

Performance Analysis of OSPF and EIGRP Routing Protocols

Abstract

Routing protocol is the brain behind communication between routers in computer networks. Although there are many routing protocols available, OSPF and EIGRP are the most common due to their ability to adapt in any kind of network Macfarlane (2006). The aim of this research is to analyse and compare the performance of OSPF and EIGRP routing protocols when it comes to selecting between them. This research is carried out in simulation environment using OPNET Modeler and in the Lab using real equipment. In OPNET, two network scenarios were designed; OSPF scenario and EIGRP scenario, both configured with OSPF and EIGRP respectively. The evaluation parameters selected for the routing protocols are convergence duration and number of packets dropped. In the lab experiment, two experiments were performed using different network topology. The first experiment is to monitor the convergence process of OSPF and EIGRP in a point – to – point network connection and the second experiment is to monitor the convergence process in a shared Ethernet segment kind of network. Results from the simulation and lab experiment are gathered and compared. Results show that EIGRP converges faster than OSPF in a point – to – point network, while both protocols converged at the same time in a shared Ethernet network.

Table of Contents

Declaration.....	Error! Bookmark not defined.
Acknowledgment.....	Error! Bookmark not defined.
Abstract	2
List of Tables	6
List of Figures.....	7
Acronyms	9
1 Introduction.....	11
1.1 Research Aim.....	12
1.2 Research Objectives	12
1.4 Document Outline	13
2 Literature review	15
2.1 Introduction.....	15
2.2 Routing	15
2.3 Routing protocols	16
2.4 Metrics of routing protocols	16
2.5 Routing Protocol Classification	17
2.5.1 Distance Vector	17
2.5.2 Link State	18
2.6 Types of Routing Protocol	19
2.6.1 Open Shortest Path First (OSPF) Routing Protocol	20
2.6.2 Enhanced Interior Gateway Routing Protocol (EIGRP)	20
2.7 Performance of OSPF and EIGRP	21
2.8 Comparison of OSPF and EIGRP	26
2.9 Selecting between OSPF or EIGRP Routing Protocol	27
2.10 Conclusion	30
3 Open Shortest Path First (OSPF) Routing Protocol.....	31
3.1 Introduction.....	31
3.2 Overview	31
3.3 OSPF Packet Header	31
3.4 OSPF Packet Types	32
3.5 OSPF Areas.....	37
3.6 OSPF Router Types	38

3.7	OSPF Neighbour Relationship Establishment.....	39
3.8	Advantages and Disadvantages of OSPF.....	42
3.9	Conclusion	43
4	Enhanced Interior Routing Protocol (EIGRP).....	44
4.1	Introduction.....	44
4.2	Overview	44
4.3	EIGRP Packet Format	44
4.4	EIGRP Packet Types	46
4.5	EIGRP Routing Process	47
4.5.1	Neighbour Table	47
4.5.2	Topology Table	47
4.5.3	Routing Table.....	50
4.6	Diffusing Update Algorithm (DUAL)	50
4.7	Advantages and Disadvantages of EIGRP.....	51
4.8	Conclusion	51
5	Methodologies	52
5.1	Introduction.....	52
5.2	Research Methodology.....	52
5.3	Simulation Methodology.....	52
5.3.1	Optimised Network Engineering Tool (OPNET)	52
5.3.2	Network Topology.....	56
5.3.3	OSPF Scenario	59
5.3.4	EIGRP Scenario	59
5.4	Lab Experiment Methodology	60
5.4.1	Experiment 1	60
5.4.2	Experiment 2	62
5.5	Conclusion	64
6	Results and Analysis	65
6.1	Introduction.....	65
6.2	Simulation	65
6.3	Lab Experiment	67
6.3.1	Experiment 1	67
6.3.2	Experiment 2	69

6.4	Conclusion	73
7	Conclusion	74
7.1	Introduction.....	74
7.2	Research Summary	74
7.3	Conclusion	76
7.4	Research Limitation	76
7.5	Further Work.....	76
8	Critical Evaluation	78
8.1	Introduction.....	78
8.2	Discussion	78
8.3	Conclusion	79
	References	80
	APPENDIX A. OPNET Modeler Simulation Set Up and Wireshark Captures	88
	OPNET Setup	88
	Wireshark Capture.....	95
	Bibliography	98

List of Tables

Table 2.1: Routing metric classification (McGregor, 2001)	17
Table 2.2: Common OSPF Cost (Sendra et al, 2010).....	20
Table 2.3: OSPF and EIGRP comparison (Ashraf, 2010), (Balchunas, 2007), (Andrew, 2011) and (Pethe & Burnase, 2011)	27
Table 3.1: OSPF LSA Types and Description (Rob, 2011)	35
Table 6.1: Simulation Convergence Duration and Traffic Dropped (Point – to – Point Network).....	67
Table 6.2: Lab Experiment 1 Convergence Duration (Point – to – Point Network)	69
Table 6.3: Lab Experiment 2 Convergence Duration (Shared Ethernet Segment network) ...	73

List of Figures

Figure 2.1: Ayub et al Hope and Spoke Topology (Ayub et al, 2011)	22
Figure 2.2: Thorenoor's Network topology on USA demography (Thorenoor, 2010)	22
Figure 2.3: Wu's Star Topology (Wu, 2011)	23
Figure 2.4: Wu's Partial Mesh Topology (Wu, 2011)	23
Figure 2.5: Wu's Ring Topology (Wu, 2011)	24
Figure 2.6: Sendra et al Network Topology (Sendra et al, 2010)	25
Figure 2.7: Kaur & Sharma Network Topology (Kaur & Sharma, 2011)	25
Figure 2.8: Islam & Ashigue Network Topology (Islam & Ashique, 2010).....	26
Figure 3.1: OSPF Packet Header (Shamim et al, 2002)	31
Figure 3.2: OSPF Hello Packet (Shamim et al, 2002)	32
Figure 3.3: Database Description Packet (Shamim et al, 2002).....	34
Figure 3.4: OSPF LSA Exchange between Areas (Caue, 2008)	35
Figure 3.5: OSPF LSR Packet (Shamim et al, 2002).....	36
Figure 3.6: OSPF LSU Packet (Shamim et al, 2002).....	36
Figure 3.7: OSPF LSAck Packet (Shamim et al, 2002).....	36
Figure 3.8: OSPF Area Types (Shamim et al, 2002)	38
Figure 3.9: OSPF Neighbour Relationship Process (etutorials, 2011)	42
Figure 4.1: EIGRP Packet Format (Shamim, 2002)	45
Figure 4.2: EIGRP Time and Value Fields (Shamim, 2002)	46
Figure 4.3: Feasible Distance Calculation (Shamim, 2002)	48
Figure 4.4: Reported Distance Calculation (Shamim, 2002)	49
Figure 4.5: Feasible Successor Calculation (Shamim, 2002)	49
Figure 5.1: Network Model (OPNET Modeler, 2011)	53

Figure 5.2: Node Domain (OPNET Modeler, 2011)	54
Figure 5.3: Process Domain (OPNET Modeler, 2011).....	54
Figure 5.4: Statistics Collection and Workflow (OPNET Modeler, 2011)	55
Figure 5.5: Network Topology	56
Figure 5.6: OSPF Scenario	59
Figure 5.7: EIGRP Scenario	59
Figure 5.8: Lab Experiment 1 Network Diagram	61
Figure 5.9: Lab Experiment 2 Network Diagram	62
Figure 6.1: IP Network Convergence Duration (sec)	66
Figure 6.2: IP Traffic Dropped (packets/sec)	66
Figure 6.3: Debug IP OSPF Output	67
Figure 6.4: Ping Command (PC1>PC2)	68
Figure 6.5: Debug IP EIGRP Output	68
Figure 6.6: Ping Command (PC1>PC2)	69
Figure 6.7: Debug IP OSPF Command Output Showing DR/BDR Election.....	70
Figure 6.8: Ping Command (PC1>PC2)	70
Figure 6.9: Debug IP OSPF Command Output (No DR/BDR Election)	71
Figure 6.10: Ping Command (PC1>PC2)	71
Figure 6.11: Debug IP EIGRP Command Output.....	72
Figure 6.12: Ping Command (PC1>PC2)	72

Acronyms

ABR: Area Border Router

AS: Autonomous System

ASBR: Autonomous System Boundary Router

BDR: Backup Designated Router

BR: Backbone Router

DDB: Database Description Packet

DES: Discrete Event Simulation

DR: Designated Router

DUAL: Diffusing Update Algorithm

DVR: Distance Vector Routing

EIGRP: Enhanced Interior Gateway Routing Protocol

FC: Feasible Condition

FD: Feasible Distance

FS: Feasible Successor

IGRP: Interior Gateway Routing Protocol

IS-IS: Intermediate System to Intermediate System

ISO: International Standard Organisation

LSA: Link-State Advertisement

LSAck: Link-State Acknowledgement

LSR: Link-State Request

LSU: Link-State Update

NSSA: Not-So-Stubby-Area

OPNET: Optimized Network Engineering Tool

OSI: Open Systems Interconnection

OSPF: Open Shortest Path First

RD: Reported Distance

RIP: Routing Information Protocol

RTP: Reliable Transport Protocol

SA: Stub Area

SPF: Shortest Path First

TSA: Totally Stubby Area

1 Introduction

A computer network consists of two or more network devices (computers, routers, switches) able to communicate either via wireless or wired connection. Network devices are manufactured by different vendors, so in order for the network devices interoperate, they are manufactured base on the seven layered OSI model. The OSI model was first published in 1978 by the International Standard for Organization (ISO), an international engineering organization based in Paris (Velte, 2007). The goal of the OSI is to allow interoperability among network devices from different vendors (Velte, 2007). The ISO proposes a set of rules that govern communication between network devices known as routing protocol, classified in the network layer (layer 3) of the OSI.

Routing protocol is a protocol that specifies the path network devices choose to exchange information, the choice of the path depends on the routing protocol's algorithm (Wikipedia, 2011). Routing protocols are classified as interior or exterior routing protocol. Interior routing protocols (IGP) are those configured within a single network or autonomous system, most common include RIP (v1 & v2), IGRP, IS-IS, OSPF, EIGRP etc. Exterior routing protocols (EGP) are configured to connect separate networks or autonomous systems, most common include BGP v4. Among all the routing protocols the most widely used in organisations and the internet are OSPF and EIGRP, because of their ability to adapt to any kind and size of network Macfarlane (2006). These protocols are built base on different algorithms, so their behaviour differ from one another.

Open Shortest Path First (OSPF) is a link state routing protocol built based on SPF/Dijkstra algorithm while Enhanced Interior Gateway Routing Protocol (EIGRP) is a distance vector routing protocol built based on DUAL algorithm. This research will analyse and compare the performance of OSPF and EIGRP in OPNET Modeler simulator and in the Lab using real network equipment. In OPNET, two network scenarios were designed; OSPF scenario and EIGRP scenario, both configured with OSPF and EIGRP respectively. The evaluation parameters selected for the routing protocols are convergence duration and number of packets dropped. In the lab experiment, two experiments were performed using different network topology. The first experiment is to monitor the convergence process of OSPF and EIGRP in a point – to – point network connection and the second experiment is to monitor the convergence process in a shared Ethernet segment kind of network. Results from simulation are compared with results collected from the Lab experiments.

1.1 Research Aim

This research aims to analyse and compare the performance of OSPF and EIGRP routing protocols in terms of convergence duration. This would also help to know which among the protocols is suitable for a certain network connection.

1.2 Research Objectives

1. Research on routing protocols in general.
2. Write a literature review on routing protocols, OSPF and EIGRP from journals, books, previous researches and previous thesis.
3. Learn OPNET Modeler to use for simulation.
4. Decide on type of network connection, shared Ethernet or point – to – point network connection.
5. Design two scenarios in OPNET; first scenario name OSPF configure with OSPF routing protocol and second scenario name EIGRP configure with EIGRP routing protocol (point – to – point connection).
6. Analyse results gathered from the simulation.
7. Design the same network (point – to – point connection) in the Lab with real equipment.
8. Analyse results gathered from the Lab experiment.
9. Analyse and Compare results gathered from simulation and Lab.
10. Design a shared Ethernet network connection in the Lab.
11. Analyse the effect hello messages have on OSPF and EIGRP convergence process and the effect DR/BDR election has on OSPF convergence duration.
12. Write a research report.
13. Evaluate the project as a whole to determine if research aim and objective is achieved.

1.4 Document Outline

2 Literature Review

This chapter explains routing protocol in general. It also explains the metrics, algorithms of OSPF and EIGRP. It also reviews previous papers and researches done on routing protocols and OSPF and EIGRP.

3 Open Shortest Path First (OSPF) Routing Protocol

This chapter explains briefly about OSPF background, packet types, area types, LSA types, router types, and how OSPF form neighbour relationship. Advantages and disadvantages of OSPF are also stated.

4 Enhanced Interior Gateway Routing Protocol (EIGRP)

This chapter explains briefly about EIGRP background, packet format, routing process, DUAL algorithm. It also states the advantages and disadvantages of EIGRP.

5 Methodologies

This chapter briefly explains OPNET Modeler. It also explains the simulation methodology, the definition of requirements; equipment and configuration nodes used for the OSPF and EIGRP scenarios. Then it explains the experimental methodology, the different network connection type used (shared Ethernet segment and point – to – point connection) and the OSPF and EIGRP experiment.

6 Results and Analysis

This chapter explains the results collected from the simulation and the Lab. It also present graphs from simulation, and debug outputs from the Lab. All results are analysed in this chapter.

7 Conclusion

This chapter summarises the entire research. It also explains and compares findings gathered from the simulation and the Lab experiments together with reviews of previous research and thesis. Then it outlines some difficulties encountered during the research and some theories for further research.

8 Critical Evaluations

This chapter evaluates the project as a whole and determine how the research aim and objectives were achieved.

2 Literature review

2.1 Introduction

This chapter is a review of books, various researches etc. conducted for general knowledge of routing protocols. Routing protocols are explained in general. It also explains the metrics, algorithms of OSPF and EIGRP. Then it explains and compares findings from reviews of previous research done on routing protocols and OSPF & EIGRP. It also states some factors to consider when selecting between OSPF and EIGRP.

2.2 Routing

Nowadays, with the rapid growth of the internet, the most important layers of the OSI model are the Network and Transport Layers (Yang et al, 2009). The network layer ensures data transmission between computers and the transport layer ensures reliability. The important part of the network layer is routing (Yang et al, 2009). Macfarlane (p90, 2006) defines routing as the act of forwarding network packets from a source network to a destination network. According to Wikipedia (2011), “routing is a process of selecting paths in a network along which to send traffic”.

Yang et al (2009) mention that routing can be classified as either static or dynamic routing. Yang et al (2009) continue by describing static routing as non-adaptive algorithm because if there is any change in the network topology, it cannot adjust to meet the change, while dynamic routing on the other hand as adaptive algorithm because it can make any routing decision on its own. In a different reading, Webopedia (2011) define “static routing as the process in which the system network administrator would manually configure network routers with all the information necessary for successful packet forwarding”. While in dynamic routing, routers learn about the network automatically without any human intervention Macfarlane (p104, 2006). In another reading (Thorenoor, 2010) state that dynamic routing enable routers to know about the network topology by communicating with their neighbour routers. The main advantage of dynamic routing over static routing is its ability to grow and recover from network failure (Thorenoor, 2010).

Dynamic routing can be categorized as exterior gateway protocols (EGP) or interior gateway protocols (IGP) Khalil & Elmaghraby (2011). Khalil & Elmaghraby (2011) continue by stating that EGP are protocols used between different autonomous systems while IGP are protocols used in the same autonomous system. Yee (2006) describes an

autonomous system (AS) as a large network under one administrative control. EGP is a path vector routing protocol and the common one in use is BGP4 (Khalil & Elmaghraby, 2011). The well-known IGP are RIP, IGRP, EIGRP, OSPF, IS-IS etc. (Popoviciu, 2006).

2.3 Routing protocols

Routing protocols are classified in Layer 3 (Network layer) of the OSI model. Doyle & Carroll (p131, 2006) describe routing protocols as the language a router speaks with other routers to share information about the reachability and status of networks. In a different reading Macfarlane (p105, 2006) wrote that “a routing protocol is a specialised form of protocol that allows two or more routers to exchange information or routes about the networks they know about”. In light of the two definitions, the authors describe routing protocols as protocols that help routers know about other networks they are not connected to, so that they can reach those networks. Typically, each router only knows about its immediate neighbour. A routing protocol shares this information in order for the routers to have the knowledge of the whole network topology (Randhawa & Sohal, 2008).

2.4 Metrics of routing protocols

A metric is a numerical value assigned to link to a destination network (Schmid & Steigner, 2002). McGregor (p129, 2001) wrote that “a metric is a value that measures how good a route is”. In another reading, Doyle & Carroll (p133, 2006) explain metric as “a variable assigned to routes as means of ranking them from best to worst or from most preferred to least preferred”. Basically, from the above definitions, the authors describe a metric as a value used by routing protocols to determine which routes are better than others.

There are some factors a routing protocol takes into account when calculating or assigning a metric to a route (Macfarlane, 2006)

- **Hop count:** Number of routers to destination network (Macfarlane, 2006). The path with less number of hops to destination is preferred (Doyle & Carroll, 2006).
- **Bandwidth:** The speed of the link connecting routers (Macfarlane, 2006). Higher bandwidth is preferable (Doyle & Carroll, 2006).
- **Delay:** Time in milliseconds it takes a packet to cross a link (Macfarlane, 2006). Path with least delay is preferable (Doyle & Carroll, 2006).
- **Load:** The amount of traffic in the link (Macfarlane, 2006). Path with least load is preferable (Doyle & Carroll, 2006).

- **Reliability:** How reliable the link is in terms of failure (Doyle & Carroll, 2006). Number of bit errors in link is used to measure the reliability of that link (Macfarlane, 2006).

Not all of these factors are used by routing protocols to calculate metric (Macfarlane, 2006). In his book, McGregor (p129, 2001) wrote that routing protocols use different factors in calculating a metric. McGregor (2001) continued by stating that for example RIP use only one factor which is hop count, while IGRP uses factors of bandwidth, delay, load and reliability.

Routing Protocol	Metric
RIP	Hop Count
IGRP, EIGRP	Bandwidth, Delay, Load, Reliability
IS-IS	Cost (based on link bandwidth)
OSPF	Cost (based on link bandwidth), High cost indicates low bandwidth

Table 2.1: Routing metric classification (McGregor, 2001)

2.5 Routing Protocol Classification

Routing protocols are classified as distance vector or link state (Albrightson, Garcia-Luna-Aceves & Boyle 1994). The difference between them is the way they send routing updates and the way they calculate routes (Clark, 2003). Yee (2006) state that this classification is based on the routing algorithm they use to find the best path to a destination network. Routing algorithm as defined by Velte et al (p476, 2007) is a system of rules that controls internetworks behaviour in such a way that it adapts to changing circumstances within the internetworks topology. Routing algorithm is a method a router used to calculate the shortest route to any given destination (Clark, 2003). Odom & Knott (p414, 2006) wrote that routing protocols might use different algorithm to calculate the best path, but they all work in the same way that they tell their neighbouring routers the routes they know about.

2.5.1 Distance Vector

In a distance vector routing algorithm, routing information is only shared between neighbouring routers (Khalil & Elmaghraby, 2011). A distance vector protocol requires a router to send periodic updates to its neighbour about the network topology it know about (Riesco & Verdejo, 2009). Routers utilize the information they have and those received from their neighbours to calculate the best path (Yee, 2006). In another reading, Thorenoor

(2010) wrote that “distance vector protocols use a distance calculation plus an outgoing network interface to choose the best path to a destination network”. Thorenoor (2010) then continued by explaining that whenever there is a topology change in a network, the router with that change will send the updates to its neighbour router which will then add a distance vector to the routing table before it forwards the updates to its neighbour router.

Doyle & Carroll (p137, 2006) wrote that distance vector routing protocols used either Bellman-Ford/Ford-Fulkerson algorithm or DUAL (Diffusing Update Algorithm) to calculate routes. The main disadvantage of Bellman-Ford algorithm is slow convergence and the possibility of routing loops (Albrightson, Garcia-Luna-Aceves & Boyle 1994). Macfarlane (p106, 2006) define Convergence as how long it takes every router in the network to synchronise their routing table or how long it takes every router to update their routing topology if there is any change in the network, and routing loops is when a packets loop round a network without reaching their destination. RIP (routing information protocol) is an example of distance vector protocol that adopts the Bellman-Ford algorithm (Yee, 2006). RIP uses a metric of hop count in making routing decision (Yee, 2006). DUAL on the other hand was developed to solve the problem of routing loops and slow convergence of Bellman-Ford algorithm (Yee, 2006). DUAL was proposed by Garcia-Luna-Aceves (1993), where routers calculate the shortest path to a destination network without creating routing loop. Macfarlane (p190, 2006) wrote that “DUAL performs a feasibility test on advertised routes before installing them, which makes DUAL 100 percent loop free at every instant”.

In a journal by Garcia-Luna-Aceves (1993), DUAL was proved to be free of routing loops and faster convergence which was the major problems of earlier distance vector protocols routing protocols. EIGRP is the routing protocol that uses DUAL (Albrightson, Garcia-Luna-Aceves & Boyle 1994). EIGRP uses the metric of bandwidth and delay in making routing decision (Macfarlane, 2006).

2.5.2 Link State

Sivabalan & Mouftah (2001) wrote that “link state protocol is a class of routing protocol in which a router know the network connectivity and the state information of all the links in the network”. In contrast to distance vector, in a link state each router must know the whole network topology (Garcia-Luna-Aceves, 1989). Routers using link state routing share their routing information with every router in the network (Khalil & Elmaghraby, 2011).

Individual routers in the network will build their own topology or road map of the complete network and work out shortest path to individual destination using SPF/Dijkstra algorithm (Doyle & Carroll, 2006). In link state routing, whenever there is a change in topology, the entire network is notified (Hummel, 2011). OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System) are examples of routing protocols that use link state routing protocols (Yee, 2006).

Doyle & Carroll (p146, 2006) provide some steps about how link state protocols function:

1. Each router establishes relationship i.e. adjacency with its neighbour router.
2. Each router exchange LSA packets (Link State Advertisement) with its neighbour. This contains all the information of the networks the router knows about. Each router that receives the packet in turn forwards it to its neighbour router.
3. Each router will then save the information they received in their database. All neighbours will be synchronised, and they will all have the same database.
4. Now each router will run SPF/Dijkstra algorithm to compute the shortest path to each network.

2.6 Types of Routing Protocol

Thorenoor (2010) stated that routing protocols differ from one another base factors like choosing the best route among multiple routes, throughput, convergence time, metrics, load balancing etc. There have been a number of different routing protocols developed over the years, and each has its advantages and disadvantages. Popoviciu (2006) wrote that “each routing protocol has its own benefits and deficiencies, and each is best suited for a certain network environment”. In another reading, Clark (2003) stated that each protocol is designed base on certain algorithm upon which it calculate the shortest distance routes.

Macfarlane (p105, 2006) wrote that “Although many routing protocols have been developed over the years, no single routing protocol is best for all kinds of network (although EIGRP and OSPF has pretty much become the choice for enterprise networks and some ISP networks)”. OSPF and EIGRP are the two most popular routing protocols now that are widely employed in the internet and various organisations (Yee, 2006) and (Ayub et al, 2011), because of their ability to adapt to any network size, ability to recover fast in a network failure (Ayub et al, 2011).

2.6.1 Open Shortest Path First (OSPF) Routing Protocol

Moy (p5, 1998) stated that OSPF is industry standard routing protocol that was developed by IETF (Internet Engineering Task Force). OSPF protocol as stated earlier is a link state protocol based on Dijkstra algorithm. OSPF uses a metric of cost to determine the best route which depends on the bandwidth of the link (Sendra et al, 2010). OSPF uses bandwidth to calculate its metric known as cost (Doyle & Carroll, 2006). As Sendra et al (2010) show in their report the formula used by OSPF to calculate the cost of a link is:

$$\text{Cost} = \frac{1000}{\text{Bandwidth (Mbps)}} \quad (\text{Sendra et al, 2010})$$

Link	Cost
56K	1785
64k	1562
T1 (1.544)	65
E1 (2.048)	48
Ethernet	10
Fast Ethernet	1

Table 2.2: Common OSPF Cost (Sendra et al, 2010)

Higher bandwidth yields lower cost, and the links with lower cost is more preferable by OSPF as the best route (Ashraf, 2010). OSPF send HELLO message periodically to its neighbour routers to ensure network connectivity (Morrissey, 1999). Routers configured with OSPF protocol will have the whole topology of the network in order to compute the shortest path to a certain destination (Zhao et al, 2009). Zhao et al (2009) then continued by explaining that this consumes too much network resources which can directly influence the performance of network.

2.6.2 Enhanced Interior Gateway Routing Protocol (EIGRP)

Clark (p232, 2003) wrote that EIGRP is a Cisco proprietary routing protocol which means it can only be used with Cisco equipment. EIGRP as stated earlier is a distance vector protocol based on DUAL algorithm. Garcia-Luna-Aceves (1988) proposed DUAL to solve the problem of then distance vector protocols (RIP, IGRP etc.) which are routing loops and slow convergence. EIGRP is sometimes called hybrid routing protocol because it has the characteristics of both distance vector and link state routing protocols (Pethe & Burnase,

2011) and (Ayub et al, 2011). Like OSPF, EIGRP also sends HELLO message periodically to its neighbour router to ensure network connectivity (Morrissey, 1999) and (Expósito, 2010). EIGRP uses a combination metric of bandwidth and delay to determine the best route (Doyle & Carroll, 2006).

$$\text{Metric} = 256 * (\text{Bandwidth} + \text{Delay})$$

$$\text{Bandwidth} = 10^7 / \text{bandwidth}$$

$$\text{Delay} = \text{Delay in milliseconds}$$

Doyle & Carroll (2006)

2.7 Performance of OSPF and EIGRP

OSPF and EIGRP may be similar in some ways particularly the way they use a ‘HELLO’ protocol to inform other routers that it is alive, but the performance of the routing protocols differ from one another in many ways particularly the way they respond to changing network conditions (Teare, 2010).

Lab experiments and simulation studies has been done in recent years by different authors to test the performance of these routing protocols, based on different parameters like; convergence time, end to end delay, throughput, CPU utilization, jitter, network bandwidth utilisation etc.

In a recent simulation study by Ayub et al (2011), they analyse the performance of OSPF and EIGRP based on convergence time using OPNET simulator. The topology they used for their experiment is a hop and spoke topology containing five spoke sites and one core hub that connects the spoke sites (see figure 2.1). They deployed two different scenarios each configured with different routing protocol. After running the simulation for 8 hours, EIGRP is proven to perform better than OSPF based on “good CPU utilization, better convergence time, less memory consumption and ease in management”.

