SCALABILITY EVALUATION AND IMPROVEMENT IN IP-BASED CAMPUS NETWORKS: A CASE STUDY OF AHMADU BELLO UNIVERSITY ZARIA NETWORK

By

BASHIR HALLIRU SANI

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
FACULTY OF ENGINEERING
AHMADU BELLO UNIVERSITY ZARIA, NIGERIA

November, 2016

SCALABILITY EVALUATION AND IMPROVEMENT IN IP-BASED CAMPUS NETWORKS: A CASE STUDY OF AHMADU BELLO UNIVERSITY ZARIA NETWORK

By

Bashir Halliru SANI, B.Eng. (ABU) 2008

P15EGCP8020

bashkhid@yahoo.com

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES,

AHMADU BELLO UNIVERSITY, ZARIA

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF A

MASTER OF SCIENCE (MSc) DEGREE IN COMPUTER ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

FACULTY OF ENGINEERING

AHMADU BELLO UNIVERSITY, ZARIA

NIGERIA

November, 2016

DECLARATION

I Bashir Halliru SANI declare that the work in this dissertation entitled "**Scalability Evaluation and Improvement in IP-Based Campus Networks: A Case Study of Ahmadu Bello University Zaria Network**" has been carried out by me in the Department of Electrical and Computer Engineering, Ahmadu Bello University Zaria. The information derived from the literature has been duly acknowledged in the text and a list of references provided. No part of this dissertation was previously presented for another degree or diploma at this or any other institution.

Bashir Halliru SANI	____________________	_________________
	Signature	Date

CERTIFICATION

This dissertation entitled "**SCALABILITY EVALUATION AND IMPROVEMENT IN IP-BASED CAMPUS NETWORKS: A CASE STUDY OF AHMADU BELLO UNIVERSITY ZARIA NETWORK**" by Bashir Halliru SANI meets the regulations governing the award of the Master of Science (M.Sc.) degree in Computer Engineering in Ahmadu Bello University, and is approved for its contribution to knowledge and literary presentation.

Prof. M.B. Mu'azu
Chairman, Supervisory Committee
__________________ __________________
Signature Date

Dr. S. Garba
Member, Supervisory Committee
__________________ __________________
Signature Date

Dr. Y. Jibril
Head of Department
__________________ __________________
Signature Date

Prof. Kabir Bala
Dean, School of Postgraduate Studies
__________________ __________________
Signature Date

DEDICATION

This research work is dedicated to Almighty Allah (S.W.T) for his guidance, kindness, mercy and sympathy and to my lovely parents for their tireless prayers and support. May Allah reward them with Jannatul Firdausi. Amin.

ACKNOWLEDGEMENT

I am grateful to Almighty Allah (S.W.T) for sparing my life to finish this research work successfully.

I appreciate my lovely parents; Alhaji Halliru Sani Bawale and Hajiya Fatima Al-Mustapha for their support, prayers and otherwise, also to my late step mother Hajiya Mariya Sani Bakori. May Allah bless her with Jannatul Firdausi, Amin. I appreciate the support of my uncle and role model Muhammad Bashir Sani for his encouragement, guidance and motivations.

I am most grateful to the chairman of my supervisor committee, Prof. M.B. Muazu who patiently and tirelessly motivated and guided me through this work; he is not just my teacher but also my mentor and role model, I also thank my co-supervisor and teacher, Dr. S. Garba for his support and encouragement. To my mentor, Prof. B.J. Bajoga, I say a big thank you for your patience and time for going through my manuscripts.

I extend my profound gratitude to my Lovely wife Hajiya Zeenat Isah Umar for her encouragement, patience, support and prayers, and also to my siblings Suleiman, Sani, Mustapha, Ibrahim, Abubakar, Nura, Abdullahi, Abdulrahman, Ahmad, Aminu, Buhari, Faruk, Aliyu, Sa'adiya, Aisha, Hadiza, Hauwa, Fatima, Bilkisu, Zainab, Hafsat, and Jafar.

