



---

# Performance Comparison of EIGRP/ IS-IS and OSPF/ IS-IS

Esuendale Shewandagn Lemma  
Syed Athar Hussain  
Wendwossen Worku Anjelo

This thesis is presented as part of Degree of  
Master of Science in Electrical Engineering

Blekinge Institute of Technology  
November 2009

---

Blekinge Institute of Technology  
School of Computing  
Supervisor: Dr. Doru Constantinescu  
Examiner: Dr. Doru Constantinescu



## Abstract

In modern communication networks, routing protocols are used to determine the shortest path to the destination. Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP) and Intermediate System to Intermediate System (IS-IS) are the dominant interior routing protocols for such networks.

This thesis presents a simulation based analysis of these protocols. We used the combination of EIGRP&IS-IS, OSPF&IS-IS routing protocols on the same network in order to reveal the advantage of one over the other as well as the robustness of each protocol combination and how this is measured. To carry out the network simulations, we used Optimized Network Engineering Tool (OPNET).

The comparison analysis is based on several parameters that determine the robustness of these protocols. The routing protocol convergence time is one important parameter which determines the time needed by the routers to learn the new topology of the network whenever a change occurs in the network. The routing protocol which converges faster is considered a better routing protocol. Point-to-point link throughput, HTTP object response time, database response time and e-mail download response time are other parameters we used to measure the routing performance of the network.



## Acknowledgements

*Firstly, I would like to give thanks to God. I am heartily thankful to my brother, Kassahun, for his encouragement and support from the initial to the final level. Finally, I offer my regards to all of those who help me in any respect to complete this thesis work.*

***Esuendale Shewandagn Lemma***

*First, I would like to thank the ALMIGHTY, the most merciful, the most beneficent for His guidance and blessings in making this thesis successful. I would like to thank my parents and all my friends for their support during my studies. It would not have been possible to manage everything without them.*

***Syed Athar Hussain***

*I thank my family and almighty God with all my heart. It has been such a struggle, and I hope it was just the beginning. Last but not least, I would like to express my warm gratitude to my good friend Teddy (Dr.) for his encouragement.*

***Wendwossen Worku Anjelo***

*We would like to thank **Dr. Doru Constantinescu**, our supervisor and examiner, for his valuable guidance and contributions to our thesis work.*

***Lemma  
Athar  
Anjelo***



## TABLE OF CONTENTS

ABSTRACT .....	III
ACKNOWLEDGEMENTS .....	V
TABLE OF CONTENTS .....	VII
LIST OF FIGURES .....	XI
LIST OF TABLES .....	XIII
ACRONYMS .....	XV
CHAPTER 1 .....	1
INTRODUCTION .....	1
1.1 INTRODUCTION .....	1
1.2 PROBLEM DESCRIPTION .....	2
1.3 MOTIVATION.....	2
1.4 THESIS OUTLINE .....	3
CHAPTER 2 .....	5
ROUTING PROTOCOLS .....	5
2.1 ROUTING PROTOCOL OVERVIEW.....	5
2.2 DESIRABLE PROPERTIES.....	6
2.3 METRICS AND ROUTING.....	7
2.3.1 Metrics .....	7
2.3.2 Purpose of a metric .....	7
2.3.3 Metric Parameters .....	7
2.4 HOP COUNT VERSUS BANDWIDTH.....	8
2.5 ADMINISTRATIVE DISTANCE.....	9
2.6 CLASSIFICATION .....	10
2.7 STATIC VERSUS DYNAMIC ROUTING .....	10
2.8 CLASSFUL AND CLASSLESS ROUTING .....	11
2.8.1 Classful Routing.....	11
2.8.2 Classless Routing.....	12
2.9 DISTANCE VECTOR ROUTING.....	13
2.9.1 Methods of Routing .....	13
2.9.2 Properties of Distance Vector Routing .....	14
2.9.3 Advantages and Disadvantages of DV Routing.....	15
2.10 LINK STATE ROUTING.....	15
2.10.1 Methods of Routing .....	17
2.10.2 Properties of LSR.....	17
2.10.3 Advantages and Disadvantages of LSR.....	18
CHAPTER 3 .....	19
ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL.....	19
3.1 INTRODUCTION TO EIGRP .....	19
3.2 EIGRP PROTOCOL STRUCTURE .....	19

3.3 COMPONENTS OF EIGRP .....	21
3.3.1 Neighbour Discovery/Recovery.....	21
3.3.2 Reliable Transport Protocol .....	22
3.3.3 Diffusion Update Algorithm.....	23
3.3.4 Protocol Dependent Modules.....	26
3.4 EIGRP METRICS.....	27
3.5 EIGRP CONVERGENCE .....	28
3.6 ADVANTAGES AND DRAWBACKS OF EIGRP .....	28
CHAPTER 4 .....	31
OPEN SHORTEST PATH FIRST.....	31
4.1 INTRODUCTION TO OSPF.....	31
4.2 OSPF PROTOCOL STRUCTURE .....	31
4.3 OSPF PACKET TYPES .....	32
4.4 OSPF AREAS .....	35
4.4.1 Normal Area.....	35
4.4.2 Stub Area .....	36
4.4.3 Totally Stubby Area.....	37
4.4.4 Not-So-Stubby Area.....	38
4.4.5 Totally Not-So-Stubby Area.....	38
4.5 OSPF ROUTER TYPES .....	39
4.6 OSPF METRICS.....	40
4.7 OSPF CONVERGENCE .....	41
4.8 CHARACTERISTICS OF OSPF .....	41
4.9 PROTOCOLS WITHIN OSPF .....	42
4.9.1 The HELLO Protocol.....	42
4.9.2 The Exchange Protocol.....	43
4.9.3 The Flooding Protocol .....	43
4.9.4 The Aging Link State Record .....	43
4.10 OSPF GENERAL OPERATION.....	43
4.11 ADVANTAGES AND DRAWBACKS OF OSPF.....	46
CHAPTER 5 .....	49
INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM .....	49
5.1 INTRODUCTION .....	49
5.2 IS-IS PROTOCOL STRUCTURE .....	50
5.3 IS-IS PACKET TYPES.....	51
5.4 IS-IS AREAS AND ROUTING DOMAINS .....	52
5.5 IS-IS ROUTER TYPES .....	53
5.5.1 Level 1 Router.....	54
5.5.2 Level 2 Router.....	54
5.5.3 Level 1/ Level 2 Router .....	54
5.6 IS-IS METRICS.....	55
5.7 IS-IS GENERAL OPERATION.....	55
5.8 ADVANTAGES AND DRAWBACKS OF IS-IS .....	56

CHAPTER 6 .....	59
SIMULATION.....	59
6.1 INTRODUCTION .....	59
6.2 NETWORK SIMULATORS.....	59
6.3 SIMULATION ENVIRONMENT USED .....	60
6.3.1 Design and Analysis in OPNET .....	62
6.4 NETWORK TOPOLOGY .....	63
6.4.1 OSPF Scenario .....	64
6.4.2 EIGRP Scenario .....	65
6.4.3 IS-IS Scenario .....	65
6.4.4 EIGRP/IS-IS Scenario .....	65
6.4.5 OSPF/IS-IS Scenario .....	67
6.5 CONFIDENCE ANALYSIS .....	68
6.5.1 Confidence Analysis of OSPF/IS-IS.....	69
6.5.2 Confidence Analysis of EIGRP/IS-IS.....	70
6.6 SIMULATION RESULT AND ANALYSIS .....	71
6.6.1 OSPF Traffic.....	72
6.6.2 EIGRP Traffic.....	73
6.6.3 EIGRP Convergence Time .....	73
6.6.4 IS-IS Convergence Time.....	75
6.6.5 Database Query Response Time .....	75
6.6.6 E-mail Download Response Time .....	77
6.6.7 HTTP Object Response Time .....	77
6.6.8 Throughput.....	78
CHAPTER 7 .....	81
CONCLUSIONS AND FUTURE WORK .....	81
REFERENCES .....	83



## LIST OF FIGURES

FIGURE 2.1: HOP COUNT VERSUS BANDWIDTH .....	9
FIGURE 2.2: CLASSFUL ROUTING WITH SAME SUBNET MASK.....	12
FIGURE 2.3: CLASSLESS ROUTING WITH DIFFERENT SUBNET MASKS .....	12
FIGURE 3.1: PROTOCOL STRUCTURE OF EIGRP.....	19
FIGURE 3.2: NETWORK TOPOLOGY FOR DUAL. ....	24
FIGURE 3.3: NETWORK TOPOLOGY WITH FAILED LINK.....	25
FIGURE 3.4: NETWORK TOPOLOGY WITH FAILED LINK.....	26
FIGURE 3.5: NETWORK USING EIGRP.....	28
FIGURE 4.1: PROTOCOL STRUCTURE OF OSPF.....	32
FIGURE 4.2: HELLO PACKET .....	33
FIGURE 4.3: NORMAL AREA.....	36
FIGURE 4.4: STUB AREA. ....	37
FIGURE 4.5: TOTALLY NOT-SO-STUBBY AREA.....	39
FIGURE 4.6: NETWORK USING OSPF.....	41
FIGURE 4.7: AS WITH LINK STATE INFORMATION.....	44
FIGURE 4.8: SHORTEST PATH FIRST TREE PERFORMED AT R4. ....	45
FIGURE 4.9: ROUTING TABLE ENTRIES. ....	45
FIGURE 5.1: IS-IS PROTOCOL STRUCTURE.....	51
FIGURE 5.2: IS-IS BACKBONE.....	52
FIGURE 5.3: IS-IS AREAS.....	53
FIGURE 5.4: IS-IS NETWORK. ....	54
FIGURE 6.1: NETWORK DOMAIN EDITOR. ....	60
FIGURE 6.2: NODE DOMAIN EDITOR. ....	61
FIGURE 6.3: PROCESS DOMAIN EDITOR. ....	62
FIGURE 6.4: DESIGN STEPS. ....	62
FIGURE 6.5: NETWORK TOPOLOGY. ....	63
FIGURE 6.6: EIGRP/IS-IS TOPOLOGY. ....	66
FIGURE 6.7: OSPF/IS-IS TOPOLOGY. ....	67
FIGURE 6.8: E-MAIL DOWNLOAD RESPONSE TIME IN OSPF/IS-IS.....	69
FIGURE 6.9: E-MAIL DOWNLOAD RESPONSE TIME IN EIGRP/IS-IS.....	70
FIGURE 6.10: OSPF TRAFFIC. ....	72
FIGURE 6.11: EIGRP TRAFFIC. ....	73
FIGURE 6.12: EIGRP CONVERGENCE TIME. ....	74
FIGURE 6.13: CONVERGENCE TIME.....	75
FIGURE 6.14: DATABASE RESPONSE TIME. ....	76
FIGURE 6.15: E-MAIL DOWNLOAD RESPONSE TIME.....	77
FIGURE 6.16: HTTP OBJECT RESPONSE TIME.....	78
FIGURE 6.17: POINT TO POINT THROUGHPUT.....	79



**LIST OF TABLES**

TABLE 3.1: EIGRP INTERVAL TIME FOR HELLO AND HOLD .....	22
TABLE 4.1: DIFFERENT LSAS .....	35
TABLE 4.2: LINK STATE DATABASE.....	44



## ACRONYMS

<b>ABR</b>	Area Border Router
<b>AS</b>	Autonomous System
<b>ASBR</b>	Autonomous System Boundary Router
<b>BDR</b>	Backup Designated Router
<b>BR</b>	Backbone Router
<b>CSNP</b>	Complete Sequence Number Packet
<b>DBD</b>	Data Base Description
<b>DR</b>	Designated Router
<b>DUAL</b>	Diffusion Update Algorithm
<b>DVR</b>	Distance Vector Routing
<b>EIGRP</b>	Enhanced Interior Gateway Routing Protocol
<b>FC</b>	Feasible Condition
<b>FD</b>	Feasible Distance
<b>FS</b>	Feasible Successor
<b>IIH</b>	Intermediate System-Intermediate System HELLO
<b>IR</b>	Internal Router
<b>IS-IS</b>	Intermediate system to intermediate system
<b>LSA</b>	Link-State Advertisement
<b>LSAck</b>	Link-State Acknowledgement
<b>LSDB</b>	Link-State Database
<b>LSP</b>	Link State Packet
<b>LSR</b>	Link-State Request
<b>LSU</b>	Link-State Update
<b>L1</b>	Level 1
<b>L2</b>	Level 2
<b>L1/L2</b>	Level 1/Level 2
<b>NET</b>	Network Entity Title
<b>NSAP</b>	Network Service Access Point
<b>NSSA</b>	Not-So-Stubby-Area
<b>OSPF</b>	Open Shortest Path First
<b>PDM</b>	Protocol Dependent Module
<b>PSNP</b>	Partial Sequence Number Packet
<b>RD</b>	Reported Distance
<b>RTP</b>	Reliable Transport Protocol
<b>SPF</b>	Shortest Path First
<b>VLSM</b>	Variable Length Subnet Mask



# CHAPTER 1

## INTRODUCTION

### 1.1 Introduction

Computer networks and networking have grown rapidly during the last few decades. They evolved to serve basic user needs such as file and printer sharing, video conferencing and more. At present, Internet is regarded as a basic necessity of any modern society. Internet is an example of computer networks, and is considered to be the largest network of all.

At the beginning of networking technology, computers shared files and printers mainly with computers from the same manufacturer. But this problem was solved by introducing the Open Systems Interconnection (OSI) reference model by the International Organization for Standardization (ISO). The OSI model was meant to help vendors create interoperable network devices and software in the form of protocols so that networks from different vendors could work with each other [1].

Internet Protocol (IP) is the most widely used network layer protocol for interconnecting computer networks. Intra domain routing protocols, also known as Internet Gateway Protocols (IGP), organize routers within Autonomous Systems (ASs). Nowadays, the most widely used intra domain routing protocols are Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP) and Intermediate System to Intermediate System (IS-IS).

This thesis provides detailed simulation analysis of the robustness of OSPF/IS-IS and EIGRP/IS-IS routing protocols. We analyze the impacts of using OSPF and IS-IS together as compared to using OSPF alone or IS-IS alone

on the same network topology. In the same manner, we analyze the impacts of using EIGRP and IS-IS together as compared to using IS-IS or EIGRP alone. The simulations are carried out by using the OPNET-Modeler simulator [35].

## 1.2 Problem Description

Interior networks mainly use the following three routing protocols: EIGRP, OSPF and IS-IS. Due to its scalability, OSPF is used more often than EIGRP [1]. OSPF and IS-IS are link state protocols. These protocols consume high bandwidth during network convergence. Both protocols are relatively complicated to setup on the network but they are the preferred protocols for larger networks. On the other hand, EIGRP has a faster convergence time than OSPF and IS-IS, it can be used in different network layer protocols and it is relatively easy to setup on the network. However, EIGRP is a CISCO proprietary protocol, which means that it can only be used on CISCO products.

In this thesis, we will look at the advantages of using OSPF and IS-IS on one network and EIGRP and IS-IS on another network. The comparison analysis of the routing protocols will be performed on OPNET.

## 1.3 Motivation

The major causes for the degradation of the service performance in Internet are network congestion, link failures, and routing instabilities [2]. In [2] it has been found that most of the disruptions occur during routing changes. A few hundred milliseconds of disruption are enough to cause a disturbance in voice and video [2]. A disruption lasting a few seconds is long enough for interrupting web transactions [3]. Hence, during routing protocol convergence data packets are dropped, delayed, and received out-of-order at the destination resulting thus in a serious degradation in the network performance [2].

To support a wide variety of network services such as web browsing, telephony, database access and video streaming, it becomes important to analyze different routing protocols so that network resources are utilized more efficiently.

Routing protocols are the main factors contributing to speed-up data transfers within the network. The performance of the routing protocols can be tested by their convergence time, link throughput and application layer service performance, e.g., HTTP and FTP. *Convergence time* is the time period required for the routing protocol to converge and reach a steady state. In routing protocols, the convergence time is an important aspect in indicating routing protocol performance.

## **1.4 Thesis Outline**

The remaining part of the thesis is organized as follows. Chapter 2 describes the types of routing protocols, the desirable properties of a routing protocol, advantages and drawbacks. Chapter 3 describes the EIGRP protocol structure and working operation in detail. Chapter 4 discusses the OSPF protocol structure, characteristics and working operation. Chapter 5 describes the IS-IS protocol structure, its characteristics and working operation. Chapter 6 describes our simulation results. Finally, Chapter 7 presents our conclusions and thoughts for future work.



# CHAPTER 2

## ROUTING PROTOCOLS

### 2.1 Routing Protocol Overview

In IP networks, the main task of a routing protocol is to carry packets forwarded from one node to another. In a network, routing can be defined as transmitting information from a source to a destination by hopping one-hop or multi hop. Routing protocols should provide at least two facilities: selecting routes for different pairs of source/destination nodes and, successfully transmitting data to a given destination.

Routing protocols are used to describe how routers communicate to each other, learn available routes, build routing tables, make routing decisions and share information among neighbors. Routers are used to connect multiple networks and to provide packet forwarding for different types of networks.

The main objective of routing protocols is to determine the best path from a source to a destination. A routing algorithm uses different metrics based on a single or on several properties of the path in order to determine the best way to reach a given network. Conventional routing protocols used in interior gateway networks are classified as *Link State Routing Protocols* and *Distance Vector Routing Protocols*.

There are also other classifications of routing protocols, i.e., *dynamic* or *static*, *reactive* or *proactive*, etc. The conventional routing protocols can be used as a basis for building up other protocols for other types of communication networks such as *Wireless Ad-Hoc Networks*, *Wireless Mesh Networks*, etc.

This chapter introduces different types of routing protocols, routing methods, network roles and characteristics.

## 2.2 Desirable Properties

To provide efficient and reliable routing, several desirable properties are required from the routing protocols:

### ➤ **Distributed Operation**

The protocol should not depend on any centralized node for routing, i.e., distributed operation. The main advantage of this approach is that in such a network a link may fail anytime.

### ➤ **Loop Free**

The routes provided by the routing protocol should guarantee a loop free route. The advantage of loop free routes is that in these cases the available bandwidth can be used efficiently.

### ➤ **Convergence**

The protocol should converge very fast, i.e., the time taken for all the routers in the network to know about routing specific information should be small.

### ➤ **Demand Based Operation**

The protocol should be reactive, i.e., the protocol should provide routing only when the node demands saving thus valuable network resources.

### ➤ **Security**

The protocol should ensure that data will be transmitted securely to a given destination.

### ➤ **Multiple Routes**

The routing protocol should maintain multiple routes. If a link fails or congestion occurs then the routing can be done through the multiple routes available in the routing table saving thus valuable time for discovering a new route.

➤ **Quality of Service (QoS)**

The protocol design should provide some class of QoS depending upon its intended network use.

Not all routing protocols used in current networks meet the above requirements. Each protocol differs in some way.

## **2.3 Metrics and Routing**

### **2.3.1 Metrics**

The *path cost* can be measured based on metric parameters of the path. To determine the best path among all the available routes, routing protocols will select the route with the smallest metric value (or cost). Every routing protocol has its own metric calculation.

### **2.3.2 Purpose of a metric**

There are scenarios where routing protocols learn about more than one route to the same destination. To select the best among the available paths, routing protocols should be able to evaluate and distinguish among these paths. Hence, for this purpose, different metrics are used. A metric is a value utilized by the routing protocols to assign a cost to reach the destination or remote network. When there are multiple paths to the same destination, metrics are used to determine which path is the best.

Calculation of metrics for each routing protocol is done in different ways. For example EIGRP uses a combination of bandwidth, load, reliability and delay. OSPF uses bandwidth while Routing Information Protocol (RIP) uses hop count.

### **2.3.3 Metric Parameters**

Different metrics are used by different routing protocols and on the basis

of the metric used, routing protocols cannot be easily compared. Due to different metrics used, two different protocols may choose different paths to same destination [1].

In IP routing protocols, the following metrics are often used:

- **Hop count:** Counts the number of routers a packet should traverse to reach the destination.
- **Bandwidth:** When used as a metric, the path with highest bandwidth is preferred.
- **Load:** It describes the traffic utilization of a certain link. When load is used as a metric the link with lowest load is the best path.
- **Delay:** It is a measure of the time a packet takes to pass through a path. The best path is selected with the least delay.
- **Reliability:** Calculates the probability of a link failure. Probabilities can be calculated from previous failures or interface error count. Path with highest reliability is chosen as the best path.
- **Cost:** Cost is a value which is decided by the network administrator or Internet Operating System (IOS) to indicate a preferred route. Cost can be represented as a metric, combinations of metrics or a policy.

## 2.4 Hop Count versus Bandwidth

Hop count is defined as the number of routers a packet needs to travel through that path before it arrives at the destination. Each router represents one hop count. Distance vector routing protocols such as RIP use the path with smallest number of hops from multiple paths that exists to reach a destination. Bandwidth is used as metric in many kinds of routing protocols, e.g., OSPF. The path with highest bandwidth value is selected as best path for routing [1]. If we use hop count as the metric, the routers will choose suboptimal routes.

For example, consider Figure 2.1. When the routing protocol uses hop count as a metric, the router R1 will select suboptimal route directly through R2 to arrive at PC2. However, in routing protocol such as OSPF, R1 will choose the shortest path depending on the bandwidth. R1 chooses the link through R3.

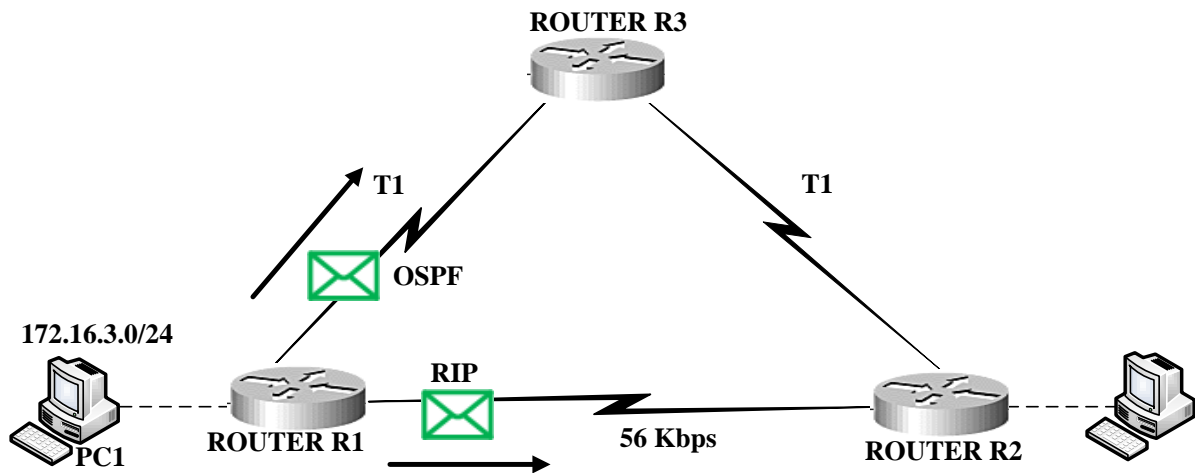


Figure 2.1: Hop Count versus Bandwidth

## 2.5 Administrative Distance

Administrative Distance (AD) describes the rate of trustiness of packet received at the receiver. It is expressed by integers (0 to 255), where 0 means very trusted and, 255 means no traffic flow on the path. AD is used for the purpose of determining which routing source to be used. The routers must determine which routes to be included in the routing table before using that route during forwarding packet.

