KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

KUMASI.

DEPARTMENT OF COMPUTER SCIENCE

COMPARATIVE ANALYSIS OF CONVERGENCE TIMES BETWEEN OSPF, EIGRP, IS-IS AND BGP ROUTING PROTOCOLS IN A NETWORK

BY

EUNICE DOMFEH ASABERE

A THESIS SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES,

KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY, KUMASI, IN

PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF

MASTER OF SCIENCE (MSC.) IN INFORMATION TECHNOLOGY

May, 2018

DECLARATION

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

EUNICE DOMFEH ASABERE . . . .
Student (PG2707314) Signature Date

Certified by:
MR. J. K. PANFORD . . . .
Supervisor Signature Date

Certified by:
DR. MICHAEL ASANTE . . . .
Head of Department Signature Date

DEDICATION

I dedicate this thesis to my family and friends for their encouragement and support and to my Boss, Stephen Anaafi for his unconditional support and guidance through the research.

ACKNOWLEDGMENTS

First of all, I praise God Almighty for His favour to me in completing this study work. I would like to express my earnest gratitude to my thesis guide, Mr. J. K. Panford for believing in my ability to work on this research. His profound insights has enriched my research work. My heartfelt thanks to Dr. J. B. Hayfron Acquah for consistently showing me innovative research directions for the entire period of carrying out the research. I am indebted to all the lecturers in the department of computer Science.

I would conclude with my deepest gratitude to my parents, siblings and all my loved ones. My full dedication to the work would have not been possible without their blessings and moral support.

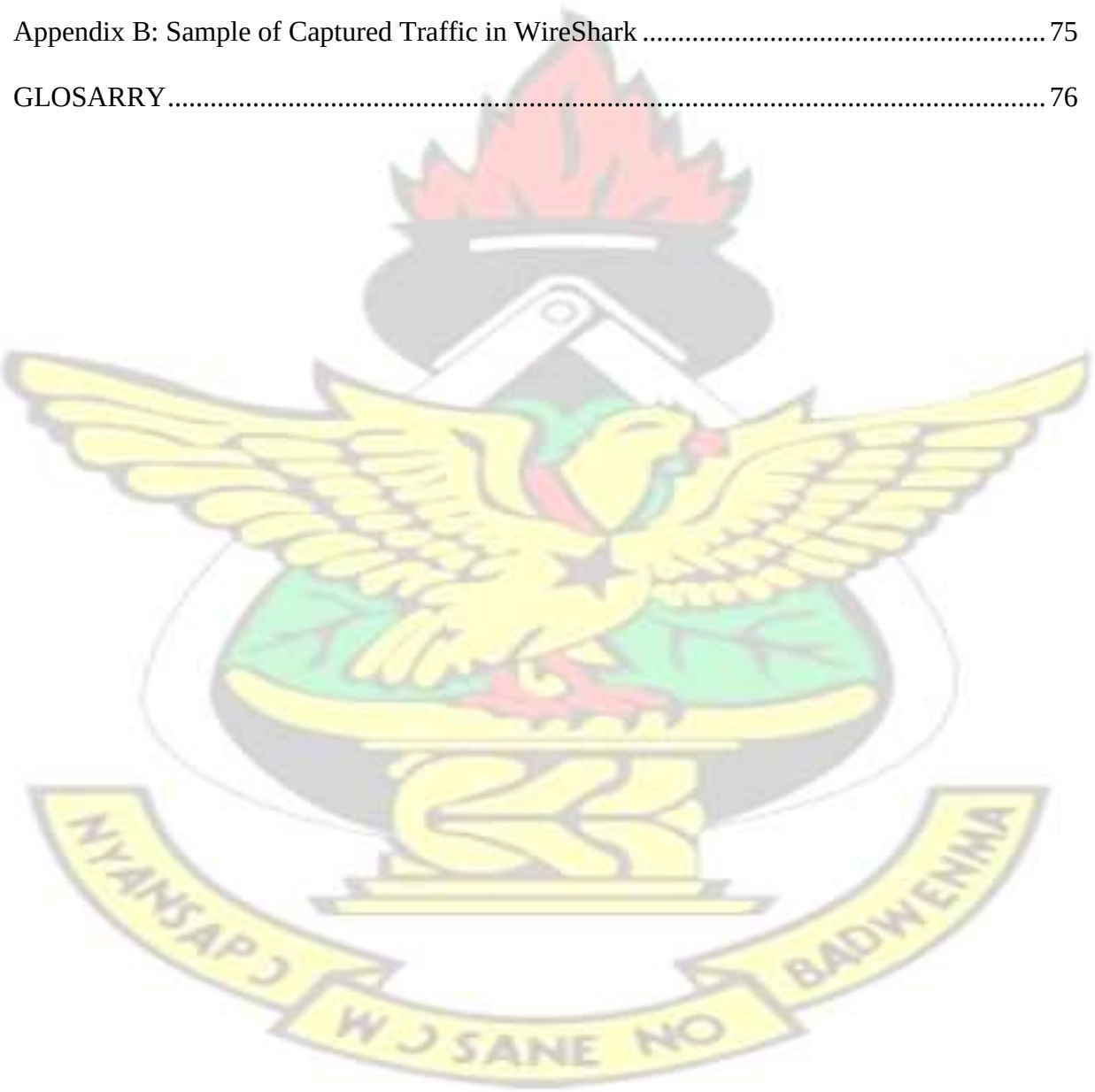
ABSTRACT

In a computer network, the transmission of data is based on the protocol which selects the best routes between any two nodes. Different types of protocols are applied to specific network environment. Routing protocol is one of the significant factor in determining the quality of IP communication. One of the factors that discriminate different protocols is convergence time. This time is one of the key factors which determines performance of the dynamic routing protocol. The time of convergence of a network is very essential and networks that converges faster are considered to be very reliable.

Routing protocols specify how routers communicate with each other by disseminating information. The router has prior knowledge about the adjacent networks which can assist in selecting the routes between nodes. There are different types of protocols in the IP networks. Four typical types of routing protocol are chosen as the simulation samples: OSPF, BGP, IS-IS and EIGRP

The primary objective of this research is to deliver an in depth understanding of OSPF, BGP, IS-IS and IGRP and compare the convergence duration of these protocols. A more detailed description of these four routing protocols will be included. In this thesis, GNS3 will be used to simulate OSPF, BGP, IS-IS and EIGRP in order to compare their attributes and performance. According to the convergence we can find out which protocols are suitable for different sizes and types of network.

TABLE OF CONTENTS



LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABR	Area Border Router
AD	Administrative distance
AS	Autonomous system.
BGP	Border Gateway Protocol
CPU	Central Processing Unit
DR	Dynamic Routing
DUAL	Diffusion Update Algorithm
DV	Distance Vector
EGP	Exterior Gateway Protocols
EIGRP	Enhanced Interior Gateway Routing Protocol
FD	Feasible Distance
FS	Feasible Successor
GNS3	Graphical network simulator
IGP	Interior Gateway Protocols
IS-IS	Intermediate system to Intermediate system
LS	Link State
LSA	Link state Advertisement
MTU	Maximum Transmission Unit
OSI	Open System Interconnection
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
SR	Static Routing

CHAPTER 1

INTRODUCTION

1.1 Background Study

In recent times, networks are developing quickly. Routers play a vital role in a network by providing efficient routing in the network. Their responsibility is to forward data packets from one point to another and also keep a watch on the data so that it remains in a controlled way. In the state within the network where all network router routing tables are complete and correct a network is said to have converged. According to (Panford *et al*, 2015), the period of resource sharing has demanded the adoption of computer networks. With the rapidly growing eagerness to share data between computer users in this present age, various forms of social media has taken over with the ability to contact friends and relatives either via video, voice or text in realtime. Due to the increase in the demand for these kind of internet applications, it is essential that the implementation of a best communication framework is applied to ensure that messages are delivered without delays. Routing protocols play a major role in the delivery of packets from source to destination addresses (Panford *et al.*, 2015).

The transfer of data from source node to destination node is referred to as Routing. Routing chooses the right route within a network and moves a packet through the network to another network's device (Chadha *et al.*, 2013). In other words, routing can be explained as pushing a packet from one device to another device on a different network. Regarding the host, routers do not seem to be concerned. Their main focus is the network's best path to each other (Malhotra, 2002). The destination host logical network address is employed for packets delivery to a network and then the host's hardware address aids in the delivery of the packet from a router to the correct destination host (Malhotra, 2002). A routing protocol shows how routers interact with each other and also disseminates information that helps in the selection of routes between nodes on a computer network (Devi *et al.*, 2015). It is the language spoken by

a router with other routers in order to share information on the status and reachability of a network (Forouzan, 2009). Routers with the help of protocols dynamically locate every network within an internetwork and also ensure that all routers have identical routing tables.

Basically, the route of a packet through an internetwork is determined by a routing protocol (Graziani *et al.*, 2008). Some common examples of protocols are EIGRP, OSPF and IS-IS. As soon as all the routers have knowledge about all networks, user data in the form of packets will be sent by a routed protocol through the established enterprise. The choice of the best path of communication is mainly the responsibility of routing algorithms. Routing and bridging are often contrasted. Their primary differences are the layer in which they are working. Routing algorithms employ metrics such as path bandwidth, reliability, delay, current load on a path and so on to ascertain the optimal path to a destination. During routing, information is first of all shared with immediate neighbours, then throughout the entire network. Each protocol has different configuration and different structure as compared to others. Routing protocols operate based on routing algorithms. The basic functionality of these protocols is to move the traffic through the network and the router must know where routers push the data in to be able to get to the destination (Singh *et al.*, 2013).

The configuration of routing tables within routers is used to establish routing. Routing table configuration can be done in two different ways. These two ways are static routing and dynamic routing. SR can be explained as the method of manually entering routes into a router's table with the help of its configuration file which is loaded in the process of device start up. The changes that happen in the logical network layout must be done manually by the network administrator in SR. DR however permits routers to choose the most appropriate path when there is a layout change in the logical network (Archana, 2015). The implementation of SR is easier in small networks. SR is safe and can be predicted as the path to the destinations do not change but remains the same. Routing algorithms or update mechanisms are not required

therefore no demand for additional resources such as memory and CPU. On the contrary, DR is suitable for large network topologies where multiple routers are needed. There is always an automatic detection of better routes if there is a topology change and it also has scalability as an advantage. DR is a better choice for medium, large, and very large inter network because of their ability to scale and recover from internetwork faults. It is further grouped into distance vector (DV) and link state (LS) routing protocols (Archana, 2015). Routing protocols are very important to a networks design (Graziani *et al.*, 2008). DR protocols run alone on routers that use them so as to get networks and update their routing tables (Kisten *et al.*, 2003). For the network administrator, using DR is simpler as compared to the use of SR method, however its cost is a lot in terms of router CPU process and bandwidth in the links. A router operating under DR shares routing information with its neighbour routers and additional CPU cycles and additional bandwidth is required to achieve that. DV protocols, with the help of simple algorithms, calculate cumulative distance value between routers based on hop count. LS protocols however make use of sophisticated algorithm that maintain complex database of internetwork topology. In communication networks today, DR protocols are being used instead of SR protocol. A set of routers operating under the same administration is known as an autonomous system (AS) or a routing domain. In IP networks, there are a lot of different routing protocols. Three common classes that are known are:

1) Interior gateway routing over link state routing protocols that communicate within an AS. LS protocols make use of complex algorithms that is responsible for the maintenance of the database of the internetwork topology. Example are OSPF, IS-IS.
2) Interior gateway routing over distance vector routing protocols use simple algorithms in the calculation of the distance value based upon hop count. Example of DV protocols are RIP, EIGRP.

3) Exterior gateway routing protocols that communicate between the two or more autonomous system. Example of exterior protocol is BGP (Border Gateway Protocol). BGP is used on the internet for the exchange of traffic between AS.

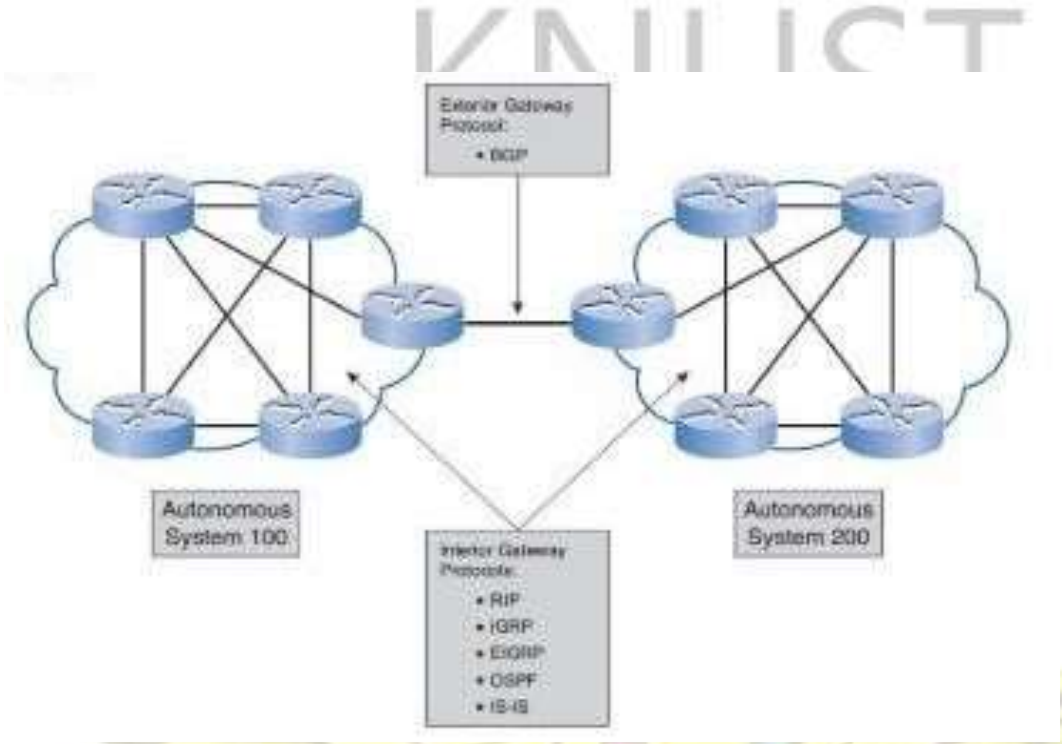


Figure 1.1: IGP VRS EGP (Lammle, 2005).

Figure 1.1 illustrates the design of IGP against EGP. IGP operates within an AS and EGP between ASs. Open Shortest Path First (OSPF) is classified under LS routing protocols. Each router here calculates its own shorter path towards the destination independently. The metrics used here are bandwidth and delay to route the packets. This protocol is preferred for large networks like internet (Singh *et al*, 2013). OSPF makes use of Shortest Path First (SPF) algorithm in the calculation of the best path.

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced version of IGRP, exclusive to CISCO. It combines the merits of LS and DV protocols. EIGRP is being used in both medium and large scale networks because of its scalability. It is a vastly used protocol

which uses DUAL for its routing computations. EIGRP, because of its LS protocol properties can be referred to as a hybrid protocol.

IS-IS (Intermediate System to Intermediate System) is classified under LS routing protocols and it was introduced by ISO. IS-IS routers perform the calculation of the cost of a route based on a single metric in order to exchange routing information. There are a great deal of similarities between IS-IS and OSPF. The design of IS-IS is in such a way that it provides routing within a domain and its network is made up of end systems, intermediate system, areas and domains. Routers acting as intermediate systems which are organized into groups are referred to as areas. The areas are also put together to form domains and the End systems are the user devices. To figure out the shortest route to a destination, the Dijkstra algorithm is employed. This protocol makes use of a LS database in the forwarding of packets. IS-IS adopts a two level hierarchical routing which allows a level 1 router to detect the topology; routers and host in the specific area but cannot know that of outside routers.

Reaching routing convergence is very critical and complicated. A change in topology comprising of a failure or recovery in link will cause an update in the routing tables which starts the convergence process. The table's updates is carried out by routers. These routers interact by a set of rules. Achieving fast convergence is the main goal of any protocol, while remaining simple, accurate, flexible and secured. This research will be carried out to analyse and compare the convergence times of four protocols: Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Intermediate system to Intermediate system (IS-IS) and Enhanced Interior Gateway Routing Protocol (EIGRP).

In the study, a simple network topology utilizing each protocol would be analysed. By examining the results, that is convergence times in particular, the best performing routing protocol for large and realistic network would be identified.

1.2 Statement of the Problem

A routing protocol under the OSI model is considered to be operated at layer three. Many different types of protocols are used in networks and one of the most important attributes or characteristics of protocols is the convergence. This attribute determines how fast the routers adapt their routing tables to topological changes.

EIGRP is a distance-vector protocol, owned by CISCO, which makes use of DUAL. IS-IS and OSPF are LS protocols and relies on the Dijkstra algorithm in the calculation of the lowestcost routes to all available destination but they have their differences and BGP is the pathvector protocol that provides routing information for AS on the Internet. Among these protocols, a proof-based advice for selecting the one with the best convergence time is aimed

at.

In this thesis, a study of the OSPF, EIGRP, IS-IS and BGP will be done and the advantages and disadvantages of using these protocols on a network will be looked at. The comparison analysis of these protocols would be carried out on GNS3 to ascertain the one with the best time of convergence.

1.3 Aims

The aim of this research is to comparatively study four routing protocols namely OSPF, BGP, IS-IS AND EIGRP to find their times of convergence in a network topology.

1.4 Objectives of the Research

The main objectives of this thesis are:

- To determine the convergence time for OSPF, BGP, IS-IS and EIGRP in a particular network topology.
- To compare the performance of OSPF, BGP, IS-IS and EIGRP.

1.5 Research Questions

The following are the research questions that were posed in order to accomplish the objectives.

- What is the convergence time for OSPF, BGP, IS-IS and EIGRP in a network Topologies?
- Which of the four routing protocols has the fastest convergence time in the topology used.

