Comparison and contrasting between IPv4 and IPv6

Abstract

As a result of the explosion of the internet in the 1990's, many devices have since been connected. The internet protocol addressing scheme became an addressing system to recognise on the internet; this was known as the Internet Protocol version 4 (Ipv4). Due to imminent exhaustion of this addressing scheme, a new addressing scheme has been developed which provides more usable addresses for devices, and it was termed IPv6. Acme Ltd is considering acquiring more offices and employing more people in the future and is concerned about the imminent lack of IPv4 addresses; it wants to investigate whether to migrate the company's addressing scheme to pure IPv6 or a mixture of both. The current predominant traffic of the company is HTTP web browsing. An investigation was conducted in this report via OPNET, using a pure IPv4 network, a pure IPv6 network and another Ipv4 and Ipv6 mixed network via tunnelling. Parameters such as page response time, Ethernet delay and packet dropped were collated across the entire network. The result indicated that having a mixture of Ipv4 and Ipv6 offers similar performance to a pure Ipv4 while a pure Ipv6 network offers better performance overall when benchmarked against this parameters.

Table of Contents

List of Figures

List of Tables

1.0. Introduction

The internet is currently an essential part of our lives, and it contains thousands of information cutting across different topics. With the internet, at the comfort of our living room, we could pay for different products and goods, pay for bills, watch movies, play music, get the latest news at our fingertips, especially via mobile or tablet devices. The internet is an enormous network of computers that are connected via a wireless or wired network. A unique address identifies each device on this network. This is known as an Internet Protocol address. The Internet Protocol version 4 (IPv4) is the dominant networking protocol used on the internet.

This protocol has been in existence since the 1970's, on other networks as well as the internet. It is mostly used with the Transport Control Protocol (TCP), and it is referred to as the TCP/IP Network. Due to the rapid explosion of the internet in the 1990's, the Internet Engineering Task Force (IETF) began working on a new protocol to replace the IPv4. After several years of hard work, the specification for IPv6 was published. This project attempts to compare and contrast the Internet protocol version 4 (IPv4) with the Internet protocol version 6 (IPv6). Also, the real environment of a large fictitious company having an IPv4 based network will be simulated. This network will be upgraded to IPv6 as well as to a network with a mixture of both IPv4 and IPv6. The reports analyse the pros and cons of the company running each variant, then a recommendation regarding the choice of protocol based on these analyses of network dynamics such as delay, packet dropped, and so on, is made.

The aims of this report are outlined below:

1. To gain in-depth technical knowledge about internet protocols especially IPv4 and IPv6.
2. To simulate and compare IPv4, IPv6 and to mix IPv4 and IPv6 via OPNET
3. To provide comprehensive guidelines about the choice of migrating to a pure IPv6 or to keeping a mixture of both IPv4 and IPv6 network.

The remaining part of the report is structured as follows:

- **Chapter 2** is a review of IPv4 and IPv6 technologies as well as the necessary steps needed in mixing and IPv4 network with an IPv6 network
- **Chapter 3** contains a detailed description of the case scenario as well as a discussion of how the experiment will be done.

- **Chapter 4** is a simulation of an IPv4 and IPv6 network on OPNET, testing various network monitoring parameters such as delay, packet drops and so on. Also, a simulation of a mixture of IPv4 and IPv6 network with tunnelling was conducted in OPNET with the same parameters being monitored.
- **Chapter 5** is the conclusion of the report. Also, future testing recommendations were made.

2.1. Internet Protocol Version 4 (IPv4)

The Institute of Electrical and Electronic Engineers (IEEE) publicised a book known as "A Protocol for Packet Network Intercommunication", the authors described a way of sharing resources in a packet switching network (Cerf & Khan, 1974). In 1981 the version of the IPv4 was produced. The IPv4 is a connectionless protocol used in a packet-switched network such as the Ethernet. IPv4 is the fourth generation of the Internet Protocol system, used in the identification of different devices and machines; providing a unique identifier for each device (Shoch, 1978), which are connected to a specific network (Hagen, 2006).

The architecture of IPv4 allows a total of approximately 4 billion IP addresses (Mun & Lee, 2005).In the present age of internet and communication, many networks in today's world use the Internet Protocol version 4 (IPv4) standard whose IP addresses uses four bytes (32 bits) in length (Leiner et al., 1985). It is expected that the number of IPv4 addresses will be entirely consumed by the growing number of internet using machines and devices (Beijnum, 2006).

2.1.1 Addressing System

Before IPv4 implementation, the engineers discussed while developing ARPANET to determine the length of an IP address; the discussion centred around whether to use a 128-bit address or a 32-bit address for its length (Olabenjo & Omar, 2014). The decision to use a 32-bit length address as against 128-bit address was made in 1977 (Cerf, 1978). This amounted to a total of 4.3 billion addresses at that time, and they never envisage the need for more address because, at that time, the internet just started (Olabenjo & Omar, 2014). IPv4 has five different classes, A, B, C, D, E. Classes A, B and C exhibit different bit length to address a network host. Class D addresses are reserved for multicasting purpose, while class E addresses are reserved for use in the future (Olabenjo & Omar, 2014). IPv4 utilises a 32 bit addressing which gives a total of 4,294,967,296 unique addresses (Amer, 2012).

A typical example of an IPv4 address is "158.80.164.3", it has four octets of 8 bits each all leading to a 32-bit address (Virgeniya & Palanisamy, 2013). The address looks like 10011110.01010000.10100100.00000011 for the four octets (Olabenjo & Omar, 2014). Table 1 below shows the assignment of IPv4 addresses with the host count of each class. The IP addressing system also has a subnet mask that makes it possible to differentiate between

network address and host addresses, e.g. if our device has an IP address of 192.168.0.9 and also a subnet mask of 255.255.255.0, "192.168.0" is the identification of the network which falls in the class C network address while the last octet in decimal, i.e. "2" is the host.

Table 1: IPv4 Network Classification

Different Classification		
Network Class	**Networks Count**	**Host Count**
A	126	16,777,214
B	16,382	65,534
C	2,097,150	254

2.1.2 Why IPv4 addresses are getting exhausted

As a result of the massive increase in the production of handheld devices such as tablets and mobile phones, coupled with an increased number of computers all of which connects to the internet, the demand for having more IPv4 addresses has been on the increase. The last bock of IPv4 addresses was released on the 3rd of February 2011 by the Internet Corporation for Assigned Names and Numbers (ICANN) in 2011 (Olabenjo & Omar, 2014). This indicates that IPv4 will be exhausted shortly and it would be difficult for companies that are expanding to get new IPv4 addresses.

2.1.3 IPv4 shortage workaround

Even though IPv4 faces imminent exhaustion, several technologies have been developed and deployed to as workaround solution to this issue. These include Classless Inter-Domain Routing (CIDR), dynamic IPv4 address assignment (DHCP) or Dynamic Host Configuration Protocol and Network Address Translation (NAT) (Next Generation Internet, 2009). Network Address Translation (NAT) ranks as the most popular amongst these technologies, and it has contributed positively by helping to move forward the time it would take to exhaust IPv4 addresses (Doshi et al., 2012).

2.1.4 Shortcomings of IPv4

Internet Protocol version 4 (IPv4) however has some few disadvantages, some of which include:

- **Network Congestion:** As a result of the IPv4 broadcast feature, it is possible for network devices to be overloaded and congested because packets could be sent to all network addresses (Olabenjo & Omar, 2014).
- **Data Priority:** As a result of the IPv4 not being able to recognise the various data that are transmitted, prioritising traffic data, e.g. video streaming over other types of data is hard (Olabenjo & Omar, 2014).
- **Security:** IPv4 has no security features such as data encryption or packet authentication during transmission (Virgeniya & Palanisamy, 2013).
- **Address Space:** As a result of increase in the number of devices that are connected to the internet, i.e. IP address being able to only cater for around 4 billion hosts, this will in the future lead to high limitation in the number of devices that are connected to get online (Olabenjo & Omar, 2014)..
- **Packet Loss:** IPv4 possesses a Time to Live (TTL) (Virgeniya & Palanisamy, 2013) field in the header of an IP; which sets the expiry time for the datagram. If the data could not reach its destination on time, that data will expire, and the receiving computer would have to request for that data again. This multiple request and delay will result in lost packets, and this is not efficient for real-time activities such as video streaming and VOIP.

2.2. Internet Protocol Version 6 (IPv6)

IPv6 also known as next-generation IP is the newer version of its predecessor IPv4, created primarily to solve the addressing exhaustion problem of IPv4, due to the 1990's internet explosion. It also features other additions that will be discussed in section 2.3. The new IPv6 features addresses of 16 bytes (128 bits) in length (Deering & Hinden, 2008).

There has been active research and development work going on to transit from IPv4 to IPv6 network. Since IPv4 and IPv6 are completely different protocols and there is no backward compatibility for IPv6; therefore, research in this direction is essential and demand a clear procedure and high-level compatibility to transit from IPv4 to IPv6 (Govil et al. 2008). Some of the possible difficulties regarding this transition include:

- the difficulty of the IPv4 hosts and routers working directly with IPv6 traffic;

- The existence of a problem with the address allocation and routing when IPv4 is used indefinitely
- It will take a long time, if possible, to switch into IPv6 (Zimu et al. 2012).

Consequently, it is necessary for there to be a development of a reliable mechanism for transitioning into IPv6. In the context of this project, the project identifies the following possible candidate solutions that shall be analysed and evaluated during this work: Zhonghua et al. (2012) presented a Dual Stack technology based broadband dial-up users IPv6 toIPv4 transition proposal, which also adopts 6to4/ISATAP Tunnel. Furthermore, the approach can run WWW, FTP, Http, DNS and other network application platform in an IPv6 environment. Wiljakka at al. (2002) discussed transition methods such as dual IPv4/IPv6 stacks in network elements/terminals, tunnelling, and translators in the network and identified three transition phases from IPv4 to IPv6. The authors also analysed different scenarios from the 2G/3G mobile network point of view, and some recommendations on the use of transition methods are also given.

All of the techniques mentioned above and approaches are primarily for static environments; the project is also interested in learning how mobility can affect this transition. To this end, an interesting work is presented by Xie and Narayanan (2009). For a dual-stack mobile node, the authors analysed various handoff scenarios in a mixed IPv4 and IPv6 environment. They investigated how handoff procedures can be designed to handle all scenarios. The performance of the approach is analysed regarding handoff's signalling cost, delay and failure. Numerical results are provided to show the results and conclusions are drawn, and recommendations are made to have cost-effective mobility support mechanisms for IPv4 and IPv6 transition. Worldwide adoption of IPv6 has been increasing in recent years with Google website capturing how many people are accessing its service via IPv6 (Google.com, 2015).

2.2.1 Solving IPv4 Problems (IPv6 to the rescue)

The primary reason for adopting IPv6 is due to IPv4 exhaustion. IPv6 nevertheless has several features and significant improvements as against IPv4. IPv6 will have more scalability and reach almost unlimited IP addresses as a result of its larger address space. It will also provide more effective routing technique, i.e. provision of global address for every device on the network as well as the enablement of end-to-end reachability and also improved network

performance. The following features are the list of benefits that IPv6 will offer to IT and network professionals in addition to solving IPv4 problems (Next Generation Internet, 2009):

- Provision of larger address space
- Auto-configuration as well as plug-and-play support
- Packet handling efficiency due to simpler header format
- No need for application's layered gateway (ALG) and network address translation (NAT)
- IPSec implementation is the built-in security feature for IPv6
- Enhanced Mobile IP and Computing device support
- Hierarchical network architecture
- Expansion of multicast address number

2.2.2 IPv6 Migration Issues

Even though migration from IPv4 to IPv6 has already begun, some major issues need to be addressed before migration (Saurabh & Shilpa, 2011):

1) Financial Issues: Migrating from IPv4 to IPv6 will require devices that will support IPv6 such as routers, switches, and so on, which automatically means more money will be spent.

2) Tunnelling Issues: IPv6 can be used in an already existing IPv4 network by configuring a Tunnel to connect IPv4 nodes to IPv6 nodes without any applications changes. This is, however, time-consuming and will require a time-consuming configuration process by network managers.

3) Infrastructure Issues: A large number of protocols as well as technologies needs redesigning to support IPv6, some these include: TCP/IP, ARP, RIP, BGP, OSPF, DHCP and others.

4) Security Issues: IPv6 is not well tested, and so, the effectiveness of the security level is still unclear.

2.2.3 IPv4 to IPv6 Interoperability Technique

Several mechanism and techniques exist which will facilitate the transmission from IPv4 to IPv6 interoperation possible, some of these techniques include:

1) **Tunnelling:** In developing a network that is fully IPv6 dependent, it is essential to implement a network that can transfer IPv6 traffic packets via an existing IPv4 infrastructure. The process of encapsulating IPv6 packets with IPv4 packets, i.e. using IPv4 as a link layer for IPv6 is known as tunnelling (Next Generation Internet, 2009).

2) **Proxying and Translation:** This is mostly used in a situation where an IPv6 device is trying to gain access to an IPv4 service, e.g. a web server. There ought to be some form of translation between both end-points to connect each other. The most reliable way to do this is via the usage of a dual-stack application-layer proxy also known as a web proxy (Next Generation Internet, 2009).

2) **Dual Stack:** Because IPv6 is an upgrade from IPv4, it has backward compatibility with IPv4 and inherits some of its features. Hence, it is easy to create networks that support both IPv6 and IPv4. This is known as a dual stack. Most new devices and software that supports IPv6 already have dual stack implemented (Amer, 2012)

3) **Addressing simplicity:** This process involves the allowance of a router or an updated host to continue with its use of an IPv4 address; this is like automatic tunnelling that provides the dual-stack host, routers or both IPv6 (Amer, 2012)

2.3. Compare and Contrast IPv4 and IPv6

Even though NAT has helped in the reduction of the number of IP address (public addresses), it, however, possesses some performance and security concerns. Issues exist when it comes to peer to peer communication (Next Generation Internet, 2009).