At the time when the router learns a route about the same network from more than one routing source, the determination of the route used in the routing table is based on the AD of the source routes. The AD with the lowest value

will have precedence as the route source. The most preferred AD is zero and only the directly connected network has zero AD, and it cannot be altered.

## **2.6 Classification**

Routing protocols can be classified as:

- Static and dynamic routing protocols
- Classful and Classless routing protocols
- Distance Vector and Link State routing protocols

## **2.7 Static versus Dynamic Routing**

In static routing, the routing table is constructed manually and routes are fixed at router boot time. The network administrator updates the routing table whenever a new network is added or deleted within the AS. Static routing is used only for small networks. It has bad performance when the network topology changes.

The main advantages of static routing are its simplicity and the fact that it provides more control for the system administrator to control the whole network.

The main disadvantages of static routing are as follows: it is impossible to accommodate rapid network topology changes and it is hard to setup all the routes manually.

In dynamic routing protocols, the routing tables are created automatically in such a way that adjacent routers exchange messages with each other and the best routes are computed using own rules and metrics. The selection of best routes is based on specific metrics such as link cost, bandwidth, number of hops and delay and these values are updated by using protocols which propagate route information.

The main advantage of this type of routing protocols is that it helps the network administrator to overcome the time consumed in configuring and maintaining routes. The drawback of dynamic routing is that it may create diverse problem such as route instabilities and routing loops.

## 2.8 Classful and Classless Routing

Routing protocols can also be divided into *classful* and *classless* routing based upon the subnet mask.

### 2.8.1 Classful Routing

In classful routing, subnet masks are the same throughout the network topology and such a protocol does not send information of the subnet mask in its routing updates. When a router receives a route, it will do the following [8]:

- Routers which are directly connected to the interface of the major network uses the same subnet mask.
- Applies classful subnet mask to the route when the router is not directly connected to interface of the same major network.

Classful routing protocols are not used widely because:

- It does not support Variable Length Subnet Masks VLSM (VLSM) for hierarchical addressing.
- It is not able to include routing updates.
- It cannot be used in sub-netted network.
- It is not able to support discontinuous networks.

Classful routing protocols can still be employed in today's networks but may not be used in all scenarios since they do not include the subnet mask.

Figure 2.2 shows a network using classful routing protocol in which the subnet mask is same throughout the network. RIPv1 and IGRP are examples of routing protocols that belong to the classful routing family of protocols.

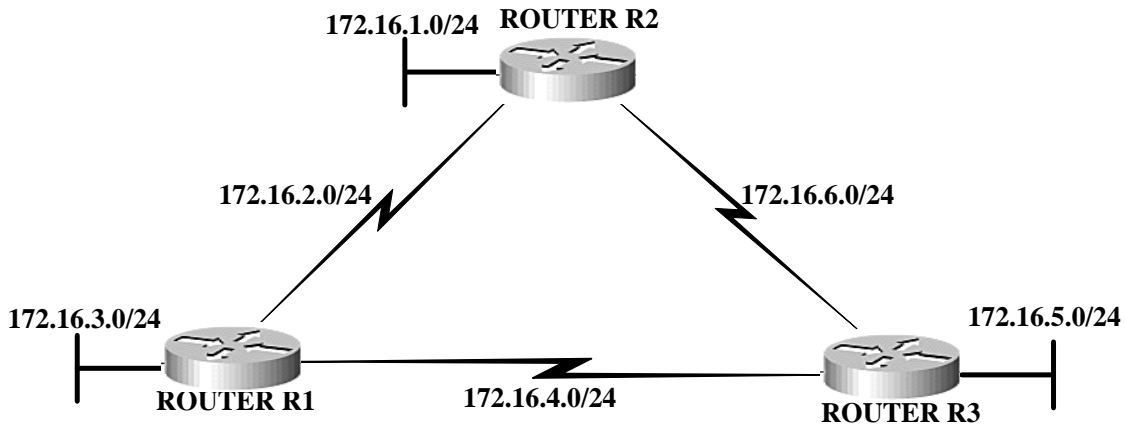


Figure 2.2: Classful Routing with Same Subnet Mask

## 2.8.2 Classless Routing

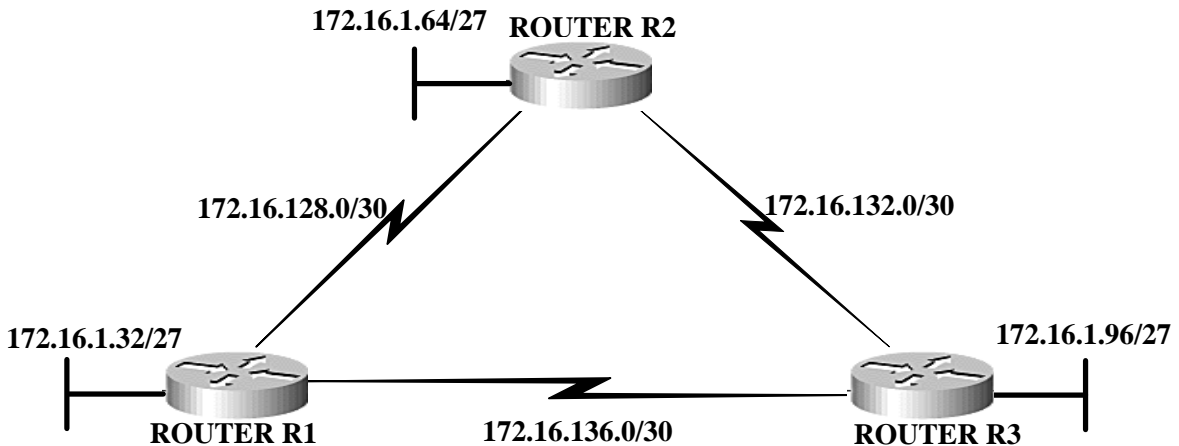


Figure 2.3: Classless Routing with Different Subnet Masks

In classless routing, the subnet mask can vary in network topology and in the routing updates and the subnet mask together with the network address are included. Most networks today are not allocated based on classes and the value of the first octet is not used to determine the subnet mask. Classless routing protocols support discontinuous networks.

Figure 2.3 shows a network using classless routing in which different

subnet mask are used within the same topology. RIPv2, EIGRP, OSPF, IS-IS and BGP are examples that belong to the classless routing family of protocols.

## **2.9 Distance Vector Routing**

As the name indicates, distance vector routing protocol advertise routes as a vector of distance and direction. Here, the distance is represented in terms of hop count metrics and direction is represented by the next hop router or exit interface. DVR is based upon the Bellman Ford algorithm. In DVR, the paths are calculated using the Bellman Ford algorithm where a graph is built in which nodes takes position of the vertices and the links between the nodes takes position of the edges of the graph.

In DVR, each node maintains a distance vector for each destination. The distance vector consists of destination ID, next hop and shortest distance. In this protocol, each node sends a distance vector to its neighbors periodically informing about the shortest paths. Hence, each node discovers routes from its neighboring nodes and then advertises the routes from its own side. For information about the routes each node depends upon its neighbor which in turn depends on their neighboring nodes and so on.

Distance vectors are periodically exchanged by the nodes and the time may vary from 10 to 90 seconds. For every network path, when a node receives the advertisement from its neighbors indicating the lowest-cost, the receiving node adds this entry to its routing table and re-advertise it on its behalf to its neighbors.

### **2.9.1 Methods of Routing**

Distance vector routing protocol is one kind of protocol that uses the Bellman Ford algorithm to identify the best path. Different Distance Vector (DV) routing protocols use different methods to calculate the best network path.

However, the main feature of such algorithms is the same for all DV routing protocols. To identify the best path to any link in a network, the direction and distance are calculated using various route metrics.

EIGRP uses the *diffusion update* algorithm for selecting the cost for reaching a destination. Routing Information Protocol (RIP) uses hop count for selecting the best path and IGRP uses information about delay and availability of bandwidth as information to determine the best path [6].

The main idea behind the DV routing protocol is that the router keeps a list of known routes in a table. During booting, the router initializes the routing table and every entry identifies the destination in a table and assigns the distance to that network. This is measured in hops. In DV, routers do not have information of the entire path to the destination router. Instead, the router has knowledge of only the direction and the interface from where the packets could be forwarded [5].

### **2.9.2 Properties of Distance Vector Routing**

The properties of DV routing protocol include [1]

- DV routing protocol advertise its routing table to all neighbors that are directly connected to it at a regular periodic interval.
- Each routing tables needs to be updated with new information whenever the routes fail or become unavailable.
- DV routing protocols are simple and efficient in smaller networks and require little management.
- DV routing is base on hop counts vector.
- The algorithm of DV is iterative.
- It uses a fixed subnet masks length.

### 2.9.3 Advantages and Disadvantages of DV Routing

DV routing protocol suffers from the problem of count to infinity and Bellman Ford algorithm has a problem of preventing routing loops [4].

The advantages of DV routing protocols are:

- Simple and efficient in smaller networks.
- Easy to configure
- Requires little management.

The main disadvantages of DV routing protocols:

- Results in creating loops.
- Have slow convergence.
- Problems with scalability.
- Lack of metrics variety.
- Being impossible for hierarchical routing.
- Bad performance for large networks.

Few techniques exist to minimize the limitations of DV routing protocols. They are [7]:

#### **Split horizon rule**

It is a one of the methods to eliminate routing loops and increase the convergence speed.

#### **Triggered update**

It uses specific timers and increases the response of the protocol.

## 2.10 Link State Routing

Link State Routing (LSR) protocols are also known as Shortest Path First (SPF) protocol where each router determines the shortest path to each network. In LSR, each router maintains a database which is known as link state database. This database describes the topology of the AS. Exchange of routing

information among the nodes is done through the Link State Advertisements (LSA).

Each LSA of a node contains information of its neighbors and any change (failure or addition of link) in the link of the neighbors of a node is communicated in the AS through LSAs by flooding. When LSAs are received, nodes note the change and the routes are recomputed accordingly and resend through LSAs to its neighbors. Therefore, all nodes have an identical database describing the topology of the networks.

These databases contain information regarding the cost of each link in the network from which a routing table is derived. This routing table describes the destinations a node can forward packets to indicating the cost and the set of paths. Hence, the paths described in the routing table are used to forward all the traffic to the destination.

Dijkstra's algorithm is used to calculate the cost and path for each link. The cost of each link can also be represented as the weight or length of that link and is set by the network operator. By suitably assigning link costs, it is possible to achieve load balancing. If this is accomplished, congested links and inefficient usage of the network resources can be avoided. Hence, for a network operator to change the routing the only way is to change the link cost.

Generally the weights are left to the default values and it is recommended to assign the weight of a link as the inverse of the link's capacity. Since there is no simple way to modify the link weights so as to optimize the routing in the network, finding the link weights is known to be NP-hard. LSR protocols offer greater flexibility but are complex compared to DV protocols. A better decision about routing is made by link state protocols and it also reduces overall broadcast traffic.

The most common types of LSR protocols are OSPF and IS-IS. OSPF uses the link weight to determine the shortest path between nodes. These protocols will be discussed briefly in chapter 4.

### **2.10.1 Methods of Routing**

Every router will accomplish the following process [1].

- Every router learns about directly connected networks to it and its own links.
- Every router must meet its directly connected neighbor networks. This can be done through HELLO packet exchanges.
- Every router needs to send link state packets containing the state of the links connected to it.
- Every router stores the copy of link state packet received from its neighbors.
- Every router has a common view of the network topology and independently determines the best path for that topology.

### **2.10.2 Properties of LSR**

- Each router maintains identical database.
- Converges as fast as the database is updated.
- Possibility of splitting large networks into sub areas.
- Supports multiple paths to destination.
- Each router maintains the full graph by updating itself from other routers.
- Fast non loop convergence.
- Support a precise metrics.

### 2.10.3 Advantages and Disadvantages of LSR

In LSR protocols [4], routers compute routes independently and are not dependent on the computation of intermediate routers. The main advantages of link state routing protocols are:

- React very fast to changes in connectivity.
- The packet size sent in the network is very small.

The main problems of link state routing are:

- Large amounts of memory requirements.
- Much more complex.
- Inefficient under mobility due to link changes.

# CHAPTER 3

## ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

### 3.1 Introduction to EIGRP

Enhanced Interior Gateway Routing Protocols (EIGRP) is a CISCO proprietary protocol and it is an enhancement of the interior gateway routing protocol (IGRP). EIGRP was released in 1992 as a more scalable protocol for medium and large scale networks. It is a widely used interior gateway routing protocol which uses Diffusion Update Algorithm (DUAL) for computation of routes. EIGRP is also known as hybrid protocol because it has the properties of a link state protocol for creating neighbor relationships and of a distance vector routing protocol for advertisement of routes.

### 3.2 EIGRP Protocol Structure

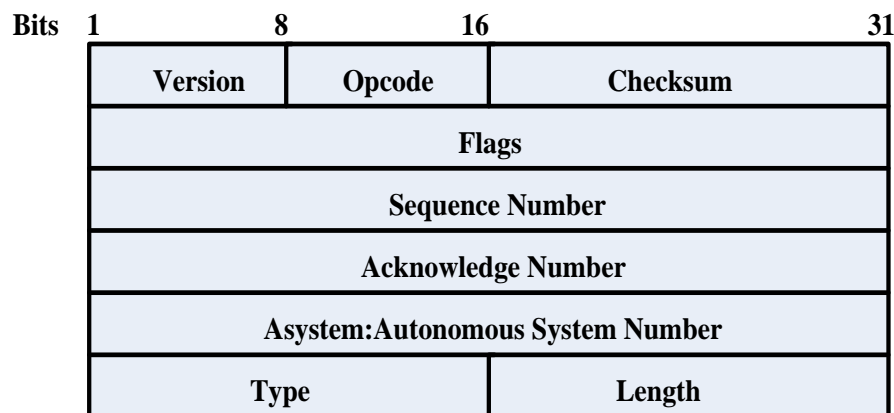


Figure 3.1: Protocol Structure of EIGRP

Figure 3.1 illustrates the protocol structure of EIGRP [1][16].

**Version:** Defines the version of EIGRP

**Opcode:** Message types are specified by the Operation code. Following are the message types.

1. Update
2. Reserved
3. Query
4. Reply
5. HELLO
6. IPX-SAP.

**Checksum:** Defines IP checksum which is computed using the same checksum algorithm as the UDP checksum.

**Flag:** First bit (0x00000001) is the initialization bit and is used in establishing new neighbor relationships. Second bit (0x00000002) is the conditional receive bit and is used in proprietary multicast algorithm. Other bits are not used.

**Sequence and Acknowledge number:** used to send messages reliably.

**Asystem:** It describes the autonomous system number of the EIGRP domain. Since a gateway can participate in more than one AS, separate routing tables are associated with each AS. This field is used to indicate which routing table to be used.

**Type:** Defines the value in the type field.

- 0x0001-EIGRP Parameters (Hello/hold time)
- 0x0002-Reserved
- 0x0003-Sequence
- 0x0004-Software Version of EIGRP
- 0x0005-Next Multicast Sequence
- 0x0012-IP Internal Routes
- 0x0013-IP External Routes

**Length:** Describes the length of the frame.

### 3.3 Components of EIGRP

There are four components of EIGRP:

- Neighbor Discovery/Recovery
- Reliable transport protocol (RTP)
- Diffusion Update Algorithm (DUAL)
- Protocol Dependent Modules (PDM)

#### 3.3.1 Neighbour Discovery/Recovery

The neighbor discovery/recovery method permits the routers to dynamically gain knowledge about other routers directly connected to their networks [10] [11]. When the neighbors become inoperative or unreachable they should be able to discover it. This can be achieved with a relatively low overhead by sending HELLO packets periodically.

When a router receives a HELLO packet from its neighboring routers it assumes that its neighboring router is alive and exchange of routing information can be done. In high speed networks the default HELLO time is 5 s. Each HELLO packet advertises a hold time so as to keep the relationship alive. *Hold time* is defined as the time the neighbor should consider the sender as alive.

The default hold time is 15 s. If in the hold time interval the EIGRP router does not receive any HELLO packets from the neighboring router then the neighbor is discarded from the routing table.

Thus, hold time is also used to detect the loss of neighbors in addition to the discovery of neighbors. HELLO/hold time for networks on multipoint interfaces with link speed T-1 or less is set to 60/180 seconds [12].

The HELLO interval time can be lengthened but the convergence time also gets lengthened. However, long HELLO intervals can be implemented in

congested networks where there are many EIGRP routers. In a network, the HELLO/hold time may not be the same for all routers. A rule of thumb is that the hold time should be thrice the HELLO time [13]. Table 3.1 shows the default values of HELLO and hold times for EIGRP [1].

**TABLE 3.1: EIGRP INTERVAL TIME FOR HELLO AND HOLD**

Bandwidth	Example Link	Hello Interval Default Value	Hold Interval Default Value
1.544 Mbps or slower	Multipoint Frame Relay	60 seconds	180 seconds
> 1.544 Mbps	T1,Ethernet	5 seconds	15 seconds

### 3.3.2 Reliable Transport Protocol

To provide guaranteed, ordered delivery of EIGRP packets to all the neighbors in the network EIGRP uses Reliable Transport Protocol (RTP). The routing update information transmitted is sorted in series by using the sequence number. RTP supports intermixed transmission of multicast or unicast packets [10] [11] [15]. Certain EIGRP packets are required to be transmitted reliably whereas others do not [15]. Hence reliability is provided only when needed.

For example in Ethernet, which is a multi access network and has the capacity of multicasting, it is not necessary to send HELLOs reliably to all the neighbors. So, when EIGRP sends a single multicast HELLO it informs the receivers by indicating in the packet that the packet received need not be acknowledged. When update packets are sent, they need to be acknowledged and hence this is indicated in the packet [15]. When there are unacknowledged packets pending, RTP has a provision to send the multicast packet very fast. Hence, in presence of varying speed links this helps to ensure that convergence time remains low.

### 3.3.3 Diffusion Update Algorithm

The Diffusion Update Algorithm (DUAL) uses some terms and concepts which play an important role in loop-avoidance mechanism:

➤ **Reported Distance (RD)**

The cost to reach the destination by a router is known as reported distance.

➤ **Feasible Distance (FD)**

The lowest cost to reach the destination is referred to as the feasible distance for that destination.

➤ **Successor**

A Successor is a neighboring router and represents the least-cost route to the destination network.

➤ **Feasible Condition (FC)**

FC is used to select the feasible successor if the FD is met. The condition is that the RD advertised by a router to a destination should be less than the FD to the same destination.

➤ **Feasible Successor (FS)**

FS is a neighboring router which provides a loop free backup path to the destination as the successor by satisfying the FC.

In EIGRP all route computations are handled by DUAL. One of the tasks of DUAL includes maintaining a table which is referred to as topology table and which contains all the entries of loop-free paths to every destination advertised by all routers. DUAL uses the distance information as a metric to select the best loop-free path known as successor path and a second best loop free path known as feasible path from the topology table and save this into the routing table. The neighbor which has a least cost route to the destination is known as successor.

When the successor path is unreachable, DUAL uses the topology table to check whether another best loop-free path is available. This path is known as feasible path. The feasible path is chosen if it meets the FC. When the neighbor's RD to a network is less than the local router's RD then the FC condition is met by the neighboring router. If a neighbor satisfies the FC then it is known as FS.

If there is no loop-free path in the topology table, re-computation of the route must occur, during which DUAL queries its neighbors, who in turn query their neighbors and so forth [13]. This is the time when the re-computation occurs in search of a new successor. Although the re-computation of the route is not processor-intensive it may affect the convergence time and therefore it is beneficial to avoid unnecessary computations [10][11][15]. If there are any FS, DUAL uses it in order to avoid any unnecessary re-computation. To illustrate how DUAL converges, consider Figure 3.2. This example focuses on router K as a destination only. The cost to K (in hops) from each router is shown.

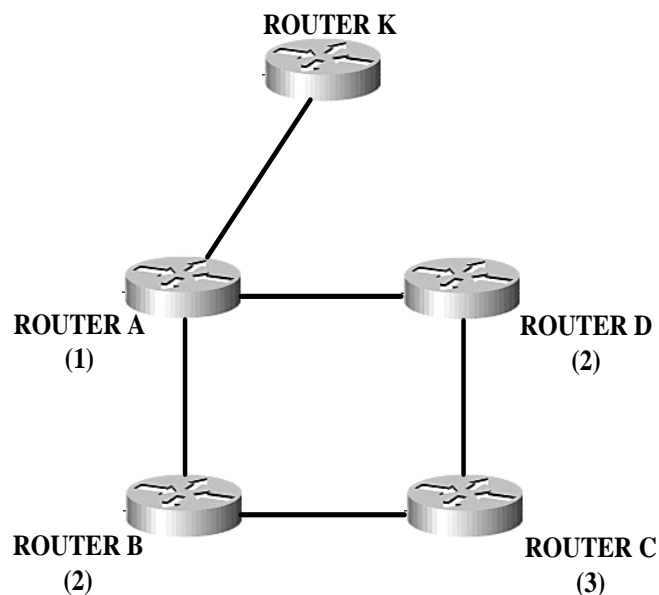


Figure 3.2: Network Topology for DUAL.