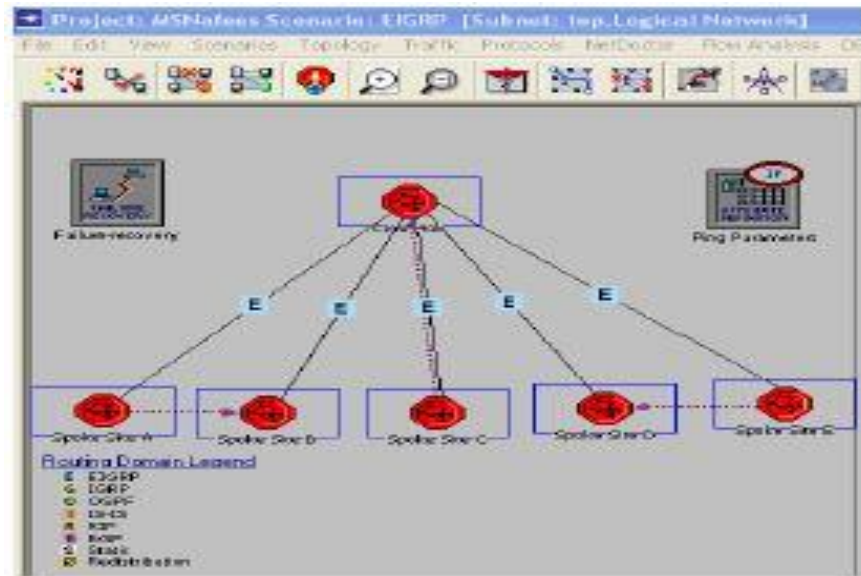


Figure 2.1: Ayub et al Hope and Spoke Topology (Ayub et al, 2011)

In a different simulation study by Thorenoor (2010), an analysis of the performance of dynamic routing protocols (i.e. RIP, OSPF and EIGRP) was carried out using OPNET. The network consists of routers located in different places of the USA demography (see figure 2.2). Three different scenarios were deployed each with the respective routing protocols (RIP, OSPF and EIGRP) using same network model. After running the simulation for 1 hour, EIGRP performs better than RIP and OSPF in terms of; “network convergence activity, network convergence duration, routing protocol traffic, CPU utilization, network bandwidth utilization, throughput and queuing delay”.

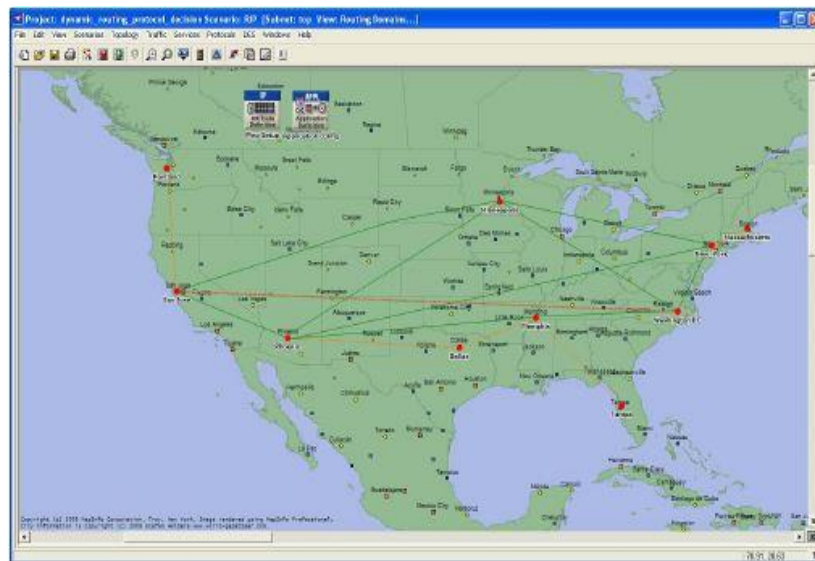


Figure 2.2: Thorenoor's Network topology on USA demography (Thorenoor, 2010)

Another simulation studies was carried out by Wu (2011) on performance analyses of RIPv2, EIGRP and OSPF using OPNET. Wu (2011) compared the performance of these routing protocols based on size of the network using three different topologies i.e. star, partial mesh and ring topology (see figures 2.3, 2.4 and 2.5). Wu (2011) concluded by saying that RIPv2 performs better when using small networks, while OSPF and EIGRP performs better in large network. Wu (2011) then continued by stating that above all, EIGRP performs well in both small and large networks in terms network stability and consistency.

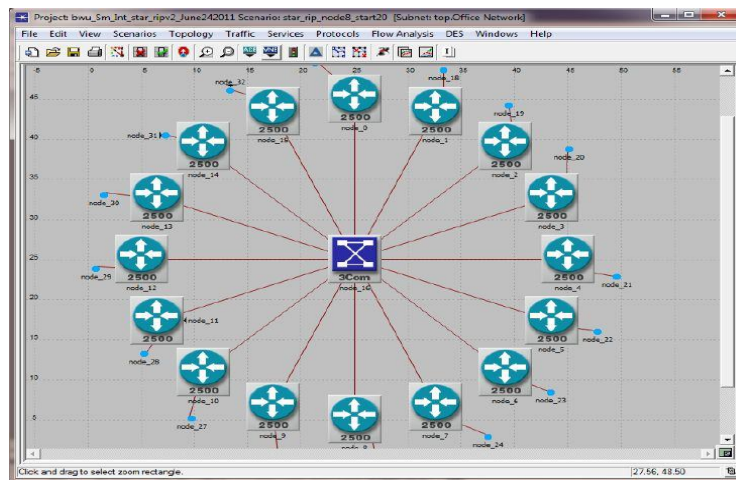


Figure 2.3: Wu's Star Topology (Wu, 2011)

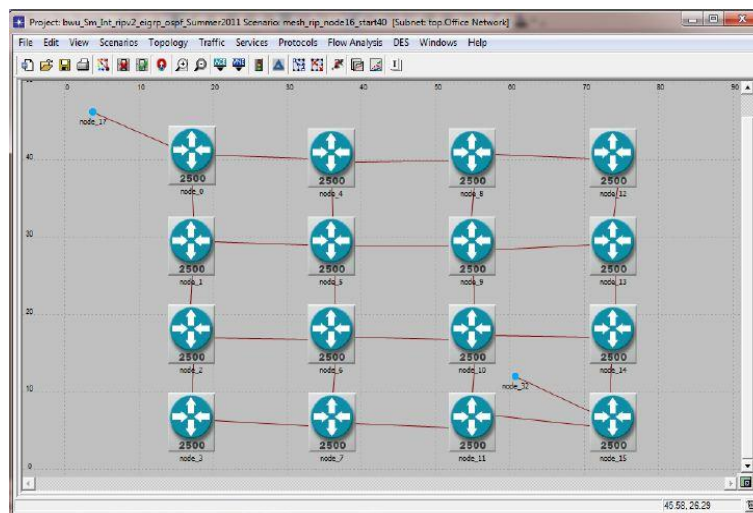


Figure 2.4: Wu's Partial Mesh Topology (Wu, 2011)

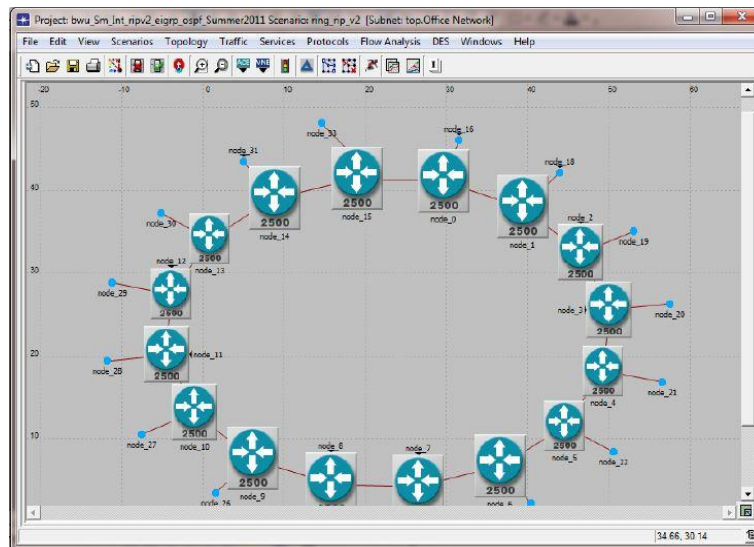


Figure 2.5: Wu's Ring Topology (Wu, 2011)

Sendra et al (2010) conduct an experiment to study the performance of routing protocols (RIP, OSPF and EIGRP) using real equipment. The network consists of 12 Cisco routers and 3 PCs (2 PCs for sending and receiving data and the other PC for monitoring traffic) (see figure 2.6). Sendra et al (2010) concluded that after some links failure and passing of data across the network, the following was observed:

- When there is a link failure in the network, EIGRP tends to converge faster than OSPF and RIP.
- OSPF has the lowest average uplink and downlink bandwidth consumption.
- EIGRP tends to stabilize faster than OSPF and RIP.
- And in terms of bytes sent per second, EIGRP has the lowest average number of bytes while RIP has the highest.

Islam & Ashique (2010) concluded that, EIGRP converge faster than OSPF and combination of EIGRP & OSPF in a network, while the combination of EIGRP & OSPF in a network performs better than EIGRP or OSPF configured alone in terms of end to end packet delay, jitter and OSPF has the lowest packet loss than EIGRP and EIGRP&OSPF combined.

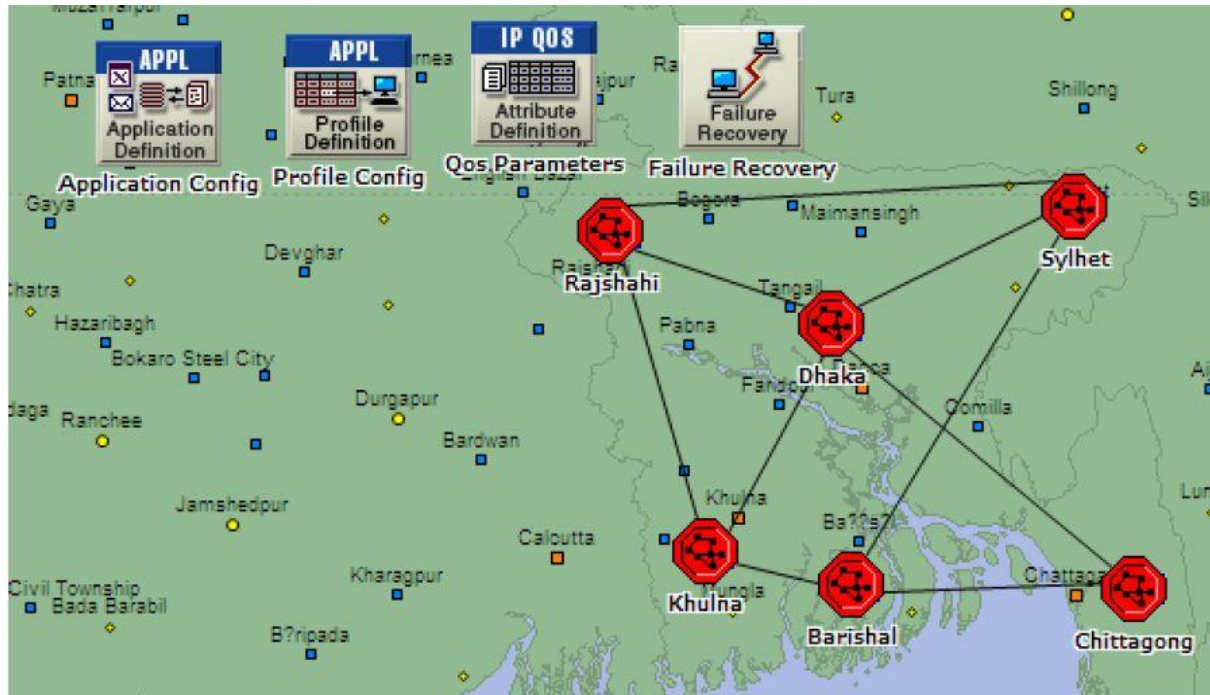


Figure 2.8: Islam & Ashique Network Topology (Islam & Ashique, 2010)

In light of the different experiments and simulation studies by the authors, Ayub et al (2011), Islam & Ashique (2010), Thorenoor (2010) and Sendra et al (2010) concurred that EIGRP performs better than OSPF in terms of convergence time and CPU utilization, while Ayub et al (2011) and Thorenoor (2010) found out that EIGRP is better than OSPF in terms of throughput and less memory consumption. Kaur & Sharma (2011) and Sendra et al (2010) both agreed that OSPF is better than EIGRP in terms of downloading processes. Lastly, Islam & Ashique (2010) also found out that the combination of OSPF & EIGRP in a network could improve the performance of the network in terms of end to end packet delay, jitter and packet loss.

2.8 Comparison of OSPF and EIGRP

OSPF and EIGRP have some similarities in the sense that they both; Send HELLO messages periodically to neighbour routers in order to maintain neighbour relationship, adapt to various sizes of networks be it (small, medium or large networks), classless routing

protocols. But they also differ in how they form their routing table, route packets across network and how they respond to network failure (Thorenoor, 2010).

Compare Point	OSPF	EIGRP
Standard	Industry standard, compatible with different vendor equipment	Cisco proprietary, only works with Cisco equipment
Algorithm	Dijkstra algorithm	DUAL algorithm
Knowledge Network Topology	Maintains the topology of the entire network or area in terms of hierarchal design	Maintains limited topology table
Load Balance	Load balance between equal cost paths	Load balance between unequal cost path
Type	Link state	Distance vector (Hybrid)
Convergence	Fast	Very fast
Routing Update	Floods update cross whole network	Sends updates only to affected routers

Table 2.3: OSPF and EIGRP comparison (Ashraf, 2010), (Balchunas, 2007), (Andrew, 2011) and (Pethe & Burnase, 2011)

2.9 Selecting between OSPF or EIGRP Routing Protocol

Ballew (1997) wrote that the common routing protocols in use today in organizations and the internet today are; RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System), EIGRP (Enhanced Interior Gateway Protocol). But the choice for the right one for routing depends on many factors like convergence time, memory and CPU usage, type of protocol, proprietary or industry standard (Ballew, 1997).

Convergence time: Zaumen & Garcia-Luna-Aceves (1992) and Doyle & Carroll (2006) state that EIGRP based on DUAL algorithm maintains two links to every destination, a successor which is selected as shortest path to a destination network and feasible successor as backup path, so if the successor link fails, feasible successor is selected immediately. If there is no feasible successor, EIGRP will send a query message to its neighbour routers requesting for information about how to reach the network (Zhao et al, 2009), (Zaumen & Garcia-Luna-Aceves, 1992) and (Doyle & Carroll, 2006). While Moy

(1998) and Doyle & Carroll (2006) wrote that OSPF routing protocol does not save a backup path, so if the selected path to certain destination fails, OSPF performs SPF algorithm to find another path to the destination. The DUAL algorithm used by EIGRP to compute shortest path to destination networks compared to SPF algorithm which is used by OSPF, makes EIGRP to converged faster than OSPF. Ayub et al (2011), Thorenoor (2010) and Sendra et al (2010) found out in their experiments that EIGRP performs better than OSPF in terms of convergence time.

Memory/CPU usage: Routers using OSPF routing protocol save the whole topology of the network, which in turns consumes huge amount of memory (Thorenoor, 2010) and (Clark, 2003). Also with OSPF routing protocol having to perform SPF algorithm anytime a link fails, these can be very processor intense which in turns might degrade the network performance (Moy, 1998) and (Basu & Riecke, 2001). When OSPF is designed in hierarchy or areas, it limits the flooding of updates within areas, which in turns significantly reduces the amount of CPU utilization (Moy, 1998) and (kim & Tcha, 2000). In a study by (Kleinrock & Kamoun, 1977), they proved that in large networks, when the network is divided into hierarchy/areas, it will reduce the size of the routing table which in turn which will require less storage and processing in the routers and less communication overhead. When using EIGRP as proved by (Zaumen & Garcia-Luna-Aceves, 1992), it consumes much less processor than OSPF.

Ayub et al (2011), Thorenoor (2010) and Sendra et al (2010) both concluded in their research that EIGRP performs better than OSPF in terms of CPU utilization.

Bandwidth usage: Morrissey (1999) said that when there a link failure, the affected router will recalculate the shortest path to the destination base on the type of routing protocol it is configured with. When using OSFP, the change is flooded across the whole network, while EIGRP only send changes to affected routers (Morrissey, 1999) and (Ashraf, 2010). EIGRP only sends partial updates when change occurs in the network (Expósito, 2010). This in turns makes EIGRP to consume less bandwidth than OSPF (Morrissey, 1999) and (Ashraf, 2010). A simulation study by Thorenoor (2010), proved EIGRP to consume less bandwidth than OSPF.

Protocol: EIGRP supports multiple protocols e.g. IP, IPX, AppleTalk etc. OSPF only supports IP (Pepelnjak, 2000) and (Morrissey, 1999).

Proprietary/Open Standard: EIGRP is a Cisco proprietary protocol, so it only works in Cisco equipment while OSPF is an open standard routing protocol developed by the IETF which means OSPF can be configured with any type of vendor equipment (Morrissey, 1999) and (Ashraf, 2010).

Selecting a routing for a network dose not just depends on the properties of the routing protocol, but also the network requirement should be taking into account (Davis, 2002). Ballew (1997), Davis (2002), (Murhammer et al, 1999) and Ashraf (2010) Provides some few aspects that should be taking into account when selecting a routing protocol:

- The size of the network.
- The bandwidth of the available links.
- The processing capacity of the routers.
- The manufacturer and models of the routers.
- The protocols that are already in use on the network.

When considering network size, OSPF or EIGRP will be the ideal choice, because they both scale in any size network (Murhammer et al, 1999). And in terms of link bandwidth, OSPF is proved to consume more link bandwidth than EIGRP (Thorenoor, 2010). So if there is any bandwidth constraint EIGRP will be the choice (Sendra et al, 2010).

Processing capacity of the routers is an important aspect that should be considered when it comes to selecting a routing protocol (Ballew, 1997), because if the wrong protocol is chosen, it will significantly degrade the routers performance resulting in poor network performance (Ayub et al, 2011). EIGRP is proved to have better processor usage than OSPF (Ayub et al, 2011), (Thorenoor, 2010) and (Sendra et al, 2010). Another important aspect is the type of router in the network which will determine the type of routing protocol it will support (Ballew, 2007). EIGRP is a Cisco proprietary, so it only works with Cisco equipment, while OSPF is an open standard which works with any kind of vendor equipment (Morrissey, 1999). If the network equipment is all Cisco, EIGRP will be the ideal choice otherwise OSPF is preferred (Ashraf, 2010).

EIGRP is known to support multiple protocols (IP, IPX, and AppleTalk etc.) while OSPF supports IP only network (Ashraf, 2010), (Pepelnjak, 2000) and (Morrissey, 1999). So if the network has multiple protocols, EIGRP should be chosen (Ashraf, 2010) and (Morrissey, 1999).

2.10 Conclusion

In this chapter, the difference between OSPF and EIGRP routing protocol is explained. Factors to consider when selecting a routing protocols like; routing protocol convergence duration, bandwidth usage, open standard or proprietary etc. were also explained. From the reviews of research papers by Ayub et al (2011), Islam & Ashique (2010), Thorenoor (2010) and Sendra et al (2010), they all concurred that EIGRP performs better than OSPF in terms of convergence duration and CPU utilization. These will be used to compare the findings collected in this research experiments.

3 Open Shortest Path First (OSPF) Routing Protocol

3.1 Introduction

In this chapter, OSPF is explained in more detail. OSPF packet types, router types and area types are explained. Finally, the steps OSPF follow to form neighbour relationship is also explained and the advantages and disadvantages of OSPF are stated.

3.2 Overview

Open Shortest Path First routing protocol was developed by the Internet Engineering Task Force (IETF) OSPF Working Group for Internet Protocol (IP) networks (Moy, 1998). There are three versions of OSPF, the current version OSPFv2 for IPv4 was published in RFC 2328 (Moy, 1998). OSPF is an open standard protocol that is based on link state routing protocol. In link state routing protocol, every router in the network running OSPF maintains the same topology called link state database (Moy, 1998). The routers then use the link state database to find the shortest path to every destination network by using the SPF/Dijkstra algorithm.

In OSPF, routers are grouped together called areas. Depending on the size of the network, there can be one or more areas in an OSPF network with area 0/backbone the default area. The grouping of routers into areas helps reduce network updates, making the network more efficient (Moy, 1998). All areas must connect to area 0/backbone area. Routers within an area are called area routers, routers connecting other areas to area 0/backbone area are called area boundary routers (ABR), and routers connecting to other autonomous system are called autonomous system boundary routers (ASBR) (Moy, 1998).

3.3 OSPF Packet Header

The OSPF packet header has eight fields as shown in figure 3.1. The OSPF packet header is included in any OSPF packet, regardless of the packet type (Shamim et al, 2002).

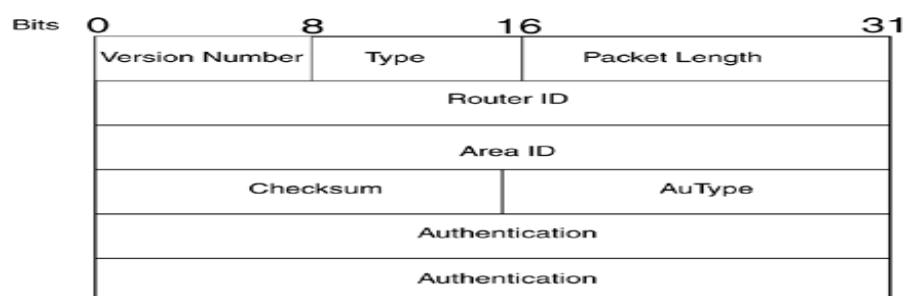


Figure 3.1: OSPF Packet Header (Shamim et al, 2002)

Version: indicates the version of OSPF.

Type: indicates the type of OSPF packet i.e. HELLO packet, DBD packet, LSR packet, LSU packet or LSAck packet.

Packet Length: the length of the entire OSPF packet.

Router ID: indicates the name of the OSPF router.

Area ID: indicates the area which the packet belongs.

Checksum: check errors in the packet.

Authentication Type: the type of authentication used. There are 3 authentication types in OSPF:

- 0 - Means no authentication.
- 1 - Means simple authentication.
- 2 - Means MD5 authentication.

Authentication Data: contains encrypted data

3.4 OSPF Packet Types

1. **Hello Packet:** Hello packets are used in OSPF process to establish and maintain neighbour relationship between OSPF enabled routers (Shamim et al, 2002).

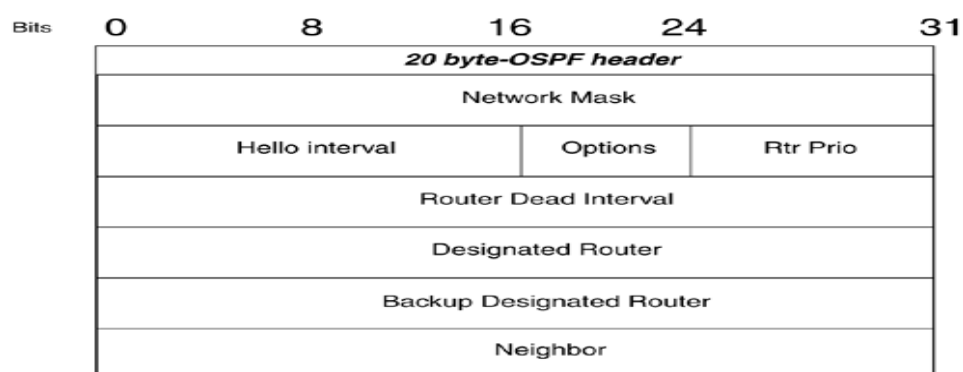


Figure 3.2: OSPF Hello Packet (Shamim et al, 2002)

Network Mask: subnet mask that determine the network address of each interface

Hello Interval: time in seconds between which routers send hello message. Hello messages are sent once every 10 seconds on broadcast or point-to-point networks, and once every 30 seconds on non-broadcast multi-access (NBMA) networks like frame-relay, ATM etc. (Macfarlane, 2006).

Options: represent optional features of OSPF.

Router Priority: this field is used when electing the DR/BDR router on a shared network segment. The router with highest priority is elected the DR router (Cisco, 2003).

Router Dead Interval: number of seconds a router is considered down. Dead interval is 4 times the hello interval.

Designated Router (DR): This field indicates that the router is elected as the DR. The router with highest priority is elected DR (Cisco, 2003). If there is a tie in priority, then the router with highest router ID is elected the DR. When there is any change in the network, the router with the change will send a multicast update using the address 224.0.0.6 to the DR and BDR only, which in turn the DR will flood the whole network with the update using the multicast address 224.0.0.5 (Cisco, 2003). This helps in eliminating a huge amount of traffic when changes occur in OSPF network.

Backup Designated Router (BDR): This field indicates that the router is elected the BDR, in case the DR fails. The router with the second highest router priority or router ID is elected the BDR (Cisco, 2003).

Neighbour Router: The router ID of neighbour router.

2. DBD Packet: Database Description packet contains a summary list of sending router's link state database, which is used by the receiving router to cross check against its local link state database (Shamim et al, 2002). The DBD allows the receiving router to know what networks it knows about from the sending router and the ones it did not know about (Shamim et al, 2002).

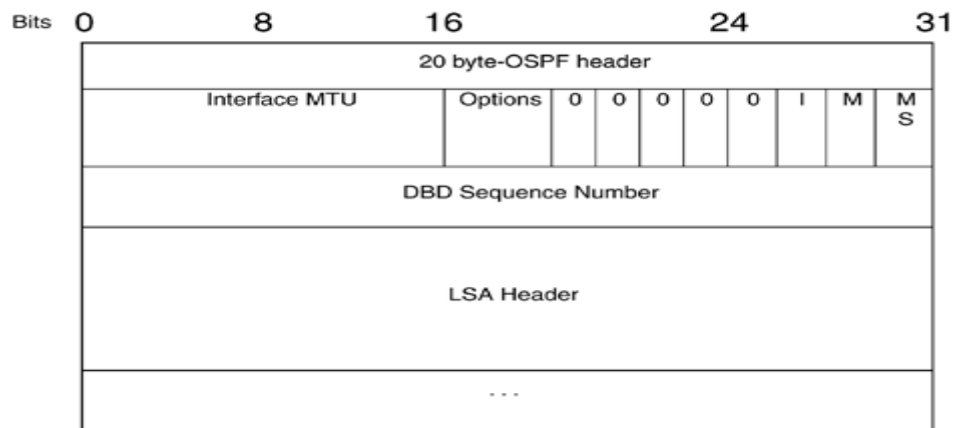


Figure 3.3: Database Description Packet (Shamim et al, 2002)

Interface MTU: this field indicate the largest amount of data that can be sent through an interface.

Options: represent optional features of OSPF.

I bit: This field determine whether the packet is the first in DBD exchange. When it is set to 1, it means that this is the first DBD packet exchange.

M bit: Indicate whether there are more packets left in the DBD exchange. When set to 1, means that there are more packets to follow.

MS bit: indicate which router is the master or slave in the DBD exchange process. The router with highest router priority is selected as master or router ID breaks tie. When set to 1, indicates that the router is selected as master and when set to 0, is slave. The master will first send its DBD, and then the slave will send its own.

