

Major project report

by Million Gashaw Woldemarian

FILE	16142_MILLION_GASHAW_WOLDEMARIAN_MAJOR_PROJECT_REPORT _78196_724146676.DOC (4M)		
TIME SUBMITTED	20-APR-2016 12:30PM	WORD COUNT	13614
SUBMISSION ID	56116953	CHARACTER COUNT	86334



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Comparing and Evaluating Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) routing protocols in IPv6 network operation.

By

Million Gashaw Woldemariam

Supervisor: Dr Kapilan Radhakrishnan

Second Marker: Dr Carlene Campbell

Project submitted as part of the requirements for
the award of BSc (Hons) Computer Networks

April 2016

Declaration of Originality

I, Million Gashaw Woldemariam declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed :

Date :

FORM OF CONSENT

I Million Gashaw Woldemariam hereby consent that my Project, submitted in candidature for the B.Sc.(Hons) Computer Networks degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed :

Date :

Copyright Acknowledgement

I acknowledge that the copyright of this project report, and any product developed as part of the project, belong to University of Wales Trinity Saint David, Swansea.

ABSTRACT

The aim of this project is to compare and evaluate Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) routing protocols in IPv6 network operations. To meet this aim, specific and achievable objectives have been set.

In this paper the first step was to focus on the literature review of scientific research and experiments to compare and evaluate the two most popular routing protocols in IPv6 network environment.

The second step was investigating and gathering performance parameters used by other networking professionals to compare and evaluate EIGRP and OSPF in IPv4 and IPv6 routed protocols.

The proliferation of the Internet user population and the depletion of IPv4 address space are two of the main motivating factors behind the development and implementation of IPv6 routed protocols. The current trend of internetworking growth requires adaptation of the routing for IPv6. Hence, it is vital to investigate the performance of EIGRP and OSPF routing protocols in IPv6 network operations.

To conduct a comprehensive and thorough comparison between EIGRPv6 and OSPFv3, different network topologies have been designed with point-to-point and multi-access network scenarios. Furthermore, a series of controlled experiments have been undertaken using Cisco packet tracer 6.2, GNS3 and 16 dedicated Cisco routers in a laboratory environment.

Based on the key findings, EIGRP for IPv6 has performed better in all scenarios compared to OSPFv3. The generated results indicate that EIGRP for IPv6 is the best choice for both point-to-point and multi-access networks as it is not only converging faster from cold start, but also it has a faster re-convergence speed when a topology change occurs.

In order to assess the performance of dynamic routing protocols in a large network scenario, an appropriate network simulator software is recommended as it is not only time-saving, but also it can provide a wider range of performance parameters for comparison and evaluation of dynamic routing protocols.

Table of Contents

Copyright Acknowledgement.....	ii
LIST OF TABLES	VI
CHAPTER 1 INTRODUCTION.....	8
1.1 Introduction	8
1.2 Aim.....	9
1.3 Objectives	9
1.4 Structure of the Project	10
CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE.....	11
2.1. ROUTING CONCEPT	11
2.1.1 Introduction	11
2.1.2 Basic IP Routing.....	11
2.1.3 Static Routing	13
2.1.4 Dynamic Routing	17
2.2 An overview of IPv6	18
2.2.1 IPv6 Essential	18
2.2.2 Types of IPv6 Addresses	19
2.3 Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRPv6)	20
2.3.1 Establishment of EIGRP Neighbour Relationships.....	20
2.3.2 Features of EIGRP	21
2.3.3 EIGRP Packet Types	21
2.3.4 DUAL Concepts	22
2.3.5 EIGRP Tables	24
2.3.6 EIGRP Metrics.....	24
2.3.7 EIGRPv6 Routing	25
2.3.8 Configuration of EIGRPv6	27
2.4 Open Shortest Path First routing protocol for IPv6 (OSPFv3).....	27
2.4.1 OSPF features	28
2.4.2 Establishment of OSPF Neighbour Relationships	28
2.4.3 OSPF Packet Types.....	28

2.4.6 Similarities and differences between OSPFv2 and OSPFv3	31
2.5 Related works	32
3. RESEARCH METHODOLOGY	35
CHAPTER 4- DESIGN AND IMPLEMENTATION	38
4.1 Design.....	38
4.2 Implementation	39
4.2.1 Configuration of EIGRPv6.....	40
4.2.2 Configuration of OSPFv3	42
5. TESTING AND EVALUATION	44
5.1 Test scenarios	44
5.2 Test Analysis	48
6. CONCLUSIONS AND RECOMMENDATIONS.....	50
7. REFLECTIONS	52
8. REFERENCES	55

LIST OF TABLES

Table 1: Routing table output from Cardiff router	15
Table 2: Routing table output from R1 router	16
Table 3: Comparing EIGRPv4 and EIGRPv6 [22]	26
Table 4: Test summary for point-to-point network scenario	44
Table 5: Test summary for multi-access network scenario.....	45

LIST OF FIGURES

Figure 1: Basic Network Topology	13
Figure 2: Static route configuration.....	14
Figure 3: Configuration of static default route	16
Figure 4: Mesh Point-to-point network topology.....	38
Figure 5: Multi-access network topology in GNS3 simulator	38
Figure 6: Ping result from OSPFv3 in point-to-point network Cisco Lab experiment.....	45
Figure 7: Ping result from EIGRP for IPv6 in point-to-point network Cisco Lab experiment.....	46
Figure 8: ping result from EIGRP for IPv6 in multi-access network (GNS3) .	46
Figure 9: ping result from OSPFv3 in multi-access network (GNS3).....	46
Figure 10: EIGRPv6 and OSPFv3 Re-convergence Time Comparison	47
Figure 11: EIGRPv6 and OSPFv3 Neighbour-down detection Time Comparison	47

Figure 12: EIGRPv6 and OSPFv3 Round-Trip Success rate Comparison from cold start	48
---	-----------

Figure 13: Project planning	54
--	-----------

CHAPTER 1 INTRODUCTION

1.1 Introduction

Network connection maximises the value of business operations of governments and enterprises and gain positive benefits in different aspects. Internet protocol (IP) address enables networking devices to communicate in different geographical locations by uniquely identifying the machine over the network. The router is responsible for the delivery of packets across different networks [1]. Routers are now even being added to satellites in space. These networking devices use dynamic routing protocols to perform network discovery, updating and maintaining routing tables. As discussed by [1] and [2] routers are intermediary network devices; whereas, routing protocols define the set of rules used by routers when they communicate routing information between neighbour routers. For the modern Internet era, routing protocols enable routers to communicate with each other to forward the packets to desired destinations [3].

The growth of Internet and evolution of high speed data networks has led to the inevitable adoption of IPv6 [4] [5]. Wijaya [4] argues that computers and data networking have become an essential part of our daily lives. This implies that communication in the Internet has been growing and becoming an integral part of human life.

The motivating factors behind the development and implementation of IPv6 routed protocol are the followings:

- The proliferation of Internet population
- The Internet of everything
- The depletion of IPv4 address space
- Issues with Network Translation Address (NAT).

Many organisations and some countries have been implementing IPv6 [6]. This in return, requires investigating the performance of routing protocols in IPv6 network operation.

When selecting the most appropriate routing protocol for an organisation, several requirements can be considered. There are benefits and drawbacks for each specific routing protocol.

This project will focus on comparison and evaluation of Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) routing protocols in IPv6 network operation.

1.2 Aim

The aim of this project is to compare and evaluate Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) routing protocol in IPv6 routed protocol.

1.3 Objectives

- Conduct a literature review in order to develop a thorough understanding of the features and characteristics of the two routing protocols.
- From researches undertaken by academic network professionals, gather performance parameters, such as: cpu utilisation, packet loss, bandwidth, network convergence and re-convergence time and neighbour-down detection time used by other researchers for comparison and evaluation of EIGRPv6 and OSPFv3
- Design point-to-point mesh network topology using Cisco packet tracer and dedicated Cisco hardware in a laboratory environment
- Design a multi-access network topology using Graphical Network Simulator (GNS3)
- Configure EIGRPv6 and OSPFv3 for both the point-to-point and the multi-access network topologies
- Analyse which one of the routing protocols re-converges faster after an unexpected link-failure
- Identify the response times when a change occurs such as neighbour down condition
- Examine each protocol's operational differences upon implementation of their authentication mechanisms
- Investigate which protocol converges faster from a cold start by pinging from source to destination as soon as the routing protocols are initially started
- Find out which of the two routing protocols is more robust than the other

1.4 Structure of the Project

The remainder of this paper is organised as follows:

Chapter 2 concentrates on the literature review. In this chapter, basic IP routing, types of routing, an overview of routing protocols, IPv6, EIGRP and OSPF for IPv6 will be discussed.

In chapter 3, Research philosophy, approach, methodology and strategy will be described.

Chapter 4 consists of Design and Implementation for comparison and evaluation analysis of EIGRPv6 and OSPFv3 routing protocols.

Chapter 5 shows evaluation analysis and results.

Chapter 6 presents conclusions and recommendations.

Chapter 7 shows conduct and progress of the given research to achieve the aim and objectives of this project.

Chapter 8 presents all necessary references.

CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE

2.1. ROUTING CONCEPT

2.1.1 Introduction

To ensure communications between networking devices, routing protocols are required and they are functioning at layer 3 which is network layer. Ethernet switches function at the data link layer, which is layer 2; thus, Ethernet frames can be forwarded between devices (nodes) within the same network. However, when the source IP and destination IP addresses are on different networks, the Ethernet frames must be sent to a router [7]. The router connects one network to another network. To perform this process, the router uses its routing table. The routing table enables router to determine the best path to forward a packet. The effectiveness of internetwork communications depends on the ability of routers to forward packets in the most efficient way possible [4] [8] [2].

2.1.2 Basic IP Routing

When a host sends a packet to another host on a different IP network, the packet is forwarded to the default gateway as hosts outside of a local network cannot communicate to each other. The default gateway is often used to connect the local network to the Internet [8].

Nowadays, networks have changed the way people live, work, and play. Interaction, communication and collaboration of modern societies have been changed by latest network technologies. Graziani [2] specifies Some of the activities and interaction performed by modern networking on daily basis as follows:

- Web applications
- IP telephony
- Video conferencing
- Interactive gaming
- Electronic commerce

➤ Education and many more

Routing table is used to find the best match between the destination IP of a packet and a network address [8] [2]. An internetwork can be created by connecting WANs and LANs using routers. Routers communicate to each other and maintain their routing tables through the transmission of a variety of messages such as update message and a link-state advertisement.

Routing is the process of determining the best paths and taking data packets from one device to another device on a different network [8]. Understanding the difference between a routed protocols and routing protocols is important. A routed protocol is a protocol by which data can be routed. Examples are IPV4, IPV6, Apple talk, and IPX. Routed protocols are the actual data that is transferred from router to router; for example, the actual packet itself [8]. For these routed protocols, an addressing scheme and subnetting are required. Addressing scheme is used to determine the network to which a host device belongs and to identify the host on that particular network.

A routing protocol is used between routers to build and maintain routing tables [9]. Routing protocols disseminate routing information throughout routers on a network [1] [4] [2]. Routing protocols can be classified as distance vector, link-state and path vector. Distance vector and link-state routing protocols are Interior Gateway Protocols; whereas, path vector routing protocols are Exterior Gateway Routing protocols.