1.6 Hypothesis

In an effort to address the above mentioned questions, the following Hypotheses were put up.

H_0 – There is no significance difference between the performances of the Routing Protocol.

H_1 – There is significance difference between the performance of the Routing Protocol.

1.7 Significance of the Study

This study will be significant in offering an intensive understanding of the four routing protocols OSPF, BGP, IS-IS and EIGRP and determining the convergence time of these protocols in a network. The study will also compare the times of these protocols and come out with the best one.

1.8 Scope of the Study

The last couple of years, a lot of protocols have been proposed and enhanced to efficiently route data packets between nodes in a network. It is however not clear how different protocols behave in different environments. A protocol may be the suitable to use in one network topology but not suitable to use in another.

The scope of this work is associated with the coverage of convergence times OSFP, EIGRP, IS-IS and BGP routing protocols in a network.

1.9 Organization of Research

This research is grouped into five chapters to bring out a better understanding of the study. The first chapter offers the general concept regarding the theme of the work. It additionally discusses the brief and concise overview of issues involved, look at objectives, hypothesis, and importance of the study and scope of work.

The second chapter is of literature review which will be covering all the related topics in extra detail for further understanding. The motive of this chapter is to make the grounding of work intensive through all the searched and reviewed stuff in order that everything must be clear beforehand.

The third chapter is elaborates the research methodology and this is where the useful working way will be conferred in the step wise layout. This chapter discusses the procedures and approaches to be adopted for attaining the objectives.

The fourth chapter contains the Results and analysis of the work done in the previous chapter

The fifth and final chapter gives a Conclusion of the research and Recommendations that can be used to improve the work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The chapter gives a detailed review of studies conducted on the convergence of routing protocols. It is trusted that the inside and out clarification of the elements of the included protocols and IP conventions gives a broader knowledge foundation that is totally vital for the reader to grasp with the research. Other important areas that will give meaning to this research are presented in this chapter.

2.2 General Overview of Routing

2.2.1 Routing and Routing Protocols

Routing in computer networking is defined as the procedure amid which a packet data is moved or exchanged from a device source in a network, to a device destination in another network. A network gadget with specialized software called the router usually performs this procedure. Routers function on the Internet Layer of the TCP/IP protocol stack and are in charge of sending data packets. Each data packet is made up of the IP address of the source device and also the IP address of the device to which it is destined for. Routers after accepting a packet take choices. They look for the next hop device they ought to forward the packets, keeping in mind the end goal to ensure the delivery of the packet to the destination in the most ideal and fastest way. The routers adopts procedures to choose the best route for each destination network. Rules that are followed in order to exchange information with other routers about the networks that are reachable through them are referred to as routing protocols. Their responsibilities are the creation of routing tables at the routers end, the communication between them and therefore the procedure of learning new routes, and in the long run the choice of the best available path towards a destination according to protocol metrics. Routing can be in two forms static or

dynamic. Static routing is when the network administrator manually adds routes into the routers' routing tables and so network changes cannot be reflected. SR is normally used for smaller networks. On the other hand, DR is for scalable networks. It makes utilization of a DR protocol that helps it to automatically build routing tables through the exchange of route update information between neighbour routers. This kind of routing is the most widely recognised and can without much of a stretch adapt network changes such as network additions or link failures, making it imperative for large network infrastructures (Aslam, 2008).

2.2.2 Routing in IP Networks

The Internet is comprehensively grouped into networks referred to as Autonomous System. Examples of AS's are the internetwork of a university, a company, or an Internet Service Provider (ISP). The connection of a router to a network can be done through its interfaces and the connections among routers and networks define the topology. Figure 2.1 gives a picture of an AS with four routers (black squares) and four networks (clouds). The interfaces of Router r1 are i1, i2 and i3, which associate it to the networks n1, n2 and n3 respectively. Hosts h1 and h2 belong to the n1. Routers may be called neighbours in the event that they have interfaces to a common network. Every one of the routers are neighbours of r1. r2 however and r4 are not neighbours. The objective of the routers is to push packets between hosts that is the circles that are attached to the networks.

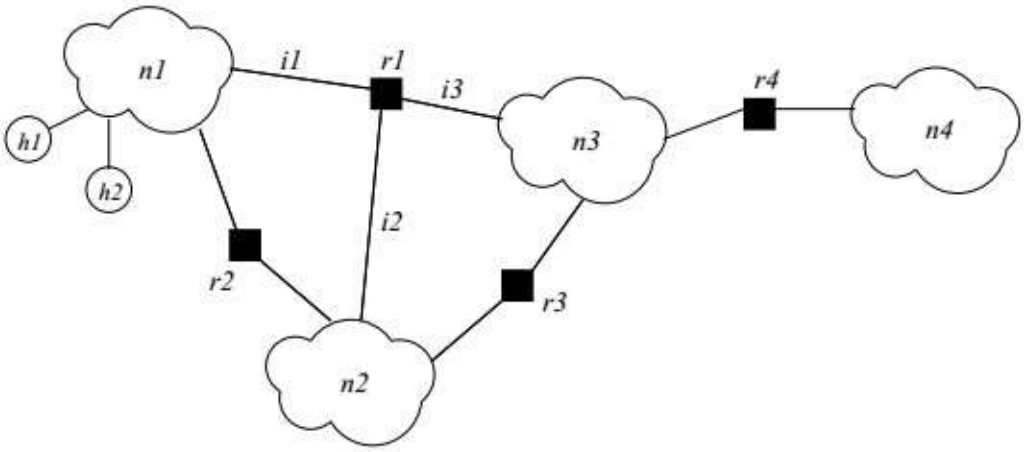


Figure 2.1: An Autonomous System (Obradovic, 2000).

On the arrival of a packet at an interface, the router has to decide the best and shortest path to the destination address. A router needs to choose when a packet arrives over one interface, which interface it should use to forward the packet nearer to its destination. To be able to make appropriate forwarding decisions, routers must keep partial information on the topology in their tables. The objective of a protocol is to build up a methodology for keeping these tables up to date. Routing information can be exchanged only locally (i.e. between neighbouring routers) in most cases. The overall aim of a protocol is to establish good global paths across the network. There are generally two levels on which routing on the internet happens. The first is where packets are directed towards their destination AS (that is external level). From that point onward, they are directed internally within the AS to the destination. The protocols for external routing between AS's are known as Exterior Gateway Protocols (EGPs). On the other hand the protocols for internal routing are Interior Gateway Protocols (IGPs). The main EGP is the BGP. IGPs are categorised into two classes. These are DV routing and LS routing. As part of the rollout of the internet the DV protocols were part. The DV routing used a mechanism where every router keeps information about the next adjacent router and the estimated number of hop to the destination router.

The information is intermittently advertised to adjacent routers and refreshed to get updates on information from the advertisements of adjacent routers. Amongst the many protocols under this category RIP is the best-known. EIGRP, is an example of a DV protocol. It is propriety to Cisco, a noteworthy router vendor. Simplicity is one major benefit of DV protocols. The correct implementation of RIP is easy and the protocol performs well on smaller networks. On the other hand, due to the fact that the network nodes do not keep an overall view of the network topology, they are limited concerning how much they can know and hence exploit the paths available to a destination. Specifically, RIP has minimal overall information available to the point that the protocol cannot anticipate and prevent slowness in convergence when the internetwork encounters failures. LS protocols uses a different approach to routing. There is an advertisement of the state of its links to other routers. The information, as it flows is recorded in the routers memory and with the help of this a map complete topology of the AS is created. This information is important in the calculation of complete routes and the determination of the next appropriate hop for moving a packet to its destination. The OSPF is the most pervasively used protocol. The fact that routers are furnished with global information is useful in deciding good routes, however there is significant complexity involved in the protocol that propagates the link states.

BGP is the prevailing exterior routing protocol in the Internet. The BGP can be said to be a hybrid between DV and LS protocols in the sense that advertisements portray complete routes, as opposed to hop counts. Moreover, the determination of a best route to an AS is a component of both the local router's policies and the best routes as determined by its neighbours. That is, BGP permits distance metrics based on hop count to be overridden by policy-based metrics.

2.2.3 Routing Basics

To route packets from one destination to another, a router must have information on (Lammle, 2005):

- The Destination Address
- Neighbour routers
- The most appropriate route to each remote network
- Possible routes to all remote networks
- Routing maintenance and verification

The router must set up a routing table which guides the connection of nodes to one another within the internetwork. It is made up of information on the path to follow and ways of achieving the remote network. The guide is based on the information shared among the nodes in the internetwork and the administrator can also build the routing table manually.

The topology is developed by updates of the nodes through what they send and receive. For the adjacent nodes, there is a way to reach neighbour nodes. In the event that a node does not have a direct connection then it must discover its path to the destination node. Information on the path can be obtained by the node through either SR or by DR. Static routing requires the manual generation and update of the route table by the administrator. The administrator inserts all network information into each nodes. Dynamic Routing is preferable to that of Static Routing.

In the case of the DR, there is an exchange of details between nodes based on the protocol set up in the node. The update of the data is done in the routing table. The sharing process begins in the event of a change in the internetwork. There is information exchange among the nodes until all nodes have the same information (Kumar et al., 2014).

2.2.4 Characteristics of Routing Protocols

The principal attributes of protocols are:

- Convergence

The time required for the routing tables to be updated in the network ought to be small to enable specific information involving routing to be accessed easily.

- Loop Free

The protocol ought to guarantee a path with no loop. This helps the routes to get the bandwidth available efficiently.

- Best Routes

To get to the destination network, the best route is chosen by the protocol.

- Security

Data transmission to a target network ought to be secured by the protocol.

2.3 Metrics and Routing

2.3.1 Metrics

Usually, the metric parameters employed in measuring a path determines its cost. The best route chosen by protocols is the one with the least metric value. Each protocol has a unique way of computing its metrics. The purpose of these metrics is to enable the protocols choose which path to use in transmitting packets.

2.3.2 Purpose of a Metric

The value assigned as a cost by routing protocols to get to a destination is termed as a metric. If there should arise an occurrence of multiple paths present in the same destination, metrics decide the best path. There are different approaches in the calculation of metrics for each protocol. For example, RIP utilizes hop count while OSPF makes use of bandwidth and EIGRP utilizes a blend of bandwidth and delay.

2.3.3 Metric Parameters

The measurement of a metric is used to choose the paths as a mean to rank them from most liked to least liked. Different protocols use different metrics. The following metrics are most often used in IP routing protocols (Islam & Ashique, 2010).

- **Bandwidth**: A path is chosen by bandwidth metric centered on bandwidth speed in this favoring high bandwidth over low bandwidth.
- **Hop count:** It takes count of the routers a packet crosses before getting to its target.
- **Delay**: The measure of time taken by a packet to move through a path. It relies on factors like link bandwidth, utilization and port queues.
- **Load:** It describes the use of traffic of a defined link. The best route is calculated by protocols based on the load.
- **Cost:** In determining an ideal route, the network administrator or Internet Operating System make cost estimates. The representation of the cost could either be one or more combination of metrics.
- **Reliability:** It computes the probability of a link to fail and this calculation can be done from previous failures or count of interface error.
- **MTU:** It represents Maximum Transmission Unit. It resembles the maximum frame length in octets which is permitted to pass to the internetwork without fragmentation.

2.4 Classification of Routing Protocols

The classification of protocols is as follows:

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

2.4.1 Static versus Dynamic Routing

Static routing is a procedure where the routing table is manually created and routes are fixed at router boot time (Lemma *et al*, 2010). There is a routing table update by the network administrator any time a new network is included or expelled in the AS. It is mostly applied to networks with small size, where it can be easily managed by an administrator. Its performance

reduces when there is a change in topology regarding the network. SR has its simplicity as its main advantage and also, more control is given to the systems administrator to maintain the entire network. The weaknesses of SR are that, it exhibits poor performance when there is a change in network topology and also difficult to manually setup every one of the routes. In DR neighboring routers constantly share information automatically with each other. Routing tables for each router is then updated to enhance consistency. The best routes are calculated using metrics and some routing rules. However, specific metrics which include delay, bandwidth, hops count and link cost are used to select the best route. Conventions that generate route information are used to update the values of these metrics.

One major merit of DR protocols is that, it aids network administrators in spending less time in the configuration and maintenance of routes. Its downside is that it may create several issues such as loops in routing and route instabilities.

2.4.2 Classful and Classless Routing

Routing protocols are divided, depending upon the subnet mask into classful and classless routing.

2.4.2.1 Classful Routing

In classful routing, the entire network topology have a common subnet mask and this kind of protocol omits in its routing updates, subnet mask information. A router upon receiving a route does the following:

- Directly linked routers to the major network's interface make use of a common subnet mask.
- Applies to the route a classful subnet mask when there is indirect connection between the router and the same main network.

Classful routing protocols are less pervasively used because:

- It is unable to support Variable Length Subnet Masks for hierarchical addressing.
- It omits routing updates.
- It cannot be utilized in sub-netted network.
- It is unable to support discontiguous networks.

Though classful protocols are useful in modern networks, they may not be applicable in every scenario, especially where subnet mask is needed. Two common classful protocols are RIPv1 and IGRP.

Figure 2.2 illustrates a classful routing protocol network which has a common subnet mask throughout the network.

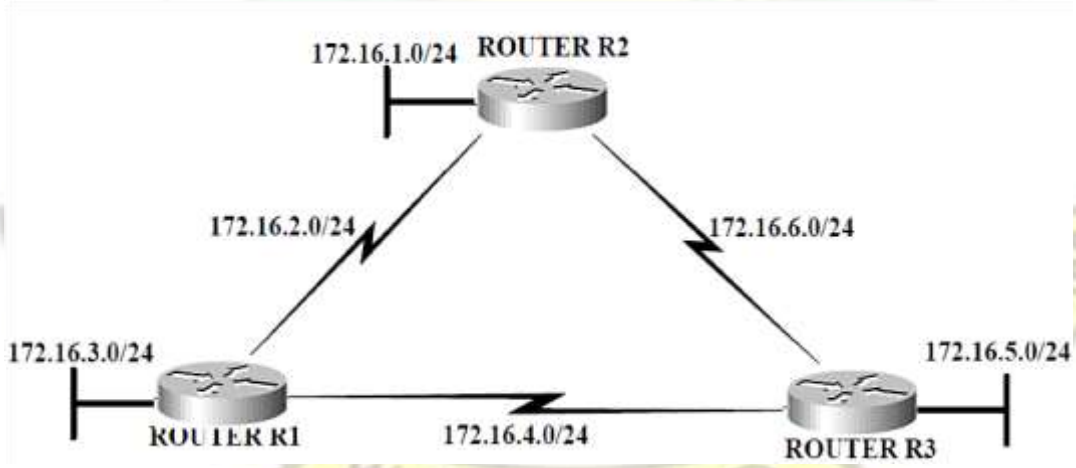


Figure 2.2: Classful Routing with Same Subnet Mask (Lemma *et al*, 2010).

2.4.2.2 Classless Routing

In classless routing, there can be variation in the subnet mask in the network topology and also in the routing updates. In today's networks, the practice of using the first outlet to find the subnet mask is not common and most networks do not rely on classes for allocation. Classless routing protocols provides support in discontiguous networks. Examples of classless routing family of protocols are RIPv2, EIGRP, OSPF, IS-IS and BGP. A classless routing in a network topology with different subnet mask is shown in Figure 2.3.

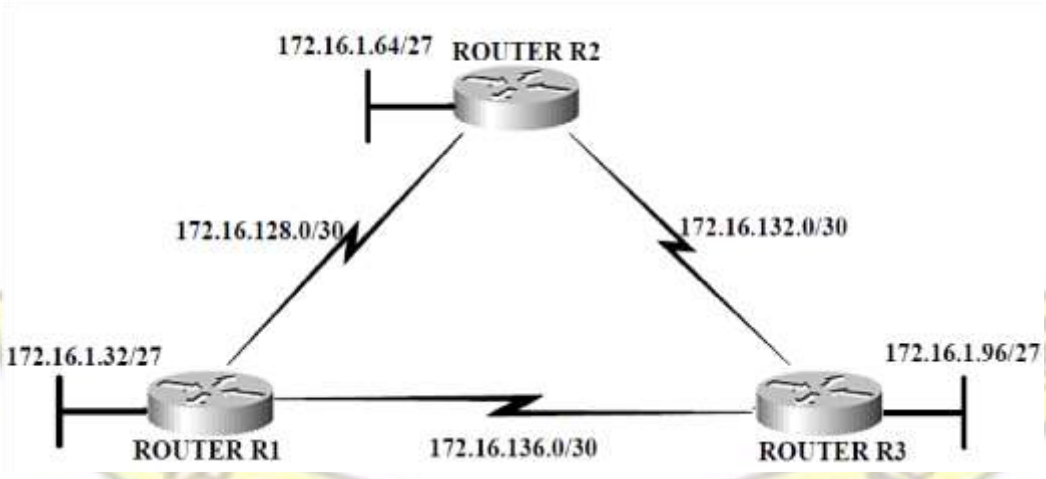


Figure 2.3: Classless Routing with Different Subnet Masks (Lemma *et al*, 2010).

