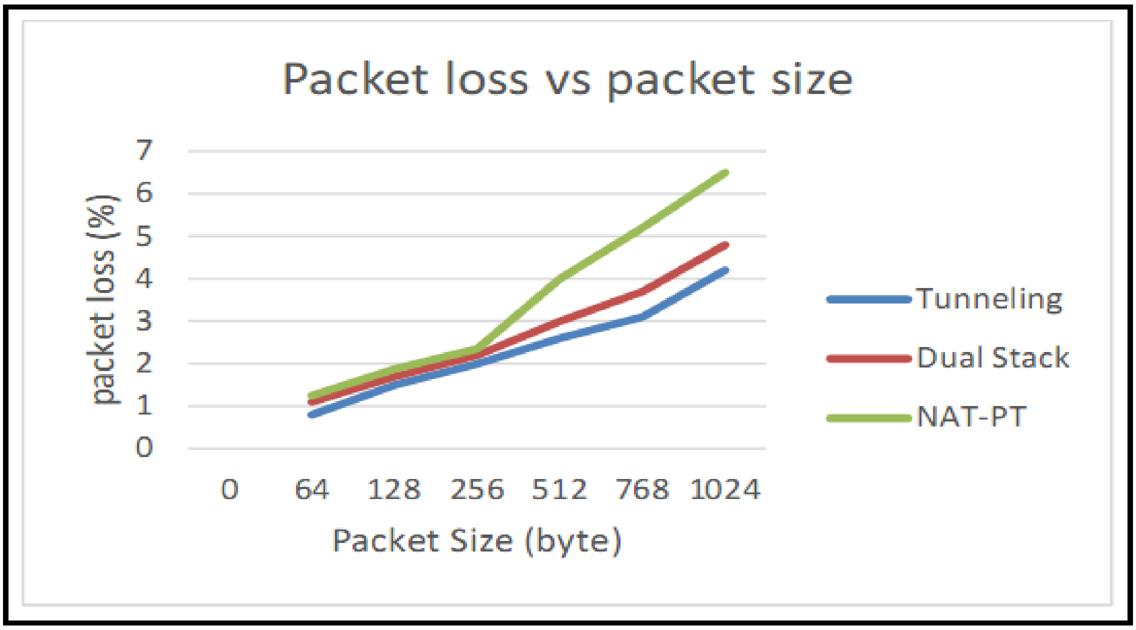


Figure 4.9 Analysis of the Packet loss

As can be seen from figure (4.9). that on the packet size (1024) Bytes the Packet loss can be in percentage (4.2%) in the tunneling mechanism, in dual stack can be seen that the Packet loss increase with packet size (1024) Bytes can be achieved (4.9%), then the Translation Mechanism (NAT-PT) the Packet loss seems to be a more increase that can be (6.5%) with same packet size.

The reason to be the Translation NAT-PT mechanism expertise highest proportion of Packet loss because of it is time overwhelming limit. On the obverse part the tunneling got all-time low Packet loss expertise.

From this Results, the throughput, latency and the Packet loss analyzing have done. After implementation the previous designs of the IPv6-IPv4 mechanisms performance , some packets have been transmitted from HOST-1 to HOST-2. In this test and analysis, ICMP packets (TCP) have been transmitted with diverse duration time and sizes. After monitoring the packet transitions, the results below has been found:

- as can seen in the Figures (4.7),(4.8), it found that the Translation NAT-PT provides the elevated latency, while the Dual stack performance mechanism provides the moderate mode ,and about the Tunneling mechanism easy to see that it is provides the lowest latency and the Translation NAT-PT mechanism provides the highest latency , the tunneling has the highest throughput , and from the figure (4.9) it's found the Translation NAT-PT mechanism had the highest Packet loss and the Tunneling Mechanism had the lowest Packet loss.

From the previous 1,2,3 Results, the next results have been found.

Table 4.7. Similar analysis of the three performance mechanisms.

Feature Analysis	Dual Stack	Tunneling	NAT-PT
The Latency	Moderate	The least	The Highest
The Throughput	Moderate	The Highest	The Lowest
The Packet Loss	Higher than tunneling	less	The Highest

From table (4.7) can be seen the result of Ping testing Jperf analyzing in all the mechanisms which using to connect between IPv4 to IPv6 per High or Less or Medium or Moderate

- As can be shown from the emulation, the results of throughput, latency and Packet loss, can be discovered that the NAT-PT mechanism provides the fast latency, while Dual stack mechanism supplies the moderate and the Tunneling mechanism provides the most minimum latency, and the throughput with packet size appeared the that Tunneling provides the very best output rate than the opposite transition mechanism and also the NAT-PT technique provides very less as a result of its time beyond regulation intense for the header translation. it's to mentioned that, throughput, R= packet size (L)/ time consumed for transmission, and the Translation NAT-PT mechanism experiences highest percentages of Packet loss because of its time overwhelming limitation. On the opposite hand tunneling has all-time low Packet loss expertise.

4.3. Discussion

The progress from IPv4 to IPv6, IPv6 conquers a significant number of the impediments of IPv4 with new highlights. This has been intended to permit smooth progress with IPv4. The mix of CIDR and NAT components possesses diminished the hanging tight energy for the IPv4 address. Be that as it may, Network Address Translation (NAT) separates start to finish IP designs, so it has numerous impediments for the convention. A bigger IPv6 address space gives an increasingly remarkable worldwide unicast address for present and future Internet development. The full usage of IPv6 requires an expansion in the quantity of utilizations, Hosts, switches, and DNS to help IPv6, which can be costly and take a long time to convey. In this circumstance, the change system is a standout amongst the best arrangements and thusly permits IPv6 and IPv4 systems to work on a similar framework.

IPv4 to IPv6 Several change components have been created dependent on the requirements of various associations. This examination physically analyzes and looks at Dual Stack, interpretation and 6to4 components. These systems have their own points of interest and hindrances in various foundations. The Dual Stack progress component is the most well-known and least demanding route for IPv6 and IPv4 hubs to speak with IPv6 and IPv4 hubs autonomously, without evolving systems. The Dual Stack is appropriate for Internet specialist organizations, corporate systems, and home clients. Then again, the manual passage is arranged between two IPv6 systems by means of the IPv4 organize foundation. Manual passages are a protected system contrasted with other progress instruments. This component is appropriate for ISPs, corporate systems, server farms, yet not home clients. In light of the way toward changing from IPv4 to IPv6, While NAT-PT allows direct correspondence between IPv6-just systems and IPv4-just systems. dual stack systems (arranges that have IPv4 and IPv6) will have some IPv6-just has composed to require favorable position of the IPv6 auto design, world tending to, and less confounded administration alternatives, and these Hosts will utilize NAT-PT to connect with existing IPv4-just systems inside a similar association ,there are a few preferences and hindrances of the three progress instruments, for example, dual stack , 6to4 manual tunneling and NAT-PT translation,

The advantages and disadvantages of the Dual Stack mechanism are:

Advantages:

- Native Dual Stack does not require a tunneling performance mechanism on the inside the network.
- IPv4 and IPv6 run autonomously of one another.
- This mechanism is simple to implement and using and can be executed at the two finishes of the system node.

Disadvantage:

- All the routers must upholding multiple stack protocols.
- Dual-stack hubs require more processor and memory assets since two separate convention stacks are running on a similar node.
- All tables are put away twice due to a stack convention.
- The directing conventions must arrangement with IPv4 and IPv6.

The points of Advantage and Disadvantage of the 6to4 tunneling mechanism are:

Advantage:

- easy and stable manual tunneling.
- Manual tunneling are more secure than other tunneling instruments.

Disadvantage:

- Tunnels should physically design the source and target of the tunnels.
- Routers at the two closures of the tunnels must help various stack conventions.
- Communication might be conceivable between two fringe hubs.
- This sort of tunnels isn't entirely adaptable, so it is appropriate for lasting associations.

The advantages and disadvantages of the Translation NAT-PT mechanism are:

Advantage:

- NAT-PT is that no changes are required on existing Hosts if NAT-PT is configured, because all NAT-PT configurations are made on a NAT-PT device.
- Static IPv4 networks can provide an IPv6 network and use NAT-PT to connect between these networks without disrupting the network. For smooth transition, you can use FTP between IPv4 and IPv6 Hosts.

Disadvantages:

- because of the fast time NAT-PT transition mechanism got the highest level of Packet loss.

CHAPTER V
CONCLUSION

5.1. Conclusion

Based on the discussion above, the conclusions can be drawn as follows:

1. the performances of these three mechanisms have been analyzed by GNS3 and JPerf in emulation system and got the results of the latency ,throughput and packet loss parameters for all the mechanisms as real time results , using the packet size 500 bytes to appear on the latency time of transfer which were 200 msec in translation mechanism (NAT-PT), 210 msec in dual stack, then 220 msec in tunneling mechanism. and using packet size 1200 Bytes to appear on the throughput which were 6.2 Kbytes/sec in Translation Mechanism (NAT-PT) , and the throughput increased in dual stack with 7.2 kbytes/sec ,then the tunneling mechanism the throughput also seems to increase with 8 Kbytes/sec., and by using packet size 1024 Bytes can be know how the Packet loss by percentage, the Packet loss in the tunneling mechanism 4.2%, in dual stack the Packet loss increased by 4.9%, then the Translation Mechanism (NAT-PT) the Packet loss got more increase by 6.5% the reason of that high packet loss the time of the transition in Translation performance is so fast.

2. As can be shown from the emulation results of this research, the results of throughput, latency and Packet loss, can be discovered that the Translation NAT-PT mechanism had the fast latency ,the tunneling had the best throughput and less packet loss , and the dual stack keeps the moderating in all of the parameters .

5.2. Future work Recommendations

For the Recommendations, the Tunneling instrument technique has some of security issues that can will be understood by IP security (IPSec) . that is the reason I prescribe to utilize tunneling mechanism mode with IP security (IPSec) for the most secure progress reason.

REFERENCES

[1] S. Deering, R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460. 2005.

[2] Raicu, I. and Zeadally, S., "Evaluating IPv4 to IPv6 transition mechanisms," in Telecommunications, ICT 2003. 10th International Conference on, vol.2, no., pp.1091-1098 vol.2, 23 Feb.-1 March 2003.

[3] Hossain, M.A., Poddre, D., Jahan, S., Hussain, M. Performance Analysis of Three Transition Mechanism Between IPv6 Network and IPv4 Network: Dual Stack, Tunneling and Translation. IJC. 2016.

[4] Shiwani, S., Purohit, G.N., Hemrajani, N. Performance Analysis of IPv4 v/s IPv6 in Virtual Environment Using UBUNTU. IJCA. 2011.

[5] Albkerat, A. and Issac, B. Analysis of IPv6 Transition Technologies. IJCN: 6(5). 2014

[6] Punithavathani, D.S and Sankaranarayana, IPv4/IPv6 Transition Mechanism. European Journal of Scientific Research. 34(1): 110-124. 2009.

[7] Rajkumar, A. and Kannan, G. IPv6 Performance Analysis Based on Protocol and Tunnel Transition. IJSR. ISSN (Online): 2319-7064.

[8] Khannah, B. and Alsa'deh, A. Impact of IPv4/IPv6 Transition Techniques on Applications Performance. Conference Paper. 2017.

[9] Hanumanthappa, J. and Manjaiah, D.H. IPv6 an IPv4 Threat Review with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model: A Case Study for University of Mysore Network. IJCSIS. 3(1): 1-12. 2009.

[10] Alzaid, W. and Issac, B. Analysis of IPv6 Through Implementation of Transition Technologies and Security Attacks. International Journal of Business Data Communications and Networking. 2016.