I am grateful to all my lecturers, colleagues and friends; Dr. Y. Jibril, Dr. A.M.S. Tekanyi, Dr. K.A. Abu-Bilal, Dr. A. Adewale, Dr. S.M. Sani, Ibrahim Sani, Ibrahim Umar, Jameelu Abdulhameed, Engr. Muhammad Abdullahi, Engr. Yusuf Abdullahi, Engr. Ibrahim Ladan, Engr. M Ali, Nura Haruna and all those whose names are not captured here.

ABSTRACT

This research presents the design and configuration of Multi-Protocol Label Switching (MPLS) technology to address scalability issues on a large and complex campus network such as Ahmadu Bello University campus network that is currently designed, configured and implemented with Open Shortest Path First Protocol (OSPF) network. Graphical Network Simulator (GNS3) was used to model and emulate the campus network to identify areas most vulnerable to scalability issues. The network was redesigned and configured with MPLS technology, which showed significant improvement in the speed of CPU, RAM, and link utilizations of the routers and switches as the network resources were accessed. The network was also modeled in OPNET modeler with OSPF and then with MPLS to verify the results obtained using GNS3. The models were configured with network services such as File Transfer Protocol (FTP), Web, e-mail, voice and video traffic. Traffics were generated at peak hours and data was collected for performance metrics; throughput, delay (end-to-end and queuing), and jitter. The results obtained during the simulation showed that MPLS-Based network have higher throughput from 4,000 (bps) to 81,000 (bps) compared with OSPF network from 3,000 (bps) to 41,000 bps, lower end-to-end delay from 0.0000019 to 0.0000050s compared with 0.000002s to 0.0000092s, lower queuing delay from 0.00002s to 0.000074s compared with 0.000045s to 0.000084s, lower jitter from 0.00005s to 0.0004s compared with 0.00005s to 0.00080s, lower server load of 250,000,000 (bits/sec) compared with 790,000,000 (bits/sec). The validation, based on the developed and simulated configuration was carried out using live routers and switches and the results showed an average reduction of Central Processing Unit (CPU) utilization from about 97.5% for OSPF-based network to about 37% for MPLS-based network, and reduction of Random Access Memory (RAM) utilization from 97% for OSPF-based network to 32% for MPLS-network, there was also reduction in link utilization from 80% for OSPF-based network to 19% for MPLS-based network. The results obtained using MPLS-based network design showed that MPLS network provided more scalable and efficient solution than conventional OSPF network even with the addition of more network services, network devices or end users.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF PLATES

LIST OF ABBREVIATIONS

Acronyms	Definition
ABU	Ahmadu Bello University
ATM	Asynchronous Transfer Mode
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BPDUs	Bridge Protocol Data Units
CE	Customer Edge
CPU	Central Processing Unit
CR-LDP	Constraint-based Routing Label Distribution Protocol
DCDN	Distributed Content Delivery Network
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DoD	Department of Defense
DR	Designated Router
DVMRP	Distance Vector Multicast Routing Protocol
ECMP	Equal-cost multi-path routing
EIGRP	Enhanced Interior Gateway Routing Protocol
FEC	Forward Equivalent Class
FIB	Forward Information Base
FRR	Fast Re-Route
FTP	File Transfer Protocol
GNS3	Graphical Network Simulator version 3
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
IACC	Iya Abubakar Computer Center
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force

IGP	Interior Gateway Protocol
IOS	Internetwork Operating System
IPv6	Internet Protocol version Six
IS-IS	Intermediate System - Intermediate System
ISP	Internet Service Providers
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LIB	Label Information Based
LSA	Link State Advertisement
LSP	Label Switched Path
LSR	Label Switch Router
MKCL	Mamman Kontagora Computer Laboratory
MLTU	MultibitTrie Lookup Table Update
MOSPF	Multicast Open Shortest Path First
MPLS	Multi-Protocol Label Switching
MPLS-TE	Multi-Protocol Label Switching - Traffic Engineering
MST	Multiple Spanning Tree
NGN	Next Generation Network
NgREN	Nigerian Research Education Network
OPNET	Optimized Network Engineering Tool
OSI	Open System Interconnect
OSPF	Open Shortest Path First
PDV	Packet Delay Variation
PE	Provider Edge
PIM-DM	Protocol Independent Multicast - Dense Mode
PIM-SM	Protocol Independent Multicast - Sparse Mode
QoS	Quality of Service

