Routing Behavior of IS–IS and OSPFv3 with Database Query, Remote Login, and FTP in IPv6 Networks

Gideon E. Norvor, Michael Asante, Francis Xavier Kofi Akotoye

Abstract: ***IPv6 is the next–generation Internet Protocol developed to solve the problems of IPv4. 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. In this paper, performance of two routing protocols supported by IPv6 has been evaluated and compared for some applications such as database query, remote login, and ftp using Riverbed Modeler Academic Edition 17.5. These protocols are OSPFv3 and IS–IS. Performance evaluation is based on database query response time, remote login response time, ftp download/upload response times and traffic received as the main parameters. The main objective of this paper is to compare both protocols and to evaluate their performance in order to determine which of them will be the more suitable one for routing these applications in IPv6. In order to achieve the objective of this paper, two scenarios were used: OSPFv3 scenario and IS–IS scenario. Both scenarios were simulated against the chosen parameters. Overall, simulation results have shown that IS–IS is the more suitable protocol for the selected applications.***

Keywords: Remote login, Database query, ftp, OSPFv3, IS–IS, and IPv6.

I. INTRODUCTION

Nowadays, internet usage has become an important part of our lives. We often rely on several applications including email, http, and database that are provided on the internet. The internet is made up of millions of networks connected together. The transfer of each internet application is based on datagrams or packets that are forwarded by routing protocols through these networks to their intended destinations. 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. 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. Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and Intermediate System–to–Intermediate System (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 (Lammle, 2007). 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. RIP and IGRP both 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). IPv6 is the new internet protocol developed to replace the legacy IPv4.

Revised Version Manuscript Received on November 05, 2016.

Gideon E. Norvor, Department of Computer Science, Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana

Michael Asante, Department of Computer Science, Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana.

Francis Xavier Kofi Akotoye, Department of Computer Science and Information Technology, University of Cape Coast (UCC), Cape Coast, Ghana.

To support routing in IPv6, the different routing protocols used in IPv4 were modified for this purpose. These protocols include Enhance Interior Gateway Protocol version 6 (EIGRPv6), Open Shortest Path First version 3 (OSPFv3), Routing Information Protocol next–generation (RIPng) and Intermediate System–to–Intermediate System (IS–IS) for IPv6. These protocols have their advantages and disadvantages. For example research has always revealed that EIGRP converges faster than the rest of these protocols. However, it is Cisco proprietary making it hardware (router) dependent. Acquiring only one set of hardware for an internetwork will certainly come with a cost. RIPng is the successor of RIP used in IPv4. Like OSPF and IS–IS, RIP is an open standard protocol but a typical distance vector protocol (Kaur et al, 2014). Distance vector protocols do not scale well in larger networks as do by link state protocols. Therefore the choice is now left between OSPFv3 and IS–IS. In this paper, performance of OSPFv3 and IS–IS has been evaluated and compared for some applications such as database query, remote login, and file transfer using Riverbed Modeler Academic Edition. Performance evaluation is based on database query response time, remote login response time, file download/upload response times and traffics received 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.

II. RELATED WORK

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 these 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. 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 shows 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. Kaur & Singh (2014) again carried out a simulation based performance analysis of IS–IS, OSPFv3, and a combination of both protocols for IPv6 using OPNET. Performance comparison of these protocols and their combination was carried out based on email download/upload and http page response times. Results obtained from their simulation show that IS–IS performs better than OSPFv3 and the combination of both protocols for email and http page download response times. For email upload response time, OSPFv3 performs better than IS–IS and the combination of both protocols. 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. 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. This paper 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, and remote login. Performance evaluation was carried out on the basis of database query, remote login, ftp download/upload response times and traffics received. Both routing protocols have some similarities but differ in routing behavior. They both use the same routing algorithm to determine the shortest paths to all destinations within a network.

2.1. OSPFv3

Open shortest path first version 3 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. 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. 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 a 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 devices are called end systems (ESs). The end systems and the intermediate systems are grouped together to form a routing domain. Similar to OSPFv3, IS–IS also uses Dijkstra's 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.

III. METHODOLOGY

3.1. Simulation tool:

In this paper, Riverbed Modeler Academic Edition 17.5 is the main simulation tool used. This simulator is a Graphic User Interface (GUI) based and an object–oriented simulator enabling users to model real world systems in form of graphics (Pan et al, 2008). 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. Simulation design:

In this paper, two routing protocols have been compared in IPv6 network. These protocols are OSPFv3 and IS–IS. In other to achieve the objectives of this paper, 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: database query, remote login, ftp download/upload response times and traffics received. The purpose of the comparison is to determine which protocol will perform better than the other for the selected simulation parameters.

