EAST WEST UNIVERSITY

Thesis Title

Basic Study of IPv4 and IPv6

Supervisor:

Muhammad Suhail Najeeb

Lecturer

Department of Electronics and Communications Engineering

Submitted by:

Md. Sagir Ahmed Sarkar

ID : 2014-1-55-038

Asif Ishtiaqe Anik

ID: 2015-2-58-078

Date of Submission: 02-05-2020

Declaration

We hereby declare that the report submitted on ‘Basic Study of IPv4 and IPv6’ is based on the work done and results found by me. Any material of the work used by the group is mentioned along with the references. This report, neither in whole nor in part, has been previously submitted for any degree by anyone other group. This report is purely based on my work, findings and is being submitted to the Department of Electrical and Communications Engineering of East West University

Signature of Supervisor

Signature of Authors

.....

Name: Md. Sagir Ahmed Sarkar

ID: 2014-1-55-038

…….....

Name: Asif Ishtiaqe Anik

ID: 2015-2-58-078

……

Date of Submission: 02/05/2020

Acknowledgements

I would graciously want to acknowledge my supervisor Mr. Muhammad Suhail Najeeb for his guidance and kind advice in helping throughout the work and monitoring my work. He gave me various ideas and broadened my concept with the basics of Internet Protocols. Despite his busy schedule he has always managed to take out that time and guide me through. I am privileged enough to have been assisted and guided by him throughout the project.

Abstract

This paper aims at evaluating, compare and report result based on the performance of two protocol stacks (IPv4 and IPv6) in terms of various parameters that is analyzed when the data is being transmitted from one client to another or to a server over a wired network on IPv4 in comparison with the IPv6, thus proposing a system that compares both IPv4 and IPv6. The issue of the new-generation numbering system of the Internet Protocol version 6 (IPv6) is addressed as exhaustion of address space of the numbering system of Internet Protocol version 4 (IPv4) becomes a problem. IPv4/IPv6 transition unfolds a lot of problems relating to the internet world. This paper proposes some transition mechanisms involving different transition techniques. An explained study is performed on the addressing architecture.

However these techniques prove to be most efficient in the study which has been performed. This paper targets at a comparative study on the throughputs in bits/ seconds, packet throughputs, delay in networks, response time in seconds of both IPv4 and IPv6. Hence, since the system proposes for co-existence of both IPv4 and IPv6, the solution projected the comparison between the two.

Content

Chapter 1
Introduction

This research details on the study of Network Layer of the OSI. This involves the movement of packets from source to destination; to provide internetworking. The Network Layer is responsible for the delivery of individual packets from the source host to the destination host.
Reddy et al (2012) discussed about the Internet Protocol (IP) as the Network Layer of the TCP/IP protocol suite. IP architecture is designed to allow application layer protocols and mechanisms to evolve independently of the underlying network protocols and mechanism however the IP architecture has also been thoroughly field- proven regarding scalability through the use of IP over the public internet.

Geoff (2008) stated that, hidden from view of typical users, every Internet communication relies on an underlying system of numbers to identify data sources and destinations. Users typically specify online destinations by entering domain names (e.g. "congress.gov"). But the Internet's routers forward data according to numeric IP addresses (e.g. 140.147.249.9).
Sequel to the issues to be addressed in this study of IPv4 in comparison with IPv6 as it covers mainly the throughputs in bits/ seconds, packet throughputs, delay in networks, and response time in seconds, the researcher detects a means of providing reliable process to process communication delivery of packets data and error recovery. This will hence bring forth the reason for their co-existence either via Dual Stacking or Tunneling.
In dual-stack architecture, all the components of the network system should support the both protocols. Applications must choose either IPv4 or IPv6, by selecting the correct address based on the type of IP traffic and particular requirements of the communication. This is because they are fused together so their functionality is based on priority. Tunneling will explain a mechanism by which the existing IPv4 backbone can be used to carry IPv6 traffic and vice versa.
The tunneling protocol carries the tunneled protocol. Tunneling can be either IPv6 over IPv4 or IPv4 over IPv6 networks. In the transition period while the IPv6 infrastructure is being deployed, the existing IPv4 backbone over the network can be used to carry IPv6 packets. This is to say that IPv6 or IPv4 hosts and routers can tunnel IPv6 datagram over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Using this technique an IPv4 user can communicate with IPv6 network using the existing IPv4 network.
In this research study, the performance parameters like throughput, packet loss, etc were discussed. For both the protocols IPv4 and IPv6 networks were evaluated. Baseline IPv4 and
IPv6 network have been simulated using OMNeT++, which is a discrete event simulator. A comparative study of parameters was carried out in two different networks based on IPv4 and IPv6 respectively. For clarification of the comparison, screenshots of the simulation has been attached and detail of the scenario explanation [2].
As IPv6 is now the trendy Internet Protocol that has come to replace IPv4 based on the design and related statistical report. IPv6 is acknowledged to provide more address space, better address design, and greater security. IPv4 offers 32 bit address space and IPv6 offers 128 bit address

space. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. However, the two protocols are incompatible i.e. an IPv6 node cannot communicate directly with another IPV4 only node and vice versa. Different mechanisms for transition have been developed so that both the protocols may coexist.

Geoff Mulligan

Roughly 25 billion people are currently connected to internet computer networks worldwide via internet and these networks are connected via routers. Routers are tasked with sending data between the various networks. The router is called the internet protocol IPv4 along with an addressing scheme and transport protocol, which provides a direction of communication between

any pair of hosts. Some parts of the world are starting to run out of addresses because of the lack of address space and allocation mechanism i.e. used to allocate addresses in the internet protocol. A new version of the internet protocol called IPv6 has been developed to solve the address and other issues in the Internet protocol currently in use. To stationary users, the only Internet connection accessible to mobile customers through cellular phone networks operating on IPv6, IPv4 network is also currently suitable. Implementing the switch and interoperation between IPv4 and IPv6 demands a simple method for smooth IPv6 rollout, because Mobile IP cannot offer IPv4 mobility from the IPv6 access network. It needs massive needless investment in IPv6 technology to achieve this. We still cannot switch straight from IPv4 to IPv6 and we need to establish a framework such that IPv4 and IPv6 remain together for at least 20 years and IPv4 network can fully vanish during the transition period [2] .this paper deals with advantages, disadvantages, comparison, constraints and various transitions mechanisms from IPv4 to IPv6.

The purpose of differentiated services is to provide a framework and building blocks to enable the deployment of scalable discrimination on the Internet. The differentiated service approach aims to speed up deployment by separating the architecture into two main components, one of which is fairly well understood and the other of which is just beginning to be understood. Through this, we are directed by the initial Internet architecture, where it was agreed to distinguish the forwarding and routing elements. Packet forwarding is the fairly straightforward process which must be carried out as easily as possible on a per-packet basis. Forwarding uses the packet header to locate an entry in a routing table which specifies the output interface for the packet. Routing sets the entries in that table and will need to represent a variety of transportation and other strategies, as well as keep track of faults on routes. To the forwarding task, routing tables are maintained as background process. Additionally, routing is the most complex activity and it has developed over the last 20 years.

Analogously, there are two main components in the differentiated architecture of the services. One is the fairly well-understood behavior in the forwarding path and the other is the more complex and still emerging component of background policy and allocation that configures parameters used in the forwarding path. The activities of the forwarding route include the differential treatment which an individual packet gets, as applied by disciplines of queue operation and/or queue management. These per-hop behaviors are useful and necessary for delivering differentiated packet treatment in network nodes, no matter how we build end-to-end or intra-domain services. Our focus is on general behavioral semantics rather than the specific mechanisms used to implement them, as these behaviors will evolve less quickly than the mechanisms.

Per-hop activities and processes for choosing them per-packet can be implemented in network nodes today and it is this dimension of the separated architecture of networks that is discussed first. Furthermore, the forwarding path may require any control, policing and shaping of the network traffic allocated for "special" care to fulfill the criteria associated with the provision of the special treatment. Mechanisms are also fairly well understood for this kind of traffic

conditioning. The wide deployment of such traffic conditioners is also important to enable services to be constructed, although their actual use in service construction may evolve over time.

Much less well understood is the configuration of network elements regarding which packets are given special treatment and what kinds of rules are to be applied to resource use. Nonetheless, using simple policies and static configurations it is possible to deploy useful differentiated services in networks. There are a variety of methods, as defined in [ARCH], of writing per-hop behaviors and traffic conditioners to build services. Additional expertise is gained in the process which will drive more complex allocations and policies. The basic behaviors in the forwarding path may stay the same while this architectural component evolves. Experiences of constructing these facilities will persist for some time, but we will not standardize this development because it is premature. Furthermore, many of the aspects of service development are protected by legal arrangements involving multiple business organizations and this is excluded because it is beyond the control of the IETF [3].

Chapter 2

Background

In 1991, the IETF announced that its architecture had outlived the existing version of IP, dubbed IPv4. The new version of the IP, either named IPng (Next Generation) or IPv6 (version 6), was the culmination of a long and turbulent cycle that came to a head in 1994, when the IETF gave IPv6 a straight path. IPv6 is conceived to solve IPv4 problems.

This does so by developing a new protocol version that serves the IPv4 purpose but without the same IPv4 limitations. IPv6 isn't completely different from IPv4: everything you learned in IPv4 would be useful when you implement IPv6. The differences between IPv6 and IPv4 are in five key areas: addressing and routing, protection, network address translation, administrative workload and mobile device support. IPv6 also includes one significant feature: a compilation of potential IPv4 migration and transfer plans. Nevertheless, the IETF is not so crazy as to believe that anything will change overnight. Thus there are also specifications and protocols and procedures for the coexistence of IPv4 and IPv6: IPv6 tunneling in IPv4, IPv4 tunneling in IPv6, IPv4 and IPv6 running on the same device (dual stack) for an extended period of time, and mixing and matching the two protocols in a number of environments [4].

There have been more than 30 IPv6 RFCs published since 1994. Changing IP means changing dozens of Internet protocols and conventions, ranging from how IP addresses are stored in DNS (domain name system) and applications, to how datagrams are sent and routed over Ethernet, PPP, Token Ring, FDDI, and any other medium, to how the call network programmers work.

Currently IPv6 penetration is still low and the IPv4 is going to run out of addressing space, while in the other hand, a study of IPv6 Internet traffic from June 2007 to June 2008 shown that IPv6 penetration is stagnant compared to overall Internet traffic. Several reasons that can lead this situation to happen are high cost of migration, no added revenue, no users, no IPv6 content and lack of IPv6 awareness. So from the comparative review of IPv4 and IPv6 that we carried out in this paper, we expect that IPv6 advantages and support product that we have point out can increase IPv6 awareness to the readers. This paper will also be the starting point of the next research test bed that we going to carry out along with case study between University students.