DBD Sequence Number: Used in the master/slave DBD exchange process to avoid DBD exchange redundancy. Only the master routers increment the sequence number.

LSA Header: contains list of LSAs headers.

3. LSA Packet: Link State Advertisement packet is individual advertisement about specific networks (Shamim et al, 2002). There are several types of LSA packets that help build the OSPF database. The most common ones are shown in the table below (Shamim et al, 2002).

LSA Type	Name	Description
1	Router LSA	Advertisement about one network. Flooded within an area.
2	Network LSA	Advertisement about all routes in the same Ethernet segment. This type of LSAs are generated by the DR.
3	ABR Summary LSA	Advertisement of the summarised route of another area. The summarised route is flooded to the backbone area. This type of LSA is generated by the ABR.
4	ASBR Summary LSA	Advertises the location of the ASBR. This is the IP address of the ASBR router.
5	AS-External LSA	Advertisement of summarised external routes from outside the Autonomous System. This type is generated by the ASBR.

Table 3.1: OSPF LSA Types and Description (Rob, 2011)

Figure 3.4 shows the LSA packets generated by OSPF routers and how ABR and ASBR routers flood the LSAs between different areas.

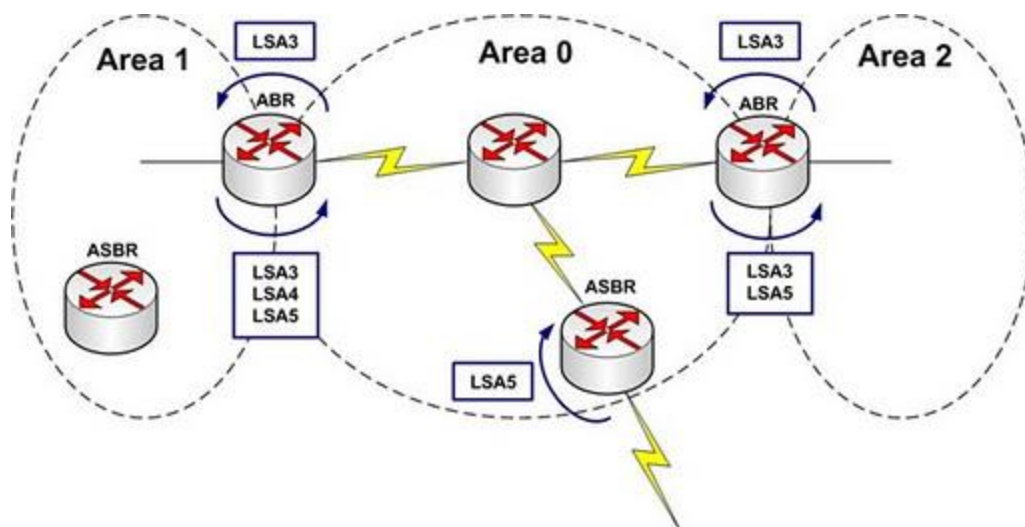


Figure 3.4: OSPF LSA Exchange between Areas (Caue, 2008)

4. LSR Packet: Link State Request packet is send by the receiving router about any network in the DBD it did not know about (Shamim et al, 2002).

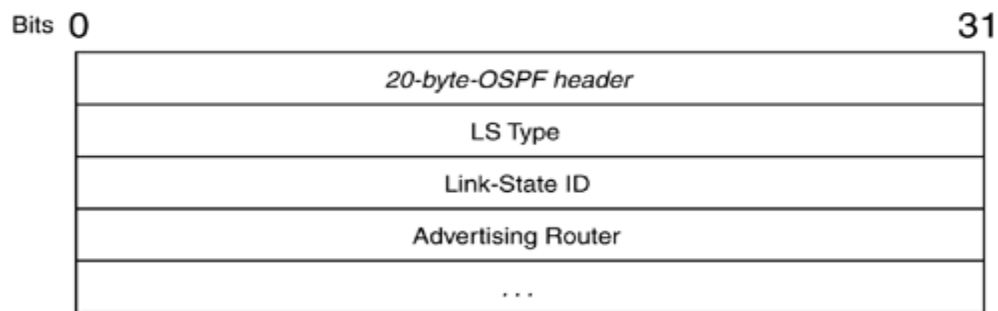


Figure 3.5: OSPF LSR Packet (Shamim et al, 2002)

LS Type: The type of LSA that is requested.

Link-State ID: Link-State ID of the type of LSA requested.

Advertising Router: Is Router ID of the router that sends the LSR packet.

5. LSU Packet: Link State Update is a reply (contains one or more LSAs) to LSR packet. Contain link state information that the receiving router requested (Shamim et al, 2002).

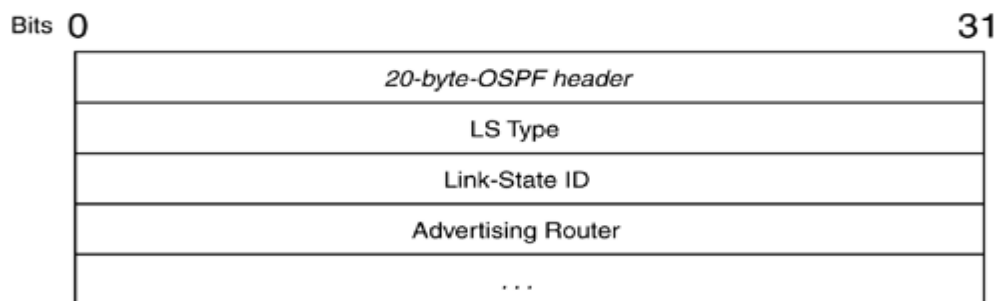


Figure 3.6: OSPF LSU Packet (Shamim et al, 2002)

6. LSAck Packet: Link State Acknowledgement packet is send by OSPF router to confirm receipt of LSU (Shamim et al, 2002).

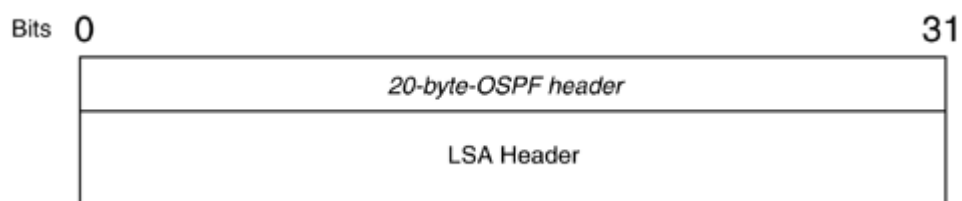


Figure 3.7: OSPF LSAck Packet (Shamim et al, 2002)

3.5 OSPF Areas

All routers in OSPF network are configured initially in area 0 sometimes called the backbone area, but as the network grows and updates has become to numerous, there will be need to divide the network into multiple areas with every single area containing a group of routers (Microsoft, 2012). OSPF have some specifics that; all areas must connect to area 0 (but with the exception of virtual links) and all routers in an area have the same topology table (Moy, 1998) & (Haas, 2005). The goal of dividing the network into areas is to localise OSPF updates within an area, which can help reduce network updates with route summarisation at the area boundary routers and also make the OSPF network more efficient (Haas, 2005).

Backbone Area: this is the area that all other areas connect to, sometimes known as area 0. All LSA type updates passes through the backbone area, and consequently any information from other areas must pass through the backbone area (Haas, 2005). The backbone area is the centre of the OSPF network.

Ordinary Area: is the default configuration of OSPF network areas. Default area configuration exhibits the following characteristics (Moy, 1998):

- Summary LSAs are allowed between different areas.
- External LSAs are also allowed.

Stub Area (SA): block type 4&5 LSAs from entering the area (ASBR summary routes & external routes) (Haas, 2005). Stub areas only accept routes from within the autonomous system. A default route is generated by the ABR for all external routes in this type of area (Haas, 2005).

Totally Stubby Area (TSA): TSA was created by Cisco, it blocks all LSAs from entering the area (Haas, 2005). In totally stubby area, a default route is generated by the ABR for all other routes (Haas, 2005).

Not – So – Stubby Area (NSSA): acts just like the stub area, only that these types of areas allow passage of external routes (Haas, 2005). NSSA passes external routes through type 7 LSA and converts back to type 5 LSA once they reach the backbone area (Haas, 2005).

Figure 3.8 illustrates the different types of areas and LSA propagation. From the figure 3.4, it shows that all other areas connect to the backbone area with summary LSAs generated by

the ABR being injected into the backbone area. Stub area and totally stubby areas block external LSAs, so instead the ABR router injects a default route into the areas, stub area though allows summary LSAs of other areas. ABR for the ordinary area injects external and summary LSAs into the area. NSSA allow external LSAs as type 7 but converts it to type 5 LSA as its ABR passes it to the Backbone area.

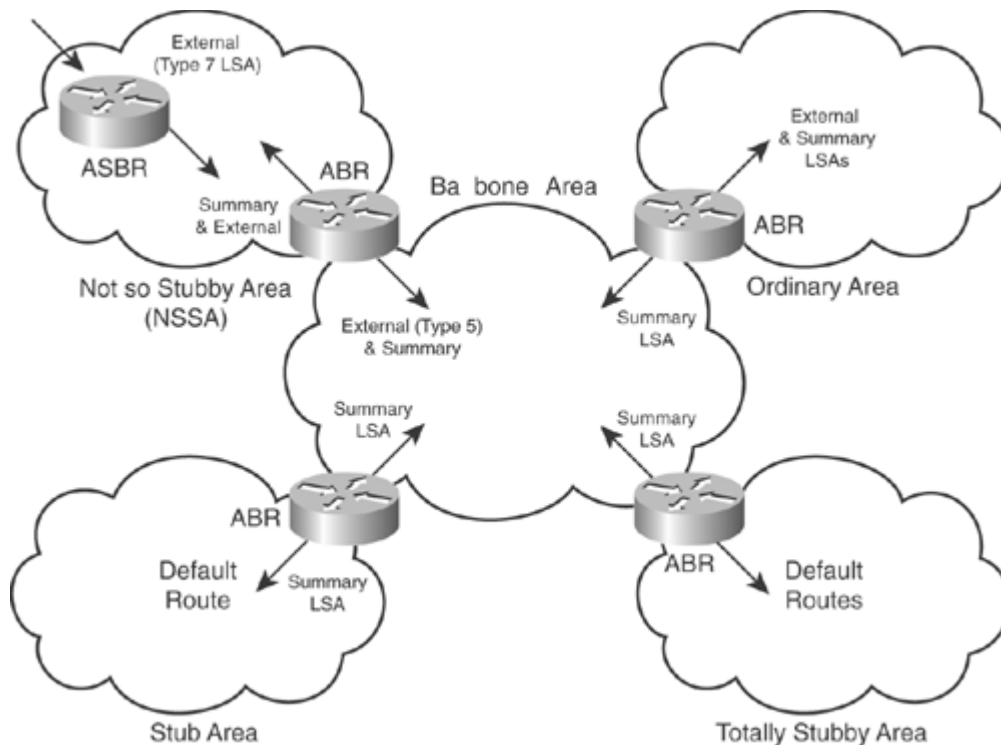


Figure 3.8: OSPF Area Types (Shamim et al, 2002)

3.6 OSPF Router Types

In OSPF, routers play different roles depending on where they are placed in the network. The following are the types of routers and their roles in an OSPF network.

Internal Routers: these are routers that are completely within an area, they do not have any interface connecting to other area (Haas, 2005). Each router in the area runs SPF algorithm to determine the best paths to reach other routers within that area.

Backbone Routers: these are routers that are located in area 0 or any other router in the network that has an interface connected to area 0 (Haas, 2005). Internal routers and ABR are considered backbone routers.

Area Boundary Routers (ABR): these are routers that have one interface in multiple areas. ABR link up two or more areas together (Haas, 2005). Typically ABR link other areas to area 0/backbone area. OSPF route summarisation happens at the ABR.

Autonomous System Boundary Routers (ASBR): these are routers that connect the OSPF network to an outside domain network. It has one interface in the OSPF network and one or more interfaces in other routing domains (Haas, 2005).

Designated/Backup Designated Routers: The DR/BDR act as a control for shared segment non – broadcast multi – access (NBMA) networks (Lammle, 2011). In a shared segment network, whenever there is change in link or update, the router with the change will send the update to the DR/BDR (with multicast address: 224.0.0.6) instead of flooding the whole network with the update and in turn the DR will flood the update to the rest of the network (with multicast address: 224.0.0.5) (Lammle, 2011). The BDR is a backup in case the DR fails. These help eliminate a huge amount of traffic that is going to be sent between the routers for every single change (Cisco, 2003).

3.7 OSPF Neighbour Relationship Establishment

In OSPF network, neighbour relationship only exists within routers in the same area (Lammle, 2011). The following steps describe how OSPF enabled routers form neighbour relationship.

Step 1: Determine router ID

When the OSPF process is started, the first thing a router do is to determine its own router ID. It's a number the router picks to identify itself to the neighbours. The highest IP address is selected as the router ID, Loopbacks interface beat physical interfaces. Router ID can also be hard coded in the router using the `#router-id` command, this overrule everything.

Step 2: Add Network Interfaces to the Link State Database

This is done by using the `#network` command to add interfaces in the OSPF process. This dictates which interfaces to include in the OSPF process.

Step 3: Send a HELLO Message

Down state: Then the router will start exchanging hello messages within the OSPF enable interface(s) (Moy, 1998). This is considered a down state. In order for the routers to

establish neighbour relationship, some information inside the hello message must be the same on both routers. These are:

- Hello and Dead Timers
- Network Mask
- Area ID
- Authentication Password

Step 4: Receive Hello

Init State: routers have received hello message and are checking the information (Hello and Dead Timers, Network Mask, Area ID and Authentication Password) inside the hello message to see if they are the same (Moy, 1998). This is considered init state. If any one of these parameters does not correspond, the neighbour relationship will not be established and state will be flapping between init and down state and vice versa.

Step 5: Send Reply Hello

2 – Way State: when the receiving router check all the parameters and they all correspond, it then send a reply Hello message indicating that they can form neighbour relationship (Moy, 1998). This is known as the 2 – Way State. In this state, both routers will check the neighbour field in the Hello packet to see whether is already listed as a neighbour. If it is listed in the Hello packet, they router will know that this is just one of those Hellos that is send after every 10 second (in broadcast or point-to-point networks) or 30 second (in non-broadcast multi-access (NBMA) networks), in which the dead timer is reset (by default 4 times the Hello time) (Cisco, 2005). This is where the neighbour relationship ends. If it is not listed as a neighbour in the Hello packet, then this is a new neighbour relationship.

Step 6: Master – Slave Relationship determined

Exstart State: when routers enter this state, it shows that their Hello packets agree and they are now ready to form neighbour relationship (Moy, 1998). They routers are now ready to start exchanging their link state databases also known as DBD (Database Description Packet). This state is known as the exchange start or Exstart state. The master – slave relationship determines which router sends its DBD first (Cisco, 2005). The router with the highest priority is set as the master or the higher router ID breaks tie (Cisco, 2005). The

router set as master will send its DBD first, and then the slave will send it DBD second (Cisco, 2005).

Step 7: DBD are Acknowledged and Reviewed

Loading State: both routers will then acknowledge that it receives the DBD by sending a little acknowledgment packet, because OSPF is reliable (Moy, 1998). The DBD packet is reviewed by each router so as to know which network it knows about and those it those not know about (Cisco, 2005). While the DBD is being reviewed, the state will change to loading state (routers are loading the information in the DBD they need into memory). During this process, the slave router will first send a LSR packet (Link State Request Packet) about any network in the DBD It did not know about, and the master will respond with LSU packet (Link State Update Packet) containing all information about the network (Cisco, 2005). Once the slave has finish requesting all the networks it did not know about, the master router will then start sending LSR packets about any network it did not know about and the slave router will respond with LSU packet (Cisco, 2005).

Step 8: Neighbour are Synchronised

Full State: the exchange process of LSR and LSU packets will continue between the master and slave router until they are synchronised (Moy, 1998). All the routers in the network using OSPF now have the same link state database. This state is known as the full state.

Figure 3.9 shows the steps router 2800 follow to establish neighbour relationship with router 7200. Initially, all routers interfaces are down. Router 2800 sends a hello message to router 7200 with its name (Init State), router 7200 send a reply hello message with its name too (2-Way State). Then master-slave relationship is determine, router 7200 is declared the master because it has the highest interface address and router 2800 is the slave. So the routers will now start exchanging their DBDs (Exstart/Exchange State), router 2800 is the first to send its DBD because it is the slave then router 7200 will sends its own DBD afterwards. Both routers will then loads the DBD packets into their own database as the same time sending a LSR for any network information they do not know about (Loading State). Finally, all the routers now have identical database (Full State).

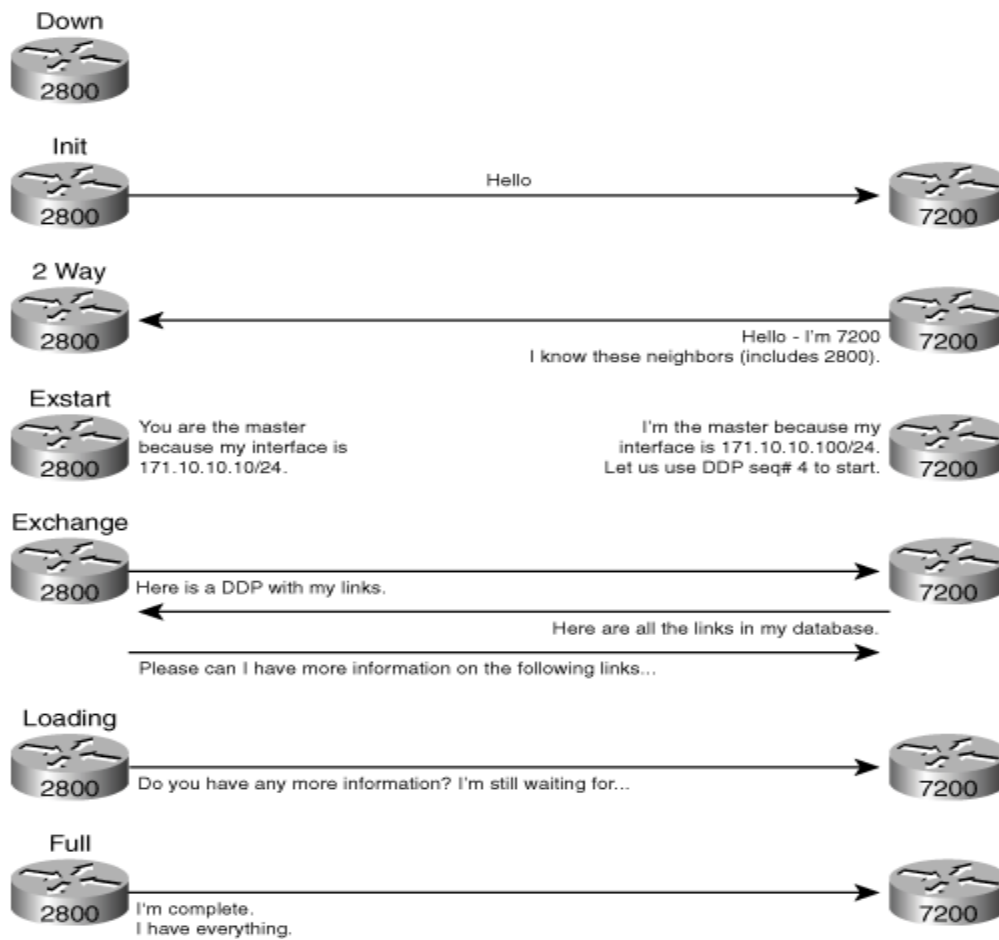


Figure 3.9: OSPF Neighbour Relationship Process (etutorials, 2011)

Once neighbour relationship is formed between OSPF enable routers where by all of them will have identical topology table, each router in the network will put itself as the root of the network and run Dijkstra/SPF algorithm to figure out the shortest path around the network.

3.8 Advantages and Disadvantages of OSPF

Advantages

- Industry standard.
- Fast to converge.
- Supports multiple routes.
- Supports VLSM (Variable Length Subnet Mask).
- Hierarchical in design with area 0 as the backbone of the network.
- Support all types of networks (small, medium or large).
- Route summarisation reduces size of routing table, which helps reduce consumption of router memory.

Disadvantages

- Difficult to understand and configure.
- Consumes router memory because it keeps the whole topology of the network and also consumes processor during convergence.

3.9 Conclusion

In this chapter, OSPF packets are explored and explained. It also explains the OSPF areas and DR/BDR process which all help reduce the network traffic in an OSPF network. Then it explains the steps OSPF enable routers follow from sending Hello message to exchanging link state database and loading the database into memory when forming neighbour relationship.

4 Enhanced Interior Routing Protocol (EIGRP)

4.1 Introduction

In this chapter, EIGRP is explained in more detail. EIGRP packet format, routing process and the three tables of EIGRP (neighbour, topology and routing table) are all explained. Finally, the DUAL process of EIGRP is also explained and the advantages and disadvantages of EIGRP are stated.

4.2 Overview

Enhanced Interior Gateway Protocol (EIGRP) was created by Cisco in the early 90s to solve the problems of distance vector routing protocols (RIP and IGRP) that is slow convergence and routing loops (Shamim, 2002). EIGRP is a Cisco proprietary routing protocol (works only with Cisco equipment) based on distance vector routing protocol but also have some features of link state routing protocol (Clark, 2003). EIGRP is sometimes considered a hybrid routing protocol because of it possesses the features of link state routing protocol such as neighbour discovery and partial updates (Ayub et al, 2011).

Unlike OSPF that has the whole topology of the network, EIGRP only have the knowledge about its neighbours. Also EIGRP use DUAL algorithm to calculate the shortest path to destination network (Cisco, 2005). The DUAL algorithm keeps a backup path to every destination called the feasible successor while the primary path is called successor. So whenever the successor fails, it will instantly switch to the feasible successor (Shamim, 2002). If there is no feasible successor, the router will send a query message to its neighbours whether they have another path to the failed network, and routers will either reply with the route to that network or reply to infinity indicating they do not have another path. This process helps prevent routing loops.

4.3 EIGRP Packet Format

The EIGRP packet is 32 bit in size comprising of different fields that is encapsulated in IP. The different fields of EIGRP packet is shown in figure 4.1 below (Shamim, 2002).

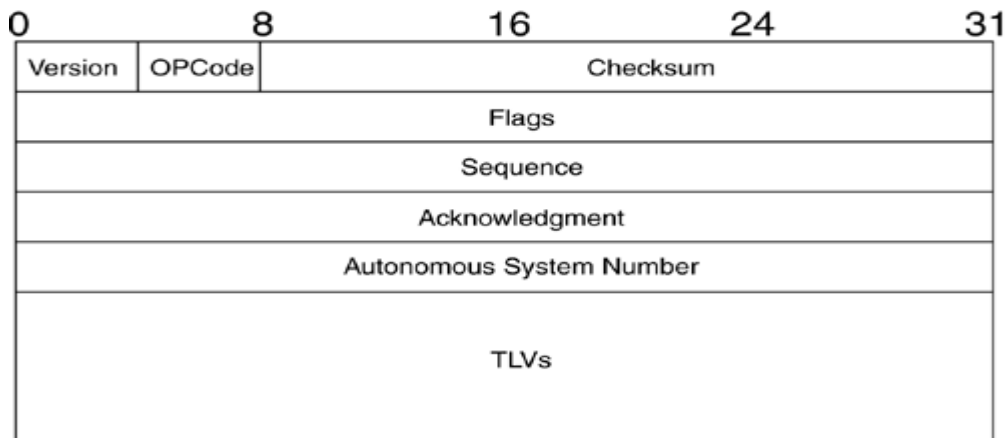


Figure 4.1: EIGRP Packet Format (Shamim, 2002)

Version: Indicates the version of the EIGRP process. EIGRP version 2 is the most recent.

OPCode: this is known as the operation code which indicates the type of EIGRP message. There are five types of EIGRP message: 1 – Update, 3 – Query, 4 – Reply, 5 – Hello and 6 – IPX SAP.

Checksum: specifies IP checksum of the EIGRP packet.

Flags: indicates the type of EIGRP flag. There are two types of flags in EIGRP. The first bit (0x00000001) called the init bit indicates new neighbour relationship while the second bit (0x00000002) called the conditional receive bit is used in proprietary multicast algorithm.

Sequence: indicates the sequence number used by RTP to send message reliably.

Acknowledgment: used by neighbours to acknowledge packets received.

Autonomous System Number: specifies the network EIGRP packet belongs. Routers running EIGRP will only process packets with the same autonomous system number (Shamim, 2002).

Time and Value Fields (TLVs): the most important value in the TLV is the EIGRP parameter which used in EIGRP process to establish neighbour relationship (Shamim, 2002).

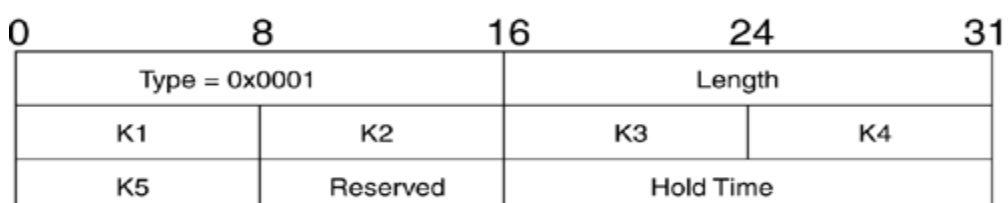


Figure 4.2: EIGRP Time and Value Fields (Shamim, 2002)

Type: determines the type of TLVs. The common ones are:

0x0001: Hello/Hold time.

0x0102: EIGRP IP Internal Routes TLV.

0x0103: EIGRP IP External Routes TLV.

Length: Indicates the length of the frame.

K Values: the K values between two routers must be the same in order to establish neighbour relationship.

Reserved: not used.

Hold Time: the time before a neighbour is considered dead.

4.4 EIGRP Packet Types

EIGRP uses five types of packets to communicate between neighbour routers (Cisco, 2005).

EIGRP uses a multicast address of 224.0.0.10 to communicate between neighbours.

Hello: The hello message form neighbour relationship between routers. EIGRP neighbour routers exchange hello packets after every 5 seconds in T1 and Ethernet networks and once every 60 seconds in multipoint frame relay networks (Cisco, 2011). Hello message dose need to be acknowledged (Cisco, 2005).

Update: Once neighbour relationship is formed, the routers will start sending update about the routes they know about. EIGRP does not send its whole routing table to its neighbours, is uses triggered updates meaning it only sends partial update of what needs to be sent (Cisco, 2011)

Query: If there is link failure, and the EIGRP router with the link failure does not have a backup path, the router will send a query message asking its neighbours if they have a backup path to the network (Cisco, 2011).

Reply: This is a response to a query message, indicating whether there is a backup path to a failed network or not (Cisco, 2011).

Acknowledgment: EIGRP uses RTP (Real – time transport protocol) to acknowledge every message it received reliably (Cisco, 2005). EIGRP acknowledges every single message (update, query and reply) except a hello message (Cisco, 2005).