3.3. Network topology and connections:

Figure 3.1 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.

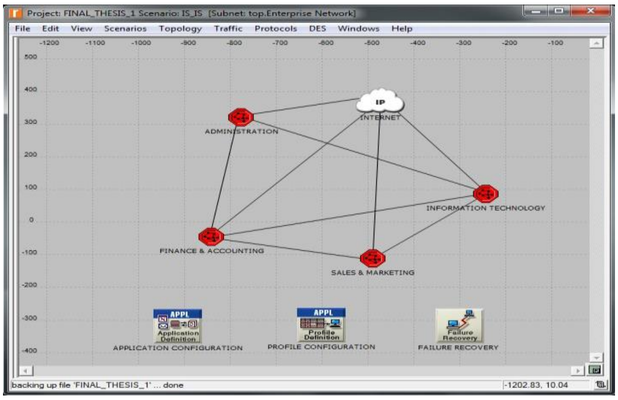

Figure 3.1: Network topology

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

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 internet connection to all the subnets, an IPv32 cloud device was used. Figure 3.2 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.

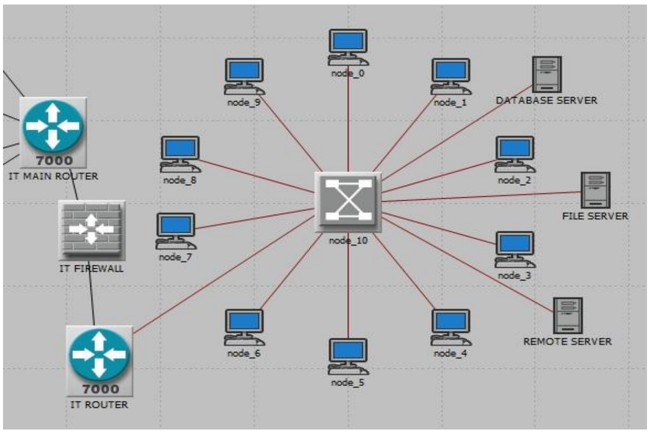

Figure 3.2: Internal Infrastructure of IT department

3.4. Application configuration:

In order to specify the selected applications and to generate network traffic for each of them in the network topology, the Application Definition and the Profile Definition objects were added from the object pallet into the modeler's workspace. Both objects were respectively renamed as application configuration and profile configuration in the modeler's workspace as shown in Figure 3.1. The application configuration object is set to support database (high load), remote login (high load), and ftp (high load). In order to generate network traffic for each application specified in the network, three profiles were defined in the profile configuration utility to support each application specified in the application configuration object.

3.5. Node configuration:

In order to fully model the real world enterprise network, each server in the IT department was configured to support the application it was meant for. Figure 3.3 shows this configuration for the database server.

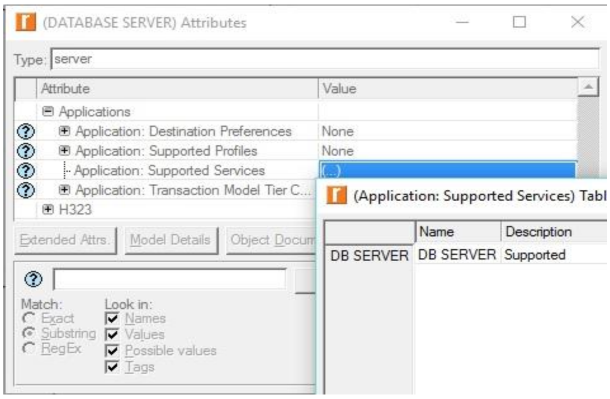

Figure 3.3: Database Server Application Configuration

Similarly, each workstation in the network topology was set to support all the applications supported in each server. Figure 3.4 shows this configuration.