Table 2 below highlights the major differences between IPv4 and IPv6 (Babatunde and Al-Debagy, 2014):

Table 2: Major difference between IPv4 and IPv6

Comparison of IPv4 and IPv6	
IPv4	**IPv6**
IPsec is not mandatory. Traffic to all host on the same subnet are sent via broadcast	IPsec is needed. Multicasts replace broadcast causing a decrease in broadcast floods experienced in IPv4

IPv4 utilises a 32-bit address space	IPv6 utilises a 128 bits address space hence it can accommodate more network IP addresses
Depending on IP header options, the header could have a variable length of between 20 to 60 bytes	IP header options are unavailable. Instead, it uses a fixed header of length 40 bytes
It needs to support DHCP, or it can be manually configured	It supports stateless automatic configuration., hence does not support manual configuration or DCHP (Amer, 2012)

3.0. Acme Ltd Scenario

Acme Ltd is a large conglomerate of companies with several branches in 10 different cities located in the United Kingdom specialising in selling household goods to its customers. Its staff strength is about 5000 employees. However, it intends to expand the company by including ten more branches and recruiting around 2500 employees. The present objectives of the business include:

- The company does not want to prevent increased costs on coping with the scarcity of address
- It wants to prevent disruption to the company websites
- It intends to grow its business to global business
- It intends to provide increasing experience to their customer and access to their supply chain.
- It intends to stand out in its competitive supermarket environment
- The company intends to use several advanced new software which is compatible with IPv6 that will boost sales
- The company intends to strengthen its internet security to prevent theft of valuable information.
- The day to day use of the link will be used predominantly for web browsing.

In this light, the company has currently exhausted its Public IP allocation and is wary of future scarcity to get new IP's and so is considering migrating its network to pure IPv6 or a mixture of both, even though it currently implements NAT.

3.1. Configuration Tools

As a result of networking systems being more expensive, hands-on experiments on networking simulation has become a key factor when choosing to try out new equipment, devices and technology before purchasing them in real life. OPNET has been chosen to model the Acme situation because it provides detailed analytical features. OPNET provides a Virtual Network Environment which can model the entire network of any enterprise including its switches, routers, servers, protocols and individual applications. Using this virtual environment makes it easy for network and system planners, IT managers, operations staffs and so on, to diagnose

difficult issues more efficiently and effectively. It can also help validate changes before the implementation of these changes, and with that, the server as a planner for future network enhancement (Hammoshi & Al-Ani, 2010).

OPNET provides the following benefits:

- It has a simple and yet convenient graphical user interface that is easy to learn
- There are excellent readme sample configuration tips in the examples folder already that ships with the software. There is also a good description of what each component means and what they support.
- OPNET has a large chunk of network components and is suitable to carry out research work on the network. Hence, it can be used to model the entire network of any organisation
- The Academic edition of the software is free which is what is used in this experiment
- The simulation engine is fast and takes a relatively short period to complete a network simulation
- It has a large user base that includes major fortune 500 companies

3.1.2 System Requirements

The installation of OPNET requires the following system configuration (OPNET Modeler Accelerating Network R&D, 2012):

- **Operating Systems**
  - **Microsoft:** Windows XP, Windows Vista Business, Windows 7, Windows Server 2003, Windows Server 2008. Can support both 32 and 64-bit variant of all these OS.
  - **Fedora Project:** Fedora Linux 6 (v2.6.18 Linux kernel)
  - **Red Hart:** Red Hat Enterprise Linux 4 (v2.6 Linux Kernel), Red Hat Enterprise Linux 5 (v2.6.18 Linux Kernel), Red Hat Enterprise Linux 6 (v2.6.32 Linux Kernel),
- **CPU**
  - **Required:** 2.0 GHz for Windows, 1.0 GHz for Linux using x86, EM64T, x86 AMD, or AMD64
  - **Recommended:** 3.0+ GHz using x86, EM64T, x86 AMD, or AMD64 (dual-core))

- **RAM**
  - **Required:**512MB
  - **Recommended:** 1-2GB
- **System File Space**
  - 3 GB is required for installation. The system also requires an additional 2 GB of free disk space
- **Working File Space**
  - It requires 100 MB or more for temporary and log files
- **Display**
  - Resolution: 1024x768 minimum

4.0. Building the Network Topology with OPNET Network Simulator

The Optimised Network Engineering Tool (OPNET), version 17.5 of the network simulation tool is used to run simulations on two of the office's location of Acme Ltd; this will indicate how the other office location will behave. The OPNET simulator tool can simulate and analyse the network performance parameters such as delay, packet loss, and HTTP web browsing. The major components used in the suggested network models running on OPNET 17.5 are 20 clients, 2 switches and 2 routers. The following are a description of each component extracted from the OPNET node model description, see Appendix E for details.

- The **ethernet4_slip8_gtwy** node model signifies an IP based gateway supporting four ethernet hub interfaces with eight serial lines interfaces. It represents a router that is connected to an IP network, using a PPP_DS1 in our case scenario
- The **Ethernet16_switch** represents a switch that supports up to 16 Ethernet interfaces. The Switch utilises the spanning tree algorithm in order to ensure a loop-free network topology
- The **Application Config** comprises a name and a description table which specifies various parameters for the different applications (i.e. HTTP Light, HTTP Heavy, Emails Heavy, Video Conferencing and so on).
- The **Profile Config** is used to create the profiles of users. It is possible to specify these user profiles on different nodes in the network to generate application layer traffic. This subject uses the applications that the Application Config defined to configure profiles. Traffic patterns can be specified. The configured profiles and the applications follow after.

- The **Ethernet_wkstn** node model represents a workstation with client-server applications running over TCP and UDP. The workstations support only one Ethernet connection at either 10 Mbps, 100 Mbps, or 1000 Mbps. A fixed amount of time is what a workstation requires to route each packet, as determined by the "IP Forwarding Rate" feature of this node. Packets are routed on FCFS (First come, first serve) basis. It might also encounter queues at the lower layers of the protocol inasmuch it depends on transmission rates of corresponding interface output
- The **10BaseT link**: -Links between hosts and routers or hosts and switch. Represents an Ethernet connection operating at 10 Mbps. It can connect any combination of the following nodes (except switch to router, which connect hub to hub or switch to switch or switch to the workstation.
- The **PPP_DS1**:- is used in connecting two nodes running IP together. In our case, this is the two routers in the two office location.
- **The ip32:-** Is an IP cloud that supports up to 32 serial line interfaces within a selectable data rate, where IP traffic can be modelled. It supports several protocols including RIP, IP, UDP, BGP, OSPF, IGRP and TCP

In the scenario below (Figure 1, see Appendix D for the configuration of the network), IP traffic was sent across the network. See Appendix F for traffic creation settings. The network simulation consists of a subnetwork in two of the virtual offices out of the possible ten offices connected via an IP cloud link through a PPP_DS1 link.

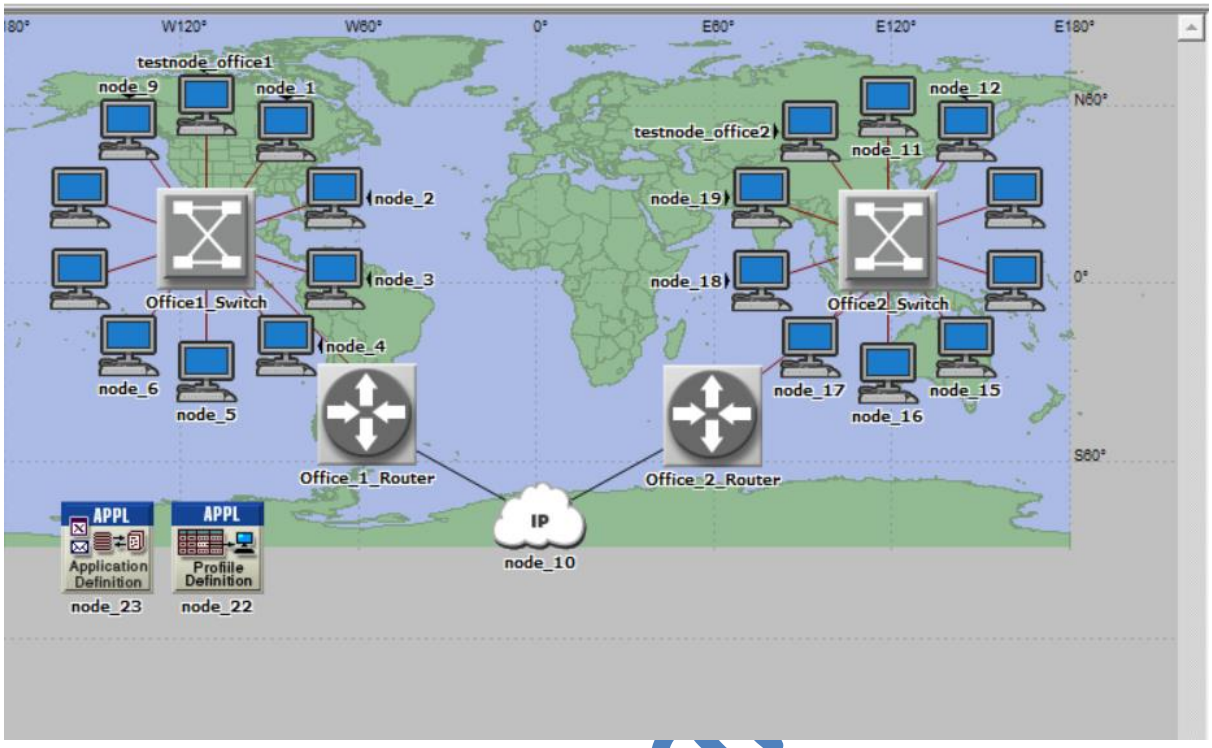


Figure 1: Office Network Configuration in OPNET

4.1. Simulation of a pure IPv4, pure IPv6 and IPv4 mixed with IPv6 with Tunnelling Network in OPNET

Three similar scenarios were created. The only difference between them is that the first network has IPv4 assigned to all devices. The second had IPv6 assigned to it, while the third had the office1_switch nodes running on IPv4. The Office_1_router is configured to tunnel the traffic from that subnet to the other office subnet, i.e. Office2_Switch with all the workstation and the Office_2_Router which are all running on IPv6. A third configuration was also done, which is a mixture of IPv4 and IPv6 network with Office1 running on IPv4 and Office2 running on IPv6. However, office2 has its router configured to tunnel traffic from IPv4 through the network (see Appendix D for full network configuration details). A simulation was run in OPNET, and the following parameters were measured and compared between the three scenarios. Our test will focus on IP unicast traffic passed through the network in different packets amount (see Appendix G for how this traffic was configured). We have configured OPNET to pull individual Global Statistics for the network for **HTTP**, **Ethernet** and **IP** (See Appendix J). We have also configured individual statistics for one node on each subnet, i.e**. testnode_office1** or **testnode_office2** to pull statistics on a workstation on each subnet (See Appendix I)

4.1.1. Experiment 1

This involves passing 10000 packets/seconds for 1 hour. We will compute the Global statistics for Ethernet, HTTP and IP.

Ethernet Delay: This represents the end to end packets received by all the workstations on the network.

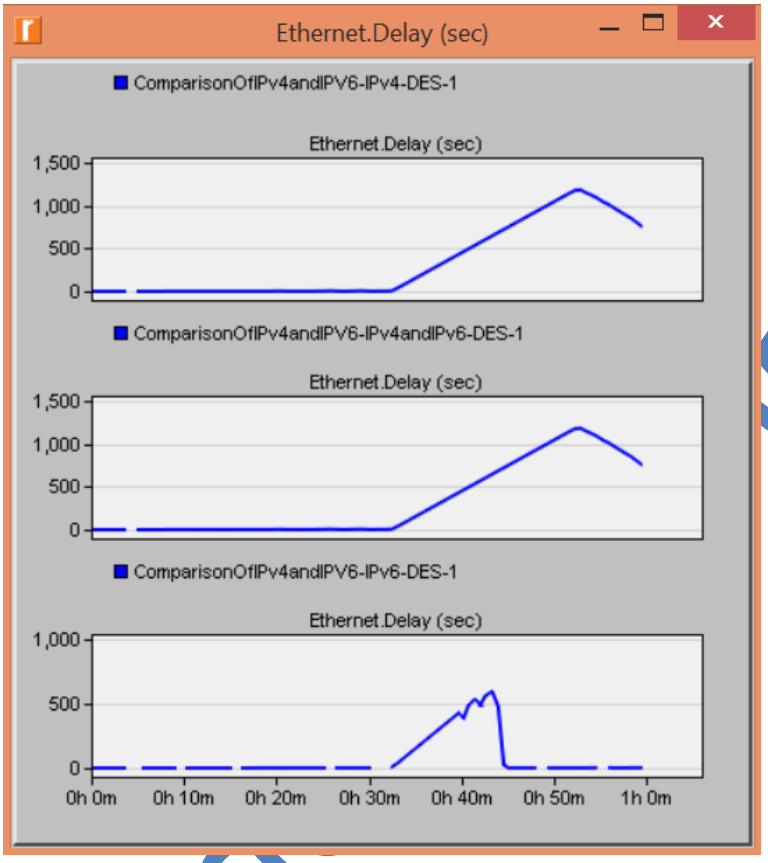


Figure 2: Network Ethernet Delay

- **Graph 1** is the Network Ethernet delay of IPv4
- **Graph 2** is the Network Ethernet delay of IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Ethernet delay of IPv6

From figure 2, the delay of IPv4 and IPv6 using tunnelling is similar to the delay experienced on a pure IPv4 network. It increased rapidly at about 30 minutes into the simulation and continued till 55 minutes before it started decreasing towards the end of the simulation. While the delay of IPv6 is considerably lower, approaching 500 seconds around 42 minutes and decrease towards zero at around

Page Response Time: This specifies the time that is needed to retrieve the entire page with all inline objects. If however, a page contains a video that is not preloaded, then the retrieval of this video is not taken into consideration.