[11] Yu, S. and Carpenter, B.E. Measuring IPv4 – IPv6 Translation Techniques. The University of Auckland. 2012.

[12] C. V. Ravi Kumar, KakumanilakshmiVenkatesh, MarriVinaySagar and Kala Praveen Bagadi. Performance Analysis of IPv4 to IPv6 Transition Methods. Indian Journal of Science and Technology, Vol 9(20), 2016.

[13] Xie, L., Bi, J., and Wu, J. A Multihoming Based IPv4/IPv6 Transition Approach. LNCS 4479: 902-911. 2007.

[14] Mackay, M. and Edward, C. A Comparative Performance Study of IPv6 Transitioning Mechanisms - NAT-PT vs. TRT vs. DSTM. F. Boavida et al. (Eds.): NETWORKING 2006, LNCS 3976, pp. 1125 – 1131, 2006.

[15] Narayan, S. and Tauch, S. Network Performance Evaluation of IPv4-v6 Configured Tunnel and 6to4 Transition Mechanisms on Windows Server

Operating Systems. International Conference On Computer Design And Appliations (ICCDA). 2010.

[16] Raste, T.M. and Kulkarni, D.B. Design and Implementation Scheme for Deploying IPv4 over IPv6 Tunnel. Journal of Network and Computer Application. 31: 66-72. 2008.

[17] Kanthikeyan, N. and Mouli, K. C. Corporate Migration from IPv4 to IPv6 using Different Transition Mechanism. IJESS7. 5(10): 802-808. 2016.

[18] Oliviera, L., Amaral, A., de Sousa, A. Mobility in IPv4-IPv6 Transition Scenarios. Institute of Telecomunication Portugal. 2002.

[19] Gao, J. and Zhao, Q. 6in4 Tunnel Based IPv6 Transition Solution for IPv4 Mobile Terminals. International Journal of Computer and Communication Engineering. 3(6). 2014.

[20] Dawadi, B.R., Joshi, R.S., Khanal, A.R. Service Provider IPv4 to IPv6 Network Migration Strategies. Journal of Emerging Trends in Computing and Information Sciences. 8(10). 2015.

[21] Mukti, A. R., Ismail, Z., and Negara, E.S. Performance Analysis for Migration Method IPv4 to IPv6 Using Dual-Stack Technique. International Conference on Information Technology and Engineering Application. 2016.

[22] Wu, P., Cui, Y., Wu, J., Liu, J. and Metz, C., “Transition from IPv4 to IPv6: A state-of-the-art survey”, IEEE Communications Surveys & Tutorials, 15(3), pp.1407—1424, 2013.

[23] van Beijnum Comparison of IPv6 over IPv4 Tunnel Mechanisms draft-steffann-tunnels-03I. Institute IMDEA Networks April 11, 2013

[24] Arafat, M., Ahmed, F. and Sobhan, M. (2014). On the Migration of a Large Scale Network from IPv4 to IPv6 Environment, International Journal of Computer Networks & Communications (IJCNC), 6(2), pp.111-126.

[25] Wu, Y. and Zhou, X. (2011). Research on the IPv6 performance analysis based on dual-protocol stack and Tunnel transition, Proceedings of the 6th International Conference on Computer Science & Education (ICCSE), pp.1091--1093.

[26] Coonjah, Irfaan; Catherine, Pierre Clarel; Soyjaudah, K.M.S., "6to4 tunneling framework using OpenSSH," in Computing, Communication and Security (ICCCS), 2015 International Conference on , vol., no., pp.1-4, 4-5 Dec. 2015.Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2005.

[27] Chen, J., Chang, Y. and Lin, C. (2004). Performance investigation of IPv4/IPv6 transition Mechanisms, Proceedings of the 6th International Conference on Advanced Communication Technology, pp.545--550.

[28] Narayanan, A., Mohideen, M. and Raja, M. (2012). IPv6 TunnellingOver IPV4, International Journal of Computer Science Issues (IJCSI), 9(2), pp.599-604.

[29] Xiaodong, Z., et. al. (2009). Research on the Next-generation Internet transition technology, Proceedings of Second International Symposium on Computational Intelligence and Design (SCID '09), pp.380-382.

[30] Ahmad, N. and Yaacob, A. (2012). IPSec over Heterogeneous IPv4 and IPv6Networks: Issues and Implementation, International Journal of Computer Networks & Communications (IJCNC), 4(5), pp. 57-72.

[31] Bi, J., Wu, J. and Leng, X. (2007). IPv4/IPv6 transition technologies and univer6 architecture, International Journal of Computer Science and Network Security, 7(1), pp.232--242.

[32] S. Hagen, IPv6 Essentials, O'Reilly, July 2002.

[33] K. Wang, A.K. Yeo and A.L. Ananda, “DTTS: a Transparent and Scalable Solution for IPv4 to IPv6 Transition,” Proceedings of the tenth International Conference on Computer Communications and Networks, 2001, pp.248-253.

[34] Handbook of IPv4 to IPv6 Transition, Methodologies for Institutional and Corporate Networks, By John J. Amoss& Daniel Minoli.

[35] https://sourceforge.net/projects/jperf/

[36] http://www.allconsuming.net/what-is-gns3-and-why-do-you-need-it/

APPENDICES

❖ Scenario 1 6to4 tunneling.

Router HQ

```
HQ#show run hostname HQ
!
!
ipv6 unicast-routing
!
interface Tunnel0
noip address
ipv6 address fec0::12:1/128
ipv6ospf 64512 area 0 tunnel source Serial0/0/0
tunnel destination 192.168.12.2
tunnel mode ipv6ip
!

interface Loopback0

ip address 190.168.5.1 255.255.255.0

ipv6 address fec0::11:1/128 ipv6 ospf 64512 area 0
!

interface FastEthernet0/0 no ip address
duplex auto

ipv6 address FEC0:87:1:3::1/64
ipv6ospf 64512 area 1
!
!

interface Serial0/0/0

ip address 192.168.11.1 255.255.255.252

clock rate 64000

!

interface Serial0/0/1
noip address
shutdown
clock rate 2000000

!

routerbgp 64000

bgp log-neighbor-changes
```

```
neighbor 192.168.11.2 remote-as 64000

!
address-family ipv4

neighbor 192.168.11.2 activate no auto-summary
no synchronization

network 192.168.11.0 mask 255.255.255.252  exit-address-
family
!

ip classless

!
ip http server
noip http secure-server

!

ipv6 router ospf 64512 log-adjacency-changes area 0
range FEC0::/64
area 1 range fec0:87:1:3::0/64

!

end
```

ROUTER ISP

```
ISP#show run
hostname ISP
!

!

noaaa new-model

!

resource policy

!

memory-sizeiomem 5

mmi polling-interval 60 no mmi auto-configure no mmi pvc
mmisnmp-timeout 180 ip subnet-zero ipcef!
```

```
voice-card 0

!
!
interface Loopback0

ip address 190.168.6.1 255.255.255.0

interface Serial0/0/0

ip address 192.168.11.2 255.255.255.252

!
interface Serial0/0/1
ip address 192.168.12.1 255.255.255.252

!
routerbgp 64000 no synchronization
bgp log-neighbor-changes

network 192.168.11.0 mask 255.255.255.252

network 192.168.12.0 mask 255.255.255.252

neighbor 192.168.11.1 remote-as 64000

neighbor 192.168.12.2 remote-as 64000 no auto-summary
!

ip classless

!

End
```

ROUTER BRANCH OFFICE

```
Br#showrun
hostname Br
!

noaaa new-model

!

resource policy

!
```

```
mmi polling interval 60 no mmi auto-configure no mmi pvc mmi
snmp-timeout 180 ip subnet-zero ipcef

!

ipv6 unicast-routing

!

voice-card 0

!
interface Tunnel0 no ip address
ipv6 address fec0::4:4/128   ipv6 ospf 64513 area 0 tunnel
source Serial0/0/0
tunnel destination 192.168.11.1 tunnel mode ipv6ip
!

interface Loopback0
ip address 190.168.7.1 255.255.255.0

ipv6 address FEC0::13:1/128 ipv6 ospf 64513 area 0
!


interface FastEthernet0/0 no ip address
duplex auto speed auto
ipv6 address FEC0:87:1:4::1/64 ipv6 ospf 64513 area 1
!

interface
!

interface Serial0/0/0

ip address 192.168.12.2 255.255.255.252

clock rate 64000

!

routerbgp 64000

bgp log-neighbor-changes

neighbor 192.168.12.1 remote-as 64000 address-family ipv4
neighbor 192.168.12.1 activate no auto-summary
no synchronization network 192.168.12.0
network 192.168.11.0 exit-address-family
```

```
!

ip classless

!
ipv6 router ospf 64513
log-adjacency-changes area 0 range FEC0::/64
area 1 range FEC0:87:1:4::/64

!

ipv6 router ospf 64512 log-adjacency-changes
!

control-plane

!

line con 0

line aux 0

linevty 0 4 login
!

End
```

❖ Scenario 2 Dual Stack

Router HQ

```
HQ#showrun
hostname HQ

!

boot-start-marker boot-end-marker
!

noaaa new-model
!

interface Loopback0

ip address 190.168.5.1 255.255.255.0

ipv6 address fec0::11:1/128 ipv6 ospf 64512 area 0
!
```

```
interface FastEthernet0/0

ip address 192.168.14.1 255.255.255.0

duplex auto speed auto
ipv6 address fec0:87:1:3::1/64 ipv6 ospf 64512 area 1
!
interface FastEthernet0/1 no ip address
shutdown duplex auto speed auto

!

interface Serial0/0/0

ip address 192.168.11.1 255.255.255.252

ipv6 address 2001:2:11::1/112 ipv6 ospf 64512 area 0
clock rate 64000

!

interface Serial0/0/1
noip address shutdown
clock rate 2000000

!

routerospf 64512

log-adjacency-changes

passive-interface  FastEthernet0/0 network 192.168.11.0
0.0.0.3 area 0
network 190.168.5.1 0.0.0.255 area 0

network 192.168.11.0  0.0.0.3 area 1

!

ip classless

!

!

ip http server

noip http secure-server
```

```
!

ipv6 router ospf 64512 log-adjacency-changes

area 0 range 2001:2:11::/48 area 0
range fec0::/112
area 1 range fec0:87:1:3::1::/64
passive-interface FastEthernet0/0
!

control-plane

!

line con 0

line aux 0

linevty 0 4 login
!

end
```

Router ISP

```
ISP#showrun
hostname ISP
!

boot-start-marker boot-end-marker
!

!

noaaa new-model

!
resource policy

!

memory-sizeiomem 5

mmi polling-interval 60 no mmi auto-configure no mmi pvc
mmisnmp-timeout 180 ip subnet-zero ipcef

!
```

```
ipv6 unicast-routing

!

voice-card 0

!

interface Loopback0

ip address 190.168.6.1 255.255.255.0

ipv6 address fec0::12:1/128 ipv6 ospf 64000 area 0
!

interface FastEthernet0/0 no ip address
shutdown duplex auto speed auto
!

interface FastEthernet0/1 no ip address
shutdown
duplex auto speed auto
!

interface Serial0/0/0

ip address 192.168.11.2 255.255.255.252

ipv6 address 2001:2:11::2/112
ipv6ospf 64000 area 0
!

interface Serial0/0/1

ip address 192.168.12.1   255.255.255.252

ipv6 address 2001:22:11::1/112
ipv6ospf 64000 area 0
!

routerospf 64000

log-adjacency-changes

network 192.168.11.0 0.0.0.3 area 0

network 192.168.12.0  0.0.0.3 area 0

network 190.168.6.0 0.0.0.255 area 0
```

```
!

ip classless

!

!

ip http server

noip http secure-server ipv6 router ospf 64000 log-
adjacency-changes
area 0 range 2001:22:11::/112  area 0
range fec0::/112
!

End
```

