KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

DYNAMIC ROUTING IMPLEMENTATION DECISION BETWEEN OSPFv3 AND IS–IS FOR REAL–TIME APPLICATIONS IN IPv6 NETWORKS

BY

GIDEON EVANS NORVOR

(BSc. INFORMATION TECHNOLOGY)

PG2575314

A THESIS SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, COLLEGE OF SCIENCE IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF PHILOSOPHY

NOVEMBER, 2016.

DECLARATION

I hereby declare that this submission is my own work towards the MPhil and that, to the best of my knowledge, it contains no material previously published by another person, nor material which has been accepted for the award of any other degree of the University, except where due acknowledgement has been made in the text.

Gideon Evans Norvor	……	….....
(PG2575314)	Signature	Date

Certified by:

Dr. Michael Asante	……	….....
(Supervisor)	Signature	Date

Certified by:

Dr. J. B. Hayfron–Acquah	……	….....
(Head of Department)	Signature	Date

DEDICATION

Indeed “Jesus Christ is alive and victory is upon His shoulder”. I dedicate this thesis to the Almighty God for His non relenting grace and guidance throughout the period of execution of this work.

ACKNOWLEGEMENT

I hereby wish to acknowledge the good people who have contributed in diverse ways to make this thesis a success. First and far most is my supervisor, Dr. Michael Asante. This thesis will not have been possible without his fatherly love, help, patience and guidance. While working on this thesis, he kept me focused and helped me improve its quality by giving me directions and also providing invaluable feedback. Secondly, I wish to thank all lecturers at the Department of Computer Science–Kwame Nkrumah University of Science and Technology for their outstanding support throughout the entire degree programme. Finally, an endeavor of this caliber will never have been successful without the continual prayer and the support of the following: Prophet E. Gamel, Ms. Irene Yorm Letsa, Ms. Stella Norvor and Messrs, Alex Kofi Norvor, Bismark Bedzrah, Cartious Enyonyoge Aziedu, Brain Mensah, Godwin Awuitor, Thompson Bedzrah, Anokye Acheampong Amponsah, Oluwaseyifunmi Obaweya, Michael Osei–Boakye, Michael Darkwa and Sudi Logo Cornelius (Corney). I am indebted to you all. May God keep blessing you.

All those who are not mentioned here but have contributed in any way to make this thesis a success are affectionately acknowledged.

ABSTRACT

The current growth of the internet resulting in IPv4 address space exhaustion has given IPv6 the legitimacy and inevitability that cannot be ignored.IPv6 is the next–generation internet protocol developed to replace IPv4 in the future. IPv6 is an innovate step from IPv4. However, both protocols differ in header structure. The difference in header structure between the two protocols means that routing network traffic in IPv6 will no longer be supported by the conventional routing protocols used in IPv4. New routing protocols that are supported by IPv6 must be used. Also even though there are different IPv6 supported routing protocols, these protocols operate based on different routing algorithms and therefore differ in their routing characteristics. For instance not all routing protocols have the same scalability. Scalability of a routing protocol enables that protocol to automatically adapt to any change in network topology. For example when a new network is added to an existing network, dynamic routing protocols are able to discover the new network automatically. Also when there is a node or a route failure, they are able to determine alternative routes and retransmit traffic via these routes with minimal disruption. Routing protocol scalability is essential when considering current network growth rate. Therefore when deciding on which routing protocol to implement on a network, the protocol that scales well must be chosen. Choice of a suitable routing protocol for implementation does not only depend on routing protocol scalability. During this stage in the

network design, other factors are considered in order to select which protocol will be the most appropriate to route network traffic.These factors are usually considered on the basis of some parameters that are used to determine which protocol will perform better than others whenever there are different routing protocols available. The routing protocol with the best performance in terms of these parameters is considered the most suitable protocol and is selected for implementation. In this thesis, performance of two link state protocols for IPv6, OSPFv3 and IS–IS has been evaluated and compared for the most frequently used enterprise applications such as database query, remote login, file transfer, email and web browsing using Riverbed Modeler Academic Edition 17.5. Performance evaluation is based on network convergence duration, IPv6 packets dropped, throughput, link utilization, database query response time, remote login response time, file download/upload response times, email and http page response times as the main parameters. The main objective of this thesis is to simulate, compare and analyze the performance of both routing protocols in order to determine which protocol will be the more suitable one for routing network traffics in IPv6. The protocol which performed better than the other on the basis of the parameters used will then be recommended for routing network traffic in IPv6. In order to achieve this objective, the entire work was divided into two scenarios: OSPFv3 scenario and IS–IS scenario. The network topology used is a model of an IPv6 enterprise network. Scenario one is the OSPFv3 scenario. In this scenario, only OSPFv3 was configured and then simulated against the proposed parameters. Results obtained from the simulation was observed and recorded. Scenario two is the IS–IS scenario. This scenario is a duplicate of the OSPFv3 scenario but only IS–IS was configured in it. This scenario was also simulated using the same parameters used to simulate the OSPFv3 scenario. Results obtained from this scenario was also observed and recorded. After the simulation was performed for the IS–IS scenario, results obtained from both scenarios on the basis of the proposed parameters were compared and analyzed to determine which protocol performed better than the other. Overall, simulation results obtained have indicated that IS–IS performed better than OSPFv3 on the basis of most of the simulation parameters used.

TABLE OF CONTENTS

Contents **Page**

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ABR - Area Border Router

ARPANET - Advanced Research Project Agency Network

ASBR - Autonomous System Border Router

AS - Autonomous System

BDR - Backup Designated Router

BGP - Border Gateway Protocol

BR - Backbone Router

CIDR - Classless Inter–Domain Routing

CLNP - Connectionless–mode Network Protocol

CLNS - Connectionless–mode Network Service

CSNP - Complete Sequence Number Packet

CPU - Central Processing Unit

DBD - Database Description

DEC - Digital Equipment Corporation

DECnet - Digital Equipment Corporation Network

DHCP - Dynamic Host Control Protocol

DHCPv6 - Dynamic Host Control Protocol Version 6

DIS - Designated Intermediate System

DR - Designated Router

EGPs - Exterior Gateway Protocols

EIGRP - Enhanced Interior Gateway Routing Protocol

EIGRPv6 - Enhanced Interior Gateway Routing Protocol Version 6

ESs - End Systems

GUI - Graphical User Interface

ICMP - Internet Control Message Protocol

CHAPTER 1

INTRODUCTION

1.1 Background

The internet and all corporate networks are based on a standard network layer protocol referred to as the internet protocol (IP) that allows communication among heterogeneous networks. IP belongs to the TCP/IP protocol suite that is responsible for addressing and routing of packets between hosts and networks. The current version of IP that is widely used in the internet and private networks is known as Internet Protocol Version 4 (IPv4).

IPv4 was developed in 1980 to replace an already archaic NCP protocol that existed on the ARPANET. When IPv4 was first deployed, fewer than 1,000 computers were linked to it. The developers of the protocol did not imagine that its 32–bit address size will not be enough to cope with the current growth rate of the internet (Andress, 2005). Even though there were some techniques including Network Address Translation, which was used in an attempt to extend the dearth of its address size, IPv4 could still not be saved from address exhaustion problem. Besides its address space shortage, securing data within the IP layer, Quality of Service and mobility issues were other challenges faced in IPv4.

To tackle these limitations in IPv4 and to cope with the current growth rate of the internet, Internet Protocol version 6 (IPv6) was developed to replace IPv4. IPv6 is an innovative step from IPv4 but has several improvements over its predecessor. In IPv6, the total address space is extended from 32 bits to 128 bits, providing 2^{128} (about 3.4×10^{38}) IP addresses. This expansion in IP address space means that assigning IP address to devices on the internet can now be done with much flexibility. It has also eliminated the use of NAT, which is now widely adopted in an attempt to save IPv4 from address space shortage (Ali, 2012).

In addition to its larger address size, IPv6 also has other features that offer many advantages over IPv4. These are:

- **Quality of Service mechanisms**: Although there is type of service field included in the IPv4 header for traffic classification, traffics generated by different applications in current networks are treated the same way. This treatment is often called best–effort service. Best–effort service does not favor network applications whose transmissions are time bound. They are rather delayed leading to packet loss or jitter that reduces their quality (Bouras et al, 2006). The header of IPv6 is designed to include QoS mechanisms. Inside the header of IPv6 are the traffic class and the flow label fields that are intended for traffic classification in order to provide quality of service. With these two fields, nodes in IPv6 can distinguish certain packets so that routers can take special care of those packets (Cooper et al, 2005).
- **Stateless auto configuration**: Stateless auto configuration is an essential feature built into the next–generation internet protocol. Every device connected in an IP based network must be assigned an IP address. In IPv4, the task of assigning IP address is only done either manually or using a stateful protocol like the DHCP, which requires a server to store configuration information requested by a host. IPv6 also supports stateful auto configuration via the use of DHCPv6. In addition to this, IPv6 provides a stateless auto configuration allowing each network device to automatically acquire its IP address without the help of a server (Caicedo et al, 2009).
- **Mobile IP (MIP)**: The main purpose of this feature is to enable every mobile device to maintain its IP address while it moves from one network segment to another (Davies, 2003). Thus with the mobile IP, a mobile device can change its location and address without losing the connection through which it is communicating (Durgadi et al, 2010).

- **Simplified Header**: The header of IPv6 is simplified in contrast to the IPv4 header. The length of the IPv4 header is 20 bytes. However, its optional fields are variable in length. This adds to the actual size of the IPv4 header. The size of the IPv6 header is fixed. It is only 40 bytes. Also in IPv6, some fields used in IPv4 are removed. Removal of these fields makes processing of IPv6 header faster and improves overall router performance (Ferry, 2003). Figure 1.1 shows the header structure of IPv4 and IPv6.
- **Integrated Internet Protocol security (IPsec)**: Initially, Internet Protocol was not designed with security in mind (Kumar et al., 2011) therefore data was not protected in the IP layer. When data security became a major issue, different security techniques were developed but implemented in the upper layers of the protocol suite to protect data from unauthorized access. An example of this is the Secure Socket Layer (SSL) used to protect web data in the application layer. Besides SSL, other security technologies exist for the same purpose. The use of different security technologies in the upper layers for the same purpose means that security functionality is duplicated. To overcome this problem, a new security layer called IPsec was built into IPv6 to protect packets in the IP layer. IPsec protects packets by providing integrity, confidentiality, authentication and non–repudiation (Kent et al, 1998). Although IPsec can also be used in IPv4, it is optional but not mandatory as in IPv6. Also, when IPsec is deployed together with NAT, packet protection becomes difficult. With NAT the IP address and the port number of a packet must be changed and hence complete packet protection cannot be guaranteed. This can also lead to a compromise in end to end security deployment. In IPv6, the use of NAT is eliminated and so complete end to

  end security can be deployed without this issue. Also when the IP layer is protected, there is no need to protect packets in upper layers that might lead to duplicated security functionality (Blanchet, 2009).

Improvements in IPv6 packet structure makes it different from the packet structure of IPv4 and this means that routing IPv6 traffic will not be supported by older routing protocols used in IPv4 (Genkov, 2011). Also, considering the importance given to network scalability and reliability during routing protocol implementation, development of dynamic routing protocols supported by IPv6 became a necessity.

Routing protocols perform a vital job in every communication network. In an IP network, the major function of routing protocols is to forward packets received from one network node to another. Routing in a communication network refers to the transmission of data from source to destination by hopping either one hop or multiple hops (Kannagi et al, 2013). Routing protocols work by providing at least two services; selecting best paths between source and destination nodes, and successfully transmitting data to a specified destination (Lemma et al., 2009). Routing protocol is a combination of processes, algorithms, and messages that enable routers to exchange routing information. Based on routing algorithms, routing protocols are able to discover available routes, construct routing tables, take routing decisions, and exchange information with each other. The routing algorithms use different metrics based on some properties of a path which helps to determine the best route to reach a destination network.

When it comes to larger communication networks, dynamic routing is preferred over static routing. Both static and dynamic routing are just two ways by which routers can learn about remote networks. In static routing, each network location must be entered into the routing table by the network administrator. In dynamic routing, similar routing protocols are configured on routers to enable them discover remote networks. Both routing methods have their advantages and disadvantages. In a smaller network, updating routing tables will be easy for the network administrator. However, on a larger network, doing so will be very difficult and time consuming. Hence dynamic routing protocols must be used. Using dynamic routing protocols on larger networks saves time but it also consumes network resources. Dynamic routing

protocols are also more scalable; something that enables them to automatically adapt to any change in network topology. For example when a new network is added to the existing network, dynamic routing protocols are able to discover the new network automatically. Also when there is a node or a route failure, they are able to determine alternative routes and retransmit traffic via these routes with minimal disruption. Scalability is not the same for all routing protocols. Some protocols are more scalable than others. Routing protocol scalability is essential when considering current network growth rate. Therefore when deciding on which routing protocol to implement on a network, the protocol that scales well must be considered.

Routing protocols are grouped into two types. These are interior gateway protocols (IGPs) and exterior gateway protocols (EGPs). Interior gateway protocols are used to enable routers exchange routing information among themselves in the same autonomous systems (AS). An AS consists of a group of networks that are solely managed by a single organization. In an AS, information in a routing table is the same for all routers. RIPv1, RIPv2, IGRP, EIGRP, OSPF and IS–IS, all fall under IGP. Exterior gateway protocols on the other hand are used to enable different autonomous systems to communicate. An example of exterior gateway protocol is the border gateway protocol (BGP).

Interior gateway protocols differ in routing behavior and are further classified into Distance Vector Protocols, Link State Protocols and Hybrid Protocols (Kaur et al, 2014). Distance vector protocols determine best paths to a remote network on the basis of distance. Whenever a router forwards packets to another router, it is termed as a hop. The path that has the least number of hops to reach the remote network is taken as the best path. The vector points to the direction to reach the remote network. RIPv1, RIPv2, and IGRP all fall under distance vector protocols. Link state protocols operate on a different principle. They create three different tables which they use in their routing process. The first table is used to store all networks directly connected to the routers. The second table is used to store the map of the

complete internetwork. The third table is the routing table which is used to store the shortest path to reach all remote networks in the entire internetwork. The main distinction between these two routing algorithms is that in distance vector routing, the entire routing table content is exchanged between routers that are directly connected to each other whereas in link state routing, routers only share routing updates which contains the state of their own links with other routers in the network. OSPF and IS–IS are typical link state protocols. Hybrid protocols combine some routing characteristics of distance vector protocols and link state protocols. An example of hybrid protocol is EIGRP (Lammle, 2007).

The focus of this thesis is on two IGPs for IPv6. These are OSPFv3 and IS–IS. Both protocols are modified versions of OSPF and IS–IS supported in IPv4 and have been chosen for performance evaluation for routing some of the most frequently used applications in IPv6 networks.

1.2 Problem description

The current growth of the internet resulting in IPv4 address space exhaustion has given IPv6 the legitimacy and inevitability that cannot be ignored. IPv6 is the next– generation Internet Protocol, with a large addressing space, and will be used to replace the legacy IPv4 in the near future. Demand for IPv6 deployment is rising gradually and will no longer be an optional task but mandatory, especially for organizations that will require expansion in the future.

IPv6 was completely designed on the basis of IPv4. However, some existing features in IPv4 are replaced with newly enhanced features in IPv6, and this has changed the packet layout of IPv6 making it different from IPv4 packet layout. The difference in packet structure between the two protocols means that routing traffic in IPv6 will no longer be supported by conventional routing protocols used in IPv4; hence new routing protocols that are compatible with IPv6 must be used.

Besides, even though there are different IPv6 supported routing protocols like RIPng, EIGRPv6, IS–IS and OSPFv3 that keep track of routes in communication networks using different algorithms for better performance, when large networks increase, routed traffic also increases leading to a reduction in network stability. Routing instability is found to be one of the major causes of network degradation in internet service performance. For example any disturbance in a network within a few hundreds of milliseconds is sufficient to disrupt voice or video transmission during protocol convergence. Voice packets for instance can be lost, delayed or suffer from jitter causing the network to degrade in performance.

Therefore, to efficiently and effectively route data in communication networks, implementation of a suitable routing protocol is a critical success factor to achieve high performance.

In this thesis, performance of OSPFv3 and IS–IS has been evaluated and compared for some applications such as database query, remote login, file transfer, email and web browsing using Riverbed Modeler Academic Edition. Performance evaluation is based on network convergence duration, IPv6 packets dropped, throughput, link utilization, database query response time, remote login response time, file download/upload response times, email and http page response times as the main parameters. Both protocols use the same routing algorithm for optimal route selection within networks but have different routing characteristics. Hence understanding their routing behavior is very important in selecting which is the more appropriate to route traffic in IPv6 networks.

1.3 Research objective

The main aim of this thesis is to compare OSPFv3 and IS–IS and to evaluate their performance in order to determine which protocol is the more suitable one for routing network traffics in IPv6.

The objectives of this thesis are:

1. To identify and discuss the exclusive features of the selected routing protocols.
2. To implement the selected protocols in IPv6 network.
3. To simulate, compare and analyze protocol performance in the same network model based on some quantitative parameters.
4. To recommend which of the two routing protocols is more suitable to route traffic generated by some applications in IPv6 networks.

1.4 Research questions

With respect to the research objectives outlined, this thesis seeks to answer the following research questions.

1. Which protocol converges faster for the designed network model?
2. Which protocol dropped the least IPv6 traffic?
3. Which protocol has the highest throughput?
4. Which protocol recorded the minimum link utilization?
5. Which protocol performs better for the selected applications?

1.5 Research methodology

In order to accomplish the objectives of this thesis, the work is divided into two scenarios. The first scenario is a design of an IPv6 network model configured with OSPFv3. The second scenario is a copy of the first scenario but configured with IS–IS. The two scenarios are simulated and the impact of using each routing protocol separately to route the selected applications is observed and recorded. Performance evaluation of both routing protocols was done based on quantitative parameters stated in section 1.2. The simulation and analysis of results were carried out using Riverbed Modeler Academic Edition 17.5.

1.6 Research motivation

Although the transition from IPv4 to IPv6 is slow, the process is inevitable. As

preparations are being made for this biggest industrial shift in the history of the internet, it is imperative to know about the routing characteristics of the two link state protocols available for IPv6. Also, there is no perfect document stating clearly which of these two protocols is better than the other. While the developers of OSPF say it is the best among the two, developers of IS–IS equally argue that it is better than OSPF. These reasons have led to this research work that aims to compare both protocols on the basis of some of the most frequently used applications in communication networks.

1.7 Research contribution

This thesis contributes to ongoing research on the routing behavior of OSPF and IS– IS by comparing both protocols for the following applications in IPv6: Database query, ftp, remote login, email and http. Volumes of papers were published on the behavior of both protocols but most of the comparisons where done in IPv4. This thesis therefore creates a simulation environment that can be used to investigate the routing characteristics of both protocols for the selected applications in IPv6. Knowledge obtained from this thesis is aimed at helping network administrators and network engineers when deciding on which of these two protocols is more suitable for routing these applications in IPv6.

1.8 Scope of research

This thesis is a comparison between only two routing protocols supported by IPv6. These protocols are OSPFv3 and IS–IS. The comparison between these protocols was carried out by simulation. Riverbed modeler academic edition is the only simulator used. The main focus of this thesis is to investigate how the performance of these protocols affects some of the most frequently used network applications. The protocol that performs better than the other will be recommended for routing these applications. The major stakeholders targeted by this thesis are stated in section 1.7.

1.9 Research organization

This thesis is organized into 5 chapters as follows: Chapter 1 introduces the background of the thesis work. Chapter 2 is a survey of related literature. It also presents a detailed discussion of the two routing protocols in terms of their features, routing metrics and fundamental concepts associated to them. Chapter 3 covers the methodology. It proposes the network topology for the entire thesis work and also covers the simulation. Chapter 4 covers the analysis of the simulation results. Chapter 5 covers the conclusion of the thesis and recommendation. It also suggested a future study which could be done in this area.

IPv4 Packet Header

IP Version No.(4)	IHL (4bits)	Type of service (8bits)	Total Length (16 bits)	
Identification (16 bits)			Flags (4bits)	Fragment offset (12 bits)
Time to Live (8bits)	Protocol (8bits)		Header checksum (16 bits)	
Source Address (32 bits)				
Destination Address (32 bits)				
Options (variable)			Padding (variable)	

IPv6 Packet Header

IP Version No.(6)	Traffic Class (8 bits)	Flow Label (20 bits)
Payload Length (16bits)	Next Header (8bits)	Hope Limit (8bits)
Source Address (128 bits)		
Destination Address (128 bits)		

Figure 1. 1: IPv4/IPv6 Packet Comparison (Source: Adopted from Singhania 2015)

CHAPTER 2

RELATED LITERATURE

2.0 Introduction

This chapter is divided into two parts. The first part of the chapter enumerated the related works that have been done by some researchers to investigate the behavior of different routing protocols including OSPF and IS–IS. In order to get a better understanding of this thesis, the second part of the chapter is an overview of both routing protocols. It highlighted the features and the fundamental concepts of routing protocols upon which both OSPF and IS–IS are based.