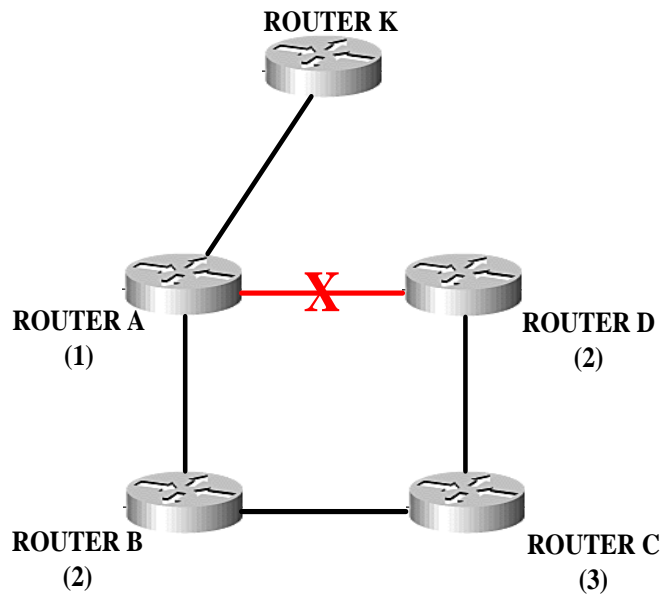


Figure 3.3: Network Topology with Failed Link.

Assume that the link between A and D fails, as shown in Figure 3.3. D sends a query to its neighbors informing about the loss of the FS. The query is received by C and determines if there are any FS. If no FS exist, then C has to start a new route computation and enters active state. However, the FS to router K is router B because the cost to destination router K from router C is 3 and it is 2 from router B. Therefore C can switch to B as its successor. Router A and B were unaffected by this change and hence they did not participate in finding the feasible successor.

Consider a case in which the link between A and B fails. This scenario is shown in Figure 3.4. In this scenario B determines that it has lost its successor and no other FS exist. Router C cannot be considered as FS to B because the cost of C, 3 to destination K, is greater than the current cost of B which is 2. As a result, B needs to perform route computation. A query is sent from B to its only neighbor C. C replies to the query, because its successor has not changed and C does not require performing route computation.

When the reply is received by B, it knows that all the neighbors have processed the link failure to K. To reach destination K, B can choose C as its successor with cost 4. The topology change has not affected A and D and C needed to simply reply to B.

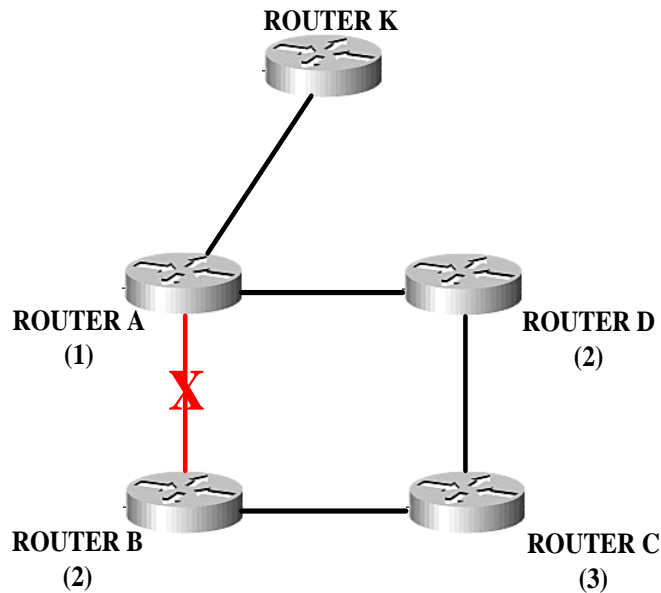


Figure 3.4: Network Topology with Failed Link.

### 3.3.4 Protocol Dependent Modules

EIGRP uses Protocol Dependent Module (PDM) to support different network layer protocols [4]. So, EIGRP supports Internet Packet Exchange (IPX) and Apple Talk. For example, for sending and receiving *EIGRP Packets* encapsulated in IP is the responsibility of the IP-EIGRP module.

Other responsibilities of the IP-EIGRP include redistributing routes learned by other routing protocols, parsing *EIGRP Packets*, informing DUAL of the new information received, asking DUAL to take routing decisions [10][11][15].

### 3.4 EIGRP Metrics

In EIGRP, to determine routing metrics, the total delay and the minimum link bandwidth are used. In EIGRP, composite metrics that can be used to calculate the preferred path to the networks consists of bandwidth, delay, reliability and load. Hop count is included in the routing update of EIGRP. However, EIGRP does not use hop count as part of composite metrics.

The minimum bandwidth and the total delay metrics can be obtained from values configured on interfaces in the path to the destination network of the routers. The formula used to calculate the metric is given by [12]

$$256 * \left[ \left( K_1 * Bw + \frac{K_2 * Bw}{256 - Load} + K_3 * Delay \right) * \frac{K_5}{K_4 + Reliability} \right] \quad (1)$$

The default values for weights are

$$K_1 = 1, K_2 = 0, K_3 = 1, K_4 = 0, K_5 = 0$$

Substituting above values in equation 1, the default formula for EIGRP metric becomes

$$256 * (Bw + Delay) \quad (2)$$

If  $K_5$  is zero, the term  $(K_5 / (K_4 + Reliability))$  is completely ignored.

The formula used by EIGRP to calculate scale bandwidth is given by

$$Bw = \left( \frac{10000000}{B(n)} \right) * 256 \quad (3)$$

Where  $B(n)$  is in kilobits and represents the minimum bandwidth on the interface to destination.

$Bw$  = bandwidth

The formula used by EIGRP to calculate scale delay is given by

$$Delay = D(n) * 256 \quad (4)$$

Where  $D(n)$  is in tens of microseconds and represents the sum of delays configured on the interface to destination.

### 3.5 EIGRP Convergence

Consider the network in Figure 3.5 running EIGRP. Assume that the link between R4 and R6 fails and R4 detects the link failure. No FS exists in its topology database and R4 enters into active convergence. R5 and R3 are the only neighbors to R4 and since there is no route with lower FD available, R4 sends a query to R5 and R3 to get a logical successor. R3 replies to R4 indicating that there is no successor available. R5 replies to R4 indicating FS is available with higher FD. The new path and distance is accepted by R4 and added in its routing table. R4 sends an update to R3 and R5 about the higher metric. This update is sent to all the routers in the network and all the routes converge.

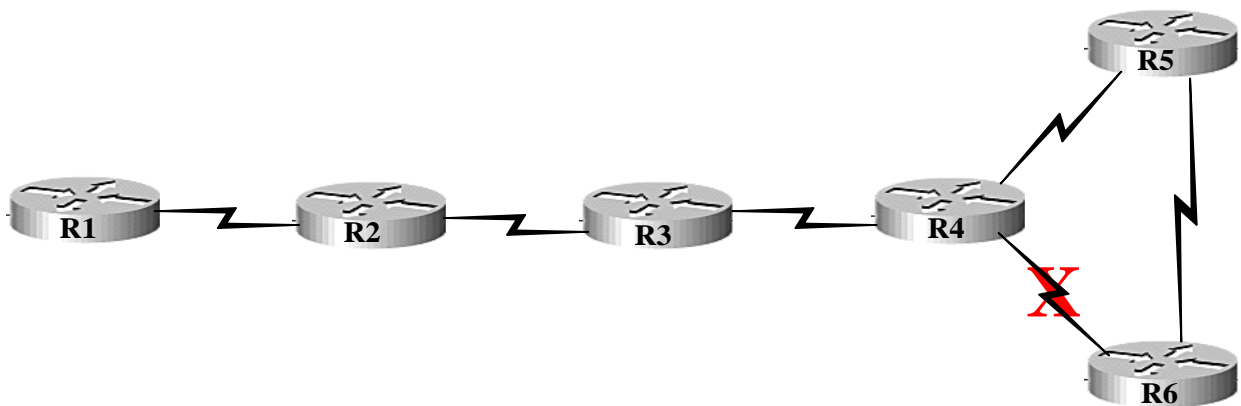


Figure 3.5: Network using EIGRP.

### 3.6 Advantages and Drawbacks of EIGRP

EIGRP provides the following advantages

- Loop free routes are provided.

## **MEE09:77**

- It additionally saves a back up path to reach the destination.
- Multiple network layer protocols are supported
- Convergence time for EIGRP is low which in turn reduces the bandwidth utilization.
- Supports VLSM, discontinuous network and classless routing.
- Routing update authentication is supported by EIGRP.
- Topology table is maintained instead of the routing table and consist of best path and an addition loop free path.

Drawbacks of EIGRP are

- It's a Cisco proprietary routing protocol.
- Routers from other vendors cannot utilize EIGRP.



# CHAPTER 4

## OPEN SHORTEST PATH FIRST

### 4.1 Introduction to OSPF

Open Shortest Path first (OSPF) is a link state routing protocol that was initially developed in 1987 by Internet Engineering Task Force (IETF) working group of OSPF [17]. In RFC 1131, the OSPFv1 specification was published in 1989. The second version of OSPF was released in 1998 and published in RFC 2328 [18]. The third version of OSPF was published in 1999 and mainly aimed to support IPv6.

### 4.2 OSPF Protocol Structure

Figure 4.1 represents the OSPF protocol structure [1] [19] [21].

**Version:** Describes the OSPF version. The current version used is 2.

**Type:** This field indicates type of OSPF packet. Five types of OSPF packets exist:

- HELLO
- Database Description (DBD)
- Link-state request (LSR)
- Link-state update (LSU)
- Link-state acknowledgement (LSAck).

**Packet Length:** Describes the length of the OSPF packet in bytes including the OSPF header.

**Router ID:** This field is used to identify the router throughout the AS.

**Area ID:** This field indicates the area to which the packet belongs. Areas can be written in two ways: Area 1, or Area 0.0.0.1.

**Checksum:** This field checks whether the contents of the packet are damaged or not due to transmission.

**Au Type:** Defines the authentication type to be used. Three values are defined.

- 0- No authentication
- 1- Simple Authentication containing plain text
- 2- Cryptographic Authentication using MD5 (Message Digest) algorithm.

**Authentication:** This 64 bit field contains authentication information. If Au type 1 is used, this field contains authentication key. If Au type 2 is used, this field is redefined into several other parameters.

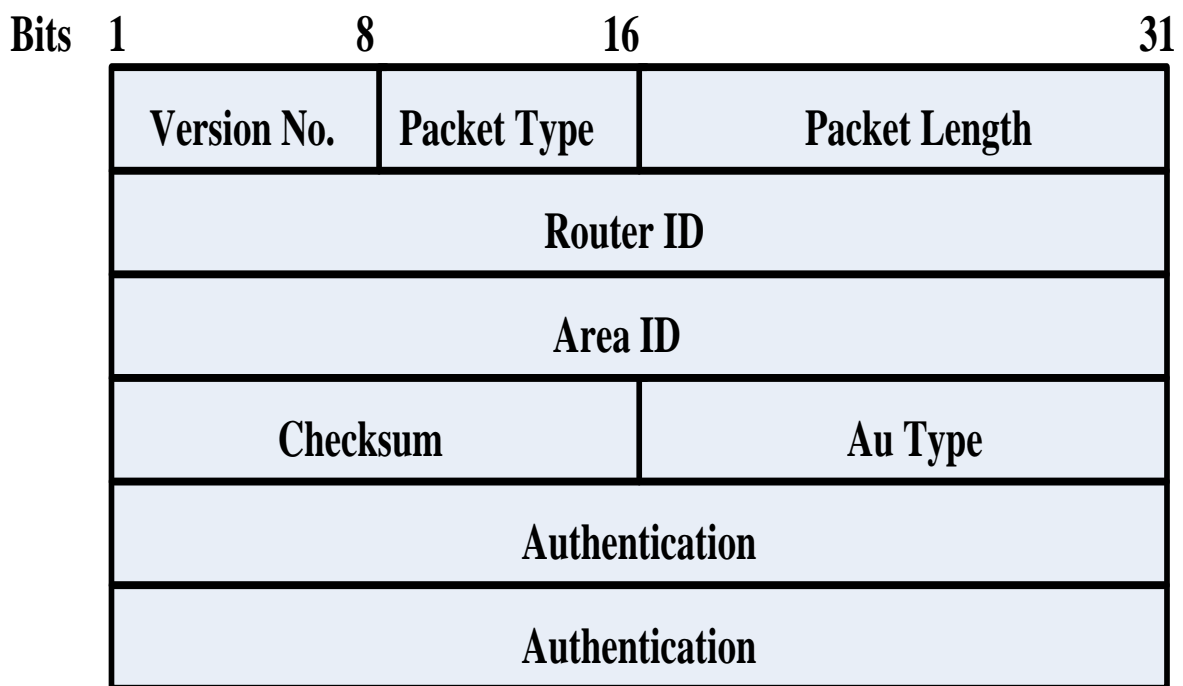


Figure 4.1: Protocol Structure of OSPF

### 4.3 OSPF Packet Types

There are five different types of OSPF LSPs [1] [22]. Each packet provides a specific purpose in the OSPF routing process. The five OSPF packet

types are

## 1. HELLO Packet

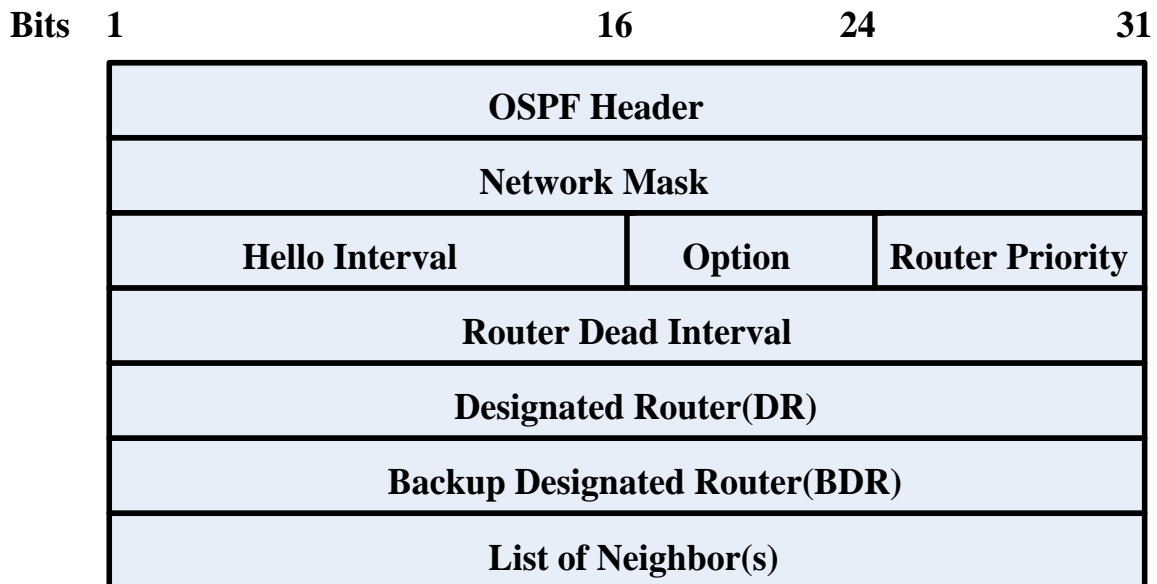


Figure 4.2: HELLO Packet

To set up and maintain adjacency with other OSPF routers, HELLO packets are used. In scenarios that consist of broadcast/non-broadcast media, HELLO packets are utilized to choose the designated router (DR) and backup designated routers (BDR).

Figure 4.2 illustrates the HELLO packet format.

**Subnet mask:** This field indicates the associated subnet mask with the sending interfaces.

**Hello Interval:** Represents the number of seconds between two consecutive HELLO packets. To form adjacency this interval should be the same for both routers. For point to point and broadcast media, the HELLO interval is 10 s and 30 s for other media types.

**Options:** Defines the optional capabilities the router can support.

**Router Priority:** Indicates router's priority. This field is used in selecting the

DR/BDR. If a router has a higher priority the router may become DR.

**Router Dead Interval:** Defines the time to declare a neighbor as dead. The default dead interval is set to 4 times the HELLO interval.

**Designated Router:** Lists the router ID of the DR. If there is no DR, this value is set to 0.0.0.0.

**Backup Designated Router:** recognizes the BDR and lists the IP interface address of BDR. If BDR doesn't exist this value is set to 0.0.0.0.

**List of Neighbors:** Contains lists of OSPF router IDs of the neighboring router(s).

## 2. Database Description Packet

Exchange of routing database information is done through DBD packets. These packets include an abbreviated list of the sending router's link-state database used by the receiving routers to check against the local link-state database.

## 3. Link State Request Packet

The receiving routers can request more information about any entry in the DBD by sending a LSR. By sending the LSR packet the database information missing can be retrieved. LSR packets can also be used to request the LSAs seen during the DBD exchange.

## 4. Link-State Update Packet

To announce new information and reply to LSRs, LSU packets are used. Seven different types of LSA are included in LSUs, as shown in Table 4.1.

## 5. Link-State Acknowledgement Packet

These packets are utilized to acknowledge each LSA. A router sends an LSAck as a confirmation receipt of the LSU received. In a single LSAck packet multiple LSAs can be acknowledged.

TABLE 4.1: DIFFERENT LSAS

<b>LSA Type</b>	<b>Description</b>
<b>1</b>	<b>Router LSAs</b>
<b>2</b>	<b>Network LSAs</b>
<b>3 or 4</b>	<b>Summary LSAs</b>
<b>5</b>	<b>Autonomous System External LSAs</b>
<b>6</b>	<b>Multicast OSPF LSAs</b>
<b>7</b>	<b>Defined for Not-So-Stubby Areas</b>

## 4.4 OSPF Areas

Two levels of hierarchy are provided by OSPF throughout the concept of Areas [1]. An Area is a 32-bit number denoted in an IP address format 0.0.0.0 or in decimal number format like Area 0. If there is more than one Area used in the network, Area 0 is assigned to the backbone of the network. All other Areas should be connected to the backbone.

If the Areas cannot be connected to the backbone then, with the help of virtual links, that Area should be connected to the backbone. Depending upon the requirements of the network, OSPF has several types of Areas [1] [21]. These are

### 4.4.1 Normal Area

Areas defined by default are known as normal or regular Area. Following features are associated with normal Areas [22].

- Summary LSAs which belongs to other Areas can be inserted.
- External LSAs can be inserted.
- External default LSAs can be inserted.

In Figure 4.3 Area 1 and Area 2 are normal Areas. RIP routes are redistributed into Area 1 and IGRP routes are redistributed into Area 2.

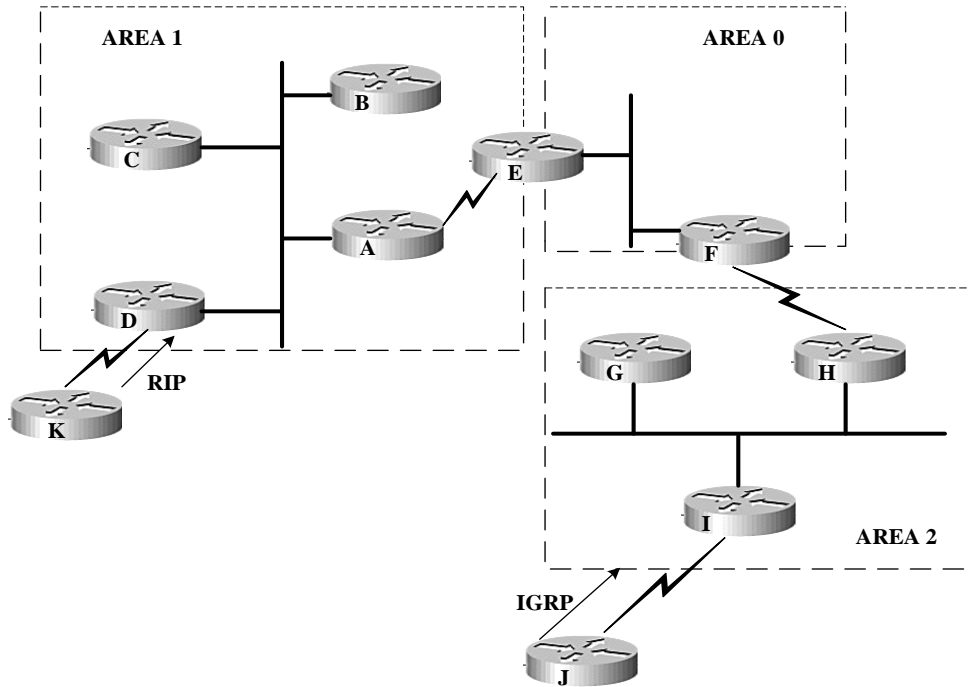


Figure 4.3: Normal Area.

#### 4.4.2 Stub Area

Areas which do not receive route advertisements and are external to the AS are known as stub Areas. Following features are associated with Stub Areas [20].

- Summary LSAs which belong to other Areas can be inserted.
- As a summary route, default route is inserted into the stub Area.
- External LSAs cannot be inserted.

By configuring a stub Area, the advantage is that the size of the LSDB is decreased along with the routing table while for processing LSAs, fewer CPU cycles are utilized. If any router desires to access the network outside its area, the router sends the packets to the backbone area.

In Figure 4.4, Area 2 is defined as stub Area in which no external LSAs can be injected. RIP routes which are inserted at router D are blocked at router F. However, summary routes created for Area 1 are still received by Area 2 through router F. Through router F a default summary route is also injected into Area 1 which means that the routers in Area 1 can send packets to the external Areas through router F.