The projection of impending depletion of IPv4 address space led network engineers to implementIPv6 address system. It is assumed that the IPv6 header has been streamlined for efficiency. The format introduces the concept of an extension header, allowing greater flexibility to support optional features. It was reported in this paper that all networking equipment’s and the new devices like mobile handsets, tablets etc are provided with IPv6 support i.e. it allows dual

stack architecture. The backbone network is largely based on IPv4; all routing tables are based on IPv4 entries [5].

Report analysis shows that MPLS enabled networks were having less queuing delay as compared to traditional networks. Thus it is discussed and explained by the fact that in MPLS, only the label is checked and the underlying IP header is not used or forwarding and routing decisions. IPv6 MPL shows more queuing delay than IPv4 regarding the fact that the packet header is larger in IPv6 than IPv4. The addition of the MPLS header increases the packet size even more. The maximum queuing delay in all the cases was for IPv6 [6].

Rey (1991), stated that the design of the TCP/IP architecture brought about the flexibility which enabled the internet grow in vast host of over a billion supporting series of services over a variety of media. The TCP/IP architecture at first aimed to provide undisrupted internet communication despite the loss of networks or gateways, IPv4 is the most common protocol.

Chapter 3

Limitations of Ipv4

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) and is the first largely deployed version of the protocol. It is at the core of Internet standards-based internetworking methods, along with IPv6. IPv4 is still the Internet Layer protocol with the greatest deployment. It uses a 32 bit address and permits 4,294,967,296 separate addresses [7].

Although the name appears to imply that this is the fourth iteration of the key Internet Protocol, the first version of IP that has been widely used in modern TCP / IP. IPv4, as it is often named to distinguish it from the older IPv6, is the Internet Protocol variant in use today on the Internet, and the protocol is being implemented on hundreds of millions of computers. It offers the essential datagram distribution functionality all of TCP / IP operates on, and has proved its quality of use for more than two decades.

Figure 1 shows a typical IPv4 Internet edge network.

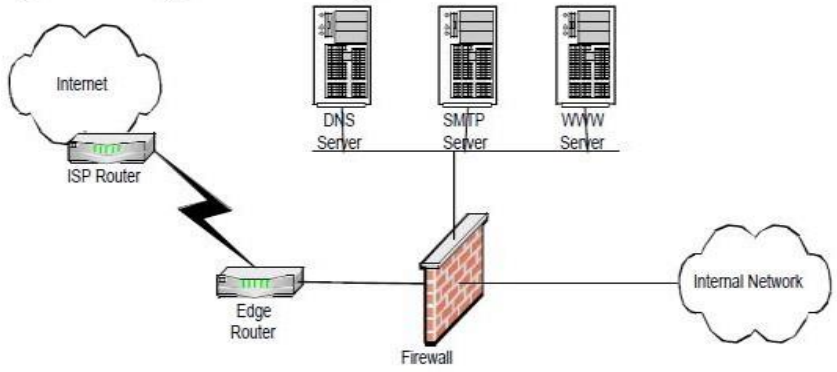


Figure 1 Typical IPv4 Internet Edge Network

It has been evident since the 1980s that the number of IPv4 addresses available is being exhausted at a rate not initially anticipated in network design. This was the driving factor in establishing classy networks, in creating CIDR addressing. But despite these measures the IPV4 addresses are being consumed at an alarming rate and it is estimated that 2010 will be the last year for IPV4, some sources say they may last until 2012. The primary reason for IPV4 exhaustion is enormous growth in the number of internet users, mobile devices that use Internet connection and always on devices such as ADSL modems and cable modems. This takes us to creating and accepting IPV6 as an alternative solution.

A. Addresses exhaustion

IPv4's first limit lies in the depletion of public IPv4 emails. Developing such mobile and home services will lead to faster IPv4 address consumption, even if ISPs allocate only one static public IP address to each home network. Based on digital subscriber line (DSL) or 3 G accesses, customers will increasingly use permanent connections. Meanwhile, dynamic addressing is not a feasible approach for such customers who expect the two-way symmetric connectivity to the Internet. For reality, the network would require loads of public IP addresses for all IP devices in the mobile and home networks to be addressable from outside.

B. Private addressing and translation

One solution for saving public addresses is to use private intranet addresses [8]. A home network uses a special reserved set of IPv4 addresses to communicate over the local network between devices. This allows internal communications to be established easily, but any external access requires the use of IP translation. In some cases, it uses mechanisms for Network Address Translation. It's because private addresses on public IP networks cannot be redirected to. It represents a drawback for home networking because end-to - end networks are difficult to configure. Another disadvantage of using private address and translation is that it can slow the performance of network access especially when there is a lot of private IP need to be translated.

C. IP configuration

Most current IPv4 implementations must be either manually configured or use a stateful address configuration protocol such as Dynamic Host Configuration Protocol (DHCP). With the drastic increase in IP devices, a simpler and more automated configuration of addresses and other configuration settings that do not depend on the management of a DHCP infrastructure is needed.

D. Low security level

Private communication over a public medium such as the Internet includes cryptographic services that protect the transmitted data from being sniffed, accessed or changed in transit. While IPv4 security standard such as Internet Protocol Security (IPSec) does exist, this standard is optional for IPv4. Some of them are proprietary and allow users to use the protection service on the client's site to pay more money for license fees.

E. Limited QoS support

Real-time traffic support is based on the 8 bits of the historic IPv4 Service Type (TOS) field and payload identifier. Unfortunately, the functionality of the IPv4 TOS field is limited. It has been redefined over time, and has various interpretations.

F. Large routing table

Demand for IPv4 address and Internet access continues to grow significantly [8], causing the Internet's routing tables also to increase at high rates. This is due to the way IPv4 network was allocated which combines flat and hierarchical routing information. The need to document routes to large numbers of devices using limited storage space represents a major challenge in the construction of routing table. Illustration. This figure Shows the current growth of the table for the Border Gateway Protocol.

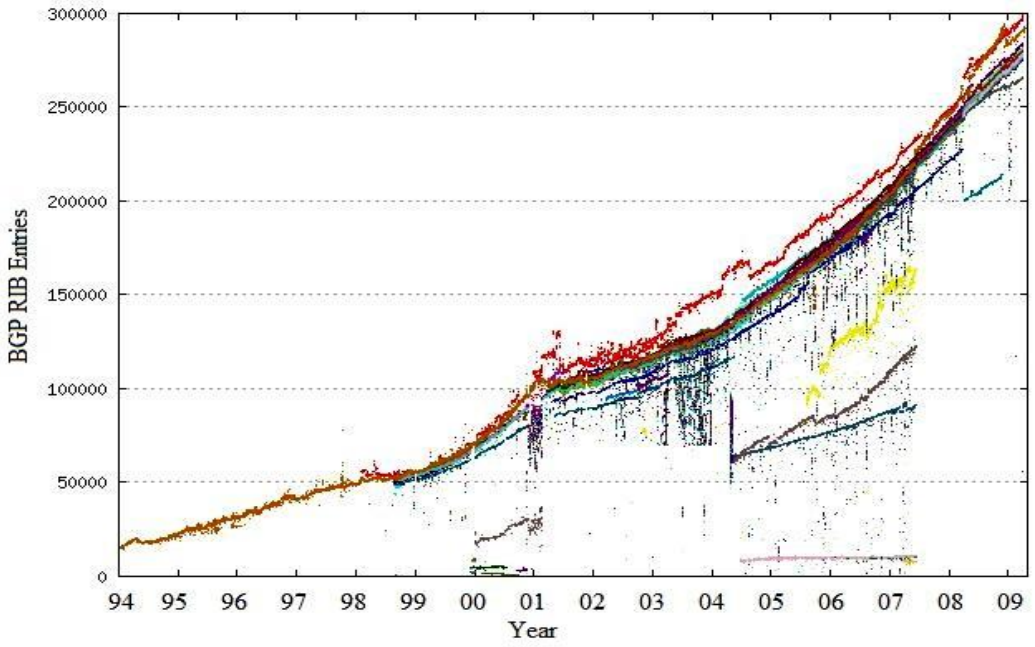


Fig. Growth of the Border Gateway Protocol (BGP) from 1994 to 2009

IPv4 has been updated through the years to tackle new challenges. Even with changes, however, IPv4 still has three major problems [9]:

Depletion of IP addresses-IPv4 has a limited number of unique public IP addresses. While there are around 4 billion IPv4 addresses, the increasing number of new IP-enabled devices, always-on

connections and the potential growth of less-developed regions have increased the need for more addresses.

Expansion of the Internet routing Table-Routers use a routing table to allow best path determinations. When the number of servers (nodes) connected to the Internet increases, so does the number of routes in the network. On Internet routers these IPv4 routes use a lot of memory and processor power.

Lack End-to-End Connectivity-Network Address Translation (NAT) is a technology commonly implemented in IPv4 networks. NAT allows for the use of a single public IP address by multiple users. However, the IP address of an internal network host is secret since the public IP address is shared. It can pose problems for technologies requiring end-to - end connectivity.

Chapter 4

Ipv6 Advantages

With such an enormous address space, ISPs will have enough IP addresses to allocate enough addresses to each customer so that each IP device has a unique address – be it behind a firewall or not. NAT (network address translation) became a very common technique for dealing with IP address shortages. Unfortunately, for many Internet applications, NAT does not function very well, ranging from old reliable applications like NFS and DNS to newer applications like community conferencing.

NAT has also been an obstacle to business-to - business direct network connections, requiring baroque and complicated address translators to make it work effectively, scaling poorly, and providing a single point of failure which is highly vulnerable [10].

One of the aims of IPv6 's expansion of address space is to make NAT unnecessary, improving total connectivity, reliability and flexibility. IPv6 is expected to restore openness and end-to - end Internet traffic. The new IPv6 addresses are wide and difficult to manage, so IPv6 limits the number of people reading and writing them.

A second major objective of IPv6 is to reduce the total amount of time that people have to spend configuring and managing systems. An IPv6 system can participate in "stateless" auto configuration, where it creates a unique, guaranteed IP address by combining its LAN MAC address with a network router prefix – DHCP is not required.

Of course, DHCP is still useful for other parameters, such as DNS servers, and is supported as DHCPv6 where needed. IPv6 also provides a middle ground between the two extremes with protocols such as SLP (the "Service Location Protocol"), which can make network managers' lives easier. The fourth big IPv6 target is based on high-bandwidth multimedia and fault tolerance applications. Multimedia systems may take advantage of multicast: a single datagram is transmitted to multiple receivers.