2.4.3 Link State Routing

Shortest Path First (SPF) protocol is another name given to Link State Routing (LSR) protocols where the shortest path to each network it determined by each router. In LSR, every router

keeps a record referred to as link state database. The description of the AS topology is performed by this database. The LS Advertisement handles information exchanges among nodes in regard to routing. The information of neighbour nodes are contained in each LSA of a node and adjustments in the link of the neighbours of a node is communicated by flooding in the AS through LSAs. Nodes take note of changes after receiving LSAs and the routes are recalculated and sent again to its neighbours via LSAs. All nodes therefore have similar database portraying the networks topology. These databases keeps records of each link's cost which is used to generate a routing table. This table defines the destination packets can be forwarded to, set paths and also the link cost. The cost and path for each link is calculated with Dijkstra's algorithm. The network operator sets the link cost and it is represented by either the links' weight or length (Lemma *et al*, 2010). By assigning link costs, load balancing can be achieved and if this happens, there will be an avoidance of congested links and the prevention of the inefficient use of the network resources. The network operator can only alter the routing by making changes to the link cost. The default values are usually allocated to the weights and there is a recommendation that the link's weight is assigned as the inverse of the link's capacity. Determining the weights of the link is known to be NP-hard and this as a result of the fact that there is no easy procedure to make changes to the link weights in order to optimize the routing in the network. Greater flexibility is offered by LSR protocols but as compared to DV protocols they are complex. A preferred routing decision is made by LS protocols and also, it minimizes total broadcast traffic.

OSPF and IS-IS are two well-known LSR protocols. OSPF utilizes the link weight to identify the best node paths.

2.4.3.1 LS Routing Methods

Every router is responsible for accomplishing these processes.

- Every router finds out about networks directly associated to it and its own connections.
- Every router should connect to directly linked neighbour networks with HELLO packet exchanges.
- Every router must broadcast the packets links state it is connected to.
- Each router keeps a duplicate of LS packet received from its neighbours.
- Every router has equal view of the network topology and all alone decides the best topology path.

2.4.3.2 Characteristics of LSR

The characteristics of LSR protocols include

- An indistinguishable database is kept up by every router.
- They have fast convergence as there is an update of the database.
- They have the capability to split large networks into sub areas.
- Provides support for several ways to a destination.
- Every router keeps the full graph by getting updates from different routers.
- Provides precise metrics support.

2.4.3.3 Advantages and Disadvantages of LSR

In LSR protocols, each router computes its own routes independent on that of intermediate routers. The advantages of LS routing protocols are:

- They have fast reaction to connectivity changes.
- Small size packets are transmitted in the network.

The disadvantages of LS routing are:

- They require a lot of memory.
- Their configuration is more complex.

- They are inefficient under mobility due to changes in link.

2.4.4 Distance Vector Routing

In DV routing protocols, routes are presented as a vector of distance and direction. The representation of the distance is of hop count metrics and that of the direction by next hop router. The Bellman Ford algorithm is used by DV Routing to calculate paths. In its graph, nodes are illustrated as vertices and the edges of the graph represents the links between the nodes. Each node in DVR, maintains for every destination a distance vector. The DV comprises of destination ID, next hop and shortest distance. Each node in this protocol broadcasts a DV to its neighbours from time to time to inform about the shortest paths known. The neighbouring nodes therefore aid in the discovery of routes and each node then exhibits from its own side, the routes. Nodes rely on neighbour nodes for information about the routes which in turn relies on their neighbour nodes et cetera. Periodic exchange of these distance vectors are done by the nodes. The time range is from 10 to 90 seconds. For each network path, when a node gets the information from its neighbouring nodes demonstrating the most minimal cost, this entry is added to the routing table of the receiving node and an advertisement made to its neighbours.

2.4.4.1 DV Routing Methods

DV routing protocol utilizes Bellman Ford algorithm to identify the best path (Aslam, 2008). Different methods are used in the calculation of the best network path for various DV routing protocols. These algorithms have common major features. In the identification of the best path in a network for any link, several metrics are employed to compute the distance and direction. EIGRP makes use of the diffusion update algorithm in choosing the cost of getting to a target. In determining the best path, RIP utilizes hop count whiles IGRP draw on delay information and bandwidth availability (Jaffar, 2007). In DV routing protocol, records are kept on all known routes in the table at boot time. The routing table then starts and each entry makes out the

destination in the table and gives the network the distance. The measurement is done in hops. Routers, in DV have no knowledge of the full path to the target router. Rather, they know only the packet's possible direction and interface (Larsson & Hedman, 1998).

2.4.4.2 Characteristics of DV Routing

The features of DV routing protocol are as follows:

- DV routing protocol displays to all neighbours that have direct connection to it, its routing table, periodically at a regular interval.
- Updates with new information to each routing tables needs to be done whenever the routes become unavailable or fail.
- DV routing protocols require little management in smaller networks because they are simple and efficient.
- Hop counts vector is the basis of DV routing.
- It is iterative.
- DV routing employs a fixed subnet masks length.

2.4.4.3 Advantages and Disadvantages of DV Routing

DV routing protocol advantages of are:

- They work well in smaller networks.
- Their configuration is simple.
- They need little management.

The impediments of DV routing protocols:

- They create loops.
- They converge slowly.
- They have scalability issues.

- They lack variety of metrics.
- They are impossible for hierarchical routing.
- They perform badly in large networks.

There are a couple of strategies to limit the restrictions of DV routing protocols. These are **Split horizon rule** which is a technique to get rid of loops in routing and improve the speed of convergence and **Triggered update** which makes use of specific timers to improve the reaction of the protocol.

2.5 Terms Used In Dynamic Routing

2.5.1 Autonomous System

An autonomous system is a group of networks under the same administrative domain. This implies all routers having the same routing table information are in the same AS.

2.5.2 Administrative Distance

An administrative distance determines if routing information received router from a neighbour router is trustworthy. AD is measure in number ranging from 0 to 255, where 0 is the most trusted and 255 implies no traffic will be passed through this route. A router checks the AD first if it gets two updates listing the same remote network. The one with the lowest AD would be stored within the routing table, but if the two routes have similar AD, then the best path to the remote network will be found from the routing protocol metrics. The routing table will keep the advertising route with the lowest metric. If the AD, as well as the metric are same for both advertised routes, then there will be load balancing by the protocol to the remote network (Chinara & Kumar, 2009). A case of Administrative distance is illustrated in Figure 2.4

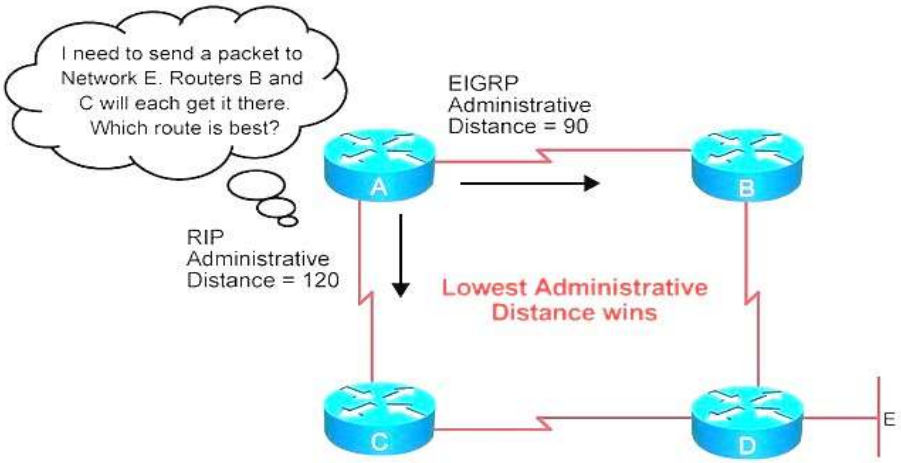


Figure 2.4 Administrative Distance Diagram (Chinara & Kumar, 2009).

The value is dependent on the information received by a router from its neighbour routers. If a router receives more than one update from the same network, then the router checks for the AD value. Each update's AD value will be different and the router takes only the AD value which is the most minimal and this value is used to update the router's routing table (Chinara & Kumar, 2009).

2.6 Convergence of Routing Protocols

Convergence, according to computer networks implies that in an internetwork every router has the same topological information about their network. Routers gather topological information for other routers with the help of implemented routing protocols (Shah & Waqas, 2013). This information should not contrary to the real time information in the network. The actual state of the network can be found based on this information.

For a network topology to have been declared as converged, all routing tables in the network should be complete and correct (Todorovic & Sepanovic, 2011). Converged network can also be defined as a network where every router knows the type of topology running and as indicated by the topology, they share packets to each other.

The process of establishing routes is termed convergence (Todorovic & Sepanovic, 2011). Convergence takes time because distribution of routing information within the network takes

some time. Eventually, every important information will be disseminated and a stable network state will be attained. There will no more be changes in the routes. There are two relevant questions that can be addressed:

1. What occurs with the routes prior to a stable state?
2. Can a stable state be attained and if yes, how soon?

The former question is relevant in light of the fact that packets incoming must be to be routed while the protocol convergence is underway. A packet following an invalid route or a route that leads to no destination will be lost. An instance of invalidity is a looping route, where packets fail to arrive at their destination and also cause bandwidth waste.

Routing protocol specifications are normally indicated in the design phase. The design process can be directed in the right direction when these requirements are proved or disproved early. These requirements can also be created for an already existing protocol and this can aid in a better understanding of the protocol and also its efficient use.

2.6.1 Convergence process

Upon the activation of routing protocol process, all routers attempt to send and receive packets of data related to the network. The extent of the exchange, the way the exchanged occurs and the type of packets exchanged depends mainly on the protocol being used. A state of convergence happens when every network related information of all routers are being exchanged with each other. Convergence is temporarily affected at the slightest network change that has effect on routing tables until the network change is communicated successfully to every other routers in the network.

2.6.2 Convergence Time

Convergence time is the needed time for the routers to learn routes of the entire network (Shah & Waqas 2013). It measures the speed with which a group of routers attain the state of convergence. Convergence time is relevant because it informs the network administrator when some network fails, how much time it takes to come to a normal condition. It is one of the primary design objectives and a critical performance indicator for protocols. It is virtually not possible for every router in a network to simultaneously recognize a change in topology. Depending on the protocol being used and also various other factors, a significant delay in time may pass before every one of the routers in that network achieve a consensus or agreement on what the new topology is. The delay is known to as convergence time. It very important to remember is that convergence doesn't happen immediately. However, how much time is needed for convergence to occur is the main uncertainty.

Some factors that can increase the time delay which is inherent in convergence include:

- The distance between the router and the point of change (in hops).
- The count of routers in the network that adopts DR protocols.
- The traffic load on links and Bandwidth.
- The load of the router.
- The traffic patterns versus the topological change.
- The routing protocol being used.

The impact of some of these factors can be reduced through good network engineering. The placed load on a router or link can be reduced. Also factors such as the router count in the network must be acknowledged as risk in a network's design. By adopting static routes to join stubs to the network, there is a reduction in the number of routers that must converge. This

specifically minimises convergence times. From the factors stated, it can be concluded that the points to consider in the reduction of the time of convergence are

- Choosing a protocol that can compute routes efficiently.
- A proper design of the network.

2.6.3 Quality of Service

Packets sent between nodes in a network is called flow. Delay and Jitter are some of the main properties for a network connection. These properties determine the QoS the flow requires. The QoS may not matter for some applications but it may for others (Fjeldbo, 2005).

Table 2.0.1: Quality of Service requirement

Application	Delay	Jitter
E-mail	Low	Low
File Transfer	Low	Low
Web Access	Medium	Low

The interpretation of Table 2.1 is that applications like email and file transfer are more delay tolerant and an interactive programs like web access require relatively low delay. All these applications however are immune for jitter as the connection can be smoothen with buffers

2.6.3.1 Delay

Delay is the time it takes to send a packet from a source to node to a destination node. Delay is expressed in time and since it is quite small it is expressed in ms (Fjeldbo, 2005).

Table 0.2.2: Standard Delay

Time Delay	Quality
0 – 150ms	Good
150 – 400ms	Fair acceptable
>400ms	Bad

From table 2.2 the range of time delay and their quality is stated. Any delay above 400 ms is recognised as bad. The causes of end-to-end delay are Processor delays, Buffer delays, Transmission delays, and Propagation delays.

2.6.3.2 *Jitter*

Jitter is defined as the variation in arrival times of successive packets from source to destination. It can be measured by monitoring the time for round trips for packets between nodes. Information about jitter comes from the distribution of the jitter, when the distribution is within a few seconds the jitter said to be low. If the distribution spread across several seconds, the connection is has a high jitter and therefore unpredictable (Fjeldbo, 2005).

Even though data packets are generated periodically with equal time difference between them from the sender side (Server), the variability of the path they take during transmission, causes the packets to arrive with variable time difference at the receiver end (Client). The congestion in the link between the end points is also a significant cause of unacceptable packet jitter.

Table 2.0.3: Standard Jitter

Jitter (ms)	Quality
0 – 20ms	Good
20 – 50ms	Fair acceptable
>50ms	Not acceptable

Table 2.3 shows jitter values and what message they plan to convey. If jitter is higher than 50ms it is no acceptable.

2.7 Routing Protocols

2.7.1 Open Shortest Path First

OSPF is an IGP utilized in the circulation of routing information in an Autonomous System (Moy, 1989).

The OSPF protocol relies on link-state technology. OSPF has brought new ideas such as Variable Length Subnet Masks (VLSM), confirmation of routing updates, route summarization and so on. IP packets in OSPF are only routed on destination IP address located in the header of the IP packet. OSPF is a dynamic protocol and it rapidly identifies changes in the topology and calculates new loop-free routes after a time of convergence. This period of convergence is short and involves a minimal routing traffic (Manjeshwar & Agrawal, 2015). OSPF figures the least distance for every route using a procedure based on a shortest path first algorithm known as Dijkstra algorithm. OSPF is very prominent in vast networks and it is employed to obtain the most useful route through which the packets can be delivered within an IP networks. Every OSPF router keeps the state of the local network connection with LSA and broadcast to the whole AS (Patil & Deshmukh, 2014).

2.7.1.1 Characteristics of OSPF

The characteristics of OSPF are:

- OSPF network management is easy. All routers in the same area will have similar database and a separate computation is done for each Area.
- OSPF distributes traffic through various routes to a particular target, a procedure referred to as Load balancing.
- OSPF uses low bandwidth and guarantees routers are less burdened with processing as updates are sent only when there is a change.
- OSPF allows maximum flexibility.
- It helps in the exchange of information acquired from external sites.
- OSPF runs directly over IP.
- OSPF gives verified updates on routing by unique authentication procedures.

2.7.1.2 Advantages and Drawbacks of OSPF

The advantages of OSPF are:

- OSPF is unrestricted
- Its convergence is fast and loop less
- It uses low bandwidth
- It supports both exact and diverse metrics
- It supports several paths
- It represents exterior routes distinctly
- It has no limit on hop count
- It supports VLSM
- It supports huge networks

Drawbacks of OSPF are

- OSPF has complicated configuration
- OSFP uses a lot of memory
- OSPF consumes more processing power when topology changes occur.

2.7.1.3 OSPF Convergence

Taking into consideration the network in Figure 2.5 running OSPF, if it is assumed the connection between R4 and R6 fails, R4 identifies the breakdown in the link and transfer LSA to R3 and R5. The forwarding of packets is put on hold as soon as a network change is detected. R3and R5 reforms their topology database, duplicates the LSA and flood their neighbours.

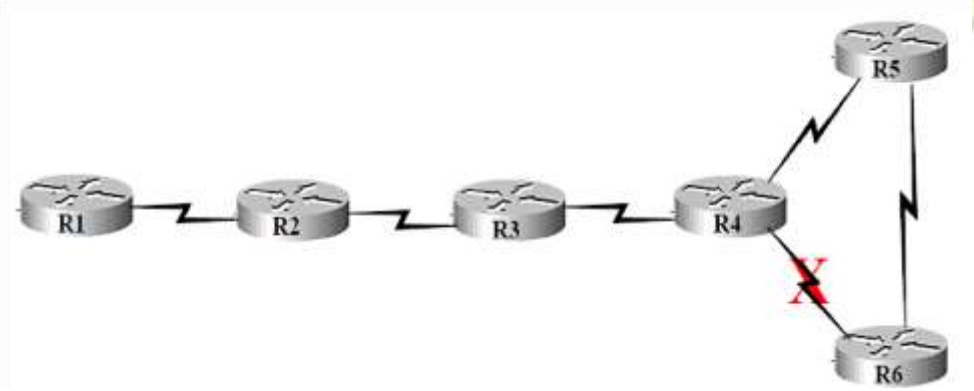


Figure 2.5: Network using OSPF (Lemma *et al*, 2010).

In so doing, all the devices in the network have become aware of the change. All the routers with the help of Dijkstra's algorithm, create new routing tables. The traffic is now forwarded through R5.

2.7.2 Enhanced Interior Gateway Routing Protocol

EIGRP is an improved version of IGRP. In 1992 EIGRP emerged a very scalable protocol for large and medium scale networks. It is the most utilised IGRP that makes use of DUAL for the calculation of its routes (Lemma *et al*., 2010). It has fast convergence than any other IGP. EIGRP is classified as hybrid protocol because it possesses the attributes of a LS protocol for establishing neighbour relationships and also the attributes of a DV routing protocol for advertising routes. To implement routing, EIGRP keeps three tables to aid routing traffic. These tables are neighbour table, routing table and topology table. EIGRP keeps records of all routes instead of the best route to ensure fast convergence. EIGRP stores all neighbour routing tables and it only exchange information that its neighbour would not contain and this assist in the reduction of the undesirable traffic in the network. EIGRP is preferred in large networks and it updates only when there is a change in topology but not periodically as opposed to old Distance-Vector protocols.

EIGRP metric has its basis on its bandwidth, delay, reliability and load.

EIGRP makes use of four key technologies that come together to differentiate it from other routing technologies and they are as follows:

1) Neighbour discovery/recovery mechanism: This permits routers to discover other routers linked directly to their networks dynamically.
2) Reliable transport Protocol: EIGRP utilizes this for ensured, ordered delivery of packets to neighbours.

3) Diffusion Update Algorithm: DUAL takes care of all route calculations and amongst its duties is the maintenance of a topology table, which comprises of all ways to avoid loops to each destination publicized by every router.

4) Protocol Dependent Modules: EIGRP's protocol-reliant modules are used to aid diverse network layer protocols.