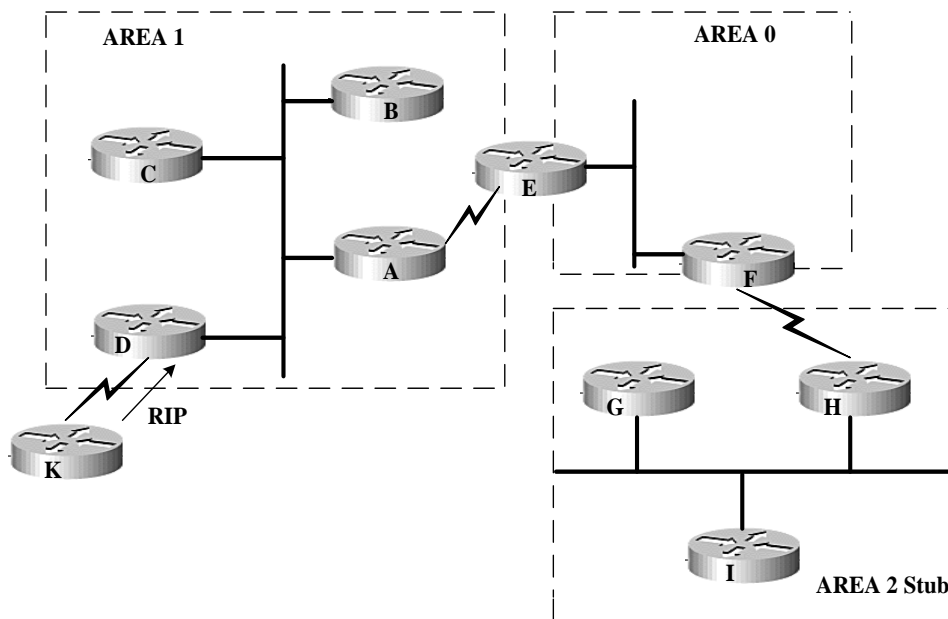


Figure 4.4: Stub Area.

### 4.4.3 Totally Stubby Area

This type of Area is the most restricted form of Areas in OSPF. Routers belonging to this type of Area depend only on the default summary route injected by the ABR. Features of Totally Stubby Areas are [22]

- External LSAs are not allowed.
- Summary LSAs are not allowed.
- As a default route a summary route is inserted.

#### 4.4.4 Not-So-Stubby Area

This is an extension of stub Area. If Area 2 is defined as stub Area and a situation arises where IGRP routes needs to be redistributed then it is not possible to insert the IGRP routes. To insert the IGRP routes into Area 2, Area 2 has to be changed to NSSA. When this change occurs i.e., when Area 2 is named as NSSA, IGRP routes can be redistributed into this Area as type 7 LSAs.

NSSA have the following characteristics [22].

- Within an NSSA Type 7 LSAs carry external information.
- At NSSA ABR Type 7 LSAs are converted into Type 5 LSAs.
- Summary LSAs are inserted.
- External LSAs are not allowed.

When Area 2 is named as NSSA following properties hold [22]

- LSAs of Type 5 are not permitted into Area 2 meaning that no RIP routes are allowed to enter into Area 2.
- Routes associated with IGRP are redistributed as Type 7 routes. Only within NSSA these routes exist.
- All the routes of Type 7 are converted into Type 5 by NSSA ABR and disclosed into OSPF domain as a Type 5 route.

#### 4.4.5 Totally Not-So-Stubby Area

This Area is an extension of NSSA. If exists only one point of exit, this type of Area is the most recommended form of NSSA. The features of Totally NSSA are

- External LSAs are not allowed.
- Summary LSAs are not allowed.
- As a summary route default route is inserted.

- At the NSSA ABR Type 7 LSAs are converted into Type 5 LSAs.

In Figure 4.5 Area 2 is a totally NSSA, then following are true [22].

- RIP routes which are external routes cannot be injected into Area 2.
- By the definition of NSSA no summary LSAs of other Areas can be inserted into Area 2.
- ABR generates the default summary LSA. In Figure 4.5, router F is the ABR.

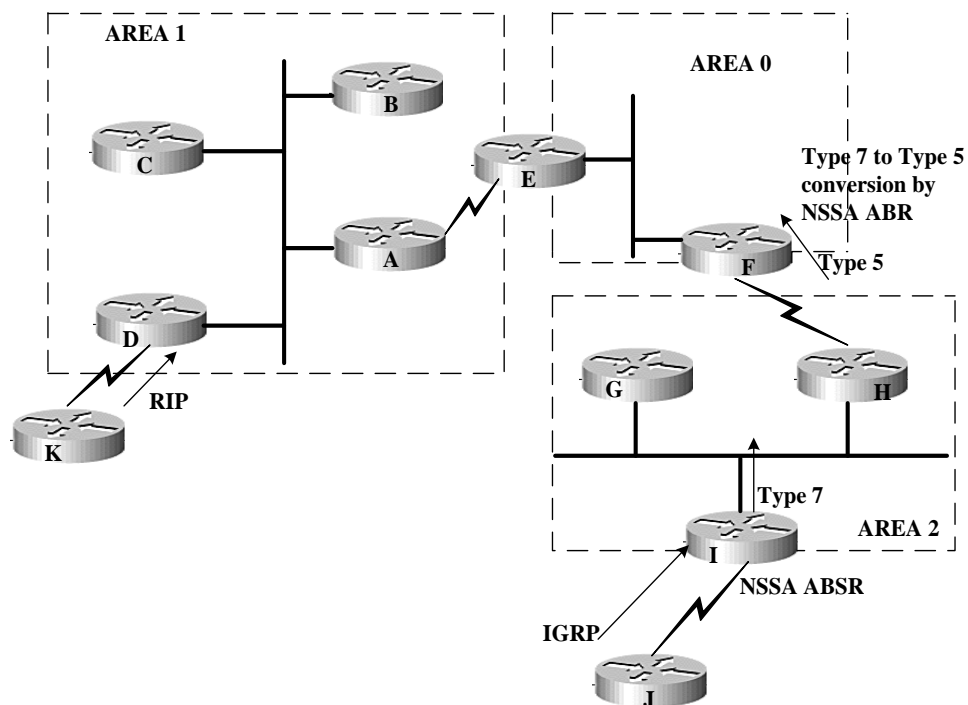


Figure 4.5: Totally Not-So-Stubby Area.

## 4.5 OSPF Router Types

The following router types are defined in OSPF. They are [23] [24]

- **Internal Router (IR)**

IR resides within an Area. An IR has all its directly connected neighbors in the same Area. Only one copy of OSPF algorithm is run in the IR and is concerned with the LSDB that belong to their Area only.

➤ **Area Border Router (ABR)**

These routers connect to more than one Area and also to the backbone Area. ABR acts as member to all the Areas it is connected to. Multiple copies of the OSPF algorithm are run with one copy containing a database for each Area they are connected and one copy for the AS backbone. Summary link advertisements are sent and received by ABR from the backbone Area.

➤ **Backbone Router (BR)**

Routers which have the interface to the OSPF backbone are known as backbone routers. Backbone routers can be ABR or internal routers of the backbone area.

➤ **Autonomous System Boundary Router (ASBR)**

To connect more than one AS, ASBR are used for the exchange of information to other routers belonging to other AS. A path is maintained by each router in the AS to the ASBR. ABR or IR can be ASBR and may share or not the backbone.

## 4.6 OSPF Metrics

The metric used for OSPF is known as cost and is associated with the output interface of the router. The interface with the lower cost has a better chance to be used to forward traffic. Cisco IOS software uses cumulative bandwidth at each router to calculate the cost using the following formula [1].

$$Cost = \frac{10^8}{Bandwidth\ in\ Bps} \text{ ----- (5)}$$

The value  $10^8$  which is 100,000,000 bps is called reference bandwidth. When the reference bandwidth is divided by the interface bandwidth will give the cost. From the formula, it can be seen that the link with the higher

bandwidth will have a lower cost so that it is more likely the interface is to be preferred to forward traffic.

## 4.7 OSPF Convergence

Consider the network in Figure 4.6 running OSPF. Assume the link between R4 and R6 fails. R4 detects link failure and sends LSA to R3 and R5. Since a change in the network is detected traffic forwarding is suspended. R3 and R5 updates their topology database; copies the LSA and flood their neighbors.

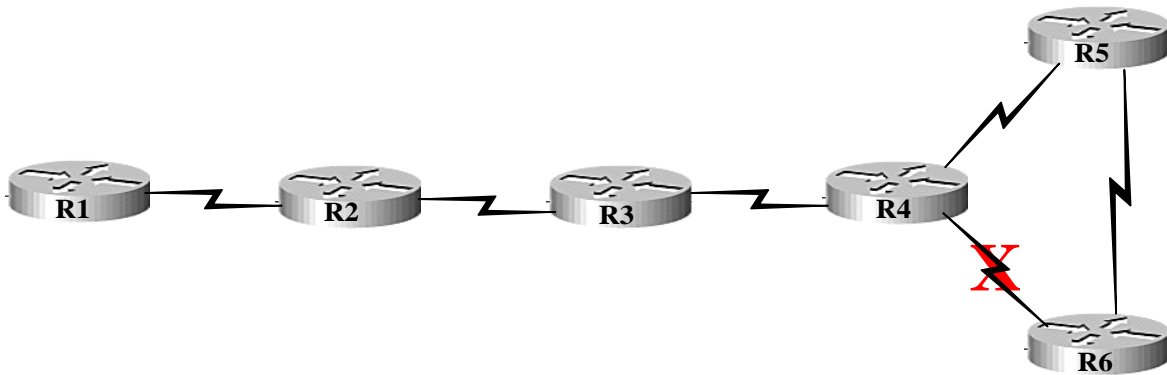


Figure 4.6: Network using OSPF.

By flooding LSA all the devices in the network have topological awareness. A new routing table is generated by all the routers by running Dijkstra's algorithm. The traffic is now forwarded via R5.

## 4.8 Characteristics of OSPF

Following characteristics are associated with OSPF [24].

- OSPF provides load balancing by distributing traffic through multiple routes to a given destination [24].
- OSPF provides partition of networks and routers into Areas make thus the network easier to manage. All routers belonging to the same Area

will have an identical database and calculation is performed separately for each Area. Database information of an Area consists of advertisements of router link, AS, summary links and network links.

- For OSPF Area mapping, Area can be networks, subnets or combination of networks and subnets. Dividing into Areas limits the explosion of link state updates in the whole network and helps to avoid unnecessary propagation of subnet information.
- It allows maximum flexibility and provides transfer and tagging of external routes injected into AS.
- It helps exchange information obtained from external sites.
- Runs directly over IP.
- Provides authenticated routing updates using different methods of authentication.
- It has low bandwidth utilization and ensures less processing burden on routers because updates are only sent when changes occur.

## **4.9 Protocols within OSPF**

The protocols within OSPF are common header HELLO protocol, exchange protocol, flooding protocol and aging link state record [1] [21].

### **4.9.1 The HELLO Protocol**

The HELLO protocol enables every machine to compute the shortest cost paths to the destination network. The messages set up relationship among adjacencies and exchange key parameters about how OSPF is used within AS. HELLO packets help do the following tasks [1].

- Identify OSPF neighbors and establish neighbor adjacencies.
- Advertise parameters so that two routers must agree to become neighbors.

- Elect the DR and BDR.

### **4.9.2 The Exchange Protocol**

The exchange protocol uses database description packets. It is asymmetric, i.e., it is a master-slave protocol in which the master sends database description packets and the slave sends the acknowledgements. Exchange protocol consists of request records to send in case of the sequence number of the link state is smaller and the other router will answer with a link state update.

### **4.9.3 The Flooding Protocol**

When the link state changes, a router responsible for that link assigns a new update of the link state and the new version is retransmitted at regular intervals until an acknowledgment is received.

### **4.9.4 The Aging Link State Record**

In link state routing, old records are required to be avoided from the link state database and the procedures must be synchronized. In order to do this, the age is set to 0 when the record is issued and incremented in each hop by 1 every second. When it reaches “maxAge” the router will remove it and the neighbors needs to be informed about this [21].

## **4.10 OSPF General Operation**

As any routing protocol, OSPF is used to assist the exchange of routing information between routers in AS. OSPF protocol operation follows the following stages [19] [20].

Consider Figure 4.7 representing a simple AS. A unitless cost metric is assigned at each router interface as an indication of the preference of using that

interface. This indication can be delay, bandwidth or reliability factors assigned by the network administrator.

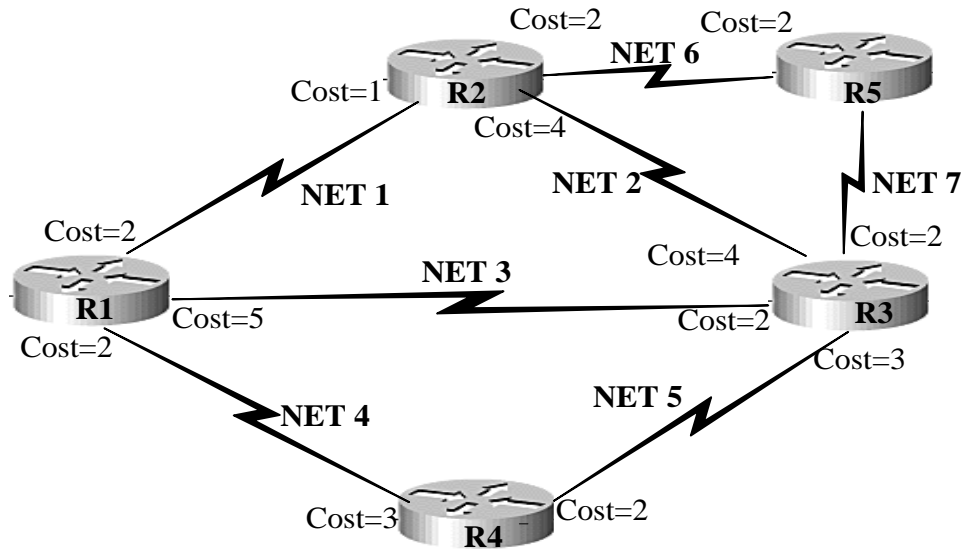


Figure 4.7: AS with Link State Information.

➤ **Link state database (LSDB) compiling**

OSPF routers are required to receive a valid LSA from other routers in order to create LSDB. Initially, each router will send an LSA that contains its own configuration. As the router receives LSAs from other routers, it transfers those LSAs to its neighboring routers. After convergence, each router in the AS has an LSA from all other routers [19]. Each router in the AS in Figure 4.7 has the LSDB shown in Table 4.2.

TABLE 4.2: LINK STATE DATABASE

Router	Attached Networks and Costs
R1	NET 1 - COST 2, NET3 - COST 5, NET 4 - COST 2
R2	NET 1 – COST1, NET2 - COST 4, NET 6 - COST 2
R3	NET 2 – COST4, NET3 - COST 2, NET 5 - COST 3,NET 7-COST2
R4	NET 4 – COST3, NET5 - COST 2
R5	NET 6 – COST2, NET7 – COST 3

➤ Shortest Path first (SPF) calculation

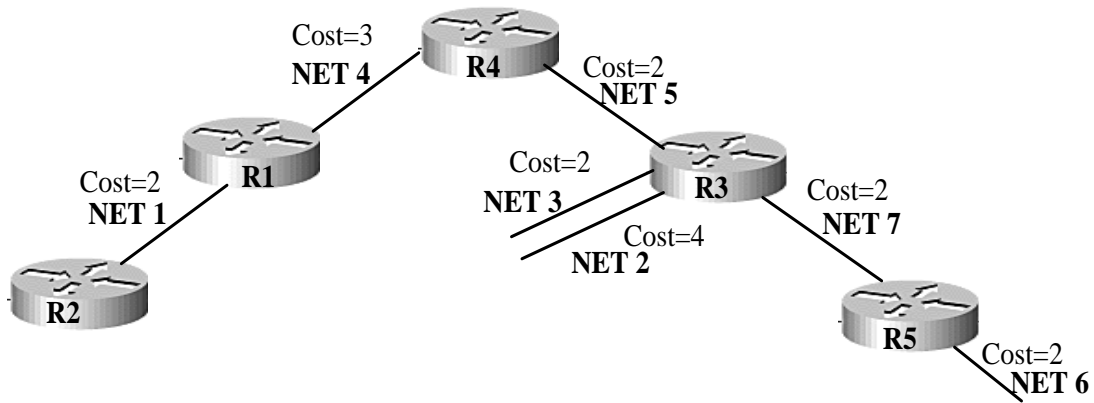


Figure 4.8: Shortest Path First Tree Performed at R4.

After the LSDB is compiled, least cost calculation is performed by every OSPF router using Dijkstra’s algorithm [19]. The SPF tree contains a least cost path of each router and network in AS. Figure 4.8 represents SPF tree performed by Router R4.

➤ Routing table entries creation

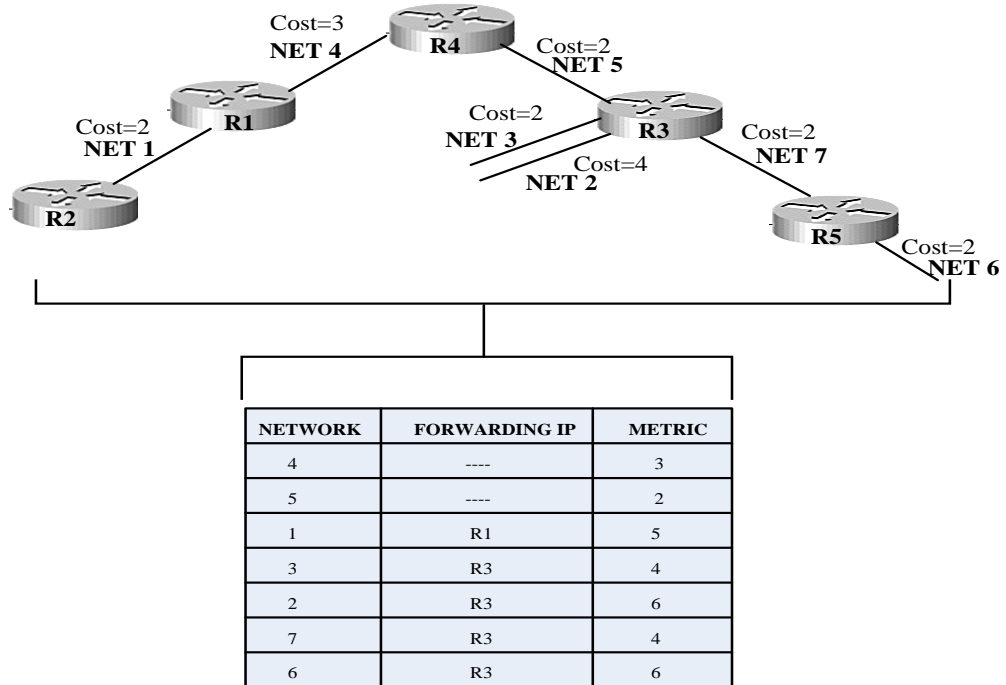


Figure 4.9: Routing Table Entries.

SPF tree is used to create the OSPF routing table entries [19]. A single entry for every network is created in the AS from the SPF tree. The SPF is analyzed and results in a series of OSPF routes containing the destination IP and its network mask. The routing table entries for the AS shown in Figure 4.7 are created using the SPF tree represented in Figure 4.8. Figure 4.9 illustrates the routing table created from the SPF tree.

## **4.11 Advantages and Drawbacks of OSPF**

The advantages of OSPF are

- OSPF is not a proprietary protocol.
- Fast and loop less convergence
- Low bandwidth utilization
- Precise metrics are supported and if needed multiple metrics can be used.
- Multiple paths are supported.
- External routes are represented separately.
- No hop count limit.
- Supports VLSM.
- Supports larger networks.

Drawbacks of OSPF are

- Complex to configure
- Memory overhead. To keep track of all Areas and networks connected within an Area OSPF utilizes link-state databases. These LSDB may become large if the topology is complex which may result in the reduction of the maximum size of an Area.

**MEE09:77**

- Processing overhead is high when topology changes occur. This is due to the fact that all routing information needs to be flooded. Furthermore, recalculation of the routes needs also to be performed.



# CHAPTER 5

## INTERMEDIATE SYSTEM to INTERMEDIATE SYSTEM

### 5.1 Introduction

Intermediate system to Intermediate system (IS-IS) is a link state routing protocol introduced by ISO [25]. To exchange routing information, IS-IS routers calculate the cost for the route based on a single metric. IS-IS routing protocol is very similar to OSPF.

IS-IS is designed to provide intra domain routing or routing within an area. IS-IS network includes end systems, intermediate system, areas and domains. In IS-IS network, routers are intermediate systems organized into local groups known as areas. Several area are grouped together to form domains. User devices are End systems.

IS-IS and OSPF are link state routing protocols that can be used for larger networks. IS-IS uses Dijkstra algorithm to determine the shortest path and utilizes a link state database to route packets between intermediate systems. IS-IS usually use two level hierarchical routing in which a level 1 router can identify the topology in the area including every router and host. However, a level 1 router cannot know the identity of routers outside their area. Level 1 routers of are similar to OSPF intra area routers since it has no connections outside.

Level 2 routers are not required to identify the topology within level 1 area but there is a possibility that a level 2 router can be a level 1 router in a single area. Level 2 of IS-IS is similar to OSPF Area 0 that comprises the backbone Area in order to connect different areas.

HELLO packets are used to establish adjacencies on point to point and point to multipoint links of neighboring routers. On broadcast multi-access media, IS-IS routers use a Designated Intermediate System (DIS) to flood the information.

## 5.2 IS-IS Protocol Structure

Figure 5.1 represents the protocol structure of IS-IS [26].

**Intradomain routing protocol discriminator:** This field indicates network layer protocol identifier given to IS-IS protocol

**Length indicator:** describes the fixed header length in octets.

**Version/protocol ID extension:** set to 1.

**ID length:** defines the length of field and NETs used in the routing domain.

**R** is reserved bit

**PDU:** describes the type of PDU, bits 6, 7 and 8 are reserved.

**Version:** set to 1.

**Maximum area addresses:** This field indicates the number of area addresses allowed.

IS-IS has two kinds of addresses

- Network Service Access Point (NSAP): NSAP addresses discover network layer services.
- Network Entity Title (NET): NET addresses discover network layer entities or processes rather than services.
- There is a possibility that devices have more than one type of addresses, but NET's and the system ID portion of the NSAP must be unique for each system.