RAM	Random Access Memory
RIP	Routing Information Protocol
RPVST+	Rapid Per VLAN Spanning Tree Plus
RSVP	Resource Reservation Protocol
SPF	Shortest Path First
SSP	Single Shortest Path
STM-1	Synchronous Transport Module level-1
STP	Spanning Tree Protocol
TC	Topology Change
TCP/IP	Transmission Control Protocol/Internet Protocol
TRILL	Transparent Interconnection of Lots of Links
TTL	Time To Live
USP	Unique Shortest Path
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VPLS	Virtual Private LAN Services
VPN	Virtual Protocol Network

CHAPTER ONE

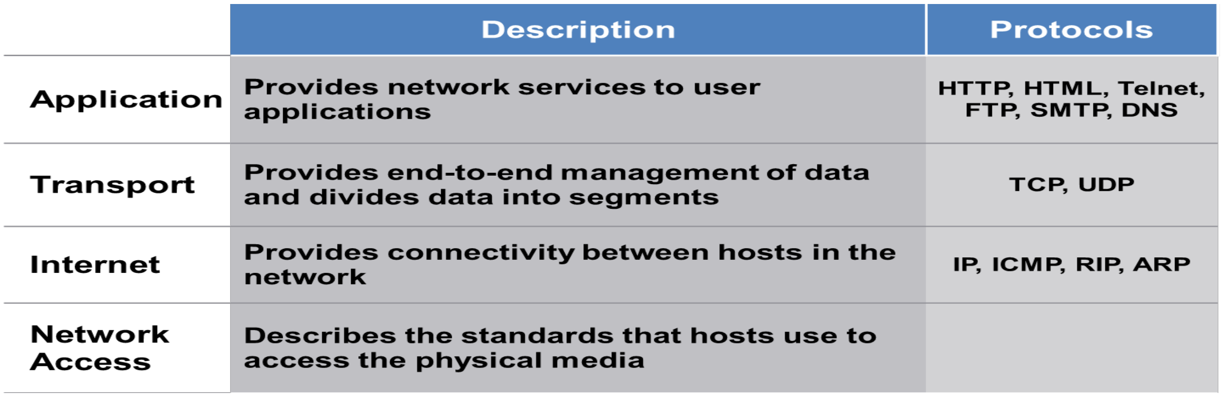
INTRODUCTION

1.1 BACKGROUND

Early computer networks carried continuous bit streams over physical links in a technique called circuit switching. This was well suited for transmitting voice or real time data from a single sender to a single receiver (Unicast communication). In this kind of network, a single physical link failure had dramatic consequences, leading to the interruption of all communications that was using the failed link, popularly known as circuit switched network (Andrew, 2011; Stallings, 2007).

The Internet today is a datagram packet-switched network that addressed the drawback of the circuit switched network by cutting data into small chunks called packets. These packets are individually routed through the network, such that two packets from the same communication network are individually handled in the network. Therefore, if a link fails, packets can be rerouted to avoid the failed link and communications are not interrupted, this feature of a packet switched network is called resilience because it hides network failure from the end users (Andrew, 2011; Stallings, 2007).

The Internet uses Transmission Control Protocol / Internet Protocol (TCP/IP) suites of protocols as in Figure 1.1 to transport traffic over the network and the Internet, this suite of protocols was designed by Department of Defense (DoD) from United States of America to ease communications between troops in the war field and later being adopted into all other means of communication and data sharing. Many protocols consist of a suite (or group) of protocols stacked into layers, these layers depend on the operation of the other layers in the suite to function properly. TCP/IP consists of four layers that perform functions necessary to prepare data for transmission over a network (Lammle, 2012).