Router Branch office

```
Br#showrun
hostname Br
!

noaaa new-model

!

mmi polling-interval 60 no mmi auto-configure no mmi pvc
mmisnmp-timeout 180 ip subnet-zero
ipcef

!

ipv6 unicast-routing

!

voice-card 0

!

!

interface Loopback0

ip address 190.168.7.1 255.255.255.0

ipv6 address fec0::13:1/128 ipv6 ospf 64513 area 0
```

```
!

interface FastEthernet0/0

ip address 192.168.13.1 255.255.255.0

duplex auto speed auto
ipv6 address FEC0:87:1:4::1/64

ipv6ospf 64513 area 1

!

interface FastEthernet0/1 no ip address
shutdown duplex auto speed auto
!
interface Serial0/0/1 no ip address shutdown
no fair-queue clock rate 2000000
!

interface Serial0/0/0

ip address 192.168.12.2  255.255.255.252

ipv6 address 2001:22:11::2/112
ipv6ospf 64513 area 0
clock rate 64000

!

routerospf 64513

log-adjacency-changes

passive-interface FastEthernet0/0 network 192.168.12.0
0.0.0.3 area 0
network 190.168.7.0 0.0.0.255 area 0

network 192.168.13.0 0.0.0.255 area 1

!

ip classless

!

ip http server

noip http secure-server
```

```
ipv6 router ospf 64513 log-adjacency-changes
area 0 range 2001:22:11::/112 area 0
range fec0::/112
area 1 range fec0:87:1:4::/64 passive-interface
!

end
```

❖ Scenario 3 NAT-PT

ROUTER ISP

```
Hostname ISP
ipv6 unicast-routing
!
interface Serial0/0/0
ip address 192.168.11.2 255.255.255.0
duplex auto
speed auto
ipv6nat
!
interface Serial0/0/1
noip address
duplex auto
speed auto
ipv6 address 2001:2:22::1/112
ipv6 enable
!
ipv6 route ::/0 2001:2:22::
ipv6nat v4v6 source 192.168.11.3 2001::960B:202

!--- Translates the ipv4 add of R2 fa0/0 to ipv6 address.

ipv6nat v6v4 source fec0::13:1 150.11.3.1

!--- Translates the ipv6 add of loop0 of R3 to ipv4 address.

ipv6nat prefix 2009::/96

!--- The destination prefixes that matches 2009::/96
!--- are translated by NAT-PT.

!
End
```

ROUTER HQ

```
hostname HQ
!
interface Serial0/0/0
ip address 192.168.11.1 255.255.255.252
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 192.168.11.0
!
interfacefastethernet 0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
!
End
```

ROUTER BRANCH OFFICE

```
hostname BO
ipv6 unicast-routing
!
interface Loopback0
noip address
ipv6 address fec0::13:1/128
!
interface Serial0/0/0
noip address
duplex auto
speed auto
ipv6 address 2001:2:22::2/112
!
ipv6 route ::/0 2001:2:22::
!
interfacefastethernet 0/0
noip address
duplex auto
ipv6 address FEC0:87:1:4::1/64
!
End
```

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH

Saya yang bertandatangandibawahini:

Nama	:Musab Ali Saleh El Nefati
NIM	:MTE.16180191
Program Studi	:MagisterTeknik Electro
Alamat asal	:Tripoli-Tajoura-State of Libya
No.Hp/Email	:+218919752895 whatsapp / mosabalnfatti@gmail.com

Dengan ini menyampaikan karya ilmiah berupa tesis dengan judul:

Analysis The Connection Performance Between IPv6 Network and IPv4 Networks using GNS3 and Jperf

Dan menyetujuinya menjadi hak milik Universitas Islam Sultan Agung serta menyediakan Hak Bebas Royalti Non-eksklusif untuk disimpan, dialihmeciakan, dikelola dalam pangkalan data, dan dipubillasikannya diinternet atau media lain untuk kepentingan akademis selama tetap mencantumkan nama penulis sebagai hak pemilik Hak Cipta.

Pernyataan ini saya buat dengan sungguh-sungguh Apabila dikemudian hari terbukti ada penyalahgunaan hak Cipta / Plagiatisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan pihak lain Universitas Islam Sultan Agung.

Semarang 2019

TERAI TEMPEL enyatakan

6000

Musab Ali Saleh El Nefati

JOURNAL

PERFORMANCE ANALYSIS OF THE CONNECTION BETWEEN IPv6 AND IPv4 NETWORKS

Musab Ali Saleh El Nefati[1], Arief Marwanto[2], Ir. Suryani Alifah[3] ,Qomaruddin[4]

(1) Student of postgraduate Electrical Engineering at Master of Electrical Engineering Department, Industrial Technology Faculty, Sultan Agung Islamic University

(2,3,4) Staff of Master of Electrical Engineering Department , in Industrial Technology Faculty, Sultan Agung Islamic University

Semarang ,Indonesia , +62 896-6831-4951

e-mail:

(1) mosabalnfatti@gmail.com
(2) arief@unissula.ac.id
(3) Suryani.alifah@unissula.ac.id
(4) mqomaruddin@unissula.ac.id
Correspondent Author: arief@unissula.ac.id

Abstract

The IPv4 that is currently used is limited to handle new requests from IP addresses. To fix this problem IPv6 has been deployed. But the IPv4 can't be directly used , it should be get along with IPv6 . For the connection from IPv4 to IPv6 and opposite, there are three transition mechanisms. which are tunneling, translation and dual stack. In this research, the performances of these three mechanisms have been analyzed by GNS3 and JPerf in emulation system. the performance to get the results that shown of latency ,throughput and packet loss parameters for all the mechanisms as real time results. it can be seen that the Translation NAT-PT mechanism has the fast latency ,the tunneling has the best throughput and less packet loss and the dual stack keeps the moderating in all of the parameters, The Packet loss in the tunneling mechanism (4.2%), in dual stack the Packet loss increased by (4.9%), then the Translation Mechanism (NAT-PT) the Packet loss got more increase by (6.5%) the reason of that high packet loss the time of the transition in Translation is so fast.

***Keywords**: IPv6, IPv4, dual stack, tunnel, translation*

1. Background

Each node and hub needs an IP address to convey between the hosts. Address number of as of now utilized IP variant 4 is too restricted to even consider handling the new interest of IP addresses [1].

Switching from IPv4 to IPv6 requires a uniform method of disconnections and errors in the network. This requires a significant management of the main nodes, devices and systems for new IP generation. However, IPv6 addresses still work with IPv4 addresses; This means that IPv6 networks will join future IPv4 networks. However, IPv4 does not support the new network criteria. The current IPv4 network is large and complex, because IPv4 cannot be changed with IPv6. Switching from one technology to another is very difficult, because IPv4 and IPv6 are not the same set of communications. Three well-known transition mechanisms are known as Dual Stack, tunneling and translation [2]

There are some techniques developed to handle this address space problem, they are Network Address Translation (NAT), Variable Length Subnet Mask (VLSM), Classless Inter domain Routing (CIDR), Port address translation (PAT) and so on. But these all technology are not able to save the IP address shortage's problem. Due to the limitation of IPv4 addresses, another technology raised: Internet Protocol Version 6 (IPv6). The IPv6 was designed for sufficient address space for the present and the future demand for the increased growth of internet. IPv6 increases IP address scheme size from IPv4-32 bits to 128 bits [2]. IPv6 address is cooperated with IPv4 address; this means IPv6 networks is able to merge with IPv4 networks for the future networks. But, anyhow IPv4 does not support new upcoming network criteria. The present IPv4 network is huge and complex, so IPv4 could not be replaced by IPv6 suddenly. Migration from one technology to another technology is absolutely difficult, because of IPv4 and IPv6 are not same assemblage for communication. The three prominent transition mechanisms are widely known as Dual Stack, Tunneling and Network address translation [3].

Though previous works have been done on the comparison and the analyzing between these mechanisms, but by simulation tools not emulation tools and still many problems not resolved yet, calling for huge challenges on IPv6 transitions research. In this paper, the analysis has been done after implement the networks one by one for each performances.

2. Problem Statement

Based on the description in the background above, the formulation of the problem of the research is the performance of Dual Stack, Tunneling and Translation between IPv6 Network and IPv4 Network using emulation system more than simulation system are analyzed:

How the performance of dual stack, tunneling, and translation are analyzed?

How the performance of dual stack, tunneling, and translation in emulation system?

Purpose of this study to analyze dual stack, tunneling, and translation performance that used to communicate with IPv6 and IPv4 nodes independently without changing networks. which is analyzed using GNS3 and JPerf in emulation system.

3. Literature Review

a. Dual Stack

The dual stack approach is considered one of the most straight forward transitions. This dual stack method assumes that both the host / router provides support for both IPv4 protocols, IPv6 in its architecture and has the ability to send / receive IPv4 and IPv6 packets. It can also operate in one of three modes such as (1) When both the host / host source / stack is enabled IPv4, or (2) When both the Source / Destination host is the IPv6 stack that is activated, or (3) One source host / The recipient host is an IPv4 / IPv6 stack that is activated. Dual stack is one that supports both IPv4 or IPv6 protocols, can be configured with IPv4 32 bit addresses or IPv6 128 bit addresses using mechanisms such as DHCP to obtain IPv4 addresses and use IPv6 mechanisms such as automatic configuration without status, or DHCPv6 to obtain addresses IPv6.[4]

According to Wu, et. al (2013), the ethernet contains nodes and these nodes can support both protocols in parallel in the same infrastructure. Therefore, nodes can provide data transmission for IPv4 and IPv6. This technique is not suitable for large networks such as the Internet because it is difficult and expensive to close all nodes on such a large network. On the other hand, it is suitable for small networks, which require less management and are easily controlled. Double piles are considered to be the basis for creating two other techniques for the transition between IPv4 and IPv6.[4]

b. Tunneling

By encapsulating IPv6 packets inside IPv4 packets, IPv6-capable hosts and IPv6-capable networks isolated from other IPv6-capable systems or the IPv6 internet at large can exchange IPv6 packets over IPv4-only infrastructure[5].