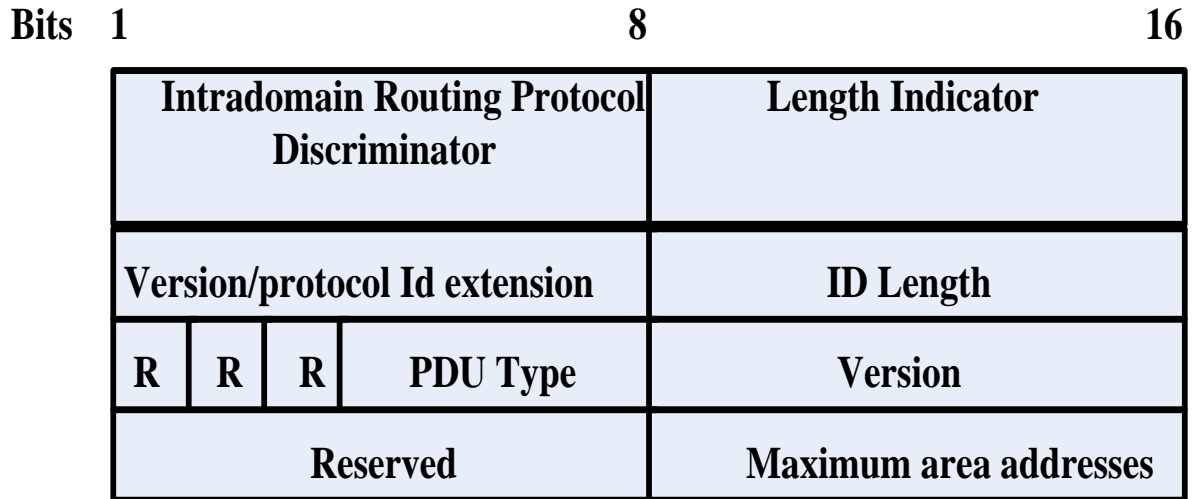


Figure 5.1: IS-IS Protocol Structure

### 5.3 IS-IS Packet Types

Four general packet types are defined for Level 1 or Level 2 [27].

#### 1) Intermediate System – Intermediate System HELLO (IIH)

- It is used to detect neighbours and maintain adjacency.
- Padded to full Maximum Transmission Unit (MTU).
- Different on p2p links and LANs.

#### 2) Link state packet (LSP)

- It consists of Level 1 pseudo node, Level 1 non pseudo node, Level 2 pseudo node and level 2 non pseudo node.
- One LSP per router and fragment.
- One LSP per LAN network.

#### 3) Complete sequence number PDU (CSNP)

- It consists of a list of LSPs from the database.
- It is used to inform other routes of LSPs that might be missing or outdated. This is important for routers in order to have the same information.

#### 4) Partial sequence number PDU (PSNP)

- It is used to request LSP.
- It is also used to acknowledge receipt of LSPs (or an LSP).

## 5.4 IS-IS Areas and Routing Domains

A routing domain is a collection of areas that implement routing policies within a domain of an AS.

### Backbone

IS-IS does not include a Backbone area such as OSPF Area 0 [27]. A contiguous collection of IS-IS level 2 routers forms the backbone area where each of them can be in different areas. In Figure 5.2 IS-IS backbone area is shown in red in which L1/L2 routers are located in different areas.

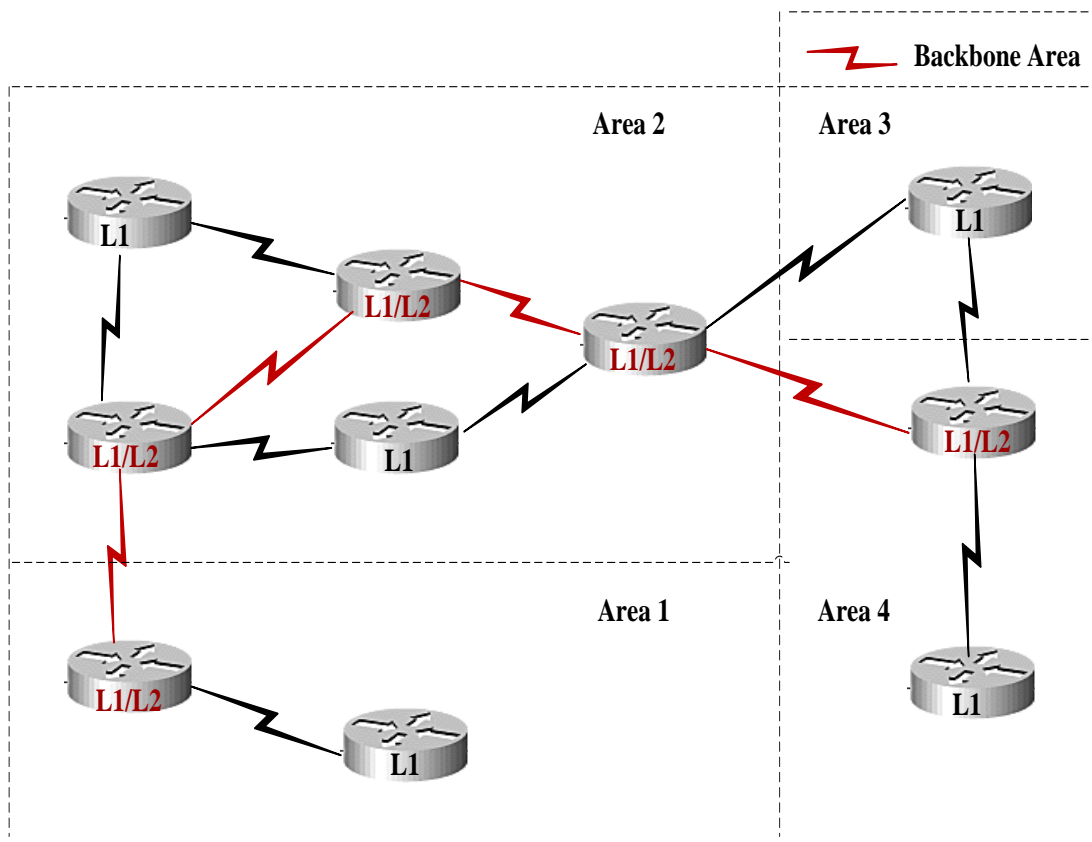


Figure 5.2: IS-IS Backbone.

## Areas

In IS-IS, each router is located only in one area in which the border between areas is on the link connecting the routers in a different area. This makes it different from OSPF. IS-IS enabled router has one network service access point (NSAP) address.

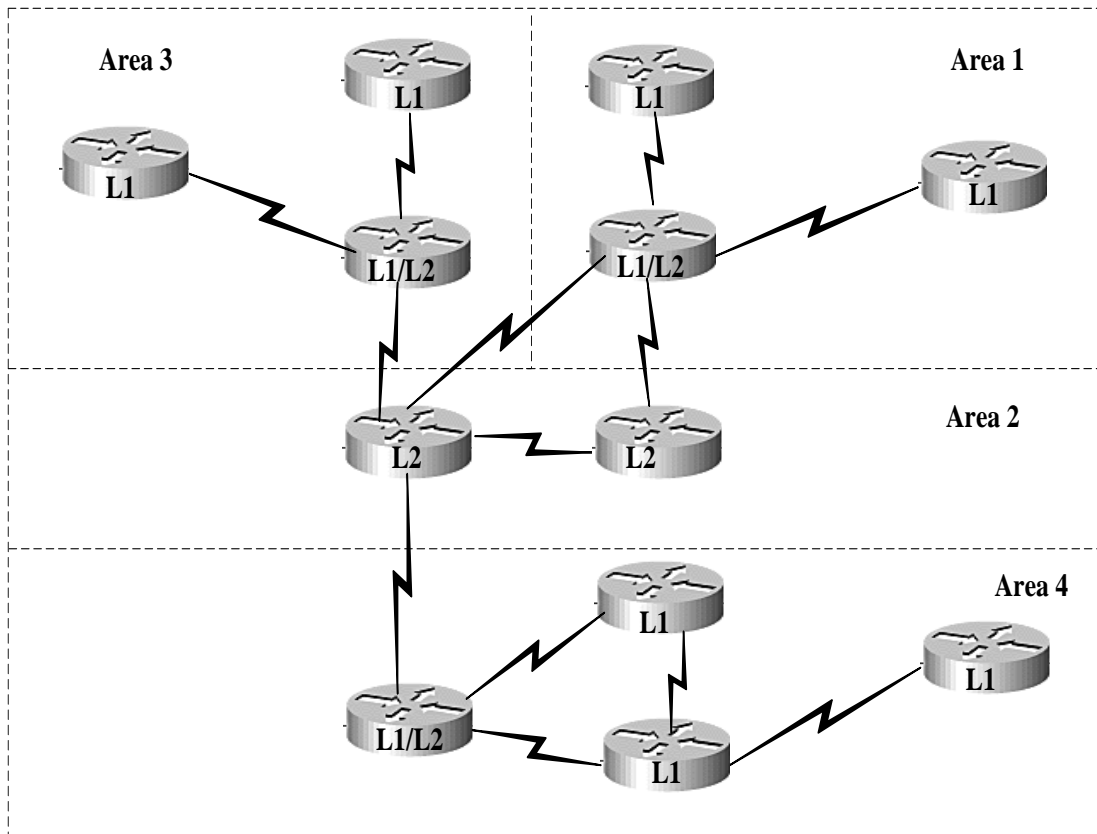


Figure 5.3: IS-IS Areas.

## 5.5 IS-IS Router Types

Three types of routers exist in IS-IS networks [27]. Figure 5.4 shows an IS-IS network topology consisting of three types of routers.

- Level 1 (L1)
- Level 2 (L2)
- Both (L1/L2)

### 5.5.1 Level 1 Router

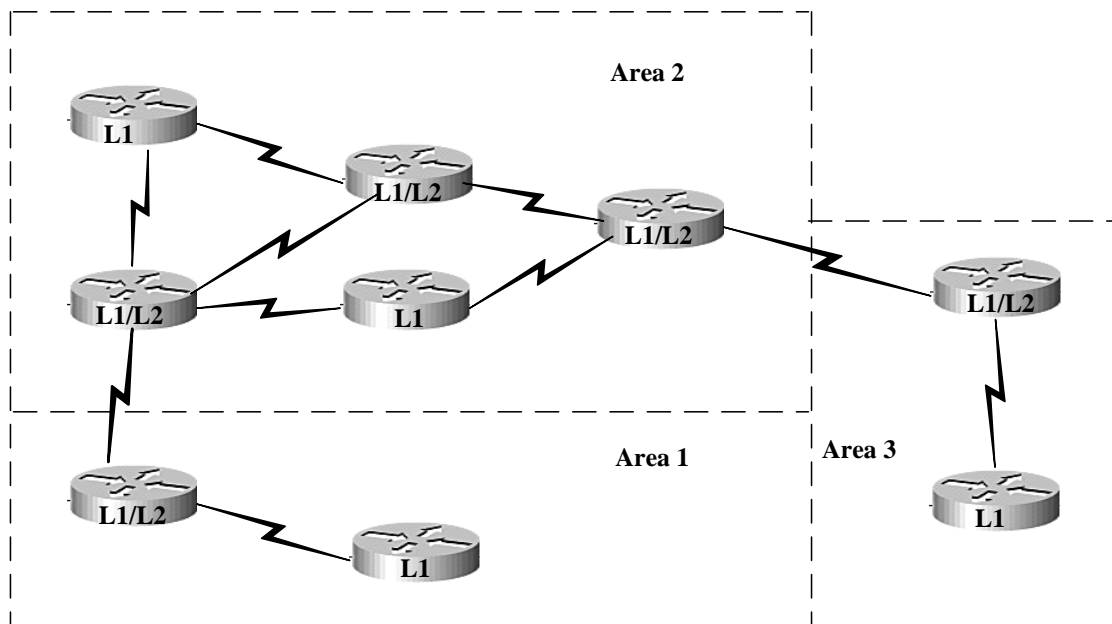


Figure 5.4: IS-IS Network.

A L1 router identifies only the routers in its own area and has neighbours of L1 or L1/L2 in its area. It includes a link state L1 database with the whole information for intra-area routing. To send packets out of its area, L1 router uses the closest L2 capable routers available in its area.

### 5.5.2 Level 2 Router

L2 routers can include neighbours in the same or different area and consists of a L2 link state database with information for intra-area routing. A L2 router can identify other areas but does not have L1 information.

### 5.5.3 Level 1/ Level 2 Router

A L1/L2 router can include neighbours in any area and consists of the following two link state database

- A L1 link state database for intra-area routing.

- A L2 link state database for inter-area routing.

A L1/L2 router runs two SPF's in and it requires more memory and processing.

## 5.6 IS-IS Metrics

IS-IS originally defines four kinds of metrics, namely cost, delay, expense and error [27]. Cost is usually an arbitrary metric. The default metric should be supported on all the routers. The optional metrics are intended for providing differentiated QoS routing.

- **Cost**

Cost is the default metric supported. This metric indicates the link speed. Low value of cost on a link indicates more bandwidth or high speed link.

- **Delay**

Measures the transmission delay of the link.

- **Expense**

Measures monetary link utilization cost.

- **Error**

Measure the residual error probability found in the link.

## 5.7 IS-IS General Operation

From a high level, the operation of IS-IS can be described as follows [27] [28].

- In IS-IS, routers send HELLO packets to all IS-IS enabled interfaces to identify neighbors and create adjacencies.
- Routers sharing a common data link become IS-IS neighbors only when the HELLO packets sent by IS-IS routers contain information

that fulfils the criteria to become an adjacency. Depending upon the media used, the criteria to form an adjacency differ.

- Routers might establish a link state packet depending on the local interfaces configured for IS-IS and prefixes learned from other adjacent routers.
- Routers flood link state packets to every adjacent neighbor excluding the neighbor from which they get the link state packet. There are different types of flooding and depending upon the scenarios, the flooding operation differs.
- Every router builds its link state database from links state packets.
- Each IS will calculate a shortest path tree and from this, the routing table will be constructed.

## 5.8 Advantages and Drawbacks of IS-IS

### Advantages

- Fast convergence. For transmitting routing information, IS-IS utilizes a low number of packet types.
- Support large areas of several intermediate systems without degradation of SPF performance.
- It does not implement virtual links
- Scalable. Backbone is not an area in IS-IS but instead is a collection of contiguous ABRs.
- Simple to implement.

### Drawbacks

- Metrics are 6 bit wide (0-63). Default metric is 10 if it is not manually specified.
- All areas in IS-IS networks are stub areas which may result in sub-

optimal routing between areas.

- All ISs must have identical views of an area.
- For node identification, NSAP addresses are needed in combination with Connectionless Network Protocol (CLNP) as an additional network layer protocol.



# CHAPTER 6

## SIMULATION

### 6.1 Introduction

Simulation can be defined as creating a system model for studying the behavior of the real system under observation. By using the simulation results, we can predict the behavior of the real system.

Furthermore, verification of the simulation software and source code, validation of the data and model used credibility of the obtained result, true randomness, good programming skills, statistical knowledge are also closely related to simulation [29].

There are three main notions that define simulation. These are Verification, Validation and Credibility. Verification checks whether the simulation computer program performs as intended [29].

Validation checks whether the conceptual simulation model is an accurate representation of the system under study [29].

Credibility describes when a simulation model and its results are accepted by the customer as being valid and are used as an aid in making decisions [29].

### 6.2 Network Simulators

Nowadays there are mainly four network simulators used by developers and researchers; these are OMNET++, OPNET, NS-2 and GLASS.

Network Simulator version 2 (NS-2) is a powerful network simulator software. NS-2 and OPNET are mainly designed for simulation of networks. NS-2 architecture takes an object oriented approach using C++ and otcl [30]. Otcl is used for simulation scenario generation, periodic or triggered action

generation and manipulating the existing C++ objects [29]. Unlike OPNET, the NS-2 simulator is open source. OPNET needs a license to be used. NS-2 is a discrete event driven tool, while OPNET is a discrete event driven and flow based simulator. OPNET has a huge documentation while NS-2 has a small documentation.

### 6.3 Simulation Environment Used

In this thesis, the simulation environment used is OPNET. OPNET is developed and distributed by OPNET Technology. It is a powerful network simulator. One can design and study small to very large scale networks, different devices, network protocols and applications with great flexibility.

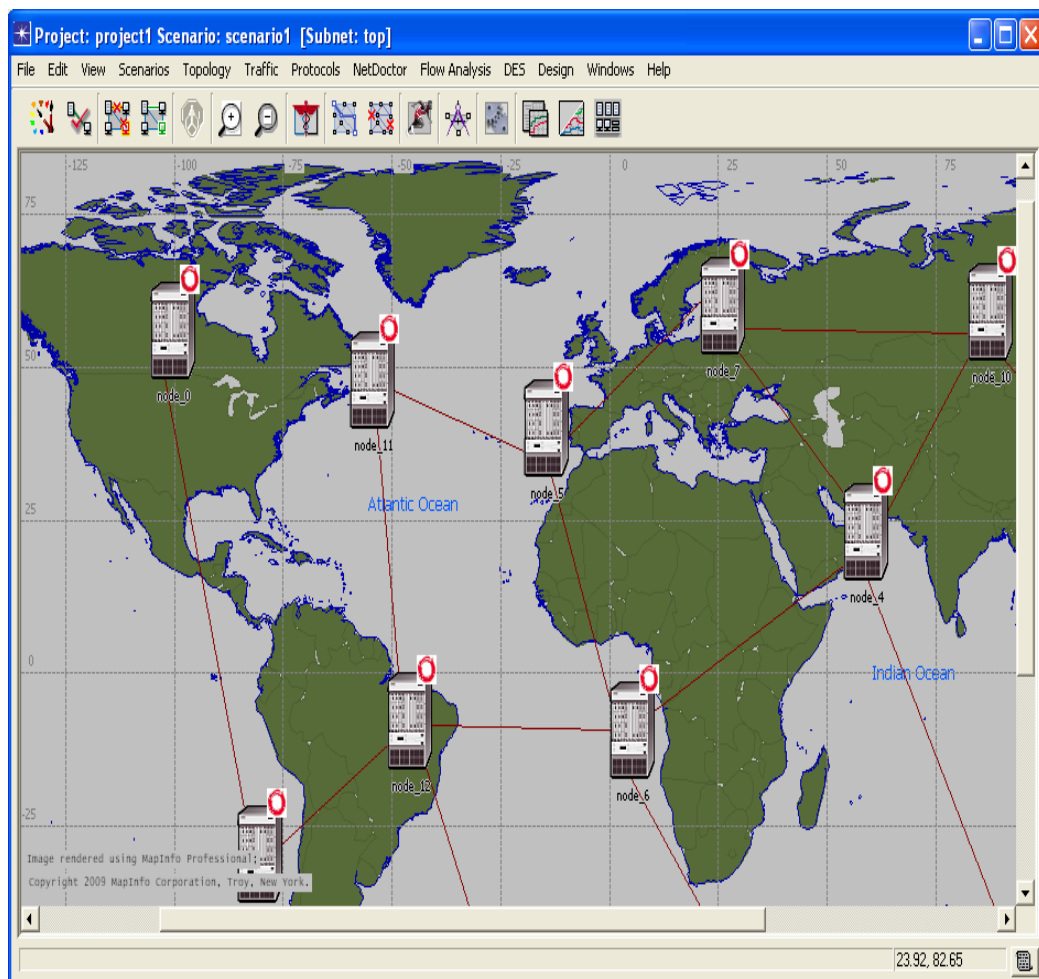


Figure 6.1: Network Domain Editor.

OPNET is a simulator built on top of discrete event system and it simulates the system behavior by modeling each event in the system and processes it through user defined processes [32].

Modeling in OPNET can be done in three different domains. These domains are: Network domain (shown in Figure 6.1), Node domain (shown in Figure 6.2) and process domain (shown in Figure 6.3).

Network domain is a physical representation of network and sub-network on the geographical map of the graphical user interface of the simulator. Node domain is used to develop a model of the node.

Process domain is used to create a model using programming codes. OPNET consists of high level user interface, which is constructed from C and C++ source code blocks with a huge library of OPNET specific function [33].

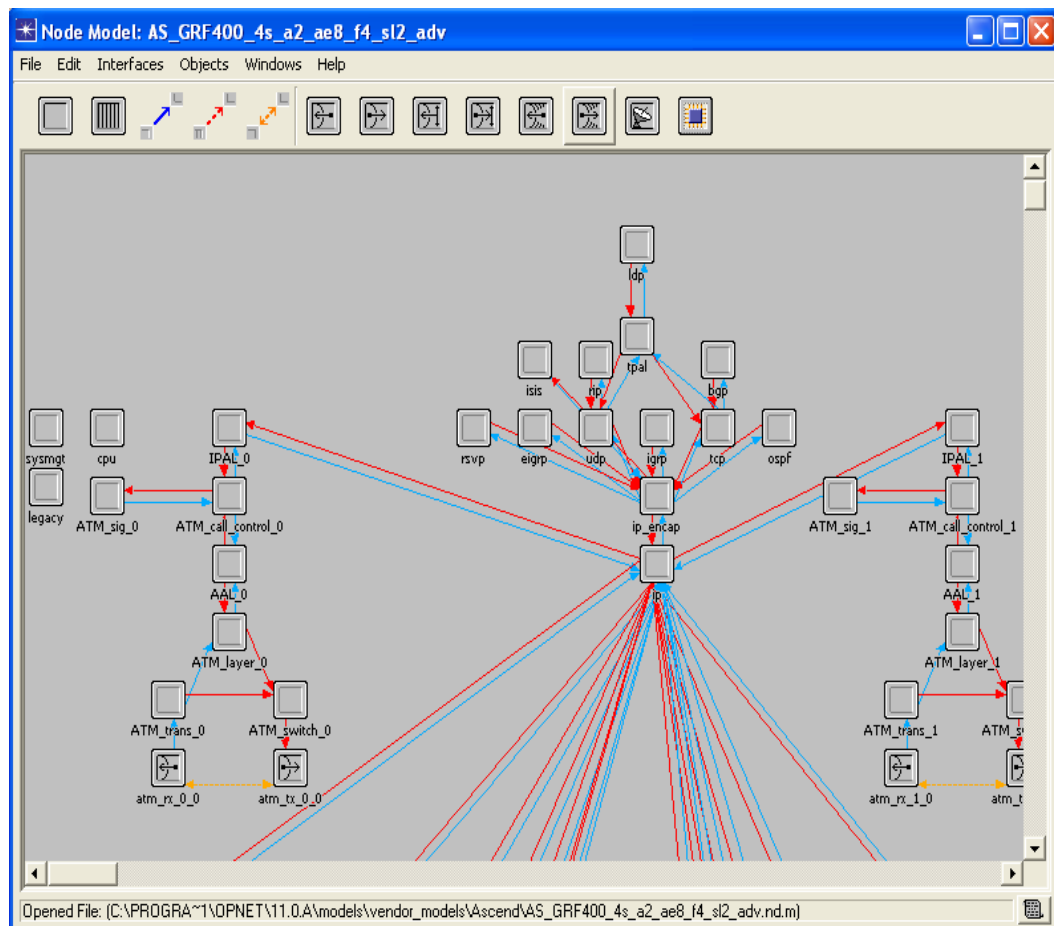


Figure 6.2: Node Domain Editor.