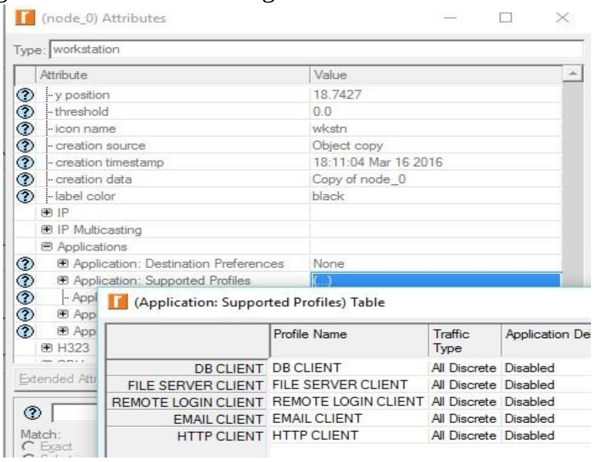

Figure 3.4: Workstation Application Configuration

3.6. OSPFv3 scenario:

Figure 3.5 shows the OSPFv3 scenario used in this paper. The network topology shown in this figure is the same as the network topology described in Figure 3.1. 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.

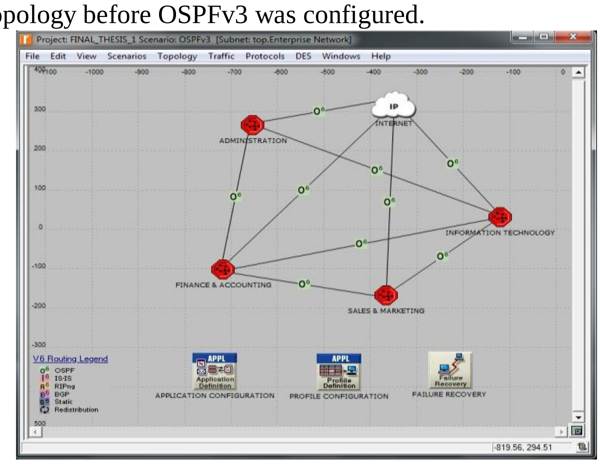

Figure 3.5: OSPFv3 Scenario

After enabling IPv6 Addresses and OSPFv3, the following parameters were chosen to measure how OSPFv3 will perform when it is used separately to route the selected applications in IPv6: Database query response time, remote login response time, file download/upload response times, and ftp traffics received. After choosing these parameters, total simulation time for this scenario was set to 30 minutes and then the simulation was run. After the simulation, results obtained for each parameter were observed and recorded in the following tables:

Table 3.1 shows the results recorded for database query response time in the OSPFv3 network for the simulation time interval with their corresponding values for database query response time (in seconds).

Table 3.1 OSPFv3 Database query response time.

Simulation time (minutes)	OSPFv3 (seconds)
2	0.02–4.90
3–5	4.0–2.4
10	2.0
15	2.1
20	1.9
25	1.8
30	1.7

Table 3.2 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. 2:OSPFv3 Database query traffic received

Simulation time (minutes)	OSPFv3 (bytes/second)
2	10000
10	70000
20	77000
30	78000

Table 3.3 shows the values recorded for remote login response time (in seconds) in 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 3.3: 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 3.4 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. 4: 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 3.5 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 3.6: 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 3.6 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 3.6: OSPFv3 Ftp traffics received

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

3.7. IS–IS scenario:

Figure 3.6 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.

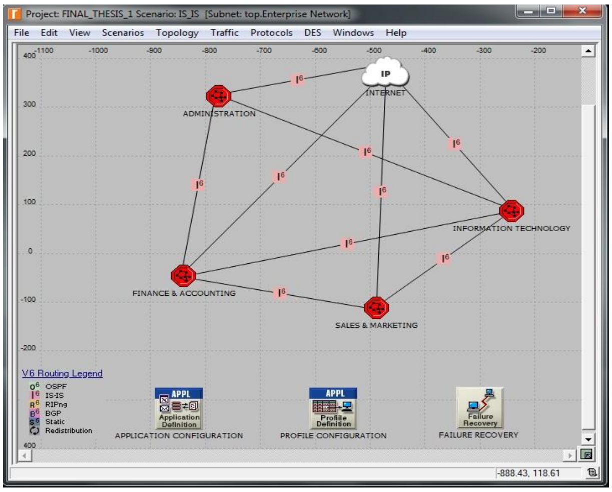

Figure 3.6: IS–IS Scenario

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. After choosing these parameters, total simulation time for this scenario was set to 30 minutes and then the simulation was run. After the simulation, results obtained for each parameter were observed and recorded in the following tables:

Table 3.7 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 3.7: 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 3.8 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 3.8: IS–IS Database query traffics received.