Examples of IGP routing protocols are Routing Information Protocol (RIP), RIPv2, and RIP next generation, Enhanced Interior Gateway Routing Protocol (EIGRP), EIGRPV6, Open Shortest Path First version 2 (OSPFV2), OSPFV3, Intermediate-System-to Intermediate System (IS-IS) and IS-IS for IPV6. Examples of Exterior Gateway Protocols are Boarder Gateway Protocol-4 and MBGP. These routing protocols determine the best paths of a packet through an internetwork. In this paper the two routing protocols, namely Enhanced Interior Gateway Routing protocol and Open Shortest Path First Routing protocols in both IPV4 and IPV6 network operation will be discussed in detail later in chapter 2.2.5.

IP works with Address Resolution Protocol (ARP) to determine the destination of packet by looking at the IP address and the subnet mask of a host. The best path to a destination network and forwarding data packet is determined by a router.

As a packet arrives on the router's interface, the router uses its routing table to determine the best path to the destination network.

There are numerous routers in the internal network and on the Internet as well. When users want to send emails or access web pages, packets traverse through a number of routers. Routers find the destination of required network in their routing tables and forward the packets to their destinations.

If packets are destined for outside the Local Area Network (LAN), the destination Medium Access Control (MAC) address will always be the router's interface.

The following figure shows simple basic IP routing process when Host 1 sends data to the HTTPs server.

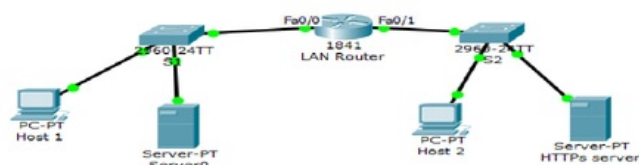


Figure 1: Basic Network Topology

Referring to figure 1, the MAC address of the Fa0/0 interface of the router is the destination address of a frame from Host 1; whereas, the destination address of a packet will be the IP address of the network interface card (NIC) of the HTTPs server. In the segment header, the destination port number will have a value of 443. There are different ways to configure the routing tables to include all networks in an internetwork. The types and best routing configuration for any network depends upon the specific environment and business requirements.

2.1.3 Static Routing

Static routing occurs when routes are manually added in each router's routing table. There are some advantages and disadvantages of using static routes.

Advantages:

- Improved security as the network administrator has a full control over the entire network
- There is no CPU usage; thus, cheaper router can be purchased
- There is no bandwidth usage between the routers

Disadvantages:

- If the network topology changes, the routers are not automatically updated hence, the administrator must configure all routers manually by hand. Therefore, static route is not feasible in large networks.
- When dealing with a large network, it is extremely time-consuming task.

Two common types of static routes are:

- Static route to a specific network
- Default static route.

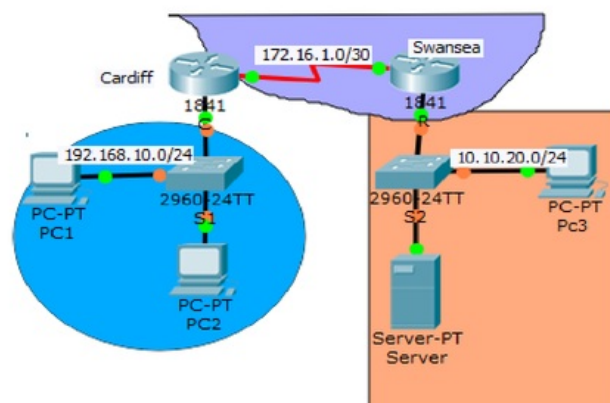


Figure 2: Static route configuration

The above figure (Figure 2) displays that the hosts and routers are manually configured with the correct IP addresses, subnet masks and appropriate default gateways.

For PC1 to communicate with Email server, static routes should be configured on both Cardiff and Swansea routers as shown on the next page:

Cardiff (config) #ip route 10.10.20.0 255.255.255.0 172.16.1.2

Swansea (config) #ip route 192.168.10.0 255.255.255.0 172.16.1.1.

The 'ip route' command creates the static route, while 10.10.20.0/24 and 192.168.10.0/24 are remote networks to each other; whereas, 172.16.1.2 and 172.16.1.1 represent the next hop addresses for respective networks.

When using the exit interface, the configuration will be as follows:

Cardiff (config) #ip route 10.10.20.0 255.255.255.0 s0/0/0

Swansea (config) #ip route 192.168.10.0 255.255.255.0 s0/0/0

Table 1: Routing table output from Cardiff router

Cardiff#show ip route

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - Periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets
S 10.10.20.0 [1/0] via 172.16.1.2
172.16.0.0/30 is subnetted, 1 subnets
C 172.16.1.0 is directly connected, Serial0/0/0
C 192.168.10.0/24 is directly connected, FastEthernet0/0
```

The above table (Table 2) depicts the routing table of Cardiff router. As shown above in table 2, when the specific static route is configured, it is identified with the code's' in the routing table.

Default route or gateway of last resort is used to send packets with a remote destination network not included in the routing table. In this case, the packets are being sent to the next-hop router or out an exit interface. Default routing should be used on stub networks and on router that is connected to the Internet Service Provider. When default route is configured, it can route traffic to unknown network across the Internet [8].

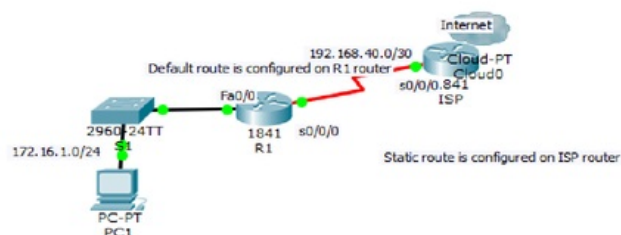


Figure 3: Configuration of static default route

Referring to Figure 3, R1 needs a default route to reach the Internet and it can be configured as follows:

R1 (config) #ip route 0.0.0.0 0.0.0.0 192.168.40.1. This is using next-hop router's ip address; whereas, when using the router's exit interface, the default route is configured as shown next: **R1 (config) #ip route 0.0.0.0 0.0.0.0 s0/0/0.** The last configuration with the exit interface shows that when there is no an entry in the routing table for the required network, it needs to forward the packet out **serial 0/0/0**.

Table 2: Routing table output from R1 router

R1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - Periodic downloaded static route

Gateway of last resort is 192.168.40.1 to network 0.0.0.0