	Description	Protocols
Application	Provides network services to user applications	HTTP, HTML, Telnet, FTP, SMTP, DNS
Transport	Provides end-to-end management of data and divides data into segments	TCP, UDP
Internet	Provides connectivity between hosts in the network	IP, ICMP, RIP, ARP
Network Access	Describes the standards that hosts use to access the physical media	

Figure 1.1: TCP/IP Reference Model (Lammle, 2012)

Campus network is a proprietary local area network (LAN) or set of interconnected LANs serving a corporation, government agency, university, or similar organization. It is usually administered by a single organization or individual, the administrative control that governs the security and access control policies are enforced on the network level, it also provides high speed bandwidth to internal end devices and intermediary devices. The need for constant reliable data delivery service leads to high demand for effective network resources, network elements such as applications, hosts, switches, routers or gateway devices should guarantee that network traffic should be routed more efficiently. It becomes increasingly essential to manage networks effectively and utilize network resources efficiently to fulfill the requirements of various Internet and network services (Lammle, 2012).

The speed, scalability and reliably of any campus network depends on the ability of the design to address some of the critical hardware like memory, CPU utilization and link utilization to have higher throughput, and minimize delays and jitter, this would be achieved with the selection of more scalable routing protocol. The network design and configuration should be done to take care of all the necessary parameters to provide a highly scalable network.

1.2 STATEMENT OF THE PROBLEM

ABU campus network was designed, configured, and implemented using both switching (layer-2) technologies at the network edge (Access layer) and routing (layer-3) technologies at the core (Distribution and Core layers). At layer-2, the network design is achieved by means of Virtual Local Area Networks (VLANs) and STP protocols, and layer-3 by means of routing protocols, which has some of the following limitations.

a) Impossibility to group services that span across the entire campus network such as confidential student records.

b) Lack of full implementation of the Spanning Tree Protocol (STP) on the network, this can lead to (STP) loops in a large campus network which can cause very high delays and frame duplications.

c) OSPF protocol has many redundancy issues as it uses metric calculation to over utilize or underutilize some links which can affect routing performance.

d) Poor IP Address Planning on the active devices which affects the performance of the hardware's CPU, RAM, and link utilization.

e) In the design, configuration and implementation of OSPF routing protocol on a campus network, poor IP address Planning will result into having a very large routing table in the routers and switches, which causes slower routing table lookup and tendency of routing loop.

1.3 AIMS AND OBJECTIVES

The aim of the research is the evaluation of the scalability robustness of the ABU campus network with a view to improving network performance.

The objectives of the research are then as follows:

a) Modeling and emulation/simulation of OSPF-based and proposed MPLS-based ABU Zaria campus network using GNS3 and evaluation of the scalability robustness of the modeled network based-on Layer-2 and Layer-3 technologies.

b) Development of configuration codes for all the routers and switches on the proposed MPLS-based network for improved performance.

c) Modeling and simulation of OSPF-based and proposed MPLS-based ABU Zaria campus network using OPNET Modeler based-on a); configuration of network services; FTP, Web, Email, Voice, and Video conferencing.

d) Analysis of the data generated in c) using performance metrics; throughput, end-to-end delay, queuing delay, jitter, and server load.

e) Validation of b) above using live routers and switches.

1.4 METHODOLOGY

In order to actualize the objectives of the research, the following methodology is adopted:

a) MPLS as a scalable network design solution was selected and emulated/simulated the ABU Campus network for improved performance.

b) ABU Zaria Campus Network was designed, configured and emulated using GNS3 emulator to identify possible scalability issues that affect the performance of network hardware components such as CPU, memory, and link utilization due to lack full implementation layer-2 and layer-3 technologies.

c) ABU Zaria Campus network was redesigned, configured and emulated using GNS3 emulator using the MPLS technology which was implemented to address the scalable issues in (b) and achieve optimum network resources utilization.

d) ABU Campus network topology was replicated from GNS3 emulator to OPNET modeler based-on (b), FTP, Web, Email, Voice, and Video conferencing network services were configured and simulated to test the capability and efficiency of the hardware components in handling all the traffic at the same time.

e) ABU Campus network topology was replicated from GNS3 emulator to OPNET modeler based-on (c), MPLS technology solution was configured and simulated to address the scalability issues and achieve optimum network resources utilization.

f) Using the simulated network model in (d), and (e), data was generated for throughput, end-to-end delay, queuing delay, jitter, and server load as the performance metrics and compared.

g) The improved designed solution was validated using live routers, and multi-layer switches.