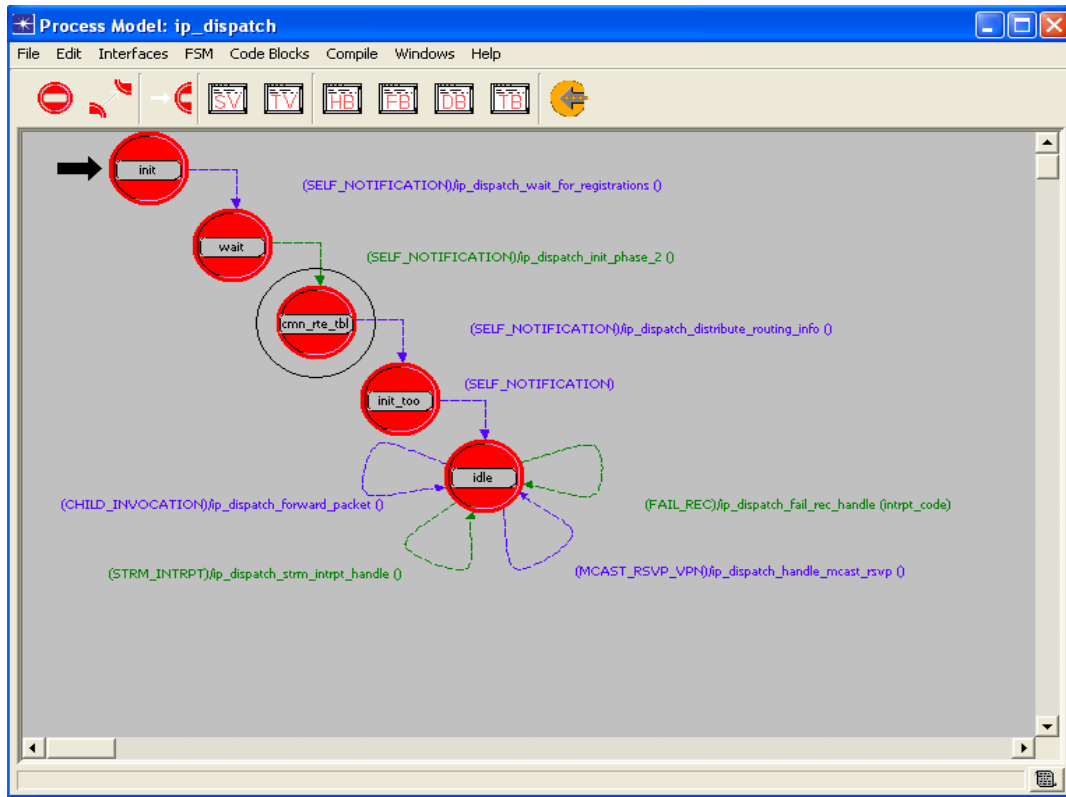


Figure 6.3: Process Domain Editor.

### 6.3.1 Design and Analysis in OPNET

The first step is to create the network model on the network domain editor. After creating the network model, choosing the statistics that will be viewed as a graph is the second step. The next process is to set the *Simulation Duration*, this value is expressed in hour, minute or second. After setting the *Simulation Duration*, the simulation will be ready to be run. The last step is, to view and analyze the result.

Figure 6.4 shows, the flowchart of the step to design on OPNET simulator.

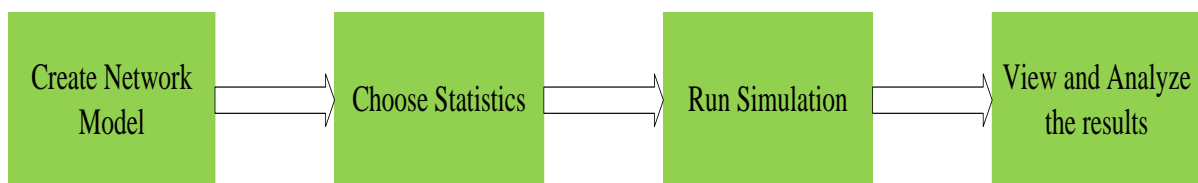


Figure 6.4: Design Steps.

## 6.4 Network Topology

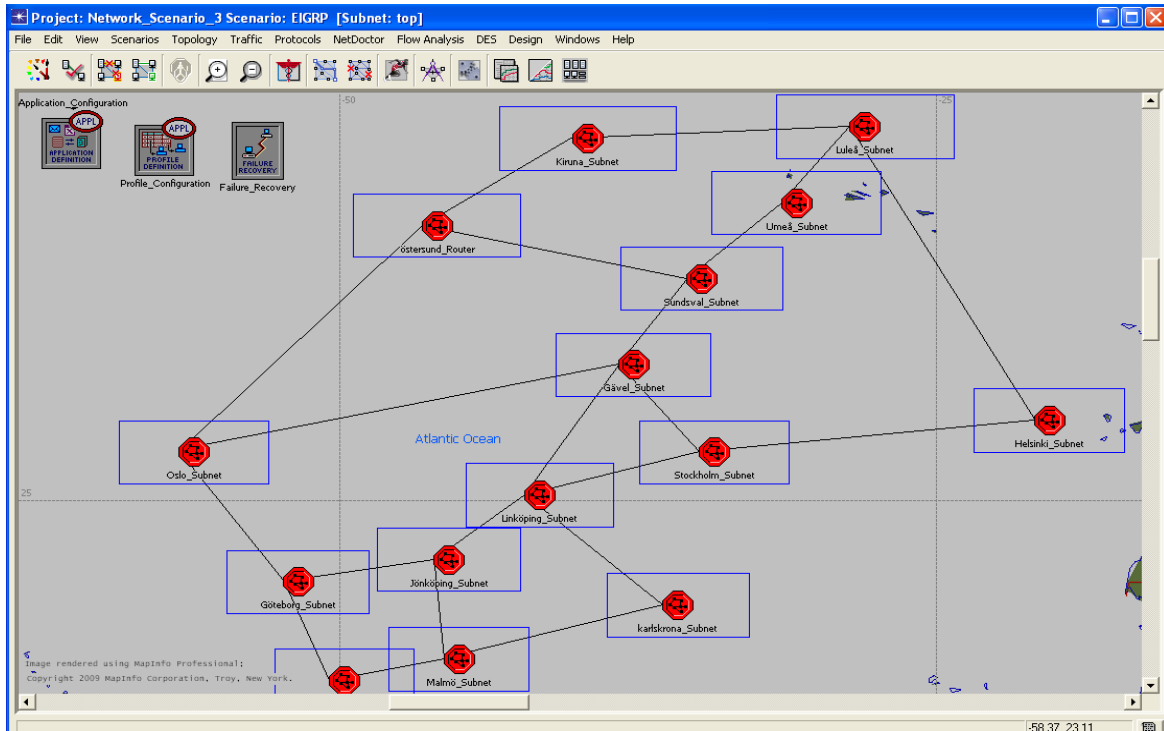


Figure 6.5: Network Topology.

In our thesis, we used five different scenarios. The scenarios are created based on the routing protocols presented. The network topology consists of the following network devices and configuration utilities:

- CS\_7206 Cisco routers
- Ethernet server
- switch
- 100base-T LAN
- Point to point link
- 100base-T link
- 15 Subnets
- Configuration and profile definitions
- Failure/Recovery configurations

### IP-ping configurations

We configured our network topology based on the geographical layout of Sweden shown in Figure 6.5. We designate most of the subnets, routers, switches, servers and LAN networks with the name of the cities in Sweden. In addition to that, we use Helsinki, Oslo and Copenhagen. Half of the subnets contain LANs, switches and Ethernet servers.

The application definition is set to support all applications. In the profile definition, we create a profile that has an application support of Database access (DB), E-mail access and web-browsing (HTTP). Göteborg and Umeå routers are set to be failed at 150 s and 250 s later respectively. The servers support all the applications set in the profile definition. LANs are set to support DB access, e-mail access and HTTP access.

The routers are connected using PPP\_D3 links and the switch connected with the router is using a 100Base-T link. The server and LAN are directly connected to the switch.

### **6.4.1 OSPF Scenario**

This scenario implements OSPF as a routing protocol on the selected network topology. As a first step, we created the network topology without a routing protocol and then, we duplicated it to five scenarios so that we could simulate OSPF, EIGRP, IS-IS, OSPF/IS-IS and EIGRP/IS-IS on each of them. So, on one of the duplicated scenarios, OSPF is configured as a routing protocol for the whole routers in the network.

After configuring the routing protocol, we choose the statistics that will be viewed on the result. These statistics are: OSPF Traffic received (bits/s), HTTP object response time (s), E-mail download response time (s), Database response time (s) and point to point throughput. IP-ping configuration is setup to check the connectivity between Copenhagen and Luleå routers.

### **6.4.2 EIGRP Scenario**

On this scenario, EIGRP is configured as routing protocol for the selected network topology. We used one of the duplicated scenarios with no routing protocol and configure EIGRP on it.

Then, we choose the statistics that will be viewed on the result: EIGRP Traffic received (bits/s), EIGRP Convergence duration (s), HTTP object response time (s), E-mail download response time (s) and point to point throughput. IP-ping configuration is setup to check the connectivity between Copenhagen and Luleå routers.

### **6.4.3 IS-IS Scenario**

On this Scenario, IS-IS is configured as routing protocol for the network topology. Then, we choose the statistics that will be viewed on the result: IS-IS Traffic received (bits/s), IS-IS Convergence activity (s), HTTP object response time (s), E-mail download response time (s), Database response time (s) and point to point throughput. IP-ping configuration is setup to check the connectivity between Copenhagen and Luleå routers.

### **6.4.4 EIGRP/IS-IS Scenario**

One of the main focuses of our thesis is to analyze the network that is configured with EIGRP and IS-IS routing protocols together and deduce the advantages of using both protocols together. This scenario is a little different from the others because two routing protocols are configured on the network.

As shown in Figure 6.6, some part of the network uses EIGRP and the other part uses IS-IS. Both protocols use route redistribution for exchanging route information to each other. Route redistribution is a feature that allows for the exchange of route information among multiple protocols and multiple

sessions [34]. The characteristics of each routing protocols is analyzed, while using both protocols together.

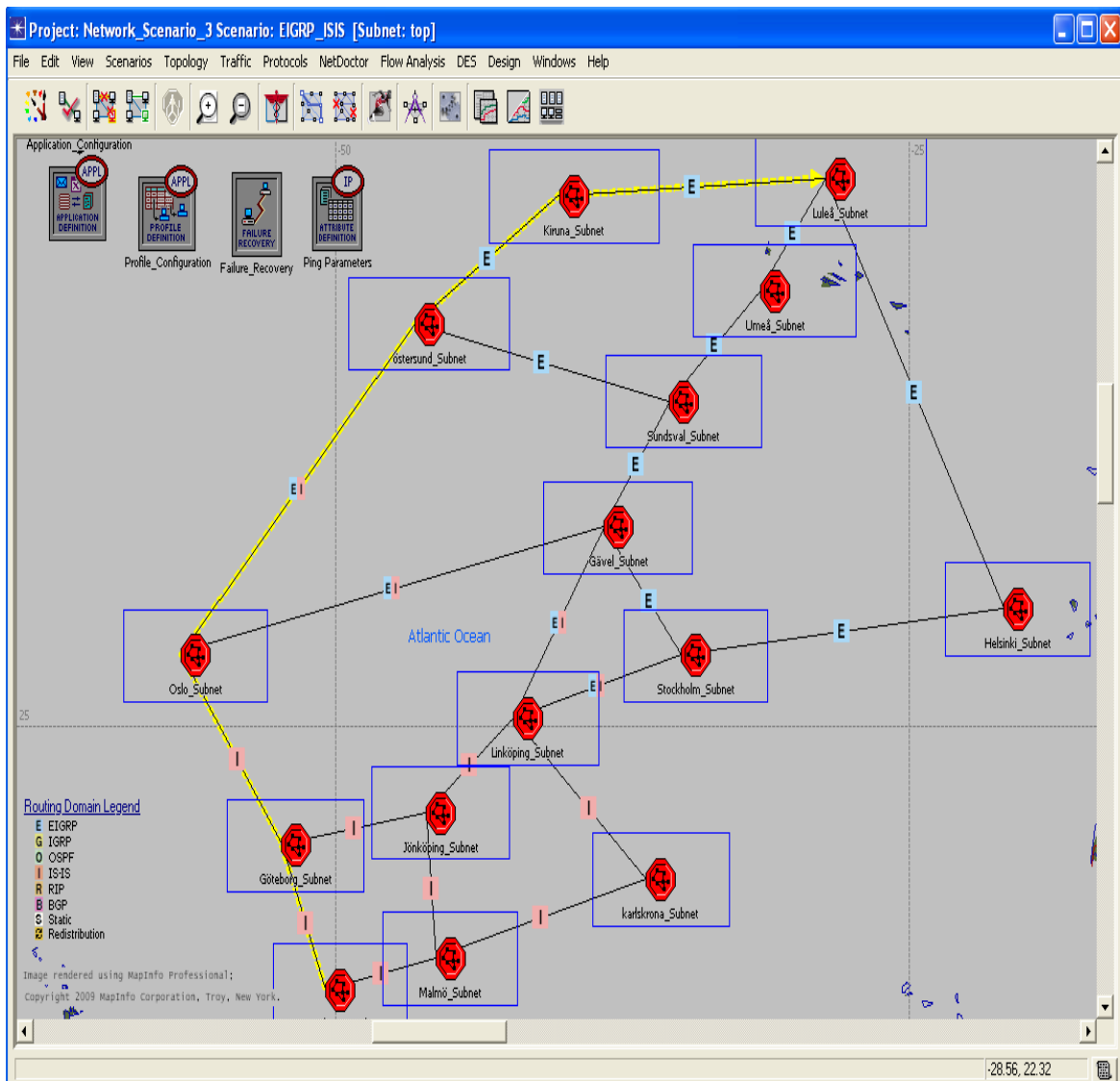


Figure 6.6: EIGRP/IS-IS Topology.

The statistics chosen for this scenario: IS-IS Traffic received (bits/s), IS-IS Convergence activity (s), HTTP object response time (s), E-mail download response time (s), Database response time (s), EIGRP convergence activity, EIGRP traffic sent (bits/s) and point to point throughput (packet/s). IP-ping configuration is setup to check the connectivity between Copenhagen router and Luleå router. On Copenhagen router only IS-IS is configured and on Luleå

router only EIGRP is configured. The successful connectivity is shown with yellow color.

### 6.4.5 OSPF/IS-IS Scenario

The other main focus of our thesis is the combination OSPF/IS-IS, which analyzes the implementation of OSPF and IS-IS together on the topology network.

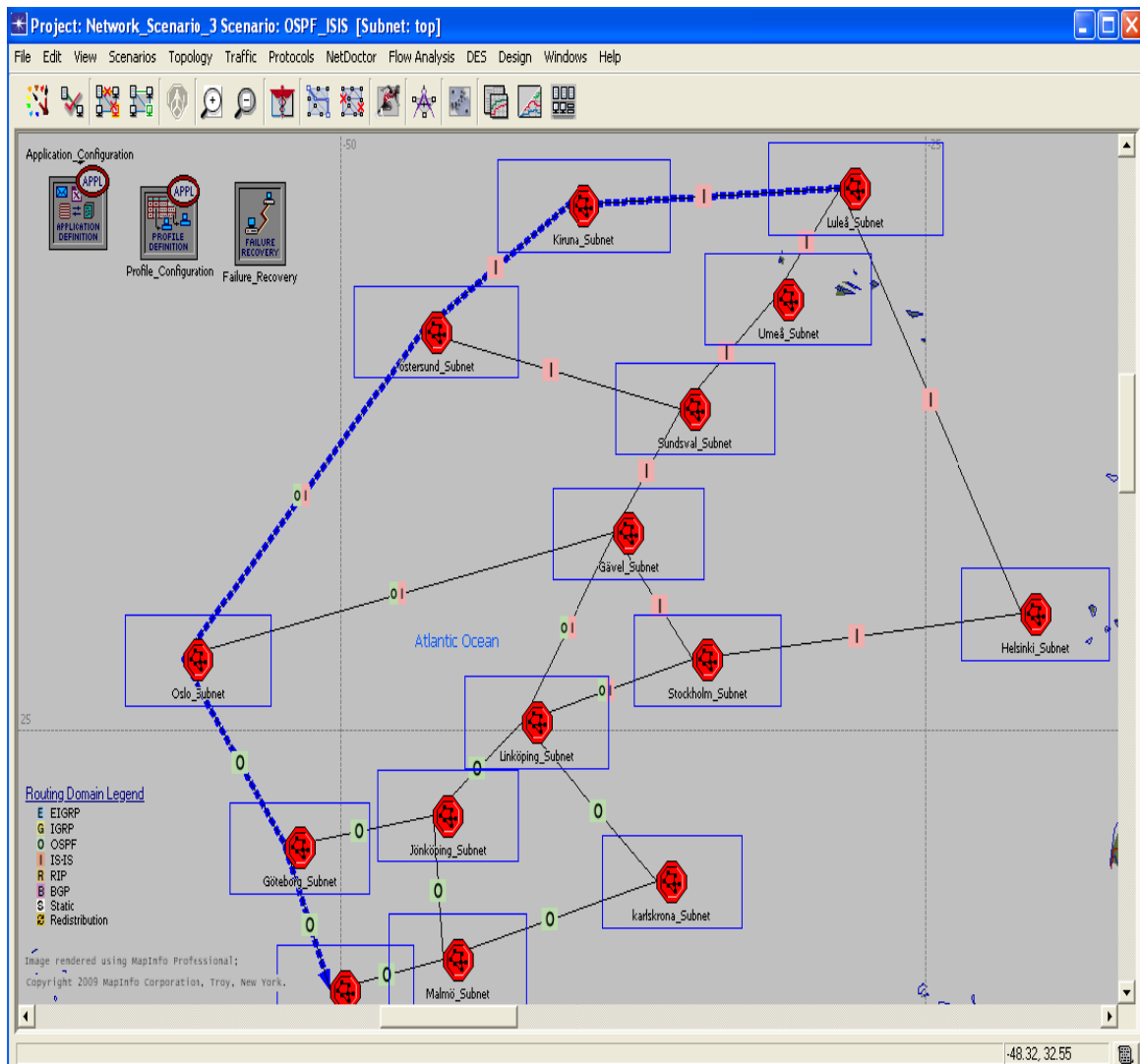


Figure 6.7: OSPF/IS-IS Topology.

As shown in Figure 6.7, some part of the network uses OSPF and the other part uses IS-IS. In order to exchange route information between the

protocols, route redistribution is enabled on the network. The statistics of the simulation is selected as follows: IS-IS Traffic received (bits/s), IS-IS Convergence activity (s), HTTP object response time (s), E-mail download response time (s), Database response time (s), point to point throughput (packet/s) and OSPF traffic sent (bits/s). IP-ping configuration is setup to check the connectivity between Copenhagen router and Luleå router.

This is shown in Figure.6.7 as a successful connectivity between the two routers. On Copenhagen router only OSPF is configured, while on Luleå router only IS-IS is configured. On the Figure, the successful connectivity is shown with green color.

## 6.5 Confidence Analysis

We run each simulation scenarios 21 times with different seed values, and each simulation is run for 30 minutes. Then based on the sampled mean value of each simulation, we analyzed the variability of the results of each simulation.

When the variation of the simulation result is large, it reflects insecurity on the result. When the variation is small, it denotes a good confidence and when there is no variation on the simulation result, it shows there is an error on the simulation [29].

As it is shown on Figure 6.8 and Figure 6.9, our simulation results are close to each other, which shows a good confidence on the simulation. The confidence interval of each simulation is calculated using the following formula.

$$CI = X \pm Z_{1-\alpha/2} \left( \frac{S}{\sqrt{n}} \right) \text{-----} (6)$$

$X$  is the mean value

$Z_{1-\alpha/2}$  the Z transform value of  $1 - \alpha/2$

$\alpha$  depends on the confidence level, in our case it'll be 0.2,

$s$  standard deviation,  $n$  the batch size.

### 6.5.1 Confidence Analysis of OSPF/IS-IS

In our analysis, we take two results in order to analyze their confidence parameters. These results are just a representative result of the whole simulation.

It's shown in Figure 6.8 and Figure 6.9 that the variability analysis of the result of our simulation for e-mail download response time in OSPF/IS-IS and EIGRP/IS-IS . The confidence interval of those simulations is also calculated.

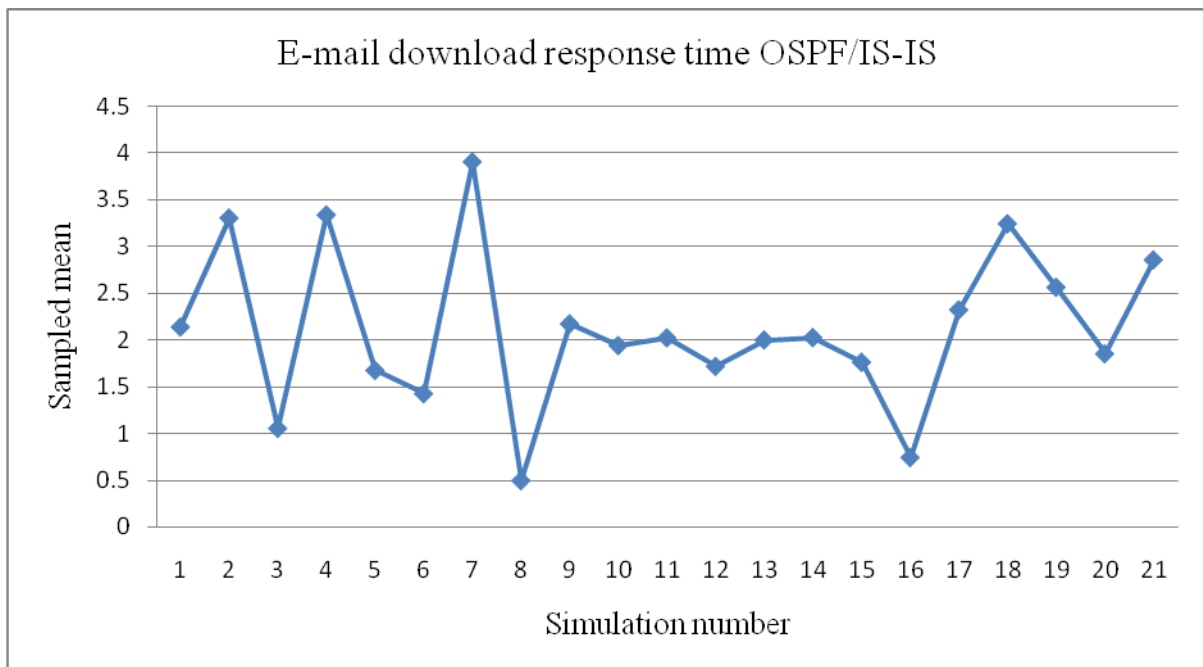


Figure 6.8: E-mail Download Response Time in OSPF/IS-IS.