```
172.16.0.0/24 is submitted, 1 subnets
C 172.16.1.0 is directly connected, FastEthernet0/0
192.168.40.0/30 is submitted, 1 subnets
C 192.168.40.0 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 192.168.40.1
```

As displayed in Table 1, the 's' verifies that the route source is a static; whereas, the asterisk (*) in table 2 identifies this route as a possible candidate to be the default route.

2.1.4 Dynamic Routing

Router learns about remote networks in two ways:

- Static routes
- Dynamic routes

As discussed earlier, configuring and maintaining static routes within a large networks require operational and administrative overheads. Thus, it is difficult and inefficient to manage when changes occur within the network. Static routing can be advantageous in a small networks; whereas, dynamic routing is used in a large networks [8] [2].

Dynamic routing is the process of implementing routing protocols on routers to update routing tables and find networks for communication. Dynamic routing protocols reduce the burden of configuration and maintenance tasks. In data networking, dynamic routing provides optimal routing by allowing routing tables in routers to be updated as the possible routes change [6] [4]. Routers use dynamic routing protocols to share information about remote networks.

Graziani and Johnson in [9 p151] define routing protocols as: "The set of rules, processes, algorithms, and messages that are used to exchange routing information and populate the routing table with routing protocol's choice of best paths".

For dynamic routing to take place, it is routing protocol that facilitates the exchange of routing information between routers. Dynamic routing protocols have been used in networks since the late 1980s and one of the first routing protocols was Routing Information Protocol (RIP). It was released as RIPv1 in 1988. Then it was updated to RIPv2 to accommodate growth in the network environment. However, RIPv2 could not scale to the large network implementations. To address the needs of large networks, an advanced routing protocols such as Open Shortest Path Routing protocol (OSPF), Intermediate System-to Intermediate System (IS-IS) were developed. Cisco also first developed the Enhanced Interior gateway Routing Protocol (EIGRP).

2.2 An overview of IPv6

2.2.1 IPv6 Essential

IPv6 has features and functionalities that will satisfy the requirements of future growing modern networking technologies [4]. This implies that the development of IPv6 is to handle the growth rate of the Internet and to cope with the demanding requirements on services, mobility, and end-to-end security.

IPv6 protocol is installed as a software upgrade in most devices and operating systems and it needs only activation or configuration. In addition, the transition mechanisms to IPv6 does not put the current IPv4 infrastructure at risk [10]. IT industry, governmental, business organisations and Internet service providers need to adapt to IPv6. The evolution of the Internet and services requires that all sorts of devices and items need IP addresses for permanent Internet connections. For example, car manufacturers' plans to design the networked car need some IP addresses per car. These addresses can be used to monitor, maintain, and access to services such as weather and traffic information. Its address size has been increased from 32 bits to 128 bits or 16 octets, thus, mathematically; the new address space provides the potential for a maximum of 2^{128} , or 3.403×10^{38} unique addresses [11] [12]. Therefore, IPv6 outperforms in generating 3.403×10^{38} unique addresses as compared to 4.3×10^9 unique IP addresses in IPv4. The main benefits of IPv6 can be an increased addressing capacity, capability, quality of services control, mobility, built in IPSEC security and improved routing efficiency [6].

Migration from IPv4 to IPv6 is not a straightaway process as it requires some developing mechanisms [3] [6] [7] [10]. Hence, for some time in the future, both IPv4 and IPv6 will coexist. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously to allow them to coexist on the same network. In addition, tunnelling mechanism transports an IPv6 packet over IPv4 networks.

The development of the new IP schema (IPv6) has removed the limitation of the IPv4 schema [6]. IPv4 relies upon higher level protocols to handle authentication and encryption of packets and this can lead to vulnerabilities when deploying IPv4 systems. This security issue can be solved by IPv6 as it uses integrated Internet

Protocol Security (IPsec) [13] [12]. IPsec provides authentication and encryption using cryptographic keys within the IPV6 protocol [14].

IPV4 does not include Quality of Service mechanisms; whereas, IPV6 supports Quality of Service (QoS) through the use of flow control bits.

QoS mechanisms enables routers to prioritise packets based upon QoS considerations and economise storage by aggregating routing tables [6].

2.2.2 Types of IPv6 Addresses

In IPV4, the well-known addresses are unicast, broadcast and multicast addresses. Broadcasts have been eliminated in IPV6 as they are not efficient. The types of IPV6 addressing and communication methods can be seen as follows:

Unicast Address. This address is a single interface identifier to uniquely identify an interface of an IPV6 node [15]. Packets sent to a unicast address is delivered to the unique interface. It is the point-to-point or one-to-one communication.

Multicast Address. A set of interfaces that are belonging to different nodes in a group of IPV6 interfaces [8]. A packet sent to a multicast address is processed by all members of the multicast group. Multicast is a multipoint communication and also known as a one-to-many. An IPV6 multicast addresses are always start with FF.

Multicast and IPV6 Internet Control Message Protocol work together to perform auto configuration of a host [8]. An auto configuration of a host is accomplished by using IEEE's Extended Unique Identifier (EUI-64). ICMPV6 Neighbour discovery protocol replaces Address Resolution Protocol (ARP) and assists discover neighbour and routers on the link. In addition, ICMPV6 discovers and configures Domain Name Service (DNS) for hosts. DHCPV6 enabled hosts do not require any DHCPV6 server to acquire IP addresses as they can be auto-configured.

Link-local Addresses. These addresses are not meant to be routed just the same as private addresses in IPV4 [15]. Link-local addresses always start with FE80::/10. The first 16 bits of link-local address is set to **1111 1110 1000 0000** which is equivalent to **FE80**. A small LAN can be created using the link-local addresses to share and access files and services locally.

Global Unicast Addresses. These are publicly routable addresses in a similar way as they are in IPV4. Global unicast addresses begin at 2000:: /3.

An IPV6 address consists of the first 48-bits for the network prefix and then 16-bits for the subnet ID to identify subnets. Finally, the last 64-bits are assigned for interface ID or device ID.

Anycast Address. This is a new communication mode and can be used by a device, but may not be used as a source address.

Anycast address is assigned to multiple interfaces on multiple nodes [14]. Packets sent to Anycast address is delivered to the topologically nearest interface of nodes in a group of potential receivers [8]. This address has a one-to-any communication mode.

2.3 Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRPv6)

The two well-known dynamic routing protocols are Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF). Both routing protocols are the members of Interior Gateway Protocols which are used for intra-autonomous system routing, that is, routing inside an autonomous system. Even though EIGRP combines the advantages of link-state and distance vector routing protocol, it is still a distance vector routing protocol [7] [2] [16]. However, EIGRP has several features that are not commonly found in other distance vector routing protocols, such as: RIPv1, RIPv2 and IGRP.

EIGRP does not have a map of the network topology as it is the distance vector routing protocol; thus, EIGRP only knows about remote networks information through its neighbours.

2.3.1 Establishment of EIGRP Neighbour Relationships

Routers must first establish adjacencies with their neighbours for EIGRP to send and receive routing updates [2]. EIGRP uses hello packets for neighbour discovery and establishing adjacencies with neighbours. Hence, routers running EIGRP form adjacencies with neighbours by exchanging EIGRP hello packets. In addition, EIGRP uses light-weight hello packets to monitor the connection status

of its neighbours. The neighbour relationships are used to track the status of neighbours; hence, EIGRP sends hello packets every 5 seconds on most networks; whereas, every 60 seconds on NBMA networks such as Frame Relay, ATM and X.25 [17] [18]. The hold time on most networks is 15 seconds; while it is 180 seconds on NBMA networks which is 3 times the hello packets. Hello packets are multicast and they do not use the reliable transport; therefore, response is not required from the recipient.

2.3.2 Features of EIGRP

As already described, EIGRP has several features that are not found in other distance vector routing protocols. These features can be listed as follows:

- Reliable Transport Protocol (RTP)
- Bounded updates or partial updates
- Diffusing Update Algorithm (DUAL)
- Establishing adjacencies
- Neighbour and topology tables
- Support for multiple network layer protocols
- Fast convergence
- Use of multicast and unicast

Comparing to traditional distance vector routing protocols, EIGRP does not age out routing entries or use periodic updates. EIGRP maintains topology table. This topology table is separate from the routing table and it includes the best path and any loop-free backup paths.

2.3.3 EIGRP Packet Types

EIGRP uses the following five packet types:

- Hello packets
- EIGRP update packets
- EIGRP query and reply packets
- Acknowledgment packets

Hello messages are used to establish neighbour-ship or adjacency and to help neighbouring routers realise when the new peer has connected or an old one has gone down [17] [19].

EIGRP enabled routers must also continue receiving hello packets from their neighbours to maintain neighbour relationship and keep existing neighbour relationship alive. As long as EIGRP router receives hello packets from a neighbouring router, it assumes that the neighbour router and its route remains viable.

EIGRP update packets are used by EIGRP to transmit the actual routing information. Update packets are sent only if a change occurs and are sent only to those routers that require the routing information.

The update packets always use reliable delivery. In general, EIGRP update packets are multicast to 224.0.0.10 for IPv4 and FF02::A for IPv6 just similar to EIGRP hello packets. However, during the initial exchange of routes between two new EIGRP neighbours, update packets are unicast rather than multicast; therefore, update packets can be sent to a single neighbour using unicast or to a group of neighbours using multicast. Instead of sending the entire contents of the routing table, EIGRP sends incremental updates when the state of a destination changes [20]. This feature minimises the bandwidth usage that is required for the EIGRP packets.

Query and Reply packets are part of the DUAL process and play an important part in the diffuse computations (calculations). They always use reliable delivery. Query can use multicast or unicast; whereas, replies are always sent as unicast. Query packets sent when a router loses a successor route and has no feasible successor (DUAL Query).

Acknowledgment (Ack) packets are used to confirm the receipt of an EIGRP packet. Acknowledgments are always sent as a unicast address.

2.3.4 DUAL Concepts

EIGRP utilises the Diffusing Update Algorithm (DUAL). This feature distinguishes EIGRP from the rest of distance vector routing protocols.

DUAL provides EIGRP with the fastest route convergence time among all routing protocols [21]. DUAL is an algorithm which handles route computations and determines the best loop-free path and loop-free backup paths [22]. In the process of route paths selection, the distance in the network from an origin to a destination is taken into account.

Those paths with length equal to the shortest paths are selected for data packet transport. DUAL finite state machine embodies the decision process for all routes computations and tracks all routes advertised by all neighbours [7] [2]. The DUAL finite state machine is an abstract machine which contains all the logic for calculation and comparison of routes in an EIGRP network.

DUAL terminologies are explained as follows:

Feasible distance: This is the cost between the local router and the destination prefix. In the routing table entry, feasible distance is the metric listed as the second number inside the brackets [2] [15].

Advertised distance: Advertised distance, also known as reported distance, is the cost from the next hop to the destination prefix (network). This is the metric to the remote network which is reported by the neighbouring router. It is also the routing table metric of the neighbour which is displayed as the second number in the parenthesis in the topology table [8] [2].

Successor is the best lowest cost route to the destination. EIGRP uses successor route to forward data traffic to a destination network and is stored in the routing table. The IP address of the successor is displayed in the routing table entry just after the word via [2].

Feasible successor: This is the next best route to the destination network. To be a feasible successor, a neighbour router must satisfy the feasibility condition. The feasibility condition is met when a neighbour's advertised distance to a network is less than the local router's feasible distance to the same destination network [2]. The feasible successor is the backup route and stored in the topology table [8].

When DUAL does not perform its diffusing computations to determine a path for a network, the route is in a stable mode. This condition is known as the passive state; whereas, if the DUAL recalculate or search for a new path, the state will be in an active mode.

If the neighbouring router does not satisfy the feasibility condition, DUAL will have no a feasible successor. However, this does not mean that there is not another path to that remote network. DUAL finite state machine searches for and finds a feasible successor for the route in the EIGRP topology table. Then the new successor will be installed into the routing table [8] [2] [21].

2.3.5 EIGRP Tables

An EIGRP uses the following tables for its operation:

Neighbour table: After an EIGRP neighbour relationships are established, all the neighbours' addresses and the interfaces are stored in an EIGRP neighbour table [7].

When newly discovered neighbours are learned, their addresses and interfaces are recorded in the neighbour table. This table lists all neighbours with which it formed adjacency and exchange routing information.

Topology table: It has already been explained in 2.3.3 that an EIGRP uses update packets to exchange routing information. These updates populate the topology table.

All the routing information received from neighbours is stored in an EIGRP topology table [7] [2] [23]. This implies that each router stores its neighbours' routing tables in its EIGRP topology table. The topology table lists all the paths to all destinations learned.

Routing table: DUAL runs computations against the topology table, and then picks the best routes and adds them into the routing table. The routing table holds the best metric routes that are used to send the data traffic.

2.3.6 EIGRP Metrics

EIGRP uses the following values in its composite metric to calculate the preferred path to a destination network. These values are:

- bandwidth
- delay
- reliability

- load

By default, only bandwidth and delay are used. A maximum transmission unit (MTU) is included in the routing table updates; however, EIGRP does not use it as a routing metric [8] [2].

The composite metric consists of values K1 through K5 and they are known as metric weights [2]. By default K1 and K3 are set to 1; whilst K4 and K5 are set to 0. Thus, the result is that only the bandwidth and delay values are used in the computation of the default composite metric [2]. The show ip protocol command is used to verify the K values.

The show interface command is used to examine the actual values used for bandwidth, delay, reliability and load in the computation of the routing metric. The bandwidth is displayed in kilobits per second (kbps).

On most serial links the bandwidth metric defaults to 1544 kbps [2]. However, if the actual bandwidth of the link differs from the default bandwidth of the interface, it requires to modify the bandwidth by using the interface command bandwidth. EIGRP uses the slowest bandwidth in its metric calculation to reach the destination network.

Delay is a measure of the time it takes for a packet to traverse a route [7]. It is expressed in a microseconds. Reliability is a measure of the probability that the link will fail or how often the link has experienced errors. It is measured dynamically with a value between 0 and 255, with 1 being a minimally reliable link and 255 being 100 percent reliable [7] [8] [2].

2.3.7 EIGRPv6 Routing

Most of routing protocols in IPv4 have been modified to be used for longer IPv6 addresses and different header structures [8] [12]. IPv6 routing protocols are similar to IPv4. However, IPv6 prefix is four times larger than an IPv4 prefix; hence, routing updates have to carry more information. Much of the theory, in main important parts such as DUAL and metrics are the same; however, configuration and operation can slightly differ.

Table 3 displays a comparison for EIGRPv4 and EIGRPv6 as follows:

Table 3: Comparing EIGRPv4 and EIGRPv6 [22]

Characteristic	EIGRPv4	EIGRPv6
Advertised routes	IPv4 networks	IPv6 prefix
Distance vector	Yes	Yes
Convergence technology	DUAL	DUAL
Metric	Bandwidth and delay by default, reliability and load are optional	Bandwidth and delay by default, reliability and load are optional
Transport protocol	RTP	RTP
Update messages	Incremental, partial, and bounded updates	Incremental, partial, and bounded updates
Neighbour discovery	Hello packets	Hello packets
Source and destination addresses	IPv4 source address and 224.0.0.10 IPv4 multicast destination address	IPv6 link-local source address and FF02::10 IPv6 multicast destination address
Authentication	Plain text and MD5	MD5
Router ID	32-bit router ID	32-bit router ID

As described in table 3 by [22], some of the similarities shared by EIGRPv4 and EIGRPv6 are:

- DUAL is used for route calculation and selection with the same metrics
- Scalability to large network implementation
- Neighbour, routing, and topology tables are maintained in both EIGRPv4 and EIGRPv6
- Both equal-cost load balancing and unequal-cost load balancing are offered
- Similar to EIGRPv4, EIGRPv6 is an advanced distance-vector routing protocol with some link-state features

Some examples of differences are as follows:

- EIGRPv6 is designed to send IPv6 prefixes/lengths; whereas, EIGRPv4 uses subnet/mask
- EIGRPv6 uses IPV6 link-local address to establish neighbour relationship
- There is no automatic summarisation at the class boundaries as IPV6 has no concept of classful network
- EIGRPv4 uses multicast destination address of 224.0.0.10; whereas, EIGRPv6 uses multicast destination address of FF02::A (A= 10 in hexadecimal notation)

- Hellos are sourced from the link-local address and destined to FF02::A (all EIGRPv6 routers)

EIGRPv6 enabled routers exchange messages between neighbouring routers on the same link or subnet. The exchanged messages are always sent from the source IPv6 address, which is the IPv6 link-local address of the exit interface of the router that is performing the forwarding.

Routers will not forward any packets with link-local source or destination addresses.

EIGRPv6 uses its link-local addresses to exchange establish adjacencies [12]; therefore, manually configured link-local addresses are easier and more recognisable. Routers use their link-local address as the default gateway address in their router advertisements [12] [22].

2.3.8 Configuration of EIGRPv6

To configure the EIGRPv6, the knowledge of EIGRPv6 and IPv6 addressing are required. By default, IPv6 traffic forwarding is disabled; therefore, it needs to enable it as follows:

Router (config) # ipv6 unicast-routing. This enabling process has to be done on each interface individually as EIGRPv6 is enabled directly on the interface without the network command. Configuration of EIGRPv6 will be discussed in design and implementation section.

2.4 Open Shortest Path First routing protocol for IPv6 (OSPFv3)

OSPF is a link-state routing protocol for IP networks and is based on the shortest path first algorithm. It was developed to replace Routing Information Protocol RIP [24]. This routing protocol uses the shortest path first (SPF) algorithm. The SPF or Dijkstra's algorithm was first formulated by a Dutch computer scientist and mathematician Edsger Wybe Dijkstra for finding the shortest paths between nodes in a network topology [25].

2.4.1 OSPF features

As explained by [7] [12] [23], the key features of OSPF protocol are as follows:

- ❖ OSPF is classless by design; therefore, it supports VLSM and CIDR
- ❖ No periodic updates. When a new link comes up or a link becomes unavailable, an OSPF sends only a partial update to all its neighbours.
- ❖ The shortest path first (SPF) tree is used to calculate the best routes
- ❖ It quickly propagates network changes; hence, it is fast convergence
- ❖ It works well in small and large network sizes
- ❖ Routes can be grouped into areas to support a hierarchical system; thus it uses the concept of areas for scalability
- ❖ It supports Message digest 5 (MD5) authentication

2.4.2 Establishment of OSPF Neighbour Relationships

In an OSPF operation, there are three main elements: Neighbour discovery, link-state information exchange, and best-path calculation. An OSPF router must form adjacencies before they can share information with their neighbouring routers.

The OSPF routers send hello packets out all OSPF-enabled interfaces to determine whether there are any neighbours on those links. The information in the hello packets includes the OSPF router ID of the router sending the hello packet.

Before two routers can form an OSPF neighbour adjacency, they must agree on three values: hello interval, dead interval, and network type. The OSPF interval shows the frequency an OSPF router transmits its hello packets. By default, the OSPF hello packets are sent every 10 seconds on multi-access and point-to-point networks; whereas, every 30 seconds on non-broadcast multi-access (NBMA) networks such as Frame Relay, ATM, and X.25.

2.4.3 OSPF Packet Types

OSPF exchanges messages to convey routing information using five types of packets as shown below and on the next page:

- Hello packets

- Database Description packets (DBD)
- Link-State Request (LSR)
- Link-State Update (LSU)
- Link-State Acknowledgement (LSAck)

The purpose of the above given packets are used to discover the neighbouring routers and also to exchange routing information to maintain accurate information about the network [4]. OSPF enabled routers need to recognise each other on the network, and then they can share information [2]. When an OSPF enabled router sends hello packets out all interfaces, the other OSPF enabled router attempts to establish a neighbour adjacency with that neighbour. After adjacencies are established, routers start exchange link-state advertisements (LSAs) [26]. The LSAs are flooded to other directly connected neighbours until all routers in the area have all LSAs [27].

The CPU processes the neighbour and topology tables using Dijkstra's SPF algorithm [8].

A shortest path first tree is constructed first and then the routing table is populated with resulting best paths. The SPF tree is used to calculate the best routes.

2.4.4 OSPF Terminology

Some important OSPF terms will be described as follows:

Link. When an interface is added to the OSPF process, it is considered by OSPF to be a link. This link or interface has state information associated with it. For example, up or down. In addition, one or more IP addresses can be associated with the interface or link for OSPFv2 protocol; whereas, OSPFv3 connects to a link instead of IP subnet and this will be explained in section 2.4.6.

Router ID. The OSPF router ID is used to uniquely identify each router in the OSPF routing domain. The router ID is simply an IP address used to identify the router [6-8].

Cisco routers derive the router ID based on the following three criteria:

- An IP address can be configured with the OSPF **router-id** command
- With no router ID configuration, the router chooses the highest IP address of all configured loopback interfaces
- If no loopback interfaces are configured, the router chooses the highest IP address of all active physical interface

Neighbour. Two or more routers that have an interface on a common network are considered as neighbours. OSPF-enabled router directly shares routes only with neighbours that have also established adjacencies.

Neighbour-ship database. This database contains a list of all OSPF routers for which hello packets have been seen. The router ID and state are also maintained on each router in the neighbour-ship database.

Topological database. This database contains information from all of the Link-state advertisement packets that have been received for an area.

2.4.5 OSPF Metric

The OSPF metric is known as cost. The cost is associated with the output side of each router interface and can be configured by the network system administrator. With the lower cost, the more likely the interface is used to forward data traffic [2] [28]. In Cisco IOS software, the cost value is the cumulative bandwidth of the outgoing interface from the router to the destination network.

The cost for an interface is derived by dividing 10^8 by the interface bandwidth in bits per second (bps). Therefore, interfaces with the higher bandwidth values will have a lower calculated cost; thus, the lowest-cost route is the preferred route in routing metrics [2]. For example, interface type with Fast Ethernet and faster have the cost value of 1, which is dividing $10^8/100,000,000$ bps=1; whereas, $10^8/10,000,000=10$ with Ethernet inter interface connection. Interfaces with a bandwidth of 100 Mbps and higher have the same OSPF cos of 1. The value 10^8 is called the reference bandwidth [8].

2.4.6 Similarities and differences between OSPFv2 and OSPFv3

The similarities between OSPFv2 and OSPFv3 can be explained as follows on the next page by [12]:

- OSPFv2 and OSPFv3 are both link-state routing protocol
- In both OSPFv2 and OSPFv3 the metric is defined as cost
- OSPFv3 uses the same five basic types as OSPFv2 as described previously in section 2.4.3
- Link-State Advertisement (LSA) flooding mechanism in OSPFv2 remains unchanged in OSPFv3
- Both OSPFv2 and OSPFv3 use a 32-bit number for the router ID represented in dotted-decimal notation
- DR/BDR election process remain the same in both cases
- Neighbour discovery mechanism also remain unchanged in both routing protocols

Differences between OSPFv2 and OSPFv3 are outlined by [12] and [15] as follows:

- To communicate between nodes at the link layer, OSPFv3 uses the term link instead of subnet or network
- OSPFv3 does not require a network mask to form an adjacency. OSPFv3 runs on per link instead of per subnet; thus, adjacency is formed on the link local
- OSPFv3 introduces new LSA types. Two new types of LSAs are Link-LSA (Type 8) and Intra-Area-Prefix LSA (Type 9). Some existing LSA types were also renamed
- OSPFv3 has different packet format
- Interfaces can have multiple IPV6 addresses
- OSPFv3 uses multicast address of FF02::5 (all OSPF routers) and FF02::6 (all OSPF DRs)
- OSPFv3 protocol uses IPsec security mechanism to protect its routing updates; whereas, OSPFv2 uses Message Digest 5 (MD5) authentication
- OSPFv3 requires that a router ID is configured before routing can begin
- In OSPFv3 IPV6 addresses are located within the payload; whereas, in OSPFv2 IP addresses are located within the packet header.

2.5 Related works

EIGRP routing protocol has the characteristics of both a distance vector and a link-state routing protocols [7] [2]. It enables a router to share information it knows about the network with a neighbouring routers within the same logical area of an autonomous system. In the past, the disadvantage of using EIGRP was that routers from other vendors than Cisco were not able to utilize EIGRP; however, it has become an open standard since 2013 [5].

The growth of Internet and evolution of high speed data networks has led to the inevitable adoption of IPv6 [4]. This implies that, the IT industry, governmental, business organisations and internet service providers need to adapt to IPv6. Thus, IPv4 routing protocols will be replaced with IPv6 compatible routing protocols to ensure effective networking system operation within an IPv6 environment.