2.1 Related works

As far as routing of different network applications are concerned, volumes of simulation experiments have been performed to investigate the routing behavior of different routing protocols with much of the studies being centered on OSPF, IS–IS, and EIGRP due to their scalability over other routing protocols. Oftentimes, simulation results show that EIGRP performs better than both OSPF and IS–IS. However, EIGRP is a proprietary protocol and does not support multi–vendor deployment. The choice is now left between OSPF and IS–IS because they are open standard protocols. Also, a survey of related works indicated that only little is done to compare these protocols in IPv6 even as the internet gradually transit towards the new generation internet protocol. These studies are recalled as follows:

Pandey et al. (2015) have performed a simulation based comparative study for OSPF, IS–IS, EIGRP and the combinations of EIGRP_IS–IS and OSPF_IS–IS using OPNET simulator. In their study, throughput, database, http object and email download response times were the parameters used to measure the performance of these protocols and their combinations. In all their five scenarios, simulation results show that the performance of the EIGRP_IS–IS protocol combination is better than the rest.

Roussinos (2014) also measured the performance of IS–IS and OSPF in a dual stack enterprise network using OPNET. The main parameters he used to measure the performance of both protocols were convergence duration, routing table size, end to end delay, jitter, and throughput. Results obtained from his simulation show that performance of IS–IS outweighs that of OSPF. Based on his findings, he concluded that IS–IS is a good choice for dual–stack enterprise networks than OSPF.

Kaur, & Singh (2014) have carried out a simulation based performance analysis of IS–IS, OSPFv3, and a combination of both protocols for IPv6 using OPNET. Their work consists of three scenarios on which IS–IS, OSPFv3 and the combinations of both protocols were configured respectively. End to end delay and variation in delay were the parameters used to measure the performance of the protocols. The network applications that were considered are voice and video. Results obtained from their simulation show that IS–IS performs better than OSPFv3 and the combination of both protocols for video end to end delay. For variation in delay or jitter, OSPFv3 performs better than IS–IS and the combination of both protocols. For voice end to end delay, the IS–IS_OSPF combination performs better than the two.

Farhangi et al, (2012) have also measured the performance of the combination of OSPF_IS–IS and EIGRP_OSPF_IS–IS for voice and video conferencing traffic using OPNET. Performance comparison of these protocol combinations was carried out based on convergence duration, jitter, end to end delay and throughput. Results obtained from their simulation indicated that while the OSPF_IS–IS combination recorded the minimum convergence duration, the EIGRP_OSPF_IS–IS combination has shown better performance on the basis of jitter, end to end delay and throughput for both applications. They therefore concluded that to achieve maximum network efficiency, a combination of three or more protocols should be used.

Thorenoor (2010) performed a comparative analysis on OSPF and IS–IS using OPNET. The main aim of his simulation experiment is to provide implementation criteria that should be considered when the choice is between OSPF and IS–IS. He divided this work into two scenarios configured with OSPF and IS–IS respectively. To measure the performance of both routing protocols, router convergence time, bandwidth utilization, throughput and queuing delay were the parameters used. Results obtained from her simulation have shown that the IS–IS network outweighed the OSPF network in terms of all the simulation parameters used.

In this thesis, performance of OSPFv3 and IS–IS have been measured in IPv6 network for some enterprise applications. Performance evaluation was carried out on the basis of network convergence duration, IPv6 traffic dropped, throughput, link utilization, database query, remote login, Http page, and email download/upload response times.

2.2 Overview of OSPFv3 and IS–IS

OSPFv3 and IS–IS are link state protocols and have some similarities but differ in routing behavior. Both protocols use the same routing algorithm to determine the shortest paths to all destinations within a network. While OSPF was natively developed to route datagram in IP, IS–IS was natively developed for ISO CLNS environments but was later adopted by IETF to support routing in IP (Kaur et al., 2014). Both routing protocols have now become popular due to the widespread adoption of IP.

2.2.0 Open shortest path first version 3 (OSPFv3)

OSPFv3 is the modified version of OSPF that is used to support routing in IPv6. In OSPFv3, some basic techniques used in OSPF are still maintained. These techniques include designated router election, flooding, shortest path first calculation, and area support. While these basic mechanisms are still maintained in OSPFv3, some necessary changes have also been introduced because of the difference in protocol structure between IPv4 and IPv6.

(Coltum et al, 2008). OSPF was developed by the IETF in 1987. The version now used in IPv4 is OSPFv2. It was published in RFC 2328. OSPFv2 was later updated to OSPFv3 to support IPv6. OSPFv3 was release in 1999 and was published in RFC 5340. OSPFv3 is a link state protocol which works by using Dijkstra's algorithm to determine the shortest path to a destination within a network. To determine the shortest path to each destination, OSPFv3 first constructs a shortest path tree from the network. The shortest path tree contains all paths leading to remote networks. From the shortest path tree, OSPFv3 then selects all resulting best paths and use them to populate its routing table (Lammle, 2007). OSPF supports hierarchical network design, enabling network designers to separate larger networks into smaller ones called Areas. Separating larger networks into areas minimizes the amount of routing information that can be propagated at a time. This reduces convergence time of the network. Also, when any fault occurs in the whole network it can be traced to each area within the network (Lammle, 2007). OSPFv3 is not a proprietary protocol but an open standard routing protocol implemented by different network vendors.

2.2.1 Changes for OSPFv3

As discussed by Teare (2010), one of the major changes introduced in OSPFv3 is that the protocol's header has been redesigned. The header is no longer complex as compared to the header in OSPFv2. The header now includes an instance ID field. Routing in IPv6 is done on a per–interface basis not on per–subnet. Each IPv6 routing protocol is more concerned about the link on which it is configured but not the subnet. The addition of the new instance ID field to the protocol structure therefore makes it possible for several OSPFv3 instances or addresses to be enabled on the same link. By default, instance ID is 0. When there is an additional instance, it is increased. Each OSPF instance is assigned a separate instance ID. Also, instance ID has local link significance only. This means that before OSPFv3 routers can become neighbors,

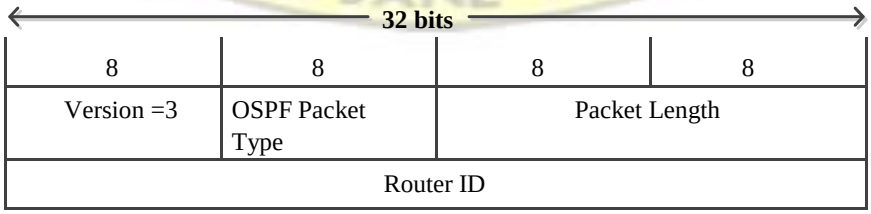
they must have identical instance IDs. For example, if a router receives a packet whose instance ID is not the same as its own instance ID, it simply discards the packet.

Additionally, because the OSPFv3 header has been redesigned its hello packet structure has also been changed (Coltun et al, 2008). As discussed by Teare (2010), the changes made to the OSPFv3 include the following:

- In OSPFv3, the multicast addresses reserved for all SPF or link state routers and all designated routers are now FF02::5 and FF02::6 respectively; they are no longer 224.0.0.5 and 224.0.0.6 as used in OSPFv2 for IPv4.
- The packet header of OSPFv3 is not designed to include IPv6 addresses. Rather, IPv6 address is carried inside the payload of the link state update packet.
- In OSPFv2, network LSAs carry IPv4 addresses but in OSPFv3, network LSAs do not include IPv6 addresses.
- To configure OSPFv3 on routers, the router ID must be enabled before routing can start.
- In OSPFv3, identification of the designated router and backup designated router is done with the router's ID; not with its IP address as in the case of OSPFv2.

Also, another notable change for OSPFv3 is the security mechanism it uses to protect its routing information. In OSPFv2, Message Digest 5 is the main security technique used to secure routing information. However, in OSPFv3 this is not used. Securing routing information in OSPFv3 is done by using IPsec found in the IPv6 protocol (Wen et al, 2010).

Figure 2.1 shows the OSPFv3 packet structure.



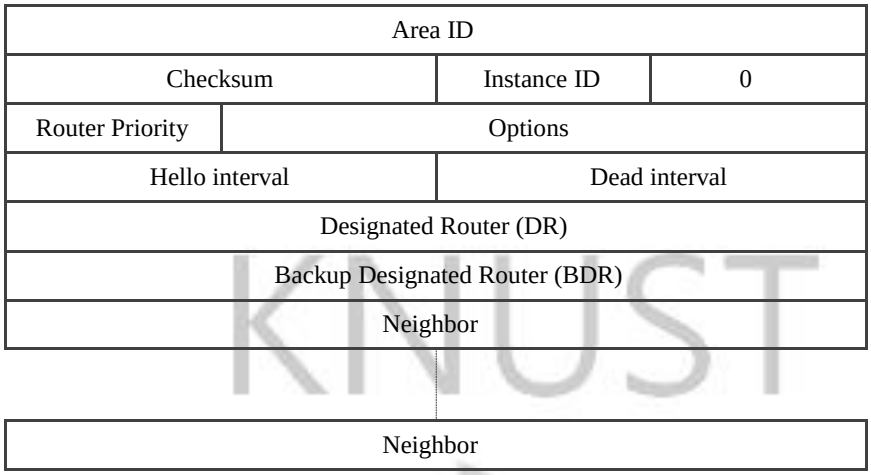


Figure 2. 1: OSPFv3 Packet structure (Source: Adopted from Doyle et al., 2005)

2.2.2 Features of OSPFv3

2.2.2.0 Hello protocol

The Hello protocol enables OSPF routers to dynamically discover and maintain neighbor relationships. The Hello protocol contains a special packet called the Hello packet which is sent out periodically by each router on every OSPF–enabled interface to establish and confirm neighbor relationships with other routers before exchange of routing information can occur between them. The OSPF Hello packet is mainly used for:

- discovering neighbors
- establishing a two–way communication between neighbors
- electing the DR and the BDR
- maintaining neighbor relationships

The Hello packet when sent contains information about the OSPF interface and the router which is sending the packet. This information includes the router ID, area ID, router priority, hello interval, dead interval, designated router and backup designated router. The Hello packet information also includes a list of all neighbors and other optional capabilities of the sending router. The hello interval is used to determine how often the router sends the Hello packet to its neighbor. The dead interval is the time after which the router can declare its neighbor dead

if during this time the router cannot receive any Hello packets from its neighbor (Cobb et al, 2005). By default, hello interval on a broadcast medium is ten seconds while dead interval is forty seconds. Dead interval enables Hello packet to be used as a keepalive message in order to determine if a neighbor is still communicating. If a router has not received any Hello packet from its neighbor during the configured dead interval, the router drops that neighbor from its local neighbor table. Router priority is used to elect or prevent a router from being elected as the designated router and backup designated router. The designated and backup designated router fields are also used to indicate whether the neighbor has already been elected as the DR or the BDR.

When an OSPF router receives Hello packet from another router, it checks to see if information contained in the Hello packet matches the information on the interface it used to receive the packet. If the information for both interfaces is the same, the routers are considered neighbors.

To establish a two–way communication between two interfaces, the router ID field is used. This field contains a list of router IDs of all the routers that the sending router has communicated with. A receiving interface checks to see if its own router ID can be found in the list of the router IDs. If this information is found, then a two–way communication is established between the sending and the receiving interfaces.

2.2.2.1 OSPF Neighbors

Open shortest path first neighbors are routers that have an interface on a common network. Neighbor discovery in OSPF is done using the Hello packet which is sent periodically from each router. For two routers to be considered neighbors, the following information on their interfaces must be the same:

- Hello interval
- Dead interval

- Area ID
- Optional capabilities

If this information is the same for both interfaces, it is entered into the neighbor table. A typical neighbor table contains the neighbor ID, and the priority of the neighbor router. Neighbor table also include the following information:

- **State**: used to indicate whether the communication with the neighbor is still in progress and whether the neighbor is in the process of establishing a two–way communication between itself and the router sending the Hello packet. State is also used to indicate whether the neighbor has attained full adjacency and is sharing its link–state information.
- **Dead time**: used to indicate how long has the last Hello packet been received from the neighbor.
- **Link–local IPv6 address**: used to indicate the neighbor's link–local IPv6 address.
- **Local interface**: used to indicate the router interface that was used to receive the Hello packet for this neighbor.
- **Designated router**: used to indicate whether the neighbor has been chosen as the DR or the BDR.

When a router receives the first Hello packet from a new neighbor, it adds this neighbor to the neighbor table in the init state. Once a two–way communication is established between the router and this neighbor, the neighbor state changes to a two–way state. Followed by the two–way state are the exstart and exchange states, where both routers will now exchange their link–state database. Once all these are completed, the neighbor enters the full state indicating full adjacency. However, if the neighbor does not send any Hello packets during the dead interval, it is moved to the down state and it is no longer considered adjacent. Creating neighbor relationships in OSPF has some advantages. It is used as a mechanism to determine whether a

router is down or active. Neighbor relationship is also used to streamline communication results because when topology databases remain the same for all routers, only periodic updates will be sent to neighbors when a change occurs within the network topology (Cisco.com, 2014).

2.2.2.2 Adjacency

After neighbor relationship is established using the Hello packet, exchange of routing updates occurs between neighbors. Information about the network is stored in the topology database or table from which the best path to every destination is computed and stored in the routing table. When the topology databases for all neighbor routers become synchronized, the neighbors become fully adjacent. To ensure that neighbor relationship is maintained and the content of the topology tables are accurate and up–to–date, a router must periodically send the Hello packet. This enables all receiving routers to keep the transmitting router and its networks in their topology tables for as long as they continue to receive the Hello packet.

Adjacency is not established between all neighbors. Adjacency formation depends on a network type and how the routers are configured in the network. OSPFv3 establishes adjacency using three different packets. These are database description (DBD), link state request (LSR), and link state update (LSU) packets. The DBD packet contains only LSA headers from the neighbor's link–state database. When these LSA headers are received by a local router, it compares them to its own link–state database header to determine which LSAs are new or which ones are up–to–date. If some of the LSAs need to be updated, the local router sends LSR packets to its neighbors asking them to provide update information for these LSAs. When the neighbors receive the LSR packets, they reply with an LSU packet in which they provide update information for the LSAs. The routers continue with this exchange until they all have identical link–state information.

OSPF neighbor relationship and adjacency are key features of the protocol since the neighbor of a router collects information about the network and forwards this information to other neighbors directly connected to it. Also, the creation of both relationships between routers is used to control the distribution of OSPF packets making the network to converge faster (Leahy, 2011).

2.2.2.3 Link State Advertisement

Apart from the Hello packet, OSPF uses a special packet called Link State Advertisement (LSA) to build its routing table. LSA is the basic means by which OSPF communicates a router's local routing topology to other routers connected together in the same area. After OSPF routers establish adjacency, neighbor routers exchange LSAs so that all routers can have identical link–state databases. A typical LSA contains information about the state and the cost associated to each link and any other information about a neighbor. Each router generates LSAs about a link attached to it and then floods these LSAs via every OSPF–enabled interface to other routers. Once the content of the link–state database for all routers become identical, all the routers use SPF algorithm to build their routing table, where the shortest path to every destination network is placed for efficient routing of packets.

Instead of using a single LSA packet, OSPFv3 uses different LSA types for specific purposes. These LSA types include:

- **Type 1 or Router LSA**: This LSA is flooded by each router within an area. Type 1 LSA contains the list of all links (including their states and costs) attached to each router that is flooding the LSA. Type 1 LSA causes SPF re–computation to occur.
- **Type 2 or Network LSA**: These LSAs are created for multiple access networks that require the use of DR and BDR. The DR or the BDR generates these LSAs and floods all the multi–access networks connected to it. Network LSAs include a list of all routers in the multi–access network. Type 2 LSA also causes the re–computation of the SPF.

- **Type 3 or Inter–Area Prefix LSA**: These LSAs are flooded by the area border router (ABR) to external areas for every destination within the local area. Inter–Area Prefix LSAs contain the cost of the link from the ABR to the local destination.
- **Type 4 or Inter–Area Router LSA**: This LSA is generated by the ABR and then sent to external areas. Type 4 LSA is used to advertise the cost of the link to the autonomous system border router (ASBR) only.
- **Type 5 or AS External LSA**: Type 5 LSA is flooded by the ASBR. Type 5 LSAs include the cost of the link to a destination in an external autonomous system. These LSAs are flooded throughout the autonomous system.
- **Type 7 LSA**: Type 7 LSA is generated by the ASBR and flooded only in an NSSA. Type 7 LSA includes the cost of a link to a destination within an external autonomous system.
- **Type 8 or Link LSA**: This LSA is flooded by every router. Each router uses a link–local flooding scope to send this LSA. In link–local flooding scope, link LSAs include the link–local address and IPv6 prefixes for that link.
- **Type 9 or Intra–Area Prefix LSA**: This LSA is flooded by every router. When the state of links change, the update is sent in intra–area prefix LSA to a local area. Intra–area prefix LSA does not cause the re–computation of the SPF algorithm.
- **Type 11 or Grace LSAs**: Grace LSAs are used for a graceful restart of OSPFv3. These LSAs are sent by a router that is restarting. Each time the router is restarting, it sends this LSA using a link–local flooding scope (Cisco.com. 2016).

2.2.2.4 Flooding and LSA Group Pacing

OSPFv3 floods LSAs to different segments of a network, depending on the LSA type. The protocol uses three different flooding scopes namely:

- **Link–local** where LSAs are flooded only on links that are directly attached to the router's interface. This flooding scope is used to send Link LSA and Grace LSA.
- **Area–local** where LSAs are only flooded within a single OSPF area. LSA types 1, 2, 3, 4, and 9 are flooded using this flooding scope.
- **AS scope** where LSAs are only flooded within a single routing domain. This flooding scope is used for sending AS External LSAs (Cisco.com, 2016).

Using OSPF flooding scope guarantees that routing information for all routers remains identical throughout the network. LSAs are flooded depending on the configuration of the OSPFv3 area. The LSAs are sent based on a link–state refresh time. By default, link– state refresh time is every 30 minutes even though all LSAs do not have the same link–state refresh time.

The rate at which LSAs are flooded in the network can be controlled by using LSA group pacing feature of OSPF. Using OSPF LSA group pacing ensures that high router CPU utilization is greatly reduced. Group pacing feature allows OSPFv3 to combine multiple LSAs with identical link–state refresh time into a single routing update instead of flooding them separately.

2.2.2.5 Link–State Database (LSDB)

This database is used to store all LSAs that are collected by each router. LSDB includes information on all paths through the network. OSPF uses information in LSDB to compute the best path to every destination. The LSDB contains best paths that are entered into the routing table and are used to locate remote networks. In order to keep the content of LSDB up to date, OSPF removes LSAs whose updates have not been received using a time interval called MaxAge. OSPF routers flood LSA updates every 30 minutes to prevent accurate link–state information from being aged out in the LSDB.

2.2.2.6 OSPF Areas

OSPF Area is a feature that can be used to limit memory and CPU requirements that the protocol can put on routers. OSPF communicates routing updates by flooding them via links to other routers, and one way to control this is to divide the network into logical segments called Areas. By dividing the network into areas, LSA flooding is limited to an area and this consequently limits LSDB formation to links within areas. Routers connected together in an area are identified by that area ID. This area ID must be the same for all the routers. Also all routers within an area have the same topology table. Area ID is assigned to specific interface on the router since a router can belong to more than one area at a time. When configuring more than one OSPF area there must be an area 0 which is a reserved area configured on any router that forms the backbone of the network. Designing the network in a hierarchical fashion using areas is an added advantage because it enhances the scalability of
OSPF (Lammle, 2007). In OSPFv3, Area ID is still a 32–bit value that can be expressed as a decimal number or in dotted decimal notation. For example, Area 0 can also be configured as Area 0.0.0.0 (Islam et al., 2010).

The use of OSPF area in a routing domain (autonomous system) allows some routers to be designated for specific purposes. These routers are used when the network is divided into multiple areas. According to Rousinnos (2014), OSPF router types include the following:

- **Internal router (IR)**: A router that has all its interfaces belonging to the same area is referred to as an IR.
- **Area border router (ABR)**: An ABR is a router used to connect at least one area to the backbone area. An ABR is considered a member of each area it connects to. It stores multiple copies of LSAs for each area it is connected to. The ABR forwards type 3 LSAs received from one area to the backbone area. For example in Figure 2.2,

ABR2 and ABR1 will send type 3 LSAs from areas 1 and 2 to the backbone area (Area 0). The backbone area also uses the ABR to send summarized information about an area to another area. For example in Figure 2.2, Area 0 will send summarized information about Area 2 to Area 1

- **Backbone router (BR)**: A backbone router is the router that has its interface connected to the backbone area.
- **Autonomous system boundary router (ASBR)**: An ASBR connects an OSPF area to another autonomous system. This allows OSPF to redistribute its routing information into or receive redistributed routes from that autonomous system.