$\bar{X}$  is the average value of the sampled mean of the data, Standard deviation ( $S$ ) calculated using the 21 sampled means , since the confidence level of the simulation is 80% the value of  $\alpha$  is 0.2. So, we calculated the confidence interval of E-mail download response time of OSPF/IS-IS as follows:

$$X = 2.121735 \quad n = 21 \quad S = 0.862367 \quad \alpha = 0.2$$

$$CI = 0.241167$$

The confidence interval value shows, the simulation result of OSPF/IS-IS is a good result.

### 6.5.2 Confidence Analysis of EIGRP/IS-IS

In this section, we will analyze the confidence analysis of e-mail download response time of EIGRP/IS-IS. As it is shown in Figure 6.9, the variability of the result is very small, so the simulation result is good. We calculated the confidence interval of the result as follows.

X is the average value of the sampled mean of the data, Standard deviation (S) calculated using the 21 sampled means, since the confidence level of the simulation is 80% the value of  $\alpha$  is 0.2.

$$X = 0.005025853, \quad n = 21, \quad S = 0.862367, \quad \alpha = 0.2$$

$$CI = 0.000194$$

The confidence interval value shows, the simulation result of EIGRP/IS-IS is a good result.

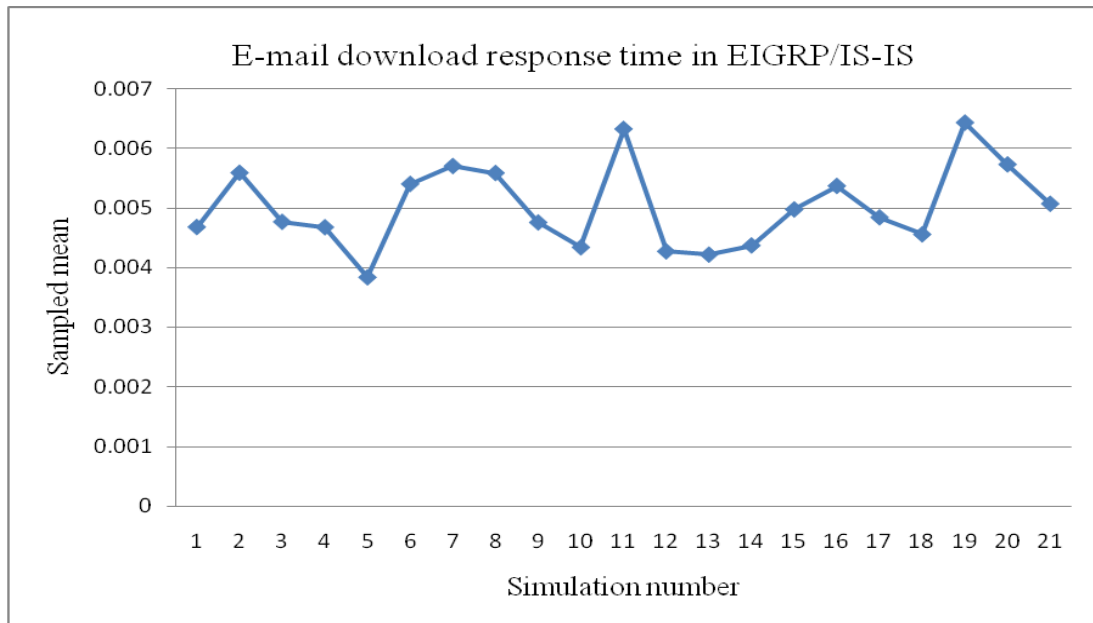


Figure 6.9: E-mail Download Response Time in EIGRP/IS-IS.

## 6.6 Simulation Result and Analysis

As we mentioned earlier, we have five simulation scenarios: OSPF, EIGRP, IS-IS, OSPF/IS-IS and EIGRP/IS-IS. This helps us compare one protocol with the other. So, we select a specific parameter and compare the results of all protocols on one graph based on the selected parameter. In all the scenarios, Göteborg router and Umeå router are setup to fail at 150 s and 250 s. Consequently, there will be three convergence times.

First convergence time is the time elapsed to build up the topology table, neighbor table and routing table at the start of the protocol implementation on the network.

Second convergence time is due to the failure of Göteborg router at 150<sup>th</sup> s there will be an advertisement of the failure of the failed router to the whole network. The second convergence is the time elapsed to advertise the failed router for all the routers.

Third convergence time is due to another advertisement for the whole network about the failure of the Umeå router at 250<sup>th</sup> s. The third convergence is the time elapsed to advertise the failed router for all the routers.

There are two ways of showing the convergence time on OPNET. Using Convergence duration (s), this shows the convergence time of the selected protocol at particular time on the vertical axis.

The other way of showing convergence time is, using Convergence activity (s). Convergence activity shows the convergence time of a selected protocol on the horizontal axis of the graph, the width of the bar at a particular time gives the convergence time of the protocol. In our thesis, we used both ways, which are shown in Figure 6.12 and Figure 6.13.

In our thesis, we used three different applications that can help us to measure the performance of the protocols, E-mail, HTTP and Database. The

parameter that we used is the application download response time. This shows how the routing protocol facilitates the E-mail service, the HTTP service and the Database access service.

### 6.6.1 OSPF Traffic

Figure 6.10 shows the OSPF traffic sent in bits per Sec. On the graph OSPF traffic is higher at the time of first convergence in OSPF/IS-IS protocol than in OSPF. At the time when Göteborg router fails, there will be a network topology update; therefore the routers will exchange route information with the whole network.

Again, the second time, when Umeå router fails, it will update the network tables, so there will be another route information exchange. At the second and third convergence, the OSPF traffic will be higher in OSPF than OSPF/IS-IS.

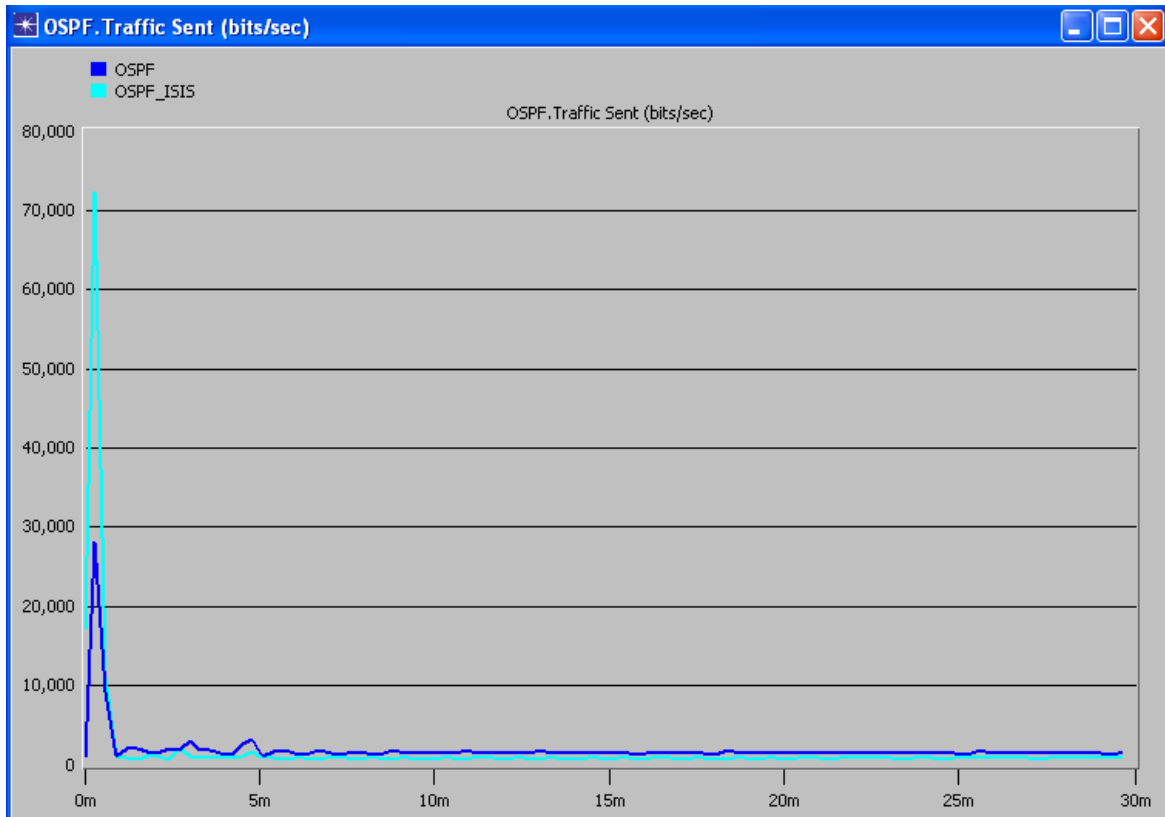


Figure 6.10: OSPF Traffic.

## 6.6.2 EIGRP Traffic

Figure 6.11 shows EIGRP traffic sent in bits/s. It is shown that during the time of convergence, the EIGRP traffic is much higher in EIGRP network than of EIGRP/IS-IS network.

In EIGRP/IS-IS network, the EIGRP route information will be lower because the EIGRP traffic is exchanged within the interface that uses EIGRP protocol. The network that use EIGRP for the whole network will have more interfaces that use EIGRP, so there will be more EIGRP traffic than a network that use EIGRP and IS-IS in the network.

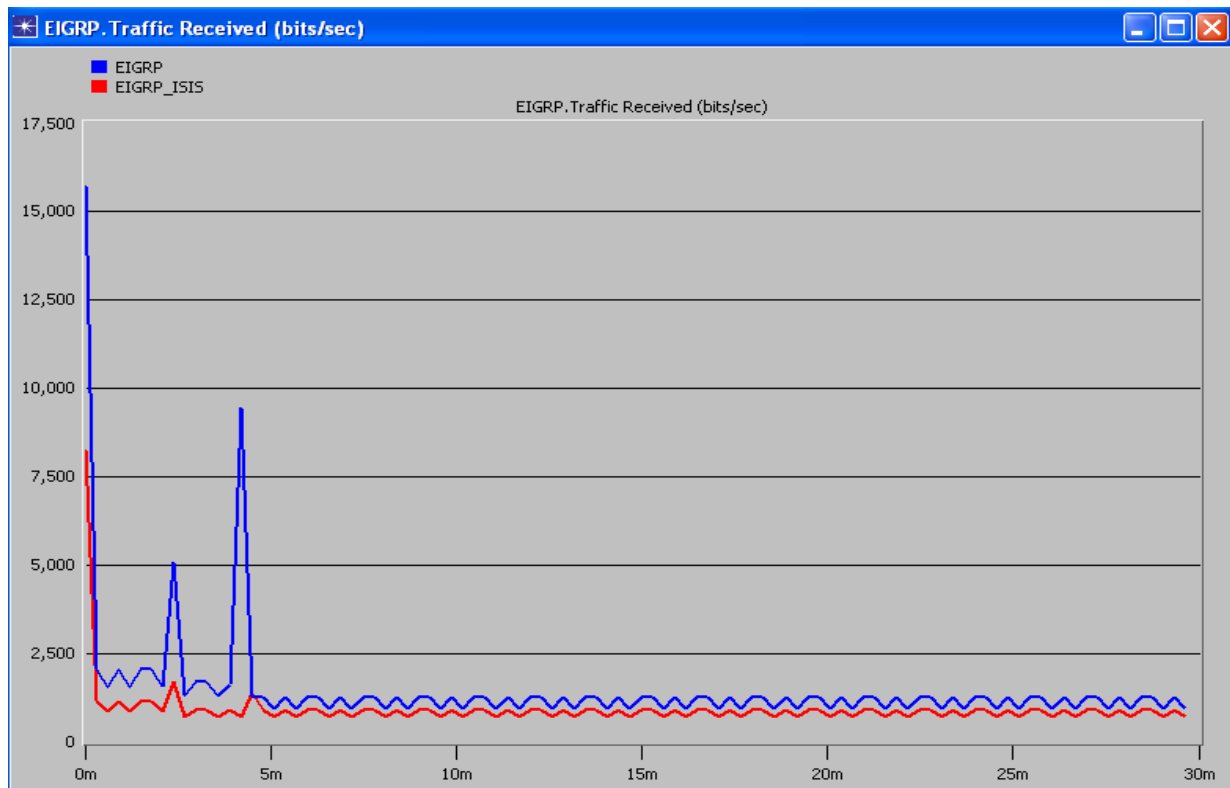


Figure 6.11: EIGRP Traffic.

## 6.6.3 EIGRP Convergence Time

Figure 6.12 shows the convergence time of EIGRP in the network that uses EIGRP routing protocol and EIGRP/IS-IS routing protocol. As it's shown

in Figure 6.12, the convergence time of EIGRP in EIGRP/IS-IS network is relatively smaller than the network that uses only EIGRP.

EIGRP route information update will be advertised within the interface that use EIGRP routing protocol, since the interfaces enabled to use EIGRP are smaller in EIGRP/IS-IS than EIGRP, it will take a smaller time to update the topology table, routing table and neighbor table.

The first convergence time of EIGRP/IS-IS is 5.5 s, whereas for EIGRP it is around 0.025 s. The second convergence time, it is 0.075 s for EIGRP, whereas for EIGRP/IS-IS it is 0.025 s. The third convergence time is 0.065 s for EIGRP, whereas for EIGRP/IS-IS it is around 0.005 s.

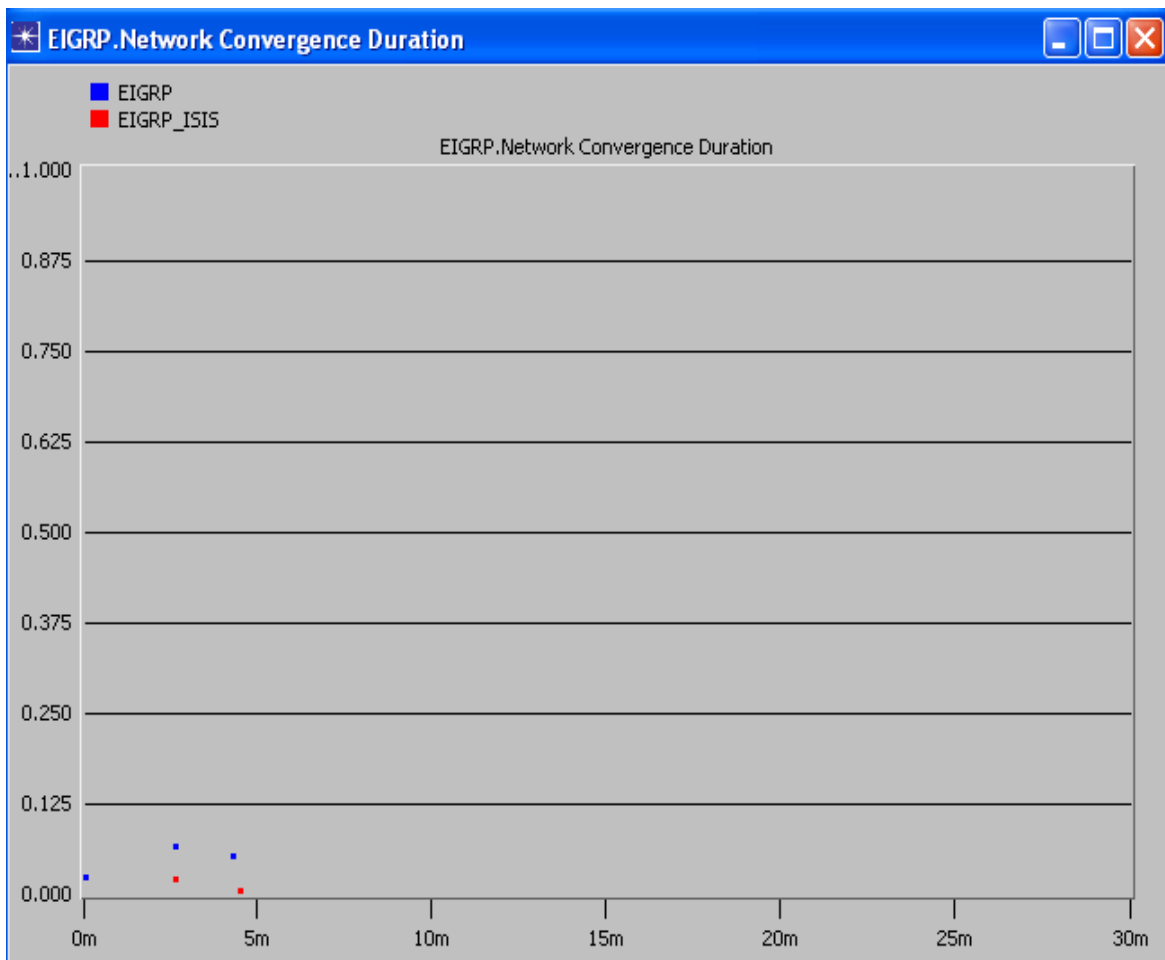


Figure 6.12: EIGRP Convergence Time.

### 6.6.4 IS-IS Convergence Time

As it is shown in Figure 6.13, the elapsed time to converge the network on IS-IS network is slower than OSPF/IS-IS network and EIGRP/IS-IS network. On the other hand, the network convergence time for EIGRP/IS-IS network is faster than the other networks.

The first convergence time of IS-IS is 11 s, whereas for EIGRP/IS-IS is around 0.9 s and for OSPF/IS-IS is 12 s. The second convergence time of IS-IS is 11 s, whereas for EIGRP/IS-IS it is around 0.9 s and for OSPF/IS-IS it is 6 s. The third convergence time of IS-IS is 10 s, whereas for EIGRP/IS-IS is around 6 s and for OSPF/IS-IS is 6 s.

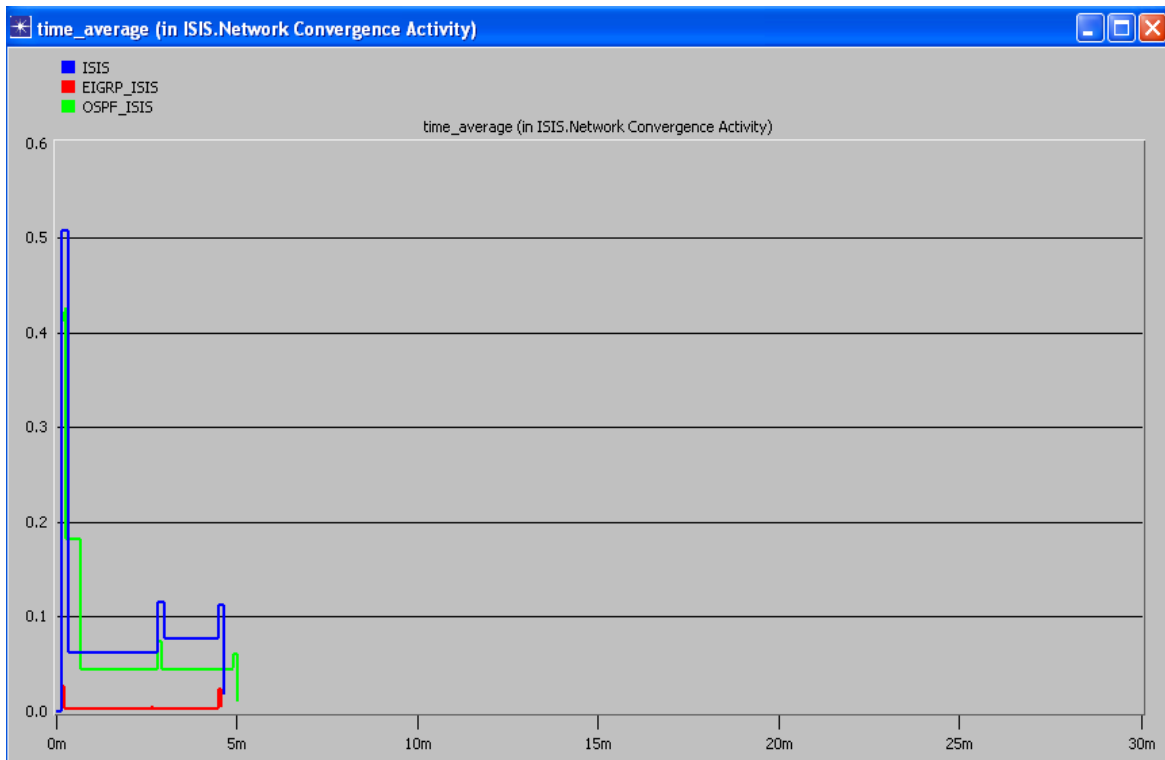


Figure 6.13: Convergence Time.

### 6.6.5 Database Query Response Time

Figure 6.14 shows the database query response time in the second scenario. The LAN network is able to access the database from the server, so in

this scenario we show how the protocols affect the performance to access the database from the server.

In the comparison of these protocols in database query response time, EIGRP/IS-IS shows a better response time than of the other protocols at the whole time.

On the other hand, OSPF/IS-IS shows a slower response time than of all the other protocols. At the beginning, the response time of OSPF, IS-IS, OSPF/IS-IS and EIGRP is almost similar but as time increases, OSPF/IS-IS becomes slower in response time. On the other hand EIGRP shows better performance than the other three protocols. OSPF and IS-IS protocols show almost similar database response time in the whole time.