Tunneling mechanisms [7] are techniques in which one protocol is encapsulated in another protocol according to the network where the packet has to be routed. Several tunneling mechanisms can be used for this reason, and according to their configuration, they can be classified into manual and automatic tunnels. Manual Tunneling The manual tunnel [6; 7], also called static tunnel, is a point-to-point tunnel used to allow IPv6 hosts/sites to communicate between them by encapsulating IPv6 packets in IPv4 packets (Protocol v4 number 41) and route them through IPv4 routing infrastructures. Both ends of the tunnel have to be dual stack nodes and configured manually. The node that is performing the tunnel has configuration information that determines the endpoint address of the tunnel. Once the IPv6 packet arrived at the endpoint of the tunnel, it will be decapsulated and then transmit to its destination. Automatic Tunneling Automatic tunnels [6] are point-to-multipoint tunnels in which nodes that are performing the tunnel have to be dual stack nodes and affected by IPv6 IPv4-compatible addresses where the IPv4 address of the tunnel endpoint is integrated into the IPv6 IPv4-compatible address [7].

c. Translation

The translation mechanism changes the header format from IPv4 to IPv6 format and vice versa. This scheme translates packages from both addresses. Using this translation, IPv6 hosts can only communicate with IPv4 hosts only. The translation method consists of two types, such as stateless and stateful. Citizenship translation, packages are not interrelated with one another while translations with state are interrelated. Translation without state, there is no reference to translucent packages during the temporary conversion of translations related to the previous package[8].

d. IPv4

IPv4 is considered as the core of internet addressing, because it allows data transmission using TCP / IP. IPv4 contains 32 bits. This can include 4.3 billion addresses. The address is represented as 192.168.2.1. Each can be from 0 to 255, can theoretically address up to 4 billion computer hosts or more precisely 4,294,967,296 hosts worldwide, the number of hosts is obtained from 256 (obtained from 8 bits) in the 4th rank (because there are 4 octets) so the maximum value of the IP version 4 address is 255.255.255.255 where the value is calculated from zero so that the value of the host value that can be accommodated is 256x256x256x256 = 4,294,967,296 hosts, if the host exceeds the quota then IP version 6 or IPv6 is made. In general, IPv4 contains five classes. Each class provides different restrictions for address numbers for networks and hosts.The IP address of version 4 is divided into several classes, seen from the first octet, as shown in the table. Actually the difference between the IP class version 4 is the binary pattern found in the first octet (mainly the initial / high-order bits), but to be easier to remember, it will be remembered faster by using decimal representations [9].

e. IPv6

IPv6 Internet Protocol was developed as a future network layer protocol to come, to overcome the shortage of IPv4 address space. IPv6 is the sixth version of the IP address. The IPv6 protocol address is 128-bit long. To represent a 128-bit address, IPv6 uses a total of 8 fields consisting of 4 hexadecimal values separated by colons represented like (:). So that it allows 2 ^ 128 = 3,4 × 1038 addresses.[10]

4. System Method

The transition between IPv4 Internet and IPv6 Internet will be a long process as long as the two protocols coexist. Various transition strategies can be divided into three categories, including dual stack, tunneling and translation mechanisms. In this research to analyzed the transition strategy IPv4 to IPv6 will use GNS3 and JPERF.

The Implementation agreements have been concluded between the head office and the branches of an enterprise through a public network (Internet Service Provider). Three model samples were tested in the laboratory to assess the complexity, advantages and disadvantages of each method. The implementation work is carried out according to two scenarios by applying three methods such as the 6to4 manual tunnel and the double stack.

- Method Scenario 1: 6to4 manual tunnel.
- Method Scenario 2: Dual stack.
- Method Scenario 3: Translation NAT-PT

Behind the choice of these two special methods, it is easy to implement the existing material in an organization rather than spending the budget on new equipment and accessories. The basic topology has been established with three routers named Headquarters (HQ), Internet Service Providers (ISP) and Branches (Br). With this, two clients named Host1 and Host2 are used. The detailed connectivity process was explained in each scenario. In the three connectivity scenarios are the same. The equipment that will be usedare:

- Router: Cisco 2800 Series with Cisco IOS Release 12.4 (4) T8.
- Client: Windows with a IP.

4. Scenario 1 6to4 manual tunnel

d. Physical connection

The network will be built between HQ and Br branches through an ISP. In Scenario 1, prepare a network, three routers, and two clients to use. Host 1 will be connected to the fa0 / 0 HQ interface with an Ethernet cable. The HQ 0/1/0 interface series [DCE] will be connected to the ISP 0/1/0 [DTE] serial interface using a serial cable. The serial interface ISP 0/1/1 [DTE] is connected to the serial interface Br 0/1/1 [DCE] using a serial cable. The Br fa0 / 0 interface is connected to Host2 with an Ethernet cable. This ensures physical connectivity between headquarters and the branch (Figure 1).

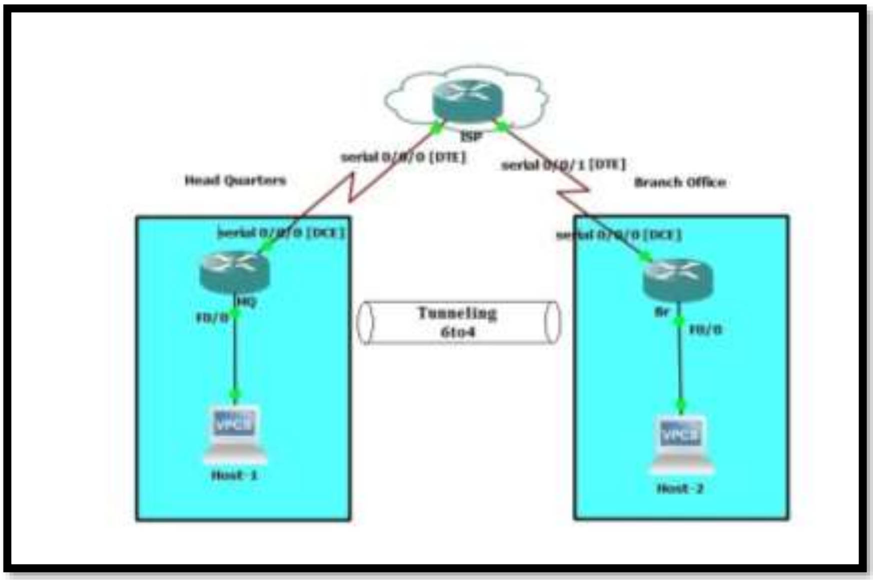


Figure1. Tunneling Topology

e. IP Address Scheme

Table 1. Host 1 and 2 IP Address

Host	IPv6 address	IPv6 Gateway address
Host 1	FEC0:87:1:3::2/64	FEC0:87:1:3::1/64
Host 2	FEC0:87:1:4::2/64	FEC0:87:1:4::1/64

Table 2. Headquarters', ISP and Branch IP Addresses [8]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	FastEthernet 0/0	--	FEC0:87:1:3::1/64
	Serial 0/0/0	192.168.11.1/30	--
	Loopback 0	190.168.5.1/24	FEC0::11:1/128
	Tunnel 0	--	FEC0::12:1/128
ISP	Loopback 0	190.168.6.1/24	--
	Serial 0/0/0	192.168.11.2/30	--
	Serial 0/0/1	192.168.12.1/30	--
Branch	Loopback 0	190.168.7.1/24	FEC0::13:1/128
	Serial 0/0/0	192.168.12.2/30	--
	FastEthernet 0/0	--	FEC0:87:1:4::1/64
	Tunnel 0	--	FEC0::4:4/128

f. Establishment of routing

Routing of communication protocols from HOST-1 to HOST-2, performed on all routers (Table 2 and 3). This routing protocol uses two types of protocols on the network. Thus, BGP as the External Gateway Protocol (EGP) for public networks such as the ISP network and the Inner Gateway Protocol (IGP) is OSPFv3 for private networks such as LAN connections. OSPFv3 is a status binding protocol that speeds up the merge of the wide network routes and preserve a copy of the tables of the routing that support IPv6 routing primarily.BGP is a vector-based steering convention, generally utilized as an EGP convention on the Internet. Two IP conventions are utilized in this situation, for example, IPv4 for open networks and IPv6 for close networks . Open systems are utilized between home office to ISP and among ISP and Br. close networks are utilized to set up an association between HOST-1's central command and HOST-2's base Router. with the [H Q] Router, OSPFv3 is arranged for IPv6 and BGP networks for IPv4 systems. Since the ISP switch is on a public open network BGP is configured. On the [B R] router, OSPFv3 is configured for IPv6 and BGP networks for IPv4 networks. Routing protocols are established on all routers, but the incompatibility between IPv4 and IPv6 does not allow the connection between HOST-1 and HOST-2.

In the first Scenario, an IPv6 packet from Host-1 is created to the send point as Host-2 and already sent to [H Q] . The [H Q] router is the first point of the tunnel that encapsulates IPv6 packets in IPv4. It is sent via ISP by IPv4 routes to the final point in the tunnel. The final point of the tunnel is the [B R] router that will separate IPv6 packet from IPv4 packets and send it to Host-2.

5. Scenario 2 (Dual stack)

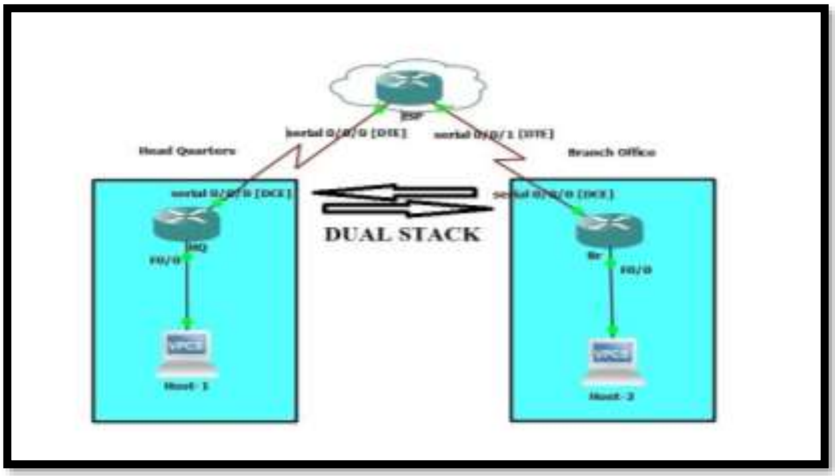


Figure 2. Dual Stack Topology

e. Physical connection
   The physical settings of second Scenario have done by the same method as the first Scenario. three routers and two clients are used. Host-1 connected to the FA0 / 0 [H Q] interface with a straight Ethernet cable. The [H Q] 0/0/0 series interface [DCE] is connected to the ISP 0/0/0 [DTE] serial interface with a serial cable. The serial interface ISP 0/0/1 [DTE] is connected to the serial interface [Br] 0/0/0 [DCE] using a serial cable. The [B r] FA0 / 0 interface is connected to HOST-2 with a straight Ethernet cable. This ensures physical connectivity between headquarters and the branch (Figure 2).

f. IP Address Scheme

Table 3. Host 1 and 2 IP Address

Host	Criteria	IPv4 address	IPv6 address
Host 1	Ethernet	192.168.14.10/24	FEC0:87:1:3::2/64
	Gateway address	192.168.14.1/24	FEC0:87:1:3::1/64
Host 2	Ethernet	192.168.13.20/24	FEC0:87:1:4::2/64
	Gateway address	192.168.13.1/24	FEC0:87:1:4::1/64

Table 4. Headquarters’, ISP and Branch IP Addresses [8]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	FastEthernet 0/0	192.168.14.1/24	FEC0:87:1:3::1/64
	Serial 0/0/0	192.168.11.1/30	2001:2:11::1/112
	Loopback 0	190.168.5.1/24	FEC0::11:1/128
ISP	Loopback 0	190.168.6.1/24	FEC0::12:1/128
	Serial 0/0/0	192.168.11.2/30	2001:2:11::2/112
	Serial 0/0/1	192.168.12.1/30	2001:22:11::1/112
Branch	Loopback 0	190.168.7.1/24	FEC0::13:1/128
	Serial 0/0/0	192.168.12.2/30	2001:22:11::2/112
	FastEthernet 0/0	192.168.13.1/24	FEC0:87:1:4::1/64

g. Establish routing
In the second Scenario, the both versions of the IP protocols are used on the all routers (Table 3 and 4). Two protocols (IPv4 and IPv6) work together, so all the routers must have duo routing protocols to uphold that infrastructure. The routing protocol OSPFv3 can support IPv4 and IPv6 on single node but is classified into duo routing tables on each node. SPFv3 is configured on each router ([H Q] , ISP, Br) for the both IP versions addresses. This allows the mechanism of dual stack routing between the nodes. The Dual Stack transition is used to uphold each network IP protocol. The node of Dual Stack can send and communicate together with IPv6 and IPv4 traffic.