Though IPv4 has some multicast capabilities, these are optional, and they are not supported by every router and host. Multicast is a requisite with IPv6. IPv6 also defines a new type of service, called anycast. As with multicast, anycast has node groups that send and receive packets. But when a packet is sent in IPv6 to anycast group it is delivered only to one of the group's members. For a fault-tolerant environment this new functionality is particularly appropriate: Web servers and DNS servers will all benefit from anycast technology from IPv6.

QoS (Quality of Service) is another aspect of VPNs built into IPv6. IPv6 supports the same QoS functions as IPv4, including the DiffServ indication, as well as a new traffic flow field of 20 bits. Although this part of IPv6 is not specified for use, it is given as a solid basis for building QoS protocols. IPv6 's fifth major goal is VPNs, the private virtual networks. Add-ons to IPv4 are the latest security protocols IPSec, ESP (encapsulating security protocol) and AH (authentication header). IPv6 builds in and allows these protocols which will make it easier to develop and deploy stable networks in an IPv6 environment [4].

A. Large address space

IPv6's principal advantage over IPv4 is address space. It was designed to support +340 undecillion (2128) IP addresses, compared to IPv4 addresses of 4.3 billion (232). If we estimate that everyone in this world (6.77 billion) will need 3 IP addresses per person, then we can estimate the total IP addresses required for all people worldwide, which is 6.77 billion x 3 = 20.31 billion IP addresses. If we assume this number (people) is using IPv6, we still have extra IP addresses of +340 undecillion (+340 undecillion – 20.31 billion). This is the main reason why we should migrate to IPv6 instead of keeping the IPv4 exhausted.

B. Better security

The IPv6 specification requires nodes allowed by IPv6 to support the IP Security Protocol (IPSec), hence IPv6nodes that are more protected than IPv4 nodes. It also includes security features in its specifications, such as payload encryption and authentication of the source of the communication.

C. Enhance QoS support

IPv6 includes "labeled flows" in its specifications to provide better support for real-time traffic (e.g., voice over IP). This mechanism helps routers to identify the end-to - end flow to which the transmitted packets belong. This is similar to the Multi-Protocol Label Switching (MPLS) service but is built-in with the IP system rather than an add-on.

D. Auto configuration

IPv6 includes a plug-and - play mechanism which makes it easier to connect equipment to the network. The configuration which is required is automatic. This feature is called stateless auto configuration, which will speed up network connection particularly in IPv6 networks of large scale. It is because the network administrator did not have to manually configure the entire network device. Router must include the prefix from router advertising in stateless system.

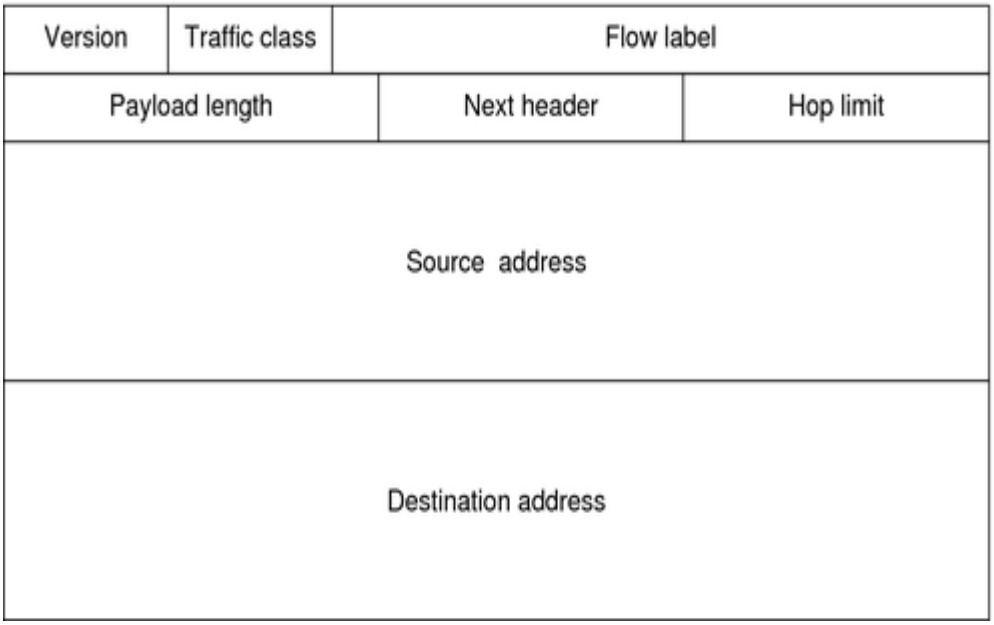
Although Dynamic Host Configuration Protocol (DHCP) server must provide the address in stateful process, there is no need for router advertising and DHCP server to allocate the address to connect local address auto configuration.

E. Enhance mobility support

IPv6 was designed with usability in mind, and is not a feature add-on. Mobile IPv6's purpose is to allow a mobile node to switch from link to link while maintaining the same IPv6 address as its home. IPv6 Neibours Discovery and auto configuration allows mobile node connectivity in a transparent manner, regardless of where the node is connected to the network without any special device needs.

F. Optimized protocol

IPv6 embodies best practices for IPv4 but excludes unused or redundant IPv4 functionality. This leads to the optimisation of the Internet Protocol. It also improves hierarchy in addressing and routing. IPv6 was designed to be extensible and offers new options and extensions to support it. [11]



Packet format of IPv6

In honor of World IPv6 Day, here are more good reasons to make sure your hardware, software, and services support IPv6 [12]-

More Efficient Routing-IPv6 reduces the size of routing tables, making it more efficient and hierarchical to route. IPv6 enables ISPs to aggregate their customer network prefixes into a single prefix, and to announce this one prefix to the IPv6 Internet. Furthermore, fragmentation is handled in IPv6 networks by the source device, rather than the router, using a protocol to discover the maximum transmission unit (MTU) of the path.

More Efficient packet handling-The simplified packet header IPv6 makes processing of packets more efficient. Compared to IPv4, IPv6 does not contain an IP-level checksum, so there is no need to recalculate the checksum at each router hop. It was possible to get rid of the checksum at the IP level because most connection layer technologies already contain checksum and error-control capabilities. Furthermore, most transport layers, which handle end-to - end connectivity, have a checksum allowing error detection.

Directed data flows-IPv6 supports multicast, instead of broadcasting. Multicast allows for the simultaneous sending of bandwidth-intensive packet flows (such as multimedia streams) to multiple destinations, saving network bandwidth. Disinterested hosts must no longer process packets for broadcast. Furthermore, the IPv6 header has a new field, named Flow Label, which can identify packets that belong to the same flow.

Simplified Network Configuration-Auto-configuration of the address (address assignment) is installed on IPv6. In their router advertisements a router will send the local link prefix. By inserting its link-layer (MAC) address, converted to Extended Universal Identifier (EUI) 64-bit format, a host may generate its own IP address.

Security-In IPv6, IPSec provides confidentiality, authentication and data integrity. IPv4 ICMP packets are frequently blocked by corporate firewalls because of their ability to carry malware, but ICMPv6, the implementation of the Internet Control Message Protocol for IPv6, may be enabled because IPSec can be applied to the ICMPv6 packets.

support for New Services-By eliminating Network Address Translation (NAT), true end-to - end connectivity is restored at the IP layer allowing new and valuable services to be provided. Peer-to - peer networks are easier to create and maintain, and the robustness of services such as VoIP and Quality of Service (QoS).

Chapter 5

Comparison

REASON FOR THIS COMPARATIVE STUDY [11]-

IPv6 penetration is still small at present, and IPv4 is an analysis of IPv6 Internet traffic from June 2007 to June 2008, on the other hand, showed that IPv6 penetration is stable relative to overall Internet traffic [13]. High migration costs, no added revenue, no users, no IPv6 content and lack of IPv6 awareness are several reasons that can lead to this situation happening. Thus, from the comparative review of IPv4 and IPv6 we conducted in this paper, we expect that the IPv6 benefits and the support of the product we point out can increase the readers' awareness of IPv6. Thus, from the IPv4 and IPv6 comparative review we conducted in this paper, we expect that the IPv6 advantages and the support of the product we have pointed out can increase the readers' awareness of IPv6. To plan, understand and design the migration from IPv4 to IPv6, we have to correctly determine the compromising of the network component element's test bed architecture as shown in Fig. 2-A, 2-B.

By Fig. 2-A End to End IPv4 and IPv6 performance is calculated using Basic Network Management Protocol (SNMP) network monitoring tools. In the investigation test bed and case study, measurements such as real bandwidth, delay jitter, and packet loss will be obtained and analyzed. This paper is important, as it will lead us to identify the appropriate IPv6 support product for our next study. It will also have an impact on IPv6 performance readers or users, and ultimately increase IPv6 penetration.

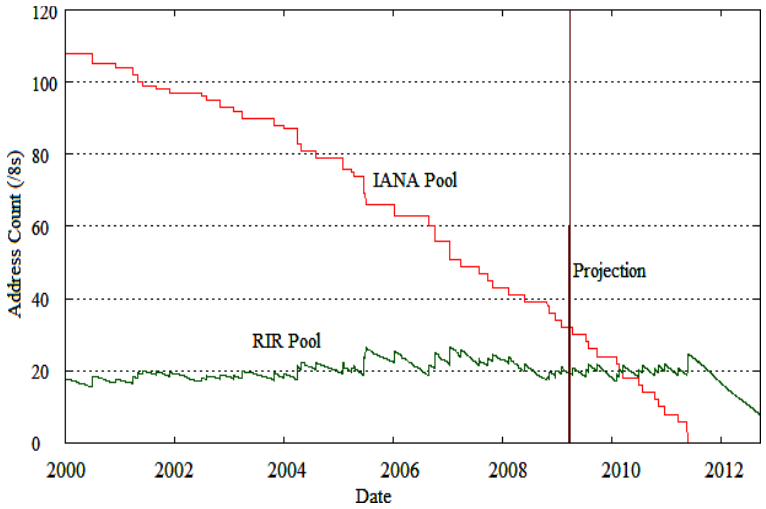


Fig. 1 Projection of IPv4 pool exhaustion in Internet Assigned Numbers Authority (IANA) and regional Internet registry (RIR) [8]