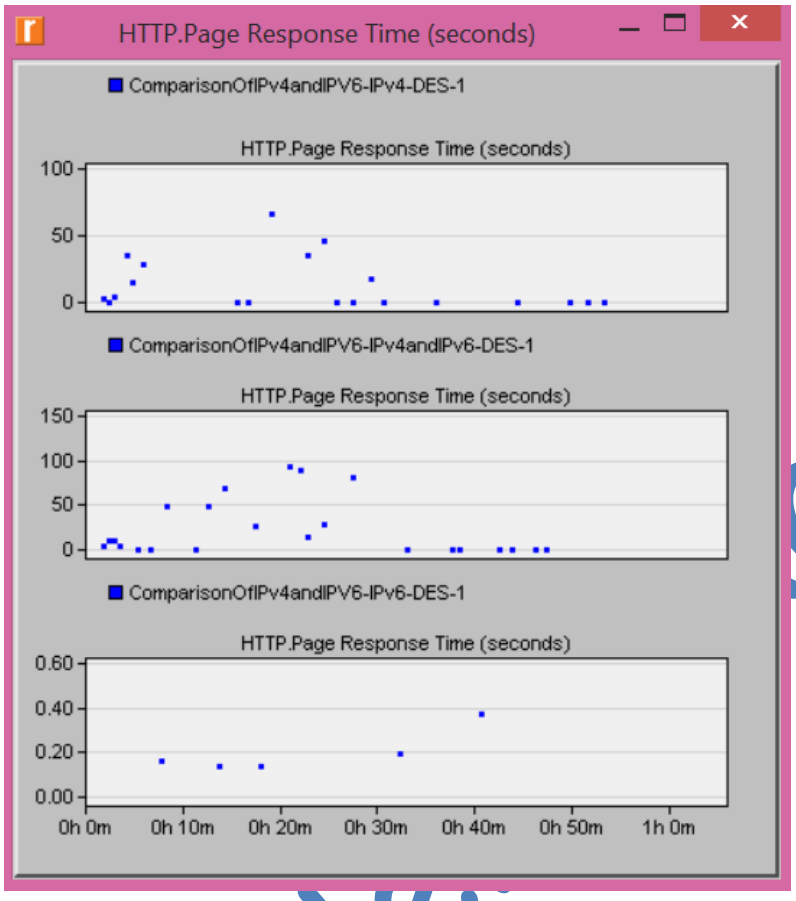


Figure 3: Network HTTP Page Response Time

- **Graph 1** is the Network Page Response Time of IPv4
- **Graph 2** is the Network Page Response Time of IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Page Response Time of IPv6

Figure 3 shows that the page response time is mostly at 0, but shoots up occasionally to as high as around 53 seconds for IPv4 graph. The value of the page response time for an IPv4 and IPv6 using tunnelling ranges from 0 to 50 seconds and then to 100 seconds occasionally. The page response time for a pure IPv6 Network hovers around 20 seconds and occasionally shut up to 40 seconds

Traffic Dropped: This is the number of IP datagram that is dropped in all nodes across the network amongst all IP interface. One of the reasons why this is possible is due to the exceeded

number of hops by an IP datagram. It could also be as a result of a lack of space in the central processor's queue.

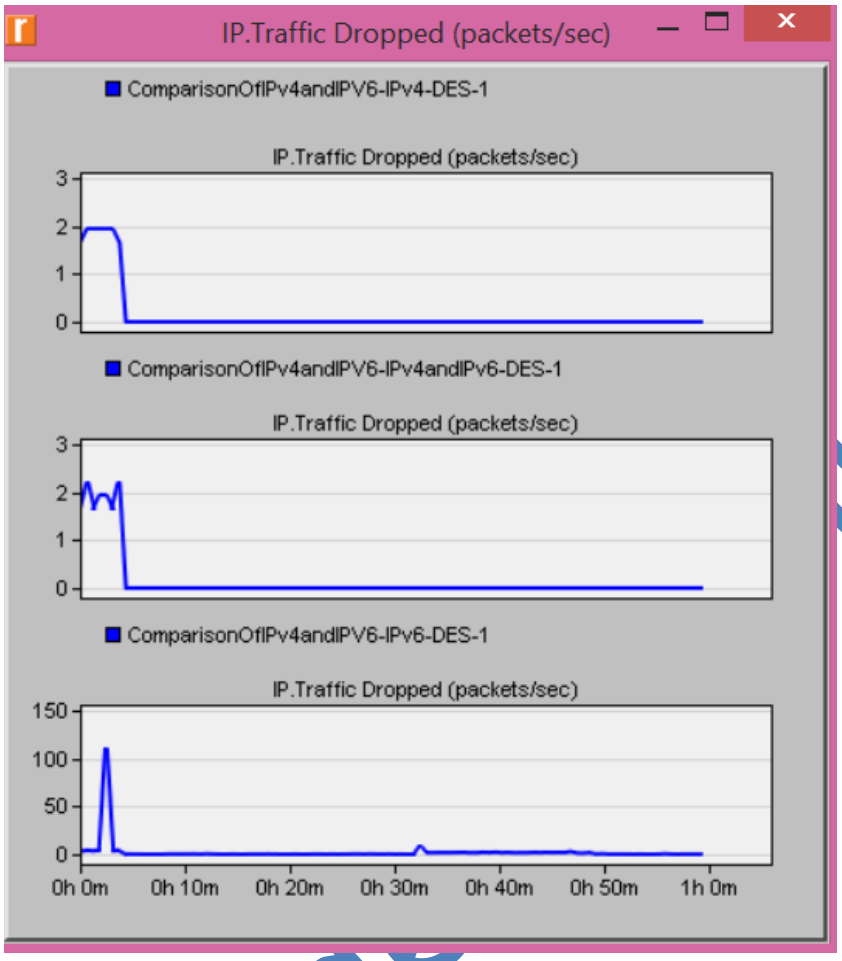


Figure 4: Network Traffic Dropped

- **Graph 1** is the Network Traffic Dropped for IPv4
- **Graph 2** is the Network Traffic Dropped for IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Page Response Time of IPv6

From figure 4, towards the beginning of the simulation, two packets were dropped per seconds, while a similar situation is observed in IPv4 and IPv6 network using tunnelling. The pure IPv6 did not drop any packet except around 3 minutes into the simulation where it dropped up to 100 packets. Lastly, the test node at both office exhibited similar behaviour to the global network statistics. E.g. Figure 5 is the Ethernet Delay of testnode_office2

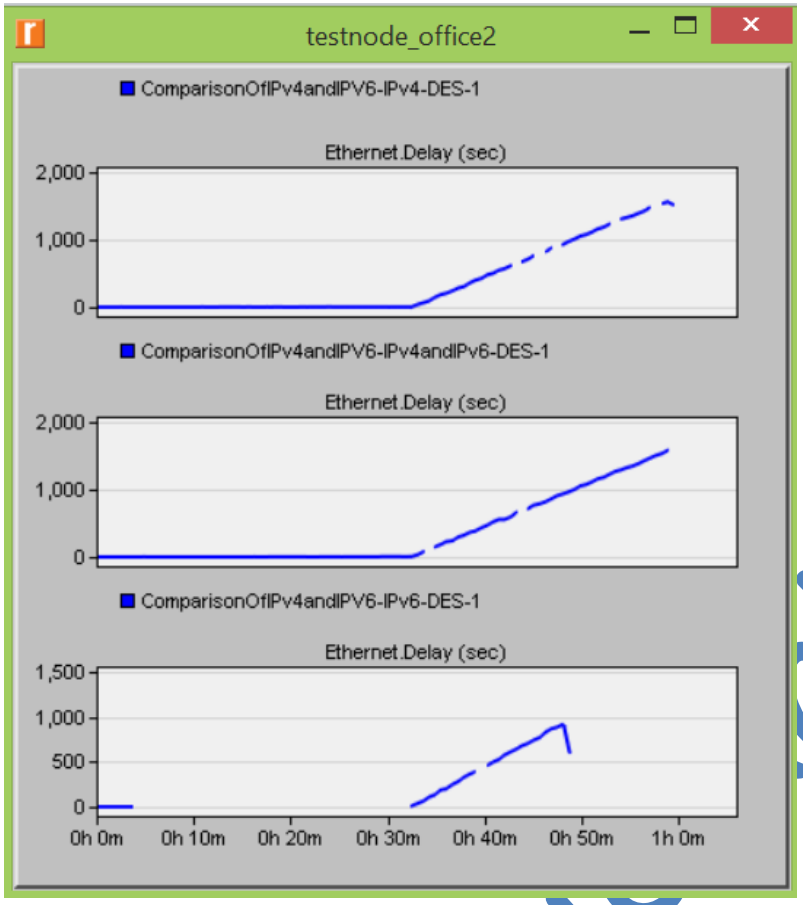


Figure 5: Ethernet Delay of testnode_office2

4.1.2. Experiment 2

In this simulation, we have doubled the number of packets passed across the network to 10000000 packets/seconds for 1 hour. We will compute the Global statistics for Ethernet, HTTP and IP.

Ethernet Delay:

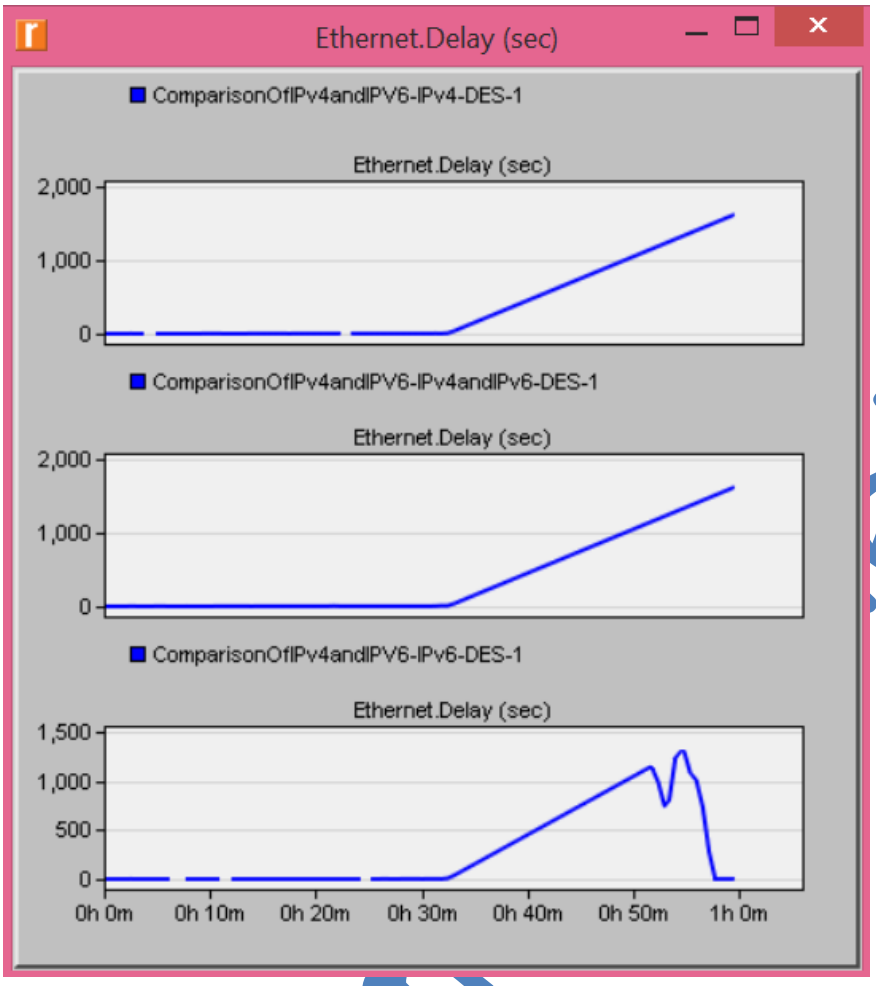


Figure 6: Network Ethernet Delay

- **Graph 1** is the Network Ethernet delay of IPv4
- **Graph 2** is the Network Ethernet delay of IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Ethernet delay of IPv6

Figure 6 shows that the delay of IPv4 and IPv6 using tunnelling is similar to the delay experienced on a pure IPv4 network increasing rapidly at about 30 minutes into the simulation and continued towards the end of the simulation. The delay of IPv6 is considerably lower approaching 500 seconds in about 42 minutes, and then increasing and approaching 1000 seconds before decreasing. In general, when compared to the first experiment, the doubling of the packets results in the overall Ethernet delay to be almost twice the delay from experiment 1 for all networks.