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

Table 3.9 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 3.9: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 3.10 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 3.10: 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 3.11 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 3.11: 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 3.12 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 3.12: 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

IV. 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. 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.

4.1. Database query response time:

This parameter was 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 4.1 indicates how protocol performance has affected the way the database server has been accessed in the network. From this simulation result, it can be inferred 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.

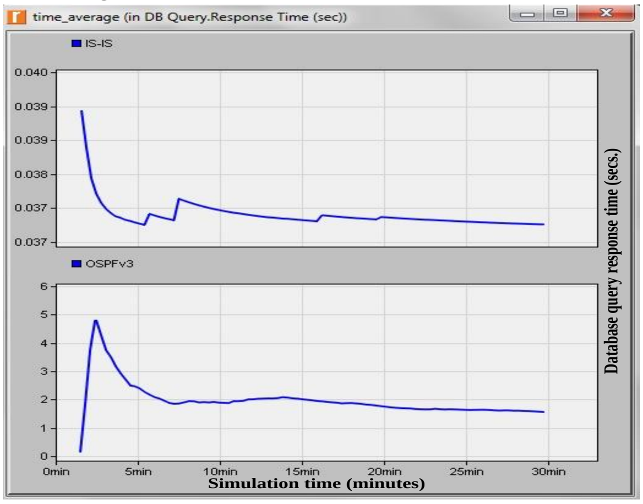

Figure 4.1: Database query response time (Seconds)

4.2. Database query traffics received:

The database query traffics received in the network is shown in Figure 4.2. This statistic represents the average bytes that are forwarded every second by the transport layers to a database query application that accesses the server. 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.

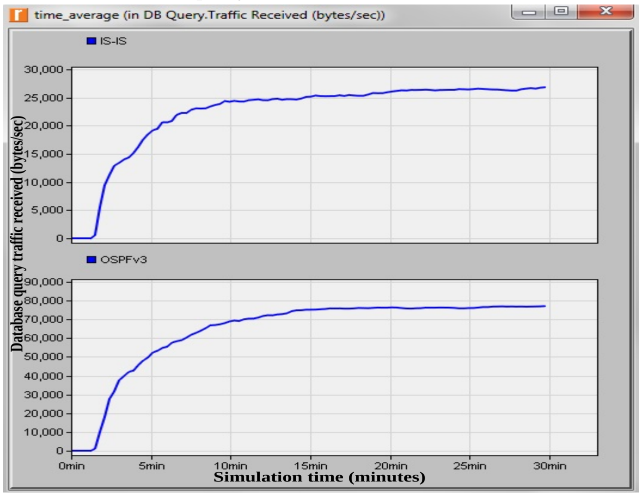

Figure 4.2: Database query traffics received (bytes per second)

4.3. Remote login response time:

Figure 4.3 shows how protocol performance affected remote access or login response times in both scenarios. This parameter was used in measuring how long it takes client applications to send their requests to a 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 to 0.048 seconds. 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.

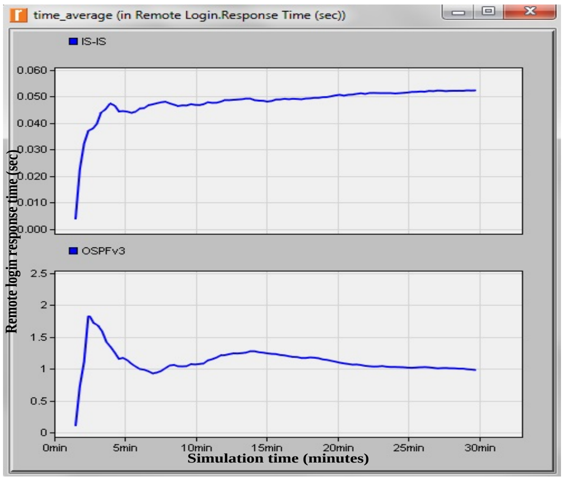

Figure 4.3: Remote Login Response Time (seconds.)

4.4. Ftp download response time:

Simulation result obtained for this parameter is shown in Figure 4.4. 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 4.4, 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. At 15 minutes during simulation, ftp download response time of both scenarios rose again 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 seconds 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 more suitable.

