DETERMINATION OF THE OPTIMAL ROUTING PROTOCOL FOR AN INTER-CAMPUS PRIVATE CLOUD NETWORK SYSTEM

BY

EZEANI, CHUKWUEMEKA OBIOMA
(B.ENG.)
20104771768

A THESIS SUBMITTED TO THE POSTGRADUATE SCHOOL, FEDERAL UNIVERSITY OF TECHNOLOGY OWERRI

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE (M.Sc.) DEGREE IN INFORMATION MANAGEMENT TECHNOLOGY

MAY, 2024

© Federal University of Technology,

Owerri

CERTIFICATION

This is to certify that this work *"Analysis of optimal routing protocol for an inter-campus private cloud network system"* was carried out by Chukwuemeka Obioma Ezeani (20104771768) in partial fulfillment for the award of the degree of M.Sc in Information Technology in the Department of Information Technology of the Federal University of Technology Owerri.

Engr. Dr. E. C. Amadi
(Project Supervisor)

03/07/2024
Date

Dr. C. Etus
(Co-Supervisor)

29/05/2024
Date

Dr. A. I. Otuonye
(HOD – Information Technology)

3/7/24
Date

Prof. Mrs. U. F. Eze
(Dean, SICT)

3/7/24
Date

Prof. B. O. Esonu
(Dean, PGSchool)

Date

Prof. F. N. Ugwoke
(External Examiner)

29/05/2024
Date

DEDICATION

I dedicate this project work to God Almighty with whom all things are possible. I also dedicate this work to my wife Mrs. Ruth Ezeani and my parents, Chief Francis & Josephine Ezeani whose words of encouragement and push for tenacity ring in my ears.

ACKNOWLEDGEMENT

I give special thanks to Almighty God, without whom the completion of this project work would have been impossible. For his mercies, protection, provisions, sustenance, good health and favour, I am highly grateful.

A special gratitude I give to my project supervisor, Engr. Dr. E. C. Amadi who supported me throughout this process. Without your help and guidance, this thesis would not have been possible.

I would like to express my deepest appreciation to my Head of Department; Engr Dr. Anthony I. Otuonye and the Dean of Faculty SICT; Prof. Mrs. U. F. Eze Udoka. Thank you for your support, time and contribution.

I am grateful to my Lecturers; Prof. Mrs. U. F. Eze Udoka, Engr Dr. Anthony I. Otuonye, Engr. Dr. E. C. Amadi, Dr. C. Etus, Dr. A. M. John-Otumu, Engr. Dr. O. C. Nwokonkwo and Engr. Dr. E. M. Nwanga, whose teachings, suggestions and encouragement helped me to coordinate my project work and to write this report.

I am deeply thankful to my family for their love and support during this process. Without their encouragement and motivation, I would not have been able to complete this journey.

I also acknowledge all the scholars and research fellows whose materials and work provided important insights that helped during this project work.

Finally, I acknowledge all my friends and colleagues for all their support and encouragement during this project work.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

With the need for resources sharing and the integration of cost-effective IT solution across tertiary institution in Nigeria, modalities for an inter-campus cloud network is presented in this project. The inter-campus cloud network provides a platform for sharing resources across campuses instead of replicating such resources which are in many cases underutilized. This work presents the optimal routing protocol for an inter-campus cloud network system that connects 5 campuses together within Owerri city in Nigeria. A star-star hybrid network topology was adopted in this project work and was modelled using Packet Tracer simulator. The network was simulated using the three main routing protocols namely RIP (routing information protocol), OSPF (open shortest path first) and EIGRP (enhanced interior gateway routing protocol) which were tested and compared to determine the routing protocol with the shortest convergence time. The connection time of the three routing protocols used on the exchange point network was run at a TTL value of 24 and packet size of 32 bytes. The RIP provided a convergence time that is within 3 and 4 seconds, with slightly varied spikes of not up to 10 seconds, OSPF and EIGRP also tries to maintain a time of between 3 and 4 seconds but is plagued with so much spikes of up 20 seconds for EIGRP and 17seconds for OSPF. The results showed that with a routing protocol like RIP, connections between the campuses via the exchange point will converge faster. As a result, RIP routing protocol was adopted as the optimal routing protocol to be used for the network configuration due to its better convergence time.

Keywords: Internetwork, Routing Protocol, Inter Campus, Cloud Network, RIP.

CHAPTER ONE

INTRODUCTION

1.1 Background Information

What comes to mind when information needs to be shared is “Networks”. Networks cuts across different fields of learning; business, human body mechanism, organization work flow and lots more. Computer networks has become a critical component of organization infrastructure as it provides the platform for easy information flow. Networks can be localized or globalized; the internet is a global network while a network that runs within an organization is local.

Internetworking is the communication between two or more networks of systems, which encompasses every aspect of connecting computers together for the purpose of sharing resources. Internetworks have grown to support vastly disparate end-system communication requirements. The internetwork layer defines the protocols responsible for the logical transfer of data throughout the network (Vakaliuk *et al*., 2023). An internetwork requires many protocols and features to permit scalability and manageability without constant manual interventions. (Cloudflare, 2019).

Internetworks have grown to support vastly disparate end-system communication requirements. Traditionally, internetworks can either work as an intranet network where connection between devices are localized or and extranet where known external users connect to a local network. On a broader scale however, the internet is a global network that connects devices all over the globe using the Transmission Control Protocol and the Internet Protocol (TCP/IP) suite.

The growing bandwidth power of the Internet has pushed the client/server model one step further towards what is called the “Cloud Computing Model”. Cloud computing refers to a model of computing that provides access to a shared pool of computing resources (computers,

storage, applications, and services) over an Internet protocol driven network. These “clouds” of computing resources can be accessed on an as-needed basis from any connected device and location (Taleb & Mohamed, 2020).

An inter-campus Private Cloud network is a cloud installation that is largely controlled from within an organization’s premises. Local users of applications hosted on the private cloud-driven infrastructure have access to the facility without need for internet connectivity. Only external users of the facility require some form of internet connectivity to gain access. This installation is modular in nature such that it can be easily replicated and interconnected with each other to form a cluster.

With the increased privacy challenges faced by public cloud users, organizations are now defaulting back to setting up private clouds and, in some cases, allowing only some of their data to be fed into the internet in a public-private hybrid fashion (Abdulle et al., 2022).

Exiting cloud platforms like Amazon Web Services, Google Cloud Platform, Alibaba, Microsoft Azure and IBM Bluemix among others provide ready to use infrastructure or applications that organization leverage on to setup their cloud presence online. Using these cloud platforms, organization rely heavily on the security plugins provided by their cloud providers in addition to their private security instance. This is one major drawback of public cloud as entire organizations data are domicile in cloud providers premises. The need for internet connection and cloud subscription are important considerations when adopting public cloud platforms. On the other hand, aside from providing organizations with more control over sensitive data, a private cloud infrastructure helps to support organizations' data privacy needs by keeping data within company’s premises. Organizations that are very concerned about data privacy while needing online presence opt for a hybrid cloud installation that integrates the private cloud facility alongside the public cloud platforms (Hosseini Shirvani *et al.*, 2022).

For institutions of learning, cloud computing provides a fresh alternative to building a flexible and cost-effective learning environment with minimal access to hardware. The adoption of various technological innovations in academia has been accelerated by cloud computing infrastructures. Applications like the Computer based test (CBT), result processing application, transcript generating applications can run conveniently on private cloud installations with minimal connection to the internet for remote users.

Adopting private cloud-driven installation can largely minimize cost associated with cloud and internet bandwidth subscription. Investigation into the current approach to application hosting in tertiary institution, shows that most applications run on public hosting platforms with almost nothing running on private facilities (Muhairat *et al*., 2019).

The significance of using private cloud computing in education was demonstrated in a case study conducted at Al-Zaytoonah University (Jordan). The case study results indicate that cloud computing can save the cost and resources of university. The main reasons to select the private model for Al-Zaytoonah University were to reduce associated costs, deliver high quality and consistent services, and to ensure a stable system for students. Al-Zaytoonah cloud computing infrastructure is based on OpenStack architecture which is an open source platform. (Muhairat et al., 2019).

This work integrates the three cloud computing models in one modular, scalable, and movable block. The models integrated include Software as-a-service (SaaS), Platform as-a-service (PaaS) and Infrastructure as-a-service (IaaS). The scalability feature allows each block of installation to be easily expanded, while the mobility feature makes each block of installation to be easily redeployed or replicated at a different location.

As population increases in societies, the need for more efficient means of communication becomes inevitable. Individuals desire to communicate with each other while organization seek

to communicate with their employees and customers. Institutions of learning are also facing similar challenges and thus the need for networks as currently being experienced in Nigeria.

Many times, staff and student find it difficult to connect to resource repositories online due to poor network infrastructures. Lots of resources are being budgeted for internet subscription at different levels of institutional management and yet there is still gross internet deficiency. Optimal routing protocol for Internetworks designs have grown to support vastly disparate end-system communication requirements in campuses, making sure that scalability, availability, security and manageability of the network is guarantee. An internetwork requires many protocols and features to permit scalability and manageability without constant manual intervention.

The purpose of routing protocols is to learn of available routes that exist on the Internetwork, build routing tables and make routing decisions. Some of the most common routing protocols include IGRP, EIGRP, OSPF, IS-IS and BGP. There are two primary routing protocol types although many different routing protocols defined with those two types. Link state and distance vector protocols comprise the primary types. Distance vector protocols advertise their routing table to all directly connected neighbors at regular frequent intervals using a lot of bandwidth and are slow to converge (Amadi, 2014). When a route becomes unavailable, all router tables must be updated with that new information. The problem is with each router having to advertise that new information to its neighbors, it takes a long time for all routers to have a current accurate view of the network. Distance vector protocols use fixed length subnet masks which aren't scalable. Link state protocols advertise routing updates only when they occur which uses bandwidth more effectively.

Routers don't advertise the routing table which makes convergence faster. The routing protocol will flood the network with link state advertisements to all neighbor routers per area in an

attempt to converge the network with new route information. The incremental change is all that is advertised to all routers as a multicast LSA update. They use variable length subnet masks, which are scalable and use addressing more efficiently (Syahputra *et al*., 2020)

1.2 Problem Statement

Designing an intercampus cloud network can be a challenging task. To design reliable and scalable internetworks, network designers must aim to proffer solution to the following:

1. Scalability: ability of the network to expand when needed
2. Low performance in network configuration
3. Poor network security from internal and external hackers
4. Redundancy: because robust network require redundancy so that if a key element of the network fails, the network itself will still operate
5. Compatibility: hardware and software
6. Compatibility: organization and people
7. Manageability: ability to manage the network within organization budgeted resource
8. Network operational policy: Network should provide privilege levels for users.

There has been challenge of poor network performance within campuses in developing countries like Nigeria. These challenges can be classified under the following headings:

1. High cost of internet subscription to meet the internet need of a growing population within the campus (staff and student).
2. Low quality equipment available in the market that are easily damaged with the slighted environmental challenge like lightening.
3. Poor network management approaches due to lack of skilled manpower.
4. Poor network design structure.

In general, the network design problem consists of the following three general elements (Benefa, 2015):

i. **Environmental givens**-Environmental givens include the location of hosts, servers, terminals, and other end nodes; the projected traffic for the environment; and the projected costs for delivering different service levels. Houses, rivers mountains and drainages are network problems.

ii. **Performance constraints**-Performance constraints consist of network reliability, traffic throughput, and host/client computer speeds (for example, network interface cards and hard drive access speeds).

iii. **Internetworking variables**-Internetworking variables include the network topology, line capacities, and packet flow assignments, which relies largely on the network protocol.

Traditionally, campus networks have been characterized by relatively low throughput, high delay, and high error rates due to the use or choice of inappropriate routing protocols. Networks that grow unheeded without any plan tend to develop in an unstructured format. When network devices communicate with many other devices, the workload required of the CPUs on the devices can be burdensome. For example, in a large flat (switched) network, broadcast packets are burdensome. A broadcast packet interrupts the CPU on each device within the broadcast domain, and demands processing time on every device for which a protocol understanding for the broadcast is installed. This includes routers, workstations, and servers. This project proposes an inter-campus cloud network system with optimal routing that solves the network challenges experiences across campuses in Nigeria as mentioned above while at the same providing a platform for resource sharing and reduction in network management cost.

1.3 Objectives

The main objective of this project is to determine the optimal routing protocol for an inter-campus cloud network system.

Specifically, this work will achieve the following specific objectives:

1. Empirical review of existing network infrastructure of selected institutions in the South-East.
2. Model an Inter-Campus Cloud Network System (ICCNS) for five (5) institutions.
3. Simulate the model on packet tracer network simulator using the exchange point approach.
4. Simulate selected routing protocols on the network topology model to determine the best routing protocol for the exchange point network.
5. Analyze the output of the simulation using the convergence time for each protocol tested.

1.4 Research Questions

This work answered the following questions:

1. What is the network structure of selected campuses in southeast Nigeria?
2. Can an inter-campus network be modelled for institutions using existing network architecture?
3. Can an inter-campus network be modelled using packet tracer?
4. What routing protocol best suits an inter-campus cloud network?
5. What convergence time is the lowest for selected routing protocols?

1.5 Justification of the Study

This work provides details of the equipment requirements and configuration for an inter-campus cloud-based network that is cost-effective and easy to deploy.

This work will provide to network engineers a guide for network design and configuration within campus environment, paying attention to network efficiency. It pays attention to equipment, topology and protocol in the design and deployment of network in campuses.

This work also provides a guide to institution administrators and the government to help check the quality of infrastructure being deployed by contractors in our tertiary institutions.

1.6 Scope of the Study

The work covers Inter-Campus Cloud Network System (ICCNS) modeling for 5 Major campuses in Nigeria. This work will be limited to providing network experiences with a basis for the choice of a particular routing protocol that is suitable for an intercampus network covering the 5 selected higher institutions in Imo State. The selected institutions are within the Owerri city and they include: Federal University of Technology Owerri (FUTO), Alvan Ikoku Federal College of Education (AIFCE), Federal Polytechnic Nekede (FEDPOLY), University of Agriculture and Environmental Sciences (UAES) and Imo State University (IMSU).

CHAPTER TWO

LITERATURE REVIEW

2.1 Conceptual Framework

Network systems have evolved over the year from small units of computers interconnected to each other to a very massive network of computers that form the modern-day internet. The internet is a system of interconnected computers all over the world with the soul aim of sharing resource via a web known as the World Wide Web (WWW).

2.1.1 Historical Development of Network Systems

Although the computer industry is still far younger than a host of other industries (e.g. automobile and air transportation), computers have made significant progress in a short time. During the first 20 years of their existence, computer systems were highly centralized, usually within a location like a single room. A medium sized company or university might just have one or two computers, while large institutions had at most a few dozen. Computer systems have grown over the years to the extent that the concept of bringing a works to a particular central system for processing is now totally obsolete (Froehlich et al., 2021). Also fading away is the use of the conventional 'cybercafé' mainly obtainable in less developed environments.

The old model of a single computer or some selected group of computers serving all the organization's computational needs has been replaced by one in which a large number of separate but interconnected computers do the job. These systems are called computer networks. The integration of this network to form a specialized communication framework known as an exchange point is the subject of the work. Exchange points are physical network infrastructures where multiple networks can interconnect to exchange traffic (Mazzola *et al*., 2022)

With the advent of Internet of Things (IOT) today, there is need to design a network that support future expansion in a scalable, secure and reliable manner in our university campuses. Network

users expect access from any device within their campuses at any time. Designing a network that support the end user's expectation is not just simple task, because of nature of applications is changing, becoming more immersive and band width intensive.

Cisco has defined a hierarchical model known as the hierarchical internetworking model. This model simplifies the task of building a reliable, scalable, and less expensive hierarchical internetwork because rather than focusing on packet construction; it focuses on the three functional areas, or layers, of your network (Zhao *et al*., 2022).

According to Thomas (2002), the three layer of the hierarchical model that have paved the way for the proper organization and implementation of a computer network are:

1. **Core layer:** This layer is considered the backbone of the network and includes the high-end switches and high-speed cables such as fiber cables. This layer of the network does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed and ensures reliable delivery of packets
2. **Distribution layer:** This layer includes LAN-based routers and layer3 switches. This layer ensures that packets are properly routed between subnets and VLANs in your enterprise. This layer is also called the Workgroup layer
3. **Access layer:** This layer includes hubs and switches. This layer is also called the desktop layer because it focuses on connecting client nodes, such as workstations to the network. This layer ensures that packets are delivered to end user computers

2.1.2 Cloud Computing Overview

Historically, computing power was a scarce, costly tool. Today, with the emergence of cloud computing, it is plentiful and inexpensive, causing a profound paradigm shift, a transition from scarce computing scenario to abundant/ubiquitous computing. This computing revolution

accelerates the commoditization of products, services, and business models and disrupts the current Information and Communications Technology (ICT) Industry. The simplest example of cloud computing is an email account with a web-based e-mail service like Hotmail, Yahoo! Mail or Gmail. Here, instead of running an e-mail program on your computer, you log in to a web e-mail account remotely (Taleb & Mohamed, 2020)

Cloud Computing offers on-demand computing, storage, software, and other IT services with usage-based metered payment. Cloud Computing helps re-invent and transform technological partnerships to improve marketing, simplify and increase security, and increase stakeholder interest and consumer experience while reducing costs. With cloud computing, you don't have to over-provision resources to manage potential peak levels of business operation. With cloud computing, you can scale resources to meet your requirements; you can expand or shrink capability instantly as the business requirements evolve.

Cloud computing is unique in terms of four major characteristics. The first one is called on-demand service. When users need more computing resources such as CPU capability, storage capacity, or RAM, they will request for an increase and get what they want from the service provider if they can pay for it. Secondly, cloud computing platforms provide resource pooling which means that cloud services are offered in combination with various resources. The third characteristic of cloud computing platforms is known as rapid elasticity. From this point of view, clients would be able to enjoy dramatic change in services whenever it is needed to boost their current needs. This characteristic makes cloud computing a better option than traditional client-server mechanisms such that you pay for what you consume, and you can scale down when you have limited resources. The last one is measured service. Cloud computing applies metering capabilities such that cloud providers are able to measure how many services or

resources have been used by particular users or shared by multiple ones and they are billed accordingly (Syamsuddin *et al*., 2021).

In terms of the Cloud service model, there are three basic models that show how cloud computing can be integrated or deployed. This classification focuses on the user experience on the cloud platforms. The first service model is Software-as-a-Service (SaaS) where applications are hosted and run over the cloud, whenever users need them, they are able to access the application and work on them directly on the cloud without necessarily downloading them to their various computers. The second model of cloud computing is called Platform-as-a-Service (PaaS) where any client can use different cloud platforms to create any applications and at the same time host them on Cloud. The third service model is the Infrastructure-as-a-Service (IaaS) model which provides any kind of computing infrastructure to rent by users. Instead of having such expensive computing infrastructures which sometimes are not used all the time, cloud computing with the IaaS model offers an economic solution for clients to use extra hardware resources such as storage, networks, and computing resources as they need and simply release whenever they do not need (Syamsuddin *et al*., 2021; Tricomi *et al*., 2020)

Cloud computing is becoming an adoptable technology for many organizations including academic institutions like universities. With its dynamic scalability and usage of virtualized resources as a service through the Internet the use of cloud computing is giving institutions a great boost in their overall operations (Abdulle *et al*., 2022).

A hybrid, multi-cloud approach is one approach to cloud deployment that is presently used among most organizations, but there was a slight drift toward single public cloud usage from nine to eleven percent over the last year. Eighty-seven percent of respondents reported having a multi-cloud strategy, and 72 percent are taking a hybrid approach by combining the use of

both public and private clouds (Weins, 2020). It became obvious that the challenges around having strictly public cloud option have become a thing of concern for most companies.

Researchers in recent times have tried to provide hybrid cloud models that will combine the use of private and public cloud setups in an optimized manner, it still has not completely eliminated the direct usability issues developing economies have as regards power and internet connectivity associated with the use of public cloud platforms (Mehdi & Nachouki, 2020).

Private cloud platforms are increasingly become popular in recent times, largely because of security concerns around organizations' sensitive data hosted on public cloud platforms. Companies now prefer to have full control of their resources while still leveraging on the platform provided by public cloud companies to make their applications visible globally to their clients. This challenge has given rise to hybrid cloud deployment. The cost of setting up the cloud infrastructure and managing it has always been a big issue for organizations that seek to adopt a private cloud deployment model. An approach to cloud deployment that is modular in nature and will make the deployment of private cloud facilities seamless and progressive is a critical consideration moving forward. Each instance of the private cloud installation powered by alternative sources of energy like solar energy and can easily be replicated at a location. Educational institutions can leverage on private cloud installations to manage their result, and transcript issues.

Several theories underline the concept of network systems as it relates to routing within networks. Some of such concepts include IP addressing, IP routing and routing protocols. This section reviews some of these concepts.

2.1.3 Overview of IP Routing

IP routing is the process of moving packets from one network to another network using routers. The essence of IP Routing is to create communication between devices and network. It is also used to find updates of routes in the network (Telesis, 2016).

There are two terminologies used in IP routing. The two terminologies are: Routed Protocol and Routing Protocol

Routed Protocol is used to send packet from source to destination or from one network to another. Routed protocols are assigned to an interface and determine the method of packet delivery. Examples of Routed Protocol are Internet Protocol (IP) and Internet Protocol Exchange (IPX).

Routing Protocol is used to update and maintain the routing table of a router. The routing table of a router is like the memory of the router. It stores IP addresses of its neighbour router that is connected to it. A routing protocol determines the path of a packet through an internetwork. Examples of routing protocols are Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF).

2.1.4 Things Router Must Know

The router must know the following:

1. The Source Address: - This is where it receives the packet.
2. The Destination Address: - This is where the packet is sent.
3. All possible route to the remote (neighbour) router.
4. The best route to the remote router.
5. The routing information: - This is the packet itself.

2.1.5 Design Goals of Routing Protocols

Routing Protocols often have one or more of the following design goals:

a. Optimality
b. Simplicity and low overhead
c. Robustness and stability
d. Rapid convergence

a. Optimality

Optimality refers to the capability of the routing protocol to select the best route, which depends on the metrics. For example, routing protocol may use a number of hops and delays (Clausen & Jacquet, 2003).

b. Simplicity and Low Overhead

Routing protocols also are designed to be as simple as possible. In other words, the routing protocol must offer its functionality efficiently, with a minimum of software and utilization overhead (minimum CPU usage).

Efficiency is particularly important when the software implementing the routing protocol must run on a computer with limited physical resources.

c. Robustness and Stability

Routing protocols must be robust, which means that they should perform correctly in the face of unusual or unforeseen circumstances, such as hardware failures, high load conditions, and incorrect implementations. Because routers are located at network junction points, they can cause considerable problems when they fail. The best routing protocols are often those that

have withstood the test of time and that have proven stable under a variety of network conditions.

d. Rapid Convergence

In addition, routing protocols must converge rapidly. Convergence is the process of agreement, by all routers, on optimal routes. When a network event causes routes to either go down or become available, routers distribute routing update messages that permeate networks, stimulating recalculation of optimal routes and eventually causing all routers to agree on these routes. Routing protocols that converge slowly can cause routing loops.

2.1.6 Types of IP Routing

There are three types of IP Routing (Mudhoep *et al*., 2021)

1. **Static Routing: -** occurs when the network administrator manually adds IP routes or network address in the routing table of each router. It has a default administrative distance of one.

2. **Default Routing:** - is used when the destination address is not known. It is used in a stub network. A Stub Network is a network with a single exit path out of the network. Default Routing uses Wild Card Mask. To configure a default route, you use wildcards in the network address and mask locations of a static route (Carson & Macker, 1999). In fact, you can just think of a default route as a static route that uses wildcards instead of network and mask information.