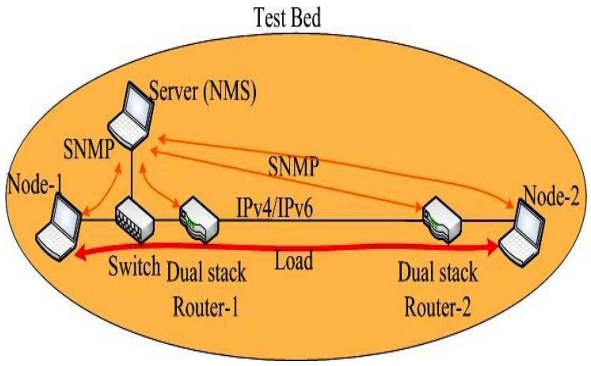


Fig. 2-A Dual stack network test bed

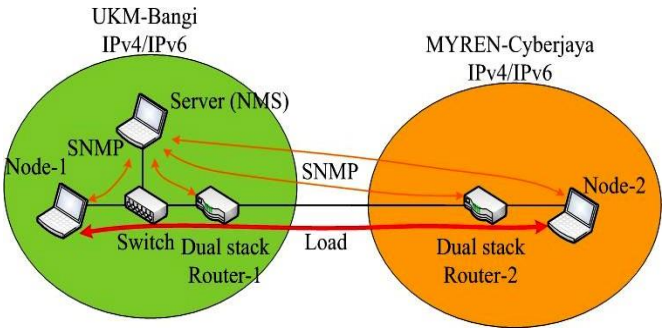


Fig. 2-B Dual stack network case study

In this paper, we assess the comparison between IPv4 and IPv6 using OPNET SIMULATOR [14] . The great expansion of the internet, these days, creates more significant challenges. Not only addressing modern hosts such as pcs, smartphones, laptops, mobile phones but electronics as well. Requires that its overall architecture evolve to accommodate the emerging technologies that meet the demand for use (by users, applications, or services).

The Internet Protocol Version 6 (IPv6) [15] is designed to meet these requirements and allow a global environment where the network's rules for addressing applications are again transparent. IPv6 dynamically makes major changes to network topologies (exp. peer-to-peer, client / server,

or mesh networks). It also enhances most network functions, especially in the areas of security, mobility, auto setup, quality of service (QOS) and multicasting [16].

IPv6 is proposed to have a bigger address space and better efficiency on the Internet [17] .Consequently, Substantial progress in the communications revolution is asking us to commit all devices to be in constant contact, consistent and high quality and to take the piece into account. We have two types of networks in this paper which are planned for IPv4 and IPv6. In an effort to understand the contrast of both Protocols in a simulated OPNET environment [18].

NETWORK ARCHITECTURE OF IPV4 AND IPV6 IN OPNET-

Using the OPNET simulation tool the editor designed an IPv4 and IPv6.Take a set of parameters that define the work 's features, and the variations between each protocol 's performances. To illustrate the fundamental differences between IPv4 and IPv6 network protocols, all attached to the results have been developing networks and evaluating various parameter aspects (delay, latency, response time and jitter), showing the attributes of these protocols have emerged.

We have used OPNET software to simulates IPv4 and IPv6, and to measure the performance of the network using each protocols according to four parameters (dela, ,jitte,, utilization and throughput. . The objective of this simulation to compare between IPv4 and IPv6 by using two scenarios of WAN network Containing two local networks (LAN each containing 14 Ethernet _weakest and 1 Ethernet _server. Each local network, is linked by a router, and the two routers are linked 2 by ppp-sd3 show figure (3,4)

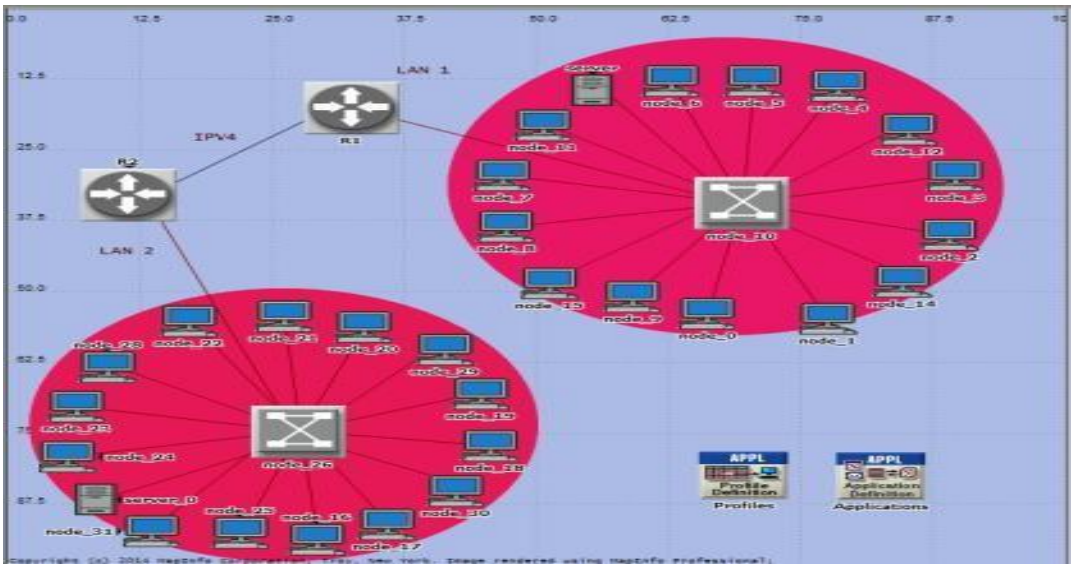


Figure 3: IPv4 Architecture

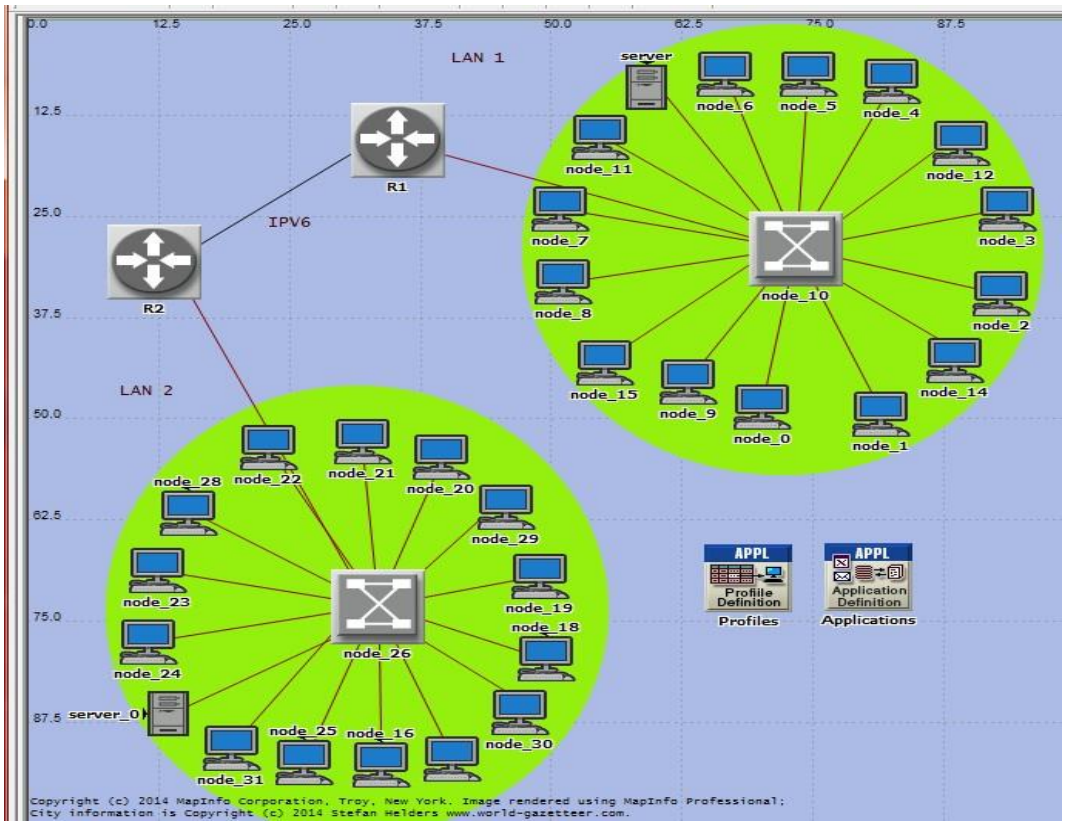


Figure 4: Ipv6 Architecture

METHOD-

The method consisted of one server set, 14 Ethernet workstation switches, and a router. This selection represents one office. In this case the switch is connected to the 14 workstations and 1 server via Ethernet 100baseT. Each office has one router connected to the switch. The two offices are connected to each other using the ppp-ds3 link which connects the two routers. Using the above-mentioned approach, after establishing the link, we specified the application using Application Description to set the application we need to apply in this scenario. In this case, in our scenario, we need to apply voice, http and Email.

After that we used profile definitions to set which profile you need to apply. We need to use Voice Service, http and Ethernet in this situation. To do this, right-click in free space and select individual DES statistics, then select which parameter to analyze in your scenario, in this case we select Ethernet delay and node delay and throughput, jitter, response time (http), voice (send and receive traffic) and, use. Network IPv6 addresses using Protocols > IPv6 > Auto-Assign IPv6 Addresses option and network IPv4 addresses using Protocols > IPv4 > Auto-Assign IPv4 Addresses [19].

Network Components-

This section discusses the following network components used in the suggested network models running on OPNET [20]

• The "User Config" node: -Can be used to create user profiles that can be extended to different network nodes that generate traffic on layer 7 (application layer). You will use crate framework in the "ApplicationConfig" to use that profile.

• Before using this object, use the object "Application Config" You may define the patterns of traffic followed by the applications as well as the profiles configured for this object.

• System Ethernet wkstn node: -represents a workstation running TCP and UDP client-server applications. The workstations support a single 10 Mbps, 100 Mbps, or 1000 Mbps Ethernet link. This workstation needs a fixed amount of time for forwarding each packet, as defined by this node's "IP Forwarding Rate" function. Packets are delivered on FCFS basis (First come, First serve). It can also find queues at the protocol's lower layers because it depends on the transmission rates of the corresponding interface output.

• Object type of router: ethernet4 slip8 gtwynode

• The Ethernet server model represents a server node running over TCP and UDP applications.

• 100BaseT link: -Links and switches between host and router, or host. Represents a 100 MBps Ethernet connection. It can connect any combination of the following nodes (with the exception of switching to router, connecting hub to hub or switching to switch to workstation.Packet Formats: ip3 dgram. Data Rate: DS3 (44.736 Mbps).