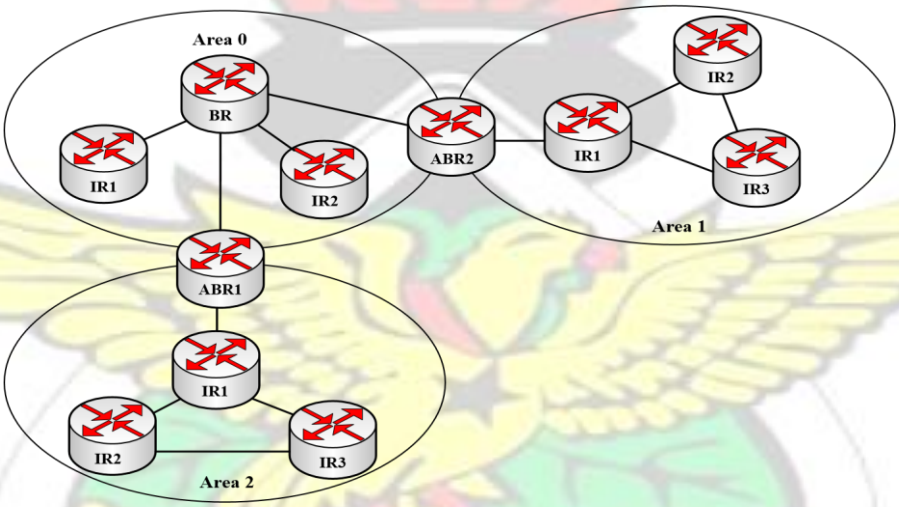


Figure 2. 2: OSPF area structure (Source: Adopted from Kaur & Kumar, 2015)

OSPFv3 supports different types of areas depending on the requirements of a network. These areas are:

- **Normal Area**: Normal area also referred to as regular area connects to the backbone area via one or more area border routers. The link state advertisement (LSA) types that are exchanged between a normal area and the backbone area are the Inter–Area– Prefix LSAs and AS External LSAs. ASBRs are used in normal Areas.

- **Stub Area**: In order to reduce the amount of external routing information that is flooded in an area, that area can be configured as a stub area. A stub Area also connects to the autonomous systems backbone Area via one or more ABRs but does not allow the use of internal ASBRs and flooding of AS External LSAs, since these LSAs are normally flooded all over the autonomous system to disseminate external route information. A stub area uses Inter–Area–Prefix LSA as a default route for all routing information that needs to be forwarded via the backbone area to the external autonomous system. For IPv6, prefix length of this LSA is set to 0.
- **Not–So–Stubby–Area (NSSA)**: NSSA is like a stub area. However, in an NSSA, ASBR is used to allow autonomous system external routes into an NSSA using redistribution. The ASBR redistributes the external routes and then generates type 7 LSAs that are flooded within the NSSA. In NSSA, Type 5 LSA is not allowed. However, an ABR can be optionally configured to connect the NSSA to other areas to convert type 7 LSAs to Type 5 LSAs and then floods these converted LSAs all over the autonomous system (Cisco.com, 2016).

2.2.2.7 Designated Router (DR) and Backup Designated Router (BDR)

Different types of networks present OSPF with a unique challenge to manage. A network could be point–to–point or a multiple access network providing a shared medium for multiple routers to communicate. In a multiple access network, if each router floods the network with LSAs, the same information about a link state will be forwarded from multiple sources, leading to a large amount of router CPU load and bandwidth consumption. In a multi–access network, OSPF uses a single router called designated router (DR) to control how LSAs are flooded. The purpose of using the DR is to minimize the number of

adjacencies formed so that all topology tables on routers can be synchronized.

A backup designated router (BDR) is a hot standby router for the DR in the same network type. The BDR receives LSA packets and routing updates from OSPF adjacent routers but does not flood the LSA updates. The BDR only works if the DR fails. Each router in a multiple access network establishes adjacency with the DR and the BDR.

Election of the DR and the BDR is won based on information in the Hello packet. What happens is that when OSPF sends a Hello packet via an interface to other routers, it will set the priority of the DR and the BDR fields if it knows which routers are the DR and the BDR. If no routers declare themselves as the DR or the BDR, the routers then follow an election procedure which is solely dependent on which router interfaces have the highest priority. A router whose interface has the highest priority is elected as the DR. The highest router priority by default is 1. This means that if the value of a router interface is changed to 0, it prevents that router from being elected as the DR or the BDR. Also, if the routers have the same router priority, router ID is used as the tiebreaker. Basically, what happens is that whenever there is a change in a link status, instead of flooding each and every path with LSA packets, OSPFv3 only sends the updates to the DR which then floods all the remaining routers in its network segment with the update using the IPv6 multicast address, FF02::5. In a scenario where the DR fails or stops functioning, the BDR is used as the newly elected DR, and OSPF elects a new BDR (Cisco.com, 2016).

2.2.2.8 Shortest Path First Algorithm

Consider an AS with link–state information shown in Figure 2.3. The cost metric (CST) assigned on each router interface to every network (NET) indicating the choice of using that interface is given by the arabic numerals shown in the figure. In order to build a LSDB from which the shortest path to every network can be calculated, each router is expected to receive a valid LSA from its neighbors in the network. Before the LSDB is built, each router will forward an LSA containing link–state information (cost) on all the networks that are directly

attached to it. When a router receives an LSA from other routers, it will send this LSA to its neighbors. When the network is converged, each router in the AS shown in Figure 2.3 will have the LSDB shown in Table 2.1.

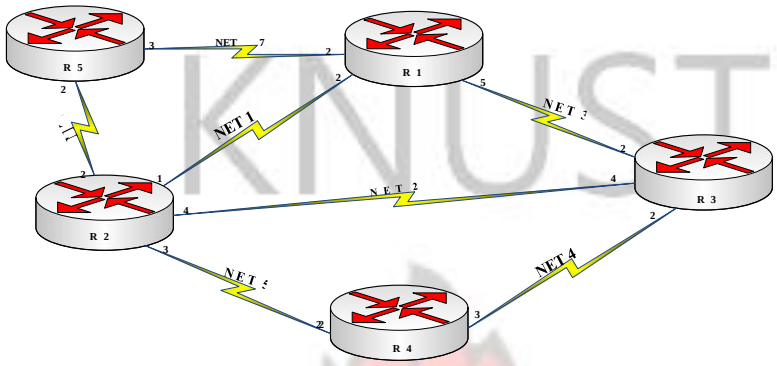


Figure 2. 3: Autonomous System with link–state information (Source: Adopted from Lemma et al, 2009)

After the LSDB is built, each router uses SPF algorithm to construct a shortest path tree from which the least cost path to every network is calculated and then stored in the routing table. Figure 2.4 shows how R1 has constructed its SPF tree from the AS shown in Figure 2.3.

Table 2.1: AS Link–State Database

Router	Connected network and Costs
R1	NET7;CST=2, NET3;CST=5, NET1;CST=2
R2	NET6;CST=2, NET5;CST=3, NET2;CST=4, NET1;CST=1
R3	NET3;CST=2, NET4;CST=2, NET2;CST=4
R4	NET5;CST=2, NET4;CST=3
R5	NET6;CST=2, NET7;CST=3

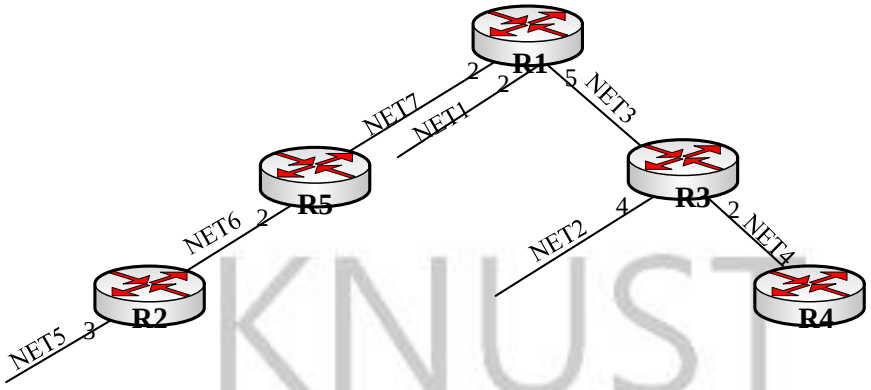
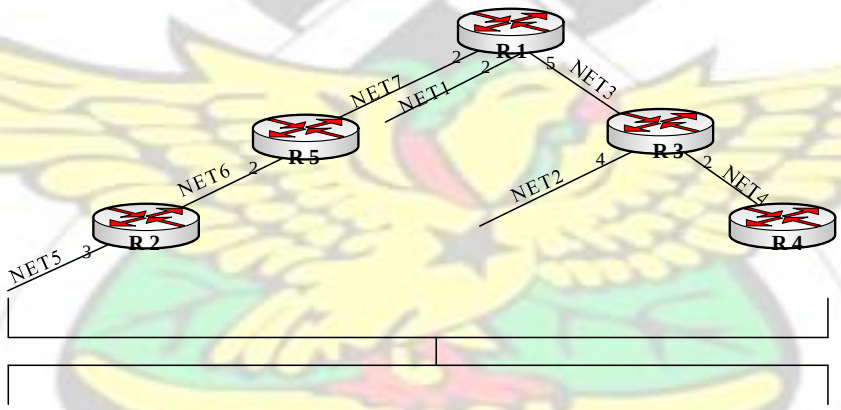


Figure 2. 4: SPF tree constructed by R1 (Source: Author's construct)

After the SPF tree is constructed, OSPF creates the routing table entries using information obtained from the SPF tree. The SPF tree includes a single cost to each destination network as created within the AS. Figure 2.5 shows the routing table entries constructed from the SPF tree shown in Figure 2.4.



Network	Forwarding Router	Metric
7	-	2
3	-	5
6	R5	4
5	R2	5
1	-	2
2	R2	6
4	R3	7

Figure 2. 5 : R1 routing table entries (Source: Author's construct)

2.2.3 OSPF Cost

To compute the shortest path to a destination, OSPF uses cost as the main metric. Cost is attached to the interface via which the router forwards LSAs. The interface which has the least cost to the destination is selected to be used to forward traffic (Lemma et al, 2009). The cost of an interface is computed using the bandwidth on that interface. Each OSPF router executes the SPF algorithm to construct the shortest–path tree from itself to every subnetwork in its area. However, RFC 2328 does not specify how a router should compute the cost of an attached network; this choice is left with the vendor (Malhotra, 2002). Cisco uses cumulative bandwidth at each router to calculate the cost of an attached network using the following formula (Graziani et al, 2008):

$$Cost = \frac{10^8}{bandwith\ in\ bps}$$

The value, 10^8 is called the referenced bandwidth. It is measured in bits per second (bps). By default, referenced bandwidth is set to 100000000. From this formula, it can be seen that cost is inversely proportional to bandwidth. Therefore a link with a higher bandwidth will have the least cost and is more likely to be used to forward traffic.

2.2.4 OSPF Convergence

Consider the network shown in Figure 2.6 with OSPF running on all the routers. Assuming that the link between R3 and R4 fails, R3 will detect the link failure and send an LSA to its neighbors R2 and R5. Since there is a change in the network topology, routing of any traffic is suspended. R2 and R5 quickly update their topology database, copy the new LSA received from R3 and flood their neighbors, R1 and R4. When R1 and R4 receive the new LSA, they also update their topology databases making all the routers to have the same topology

database. Once all the routers receive the new LSA and update their topology databases, the network is converged.

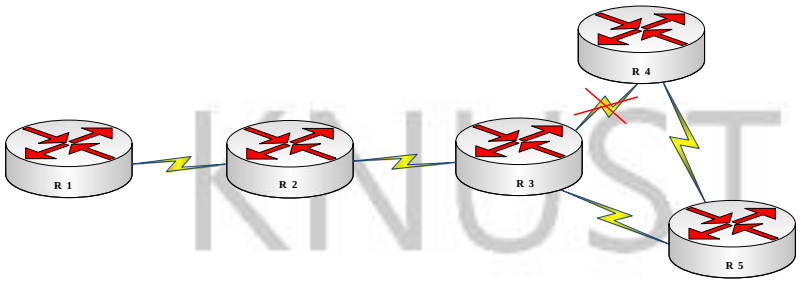


Figure 2. 6 : OSPF convergence (Source: Adopted from Islam et al., 2010)

2.2.5 Advantages of OSPF

- OSPF is an open standard protocol and so allows multi–vendor deployment.
- OSPF is more scalable and is therefore suitable for large networks.
- OSPF keeps several routes having the same cost to a single destination.
- By configuring areas, OSPF minimizes routes and reduces the size of routing tables.
- If there is a change in network topology, it is quickly communicated among routers.

2.2.6 Disadvantages of OSPF

- OSPF is difficult to configure
- Even though the flooding mechanism is controlled in OSPF, it still consumes network resources (Pavani et al., 2014)

2.2.7 Intermediate System to Intermediate System (IS–IS)

Intermediate System to Intermediate System is an extensible intra domain routing protocol designed by Digital Equipment Corporation (DEC) as part of DECnet Phase V networks. IS–IS was made a standard routing protocol by the ISO in 1992 for communication between network devices referred to as intermediate systems (Kaur et al, 2014). The purpose of standardizing IS–IS is to make it possible for packets to be routed in the OSI protocol suite that uses the connectionless–mode network protocol (CLNP) and the connectionless–mode network service (CLNS) to provide connectionless data delivery for the transport layer within the protocol stack.

In order to allow the CLNS to carry IP information, IS–IS was later extended to support routing of data packets in IP, which has become the standard network layer protocol for the internet. The IP implementation of IS–IS is called integrated IS–IS. It was published in RFC 1195. The word integrated was used in the sense that the protocol can be used to support network traffic in IP environments only, OSI environments only, and can also support interconnection between hosts in both environments.

In IS–IS networks, routers are called intermediate systems (ISs) and other user devices are called end systems (ESs). The end systems and the intermediate systems are grouped together to form a routing domain.

Similar to OSPFv3, Integrated IS–IS also uses Dijkstra's (SPF) algorithm to determine the shortest path to a destination in a network. Each IS–IS router separately builds a topology database of the network using link–state information collected from other routers in the network. Every router in the routing domain sends an IS–IS Protocol Data Unit (PDU) or a packet called Link State Packet (LSP), which contains information about itself and the links attached to it. The LSP contains information encoded in a variable length data structure that is made up of type, length, and value. This data structure is often referred to as TLV (Hopps, 2008). TLVs are the extensible parameter portions of the IS–IS PDUs that are used to carry different kinds of information. The protocol also supports hierarchical networking allowing a larger network domain to be separated into logical divisions called areas. Each intermediate system resides in at least one area. The hierarchy defines two levels that are used to organize routers in larger routing domains. These are Level 1 and Level 2. Level 1 routers are the same as IRs in OSPF. Level 2 routers are used to connect two or more areas in the routing domain (Lemma et al., 2009).

2.2.8 IS–IS Changes for IPv6

The ability of the IS–IS packets to be modified to include additional TLVs has given the protocol an added advantage. The addition of these new TLVs enables the protocol to support routing in newer network addressing schemes without changing the protocol operation. This in contrast to OSPF is different. In order to support routing in IPv6, the OSPF protocol was completely upgraded to a newer version. This has changed the protocol structure and makes its operation slightly different from the version supported by IPv4. In IS– IS, only two new TLVs are added to the protocol structure to support routing in IPv6. These TLVs are:

- IPv6 Reachability
- IPv6 Interface Address

Also, an IPv6 protocol identifier was included in the protocol structure. However, the extended metrics and up or down semantics of RFC 5305 are still used in the new TLVs (Hopps, 2008).

2.2.9 IS–IS features

2.2.9.0 IS–IS Packets

Intermediate System to Intermediate System packets are called Protocol Data Units (PDUs). There are four PDUs defined for IS–IS routers. These include:

- **IS–IS Hello (IIH) packet**:IIH is used for detecting neighbor routers, establishing and maintaining adjacency between them.
- **Link State Packet (LSP)**: LSP is the main packet the IS–IS protocol uses to transmit routing information in its routing domain. Each IS–IS router sends an LSP containing information about itself and the links that are connected to it. The content of an LSP includes a header that describes the PDU type and length, the LSP ID and a sequence number, and a remaining lifetime timer. It also includes the TLV which contains links to neighbor routers, including the metrics on those interfaces. The sequence number is used to ensure that receiving routers do not use outdated LSPs to calculate best routes

to destinations. This avoids having the same copy of LSPs that can be added to the topology table. The remaining lifetime timer is used to determine how long the LSP can be kept valid in the IS–IS LSP database. This timer is used by the LSP aging process to ensure that LSPs that are not valid or that are outdated are dropped from

the topology table after every 20 minutes. There is also an LSP refresh timer specified in ISO 10598 by which routers sending LSPs must use to update their entries in the topology table.

- **Complete Sequence Number PDU (CSNP)**: This packet is made up of a list of LSPs that are stored in the link state database. IS–IS routers use CSNP to inform each other about outdated or lost LPSs. Using CSNP ensures that all routers have the same information in their link state database.
- **Partial Sequence Number PDU (PSNP)**: If an LSP becomes outdated or lost, PSNP is used to request a router to send a new LSP. It is also used to acknowledge the receipt of an LSP (Lemma et al, 2008).

2.2.9.1 Type Length Values (TLVs)

Type length value is the main data portion of the IS–IS packet through which the protocol can be extended. A typical TLV contains routing information that is propagated throughout the IS–IS routing domain. TLV is divided into three fields. These fields are identified by one octet of type (T), one octet of length (L) and "L" octets of value (V). The type field is used to specify the type of data in the value field. The length field is used to indicate the length of value field while the value field is the data portion of the IS–IS packet where routing information is carried for transmission (Cisco.com, 2005).

To support routing in IP, IP information is encoded in a new TLV 128 defined for the IS–IS PDUs. The purpose of this is to allow the distribution of IP destinations before they can be

reached. Since IP information resides in the same packet as CLNS information, there is a protocol supported field included in the IS–IS Hello packet to indicate the type of protocol supported by a sending router. In addition to that, the Hello packet also includes the IP address on the interface of a neighboring router because ICMP redirect messages to end systems must include the next hop address. Thus each Hello packet contains the IP address of the interface on which it is sent (Roussinos, 2014). Also, for the router to know about the IP networks that are connected to other routers within the same area, the LSPs are redesigned to contain the IP addresses of these networks on the interface of the routers. The IP addresses are included in both level 1 and level 2 LSPs. In IPv4, the TLV that includes this information is called IP Interface Address (Callon, 1990).

Apart from the IP addresses, information for reaching an IP destination is also made up of subnet mask and a metric. Depending on the level from which the LSP is sent, information for reaching an IP destination is carried in a TLV known as the IP Internal Reachability Information TLV for level 1. For level 2, this information is carried in a TLV known as the IP External Information TLV (Callon, 1990).

To support routing in IPv6, the IPv6 reachability TLV was added to the IS–IS Hello packet and the LSP. This TLV is used to provide IPv6 equivalent data. It describes how a particular network can be reached using information such as the routing prefix and metrics on a path to that network. It also includes a bit to indicate if the prefix on the path is being advertised from a higher level and a bit to indicate if the prefix is being forwarded from another routing protocol. It also includes sub–TLVs that are optionally added to allow for later extension. IPv6 reachability TLV may appear several times or not all within an LSP.

Figure 2.7 shows the structure of IPv6 reachability TLV.

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

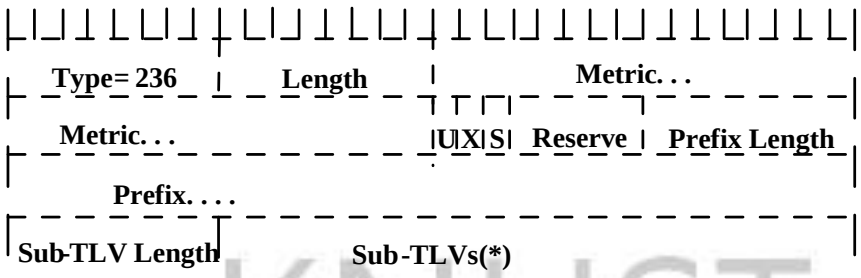


Figure 2. 7 : IPv6 Reachability TLV (Source: Adopted from Hopps, 2008)

Also, for the LSPs to include IPv6 addresses on router interfaces, IPv6 interface address TLV is added to the link state packets.

2.2.9.2 IS–IS Areas

Similar to OSPF, IS–IS also supports hierarchical network design allowing a larger network to be divided into logical divisions called areas. However, there is a difference between how areas are configured for both routing protocols. Whereas in OSPF a backbone area is configured and used for connecting other areas, IS–IS does not include a backbone area. The routers are grouped into a hierarchy called levels and are used to manage communication between areas. The levels are simply routers or intermediate systems that are configured to manage communication within areas and between areas. There are two router levels defined in the hierarchy. These are level 1 and level. 2 (Kaur & Kumar, 2015).

Level 1 (L1) routers are the same as internal routers used in OSPF areas. They all have their interfaces connected within the same area. All L1 routers exchange routing information belonging to a specific area. On the other hand, Level 2 routers are used to connect different areas. They are similar to ABRs used in OSPF. An L2 router is not required to identify the topology within level 1 area but there is a possibility that an L2 router can be an L1 router in a single area (Roussinos, 2014). Figure 2.8 shows the IS–IS area structure and all the router types used to manage communication within the IS–IS routing domain.

2.2.9.3 Designated Intermediate System (DIS)

DIS is the same as DR used in OSPF. However, there is a slight difference between the two. In OSPF, once the DR and BDR are chosen, all the other routers establish adjacency relationship with the DR and the BDR so that when the DR fails, the BDR will become the DR. In IS–IS, all the routers in the broadcast medium form adjacent relationships with other routers and the DIS. When the DIS fails, any router can take over as the new DIS. Election of a DIS is based on router priority. Thus a router with the highest priority is elected as the DIS.

If all the routers have the same priority, MAC address is used as the tiebreaker (Empson, 2007).