6. Scenario 3 (Translation)

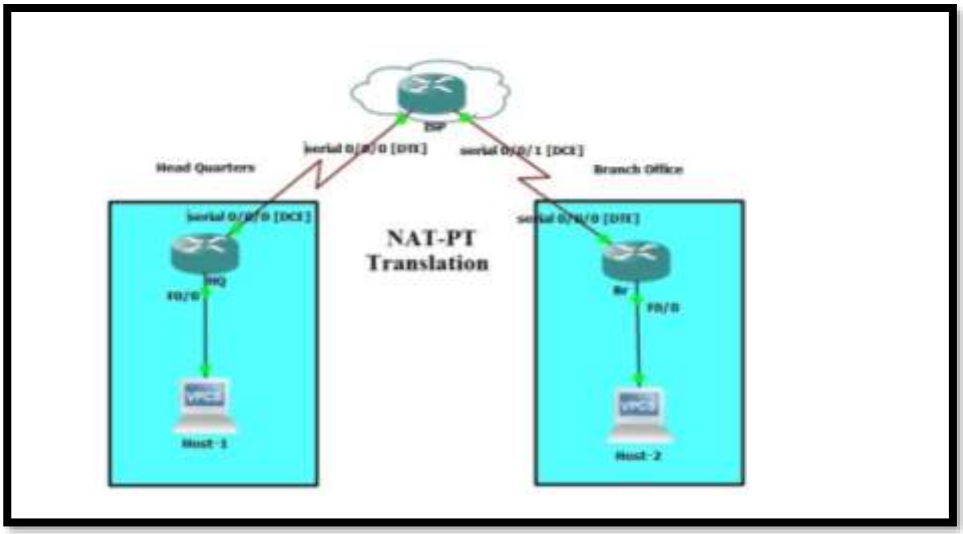


Figure 3.NAT-PT Topology

b. Physical connection
The network will be built between [H Q] and [B R] branches through an ISP. In Scenario 3, prepare a network, three routers, and two clients (Hosts) to use. Host-1 will be connected to the Ethernet interface FA 0/0 [H Q] with a straight Ethernet cable. The [H Q] Se0/0/0 interface series [DCE] will be connected to the ISP Se0/0/0 [DTE] serial interface using a serial cable. The serial interface ISP Se0/0/1 [DCE] is connected to the serial interface [B R] Se0/0/0 [DTE] using a cable serial. The [B R] FA 0/0 interface is connected to HOST-2 with a straight Ethernet cable (Figure 3).

.

c. IP Address

Table 5. Host 1 and 2 IP Address

Host	Criteria	IPv4 address	IPv6 address
Host 1	Ethernet	192.168.13.10/24	--
	Gateway address	192.168.13.1/24	--
Host 2	Ethernet	--	FEC0:87:1:4::2/64
	Gateway address	--	FEC0:87:1:4::1/64

Table 6. Headquarters', ISP and Branch IP Addresses [9]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	Fast Ethernet 0/0	192.168.13.1/24	--
	Serial 0/0/0	192.168.11.1/30	--
ISP	Serial 0/0/0	192.168.11.2/30	--
	Serial 0/0/1	--	2001:2:22::1/112
	ipv6 NAT v4v6 source	192.168.11.3	2001::960B:202
	ipv6 NAT v6v4 source	150.11.3.1	FEC0::13:1/128
	ipv6 nat prefix		2009::/96
Branch	Loopback 0		FEC0::13:1/128
	Serial 0/0/0	--	2001:2:22::2/112
	Fast Ethernet 0/0	--	FEC0:87:1:4::1/64

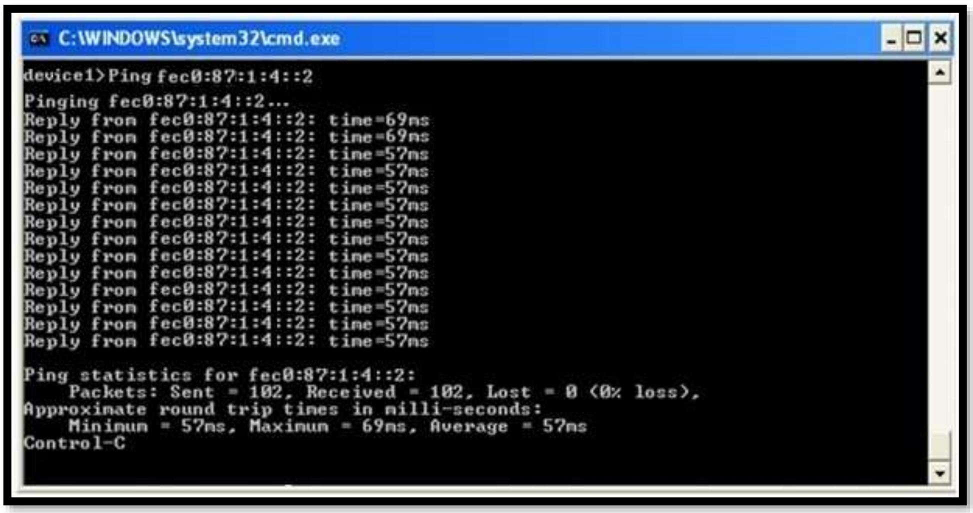
In the third Scenario, an IPv6 packet from Host-1 is created to the point as Host-2 and sent to [H Q] (Table 5 and 6). The [H Q] router is the first point of the send traffic that encapsulates IPv4 packets in IPv6. It is sent via ISP via IPv6 routes at the final point of the destination . The final point of the send traffic is the [B R] router that separates IPv4 packets from IPv6 packets and sends them to HOST-2 using OSPFv3

3. Results and Analysis

3.1. Testing Result

3.1.1. Ping and trace route Testing for 6to4 Tunnel (Scenario 1)

A ping and trace route test are a commands to test the connections between two nodes of a network. The use of the latency ping command between two nodes will be explained. Ping results between host1 to host2 between host1 to host2 (IPv6:FEC0:87:1:4::2) to determine latency and packet loss over of 100 packages the following (Figure 4 and 5):

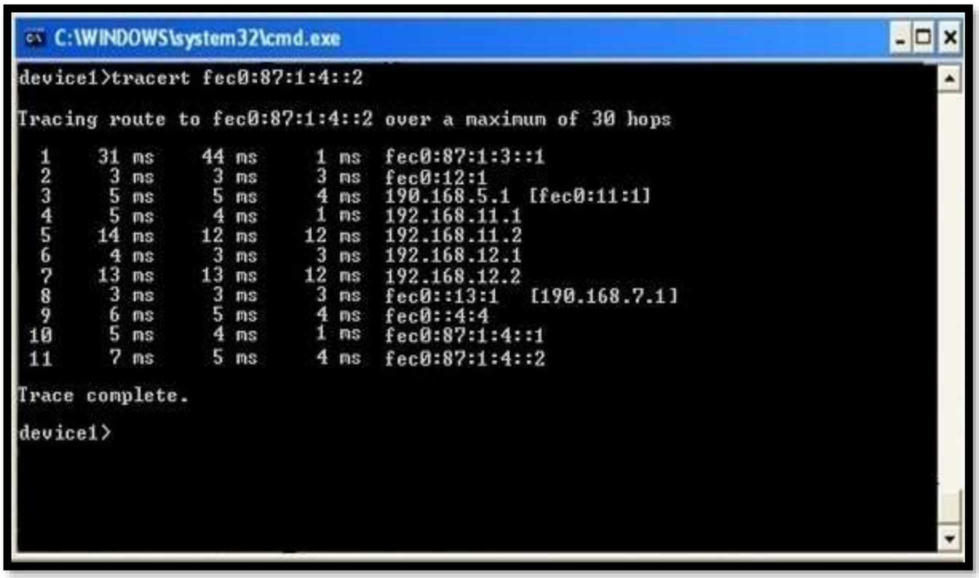


```
device1>Ping fec0:87:1:4::2

Pinging fec0:87:1:4::2...
Reply from fec0:87:1:4::2: time=69ms
Reply from fec0:87:1:4::2: time=69ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms

Ping statistics for fec0:87:1:4::2:
    Packets: Sent = 102, Received = 102, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 69ms, Average = 57ms
Control-C
```

Figure 4. Ping Test Result



```
device1>tracert fec0:87:1:4::2

Tracing route to fec0:87:1:4::2 over a maximum of 30 hops

  1    31 ms    44 ms     1 ms  fec0:87:1:3::1
  2     3 ms     3 ms     3 ms  fec0:12:1
  3     5 ms     5 ms     4 ms  190.168.5.1  [fec0:11:1]
  4     5 ms     4 ms     1 ms  192.168.11.1
  5    14 ms    12 ms    12 ms  192.168.11.2
  6     4 ms     3 ms     3 ms  192.168.12.1
  7    13 ms    13 ms    12 ms  192.168.12.2
  8     3 ms     3 ms     3 ms  fec0::13:1   [190.168.7.1]
  9     6 ms     5 ms     4 ms  fec0::4:4
 10     5 ms     4 ms     1 ms  fec0:87:1:4::1
 11     7 ms     5 ms     4 ms  fec0:87:1:4::2

Trace complete.

device1>
```

Figure 5. Trace rout Test Result

Table 7. Ping Test Result

Source Host 1	Destination Host 2
Packets Sent	102
Packets Received	102
Loss	0

Table 8. Latency Test Result

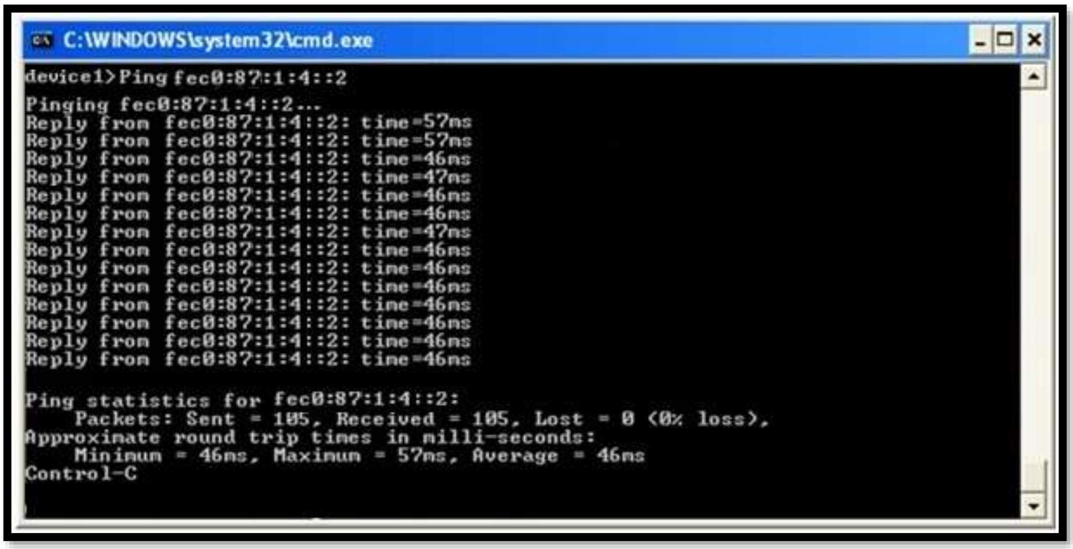
Level	Latency MS
Minimum	57
Maximum	69
Average	57

Here per a ping testing which in figure (4) we got the results in the table (7) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 102 packets and received 102 packets so there is no Packet loss, but for the latency can see from the table (8) the time of the mechanism the highest time is 69ms and the lowest time is 57ms then the average is 57ms.

3.1.2. Ping and trace route Testing for dual stack (Scenario 2)

Figure 6 and 7.below shows a ping and trace route test in scenario 2 between host1 to host 2 (FEC0:87:1:4::2) to determine the latency and the loss of packets made for more than 100 packages.