1.5 DISSERTATION ORGANIZATION

The general introduction of computer networks, statement of the problem, methodology, and aims and objectives has been presented in chapter one. The rest of the chapters are presented as follows: a detailed review of the fundamental concepts of IP address technology, Open Shortest Path First Protocol (OSPF), Multi-Protocol Label Switching (MPLS), OPNET Modeler, GNS3 as well as a review of similar research works is presented in chapter two, detailed Abu campus network, and step by step guide in the configuration and implementations of ABU campus network and proposed solution design model are presented in chapter three, analysis and discussions of the results are presented in chapter four, summary, conclusions, significant contributions, limitations and recommendations are presented in chapter five.

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

This section contains an overview of concepts fundamental to the research and a review of similar works relevant to the research.

2.2 OVERVIEW OF THE FUNDAMENTAL CONCEPTS

This section provides an overview of the concepts fundamental to the research such as IP address technology, OSPF technology, MPLS technology, and network metrics and performance tools.

2.2.1 Internet Protocol Version Four (IPv4)

Computer networks and the Internet uses Internet Protocol version 4 and version 6 (IPv4 and IPv6) as routed protocols to transport data from sources to destinations, it's the dominant protocol on the internet because of the following reasons (Jeff, 2009);

i. It's open language (i.e its not a proprietary protocol)

ii. It's Simple protocol

iii. It's Scalable and Robust protocol

iv. It's Distributed Protocol

v. It's Flexible and Extendable and protocol

The basic design principle for Internet Protocol IP-based network was to share information or data from sources to destinations over the network were all the intermediate hosts or devices along the line of communication play their role anonymously. Active network devices check the destination IP address according to a forwarding table to select the next hop for an IP datagram, in a complex network environment, datagram is sometimes delayed due to the long queue for the next hop. Every network device along the path to destination performs two operations for each packet received as follows;

i. Looks up the packet's next-hop at the routing table.

ii. Forwards the packet to the outgoing interface determined by the forwarding table. (Kevin, 2011; Douglas, 2009).

Network device can drop a datagram if the queue is full or the destination of the datagram is unavailable. Conventional IP packet forwarding has several limitations such as unpredictable delays, data loss, and limited capability to deal with addressing information beyond just the destination IP address carried on the packet; because all traffic to the same IP destination – prefix is usually treated similarly, various difficulties arise. IPv4 packet forwarding does not easily take into account extra addressing-related information such as Virtual Private Network (VPN) membership, no means of tagging, cataloging, or monitoring packets that cross them (Narbik, 2015).

IPv4 address is 32 bits addressing that has approximately 4.3 billion addresses, which were classified into classes A to E or what is called classful addressing, the classes of represent the number of host address that can be allocated per block and per user demand. Variable Length Subnet Mask (VLSM) or classless addressing was introduced and adopted to over the limitation of classsful addressing. IPv6 is designed to be the successor to IPv4, it has a larger 128-bit address space providing up to 340 undecillion addresses (i.e the number 340, followed by 36 zeroes). However, apart from larger addresses space, it provides other advanced and additional features than IPv4 address such as VPN technologies, improved packet handling, end-to-end connectivity by eliminating NAT. Both IPv4 and IPv6 provide hierarchical addressing for packets that carry data. Designing, implementing and managing an effective IP addressing plan ensures that networks can operate effectively and efficiently. Both IPv4 and IPv6 coexist because there is not a single date to move totally to IPv6 in the foreseeable future. The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6 such as dual stacking, tunneling and translation (Jeff, 2009, Narbik 2015). A typical IPv4 header is shown in Figure 2.1 (Jeff, 2009).