2.7.2.1 Advantages and Disadvantages of EIGRP

EIGRP render these advantages:

- EIGRP has low convergence time and this reduces the bandwidth utilization.
- It supports multiple network layer protocols.
- Its configuration is easy.
- It offers Loop free routes.
- It maintains a backup path to get to the destination in the network.
- It maintains a topology table rather than a routing table and is made up of best path and loop free path.
- EIGRP also promotes the routing update authentication.

Disadvantages of EIGRP are:

- It is considered exclusive to Cisco.
- Other vendor routers are unable to use EIGRP.

2.7.2.2 EIGRP Convergence

Considering figure 2.6, running EIGRP, it is assumed that the connection that exist between R4 and R6 experience failure and the failure in connection is diagnosed by R4. No feasible successor is available within the database of the topology and R4 advance into active convergence. The only neighbours to R4 are R5 and R3. Due to the fact that there is the absence of a route with lower Feasible Distance present, R4 dispatch a query to its neighbours in order

to get a logical successor. There is a response by R3 to R4 showing that no successor is present and R5 responds to R4 showing FS is present with higher FD. R4 accepts the fresh path and distance and appends it to its routing table. An update is then conveyed by R4 to R3 and R5 concerning the higher metric. There is then a dispatch of the update to the networked routers, then the routes converge.

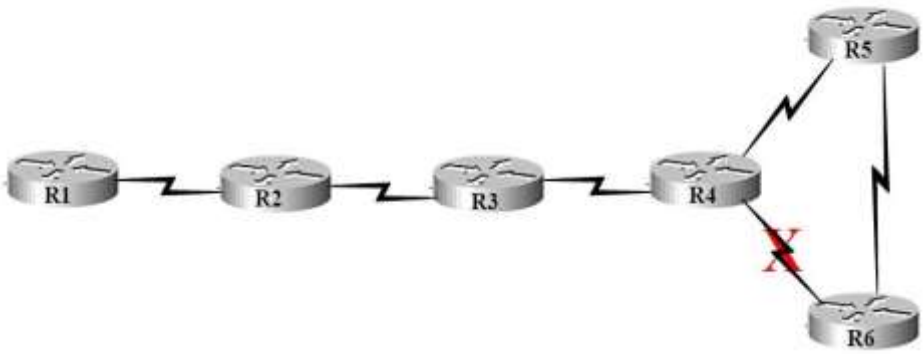


Figure 2.6: Network using EIGRP (Lemma *et al*, 2010).

2.7.3 Intermediate System to Intermediate System

IS-IS was instigated by ISO and it is a LS protocol (Fortz & Thorup, 2002). IS-IS routers use one metric in calculating the route cost to enable it exchange routing information. IS-IS and OSPF routing protocols have similarities. IS-IS network comprises of end systems, intermediate system, areas and domains and is intended to assign routing within an area.

Routers in IS-IS network are intermediary structures categorised into groups called areas. These areas put together forms a domains and the user devices are referred to as end systems. Dijkstra algorithm is used in IS-IS to detect the shortest path. It uses LS database in directing packets between intermediate systems. A two level hierarchical routing is adopted by IS-IS where a router on level 1 can recognise the area topology which includes all routers and hosts. A level 1 router however is unable to identify routers not within their area. Routers on Level

1can be compared to OSPF intra area routers because it does not have connectivity outside. Routers on Level 2 are not obliged to know level 1 area topology. An IS-IS network is illustrated in Figure 2.7.

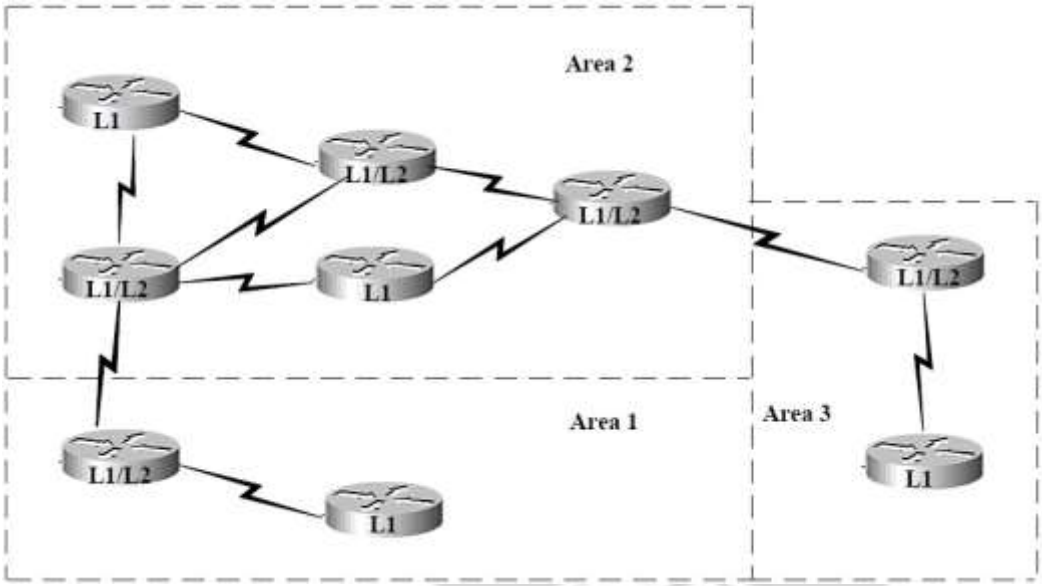


Figure 2.7: IS-IS Network (Lemma *et al*, 2010).

IS-IS has features including:

- Hierarchical routing
- Classless behavior
- Rapid flooding of information
- Fast Convergence
- Very scalable
- Adjustable timer tuning

IS-IS Protocol is an intra-domain OSI dynamic protocol defined in International Organization for Standardization (ISO) 10589. The protocol is outlined to function in OSI Connectionless Network Service (CLNS). Data is transported with the help of the protocol specified in ISO 8473.

2.7.3.1 Integrated or Dual IS-IS

The IS-IS routing protocol might be utilized as an IGP to help IP and OSI in addition. This permits a single protocol to be used to aid pure IP environments, pure OSI environments, and dual environments. Integrated IS-IS is extensively deployed in an IP-only environment in the top-tier Internet service provider (ISP) networks. The IS-IS working group of the Internet Engineering Task Force (IETF) built up the specification for Integrated IS-IS (RFC 1195).

Two essential techniques are accessible for protocols to aid dual OSI and IP routers. One technique, known as "Ships in the Night," makes use of totally independent routing protocols for each of the two protocol suites. This specification shows an alternative approach, which uses a single integrated protocol for interior routing (that is, for computing routes within a routing domain) for both protocol suites (Kumar et al., 2014).

By assisting both IP and OSI traffic, this integrated protocol model supports traffic to IP hosts, OSI end systems, and dual end systems. The IS-IS Protocol can be applied to sustain pure-IP environments, pure-OSI environments and dual environments. IS-IS allows the interconnection of dual (IP and OSI) routing areas with other dual domains, with IP-only domains, and with OSI-only domains.

2.7.3.2 IS-IS Operations

The operation of IS-IS from an advanced level is as follows:

- IS-IS routers broadcasts Hello packets to all IS-IS-enabled interfaces to detect neighbours and create adjacencies.
- Routers that offer similar data link will progress towards becoming IS-IS neighbours if their hello packets contain information which satisfy for forming an adjacency. The criteria vary slightly based on the type of media being used (p2p or broadcast). The primary criteria are matching authentication, IS-type and MTU size (Kumar et al, 2014).

- Routers may build a link-state packet (LSP) in view of their local interfaces that are set up for IS-IS and prefixes gained from others next to it.
- Generally, routers surge LSPs to all adjacent neighbours with the exception of the neighbour from which they got the same LSP. Notwithstanding, there are distinctive forms of flooding and furthermore various scenarios in which the flooding operation may differ.
- All routers will develop their link-state database from these LSPs.
- A SPT (shortest-path tree) is computed each IS, and from this SPT the routing table is built.

2.7.3.3 Advantages and Drawbacks of IS-IS

IS-IS provides the following advantages:

- Rapid convergence. IS-IS uses a low number of packet types for the transmission of routing information.
- It provides support for expansive areas of different intermediate systems without causing the deterioration in the performance of SPF.
- It is unable to support the implementation of virtual links
- Scalable. In IS-IS, Backbone cannot be classified as an area but rather a group of contiguous ABRs.
- Its implementation is uncomplicated.

IS-IS limitations are:

- The width of a metric 6 bits (0-63). A default value of 10 is assigned a metric if its specification is not done manually.
- Every area within IS-IS networks are referred to as stub areas.

2.7.4 Border Gateway Protocol

The BGP is an inter-autonomous system routing protocol. An AS can be defined as a collection of networks under one administration and with common routing policies. The use of this protocol is for exchanging routing information on the Internet and also between ISPs. BGP is a standardized exterior gateway protocol modelled to exchange routing and reachability information between AS on the Internet. The protocol is mostly classified as a path vector protocol however it is likewise classed as a DV routing protocol (Caesar & Rexford, 2013). BGP decide on routing choices based on paths, network policies or rule-sets configured by a network administrator and it plays an important role in making important routing decisions.

BGP is the routing protocol used to trade reachability information across AS (Caesar & Rexford, 2013). It was conceived out of the need for ISPs to manage route selection that is where to forward packets and propagation (who to forward routes to). In the initial state of the introduction of BGP, it was a relatively simple path vector protocol. After a while, numerous incremental modifications to permit ISPs to manage routing were recommended and added to BGP. The revised version of BGP is version 4 (BGP4).

When BGP is applied between AS, the protocol is termed as EBGP (External BGP). A protocol is referred to as IBGP (Interior BGP) if a service provider implements BGP within an AS.

BGP is a robust and scalable protocol employed on the Internet. Its internet routing tables numbers over 90,000 routes. To obtain scalability, BGP uses numerous route parameters (attributes) to outline routing policies and keep up a stable condition.

2.7.4.1 Types of BGP

- Internal BGP (iBGP): BGP that runs between two peers within the same AS is termed as iBGP. This iBGP assigns every AS a way to broadcast reachability information to all routers in the AS.

- External BGP (eBGP): When BGP keeps running between various AS, it is termed eBGP. The eBGP provides every AS a way to obtain subnet reachability information from neighboring AS.

2.7.4.2 BGP Attributes

In a situation where there are multiple paths to a particular destination, routes learnt via BGP have some characteristics that are utilized in deciding the best route to a destination. These characteristics are called BGP attributes. In designing robust networks, understanding the influence of these attributes is essential in choosing the routes. The attributes used by BGP in the route selection are:

- Local preference
- Next hop
- Weight
- Origin
- AS_path
- Community
- Multi-exit discriminator

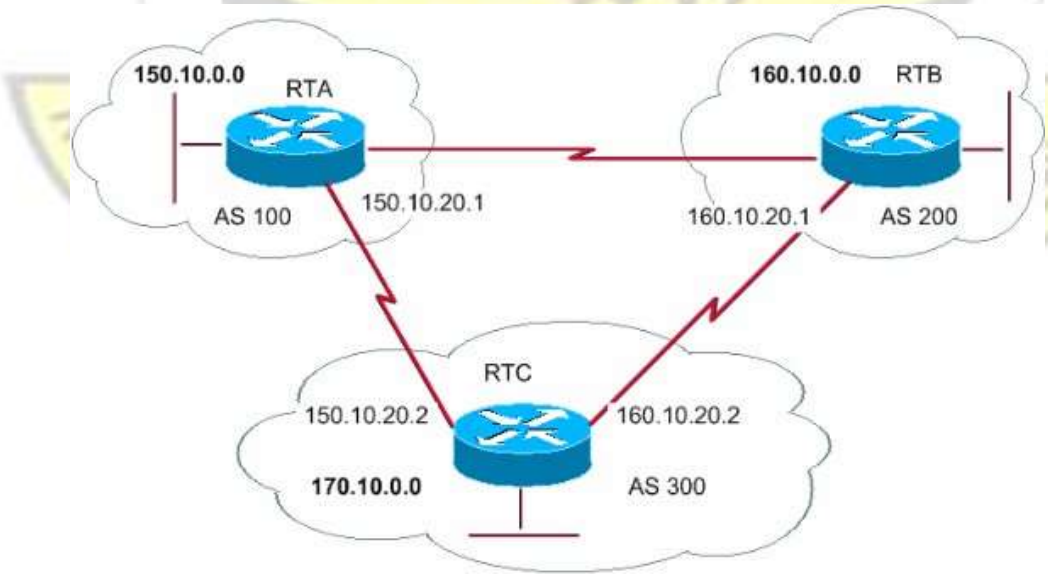


Figure 2.8: BGP Network Diagram (Pei et al., 2005).

2.7.4.3 Convergence of BGP

BGP supports policy-based routing, where policies are basically arbitrary (Obradovic, 2000). When computing the degree of preference, a router sees the entire route but it decides on just the next hop. The router chooses a route based on a one-hop extension of a neighbour's choice. BGP has convergence instability. A typical BGP Network is illustrated in figure 2.8.

Considering a group of AS, each having one or multiple BGP routers, the configuration of every router's policy is done individually. BGP sessions is started amongst a number of the routers and it is assumed that no topological changes happen when the protocol is being run. The system can behave in two possible ways:

- All routers eventually get to the point where they are unable to further improve their routes by extending their neighbours routes. When this happens, it can be said that there is a convergence to a stable state in the system.
- Routers continuously update the information in their tables and thus advertise new routes. A situation like this depicts that the system diverges.

It is important to understand that convergence is a major goal of most routing systems. In the event of system divergence, routers revise their choice of routes. This can affect the performance of a router but more importantly, there can be an increase in the inconsistencies in states which brings about packet loss. On the other hand, stable routes provide many advantages, like better proxy caching and more stable loads.

BGP is capable of displaying convergent behaviour as well as divergent behaviour.

The choice of routing policies is an essential factor in convergence. Generally, we say that a routing protocol is safe if in the absence of topology changes, it always converges.

Currently, BGP is not a safe protocol, despite the fact that it exhibit the behaviour of being safe in practice. Several studies have exhibited anomalies related with the behaviour of BGP.

2.6.4.4 Advantages and Disadvantages of BGP

The BGP is seen as the most difficult routing protocol to design, configure and maintain but there are a numerous reasons all that difficulty is needed.

- BGP increases the network stability and provide end-to-end quality of service.
- BGP allows the specification of any IP address as the next-hop for an IP prefix. To guarantee optimum routing across a BGP AS, this property is used frequently. It can likewise be used to stop worms and denial-of-service attacks on a network.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

The research method used has been outlined and discussed in this chapter. The method for this research was a simulation of scenarios. Simulation can be explained as the creation of a model for the study of the behaviour of an actual system being observed. The real system's behaviour may be predicted based on the results obtained from the simulation. The network simulation can be explained as a computer aided simulation technique modelling the network functionality and its behaviour by determining the communication between the different network elements, monitoring and imitating observations from a real network. The data from simulation experiments, could be used to analyse in a series of offline test experiments to test the protocols

that are supported by the network and network behaviour. Application of simulation technology has been widely developed lately for simulating computer networks traffic.

Network simulator is an integrated and versatile package of tools that emulates network's behaviour like creating network topology and understanding the network. Recently, network simulators are being used extensively in different areas such as, conducting research and teaching, designing different network topologies, Quality Assurance of industrial developments for simulating, verifying, and analysing the performance of new networking topologies and evaluating effects of the different parameters on the communication protocols that are being studied.

Network simulators can be categorized based on their futures and functionality, to very simple or complex, commercial or open source simulators. A simple simulator can imitate a small network topology by clearly identifying the nodes, the data links between the nodes and network traffic but a complex one possibly emulates many different types of network devices and communication protocols to handle network traffic. They are designed to model massive network performance with variety of vendor's equipment to provide facility for designing and optimization of large and complex networks. Moreover a powerful network simulator enhances capability of network performance optimization. Graphical network simulators enable users to simply visualize the operation of their emulated computer network and serve them possible customization options.

Currently, there exists various simulators available for the implementation of virtualized networks such as: GNS3, NS2, NS3, M5 Simulator, OPNET (Optimized Network Engineering Tools), OMNET++ (Optical Micro-Networks Plus), NETSIM (Network Based Simulation and Modeling Environment), REAL (Realistic And Large), J-SIM (Java-based simulation) and QUALNET(a high-fidelity network simulator based upon GloMoSim) where some of them are

widely acknowledged in academia researches and some of them have commercial use (Siraj *et al.*, 2012).

3.2 Simulation Environment Used

The simulation environment chosen for this thesis is GNS3. This is a network emulation software commonly used as a supplementary tool for teaching advanced networking concepts. It emulates a number of Cisco devices with the help of Dynamips emulator. Dynamips was originally developed by Christophe Fillot (Liangxu *et al.*, 2013). There a number of advantages of using GNS3. First of all it is an open-source project. This means that it can be used at no cost. Secondly, GNS3 emulates the Cisco IOS. This means it creates a complete replication of the functionality of Cisco devices, enhancing realism (Gil *et al.*, 2014). This also enables GNS3 to connect to a physical network, to other virtual machines and to the host computer, allowing the use of real networking tools like Wireshark to be used for a full simulation experience (Gil *et al.*, 2014). Thirdly, all commands available on real equipment is available in the emulated environment because an actual operating system is being emulated. Fourthly, GNS3 can share the resources of multiple computers to enhance performance and to support many virtual routers (Liangxu *et al.*, 2013). Several problems or disadvantages emerges or arise with the use of GNS3. First of all, it can only emulate select Cisco devices. The Cisco catalyst switches are excluded. It is therefore not possible to use GNS3 to learn switching concepts. Secondly, GNS3 requires a lot of hardware resources. However, most modern computer should be powerful enough to run it and that distribution between machines can be used, if necessary (Liangxu *et al.*, 2013). Thirdly, the GNS3 software requires a valid Cisco IOS image because it is an open source software and therefore free. Without a valid Cisco IOS image, the software itself is useless. GNS3 is prohibited from including an IOS image with the software because of licensing restrictions. It is important to note that Cisco only grants a non-exclusive and

nontransferrable license. This implies that Cisco control over the use of Cisco IOS and also the image is not to be transferred to someone else. It may only be used on customer owned computers or on Cisco equipment with the software already embedded.