3. **Dynamic Routing:** - is the process of finding networks and updating the routing table of a router using a Routing Protocols e.g. RIP, IGRP, EIGRP and OSPF. A routing protocol defines the set of rules used by a router when it communicates routing information between neighbor routers.

2.1.7 Administrative Distance in Routing

The administrative distance (AD) is used to rate the trustworthiness of routing information received on a router from a neighbor router. An administrative distance is an integer from 0 to 255, where 0 is the most trusted and 255 means no traffic will be passed via this route (Rocha *et al*., 2022).

If a router receives two updates listing the same remote network, the first thing the router checks is the AD. If one of the advertised routes has a lower AD than the other, then the route with the lowest AD will be placed in the routing table.

If both advertised routes to the same network have the same AD, then routing protocol metrics (such as hop count or bandwidth of the lines) will be used to find the best path to the remote network. The advertised route with the lowest metric will be placed in the routing table. But if both advertised routes have the same AD as well as the same metrics, then the routing protocol will load-balance to the remote network (which means that it sends packets down each link).

The Table 2.1 shows the default administrative distances that a Cisco router uses to decide which route to take to a remote network.

Table 2.1: Routing Protocol and their Default Administrative Distances

Route Source	**Default Administrative Distance**
Static Route	1
RIP version 1 and 2	120
IGRP	100
EIGRP	90
OSPF	110

IGRP and EIGRP use Autonomous System Number. RIP does not use Autonomous System Number.

Autonomous System Number is a collection of networks under an administrative domain sharing the same routing information. The Autonomous System Number ranges from 1 to 65,538

2.1.8 Classes of Routing Protocol

There are three classes of routing protocols:

a. **Distance Vector Protocol:** The distance-vector protocols find the best path to a remote network by judging distance. Each time a packet goes through a router, that's called a hop. The route with the least number of hops to the network is determined to be the best route. The vector indicates the direction to the remote network. Both RIP and IGRP are distance-vector routing protocols. They send the entire routing table to directly connected neighbors.
b. **Link Sate Protocol:** In link-state protocols, also called shortest-path-first protocols, the routers each create three separate tables. One of these tables keeps track of directly attached neighbors, one determines the topology of the entire internetwork, and one is used as the routing table. Link state routers know more about the internetwork than any distance-vector routing protocol. OSPF is an IP routing protocol that is completely link state. Link state protocols send updates containing the state of their own links to all other routers on the network.
c. **Hybrid Protocol:** Hybrid protocols use aspects of both distance vector and link state—for example, EIGRP.

There is no set way of configuring routing protocols for use with every business. This is something you really have to do on a case-by-case basis. If you understand how the different routing protocols work, you can make good, solid decisions that truly meet the individual needs of any business.

A. Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a distance-vector routing protocol. It sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine

the best way to a remote network, but it has a maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it's inefficient on large networks with slow WAN links or on networks with a large number of routers installed. RIP has two versions.

1. **RIP version 1** uses only classful routing, which means that all devices in the network must use the same subnet mask. This is because RIP version 1 doesn't send updates with subnet mask information in tow.
2. **RIP version 2** provides something called prefix routing, and does send subnet mask information with the route updates. This is also called classless routing.

B. Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced IGRP (EIGRP) is a classless, enhanced distance-vector protocol that gives us a real edge over another Cisco proprietary protocol, Interior Gateway Routing Protocol (IGRP). That's basically why it's called Enhanced IGRP. Like IGRP, EIGRP uses the concept of an autonomous system to describe the set of contiguous routers that run the same routing protocol and share routing information. But unlike IGRP, EIGRP includes the subnet mask in its route updates. And the advertisement of subnet information allows us to use VLSM and summarization when designing our networks. EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols. For example, EIGRP doesn't send link-state packets as OSPF does; instead, it sends traditional distance-vector updates containing information about networks plus the cost of reaching them from the perspective of the advertising router. And EIGRP has link-state characteristics as well. It synchronizes routing tables between neighbors at startup, and then sends specific updates only when topology changes occur. This makes EIGRP suitable for very large networks. EIGRP has a maximum hop count of 255.

There are a number of powerful features that make EIGRP a real standout from IGRP and other protocols. The main ones are listed here:

a. Support for IP, IPX, and AppleTalk via protocol-dependent modules
b. Considered classless (same as RIPv2 and OSPF)
c. Support for VLSM/CIDR
d. Support for summaries and no contiguous networks
e. Efficient neighbor discovery
f. Communication via Reliable Transport Protocol (RTP)
g. Best path selection via Diffusing Update Algorithm (DUAL)

C. Open Shortest Path First (OSPF)

First, a shortest path tree is constructed, and then the routing table is populated with the resulting best paths. OSPF converges quickly, although perhaps not as quickly as EIGRP, and it supports multiple, equal-cost routes to the same destination. But unlike EIGRP, it only supports IP routing

OSPF provides the following features:

a. Consists of areas and autonomous systems
b. Minimizes routing update traffic
c. Allows scalability
d. Supports VLSM/CIDR
e. Has unlimited hop count
f. Allows multi-vendor deployment (open standard)

OSPF is the first link-state routing protocol that most people are introduced to, so it's useful to see how it compares to more traditional distance-vector protocols such as RIPv2 and RIPv1. Table 2.2 gives a comparison of these three protocols.

Table 2.2: RIPv2, EIGRP and OSPF Comparison

Characteristic	**RIPv2**	**EIGRP**	**OSPF**
Type of protocol	Distance Vector	Hybrid	Link State
Classless support	Yes	Yes	Yes
VLSM support	Yes	Yes	Yes
Path metric	Hops	Hops and Bandwidth	Bandwidth
Hop count limit	15	255	None
Convergence	Slow	Fast	Fast
Hierarchical network	No	No	Yes (Using Areas)
Route computation	Bellman-ford	DUAL	SPF

OSPF has many features beyond the few we have listed in Table 2, and all of them contribute to a fast, scalable, and robust protocol that can be actively deployed in thousands of production networks.

OSPF is supposed to be designed in a hierarchical fashion, which basically means that you can separate the larger internetwork into smaller internetworks called areas. This is the best design for OSPF.

The reasons for creating OSPF in a hierarchical design include:

a. To decrease routing overhead

b. To speed up convergence

c. To confine network instability to single areas of the network

This does not make configuring OSPF easier, but more elaborate and difficult.

2.2 Theoretical Framework

2.2.1 Routing Theory

Routing is the process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes that data packets follow. Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

Several routing theories exist and have been used over the years. Path selection strategies are needed that allow the nodes to decide locally in a small amount of time along which edge to forward a packet. There are basically two approaches to that: oblivious routing and adaptive routing. In oblivious routing a system of optional paths is chosen in advance for every source-destination pair, and every packet for that pair must travel along one of these optional paths. Thus, the path a packet takes only depends on its source-destination pair (and maybe a random choice to select one of the options).

Two broad theories underly routing. They include Borodin-Hopcroft lower bound and Valiant's Trick

a. The Borodin-Hopcroft lower bound

   The nice property of the x − y routing strategy in the Borodin-Hopcroft lower bound is that it just must specify one path for each source-destination pair. Here, every node is the source of exactly one source-destination pair and the destination of exactly one source-destination pair and all demands are equal to 1. Thus, the routing problem can be described by a permutation $\pi : V \rightarrow V$ on the set of nodes V (Räcke, 2002; Yekkehkhany & Nagi, 2022).

b. Valiant's Trick

Let S be the best possible solution for the multicommodity flow problem underlying the definition of F , i.e. F = max{C(S), D(S)}. This works in a way that for every source-destination pair (s, t) we first branch off the demand from s to all other nodes in the system and afterwards reunite it at the destination t. Using S twice still gives an oblivious path system, but now we have many optional paths for a flow. In the case of actually sending packets, this boils down to the following strategy, which is a generalization of a well-known trick by Valiant (Abdeen *et al*., 2022; Räcke, 2002).

2.3 Empirical Framework

Several works have been going on to improve the performance of campus networks. A campus with an internal network is an example of a network domain that requires some level of connectivity to the outside world. Data exchange between campus or corporate domains is facilitated by some actions of a third-party cooperation; these cooperate domains offer, as a service, transmission and switching facilities for data exchange between their customers. Providers usually interconnect at Internet *exchange points* and can vary in the geographical scope of their operations from regional, to national and international.

Wireless local-area networks (WLANs) are increasingly common among organizations, particularly on university and corporate campuses. For example, a contemporary survey of 392 academic institutions found that nearly all plan to install a wireless network, about half already have a limited deployment, and a few (7%) have a “comprehensive” deployment. Although technology such as IEEE 802.11b is broadly deployed and usage is increasing dramatically, little is known about how these networks are used. A clear understanding of usage patterns in real WLANs is critical information for those who develop, deploy, and manage WLAN technology, and those who develop systems and application software for wireless networks (Saini *et al*., 2021).

Researchers have over the years have tried to provide design models for campus networks that are optimal using various techniques. What is most common for campus networks are flat designs that do not pay attention to design considerations but rather focus on the campus needs and usage capacity. The use of cloud-based networks due to its scalability has found some level of application in campus networks. Most campus now run a hybrid private cloud and public cloud networks to balance availability, costs, and management (Gopalakrishnan & Uma Maheswari, 2019).

Chi *et al* (2021) proposed a cloud network that focuses on the total cost of ownership. Their focus was to get organizations to shift their management effort to third parties which is the real concept behind cloud computing. The challenge with this model is that privacy of sensitive information is not guaranteed.

Aleem *et al* (2021), focused their research on integrating software as a service cloud solution. In this context, the solution does not factor in other models like infrastructure and platforms that are critical in cloud deployment models especially where it involves private ownership.

Gopalakrishnan & Uma (2019) compared the deployment of private cloud platforms comparing them with public cloud platforms. The approach places private at a disadvantage when the environmental factors are place side by side with the technology. Such factors include availability of power supply and security.

Shah et al., (2022) Clustering vehicles is a general solution to these challenges, as it allows warning alerts to be re-broadcast to nearby clusters by fewer vehicles. Hence, trustworthy cluster head (CH) selections are critical to decreasing the number of retransmissions. The author also achieved the transfer of reliable and secure warning messages through the shortest path, particularly on highways with high mobility Beevi & Alabdulatif (2022).

While speeding up the data delivery is also considered to be an effective approach to save energy, to achieve this objective, we propose a new energy efficient routing protocol using genetic fuzzy logic system. Our primary objective is to save energy by sending data packets via the shortest path.

Alghamdi (2020) examined the selection of optimal cluster head that makes the network prompt. Consequently, he develops a new clustering model with optimal cluster head selection by looking at four major criteria such as energy, distance, delay and security. For optimality he uses hybrid algorithm having the concepts of including dragon fly and fire fly algorithms. Lastly, he compares the performance with the conventional model in terms of number of alive nodes, network energy, delay and risk probability.

Mosavvar & Ghaffari (2019) demonstrates the cluster-based data aggregation in WSN using firefly algorithm. The authors focus is the data aggregation, towards the clustering protocol that is employed in the research. The sensor nodes are divided into several sensing areas using a clustering. Cluster head selection operation is carried out using a combination of the firefly algorithm and the low energy adaptive clustering hierarchy model. The cluster-based firefly algorithm computes fitness function using distance and residual energy.

El Alami & Najid (2015) talks on how to achieve efficiency and to extend the network lifetime through fuzzy C-mean clustering for a multihop routing. In their work the entire network is divided into sub cluster each cluster has a head node. The intra routing is established by the member nodes which communicates its head directly and the head node establishing the inter cluster communication. It was an improvement of low energy adaptive clustering hierarchy protocol.

Akila *et al.,* (2017) highlighted energy efficient clustering techniques to enhance the lifetime of wireless sensor networks. The author proposes fuzzy logic-based cluster head selection, sleep duty cycle of sensor node and hierarchical clustering.

To achieve efficient bandwidth utilization and minimize message delivery time the author introduced an event-driven cluster-based method (Benkerdagh & Duvallet, 2019). Furthermore, clustering after event finding produces an end-to-end delay, which is inconvenient for time-crucial information in bi-directional road traffic. The authors (Shah *et al*., 2019) suggested a clustering strategy called time barrier-based emergency message dissemination in the vehicular ad-hoc network (TBEM) that relies on the time barrier technique and aims to reduce excessive message dissemination. If an event occurs during work, the farthest vehicle is a relay to cover a greater distance. As there are multiple vehicles along the same length of road, numerous vehicles can send the same message, causing network congestion. Furthermore, vehicles are permitted to transmit messages after the time limit expires, resulting in redundancy and affecting network performance.

The k-medoids (Xu & Wunsch, 2005) and k-means (Ben Hamida & Javed, 2016) algorithms add to the clustering diversity but have similar tendencies. However, a k-medoids algorithm performs better in some cases. The two algorithms divide the entire sample space into groups of comparable nodes depending on the shortest distance among nodes and a central node, CH. In a k-medoids algorithm, the cluster's center is always a node, but in a k-means algorithm, it may or may not be. As the mobility of nodes in VANET is high, choosing a geographical place other than the node as the cluster center can induce clustering instability. Furthermore, any approximation made in this direction by choosing the closest node to a central place will reduce accuracy and increase processing overhead. Moreover, compared to a k-means algorithm, a k-medoids algorithm is much more tolerating of outliers.

Ullah *et al* (2021) presented a clustering technique in which a gateway node is introduced as a relay node between CHs. The gateway node provides the connection between two cluster heads to increase information range without needing roadside units. This scheme is best for uni-directional traffic, and suitable for urban VANETs and unsuitable for highway environments. EEMDS also ignores the node's direction, degrading the scheme's performance.

Shah *et al* (2022) presented a network that was hierarchically partitioned into numerous clusters on a roundabout in an urban scenario, each associated with the CH. Only the CH was accountable for the retransmission of WMs in every cluster to avoid redundant transmission and ensure reliable WM dissemination. Furthermore, the author employed a k-medoids algorithm for CH selection and Hamming distance for finding a node's movement direction to maximize the cluster's lifetime, and it has been proven to operate well in a roundabout in urban settings. BURP does not apply to highways environment where mobility is very high. This paper proposes OPRP as an extension of Shah *et al* (2022) work to highway environments.

Chakroun *et al* (2022) described message dissemination using SND. However, SDN separates the data and control plane, and the controller should interact with the underlying network to have a global view of the status of the data plane. Hence, when there are dynamic changes in the network, there should be a frequent status update in the SDN controller.

Priyambodo *et al* (2021) analyses the performance optimization of MANET networks through routing protocol, where they state that Mobile Ad Hoc Network (MANET) protocol requires proper settings to perform data transmission optimally, and to overcome the problem that it was important to select the correct routing protocol and use the routing protocol's default parameter values. They examined the effect of route request parameters, such as RREQ_RETRIES and MAX_RREQ_TIMOUT, on the Ad Hoc On-demand Distance Vector (AODV) protocol, which was compared with the default AODV performance Optimized Link

State Routing (OLSR) protocols. The performance metrics used for measuring performance were Packet Delivery Ratio (PDR), throughput, delay, packet loss, energy consumption, and routing overhead. The results show that the OLSR protocol has a smaller delay than the AODV protocol, while in other measurements, the AODV protocol is better than OLSR. They pointed out that security was the challenge and needed to be addressed before deploying a MANET.

Singla et al., (2022) identified that the biosensors used to estimate physiological parameters have limited power due to its small size and hence smaller form factor. For the durability of the network, it is imperative to transmit the data in an energy-efficient manner. He further notes that it necessitates the development of effective, lightweight and secure routing protocols that provides security with minimal use of resources. The major challenge here was to use different modes of AES to meet different security requirements in the wake of limited power capacity of biosensors.

Kim et al., (2023) analyses FANET routing protocol for multi-UAV-based reconnaissance mobility models, he notes that FANET possesses characteristics such as density, mobility, and speed of flight nodes, that affects its performance. They went ahead to analyse the representative FANET protocols, AODV, DSDV, and OLSR, according to mobility models, SRWP, MP, RDPZ, EGM, and DPR, under the multi-UAV-based reconnaissance scenario. They calculated them in terms of the number of nodes, network connectivity, mobility model's reconnaissance rate, speed of nodes, and ground control station (GCS) location. They then found out that AODV showed the highest PDR performance (81%) with SRWP in multiple UAV-based reconnaissance scenarios. They observed how the number of nodes increases, the connectivity of the network increases, but the limitation was that the performance of the routing protocol decreased.

Tan *et al* (2020) analysed the performance of routing protocols for UAV communication networks. He stressed the challenges associated with designing a routing protocol that can provide efficient and reliable node to node packet transmission. They focused on developing a more realistic simulation environment based on OPNET 14.5, and performs performance tests and comparisons on four classic routing protocols: Ad Hoc on demand distance vector (AODV), dynamic source routing (DSR), optimized link state routing (OLSR), and geographic routing protocol (GRP). Their challenges were that when the source node S is using a route to the destination node D, the source node S can use the route maintenance mechanism to detect the following problems: if the network topology of the whole network has changed, then the source node S cannot continue to use the route to send service messages, because the route information has expired.

Himawan *et al* (2022) analysed the performance of communication model on position-based routing protocol. They pointed out the four categories in the Vanet system topology, which are; position-based routing protocols, broadcast-based routing protocols, cluster-based routing protocols and geocast/multicast routing protocols, and noted that the possessed fundamental differences, especially in the concept of sending data and information between nodes. For that reason, their study focused on the selection of standardization and integration of data delivery between nodes. The main limitation they encountered was the ability to send data properly in busy and fast traffic conditions.

Ganie (2021) carried out a study on private network optimization. The author noted that optimization was required as the number of devices connected to this network was more. Two parameters that were optimized are 1. Bandwidth, and 2. Cost. Cost optimization was achieved by shifting some small networks like school or medium-size office to broadband. While bandwidth optimization was achieved by global load balancing, minimize latency, packet loss

monitoring and bandwidth management. He also observed that OPNET shows better accuracy and precision than other simulations tools. OPNET provides a comprehensive development environment for the specification, simulation and performance analysis of communication networks.

Thilagam & Aruna (2021) studied the Intrusion detection for network based cloud computing by custom RC-NN and optimization. Their work was aimed at optimizing custom RC-NN-IDS model thus achieved an improved classification accuracy of 94% and also a decreased error rate of 0.0012. However, this tempts to various issues where security issues like integrity, availability and confidentiality, cyber attackers and intruders are considered as a major one.

Xu *et al*. (2020) researched on routing optimization for cloud services in SDN-based Internet of Things with TCAM capacity constraint. They addressed the routing optimization problem in SDN-based IoT with TCAM capacity constraint. They formulated the problem as a mixed integer linear programming problem and prove the problem is NP-hard. Then to solve the problem efficiently, they propose several approximate algorithms, which solve the problem in two stages. In the first stage, the algorithms calculate the routing strategies for flows without considering the TCAM capacity constraint. To meet the TCAM capacity constraint, the algorithms using different strategies to adjust the paths of some flows in the second stage. Extensive simulations are conducted on both real ISP and synthetic topologies to evaluate the performance of the algorithms. The simulation results verify that the algorithms can achieve promising load balancing performance in SDN-based IoT, where the capacity of TCAM in SDN switches is very limited. However, due to the limitations of traditional network architecture, the existing RO schemes suffer from many problems, such as low flexibility, low scalability, low performance, and high operational cost.

Manzoor *et al.* (2020) carried out a performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols. Their research article focuses on the performance and redistribution of different routing protocols in medium or enterprise IP networks. A simulated network model is established in GNS3 simulator. Five Cisco-7200 series routers and a switch is used in this simulated topology. All these routers are directly connected with each other via serial links. Routing protocols EIGRP, OSPF and BGP are used in this topology and then configured route redistribution on these routers. Their findings revealed that EIGRP is better in convergence and through put whereas OSPF is better in packet delay. The constraint is that with an increasing node scale, the cost of obtaining network state information will increase rapidly, and the network convergence will be slow.

One method used to maintain communication is by implementing a protocol redundancy system. One or more routers will act as the primary router for load balancing, and some routers are in standby mode if one main router is down. First hop redundancy protocols (FHRP) is a protocol that implements redundancy and load balancing systems. This protocol can transfer access data traffic if one of the routers on the network is down. FHRP is divided into virtual router redundancy protocol (VRRP) and gateway load balancing Protocol (GLBP). This research analyzes the design and implementation to provide information about the quality of VRRP and GLBP services on the main router and the backup router, by using an application graphical network simulator (GNS) simulation 3. In the GNS3 application, a LAN network topology is designed with eight router devices in the form of a ring topology using RIPv2 and OSPF routing protocols, then implemented in protocols VRRP and GLBP. The analysis results show that GLBP can back up the network faster than VRRP (Syahputra et al., 2020). The focus of this research is basically on load balancing and redundancy and not just on the best routing protocol suitable for interconnection.

2.4 Summary of Literature Review

The detailed literature review and comparison of various studies enabled the present study to reach at the point to conclude that one of the most important factors of all networks today is network optimization. As network engineers strive to optimize the routers to implement managerial part and optimize the overall system, the importance of the routing heuristics and optimal routine in a volume-based and random storage environment is analysed in detail and it has been concluded that routing protocols should be enhanced to have a better and more responsive network.