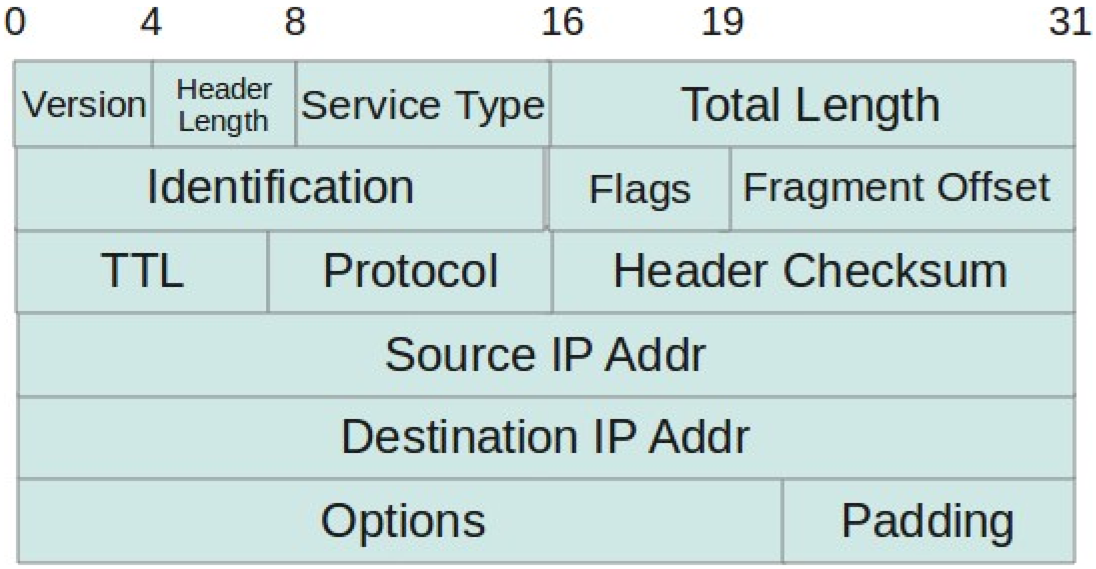


Figure 2.1 IPv4 Header

2.2.2 Open Shortest Path First (OSPF) Protocol

Open Shortest Path First (OSPF) protocol was developed and adopted by the Internet Engineering Task Force (IETF) as a replacement for the problematic Routing Information Protocol (RIP) and is now the IETF-recommended Interior Gateway Protocol (IGP). OSPF is a none proprietary link-state routing protocol that uses Dijkstra's Shortest Path First (SPF) algorithm to calculate and update its topological databases, being a complex routing algorithms, SPF consumes a lot of network hardware resources such as CPU, RAM and link utilizations. The OSPF packet composed of many fields as shown in Figure 2.1(Kevin, 2011).

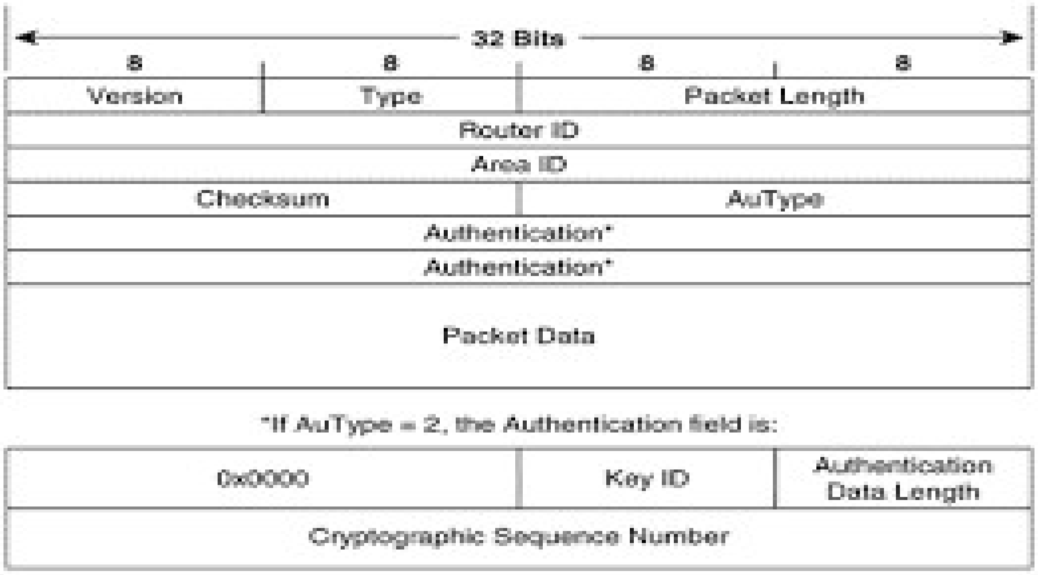


Figure 2.2: OSPF Packet Format (Kevin, 2011)

OSPF's capability to perform as a hierarchical routing protocol makes it a good candidate in many large networks, as a result of this capability; it supports a variety of techniques and designations that make operation much smoother. As a link-state routing protocol it means that all the routers configured in an area would have the same knowledge of the entire topological databases of the neighboring routers.