• PPP-DS3 duplex link: -Connection between routers.Supports one of the underlying 10 Mbps, 100 Mbps or 1 Gbps Ethernet links. The operating velocity is determined by data rate of the linked connection.

network is 0.19ms compared to that of IPv6 network which is 0.16ms respectively. This is to say that when FTP data volume increases, the number of packets in IPv4 increases thereby causing delay in the IPv4 network. Therefore, the delay in IPv6 network is less than IPv4 regarding the lesser number of packets in the network.

RESULT

Figure 5 below shows the comparison of Ethernet delay between IPv4 and IPv6and shows also both types of theoretical have transient state and stead state station and the IPv6 has small stead stated time if we compare it with IPv4.

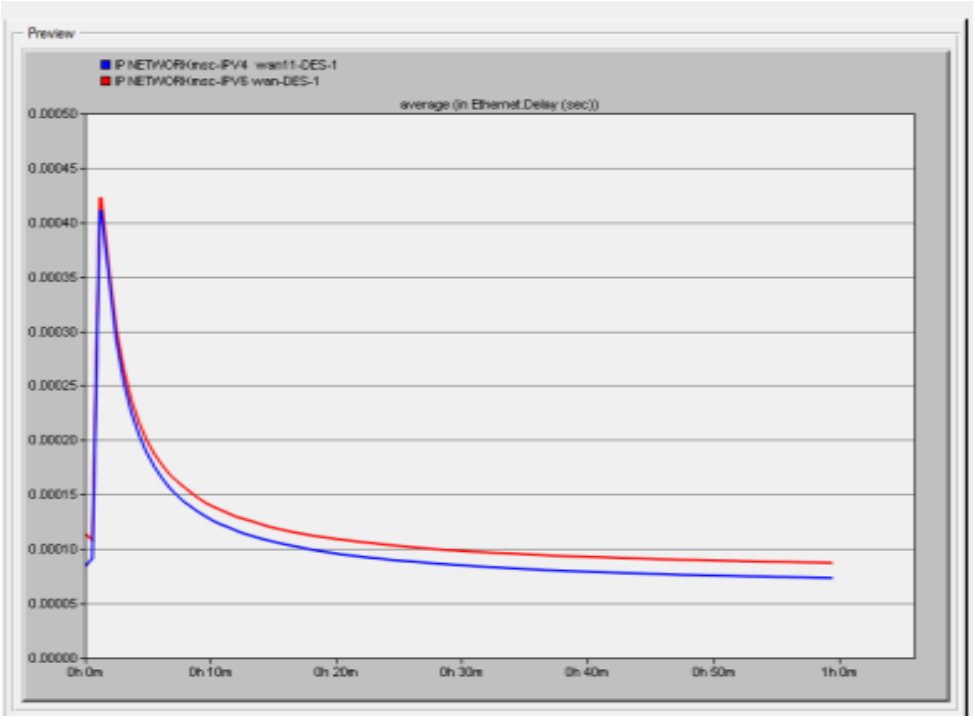


Figure 5: Ethernet Delay

In IPv6 fragmentation performed only by the host. That's why IPv6 's delay is bigger than IPv4 's delay but with a small difference. IPv6 has a higher delay than IPv4 due to the wider header area of IPv6hasa. IPv6 has a smaller header area, the curve takes up time latency in the beginning before the Guide, since the devices in the state start then curve Guide to high because the devices at the same time order. The number of devices Delay has inverse relationship. Figure 6 indicates Answer Time for the email update.

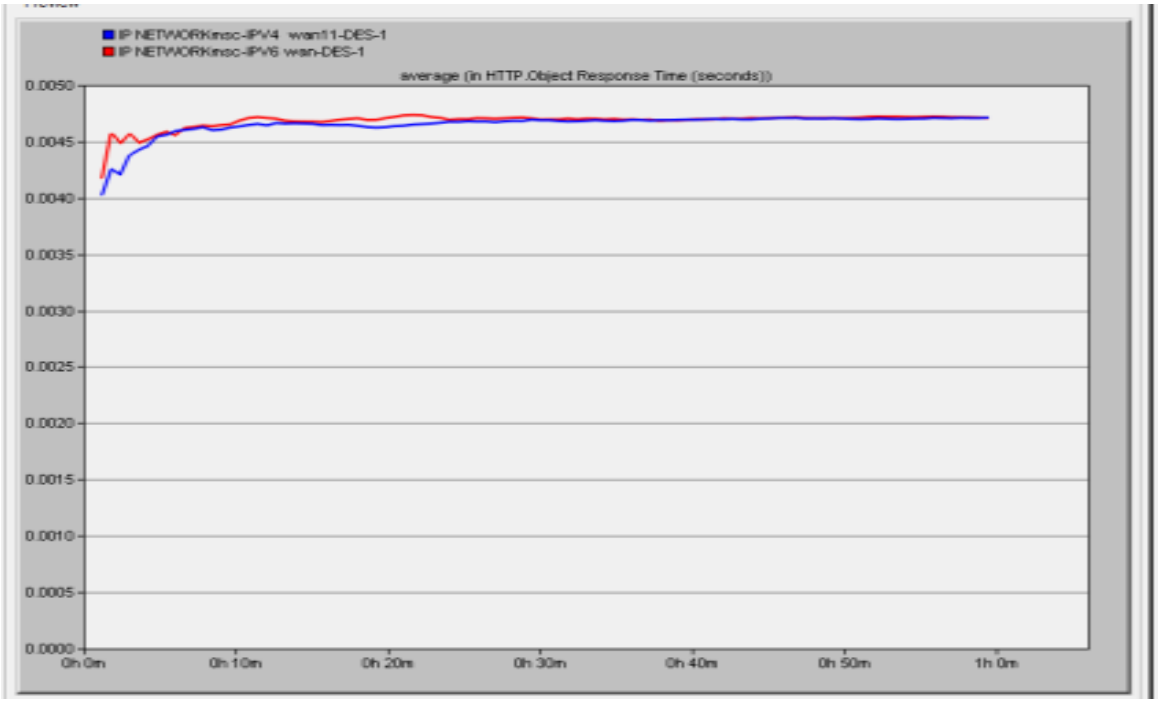


Figure 6: Http Download Response Time

The response time is measured from the time the request is sent to the server by a client application until the response packet is received. Data traffic for IPv4 network slowly increases response time. The difference in anIPv4's anIPv4download response timeand an IPv6 network is slight.Figure 7 below shows a Voice Jitter comparison.

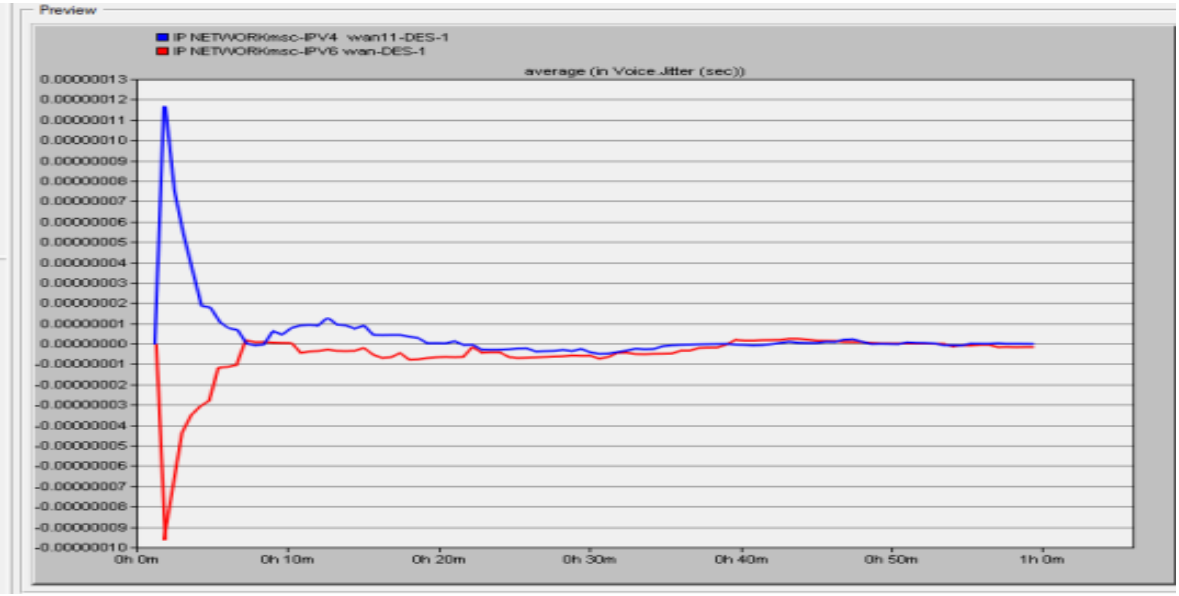


Figure 7: Voice Jitter

Jitter non uniform delays, includes endpoint buffering and reordering of application stage. It isn't easy to tell whether the packet is missing, lost or even late because of the increased jitter. IPv4 has a jitter greater than IPv6.Figure 8,9 below shows the IPV4 and IPV6voicetrafficc send and receive between IPv4 and IPv6 contrast.