4.5 EIGRP Routing Process

An EIGRP routing process maintain three different tables

1. Neighbour table
2. Topology table
3. Routing table

When EIGRP is first configured, it uses the hello message to discover its neighbours and start exchanging routes with its neighbours. These routes will then be placed in the neighbour table, and EIGRP will use DUAL algorithm to determine the best routes to destination network. The best routes are placed in the routing table also known as successor (primary routes), while the second best routes would be place in the topology table as back up routes known as feasible successor. In the case that the successor link fails, it will immediately be flushed out from the routing table and the feasible successor link will immediately be moved into the routing table without any delay.

4.5.1 Neighbour Table

Each router in the EIGRP network maintains a neighbour table which contains a list of adjacent routers (Cisco, 2005). Neighbour routers discover their neighbours by exchanging hello messages through a multicast address 224.0.0.10 in a periodic interval of 5 seconds (Cisco, 2005). The hello message is advertised together with a hold time. The hold time is the time it takes a router to consider its neighbour dead if it didn't receive any hello message for that hold time which is 3 times the hello message interval (Cisco, 2005). The hold time is reset each time a router receives a hello message (Cisco, 2005). If the hold time expires, then the router has to find another path to that router.

4.5.2 Topology Table

After neighbours are formed, the neighbours will send all their best routes to each other and the routers will put those into its topology table (Cisco, 2005). The topology table maintains all the routes to destination networks. The topology table includes the following fields which help determine a loop free path (Shamim, 2002):

Feasible Distance (FD): The feasible distance is the lowest cost distance from a router to a destination network (Shamim, 2002). The feasible distance is the sum of the metric of feasible distance and the advertised distance (Shamim, 2002).

Figure 4.3 shows how Router A calculates the feasible distance to reach network 7 by adding together the metric of its neighbour's links (Shamim, 2002).

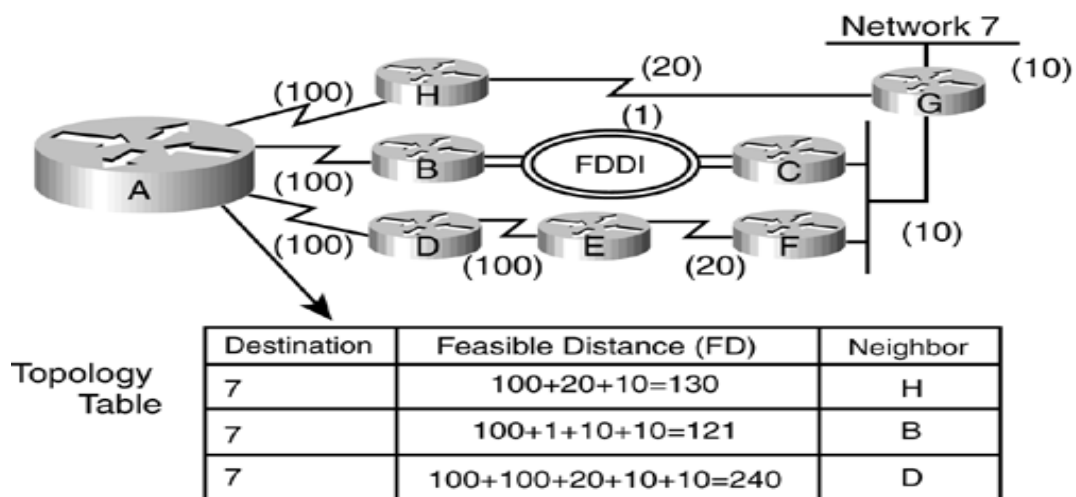


Figure 4.3: Feasible Distance Calculation (Shamim, 2002)

Advertised/Reported Distance (AD/RD): The advertised distance is the metric distance that the neighbour reported (Shamim, 2002). It is how far the neighbour router is from a destination network.

Figure 4.4 shows the reported distance of the routers from Router A's perspective. For example since Router H is Router A's neighbour, Router H will advertise a distance of 30 to Router A in order reach network 7 (Shamim, 2002).

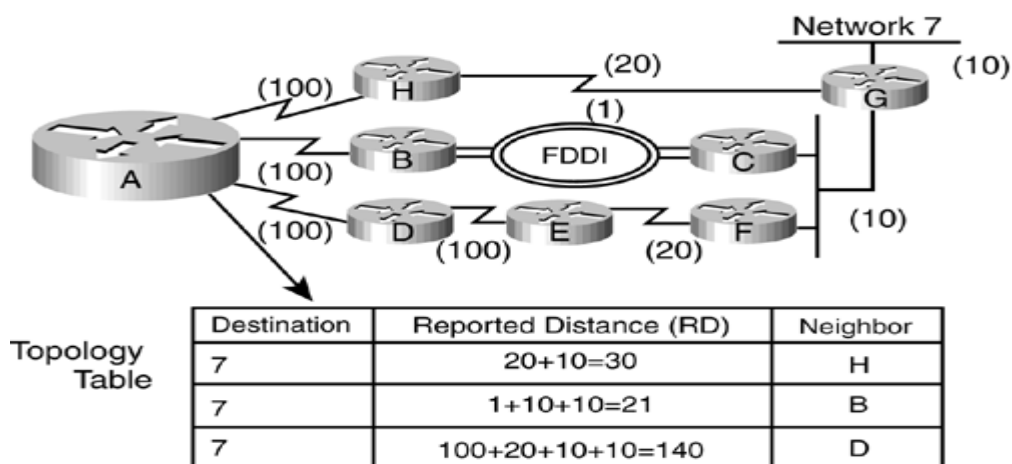


Figure 4.4: Reported Distance Calculation (Shamim, 2002)

The feasible distance and the advertised distance metrics are used in EIGRP to determine the feasible successor to a destination network.

Feasibility Condition (FC): In order for a link to become a feasible successor, it must satisfy the feasibility condition. The feasible condition rule states that “to be considered a feasible successor; the advertised distance (AD) must be less than the feasible distance (FD) of the successor” (Shamim, 2002). This helps prevent loops in the network.

Successor: The successor is the best path among other paths that is placed in the routing table. The link with lowest feasible distance to the destination network is the successor (Shamim, 2002).

Feasible Successor: Is the link that satisfies the feasible condition (Shamim, 2002). It is the backup path to a destination network in case the successor fails. The feasible successor remains in the topology table (Cisco, 2005). But when the successor fails, EIGRP will immediately look for its feasible successor and place it in the routing table reducing any delay in convergence (Shamim, 2002).

Figure 4.5 shows how Router A chooses the successor and feasible successor to destination network 7 (Shamim, 2002).

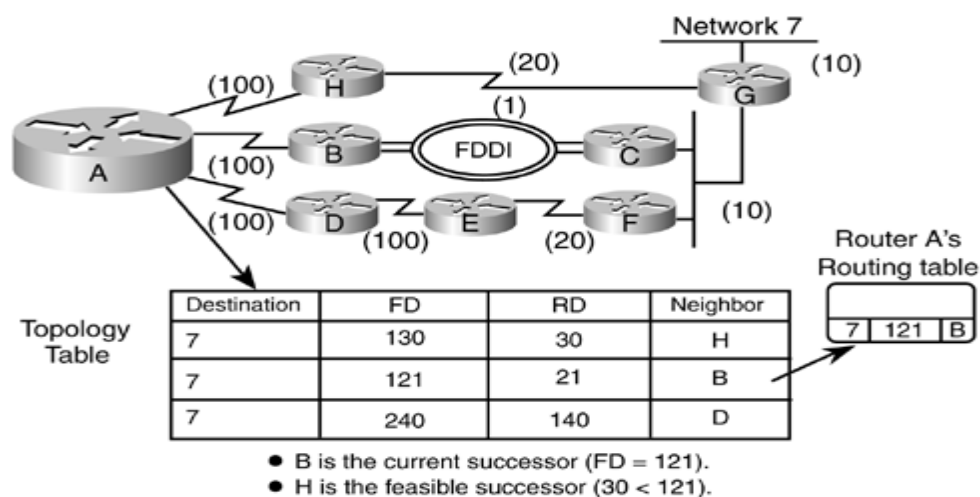


Figure 4.5: Feasible Successor Calculation (Shamim, 2002)

In the figure 4.5, it proves that Router B is the successor because it has the lowest feasible distance of 121 to destination network 7. Now Router A will choose the feasible successor between Router H and D which must satisfy the feasibility condition that the report distance

(RD) must be less than the feasible distance (FD) of the successor. In this case, Router H is the feasible successor because its RD=21 is less than the FD=121 of the successor. Router D is neither a successor nor feasible successor because its RD=140 is greater than the FD=121 of the successor.

Passive Route: A passive indicates that is a good route, nothing is happening (Shamim, 2002).

Active Route: An active is when the successor fails and there is no feasible successor to that destination network (Shamim, 2002). So the router marks the route as active indicating that it's trying to find a path another path to that network (Shamim, 2002).

4.5.3 Routing Table

Each router will then run DUAL algorithm to find the best paths across the network. The best paths are placed in the routing table. These paths are called the successors, the feasible successor remains in the topology table.

4.6 Diffusing Update Algorithm (DUAL)

The Diffusing Update Algorithm (DUAL) is mechanism that EIGRP uses to select a loop free path (known as successor) to destination network (Malhotra, 2002). DUAL also keep a backup path (feasible successor) to every destination network, these process make EIGRP to achieve faster convergence than any other routing protocol (Shamim, 2002).

When there is a link failure in the EIGRP network and the successor link fail, convergence take place immediately by switching to the feasible successor of that failed link (Malhotra, 2002). EIGRP will then send an update message telling its neighbours about the change. These process save huge amount of routers CPU usage during convergence. From figure 4.5, if Router B (successor) fails, EIGRP will immediately look in the topology table and choose Router H (feasible successor) as the new successor to Network 7.

So in any case that the successor and the feasible successor both fail, the EIGRP router will use DUAL to get another path to destination. During DUAL process, the router will enter into active state and then send a query message out to all its neighbours to see if they have a route to the failed network (Shamim, 2002). If the neighbours have a route they will send a reply message, then the querying router will have to choose the one with the lowest metric i.e. if there is more than one reply (Malhotra, 2002). But if they neighbour routers do not have a route to the failed destination, they too will send a query message to their neighbours

or send a reply message with a metric count to infinity indicating they do not have a backup route (Malhotra, 2002). From figure 4.5 for example if Router B (successor) went down and Router H (feasible successor) is also down, Router A will send a query message to Router D asking it whether it has a route to Network 7. Router D will then send a reply message with a route to Network 7, and Router A will then converges to Router D as the next hop to reach Network 7.

4.7 Advantages and Disadvantages of EIGRP

Advantages

- Only protocol to support backup route (fast convergence/DUAL).
- It is very simple to configure.
- Fast convergence.
- Route summarisation can be implemented everywhere in the network.
- Unequal cost load – balancing.
- Combines best of distance vector and link state protocols.
- Supports multiple network protocols (IP, AppleTalk, IPX etc.).

Disadvantages

- Cisco proprietary. Therefore it only operates with Cisco routers.

4.8 Conclusion

In this chapter, EIGRP packets are explored and explained. The three EIGRP tables; Neighbour, Topology and Routing tables are also explained. It also explains the EIGRP DUAL process which has two paths to every destination network i.e. the successor is put in the routing table as primary path and the feasible successor is left in the topology table as backup path. Then it explains the query packet process that EIGRP uses when both the successor and the feasible successor links fail.

5 Methodologies

5.1 Introduction

This chapter briefly explains OPNET Modeler. It also explains the simulation methodology, the definition of requirements; equipment and configuration nodes used for the OSPF and EIGRP scenarios. Then it explains the experimental methodology, the different network connection type used (shared Ethernet segment and point – to – point connection) and the OSPF and EIGRP experiment.

5.2 Research Methodology

In the past years, so many researches have been conducted to examine the difference between EIGRP and OSPF base on several parameters like convergence time, CPU and memory utilization, packet end-to-end delay etc. Base on the literature review I have conducted, most of these researches have been conducted using different kinds of simulation software. This research is carried out using both OPNET simulation software and real equipment in the lab. These will be used to compare and analyse the difference in findings between simulation and real world.

5.3 Simulation Methodology

Although there are many simulators available, common ones OPNET, NS-2, OMNet ++, NS-3, SimPy, JisT/WANS etc. (Weingartner, 2009), I choose to use Optimised Network Engineering Tool (OPNET) Modeler.

5.3.1 Optimised Network Engineering Tool (OPNET)

According to OPNET documentation (2004), OPNET Modeler is explained as “an environment to study performance changes of your network: organisational scaling, technology changes and application deployment etc.”

OPNET comes in three flavours; OPNET IT Guru, OPNET SP Guru and OPNET Modeler. OPNET IT Guru is the free version of OPNET mainly use for designing and testing Network performance while OPNET SP Guru is mainly for service providers and OPNET Modeler is a licenced version mainly for research purposes (OPNET, 2004). OPNET has various real life configuration capabilities and results are collected through Discreet Event Simulator (DES) which makes result of simulation in OPNET more accurate (Sarkar & Halim, 2011). In a research by Fritz (2004), he tested various network simulators to know

which one produces more accurate results and he concluded that OPNET produce more accurate result than all the simulators tested.

OPNET is designed in a hierarchical order with three main domains; Network Domain, Node Domain and Process Domain (Prokkola, 2006). Network Domain provides a graphical user interface (GUI) environment provides physical locations where a person can drag and drop different equipment from the object palette or choose a predefined network topology (OPNET, 2004) (refer to figure 5.1). Node domain is the internal structure of the network components whether communication node or link node (OPNET, 2004) (refer to figure 5.2). Process domain is programming level interface used for customising network equipment with C and C++ language or editing packets and changing queuing behaviour (OPNET, 2004) (refer figure 5.3).

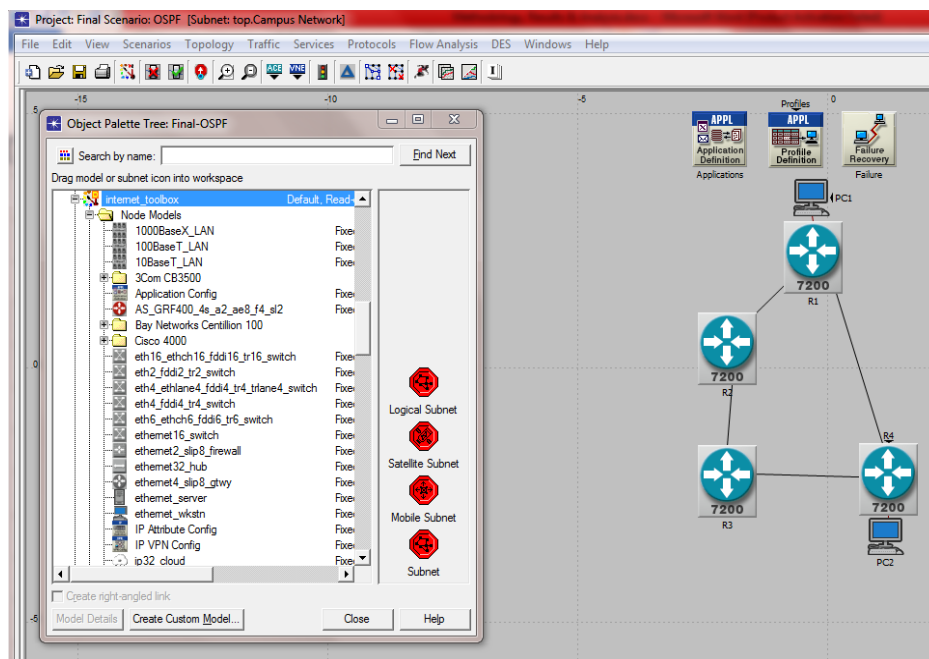


Figure 5.1: Network Model (OPNET, 2004)

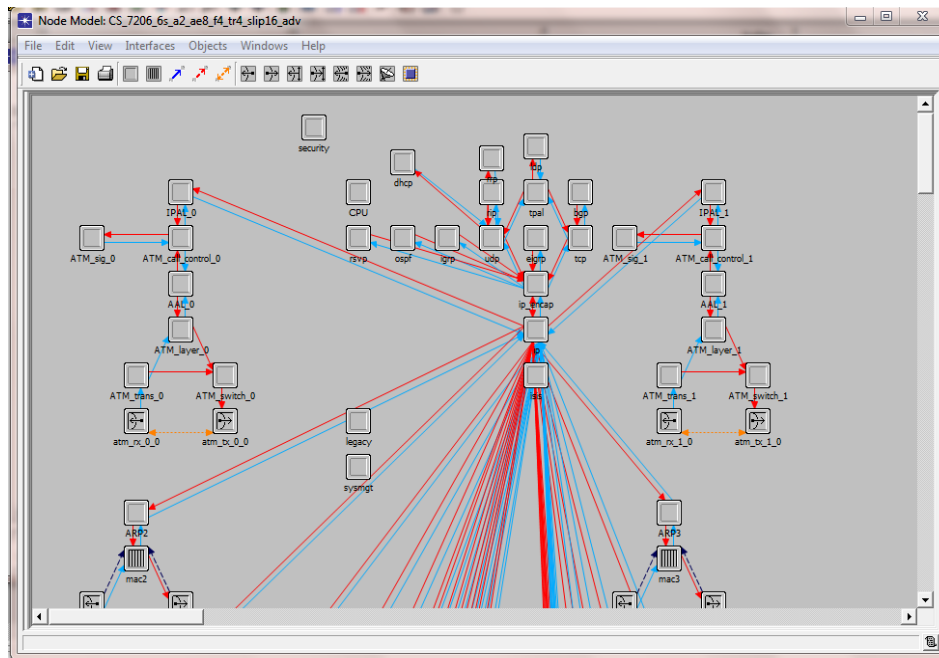


Figure 5.2: Node Domain (OPNET, 2004)

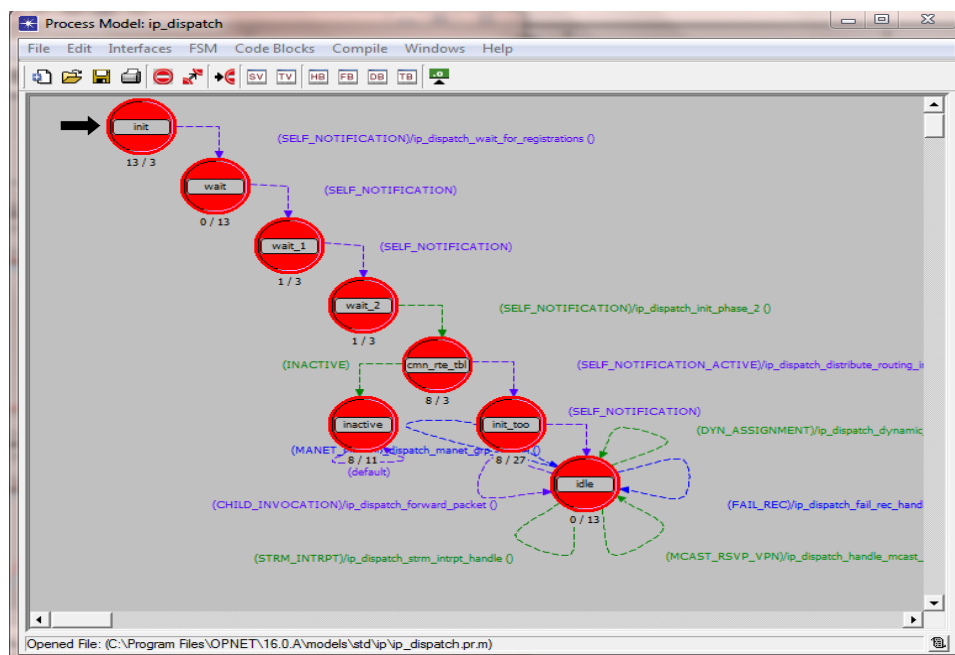


Figure 5.3: Process Domain (OPNET, 2004)

Shown in figure 5.4 is a step by step workflow chart to design a network model in OPNET simulator and statistics collection.

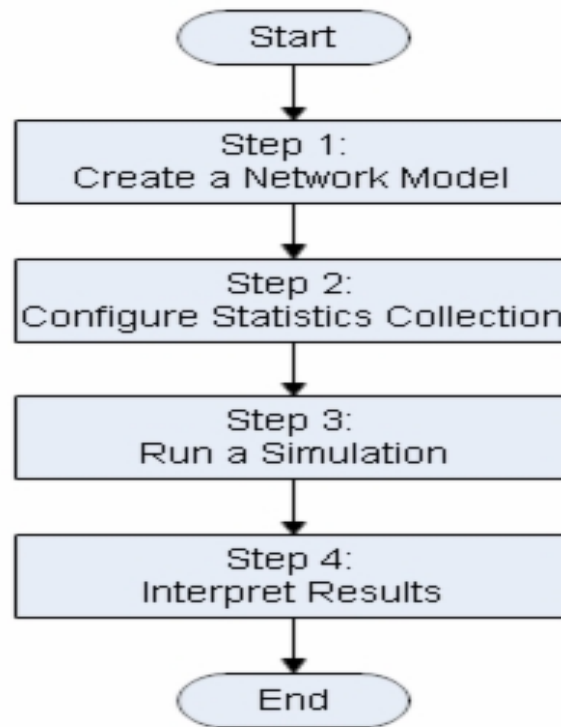


Figure 5.4: Statistics Collection and Workflow (OPNET Modeler, 2004)

Before a network model can be created in OPNET, a project and scenario has to be created first. OPNET (2004) defined a project as “a collection of related network scenarios in which each represents a different aspect of network design. A Scenario is a single instance of a network”. A scenario may contain specific settings for the network such as routing protocols, topology, applications etc.

Step 1: Create a Network Model

The next step is creating the network, which can be achieved by either importing from OPNET library or drag and drop nodes from the object palette on the network domain, and connect the nodes with different links all available in the object palette (see figure 5.1). Application and profile definition configuration is at this step, these are the traffic to be generated and which station to generate specific traffic. The manner in which the application and profile config are configured will have impact on the displayed graphs and statistics (OPNET, 2004).

Step 2: Configure Statistics Collection

After designing the network, the next step is to choose the statistics to be collected form the network model. These results will be displayed in a graph format. There three different

types of statistics that can be collected depending on what you want to analyse; Global statistics, Node Statistics and Link Statistics.

Step 3: Run Simulation

Network is set up, statistics are chosen, and now the next step is to run the simulation. The duration of the simulation can be expressed in seconds, minutes, hours, days or weeks.

Step 4: Interpret Results

This is final step in which the chosen statistics will be displayed in a graphical format.

5.3.2 Network Topology

In this dissertation, I designed the same network topology which is used for two different scenarios; first scenario configured with OSPF and the second scenario configured with EIGRP. The network topology is design with the following nodes and links:

- Application Definition.
- Profile Definition.
- Failure Recovery.
- 2 ethernet_wkstns.
- 4 Cisco 7200 Routers.
- PPP_DS3 Duplex Link.
- 10BaseT Duplex Link.

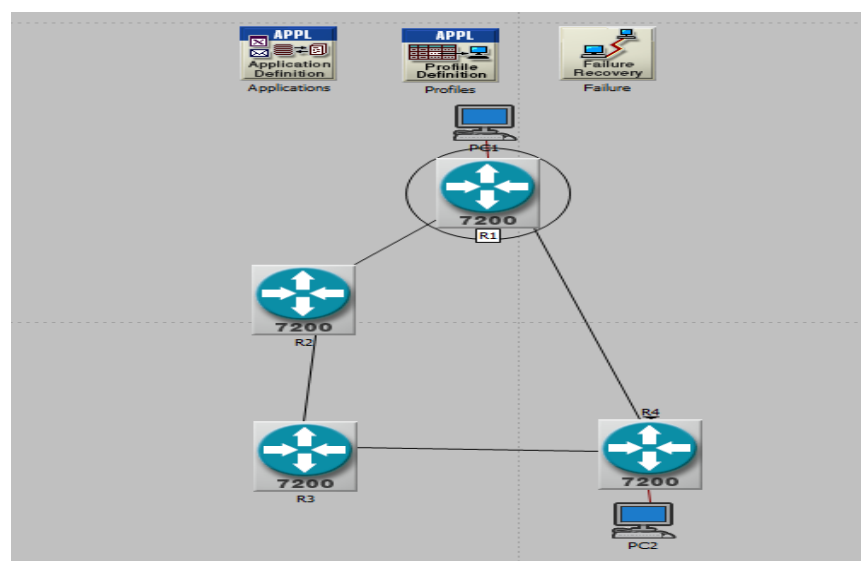
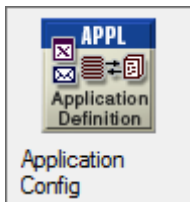


Figure 5.5: Network Topology

Figure 5.5 illustrate the network topology and equipment used in this research. The following briefly explains the network utilities, nodes and links used:



Application Definition: This is a configuration node that can be used to enable applications to be used in the network. The application definition node has predefined applications available like Email, HTTP, FTP, Voice, Video Conferencing etc. which can be enable together with the type of load (Heavy, Medium or Light) or custom application used for creating other applications if the interested application does not correspond to any of the predefined applications.



Profile Definition: This is used to create user profiles, which specifies what user to use certain application(s) enabled/configured from the application definition node. This node also defines the behaviour of each application, for example the time to start the application during simulation, the number of times to repeat the application, the time to stop the application etc. These profiles will be enabled on client and server nodes to generate traffic in the simulation.



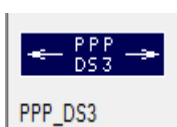
Failure Recovery: This is a controller node that can be used to model a link failure and recovery in the network during simulation.



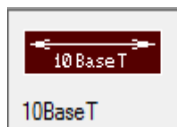
Ethernet Workstation: This represents a workstation that can be configured as a client or server used for generating the network traffic.



Cisco 7200 Router: This is a Cisco router node placed at different networks or sites. This router has the following interfaces: 2 ATM interface, 8 Ethernet interface, 4 FDDI interface, 4 Token Ring interface and 16 SLIP interface.



PPP DS3 Link: This is the link that connects the different nodes. PPP DS3 has a link speed of 44.736 Mbps.



10BaseT Link: This is an Ethernet link that can be used to connect workstations and routers or switches. It has a link speed of 10Mbps.

From figure 5.5, the network is designed on a campus workspace that is 10km by 10km in size. From the object palette; the application definition is placed in the workspace renamed Applications, the profile definition is placed in the workspace and renamed Profiles, failure recovery is placed in the workspace and renamed Failure, then four 7200 Cisco routers are placed in the workspace renamed R1, R2, R3, and R4 with PPP_DS3 link connecting the routers, two Ethernet_wkstn are placed in the workspace renamed PC1 and PC2. PC1 is connected to R1 with 10BaseT link, PC2 connected to R4 with 10BaseT link.

The application definition is configured to support two applications from the predefined applications to serve as network traffic; voice with PCM Quality Speech and video conferencing with Low Resolution Video. In the profile definition, I configure two profiles; voice profile support voice application and the video profile support video conferencing application. In the voice profile, the voice application is set to start 60 seconds after the simulation is run and stop at the end of the simulation, the application is set to keep repeating in exponential of 600 seconds interval. The same setting is done for the video profile. The voice and video profiles are set to start simultaneously.