Table 2.3: Summary of Literature Review

S/N	Authors/s	Research Topic	Finding	Limitation
1	Gopalakrishnan & Uma Maheswari (2019)	Research on enterprise public and private cloud service	Implementation of hybrid private cloud and public cloud networks to balance availability, costs and management	Identifying the security requirements which is very difficult to assess
2	Chi *et al.* (2021)	Total cost ownership optimization of private clouds: a rack minimization perspective	Proposed a cloud network that focuses on the total cost of ownership	Arbitrary deployment of servers introduces risk by overloading power as each server consume certain energy and there is a power limitation on the rack.
3	Aleem *et al.* (2021)	Focused their research on integrating software as a service cloud solution.	Focused their research on integrating software as a service cloud solution.	Architectural complexity
4	Gopalakrishnan & Uma Maheswari, (2019)	Research on enterprise public and private cloud service	Compared the deployment of private cloud platforms comparing them with public cloud platforms.	Integration and migration challenges in public cloud.
5	Shah, *et al.* (2022)	Optimal Path Routing Protocol for Warning Messages	The transfer of reliable and secure warning messages through the shortest	Traffic fatalities

		Dissemination for Highway VANET	path, particularly on highways with high mobility.	
6	Alabdulatif (2022)	Optimal Routing Protocol for Wireless Sensor Network Using Genetic Fuzzy Logic System	Save energy by sending data packets via the shortest path	Extending the life of the network in WSN is a challenging issue because energy in sensor nodes are quickly drained.
7	Alghamdi (2020)	Energy efficient protocol in wireless sensor network: Optimized cluster selection model	He uses hybrid algorithm for optimality, having the concepts of including dragon fly and fire fly algorithms	Energy and security.
8	Mosavvar & Ghaffari (2019)	Data aggregation in wireless sensor networks using firefly algorithm	Demonstrates the cluster-based data aggregation in WSN using firefly algorithm.	High energy consumption.
9	(El Alami & Najid, 2015)	SEFP: A new routing approach using fuzzy logic for clustered heterogeneous wireless sensor network	Improvement of low energy adaptive clustering hierarchy protocol	Energy conservation issues.
10	Akila *et al.* (2017)	Modern clustering techniques in wireless security networks for wireless sensor networks insights and innovation	Fuzzy logic-based cluster head selection, sleep duty cycle of sensor node, hierarchical clustering	Limitations of LEACH (low energy adaptive clustering hierarchy)
11	(Benkerdagh & Duvallet, 2019)	Cluster-based emergency message dissemination strategy for VANET using V2V communication	Effective bandwidth utilization and minimal message delivery time	Transmission of messages after the time limit expires, resulting in redundancy
12	Xu & Wunsch (2005)	Survey of clustering algorithms	Added the k-medoids and k-means algorithms to the clustering diversity	Inducement of clustering instability
13	Ullah *et al.* (2021)	EEMDS: An effective emergency message dissemination scheme for urban VANETs	Clustering technique in which a gateway node is introduced as a relay node between CHs	Unsuitable for external environment.
14	Shah *et al.* (2022)	A Robust Emergency Messages Routing Scheme for Urban VANETs	OPRP as an extension for highway environments.	BURP not suitable for external use.
15	Chakroun *et al.* (2022)	LAMD: Location-based Alert Message Dissemination scheme for	Frequent status update in the SDN controller whenever a dynamic	Time-limited connectivity losses

		emerging infrastructure based vehicular networks	change occurs in the network.	
16	Priyambodo *et al.* (2021)	Performance optimization of MANET networks through routing protocol analysis	The results of their analysis showed that the OLSR protocol has a smaller delay than the AODV protocol, while in other measurements, the AODV protocol is better than OLSR.	Security was the challenge and needed to be addressed before deploying a MANET.
17	Singla *et al.* (2022)	Challenges and Developments in Secure Routing Protocols for Healthcare in WBAN: A Comparative Analysis	Development of effective, lightweight and secure routing protocols that provides security with minimal use of resources. AES routing.	The major challenge here was to use different modes of AES to meet different security requirements in the wake of limited power capacity of biosensors.
18	Kim *et al.* (2023)	FANET Routing Protocol Analysis for Multi-UAV-Based Reconnaissance Mobility Models	That AODV showed the highest PDR performance (81%) with SRWP in multiple UAV-based reconnaissance scenarios.	Decrease in performance of the routing protocol when the number of nodes increases.
19	Tan *et al.* (2020)	Performance Analysis of Routing Protocols for UAV Communication Networks	Their simulation results show that the routing protocol of OLSR has lower network delay and higher throughput, the routing protocol of DSR has higher traffic received and the routing protocol of AODV has lower data dropped.	Expiry of route information when the network topology of the whole network has changed, as a result the source node S cannot continue to use the route to send service messages.
20	Himawan *et al.* (2022)	Performance Analysis of Communication Model on Position Based Routing Protocol: Review Analysis	The simulation results show that the packet distribution ratio is improved by more than 10 percent for	The limitation was the ability to send data properly in busy and fast traffic conditions.

			speeds of up to 70 km / hr relative to the VANET routing protocol based on ant colony optimization (VACO) that also uses an ant-based algorithm.	
21	Ganie (2021)	Private network optimization	That OPNET shows better accuracy and precision than other simulations tools. OPNET provides a comprehensive development environment for the specification, simulation and performance analysis of communication networks	The specific issue with this protocol is the complexity and high CPU usage.
22	Thilagam & Aruna (2021)	Intrusion detection for network based cloud computing by custom RC-NN and optimization	They optimized custom RC-NN-IDS model thus achieved an improved classification accuracy of 94% and also a decreased error rate of 0.0012.	The issues where security issues like integrity, availability and confidentiality, cyber attackers and intruders are considered as a major one.
23	Xu *et al.* (2020)	Routing optimization for cloud services in SDN-based Internet of Things with TCAM capacity constraint	Addressed the routing optimization problem in SDN-based IoT with TCAM capacity constraint. Formulated the problem as a mixed integer linear programming problem and prove the problem is NP-hard.	The limitations here were low flexibility, low scalability, low performance, and high operational Cost.
24	Manzoor *et al.* (2020)	Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols	EIGRP is better in convergence and through put whereas OSPF is better in packet delay.	With an increasing node scale, the cost of obtaining network state information will increase rapidly, and the network

				convergence will be slow.
25	Nurwarsito & Sindunata (2020)	Optimization of hello interval in OSPF routing protocol performance on mesh network topology	The results of this research indicate that the change of the hello interval value can affect the convergence time and selection of designated routing (DR) and backup designated routing (BDR) in the OSPF routing protocol.	Longer time for updating the routing table in the OSPF routing protocol.

2.5 Research Gap

From works reviewed, companies or organizations like educational institutions simply configure their network without the need for optimization using routing protocol as an option.

Most campus networks do not pay attention to the choice of routing protocol and researchers have not clearly paid attention to inter-campus cloud networks.

Most institutions have separate networks and operate separately but connect to the internet and public cloud.

This work will model an inter-campus cloud network and determine the best routing protocol that provides the best convergence time.

CHAPTER THREE

METHODOLOGY

3.1 Choice of Methodology

In this chapter, we will consider the guidelines for building Inter – Campus Cloud Network System (ICCNS). The ICCNS will be analyzed using Prototyping Methodology.

3.2 Prototyping Steps for the ICCNS

The prototyping steps used in prototyping the ICCNS System are stated below:

1. Evaluation of the old system: here the existing system is evaluated and noted.
2. Initial setup requirements: here the settings of the initial requirements are done.
3. Design: here the design of the system is developed and implemented.
4. Prototyping: here the prototype is modified based on the comments supplied by the users.
5. Simulation: here the system is simulated as specified using the various routing protocols.
6. Review and update: here the simulated system is reviewed and updated for any additional input.
7. System development: here the system is developed based on the prototype which represents the final product as desired.
8. System testing: here the developed system is tested for compliance and consistency in accordance with the specified values.

9. System maintenance: This is the final step after system testing. It step is designed for the routine maintenance of the system incase of failure.

Figure 3.1 shows the steps to be adopted in the design process for the ICCNS.

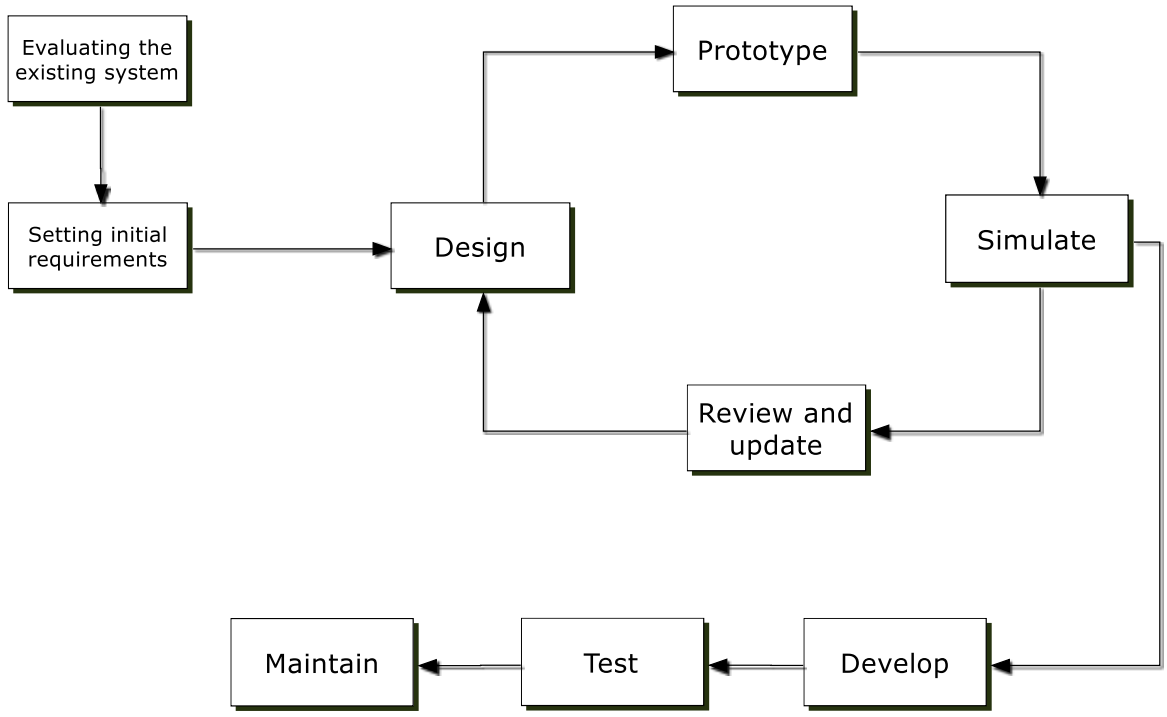

Figure 3.1: Prototyping Steps for the ICCNS

3.3 Study of the Existing System to Determine Initial Requirements

The ICCNS has not been in existence within Nigeria before now. Each campus runs their separate networks with their dedicated links.

Before the design of the proposed system, the basic problems and weaknesses confronting the present system were identified and defined in other to get the needed requirements of the proposed input/output specifications in line with what the proposed system would achieve.

Some of these challenges faced by the existing system of campus connection to the internet can be summarized as followings:

1. Low finance available for monthly subscription
2. Limited bandwidth available for users
3. Challenges of network failure
4. Lack of adequate skilled manpower
5. Management issues
6. Poor maintenance culture

The method used in data collection during the course of finding the feasibility of the new system design includes;

3.4 Campuses Under Consideration

The following campuses are considered for the research work. These institutions are government owned and are faced with the problems listed above. The institutions also cut across the major category of tertiary institutions available in Nigeria; college of education, polytechnic and the university. These institutions are also managed by the federal government or state government.

The institutions include:

1. Federal University of Technology Owerri (FUTO)
2. Federal Polytechnic, Nekede (FEDPOLY)
3. University of Agriculture and Environmental Sciences (UAES) Umuagwo
4. Alvan Ikoku Federal College of Education (AIFCE)
5. Imo State University (IMSU)

A visit to these institutions was carried out and the following section present the finding.

3.5 Evaluation of Exiting Network of the 5 Campuses

A visit the 5 campus was carried, and oral interview was used to come up with a summary presented in table 3.1

The following are the question the IT heads were asked:

1. What is the network topology of your Campus LAN/WAN?
2. What is the carrying capacity of the network?
3. What bandwidth capacity are you subscribed to?
4. Who is your service provider/s?
5. What are the challenges faced by your network?
6. What backup network do you maintain in an event of failure?
7. What equipment vendor do you subscribe to?
8. What media type is being used by your institution?
9. What network architecture is being used?

This gave us an insight into how they carry out operations with their current system, which led to the identification of problems listed above, and the zeal in finding lasting solutions to the identified problems.

The oral interview with the IT department of each institution will enable us model their existing campus network and also propose a better design for the campus where necessary.

The following headings will be used to capture data from each campus under investigation.

1. Presence of visible data network
2. Functional subscription
3. Presence of backup/s link/s
4. Bandwidth subscription
5. Network availability to students/staff

6. Network management
7. Network media type
8. Traffic volume possible
9. Equipment vendor
10. Link provider
11. Availability of skilled personnel
12. Network type
13. Network topology
14. Edge equipment
15. Network provider
16. Network architecture

Table 3.1: Summary of Network Description of the 5 Campuses

Measurement metric	**SCHOOL**				
	FUTO	**UAES**	**FEDPOLY**	**IMSU**	**AIFCE**
Presence of visible data network	Yes	Yes	Yes	Yes	Yes
Functional subscription	Yes	Yes	Yes	Yes	Yes
Backup link	Yes	No	Yes	No	No
Bandwidth subscription	300Mbps Dedicated	Not disclosed	Not disclosed	Not disclosed	600Mbps Dedicated
Available to student	Partially	Partially	Partially	Partially	Partially
Management	Contracted	Internal	Contracted	Internal	Internal
Media type	Twisted pair/fibre	Twisted pair/fibre	Twisted pair/fibre	Twisted pair/fiber	Fiber
Traffic volume possible	Not defined	Not defined	Not defined	Not defined	Not defined
Equipment vendor	Cisco/Dlink	Cisco/TPlink/ Mikrotic	Cisco	Cisco/TPlink	Mikrotic
Link provider	MTN	Not disclosed	MTN	MTN	MTN
Availability of skilled personnel	Not adequate	Not adequate	Not adequate	Not adequate	Not adequate

Network type		LAN/WAN			LAN/WAN
Network topology	Nil	Nil	Nil	Point-to-point	Hybrid star/point-point
Edge equipment	Cisco Router	Regular Router	Cisco switch	Mikrotic router	Airtel microwave
Network provider	Tenese	Not disclosed	Not disclosed	Not disclosed	Not disclosed
Network architecture	Fibre backbone	3-layer	3-layer	None	None

The major challenge these campuses are facing and that this work seeks to proffer solution to can be categorized into two headings:

1. Network availability
2. Adequate bandwidth for network users.

It is evident that the money to both maintain the networks, pay for subscription and upgrade these networks come from the same source and that is the government. The need to coordinate these limited funds is critical and as such a direct look at how these monies are being spent over time is necessary. Furthermore, school are not always in session at the same time and as such there is the fluctuation in available users to make use of internet subscriptions already paid for. School can connect to an exchange point and make available its network to other school in an event of break down or high traffic demand.

Some of the findings as described in table 3.1 can be further broken down into the following points:

1. Most of the campus administrators are not fully aware of the kind of network they run as these networks where setup by third party organization. When such occurs, there is the challenge of maintenance especially where there is limited skilled manpower

2. Campuses generally have varied network need over time. At some time, there is high traffic while at other times there is low traffic. Not paying attention to this and not being able to control these fluctuation means paying for an access that will not be fully utilized. Hence the need to make such resource available to other institutions that may need it at a particular point in time.

3.6 Component of Inter – Campus Cloud Network System (ICNS) and Devices

The broad category of the component of Inter – Campus Network System includes:

1. Sender/Receiver: These are Network Devices like PCs, Switches and Routers. The sender and receiver are basically the end devices within the network.
2. Medium: These are Network Links such as Fast Ethernet Links and Serial Links. A combination of these links are usually ideal for the network
3. Protocol: These are Routed Protocols e.g. IP and Routing Protocols e.g. RIP version 2, EIGRP and OSPF. They provide the rules for communication within the network system.
4. Message: These are the Protocol Data Units (PDU) such as Packet.

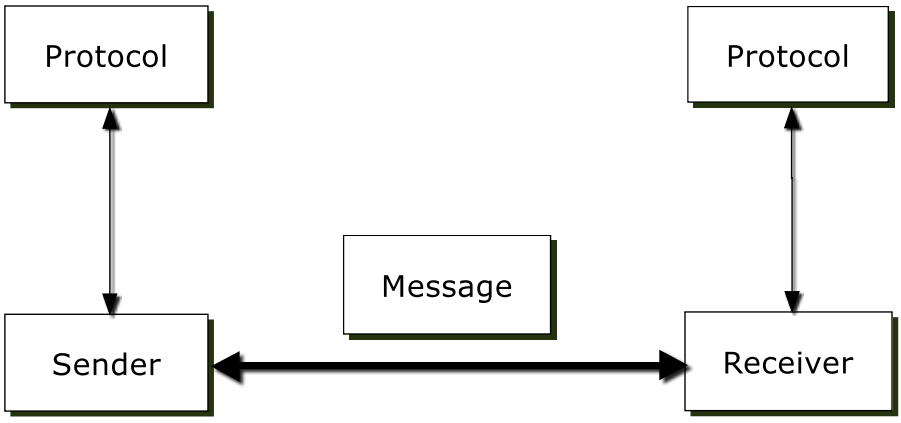

Figure 3.2 Component of the ICCNS

The ICCNS integrates certain components that are critical for its effective operation. Two basic components stand out in the network design; the network router and the network switch.

1. Network Router: A router is a networking device operating at layer 7 of the OSI model that forwards data packets between computer networks. Routers perform the traffic forwarding functions on the Internet. A data packet is typically forwarded from one router to another router using the routing table until packets reaches its destination node. A router is connected to two or more data lines from different networks using serial, fibre of twisted pair cables. When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

Figure 3.3: The Diagram of a Network Router

2. Network Switch: A network switch is a computer networking device that operates at layer 2 of the OSI model and connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device. A network switch is a multiport network bridge that uses hardware addresses also known as MAC address to process and forward data at the data link layer (layer 2) of the OSI model. Some switches

can also process data at the network layer (layer 3) by additionally incorporating routing functionality that most commonly uses IP addresses to perform packet forwarding; such switches are commonly known as layer-3 switches or multilayer switches.

Figure 3.4: Diagram of a Network Switch.

3.7 Simulation Tool and Protocols Under Consideration

The performance of the inter campus network system is simulated on a network simulator; packet tracer software. Packet tracer is a network simulation software that is used basically for testing network before they are fully deployed. The following are the reason for the choice of choosing packet tracer as a simulator:

1. Presents users with multiple functionalities especially in routing and switching. The multiuser functionality in Packet Tracer enables multiple networks on different computers to interact.
2. It provides a platform where network parameters can be monitored and modified during the design phase
3. Packet tracer is a free open-source simulator available for researchers
4. Packet tracer provides flexibility in configuration.

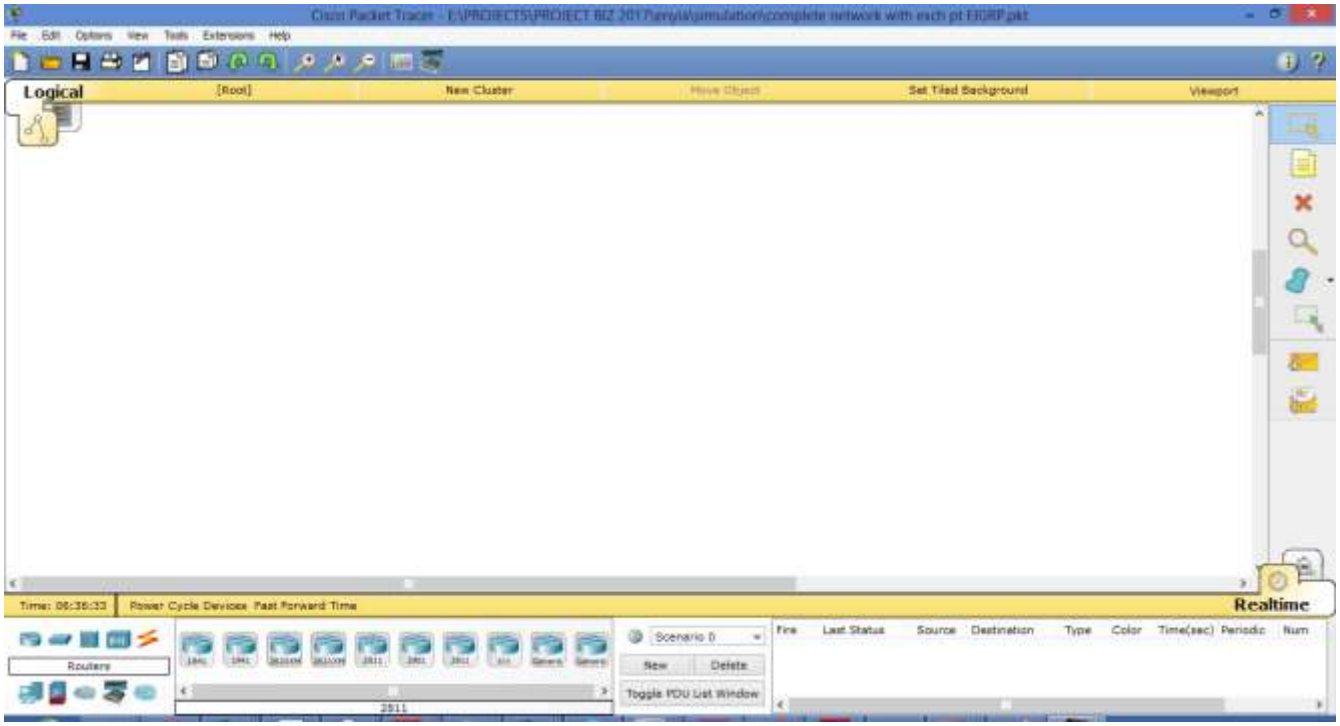

Figure 3.5: Packet Tracer Simulation Environment

3.8 PDV Calculation of Existing Networks and Improvement Options

The Calculation for the Packet Delay Value for each campus network design are shown in table 3.2-3.6. The PDV value must be less than 512Bit times for the network to be optimal. The PDV value is the delay value of the longest segment on the network. This approach is adopted to ascertain from the on-set how reliable available networks are and provide a clear guide for network design to make for maximum efficiency. Recommendations are also made from this analysis for each campus to optimize their individual network performance

Table 3.2 AIFCE Campus (Between the NOC and the Faculty of English)

Device	**Qty**	**Delay Value (BT)**	**Round Trip Delay Calculation**	**Maximum Round Trip Delay (BT)**
TX and FX DTE	10	100	Not Available	100
Class II repeater	2	92	92 x 2	184
Router	1	-		-
UTP Cat 5 Cable		1.112	1.112 x 220m	244.64
Safety Margin				5
Total				**533.64**

From the PDV calculation shown in Table 3.2, it is clearly observed that the longest part has a delay value of 533.64bt which is above the allowable 512bt for optimality.

The following steps can be adopted to optimize the network efficiency:

1. The use of cat 6 cable or fiber cable
2. Reduction in the number of intermediate devices between the longest segment

Table 3.3 IMSU Campus (Between NOC and the Administrative Building)

Device	**Qty**	**Delay value (BT)**	**Round Trip Delay calculation**	**Maximum Round Trip Delay (BT)**
TX and FX DTE	10	100	Not Available	100
Class II repeater	2	92	92 x 2	184
Router	1	-		-
UTP Cat 5 Cable		1.112	1.112 x 350m	389.2
Safety Margin				5
Total				**678.2**

From the PDV calculation in Table 3.3, the maximum allowable delay value was exceeded and as such there is a need to alter some of the network parameters. Some of the options available to the network admin to optimize their network include the following:

1. Adoption cables that have less delay values like fibre or cat6.
2. The reduction in the number of intermediate devices within the longest segment.

Table 3.4: Federal Polytechnic Nekede Campus (Between NOC and the School of Management Building)

Device	**Quantity**	**Round Trip Delay**	**Maximum Round Trip Delay**
TX and FX DTE	10	Not Available	100
Switch	2		92
Router	1		-
UTP Cat 5 Cable		1.112 x 180m	200.16
Safety Margin			**392.16**

The delay value for the Federal Polytechnic Nekede is within the allowable limit and as such no further modification on their network is needed. Some points are worthy of note to help make the Polytechnic network better. They include:

1. Demarcation of the entire campus network into a 3-layer model to help for proper management
2. Integration of more distribution points to cover the entire campus environment
3. Upgrade of the available bandwidth of the campus network

Table 3.5 FUTO Campus (Between FUTO NOC and the Senate Building)

Device	**Quantity**	**Round Trip Delay**	**Maximum Round Trip Delay**
TX and FX DTE	11	Not Available	100
Switch	2	92	184
Router	1		
UTP Cat 5 Cable		1.112 x 150m	166.8
Safety Margin			**450.8**

The delay value within the FUTO campus network is within the allowable value since it is less than the maximum delay of 512bt. No modification is required but the following points should be noted for FUTO network:

1. The network should be properly segmented to cover the entire campus
2. A clear network model should be adopted as there is no clear use of the 3-layer model as pointed out.
3. The network core layer should be properly designed to have a clear link backup mechanism
4. The end devices should be upgraded to meet the population strength of the campus

Table 3.6: UAES Campus (Between NOC and the Administrative Building)

Device	**Quantity**	**Round Trip Delay**	**Maximum Round Trip Delay**
TX and FX DTE	10	Not Available	100
Switch	1		92
R-uter	1		
UTP Cat 5 Cable		1.112 x 86m	95.632
Safety Margin			5
			287.632

From the delay values calculated for Imo Polytechnic network, it is clear that the value is within the allowable limit.