Here per a ping testing which in figure (6 and 7) we got the results in the table (9) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 105 packets and received 105 packets so there is no Packet loss, but for the latency can see from the table (10) the time of the mechanism the highest time is 57ms and the lowest time is 57ms then the average is 46ms.

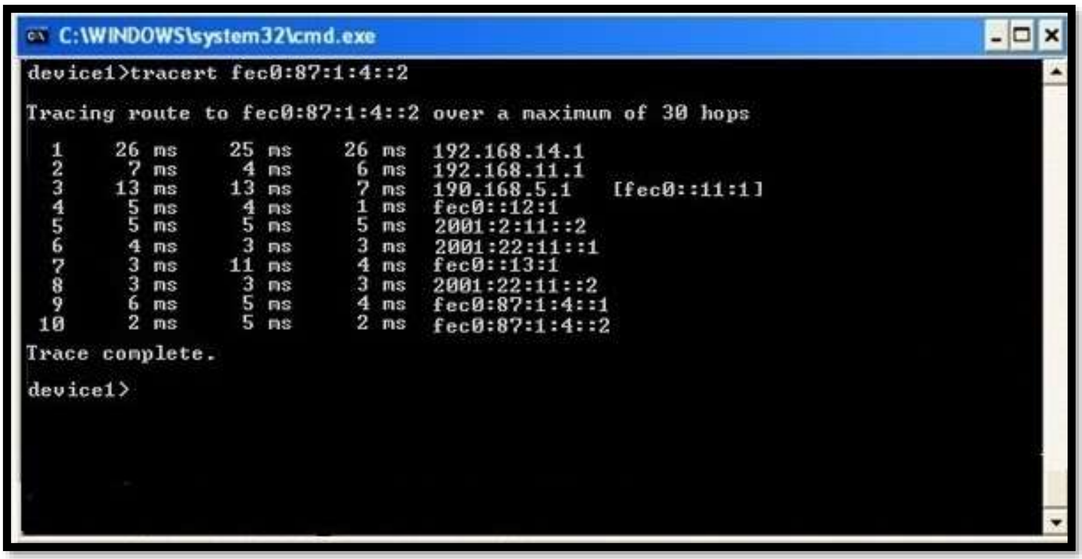


```
device1>Ping fec0:87:1:4::2

Pinging fec0:87:1:4::2...
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=57ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=47ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=47ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms
Reply from fec0:87:1:4::2: time=46ms

Ping statistics for fec0:87:1:4::2:
    Packets: Sent = 105, Received = 105, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 57ms, Average = 46ms
Control-C
```

Figure 6. Ping Test Result



```
device1>tracert fec0:87:1:4::2

Tracing route to fec0:87:1:4::2 over a maximum of 30 hops

  1    26 ms    25 ms    26 ms  192.168.14.1
  2     7 ms     4 ms     6 ms  192.168.11.1
  3    13 ms    13 ms     7 ms  190.168.5.1    [fec0::11:1]
  4     5 ms     4 ms     1 ms  fec0::12:1
  5     5 ms     5 ms     5 ms  2001:2:11::2
  6     4 ms     3 ms     3 ms  2001:22:11::1
  7     3 ms    11 ms     4 ms  fec0::13:1
  8     3 ms     3 ms     3 ms  2001:22:11::2
  9     6 ms     5 ms     4 ms  fec0:87:1:4::1
 10     2 ms     5 ms     2 ms  fec0:87:1:4::2
Trace complete.

device1>
```

Figure 7. Trace route Test Result

Table 9. Ping Test Result

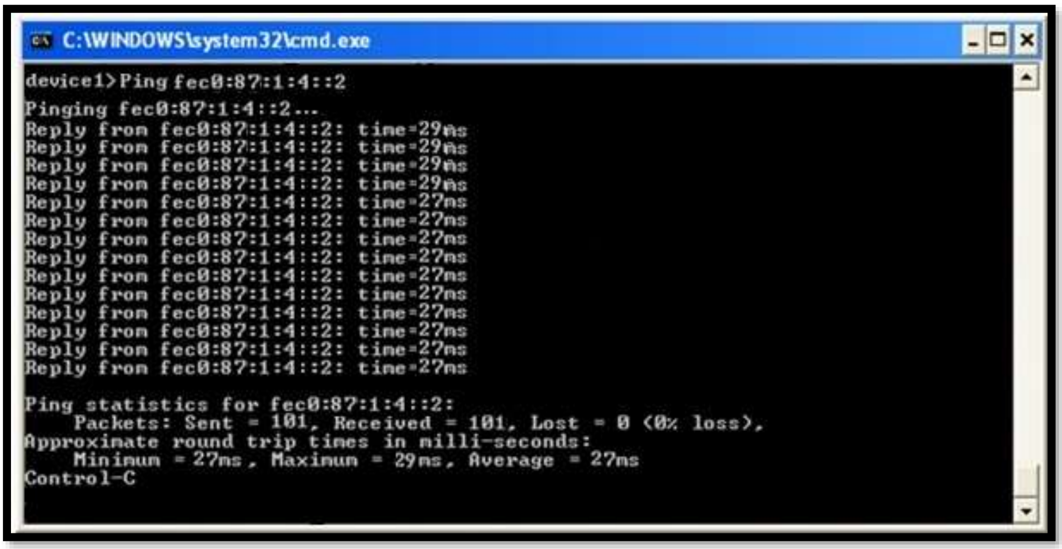
Source	Destination
Packets Sent	105
Packets Received	105
Loss	0

Table 10. Latency Result

Level	Latency MS
Minimum	46
Maximum	57
Average	46

3.1.3. Ping and trace route testingTranslation NAT-PT (Scenario 3)

Figure 8 and 9 below shows a ping and trace route test in scenario 3 between host1 to host 2 (IPv6:FEC0:87:1:4::2) to determine the latency and the loss of packets made for more than 100 packages.

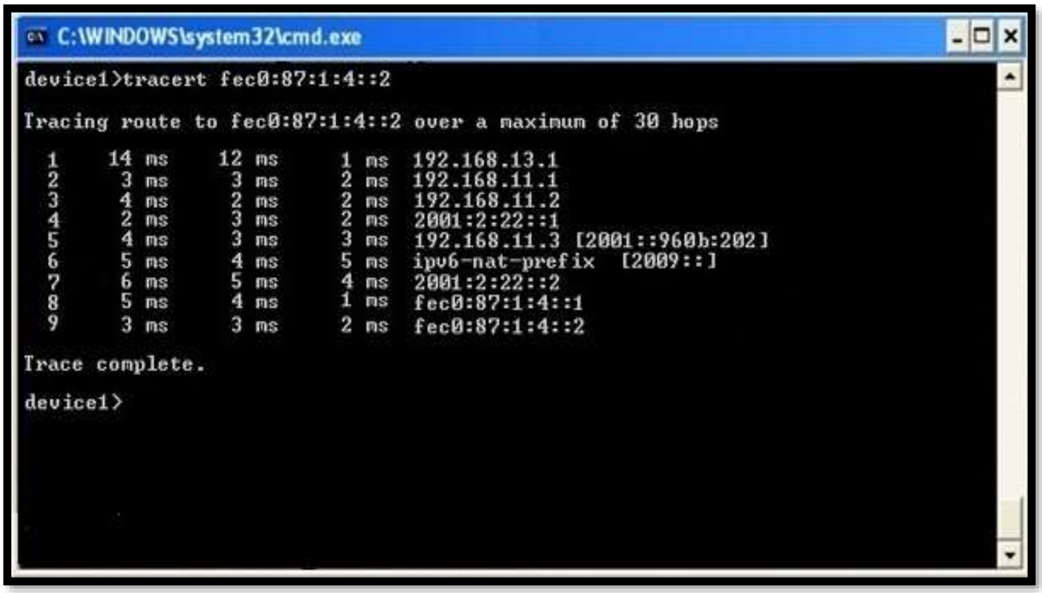


```
device1>Ping fec0:87:1:4::2

Pinging fec0:87:1:4::2...
Reply from fec0:87:1:4::2: time=29ms
Reply from fec0:87:1:4::2: time=29ms
Reply from fec0:87:1:4::2: time=29ms
Reply from fec0:87:1:4::2: time=29ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms
Reply from fec0:87:1:4::2: time=27ms

Ping statistics for fec0:87:1:4::2:
    Packets: Sent = 101, Received = 101, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms , Maximum = 29ms, Average = 27ms
Control-C
```

Figure 8. Ping Test Result



```
device1>tracert fec0:87:1:4::2

Tracing route to fec0:87:1:4::2 over a maximum of 30 hops

  1    14 ms    12 ms     1 ms  192.168.13.1
  2     3 ms     3 ms     2 ms  192.168.11.1
  3     4 ms     2 ms     2 ms  192.168.11.2
  4     2 ms     3 ms     2 ms  2001:2:22::1
  5     4 ms     3 ms     3 ms  192.168.11.3 [2001::960b:202]
  6     5 ms     4 ms     5 ms  ipv6-nat-prefix  [2009::]
  7     6 ms     5 ms     4 ms  2001:2:22::2
  8     5 ms     4 ms     1 ms  fec0:87:1:4::1
  9     3 ms     3 ms     2 ms  fec0:87:1:4::2

Trace complete.

device1>
```

Figure 9. Trace route Test Result

Table 11. Ping Test Result

Source Host 1	Destination Host2
Packets Sent	101
Packets Received	101
Loss	0

Table 12. Latency Result

Level	Latency MS
Minimum	27
Maximum	29
Average	27

Here per a ping testing which in figure (8) we got the results in the table (11) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 101 packets and received 101 packets so there is no Packet loss, but for the latency can see from the table (12) the time of the mechanism the highest time is 29ms and the lowest time is 27ms then the average is 27ms.

3.2. Jperf Results

3.2.1. Latency Analysis of the transition mechanisms

This test are performed on the behavior of the TCP latency in the all scenarios, Host2 as client, and Host1 as the server listening to the client and The client generates ICMP (TCP) traffic using the Jperf tool.

As can be seen from figure (10). the latency can be appear on using the packet size (500) Bytes the time of transfer can be achieved in (200) msec in Translation Mechanism (NAT-PT) , in dual stack can be seen that the time on the packet size (500) Bytes can be achieved (210) msec ,then the tunneling mechanism the time can be in (220) msec with same packet size bytes.