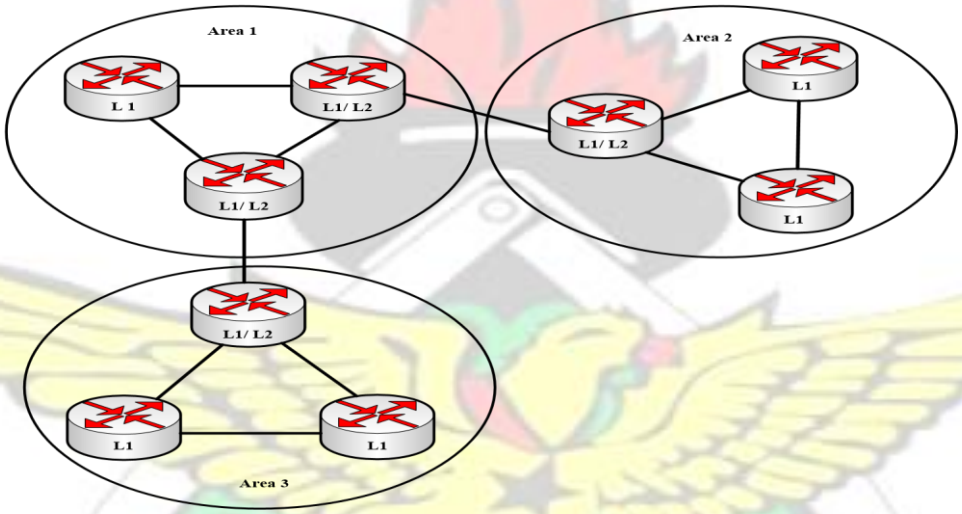


Figure 2. 8 : IS–IS area structure (Source: Adopted from Kaur & Kumar, 2015)

2.3 IS–IS Metrics

In order to compute the shortest path to a destination IS–IS uses four metrics namely Cost, Delay, Expense and Error. Cost is the default metric. It is an arbitrary metric which is supported by all IS–IS routers. Unlike OSPF that automatically calculates it metric (Cost) based on bandwidth, IS–IS does not automatically calculate its metric. By default, all the links use a metric of 10. The cost metric is used to show the speed of link. If the cost on a link is small, it means that the speed on the link is high or the link has a high bandwidth (Lemma et al., 2009). Delay, expense and error are optional metrics that are intended for providing quality of service

routing. IS–IS link metrics are associated with all outgoing interfaces to neighbor routers (Acharya, 2006).

2.4 Advantages of IS–IS

- IS–IS is easy to configure. This makes it simple to implement.
- IS–IS is more scalable. It does not use backbone area to connect other areas. Connection between areas is done using a collection of Level 2 routers.
- Because IS–IS is more scalable, it is able to support large areas made up of multiple routers without degradation of the shortest path first performance.

2.5 Disadvantages of IS–IS

- All IS–IS areas are stub areas. Using stub areas can lead to sub–optimal routing between areas.
- Node identification is difficult because it requires network service access point (NSAP) addresses and CLNP as an additional network layer protocol (Lemma et al., 2009).

CHAPTER 3

METHODOLOGY

3.0 Introduction

This chapter covers network simulation. It is the main evaluation methodology used to compare both routing protocols in this thesis. This method is chosen because it is the most widely used among researchers and network engineers. It is also less time consuming, relatively cheaper and easy to use when compared to the use of real world network devices to achieve the same purpose (Siraj et al, 2012).

3.1 Simulation Tool

In this thesis, Riverbed Modeler Academic Edition 17.5 is the main simulation tool used. This simulator was preferred because it is a GUI based and an object–oriented simulator enabling users to model real world systems in form of graphics (Pan et al, 2008). It also has a huge documentation, a comprehensive model library, and analysis tools that allow users to customize simulation results in different forms for presentation. This modeler is a limited–feature version of Riverbed Modeler available for educational use. Modeling in riverbed modeler is done on project basis. A project contains at least one scenario in which there are network devices and channels, configuration utilities, and different network application traffics that can be put together for any simulation design. The nodes and links included in the simulation represent real world network devices that are used as an input for performing the simulation.

3.2 Design and Analysis in Riverbed Modeler

Design and analysis in riverbed modeler is done by following steps that are necessary for modeling a real system under observation. Figure 3.1 shows these design steps.

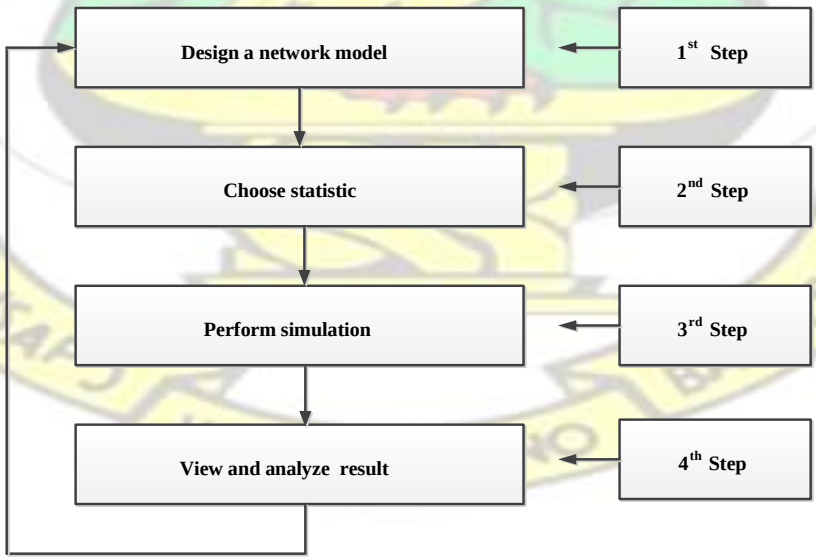


Figure 3. 1 : Riverbed modeler design steps (Source: adopted from Pandey et al., 2015)

3.3 Simulation Design

In this thesis, two routing protocols have been compared in IPv6 network. These protocols are OSPFv3 and IS–IS. In other to achieve the objectives of this thesis, the simulation was divided into two scenarios. The first scenario is an IPv6 network model configured with OSPFv3. The second scenario is a copy of the first scenario but configured with IS–IS. These scenarios were simulated and the impact of using each protocol to separately route the selected applications was observed and recoded. Performance comparison of both protocols is based on the following quantitative parameters:

- Convergence duration.
- IPv6 traffics dropped.
- Network throughput.
- Link utilization.
- Database query response time and Traffics received.
- Remote login response time.
- FTP download and upload response times.
- HTTP page response time.
- Email download response time.

The purpose of the comparison is to determine which protocol will perform better than the other for the selected simulation parameters.

3.3.0 Network Topology and Connections

Figure 3.2 shows the network topology used for the simulation. The topology models an IPv6 enterprise network consisting of four subnets. Each subnet represents a department in the company. These departments are Administration, Sales & Marketing, Finance & Accounting, and Information Technology.

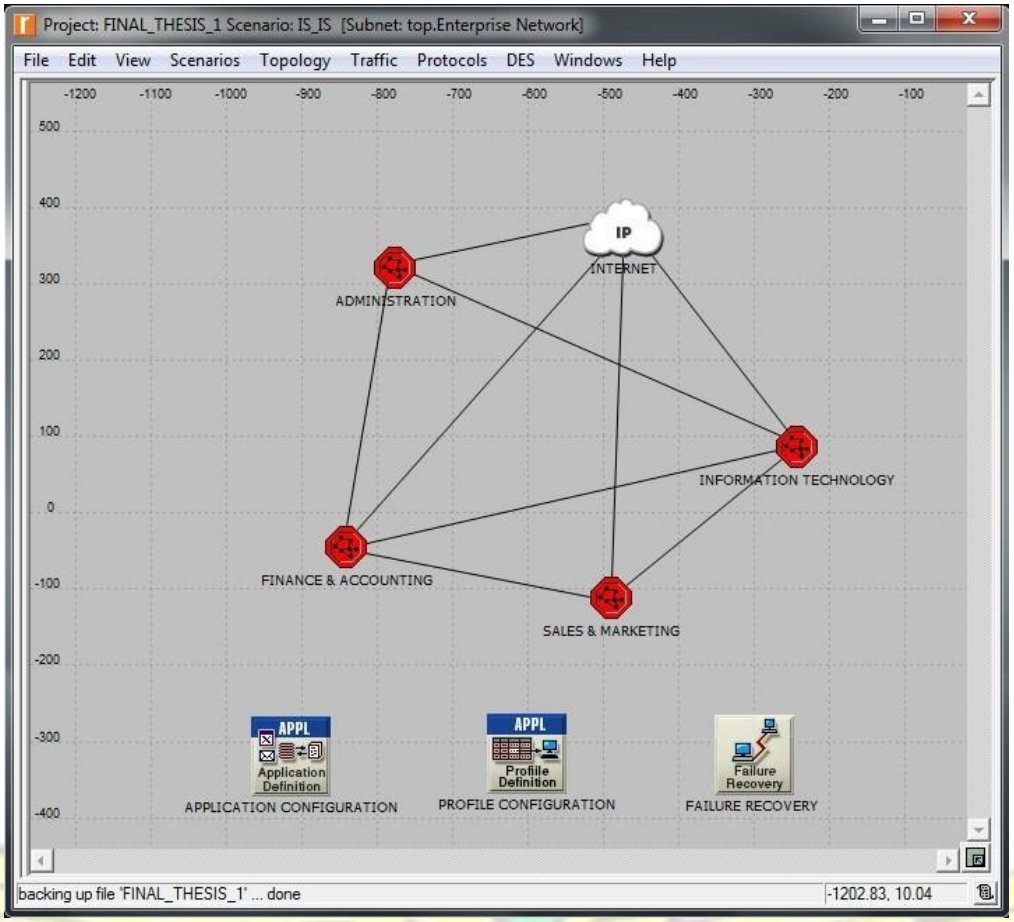


Figure 3. 2 : Network Topology

The network topology consists of routers, network switches, firewalls, workstations, servers and an IPv32 cloud that are connected together. There are two routers, one network switch, one firewall, and 10 workstations connected together in each subnet. The routers and the firewalls in each subnet are connected together using PPP DS1 duplex link. The workstations are connected to the switch using 100BaseT duplex link. The connection between the subnets is done using PPP DS1 duplex link. In order to provide email and http support, all the subnets are connected to an IPv32 cloud device which provides internet connection to each subnet. The connection between each subnet and the IPv32 cloud device was also done using PPP DS1 duplex link. The detailed description of the network devices and channels used in the topology are as follows:

- Router model: CS_7000_6s_a_e6_fe2_fr4_sl4_tr4. This router has several ports for connecting different media types. These include 4 Ethernet hubs at a data rate of 10Mbps, 4 token rings at a data rate of 4Mbps or 16Mbps, 4 frame relay serial links and 4 serial links at different data transmission rates, 2 Fast Ethernet ports at a data rate of 10Mbps, and 1 ATM slot. It also allows a total amount of 150,000 packets that can be transmitted per second. By default, it uses RIP or OSPF to forward packets.
- Network switch model: eth16_ethech16_fddi16_tr16_switch. This switch has different ports for connecting different cable types. These include 16 Ethernet ports, 16 Etherchannel ports, 16 FDDI ports and 16 Token Ring ports.
- Workstation model: ethernet_wkstn. This device is used to model any workstation that supports a client–server application running over TCP/IP or UDP/IP. It has the following ports for connecting different cable types: 1 Ethernet port at a data rate of 10 Mbps, 1 Ether port at a data rate of 100 Mbps or 1 Ethernet port at a data rate of 1000 Mbps. It also supports the attributes of some client applications such as email, database, ftp, http, remote login, etc. This allows specific application traffic to be generated in it.
- Server Model: ethernet_server. This node is used to represent any server that supports a server application running over TCP/IP or UDP/IP. It supports 1 Ethernet connection at a data transmission rate of 10 Mbps, 100 Mbps or 1 Gbps. The link connected to this node determines the speed at which it operates.
- Firewall model: ethernet2_slip8_firewall. This node is used to represent any IP based gateway that can function as a firewall. It has 2 Ethernet and 8 Serial line ports with different data transmission rates. When an IP packet arrives on any interface in this node, it is forwarded to the appropriate outgoing interface based on the packet's destination IP address. Packets are routed in this node using RIP or OSPF by default.

- IPv32 Cloud: This node is used to provide internet connection. It supports 32 Serial line interfaces that can be selected at different data transmission rates. When an IP packet arrives on any interface in this node, the packet is forwarded to the appropriate outgoing interface based on the packet's destination IP address. Packets are routed using RIP or OSPF by default.
- Link model: 100BaseT duplex link. This is used to represent an Ethernet medium with a data transmission rate of 100 Mbps. The following are the combination of network devices which can be connected together by using this link: hub, switch, station and bridge. It cannot be used to connect a hub to another hub.
- Link model: PPP DS1 duplex. This link model is used for connecting two IP based network devices. PPP DS1 operates at a data transmission rate of 1.54 Mbps.
- Application definition object: This configuration utility is used to specify applications whose traffics will be generated in the network model. With this configuration utility, the name of an application and its corresponding description can be created. For instance, "Http (Light Browsing)" is a specification of a web (Http) application performing light browsing.
- Profile definition object: In order to generate network traffic for each application specified in the network, the profile definition object is used. Profile definition object allows users to create profiles for each application they specified in the application definition object. Therefore to use this object, applications must be created using the application definition object.
- Failure recovery utility: This object is used to mimic failure recovery scenario within a given network topology. It has attributes that allow users to control the time and the status of network objects such as links and nodes. The status of an object is either "fail"

or “recover”. Status is measured in seconds. Failure status indicates when the object should fail while the recovery status is used to indicate when the object should recover.

Figure 3.3 shows the internal infrastructure of the IT department subnet. The number of network devices connected together in this subnet is the same as the other subnets.

However, it has five servers connected to the switch to support each network application. These servers are database server, remote login server, file server, http server, and email server. These servers are connected to the switch using 100BaseT duplex link.

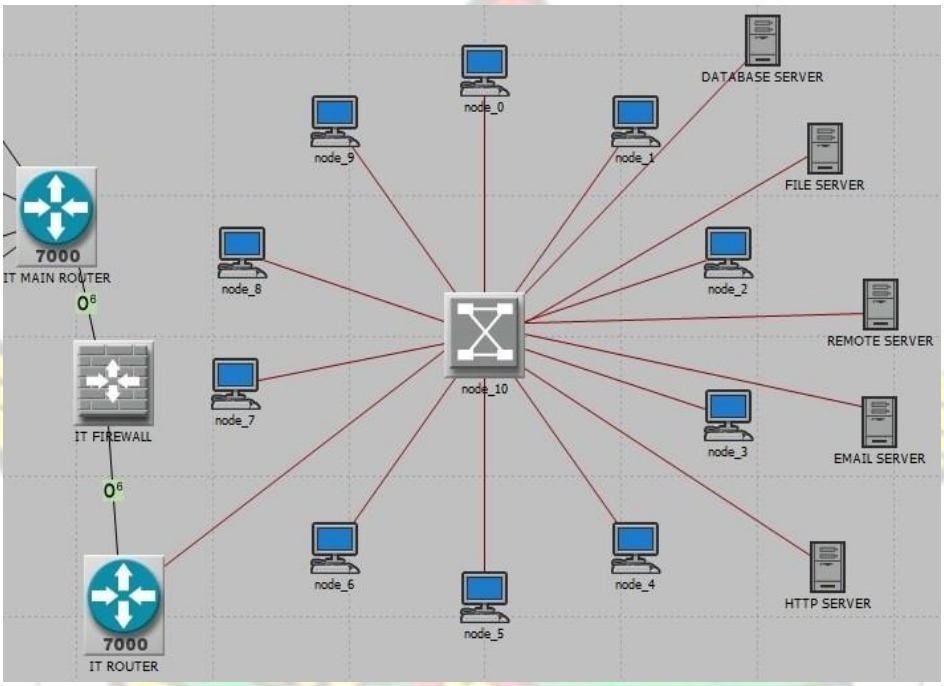


Figure 3. 3 : Internal Infrastructure of IT department

3.3.1 Application Configuration

In order to specify the selected applications and to generate network traffic for each of them in the network topology described under section 3.3.0, the Application Definition and the Profile Definition objects are added from the object pallet into the modeler’s workspace. Both objects are respectively renamed as application configuration and profile configuration in the modeler’s workspace as shown in Figure 3.2.

The application configuration object is set to support database (high load), remote login (high load), ftp (high load), email (high load) and Http (heavy browsing). Figure 3.4 shows the configuration of the database application in the application definition object. Configuring applications in this utility is done under Attributes. To configure the database application, the application configuration object was opened (right clicked) and then "Edit Attributes" was selected from the pop–up menu. From the pop–up window, "Application Definitions" under "Attribute" was expanded where the application name (Database) and its corresponding description (High Load) were specified.

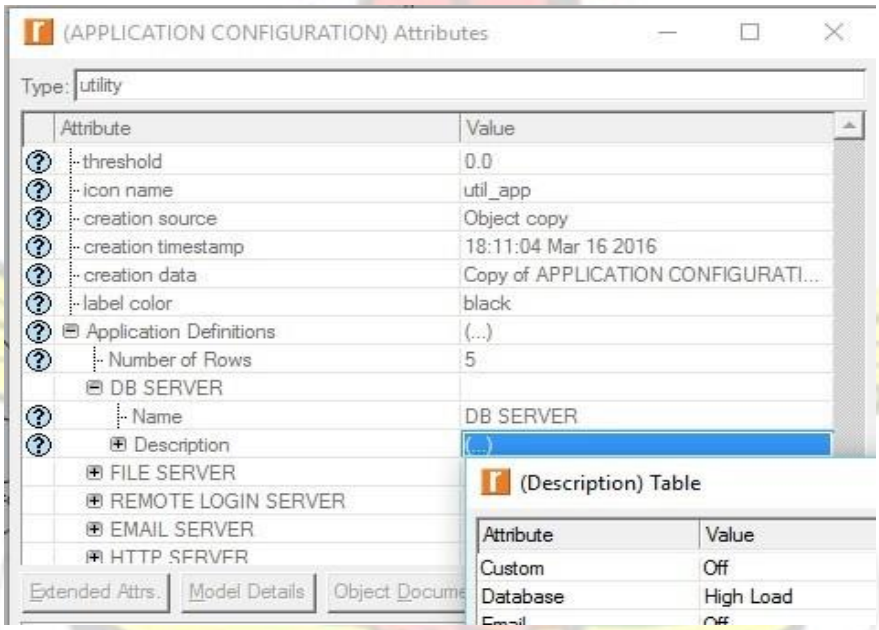


Figure 3. 4 : Database Application Configuration

In order to generate network traffic for each application specified in the network, five profiles were defined in the profile configuration utility to support each application specified in the application configuration object. This configuration is shown in Figure 3.5. To generate traffic for all the applications defined in the network topology, the profile configuration object was opened (right clicked) and then "Edit Attributes" was selected from the pop–up menu. From the pop–up window, "Profile Configurations" under "Attribute" was expanded where the value 5 was entered for "Number of Rows" signifying that there are five applications whose traffics

are to be generated. To configure traffic for each application, “Enter Profile Name” was expanded where the name of a profile or traffic was entered. To map the profile name to its corresponding application, “Applications” under “Profile Configurations” is expanded where each application defined in the application configuration object was selected.

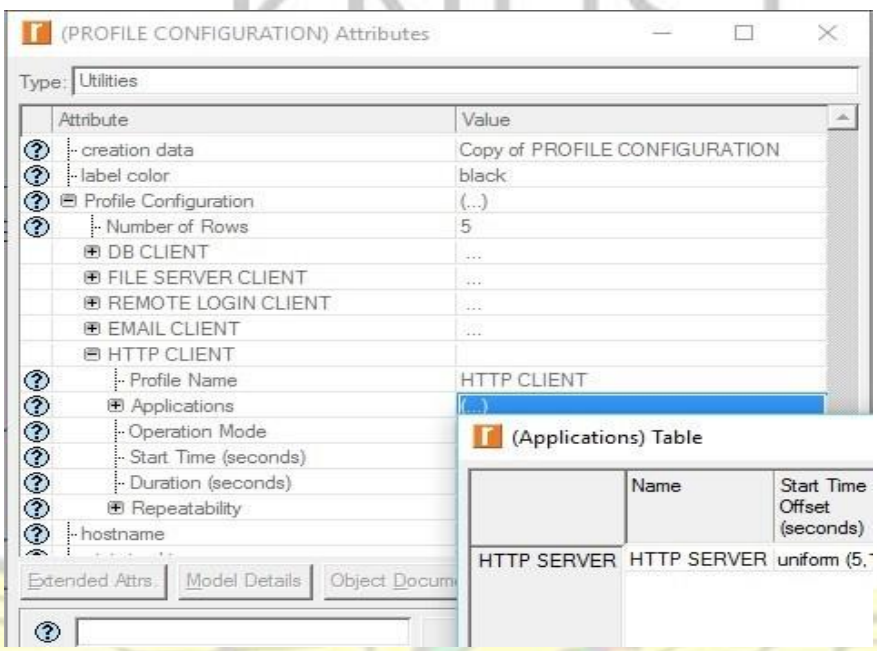


Figure 3.5 : Profile Configuration

3.3.2 Failure Recovery Configuration

In addition to the applications configured, failure recovery has also been enabled in the network topology. The purpose of this is to cause some links to fail and then recover so that the network convergence duration and throughput can be measured for both scenarios. In order to achieve this purpose, the link between Sales & Marketing department and Finance & Accounting department is set to fail at 240 seconds and recover at 480 seconds. Figure 3.6 shows how the failure recovery is configured. This configuration was done by adding the failure recovery utility from the object pallet into the modeler’s workspace. The failure recovery object was opened (right clicked) and then “Edit Attributes” was selected from the pop–up menu. From a pop–up window, “Link failure/Recovery Specification” under

"Attribute" was expanded where the name of the link (Sales & Marketing and Finance & Accounting), its status (fail and recover) and time (240 and 480 seconds) were specified.