From the PDV values calculated in Tables 3.2-3.6, it can clearly be deduced that a design with these values can be carried out as the values are all below the allowable value of 512bt. However, the following points should be noted as major issues to be done on this campus network:

1. improving the available bandwidth as what is currently being subscribed to cannot meet the needs of the users within the campus
2. optimizing various access points as the equipment currently being used do not have the capacity to carry the traffic within the environment.
3. Engaging more skilled manpower to manage the network.

3.9 Cost Analysis for an Exchange Point

To setup an exchange point, some basic components are required. Table 3.7 shows an estimation of the initial cost of setting up an exchange point connecting 5 campuses via a wireless link.

Table 3.7: Cost Estimation for Setting up an Exchange Point For 5 Campuses in Imo State

Item	**Unit**	**Cost (N)**	**Unit total (N)**	**Remark**
Mikrotik Radios	10	350,000	3,500,000	A pair for each campus link to the IXP NOC
Cisco/Mikrotic switches	5	120,000	600,000	High end cisco/mkrotic 24 port network switch
Servers 5	2	750,00	1,500,000	For link management
Cabling	-	200,000	200,000	
Routers	6	350,000	2,100,000	High end cisco 2900 routers
Panels	3	175,000	525,000	For component management
Fiber Cabling	-	-	1,500,000	Fiber cables at the campus ends
Cat 6 Cabling	-	-	75,000	Cat 6 cable for the campus end
Total			**8,500,000**	

Some campuses spend as high as 10 million per year on internet subscription, so invest such amount of money on an exchange point is not out of place especially where the institutions exchanging traffic have a lot to gain synergizing. Most of the exiting equipment within the campuses will be used for the integration to minimize cost and avoid replication of equipment.

In general, we can deduce the following from the field investigation of each campus which serves as a guide to modeling an ICNS for the institutions in Imo state. This model can be replicated anywhere in the country and same results achieved. The following are the observation in summary:

1. The link capacity provided by most campuses are not enough to meet the data need of its population
2. Links go down from time to time due to and equipment damage due to thunder and light surge.
3. With varied equipment vendor there is the need to make a proper choice of routing protocol as some are proprietary to some vendors
4. There is an obvious disregard for network topology which has a direct impact on link efficiency.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Network Block Diagram

The ICCNS is made up of two basic modules, the exchange point and the campus unit. The exchange point serves as a connection point for all the campuses subscribed to the exchange point service. For this pilot design, the five campuses in Imo state eastern Nigeria is uses (FUTO, IMSU, FEDPOLY, UAES and AIFCE)

Figure 4.1 is a block diagram showing how the campuses are connected. Each campus network is connected directly to the exchange point

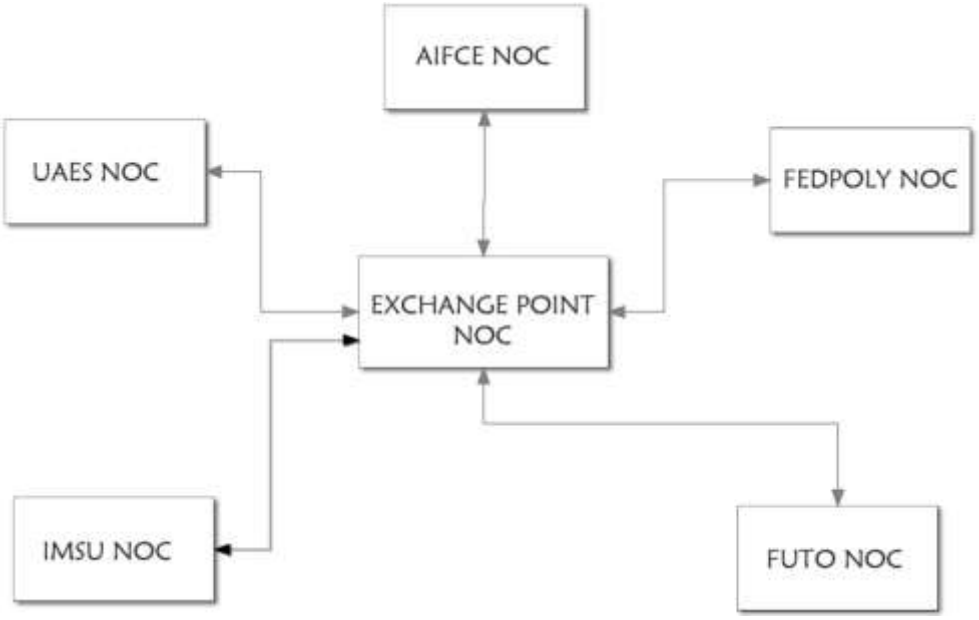

Figure 4.1: Block Diagram of the ICCNS Point Network

Figure 4.1 shows that the exchange point exchanges traffic between each campus NOC (network operations center) and allow for these campuses to also exchange traffic between each other via the exchange point NOC.

4.2 The Design Flow Chat

The flow chat describes how the network was designed and simulated on the simulated environment. This process is to be replicated for the following protocols to be tested: RIP, OSPF and EIGRP.

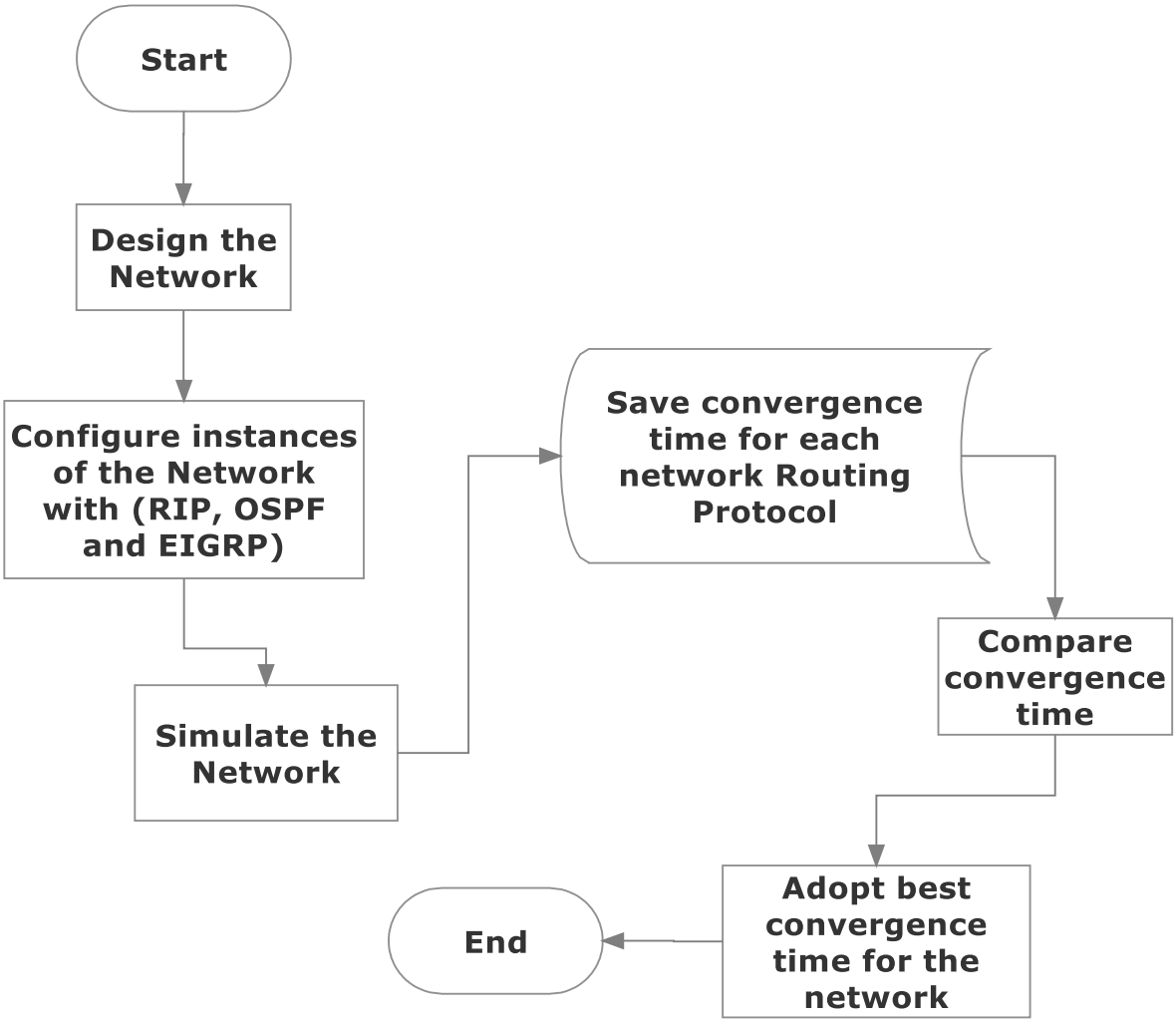

Figure 4.2: Flow Chat of the Design Process.

From Figure 4.2, the first thing to be done is to design the network for the internet exchange point connecting the five campuses together.

Configuration procedure

4.3 Network Topology

The network topology adopted in this project work is a star-star hybrid topology due to the spatial nature of the locations of the campuses. The campuses are connected using radio devices or physical cables as the case may be. For the purpose of the simulation model, cable (straight and serial) were used. Figure 4.3 shows the network topology of the design showing edge routers at each location of a campus NOC and three routers at the exchange point for purpose of load balancing and redundancy.

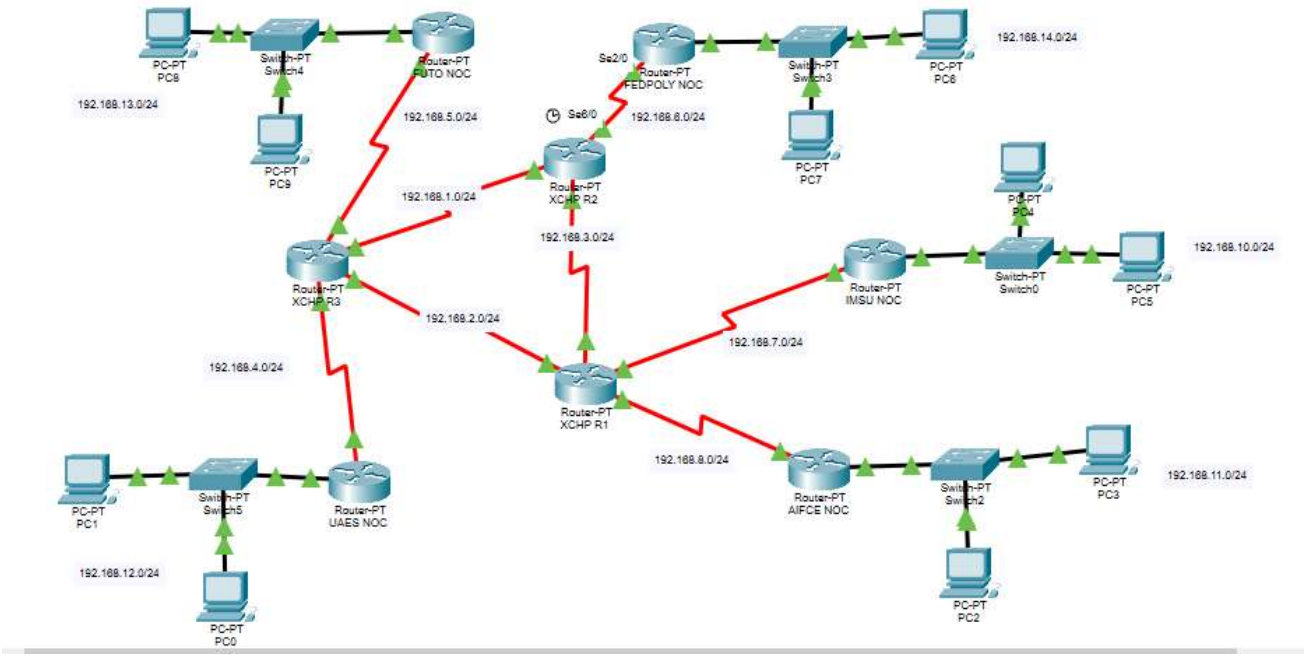

Figure 4.3: Network Topology of the Simulation Model.

Table 4.1 shows the IP configuration table of the network in figure 4.3. Private class C address where nocused between 1 and 14. Each interface of the router was assigned a whole block of IP for easy administration.

Table 4.1: IP Addressing Table for the ICCNS

Device	**Interface**	**IP address**	**CIDR value**	**Subnet mast**
XCHP R3	Se 2/0	192.168.1.1	24	255.255.255.0
XCHP R2	Se 2/0	192.168.1.2	24	255.255.255.0

XCHP R3	Se 3/0	192.168.2.1	24	255.255.255.0
XCHP R1	Se 2/0	192.168.2.2	24	255.255.255.0
XCHP R1	Se 3/0	192.168.3.1	24	255.255.255.0
XCHP R2	Se 3/0	192.168.3.2	24	255.255.255.0
XCHP R3	Se 7/0	192.168.4.1	24	255.255.255.0
UAES NOC	Se 3/0	192.168.4.2	24	255.255.255.0
XCHP R3	Se 6/0	192.168.5.1	24	255.255.255.0
FUTO NOC	Se 2/0	192.168.5.2	24	255.255.255.0
XCHP R2	Se 6/0	192.168.6.1	24	255.255.255.0
FEDPOLY NOC	Se 2/0	192.168.6.2	24	255.255.255.0
XCHP R1	Se 7/0	192.168.7.1	24	255.255.255.0
IMSU NOC	Se 2/0	192.168.7.2	24	255.255.255.0
XCHP R1	Se 6/0	192.168.8.1	24	255.255.255.0
AIFCE NOC	Se 2/0	192.168.8.2	24	255.255.255.0
IMSU NOC	Fa 0/0	192.168.10.1	24	255.255.255.0
AIFCE NOC	Fa 0/0	192.168.11.1	24	255.255.255.0
IMOPOLY NOC	Fa 0/0	192.168.12.1	24	255.255.255.0
FUTO NOC	Fa 0/0	192.168.13.1	24	255.255.255.0
FEDPOLY NOC	Fa 0/0	192.168.14.1	24	255.255.255.0

4.4 Network Configuration Phases

The network is configured using 3 routing protocols and their time to live is compared with each other to determine the optimal routing protocol that can fit the network topology for the exchange point network.

The connectivity between individual NOC is tested using internet control message protocol (ICMP) packets

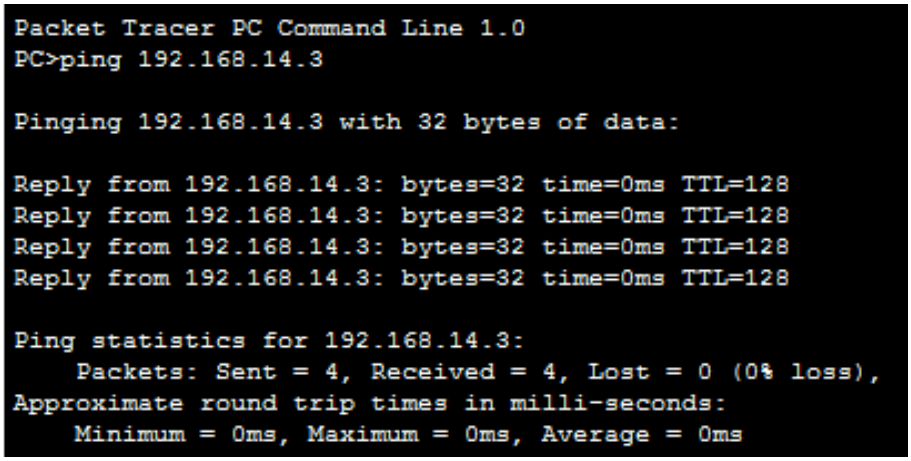

Figure 4.4: Connectivity Test Between PC6- and PC7

4.4.1 RIP Configuration

Routing Information Protocol (RIP) is a true distance-vector routing protocol. RIP sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it's inefficient on large networks with slow WAN links or on networks with a large number of routers installed. RIP version 1 uses only *classful routing*, which means that all devices in the network must use the same subnet mask. This is because RIP version 1 doesn't send updates with subnet mask information in tow. RIP version 2 provides something called *prefix routing* and does send subnet mask information with the route updates. This is called classless routing. For the first routing protocol P version 1, the network is configured using the following command line:

Router>en
Router#config t
Router(config)#router rip
Router(config-router)#network address
Router(config-router)# end

The network address in the command line above indicated all networks that are directly connected to the router. During RIP routing, only networks directly connected to the particular

router under consideration is required during the configuration process. All the other router information is leaned dynamically.

The steps involved in the RIP configuration process of the eight (8) routers that make up the internet exchange point network for the 5 campuses under consideration are explained below.

1) **RIP Router configuration for FUTO NOC**: The FUTO NOC (network operations center) router is configured with RIP using the following command line:

   Router> enable
   Router# configure terminal
   Router(config)# router rip
   Router(config-router)# network 192.168.5.0/24
   Router(config-router)# end

   Step 1: The first step is entering the command "*Router> enable"*. This command enables privileged EXEC mode. On entering the command, the system prompts the user to enter the network security password.

   Step 2: The second step is to enter the command "*Router# configure terminal"*. This command enters the global configuration mode.

   Step 3: The third step is entering the command "*Router(config)# router rip"*. This command enables the RIP routing process and enters router configuration mode.

   Step 4: The fourth step is entering the command "*Router(config-router)# network 192.168.5.0/24"*. This associates a network with the RIP routing process.

   Step 5: The fifth and last step is entering the command "*Router(config-router)# end"*. This command exits the router configuration mode and returns to privileged EXEC mode.

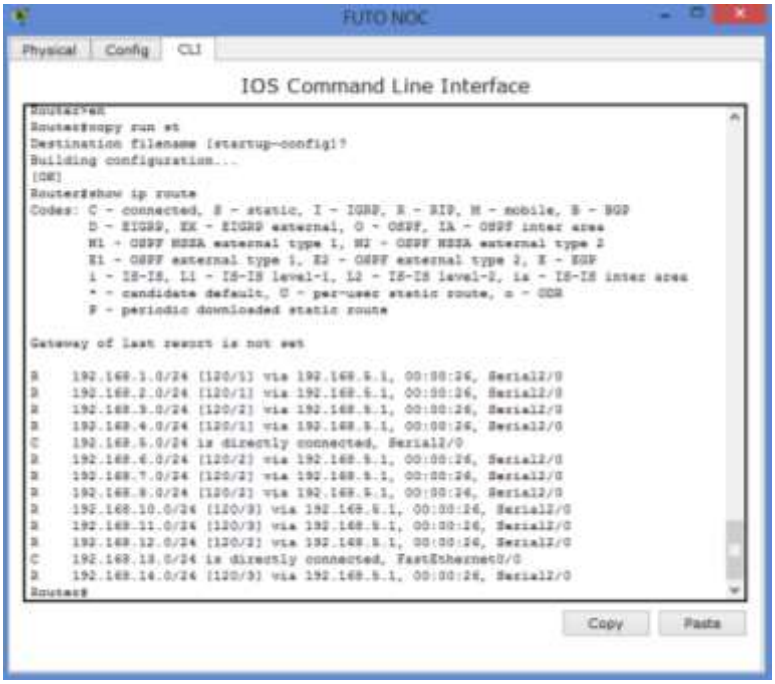

Figure 4.5: FUTO NOC Router Configuration Output

The routing information of FUTO NOC router in the network which is configured using routing information protocol (RIP) is shown in Figure 4.5. From the diagram, the lines with R indicates that those networks are reached using RIP. The lines with C indicates that those networks are directly connected to the router under consideration.

2) **RIP Router configuration for FEDPOLY NOC**: The FEDPOLY NOC (network operations center) router is configured with RIP using the following command line:

Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# network 192.168.6.0/24
Router(config-router)# end

The steps to enable RIP and configuring RIP parameters are explained below:

Step 1: The first step is entering the command "*Router> enable"*. This command enables privileged EXEC mode. On entering the command, the system prompts the user to enter the network security password.

Step 2: The second step is to enter the command "*Router# configure terminal"*. This command enters the global configuration mode.

Step 3: The third step is entering the command "*Router(config)# router rip"*. This command enables the RIP routing process and enters router configuration mode.

Step 4: The fourth step is entering the command "*Router(config-router)# network 192.168.6.0/24"*. This associates a network with the RIP routing process.

Step 5: The fifth and last step is entering the command "*Router(config-router)# end"*. This command exits the router configuration mode and returns to privileged EXEC mode.

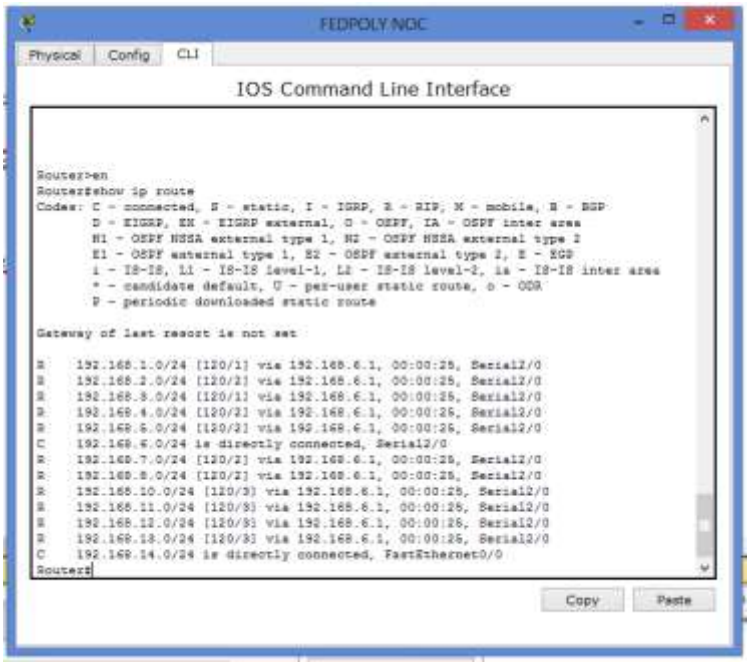

Figure 4.6: FEDPOLY NOC Router Configuration Output

The routing information of FEDPOLY NOC router in the network which is configured using routing information protocol (RIP) is shown in Figure 4.6. From the diagram, the lines with R indicates that those networks are reached using RIP. The lines with C indicates that those networks are directly connected to the router under consideration.

3) **RIP Router configuration for IMSU NOC**: The IMSU NOC (network operations center) router is configured with RIP using the following command line:

Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# network 192.168.7.0/24
Router(config-router)# end

The steps to enable RIP and configuring RIP parameters are explained below:

Step 1: The first step is entering the command "*Router> enable"*. This command enables privileged EXEC mode. On entering the command, the system prompts the user to enter the network security password.

Step 2: The second step is to enter the command "*Router# configure terminal"*. This command enters the global configuration mode.

Step 3: The third step is entering the command "*Router(config)# router rip"*. This command enables the RIP routing process and enters router configuration mode.

Step 4: The fourth step is entering the command "*Router(config-router)# network 192.168.7.0/24"*. This associates a network with the RIP routing process.

Step 5: The fifth and last step is entering the command "*Router(config-router)# end"*. This command exits the router configuration mode and returns to privileged EXEC mode.