Page Response Time:

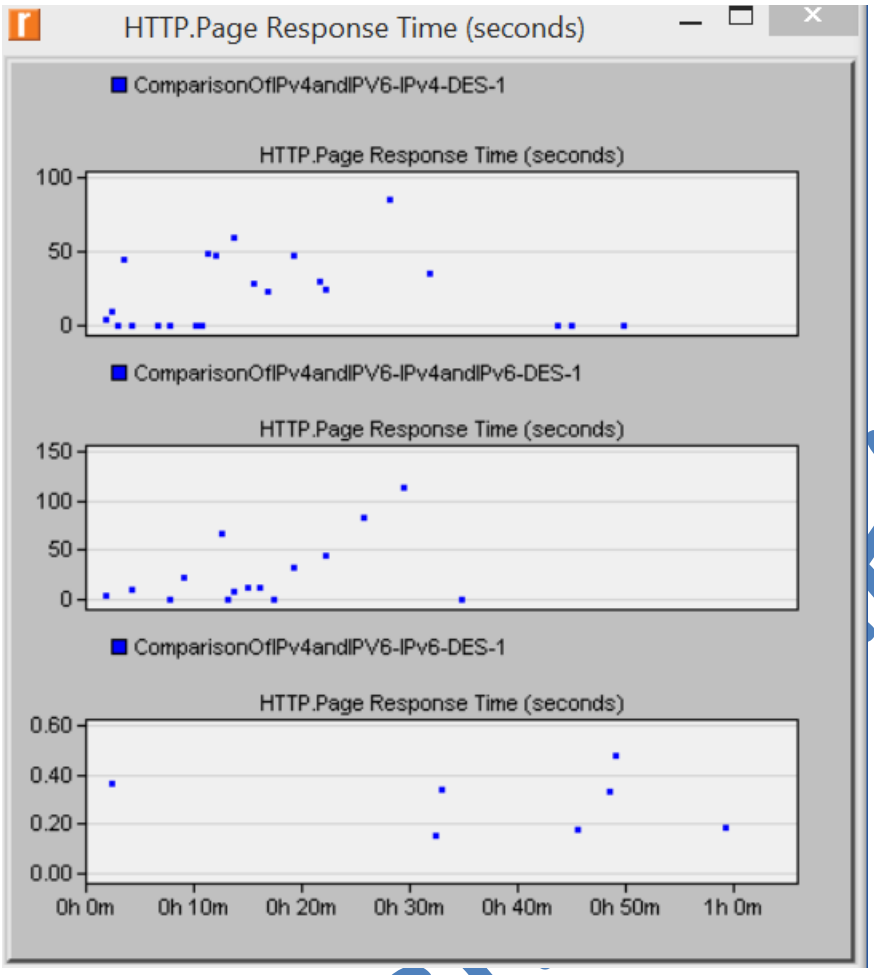


Figure 7: Network HTTP Page Response Time

- **Graph 1** is the Network Page Response Time of IPv4
- **Graph 2** is the Network Page Response Time of IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Page Response Time of IPv6

Figure 7 shows that the page response time varies randomly for IPv4 graph, tending towards 100 seconds on one occasion. The value of the page response time for an IPv4 and IPv6 using tunnelling ranges from 0 to 120 seconds occasionally. The page response time for a pure IPv6 Network hovers around 20 seconds and occasionally shut up to 50 seconds. In general, there was a slight increase in page response time for all networks.

Traffic Dropped:

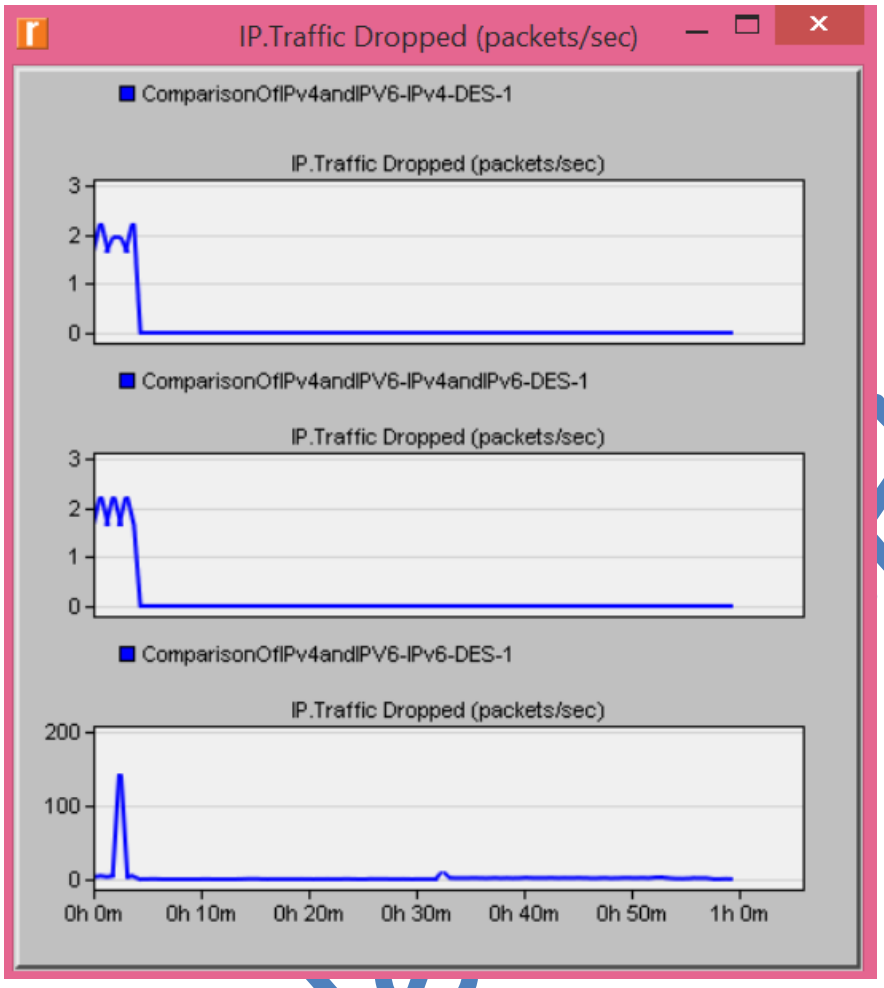


Figure 8: Network Traffic Dropped

- **Graph 1** is the Network Traffic Dropped for IPv4
- **Graph 2** is the Network Traffic Dropped for IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Page Response Time of IPv6

From figure 8 towards the beginning of the simulation, two packets were dropped per seconds for IPv4 network, while a similar situation is observed in IPv4 and IPv6 network using tunnelling. The pure IPv6 did not drop any packet except around 3 minutes into the simulation, where it dropped up to 100 packets. In general, the values was the same across when compared to the first experiment.

4.1.3. Experiment 3

In this simulation, we have tripled the number of packets passed across the network to 100000000000 packets/seconds for 1 hour. We will compute the Global statistics for Ethernet, HTTP and IP.

Ethernet Delay:

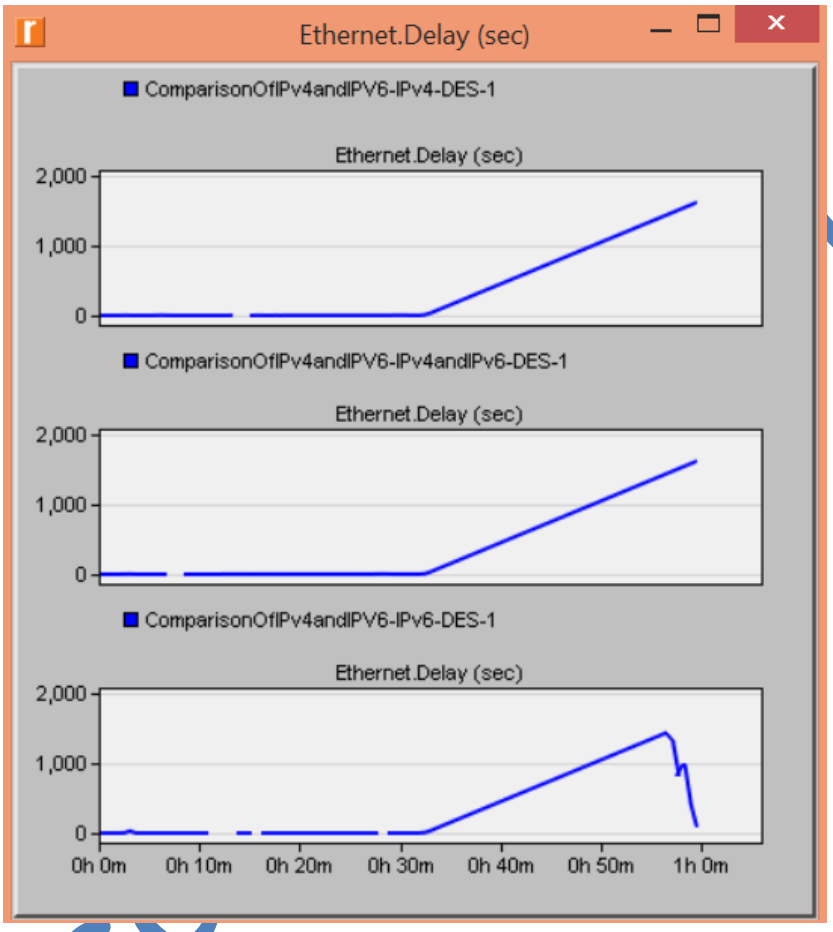


Figure 9: Network Ethernet Delay

- **Graph 1** is the Network Ethernet delay of IPv4
- **Graph 2** is the Network Ethernet delay of IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Ethernet delay of IPv6

From figure 9, there is no visible change from the last experiment for Ethernet delay. The graph looks identical to that of experiment 2.

Page Response Time:

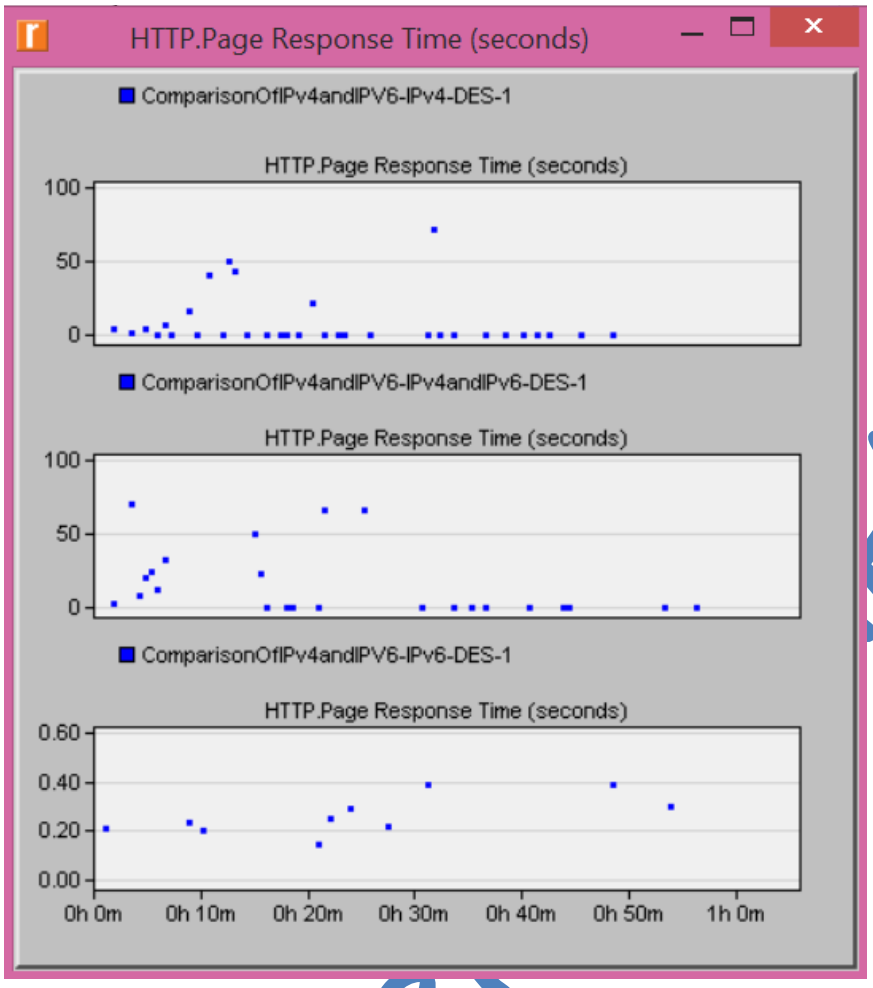


Figure 10: Network HTTP Page Response Time

- **Graph 1** is the Network Page Response Time of IPv4
- **Graph 2** is the Network Page Response Time of IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Page Response Time of IPv6

From figure 10, there is no significant change in the HTTP Page response when compared to experiment 2.

Traffic Dropped:

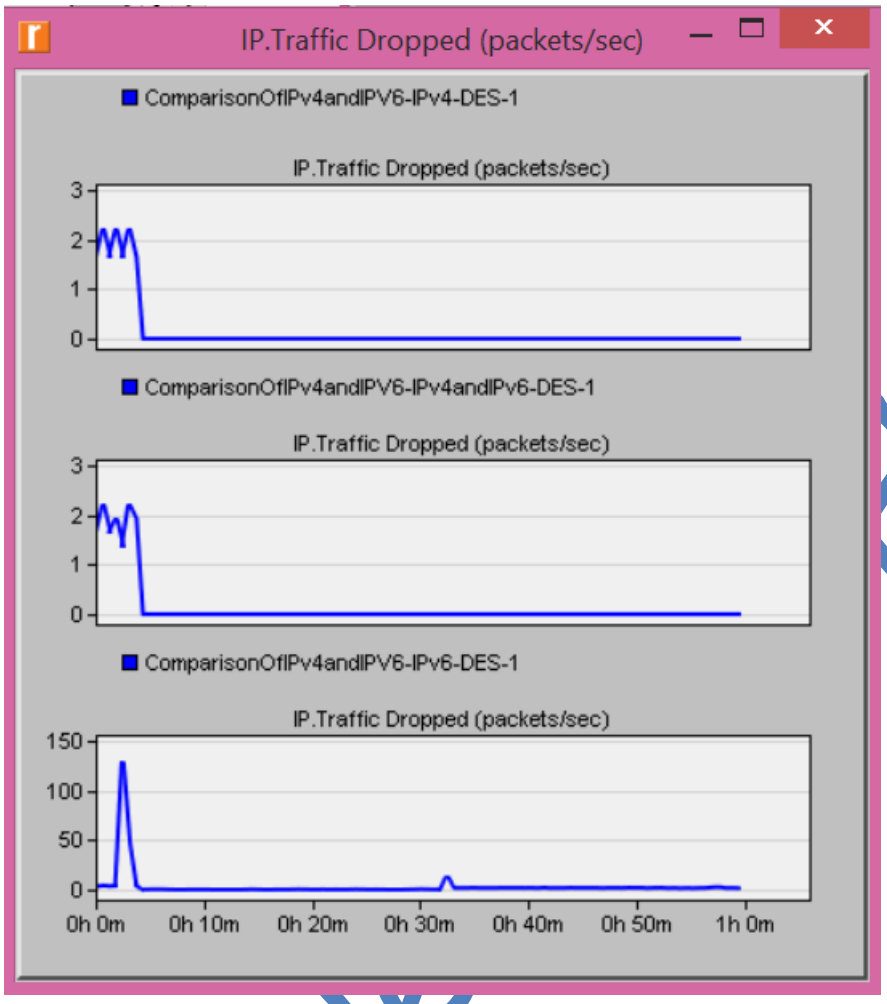


Figure 11: Network Traffic Dropped

- **Graph 1** is the Network Traffic Dropped for IPv4
- **Graph 2** is the Network Traffic Dropped for IPv4 and IPv6 using Tunnelling
- **Graph 3** is the Network Page Response Time of IPv6

From figure 11, there is no noticeable change in Network traffic dropped when compared to experiment 2.