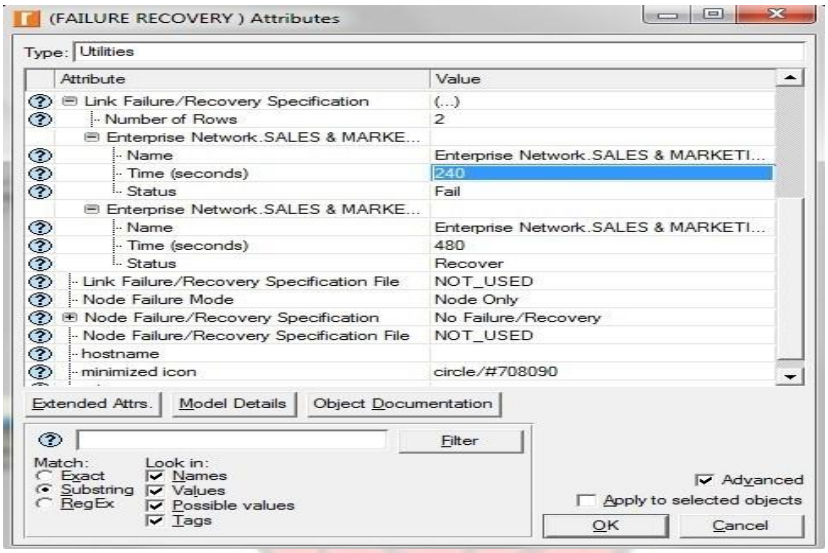


Figure 3. 6 : Failure Recovery Configuration

3.3.3 Node Configuration

In order to fully model the real world enterprise network, each server in the IT department is configured to support the application it is meant for. Figure 3.7 shows this configuration for the database server. This configuration was performed by opening (double click) the Information Technology subnet. Inside this subnet, the database server was selected (right clicked) and then "Edit Attributes" was selected from the pop–up menu. Under "Attributes", "Applications" was expanded where the database server was configured under "Supported Services".

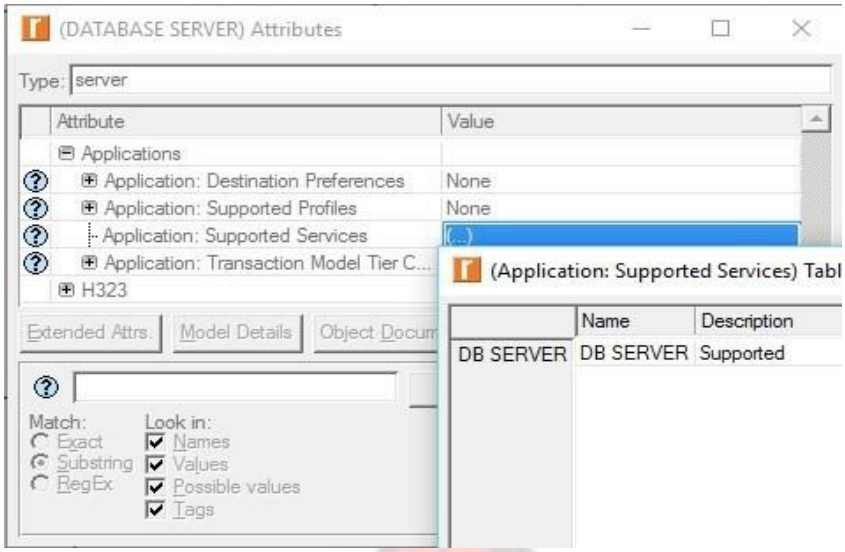


Figure 3. 7 : Database Server Application Configuration

Similarly, each workstation in the network topology is set to support all the applications supported in each server. Figure 3.8 shows this configuration. To perform this configuration, the administration subnet was opened and node_0 (workstation) was right clicked where "Select similar nodes" was selected from the pop–up menu. When all the nodes were selected, node_0 was right clicked again to select "Edit Attributes" from the pop– up menu. From a pop–up window, all the applications defined in the network topology were selected under "Application Supported Profiles". These procedures were repeated for the workstations in each subnet to complete the configuration of the workstations.

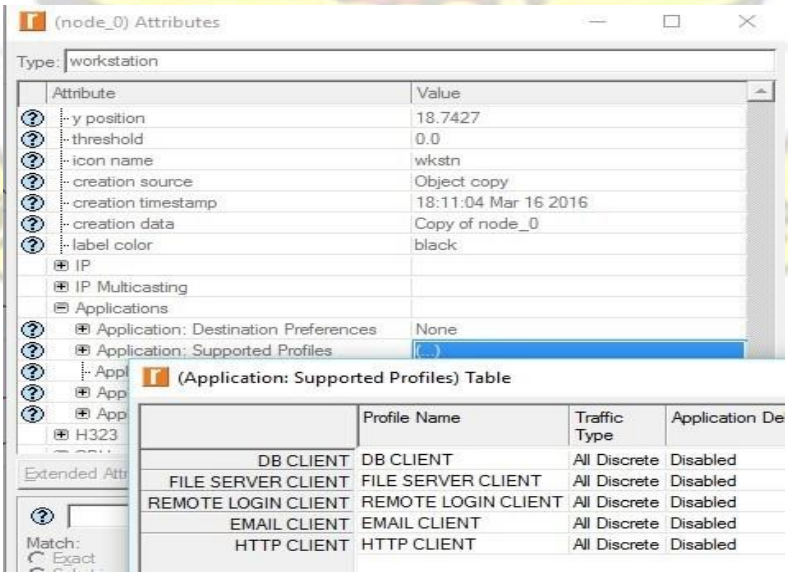


Figure 3. 8 : Workstation Application Configuration

3.3.4 OSPFv3 Scenario

Figure 3.9 shows the OSPFv3 scenario used in this thesis. The network topology shown in this figure is the same as the network topology described in Figure 3.2. However, in this topology, only OSPFv3 is enabled. The reason for doing this is to separately measure the effect of OSPFv3 performance on the selected applications that are defined in the network topology. Since OSPFv3 is an IPv6 supported routing protocol, IPv6 addresses were automatically enabled in the topology before OSPFv3 was configured. Enabling IPv6 addresses was done by using the protocols tab on the menu bar where IPv6 was selected from which Auto–Assign IPv6 addresses option was used to assign the IPv6 addresses. Similarly, OSPFv3 was enabled by following the same procedure. However, under IPv6, Configure IPv6 Routing Protocols option was used where OSPFv3 was also enabled in the topology.

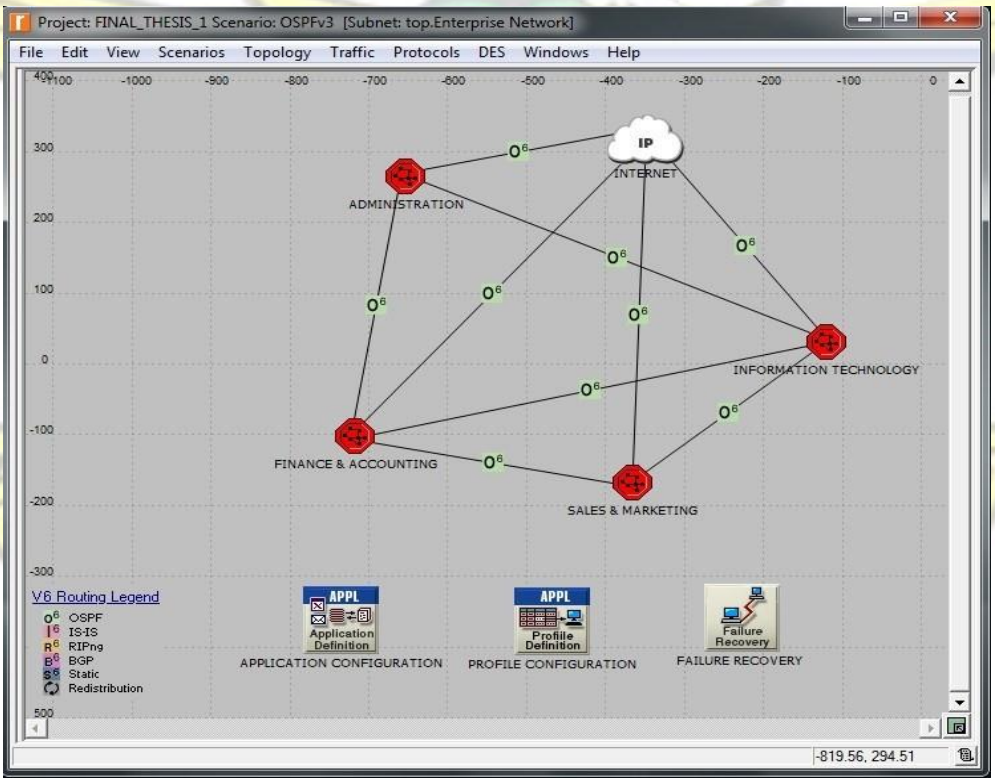


Figure 3. 9 : OSPFv3 Scenario

After enabling IPv6 Addresses and OSPFv3, various statistics were chosen for each simulation parameter. These are the parameters used to measure the performance of the OSPFv3 routing protocol. To choose these parameters, DES tab was selected on the menu bar in the modeler's workspace. From DES, Choose Individual Statistics was selected from the pop–up menu where all the simulation parameters were checked under Global statistics and Link statistics. Figure 3.10 shows how the database query parameters were chosen under Global statistics by following this procedure.

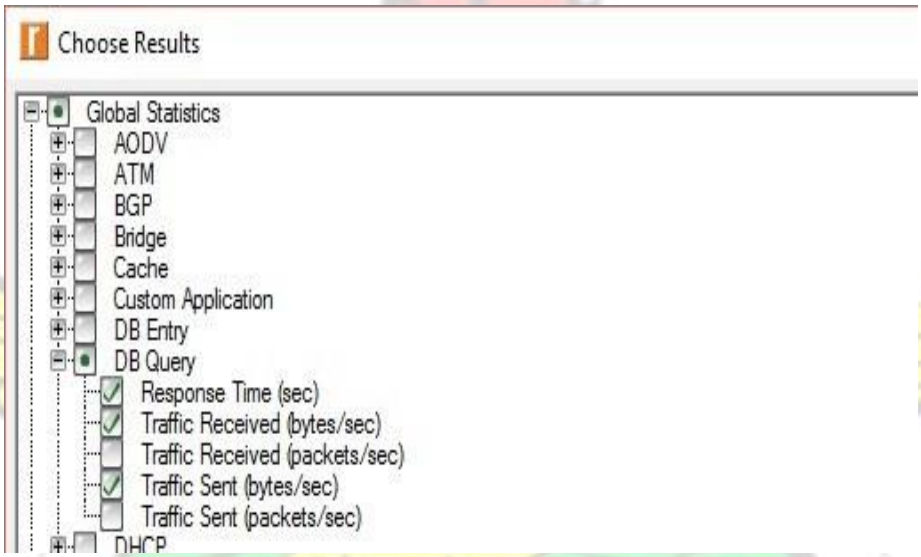


Figure 3. 10 : Database query parameter selection

After choosing the parameters, total simulation time for this scenario was set to last for 30 minutes. This is shown in Figure 3.11. Total simulation time was set using the DES tab on the menu bar in the modeler's workspace. The simulation time was set under "Configure/Run Discrete Event Simulation". From the pop–up window, duration was set to 30 (0.5 hour(s)) minutes and then the simulation was run.

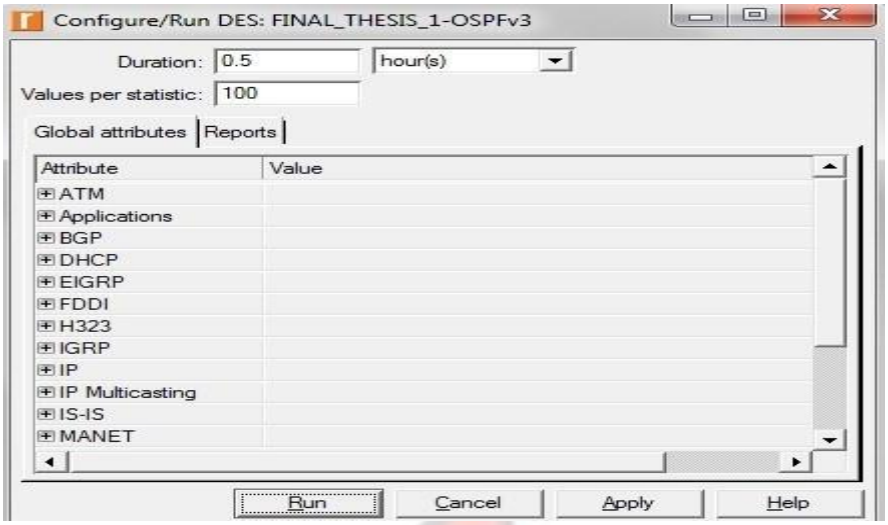


Figure 3. 11 : Simulation Time Configuration

When the simulation ended, results were recorded for the following parameters: network convergence duration, IPv6 traffic dropped, throughput, link utilization, database query (response time and traffic received), ftp download/upload response times, ftp traffics received, remote access, email and web page response times. These are the parameters chosen to measure how OSPFv3 will perform when it is used separately to route the selected applications in IPv6. Results were recorded for each parameter at a particular time during the simulation. These results and their corresponding simulation times are numerically shown in the following tables:

Table 3.1 shows the numerical values recorded for OSPv3 convergence time when the simulation ended. The simulation time intervals (in minutes) used for measuring these values are 0.5, 2, 3, 4, 5, and 8. The corresponding values of the convergence time (in seconds) are 12.5, 11.0, 10.0, 9.0, 7.0, and 2.4 respectively.

Table 3. 1: OSPFv3 Convergence time

Simulation time (minutes)	OSPFv3 (seconds)
0.5	12.5
2	11.0
3	10.0
4	9.0
5	7.0
8	2.4

Table 3.2 shows the values recorded for IPv6 traffics dropped by OSPFv3. Simulation time intervals (in minutes) during which the values were recorded are 2.5, 5, 10, 15, 20, 25, and 30. The corresponding values recorded for IPv6 traffics dropped (in packets/sec) are 4.25, 4.25, 1.6, 1.1, 0.8, 0.7, and 0.6 respectively.

Table 3. 2: OSPFv3 IPv6 traffics dropped

Simulation time (minutes)	OSPFv3 (packets/sec)
2.5	4.25
5	4.25
10	1.6
15	1.1
20	0.8
25	0.7
30	0.6

Table 3.3 shows the throughput values recorded in the OSPFv3 network. The simulation times (in minutes) that are used to measure these values are 0.5, 2, 4, 5, 10, 15, and 20. Their corresponding throughput values (in bits/sec) recorded are 1590, 600, 380, 300, 190, 170, and 100 respectively.

Table 3. 3 : OSPFv3 Throughput

Simulation time (minutes)	OSPFv3(bits/second)
0.5	1,590
2	600
4	380
5	300
10	190
15	170
20	100

Table 3.4 shows how the Sales & Marketing and Finance & Accounting link was utilized by OSPFv3. The simulation time intervals used to record the link utilization values are 0–1, 5, 10, 15, 20, 25, and 30. Their corresponding link utilization values (in %) are 0.018, 0.010,

0.008, 0.005, 0.004 and 0.003 respectively.

Table 3. 4 : OSPFv3 Link utilization

Simulation time (minutes)	OSPFv3 (%)
0–1	0.060– 0.102
5	0.018
10	0.010
15	0.008
20	0.005
25	0.004
30	0.003

Table 3.5 shows the results recorded for database query response time in the OSPFv3 network. The simulation time intervals (in minutes) used are 2, 3–5, 10, 15, 20, 25, and 30. Their corresponding values for database query response time (in seconds) are respectively 0.02–4.90, 4.0–2.4, 2.0, 2.1, 1.9, 1.8, and 1.7.

Table 3. 5 : OSPFv3 Database query response time

Simulation time (minutes)	OSPFv3 (seconds)
2	0.02–4.90
3–5	4.00–2.40
10	2.00
15	2.10
20	1.90
25	1.80
30	1.70

Table 3.6 shows the values recorded for database query traffics received (in bytes/sec) in the OSPFv3 network. These values are 10000, 70000, 77000, and 78000. The corresponding simulation times during which these values were recorded are 2, 10, 20, and 30 respectively.

Table 3. 6 :OSPFv3 Database query traffic received

Simulation time (minutes)	OSPFv3 (bytes/second)
2	10000
10	70000
20	77000

30	78000

Table 3.7 shows the values of ftp download response time (in seconds) recorded in the OSPFv3 network. The simulation time intervals (in minutes) during which these values were recorded are 3, 5, 10, 15, 20, 25, and 30. Their corresponding ftp download response time values recorded are 13.5, 10.0, 5.4, 5.5, 5.3, 5.2, and 5.1 respectively.

Table 3. 7 : OSPFv3 Ftp download response time

Simulation time (minutes)	OSPFv3(seconds)
3	13.5
5	10.0
10	5.4
15	5.5
20	5.3
25	5.2
30	5.1

Table 3.8 shows the values recorded for ftp upload response time (in seconds) for OSPFv3. The simulation times (in minutes) during which these values were recorded are 2–3, 5, 10, 15, 20, 25, and 30. The corresponding ftp upload response time values recorded are 0.20–20.00, 8.00, 7.00, 9.00, 5.60, 5.40 and 5.39 respectively.

Table 3. 8 : OSPFv3 Ftp upload response time

Simulation time (minutes)	OSPFv3 (seconds)
2–3	0.20–20.00
5	8.00
10	7.00
15	9.00
20	5.60
25	5.40
30	5.39

Table 3.9 shows the values recorded for ftp traffics received (in bytes/sec) in OSPFv3. These values are 9800, 8000, 5800, 5700, 5400, 5200, and 5000. The simulation time (in minutes) during which these values were recorded are respectively 2, 5, 10, 15, 20, 25, and 30. **Table 3. 9 : OSPFv3 Ftp traffics received**

Simulation time (minutes)	OSPFv3 (bytes/sec)
2	9800
5	8000
10	5800
15	5700
20	5400
25	5200
30	5000

Table 3.10 shows the values recorded for remote login response time (in seconds) in the OSPFv3 network. The simulation time intervals during which these values were recorded are 2–4, 5, 10, 15, 20, 25, and 30. The corresponding remote login response time values are 0.10–1.58, 1.2, 1.2, 1.4, 1.2, 1.2, and 1.0 respectively.

Table 3. 10 : OSPFv3 Remote login response time

Simulation time (minutes)	OSPFv3 (seconds)
2–4	0.10–1.58
5	1.2
10	1.2
15	1.4
20	1.2
25	1.2
30	1.0

Table 3.11 shows the values recorded for http page response time (in seconds) in the OSPFv3 network. The simulation time intervals during which these values were recorded are 2–4, 5, 10, 15, 20, 25, and 30. The corresponding http page response time values recorded against these times are 0.1–13, 8.0, 7.0, 9.0, 7.0, 6.0, and 6.5 respectively.

Table 3. 11 : OSPFv3 Http page response time

Simulation time (minutes)	OSPFv3 (seconds)
2–4	0.1–13
5	8.0
10	7.0
15	9.0
20	7.0

25	6.0
30	6.5

Table 3.12 shows email download response time values (in seconds) recorded in the OSPFv3 network. The simulation time intervals during which these values were recorded are 3, 5, 10, 15, 20, 25, and 30. The corresponding email download response time values recorded against these times are 6.4, 4.0, 2.4, 3.8, 2.8, 2.6, and 2.4 respectively.

Table 3. 12 : OSPFv3 Email download response time

Simulation time (minutes)	OSPFv3 (seconds)
3	6.4
5	4.0
10	2.4
15	3.8
20	2.8
25	2.6
30	2.4

3.3.5 IS–IS Scenario

Figure 3.12 shows the IS–IS scenario used in the simulation. This scenario is a copy of the OSPFv3 scenario but configured with IS–IS only. The reason for doing this is to separately measure the effect of IS–IS performance on the selected applications that are defined in the network topology. Since the performance of IS–IS is measured in IPv6, IPv6 addresses were automatically enabled in the topology before this protocol was configured. Enabling IPv6 addresses and IS–IS in this scenario were done by following the same procedures used to enable IPv6 addresses and OSPFv3 in the first scenario.