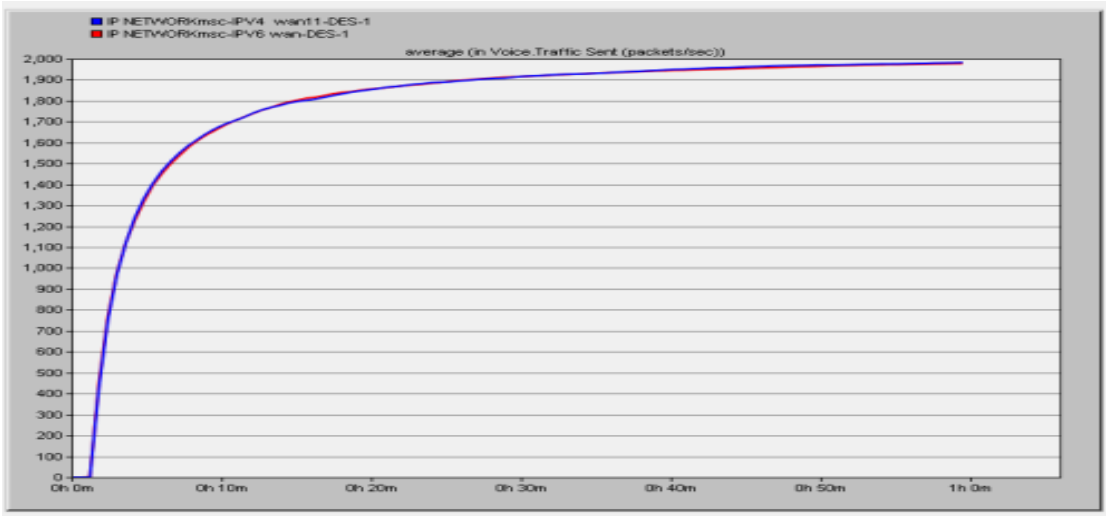


Figure 8: IPV4 and IPV6 voice traffic send

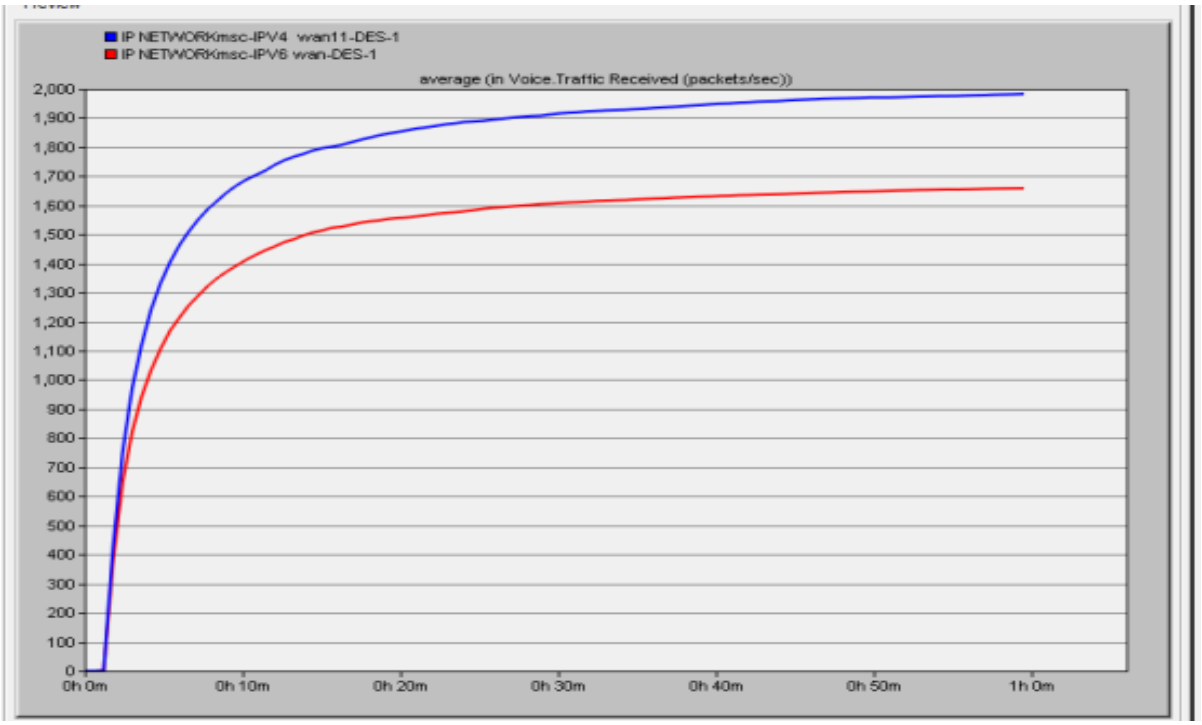


Figure 9: IPV4 and IPV6 voice traffic receive

In figure 10 there are few differences between IPv4 network and IPv6 network in Email download response second.

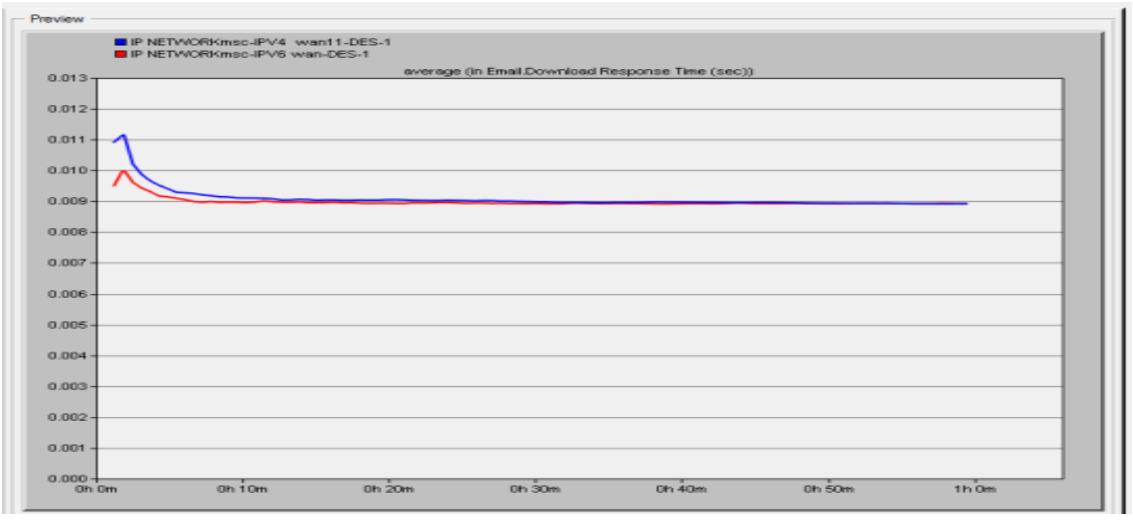


Figure 10: Email Download Response Time

Figure 10 shows the Email Download Response Time The specific objective is to test and compare the performance of two parameters of the protocol stacks (IPv4 and IPv6) to be evaluated when transmitting data from one client to another or to a server over a wired network. In this case we developed wired networks based on the protocols IPv4 and IPv6.

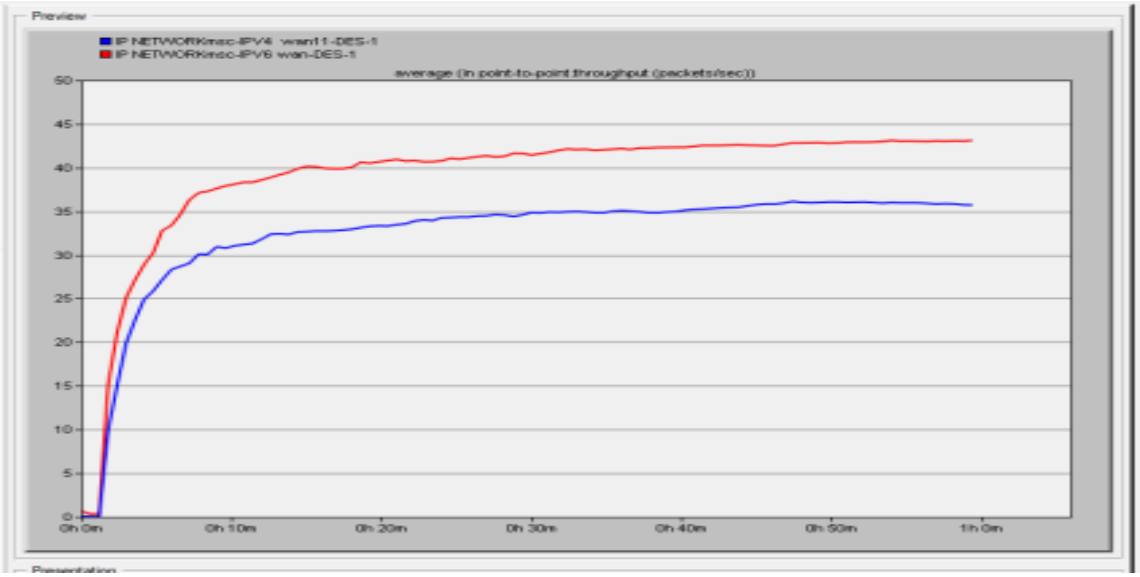


Figure 11: Point to point Utilization

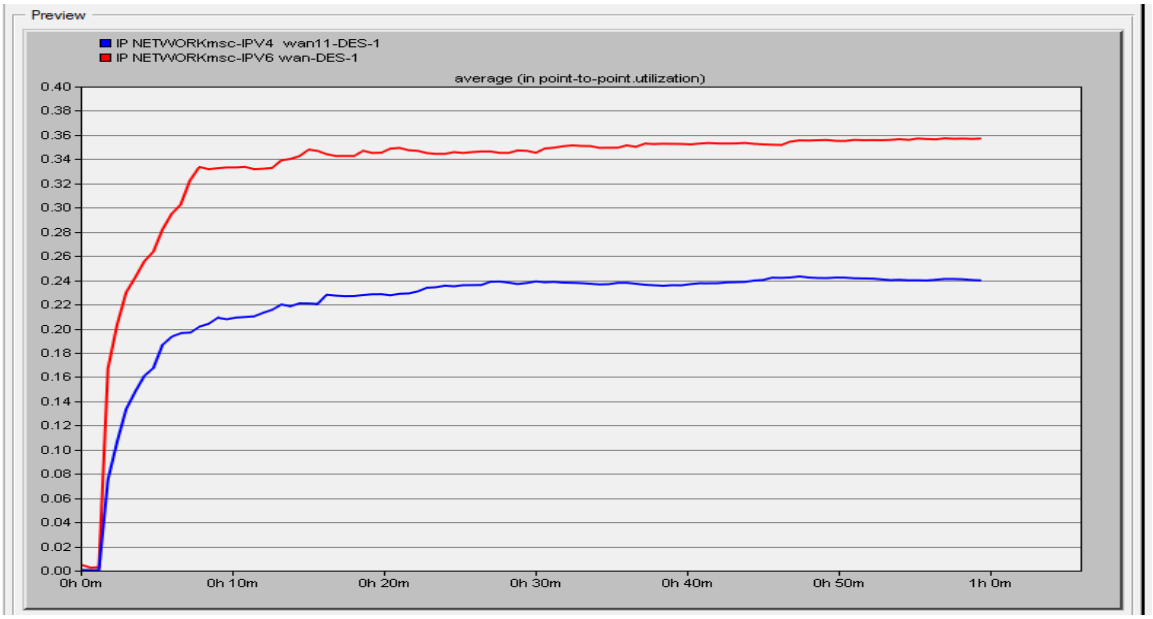


Figure 12: point to point throughput

For all IPv4 / IPv6 traffic ratios, Figure 12 below is representative of the freemen figure 11 the sizes with a 100 percent throughput value. Since the rate line rises the CPU is steadily increasing. Those traffic mixes with the most IPv6 traffic are the highest utilization per line rate.

Use of the CPU increases when more time is needed for a system process or when more network packets are sent and received. Under normal operating conditions, the CPU is busy at least 5 per cent of the time on a non-stackable switch. If the switch is stacked the CPU will be busy with a minimum consumption of (7 or 8) percent. The use of the CPU in a switch stack is only measured at the master switch. However the number of stack members specifically affects this.Figure 12 below displays a point-to - point analysis of the IPv4 and IPv6.