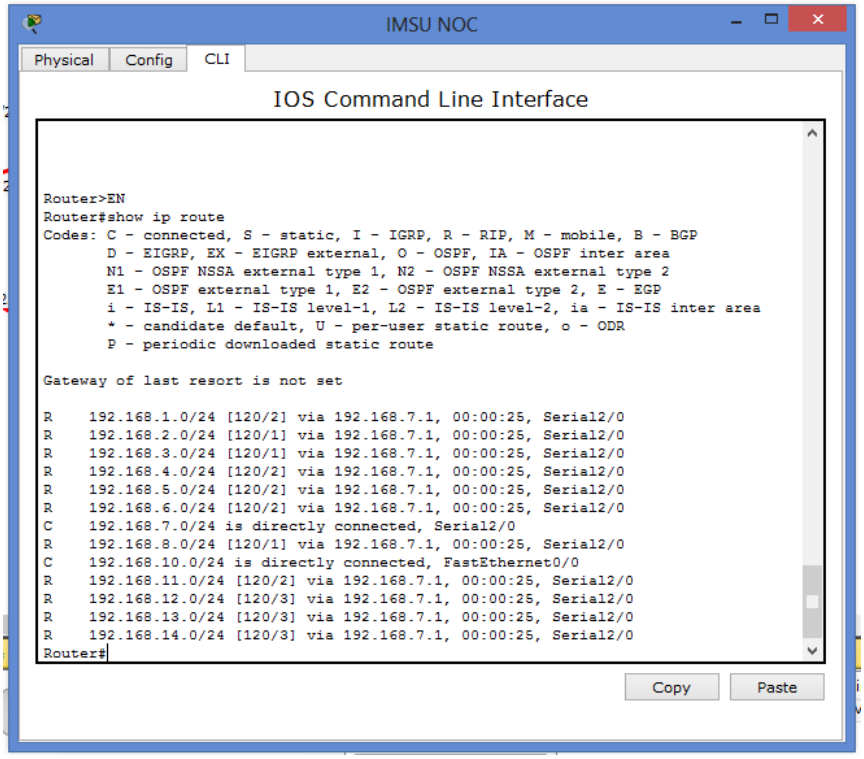

Figure 4.7: IMSU NOC Router Configuration Output

The routing information of IMSU NOC router in the network which is configured using routing information protocol (RIP) is shown in Figure 4.7. From the diagram, the lines with R indicates that those networks are reached using RIP. The lines with C indicates that those networks are directly connected to the router under consideration.

4) **RIP Router configuration for ALVAN NOC**: The ALVAN NOC (network operations center) router is configured with RIP using the following command line:

Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# network 192.168.8.0/24
Router(config-router)# end

The steps to enable RIP and configuring RIP parameters are explained below:

Step 1: The first step is entering the command "*Router> enable"*. This command enables privileged EXEC mode. On entering the command, the system prompts the user to enter the network security password.

Step 2: The second step is to enter the command "*Router# configure terminal"*. This command enters the global configuration mode.

Step 3: The third step is entering the command "*Router(config)# router rip"*. This command enables the RIP routing process and enters router configuration mode.

Step 4: The fourth step is entering the command "*Router(config-router)# network 192.168.8.0/24"*. This associates a network with the RIP routing process.

Step 5: The fifth and last step is entering the command "*Router(config-router)# end"*. This command exits the router configuration mode and returns to privileged EXEC mode.

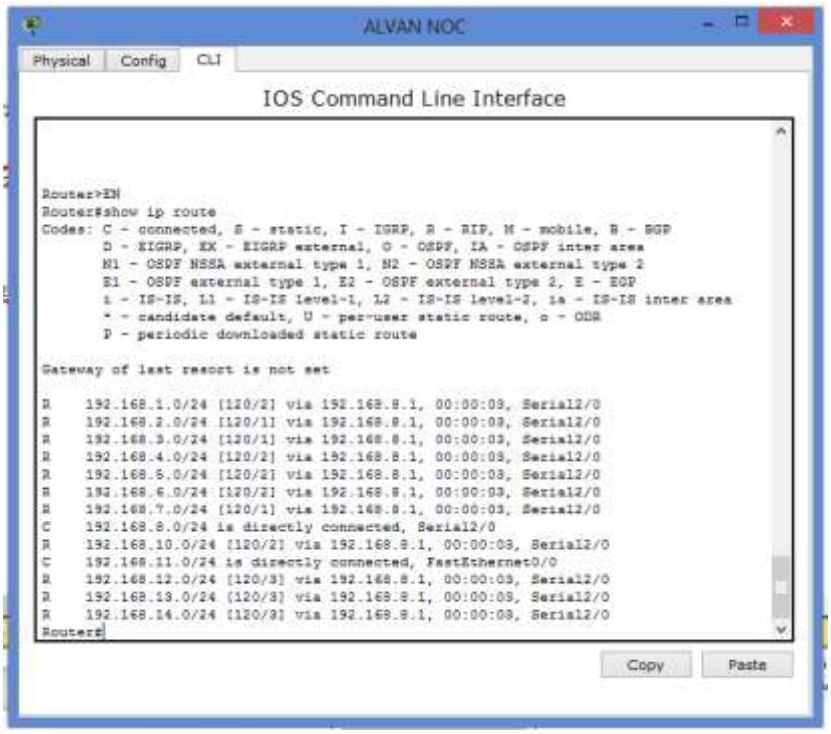

Figure 4.8: ALVAN NOC Router Configuration Output

The routing information of ALVAN NOC router in the network which is configured using routing information protocol (RIP) is shown in Figure 4.8. From the diagram, the lines with R indicates that those networks are reached using RIP. The lines with C indicates that those networks are directly connected to the router under consideration.

5) **RIP Router configuration for UAES NOC**: The UAES NOC (network operations center) router is configured with RIP using the following command line:

Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# network 192.168.4.0/24
Router(config-router)# end

The steps to enable RIP and configuring RIP parameters are explained below:

Step 1: The first step is entering the command "*Router> enable"*. This command enables privileged EXEC mode. On entering the command, the system prompts the user to enter the network security password.

Step 2: The second step is to enter the command "*Router# configure terminal"*. This command enters the global configuration mode.

Step 3: The third step is entering the command "*Router(config)# router rip"*. This command enables the RIP routing process and enters router configuration mode.

Step 4: The fourth step is entering the command "*Router(config-router)# network 192.168.4.0/24"*. This associates a network with the RIP routing process.

Step 5: The fifth and last step is entering the command "*Router(config-router)# end"*. This command exits the router configuration mode and returns to privileged EXEC mode.

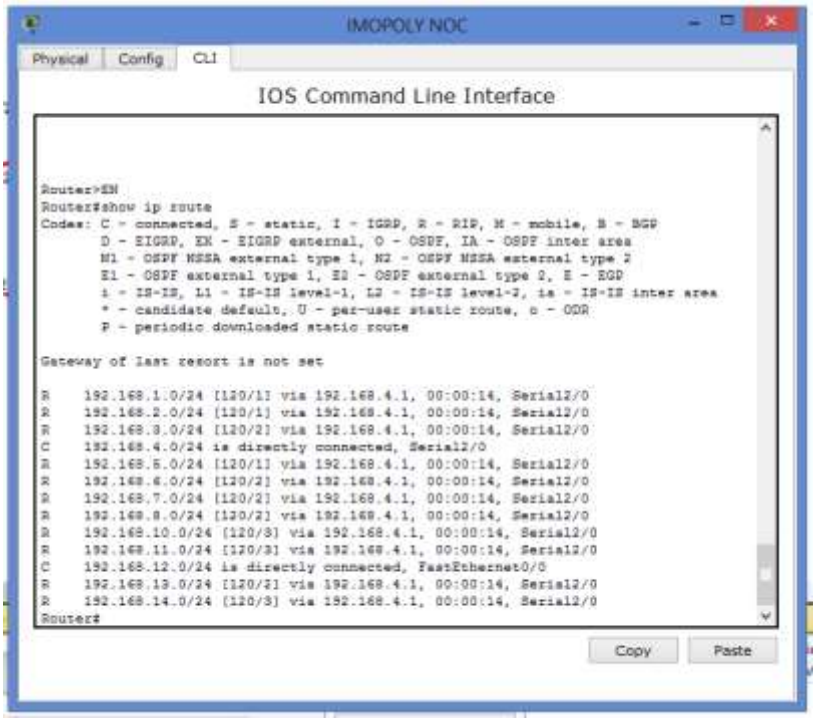

Figure 4.9: UAES NOC Router Configuration Output

The routing information of UAES NOC router in the network which is configured using routing information protocol (RIP) is shown in Figure 4.9. From the diagram, the lines with R indicates that those networks are reached using RIP. The lines with C indicates that those networks are directly connected to the router under consideration.

6) **RIP Router configuration for XCHP R3 NOC**: The XCHP R3 NOC (network operations center) router is configured with RIP using the following command line:

Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# network 192.168.1.1/24
Router(config-router)# end

The steps to enable RIP and configuring RIP parameters are explained below:

Step 1: The first step is entering the command "*Router> enable"*. This command enables privileged EXEC mode. On entering the command, the system prompts the user to enter the network security password.

Step 2: The second step is to enter the command "*Router# configure terminal"*. This command enters the global configuration mode.

Step 3: The third step is entering the command "*Router(config)# router rip"*. This command enables the RIP routing process and enters router configuration mode.

Step 4: The fourth step is entering the command "*Router(config-router)# network 192.168.1.1/24"*. This associates a network with the RIP routing process.

Step 5: The fifth and last step is entering the command "*Router(config-router)# end"*. This command exits the router configuration mode and returns to privileged EXEC mode.

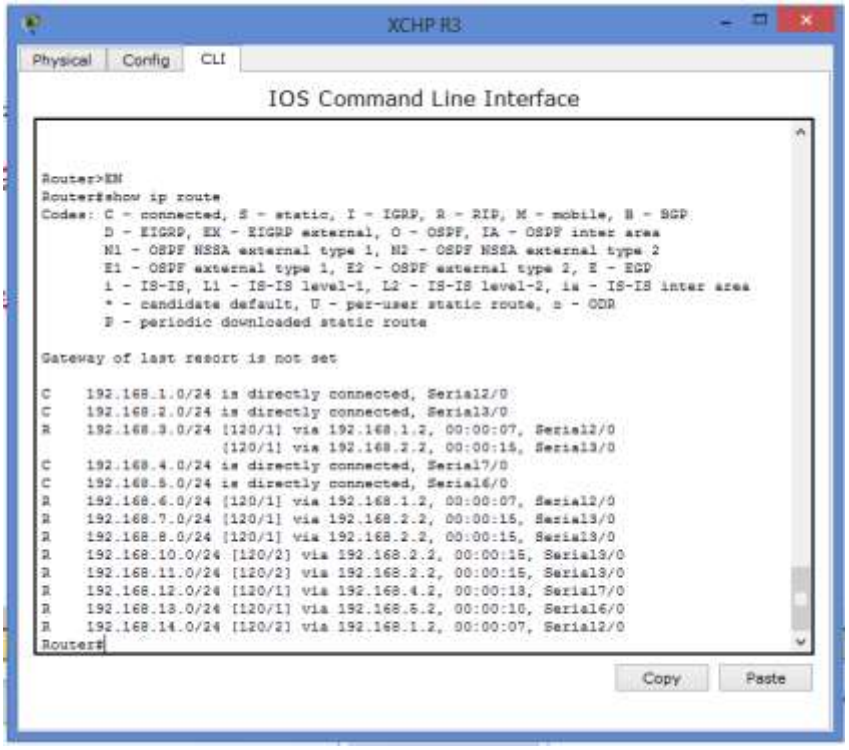

Figure 4.10: XCHP R3 NOC Router Configuration Output

The routing information of XCHP R3 NOC router in the network which is configured using routing information protocol (RIP) is shown in Figure 4.10. From the diagram,

the lines with R indicates that those networks are reached using RIP. The lines with C indicate that those networks are directly connected to the router under consideration.

7) **RIP Router configuration for XCHP R2 NOC**: The XCHP R2 NOC (network operations center) router is configured with RIP using the following command line:

Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# network 192.168.1.2/24
Router(config-router)# end

The steps to enable RIP and configuring RIP parameters are explained below:

Step 1: The first step is entering the command "*Router> enable"*. This command enables privileged EXEC mode. On entering the command, the system prompts the user to enter the network security password.

Step 2: The second step is to enter the command "*Router# configure terminal"*. This command enters the global configuration mode.

Step 3: The third step is entering the command "*Router(config)# router rip"*. This command enables the RIP routing process and enters router configuration mode.

Step 4: The fourth step is entering the command "*Router(config-router)# network 192.168.1.2/24"*. This associates a network with the RIP routing process.

Step 5: The fifth and last step is entering the command "*Router(config-router)# end"*. This command exits the router configuration mode and returns to privileged EXEC mode.

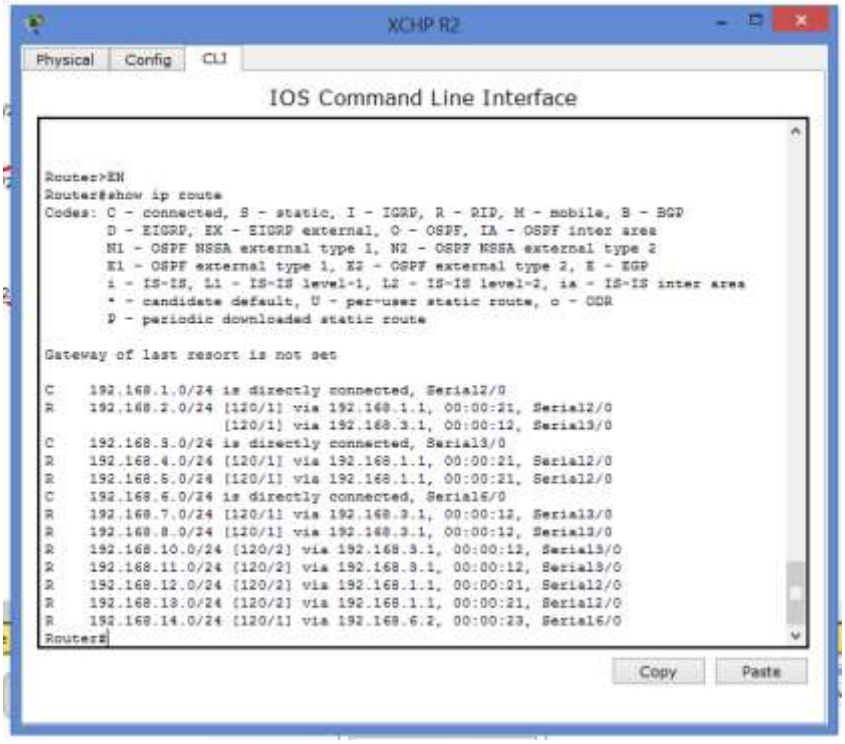

Figure 4.11: XCHP R2 NOC Router Configuration Output

The routing information of XCHP R2 NOC router in the network which is configured using routing information protocol (RIP) is shown in Figure 4.11. From the diagram, the lines with R indicates that those networks are reached using RIP. The lines with C indicates that those networks are directly connected to the router under consideration.

8) **RIP Router configuration for XCHP R1 NOC**: The XCHP R1 NOC (network operations center) router is configured with RIP using the following command line:

Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# network 192.168.2.2/24
Router(config-router)# end

The steps to enable RIP and configuring RIP parameters are explained below:

Step 1: The first step is entering the command "*Router> enable"*. This command enables privileged EXEC mode. On entering the command, the system prompts the user to enter the network security password.

Step 2: The second step is to enter the command "*Router# configure terminal"*. This command enters the global configuration mode.

Step 3: The third step is entering the command "*Router(config)# router rip"*. This command enables the RIP routing process and enters router configuration mode.

Step 4: The fourth step is entering the command "*Router(config-router)# network 192.168.2.2/24"*. This associates a network with the RIP routing process.

Step 5: The fifth and last step is entering the command "*Router(config-router)# end"*. This command exits the router configuration mode and returns to privileged EXEC mode.

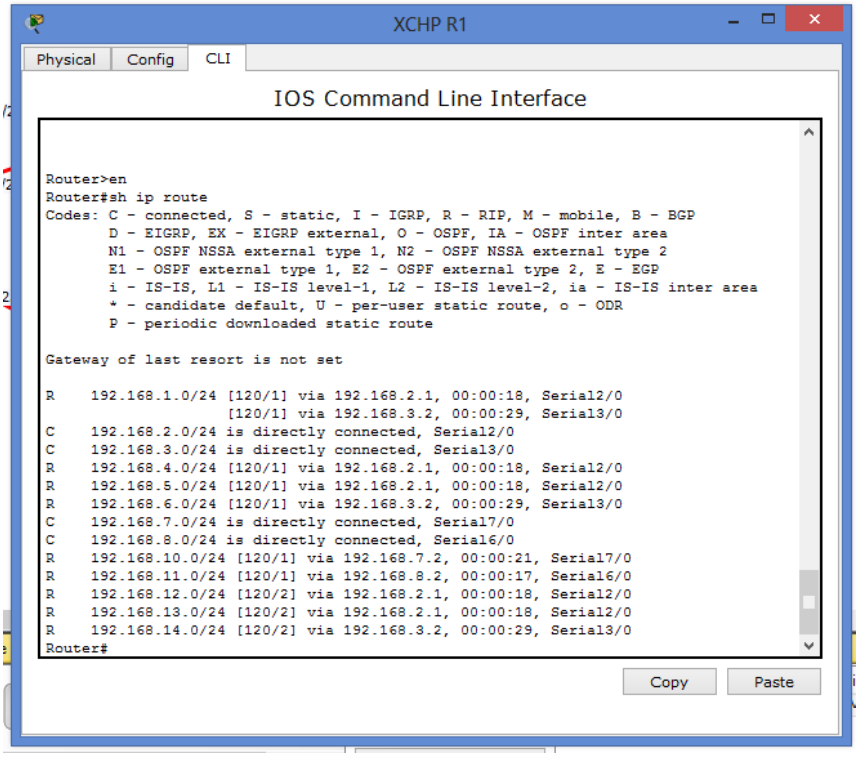

Figure 4.12: XCHP R1 NOC Router Configuration Output

The routing information of XCHP R1 NOC router in the network which is configured using routing information protocol (RIP) is shown in Figure 4.12. From the diagram, the lines with R indicates that those networks are reached using RIP. The lines with C indicates that those networks are directly connected to the router under consideration.

Figure 4.5 to 4.12 are the routing information of all the routers in the network configured using routing information protocol (RIP).

The routing information protocol (RIP) simulation panel window displays the results of the simulation of the routers in the network using RIP.

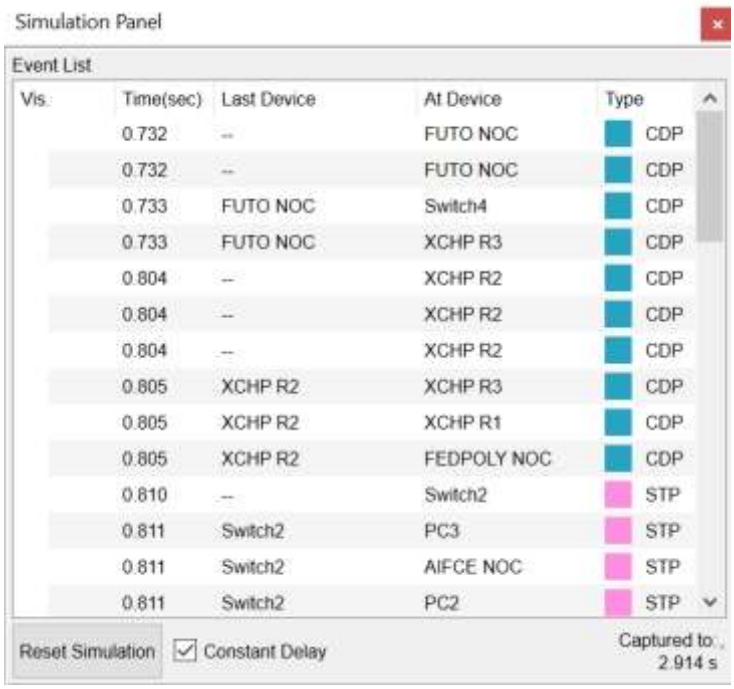

Figure 4.13: RIP Simulation Results (Brief)

Figure 4.13 shows the simulation results for RIP capturing ICMP packets over a 2.914 seconds' period. The simulation results show RIP reporting time between nodes ranging between 0.732 and 0.811seconds.

4.4.2 EIGRP Configuration

Enhanced IGRP (EIGRP) is a classless, enhanced distance-vector protocol that uses the concept of an autonomous system to describe the set of contiguous routers that run the same routing protocol and share routing information. EIGRP includes the subnet mask in its route updates because it is considered classless. And as you now know, the advertisement of subnet information allows us to use Variable Length Subnet Masks (VLSMs) and manual

summarization when designing a network. It should also be noted here that EIGRP is a routing protocol that is proprietary to Cisco.

The following command lines are used to configure EIGRP on the internet exchange point network.

Router#config t

Router(config)#router eigrp 20
Router(config-router)#network address

The EIGRP command works with an autonomous system number which should be same for all routers if they are to communicate with each other. For this network topology, the autonomous system number is 20.

Below is the detailed explanation of the steps involved in the EIGRP configuration process of the eight routers that make up the internet exchange point network for the 5 campuses under consideration.

1) **EIGRP Router configuration for FUTO NOC**: The FUTO NOC router is configured with EIGRP using the following command line:

   Device> enable
   Device# configure terminal
   Device(config)# router eigrp 20
   Device(config-router)# network 192.168.5.0/24
   Device(config-router)# end

   Step 1: The first step is entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering this command, the user will be prompted to enter the admin password.

   Step 2: The second step is entering the command "*Device# configure terminal"*. The purpose of this command is to enter the global configuration mode.

Step 3: The third step is entering the command "*Device(config)# router eigrp 20"*, where 20 is the autonomous system number in this network. This command configures the EIGRP routing process and enters router configuration mode.

Step 4: The fourth step is to enter the network *network-number* by entering the command "*Device(config-router)# network 192.168.5.0/24"* where the network address specified is that of FUTO NOC. This command associates a network with an EIGRP routing process.

Step 5: The final step is to entering the command "*Device(config-router)# end*". This command exits router configuration mode and returns to privileged EXEC mode.

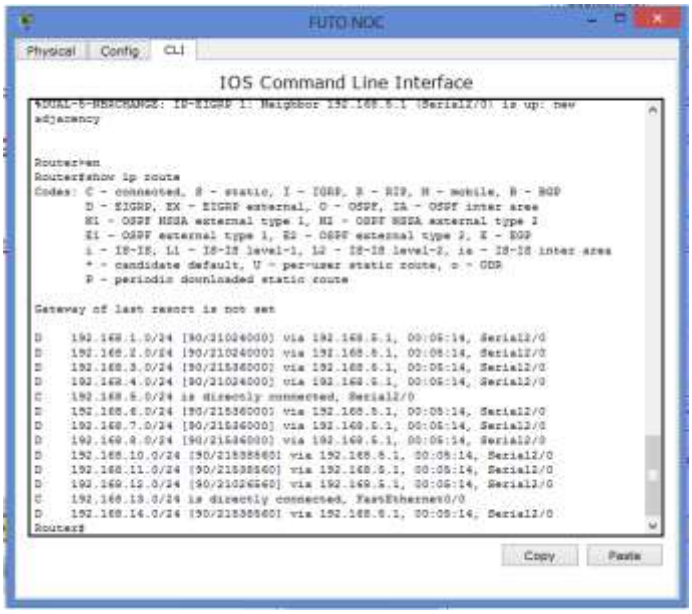

Figure 4.14: FUTO NOC EIGRP Router Configuration Output

Figure 4.14 shows screen shots of the working of EIGRP routing protocol on the FUTO NOC which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter D shows that the router learns about other networks using EIGRP. EIGRP has a slightly lower autonomous system number (AS) compared to RIP.