4.2. Result Analysis

From the experiment conducted, it is evident that an IPv4 and an IPv4 and IPv6 using tunnelling, offer similar performance regarding Ethernet delay, Http Page Response and Traffic Dropped. We also observed that IPv6 offers better performance overall regarding this

parameters, IPv6 has the least Ethernet delay which might be due to its efficient packet header and its ability to prevent network flooding. The http response time is also impressive, and it might be due to its efficient header. Its packet drop is also lesser, which is down to the fact that it can prevent broadcast and does not have a Time To Live feature like IPv4. Acme Ltd can go ahead to migrate its network to IPv6 because it offers more performance benefits. The company might also choose to introduce IPv6 in phase in some of its offices without fear of massive degradation in performance, especially in web browsing.

4.3. Issues Arising from Network Design

The major issue I faced in this project was getting proper tutorials to implement what I wanted to do in OPNET. I did many testings. Some worked, and others did not. I however later found a video tutorial that gave the foundation of what I wanted to achieve. OPNET also come pre-installed with some set of examples and configuration tips which came in handy while developing my network.

5.0 Conclusions and Future Work

IPv6 is termed as the future of the internet, and within a short period, it will be the predominant addressing scheme on the internet. However, it is essential also to note that migrating from IPv4 to IPv6 will not happen overnight, and so there was a need to build IPv6 to coexist with IPv4. Tunnelling and dual stack technologies make this a reality. Acme Ltd is looking into the future and is considering moving to IPv6. The experiment conducted for Acme Ltd indicates that Acme can benefit from the better performances offered by IPv6, especially for web browsing. IPv6 is here to stay and should be adopted by Acme Ltd. Generally, in choosing to migrate to a pure IPv6 network or a mixture of both, the following need to be taken into consideration:

- There should be skilled network engineers to configure tunnelling which is also time-consuming
- Dual stack is easier as this requires little or no configuration
- Money is to be spent on new devices, especially when the network has old devices that do not support IPv6. Hence cost-benefit analysis needs to be done to see if the migration is worth it or not
- IPv6 offers excellent performance improvement than pure IPv4 or IPv4 and IPv6 network.
- Even though literature states that IPv4 and IPv6 with tunnelling lead to lower network throughput, our experiment shows that the difference between a pure IPv4 and an IPv4 and IPv6 is not grandiose.

The focus of this test is based on Ethernet parameters such as delay in packets and HTTP parameters such as Http Response time and IP parameter such as Traffic dropped. Acme Ltd's utilisation of video, voice, file transfer and so on, might increase in the future, and it will be also beneficial to conduct a performance test for the following traffic:

- Video Streaming Performance Testing
- Voice Streaming Performance Testing
- File Transfer Performance Testing
- Email Performance Testing
- Video conference Testing

- Other advantages of IPv6 such as traffic prioritisation could be tested for network performance
- Other IP4 and IPv6 mixture network such as dual stack could also be tested for network performance.

7.0 References

Amoss, J. and Minoli, D. (2008). *Handbook of IPv4 to IPv6 transition*. Boca Raton: Auerbach Publications.

Amer Nizar Abu Ali, "Comparison study between IPV4 & IPV6", International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.

Babatunde, O. and Al-Debagy, O. (2014). A Comparative Review Of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6). IJCTT, 13(1), pp.10-13.

Beijnum, I. (2006). *Running IPv6*. Berkeley, CA: Apress.

Boson (2014): Boson NetSim version 10 Official Website, http://www.boson.com/, last accessed: 05.12.2014

Deering, S. and Hinden, R. (1998). Internet Protocol, Version 6 (IPv6) Specification. Internet Protocol, Version 6 (IPv6) Specification. [online] Available at: https://tools.ietf.org/html/rfc2460.

Google.com, (2015). IPv6 – Google. [online] Available at: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption [Accessed 15 Jan. 2015].

Guo, Zhonghua; Zhu, Zhaowei; Chen, Renlin; He, Lihua, "Analysis and Research on Transition Proposal from IPv4 to IPv6 in Metropolitan Area Network," Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on , vol., no., pp.1,4, 21-23 Sept. 2012

Hagen, S. (2006), IPv6 Essentials, 2nd ed. USA: O'Reilly Media, Inc.

Hammoshi, Mayyada, and Razan Al-Ani. 'Using OPNET To Teach Students Computer Networking Subject'. Tikrit Journal of Pure Science 1.1 (2010): n. pag. Print.

Huitema,C .1996, "IPv6: The New Internet Protocol", Prentice Hall

Jiang Xie ; Narayanan, U. (2009), "Performance Analysis of Mobility Support in IPv4/IPv6 Mixed Wireless Networks", IEEE Transactions on Vehicular Technology, Volume:59 , Issue: 2 , Page(s): 962 – 973

Jinesh Doshi, Rachid Chaoua, Saurabh Kumar, Sahana Mallya, "A Comparative Study of IPv4/IPv6 Co-existence Technologies", University of Colorado, Boulder, May 2012.

Jivika Govil; Jivesh Govil; Kaur, N.; Kaur, H., "An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms," Southeastcon, 2008. IEEE, vol., no., pp.178, 185, 3-6 April 2008Minoli, D.

Kurose, J. F. and Ross, K. W. (2013),Computer Networking: A Top-Down Approach, Addison; Wesley

Leiner, B., Cole, R., Postel, J. and Mills, D. (1985). The DARPA internet protocol suite. IEEE Communications Magazine, 23(3), pp.29-34.

Li Zimu; Peng Wei; Liu Yujun, "An innovative Ipv4-ipv6 transition way for Internet service provider," Robotics and Applications (ISRA), 2012 IEEE Symposium on , vol., no., pp.672,675, 3-5 June 2012

Mun, Y. and Lee, H. (2005). Understanding IPv6. New York: Springer.

Next Generation Internet, "IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S.", IEEE-USA White Paper, 2009.

PTracer (2014): Cisco Packet Tracer Official Website, https://www.netacad.com/web/about-us/cisco-packet-tracer, last accessed: 05.12.2014

OPNET Modeler Accelerating Network R&D. 1st ed. 2012. Print.
R. Atkinson, S. Kent. Security Architecture for the Internet Protocol. RFC 2401, Internet Engineering Taskforce (IETF), 1998.

Rappaport,T.1996), "Wireless communications: principles and practice", prentice hall.

Ruiz-Sánchez, M.A.; Dept. of Comput. Sci., INRIA, Sophia Antipolis, France ; Biersack, E.W. and Dabbous, W. (2001) , "Survey and taxonomy of IP address lookup algorithms", IEEE transactions on Network, volume 15, issue 2, page(s): 8-23

Saurabh Dey and Shilpa N., "Issues in IPv4 to IPv6 Migration", International Journal of Computer Applications in Engineering Sciences, Vol. 1, Issue1, pp. 9-13, March 2011

S.Clement Virgeniya and Dr.V.Palanisamy, "Attacks on Ipv4 and Ipv6 Protocols and its Performance Parameters", International Journal of Computer Trends and Technology (IJCTT), Vol. 4, Issue. 8, August, 2013.

Shoch, J., "Inter-Network Naming, Addressing, and Routing," COMPCON, IEEE Computer Society, Fall 1978.

Tools.ietf.org, (2015). RFC 791 - Internet Protocol. [online] Available at: https://tools.ietf.org/html/rfc791 [Accessed 15 Jan. 2015].

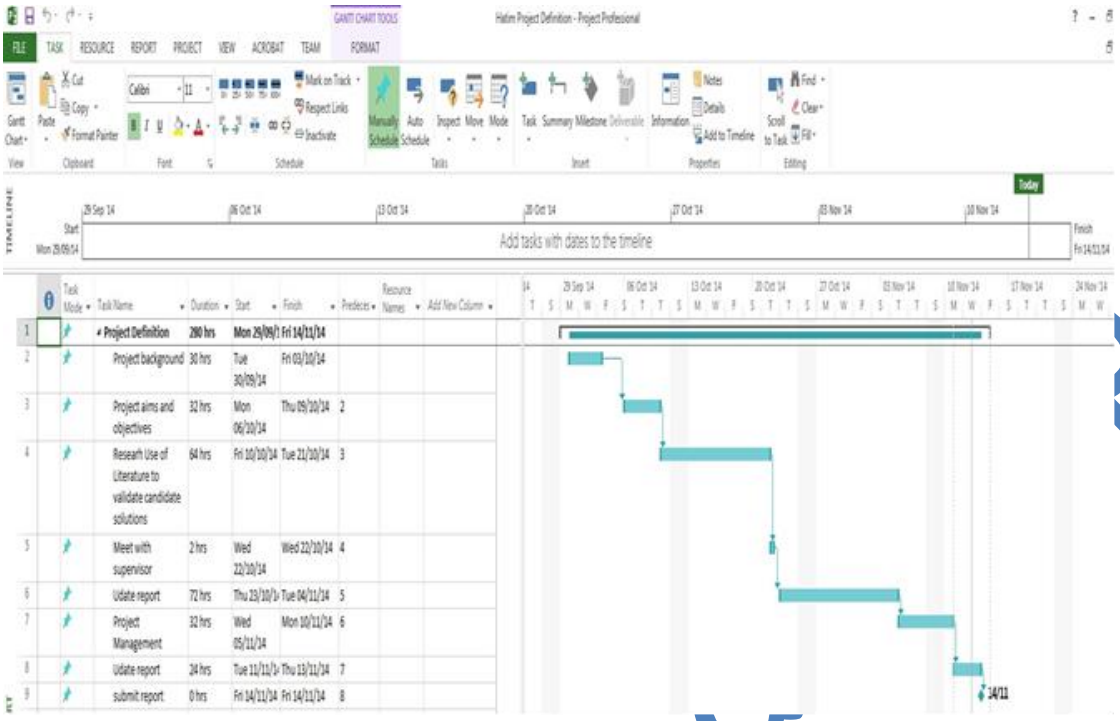
Vinton G. Cerf, "The Catenet Model for Internetworking," Information Processing Techniques Office, Defense Advanced Research Projects Agency, IEN 48, July 1978.

Vinton G. Cerf, Robert E. Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. 22, No. 5, May 1974 pp. 637–648

Waterfall Model, (2014). *Waterfall Model*. [Online] [Viewed 13 Nov. 2014].Available at: http://www.waterfall-model.com/

Wiljakka, J. ; Nokia Mobile Phones, Tampere (2002), "Finland Transition to IPv6 in GPRS and WCDMA mobile networks", IEEE Communications Magazine, volume 40, issue 4, page(s) 134-140

APPENDIX A: Old Gantt Chart



APPENDIX B: New Gantt Chart

	Task Mode	Task Name	Duration	Start	Finish	Predecess
1		**1 project Review**	**43 days**	**Thu 19/11/09**	**Sat 16/01/10**	
2		1.1 meet supervisor for feedback- update to phase 2	30 mins	Wed 19/11/14	Wed 19/11/14	
3		1.2 download and install Packet tracer	1 hr	Wed 19/11/14	Wed 19/11/14	2
4		1.3 technical knowledeg of IPV4 & IPV6	88 hrs	Wed 19/11/14	Thu 04/12/14	3
5		1.4 security Architecture of IP	64 hrs	Thu 04/12/14	Tue 16/12/14	4
6		1.5 Design network in Packet traces	7 hrs	Tue 16/12/14	Wed 17/12/14	5
7		1.6 start writing review report	12 days	Wed 17/12/14	Fri 02/01/15	6
8		**1.7 project progress**	**1 day?**	**Mon 05/01/15**	**Mon 05/01/15**	
9		1.8 use cisco packet tracer student version 6 -defined topology-PC-ROUTERS-TRANSLATION	1 day	Fri 02/01/15	Mon 05/01/15	7
10		1.9 implement the network	24 hrs	Wed 07/01/15	Fri 09/01/15	8
11		1.10 meet supervisor for feedback- update to phase 2	30 mins	Thu 08/01/15	Thu 08/01/15	9
12		1.11 update requirment-specification-show version-software version-update Gant chart-incloud previouse gantt chart	24 hrs	Fri 09/01/15	Tue 13/01/15	10
13		1.12 new update-incloude Access control-ACList-IPV4 ACL-IPV6 ACL	5 hrs	Thu 08/01/15	Thu 08/01/15	11
14		1.13 Recommendation-strangest-weakest protocol	16 hrs	Wed 14/01/15	Thu 15/01/15	12

		control-ACList-IPV4 ACL-IPV6 ACL				
14		1.13 Recommendation-strangest-weakest protocol	16 hrs	Wed 14/01/15	Thu 15/01/15	12
15		1.14 complete implementing in packet tracer	9 hrs	Thu 08/01/15	Fri 09/01/15	13
16		1.15 GNS3 Implemnte	3 days	Fri 16/01/15	Tue 20/01/15	14
17		1.16 final report draft	14 days	Tue 24/03/15	Fri 10/04/15	15
18		1.17 feedback	1 hr	Mon 13/04/15	Mon 13/04/15	16
19		1.18 final report deadline	0 hrs	Fri 08/05/15	Fri 08/05/15	17
20		1.19 poster day	1 hr	Wed 13/05/15	Wed 13/05/15	

APPENDIX C: Project Planning

Updated Risk table is provided in the table below.