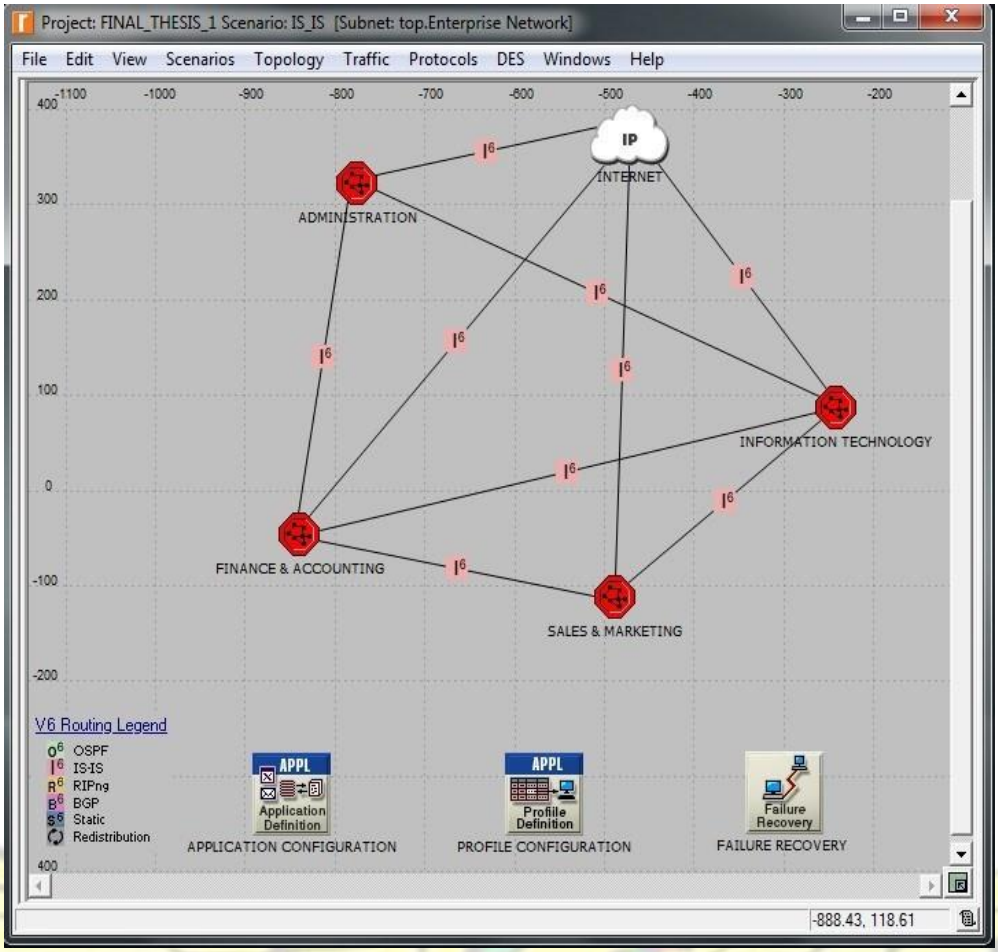


Figure 3. 12 : IS–IS Scenario

After enabling IPv6 Addresses and IS–IS, the same parameters chosen for the OSPFv3 scenario were again chosen to simulate this scenario. This was done so that the performance of the IS–IS routing protocol can be observed and recorded. Choosing the parameters was done by following the same procedure used to set parameters in the OSPFv3 scenario. Also, similarly done in the OSPFv3 scenario, total simulation time for this scenario was also set to last for 30 minutes after choosing the parameters.

When the simulation ended, results were recorded for the following parameters: convergence duration, IPv6 traffic dropped, throughput, link utilization, database query (response time and traffic received), ftp download/upload response times, ftp traffics received, remote access, email and web page response times. These are the parameters chosen to measure how IS–IS will perform when it is used separately to route the selected applications in IPv6. Results were

recorded for each parameter at a particular time during the simulation. These results and their corresponding simulation times are numerically shown in the following tables:

Table 3.13 shows the values recorded for IS–IS convergence time during the simulation. The simulation time intervals (in minutes) used for measuring these values are 0.5, 2, 3, 4, 5, and 8. The corresponding values of the convergence time (in seconds) recorded are 12.3, 10.9, 9.9, 8.9, 6.9, and 2.3 respectively.

Table 3. 13: IS–IS Convergence time

Simulation time (minutes)	IS–IS (seconds)
0.5	12.3
2	10.9
3	9.9
4	8.9
5	6.9
8	2.3
-	-

Table 3.14 shows the values recorded for IPv6 traffics dropped in the IS–IS network. Simulation time intervals (in minutes) during which the values were recorded are 2.5, 5, 10, 15, 20, 25, and 30. The corresponding values recorded for IPv6 traffics dropped (in packets/sec) are 4.25, 3.40, 2.98, 2.90, 2.80, 2.70, and 2.60 respectively.

Table 3. 14 : IS–IS IPv6 traffics dropped

Simulation time (minutes)	IS–IS (packets/sec)
2.5	4.25
5	3.40
10	2.98
15	2.90
20	2.80
25	2.70
30	2.60

Table 3.15 shows the throughput values recorded in the IS–IS network. The simulation times (in minutes) that are used to measure these values are 0.5, 2, 4, 5, 10, 15, and 20. Their

corresponding throughput values (in bits/sec) recorded are 425, 200, 140, 100, 50, 40, and 30 respectively.

Table 3. 15 : IS–IS Throughput

Simulation time (minutes)	IS–IS (bits/sec)
0.5	425
2	200
4	140
5	100
10	50
15	40
20	30

Table 3.16 shows how the Sales & Marketing and Finance & Accounting link was utilized by IS–IS. The simulation time intervals used to record the link utilization values are 0–1, 5, 10, 15, 20, 25, and 30. Their corresponding link utilization values (in %) are 0.01–0.028, 0.008, 0.005, 0.004, 0.002, 0.002 and 0.002 respectively.

Table 3. 16 : IS–IS Link utilization

Simulation time (minutes)	IS–IS (%)
0–1	0.010–0.028
5	0.008
10	0.005
15	0.004
20	0.002
25	0.002
30	0.002

Table 3.17 shows the results recorded for database query response time in the IS–IS network. The simulation time intervals (in minutes) used are 3, 5, 10, 15, 20, 25, and 30. Their corresponding values for database query response time (in seconds) are respectively 0.038, 0.0374, 0.0370, 0.0370, 0.0377, 0.0376, and 0.0375.

Table 3. 17 : IS–IS Database query response time

Simulation time (minutes)	IS–IS (seconds)
3	0.0380
5	0.0374

10	0.0370
15	0.0370
20	0.0377
25	0.0376
30	0.0375

Table 3.18 shows the values recorded for database query traffics received (in bytes/sec) in the IS–IS network. These values are 10000, 24000, 27000, and 28000. The corresponding simulation times during which these values were recorded are 2, 10, 20, and 30 respectively.

Table 3. 18 : IS–IS Database query traffics received

Simulation time (minutes)	IS–IS (packets/sec)
2	10000
-	-
10	24000
-	-
20	27000
-	-
30	28000

Table 3.19 shows the values of ftp download response time (in seconds) recorded in the IS–IS network. The simulation time intervals (in minutes) during which these values were recorded are 3, 5, 10, 15, 20, 25, and 30. Their corresponding ftp download response time values recorded are 0.155, 0.159, 0.162, 0.144, 0.162, 0.160, and 0.153 respectively.

Table 3.19: IS–IS Ftp download response time

Simulation time (minutes)	IS–IS (seconds)
3	0.155
5	1.159
10	0.162
15	0.144
20	0.162
25	0.160
30	0.153

Table 3.20 shows the values recorded for ftp upload response time (in seconds) for IS–IS. The simulation times (in minutes) during which these values were recorded are 2–3, 5, 10,

15, 20, 25, and 30. The corresponding ftp upload response time values recorded are 0.346–0.326, 0.324, 0.318, 0.320, 0.325, 0.330 and 0.325 respectively.

Table 3. 20: IS–IS Ftp upload response time

Simulation time (minutes)	IS–IS (seconds)
2–3	0.346–0.326
5	0.324
10	0.318
15	0.320
20	0.325
25	0.330
30	0.325

Table 3.21 shows the values recorded for ftp traffics received (in bytes/sec) in IS–IS. These values are 4000, 2000, 2100, 2100, 2200, 2100, and 2000. The simulation time (in minutes) during which these values were recorded are respectively 2, 5, 10, 15, 20, 25, and 30.

Table 3.21: IS–IS Ftp traffics received

Simulation time (minutes)	IS–IS (seconds)
2	4000
5	2000
10	2100
15	2100
20	2200
25	2100
30	2000

Table 3.22 shows the values recorded for remote login response time (in seconds) in the IS– IS network. The simulation time intervals during which these values were recorded are 2–4, 5, 10, 15, 20, 25, and 30. The corresponding remote login response time values are 0.002–0.048, 0.046, 0.047, 0.050, 0.051, 0.052, and 0.053 respectively.

Table 3. 22 : IS–IS Remote login response time

Simulation time (minutes)	IS–IS (seconds)
2–4	0.002–0.048
5	0.046

10	0.047
15	0.050
20	0.051
25	0.052
30	0.053

Table 3.23 shows the values recorded for http page response time (in seconds) in the IS–IS network. The simulation time intervals during which these values were recorded are 2–4, 5, 10, 15, 20, 25, and 30. The corresponding http page response time values recorded against these times are 0.39–0.29, 0.31, 0.31, 0.31, 0.31, 0.31 and 0.31respectively. **Table 3.23: IS–IS Http page response time**

Simulation time (minutes)	IS–IS (seconds)
2–4	0.39–0.29
5	0.31
10	0.31
15	0.31
20	0.31
25	0.31
30	0.31

Table 3.24 shows the values recorded for email download response time (in seconds) in the IS–IS network. The simulation time intervals during which these values were recorded are 3, 5, 10, 15, 20, 25, and 30. The corresponding email download response time values recorded against these times are 0.009, 0.008, 0.008, 0.008, 0.008, 0.007, and 0.012 respectively.

Table 3. 24: IS–IS Email download response time

Simulation time (minutes)	IS–IS (seconds)
3	0.009
5	0.008
10	0.008
15	0.008
20	0.008
25	0.007
30	0.012

CHAPTER 4

SIMULATION RESULTS

4.0 Overview

In this chapter, results obtained from the simulation are analyzed. The results are presented in form of graphs. Riverbed Modeler Academic Edition 17.5, which is the main simulator used is configured to produce a graphical result of all the simulation parameters chosen. The entire thesis is divided into two scenarios. The purpose of doing this is to measure how each routing protocol will perform when used separately to route the selected applications in IPv6. Scenario one is an IPv6 network model configured with OSPFv3. Scenario two is the same network model but configured with IS–IS. In both scenarios, the link between Sales & Marking department and Finance & Accounting department is configured to fail at 240 seconds and then recover at 480 seconds so that the network convergence duration and throughput can be measured for both scenarios. Also, the total simulation time for each scenario is set to last for 30 minutes.

4.1 Simulation Results and Analysis

This section presents the discussion of results obtained from the simulation. Each result is obtained based on the parameters chosen to measure the performance of both routing protocols.

4.1.1 Convergence time

The convergence time of both routing protocols is shown in Figure 4.1. Convergence time of a routing protocol measures the time taken by all routers using that protocol to have a complete knowledge about the topology of the entire internetwork. Convergence time of a routing protocol is an important parameter for measuring network performance because it contributes to network speed. The faster a routing protocol can converge, the faster the speed of its network. From this figure, it can be observed that convergence duration for both routing protocols is

nearly the same. However, there is a slight variation as shown in the graph. At exactly 0.5 minute into the simulation, IS–IS converged a little faster than OSPFv3. The value for convergence time in the IS–IS network at this time is 12.3 seconds while it is 12.5 seconds in the OSPFv3 network. Both protocols took these times to converge because they need to build their neighbor, topology and routing tables in order to have a complete knowledge about the network before they can start forwarding packets. Between 2 to 3 minutes during simulation, IS–IS slightly shows better performance over OSPFv3. When the link failed at 240 seconds (4 minutes), the convergence time of IS–IS and OSPFv3 decreased to 9.0 and 8.9 seconds respectively. When the link recovered at 480 seconds (8 minutes), convergence duration for both protocols again decreased to around 2.4 and 2.3 seconds respectively. Convergence duration for both protocols decreased at this time because their routers only need to communicate the link failure and update their topology tables. Although convergence time for both routing protocols keeps decreasing until the simulation ended, IS– IS converged faster than OSPFv3. The reason for this routing behavior might be the minimal number of packets IS–IS uses during its routing process. When there is a route or node failure in a network, link–state protocols will have to update their topology databases. While OSPFv3 routers will have to flood LSAs to their neighbors in order to recalculate entries in their routing table, IS–IS routers will have to flood LSPs to their neighbors in order to do the same. Though the routing process remains the same for both protocols during network topology changes, OSPFv3 uses more packets and as a result it takes much time to converge. Comparing these results to those obtained by Thorenoor (2010) confirmed that IS–IS has a better convergence time than OSPF. In her simulation, whereas both IS–IS and OSPF initially took 5.4 and 29 seconds to converge, both routing protocols initially took 12.3 and 12.5 seconds to converge in this simulation. Even though the difference in the numerical values obtained here is small, all numerical values measured for IS–IS show that IS–IS recorded the faster convergence time.

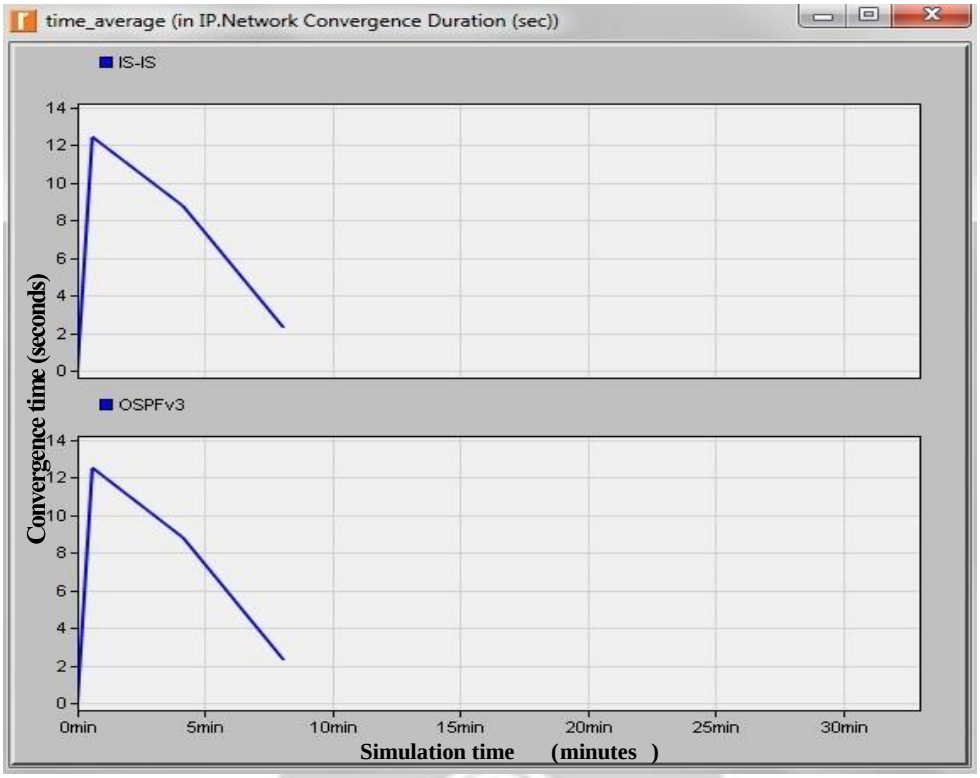


Figure 4. 1 : Network Convergence Duration (seconds)

4.1.2 Throughput

Network throughput is an important parameter. This parameter is used to measure the average number of bits received or transmitted successfully by the receiver or the transmitter channel per second. Measuring network throughput is done in bits per second or sometimes in packets per second (Pan et al., 2008). The throughput obtained from the Sales & Marketing and Finance & Accounting link is shown in Figure 4.2. It can be seen in this figure that the OSPFv3 network has a higher throughput than the IS–IS network. At around

0.5 minute during simulation, the average number of bits transmitted successfully via the Sales & Marketing and Finance & Accounting link per second in the OSPFv3 network is about 1,590 bits. This value is about four times higher than the 425 bits delivered through the same link in the IS–IS network. As the link fails at 4 minutes, throughput values for both scenarios drop significantly. While the throughput value for OSPFv3 falls to 380 bits, the value for IS–IS falls to 140 bits. Even as the link recovered at 8 minutes during the simulation, protocol performance became very poor as the throughput values for both OSPFv3 and IS–IS

respectively fall below 200 and 100 bits/sec. However, performance of the OSPFv3 network is better than the IS–IS network. The reason for this poor performance is as a result of the process each protocol has to go through after the link failure before it can converge again. When a link failure occurs within a network, link–state protocols take some time to converge and this consequently affects network throughput.

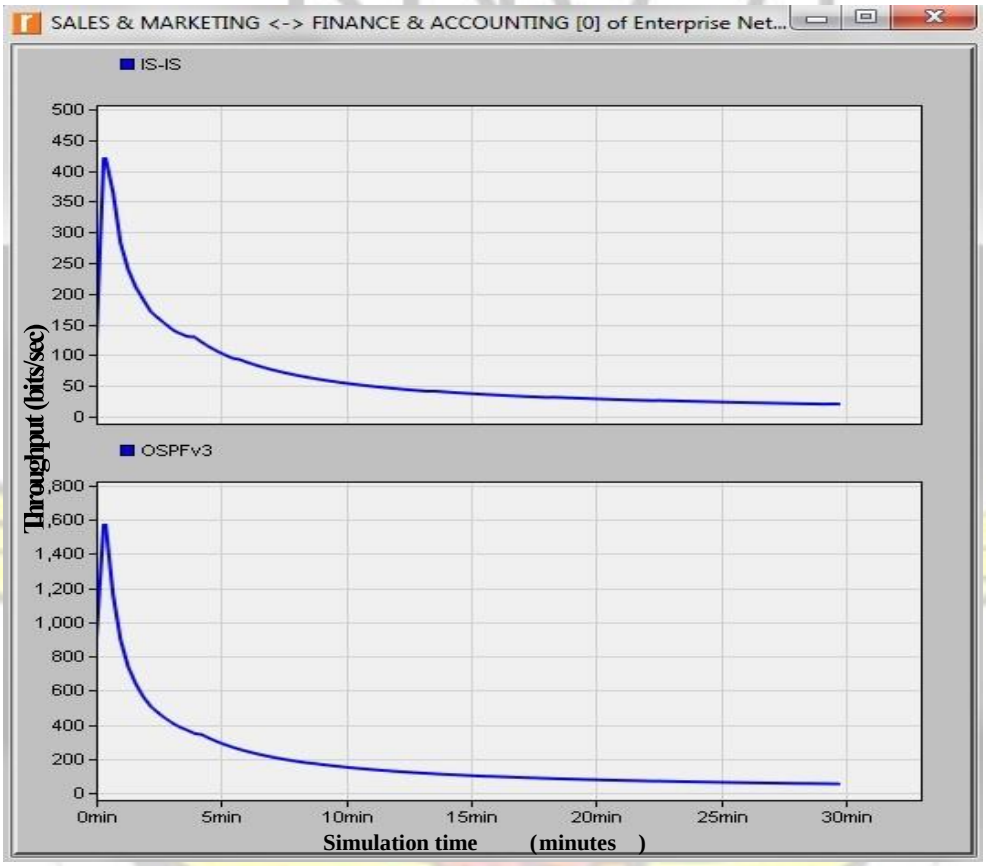


Figure 4. 2 : Throughput (bits/sec).

4.1.3 Link utilization

Link utilization measures how much of a network bandwidth (in percent) is being consumed by traffics generated in the network. Figure 4.3 shows how the Sales & Marketing and Finance & Accounting link was utilized for both routing protocols. It can be observed that as the simulation starts, link utilization value for IS–IS increases from 0.01% to about 0.028%. At around 3 minutes, this value decreases back to 0.01% and then continues to decrease from 5 minutes through to the end of the simulation. In the case of the OSPFv3 network, link

utilization value increases from 0.06% at the start of simulation time and then increases to 0.102%. At around 5 minutes, this value decreases to 0.018% and then continues to decrease until the end of simulation time. Comparing these values, it can be concluded that IS–IS has the minimum link utilization and hence it is better than OSPFv3 in terms of this parameter. This happened as a result of the small amount of network traffic received in the IS–IS network. If traffic received in the network is high it is an indication that link utilization will be high and the possibility that link congestion will happen is also high. This may be the case of the OSPFv3 network.