PC1 and PC2 are both configured support voice and video profiles (using the Application: Support Profiles) which will enable the PCs to generate traffic, and both PCs are also to be servers (using the Application: Support Services), meaning there is no need to put a separate server for video conferencing.

The recovery failure node is configured to break the link between R1 (connected to PC1) and R4 (connected to PC2) in 200 seconds (3mins 20secs) of the simulation time.

The following individual DES statistics were selected:

- Convergence Duration (sec).
- Traffic Dropped (packets/sec).

The same network topology was duplicated to produce another exact topology. First topology is named OSPF scenario and the other duplicate named EIGRP scenario.

Refer to Appendix A for graphical representation of settings and configurations of the network in OPNET.

5.3.3 OSPF Scenario

In this scenario, OSPF was enabled for the whole as shown in figure 5.6. The simulation is then set to run for 10 minutes.

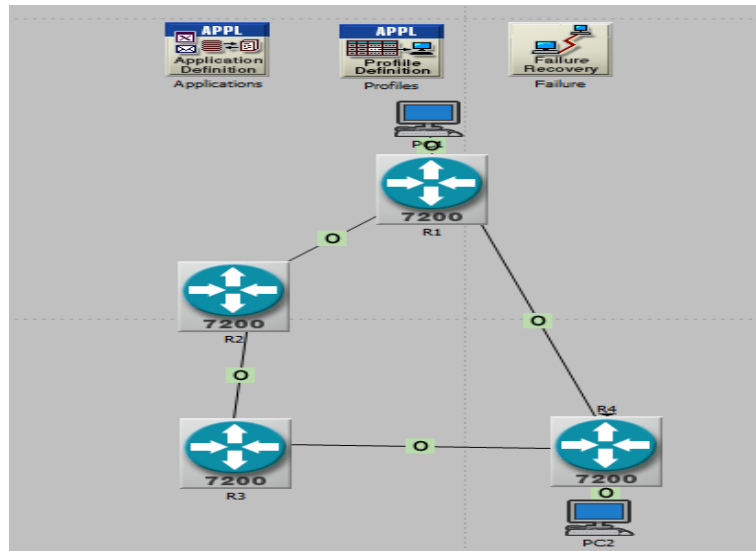


Figure 5.6: OSPF Scenario

5.3.4 EIGRP Scenario

In this scenario, EIGRP was enabled for the whole as shown in figure 5.7. The simulation is then set to run for 10 minutes.

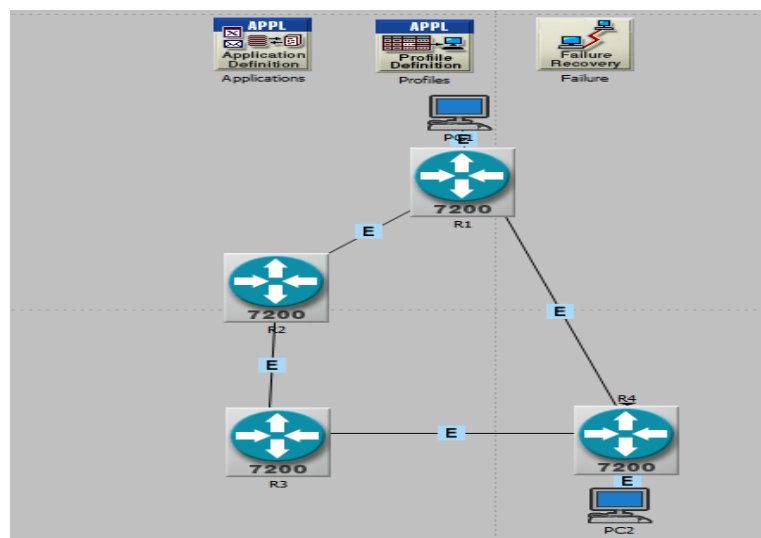


Figure 5.7: EIGRP Scenario

5.4 Lab Experiment Methodology

In this experiment, the convergence duration of OSPF and EIGRP was measured based on two different kinds of network, point – to – point and shared Ethernet connection. The difference between these two types of connection is that, in a point – to – point connection, when a link failure occurs, the neighbour routers will be notified immediately. While in shared Ethernet connection where the routers are connected via a switch, they rely on hello messages to know if their neighbour is alive or dead. So if a link fails, the neighbour routers will have to miss 3 hello messages from that neighbour in order to know that it is dead. This in turns adds a huge amount of delay in a shared Ethernet network connection, but the parameters are tuneable to achieve efficiency. Also in a shared Ethernet connection, there is DR and BDR election associated with OSPF. The election process is also analysed to see how it affects OSPF enabled network convergence process.

The lab experiment was carried out in Northumbria University Lab D003. The same network topology used in the OPNET simulation was implemented in the lab using real equipment. The equipments used for these experiments are:

- Four 2800 series Cisco Routers.
- 3500 Cisco Switch.
- Two Desktop Computers.
- Laptop PC.
- Serial Link Cables.
- 100BaseT Ethernet Cables.

5.4.1 Experiment 1

This experiment is a point – to – point connection type network. In this experiment, four Cisco routers named R1, R2, R3 and R4 are connected to each using serial links with each router having multiple connections as shown in figure 5.8. PC1 is connected to R1 with 100BaseT Ethernet cable and PC2 connected to R4 also with 100BaseT Ethernet cable.

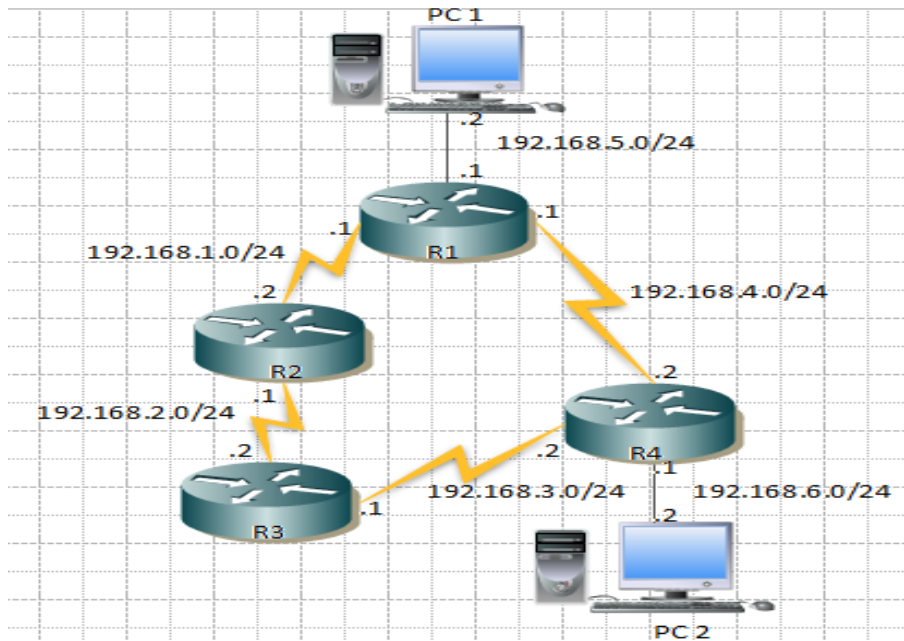


Figure 5.8: Lab Experiment 1 Network Diagram

In order to measure and compare the convergence duration of OSPF and EIGRP, two different scenarios were performed for this experiment; first scenario with OSPF configured on the network and the second scenario EIGRP was configured. The results obtained from this experiment demonstrate which protocol is best.

5.4.1.1 *OSPF Scenario*

After configuring OSPF routing protocol and the network is converged and stable, next I check the path PC1 choose to reach PC2 using the tracert command in the cmd interface. The path between PC1 and PC2 was R1 – R4. Then a continuous ping was send from PC1 to PC2. While the ping is going through the link between R1 and R4 was broken to measure how many pings were missed when PC1 is trying to find another path to reach PC2. #Debug IP OSPF adjacency command is also enabled on R1 command line interface to monitor the packets exchanged between the routers during network failure.

5.4.1.2 *EIGRP Scenario*

OSPF as previously configured was removed, EIGRP was configured and after waiting for a while for the network to converge and stabilise, I check the path PC1 choose to reach PC2 using the tracert command in the cmd interface. The path between PC1 and PC2 was R1 – R4. Then a continuous ping was send from PC1 to PC2. While the ping is going through the link between R1 and R4 was broken to measure how many pings were missed when PC1 is trying to find another path to reach PC2. #Debug IP EIGRP command is also enabled on R1

command line interface to monitor the packets exchanged between the routers during network failure.

5.4.2 Experiment 2

This experiment is a shared Ethernet connection type network. In this experiment, three Cisco routers named R1, R2 and R3 are connected to a Cisco switch using 100BaseT Ethernet cable, then R2 is connected to R3 which is also connected to R4 using a serial link. This type of network connection will test how hello messages add some delay in network convergence. Because if any link connected to switch fails, the router will not know immediately until it miss certain number of hello messages. PC1 is connected to R1 with 100BaseT Ethernet cable and PC2 connected to R4 also with 100BaseT Ethernet cable. A laptop is also connected to the switch to monitor the network traffic using wireshark.

Figure 5.9 shows the network topology used in the experiment and IP address of each device interface.

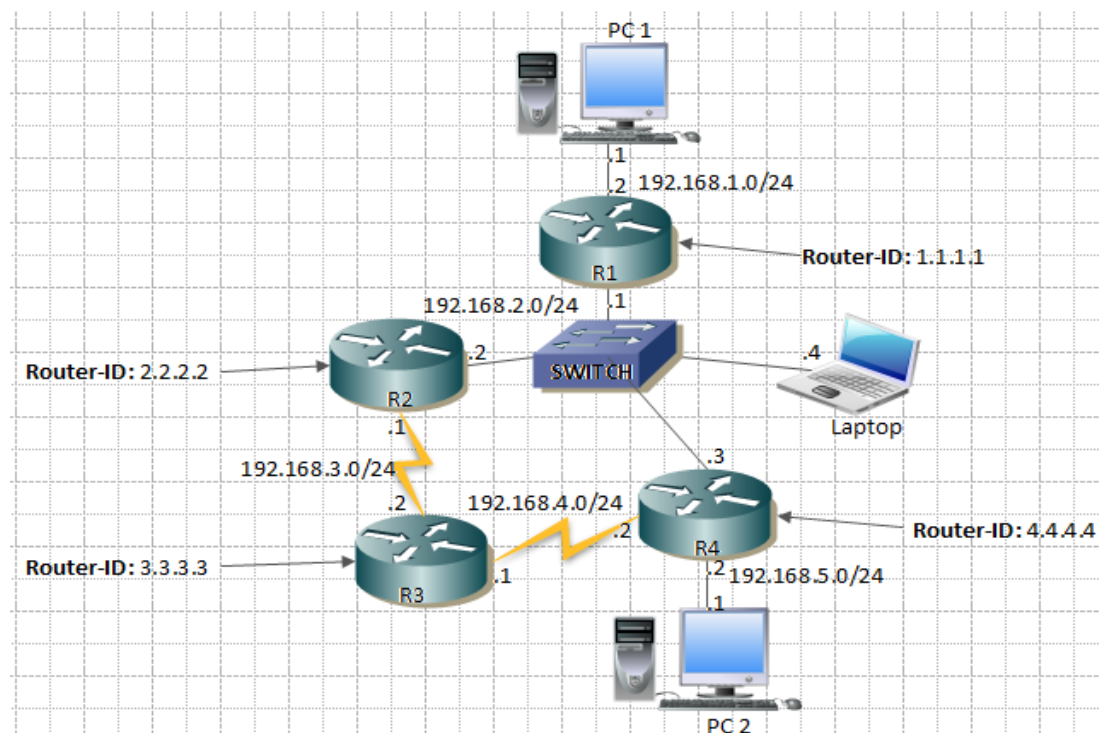


Figure 5.9: Lab Experiment 2 Network Diagram

Two different scenarios were performed for this experiment. In the first scenario, the network was configured with OSPF and the second scenario EIGRP was configured. In the OSPF scenario, the DR and BDR election process is also monitored to see how it affects the

routing protocol behaviour. The results obtained from this experiment demonstrate which protocol has best behaviour.

5.4.2.1 OSPF Scenario

After configuring OSPF routing protocol and the network is converged and stable, next I check the path PC1 choose to reach PC2 using the tracert command in the cmd interface. The path between PC1 and PC2 was R1 – R4. Then a continuous ping was send from PC1 to PC2, while wireshark was configured in the laptop to monitor the network traffic. While the ping is going through the link between R4 and the switch was broken to measure how many pings were missed when PC1 is trying to find another path to reach PC2. As discussed earlier, in a shared Ethernet segment network regarding OSPF, it elects a designated router (DR) and backup designated router (BDR) to reduce the amount of network updates across the network. The router with the highest priority (if priority is tied) or router-id is elected as the DR and second highest is the BDR. As shown in figure 5.9, the router-id for R1 is 1.1.1.1, R2 is 2.2.2.2, R3 is 3.3.3.3 and R4 is 4.4.4.4. In order to see how the DR and BDR election process affects the convergence duration of the OSPF network, since R4 has the highest router-id, it is elected as the DR while R2 which has the second highest router-id is the BDR. So when the link between R4 and the switch is broken, the routers (R2 and R1) will have to miss 3 hello messages from R4 to know it is down, then a new election take place for the DR and BDR. The second scenario is to make R2 the DR and R1 the BDR. To do this, the route priority of R4 is set to 0, meaning it will never participate in the DR/BDR election process, so R2 (highest router-id) will be the DR and R1 is BDR. When the link between R4 and the switch is broken, the routers (R2 and R1) will have to miss 3 hello messages from R4 to know it is down, but in this case there will be no new election of the DR and BDR. Election occurs only if there is DR/BDR in the network. In all of the experiments #Debug IP OSPF adjacency command is enabled on R1 command line interface to monitor the packets exchanged between the routers during network failure.

5.4.2.2 EIGRP Scenario

EIGRP was then configured and after the network was converged and stable, next I check the path PC1 choose to reach PC2 using the tracert command in the cmd interface. The path between PC1 and PC2 was R1 – R4. Then a continuous ping was send from PC1 to PC2, while wireshark was configured in the laptop to monitor the network traffic. While the ping is going through, the link between R4 and the switch was broken to measure how many pings were missed when PC1 is trying to find another path to reach PC2. #Debug IP EIGRP

command is also enabled on R1 command line interface to monitor the packets exchanged between the routers during network failure.

5.5 Conclusion

In this chapter, different experiments were carried out in different environment to achieve the aim of the research. The network equipment, configuration nodes and network topologies used in the OPNET simulation have been explained. The Lab experiments have also been explored. In the Lab experiments, ping command is used as the network traffic, debug was also enabled to monitor network packets and wireshark was configured to capture network traffic. All the gathered results and outputs are analysed in the next chapter.

6 Results and Analysis

6.1 Introduction

In this chapter, the results collected from the simulation and the Lab experiments are presented in graphs for the simulation, debug and ping command outputs for the Lab experiment. Results collected from the simulation and Lab experiments are analysed in this chapter.

6.2 Simulation

As already discussed earlier, in order to compare the performance of OSPF and EIGRP in an IP network, the following as parameters were selected:

- Convergence Duration (sec)
- Traffic Dropped (packets/sec)

Convergence Duration

Convergence duration is how long it takes every router in a network to synchronise their routing table or how long it takes every router to update their routing topology if a change occur in the network (Macfarlane, 2006). The convergence duration of OSPF and EIGRP can be measure by setting a link in the network to fail at certain time and then monitor how the protocols (OSPF or EIGRP) react to the change.

Figure 6.1 shows the network convergence duration of OSPF and EIGRP. It shows that when the simulation first started, it took OSPF almost 12.8 seconds to converge while EIGRP converged in 5 seconds. Then link between R1 and R4 (refer to figure 5.5) is set to fail at 200 seconds (3minutes 20 seconds) of the simulation time. It can be seen in figure 6.1 that after the link failed; OSPF converged in 5 seconds while EIGRP converged in under 0 seconds almost instantly. This proves that EIGRP keeps a backup path. So after the link failure, it immediately switches to the backup link. But in OSPF, the routers have to run the SPF algorithm every time a network failure occurs in order to find another path, in turn adding a little delay.

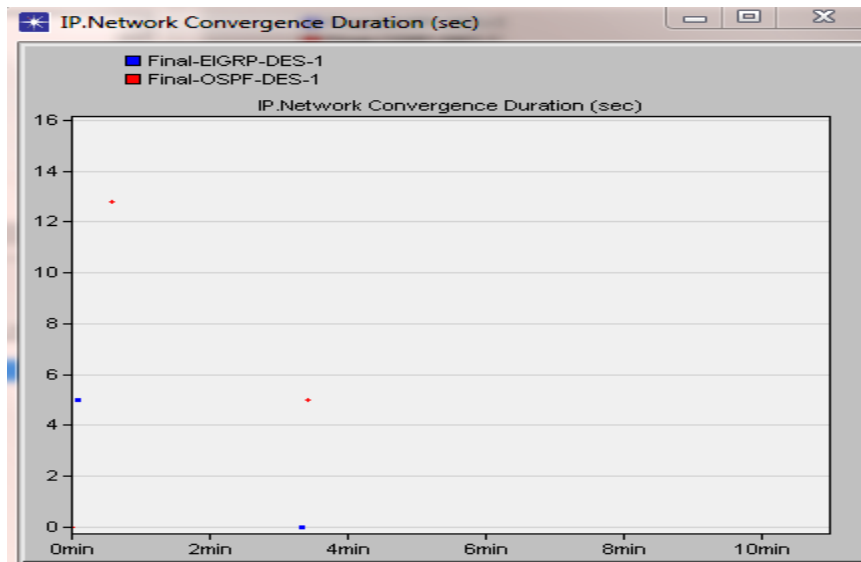


Figure 6.1: IP Network Convergence Duration (sec)

Traffic Dropped

This is the number of packets that are dropped by all the routers interfaces in the network, which might occur due to insufficient space in the routers memory in queuing or in a link failure before the router finds another path (OPNET, 2004).

Figure 6.2 shows the Number of IP traffic or Packets that are dropped per second. It can be seen that there were no packets dropped until after the link failure in the network. After the link failed at 3 minutes 20 seconds of the simulation time, it is shown in figure 6.2 that OSPF dropped up to 520packets/sec while EIGRP just dropped few packets.

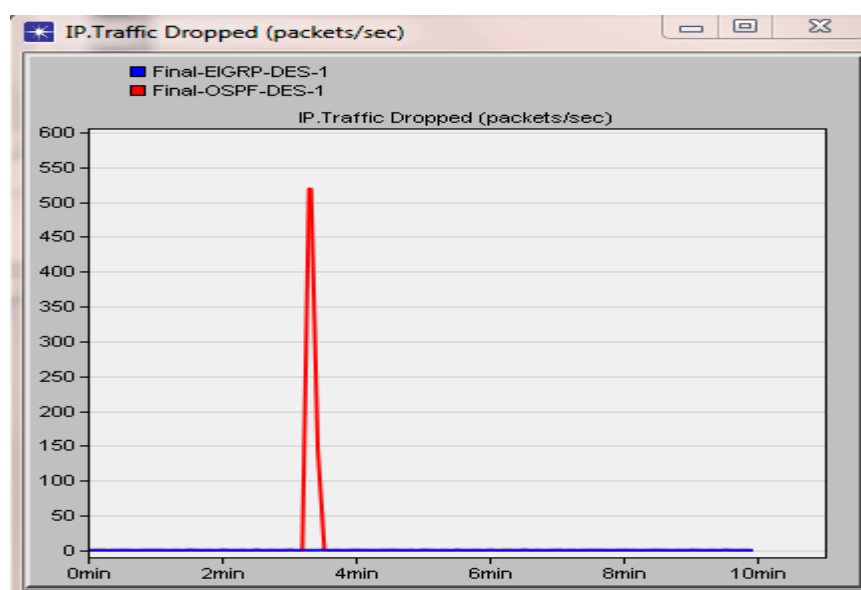


Figure 6.2: IP Traffic Dropped (packets/sec)

Scenario	Routing Protocol	Convergence Duration (Seconds)	Traffic Dropped (packets/seconds)
OSPF	OSPF	5	520
EIGRP	EIGRP	0.02	0.67

Table 6.1: Simulation Convergence Duration and Traffic Dropped (Point – to – Point Network)

6.3 Lab Experiment

The Lab experiment was carried out in Northumbria University Lab D003. The results and outputs from these experiments are collected and analysed.

6.3.1 Experiment 1

The type of network topology used for this experiment is a point – to –point connection, so when a link failure occur, neighbour routers would be notified immediately. This experiment is done for both OSPF and EIGRP to measure the performance of the routing protocols.

6.3.1.1 OSPF Scenario

Figure 6.3 shows that after the link between R1 and R4 went down, the neighbour router immediately know about the change and the link is declared dead/down. It can be seen in the figure 6.3 that R1 immediately send the update to R2, its neighbour.

```

1.Link is down      *Dec 23 17:59:54.494: %LINK-3-UPDOWN: Interface Serial0/2/1, changed state to down
                   *Dec 23 17:59:54.494: OSPF: Interface Serial0/2/1 going down
2.Update is send    *Dec 23 17:59:54.494: OSPF: 1.1.1.1 address 192.168.4.1 on Serial0/2/1 is dead, state DOWN
instantly to neighbour *Dec 23 17:59:54.494: OSPF: 4.4.4.4 address 192.168.4.2 on Serial0/2/1 is dead, state DOWN
routers              *Dec 23 17:59:54.494: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/2/1 from FULL to DOWN, Neighbor Down: Interface down or detached
                   *Dec 23 17:59:54.994: OSPF: Build router LSA for area 0, router ID 1.1.1.1, seq 0x8000000D
                   *Dec 23 17:59:54.994: OSPF: Rcv LS UPD from 2.2.2.2 on Serial0/2/0 length 88 LSA count 1
                   *Dec 23 17:59:55.494: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to down

```

Figure 6.3: Debug IP OSPF Output

After all routers in the network receive the update about topology change, all the routers then run the SPF algorithm to find another path to the failed network.

Figure 6.4 shows the continuous ping message from PC1 to PC2. It shows the number of ping messages that are lost before PC1 can reach PC2 again. It can be seen that after some few amount of pings are lost, the network was converged. From the amount of lost pings shown in figure 6.4, it can be deducted that the network converged in 5 seconds.

```

Administrator: Command Prompt
C:\Users\student>ping 192.168.6.2 -t

Pinging 192.168.6.2 with 32 bytes of data:
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Request timed out.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.6.2: bytes=32 time=2ms TTL=124
Reply from 192.168.6.2: bytes=32 time=2ms TTL=124
Reply from 192.168.6.2: bytes=32 time=2ms TTL=124

```

Figure 6.4: Ping Command (PC1>PC2)

6.3.1.2 EIGRP Scenario

Figure 6.5 shows that after the link between R1 and R4 went down, the neighbour router immediately know about the change and the link is declared dead/down. This means that the successor link has failed, so the feasible successor/backup path that is in the topology table is instantly installed into R1 routing table.

```

*Dec 23 20:04:31.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Dec 23 20:04:31.423: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.4.2 (FastEthernet0/1) is down: interface down
*Dec 23 20:04:31.423: IP-EIGRP(Default-IP-Routing-Table:1): route installed for 192.168.1.0 ()
*Dec 23 20:04:31.423: IP-EIGRP(Default-IP-Routing-Table:1): route installed for 192.168.2.0 ()
*Dec 23 20:04:31.423: IP-EIGRP(Default-IP-Routing-Table:1): route installed for 192.168.3.0 ()
*Dec 23 20:04:31.423: IP-EIGRP(Default-IP-Routing-Table:1): route installed for 192.168.6.0 ()
*Dec 23 20:04:31.439: IP-EIGRP(Default-IP-Routing-Table:1): 192.168.4.0/24 - not in IP routing table
*Dec 23 20:04:31.439: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.4.0/24 metric 4294967295 - 0 4294967295
*Dec 23 20:04:31.495: IP-EIGRP(Default-IP-Routing-Table:1): Processing incoming REPLY packet
*Dec 23 20:04:31.495: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.4.0/24 M 4294967295 - 0 4294967295 SM 4294967295 - 0 4294967295

```

Figure 6.5: Debug IP EIGRP Output

Figure 6.6 shows the continuous ping message from PC1 to PC2. It shows the number of ping messages that are lost before the network converged. It can be seen that only 1 ping was lost before PC1 can again reach PC2. From the amount of lost pings shown in figure 6.6, it can be deducted that the network converged in 1 second.

```

Administrator: Command Prompt
C:\Users\student>ping 192.168.6.2 -t

Pinging 192.168.6.2 with 32 bytes of data:
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Reply from 192.168.6.2: bytes=32 time=1ms TTL=126
Request timed out.
Reply from 192.168.6.2: bytes=32 time=2ms TTL=124
Reply from 192.168.6.2: bytes=32 time=2ms TTL=124
Reply from 192.168.6.2: bytes=32 time=2ms TTL=124

```

Figure 6.6: Ping Command (PC1>PC2)

Scenario	Routing Protocol	Convergence Duration (Seconds)
OSPF	OSPF	5
EIGRP	EIGRP	1

Table 6.2: Lab Experiment 1 Convergence Duration (Point – to – Point Network)

6.3.2 Experiment 2

In this type of network topology (shared Ethernet segment), both OSPF and EIGRP have to rely on Hello message to know whether their neighbour is alive. So when a link fails, the neighbour routers have to miss three hello messages to declare that link dead/down. This experiment shows the delay hello messages can add to the network convergence process. And also the delay the election process of DR/BDR will add to the network convergence when using OSPF.

6.3.2.1 OSPF Scenario

Because the network topology is a shared Ethernet type connection (refer to figure 5.9), there would be DR/BDR election in this type of network topology. But the DR/BDR election depends on where the failure occurs. The DR/BDR election occurs only when there is DR and BDR in the network. This scenario is divided into two:

1. DR/BDR Election

Figure 6.7 shows that after the link between R4 and the switch went down, it took a while before the link is declared dead/down, meaning the dead timer has expired. After which router R4 the DR with id 4.4.4.4 is declared dead/down. So immediately that occurred, the election process will start where R2 now has the highest router-id was elected as the DR. R2 will then send update to its neighbours informing them it is the new DR, then an election for

the BDR will occur and R1 was the BDR because it has second highest router-id. After this time the network was converged.