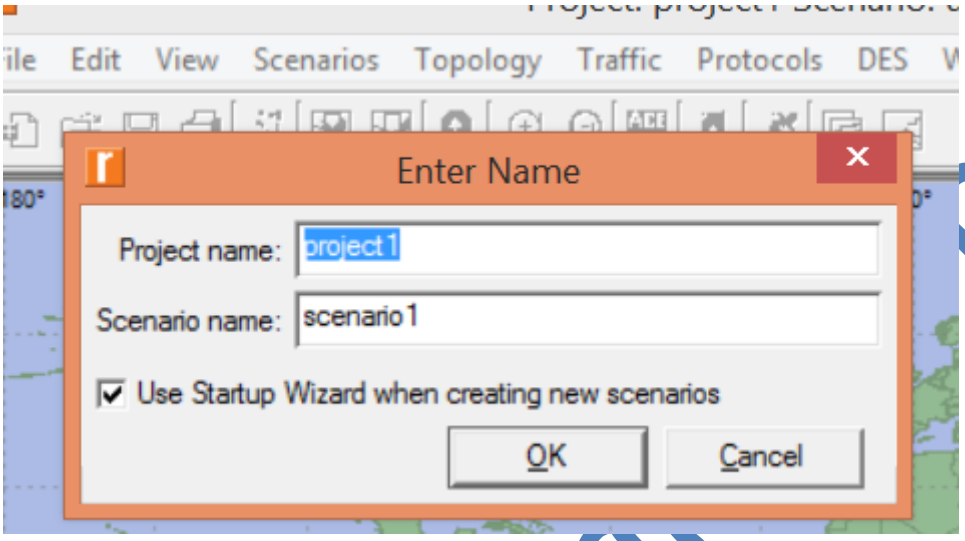
Risk Factor	Impact	Reason	Possible solution(s)
Simulation software(s)	Low	Conventional tools shall be used	-
Hardware	Low	No dedicated/ additional hardware is required	-
Health	Medium	unknown	If required, talk to supervisor for extension
Funding	Low	No additional hardware is required/ Library shall be used for research	-
Safety	Low	No construction or chemicals are involved	-
Time Schedule	Medium	Possible system crash etc.	If required, talk to supervisor for extension, backing up of data online.
Research related issues	Medium	Accessing necessary academic resources.	Using university library help desk
Installation issues	Low	Compatibility with the laptop for software	Finding the compatible version of the software for the laptop or approaching IT support desk in the university
Report writing issues	Low	Grammar check and proof reading	Approaching university international students proof reading desk

Contingency Plan: By ensuring that the plan is followed would make the project completion be on time, and also allowing extra one week will place the project one step ahead.

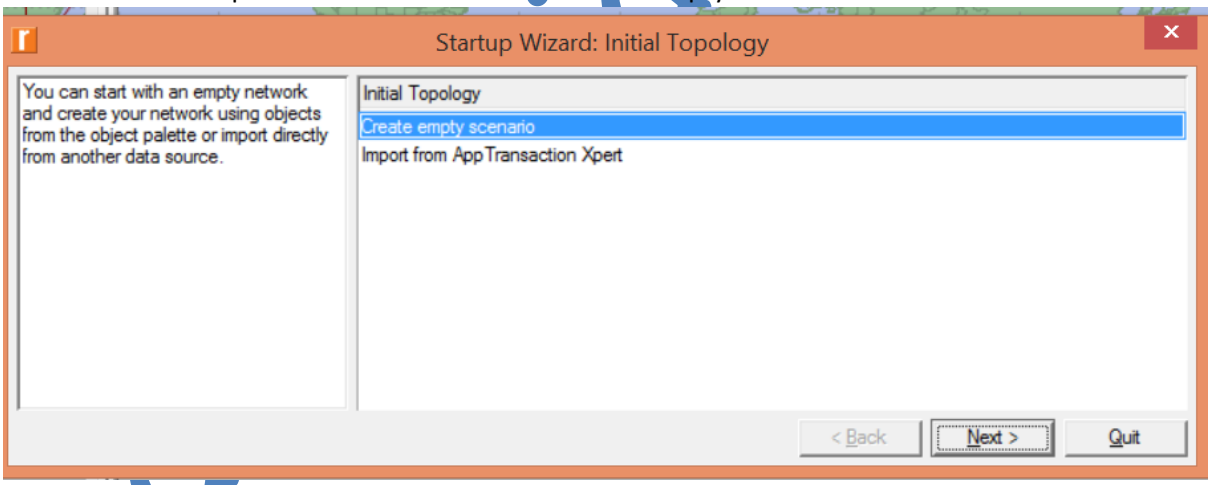
APPENDIX D: How the network was configured

After launching OPNET

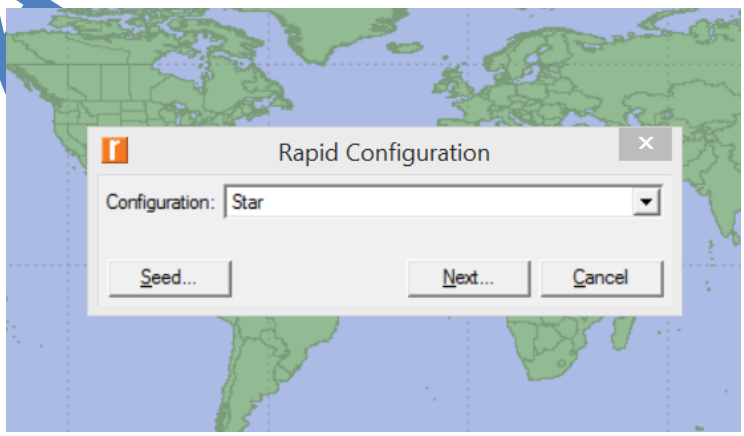
- Click on **File > New** to create a new project
- Enter a project name and Scenario name



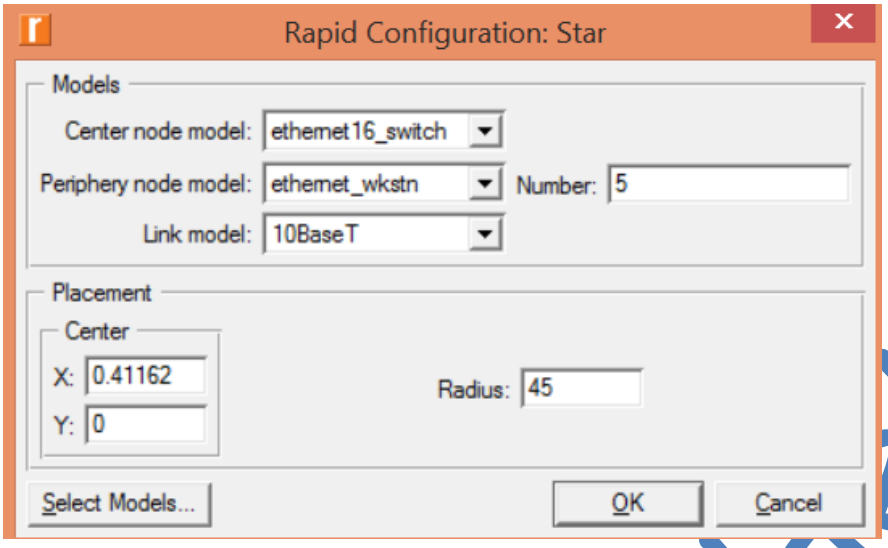
- Use the start-up wizard to create an empty scenario as seen below



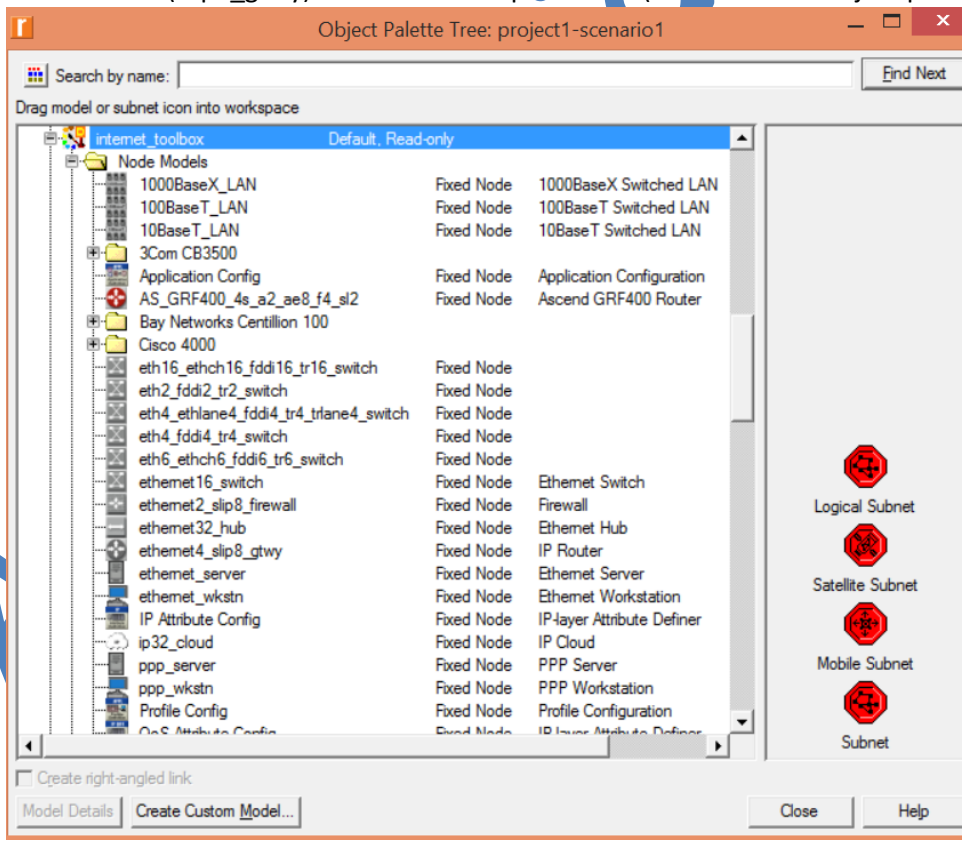
- Click **Next**, then choose next selecting the preselected values till the configuration finishes.
- To create the subnet, Click on **Topology** on the topmost menu, then **Rapid Configuration**, choose a start and click on **Next**



- Choose the following as seen below, then Ok.

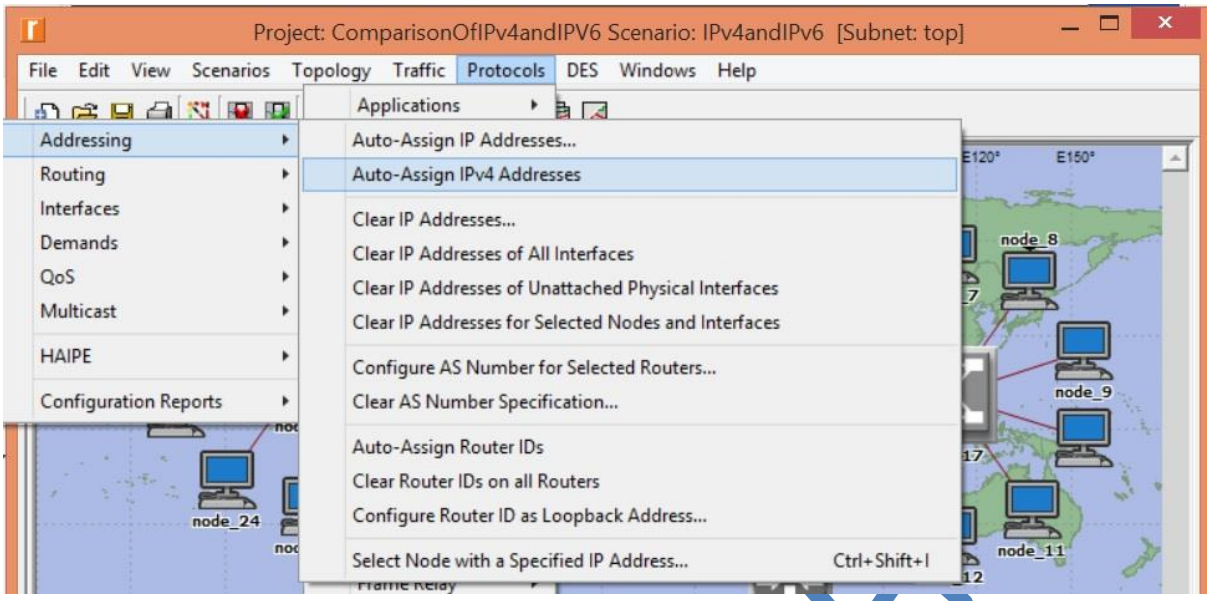


- To create an Ip32 cloud, Profile definition, Application Definition and Etherent4_slip8_gtwy, open the **Object Palette** by clicking on **Topology** in the first menu, then **Open Object Palette.** Note that this ought to be open by default.
- Locate a 10BaseT cable in the Object Pallete and drag from the subnet central 16 port switch to the router (slip8_gtwy) and also to the Ip32 cloud. (see below the object palette)

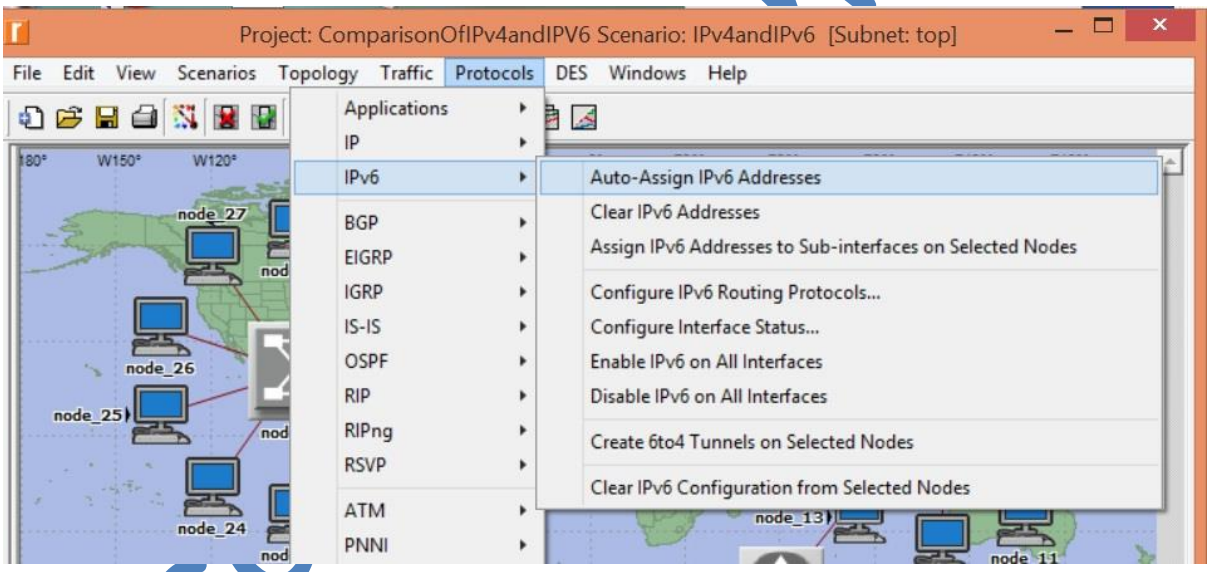


- See Appendix F, G, and H for how the application definition, profile definition and traffic configuration were done.