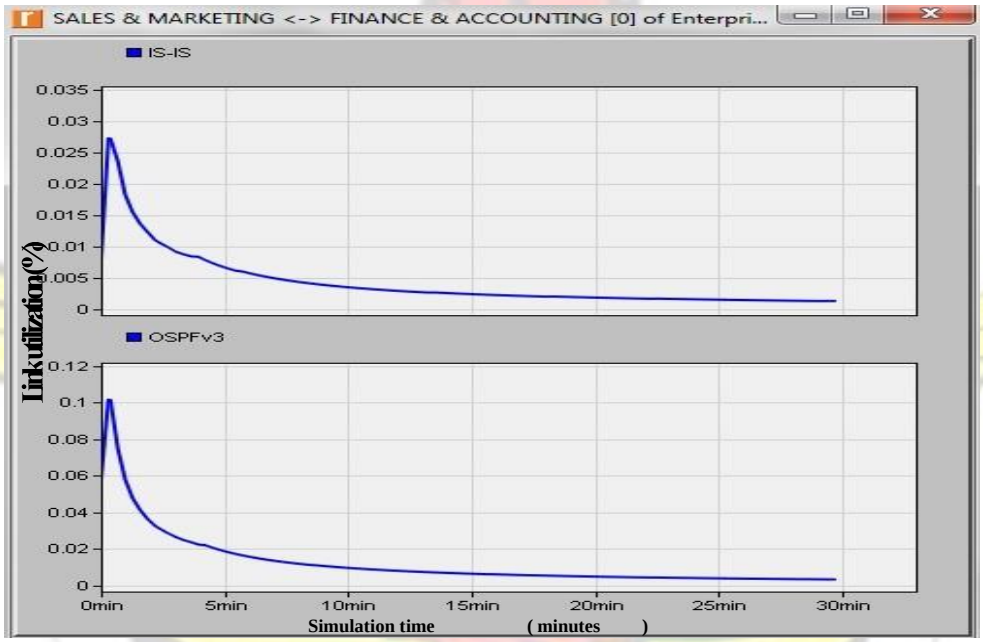


Figure 4. 3 : Link utilization (%)

4.1.4 IPv6 traffics dropped

This parameter measures the total amount of IPv6 packets lost by every node within a network. Several reasons could lead to a packet being dropped in a network. For example when more traffic is forwarded through the network, the network can become congested leading to higher bandwidth utilization. In a congested network, packet delivery is delayed. When this happens some packets are dropped without reaching their destination. Figure 4.4 shows IPv6 traffic dropped by both OSPFv3 and IS–IS. From this figure, it can be seen that both protocols

dropped a maximum number of 4.25 packets per second within 2.5 minutes of simulation time. However, in the IS–IS network, this value started from 0 and then rises to the maximum value (4.25) before it begins to decrease. In the OSPFv3 network, this value rather started from 3.7 and then increased to the maximum value (4.25). OSPFv3 maintained this value through to about 4 minutes before it started decreasing. In the IS–IS scenario, the value for this statistic starts dropping from around 3 minutes during simulation time. At around 10 minutes, the number of IPv6 traffic dropped in the IS–IS network is around 2.9 packets. Just before the end of simulation time, this valued gradually reduced to about 2.6 packets per second. Even though when the simulation was about to end, total number of IPv6 traffic dropped in the OSPFv3 network significantly reduced to 0.6 packets per second. OSPFv3 dropped more IPv6 packets when the simulation stated. This must have happened as a result of the more traffic received in the OSPFv3 network indicating the possibility of network congestion.

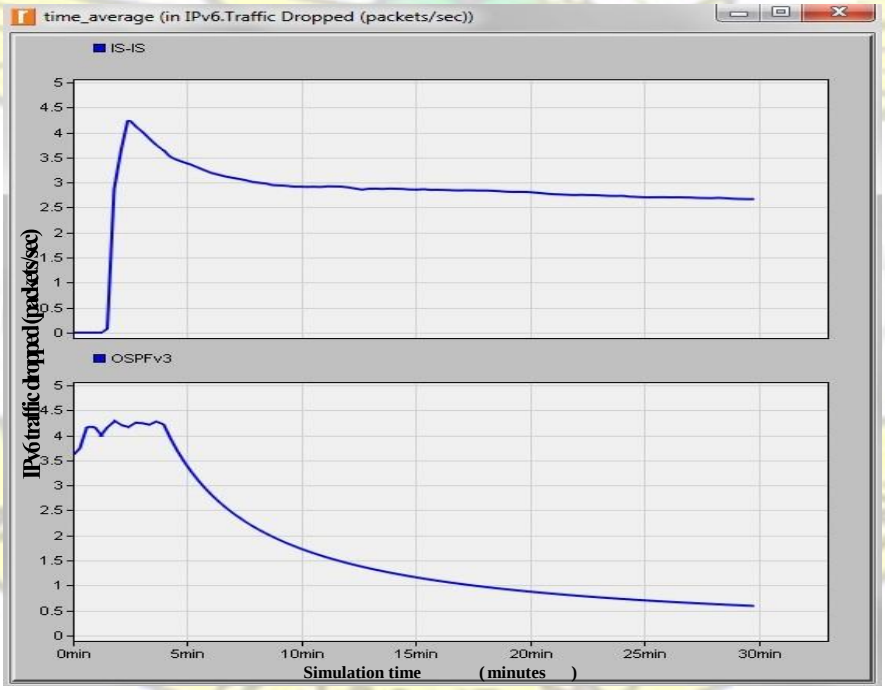


Figure 4. 4 : IPv6 traffics dropped (packets/sec)

4.1.5 Database query response time

This parameter is used to measure how long it takes a database query application to submit request and then get the reply back from the database server. Figure 4.5 indicates how protocol performance has affected the way the database server has been accessed in the network. From this simulation result, it is observed that IS–IS performed better than OSPFv3. At exactly 2 minutes into the simulation time, database query response time for the IS–IS network is 0.038 second while that of the OSPFv3 network increased from 0.02 second to 4.9 seconds. Between 3 to 5 minutes during simulation, database query response time for both scenarios began to decrease significantly. Database query response time of IS–IS reduced to 0.0374 second while that of the OSPFv3 network decreased from 4 seconds to 2.4 seconds. When the simulation was about to end, the value for this parameter in the IS–IS network further decreased below 0.037 second. In the OSPFv3 network, this value also further decreased below 2.1 seconds and keeps decreasing until the simulation ended. Performance of OSPFv3 is slow in terms of database query response time because the protocol took some time to converge and this consequently affected its speed. As a result, more time is taken to receive database queries from the server in the OSPFv3 network.

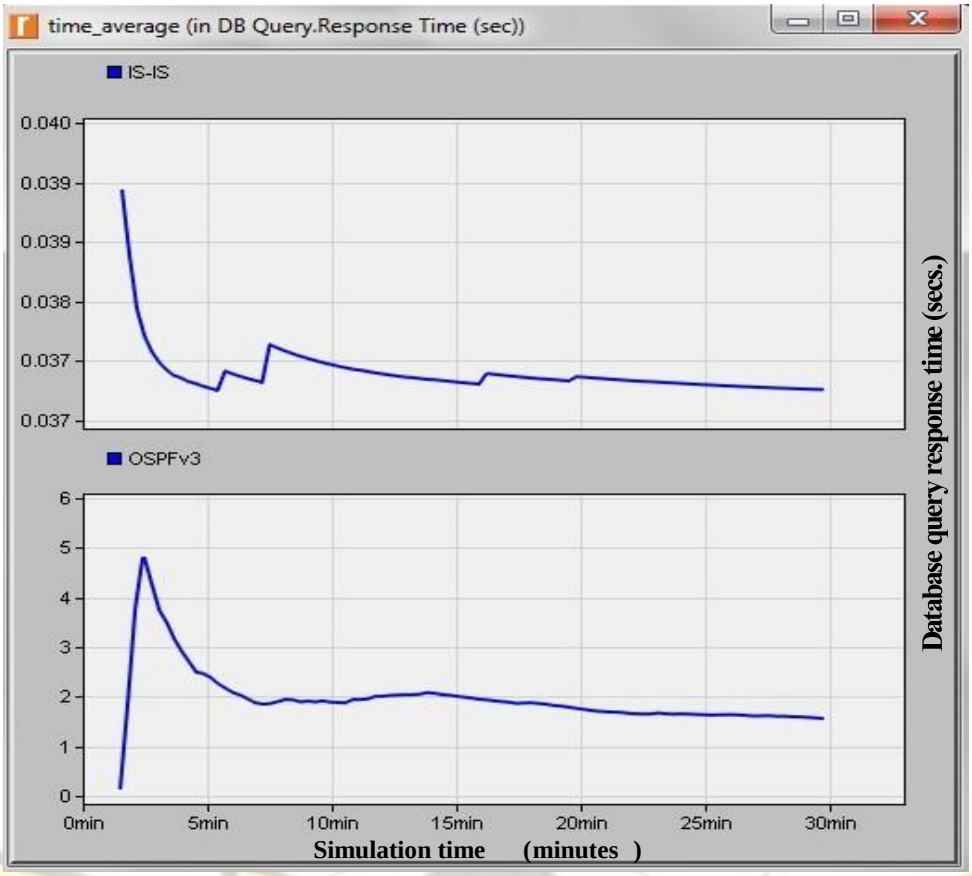


Figure 4. 5 : Database query response time (Seconds)

4.1.6 Database query traffics received

The database query traffics received in the network is shown in Figure 4.6. This statistic represents the average bytes that are forwarded every second by the transport layers to a database query application that accesses the server. From the figure, it can be seen that the OSPFv3 scenario performs better than the IS–IS scenario. During 2 minutes of simulation time, 10,000 bytes of database query traffic was received in both scenarios. However, at around 10 minutes, 70,000 bytes of database query traffic was received in the OSPFv3 network. This value increased to about 77,000 bytes at 20 minutes during simulation. It further increased to 78,000 bytes and remains approximately the same until the end of the simulation. In the IS–IS network, database query traffic received was only 24,000 bytes even though the simulation time increases. Getting to the end of the simulation, database query traffic received in the IS–IS network increased to about 27,000 bytes. This value further increased to 28,000 bytes and

remains approximately the same until the end of the simulation. From this simulation result, it can be concluded that the OSPFv3 network performs better than IS–IS in terms of database query traffic received.

Figure 4. 6 : Database query traffics received (bytes per second)

4.1.7 FTP download response time

Simulation result obtained for this parameter is shown in Figure 4.7. FTP download response time is used in measuring how long it takes all ftp applications to submit a request and then get a reply back from the FTP Server. In Figure 4.7, it is observed that the performance of the IS–IS scenario outweighs that of the OSPFv3 scenario. Both scenarios start after 3 minutes during simulation time but the OSPFv3 network recorded a peak value of

13.5 seconds while the IS–IS network recorded a peak value of 0.155 second. As seen in the figure, ftp download response time of the OSPFv3 network drops significantly between 5 and 10 minutes into the simulation while in the IS–IS network this value increased from 1.55

seconds to 1.59 seconds. This happened as a result of the link failure introduced in both scenarios. After both networks converged, ftp download response time of both scenarios rose again at 15 minutes during simulation with the IS–IS network performing better than the OSPFv3 network. Although the value of this parameter in the IS–IS network increased to about 0.162 second and kept decreasing again toward the end of simulation time, it is still smaller than the values recorded in the OSPFv3 scenario. Hence on the basis of ftp download response time, IS–IS is more suitable.

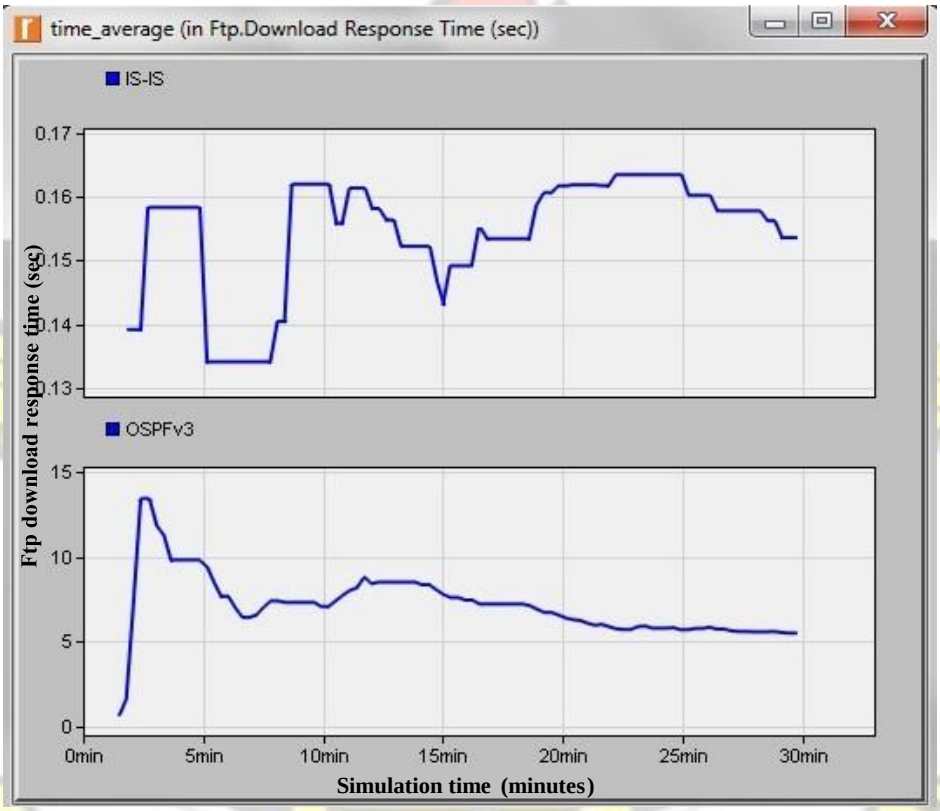


Figure 4. 7 : FTP Download Response Time (seconds.)

4.1.8 FTP upload response time

Simulation result obtained from scenario one and scenario two for this parameter is shown in Figure 4.8. From this figure, it can be seen that the performance of IS–IS is better than OSPFv3. Between 2 to 3 minutes into the simulation time, the IS–IS scenario recorded the highest ftp upload response time of 0.346 second. This value then decreased to 0.326 second between the same time intervals. At this time into the simulation, ftp upload response time for the OSPFv3

scenario increased from 0.2 to 20 seconds. Between 5 and 10 minutes during simulation, ftp upload response time for IS–IS scenario decreased from 0.324 to 0.318 seconds while that of the OSPFv3 decreased from 8 to 7 seconds. Towards the end of simulation time, ftp upload response time for IS–IS network kept rising and falling between 0.320 and 0.325 seconds till the end of the simulation. However, although the values for ftp upload response time for the OSPFv3 network kept decreasing from 15 minutes through to the end of simulation, these values are still higher than that of the values recorded in IS–IS network. Hence IS–IS performs better than OSPFv3 in terms of this parameter.

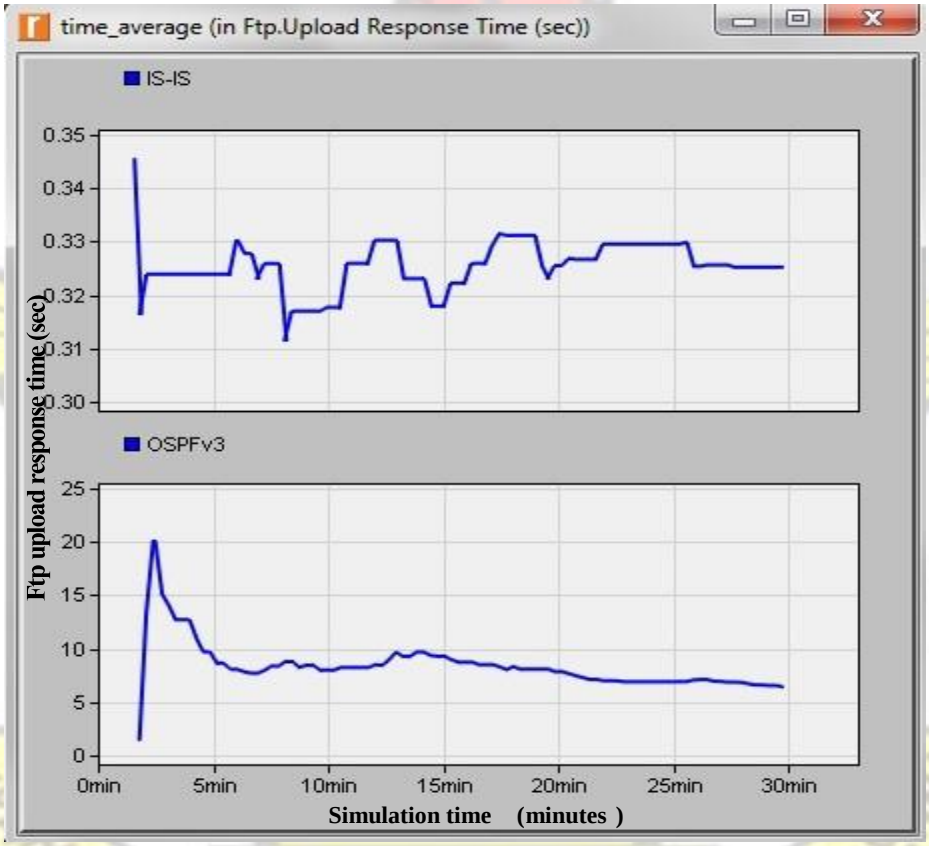


Figure 4. 8 : FTP upload response time (seconds.)

4.1.9 FTP traffic received

This parameter measures the total traffic in bytes or packets that are forwarded every second, by the transport layer to each Ftp application within a network. Figure 4.9 shows how protocol performance affected total ftp traffic received in both scenarios. At around 2 minutes during

simulation, both scenarios recorded their peak values for the ftp traffic received. At this time total ftp traffic received in the OSPFv3 network is approximately 9,800 bytes per second whereas the ftp traffic received in the IS–IS network is 4,000 bytes per second. However, as simulation time approaches 5 minutes, the values for ftp traffic received in both scenarios began to decrease. At exactly 10 minutes, total ftp traffic received in the OSPFv3 scenario and the IS–IS scenario respectively decreased to about 5,800 bytes and 2,100 bytes per second. These values further decreased to 5000 bytes and 2,000 bytes per second at the end of the simulation. From these simulation results, it can be concluded that the OSPFv3 network performs better than the IS–IS network in terms of ftp traffic received.

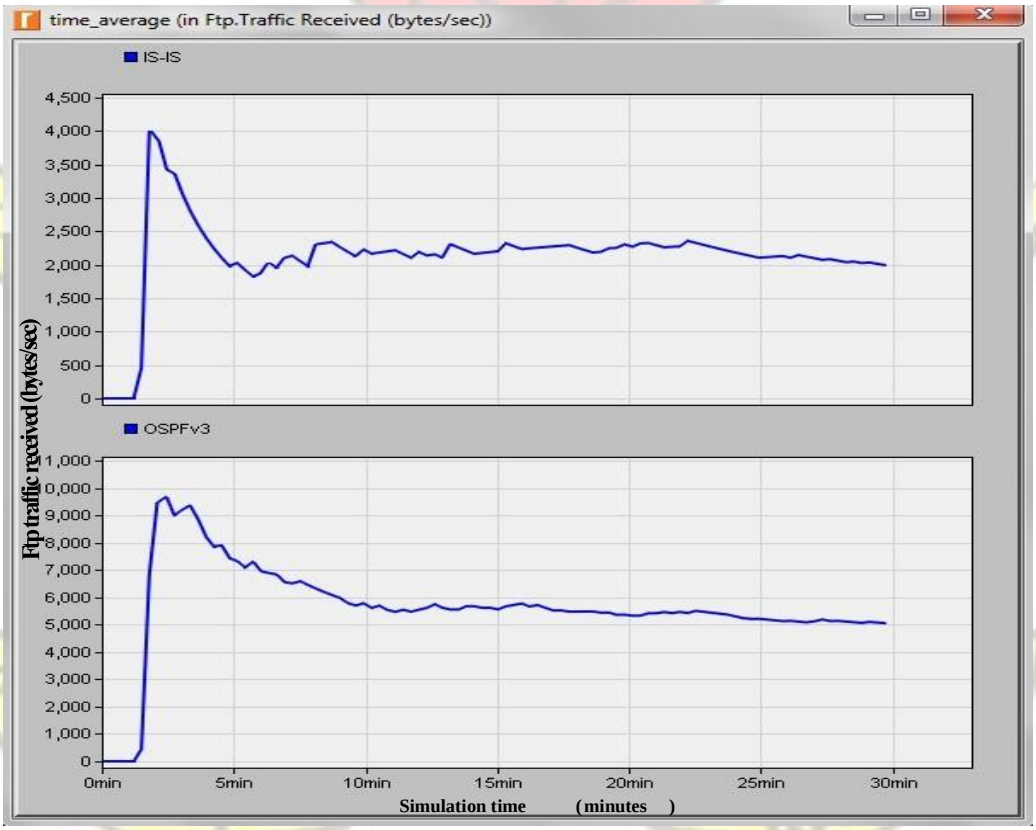


Figure 4. 9 : Ftp Traffic Received (bytes/sec.)

4.1.10 Remote login response time

Figure 4.10 shows how protocol performance affected remote access or login response times in both scenarios. This parameter is used in measuring how long it takes client applications to send their requests to a remote login server and receive their response packets.

From Figure 4.10, it can be seen that remote login response time for both scenarios increased from 2 to 4 minutes of simulation time. While the value for the OSPFv3 network at this time increased from 0.1 to 1.58 seconds, the value of the IS–IS network increased from 0.002 second to 0.048 second. These values further decrease to 1.2 seconds between 5 to 10 minutes in the OSPFv3 network. At 15 minutes during simulation, remote login response time of the OSPFv3 network increased again to 1.4 seconds. It then kept decreasing from 20 minutes until the simulation ended. However, as simulation time increases towards 5 minutes, remote login response time of the IS–IS network decreased to 0.046 second. This value then kept increasing again from 0.047 second at 10 minutes through to the end of the simulation. At the end of the simulation, remote login response time recorded in the IS–IS network is around 0.053 second. This value is smaller than the 1 second recorded by the OSPFv3 network and hence IS–IS network performs better than the OSPFv3 network for this parameter.