Chapter 6

Simulation

For simulation we are taking a netwrok consisting of 2 main LAN systems. One consisting of IPv4 the other IPv6. The configurations are as follows,

IPv4: 172.16.0.0/20
IPv6: 2001:211:DAC::/48

User LAN has 520 Hosts whereas Server LAN has 12 hosts.

For IPv4 we are going to,

Subnet the given network and assign the first usable subnet to User LAN while wasting the fewest addresses.
Subnet further the third usable subnet and assign the seventh usable subnet to Server LAN.
- IPv4 gateway for both User and Server LAN should use the last usable IP address of the corresponding subnet.
- Assign the 1st usable IP address of the corresponding subnet to User PC1
- Assign the 260th usable IP address of the corresponding subnet to User PC2
- Assign the 515th usable IP address of the corresponding subnet to Printer
- Assign the 3rd usable IP address of the corresponding subnet to DNS and TFTP Server
- Assign the 2nd to the last usable IP of the corresponding subnet to User LAN and Server LAN Switch

For IPv6 we are going to,

Subnet the given network and assign the 11th subnet to User LAN and 15th subnet to Server LAN.
- IPv6 gateway for both User and Server LAN should use the 1st IP address of the corresponding subnet.
- Assign the 2nd IP address of the corresponding subnet to User PC1
- Assign the 3rd IP address of the corresponding subnet to User PC2
- Assign the 4th IP address of the corresponding subnet to Printer
- Assign the 4th IP address of the corresponding subnet to DNS and TFTP Server

Configurations

- Configure the router hostname: SM
- Set Banner Message of the Day to Unauthorized Access Prohibited!
- Newly-entered passwords must have a minimum length of 8 characters
- Protect device configurations from unauthorized access with the encrypted password. Set the password to enpa$$word

- Secure all the ways to access the router. Set the passwords to smpa$$word
- Prevent all passwords from being viewed in clear text in device configuration files
- Set IP domain-name to sm.net
- Configure SSH version 2. Use the value 1024 for encryption key strength. Set time out to 60 seconds and limit authentication retries to 5
- Create an user having username: admin and encrypted password: adminpa$$. Configure user authentication for in-band management connections.
- Configure the two Gigabit Ethernet interfaces using the IPv4 and IPv6 values you calculated. Use description for both interfaces. Set interface descriptions to 'User LAN' and 'Server LAN' respectively.
- Set the hostname of User LAN switch to USW and Server LAN switch to SSW
- Configure User LAN and Server LAN switch for remote management. Use Telnet for remote access to Switch.
- Backup the running configuration of router and switches to the TFTP Server. Use the default file name.

For testing at the end of the configuration

- We are able to remotely login to Router using SSH.
- We are able to remotely login to Switches using Telnet.

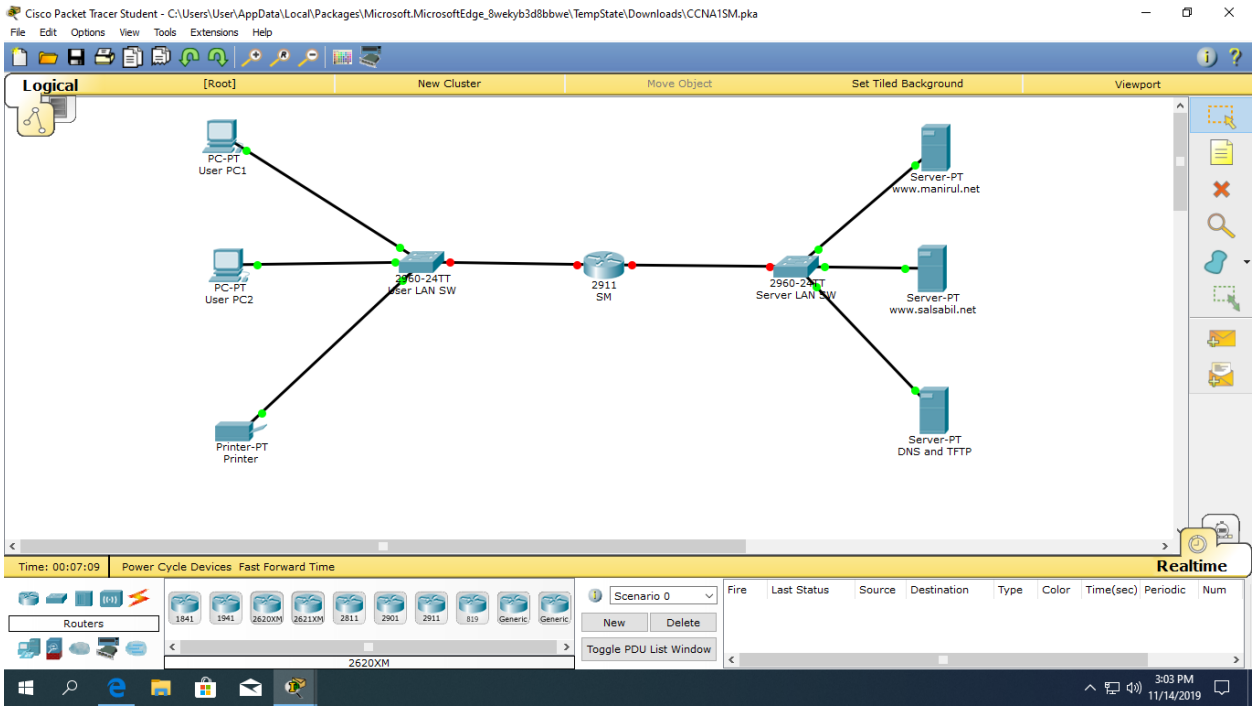


Fig: Network used for implementation

OutCome:

With the proper implementations of the code and configuring the end users, a proper network is established and both IPv4 and IPv6 is funcional in it.

Chapter 6
Conclusion

The selected subject was in near comparison based on the assessment of version 4 of the Internet Protocol (IPv4) and version 6 of the Internet Protocol (IPv6). Some issues relating to the IPv4 problem have been addressed. Knowledge of the researcher in Internet Protocol Addressing initiated the study and analysis on several papers to address some TCP / IP issues. There have been some justifications on several review journals condemning the IPv4 and IPv6 but the obvious reasons for coexistence are rising. Most users discover the resources they need along with good information, despite bad information, and cause unjustified concern. Now the fact that performance is one great reason for this study, the analysis of IPv4 and IPv6 networks illustrated with their performance showed that the performance of IPv6 seems better than the IPv4 with no much difference but yet did not shown 100 % absolute performance over IPv4. This analysis includes their inputs, delays, throughputs of packets and response time.

Through this paper the researcher concluded that while IPv6 deployment is a requirement, given the various advantages associated with the new version, it is still a gradual transition. For a long time, IPv4 and IPv6 will coexist, hence the need for communication methods between the new and the old versions. Having gathered and checked this fact, the researcher is of the opinion that there is an urgent need to implement either of the practices; DUAL-STACKING or TUNNELING as soon as possible, in order to prevent future problems in internet networks as the related issues / challenges address spaces in the Internet Protocol version 4 (IPv4) numbering system.

We evaluated low- and medium-load (http) and heavy-load Ethernet delays on IPv4 / IPv6 networks. Two network scenarios were simulated, named IPv4 network and IPv6 network. The simulation was made using OPNET. In both network scenarios a comparative investigation of Ethernet delay was carried out based on simulative and analytical approaches. Based on this research, the purpose of the research question was to understand and investigate what is the difference in the delay experienced in the IPv4 and IPv6 networks or what is best from the (QoS) site for users. The simulation result at low load notice IPv4 is a lower delay than IPv6, at medium load the delay between them is very low at high load the delay is similar.

Thus, the analysis of the IPv4 and IPv6 networks presents us through statistical analysis with their performance characteristics. The statistics obtained from simulation tell us IPv6 performance is much better than IPv4 performance. Under different conditions the IPv6 performs better. As far as performance is concerned; the IPv6 protocol has better transmission efficiency and high throughput, and those traffic mixes with the most IPv6 traffic are the greater utilization per line rate.

IPv6 has a higher delay than IPv4 due to the wider header area of IPv6hasa. IPv4 has a smaller header field and frame for the packets. The jitter is another key aspect of that. Jitter is essentially a slight irregular directional flow of electrical signals, which are the data packets in fact. When the simulation was a running state, then there was more or less no significant difference in both protocol jitter values observed. Though IPv6 showed less jitter than IPv4 protocol in a comparison. With the extinction of address spaces in IPv4, the need to adopt IPv6 protocol as soon as possible to avoid future impediments in the Internet network is immediate.

Code:

User LAN => 520 => /22
Server LAN => 12 => /28

Given

IPv4: 172.16.0.0/20

Subnetting the given network to /22

172.16.0000 00 00.00000000 => First Usable Subnet
01
10
11

Subnetting further the third usable subnet to /28
172.16.0000 10 00.0000 0000
00.0001
00.0010
00.0011
00.0100
00.0101
00.0110 => Seventh Usable Subnet
00.0111
.....
11.1111

User LAN

172.16.000000 00.00000000 /22 => 172.16.0.0/22 => Network Address
00.00000001 => 172.16.0.1 => First Usable Address => PC1

01.00000100 => 172.16.1.4 => 260th Usable Address => PC2

10.00000011 => 172.16.2.3 => 515th Usable Address => Printer

11.11111101 => 172.16.3.253 => Second to the Last Usable Address
11.11111110 => 172.16.3.254 => Last Usable Address
11.11111111 => 172.16.3.255 => Broadcast Address

Server LAN

172.16.00001000.0110 0000 /28 => 172.16.8.96/28 => Network Address
0001 => 172.16.8.97 => First Usable Address => manirul.net
0010 => 172.16.8.98 => Second Usable Address => salsabil.net
0011 => 172.16.8.99 => Third Usable Address => DNS & TFTP
....
1101 => 172.16.8.109 => Second to the Last Usable Address
1110 => 172.16.8.110 => Last Usable Address
1111 => 172.16.8.111 => Broadcast Address

IPv6

2001:211:DAC::/48

Assigning the 11th Subnet to User LAN
2001:211:DAC:A::/64
2001:211:DAC:A::0/64 => First Usable IP => Gateway
2001:211:DAC:A::1/64 => Second Usable IP => User PC1
2001:211:DAC:A::2/64 => Third Usable IP => User PC2
2001:211:DAC:A::3/64 => Fourth Usable IP => Printer