In order to support IPv6, EIGRP has undergone some changes; however, EIGRP's features for IPv4 have been integrated into IPv6 [5]. The similarities and differences have been discussed in section 2.3.7 table 3. Understanding these changes is important when comparing and evaluating EIGRPv6 with others routing protocols for IPv6 such as OSPFv3.

Choosing the most appropriate and best routing protocols for specific networks depends on the requirements and business needs of organisations [2] [29]. Many studies have been done on EIGRP which discussed its appropriate deployment in networks with very specific routing metric requirements. In addition, researchers found out that EIGRP can be deployed in networks which require very fast convergence times.

A number of researchers such as [1-5] have conducted a comparison and evaluation of EIGRPv6 and OSPFv3 using different network simulators and Cisco hardware. All researchers argue that the performance parameters that should be considered in the selection of the right routing protocol for the specific network scenario are: Scalability of the network, utilisation of resources, security mechanism, packet loss, packet delay variation, and convergence speed.

EIGRP maintains both successor and feasible successor routes in its topology table. Thus, whenever the successor route goes down, EIGRPv6 immediately

installs the feasible successor into the routing table; hence, convergence is very fast.

EIGRP combines the advantages of link-state and distance vector routing protocol; thus, described as a hybrid routing protocol as described by [9]. However, some network professionals argue that it is still a distance vector routing protocol [7] [2] [16]. EIGRP routing updates are event-driven that it sends updates only when the path or the metric for a route changes [30]. This implies that instead of periodically, an update will be sent when needed.

Most researchers compared the behaviour of EIGRP routing protocol with others routing protocols. For example, comparing to OSPF routing protocol, EIGRP does not demand a lot of resources from router as it does not undergo Designated Router (DR) and Back up Designated Router (BDR) election process. Cooling cost is also saved as EIGRP produces less heat when performs routing process.

OSPF has to perform DR and BDR election process in multi-access and Non-Broadcast multi-access networks. In addition, the router ID has to be compared on each router. Hence, the above given findings indicate that a lot of delay can happen in case of OSPF comparing to EIGRP routing process. The performance evaluation was made with respect to the followings:

- Scalability of the network
- utilisation of resources
- security mechanism
- packet loss
- packet delay variation
- convergence speed

Different tests have been conducted by different researchers and as explained by [5] and [31], EIGRPv6 performs better within a point-to-point configuration rather than a LAN environment. OSPFv3 uses the IPsec authentication header (AH) and IPv6 encapsulating security payload (ESP). This security mechanism helps to secure the routing infrastructure from unauthorised access and prevent network attacks which can cause denial of service by compromising routing protocol deployment [6]. When EIGRP uses MD5 authentication mechanism, its performance negatively affected; whereas, IPsec noticeably improves OSPFv3's

performance [26]. In smaller and flat networks, EIGRPv6 is more efficient routing protocol. However, in larger networks, OSPFv3's hierarchical nature increases scalability and gives an advantage over EIGRPv6 [6].

The advantages of the hierarchical feature of multi-area OSPF are explained by [7] as follows:

- Smaller routing table entries as network addresses can be summarised between areas
- Reduced link-state update overhead which minimises processing and memory requirements as there are fewer routers exchanging LSAs
- Reduced frequency of SPF calculations

When comparing EIGRPv6 with OSPFv3 within small flat IPV6 enterprise network, EIGRPv6 outperforms OSPFv3 in terms of start-up and re-convergence speed [3-5].

Some advantages of EIGRPv6 are:

- Easy to configure
- Does not require to know much about network topology
- Works well in networks up to a certain size

Based on the comparison and evaluation of the two protocols performance by [3], [4] and [16], it can be argued that EIGRPv6 exhibited better CPU and memory utilisations and bandwidth control compared to ospfv3 through the intelligent use of metrics within DUAL algorithm.

When network grows larger, EIGRPv6 has some scaling limits. The scaling limitation of EIGRP is that it does not have a capability for setting internal boundaries which is important for controlling prefix summarisation and database sizes the way OSPFv3 allows [32].

Dynamic routing protocols play an important role in today's business environment. Routing protocols facilitate the exchange of routing information between routers. Several researchers like [2] and [29] have highlighted that Choosing the most appropriate and best routing protocols for specific networks depends on the requirements and business needs of organisations. The current trend of Internetworking growth requires adaptation of the routing for IPv6. This in return, requires investigating the performance of routing protocols in IPv6 network operation.

3. RESEARCH METHODOLOGY

A positivism research philosophy, which involves deductive approach methodology with literature review strategy, has been chosen. Positivism because knowledge gain will be based on the observation and collection of performance parameters (metrics) of both EIGRP and OSPF routing protocols in IPv6 networks by using latest Cisco packet tracer and GNS3 simulators. Collecting data about an observable reality and search for regularities and relationships in data reflects the philosophy of positivism [33] [34]. Moreover, deductive approach suits for collecting a quantitative data and measuring variables (performance metrics), then verifying and developing the existing theory and hypothesis of the above given routing protocols in IPv6 routed protocol.

Deduction approaches involve the development of a theory through rigorous tests [35]. This project will test the performance of EIGRPv6 and OSPFv3 routing protocols in IPv6 network operations by using Cisco lab, latest Cisco packet tracer software and GNS3 simulation. Testing will be carried out by collecting an appropriate data (performance metrics) from simulation results, the variables will be measured and analysed. Finally, based on the simulation results; this project will identify which of the two given routing protocols is more suitable and better in IPv6 network. An object-oriented approach may also be chosen as the lab simulation environment will be involved. Using simulation software reduces the time taken to configure, run simulation, analyse and collect an appropriate data. Object-oriented can be beneficial for simulation based data gathering [33]. Strategy is a plan of action to achieve a goal [36]. The research strategy of this project will be laboratory based research and by using simulation software. The data collection method (approach) will be based on structured observation as this project aims on fact findings and verification of the existing theory and hypothesis [34] [37].

A literature review is an essential part of any project [36]. It also crucial to the success of the project and boosts knowledge of chosen field. In addition, a literature review enables a researcher to identify if the topic of the project is feasible and highlights potential project issues. Therefore, using a document review (literature) strategy enables to understand and critically analyse which of the two given routing protocols is more suitable in IPv6 network operation.

As discussed by [35], a well-conducted literature review allows researchers to establish credibility through intensive and crucial evaluation of relevant research works. Hence, reading is an essential part of the research process. The role of literature review can help in exploring academic books, conferences, and journal-based research studies. It also helps in writing up a well-organised major project report.

As emphasized by [35], a thorough literature review is essential in comparing, contrasting, and correlating various academic books, journal articles, and other relevant sources that are directly related to this project work. Thus, a detailed theoretical background of EIGRP and OSPF and their IPv6 versions and modifications have been reviewed accordingly. Hence, literature review is not only self-education process, but it also fact-finding and fact-checking mission.

The research methodology for this project involves experiments using Cisco lab routers and relevant simulation works. The chosen research topic is suitable with using theory and hypothesis to identify data (performance parameters) of EIGRP and OSPF routing protocols in IPv6 networks and compare the results for evaluation. For these reasons, the literature review will be one of the research strategies. Performance comparisons and evaluations will be conducted in Testing and Evaluation section.

Alongside with Cisco lab, the relevant network simulations will be GNS3 and the latest Cisco packet tracer 6.2. Using the above mentioned simulator software and Cisco dedicated hardware in a laboratory environment will be a clear and concise methodology for this research as most relevant performance parameters can be gathered for comparison and evaluation of EIGRPv6 and OSPFv3 [5] [24]. Some researchers such as [1] [17] [18] [23] have used Opnet simulator. QualNet simulation software is also available at the UWTSD computer laboratory. For this research, Opnet, QualNet, and Riverbed Modeler Academic Edition (Opnet it Academic Guru) network simulators will not be used. The reason for this is that all these simulators do not support EIGRPv6. Cisco has opened up its EIGRP routing protocol as an open standard in order to help companies operate in a multi-vendor environment [38]. However, apart from Cisco packet tracer and GNS3 network simulators, other simulation software do not support EIGRPv6.

For this research process and precise comparison, both routing protocols should be conducted using the same experimental methodology. Hence, a comparison and evaluation of EIGRPv6 and OSPFv3 will be conducted using Cisco equipment in a laboratory environment.

Moreover, performance parameters will be gathered using dedicated Cisco hardware and Graphical Network Simulator (GNS3). The simulation process consists three scenarios:

- Using default bandwidth (1544 k bit/sec) of both EIGRPv6 and OSPFv3
- Changing the bandwidth to 64 k bit/sec
- Implementing security mechanisms for both routing protocols to test the effects after implementation

To meet the objectives that have been set in section 1, 16 dedicated Cisco routers will be connected by a serial links in a laboratory environment. After cable connection, EIGRPv6 routing protocol will be configured based on the above mentioned three scenarios.

Firstly, Network Time Protocol (NTP) should be configured by implementing the correct clock set and clock time zone to get the synchronised NTP status on all 16 routers. Several experiments will be carried out on each routers based on EIGRPv6 routing protocol and then the average results will be recorded in table as required.

The second step will be to execute several experiments to investigate the performance of OSPFv3 routing protocol on all 16 Cisco routers. Similar to EIGRPv6, the average results will be recorded in table.

To examine the performance of EIGRPv6 and OSPFv3 in a multi-access network scenario, Graphical Network Simulator (GNS3) will be used. Seven to eight routers will be connected to each other through several switches. A comprehensive and thorough comparison and evaluation of EIGRPv6 and OSPFv3 will be conducted in the multi-access network.

CHAPTER 4- DESIGN AND IMPLEMENTATION

4.1 Design

To conduct a comprehensive and thorough comparison between EIGRPv6 and OSPFv3, different network topologies have been designed with point-to-point and multi-access network scenarios as shown below:

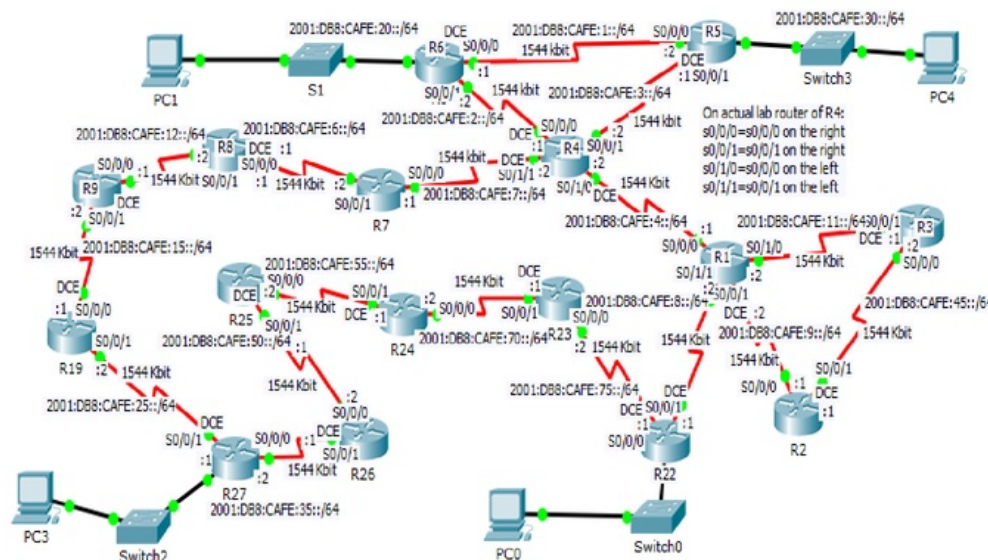


Figure 4: Mesh Point-to-point network topology

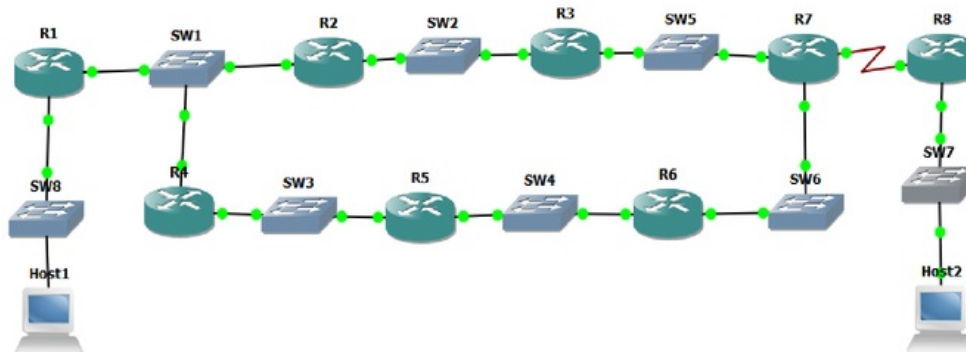


Figure 5: Multi-access network topology in GNS3 simulator

In the first topology, all routers are connected to each other through serial links. This type of network topology is known as point-to-point network [4] [16]. In the second topology, the seven routers are connected to each other through the switch which is further connected to the eighth router through serial links using GNS3 network simulator. This type of network is called multi-access network [4] [16].

Furthermore, to meet the objectives that have been set in section 1, a series of controlled experiments have been performed using Cisco packet tracer 6.2, GNS3 and dedicated Cisco equipment.

As shown in point-to-point topology diagram, 16 cisco routers are interconnected in a laboratory environment to investigate the performance of EIGRPv6 and OSPFv3 routing protocols. Referring to the mesh point-to-point diagram, R1 and R4 have four serial links. The rest of 14 cisco routers are with two serial links and all 16 routers are interconnected through serial links.

As depicted on the mesh one-to-one topology diagram, the link between each router indicates the default bandwidth of Cisco routers as 1544 Kbits per second.

4.2 Implementation

Several researchers in computer networking profession use network simulators such as Opnet and QualNet, while some employ Cisco hardware in a laboratory environment to assess the performance of EIGRP for IPv6 and OSPFv3.

Even though QualNet simulation software is available at the UWTSD computer laboratory. For this research, Opnet, QualNet, and other commercial network simulators have not been used. The reason for this is that apart from Cisco packet tracer, commercial network simulator (cannot be afforded for this experiment) and GNS3 network simulators, other simulation software do not support EIGRP for IPv6. Therefore, for this research process and precise comparison, both routing protocols should be conducted using the same experimental methodology. Hence, a comparison and evaluation of EIGRPv6 and OSPFv3 has been conducted using Cisco equipment in a laboratory environment, Cisco packet tracer and GNS3 simulation software.

Firstly, Network Time Protocol (NTP) was configured by implementing the correct clock set and clock time zone to get the synchronised NTP status on all 16 routers.

The purpose of NTP configuration was to get exact same time-reading on all routers for the accurate calculation of neighbour-down detection time and re-convergence speed. The following output shows that the clock is synchronised on all routers.