OSPF uses the concept of areas to reduce the complexity of the SPF algorithm execution, the areas are configured to build a hierarchical structure to maintain a flow of data packet in the network; they are used to group routers to exchange routing information locally and will have at least one area in a network, and if more than one area exists, one of the areas must be a backbone area which is to be connected to all other areas. The areas are named as Normal, Backbone, Stub, Totally Stub, Not-So-Stubby, and Totally Not-So-Stubby areas (Narbik, 2015).

OSPF routing protocol use costs as a metric to determine the shortest path to destination after SPF algorithm have been executed, the cost of an interface is calculated on the basis of bandwidth, and cost is inversely proportional to the interface bandwidth, therefore higher bandwidth is attained with a lower cost (Jeff, 2009).

2.2.2.1 Operation of OSPF Protocol

A typical operation of the OSPF is described as follows (Jeff, 2009):

a) OSPF-speaking routers send Hello packets out to all OSPF-enabled interfaces, if two routers sharing a common data link agree on certain parameters specified in their respective Hello packets, they will become neighbors.

b) Adjacencies, which may be thought of as virtual point-to-point links, are formed between some neighbors, OSPF defines several network types and several router types, and the establishment of an adjacency is determined by the types of routers exchanging Hellos and the type of network over which the Hellos are exchanged.

c) Each router sends link state advertisements (LSAs) over all adjacencies, LSAs describe all of the router's links, or interfaces, and the state of the links, these links may be to stub networks (i.e networks with no other router attached), to other OSPF routers, to networks in other areas, or to external networks (i.e networks learned from another routing process). Because of the varying types of link state information, OSPF defines multiple (LSA) types.

d) Each router receiving an (LSA) from a neighbor records the (LSA) in its link state database and sends a copy of the (LSA) to all of its other neighbors.

e) By flooding (LSAs) throughout an area, all routers will build identical link state databases.

f) When the databases are complete, each router uses the shortest path first (SPF) algorithm to calculate a loop-free graph describing the shortest (lowest cost) path to every known destination, with itself as the root. The graph is the shortest path first SPF tree.

g) Each router builds its route table from its SPF tree.

2.2.2.2 OSPF Network Scalability

The ability to scale an OSPF internetwork depends on the overall network structure and addressing scheme, adopting hierarchical addressing environment and a structured address assignment will be the most important factors in determining the scalability of any network. Network scalability is affected by operational and technical considerations (Kok-Koeng, 2012):

a) **Operationally;** OSPF networks should be designed so that areas do not need to be split to accommodate growth, address space should be reserved to permit the addition of new areas.

b) **Technically;** scaling is determined by the utilization of three resources: memory, CPU, and bandwidth utilization.

   i) **Memory:** OSPF router stores all of the link states information for all the areas associated with it, it can store summaries and externals routes information, careful use of route summarization and stub areas can reduce memory use substantially.

   ii) **CPU:** OSPF router uses CPU cycles whenever a link-state change occurs, keeping areas small and using summarizations reduces CPU usage and creates a more stable environment for OSPF.

   iii) **Bandwidth:** OSPF speaking routers send partial updates when link-state changes occur, the updates are flooded to all routers in the area, in an OSPF network, substantial topology changes are partially updated to minimize bandwidth usage.