3.3 GNS3 Capabilities

GNS3 is a network simulator that allows emulation of networks of complex nature. It is an open source simulator and is written in python. GNS3 is promoted by user- friendly Graphical User Interface (GUI) as illustrated in Figure 3.1 that enables users to configure a network component in a virtual machine that runs the OS same as the original network component (Siraj *et al.*, 2012). GNS3 is a virtualization platform which consists of three software programs that runs on common PC hardware and could be installed on Microsoft Windows, Linux and MAC operating systems. To attain a complete network emulation, GNS3 makes use of the following emulators, to run the exact OS as in actual networks:

- Dynamips, the famous Cisco IOS emulator
- Virtual Box, which runs server and desktop OS as well as Juniper Jun OS
- QEMU (a comprehensive open- sourced machine emulator). it runs Cisco ASA, PIX and IPS

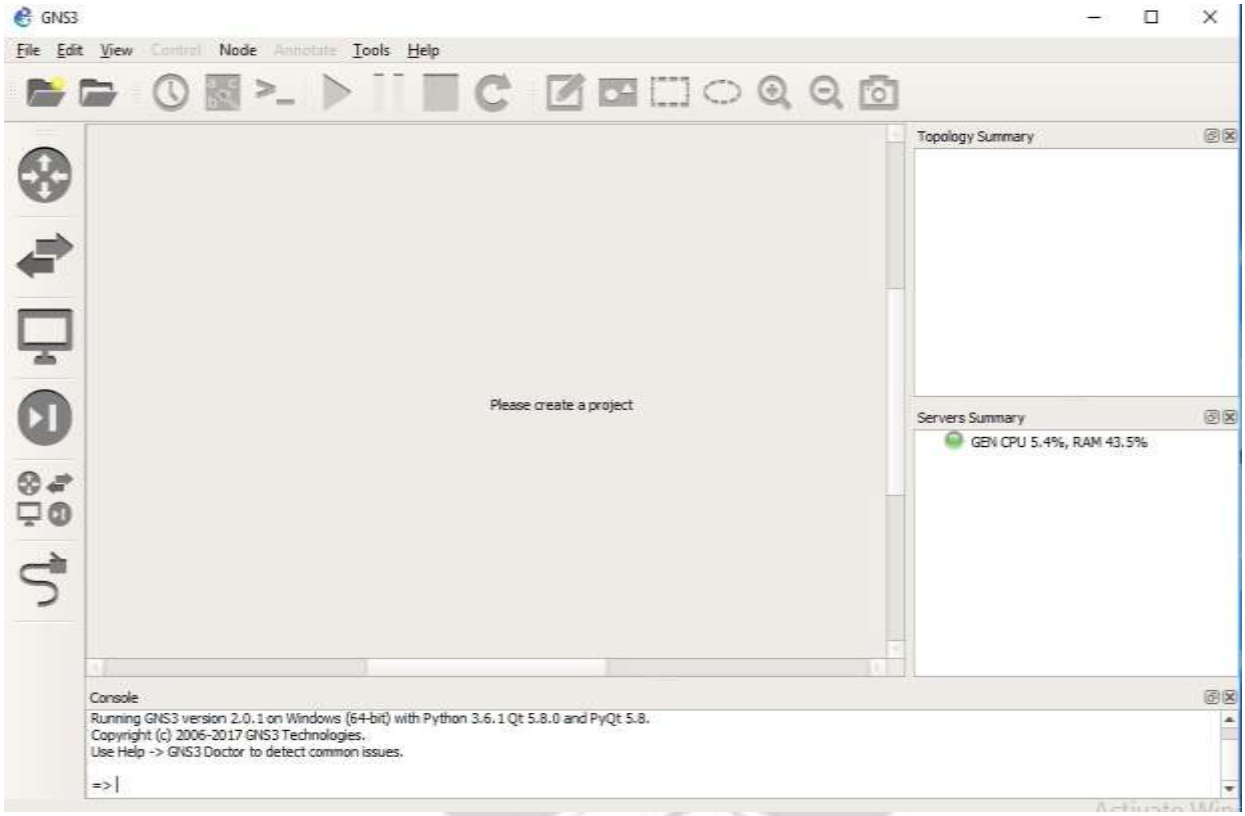


Figure 3.1: GNS3 User Interface

GNS3 operates on the top of Dynamips. By this it creates a more user friendly, graphical environment as compared to other simulators. Dynamips provides emulation of multiple instances of router devices as a virtualization hypervisor. As result every emulated router operates actual IOS software image, so it is able to emulate most of the commands and functions available in the IOS image. Another very handy feature of GNS3 is the capability of capturing packets on serial interfaces as well as virtual Ethernet by using Wire shark packet analyzer to monitor traffic of network (Li *et al.*, 2010).

3.4 Simulation Study

The routing protocols under study in this thesis are OSPF, EIGRP, IS-IS and BGP. These protocols are compared and evaluated based on convergence time. Metrics such as delay and jitter will also be used with the intention of getting a better performing protocol.

1. How long does it take for the forwarding of traffic to begin once a topology change has occurred? This explore how the protocols automatically detects service interruptions and how long it takes until the protocol and failover or switch over to an alternate path. The measurement of the gap between the first service interruption and the resumption of full data flow, otherwise known as Convergence time will then be recorded.

2. How long does it take for the protocol to adjust to a change in topology?

   This lab explore how the protocols detects changes to the network topology and how long it takes until the protocols updates the routing tables to reflect the new topology. In this simulation additional routers are added to the network topology and an observation of how the routing tables reorganize themselves after this change in the topology will be made.

Convergence focuses on the recovery of network failure and changes. In today's networks, alternate, redundant or standby paths are made available in anticipation to problems that may arise. Failover can be defined as the process in which networks automatically detect interruptions in service and adjustments and switch over to an alternate path. The event that happens within the transport network when the re-routed information flow merges back to a point in the error-free path is convergence. Conversely, failback is the process of restoring a network back to its original state when the service interruption is fixed.

Routing protocols in Layer 3 group such as EIGRP, OSPF, ISIS and BGP has the capability to re-route IP traffic if a network or link fails. These techniques however can take seconds to complete. It is dependent on the size and complexity of the network that they are handling.

3.5 Routing Protocol Scenarios

3.5.1 Routing Protocol Scenarios for Failure in Topology

The network topology for the simulation of the four protocols that consists of five routers or nodes, two switches, a server which is the destination of the traffic and a PC which is the source of the traffic. The way of connection of the routers or nodes to each other is displayed in Figure 3.2.

The five routers were dragged from the nodes type into the topology workspace and configured. The routers were then selected and manual option chosen to connect the routers.

The routers are then connected to each other physically as shown in the Figure 3.2.

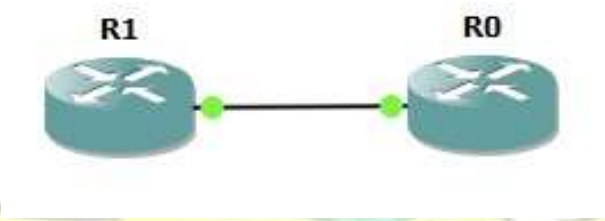


Figure 3.2: Routers Connected by Wire

The interfaces were given IP addresses and subnet mask and then the protocols tested for their convergence time.

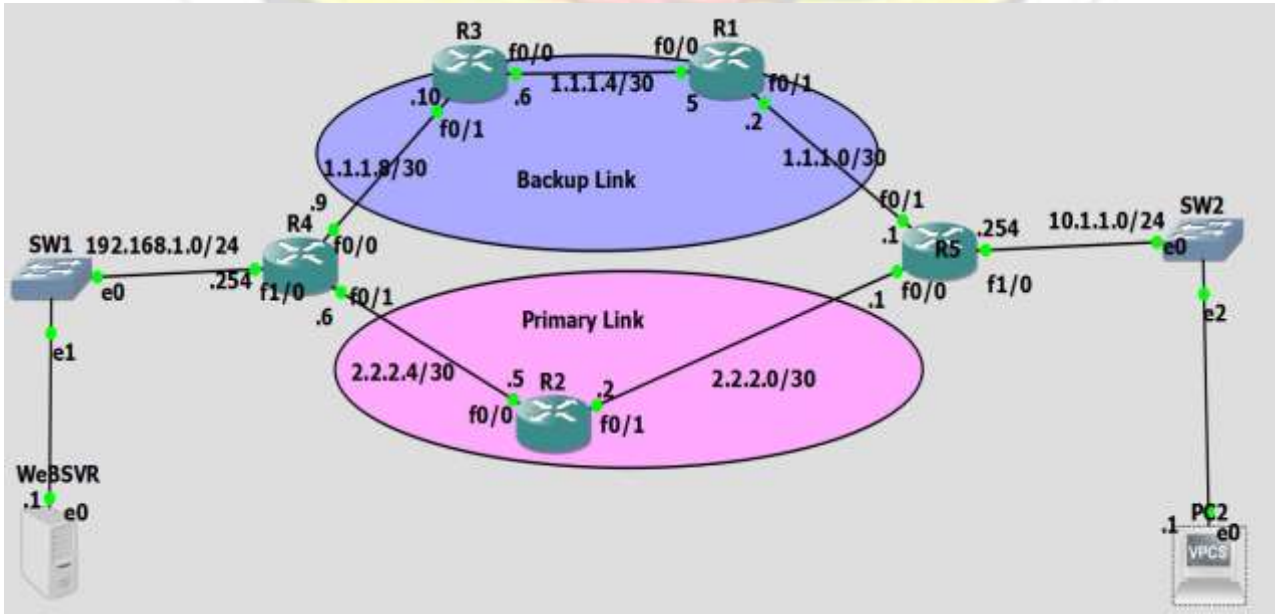


Figure 3.3: Network Diagram for Simulation

In Figure 3.3, a data packet of size 1000 bytes was sent from a PC to a webserver. The packet went through routers R5, R2 and R4 to destination (Server). The also exists a backup link though routers R5, R1, R3 and R4 should there be an interruption or failure in the primary link to the Server. A break was introduced in the primary link or the data path closer to the source of the traffic that is the PC as shown in Figure 3.4 to determine how long it takes for the network to recognise the alternative path. Wireshark was used to monitor the network to record the times. Wireshark is a Network Analyser most of the time used by network administrators to analyse network performance. It is able to capture data packets or information running through network and ensure proper analysis.

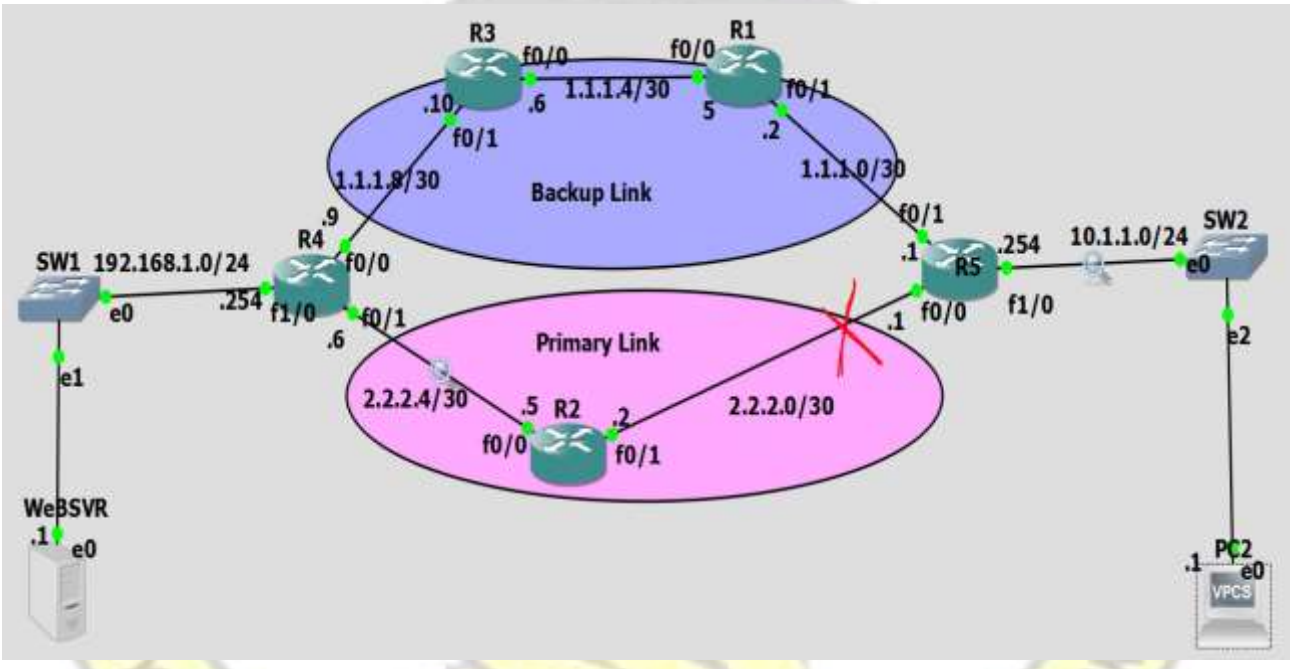


Figure 3.4: Network Diagram with Failure closer to the source of the traffic

The protocols EIGRP, OSPF, ISIS and BGP were tested one after the other to check for the times of convergence. The break or failure was then introduced close to the destination of the traffic as shown in figure 3.5 to determine if there was a great difference in the convergence times of the protocols when the failure is close or not close to the source of the traffic.

3.5.1.1 Results of Routing protocols with Failure closer to the source of the traffic

Ten different tests were run to determine the convergence times for the four protocols under study. For each test a break or failure was introduced into the network closer to the source of the traffic which is the PC in the network diagram. The Down times that is the time the network recognises the failure and the Recovery time that is the time the network recognises an alternative path are recorded. The time of convergence were then determined from the difference between the Down times and the recovery times and the results for the scenarios are tabulated.

OSPF Scenario

In this scenario, OSPF is implemented on the selected network topology and the results from the simulation recorded in table 3.1.

Table 3.0.1: Convergence time Measurement for OSPF with Failure closer to the source of the traffic

Test Number	Down Time (hh:mm:ss.ms)	Recovery time (hh:mm:ss.ms)	Convergence Time(s)
1	20:58:05.873	20:58:14.219	8.346
2	21:07:24.986	21:07:33.623	8.637
3	21:12:10.377	21:12:18.871	8.494
4	21:15:33.173	21:15:42.052	8.879
5	21:19:24.778	21:19:32.940	8.162
6	21:29:00.523	21:29:10.124	9.601
7	23:10:49.235	23:10:57.023	7.788
8	23:16:37.560	23:16:46.152	8.592
9	23:23:23.283	23:23:32.119	8.836
10	23:27:54.788	23:28:00.975	6.187

EIGRP Scenario

Considering the network in Figure 3.4 running EIGRP. Assume the link between R5 and R2 fails. Since a change in the network is detected traffic forwarding is suspended. Routers update their tables and the results of this simulation is shown in table 3.2.

Table 3.0.2: Convergence time Measurement for EIGRP with Failure closer to the source of the traffic

Test Number	Down Time (hh:mm:ss.ms)	Recovery time (hh:mm:ss.ms)	Convergence Time(s)
1	23:22:35.002	23:22:41.080	6.078
2	23:27:54.026	23:28:00.011	5.985
3	23:29:34.408	23:29:40.346	5.938
4	23:31:40.852	23:31:46.803	5.951
5	23:35:12.815	23:35:18.284	5.469
6	23:36:41.725	23:36:47.764	6.039
7	23:39:28.694	23:39:34.185	5.491
8	23:42:00.974	23:42:06.143	5.169
9	23:43:46.772	23:43:54.070	7.298
10	23:45:31.267	23:45:37.471	6.204

IS-IS Scenario

In this scenario, the results of IS-IS configuration as a protocol for the network topology is displayed. The recorded times are being displayed in table 3.3.

Table 3.0.3: Convergence time Measurement for IS-IS with Failure closer to the source of the traffic

Test Number	Down Time (hh:mm:ss.ms)	Recovery Time (hh:mm:ss.ms)	Convergence Time(s)

1	09:35:18.938	09:35:26.737	7.799
2	09:38:52.464	09:39:00.804	8.340
3	09:43:31.586	09:43:39.954	8.368
4	09:53:54.496	09:54:02.681	8.185
5	09:58:07.119	09:58:15.709	8.590
6	10:03:10.456	10:03:19.551	9.095
7	10:08:50.612	10:08:59.144	8.532
8	10:13:38.835	10:13:46.877	8.042
9	10:18:36.980	10:18:45.031	8.051
10	10:23:06.338	10:23:13.779	7.441

BGP Scenario

BGP is configured on the network topology and the times of link interruption and recovery are captured and displayed in table 3.4.