To Configure a Pure IPv4 network

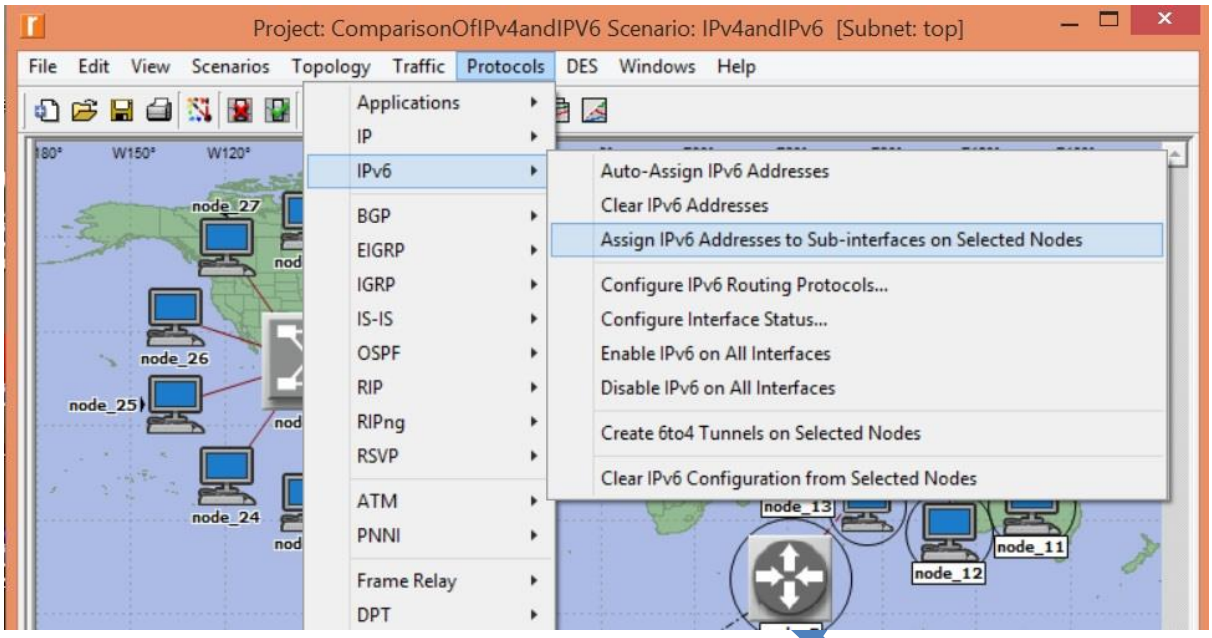


To Configure a Pure IPv6 network

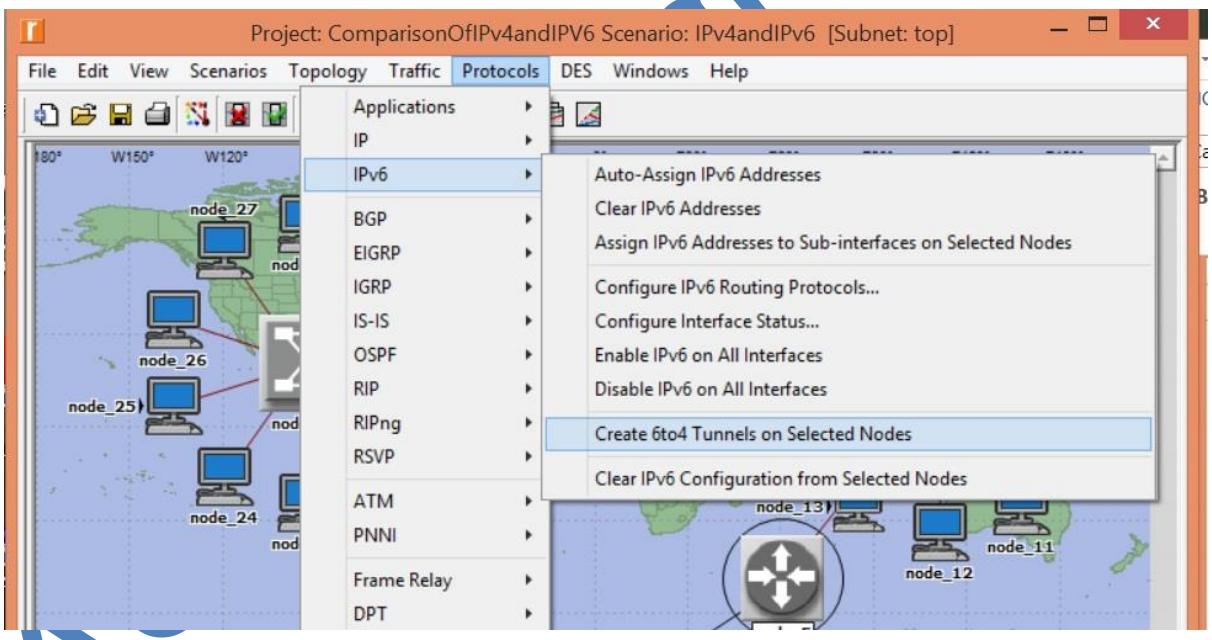


To Configure an IPv4 and IPv6 network via tunnelling

- Configure a pure IPv4 network as above
- Select all office 2 subnet by highlighting with the mouse and assigning IPv6 to that selected node as seen below:

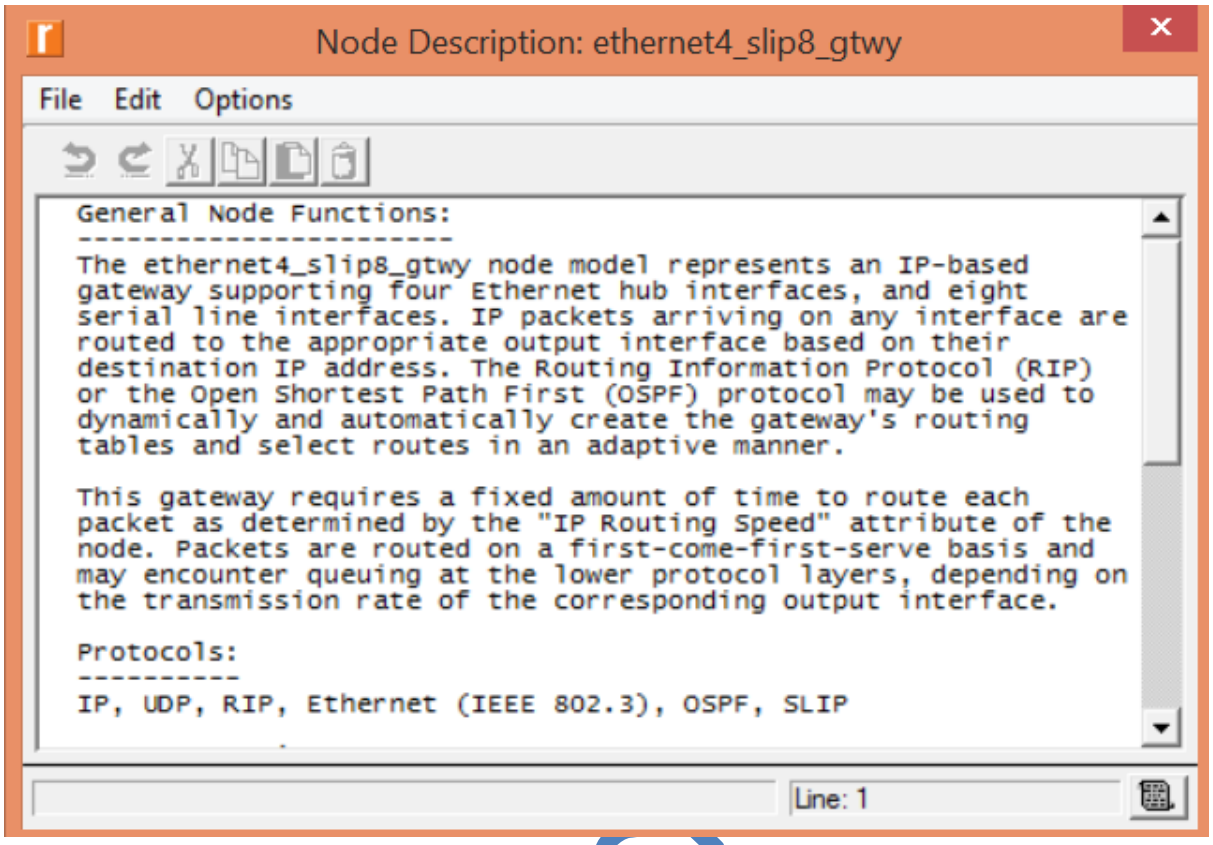


- Lastly, select office2 router and create a tunnel as seen below



APPENDIX E: Node model Description for ethernet4_slip8_gtwy

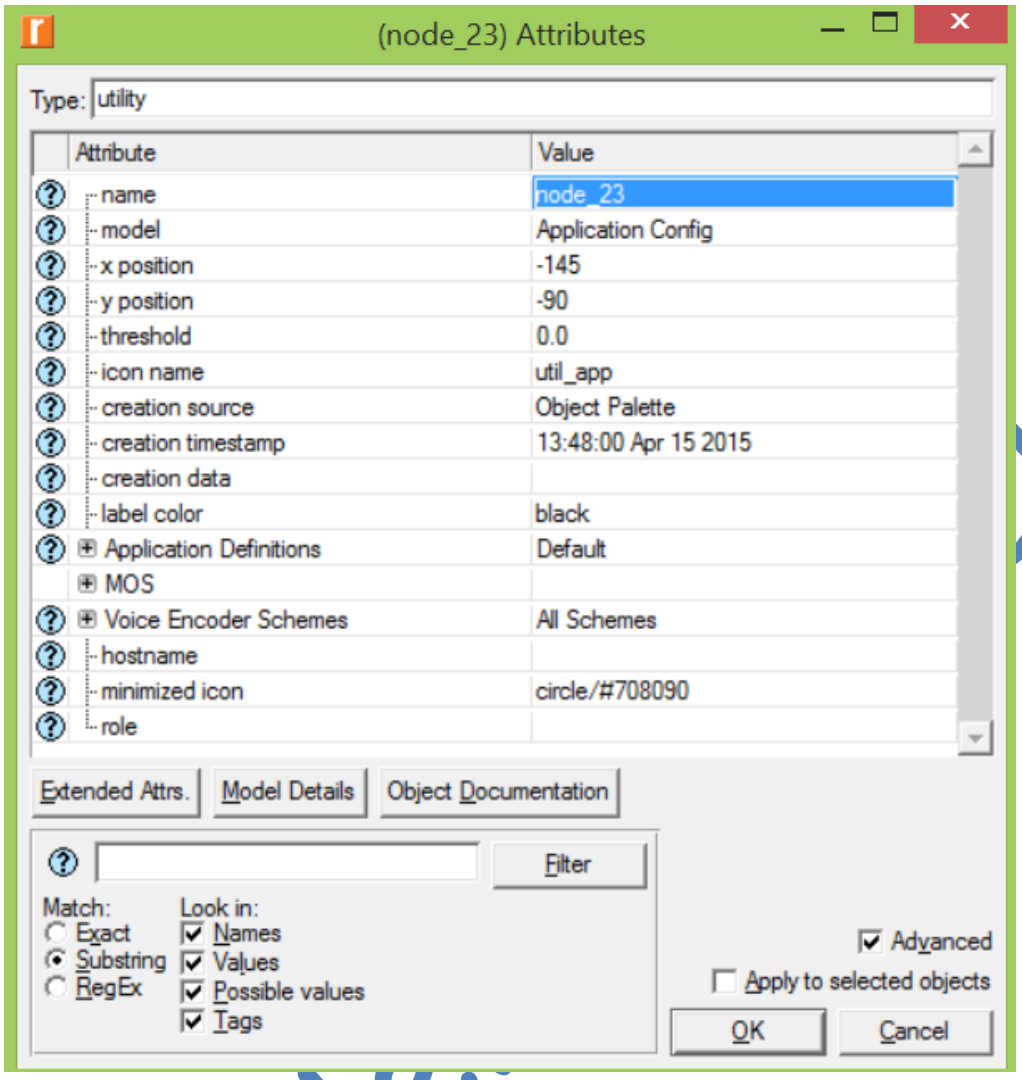
- Right click on the device and click on **View Node Description**