```
R4#show ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is
2**24
reference time is DAACF3F7.8DA56A1A (14:08:55.553 gmt Mon Apr 4 2016)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000
s/s
system poll interval is 16, last update was 3 sec ago.
```

The second step was assigning IPv6 addresses by configuring the global unicast addresses and link-local addresses per interface on all routers. After implementation of IPv6 addresses per interface, IPv6 unicast-routing have been enabled to configure EIGRP for IPv6 routing protocols.

4.2.1 Configuration of EIGRPv6

Using the topology diagram in figure 4, the global unicast address of 2001:db8:cafe::/48 network has been assigned and subnetted accordingly. The global unicast addresses are configured on each router per interfaces manually and this is similar to configuring a static IPv4 addresses.

As discussed by [7] and [12] the global unicast addresses are globally routable and reachable in the IPv6 Internet. These addresses are equivalent to public IPv4 addresses.

Besides the global unicast addresses shown on the mesh point-to-point network topology diagram, each router has been manually configured with a link-local unicast addresses.

Both EIGRP for IPv6 and OSPFv3 employ a link-local unicast addresses for establishing adjacencies and other messages [12]. Thus, a static link-local unicast addresses have been configured manually in the FE80::/10 format using the **IPv6 address link-local command**. Hence, it is easier for these two routing protocols to use manually configured link-local addresses that are more recognisable.

By default, IPv6 traffic forwarding is disabled; therefore, it requires enabling IPv6 as follows:

Router (config) # ipv6 unicast-routing. Hence, firstly, IPv6 routing has been enabled on each of the 16 routers with the **IPv6 unicast-routing command**. Then, the configuration of EIGRP for IPv6 begins with the **ipv6 router eigrp 1** command in global configuration mode to create an EIGRP for IPv6 routing process using the as number 1.

EIGRP for IPv6 is configured on interface basis and networks are advertised based on interface command. IPv6 EIGRP requires a router-id in IPv4 format in dotted decimal notation. When configured on interface, EIGRP for IPv6 is initially placed in a shutdown state; therefore, the no shutdown command is required to activate the EIGRP for IPv6 routing process.

The second step in the configuration of EIGRP for IPv6 process is to enable the protocol on each router's interfaces. The output from the show run on R1 router is displayed below and on the next page:

```
interface Serial0/0/0
  no ip address
  ipv6 address 2001:DB8:CAFE:4::1/64
  ipv6 eigrp 1
  no fair-queue
!
interface Serial0/0/1
  no ip address
  ipv6 address 2001:DB8:CAFE:9::2/64
  ipv6 eigrp 1
  clock rate 64000
!
interface Serial0/1/0
  no ip address
  ipv6 address 2001:DB8:CAFE:11::2/64
```

```
ipv6 eigrp 1
!  
interface Serial0/1/1  
no ip address  
ipv6 address 2001:DB8:CAFE:8::2/64  
ipv6 eigrp 1  
clock rate 2000000
```

4.2.2 Configuration of OSPFv3

The ipv6 unicast-routing must be enabled on any IPv6 routing protocols. Thus, to start OSPFv3, the first step is to execute **ipv6 unicast-routing** in global configuration mode on all routers.

The second step is to perform **ipv6 router ospf process-id** global command on each router to begin the configuration process of OSPFv3 on routers. Similar to EIGRP for IPv6, OSPFv3 routing protocol requires a 32-bit value for the router ID with IPv4 address notation. Thus, the **router-id** command in router configuration mode must be configured on all routers in the topology diagram.

Finally, interfaces on all routers are enabled for OSPFv3 by using the **ipv6 ospf process-id area area-id** command. However, firstly, IPv6 addresses must be configured on all interfaces of each router. Similar to EIGRP for IPv6, OSPFv3 is configured directly on an interfaces of each router and does not require to use the network router configuration mode command. The process-id value must be the same as the process id used to create the routing process in the **ipv6 router ospf process-id** command.

The link-local address can be configured per interfaces on each router using the same interface command to create IPv6 global unicast address; however, the link-local keyword must be added to the **ipv6 address** command as follows:

R1 (config) # interface fa0/0

R1 (config-if) # ipv6 address fe80::link-local

The output from the show run on R1 router is displayed below and on the next page:

```
interface Serial0/0/0  
bandwidth 64  
no ip address
```

```
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:CAFE:4::1/64
ipv6 ospf 1 area 0
no fair-queue
!
interface Serial0/0/1
bandwidth 64
no ip address
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:CAFE:9::2/64
ipv6 ospf 1 area 0
clock rate 64000
!
interface Serial0/1/0
bandwidth 64
no ip address
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:CAFE:11::2/64
ipv6 ospf 1 area 0
!
interface Serial0/1/1
bandwidth 64
no ip address
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:CAFE:8::2/64
ipv6 ospf 1 area 0
clock rate 2000000
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
ipv6 router ospf 1
router-id 1.1.1.1
log-adjacency-changes
area 0 authentication ipsec spi 500 sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

5. TESTING AND EVALUATION

5.1 Test scenarios

As discussed in section 4, three test scenarios for each topology have been designed and implemented to assess the performance of EIGRP for IPv6 and OSPFv3.

The three scenarios are as follows:

- Using default bandwidth (1544 k bit/sec) of both EIGRPv6 and OSPFv3
- Changing the bandwidth to 64 k bit/sec
- Implementing security mechanisms for both routing protocols to test the effects after implementation

For all three scenarios, the inputs were configuration of EIGRP for IPv6 and OSPFv3 routing protocols. Several tests had been executed and the average results were gathered in both point-to-point and multi-access topologies and recorded in table 4 and 5 respectively.

Table 4: Test summary for point-to-point network scenario

	EIGRPv6			OSPFv3		
Test Details	With default bandwidth of 1544 kbits/s	With bandwidth of 64 kbits/s	With Authentication	With default bandwidth of 1544 kbits/s	With bandwidth of 64 kbits/s	With Authentication
Re-convergence time	2.5 s	3 s	3.2 s	4.2 s	3.6 s	3.5 s
Neighbour down detection time	1.5 s	1.9 s	2 s	2.1	2 s	1.9 s
Packet loss during start-up	0%:Referring to figure 7, 100% success rate	-	-	40%:Referring to figure 6, 60% success rate	-	-

Table 5: Test summary for multi-access network scenario

	EIGRPv6			OSPFv3		
Test Details	With default bandwidth of 1544 kbits/s	With bandwidth of 64 kbits/s	With Authentication	With default bandwidth of 1544 kbits/s	With bandwidth of 64 kbits/s	With Authentication
Re-convergence time	2.6 s	2.8 s	3.5 s	6 s	5.9 s	5.8 s
Neighbour down detection time	14 s	12 s	13 s	35 s	31 s	32 s
Packet loss during start-up	0%: Referring to figure 8, 100% success rate	-	-	100%:Referring to figure 9, 0% success rate	-	-

```
R27#ping 2001:db8:cafe:20::1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 2001:db8:cafe:20::1, timeout is 2 seconds:
```

```
..!!!
```

```
Success rate is 60 percent (3/5), round-trip min/avg/max = 11/24/32 ms
```

Figure 6: Ping result from OSPFv3 in point-to-point network Cisco Lab experiment

```
R27#ping 2001:db8:cafe:20::1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:db8:cafe:20::1, timeout is 2 seconds

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 6/35/70 ms

Figure 7: Ping result from EIGRP for IPv6 in point-to-point network Cisco Lab experiment

```
*Mar 1 00:00:05.943: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/3, changed state to down
*Mar 1 00:00:05.943: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:00:06.659: %DUAL-S-NBRCHANGE: IPv6-EIGRP(0) 1: Neighbor FE80::3 (FastEthernet0/0) is up: new adjacency
*Mar 1 00:00:06.695: %DUAL-S-NBRCHANGE: IPv6-EIGRP(0) 1: Neighbor FE80::2 (FastEthernet0/0) is up: new adjacency
*Mar 1 00:00:06.927: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
*Mar 1 00:00:06.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar 1 00:00:07.339: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
*Mar 1 00:00:07.395: %LINK-5-CHANGED: Interface Serial0/1, changed state to administratively down
*Mar 1 00:00:07.399: %LINK-5-CHANGED: Interface Serial0/2, changed state to administratively down
*Mar 1 00:00:07.415: %LINK-5-CHANGED: Interface Serial0/3, changed state to administratively down
*Mar 1 00:00:07.415: %LINK-5-CHANGED: Interface Serial0/4, changed state to administratively down
*Mar 1 00:00:07.427: %LINK-5-CHANGED: Interface Serial0/5, changed state to administratively down
*Mar 1 00:00:08.215: %NTP-6-PEERREACH: Peer 127.127.7.1 is reachable
Mar 1 00:00:08.215: %NTP-6-PEERSYNC: NTP synced to peer 127.127.7.1
Master#
Master#ping 2001:db8:cafe:10::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:10::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/85/100 ms
Master#
```

Figure 8: ping result from EIGRP for IPv6 in multi-access network (GNS3)