Table 3.0.4: Convergence time Measurement for BGP with Failure closer to the source of the traffic

Test Number	Down Time (hh:mm:ss.ms)	Recovery Time (hh:mm:ss.ms)	Convergence Time(s)
1	22:45:10.849	22:45:32.824	21.975
2	22:49:28.486	22:49:51.655	23.169
3	22:54:40.318	22:54:59.649	19.331
4	23:03:37.869	23:03:53.144	15.275
5	23:07:17.020	23:07:32.763	15.743
6	23:10:31.895	23:10:51.769	19.874
7	23:13:39.764	23:14:05.410	25.646
8	23:16:38.082	23:17:06.589	28.507
9	23:19:47.440	23:20:02.104	14.664
10	23:22:43.275	23:23:11.915	28.640

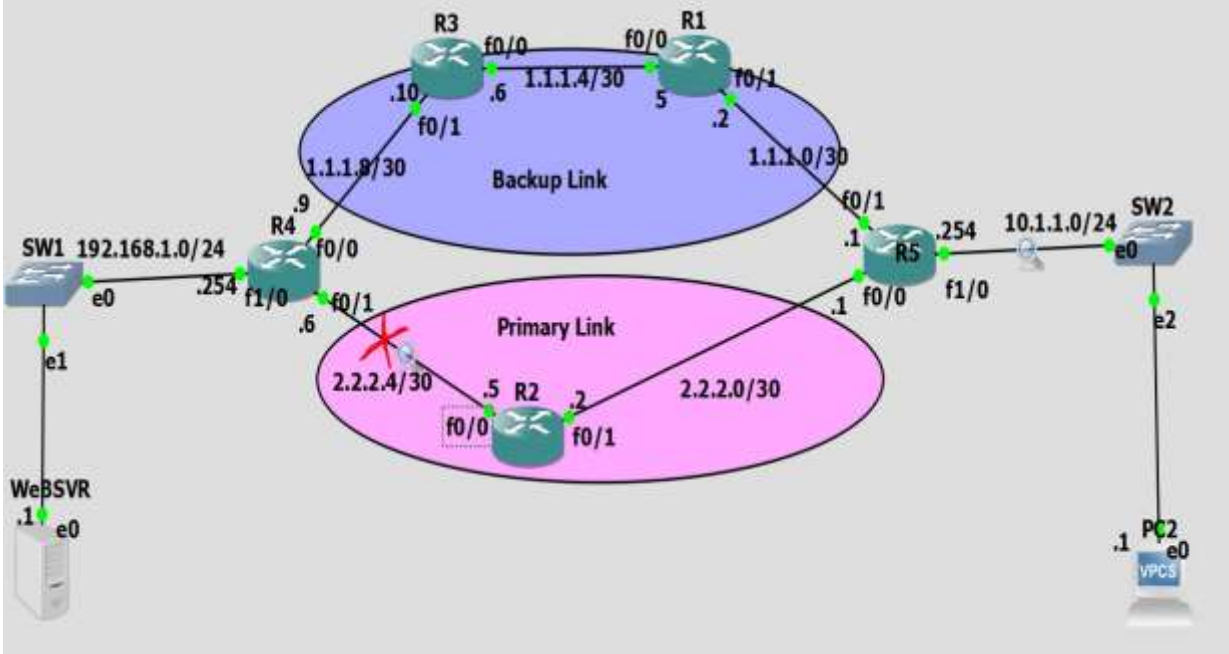


Figure 3.5: Network Diagram with Failure closer to the Destination of the Traffic

3.5.1.2 Results of Routing protocols with Failure closer to the destination of the traffic

For the same network, the break or failure in the network was moved closer to the destination of the traffic and a packet of data sent to determine if there was a difference in the time it takes to converge when the failure is closer or far from the source and again ten tests were run. The convergence times were then determined from the difference between the down times and the recovery times.

OSPF Scenario

In this scenario, OSPF is configured like in the first OSPF scenario but the link failure is moved away from the source of the traffic to an area closer to the destination to determine if there is much difference in the convergence time depending on the position of the failure in link. The results from this scenario is tabulated in table 3.5.

Table 3.0.5: Convergence time Measurement for OSPF with Failure closer to the destination of the traffic

Test Number	Down Time (hh:mm:ss.ms)	Recovery time (hh:mm:ss.ms)	Convergence Time(s)

1	09:04:08.502	09:04:16.495	7.993
2	09:06:34.673	09:06:43.163	8.490
3	09:09:02.580	09:09:10.377	7.797
4	09:11:12.232	09:11:21.310	9.078
5	09:12:54.533	09:13:03.538	9.005
6	09:21:45.983	09:21:54.156	8.673
7	09:26:20.569	09:26:29.507	8.938
8	09:28:54.645	09:29:03.486	8.841
9	09:31:35.768	09:31:43.503	7.735
10	09:34:17.947	09:34:25.651	7.704

EIGRP Scenario

This link failure scenario shows the configuration of EIGRP protocol on the selected network topology. EIGRP is configured and simulation run for it with failure close to the destination of the traffic. The simulation results are shown in table 3.6.

Table 3.0.6: Convergence time Measurement for EIGRP with Failure closer to the destination of the traffic

Test Number	Down Time (hh:mm:ss.ms)	Recovery time (hh:mm:ss.ms)	Convergence Time(s)
1	22:54:08.390	22:54:12.610	4.220
2	22:56:27.314	22:56:31.283	3.969
3	22:58:09.088	22:58:13.167	4.079
4	22:59:37.178	22:59:41.185	4.007
5	23:01:30.069	23:01:36.037	5.968
6	23:03:17.057	23:03:23.029	5.972
7	23:04:45.453	23:04:49.751	4.298
8	23:12:24.771	23:12:30.772	6.001
9	23:13:59.635	23:14:05.510	5.875
10	23:20:20.242	23:20:26.211	5.969

IS-IS Scenario

In this Scenario, the results of the configuration of IS-IS protocol for the network with the failure in link closer to the destination are shown. The recorded times are being displayed in table 3.7.

Table 3.0.7: Convergence time Measurement for IS-IS with Failure closer to the destination of the traffic

Test Number	Down Time (hh:mm:ss.ms)	Recovery Time (hh:mm:ss.ms)	Convergence Time(s)
1	22:24:32.925	22:24:41.016	8.091
2	22:26:48.265	22:26:56.750	8.485
3	22:28:03.816	22:28:12.160	8.344
4	22:29:19.759	22:29:28.197	8.438
5	22:30:36.038	22:30:44.943	8.905
6	22:32:01.542	22:32:09.839	8.297
7	22:33:26.264	22:33:34.065	7.801
8	22:34:54.972	22:35:03.410	8.438
9	22:36:15.020	22:36:23.680	8.660
10	22:29:19.759	22:29:27.197	7.438

BGP Scenario

The BGP scenario here shows simulation results for BGP with failure closer to the destination of the traffic in the network topology. Table 3.8 displays the results gathered.

Table 3.0.8: Convergence time Measurement for BGP with Failure closer to the destination of the traffic

Test Number	Down Time (hh:mm:ss.ms)	Recovery Time (hh:mm:ss.ms)	Convergence Time(s)
1	08:15:57.964	08:16:11.517	13.553
2	08:19:21.235	08:19:50.752	29.517
3	08:22:39.986	08:23:11.206	31.220
4	08:25:22.570	08:25:52.563	29.993

5	08:27:54.733	08:28:11.127	16.394
6	08:32:29.893	08:32:48.752	18.859
7	08:35:57.283	08:36:24.785	27.502
8	08:39:24.221	08:39:44.867	20.646
9	08:41:20.564	08:41:38.205	17.641
10	08:48:05.083	08:48:29.287	24.204

3.5.2 Routing Protocol Scenarios for Change in Topology

The layout of the network for the simulation of the four protocols that is OSPF, EIGRP, IS-IS and BGP was changed to determine the effect of change in topology on convergence time. Additional routers were added to the network to grow the size of the network. Figures 3.6 and 3.7 respectively show the network with one and two additional routers.

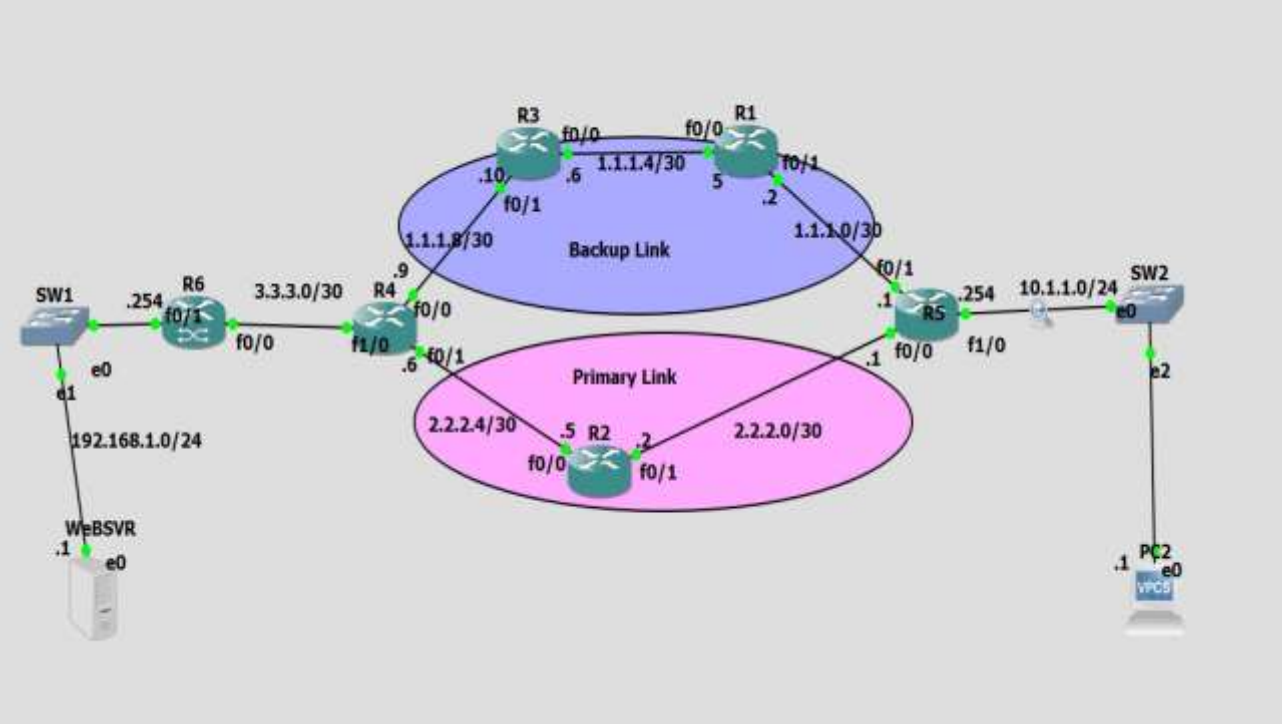


Figure 3.6: Network Diagram with one additional router

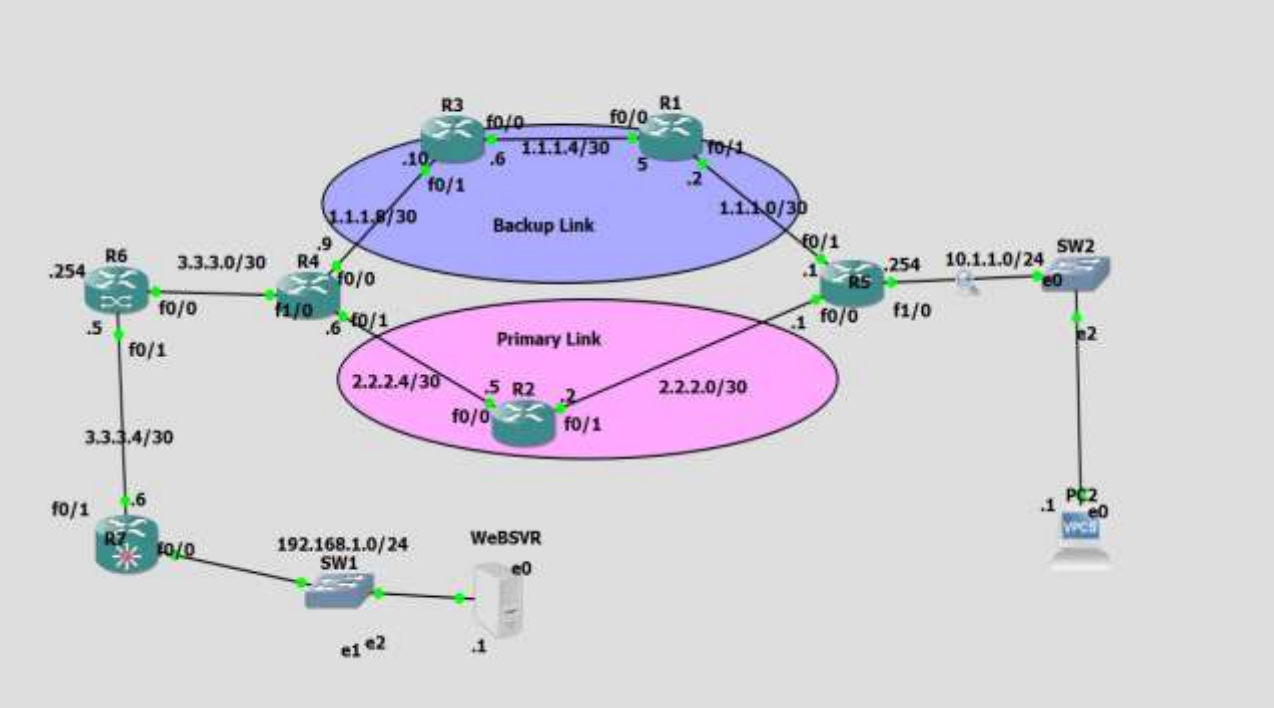


Figure 3.7: Network Diagram with two additional routers

To determine how long it takes for the network to recognise the change in topology or the time it takes for the routing tables to be updated, simulation tests were run with one to ten additional routers. The times the topology change took place was recorded and the time of recognition for all router was also recorded. The convergence time was then determined from the difference between these times.

3.5.2.1 Results of Topology Change

The key issue here is to analyse the convergence time of the protocols on the network as the size of the network grows. More routers are added to the network and the time it takes for the network to converge are recorded

OSPF Scenario

In this scenario, one to ten additional routers are added to the network and the simulation results obtained after every addition is shown in Table 3.9

Table 3.0.9: Convergence time Measurement for Topology Change for OSPF

Additional Routers	Topology Change Time (hh:mm:ss.ms)	Recognition time for all routers (hh:mm:ss.ms)	Convergence Time(s)
1	15:07:00.920	15:07:13.058	12.138
2	15:18:00.764	15:18:11.881	11.117
3	15:27:06.111	15:27:17.024	10.913
4	15:39:02.224	15:39:13.754	11.530
5	15:50:05.206	15:50:15.232	10.026
6	16:00:00.012	16:00:11.005	10.993
7	16:01:48.524	16:09:59.886	11.362
8	16:18:14.422	16:18:25.544	11.122
9	16:27:15.622	16:27:26.834	11.212
10	16:39:34.712	16:39:45.122	10.410

EIGRP Scenario

Table 3.10 shows the times recorded for the simulations run for EIGRP.

Table 3.0.10: Convergence time Measurement for Topology Change for EIGRP

Additional Routers	Topology Change Time (hh:mm:ss.ms)	Recognition time for all routers (hh:mm:ss.ms)	Convergence Time(s)
1	13:53:00.297	13:53:03.324	3.027
2	13:59:02.628	13:59:05.659	3.031
3	14:05:16.366	14:05:19.834	3.468
4	14:11:33.245	14:11:36.722	3.477
5	14:16:24.123	14:16:27.225	3.102
6	14:22:02.457	14:22:05.655	3.198
7	14:26:36.544	14:26:39.688	3.144
8	14:31:45.254	14:31:48.366	3.112
9	14:36:22.259	14:36:25.358	3.099
10	14:42:17.054	14:42:20.059	3.005

IS-IS Scenario

IS-IS after being simulated had the results as stated in Table 3.11. This determines the convergence times of the IS-IS under this scenario

Table 3.0.11: Convergence time Measurement for Topology Change for IS-IS

Additional Routers	Topology Change Time (hh:mm:ss.ms)	Recognition time for all routers (hh:mm:ss.ms)	Convergence Time (s)
1	11:57:00.741	11:57:08.785	8.044
2	12:08:00.654	12:08:12.802	12.148
3	12:19:26.172	12:19:37.254	11.082
4	12:20:02.847	12:20:12.122	9.275
5	12:31:07.130	12:31:16.326	9.196
6	12:40:11.220	12:40:21.304	10.084
7	12:49:50.011	12:49:59.154	9.143
8	12:58:12.124	12:58:20.136	8.012
9	13:07:02.034	13:07:10.084	8.050
10	13:15:00.002	13:15:07.050	7.048

BGP Scenario

BGP turned out to converge slower as compared to the other protocols. The results of the simulation are shown in Table 3.12.

Table 3.0.12: Convergence time Measurement for Topology Change for BGP

Additional Routers	Topology Change Time (hh:mm:ss.ms)	Recognition time for all routers (hh:mm:ss.ms)	Convergence Time(s)
1	12:21:00.903	12:21:19.130	18.227
2	12:26:02.377	12:26:22.635	20.258
3	12:31:01.896	12:31:20.125	18.229
4	12:37:05.105	12:37:24.646	19.541
5	12:42:27.050	12:42:46.255	19.205
6	12:48:12.388	12:48:31.102	18.714
7	12:54:18.222	12:54:39.317	21.095
8	13:00:05.503	13:00:25.024	19.521
9	13:06:14.094	13:06:32.102	18.008
10	13:12:05.788	13:12:23.823	18.035

3.6 Monitoring Delay and Jitter on the Network

Jitter and delay are characteristics that can significantly influence various network applications. Wireshark measures the influence they have on the network traffic.

3.6.1 Packet Delay

Networks are sensitive to packet delays and hence importance should be given to it to optimise these packet delays. Evaluating the delay and displaying the delay in real-time will provide valuable support for the network administrators when designing or monitoring the network conditions in real-time.

First, the routing protocol is configured by activating the protocols one after another for all routers in the network. Different packets of data were sent through the network and the time taken to transmit the packet through the network from source to destination recorded in table 3.13.