1.Link is down	*Dec 13 16:59:28.303: OSPF: Rcv LS UPD from 2.2.2.2 on FastEthernet0/1 length 88 LSA count 1
	*Dec 13 16:59:28.339: OSPF: Rcv LS UPD from 2.2.2.2 on FastEthernet0/1 length 64 LSA count 1
2.Link is declared down	*Dec 13 17:00:03.735: OSPF: 4.4.4.4 address 192.168.2.3 on FastEthernet0/1 is dead
	*Dec 13 17:00:03.735: OSPF: 4.4.4.4 address 192.168.2.3 on FastEthernet0/1 is dead, state DOWN
	*Dec 13 17:00:03.735: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on FastEthernet0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
3.Election:BDR is the DR	*Dec 13 17:00:03.735: OSPF: Neighbor change Event on interface FastEthernet0/1
	*Dec 13 17:00:03.735: OSPF: DR/BDR election on FastEthernet0/1
	*Dec 13 17:00:03.735: OSPF: Elect BDR 2.2.2.2
	*Dec 13 17:00:03.735: OSPF: Elect DR 2.2.2.2
	*Dec 13 17:00:03.735: DR: 2.2.2.2 (Id) BDR: 2.2.2.2 (Id)
4.DR sends update to neighbours	*Dec 13 17:00:03.735: OSPF: Remember old DR 4.4.4.4 (id)
	*Dec 13 17:00:04.235: OSPF: Build router LSA for area 0, router ID 1.1.1.1, seq 0x80000003
	*Dec 13 17:00:04.235: OSPF: Rcv LS UPD from 2.2.2.2 on FastEthernet0/1 length 88 LSA count 1
	*Dec 13 17:00:04.279: OSPF: Rcv LS UPD from 2.2.2.2 on FastEthernet0/1 length 108 LSA count 2
5.Election of new BDR	*Dec 13 17:00:04.911: OSPF: Neighbor change Event on interface FastEthernet0/1
	*Dec 13 17:00:04.911: OSPF: DR/BDR election on FastEthernet0/1
	*Dec 13 17:00:04.911: OSPF: Elect BDR 1.1.1.1
	*Dec 13 17:00:04.911: OSPF: Elect DR 2.2.2.2
	*Dec 13 17:00:04.911: OSPF: Elect BDR 1.1.1.1
	*Dec 13 17:00:04.911: OSPF: Elect DR 2.2.2.2
	*Dec 13 17:00:04.911: DR: 2.2.2.2 (Id) BDR: 1.1.1.1 (Id)
6.Update send about DR/BDR	*Dec 13 17:00:04.911: OSPF: Neighbor change Event on interface FastEthernet0/1
	*Dec 13 17:00:04.911: OSPF: DR/BDR election on FastEthernet0/1
7.Convergence achieved	*Dec 13 17:00:04.911: OSPF: Elect BDR 1.1.1.1
	*Dec 13 17:00:04.911: OSPF: Elect DR 2.2.2.2
	*Dec 13 17:00:04.911: DR: 2.2.2.2 (Id) BDR: 1.1.1.1 (Id)

Figure 6.7: Debug IP OSPF Command Output Showing DR/BDR Election

Figure 6.8 shows the continuous ping message from PC1 to PC2. It shows the number of ping messages that are lost during waiting for the hello messages, the election process, the update process and eventually convergence in the network. It can be seen that a lot of pings are lost before PC1 can again reach PC2. From the amount of lost pings shown in figure 6.8, it can be deduced that the network converged in 37 seconds.

```

C:\Users\student>ping 192.168.5.2 -t

Pinging 192.168.5.2 with 32 bytes of data:
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Request timed out.
Request timed out.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124

```

Number of pings lost during convergence process

Figure 6.8: Ping Command (PC1>PC2)

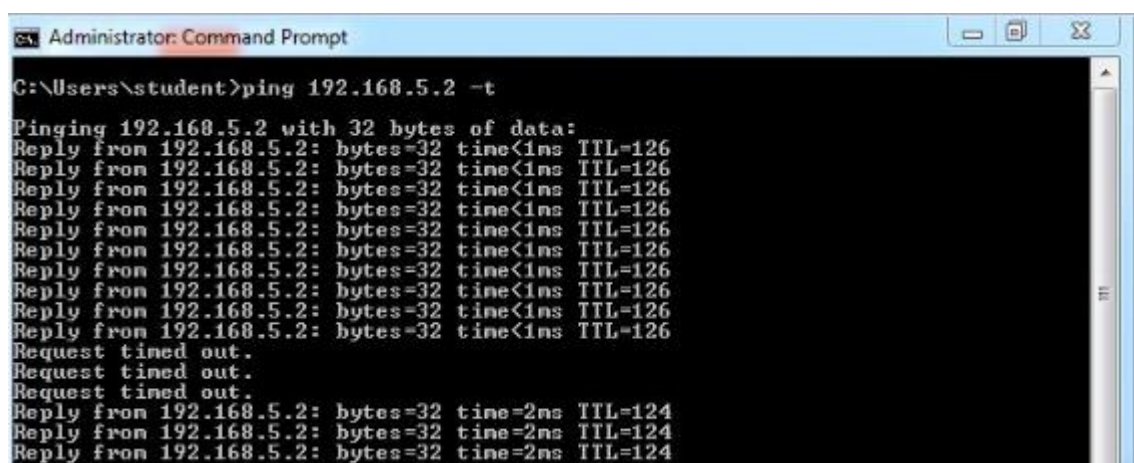
2. No DR/BDR Election

Figure 6.9 shows that after the link between R4 and the switch went down, it took approximately 29 seconds before the link is declared dead/down, meaning the dead timer has expired. After which router R4 with id 4.4.4.4 is declare dead/down. R2 and R1 will check who the DR/BDR is, but since R2 is already the DR and R1 is the BDR, there was no election. After this time the network was converged.

```
1.Link is down      *Dec 13 18:02:08.219: OSPF: Rcv LS UPD from 2.2.2.2 on FastEthernet0/1 length 88 LSA count 1
2.Link is declared  *Dec 13 18:02:36.715: OSPF: 4.4.4.4 address 192.168.2.3 on FastEthernet0/1 is dead
down               *Dec 13 18:02:36.715: OSPF: 4.4.4.4 address 192.168.2.3 on FastEthernet0/1 is dead, state DOWN
                  *Dec 13 18:02:36.715: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on FastEthernet0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
3.Election there is *Dec 13 18:02:36.715: OSPF: Neighbor change Event on interface FastEthernet0/1
no election because *Dec 13 18:02:36.715: OSPF: DR/BDR election on FastEthernet0/1
                  *Dec 13 18:02:36.715: OSPF: Elect BDR 1.1.1.1
R2 already DR &    *Dec 13 18:02:36.715: OSPF: Elect DR 2.2.2.2
                  *Dec 13 18:02:36.715: DR: 2.2.2.2 (Id) BDR: 1.1.1.1 (Id)
R1 already BDR     *Dec 13 18:02:37.211: OSPF: Rcv LS UPD from 2.2.2.2 on FastEthernet0/1 length 60 LSA count 1
```

Figure 6.9: Debug IP OSPF Command Output (No DR/BDR Election)

Figure 6.10 shows the continuous ping message from PC1 to PC2. It shows the number of ping messages that are lost during waiting for the hello messages, the update process and eventually convergence in the network. It can be seen that some amount of pings are lost before PC1 can again reach PC2. From the amount of lost pings shown in figure 6.10, it can be deducted that the network converged in 6 seconds.



```
Administrator: Command Prompt
C:\Users\student>ping 192.168.5.2 -t
Pinging 192.168.5.2 with 32 bytes of data:
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
```

Figure 6.10: Ping Command (PC1>PC2)

6.3.2.2 EIGRP Scenario

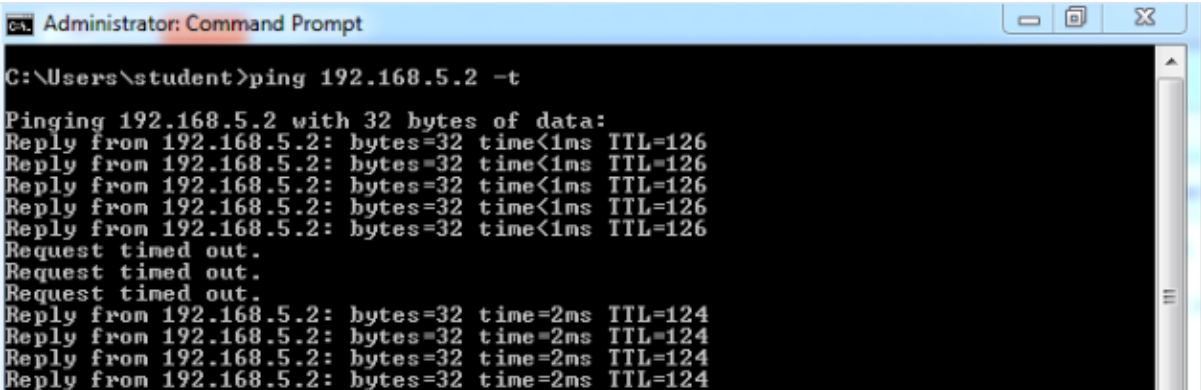
After the link between R4 and the switch went down, the routers wait for a while before the link is declared dead/down, meaning the holding time has expired. After which the router R4 is declared down. It can be seen in figure 6.11 that immediately the link was declared dead, updates are sent to neighbour routers and they all acknowledge the update message by sending a reply because EIGRP uses RTP for sending messages.

```
1. Hold time has expired, neighbour is declared down
*Dec 13 18:28:09.719: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.2.3 (FastEthernet0/1) is down: holding time expired
*Dec 13 18:28:09.731: IP-EIGRP(Default-IP-Routing-Table:1): Processing incoming QUERY packet
*Dec 13 18:28:09.731: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.5.0/24 M 4294967295 - 25600 4294967295 SM 4294967295 - 25600 4294967295
*Dec 13 18:28:09.735: IP-EIGRP(Default-IP-Routing-Table:1): Processing incoming UPDATE packet
*Dec 13 18:28:09.735: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.4.0/24 M 2684416 - 1657856 1026560 SM 2681856 - 1657856 1024000
*Dec 13 18:28:09.743: IP-EIGRP(Default-IP-Routing-Table:1): 192.168.4.0/24 - do advertise out FastEthernet0/1
*Dec 13 18:28:09.743: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.4.0/24 metric 4294967295 - 1657856 4294967295
*Dec 13 18:28:09.743: IP-EIGRP(Default-IP-Routing-Table:1): 192.168.5.0/24 - do advertise out FastEthernet0/1
*Dec 13 18:28:09.743: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.5.0/24 metric 4294967295 - 25600 4294967295
*Dec 13 18:28:09.751: IP-EIGRP(Default-IP-Routing-Table:1): 192.168.5.0/24 - do advertise out FastEthernet0/1
*Dec 13 18:28:09.751: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.5.0/24 metric 4294967295 - 25600 4294967295
*Dec 13 18:28:09.759: IP-EIGRP(Default-IP-Routing-Table:1): Processing incoming REPLY packet
*Dec 13 18:28:09.759: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.4.0/24 M 2684416 - 1657856 1026560 SM 2681856 - 1657856 1024000
*Dec 13 18:28:09.763: IP-EIGRP(Default-IP-Routing-Table:1): route installed for 192.168.4.0 ()
*Dec 13 18:28:09.763: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.5.0/24 M 2686976 - 1657856 1029120 SM 2684416 - 1657856 1026560
*Dec 13 18:28:09.763: IP-EIGRP(Default-IP-Routing-Table:1): route installed for 192.168.5.0 ()
*Dec 13 18:28:09.763: IP-EIGRP(Default-IP-Routing-Table:1): Processing incoming UPDATE packet
*Dec 13 18:28:09.767: IP-EIGRP(Default-IP-Routing-Table:1): Int 192.168.5.0/24 M 2686976 - 1657856 1029120 SM 2684416 - 1657856 1026560

2. Update send to neighbours about change in network and convergence is instantly achieved
```

Figure 6.11: Debug IP EIGRP Command Output

Figure 6.12 shows the continuous ping message from PC1 to PC2. It shows the number of ping messages that are lost during waiting for the hello messages, the update process and eventually convergence in the network. It can be seen that some amount of pings are lost before PC1 can again reach PC2. From the amount of lost pings shown in figure 6.12, it can be deducted that the network converged in 6 seconds.



```
Administrator: Command Prompt
C:\Users\student>ping 192.168.5.2 -t

Pinging 192.168.5.2 with 32 bytes of data:
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Reply from 192.168.5.2: bytes=32 time<1ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
```

Figure 6.12: Ping Command (PC1>PC2)

Scenario	Routing Protocol	Convergence Duration (Seconds)
OSPF (with DR/BDR Election)	OSPF	37
OSPF (No DR/BDR Election)	OSPF	6
EIGRP	EIGRP	6

Table 6.3: Lab Experiment 2 Convergence Duration (Shared Ethernet Segment network)

Refer to appendix A for all the wireshark capture images.

6.4 Conclusion

The results collected from both simulation environment and Lab environment are analysed. The analysis is carried out by calculating the number of pings lost between PC1 and PC2 in the Lab experiment together with debug output to see the packets generated. In OPNET, it produces a graph result of the selected parameters. The convergence duration of the different routing protocols i.e. OSPF and EIGRP are measured based on these findings. The analysis shows that the simulation results almost concurred with the results from the Lab experiment 'experiment 1'. Both environments shows OSPF converged in 5 seconds, while EIGRP converged in the simulation under 0 seconds and 1 second in the Lab experiment.

The Lab experiment 'experiment 2' shows that OSPF converged in 37 seconds with DR/BDR election process taking place, while OSPF converged in 6 seconds when there was no DR/BDR election. EIGRP also converged in 6 seconds in this experiment.

7 Conclusion

7.1 Introduction

In this chapter, the research aim and objectives achieved are stated, and the summary of all the findings gathered from the simulation and Lab experiment are compared together with previous research and thesis documented in the literature review. Then it outlines some difficulties encountered during the research and some theories for further research.

7.2 Research Summary

The aim of this research is to analyse and compare the performance of OSPF and EIGRP routing protocols when it comes to selecting between one of them. In order to achieve this, the experiment is conducted in two environments; simulation environment using OPNET Modeler simulator and Lab environment using real equipment. As most previous research regarding the topic subject has been done using simulation, this particular approach will help compare findings in simulation and Lab experiment. The following objectives were achieved during the course of the research:

1. To research on routing protocols in general.
2. To conduct a literature review on routing protocols, OSPF and EIGRP from journals, books, previous researches and previous thesis.
3. To learn OPNET Modeler use for simulation.
4. To decide on type of network connection, shared Ethernet or point – to – point network connection.
5. To design two scenarios in OPNET; first scenario name OSPF configure with OSPF routing protocol and second scenario name EIGRP configure with EIGRP routing protocol (point – to – point connection).
6. To analyse results gathered from the simulation.
7. To design the same network in the Lab with real equipment.
8. To analyse results gathered from the Lab experiment.
9. To analyse and Compare results gathered from simulation and Lab.
10. To design a shared Ethernet network connection in the Lab.
11. To analyse the effect hello messages have on OSPF and EIGRP convergence process and the effect DR/BDR election has on OSPF convergence duration.

From the literature review, it was found out that EIGRP performs better than OSPF in terms of convergence time, CPU utilization, throughput, less memory consumption, end to end packet delay, jitter and packet loss. But it is also found out that a combination of both protocols in the same network can improve the network performance.

In the OPNET simulation, point – to – point connection was implemented for two separate scenarios; OSPF scenario and EIGRP scenario. In OSPF scenario, OSPF routing protocol was configured with convergence duration and number of packets dropped selected in the discrete event simulator (DES) as parameters. The same procedure was repeated for the EIGRP scenario, only this time EIGRP was configured on the network. A link in the network in both scenarios is set to fail, in order to test the convergence duration of the routing protocols. The simulation was set to run for 10 minutes and results are obtained. Results obtained from the simulation shows that after the link fails, OSPF converges in 5 seconds while EIGRP converges almost instantly under 0 second. OSPF approximately dropped 520packets/sec during convergence process while in EIGRP there are only few packets dropped.

In the Lab experiment, two experiments were conducted. The first experiment ‘experiment 1’ was designed based a point – to – point network connection. This experiment is exactly as the simulation, so findings from the simulation are compared to findings from this experiment. The experiment has two scenarios OSPF and EIGRP experiments with OSPF and EIGRP routing protocol configured respectively. The second experiment ‘experiment 2’ was designed based on a shared Ethernet segment network. The purpose of this experiment is to monitor the effect of hello messages on convergence duration with both protocols and DR/BDR election associated with OSPF. But the DR/BDR election depends on where the failure occurs. When the failure occurs at the DR, there will be new DR/BDR election, other than that there will be no election.

A link was broken in all the Lab experiments, and debug output was recorded for each of the experiment to monitor packets exchange during the convergence process. The convergence duration was measured with the amount of ping lost during the link failure. Results collected from ‘experiment 1’ of the Lab experiment shows that after a link failure in the network, it took OSPF 5 seconds to converged while EIGRP took 1 second. Results collected from ‘experiment 2’ shows that when using OSPF; if the link to the DR fails, it

took OSPF 37 seconds to converge, while when it was not the DR that failed, it converged in 6 seconds. EIGRP also converged in 6 seconds in this experiment.

In conclusion, the results collected from the simulation concur with the results from Lab experiment 'experiment 1'. Therefore it is concluded that in a point – to – point network connection, OSPF convergence duration is 5 seconds and EIGRP convergence duration is approximately 1 second.

In summary, it can be concluded that the findings in this research agree with the findings from review of previous research and thesis explain in the literature that EIGRP performs better than OSPF routing protocol. Although in their thesis, Islam & Ashique (2010) said that the combination of OSPF & EIGRP in a network can improve the performance of the network in terms of convergence duration, end to end packet delay and packet loss.

7.3 Conclusion

From the results, it seen that EIGRP converges faster than OSPF because EIGRP uses DUAL algorithm which keeps a backup path to any destination network known as the successor (primary path) and the feasible successor (backup path). While OSPF uses SPF/Dijkstra algorithm which proves that every time a link fails, OSPF will have to run SPF algorithm to find another path.

7.4 Research Limitation

The major limitation here is time constraint, as the researcher was not able to fully learn about OPNET Modeler. The researcher attempted to duplicate experiment 2 (shared Ethernet segment network connection) done in the Lab environment using simulator but does not work. Such result to the in ability to duplicate the second experiment 'experiment 2' done in the Lab in simulation environment. Also the researcher could have selected more parameters to compare the performance of these routing protocols for example packet end to end delay, CPU utilisation, jitter, packet delay variation etc. All these parameters can be used to fully the performance of the routing protocols, but all these were not done because OPNET graphs are confusing to analyse. It will require more in depth knowledge about OPNET to understand how the graphs are presented.

7.5 Further Work

The performance of the routing protocols can be further compared by selecting more parameters like CPU utilisation, packet end to end delay etc. in the OPNET simulator. And

experiment 2 which was conducted in the Lab only, would also be repeated in the simulation environment to compare the findings.

From reviews of various books and papers, it is explained how dividing OSPF network into separate areas can reduce the routers CPU utilisation and network traffic. This scenario would be configured to compare the CPU utilisation of OSPF a network that is divided into areas and another that is not.

Another important research that would be done is the EIGRP query packet process. It is discussed earlier in this document that EIGRP uses DUAL algorithm which has two paths to every network destination known as; successor (the primary path) and feasible successor (backup path). So if the successor fails, and there is no feasible successor, EIGRP will use a query packet to find another path to the failed network. But in a very large network, the query packet process can sometimes add huge delay in the network convergence duration. For example a network with say 12 routers, if there is a link failure and there is no backup path to the failed network, the router with the change will send a query packet to its neighbour and wait for response. If the neighbours do not have another path, they too will send a query packet to their neighbours and wait for reply. So the waiting for reply message to a query can add delay in the network. A scenario like this would be configured either in simulation or Lab environment to see the effect query packet process have on the convergence duration of EIGRP.

As the networking world is now migrating to IPv6, a new OPSF v3 was designed to support IPv6. A research on this OSPF version would be interesting to compare the performance with latter version of OSPF.

8 Critical Evaluation

8.1 Introduction

This chapter evaluates the research as a whole and also explains how the aim and objectives of the research are achieved.

8.2 Discussion

The literature review has been very effective in such a way that it was used to have an insight of what to expect from the experiments conducted in this research. It was also used to compare findings of the experiments conducted in this research.

The experiments in this research were originally to be conducted using OPNET simulator only. But after several meetings with the supervisor of this research, we try analysing the findings from the simulation, but the findings were a bit questionable. So it was decided that the simulation scenario should be duplicated using Lab equipment. The results collected from the simulation are close to results from the Lab.

The graphs presented in OPNET were sometimes complex and confusing to analyse, so the experiments conducted in this research was limited to analysing the performance of OSPF and EIGRP based on convergence duration. Even though, it is explained in the literature section how various authors used different approach and parameters to compare the performance of OSPF and EIGRP, which would further help understand the routing protocol with the best behaviour. Nonetheless, comparing the performance of these routing protocols with more parameters is considered under future work in chapter 7.

Also OSPF technique of dividing network into separate areas would have been implemented to observe how it helps reduce OSPF routers CPU utilisation. EIGRP query packet would have been look into to see how it can affect EIGRP convergence duration. All these are explained under the future work section in chapter 7.

The results from the experiments both simulation and Lab concurred that EIGRP performs better than OSPF based on convergence duration because EIGRP has dual paths to every destination network. It also shows how hello messages add delay to the convergence process of OSPF and EIGRP and the DR/BDR election process associated with OSPF in a shared Ethernet segment.

8.3 Conclusion

In conclusion, the aim and objectives of this research have been achieved, and the results collected from the experiments are conclusive.

References

- Albrightson, B., Garcia-Luna-Aceves, J.J. & Boyle, J. (1994) "EIGRP – A Fast Routing Protocol Based on Distance Vectors", pp.1-13., University of California Santa Cruz [Online] Available at <http://ccrg.soe.ucsc.edu/publications/interop94.pdf> (Accessed 10 October 2011)
- Andrew. (2011) Difference between EIGRP and OSPF. EIGRP vs. OSPF. [Online] Available at <http://www.differencebetween.com/difference-between-eigrp-and-vs-ospf/> (Accessed 07 December 2011)
- Ashraf, M.T. (2010) "How to Select a Best Routing Protocol for your Network", Canadian Journal on Network and Information Security, 1(6), pp.56-59., AM Publisher [Online] Available at <http://www.ampublisher.com/August%202010/NIS-1008-011-How-to-Select-Best-Routing-Protocol.pdf> (Accessed 10 October 2011)
- Ayub, N., Jan, F., Mustafa, T., Rana, W.J., Saeed, M.Y. & Ullah, S. (2011) "Performance Analysis of OSPF and EIGRP Routing Protocols with Respect to the Convergence", European Journal of Scientific Research, 61(3), pp.434-447., European Journal [Online] Available at http://www.eurojournals.com/EJSR_61_3_12.pdf (Accessed 10 October 2011)
- Balchunas, A. (2007) Routing Protocol Comparison. [Online] Available at: <http://www.routeralley.com> (Accessed 14 October 2011)
- Ballew, S.M. (1997) Managing IP Networks with Cisco Routers. Sebastopol: O'Reilly Media
- Basu, A. & Riecke, J. (2001) "Stability Issues in OSPF Routing", Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, 31(4), pp.225-236., ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=383077> (Accessed 20 October 2011)

- Caue. (2008) OPSF – LSA Types. [Online] Available at:
http://cauew.blogspot.com/2008/03/ospf-lsa-types_18.html (Accessed 28 December 2011)
- Cisco Systems (2011) Cisco IOS Release 12.0 Network Protocols Configuration Guide, Part 1. Cisco [Online] Available at
http://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/np1_c.html
 (Accessed 12 December 2011)
- Cisco Systems (2005) IP Routing: Introduction to EIGRP. Cisco [Online] Available at
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f07.shtml#packet_formats (Accessed 10 December 2011)
- Cisco Systems (2005) IP Routing: OSPF Neighbour States. Cisco [Online] Available at
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml (Accessed 24 December 2011).
- Cisco Systems. (2003) “Lab 6.9.2a Examining the DR/BDR Election process”, Cisco Networking Academy Programme, pp1-5., Cisco [Online] Available at
http://hyse.org/pdf/ccnp/Cisco%20Networking%20Academy%20CCNP%20Semester%201%20v3.0/PDF/lab_6_9_2a.pdf (Accessed 3 January 2012).
- Clark, M.P. (2003) Data Networks, IP and the Internet. West Sussex: John Wiley & Sons Ltd.
- Davis, D. (2002) Select the right routing protocol for your network. [Online] Available at:
<http://www.techrepublic.com/article/select-the-right-routing-protocol-for-your-network/1040261> (Accessed 09 November 2011)
- Doyle, J. & Carroll, J. (2006) CCIE Professional Development Routing TCP/IP Volume 1. 2nd ed. Indianapolis: Cisco Press.
- Exposito, J., Trujillo, V. & Gamess, E. (2010) “Using Visual Educational Tools for the Teaching and Learning of EIGRP”, Proceedings of the World Congress on Engineering and Computer Science (WCECS), 1, pp.1-6., International Association of Engineers [Online] Available at
http://www.iaeng.org/publication/WCECS2010/WCECS2010_pp169-174.pdf
 (Accessed 29 October 2011)

- Garcia-Luna-Aceves, J.J. (1993) “Loop – free routing using diffusing computations”, IEEE ACM Transactions on Networking, 1(1), pp.130-141., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=222913&isnumber=5814> (Accessed 25 October 2011)
- Garcia-Luna-Aceves, J.J. (1989) “A Unified Approach to Loop – Free Routing Using Distance Vector or Link States”, SIGCOMM 1989 Symposium proceedings on Communications architectures and protocols, 19(4), pp.212-232., ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=75268> (Accessed 10 October 2011)
- Haas, H. (2005) “OSPF - Areas”, Why is OSPF Complicated Part 2, pp3-8., [Online] Available at <http://www.perihel.at/2/basics/25-Routing-OSPF-4-Areas.pdf> (Accessed 3 January 2012)
- Hummel, S. (2011) Selecting a Routing Protocol - IGRP, EIGRP, OSPF, ISIS, BGP. [Online] Available at: <http://knol.google.com/k/shaun-hummel/selecting-a-routing-protocol-igrp-eigrp/25uy11qkhuh3c/3#done> (Accessed 06 December 2011)
- Islam, M.N. & Ashique, A.U. (2010) Simulation Based EIGRP over OSPF Performance Analysis. MSc. Blekinge Institute of Technology. [Online] Available at: [http://denver.bth.se/com/mscee.nsf/attachments/4983_Thesis_Report_pdf/\\$file/4983_Thesis_Report.pdf](http://denver.bth.se/com/mscee.nsf/attachments/4983_Thesis_Report_pdf/$file/4983_Thesis_Report.pdf) (Accessed 17 October 2011)
- Jaafar, T.M., Riley, G.F., Reddy, D. & Blair, D. (2006) “Simulation-Based Routing Protocol Performance Analysis – A Case Study”, Proceedings of the 2006 Winter Simulation Conference, pp.2154-2161., IEEE Xplore [Online] Available at <http://http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4117864&isnumber=4117570> (Accessed 17 October 2011)
- Kaur, I. & Sharma, M. (2011) “Performance Evaluation of Hybrid Network Using EIGRP & OSPF for Different Applications”, 3(5), pp.3950-3960., Ijest [Online] Available at <http://www.ijest.info/docs/IJEST11-03-05-225.pdf> (Accessed 18 October 2011)