2) **EIGRP Router configuration for FEDPOLY NOC**: The FEDPOLY NOC (network operations center) router is configured with EIGRP using the following command line:

Device> enable
Device# configure terminal
Device(config)# router eigrp 20
Device(config-router)# network 192.168.6.0/24
Device(config-router)# end

Step 1: The first step is entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering this command, the user will be prompted to enter the admin password.

Step 2: The second step is entering the command "*Device# configure terminal"*. The purpose of this command is to enter the global configuration mode.

Step 3: The third step is entering the command "*Device(config)# router eigrp 20"*, where 20 is the autonomous system number in this network. This command configures the EIGRP routing process and enters router configuration mode.

Step 4: The fourth step is to enter the network *network-number* by entering the command "*Device(config-router)# network 192.168.6.0/24"* where the network address specified is that of FUTO NOC. This command associates a network with an EIGRP routing process.

Step 5: The final step is to entering the command "*Device(config-router)# end*". This command exits router configuration mode and returns to privileged EXEC mode.

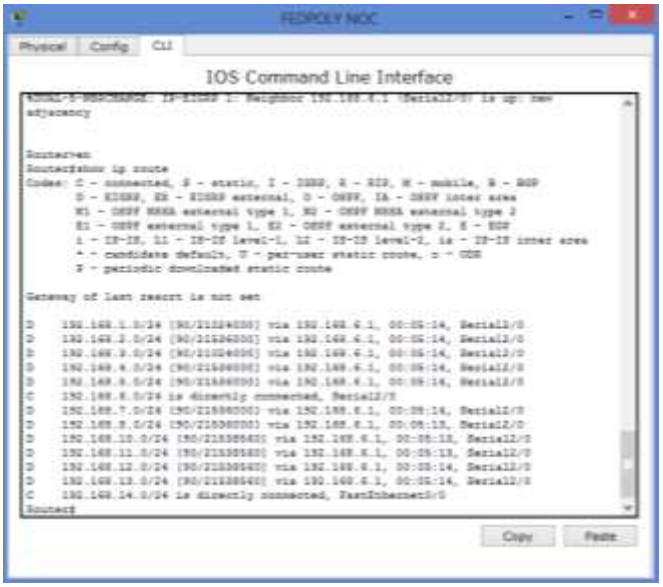

Figure 4.15: FEDPOLY NOC EIGRP Router Configuration Output

Figure 4.15 shows screen shots of the working of EIGRP routing protocol on the FEDPOLY NOC which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter D shows that the router learns about other networks using EIGRP. EIGRP has a slightly lower autonomous system number (AS) compared to RIP.

3) **EIGRP Router configuration for IMSU NOC**: The IMSU NOC (network operations center) router is configured with EIGRP using the following command line:

Device> enable
Device# configure terminal
Device(config)# router eigrp 20
Device(config-router)# network 192.168.7.0/24
Device(config-router)# end

Step 1: The first step is entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering this command, the user will be prompted to enter the admin password.

Step 2: The second step is entering the command "*Device# configure terminal"*. The purpose of this command is to enter the global configuration mode.

Step 3: The third step is entering the command "*Device(config)# router eigrp 20"*, where 20 is the autonomous system number in this network. This command configures the EIGRP routing process and enters router configuration mode.

Step 4: The fourth step is to enter the network *network-number* by entering the command "*Device(config-router)# network 192.168.7.0/24"* where the network address specified is that of FUTO NOC. This command associates a network with an EIGRP routing process.

Step 5: The final step is to entering the command "*Device(config-router)# end*". This command exits router configuration mode and returns to privileged EXEC mode.

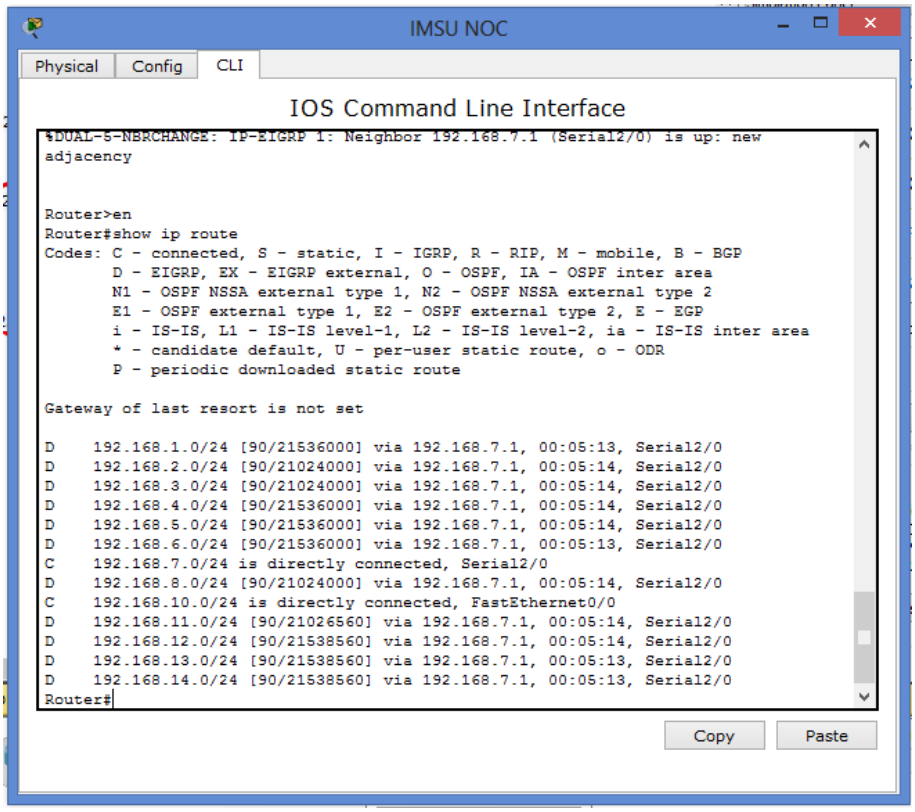

Figure 4.16: IMSU NOC EIGRP Router Configuration Output

Figure 4.16 shows screen shots of the working of EIGRP routing protocol on the IMSU NOC which is one of the eight routers that make up the internet exchange

point network for the 5 campuses under consideration. The letter D shows that the router learns about other networks using EIGRP. EIGRP has a slightly lower autonomous system number (AS) compared to RIP.

4) **EIGRP Router configuration for AIFCE NOC**: The AIFCE NOC (network operations center) router is configured with EIGRP using the following command line:

Device> enable
Device# configure terminal
Device(config)# router eigrp 20
Device(config-router)# network 192.168.8.0/24
Device(config-router)# end

Step 1: The first step is entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering this command, the user will be prompted to enter the admin password.

Step 2: The second step is entering the command "*Device# configure terminal"*. The purpose of this command is to enter the global configuration mode.

Step 3: The third step is entering the command "*Device(config)# router eigrp 20"*, where 20 is the autonomous system number in this network. This command configures the EIGRP routing process and enters router configuration mode.

Step 4: The fourth step is to enter the network *network-number* by entering the command "*Device(config-router)# network 192.168.8.0/24"* where the network address specified is that of FUTO NOC. This command associates a network with an EIGRP routing process.

Step 5: The final step is to entering the command "*Device(config-router)# end*". This command exits router configuration mode and returns to privileged EXEC mode.

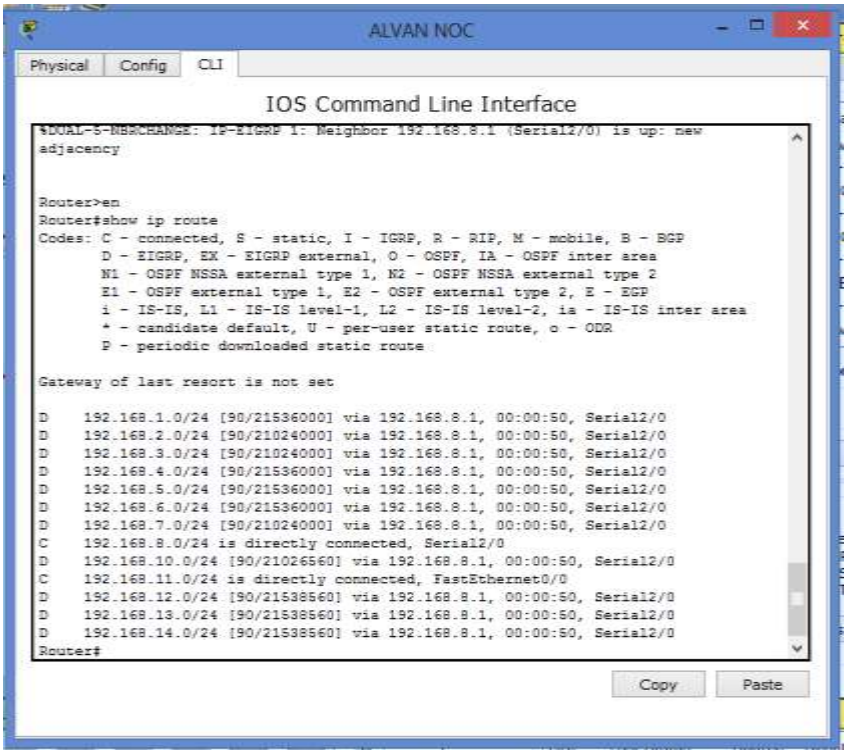

Figure 4.17: AIFCE NOC EIGRP Router Configuration Output

Figure 4.17 shows screen shots of the working of EIGRP routing protocol on the AIFCE NOC which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter D shows that the router learns about other networks using EIGRP. EIGRP has a slightly lower autonomous system number (AS) compared to RIP.

5) **EIGRP Router configuration for UAES NOC**: The UAES NOC (network operations center) router is configured with EIGRP using the following command line:

Device> enable
Device# configure terminal
Device(config)# router eigrp 20
Device(config-router)# network 192.168.4.0/24
Device(config-router)# end

Step 1: The first step is entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering this command, the user will be prompted to enter the admin password.

Step 2: The second step is entering the command "*Device# configure terminal"*. The purpose of this command is to enter the global configuration mode.

Step 3: The third step is entering the command "*Device(config)# router eigrp 20"*, where 20 is the autonomous system number in this network. This command configures the EIGRP routing process and enters router configuration mode.

Step 4: The fourth step is to enter the network *network-number* by entering the command "*Device(config-router)# network 192.168.4.0/24"* where the network address specified is that of FUTO NOC. This command associates a network with an EIGRP routing process.

Step 5: The final step is to entering the command "*Device(config-router)# end*". This command exits router configuration mode and returns to privileged EXEC mode.

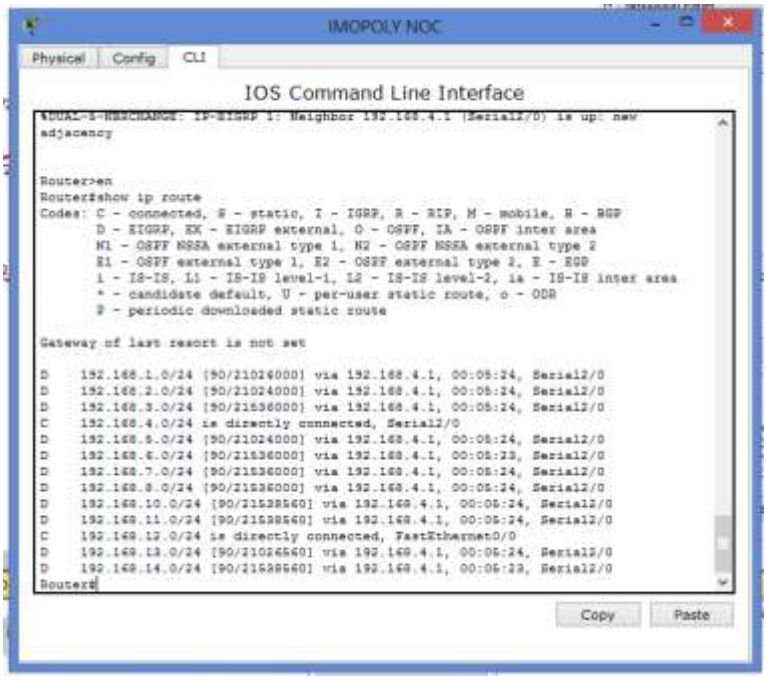

Figure 4.18: UAES NOC EIGRP Router Configuration Output

Figure 4.18 shows screen shots of the working of EIGRP routing protocol on the UAES NOC which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter D shows that the router learns about other networks using EIGRP. EIGRP has a slightly lower autonomous system number (AS) compared to RIP.

6) **EIGRP Router configuration for XCHP R3 NOC**: The XCHP R3 NOC (network operations center) router is configured with EIGRP using the following command line:

Device> enable
Device# configure terminal
Device(config)# router eigrp 20
Device(config-router)# network 192.168.1.1/24
Device(config-router)# end

Step 1: The first step is entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering this command, the user will be prompted to enter the admin password.

Step 2: The second step is entering the command "*Device# configure terminal"*. The purpose of this command is to enter the global configuration mode.

Step 3: The third step is entering the command "*Device(config)# router eigrp 20"*, where 20 is the autonomous system number in this network. This command configures the EIGRP routing process and enters router configuration mode.

Step 4: The fourth step is to enter the network *network-number* by entering the command "*Device(config-router)# network 192.168.1.1/24"* where the network address specified is that of FUTO NOC. This command associates a network with an EIGRP routing process.

Step 5: The final step is to entering the command "*Device(config-router)# end*". This command exits router configuration mode and returns to privileged EXEC mode.

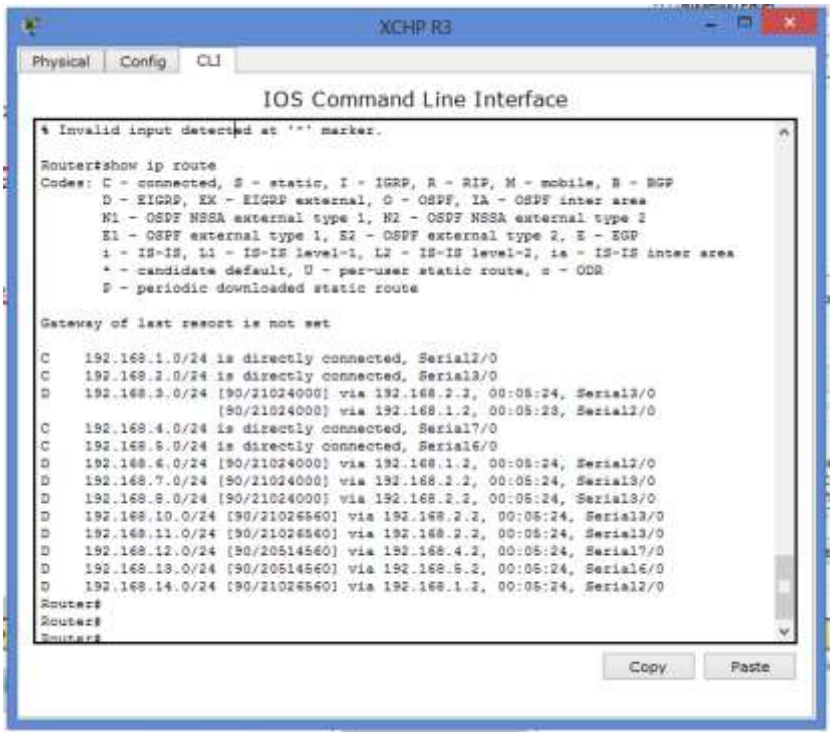

Figure 4.19: XCHP R3 NOC EIGRP Router Configuration Output

Figure 4.19 shows screen shots of the working of EIGRP routing protocol on the XCHP R3 NOC which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter D shows that the router learns about other networks using EIGRP. EIGRP has a slightly lower autonomous system number (AS) compared to RIP.

7) **EIGRP Router configuration for XCHP R2 NOC**: The XCHP R2 NOC (network operations center) router is configured with EIGRP using the following command line:

Device> enable
Device# configure terminal
Device(config)# router eigrp 20
Device(config-router)# network 192.168.1.2/24
Device(config-router)# end

Step 1: The first step is entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering this command, the user will be prompted to enter the admin password.

Step 2: The second step is entering the command "*Device# configure terminal"*. The purpose of this command is to enter the global configuration mode.

Step 3: The third step is entering the command "*Device(config)# router eigrp 20"*, where 20 is the autonomous system number in this network. This command configures the EIGRP routing process and enters router configuration mode.

Step 4: The fourth step is to enter the network *network-number* by entering the command "*Device(config-router)# network 192.168.1.2/24"* where the network address specified is that of FUTO NOC. This command associates a network with an EIGRP routing process.

Step 5: The final step is to entering the command "*Device(config-router)# end*". This command exits router configuration mode and returns to privileged EXEC mode.

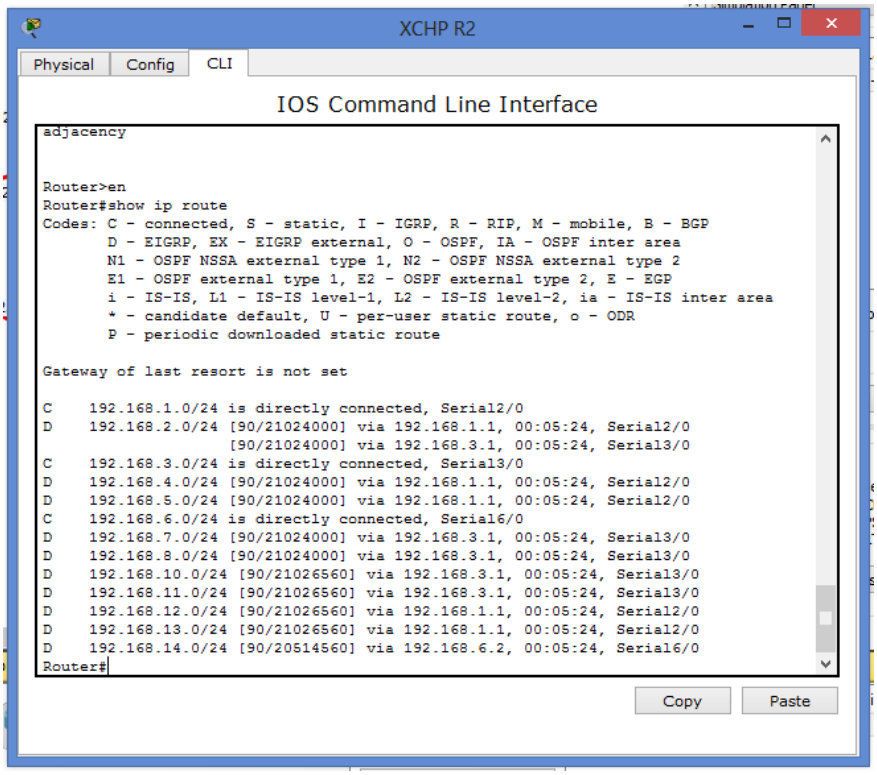

Figure 4.20: XCHP R2 NOC EIGRP Router Configuration Output

Figure 4.20 shows screen shots of the working of EIGRP routing protocol on the XCHP R2 NOC which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter D shows that the router learns about other networks using EIGRP. EIGRP has a slightly lower autonomous system number (AS) compared to RIP.

8) **EIGRP Router configuration for XCHP R1 NOC**: The XCHP R1 NOC (network operations center) router is configured with EIGRP using the following command line:

Device> enable

Device# configure terminal
Device(config)# router eigrp 20
Device(config-router)# network 192.168.2.2/24
Device(config-router)# end

Step 1: The first step is entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering this command, the user will be prompted to enter the admin password.

Step 2: The second step is entering the command "*Device# configure terminal"*. The purpose of this command is to enter the global configuration mode.

Step 3: The third step is entering the command "*Device(config)# router eigrp 20"*, where 20 is the autonomous system number in this network. This command configures the EIGRP routing process and enters router configuration mode.

Step 4: The fourth step is to enter the network *network-number* by entering the command "*Device(config-router)# network 192.168.2.2/24"* where the network address specified is that of FUTO NOC. This command associates a network with an EIGRP routing process.

Step 5: The final step is to entering the command "*Device(config-router)# end*". This command exits router configuration mode and returns to privileged EXEC mode.

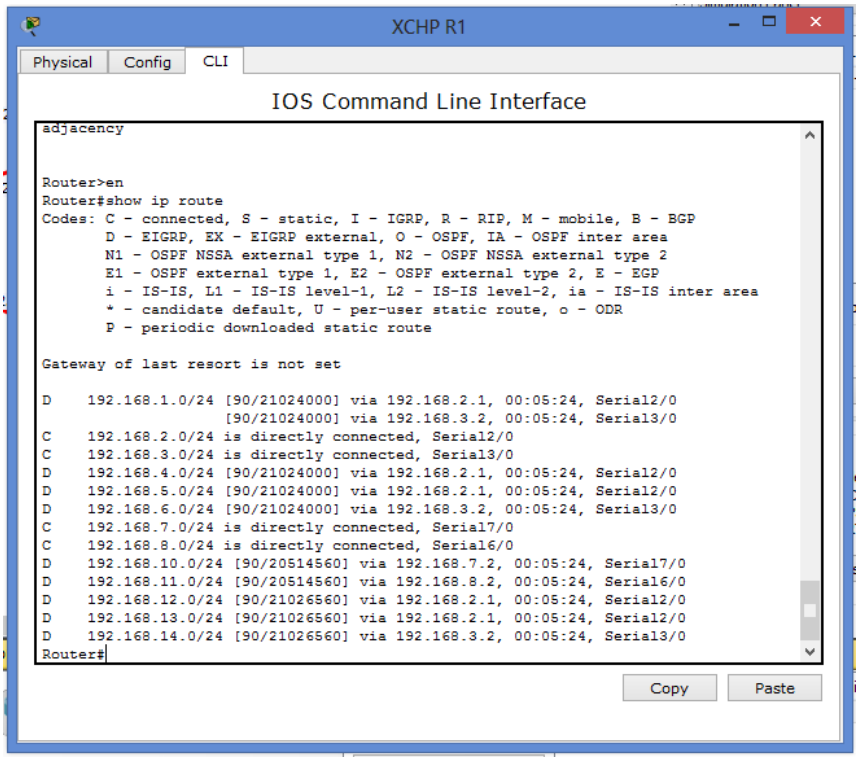

Figure 4.21: XCHP R1 NOC Router Configuration Output

Figure 4.21 shows screen shots of the working of EIGRP routing protocol on the XCHP R1 NOC which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter D shows that the router learns about other networks using EIGRP. EIGRP has a slightly lower autonomous system number (AS) compared to RIP.

Figure 4.14 to 4.21 shows screen shots of the working of EIGRP routing protocol on the eight routers that make up the internet exchange point network for the 5 campuses under consideration. It should also be noted here that EIGRP is a routing protocol that is proprietary to Cisco.

The Enhanced Interior Gateway Routing Protocol (EIGRP) simulation panel window displays the results of the simulation of the routers in the network using EIGRP.