Table 3.13: Packet Delay Measurements for the Protocols

Packet size (bytes)	Packet Delay (ms)			
	OSPF	EIGRP	IS-IS	BGP
500	0.103	0.089	0.684	1.023
700	0.186	0.176	0.792	1.713
900	0.194	0.178	0.805	1.866
1000	0.203	0.178	0.923	1.922
1100	0.312	0.181	0.988	1.941
1200	0.344	0.188	1.012	1.936
1300	0.411	0.267	1.056	2.033
1400	0.523	0.356	1.233	2.045
1500	0.622	0.446	1.311	2.049
1650	0.892	0.811	1.544	2.301

3.6.2 Packet Jitter

In the context of packet networks, jitter is the delay variation in the arrival time of packets. At the sending node, packets are sent out continuously, with constant time intervals of 20 ms between successive packets. Because of network congestion, and queuing, the time between packets becomes distorted, causing variations in the arrival time of packets. The difference between the Transmit and receive times are recorded for the packets sent in table 3.14. **Table 3.14: Packet Jitter Measurements for the Protocols**

	Packet Jitter (s)

Packet size (bytes)	OSPF	EIGRP	IS-IS	BGP
500	0.12	0.01	0.502	0.633
700	0.121	0.012	0.713	1.517
900	0.223	0.021	0.569	1.513
1000	0.223	0.022	0.632	1.518
1100	0.215	0.022	0.651	1.603
1200	0.226	0.024	0.992	1.628
1300	0.312	0.025	1.012	1.718
1400	0.322	0.026	1.087	1.725
1500	0.386	0.028	1.089	1.736
1650	0.027	0.03	1.092	1.803

CHAPTER 4

ANALYSIS AND DISCUSSIONS

4.1 Introduction

This chapter of the thesis analysis the measurements that were derived from the simulation of the protocols in the network simulator. The aim of this chapter is to summarise the results collected from the experiments, present the findings, and explain the outcome of such findings. The convergence times of the protocols under study are obtained from the acquired results. Delay and Jitter was also monitored to draw a better conclusion.

4.2 Simulation Results

This section presents a comparative analysis of EIGRP, OSPF, IS-IS and BGP. The results from the diagrams in chapter three are compared. In the case of this document convergence time is defined as the time taken for the test network to recover from failure or change in topology into a stable state. In this thesis the time the traffic is interrupted is measured, that is when the failure or change is detected to when the packets are forwarded correctly again.

Table 4.1: Convergence times for the Protocols with Failure Close to the source of Traffic

Test	OSPF	EIGRP	IS-IS	BGP
1	8.346	6.078	7.799	21.975
2	8.637	5.985	8.340	23.169
3	8.494	5.938	8.368	19.331
4	8.879	5.951	8.185	15.275
5	8.162	5.469	8.590	15.743
6	9.601	6.039	9.095	19.874
7	7.788	5.491	8.532	25.646
8	8.592	5.169	8.042	28.507
9	8.836	7.298	8.051	14.664
10	6.187	6.204	7.441	28.640

From Table 4.1, the convergence times of the protocols are tabulated and on the average, it took OSPF network 8.352s to converge, EIGRP network 5.962s to converge, IS-IS network 8.244s to converge and BGP network 21.282s to converge for link failure closer to source of the traffic. This shows that EIGRP converges faster in the scenario created

Table 4.2: Convergence times for the Protocols with Failure Close to the destination of Traffic

Test	OSPF	EIGRP	IS-IS	BGP
1	7.993	4.220	8.091	13.553
2	8.490	3.969	8.485	29.517
3	7.797	4.079	8.344	31.220
4	9.078	4.007	8.438	29.993
5	9.005	5.968	8.905	16.394
6	8.673	5.972	8.297	18.859
7	8.938	4.298	7.801	27.502
8	8.841	6.001	8.438	20.646
9	7.735	5.875	8.660	17.641
10	7.704	5.969	7.438	24.204

The results of the protocols convergence with Failure closer to the destination of the traffic are displayed in table 4.2. The average convergence times were 8.375s for OSPF, 5.036s for

EIGRP, 8.290s for IS-IS and 22.953ms for BGP. For this scenario, it can also be concluded that EIGRP converges faster

Figure 4.1 and Figure 4.2 demonstrate the convergence times of the two categories of simulations run. The bars represents the protocols for the simulations and their heights determines the convergence time of the protocol. The higher the bar the, slower the time of convergence. The time it takes to converge on EIGRP is faster than the other protocols upon link failure irrespective of the position of the failure.

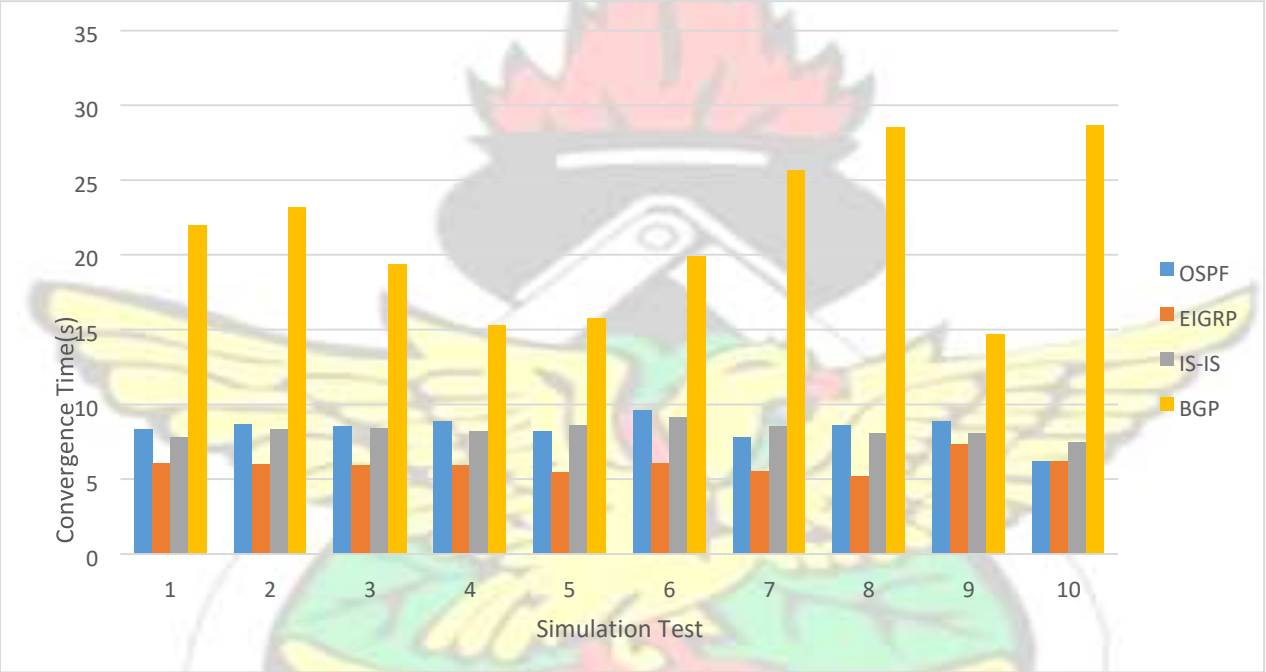


Figure 4.1 Convergence Activity for Link Failure Closer to Source of traffic

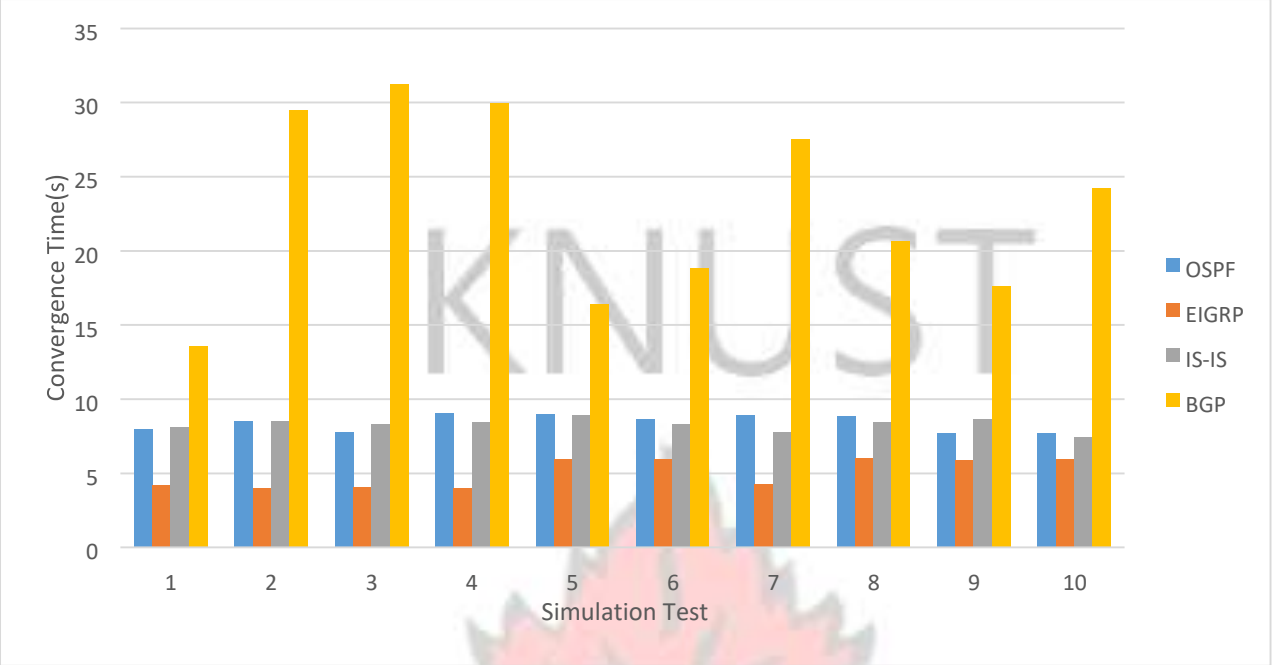


Figure 4.2 Convergence Activity for Link Failure Closer to Destination of traffic

Table 4.3: Convergence time measurement for Protocols with Topology Change Traffic

	OSPF	EIGRP	IS-IS	BGP
1	12.138	3.027	8.044	18.227
2	11.117	3.031	12.148	20.258
3	10.913	3.468	11.082	18.229
4	11.530	3.477	9.275	19.541
5	10.026	3.102	9.196	19.205
6	10.993	3.198	10.084	18.714
7	11.362	3.144	9.143	21.095
8	11.122	3.112	8.012	19.521
9	11.212	3.099	8.050	18.008
10	10.410	3.005	7.048	18.035

Table 4.3 represents the convergence times of protocols for the change in topology scenario. It took an average time of 11.082s for OSPF to converge, 3.166s for EIGRP to converge, 9.208s for IS-IS to converge and 19.083s for BGP to converge for change in topology.

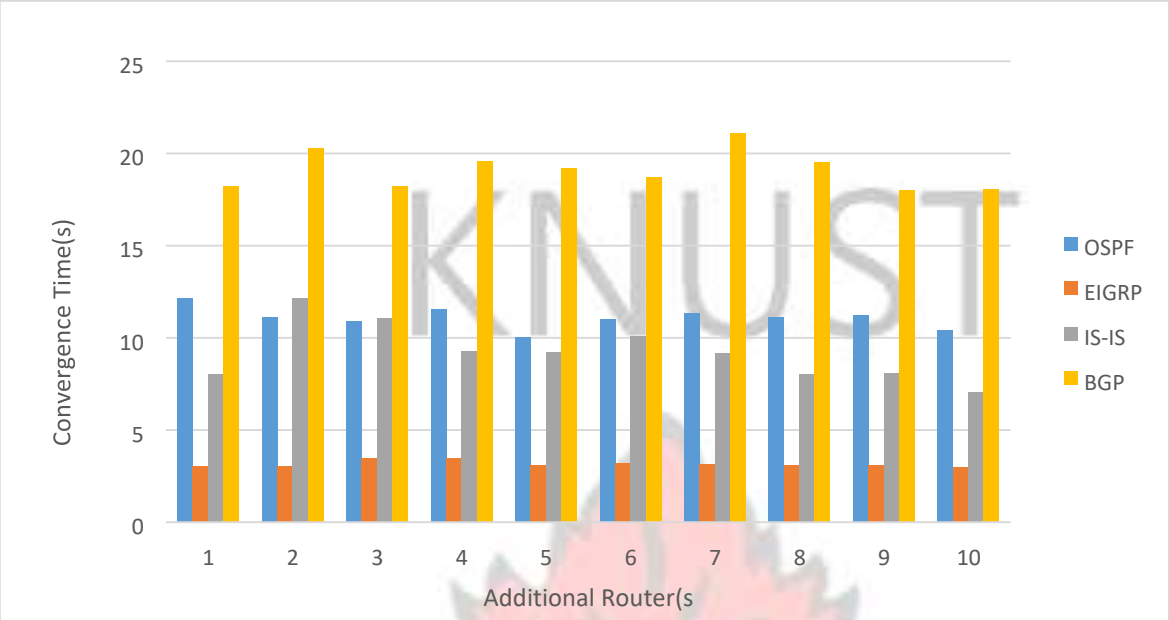


Figure 4.3 Convergence Activity for Change in Topology

An observation from Figure 4.3 shows that the convergence time of EIGRP is faster than that of the other protocols on the networks as it show the lowest height of the bars representing low times of convergence. This is due to the fact that as soon as there is a change in the network, the change is detected and a query is relayed to the immediate neighbours to get a substitute and this information is propagated to every router in the network. As the change occurred in the IS-IS network, convergence was faster as compared to the OSPF network. BGP turned out with the slowest convergence in the simulations run.

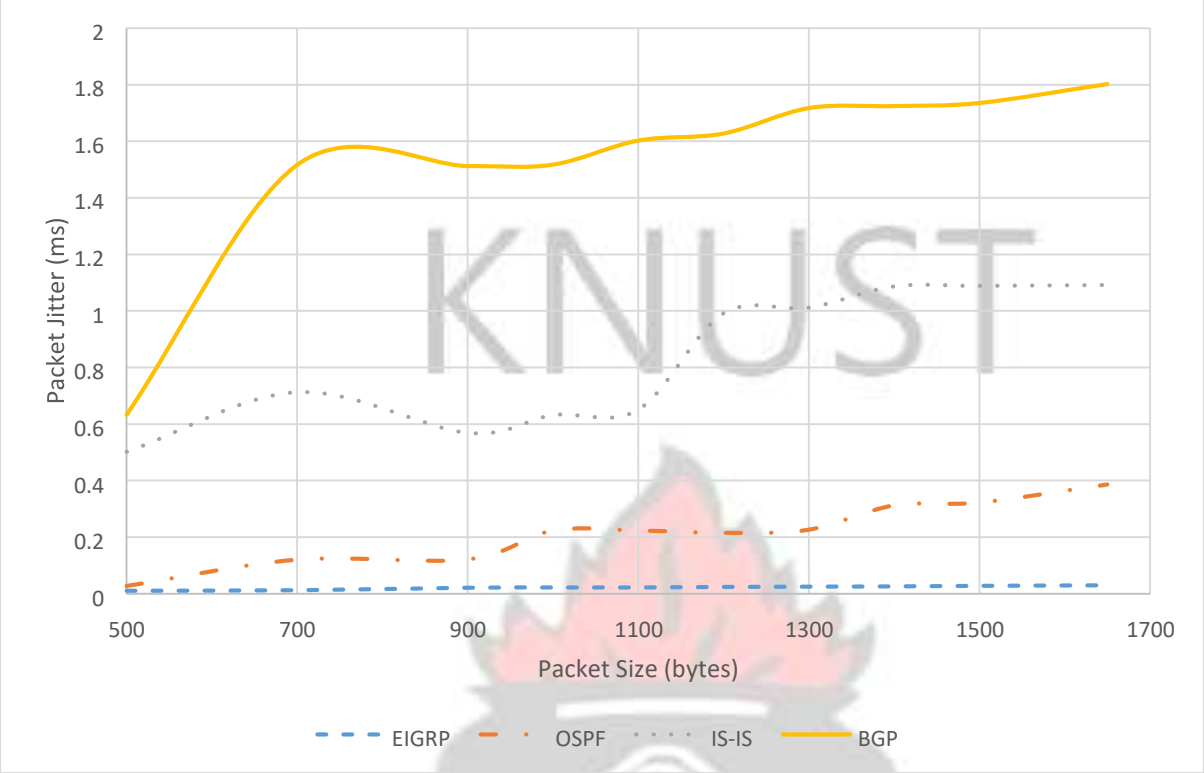


Figure 4.4 Packet Delay vs Packet size

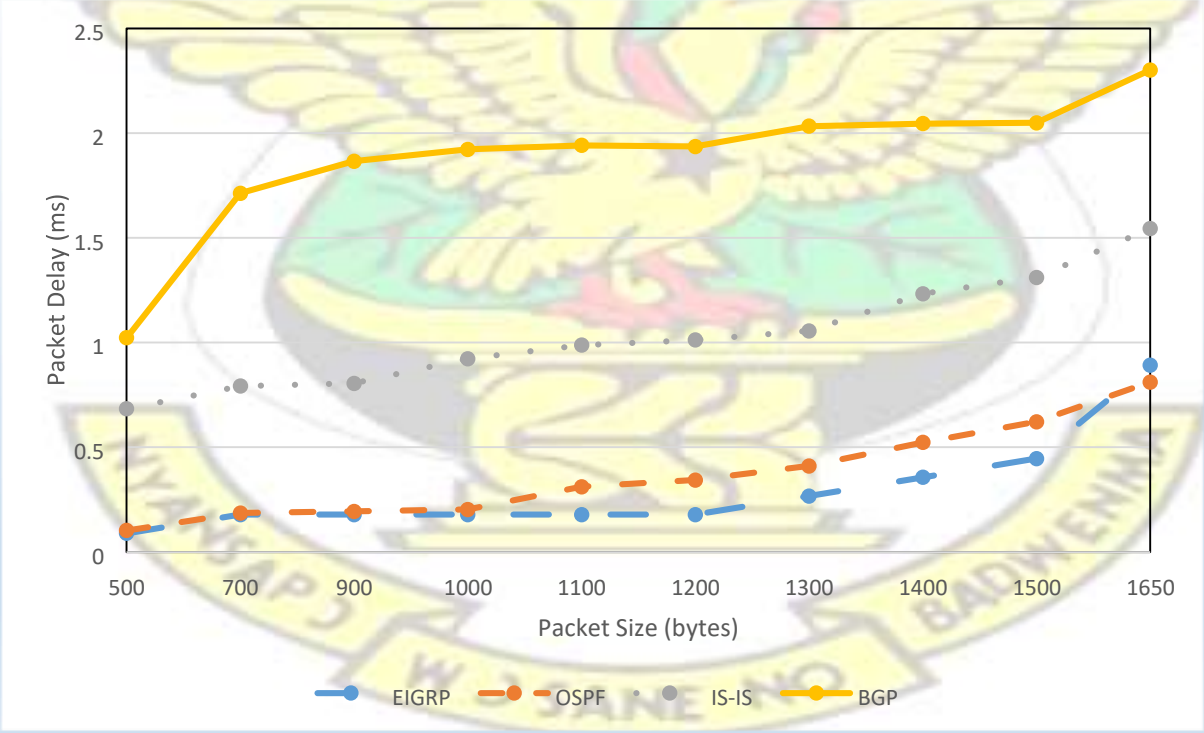


Figure 4.5 Packet Jitter vs. Packet size

Based on the simulations run on the networks, EIGRP and the BGP protocols experienced the lowest and highest delays and jitter, respectively. Figure 4.4 and Figure 4.5 shows the progress of delay and jitter as different packet sizes we being sent across the network.