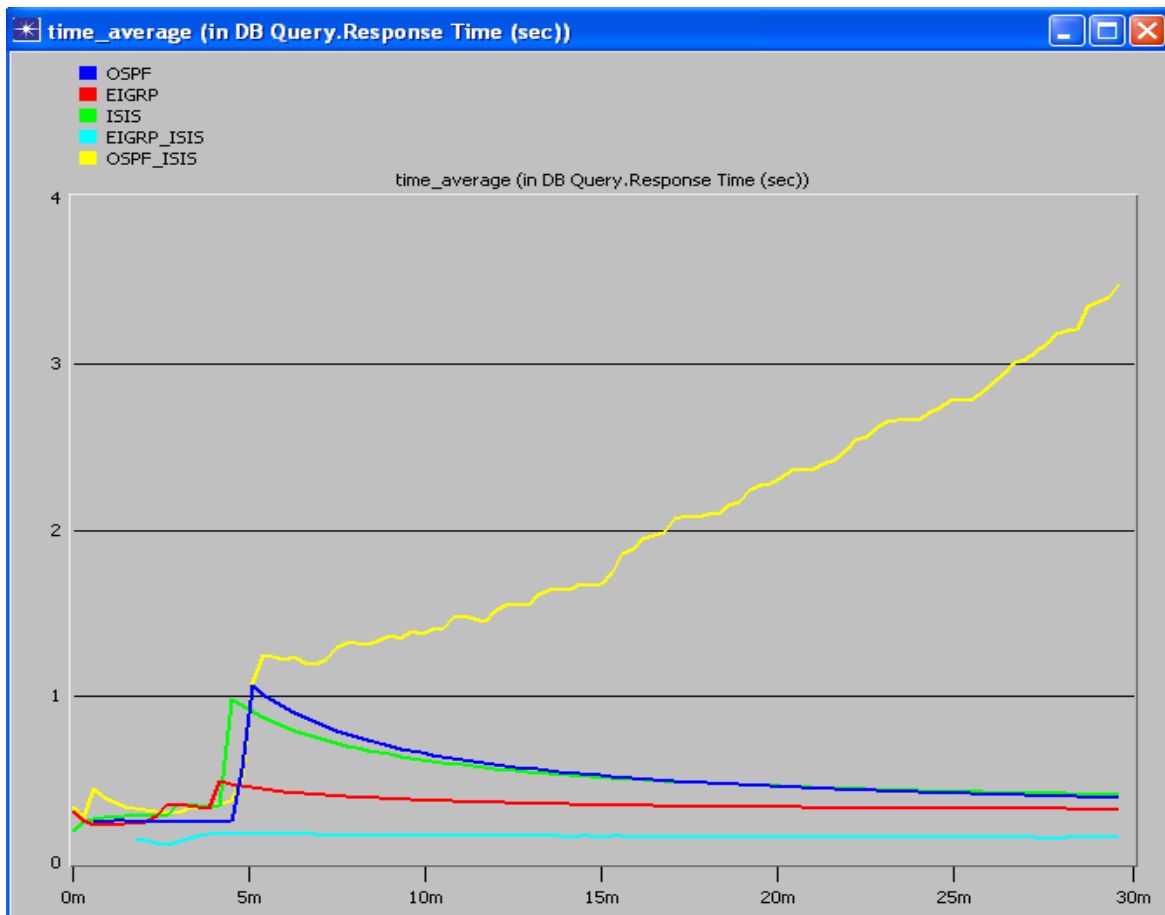


Figure 6.14: Database Response Time.

### 6.6.6 E-mail Download Response Time

E-mail application is heavily used by the users in the LAN network, the E-mail access is done from the mail server in the network. Figure 6.15 shows E-mail download response time in s. The graph shows that the EIGRP/IS-IS protocol performs very well for the whole simulation time.

On the other hand, OSPF/IS-IS performs bad compared to the other protocols. In the first 4 minutes, IS-IS shows better E-mail download response time than of EIGRP and OSPF. After 4 minutes OSPF, EIGRP and IS-IS show almost similar performance for E-mail download response time.

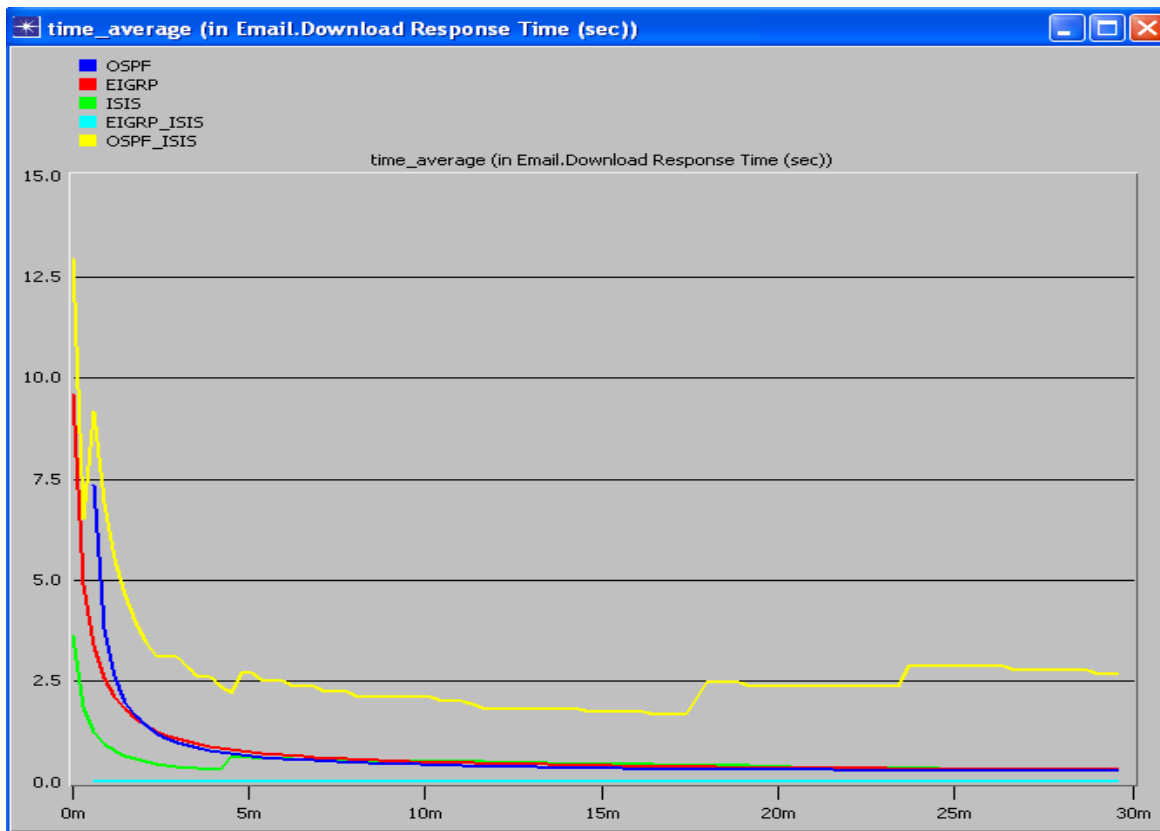


Figure 6.15: E-mail Download Response Time.

### 6.6.7 HTTP Object Response Time

Figure 6.16 shows HTTP object response time in s. Heavy HTTP application is used by the users in the network and the application service is

supported by the server. The graph shows that EIGRP/IS-IS shows a shortest object response time in the whole simulation time. For the first 3 minutes, OSPF/IS-IS has a better object response time than of OSPF, IS-IS and EIGRP. But as time increases, OSPF/IS-IS object response time increases, and instead IS-IS become better than the other four protocols.

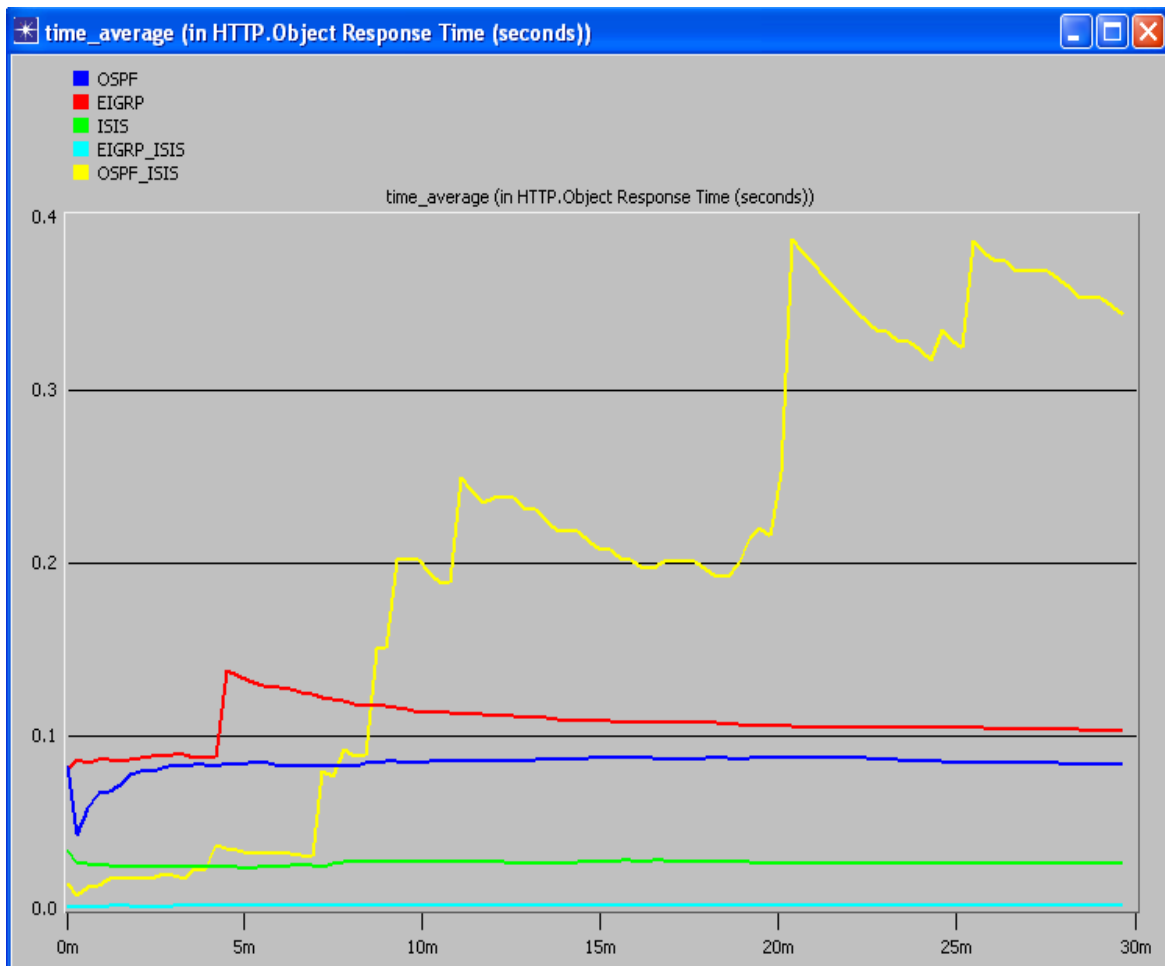


Figure 6.16: HTTP Object Response Time.

### 6.6.8 Throughput

Figure 6.17 shows point to point throughput between the Karlskrona router and Linköping router measured in packets/s. The graph shows OSPF/IS-IS has high throughput in this link. On the other hand IS-IS, OSPF, EIGRP/IS-IS and EIGRP have a lower packet throughput in this link. EIGRP/IS-IS has a

relatively better performance on point to point packet throughput than of the other three protocols.

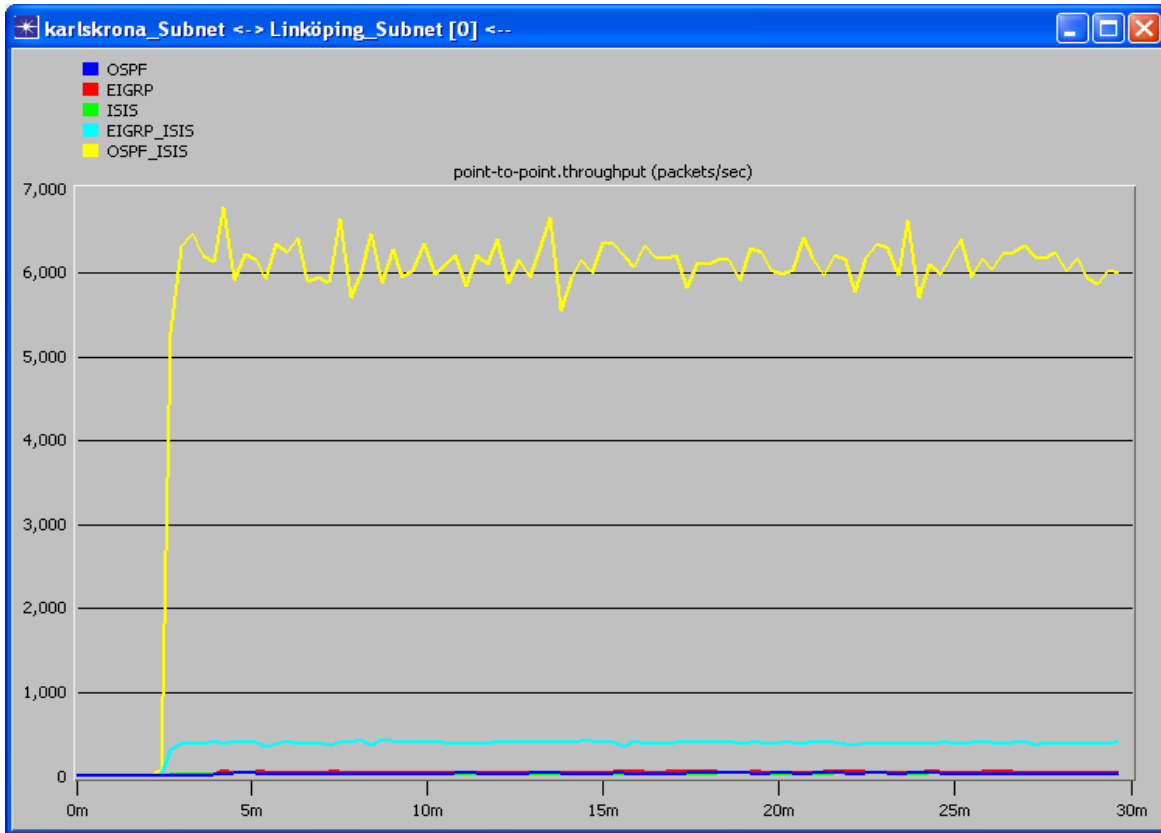


Figure 6.17: Point to Point Throughput.



## **CHAPTER 7**

### **CONCLUSIONS and FUTURE WORK**

The objective of this thesis was to configure multiple routing protocols on a selected network topology and analyze the performance improvement of the network. We aimed to configure OSPF and IS-IS together in one network, then EIGRP and IS-IS together in one another network. After configuring the protocols we analyzed the network performance improvements as compared to the network that use OSPF alone, EIGRP alone or IS-IS alone.

The OSPF traffic in the network using OSPF/IS-IS is smaller than of network using only OSPF. This indicates that the bandwidth utilization of OSPF is better and the link congestion probability is smaller in OSPF/IS-IS network than that of network using only OSPF.

The EIGRP traffic in the network using EIGRP/IS-IS is lower than of network using only EIGRP. This indicates that the bandwidth utilization of EIGRP is better in the EIGRP/IS-IS network than that of network using only EIGRP.

Convergence time of EIGRP in the network using EIGRP/IS-IS network is much faster than in the network using only EIGRP. Therefore the nodes in EIGRP/IS-IS network learn the topology faster than the nodes in the EIGRP network.

IS-IS convergence time in EIGRP/IS-IS network is much faster than in IS-IS network or OSPF/ISIS network. On the other hand, IS-IS network shows lower convergence time than the EIGRP/IS-IS network or the OSPF/IS-IS network. Then we conclude, EIGRP/IS-IS network learns all nodes in the whole network faster than of IS-IS network or OSPF/IS-IS network. And IS-IS network learns slower than of the other two networks.

Database response time is better in the network which uses EIGRP/IS-IS combination as compared to other networks using OSPF, IS-IS, EIGRP, OSPF/IS-IS. Network using OSPF/IS-IS combination shows slower database response time. Therefore database access is much faster in EIGRP/IS-IS networks and very slow in OSPF/IS-IS network.

The network using EIGRP/IS-IS shows faster HTTP object response time, E-mail download response time than of other networks using OSPF, EIGRP, IS-IS, OSPF/IS-IS. On the other hand network using OSPF/IS-IS combination shows slow response in both the cases. Hence, EIGRP/IS-IS provides the end users access to the HTTP applications and e-mails faster than networks using OSPF, EIGRP, IS-IS, OSPF/IS-IS. The overall throughput performance of all networks is similar at the beginning of the simulation. But after few minutes, network using OSPF/IS-IS combination shows much better throughput performance than of all other networks.

In our thesis, we analyzed the performance of different routing protocols and have found EIGRP/IS-IS performed better than the other protocols. So, as a future work, we recommend any interested researcher to combine EIGRP and IS-IS routing protocols, and make one advanced routing protocol. This can be done by analyzing the source code of each protocol and make a modification on the codes.

## REFERENCES

- [1] Rick Graziani and Allan Jonson, “Routing protocols and concepts: CCNA exploration companion guide,” Pearson Education. London, 2008.
- [2] Catherine Boutremans, Gianluca Iannaccone, Christophe Diot, “Impact of link failures on VoIP performance,” In Proceedings of NOSSDAV Workshop, ACM press, pages 63-71, May 2002. Florida, USA.
- [3] Renata Teixeira, Jennifer Rexford, “Managing Routing Disruptions in Internet Service Provider Networks,” IEEE Communications Magazine, March 2006.
- [4] Douglas E. Comer, “Internetworking with TCP/IP, Principles, Protocols and Architecture,” 5th ed. Vol.1, Pearson Prentice Hall, 2006.
- [5] Tony Larsson and Nicklas Hedman, “Routing Protocols in Wireless Ad-hoc Networks-A simulation Study (Master’s thesis),” Dept. Com. & Eng., Luleå Univ., Stockholm, 1998.
- [6] Talal Mohamed Jaffar, “Simulation-Based Routing Protocols Analysis (Thesis),” Ph.D., Dept. Elect. Eng., Georgia Institute of Technology, 2007.
- [7] Jeff Doyle. (2001, Nov 16). “Dynamic Routing Protocols,” <http://www.informit.com/articles/>
- [8] Online source. (2004, Aug 27), “Advanced IP Addressing Management,”CiscoSystems, <http://www.informit.com/articles/>
- [9] Radia Perlman, “A Comparison between Two Routing Protocols: OSPF and IS-IS,”IEEE Network Magazine, September, 1991.
- [10] Cisco, “Internet Technology Handbook.”

- [http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Enhanced\\_IGRP.html](http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Enhanced_IGRP.html)
- [11] Cisco, “IP Routing, Introduction to EIGRP,” Document ID:13669.  
[http://www.cisco.com/en/US/tech/tk365/technologies\\_tech\\_note09186a0080093f07.shtml#hw](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f07.shtml#hw)
- [12] <http://www.ciscocertificationacademy.com/Enhanced-Interior-Gateway-Routing-Protocol-EIGRP.php>
- [13] Ravi Malhotra, “IP Routing,” 0-596-00275-0, January 2002.  
<http://oreilly.com/catalog/iprouting/chapter/ch04.html#45434>
- [14] <http://www.rhyshaden.com/eigrp.htm>
- [15] David Billings,” A collection of materials for the study of intranet and internet networking,” GTCC.  
<http://www.gtcc-it.net/billings/eigrp.html>.
- [16] <http://www.javvin.com/protocolEIGRP.html>
- [17] Javvin network management and security. “IS-IS: Intermediate System to Intermediate system routing protocol,”  
<http://www.javvin.com/protocolOSPF.html>
- [18] Todd Lammle, “Cisco Certified Network Associate”, 5<sup>th</sup> edition, 2005
- [19] Microsoft. TechNet. “OSPF operation, ”  
<http://technet.microsoft.com/en-us/library/cc940481.aspx>
- [20] Kenneth Holter, “Wireless Extensions to OSPF: Implementation of the Overlapping Relay Proposal,” Dept. Informatics. Univ., Oslo, 2006.
- [21] Christian Huitema,” Routing in the internet,” 2. Ed, Prentice Hall PTR, cop. 2000.
- [22] Faraz Shamim, Zaheer Aziz, Johnson Liu, Abe Martey,” Troubleshooting IP Routing Protocols,” Cisco Press, Pages : 912, May 07, 2002.
- [23] <http://www.rhyshaden.com/ospf.htm>

- [24] <http://www.cellsoft.de/telecom/autonomoussystemrouting.htm>
- [25] Javvin network management and security. "IS-IS: Intermediate System to Intermediate System Routing Protocol,"  
<http://www.javvin.com/protocolISIS.html>
- [26] Javvin Technology, Inc. "Guidelines for OSI NSAP Allocation in the Internet," <http://www.javvin.com/protocol/rfc1629.pdf>.
- [27] CISCO. "Intermediate System-to-Intermediate System Protocol,"  
[http://www.cisco.com/en/US/tech/tk365/technologies\\_white\\_paper09186a00800a3e6f.shtml](http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a00800a3e6f.shtml)
- [28] CISCO. "Intermediate System-to-Intermediate System Protocol,"  
[http://www.cisco.com/en/US/products/ps6599/products\\_white\\_paper09186a00800a3e6f.shtml#wp38493](http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a3e6f.shtml#wp38493)
- [29] Law A.M, "Simulation modeling and analysis,"4th edition, McGraw-Hill 2007.
- [30] The Otcl Tutorial, 1995.  
<http://bmrc.berkeley.edu/research/cmt/cmtdoc/otcl/tutorial.html> (Current v 3 03)
- [31] "OPNET modeler and NS2,"  
<http://privatewww.essex.ac.uk/~fleum/weas.pdf>
- [32] "Introduction to OPNET Simulator, "  
<http://bolero.ics.uci.edu/~ypan/OPNET/Introduction%20to%20OPNET%20simulator.pdf>
- [33] "Simulations and Tools for Telecommunications,"  
[http://www.telecomlab oulu.fi/kurssit/521365A\\_tietoliikennetekniikan\\_silmuolinnit\\_ja\\_tyokalut/Opnet\\_esittely\\_07.pdf](http://www.telecomlab oulu.fi/kurssit/521365A_tietoliikennetekniikan_silmuolinnit_ja_tyokalut/Opnet_esittely_07.pdf)
- [34] Wade Edwards," CCNP Complete Study guide," 2005.

**MEE09:77**

[35] OPNET Technologies, Inc., The OPNET Simulator,  
<http://www.opnet.com/>