APPENDIX F: Application Definition

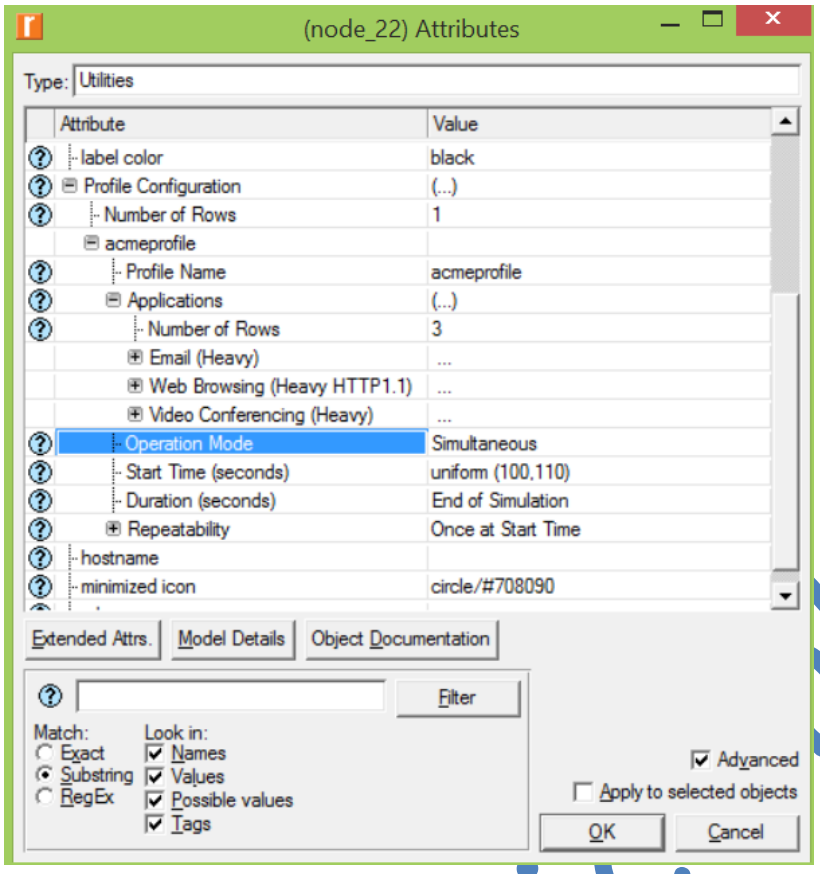
This is set to default as seen below, which means it supports all forms of traffic. To do this:

- Right click on the device and choose **Edit Attributes**
- Locate **Application Definitions** and choose **Default**

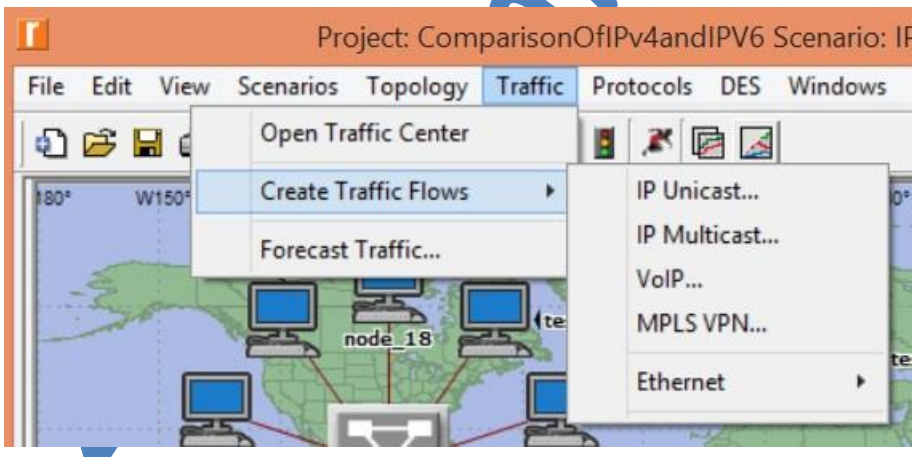


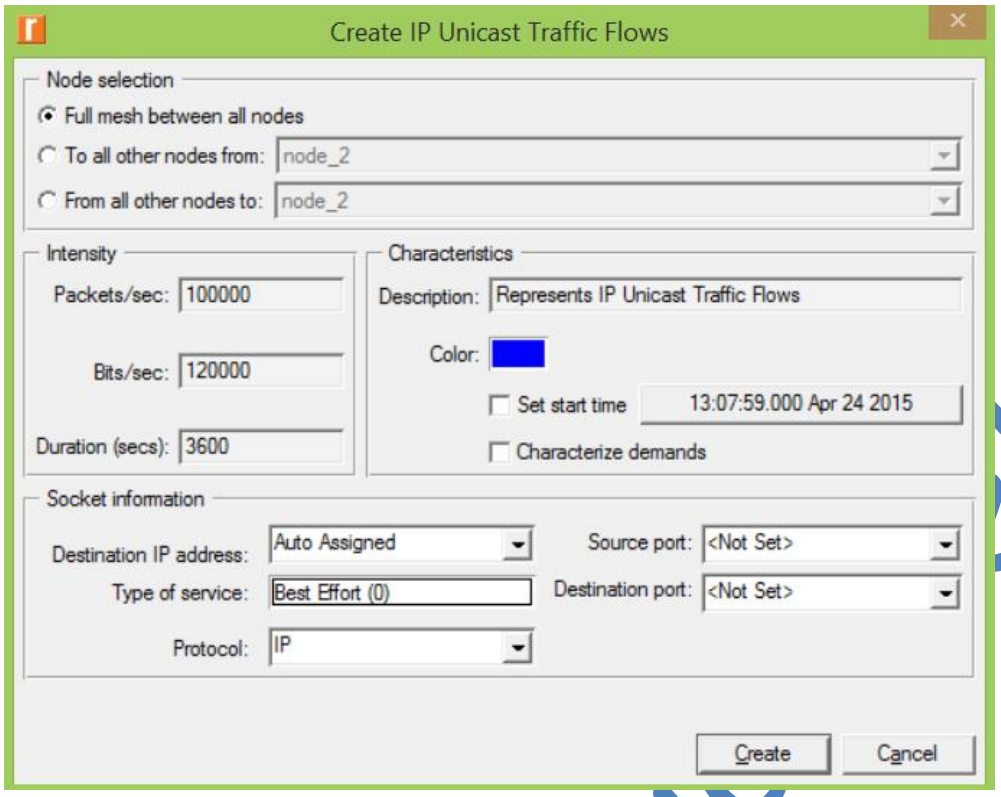
APPENDIX G: Application Profile Definition

- Right click on Profile Definition and Choose Edit Attributes
- Navigate to Profile Configuration and create a profile name and define some traffic to go along with this profile as seen below:



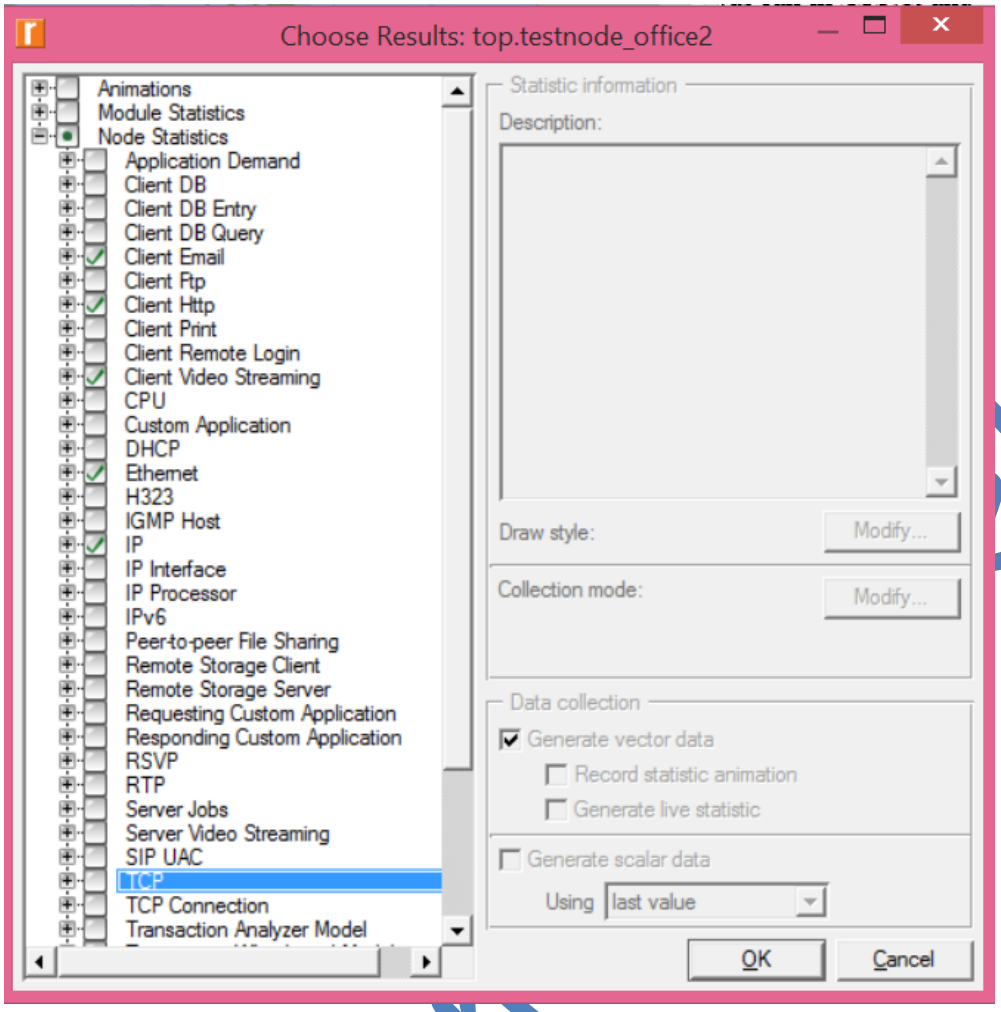
APPENDIX H: Creation of IP Traffic



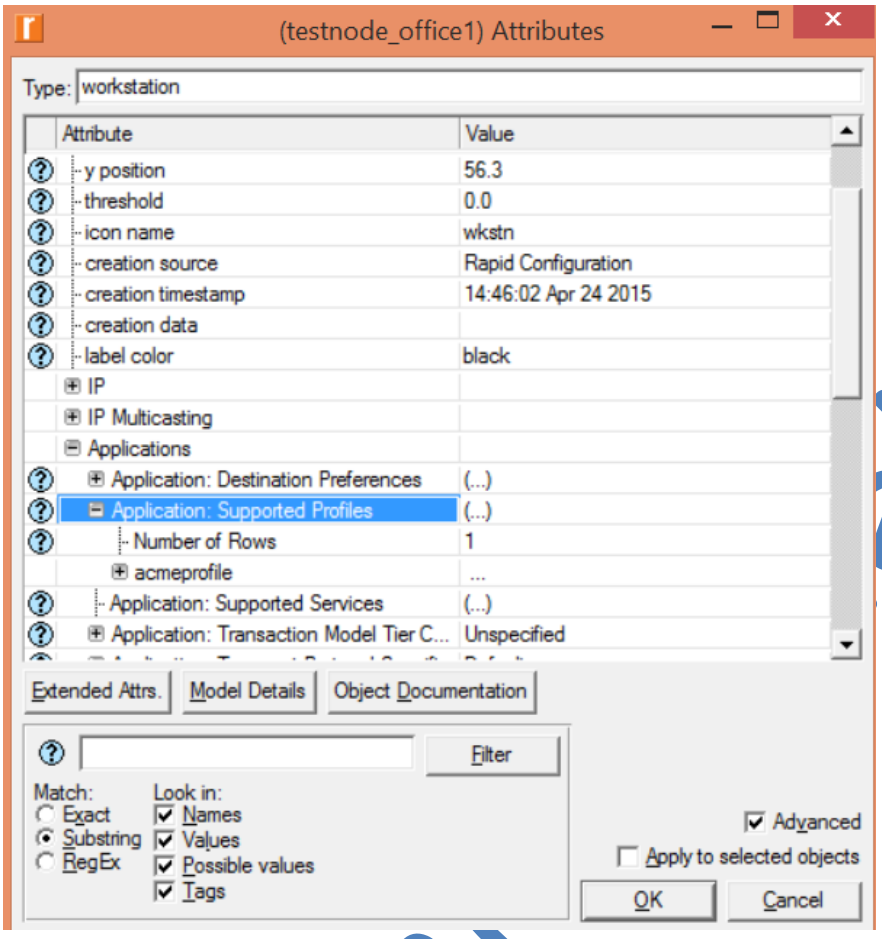


APPENDIX I: Collecting individual node statistics

- Right click on the device you wish to collect data for and select **Choose Individual DES statistics**



- Also in configuring individual statistics, the device needs to support the application profile definition we have created as seen below (here we used acmeprofile)


(testnode_office1) Attributes
Type: workstation
Attribute
Value
y position
56.3
threshold
0.0
icon name
wkstn
creation source
Rapid Configuration
creation timestamp
14:46:02 Apr 24 2015
creation data
label color
black
IP
IP Multicasting
Applications
Application: Destination Preferences
(...)
Application: Supported Profiles
(...)
Number of Rows
1
acmeprofile
...
Application: Supported Services
(...)
Application: Transaction Model Tier C...
Unspecified
Extended Attrs.
Model Details
Object Documentation
Filter
Match:
Exact
Substring
RegEx
Look in:
Names
Values
Possible values
Tags
Advanced
Apply to selected objects
OK
Cancel

APPENDIX J: Collecting Global Statistics

- Right-click anywhere apart from any device and select **Choose Individual DES statistics**