4.3 Analysis

This work was divided into two sections. First, a layout of a network model with a link failure was done and OSPF, EIGRP, IS-IS and BGP simulated by using GNS3 and Wireshark to observe the convergence duration. Secondly, in the same network scenario, the topology was changed by increasing the number of routers thereby making the network larger and the protocols were simulated in the network model to observe their convergence times.

EIGRP came out with the best convergence time for all scenarios based on the results. This is because it uses a successor table to plan ahead of time if there is a failure in a route. This means EIGRP learns the topology information and updates more rapidly. IS-IS had a better convergence time than OSPF. This result makes sense because even though both are link-state routing protocols and uses the same algorithm which is Shortest Path First (SPF) algorithm, IS-IS has superior scalability. BGP exhibited the slowest convergence. This is because in BGP after a network failure affects the availability of a path to a destination, the routers topologically closest to the failure will identify the fault, withdraw the route and make a new local decision on the preferred alternative route, if any, to the set of destinations and this takes time.

Another interesting observation made was that, with EIGRP as the number of routers increases, the time for convergence were almost the same. OSPF and IS-IS convergence times increased as the routers increased. For the link failure scenarios, it was observes that there was a slight increase in the time, but not significant for the protocols when the failure detected was far from the source of the traffic as compare to the failure being close to the source of the traffic.

The performance of packet delay for EIGRP is better than for the other protocols. The packet delay variation of OSPF, IS-IS and BGP network are higher while that of EIGRP network is

low with available network load. The simulation results have also shown that the end-to-end delay of EIGRP network is relatively less than OSPF, IS-IS and BGP network. As a result, data packets in EIGRP network reach faster to the destination compared to the other networks.

In conclusion, EIGRP came out best because looking at all the scenarios implemented. It is therefore the most appropriate protocol. Comparing OSPF and IS-IS, the former is preferred over the latter and BGP came out with the lowest performance considering all scenarios.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Introduction

This section of the research presents a precise summarised conclusion of the comparison done in terms of convergence times of the protocols under study along with recommendations for this research.

5.2 Conclusion

One of the key performance indicators in modern day high-availability networks is Convergence time. To avoid excessive traffic loss, routing tables across the entire network should converge in minimum time. It is practically impossible for all routers in a network to simultaneously discover a change in topology. Depending on the protocol being used, as well as many other factors including a router's distance from the point of change and the number of routers in the network, a considerable time delay may pass before all the routers in that network

reach a consensus on what the new topology is. It is very important to keep in mind that convergence is not immediate. How much time is required for convergence to occur is where the uncertainty lies.

In this research, GNS3 was used as a tool for the analysis and performance comparison of four protocols namely OSPF, EIGRP, IS-IS and BGP. An experimental examination of the convergence of the protocols, was conducted under three different situations. The results for the protocols were collected to aid in the comparison of the performance of the protocols. Based on the simulation results, EIGRP gave the best performance. This was so because EIGRP generate the least traffic and hence it will consume the least bandwidth, leaving enough bandwidth for data transmission. In the case of topology changes, EIGRP also performed best as well as when there was a broken Ethernet connection.

From the simulations done, EIGRP was the most appropriate choice for all scenarios as it exhibited the fastest convergence. It also utilized bandwidth efficiently.

IS-IS was next in order as far as convergence time was concerned and then OSPF came next. BGP performed poorly and is therefore not suitable for large networks. It can therefore be stated based on the results achieved that there is a significant difference in the performance of the protocols as far as convergence time is concerned.

This research can act as a guidance for service providers and network administrators to help in making better decisions when it comes to choosing the right routing protocol for networks.

5.3 Recommendation

The research work for the routing convergence times can be analyzed from the aspects of other protocols available using different metrics like bandwidth, cost, distance, Bit Error Rate and delay with appropriate and available experimental settings and tools.

In future, complex topologies can be used to measure and study the behavior of the routing convergence time taking various distinctive factors into consideration when using different topologies varying in sizes and shapes. Security analysis for OSPF, EIGRP, IS-IS and BGP can also be done. Also another simulator such as the OPNET can be used to carry out the research. OPNET is high level simulation tool which can be used in many high level researches. It enables simulation of heterogonous networks by employing various protocols. This will help to compare results and make further analysis.

REFERENCES

Archana, C. (2015). Analysis of rip v2,ospf,eigrp configuration on router using cisco packet tracer. International Journal of engineering Science and Innovative Technology (IJESIT), pg 215-220.

Aslam, W. (2008). Empirical study to observe route recoverability performance of routing protocols in real-time communication.

Caesar, M., & Rexford, J. (2013). Advances in communication networking. Institute of Electrical and Electronic Engineers.

Chadha, A., & Gupta, K. A. (2013). Review on enhanced interior gateway routing protocol. Global Journal of Computer Science and Technology, Volume XIII (Issue VI, Version I), pg 41-44.

Chinara, S., & Kumar, S. (2009). A survey on one hop clustering algorithm in mobile ad hoc network. Network system management, pg 183-207.

Devi, R., B.Sumathi, T.Gandhimathi, & G.Alaiyarasi. (2015). Performance metrics of manet in multi-hop wireless ad-hoc network routing protocols. International Journal of Computational Engineering Research (IJCER), pg 2250-3005.

Fortz, B., & Thorup, M. (2002). Optimizing ospf/is-is weights in a changing world. IEEE Journal on Selected Areas in Communications, pg 756-767.

Fjeldbo, Stig Jarle (2005). Administration of Remote Computer networks.

Gil, P., Garcia, G. J., , Delgado, A., Medina, R. M., Calderon, A., & Marti, P. (2014). Computer network visualization with gns3: Evaluating a solution to optimize resources and achieve a distance learning. IEEE journal in Frontiers in Education Conference, pg 1-4.

Graziani, Johnson, Rick, & Allan. (2008). Routing protocols and concepts: Ccna exploration companion guide in p. education.

Islam, N. M & Ashique, A. U. (2010). Simulation Based EIGRP over OSPF Performance Analysis, pg 4

Jaffar, T. M. (2007). Simulation-based routing protocols analysis (Ph.D.). Department Electrical Engineering, Georgia Institute of Technology.

Kisten, & Chung, S.-T. (2003). Analysis and experimentation on dynamic routing protocols:eigrp and ospf. I. C. Computing.

Kumar, J., Samiksha, Kaur, A., & Singh, H. (2014). Performance analysis of ripv2 protocol in wired network using cisco packet tracer. International journal Computer Technology and Applications.

Lammle, T. (2005). Cisco certified network associate, study guide (5th Edition. ed.) [Computer software manual]. San Francisco, USA.

Larsson, T., & Hedman, N. (1998). Routing protocols in wireless ad-hoc networks-a simulation study (Unpublished master's thesis). Department of Communication and Engineering, Lule University, Stockholm.

Lemma, E., Hussain, S., & Anjelo, W. (2010). Performance comparison of eigrp/is-is and ospf/is-is.

Li, T., Walter, E., & Fallon, T. (2010). The use of visualization for router network simulation. , pg 15925.1 - 15925.11. (published in American Society for Engineering Education).

Liangxu, S., Liansheng, W., Yujun, Z., & Hang, Y. (2013). comparison between physical devices and simulator software for cisco network technology teaching. In Computer science and education (pg 1357-1360). (8th Internation Conference)

Malhotra, R. (2002). Ip routing.

Manjeshwar, A., & Agrawal, D. (2015). A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. (San Francisco.)

Moy, J. (1989). The ospf specification. http://www.iet.org/rfc/rfc.

Obradovic, Davor (2000). Formal Analysis of Routing Protocols, Ph.D. Thesis, University of Pennsylvania, pg 5.

Panford, J. K., Riverson K. & Boansi O. K (2015). Comparative analysis of convergence times between rip, and eigrp routing protocols in a network. Research Journali's; Journal of Computer Science., pg 1-5.

Patil, M. V. D., & Deshmukh, P. A. R. (2014, April). Performance improvement of routing protocol using two different mobility models in vehicular adhoc vehicular network. International Journal Of Computer Science And Mobile Computing, vol. 3 (issue. 4), pg. 440-445.

Pei D., Azuma M., Nguyen N., Chen J., Massey D., and Zhang L.. BGP-RCN: Improving BGP convergence through Root Cause Notification. Computer Networks, June 2005.

Shah, A., & Waqas, J. R. (2013, November). Performance analysis of rip and ospf in network using opnet. International Journal of Computer Science Issues, vol. 6 (no. 2).

Singh, H., & Beebee, W. (2013). Basic requirements for ipv6 customer edge routers.

Siraj, S., Gupta, A. K., & Badgujar, R. (2012). Network simulation tools survey. International Journal of Advanced Research in Computer and Communication Engineering, vol. 1 (no. 4), pg 199-206.

Todorovic, I., & Sepanovic, S. (2011). Measurements of convergence time for rip and eigrp protocols.

APPENDIX

Appendix A: Sample Router Configurations

Router config R1#show running-config
!
interface FastEthernet0/0 ip
address 1.1.1.5 255.255.255.252
duplex auto speed auto
!
interface FastEthernet0/1 ip
address 1.1.1.2 255.255.255.252
duplex auto speed auto
!
!
router eigrp 100
network 1.0.0.0
no auto-summary
!

R2#show running-config

interface FastEthernet0/0 ip

address 2.2.2.5 255.255.255.252

duplex auto speed auto

!

interface FastEthernet0/1 ip

address 2.2.2.2 255.255.255.252

duplex auto speed auto

!

interface

FastEthernet1/0 no ip

address shutdown

duplex auto

speed auto

!

router eigrp 100

forsaken network

2.0.0.0 no auto-

summary

R3 interface FastEthernet0/0 ip

address 1.1.1.6 255.255.255.252

duplex auto speed auto

!

interface FastEthernet0/1 ip

address 1.1.1.10 255.255.255.252

duplex auto speed auto

!

interface

FastEthernet1/0 no ip

address shutdown

duplex auto speed auto

!

router eigrp 100

network 1.0.0.0

no auto-summary

router 4 interface

FastEthernet0/0

ip address 1.1.1.9

255.255.255.252

duplex auto speed

auto

!

interface FastEthernet0/1 ip

address 2.2.2.6 255.255.255.252

duplex auto speed auto

!

interface FastEthernet1/0 ip address

192.168.1.254 255.255.255.0 duplex

auto speed auto

!

router eigrp 100

network 1.0.0.0

network 2.0.0.0

network 192.168.1.0

no auto-summary

router 5

!

interface FastEthernet0/0 ip

address 2.2.2.1 255.255.255.252

shutdown duplex auto speed

auto

!

interface FastEthernet0/1

ip address 1.1.1.1

255.255.255.252 duplex auto

speed auto

!

interface FastEthernet1/0 ip

address 10.1.1.254 255.255.255.0

duplex auto speed auto

!

router eigrp 100

network 1.0.0.0

network 2.0.0.0

network 10.0.0.0

no auto-summary

```
PC2> trace 192.168.1.1
trace to 192.168.1.1, 8 hops max, press Ctrl+C to stop
 1   10.1.1.254   10.007 ms  5.042 ms  14.992 ms
 2   1.1.1.2   30.060 ms  25.017 ms  30.016 ms
 3   1.1.1.6   55.027 ms  60.030 ms  40.023 ms
 4   1.1.1.9   70.035 ms  65.031 ms  75.040 ms
 5     *  *  *
 6   *192.168.1.1   77.561 ms (ICMP type:3, code:3, Destination port unreachable)
```

Appendix B: Sample of Captured Traffic in WireShark

	Time	Source	Destination	Protocol	Length	Info
3	23:03:30.319	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=0/0, ttl=255 (reply in 4)
4	23:03:30.895	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=0/0, ttl=252 (request in 3)
5	23:03:31.018	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=1/256, ttl=255 (reply in 6)
6	23:03:31.606	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=1/256, ttl=252 (request in 5)
7	23:03:31.690	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=2/512, ttl=255 (reply in 8)
8	23:03:32.339	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=2/512, ttl=252 (request in 7)
9	23:03:32.447	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=3/768, ttl=255 (reply in 10)
10	23:03:33.136	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=3/768, ttl=252 (request in 9)
11	23:03:33.218	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=4/1024, ttl=255 (reply in 12)
12	23:03:33.850	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=4/1024, ttl=252 (request in 11)
13	23:03:33.925	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=5/1280, ttl=255 (reply in 14)
14	23:03:34.384	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=5/1280, ttl=252 (request in 13)
15	23:03:34.449	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=6/1536, ttl=255 (reply in 16)
16	23:03:34.997	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=6/1536, ttl=252 (request in 15)
17	23:03:35.079	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=7/1792, ttl=255 (reply in 18)
18	23:03:35.707	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=7/1792, ttl=252 (request in 17)
19	23:03:35.833	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=8/2048, ttl=255 (reply in 21)
21	23:03:36.376	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=8/2048, ttl=252 (request in 19)
22	23:03:36.511	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=9/2304, ttl=255 (reply in 23)
23	23:03:37.180	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=9/2304, ttl=252 (request in 22)
24	23:03:37.322	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=10/2560, ttl=255 (reply in 25)
25	23:03:37.797	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=10/2560, ttl=252 (request in 24)
26	23:03:37.869	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=11/2816, ttl=255 (no response found!)
28	23:03:39.905	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=12/3072, ttl=255 (no response found!)
29	23:03:41.876	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=13/3328, ttl=255 (no response found!)
30	23:03:42.006	10.1.1.254	10.1.1.1	ICMP	70	Destination unreachable (Host unreachable)
31	23:03:42.076	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=14/3584, ttl=255 (no response found!)
32	23:03:42.151	10.1.1.254	10.1.1.1	ICMP	70	Destination unreachable (Host unreachable)
33	23:03:42.219	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=15/3840, ttl=255 (no response found!)
34	23:03:42.373	10.1.1.254	10.1.1.1	ICMP	70	Destination unreachable (Host unreachable)
35	23:03:42.476	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=16/4096, ttl=255 (no response found!)
36	23:03:42.631	10.1.1.254	10.1.1.1	ICMP	70	Destination unreachable (Host unreachable)
37	23:03:42.761	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=17/4352, ttl=255 (no response found!)
38	23:03:42.847	10.1.1.254	10.1.1.1	ICMP	70	Destination unreachable (Host unreachable)
39	23:03:42.978	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=18/4608, ttl=255 (no response found!)
40	23:03:43.067	10.1.1.254	10.1.1.1	ICMP	70	Destination unreachable (Host unreachable)
41	23:03:43.156	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=19/4864, ttl=255 (no response found!)
44	23:03:45.144	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=20/5120, ttl=255 (reply in 45)
45	23:03:45.708	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=20/5120, ttl=251 (request in 44)
46	23:03:45.774	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=21/5376, ttl=255 (reply in 48)
48	23:03:46.612	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=21/5376, ttl=251 (request in 46)
49	23:03:46.771	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=22/5632, ttl=255 (reply in 50)
50	23:03:47.431	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=22/5632, ttl=251 (request in 49)
51	23:03:47.506	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=23/5888, ttl=255 (reply in 52)
52	23:03:48.354	192.168.1.1	10.1.1.1	ICMP	114	Echo (ping) reply id=0x000a, seq=23/5888, ttl=251 (request in 51)
53	23:03:48.457	10.1.1.1	192.168.1.1	ICMP	114	Echo (ping) request id=0x000a, seq=24/6144, ttl=255 (reply in 55)

GLOSARRY

Administrative Distance	A feature used by a router to select the best path when there are two or more routes to the same destination.
Algorithm	A procedure for solving a problem.
Autonomous System	A group of networks under the same administrative domain.
Computer network	A set of computers connected together for the purpose of sharing resources.
Convergence Time	The needed time for the routers to learn routes of the entire network.
Dynamic Routing	A routing technique that permits routers to choose the most appropriate path when there is a layout change in the logical network.
Metrics	Parameters employed to ascertain the optimal path to a destination.
Router	A network device that forwards data between computer networks.
Routing	It refers to the establishment of routes that data packets take on their way to a particular destination.
Routing Protocol	A set of rules that shows how routers interact with each other and also disseminates information that helps in the selection of routes between nodes on a computer network.
Simulation	The creation of a model for the study of the behaviour of an actual system being observed.
Static Routing	A routing procedure where the routing table is manually created.
Topology	A network topology is the arrangement of the elements of a communication network.