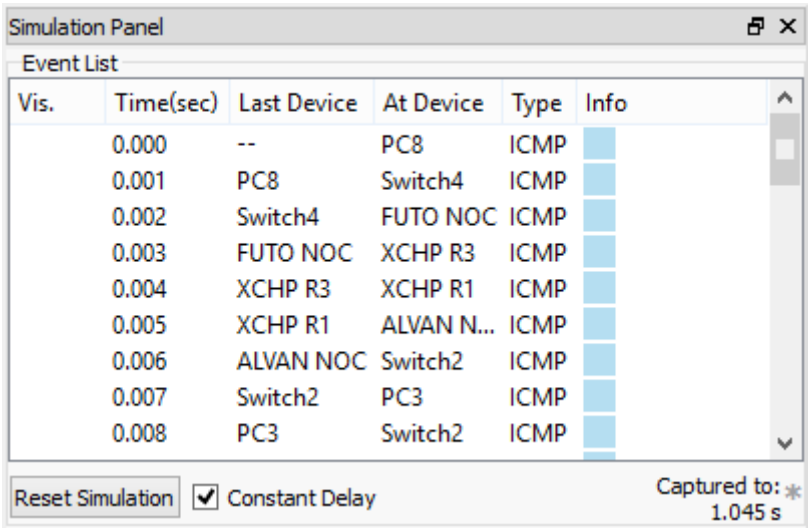

Figure 4.22: EIGRP Simulation Results

Figure 4.22 shows the simulation results for EIGRP capturing ICMP packets over a 1.045seconds period. The simulation results show RIP reporting time between nodes ranging between 0.371 and 0.974seconds.

4.4.3 OSPF Configuration

Open Shortest Path First (OSPF) is an open standard routing protocol that's been implemented by a wide variety of network vendors, including Cisco. OSPF works by using the Dijkstra algorithm. First, a shortest path tree is constructed, and then the routing table is populated with the resulting best paths.

To configure OSPF, the following command is used:

Router#config t
Router(config)#router ospf 1
Router(config-router)#<network network address> <wildcard mask> <area number>

Below is the detailed explanation of the steps involved in the OSPF configuration process of the eight routers that make up the internet exchange point network for the 5 campuses under consideration.

1) **OSPF Router configuration for FUTO NOC**: The FUTO NOC (network operations center) router is configured with OSPF using the following command line:

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 192.168.5.1 0.0.0.3 area 20
Router(config-router)# end

Step 1: The first step is to run the enable command. This is done by entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering the command, the user will be prompted to enter the network password if enabled.

Step 2: The second step is to configure the router terminal. This is done by entering the command *Router# configure terminal.* This command is used to enter the global configuration mode.

Step 3: The third step is to configure the router ospf *process-id.* This is achieved by entering the command; *Router(config)# router ospf 1*. This command enables OSPF routing and enters router configuration mode.

Step 4: The fourth step is to configure the network ip-address wildcard-mask and area area-id. This is done by entering the command; *Router(config-router)# network 192.168.5.0 0.0.0.3 area 20*, where the network address is 192.168.5.0, wildcard mask is *0.0.0.3 and* area number is 20. This defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5: The fifth step is to end the configuration process by entering the command *Router(config-router)# end*. The command exits router configuration mode and returns to privileged EXEC mode.

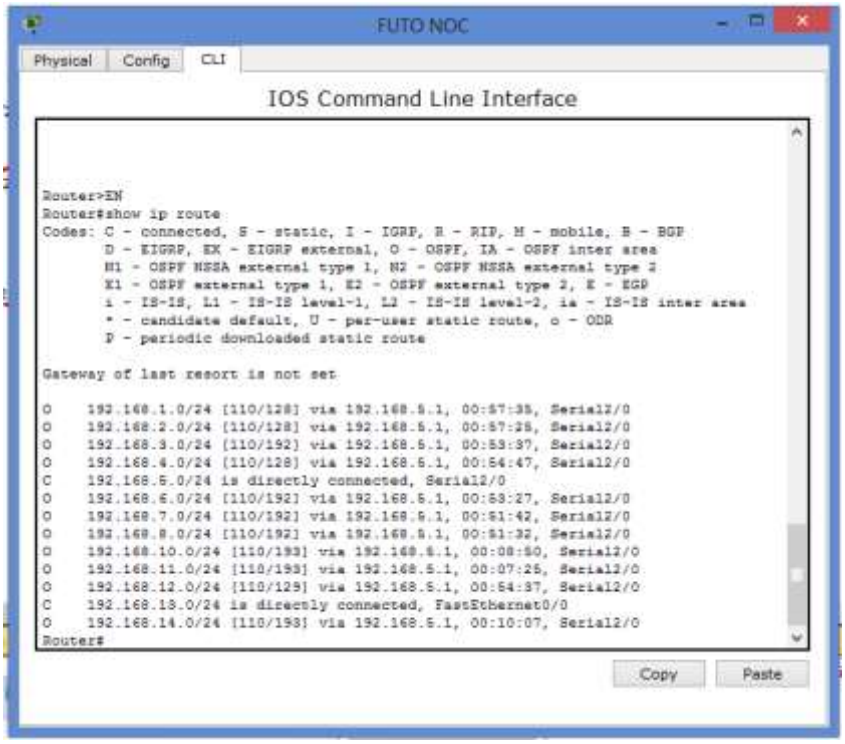

Figure 4.23: FUTO NOC OSPF Router Configuration Output

Figure 4.23 shows screen shots of the working of OSPF routing protocol on the FUTO NOC router which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter O shows that the router is connected to the other networks using OSPF. The lines with C indicates that those networks are directly connected to the router under consideration.

2) **OSPF Router configuration for FEDPOLY NOC**: The FEDPOLY NOC (network operations center) router is configured with OSPF using the following command line:

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 192.168.6.0 0.0.0.3 area 20
Router(config-router)# end

Step 1: The first step is to run the enable command. This is done by entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering the command, the user will be prompted to enter the network password if enabled.

Step 2: The second step is to configure the router terminal. This is done by entering the command *Router# configure terminal.* This command is used to enter the global configuration mode.

Step 3: The third step is to configure the router ospf *process-id.* This is achieved by entering the command; *Router(config)# router ospf 1*. This command enables OSPF routing and enters router configuration mode.

Step 4: The fourth step is to configure the network ip-address wildcard-mask and area area-id. This is done by entering the command; *Router(config-router)# network 192.168.6.0 0.0.0.3 area 20,* where the network address is 192.168.6.0, wildcard mask is *0.0.0.3 and* area number is 20. This defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5: The fifth step is to end the configuration process by entering the command *Router(config-router)# end*. The command exits router configuration mode and returns to privileged EXEC mode.

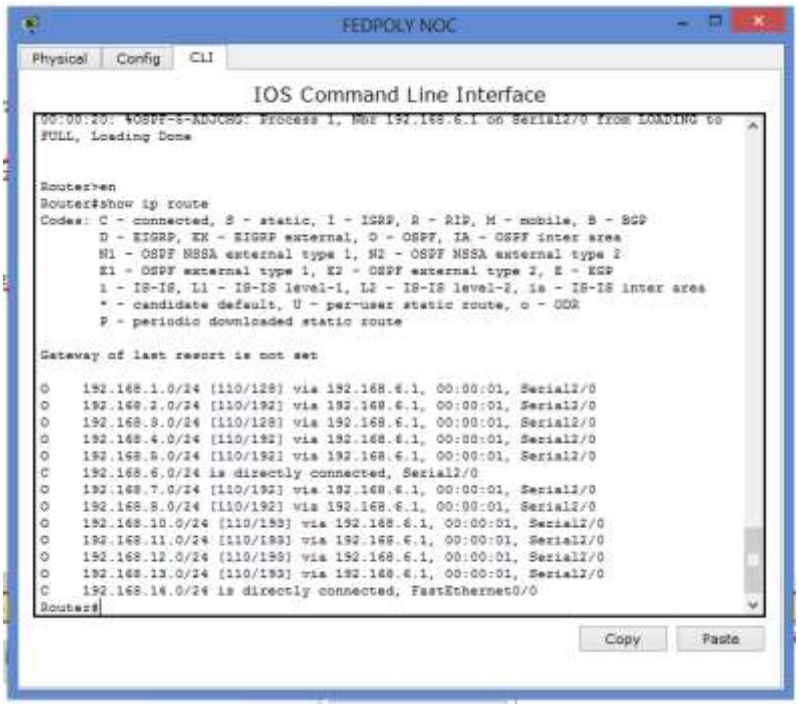

Figure 4.24: FEDPOLY NOC OSPF Router Configuration Output

Figure 4.24 shows screen shots of the working of OSPF routing protocol on the FEDPOLY NOC router which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter O shows that the router is connected to the other networks using OSPF. The lines with C indicates that those networks are directly connected to the router under consideration.

3) **OSPF Router configuration for IMSU NOC**: The IMSU NOC (network operations center) router is configured with OSPF using the following command line:

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 192.168.7.0 0.0.0.3 area 20
Router(config-router)# end

Step 1: The first step is to run the enable command. This is done by entering the command *Router> enable*. This command enables the privileged EXEC mode. On

entering the command, the user will be prompted to enter the network password if enabled.

Step 2: The second step is to configure the router terminal. This is done by entering the command *Router# configure terminal.* This command is used to enter the global configuration mode.

Step 3: The third step is to configure the router ospf *process-id.* This is achieved by entering the command; *Router(config)# router ospf 1*. This command enables OSPF routing and enters router configuration mode.

Step 4: The fourth step is to configure the network ip-address wildcard-mask and area area-id. This is done by entering the command; *Router(config-router)# network 192.168.7.0 0.0.0.3 area 20*, where the network address is 192.168.7.0, wildcard mask is *0.0.0.3 and* area number is 20. This defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5: The fifth step is to end the configuration process by entering the command *Router(config-router)# end*. The command exits router configuration mode and returns to privileged EXEC mode.

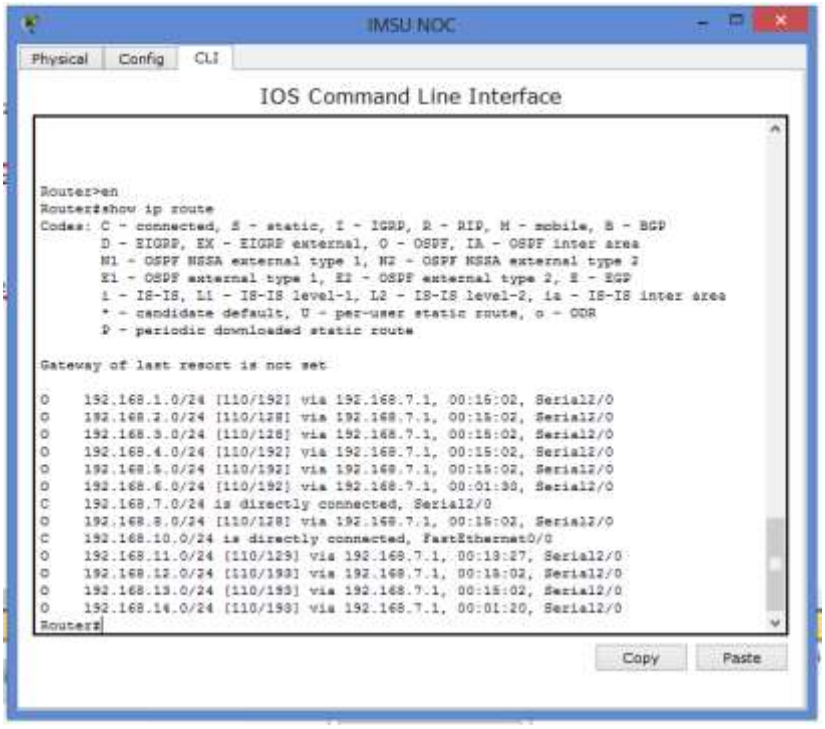

Figure 4.25: IMSU NOC OSPF Router Configuration Output

Figure 4.25 shows screen shots of the working of OSPF routing protocol on the IMSU NOC router which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter O shows that the router is connected to the other networks using OSPF. The lines with C indicates that those networks are directly connected to the router under consideration.

4) **OSPF Router configuration for ALVAN NOC**: The ALVAN NOC (network operations center) router is configured with OSPF using the following command line:

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 192.168.8.0 0.0.0.3 area 20
Router(config-router)# end

Step 1: The first step is to run the enable command. This is done by entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering the command, the user will be prompted to enter the network password if enabled.

Step 2: The second step is to configure the router terminal. This is done by entering the command *Router# configure terminal.* This command is used to enter the global configuration mode.

Step 3: The third step is to configure the router ospf *process-id.* This is achieved by entering the command; *Router(config)# router ospf 1*. This command enables OSPF routing and enters router configuration mode.

Step 4: The fourth step is to configure the network ip-address wildcard-mask and area area-id. This is done by entering the command; *Router(config-router)# network 192.168.8.0 0.0.0.3 area 20*, where the network address is 192.168.8.0, wildcard mask is *0.0.0.3 and* area number is 20. This defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5: The fifth step is to end the configuration process by entering the command *Router(config-router)# end*. The command exits router configuration mode and returns to privileged EXEC mode.

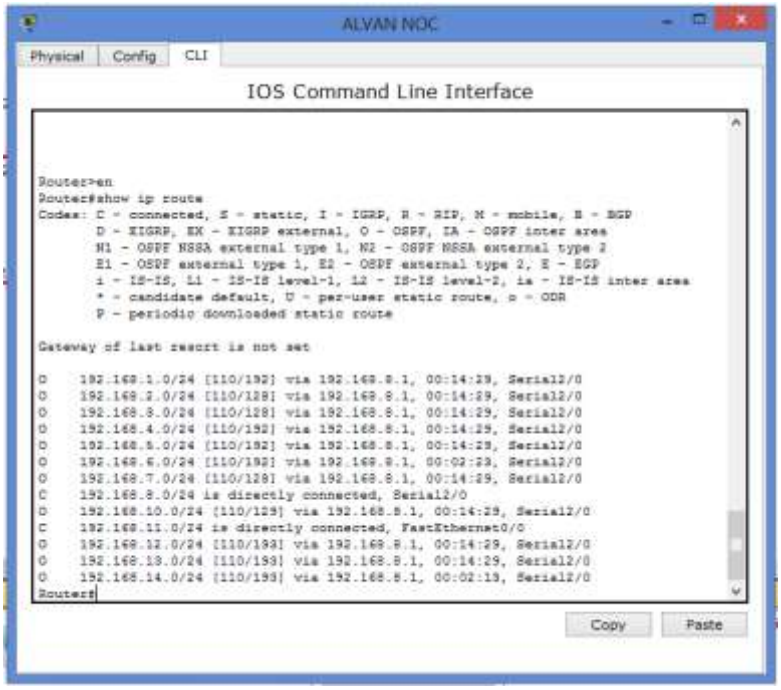

Figure 4.26: ALVAN NOC OSPF Router Configuration Output

Figure 4.26 shows screen shots of the working of OSPF routing protocol on the ALVAN NOC router which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter O shows that the router is connected to the other networks using OSPF. The lines with C indicates that those networks are directly connected to the router under consideration.

5) **OSPF Router configuration for UAES NOC**: The UAES NOC (network operations center) router is configured with OSPF using the following command line:

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 192.168.4.0 0.0.0.3 area 20
Router(config-router)# end

Step 1: The first step is to run the enable command. This is done by entering the command *Router> enable*. This command enables the privileged EXEC mode. On

entering the command, the user will be prompted to enter the network password if enabled.

Step 2: The second step is to configure the router terminal. This is done by entering the command *Router# configure terminal.* This command is used to enter the global configuration mode.

Step 3: The third step is to configure the router ospf *process-id.* This is achieved by entering the command; *Router(config)# router ospf 1*. This command enables OSPF routing and enters router configuration mode.

Step 4: The fourth step is to configure the network ip-address wildcard-mask and area area-id. This is done by entering the command; *Router(config-router)# network 192.168.4.0 0.0.0.3 area 20*, where the network address is 192.168.4.0, wildcard mask is *0.0.0.3 and* area number is 20. This defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5: The fifth step is to end the configuration process by entering the command *Router(config-router)# end*. The command exits router configuration mode and returns to privileged EXEC mode.

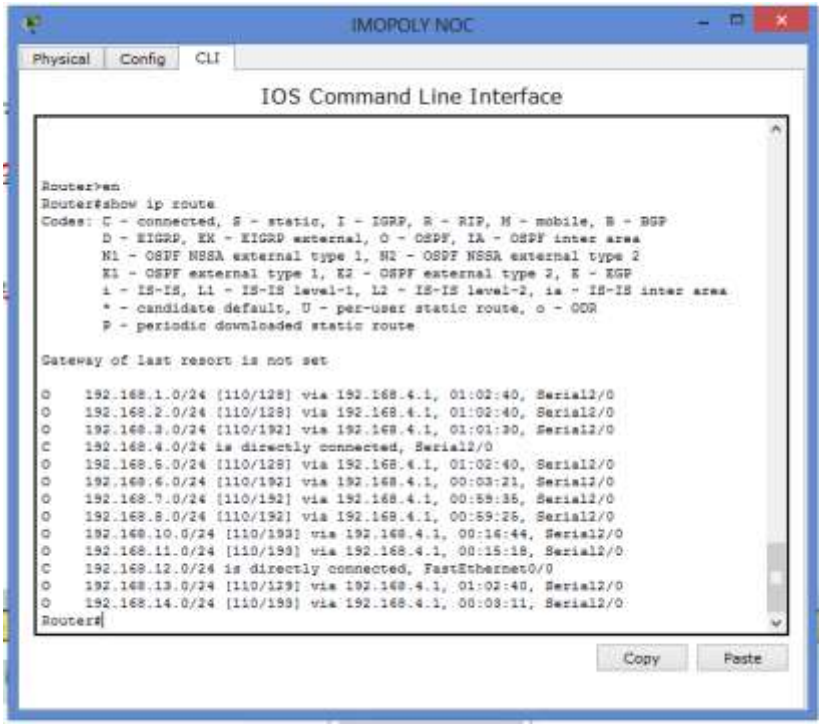

Figure 4.27: UAES NOC OSPF Router Configuration Output

Figure 4.27 shows screen shots of the working of OSPF routing protocol on the UAES NOC router which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter O shows that the router is connected to the other networks using OSPF. The lines with C indicates that those networks are directly connected to the router under consideration.

6) **OSPF Router configuration for XCHP R3 NOC**: The XCHP R3 NOC (network operations center) router is configured with OSPF using the following command line:

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.1 0.0.0.3 area 20
Router(config-router)# end

Step 1: The first step is to run the enable command. This is done by entering the command *Router> enable*. This command enables the privileged EXEC mode. On entering the command, the user will be prompted to enter the network password if enabled.

Step 2: The second step is to configure the router terminal. This is done by entering the command *Router# configure terminal.* This command is used to enter the global configuration mode.

Step 3: The third step is to configure the router ospf *process-id.* This is achieved by entering the command; *Router(config)# router ospf 1*. This command enables OSPF routing and enters router configuration mode.

Step 4: The fourth step is to configure the network ip-address wildcard-mask and area area-id. This is done by entering the command; *Router(config-router)# network 192.168.1.1 0.0.0.3 area 20,* where the network address is 192.168.1.1, wildcard mask is *0.0.0.3 and* area number is 20. This defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5: The fifth step is to end the configuration process by entering the command *Router(config-router)# end*. The command exits router configuration mode and returns to privileged EXEC mode.

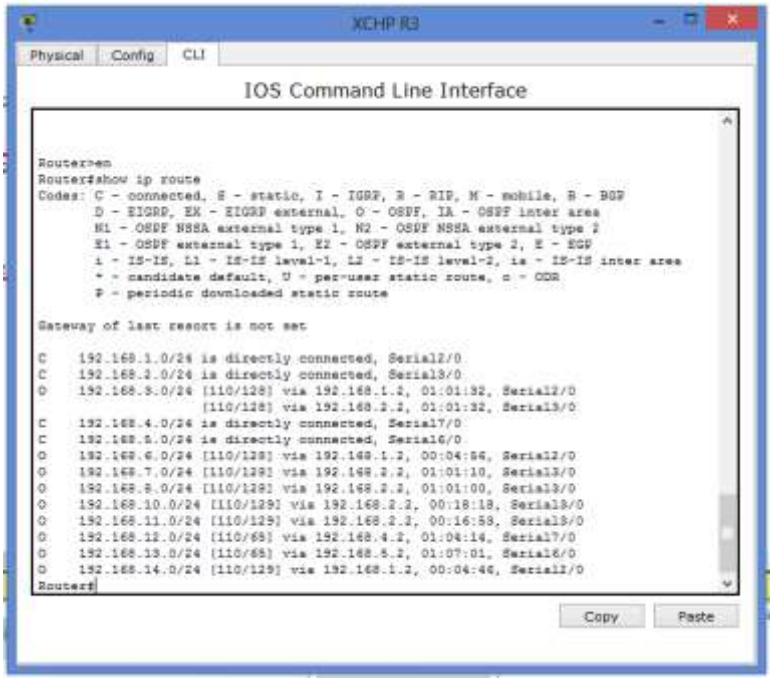

Figure 4.28: XCHP R3 NOC OSPF Router Configuration Output

Figure 4.28 shows screen shots of the working of OSPF routing protocol on the XCHP R3 NOC router which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter O shows that the router is connected to the other networks using OSPF. The lines with C indicates that those networks are directly connected to the router under consideration.

7) **OSPF Router configuration for XCHP R2 NOC**: The XCHP R2 NOC (network operations center) router is configured with OSPF using the following command line:

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.2 0.0.0.3 area 20
Router(config-router)# end

Step 1: The first step is to run the enable command. This is done by entering the command *Router> enable*. This command enables the privileged EXEC mode. On

entering the command, the user will be prompted to enter the network password if enabled.

Step 2: The second step is to configure the router terminal. This is done by entering the command *Router# configure terminal.* This command is used to enter the global configuration mode.

Step 3: The third step is to configure the router ospf *process-id.* This is achieved by entering the command; *Router(config)# router ospf 1*. This command enables OSPF routing and enters router configuration mode.

Step 4: The fourth step is to configure the network ip-address wildcard-mask and area area-id. This is done by entering the command; *Router(config-router)# network 192.168.1.2 0.0.0.3 area 20*, where the network address is 192.168.1.2, wildcard mask is *0.0.0.3 and* area number is 20. This defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5: The fifth step is to end the configuration process by entering the command *Router(config-router)# end*. The command exits router configuration mode and returns to privileged EXEC mode.

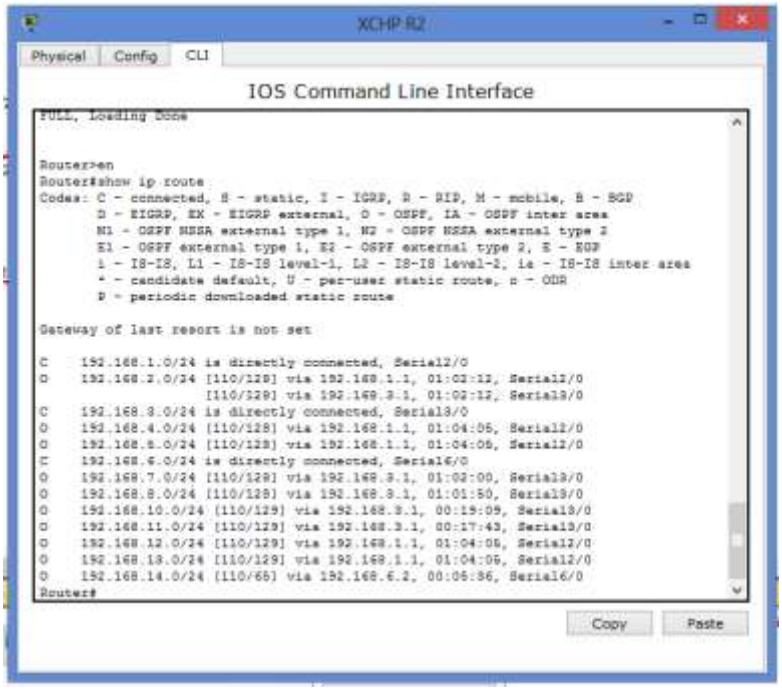

Figure 4.29: XCHP R2 NOC OSPF Router Configuration Output

Figure 4.29 shows screen shots of the working of OSPF routing protocol on the XCHP R2 NOC router which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter O shows that the router is connected to the other networks using OSPF. The lines with C indicates that those networks are directly connected to the router under consideration.