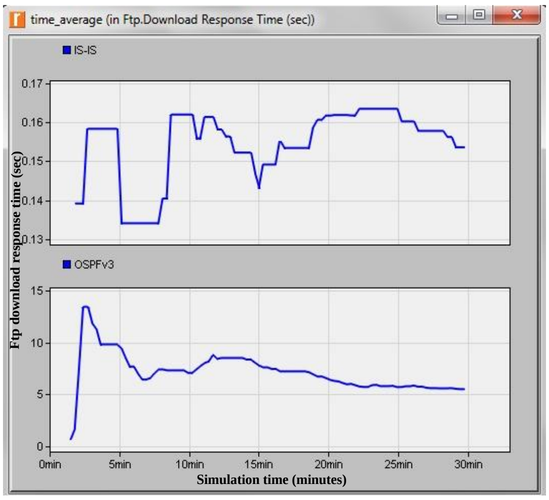

Figure 4.4: FTP Download Response Time (seconds.)

4.5. Ftp upload response time:

Simulation result obtained from scenario one and scenario two for this parameter is shown in Figure 4.5. 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, though, 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.

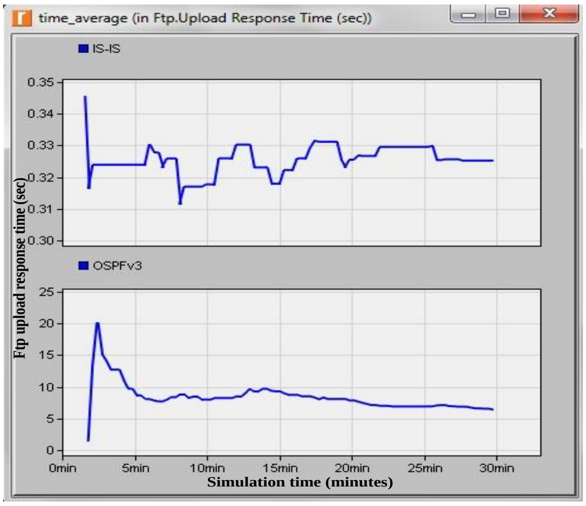

Figure 4.5: FTP upload response time (seconds.)

4.6. Ftp traffics 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 4.6 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.

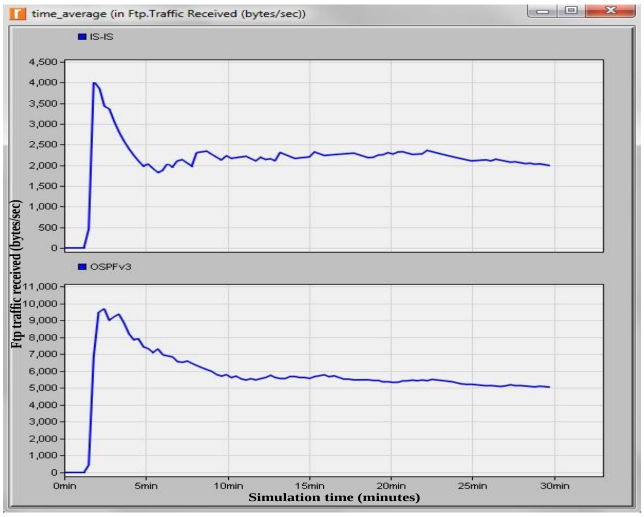

Figure 4.6: Ftp Traffic Received (bytes/sec.)

V. CONCLUSION

In this paper, performance of two routing protocols (OSPFv3 and IS–IS) for IPv6 has been measured and compared by simulation for some selected applications including ftp, database, 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. Performance comparison of both routing protocols is based on the following quantitative parameters: database query (response time and traffic received), ftp download /upload response times, ftp traffics received, remote access or login response time. 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. 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. Based on these results, it can be concluded that overall, IS–IS performed better than OSPFv3.

FUTURE WORK

The future, work will involve the investigation of the effect of protocol performance on other applications such Telnet.

REFERENCES

1. 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.
2. 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.
3. Genkov, D. (2011, June). 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.
4. Hopps, C. (2008). Routing IPv6 with IS–IS. RFC5308.[https://www.rfceditor.org/rfc/rfc5308.txt], (accessed 2016 February 18).
5. Kannagi, P., Rajasekar, M. (2013). Performance comparison of routing protocols (OSPF & EIGRP). International Journal of Advanced Research, 1 (3), 13–22
6. 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.
7. Lammle, T. (2007). CCNA: Cisco Certified Network Associate, Study Guide, 6th edition. Indiana, Indianapolis, Wiley Publishing, Inc.
8. Lemma, E. S. & Angelo, W. (2009). Performance comparision of EIGRP/IS–IS and OSPF/IS–IS [www.diva–portal.org], (accessed 2015 October 6).
9. 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.
10. 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.