Assigning the 15th Subnet to Server LAN
2001:211:DAC:E::/64
2001:211:DAC:E::0/64 => First Usable IP => Gateway
2001:211:DAC:E::1/64 => Second Usable IP => manirul.net
2001:211:DAC:E::2/64 => Third Usable IP => salsabil.net
2001:211:DAC:E::3/64 => Fourth Usable IP => DNS & TFTP

Tue Sep 11 18:59:14 2018 SM Router>enable
Tue Sep 11 18:59:16 2018 SM Router#conf t
Tue Sep 11 18:59:19 2018 SM Router(config)#hostname SM
Tue Sep 11 19:03:36 2018 SM SM(config)#banner motd #Unauthorized Access Prohibited!#
Tue Sep 11 19:03:53 2018 SM SM(config)#security passwords min-length 8
Tue Sep 11 19:04:25 2018 SM SM(config)#enable secret enpa$$word
Tue Sep 11 19:04:38 2018 SM SM(config)#line console 0
Tue Sep 11 19:04:49 2018 SM SM(config-line)#password smpa$$word
Tue Sep 11 19:04:51 2018 SM SM(config-line)#login
Tue Sep 11 19:04:51 2018 SM SM(config-line)#exit
Tue Sep 11 19:04:55 2018 SM SM(config)#line vty 0 4
Tue Sep 11 19:04:57 2018 SM SM(config-line)#password smpa$$word
Tue Sep 11 19:04:59 2018 SM SM(config-line)#login
Tue Sep 11 19:04:59 2018 SM SM(config-line)#exit

Tue Sep 11 19:05:12 2018 SM SM(config)#do sh run
Tue Sep 11 19:05:25 2018 SM SM(config)#service password-encryption
Tue Sep 11 19:05:49 2018 SM SM(config)#ip domain-name sm.net
Tue Sep 11 19:06:17 2018 SM SM(config)#crypto key generate rsa
Tue Sep 11 19:06:23 2018 SM SM(config)#ipssh version 2
Tue Sep 11 19:06:28 2018 SM SM(config)#ipssh time-out 60
Tue Sep 11 19:06:32 2018 SM SM(config)#ipssh authentication-retries 5
Tue Sep 11 19:07:29 2018 SM SM(config)#line vty 0 4
Tue Sep 11 19:07:32 2018 SM SM(config-line)#transport input ssh
Tue Sep 11 19:07:33 2018 SM SM(config-line)#exit
Tue Sep 11 19:06:58 2018 SM SM(config)#username admin secret adminpa$$
Tue Sep 11 19:08:04 2018 SM SM(config)#line console 0
Tue Sep 11 19:08:07 2018 SM SM(config-line)#login local
Tue Sep 11 19:08:08 2018 SM SM(config-line)#exit
Tue Sep 11 19:08:11 2018 SM SM(config)#line vty 0 4
Tue Sep 11 19:08:13 2018 SM SM(config-line)#login local
Tue Sep 11 19:08:14 2018 SM SM(config-line)#exit
Tue Sep 11 19:09:19 2018 SM SM(config)#ipv6 unicast-routing
Tue Sep 11 19:08:46 2018 SM SM(config)#int g0/2
Tue Sep 11 19:08:51 2018 SM SM(config-if)#description User LAN
Tue Sep 11 19:09:01 2018 SM SM(config-if)#ip address 172.16.3.254 255.255.252.0
Tue Sep 11 19:09:12 2018 SM SM(config-if)#ipv6 address 2001:211:DAC:A::/64
Tue Sep 11 19:09:14 2018 SM SM(config-if)#no shut
Tue Sep 11 19:09:15 2018 SM SM(config-if)#exit
Tue Sep 11 19:09:31 2018 SM SM(config)#int g0/1
Tue Sep 11 19:09:43 2018 SM SM(config-if)#description Server LAN
Tue Sep 11 19:09:51 2018 SM SM(config-if)#ip address 172.16.8.110 255.255.255.240
Tue Sep 11 19:09:58 2018 SM SM(config-if)#ipv6 address 2001:211:DAC:E::/64
Tue Sep 11 19:10:02 2018 SM SM(config-if)#no shut
Tue Sep 11 19:10:03 2018 SM SM(config-if)#exit
Tue Sep 11 19:14:03 2018 User LAN SW Switch>en
Tue Sep 11 19:14:05 2018 User LAN SW Switch#conf t
Tue Sep 11 19:14:12 2018 User LAN SW Switch(config)#hostname USW
Tue Sep 11 19:14:25 2018 User LAN SW USW(config)#banner motd #Unauthorized Access Prohibited!#
Tue Sep 11 19:14:35 2018 User LAN SW USW(config)#enable secret enpa$$word
Tue Sep 11 19:14:39 2018 User LAN SW USW(config)#line console 0
Tue Sep 11 19:14:52 2018 User LAN SW USW(config-line)#password smpa$$word
Tue Sep 11 19:14:53 2018 User LAN SW USW(config-line)#login
Tue Sep 11 19:14:54 2018 User LAN SW USW(config-line)#exit
Tue Sep 11 19:14:56 2018 User LAN SW USW(config)#line vty 0 4
Tue Sep 11 19:14:58 2018 User LAN SW USW(config-line)#password smpa$$word
Tue Sep 11 19:14:59 2018 User LAN SW USW(config-line)#login
Tue Sep 11 19:15:00 2018 User LAN SW USW(config-line)#exit

Tue Sep 11 19:15:10 2018 User LAN SW USW(config)#service password-encryption
Tue Sep 11 19:15:17 2018 User LAN SW USW(config)#int vlan 1
Tue Sep 11 19:15:36 2018 User LAN SW USW(config-if)#ip address 172.16.3.253 255.255.252.0
Tue Sep 11 19:15:39 2018 User LAN SW USW(config-if)#no shutdown
Tue Sep 11 19:15:41 2018 User LAN SW USW(config-if)#exit
Tue Sep 11 19:16:07 2018 User LAN SW USW(config)#ip default-gateway 172.16.3.254
Tue Sep 11 19:16:22 2018 User LAN SW USW(config)#exit
Tue Sep 11 19:16:43 2018 Server LAN SW Switch>en
Tue Sep 11 19:16:44 2018 Server LAN SW Switch#conf t
Tue Sep 11 19:16:54 2018 Server LAN SW Switch(config)#hostname SSW
Tue Sep 11 19:17:20 2018 Server LAN SW SSW(config)#banner motd #Unauthorized Access Prohibited!#
Tue Sep 11 19:17:29 2018 Server LAN SW SSW(config)#enable secret enpa$$word
Tue Sep 11 19:17:32 2018 Server LAN SW SSW(config)#line console 0
Tue Sep 11 19:17:40 2018 Server LAN SW SSW(config-line)#password smpa$$word
Tue Sep 11 19:17:41 2018 Server LAN SW SSW(config-line)#login
Tue Sep 11 19:17:43 2018 Server LAN SW SSW(config-line)#exit
Tue Sep 11 19:17:46 2018 Server LAN SW SSW(config)#line vty 0 4
Tue Sep 11 19:17:48 2018 Server LAN SW SSW(config-line)#login
Tue Sep 11 19:17:52 2018 Server LAN SW SSW(config-line)#password smpa$$word
Tue Sep 11 19:17:53 2018 Server LAN SW SSW(config-line)#login
Tue Sep 11 19:17:54 2018 Server LAN SW SSW(config-line)#exit
Tue Sep 11 19:17:57 2018 Server LAN SW SSW(config)#service password-encryption
Tue Sep 11 19:18:00 2018 Server LAN SW SSW(config)#int vlan 1
Tue Sep 11 19:18:15 2018 Server LAN SW SSW(config-if)#ip add 172.16.8.109 255.255.255.240
Tue Sep 11 19:18:17 2018 Server LAN SW SSW(config-if)#no shut
Tue Sep 11 19:18:19 2018 Server LAN SW SSW(config-if)#exit
Tue Sep 11 19:18:26 2018 Server LAN SW SSW(config)#ip default-gateway 172.16.8.110
Tue Sep 11 19:18:27 2018 Server LAN SW SSW(config)#exit
Tue Sep 11 19:18:30 2018 Server LAN SW SSW#copy run start
Tue Sep 11 19:18:37 2018 Server LAN SW SSW#copy run tftp:
Tue Sep 11 19:18:58 2018 User LAN SW USW#copy run start
Tue Sep 11 19:19:02 2018 User LAN SW USW#copy run tftp:
Tue Sep 11 19:19:28 2018 SM SM#copy running-config startup-config
Tue Sep 11 19:19:35 2018 SM SM#copy running-config tftp:

References

[1] B. Edelman, "Running Out of Number: Scarcity of IP Addresses and What to do About it," 2014.

[2] SHISA, "WIDE project," 200.

[3] s. b. F. B. ,. D. B. k. nichols, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," December 1998.

[4] A. N. A. Ali, "Comparison stdy between IPV4 & IPV6," vol. 09, 1 2012.

[5] D. c. A. S. Sharma, "A survey on Next Generation Internet Protocol IPV^," vol. 02, June 2014.

[6] F. A. K. e. Al, "Performance Analysis of Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) over MPLS," 2014.

[7] R. H. S. Deering, "Internet Protocol Version 6 (RFC2460)," 1998.

[8] D. Huston, "The Potaroo website," 2009.

[9] "Network layer Protocol".

[10] I. G. S. K. B. H. Y. A. [4] The Benefits of UsingAmer N.AbuAli, "The Benefits of Using Internet Protocol Version 6," vol. 05, pp. 583-587.

[11] R. H. A. P. Mohd. Khairil Sailan, "A Comparative Review Of IPv4 and IPv Research TestBed," 5-7 August 2009.

[12] "Six Benifits of IPv6," 08 june 2011.

[13] I. Johnson, "The Ripe website," 2009.

[14] D. A. B. A. M. Y. A. Y. A.-G. Ghaida Yagoub Ahmed Yosif Al-Gadi, "Comparison Between Ipv4 And Ipv6 Using Opnet Simulator," IOSR jornall of Engineering, vol. 04, pp. 44-50, 08 August 2014.

[15] S. D. R. Hinden, "IP Version 6 Addressing Architecture," July 1998.

[16] J. A.Dutta, "IPv6 TRANSITION TECHNIQUSFORLEGACY APPLICATION," MILCOM, 2006.

[17] A. n. a. Ali, "Comparison study between IPv4&IPv6," International journal of computer science issue, 01 May 2013.

[18] "OPNET: IPv6 for R&D Specialized Model," 15 December 2013.

[19] "OPNET Training," 29 January 2013.

[20] "OPNET: IPv6 for R&D Specialized Model," 12 December 2013.

[21] G. Huston, "IPv4 Address Report," 21 may 2008.