```
R1
Mar 1 00:00:08.159: %LINK-5-CHANGED: Interface Serial0/4, changed state to administratively down
Mar 1 00:00:08.175: %LINK-5-CHANGED: Interface Serial0/5, changed state to administratively down
Mar 1 00:00:08.175: %LINK-5-CHANGED: Interface Serial1/0, changed state to administratively down
Mar 1 00:00:08.191: %LINK-5-CHANGED: Interface Serial1/1, changed state to administratively down
R1#
R1#ping 2001:db8:cafe:10::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:10::1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
Mar 1 00:00:49.303: %OSPFv3-5-ADJCHG: Process 1, Nbr 4.4.4.4 on FastEthernet0/0 from LOADING to FULL, Loading Done
R1#
Mar 1 00:00:52.183: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from LOADING to FULL, Loading Done
R1#ping 2001:db8:cafe:10::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:10::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/93/116 ms
R1#
```

Figure 9: ping result from OSPFv3 in multi-access network (GNS3)

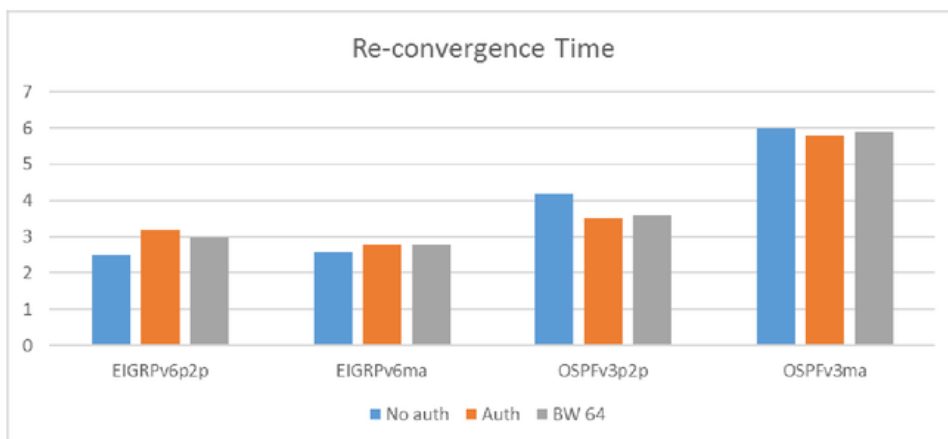


Figure 10: EIGRPv6 and OSPFv3 Re-convergence Time Comparison

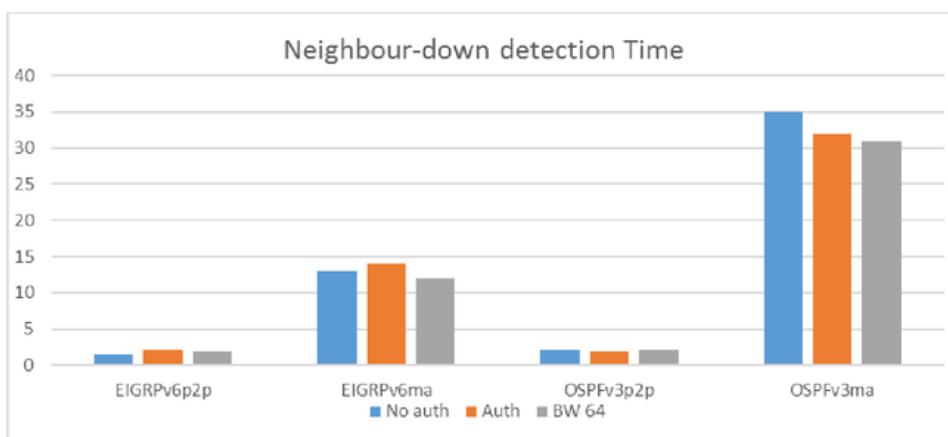


Figure 11: EIGRPv6 and OSPFv3 Neighbour-down detection Time Comparison

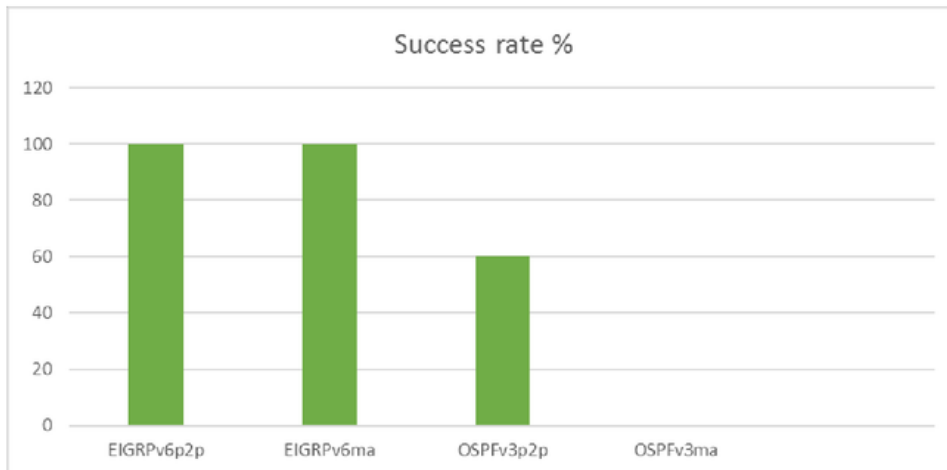


Figure 12: EIGRPv6 and OSPFv3 Round-Trip Success rate Comparison from cold start

5.2 Test Analysis

A number of key findings can be analysed and discussed as follows:

1. As shown by figures (10-12), EIGRP for IPv6 performs better than OSPFv3, irrespective of the topologies. However, EIGRP for IPv6 took marginally longer to re-converge in the multi-access network. In addition, the performance of EIGRP for IPv6 decreases after the implementation of the security mechanism. The activation of MD5 authentication reduced the protocol's performance considerably.
2. Findings shown in figure 10 reveal that Ipsec implementation slightly improved the performance of OSPFv3.
3. EIGRP for IPv6 performed better in point-to-point mesh topology compared to that of multi-access topology (figures 10-11).
4. As displayed by figure 11, for both routing protocols, the neighbour-down detection time is much longer in the multi-access network than in the point-to-point mesh network. The reason could be that the link-layer failure detection times vary depending on the physical media, layer two encapsulation used and intervening devices. For example, an Ethernet switch can hide link-layer failure from routing protocol peers.

5. As depicted by figures (6-9), OSPFv3 took longer to converge during cold start compared to EIGRP for IPv6. OSPFv3 requires mapping the entire network at the beginning as it is a link-state routing protocol. Thus, its convergence speed is much slower than that of EIGRP for IPv6 specifically during cold start up.
6. Figure 12 shows that the round-trip success rate for OSPF is 0% in the multi-access network compared to 60% success rate in the point-to-point mesh network. On a broadcast multi-access network, routers need to choose one router as a Designated Router (DR) and another router as to be a Backup Designated Router (BDR). This election process may contribute to the slow convergence speed in the multi-access network compared to the point-to-point network. In point-to-point networks, there are no DR or BDR concepts and routing information is flooded to each networking device.
7. Figure 10 shows that the re-convergence time of EIGRP for IPv6 in both topologies increased when the bandwidth was changed to 64 kilobits per second. Neighbour down detection time also increased in the point-to-point topology as shown by figure 11. However, the neighbour down detection time decreased in the multi-access topology.

As discussed by [7] [2] [21] a higher bandwidth has a lower cost or metrics for both EIGRP and OSPF; whereas, a lower bandwidth indicates a higher cost or metrics as the cost of an interface is inversely proportional to the bandwidth of an interface. Hence, when the bandwidth is changed to 64 kbit/s, the cost increases and this results in an additional overhead and time delays.

In contrast, the re-convergence time for the OSPFv3 considerably reduced in the point-to-point network, while it is slightly reduced in the multi-access network when the bandwidth was changed to 64 kbit/s as shown by figure 10.

Based on the key findings, EIGRP for IPv6 has performed better in all scenarios compared to OSPFv3. Therefore, the results indicate that EIGRP for IPv6 is the best choice for both point-to-point and multi-access networks as it not only converges faster from cold start, but also it has a faster re-convergence speed when a topology change occurs.

6. CONCLUSIONS AND RECOMMENDATIONS

This dissertation paper has compared the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) routing protocols in IPv6 network operations.

The aim was to assess the performance of these routing protocols in an IPv6 network environment. In the near future, there will be devices and services that may not be developed with IPv4. This indicates that the growth of Internet and evolution of high speed data networks has led to the inevitable adoption of IPv6. Hence, it is important to understand, investigate and identify the most appropriate dynamic routing protocols in an IPv6 network environment.

To achieve this aim, the following objectives have been set in organised and planned steps:

The first step was to conduct a literature review in order to develop a thorough understanding of the features and characteristics of the two routing protocols.

The second step was investigating and gathering performance parameters used by other networking professionals to compare and evaluate EIGRP and OSPF in IPv4 and IPv6 routed protocols.

The main challenge of this project was obtaining appropriate simulator software that supports both EIGRP for IPv6 and OSPFv3. To overcome this issue, dedicated Cisco hardware had to be chosen to assess the required performance of EIGRP for IPv6 and OSPFv3. During the design and implementation phase, another problem was the availability of the Cisco laboratory room for use. However, the problems could be resolved by using an effective time management and coordination with the supervisor.

In the third step, the point-to-point mesh network topology was designed by using dedicated Cisco hardware and latest Cisco packet tracer 6.2 simulation software. In addition, a multi-access broadcast network scenario was created by using a Graphical Network Simulator (GNS3).

During the implementation step, some configuration issues were identified. For example, some Cisco routers that are available at the University's laboratory do not have the latest Cisco Internetwork Operating System (IOS) images that support IPv6 and some do not support EIGRP for IPv6 at all.

However, the problems were solved by extending the topology design and switching to other routers.

The fourth step involved a series of controlled experiments which were carried out on 16 Cisco routers in a mesh point-to-point network environment and on eight Cisco routers by using GNS3 in a multi-access network topology. The required performance parameters were gathered by using outputs from each router's command line and an accurate time set on all routers using a Network Time Protocol (NTP).

In order to conduct these experimental tests, three scenarios were set up as explained in section 5. After running several tests, the results were recorded in tables 4 and 5.

The key tasks in testing and evaluation can be summarised as follows:

- ❖ Analyse which one of the routing protocols re-converges faster after an unexpected link-failure
- ❖ Identify the response times when a change occurs such as neighbour down condition
- ❖ Examine each protocol's operational differences upon implementation of their authentication mechanisms
- ❖ Investigate which protocol converges faster from a cold start by pinging from source to destination as soon as the routing protocols are initially started

The results that have been generated and gathered reflect what is outlined and suggested in the literature review. Hence, the key findings essentially confirm what was expected at the beginning of this project.

Based on the key findings, EIGRP for IPv6 performed better in all scenarios compared to OSPFv3. Therefore, the results indicate that EIGRP for IPv6 is the best choice for both point-to-point and multi-access networks as not only converges faster from cold start, but also it has a faster re-convergence speed when a topology change occurs.

In order to assess the performance of dynamic routing protocols in a large network scenario, an appropriate network simulator software is recommended as it is not only time-saving, but also it can provide a wider range of performance parameters for comparison and evaluation of dynamic routing protocols.

7. REFLECTIONS

I have an academic background and work experience as an aviation engineer in the past. Because of my interest in the IT sector, I started to study Cisco Certificate Network Associate (CCNA) at the University of Wales Trinity Saint David in 2012. As my results and interest had increased I decided to study Computer Networking at this University as mature student.

I have learned about computer networking theory for the past three years. Now, this project work has enabled me to link my theoretical understanding of this discipline to the practical application.

Firstly, conducting a literature review of scientific research based on the features and characteristics of EIGRP and OSPF in an IPv6 network environment has enhanced my knowledge and understanding of these two popular routing protocols. The second step was putting my skills and knowledge to practical application.

In the beginning of the practical application, there was an issue of obtaining the required network simulator software to assess the performance of EIGRPv6 and OSPFv3. Thus, when I started design and implementation, I thought I was unable to conduct the practical application of this project. I have to admit that I was terrified and panicking. However, I am pleased that I was quickly able to manage by thinking of an alternative way to perform the required experiment.

One of my personal strengths is effective time management. I have always progressed from the beginning to the end of this whole project. Besides, I was able to meet my project supervisor once a week and obtained very useful guidance to resolve the problems that arose throughout the overall project work.

Even though I have presentation skills from my past experience as an aviation instructor, as well as at this university, I could not use these skills for the interim viva. The reason could be that I misunderstood the interim viva requirements. Hence, I was very disappointed and emotional when I failed to demonstrate my presentation skills.

Overall, it has been an excellent practical experience for me that I acquired the necessary skills and knowledge to manage more than 20 dedicated Cisco routers in a laboratory environment.

In addition, I have developed my confidence in configuration and troubleshooting of networking devices in real networking environments.

The way I conducted practical experiments was very time consuming and I was limited to a few performance parameters. Using network simulators would provide a wider range of performance metrics for the comparison and evaluation of dynamic routing protocols. Therefore, I would have done practical experiments better, if I had obtained an appropriate network simulator that supported the two routing protocols investigated in this project.

Project Planning

The following figure shows the project plan from the beginning to the submission date

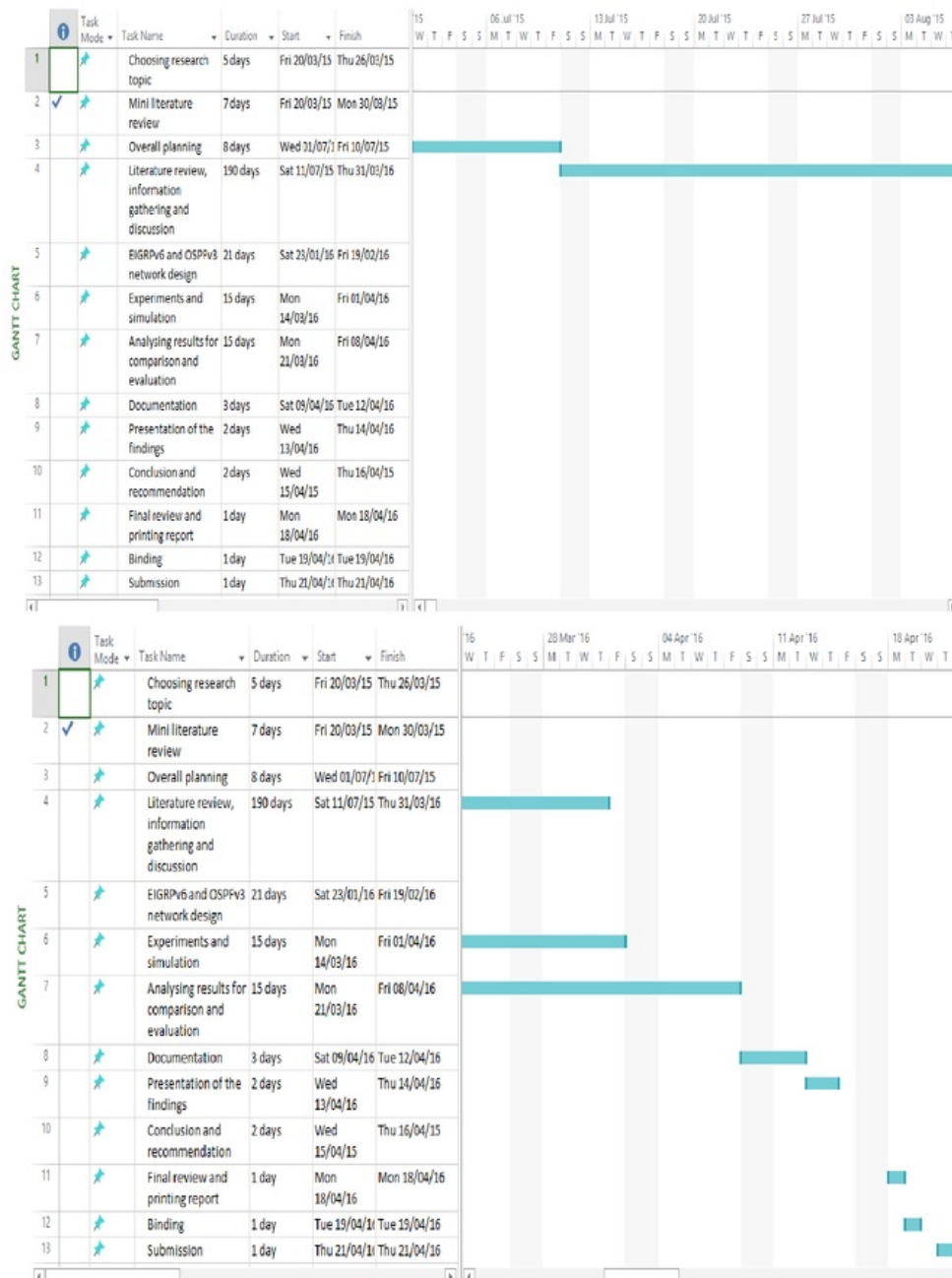


Figure 13: Project planning

8. REFERENCES

- [1] S. G. Thorenoor, "Dynamic routing protocol implementation decision between EIGRP, OSPF and RIP based on technical background using OPNET modeler," *2nd Int. Conf. Comput. Netw. Technol. ICCNT 2010*, pp. 191–195, 2010.
- [2] R. Graziani and a Johnson, *Routing Protocols and concepts, CCNA exploration companion guide*. 2007.
- [3] Y. N. Krishnan and G. Shobha, "Performance analysis of OSPF and EIGRP routing protocols for greener internetworking," *2013 Int. Conf. Green High Perform. Comput. ICGHPC 2013*, pp. 4–7, 2013.
- [4] C. Wijaya, "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network," *2011 First Int. Conf. Informatics Comput. Intell.*, pp. 355–360, 2011.
- [5] R. J. Whitfield, "A Comparison of OSPFv3 and EIGRPv6 in a Small IPv6 Enterprise Network," vol. 6, no. 1, pp. 162–167, 2015.
- [6] A. Hinds, A. Atojoko, and S. Y. Zhu, "Evaluation of OSPF and EIGRP Routing Protocols for," vol. 2, no. 4, pp. 287–291, 2013.
- [7] R. G. Diane Tear, Bob Vachon, *Implementing Cisco IP routing*. Indianapolis: Cisco press, 2015.
- [8] Todd Lammle, *CCNA Study Guide*, Seventh ed. Indiannapolis: Wiley publishing.
- [9] M. Kalendar, "Novel Processor Architecture for Modified Advanced Routing in NGN," pp. 486–491, 2011.
- [10] R. Guérin and K. Hosanagar, "Fostering IPv6 migration through network quality differentials," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 3, p. 17, 2010.
- [11] Cisco, "IPv6 Addressing," *Carcinogenesis*, vol. 35, no. 1, 2013.
- [12] R. Graziani, *IPv6 Fundamental*. Indianapolis: Cisco press, 2013.
- [13] W. N. A. W. Ali, A. H. M. Taib, N. M. Hussin, R. Budiarto, and J. Othman, "Distributed security policy for IPv6 deployment," *3rd ISESEE 2011 - Int. Symp. Exhib. Sustain. Energy Environ.*, no. June, pp. 120–124, 2011.
- [14] J. Veiga, A. Costa, and A. Santos, "Securing anycast communications in IPv6 networks by means of IPsec," *20th Int. Conf. Software, Telecommun. Comput. Networks (SoftCOM)*, 2012, pp. 1–7, 2012.
- [15] S. Hagen, *IPv6 Essentials*, Second. Sebastopol: O'Reilly Media.
- [16] C. K. Jha, P. Kumar, P. D. Parihar, and L. Garg, "Realisation of Link State Routing Protocol and Advance Distance Vector in Different IP Schema," *2014 Int. Conf. Comput. Intell. Commun. Networks*, pp. 486–491, 2014.
- [17] I. Fițișău and G. Todorean, "Network performance evaluation for RIP, OSPF and EIGRP routing protocols," *2013 Int. Conf. Electron. Comput. Artif. Intell. ECAI 2013*, no. 26, 2013.

- [18] K. Gehlot and N. C. Barwar, "Performance Evaluation of EIGRP and OSPF Routing Protocols in Real Time Applications," vol. 3, no. 1, 2014.
- [19] G. P. S. Kalyan, D. V. V. Prasad, A. R. Information, and P. Rip, "Optimal Selection of Dynamic Routing Protocol with Real Time Case Studies," pp. 219–223, 2012.
- [20] A. Sarikhani, M. Mahramian, and H. Hoseini, "Calculation of cisco router processing power for a large network with thousands of nodes," *ICSPS 2010 - Proc. 2010 2nd Int. Conf. Signal Process. Syst.*, vol. 3, pp. 757–762, 2010.
- [21] J. Dwyer and H. Jasani, "An Analysis of Convergence Delay Caused by Link Failures in Autonomous Systems," pp. 1–6, 2012.
- [22] A. Johnson, *Scaling Networks Compain Guide*. Indianapolis: Cisco press, 2014.
- [23] N. G. Com and N. I. L. Umar, "Algorithm It Follows 4He Majority of the Well Known Routing," pp. 934–938, 2014.
- [24] S. Jian, "Research and Implement ofOspfv3 in Ipv6 Network," pp. 743–746, 2011.
- [25] S. T. Niari and A. H. Jahangir, "Verification of OSPF Vulnerabilities by Colored Petri Net," *SIN '13 Proc. 6th Int. Conf. Secur. Inf. Networks*, pp. 102–109, 2013.
- [26] G. Nakibl, "O SP F V uln e rabilit y t o P e rsist e nt P o is o ning Atta c ks : A S y st e mati c Anal y sis."
- [27] B. Puype, D. Papadimitriou, and G. Das, "OSPF failure reconvergence through SRG inference and prediction of link state advertisements," *Acm Sigcomm ...*, pp. 468–469, 2011.
- [28] P. Boronat and P. Manzoni, "Efficient Metrics for Efficient Path Selection in Large Wireless Community Networks," pp. 85–92.
- [29] L. D. Circumarescu, G. Predusca, N. Angelescu, and D. Puchianu, "Comparative Analysis of Protocol RIP, OSPF, RIGRP and IGRP for Service Video Conferencing, E-mail, FTP, HTTP," *2015 20th Int. Conf. Control Syst. Comput. Sci.*, pp. 584–589, 2015.
- [30] A. Kaushik, "QoS Parameter Evaluation of UMTS under EIGRP , IGRP and RIP using OPNET," pp. 399–403, 2014.
- [31] A. Networking, "Performance Comparison of OSPF and IS-IS Routing Protocols in Dual-Stack Enterprise Networks Paris – Alexandros Roussinos Internal Examiner: Isam Wadhaj Submitted in partial fulfilment of the requirements of Edinburgh Napier University for the Degree of MSc in Advanced Networking School of Computing July," no. July, 2014.
- [32] G. Kuperman, L. Veytser, B. Cheng, S. Moore, and A. Narula-tam, "A Comparison of OLSR and OSPF-MDR for Large-Scale Airborne Mobile Ad-Hoc Networks," *MobiHoc*, pp. 17–21, 2014.
- [33] T. A. Saunders. M. Lewis. P, *Research Methods for business students*. Harlow: Pearson education limited, 2012.

- [34] M. Marder, *Research Methods for science*, 3rd ed. Cambridge: Cambridge University press, 2014.
- [35] Z. O'Leary, *Doing your research project*, 2nd ed. London: SAGE publications, 2014.
- [36] W. P, *Success in your project*. Harlow: Pearson educatio limited, 2004.
- [37] M. Breach, *Dissertation Writing for Engineers and Scientists*. Harlow (England): Pearson education limited, 2009.
- [38] E. Interior, G. Routing, I. R. F. C. This, H. Availability, W. Eigrp, I. Rfc, T. Eigrp, and I. G. Protocols, "Enhanced Interior Gateway Routing Protocol (EIGRP) Informational RFC Frequently Asked Questions," no. March, pp. 2–3, 2013.