- Khalil, Y.H. & Elmaghraby, A.S. (2011) "Computer Networks Resilience Challenges: Routing Protocols", 2010 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), pp.28-33., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5711719> (Accessed 25 October 2011)
- Kim, D. & Tcha, D. (2000) "Scalable domain partitioning in Internet OSPF routing", Telecommunication System, 15(1-2), pp.113-127., SpringerLink [Online] Available at <http://www.springerlink.com/content/l3870u3265k28312/> (Accessed 24 October 2011)
- Kleinrock, L. & Kamoun, F. (1977) "Hierarchical Routing for Large Networks; Performance Evaluation and Optimization", Computer Networks, 1(3), pp.155-174., Science Direct [Online] Available at <http://www.sciencedirect.com/science/article/pii/0376507577900022> (Accessed 14 October 2011)
- Lammle, T. (2011) CCNA, Cisco Certified Network Associate: Study Guide. 7th ed. Indianapolis: Wiley Publishing.
- Macfarlane, J. (2006) Network Routing Basics: Understanding IP Routing in Cisco Systems. USA: John Wiley & Sons Inc.
- McGregor, M. (2001) Cisco Networking Academy Program: Semester 6 Lab Companion, Remote Access - Networking academy. Indianapolis: Cisco Press.
- Microsoft Technet. (2012) Windows Server 2000: OSPF Areas. [Online] Available at <http://technet.microsoft.com/en-us/library/cc957882.aspx> (Accessed 5 January 2012)
- Morrissey, P. (1999) Choosing an Interior Gateway Protocol. [Online] Available at: <http://www.networkcomputing.com/1021/1021ws2.html> (Accessed 07 December 2011)
- Moy, J. (1998) the open shortest path first (OSPF) specification. Technical Report RFC-1131, SRI Network Information Center, October 1989. [Online] Available at: <http://www.ietf.org/rfc/rfc2328.txt> (Accessed 18 October 2011)

- Odom, W. & Knott, T. (2006) Networking Basics CCNA 1 Companion Guide.
Indianapolis: Cisco Press
- OPNET (2004) Introduction to Modeler: OPNET Training. OPNET [Online] Available at <http://www.opnet.com> (Accessed 15 November 2011)
- Pepelnjak, I. (1999) EIGRP Network Design Solutions. Indianapolis: Cisco Press
- Pethe, R.M. & Burnase, S.R. (2011) “TECHNICAL ERA LANGUAGE OF THE NETWORKING - EIGRP”, NCICT Special Issue Conference, pp.1-5., IJEST [Online] Available at <http://www.ijest.info/docs/IJEST-NCICT-002-54.pdf> (Accessed 18 October 2011)
- Popoviciu, C. (2006) Special Report. Understanding IP Routers. [Online] Available at: <http://broadcastengineering.com> (Accessed 10 October 2011)
- Prokkola, J. (2006) OPNET – Network Simulator. Simulations and Tools for Telecommunications. [Online] Available at http://www.telecomlab.oulu.fi/kurssit/521365A_tietoliikennetekniikan_simuloinnit_ja_tyokalut/Opnet_esittely_07.pdf (Accessed 3 January 2012)
- Randhawa, R. & Sohal, J.S. (2009) “Comparison and performance of routing protocols in SONET based networks”, Optik – International Journal for light and Electron Optics, 121(11), pp.997-1002., Science Direct [Online] Available at <http://www.sciencedirect.com/science/article/pii/S0030402608003732> (Accessed 3 November 2011)
- Riesco, A. & Verdejo, A. (2009) “Implementing and Analyzing in Maude the Enhanced Interior Gateway Routing Protocol”, Electronic Notes in Theoretical Computer Science, 238(3), pp.249-266., Science Direct [Online] Available at <http://www.sciencedirect.com/science/article/pii/S1571066109001455> (Accessed 17 October 2011)
- Rob. (2011) LSA Types. Common Types of LSA used by Cisco. [Online] Available at: <http://www.infracore.com/tag/lsa-types/> (Accessed 10 November 2011)

- Sarkar, N.I. & Halim, S.A. (2011) “A Review of Simulation of Telecommunication Networks”, Journals of Selected Areas in Telecommunication (JSAT), pp10-16, Cyber Journals [Online] Available at <http://www.cyberjournals.com/Papers/Mar2011/02.pdf> (Accessed 24 November 2011)
- Schmid, A. & Steigner, C. (2002) “Avoiding Counting to Infinity in Distance Vector Routing”, Telecommunication Systems, 19(3-4), pp.497-514., University of Koblenz [Online] Available at <http://userpages.uni-koblenz.de/~steigner/papers/ripmti.pdf> (Accessed 29 October 2011)
- Sendra, S., Fernandez, P.A., Quilez, M.A., Lloret, J. (2010) “Study and Performance of Interior Gateway IP Routing Protocols”, Network Protocols and Algorithms, 2(4), pp.88-117., Macrothink Institute [Online] Available at <http://macrothink.org/journal/index.php/npa/article/view/547> (Accessed 6 October 2011)
- Shamim, F., Aziz, Z., Liu, J. & Martey, A. (2002) Troubleshooting IP Routing Protocols. Indianapolis: Cisco Press
- Sivabalan, M. & Mouftah, H.T. (2001) “On Design of Link – State Routing Protocol for Connection – Oriented Networks”, Journal of Network and Systems Management, 9(2), pp.223-242., ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=596662> (Accessed 15 October 2011)
- Teare, D. (2010) Implementing IP Cisco Routing (Route) Foundation Learning Guide. Indianapolis: Cisco Press.
- Thorenoor, S.G. (2010) “Communication Service Provider’s Choice between OSPF and IS-IS Dynamic Routing Protocols and Implementation criteria Using OPNET Simulator”, 2010 Second International Conference on Computer and Network Technology (ICCNT), pp.38-42., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5474539&isnumber=5474422> (Accessed 21 October 2011)

- Thorenoor, S.G. (2010) “Dynamic Routing Protocol Implementation Decision between EIGRP, OSPF and RIP Based on Technical Background Using OPNET Modeler”, 2010 Second International Conference on Computer and Network Technology (ICCNT), pp.191-195., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5474509&isnumber=5474422> (Accessed 21 October 2011)
- Velte, T.J. & Velte, A.T. (2007) Cisco, A Beginner’s Guide. 4th ed. New York: McGraw-Hill
- Webopedia (2011) Static Routing. [Online] Available at: http://www.webopedia.com/TERM/S/static_routing.html (Accessed 18 October 2011)
- Weingartner, E., vom Lehn, H. & Wehrle, K. (2009) “A Performance Comparison of Recent Network Simulators” ,2009 IEEE International Conference on Communications, pp.1-5., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5198657> (Accessed 12 December 2011)
- Wikipedia (2011) Routing: Routing in Networks. [Online] Available at: http://en.wikipedia.org/wiki/Routing#Routing_protocols (Accessed 18 October 2011)
- Wu, B. (2011) “Simulation Based Performance Analyses on RIPv2, EIGRP and OSPF Using OPNET”, Math and Computer Science Working Papers, Fayetteville State University [Online] Available at http://www.digitalcommons.uncfsu.edu/macsc_wp/11/ (Accessed 10 October 2011)
- Yee, J.R. (2006) “On the Internet routing protocol Enhanced Interior Gateway Routing Protocol: is it optimal?” International Transactions in Operational Research, 13(3), pp.177-194., Wiley Online Library [Online] Available at <http://onlinelibrary.wiley.com/doi/10.1111/j.1475-3995.2006.00543.x/pdf> (Accessed 24 October 2011)

- Zaumen, W.T. & Garcia-Luna-Aceves, J.J. (1992) “Steady – State response of shortest – path routing protocol”, 1992 Eleventh Annual International Phoenix Conference Proceedings on Computers and Communications, pp.323-332., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=200568&isnumber=5206> (Accessed 10 November 2011)
- Zhao, C., Liu, Y. & Liu, K. (2009) “A More Efficient Diffussing Update Algorithm for Loop – Free Routing”, WiCom 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp.1-4., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5302468&isnumber=5300799> (Accessed 10 November 2011)

2. Profile Definition

The second step is to specify the behaviour of the applications in the network. This was configured in the profile definition object. Two profiles were created; voice profile supports voice application shown in figure 3 and video profile supports video application shown in figure 4

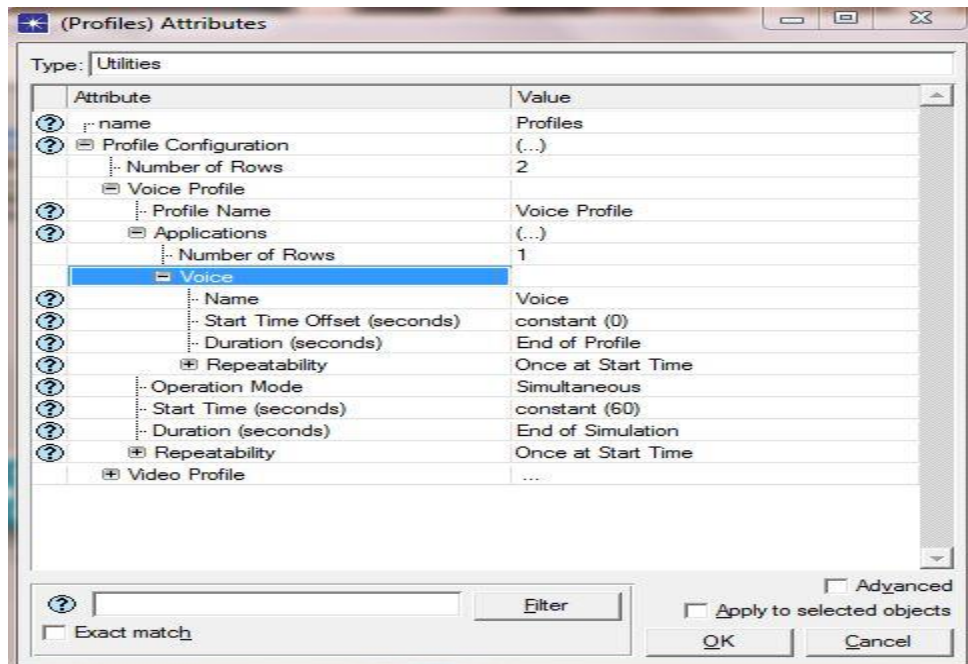


Figure 3: Voice Profile Definition

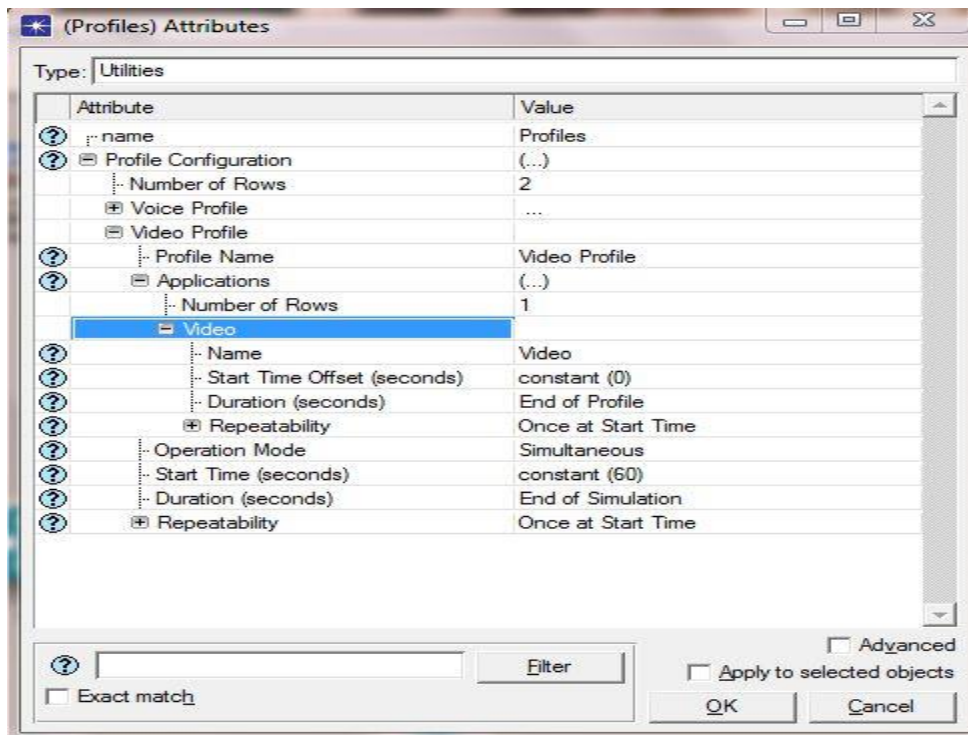


Figure 4: Video Profile Definition

3. Work Stations Configurations

The third step is to configure the PCs in the network to use the applications defined. Two PCs are configured in this network; PC 1 and PC 2. Application support profile means the work station will use the configured application as traffic and application support services means the work station will be its own server.

PC 1

In this work station, application support profiles was enabled to support two profiles previously defined in the profile definition object, voice and video profile shown in figure 5 and application support services was also enabled to support two applications defined in the application definition object, voice and video application shown in figure 6.

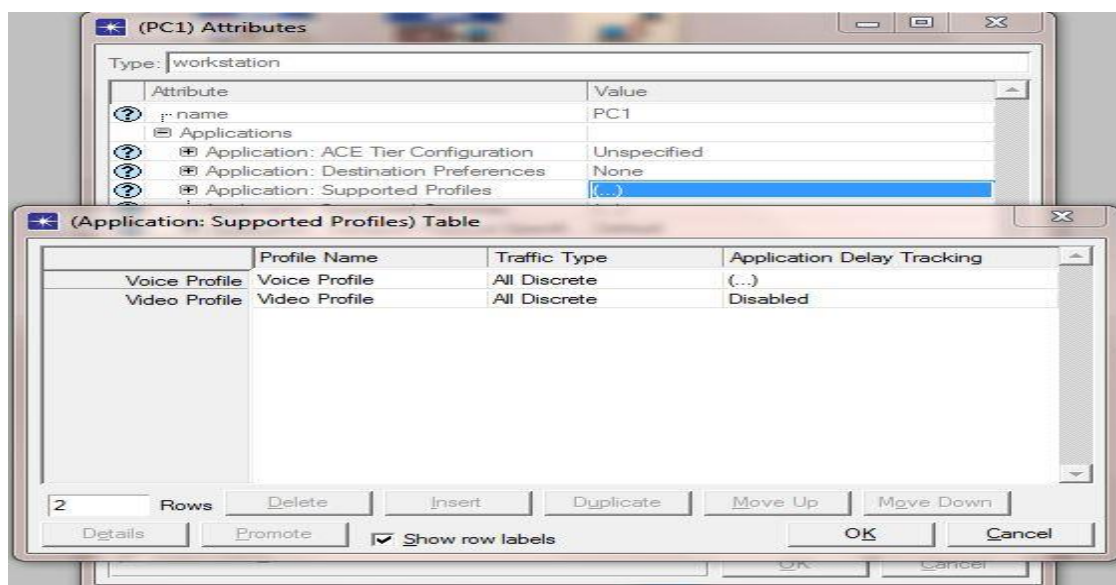


Figure 5: PC 1 Application Support Service Configuration

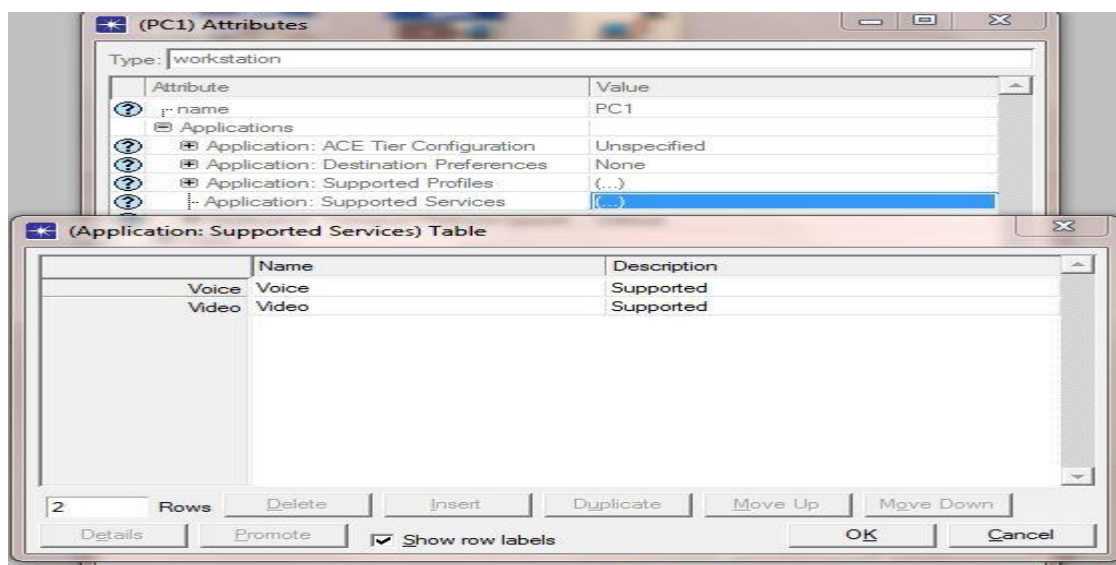


Figure 6: PC 1 Application Support Profile Configuration

PC 2

In this work station, application support profiles was enabled to support two profiles previously defined in the profile definition object, voice and video profile shown in figure 7 and application support services was also enabled to support two applications defined in the application definition object, voice and video application shown in figure 8.

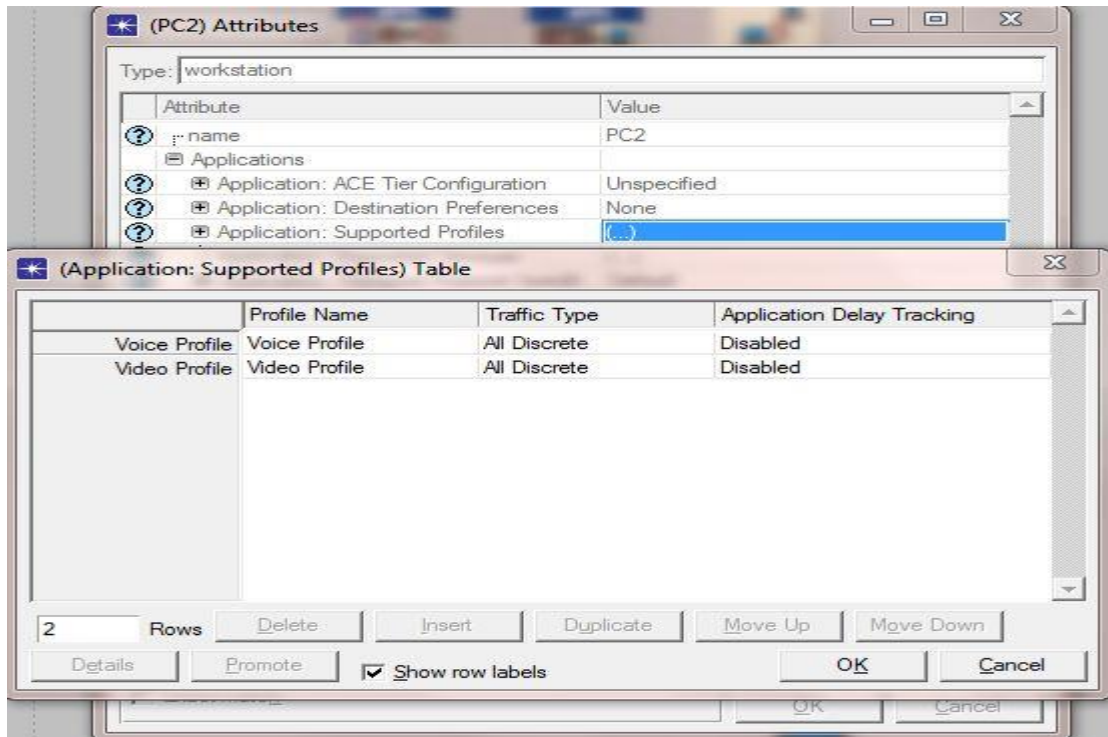


Figure 7: PC 2 Application Support Profiles Configuration

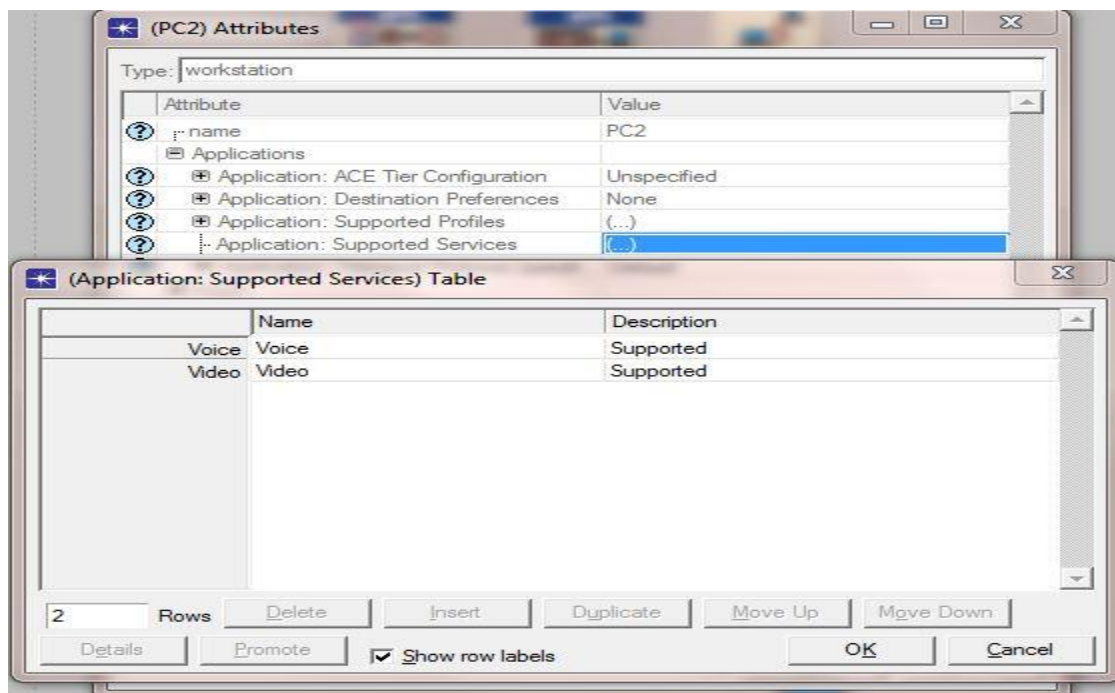


Figure 8: PC 2 Application Support Service Configuration

4. Link Failure

In the fourth step, the failure recovery object was configured to set a link failure to occur in the network when the simulation is running. The Link between R1 and R4 is set to fail at 200 seconds of the simulation time (3 minutes 20 seconds) as shown in figure 9.

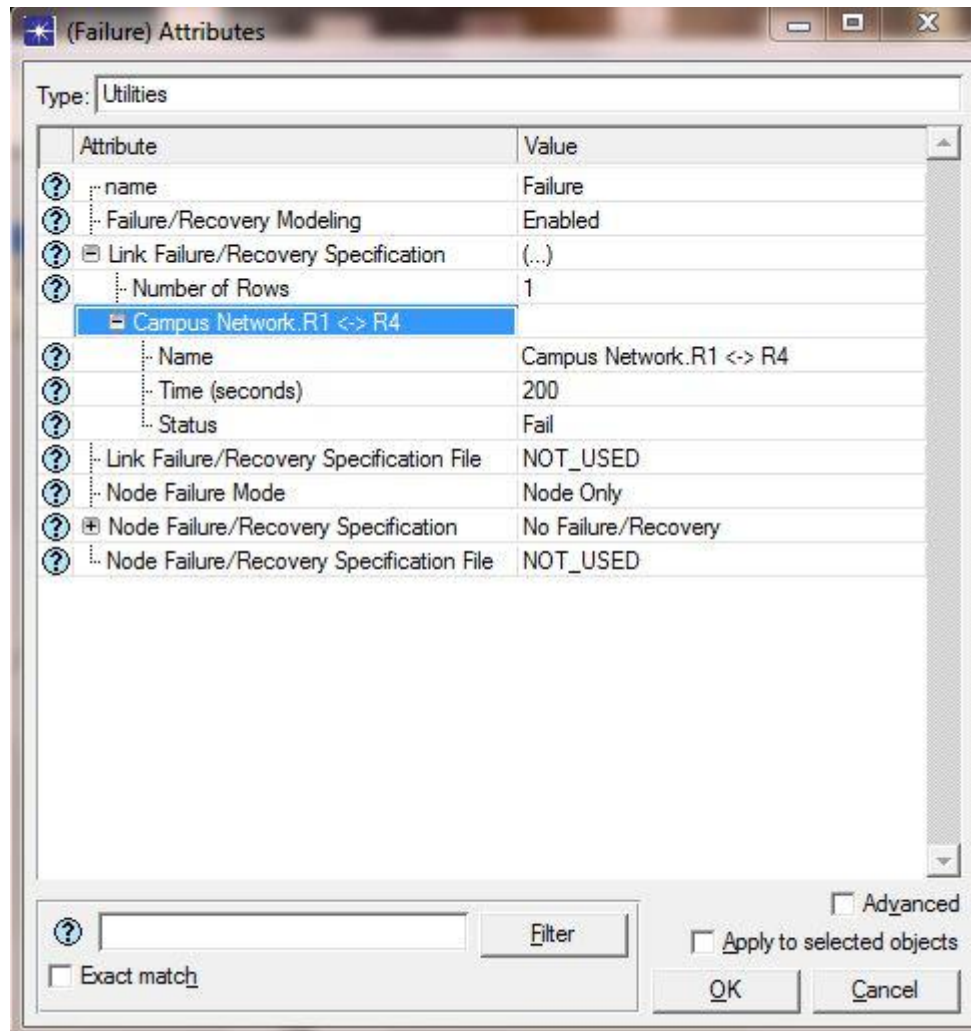


Figure 9: Link Failure Configuration

5. Choose Statistics

This is the final step in the network configure. Here the statistics to be collected for comparing the routing protocols were selected in the DES, IP Convergence Duration (sec) and IP Traffic Dropped (packets/sec) as shown in figure 10.