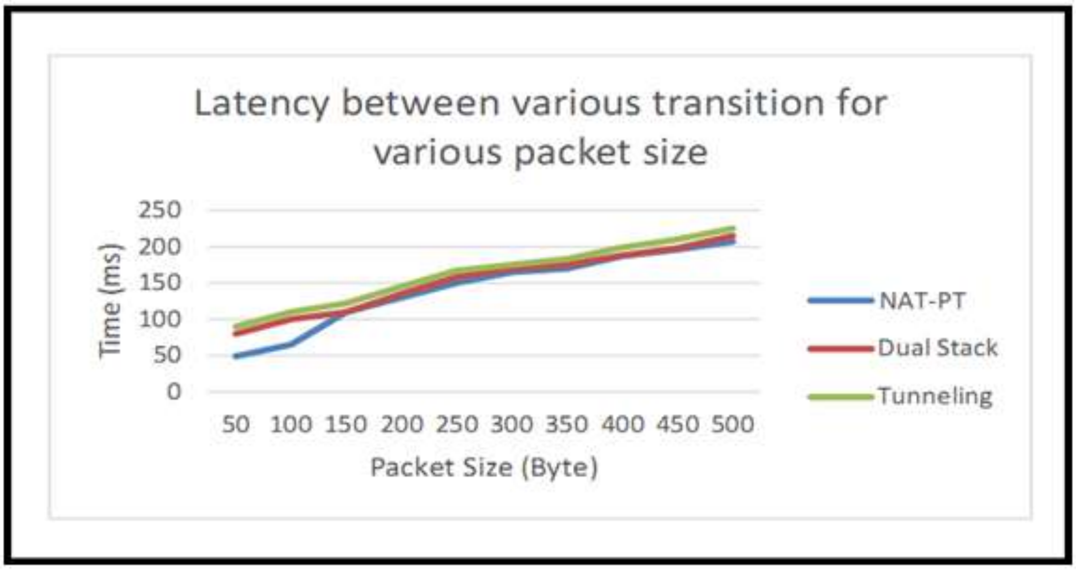


Figure 10. Latency Analysis of the transition mechanisms

3.2.2. Analysis of the Throughput

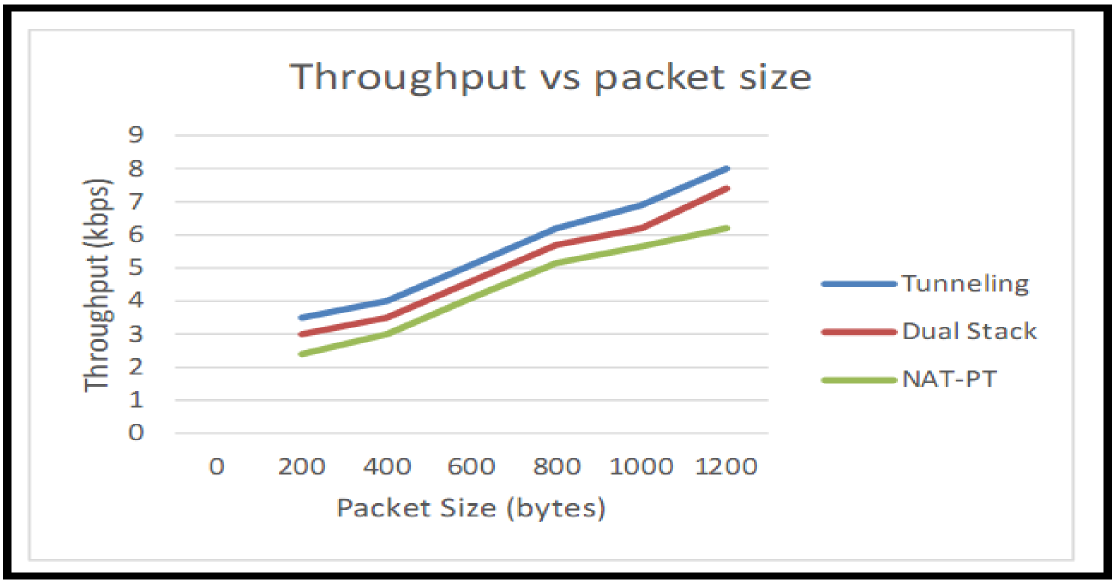


Figure 11. Analysisof the Throughput

This test are performed on the behavior of the TCP Throughput vs Packet size in the all scenarios, Host2 as client, and Host1 ICMP (TCP) traffic using the Jperf tool. As can be seen from figure (11). that on the packet size (1200) Bytes throughput can be achieved in Kbytes just under (7.2) Kbytes/sec in Translation Mechanism (NAT-PT) , in dual stack can be seen that the throughput increase is on packet size (1200) Bytes can be achieved (7.2) Kbytes/sec ,then the tunneling mechanism the throughput also seems to increase that can be seen on the same packet size (1200) Bytes throughput can be achieved in (6.1)Kbytes/sec.

3.2.3. Analysis of the Packet loss

This test are performed on the behavior of the TCP Packet loss in the all scenarios, Host2 as client, and Host1 as the server listening to the client and The client generates ICMP (TCP) traffic using the Jperf tool.

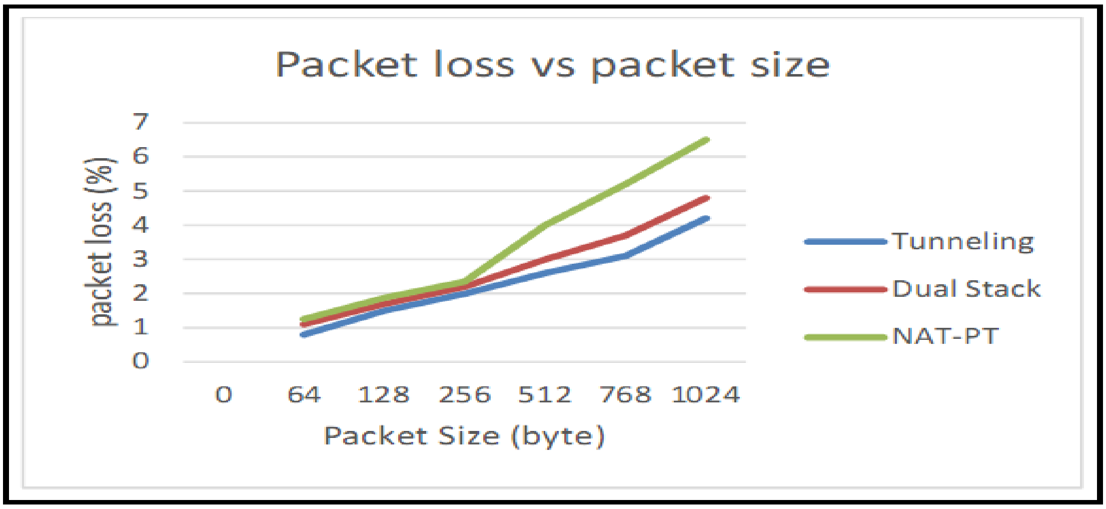


Figure 12. AnalysisofthePacketloss

As can be seen from figure (12). that on an average of the packet size (1024) Bytes the Packet loss can be in percentage (4.2%) in the tunneling mechanism , in dual stack can be seen that the Packet loss increase with packet size (1024) Bytes can be achieved (4.9%) ,then the Translation Mechanism (NAT-PT) the Packet loss seems to be a high increase that can be (6.5%) with same packet size.

The reason to be the Translation NAT-PT mechanism expertise highest proportion of Packet loss because of it is time overwhelming limit . On the obverse part the tunneling got all-time low Packet loss expertise.

From this Results, the throughput, latency and the Packet loss analyzing have done. After implementation the previous designs of the IPv6-IPv4 mechanisms performance , some packets have been transmitted from HOST-1 to HOST-2. In this test and analysis, ICMP packets (TCP) have been transmitted with diverse duration time and sizes. After monitoring the packet transitions, the results below has been found:

- as can seen in the Figures (10),(11), it found that the Translation NAT-PT provides the elevated latency, while the Dual stack performance mechanism provides the moderate mode ,and about the Tunneling mechanism easy to see that it is provides the lowest latency and the Translation NAT-PT mechanism provides the highest latency , the tunneling has the highest throughput , and from the figure (12) it's found the Translation NAT-PT mechanism had the highest Packet loss and the Tunneling Mechanism had the lowest Packet loss.

.

Table 13.Comparative analysis of three transition mechanisms.

Features	Dual Stack	Tunneling	NAT-PT
Latency	Moderate	less	faster
Throughput	Moderate	The Highest	Lowest
Packet Loss	Higher than tunneling	less	The Highest

From table (13) can be seen the result of Ping testing Jperf analyzing in all the mechanisms which using to connect between IPv4 to IPv6 per High or Less or Medium or

Moderate. As can be shown from the emulation, the results of throughput, latency and Packet loss, can be discovered that the NAT-PT mechanism provides highest latency, while Dual stack mechanism supplies the moderate and the Tunneling mechanism provides the most minimum latency, and the throughput with packet size appeared the that Tunneling provides the very best output rate than the opposite transition mechanism and also the NAT-PT technique provides very less as a result of its time beyond regulation intense for the header translation. it's to mentioned that, throughput, R= packet size (L)/ time consumed for transmission, and the Translation NAT-PT mechanism experiences highest percentages of Packet loss because of its time overwhelming limitation. On the opposite hand tunneling has all-time low Packet loss expertise.

3.3. Discussion

The progress from IPv4 to IPv6, IPv6 conquers a significant number of the impediments of IPv4 with new highlights. This has been intended to permit smooth progress with IPv4. The mix of CIDR and NAT components possesses diminished the hanging tight energy for the IPv4 address. Be that as it may, Network Address Translation (NAT) separates start to finish IP designs, so it has numerous impediments for the convention. A bigger IPv6 address space gives an increasingly remarkable worldwide unicast address for present and future Internet development. The full usage of IPv6 requires an expansion in the quantity of utilizations, hosts, switches, and DNS to help IPv6, which can be costly and take a long time to convey. In this circumstance, the change system is a standout amongst the best arrangements and thusly permits IPv6 and IPv4 systems to work on a similar framework.

IPv4 to IPv6 Several change components have been created dependent on the requirements of various associations. This examination physically analyzes and looks at Double Stack, interpretation and 6to4 components. These systems have their own points of interest and hindrances in various foundations. The double stack progress component is the most well-known and least demanding route for IPv6 and IPv4 hubs to speak with IPv6 and IPv4 hubs autonomously, without evolving systems. The double stack is appropriate for Internet specialist organizations, corporate systems, and home clients. Then again, the manual passage is arranged between two IPv6 systems by means of the IPv4 organize foundation. Manual passages are a protected system contrasted with other progress instruments. This component is appropriate for ISPs, corporate systems, server farms, yet not home clients. In light of the way toward changing from IPv4 to IPv6, While NAT-PT allows direct correspondence between IPv6-just systems and IPv4-just systems. dual stack systems (arranges that have IPv4 and IPv6) will have some IPv6-just has composed to require favorable position of the IPv6 auto design, world tending to, and less confounded administration alternatives, and these hosts will utilize NAT-PT to connect with existing IPv4-just systems inside a similar association ,there are a few preferences and hindrances of the three progress instruments, for example, dual stack , 6to4 manual tunneling and NAT-PT translation, The advantages and disadvantages of the double stack mechanism are:

The advantages and disadvantages of the Dual stack, 6to4 tunneling and Translation NAT-PT mechanisms are:

Advantages:

- Native Dual Stack does not require a tunneling mechanism on the internal network , IPv4 and IPv6 run independently of each other, And This mechanism is easy to use and can be implemented at both ends of the network node system.
- The manual tunneling simple and stable. And the Manual tunnels are safer than other tunneling mechanisms.
- NAT-PT is that no changes are required on existing hosts if NAT-PT is configured, because all NAT-PT configurations are made on a NAT-PT device. And the Static

IPv4 networks can provide an IPv6 network and use NAT-PT to connect between these networks without disrupting the network. For smooth transition, you can use FTP between IPv4 and IPv6 hosts.

Disadvantages:

- Both end routers must support multiple stack protocols, the Dual-stack nodes require more processor and memory resources because two separate protocol stacks are running on the same node , All tables are stored twice because of a stack protocol. And The routing protocols must deal with IPv4 and IPv6.
- Tunnels must manually configure the source and destination addresses of the tunnels , The Routers at both ends of the tunnel must support multiple stack protocols m the Communication may be possible between two peripheral nodes , and This type of tunnel is not very scalable, so it is only suitable for permanent connections.
- Because of the fast time NAT-PT transition mechanism it makes it experiences highest percentages of Packet loss.