8) **OSPF Router configuration for XCHP R1 NOC**: The XCHP R1 NOC (network operations center) router is configured with OSPF using the following command line:

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# network 192.168.2.2 0.0.0.3 area 20
Router(config-router)# end

Step 1: The first step is to run the enable command. This is done by entering the command *Router> enable*. This command enables the privileged EXEC mode. On

entering the command, the user will be prompted to enter the network password if enabled.

Step 2: The second step is to configure the router terminal. This is done by entering the command *Router# configure terminal.* This command is used to enter the global configuration mode.

Step 3: The third step is to configure the router ospf *process-id.* This is achieved by entering the command; *Router(config)# router ospf 1*. This command enables OSPF routing and enters router configuration mode.

Step 4: The fourth step is to configure the network ip-address wildcard-mask and area area-id. This is done by entering the command; *Router(config-router)# network 192.168.2.2 0.0.0.3 area 20*, where the network address is 192.168.2.2, wildcard mask is *0.0.0.3 and* area number is 20. This defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5: The fifth step is to end the configuration process by entering the command *Router(config-router)# end*. The command exits router configuration mode and returns to privileged EXEC mode.

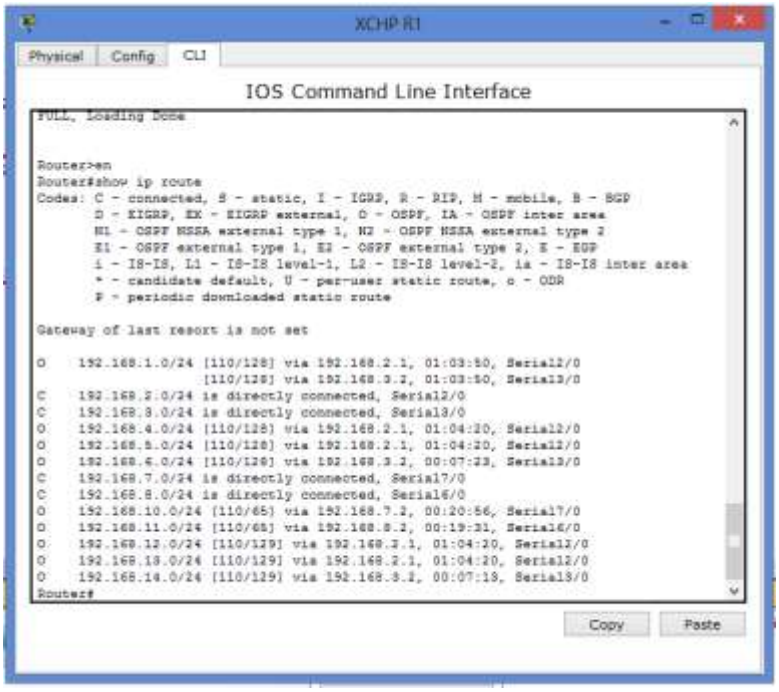

Figure 4.30: XCHP R1 NOC OSPF Router Configuration Output

Figure 4.30 shows screen shots of the working of OSPF routing protocol on the XCHP R1 NOC router which is one of the eight routers that make up the internet exchange point network for the 5 campuses under consideration. The letter O shows that the router is connected to the other networks using OSPF. The lines with C indicates that those networks are directly connected to the router under consideration.

Figure 4.23 to 4.30 shows screenshots of the working of OSPF routing protocol on the eight routers that make up the internet exchange point network for the 5 campuses under consideration.

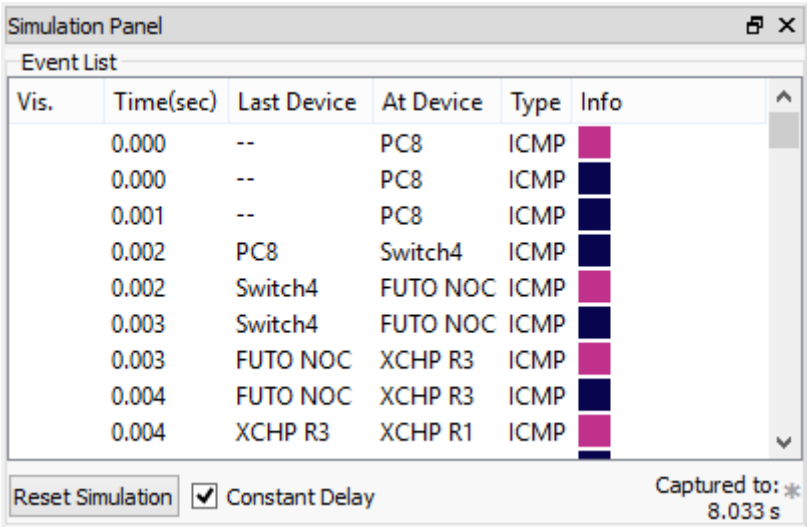

Figure 4.31: EIGRP Simulation Results

Figure 4.31 shows the simulation results for OSPF capturing ICMP packets over a 8.033seconds period. The simulation results show OSPF reporting time between nodes ranging between 7.116 and 8.005seconds.

Table 4.1 shows the connection time of the three routing protocols used on the exchange point network at a TTL value of 24 and packet size of 32 bytes. The simulation was monitored over a period of 2minutes.

Table 4.1: Simulation Output of Connection for RIP, EIGRP and OSPF

Simulation time	**Time (ms) [@ TTL=24 and PKT=32]**		
	RIP	**EIGRP**	**OSPF**
6	5	20	3
12	4	3	9
18	3	4	4
24	3	3	5
30	3	3	13
36	3	4	10
42	5	3	3
48	4	3	3
54	3	4	4
60	7	12	3
66	3	3	17
72	3	11	3
78	3	4	3

84	4	17	16
90	3	5	7
96	3	3	5
102	3	10	4
108	3	10	3
114	6	3	11
120	3	3	3

The graph shown in Figure 4.32 shows the behaviours of the various routing protocols used for the simulation.

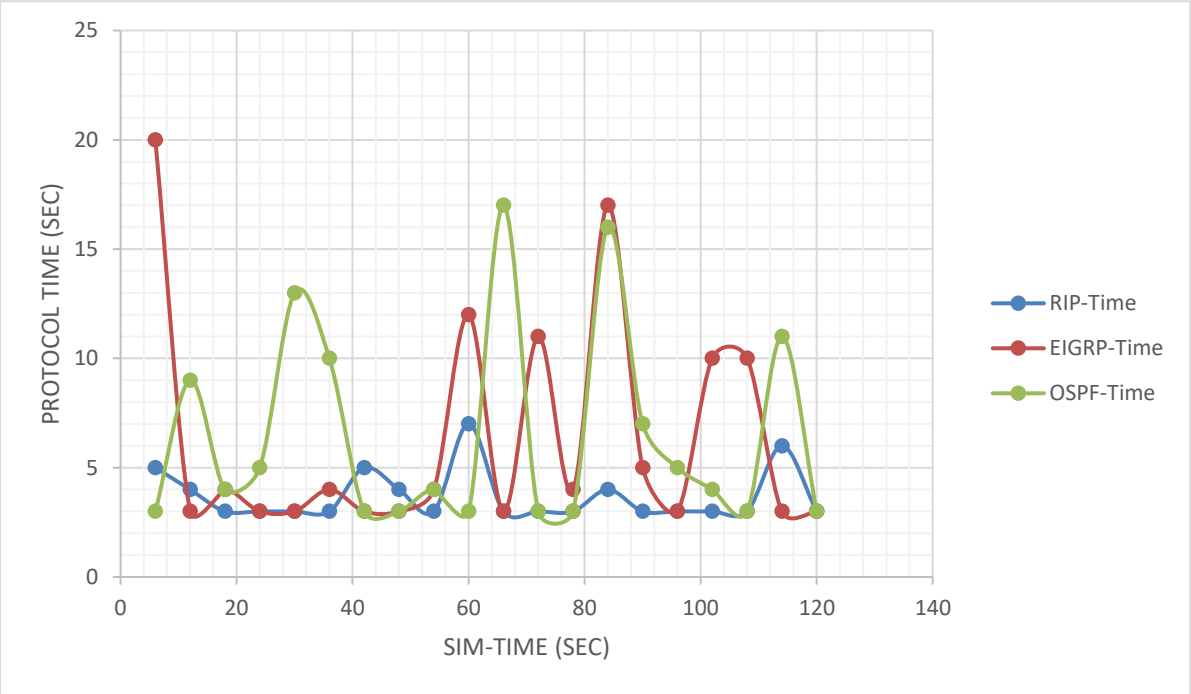

Figure 4.32: Graph Showing the Protocol Time for RIP, EIGRP and OSPF.

4.5 Discussion of Results

Form the results gotten from the simulation process, the following can be deduced:

1. RIP as a routing protocol to be used for the exchange point network provides a convergence time that is within 3 and 4 seconds, with slightly varied spikes of not up to 10 seconds.

2. OSPF and EIGRP also tries to maintain a time of between 3 and 4 seconds but is plagued with so much spikes of up 20 seconds for EIGRP and 17seconds for OSPF.
3. From the graph, it can be clearly deduced that with a routing protocol like RIP connections between the campuses via the exchange point will converge faster.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Implementing a functional internetwork is no simple task. Many challenges must be faced, especially in the areas of configuration, connectivity, reliability, network management, and flexibility. Each area is key in establishing an efficient and effective internetwork.

The challenge when connecting various systems is to support communication among disparate technologies. Different sites, for example, may use different types of media operating at varying speeds, or may even include different types of systems that need to communicate.

Because institutions rely heavily on data communication, internetworks must provide a certain level of reliability. This is an unpredictable world, so many large internetworks include redundancy to allow for communication even when problems occur. Redundancy provided could be an additional link or a special kind of link as proposed in this work; the internet exchange point.

The ICCNS is a reliable, easy to set up and cost-effective redundant link for institutions. The ICCNS points simply help the various campuses share resources when it is necessary and also balance load as they are funded from the same source in this case the government.

Furthermore, network management must provide centralized support and troubleshooting capabilities in an internetwork. Configuration, security, performance, and other issues must be adequately addressed for the internetwork to function smoothly.

Because nothing in this world is stagnant, internetworks must be flexible enough to change with new demands.

This work will provide, to network engineers, a guide for network design and configuration within campus environment, paying attention to network efficiency. It pays attention to equipment, topology and protocol in the design and deployment of network in campuses. This work also provides a guide to institution administrators and the government to help check the quality of infrastructure being deployed by contractors in our tertiary learning environment.

From the results gotten it is clear that to get the best out of an inter campus network system connecting campuses with limited number of nodes, RIP is the best bet, with a convergence time ranging mainly between 3 and 4 seconds.

5.2 Recommendations

The following are the recommendations from this work:

1. There is an urgent need for government and institution managers to look into the data need of their schools. Access to the internet is very critical for leaning as staff and student rely heavily on it to learn and carry out research.
2. Since funding public institutions is carried out by the government, it is very necessary to start looking at cutting internet subscription cost by integrating exchange points at state levels where institutions cluster.
3. Campus networks should be designed using proper design standards and their topology properly documented. One of such standards which is also very popular is the 3-layer hierarchical structure.

5.3 Contribution to Knowledge

The following are the contribution of this research:

1. Provided a design model that enables campuses share resources over an inter campus cloud network thereby minimizing link downtime.

2. Provided the best routing protocol for an intercampus network using the convergence time approach.
3. Introduced the use of an exchange point design for an intercampus wide network thereby minimizing cost for individual campus link and maximizing resources usage.

5.4 Future Work

Security within an internetwork is essential. Many people think of network security from the perspective of protecting the private network from outside attacks. However, it is just as important to protect the network from internal attacks, especially because most security breaches come from inside. Networks must also be secured so that the internal network cannot be used as a tool to attack other external sites. Research in the area of security an exchange point network is necessary for reliability and sustainability. Early in the year 2000, many major web sites were the victims of distributed denial of service (DDOS) attacks. These attacks were possible because a great number of private networks currently connected with the Internet were not properly secured. These private networks were used as tools for the attackers.

We also recommend that some other protocols should be explored and other simulation packages like GNS3, Opnet, and OmNet can be used to compare values.

REFERENCES

Abdeen, M. A. R., Beg, A., Mostafa, S. M., Abdulghaffar, A., Sheltami, T. R., & Yasar, A. (2022). Performance Evaluation of VANET Routing Protocols in Madinah City. *Electronics (Switzerland)*, *11*(5). https://doi.org/10.3390/electronics11050777

Abdulle, A. A., Ali, A. F., & Abdullah, R. H. (2022). Cost-Benefit Analysis of Public Cloud Versus In-House Computing. *International Journal of Engineering Trends and Technology*, *70*(6). https://doi.org/10.14445/22315381/IJETT-V70I6P231

Aleem, S., Ahmed, F., Batool, R., & Khattak, A. (2021). Empirical Investigation of Key Factors for SaaS Architecture. *IEEE Transactions on Cloud Computing*, *9*(3). https://doi.org/10.1109/TCC.2019.2906299

Alghamdi, T. A. (2020). Energy efficient protocol in wireless sensor network: optimized cluster head selection model. *Telecommunication Systems*, *74*(3). https://doi.org/10.1007/s11235-020-00659-9

Amadi, E. (2014). *Fundamental of Computer Networks and Server Management: A Biginners Guide*.

Beevi, S. Z., & Alabdulatif, A. (2022). Optimal routing protocol for wireless sensor network using genetic fuzzy logic system. *Computers, Materials and Continua*, *70*(2). https://doi.org/10.32604/cmc.2022.020292

Ben Hamida, E., & Javed, M. A. (2016). Channel-aware ECDSA signature verification of basic safety messages with K-means clustering in VANETs. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, *2016-May*. https://doi.org/10.1109/AINA.2016.51

Benefa, C. (2015). Optimal Routing Protocol for Inter – Campus Network System (ICNS). *PGD Thesis*.

Benkerdagh, S., & Duvallet, C. (2019). Cluster-based emergency message dissemination strategy for VANET using V2V communication. *International Journal of Communication Systems*, *32*(5). https://doi.org/10.1002/dac.3897

Carson, S., & Macker, J. (1999). *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*.

Chakroun, R., Abdellatif, S., & Villemur, T. (2022). LAMD: Location-based Alert Message Dissemination scheme for emerging infrastructure-based vehicular networks. In *Internet of Things (Netherlands)* (Vol. 19). https://doi.org/10.1016/j.iot.2022.100510

Chi, Y., Dai, W., Fan, Y., Ruan, J., Hwang, K., & Cai, W. (2021). Total cost ownership optimization of private clouds: a rack minimization perspective. *Wireless Networks*. https://doi.org/10.1007/s11276-021-02757-1

Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR) (No. RFC 3626)*.

Cloudflare. (2019). What is The OSI Model | Cloudflare. *Cloudflare*.

El Alami, H., & Najid, A. (2015). SEFP: A new routing approach using fuzzy logic for clustered heterogeneous wireless sensor networks. *International Journal on Smart Sensing and Intelligent Systems*, *8*(4). https://doi.org/10.21307/ijssis-2017-854

Froehlich, A., Rosencrance, L., & Gattine, K. (2021). What is the OSI model? The 7 layers of OSI explained. In *Tech Target*.

Ganie, A. G. (2021). Private network optimization. *Multidiszciplináris Tudományok*, *11*(4). https://doi.org/10.35925/j.multi.2021.4.29

Gopalakrishnan, P., & Uma Maheswari, B. (2019). Research on enterprise public and private cloud service. *International Journal of Innovative Technology and Exploring Engineering*, *8*(6 Special Issue 4). https://doi.org/10.35940/ijitee.F1296.0486S419

Himawan, H., Hassan, A., & Bahaman, N. A. (2022). Performance Analysis of Communication Model on Position Based Routing Protocol: Review Analysis. In *Informatica (Slovenia)* (Vol. 46, Issue 6). https://doi.org/10.31449/inf.v46i6.4024

Hosseini Shirvani, M., Amin, G. R., & Babaeikiadehi, S. (2022). A decision framework for cloud migration: A hybrid approach. *IET Software*, *16*(6). https://doi.org/10.1049/sfw2.12072

Akila I. S., Manisekaran V. S., & Venkatesan R. (2017). *Modern clustering techniques in wireless security networks for wireless sensor networks insights and innovation*. http://www.intechopen.com//books.

Kim, T., Lee, S., Kim, K. H., & Jo, Y. Il. (2023). FANET Routing Protocol Analysis for Multi-UAV-Based Reconnaissance Mobility Models. *Drones*, *7*(3). https://doi.org/10.3390/drones7030161

Manzoor, A., Hussain, M., & Mehrban, S. (2020). Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols. *Computer Standards and Interfaces*, *68*. https://doi.org/10.1016/j.csi.2019.103391

Mazzola, F., Marcos, P., Castro, I., Luckie, M., & Barcellos, M. (2022). On the Latency Impact of Remote Peering. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13210 LNCS*. https://doi.org/10.1007/978-3-030-98785-5_16

Mehdi, R. A. K., & Nachouki, M. (2020). Cost optimization of procuring cloud computing resources using genetic algorithms. *Journal of Theoretical and Applied Information Technology*, *98*(8).

Mosavvar, I., & Ghaffari, A. (2019). Data Aggregation in Wireless Sensor Networks Using Firefly Algorithm. *Wireless Personal Communications*, *104*(1). https://doi.org/10.1007/s11277-018-6021-x

Mudhoep, D. I., Linawati, & Oka Saputra. (2021). Kombinasi Protokol Routing OSPF dan BGP dengan VRRP, HSRP, dan GLBP. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi*, *10*(1). https://doi.org/10.22146/jnteti.v10i1.942

Muhairat, M., Abdallah, M., & Althunibat, A. (2019). Cloud computing in higher educational institutions. *Compusoft*, *8*(12), 3507–3513. https://doi.org/10.6084/IJACT.V8I12.964

Nurwarsito, H., & Sindunata, A. R. (2020). Optimization of hello interval in OSPF routing protocol performance on mesh network topology. *EECCIS 2020 - 2020 10th Electrical Power, Electronics, Communications, Controls, and Informatics Seminar*. https://doi.org/10.1109/EECCIS49483.2020.9263434

Priyambodo, T. K., Wijayanto, D., & Gitakarma, M. S. (2021). Performance optimization of MANET networks through routing protocol analysis. *Computers*, *10*(1). https://doi.org/10.3390/computers10010002

Räcke, H. (2002). Minimizing congestion in general networks. *Annual Symposium on Foundations of Computer Science - Proceedings*. https://doi.org/10.1109/sfcs.2002.1181881

Rocha, A. L. B., Cesila, C. H., Maciel, P. D., Correa, S. L., Rubio-Loyola, J., Rothenberg, C. E., & Verdi, F. L. (2022). CNS-AOM: Design, Implementation and Integration of an Architecture for Orchestration and Management of Cloud-Network Slices. *Journal of Network and Systems Management*, *30*(2). https://doi.org/10.1007/s10922-022-09641-z

Saini, A. S., Gupta, P., & Gupta, H. (2021). Implementation of Secured Wired and WLAN Network Using eNSP. *Lecture Notes in Electrical Engineering*, *721 LNEE*. https://doi.org/10.1007/978-981-15-9938-5_54

Shah, M. A., Khan, F. Z., & Abbas, G. (2022). A Robust Emergency Messages Routing Scheme for Urban VANETs. *Computers, Materials and Continua*, *72*(2). https://doi.org/10.32604/cmc.2022.025981

Shah, M. A., Zeeshan Khan, F., Abbas, G., Abbas, Z. H., Ali, J., Aljameel, S. S., Khan, I. U., & Aslam, N. (2022). Optimal Path Routing Protocol for Warning Messages Dissemination for Highway VANET. *Sensors*, *22*(18). https://doi.org/10.3390/s22186839

Shah, S. S., Malik, A. W., Rahman, A. U., Iqbal, S., & Khan, S. U. (2019). Time Barrier-Based Emergency Message Dissemination in Vehicular Ad-hoc Networks. *IEEE Access*, *7*. https://doi.org/10.1109/ACCESS.2019.2895114

Singla, R., Kaur, N., Koundal, D., & Bharadwaj, A. (2022). Challenges and Developments in Secure Routing Protocols for Healthcare in WBAN: A Comparative Analysis. In

Wireless Personal Communications (Vol. 122, Issue 2). https://doi.org/10.1007/s11277-021-08969-0

Syahputra, R., Rahmadi Kurnia, & Rian Ferdian. (2020). Analisis Perancangan dan Implementasi FHRP di Protokol Routing RIPv2 dan OSPF. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(1).

Syamsuddin, I., Prabuwono, A. S., Basori, A. H., & Yunianta, A. (2021). Review on OwnCloud Features for Private Cloud Data Center. *TEM Journal*, *10*(2). https://doi.org/10.18421/TEM102-59

Taleb, N., & Mohamed, E. A. (2020). Cloud computing trends: A literature review. In *Academic Journal of Interdisciplinary Studies* (Vol. 9, Issue 1). https://doi.org/10.36941/ajis-2020-0008

Tan, X., Zuo, Z., Su, S., Guo, X., Sun, X., & Jiang, D. (2020). Performance Analysis of Routing Protocols for UAV Communication Networks. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2995040

Telesis, A. (2016). *Allied Telesis Enterprise Networking Solutions*.

Thilagam, T., & Aruna, R. (2021). Intrusion detection for network based cloud computing by custom RC-NN and optimization. *ICT Express*, *7*(4). https://doi.org/10.1016/j.icte.2021.04.006

Thomas, A. (2002). *Hardening Cisco Routers* (J. Sumser, Ed.). O'Reilly and Associates Inc.

Tricomi, G., Merlino, G., Panarello, A., & Puliafito, A. (2020). Optimal selection techniques for cloud service providers. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.3035816

Ullah, S., Abbas, G., Waqas, M., Abbas, Z. H., Tu, S., & Hameed, I. A. (2021). Eemds: An effective emergency message dissemination scheme for urban vanets. *Sensors*, *21*(5). https://doi.org/10.3390/s21051588

Vakaliuk, T., Chyzhmotria, O., Chyzhmotria, O., Antoniuk, D., Kontsedailo, V., & Kryvohyzha, V. (2023). *Simulator of Computer Networks and Basic Network Protocols*. https://doi.org/10.5220/0012009800003561

Weins, K. (2020). *Cloud Computing Trends: 2020 State of the Cloud Report*. Flexera. https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/

Xu, R., & Wunsch, D. (2005). Survey of clustering algorithms. In *IEEE Transactions on Neural Networks* (Vol. 16, Issue 3). https://doi.org/10.1109/TNN.2005.845141

Xu, S., Yang, G., Ren, J., Wang, S., & Wang, X. (2020). Routing optimization for cloud services in SDN-based Internet of Things with TCAM capacity constraint. *Journal of Communications and Networks*, *22*(2). https://doi.org/10.1109/JCN.2020.000006

Yekkehkhany, A., & Nagi, R. (2022). Risk-Averse Equilibria for Vehicle Navigation in Stochastic Congestion Games. *IEEE Transactions on Intelligent Transportation Systems*, *23*(10). https://doi.org/10.1109/TITS.2022.3166880

Zhao, F., Han, Z., Cheng, D., Mao, N., Chen, X., Li, Y., Fan, D., & Liu, P. (2022). Hierarchical Synchronization Estimation of Low- and High-Order Functional Connectivity Based on Sub-Network Division for the Diagnosis of Autism Spectrum Disorder. *Frontiers in Neuroscience*, *15*. https://doi.org/10.3389/fnins.2021.810431