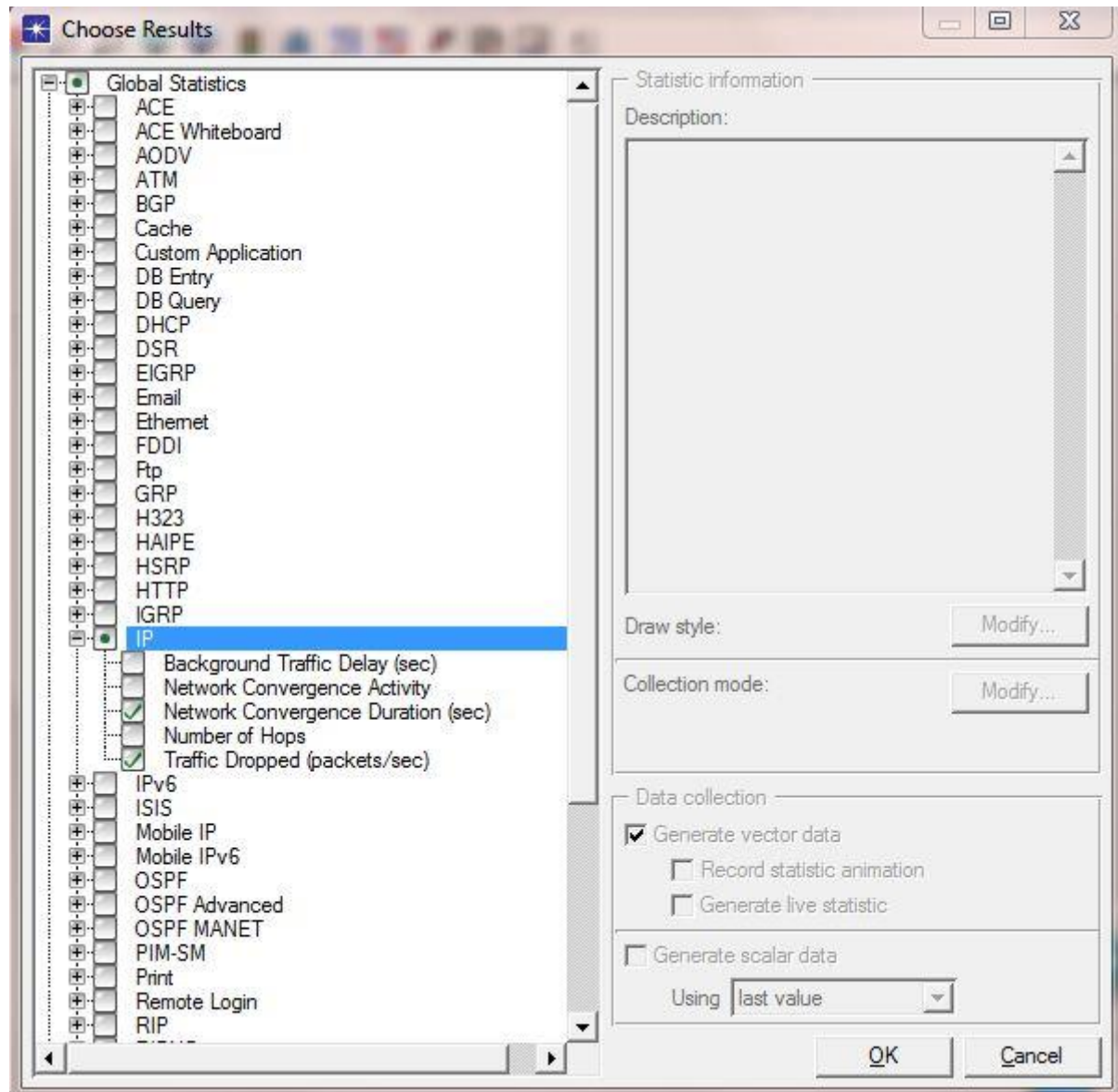


Figure 10: Discreet Event Simulator (DES) Statistics

6. Run Simulation

After all was set, now the routing protocol to be used in the network was enabled, and the simulation was set to run for 10 minutes simulation time for both OSPF and EIGRP scenario as shown in figure 11. Results are then obtained.

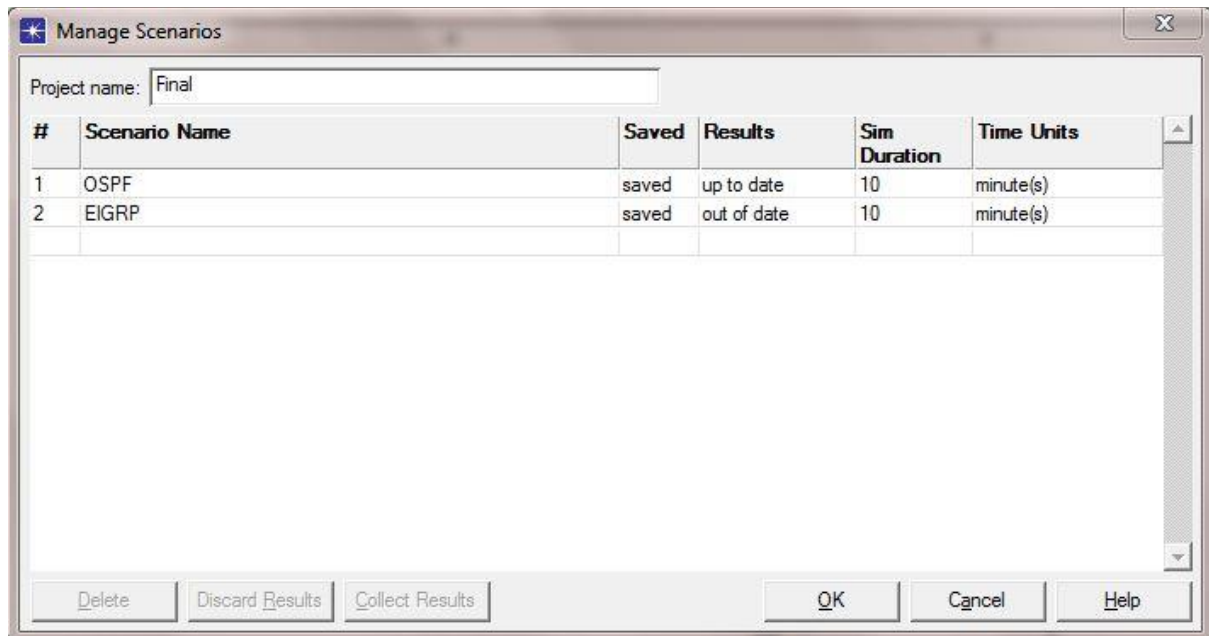


Figure 11: Manage and Run Scenarios

Wireshark Capture

Lab Experiment 2

1. OSPF Scenario

OSPF Scenario with DR/BDR Election

23	9.333681	192.168.2.1	224.0.0.5	OSPF	Hello Packet
24	10.161693	192.168.2.2	224.0.0.5	OSPF	Hello Packet
29	13.555403	192.168.2.2	224.0.0.5	OSPF	LS Update
30	13.590003	192.168.2.2	224.0.0.5	OSPF	LS Update
34	16.053882	192.168.2.1	224.0.0.6	OSPF	LS Acknowledge
38	18.262009	192.168.2.2	192.168.2.3	OSPF	LS Update
39	18.393798	192.168.2.1	192.168.2.3	OSPF	LS Update
42	19.333923	192.168.2.1	224.0.0.5	OSPF	Hello Packet
44	20.162195	192.168.2.2	224.0.0.5	OSPF	Hello Packet
46	22.909953	192.168.2.2	192.168.2.3	OSPF	LS Update
48	23.325757	192.168.2.1	192.168.2.3	OSPF	LS Update
55	27.698066	192.168.2.2	192.168.2.3	OSPF	LS Update
56	28.089996	192.168.2.1	192.168.2.3	OSPF	LS Update
58	29.333987	192.168.2.1	224.0.0.5	OSPF	Hello Packet
59	30.162010	192.168.2.2	224.0.0.5	OSPF	Hello Packet
65	32.246103	192.168.2.2	192.168.2.3	OSPF	LS Update
66	32.641879	192.168.2.1	192.168.2.3	OSPF	LS Update
75	37.090242	192.168.2.2	192.168.2.3	OSPF	LS Update
76	37.585992	192.168.2.1	192.168.2.3	OSPF	LS Update
79	39.334132	192.168.2.1	224.0.0.5	OSPF	Hello Packet
81	40.162231	192.168.2.2	224.0.0.5	OSPF	Hello Packet
85	41.658354	192.168.2.2	192.168.2.3	OSPF	LS Update
87	42.298387	192.168.2.1	192.168.2.3	OSPF	LS Update
92	46.622633	192.168.2.2	192.168.2.3	OSPF	LS Update
93	46.858220	192.168.2.1	192.168.2.3	OSPF	LS Update
99	49.334210	192.168.2.1	224.0.0.5	OSPF	Hello Packet
100	49.486285	192.168.2.1	224.0.0.6	OSPF	LS Update
101	49.487150	192.168.2.2	224.0.0.5	OSPF	LS Update
102	49.531536	192.168.2.2	224.0.0.5	OSPF	LS Update
104	50.162584	192.168.2.2	224.0.0.5	OSPF	Hello Packet
106	51.986943	192.168.2.1	224.0.0.5	OSPF	LS Acknowledge
107	51.987072	192.168.2.2	224.0.0.5	OSPF	LS Acknowledge
119	59.334776	192.168.2.1	224.0.0.5	OSPF	Hello Packet
123	60.162487	192.168.2.2	224.0.0.5	OSPF	Hello Packet

Figure 12: OSPF Scenario Wireshark Capture A (with DR/BDR Election)

OSPF Scenario with No DR/BDR Election

5	2.127899	192.168.2.2	224.0.0.5	OSPF	Hello Packet
7	3.927020	192.168.2.3	224.0.0.5	OSPF	Hello Packet
21	11.296553	192.168.2.1	224.0.0.5	OSPF	Hello Packet
23	12.128160	192.168.2.2	224.0.0.5	OSPF	Hello Packet
26	15.433972	192.168.2.2	224.0.0.5	OSPF	LS Update
32	17.931747	192.168.2.1	224.0.0.5	OSPF	LS Acknowledge
38	20.200269	192.168.2.2	192.168.2.3	OSPF	LS Update
39	20.347716	192.168.2.1	192.168.2.3	OSPF	LS Update
41	21.295920	192.168.2.1	224.0.0.5	OSPF	Hello Packet
42	22.128551	192.168.2.2	224.0.0.5	OSPF	Hello Packet
49	24.947902	192.168.2.1	192.168.2.3	OSPF	LS Update
51	25.052421	192.168.2.2	192.168.2.3	OSPF	LS Update
66	29.847897	192.168.2.1	192.168.2.3	OSPF	LS Update
67	29.960432	192.168.2.2	192.168.2.3	OSPF	LS Update
71	31.296038	192.168.2.1	224.0.0.5	OSPF	Hello Packet
72	32.128484	192.168.2.2	224.0.0.5	OSPF	Hello Packet
74	34.407968	192.168.2.1	192.168.2.3	OSPF	LS Update
76	34.916503	192.168.2.2	192.168.2.3	OSPF	LS Update
81	38.952134	192.168.2.1	192.168.2.3	OSPF	LS Update
84	39.716647	192.168.2.2	192.168.2.3	OSPF	LS Update
88	41.296268	192.168.2.1	224.0.0.5	OSPF	Hello Packet
90	42.129324	192.168.2.2	224.0.0.5	OSPF	Hello Packet
92	43.588168	192.168.2.1	192.168.2.3	OSPF	LS Update
93	44.425445	192.168.2.2	224.0.0.5	OSPF	LS Update
96	46.924091	192.168.2.1	224.0.0.5	OSPF	LS Acknowledge
103	51.296353	192.168.2.1	224.0.0.5	OSPF	Hello Packet
105	52.129887	192.168.2.2	224.0.0.5	OSPF	Hello Packet
118	61.297411	192.168.2.1	224.0.0.5	OSPF	Hello Packet
119	62.129458	192.168.2.2	224.0.0.5	OSPF	Hello Packet

Figure 13: OSPF Scenario Wireshark Capture B (NO DR/BDR Election)

EIGRP Scenario

3	1.506081	192.168.2.2	224.0.0.10	EIGRP	Hello
8	4.108937	192.168.2.3	224.0.0.10	EIGRP	Hello
9	4.343698	192.168.2.1	224.0.0.10	EIGRP	Hello
11	6.021604	192.168.2.2	224.0.0.10	EIGRP	Hello
13	9.051655	192.168.2.1	224.0.0.10	EIGRP	Hello
15	10.337576	192.168.2.2	224.0.0.10	EIGRP	Hello
19	13.723785	192.168.2.1	224.0.0.10	EIGRP	Hello
20	15.149866	192.168.2.2	224.0.0.10	EIGRP	Hello
23	18.243850	192.168.2.1	224.0.0.10	EIGRP	Hello
24	19.112086	192.168.2.1	224.0.0.10	EIGRP	Hello
25	19.114078	192.168.2.2	224.0.0.10	EIGRP	Hello
26	19.124088	192.168.2.1	224.0.0.10	EIGRP	Query
27	19.130085	192.168.2.2	224.0.0.10	EIGRP	Query
28	19.133634	192.168.2.2	224.0.0.10	EIGRP	Update
29	19.155985	192.168.2.1	224.0.0.10	EIGRP	Update
30	19.165854	192.168.2.2	224.0.0.10	EIGRP	Update
31	19.179927	192.168.2.1	224.0.0.10	EIGRP	Update
36	23.889724	192.168.2.2	224.0.0.10	EIGRP	Hello
37	23.891907	192.168.2.1	224.0.0.10	EIGRP	Hello
40	28.651872	192.168.2.1	224.0.0.10	EIGRP	Hello
41	28.757637	192.168.2.2	224.0.0.10	EIGRP	Hello
49	32.972006	192.168.2.1	224.0.0.10	EIGRP	Hello
51	33.333327	192.168.2.2	224.0.0.10	EIGRP	Hello
55	37.629264	192.168.2.2	224.0.0.10	EIGRP	Hello
56	37.844078	192.168.2.1	224.0.0.10	EIGRP	Hello

Figure 14: EIGRP Scenario Wireshark Capture

Bibliography

Aboelela, E., Peterson, L.L. & Davie, B.S. (2003) Computer Networks: Network Simulation Experiments Manual. 5th ed. San Francisco: Morgan Kaufmann.

Aidarous, S. & Plevyak, T. (2003) Managing IP Networks. Piscataway: IEEE Press

Akon, M.M., Asaduzzaman, S., Rahman, S. & Matsumoto, M. (2004) “Proposal of st – Routing Protocol”, Telecommunication Systems, 25(3, 4), pp.287-298., Carleton University [Online] Available at <http://people.scs.carleton.ca/~sasaduzz/pub/kluwer04.pdf> (Accessed 17 October 2011)

Al-saud, K.A., Tahir, H., Saleh, M. & Saleh, M. (2010) “A Performance Comparison of MD5 Authenticated Routing Traffic with EIGRP, RIPv2, and OSPF”, The International Arab Journal of Information Technology, 7(4), pp.380-387., [Online] Available at <http://www.ccis2k.org/iajit/PDF/vol.7,no.4/801final.pdf> (Accessed 19 October 2011)

Anand V. & Chakrabarty K. (2004) Cisco IP Routing Protocols(c) Trouble Shooting Techniques. India: Delmar Cengage Learning

Aslam, W. (2008) An Empirical Study to Observe Route Recoverability Performance of Routing Protocols in Real – Time Communication. MSc. Halmstad University. [Online] Available at: <http://hh.diva-portal.org/smash/get/diva2:239608/FULLTEXT01> (Accessed 24 November 2011)

Bauer, D., Yuksel, M., Carothers, C., Kalyanaraman, S. (2006) “A Case Study in Understanding OSPF and BGP Interactions Using Efficient Experiment Design”, PADS 2006 20th Workshop on Principles of Advanced and Distributed Simulation, pp.158-165., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1630727&isnumber=34195> (Accessed 10 November 2011)

Behrens, J. & Garcia-Luna-Aceves, J.J. (1994) “Distributed, Scalable Routing Based on Link – State Vectors”, 1994 Proceedings of the conference on Communications architectures, protocols and applications, 24(4), pp.136-147., ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=190809.190327> (Accessed 28 October 2011)

Difference between IGRP and EIGRP: IGRP vs. EIGRP. [Online] Available at: <http://www.differencebetween.net/technology/internet/difference-between-igrp-and-eigrp/> (Accessed 01 December 2011)

Din, I.U., Mahfooz, S. & Adnan, M. (2010) “Analysis of the Routing Protocols in Real Time Transmission: A Comparative Study”, Global Journal of Computer Science and Technology, 10(5), pp.18-22., Ijcaonline [Online] Available at <http://www.ijcaonline.org/volume26/number3/pxc3874223.pdf> (Accessed 7 October 2011)

Espetein, B. & Mehta, V. (2004) “Free Space Optical Communications Routing Performance in Highly Dynamic Airspace Environment”, IEEE Aerospace Conference Proceedings, 2, pp.1398-1406., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1367740> (Accessed 12 October 2011)

Farrel, A. (2004) The Internet And Its Protocols. San Francisco: Morgan Kaufmann

Fong, J.H., Gilbert, A.C., Kannan, S. & Strauss, M. J. (2005) “Better Alternatives to OSPF Routing”, Algorithmica, 43 (1-2), pp.113-131., Deep Blue [Online] Available at <http://hdl.handle.net/2027.42/41349> (Accessed 10 October 2011)

Garcia-Luna-Aceves, J.J. & Murthy, S. (1997) “A path – finding algorithm for loop – free routing” IEEE ACM Transactions on Networking, 5(1), pp.148-160., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=554729&isnumber=12084> (Accessed 26 October 2011)

Gouda, M.G. & Schneider, M. (2003) “Maximizable routing metrics”, IEEE/ACM Transactions on Networking, 11(4), pp.663-675., IEEE Xplore [Online] Available at

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1224464&isnumber=27488> (Accessed 14 October 2011)

Jaffe, J.M. & Moss, F.H. (1982) “A Responsive Distributed Routing Algorithm for Computer Networks”, IEEE Transactions on Communications, 30(7), pp.1758-1762., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1095632&isnumber=23961> (Accessed 15 October 2011)

Kim, D.H., Ryu, K.H. & Cho, Y.S. (2000) “A new routing control technique using active temporal data management”, The Journal of Systems and Software, 51(1), pp.37-48., Science Direct [Online] Available at <http://www.sciencedirect.com/science/article/pii/S0164121299001089> (Accessed 27 October 2011)

Le, F., Xie, G.G. & Zhang, H. (2007) “Understanding Route Redistribution”, 2007 IEEE International Conference on Network Protocols (ICNP), pp.81-92., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4375839&isnumber=4375821> (Accessed 10 November 2011)

Le, F., Xie, G.G. & Zhang, H. (2010) “Theory and Primitives for Safety Connecting Routing Protocol Instances”, 2010 Proceedings of the ACM SIGCOMM, pp.219-230., ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=1851210> (Accessed 10 November 2011)

Lemma, E.S., Hussain, S.A. & Anjelo, W.W. (2009) Performance Comparison of EIGRP/IS – IS and OSPF/IS – IS. MSc. Blekinge Institute of Technology. [Online] Available at: www.sciacademypublisher.com/journals/index.php/IJRRAN/.../129 (Accessed 15 October 2011)

Li, Y., Cui, W., Li, D. & Zhang, R. (2011) “Research based on OSI model”, 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp.554-557., IEEE Xplore [Online] Available at

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6014631&isnumber=6013532> (Accessed 20 October 2011)

Maj, S.P., Murphy, G. & Kholi, G. (2004) “State Models for Internetworking Technologies”, FIE 2004 34th Annual Frontiers in Education, pp.F2G-10-15., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1408613&isnumber=30543> (Accessed 21 October 2011)

Malhotra, R. (2002) IP Routing. Sebastopol: O'Reilly Media

Maltz, D.A., Xie, G., Zhan, J., Zhang, H., Hjalmtysson, G. & Greenberg, A. (2004) “Routing Design in Operational Networks: A Look from the Inside”, Network Geometry and Design, 34(4), pp.27-40., ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=1015472> (Accessed 26 October 2011)

Moy, J.T. (1998) OSPF: Anatomy of an Internet Routing Protocol. Boston, USA: Addison – Wesley Longman Publishing Co.

Mustafa, N.M. & Othman, M. (2007) “A Review of Routing Optimization Using OSPF”, Proceedings of the 2007 IEEE International Conference on Telecommunication and Malaysia International Conference on Communication, pp.472-477., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4448682> (Accessed 23 October 2011)

Narisetty, S.K. & Balsu, S.K., (2011) “Performance Comparison of EIGRP and ISIS/RIP Protocols”, International Journal of Research and Reviews in Ad Hoc Networks, pp.63-66., Science Academy Publisher [Online] Available at <http://www.sciacademypublisher.com/journals/index.php> (Accessed 19 October 2011)

Nelakuditi, S., Lee, S., Yu, Y., Zhang, Z. & Chuah, C. (2007) “Fast Local Rerouting for Handling Transient Link Failures”, IEEE/ACM Transactions on Networking, 15(2), pp.359-372., IEEE Xplore [Online] Available at

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4154760&isnumber=4154740> (Accessed 12 November 2011)

Pei, D., Wang, L., Massey, D., Wu, S.F. & Zhang, L. (2003) "A Study of Packet Delivery Performance during Routing Convergence", 2003 International Conference on Dependable Systems and Networks, pp.183-192., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1209929&isnumber=27228> (Accessed 10 December 2011)

Pereira, T.B. & Ling, L.L. (2010) "An OPNET Modeler Based Simulation Platform for Adaptive Routing Evaluation", pp.1-5., [Online] Available at http://www.lrprc.fee.unicamp.br/arquivos/Uni20_opnetwork2002.pdf (Accessed 10 October 2011)

Perlman, R. (1991) "A Comparison between Two Routing Protocols: OSPF and IS-IS", IEEE Networks, 5(5), pp.18-24., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=121955&isnumber=3473> (Accessed 13 November 2011)

Rastogi, R., Breitbart, Y., Garofalakis, M. & Kumar, A. (2003) "Optimal Configuration of OPSF Aggregates" IEEE Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, 11(2), pp.181-194., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1019334&isnumber=21922> (Accessed 10 October 2011)

Riedl, A. & Schupke, D.A. (2007) "Routing Optimization in IP Networks Utilizing Additive and Concave Link Metrics", IEEE/ACM Transactions on Networking, 15(5), pp.1136-1148., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4346555&isnumber=4346537> (Accessed 17 November 2011)

Routing Protocol Choice: OSPF vs. EIGRP. [Online] Available at: http://www.h3c.com/portal/Products__Solutions/Products/Other_Products/Routers/Quidway_AR18-

[2X_Series_Routers/White_Paper/200701/194231_57_0.htm#_Toc87242195](http://www.inetdaemon.com/tutorials/internet/ip/routing/2X_Series_Routers/White_Paper/200701/194231_57_0.htm#_Toc87242195)

(Accessed 05 November 2011)

Routing: IP Routing. [Online] Available at:

<http://www.inetdaemon.com/tutorials/internet/ip/routing/> (Accessed 10 December 2011)

Schwartz, M. & Stern, T.E. (1980) "Routing Techniques used in Computer Communication Networks", IEEE Transactions on Communications, 28(4), pp.539-552., IEEE Xplore [Online] Available at

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1094690&isnumber=23925> (Accessed 10 October 2011)

Shahsavari, M.M. & Alsharif, S. (2003) "A differentiated services approach: response time performance analysis of QoS application to real-time interactive multimedia over the Internet", SoutheastCon Proceedings, pp. 81-86., IEEE Xplore [Online] Available at

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1268434&isnumber=28384> (Accessed 2 January 2012)

Shaikh, A. & Greenberg, A. (2001) "Experience in black-box OSPF measurement", IMW 2001 Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, pp.113-125., ACM Digital Library [Online] Available at

<http://dl.acm.org/citation.cfm?id=505218> (Accessed 10 October 2011)

Shaikh, A., Isett, C., Greenberg, A., Roughan, M. & Gottlieb, J. (2002) "A Case Study of OSPF Behavior in a Large Enterprise Network", Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement. ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?doid=637201.637236> (Accessed 17 October 2011)

Shakar, A.U., Alaettinoglu, C., Dussa-Zieger, K. & Matta, I. (1992) "Performance Comparison of Routing Protocols under Dynamic and Static File Transfer Connections", ACM SIGCOMM Computer Communication Review, 22(5), ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=141813> (Accessed 24 October 2011)

- Shu, Z. & Kadobayashi, Y. (2004) “Troubleshooting on Intra – Domain Routing Instability”, workshop on Network troubleshooting: research, theory and operations practice meet malfunctioning reality, pp.289-294., ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=1016699> (Accessed 24 October 2011)
- Sidhu, D., Fu, T., Abdallah, S. & Nair, R. (1993) “Open Shortest Path First (OSPF) Routing Protocol Simulation”, pp.53-62., ACM Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=167954.166243> (Accessed 17 October 2011)
- Understanding Simple Single – Area OSPF: Understanding OSPF Fundamentals. [Online] Available at: <http://etutorials.org/cert/ccnp+bsci/Part+III+OSPF/Chapter+5.+Understanding+Simple+Single-Area+OSPF/Foundation+Topics/> (Accessed 17 December 2011)
- Vasudha, & Jindal, G.K. (2011) “Investigations and Performance Evaluation of Dynamic Routing Protocol with New Proposed Protocol for WAN”, International Journal on Computer Science and Engineering, 3(5), pp.1970-1979., IJCSE [Online] Available at <http://www.enggjournals.com/ijcse/doc/IJCSE11-03-05-058.pdf> (Accessed 28 October 2011)
- Vetter, B., Wang, F. & Wu, S.F. (1997) “An experimental study of insider attacks for OSPF routing protocol”, 1997 International Conference on Network Protocols, pp.293-300., IEEE Xplore [online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=643735&isnumber=13855> (Accessed 30 October 2011)
- Vutukury, S. & Garcia-Luna-Aceves, J.J. (1999) “A Practical Framework for Minimum-Delay Routing in Computer Networks”, pp.1-28., DTIC [Online] Available at <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA459412&Location=U2&doc=GetTRDoc.pdf> (Accessed 30 October 2011)
- Vutukury, S. & Garcia-Luna-Aceves, J.J. (1999) “A Simple Approximation to Minimum-Delay Routing”, 1999 Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication, 29(4), pp.227-238., ACM

Digital Library [Online] Available at <http://dl.acm.org/citation.cfm?id=316227>
(Accessed 30 October 2011)

Wang, B., Zhang, J., Guo, Y. & Chen, W. (2010) “Fast – Converging Distance Vector Routing Mechanism for IP Networks”, Journal of Networks, 5(9), pp.1068-1075., Academy Publisher [Online] Available at <http://ojs.academypublisher.com/index.php/jnw/article/viewFile/050910681075/2129> (Accessed 29 October 2011)

Yang, M.X., Wang, B.T. & Guo, W.D. (2009) “Research on the Performance of Dynamic Routing Algorithm”, 2009 International Conference on Machine Learning and Cybernetics, 5, pp.2647-2650., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5212662&isnumber=5212095> (Accessed 24 October 2011)

Zaumen, W.T. & Garcia-Luna-Aceves, J.J. (1998) “Loop-Free Multipath Routing Using Generalized Diffusing Computations”, IEEE INFOCOM 1998 Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings, 3, pp.1408-1417., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=662958&isnumber=14479> (Accessed 10 October 2011)

Zengin, A. & Sarjoughian, H. (2010) “Devs – Suite Simulator: A Tool Teaching Network Protocols”, Proceedings of the 2010 Winter Simulation Conference, pp.2947-2957., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5678989> (Accessed 07 October 2011)

Zhao, Y., Yin, X., Han, B. & Wu, J. (2001) “Online Test System Applied in Routing Protocol Test”, 2001 Ninth International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems, pp.331-338., IEEE Xplore [Online] Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=948884&isnumber=20512> (Accessed 10 October 2011)