4. Conclusion

Based on the discussion above, the conclusions can be drawn as follows:

3. the performances of these three mechanisms have been analyzed by GNS3 and JPerf in emulation system and got the results of the latency ,throughput and packet loss parameters for all the mechanisms as real time results , using the packet size 500 bytes to appear on the latency time of transfer which were (200) msec in translation mechanism (NAT-PT), (210) msec in dual stack, then (220) msec in tunneling mechanism. and using packet size 1200 Bytes to appear on the throughput which were (6.2) Kbytes/sec in Translation Mechanism (NAT-PT) , and the throughput increased in dual stack with (7.2) kbytes/sec ,then the tunneling mechanism the throughput also seems to increase with (8) Kbytes/sec., and by using packet size 1024 Bytes can be know how the Packet loss by percentage, the Packet loss in the tunneling mechanism (4.2%), in dual stack the Packet loss increased by (4.9%), then the Translation Mechanism (NAT-PT) the Packet loss got more increase by (6.5%) the reason of that high packet loss the time of the transition in Translation is so fast.
4. As can be shown from the emulation results of this research, the results of throughput, latency and Packet loss, can be discovered that the Translation NAT-PT mechanism had the fast latency ,the tunneling had the best throughput and less packet loss , and the dual stack keeps the moderating in all of the parameters .

References

[1] S. Deering, R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460. 2005.

[2] Raicu, I. and Zeadally, S., "Evaluating IPv4 to IPv6 transition mechanisms," in Telecommunications, ICT 2003. 10th International Conference on, vol.2, no., pp.1091-1098 vol.2, 23 Feb.-1 March 2003.

[3] Bi, J., Wu, J. and Leng, X. (2007). IPv4/IPv6 transition technologies and univer6 architecture, International Journal of Computer Science and Network Security, 7(1), pp.232—242.

[4] Wu, P., Cui, Y., Wu, J., Liu, J. and Metz, C., “Transition from IPv4 to IPv6: A state-of-the-art survey”, IEEE Communications Surveys & Tutorials, 15(3), pp.1407—1424, 2013.

[5] van Beijnum Comparison of IPv6 over IPv4 Tunnel Mechanisms draft-steffann-tunnels-03I. Institute IMDEA Networks April 11, 2013

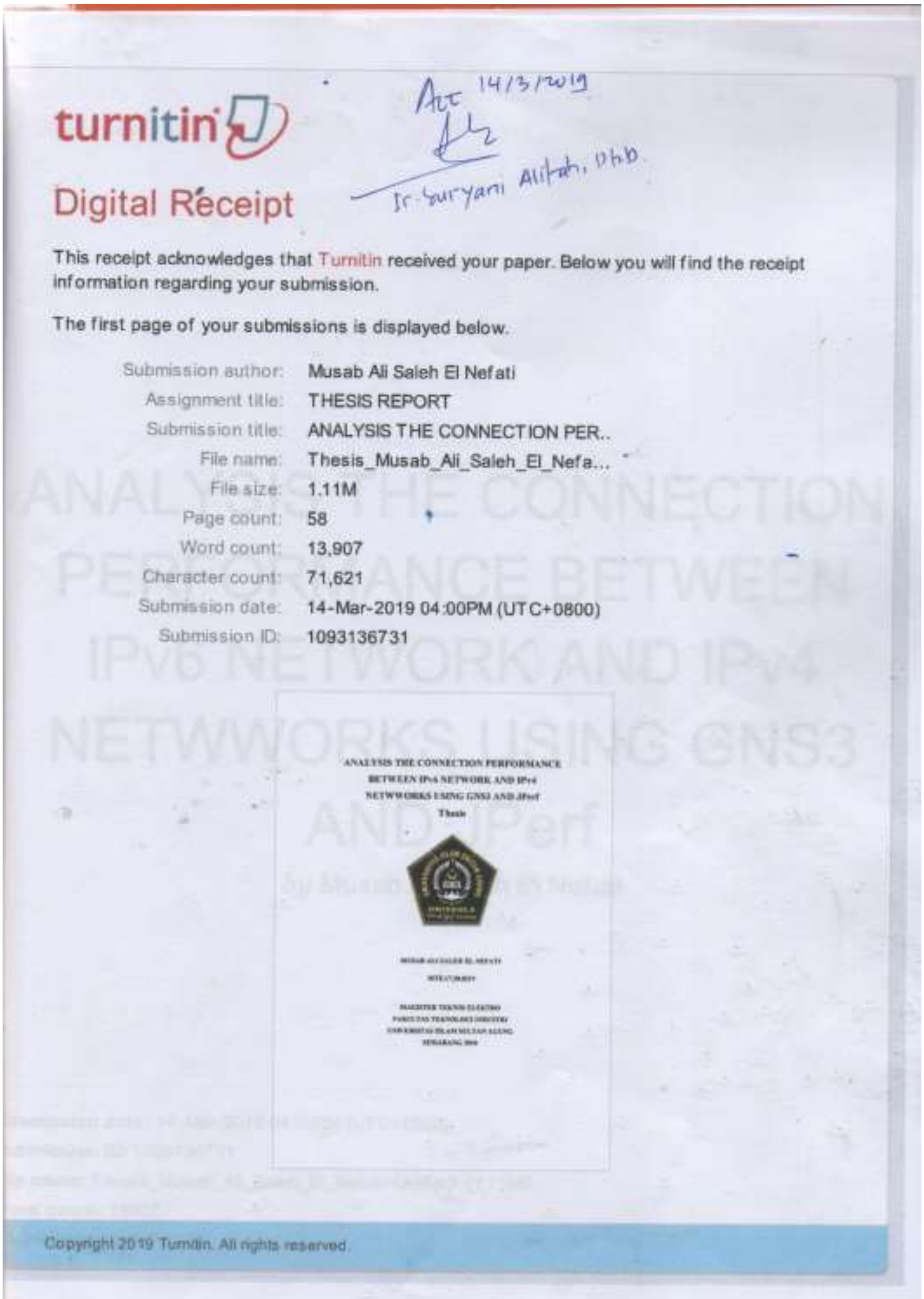
[6] E. Nordmark and R. Gilligan, “Basic transition mechanisms for IPv6 hosts and routers,” RFC 4213, Oct. 2005.

[7] R. E. Gilligan and E. Nordmark, “Transition mechanisms for IPv6 hosts and routers,” RFC 2893, Aug. 2000.

[8] Arafat, M., Ahmed, F. and Sobhan, M. (2014). On the Migration of a Large Scale Network from IPv4 to IPv6 Environment, International Journal of Computer Networks & Communications (IJCNC), 6(2), pp.111-126.

[9] Wu, P., Cui, Y., Wu, J., Liu, J. and Metz, C., “Transition from IPv4 to IPv6: A state-of-the-art survey”, IEEE Communications Surveys & Tutorials, 15(3), pp.1407—1424, 2013.

[10] Ahmad, N. and Yaacob, A. (2012). IPSec over Heterogeneous IPv4 and IPv6Networks: Issues and Implementation, International Journal of Computer Networks & Communications (IJCNC), 4(5), pp. 57-72.



turnitin

Acc 14/3/2019

Ir. Suryani Alifah, Ph.D.

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Musab Ali Saleh El Nefati
Assignment title:	THESIS REPORT
Submission title:	ANALYSIS THE CONNECTION PER..
File name:	Thesis_Musab_Ali_Saleh_El_Nefa...
File size:	1.11M
Page count:	58
Word count:	13,907
Character count:	71,621
Submission date:	14-Mar-2019 04:00PM (UTC+0800)
Submission ID:	1093136731

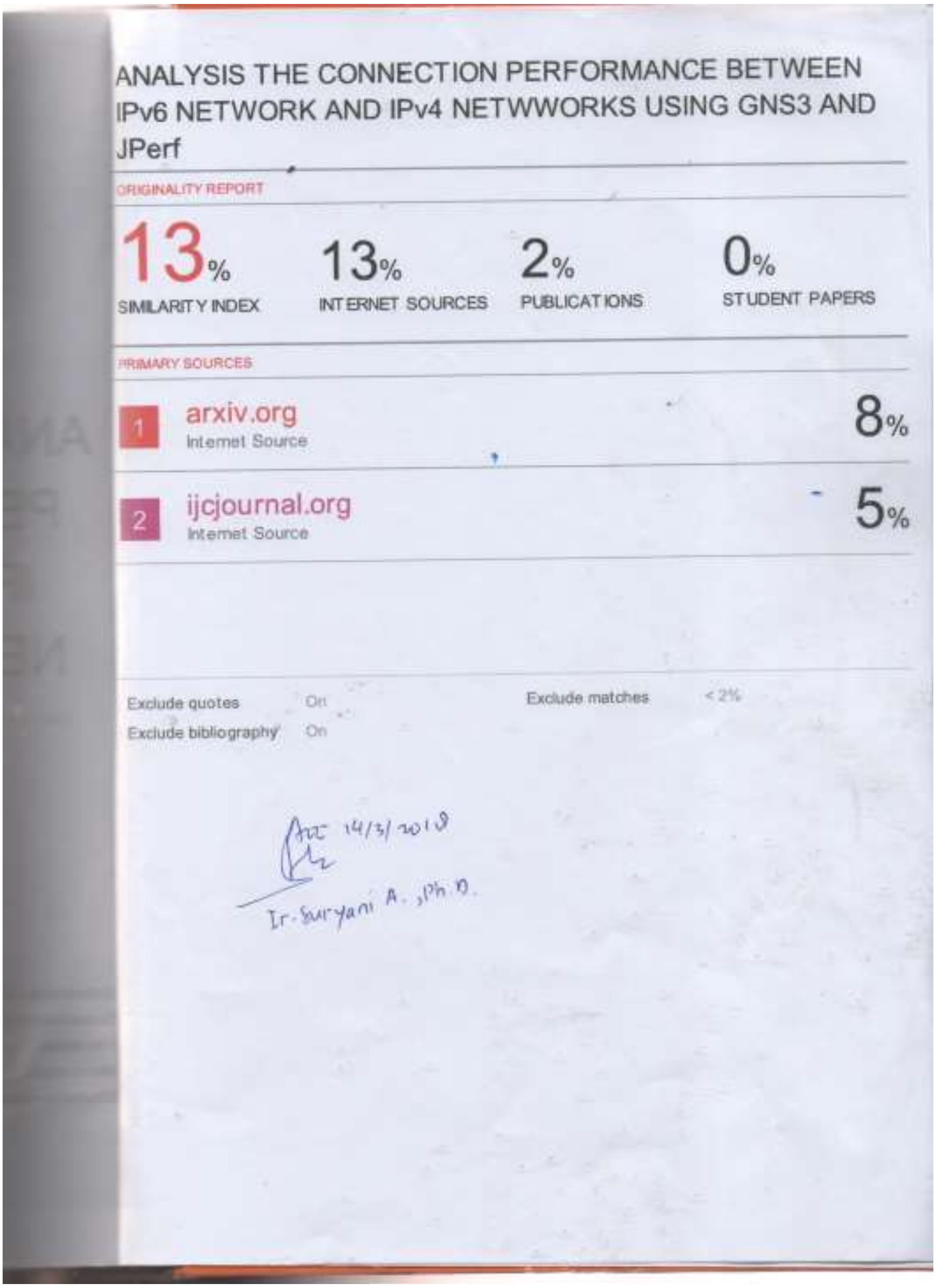
ANALYSIS THE CONNECTION PERFORMANCE BETWEEN IPv6 NETWORK AND IPv4 NETWWORKS USING GNS3 AND JPerf

Thesis

MUSAB ALI SALEH EL NEFATI

[illegible]

MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG [illegible]



ANALYSIS THE CONNECTION PERFORMANCE BETWEEN IPv6 NETWORK AND IPv4 NETWWORKS USING GNS3 AND JPerf

ORIGINALITY REPORT

13%	13%	2%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	arxiv.org Internet Source	8%
2	ijcjournal.org Internet Source	5%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		

Acc 14/3/2018

Ir. Suryani A., Ph.D.