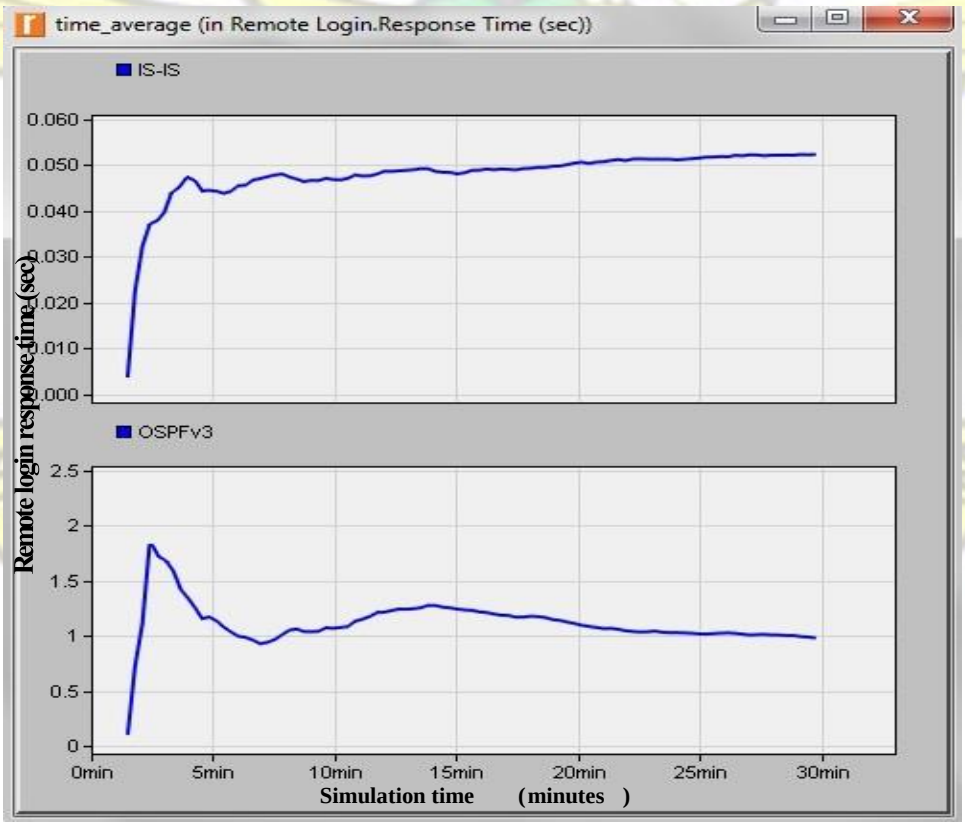


Figure 4. 10 : Remote Login Response Time (seconds.)

4.1.11 HTTP page download response time

HTTP page response time is used to measure the time taken in retrieving a whole web page with every inline object it contains. In Figure 4.11, http page response times for both the OSPFv3 and the IS–IS scenarios are shown. From this figure, it can be seen that performance of the IS–IS scenario is better than the OSPFv3 scenario. Between 2–4 minutes of simulation time, the value for this parameter falls from 0.39 second to 0.29 second in the IS–IS scenario. From around 5 minutes to the end of simulation time, http page response time of the IS–IS scenario rise a little above 0.30 second until the end of simulation time. In contrast to the OSPFv3 scenario, this is different. Between 2–4 minutes of simulation time, http page response time of the OSPFv3 scenario rather increased from around 0.1 second to 13 seconds.

As simulation time approaches 4 minutes, this value decreased significantly. Between 5 and 10 minutes, http page response time in the OSPFv3 network decreased from 8 seconds to 7 seconds. This value increased again to 9 seconds at 15 minutes during simulation and then began to decrease until the end of the simulation. From this simulation result, it can be concluded that http page response time for IS–IS is faster than that of OSPFv3.

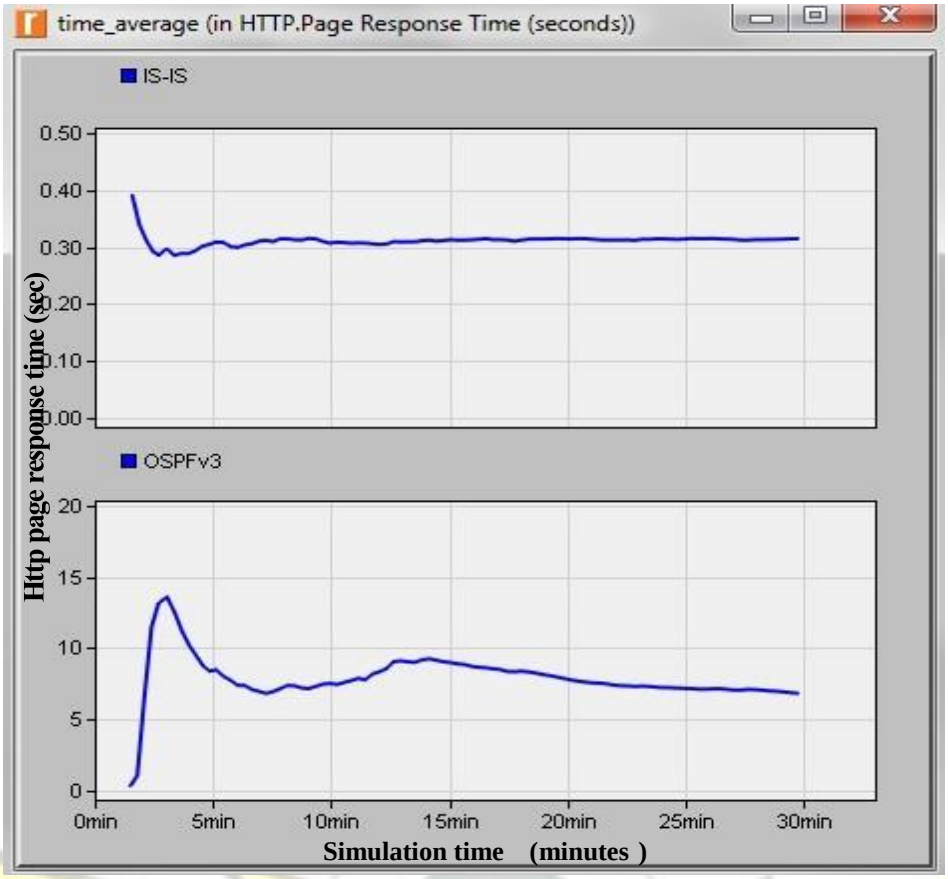


Figure 4. 11 : Http Page Response Time (sec.)

4.1.12 Email download response time

This parameter measures the time taken to send and retrieve an email from an email server in a network. Figure 4.12 shows how protocol performance has affected email retrieval in both scenarios. At 2 to 3 minutes during simulation, the value of email download response time of the IS–IS network is approximately 0.009 second. This value then decreased to 0.008 between 5 and 20 minutes of simulation time. At 25 minutes of simulation time, email download response time of the IS–IS network further decreased to 0.007 second. It then increased again to 0.012 second and remained there until the simulation ended. In contrast to the OSPFv3 network, email download response time increased from 0 to 6.4 seconds during 2 to 3 minutes of simulation time. This value decreased from 4 seconds to 2.4 seconds between 5 to 10 minutes of simulation time. At exactly 15 minutes of simulation time, this value increased again to 3.8

seconds but started to decrease until the simulation ended. Comparing these values, it can be concluded that IS–IS is more suitable for routing email than OSPFv3.

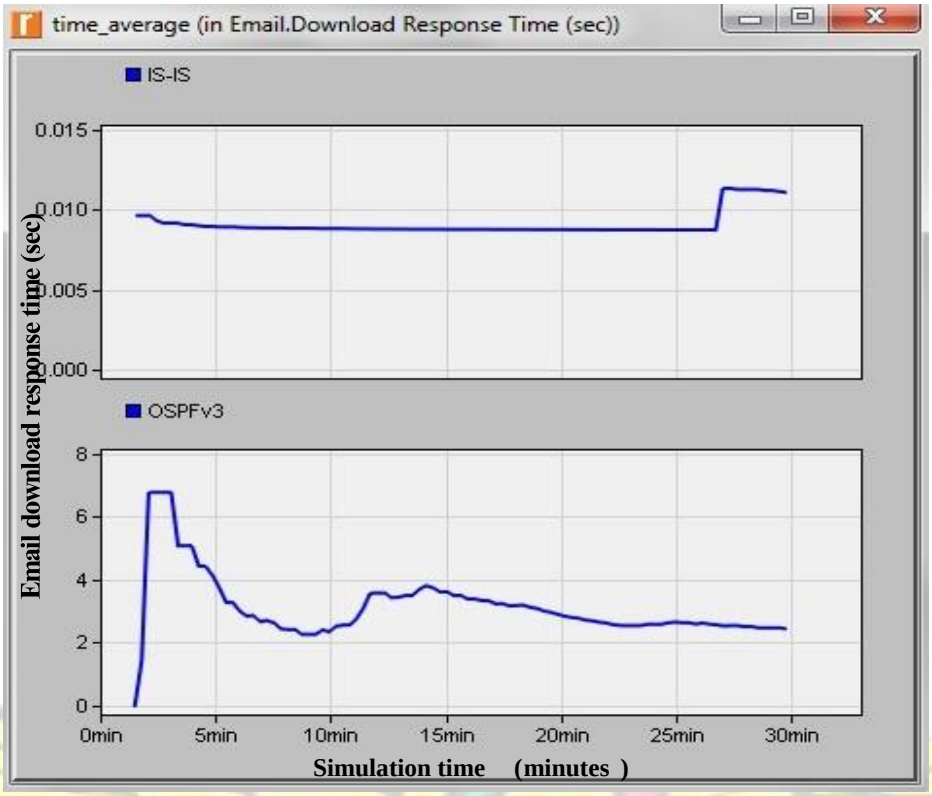


Figure 4. 12 : Email Download Response Time (seconds)

CHAPTER 5

SUMMARY, CONCLUSION, AND RECOMMENDATION

5.1 Conclusion

The choice of a suitable routing protocol for implementation is an important part of every network design. During routing protocol implementation, several decisions are considered in order to select the best protocol for deployment. These decisions are usually taken on the basis of some quantitative parameters that are used to determine which protocol will perform better than others whenever there are different routing protocols available. The routing protocol with the best performance in terms of these parameters is considered the most suitable protocol and is selected for implementation.

In this thesis, performance of two routing protocols (OSPFv3 and IS–IS) for IPv6 has been measured and compared by simulation for some selected applications including email, ftp, database, http, and remote access. The purpose of comparing these protocols is to find out which of them will be more suitable for routing the selected applications in IPv6 networks. In other to achieve this purpose, the simulation was divided into two scenarios. The first scenario is an IPv6 network model configured with OSPFv3. The second scenario is a copy of the first scenario but configured with IS–IS. These scenarios were simulated and the impact of using each protocol to separately route the selected applications was observed and recoded. Performance comparison of both routing protocols is based on the following quantitative parameters: Convergence duration, IPv6 traffic dropped, throughput, link utilization, database query (response time and traffic received), ftp download /upload response times, ftp traffics received, remote access, email and web page download response times. On the basis of convergence time, simulation result obtained indicated that the convergence duration of IS–IS is a little faster than that of OSPFv3. It was observed that when there was a link failure routers in the IS–IS network learned the topology faster than the routers in the OSPFv3 network. Hence IS–IS performed better than OSPFv3 in terms of this parameter. On the basis of throughput, it is observed that the point–to–point throughput of OSPFv3 is higher than IS–IS. In terms of which protocol has recorded the minimum link utilization values, simulation results indicated that IS–IS is better among the two routing protocols. The more traffic received in the OSPFv3 network is an indication that more bandwidth was utilized in the OSPFv3 network. On the basis of which protocol dropped the least IPv6 traffic, simulation results have indicated that IS–IS performs better than OSPFv3 in terms of this parameter when the simulation started. Because more traffic was received in the OSPFv3 network, this led to network congestion and as a result OSPFv3 dropped more IPv6 packets.

To find out which of the two protocols will be more suitable for routing the selected applications, eight parameters were considered for the selected applications that are considered in this thesis. The parameters include database query response time, ftp download and upload response times, database query and ftp traffics received, remote login, http page, and email download response times. Among these parameters, simulation results show that IS–IS remains the best choice between the two protocols in terms of response time for all the applications. Because OSPFv3 took more time to converge, this has affected the network speed in its scenario and as a result the time taken to access each application server is slower than the time taken to access each server in the IS–IS network. Based on database query and ftp traffics received, simulation results indicated that OSPFv3 is better than IS–IS since the highest database and ftp traffics were received in the OSPFv3 network. OSPFv3 was able to send and receive more application traffic because the highest throughput values were recorded in its network and as a result this has an effect on the total amount of application traffic received by OSPFv3. OSPFv3 though has sent and received more traffic than IS–IS, speed of a routing protocol is an important performance indicator because it contributes to network speed. Based on these results, it can be concluded that overall, IS–IS performed better than OSPFv3.

5.2 Recommendation

Based on the simulation results obtained in this thesis, it can be seen that between the two routing protocols, IS–IS remains the more suitable protocol for routing database query, remote login, file transfer, web and email. Its convergence time and link utilization are also better than that of OSPFv3. Therefore in IPv6 era, the use of IS–IS should not be limited to telecommunication networks only. The protocol should be considered the first choice for implementation in enterprise networks.

5.3 Challenges

Some challenges were faced with the modeler from network design through to the simulation experiment. Riverbed modeler academic edition is a stripped–down version of the modeler used to model communication networks in industries. Some capabilities in the industrial version are restricted in the academic edition. Riverbed modeler academic edition does not support the use of process and node editors that can be used to view the internal structure of nodes and processes. Design in the modeler is limited to the project editor that is used for specifying the physical interconnection between nodes. Also, detailed simulation runs cannot be configured in the modeler. This has limited the simulation run to one simulation at a time but not multiple simulations. Of cause, these capabilities can be enabled in the modeler by contacting the university program administrator but incurs additional procurement cost.

5.4 Future research

In the future, research can be under taken to investigate the effect of protocol performance on other applications such Telnet. Also, both routing protocols can be combined in the same topology so that the impact of using them together can be investigated for the same applications.

REFERENCES

Acharya, V. (2006). TCP/IP and distributed system. Firewall Media.

Ali, A. N. A. (2012). Comparison study between IPv4 and IPv6.International Journal of Computer Science Issues, 9(3), doi: ijcsi–9–3–1–3–341–317.

Andress, J. G. (2005). IPv6: the next internet protocol. Login, 30(2), 21–28.

Blanchet, M. (2009). Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks. John Wiley & Sons Ltd, England.

Bouras, C., Gkamas, A., Primpas, D., & Stamos, K. (2004). Performance Evaluation of the Impact of QoS Mechanisms in an IPv6 Network for IPv6-Capable Real-Time Applications. Journal of Network and Systems Management, 12(4), 463–483.

Caicedo, C.E., Joshi, J.B.D., & Tuladhar, S.R.(2009). IPv6 Security Challenges. Computer.org, 42, 39–42. doi: 10.1109/MC.2009.54.

Callon, R. W. (1990). Use of OSI IS–IS for routing in TCP/IP and dual environments.RFC 1195.

Cisco. (2005). Intermediate System–to–Intermediate System (IS–IS) TLVs [http://www.cisco.com/c/en/us/support/docs/ip/integrated–intermediate–system–to–intermediate–system–is–is/5739–tlvs–5739.html], (accessed 2016 March 16).

Cisco. (2016). Cisco Nexus 7000 Series NX–OS Unicast Routing Configuration Guide, Release Release5.x[http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx os/unicast/configuration/guide/l3_cli_nxos/l3_ospfv3.html], (accessed 2016 March 16).

Coltun, R., Ferguson, D., Moy, J., & Lindem, A. (2008). RFC 5340, OSPF for IPv6. IETF, [tools.ietf.org], (accessed 2015 November 20).

Cooper, M., & Yen, D. C. (2005). IPv6: Business applications and implementation concerns. Computer Standards and Interfaces, 28 (1), 27–41, doi: 10.1016/j.csi.2004.11.001.

Davies, J. (2012). Understanding IPv6. Pearson Education.

Doyle, J., & Carroll, J. D. (2005). Routing TCP/IP, Volume 1, 2nd edition. Cisco Press

Durgadi, E., & Baldu, A. (2010). IPv4/IPv6 security and threat comparisons. Procedia–Social and Behavioral Science, 2, 528–5291 doi: 10.1016/j.sbspro.2010.03.862.

Empson, E. (2007). CCNP BSCI Portable Command Guide. Cisco Press.

Farhangi, S., Rostami A., & Golmohammadi, S. (2012). Performance comparison of mixed protocols based on EIGRP, IS–IS and OSPF for real–time applications. Middle–East Journal of Scientific Research, 2(11),1502–1508, doi 10.5829/idosi.mejsr.2012. 12.11.144.

Ferry, A.S., & Tadaki, S. (2003). The Critical Needed of IPv6 Development in Indonesia. [www.apjii.or.id/DOC/Artikel4/IPv6Develop.pdf], (accessed 2015 August 1).

Genkov, D. (2011). An approach for finding proper packet size in IPv6 networks. In Proceedings of the 12th International Conference on Computer Systems and Technologies, 442–447. ACM.

Graziani, R., & Johnson, A. (2008). Routing protocols and concepts: CCNA exploration companion guide, Pearson Education, London.

Hopps, C. (2008). Routing IPv6 with IS–IS. RFC5308. [https://www.rfc–editor.org/rfc/rfc5308.txt], (accessed 2016 February 18).

Islam, M. N., & Ashique, M. A. U. (2010). Simulation-Based Comparative Study of EIGRP and OSPF for Real–Time Applications. Diss.Master Thesis Electrical Engineering, Blekinge Tekniska Hogskolan, Thesis no: MEE, 10, 53.

Kannagi, P., & Rajasekar, M. (2013). Performance comparison of routing protocols (OSPF & EIGRP). International Journal of Advanced Research, 1 (3), 13–22.

Kaur, A., & Kumar, E. D. (2015): Comparative analysis of link state protocols OSPF and IS–IS International Journal of Computer Science Trends and Technology, 3 (4), 159–168.

Kaur, J., & Singh, P. (2014). Simulation based performance analysis of IPv6 based IS–IS, OSPFv3 and OSPFv3_IS–IS protocols. International Journal of Software and Hardware Research Engineering, 2 (8), 25–28.

Kent, S., & Atkinson, R. (1998). Security architecture for the internet protocol. RFC 2401[tools.ietf.org], (accessed 2016 April 26).

Kumar, A., & Karthikeyan, S. (2011). Security model for TCP/IP protocol suite. Journal of Advances in Information Technology, 2(2), 87-91.

Lammle, T. (2007). CCNA: Cisco Certified Network Associate, Study Guide, 6th edition. Indiana, Indianapolis, Wiley Publishing, Inc.

Leahy, E. (2011): OSPF Neighbors and Adjacencies: Eric Leahy's guide to networking in the CISCO World. [http://ericleahy.com/index.php/ospf-neighbors-and-adjacencies/], (accessed 2015 November 9).

Lemma, E. S. & Angelo, W. (2009). Performance comparision of EIGRP/IS–IS and OSPF/IS–IS [www.diva–portal.org], (accessed 2015 October 6).

Malhotra, R. (2002). IP routing. O'Reilly Media, Inc.

OSPF Neighbor States (2014). [http://www.cisco.com/c/en/us/support/docs/ip/open-shortestpath first-ospf/13685-13.html], (accessed 2016 April 12).

Pan, J., & Jain, R. (2008). A survey of network simulation tools: Current status and future developments. [www.cse.wustl.edu], (accessed 2015 December 7).

Pandey, N., Kumar, D., & Palwal, H. (2015). Simulation based comparative study on EIGRP/IS–IS and OSPF/IS–IS. International Journal of Engineering Research and General Science, 3 (2), 204–214.

Pavani, M., Lakshmi, M. S., & Kumar, S. P. (2014). A review on the dynamic routing protocols in TCP/IP. International Journal of Science and Technowledge, 2 (5), 227– 234.

Roussinos, P. A. (2014). Performance comparison of OSPF and IS–IS routing protocols in dual–stack enterprise networks. (Doctoral dissertation, Edinburgh Napier University), [soc.napier.ac.uk], (accessed 2016 January 4).

Sarkar, N. I., & Halim, S. A. (2011). A review of telecommunication networks: Simulators, classification, comparison, methodology, and recommendations.[ant.researchgateway. ac.nz], (accessed 2016 January 14).

Singhania, S. (2015). Comparison of OSPF in IPv4 and IPv6. International Journal of Advanced Research in Computer Science and Software Engineering, 5 (10), 95–99.

Siraj, S., Gupta, A., & Badgujar, R. (2012). Network simulation tools survey. International Journal of Advanced Research in Computer and Communication Engineering, 1 (4), 199–206.

Teare, D. (2010). Implementing Cisco IP routing: foundation learning guide. Foundation Learning for the ROUTE 642–902 exam, Pearson Education.

Thorenoor, S. G. (2010). Communication service provider's choice between OSPF and IS–IS dynamic routing protocol and implementation criteria using OPNET. In second International Conference on Computer and Network Technology (ICCNT), Bangkok, 38 (42), 23–25.

Wen, X., Xu, C., Gua, J., Su, W., & Zhang, H. (2010). Performance investigation of IPsec protocol over IPv6 networks. Proceedings of Artificial Intelligence Applications, Larnaca, Cyprus, 174–177.

Whitfield, R. J., & Zhu, S. Y. (2015). A Comparison of OSPFv3 and EIGRPv6 in a Small IPv6 Enterprise Network. Internation Journal of Advanced Computer Science and Applications, 6 (1), 162–167.