2.2.2.3 Factors Influencing OSPF Network Scalability

The network scalability is determined by the utilization of three router resources: memory, CPU, and interface bandwidth, the workload that OSPF imposes on a router depends on these factors (Kok-Koeng, 2012):

a) **Number of adjacent neighbors for any one router**: OSPF floods all link-state changes to all routers in an area, routers with many neighbors have the most work to do when link-state changes occur, in general, any one router should have no more than 60 neighbors.

b) **Number of adjacent routers in an area:** OSPF uses a CPU-intensive algorithm, the number of calculations that must be performed given ***n*** link-state packets is proportional to **n log n**, as a result, the larger and more unstable the area, the greater the likelihood for performance problems associated with routing protocol recalculation. Generally, an area should have no more than 50 routers; areas that suffer with unstable links should be smaller.

c) **Number of areas supported by any one router:** A router must run the link-state algorithm for each link-state change that occurs for every area in which the router resides, every ABR is in at least two areas the backbone and one adjacent area, in general, to maximize stability, one router should not be in more than three areas.

d) **Designated Router (DR) selection:** In general, the DR and Backup Designated Router (BDR) on a multi-access link (for example, Ethernet) have the most OSPF process work to do, it is a good idea to select routers that are not already heavily loaded with CPU-intensive activities to be the DR and BDR. In addition, it is generally not a good idea to select the same router to be the DR on many multi-access links simultaneously. The first and most important decision when designing an OSPF network is to determine which routers and links are to be included in the backbone area and which are to be included in each adjacent areas.

2.2.3 Multi-Protocol Label Switching (MPLS) Network

Multiprotocol Label Switching (MPLS) is an evolving technology for high performance packet control and forwarding mechanism for routing the packets in the data networks, MPLS has evolved into an important technology for efficiently operating and managing IP networks because of its superior capabilities in providing traffic engineering (TE) and virtual private network (VPN) services. MPLS is not a replacement for the IP but it is an extension for IP architecture by including new functionalities and applications, the main functionality of the MPLS is to attach a short fixed-label to the packets that enter into MPLS domain, a label is a short fixed entity with no internal structure, label is placed between Layer-2 (Data Link Layer) and Layer-3 (Network Layer) of the packet to form Layer 2.5 label switched network on layer-2 switching functionality without layer 3 IP routing (Narbik, 2015; Jim 2014]. Therefore Packets in the MPLS network are forwarded based on the Labels.

2.2.3.1 MPLS Header

MPLS operates by defining a label inside MPLS "Shim header" that is placed on the packet between layer-2 and layer-3 headers. The 32-bit MPLS header is organized as in Figure 2.3

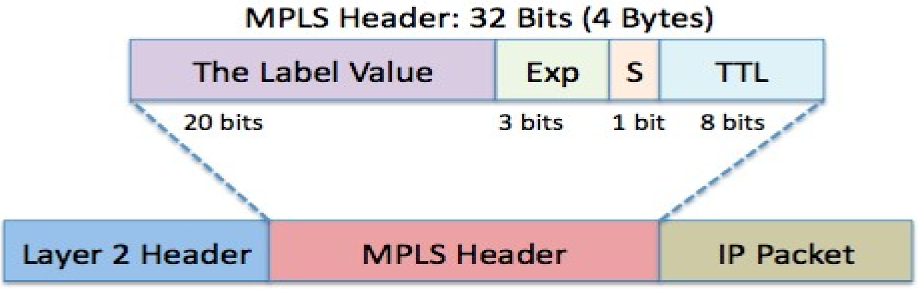


Figure 2.3: MPLS Header (Jim 2014)

The header consists of 20-bit Label which is used to identify the Label Switched Path (LSP) to which the packet belongs in the MPLS domain; the labels on the packets are established by using

Forwarding Equivalency Class (FEC). Following the Label field there are 3 bits EXP field which is called Traffic Class field (TC field), this is used for Quality of Service (QoS) related functions. Next field is called stack field which is 1 bit field and this is used to indicate bottom of label stack. The tail consists of 8-bit TTL (Time to Live) field which had similar function as that of the TTL field in an IP header (Jim 2014).

2.2.3.2 MPLS Architecture

The MPLS domain is described as a contiguous set of nodes which operate MPLS routing and forwarding, MPLS domain is divided into MPLS core which consists of Label Switch Routers (LSRs) and MPLS edge which consists of Label Edge Routers (LERs) (Luc, 2006; Jim 2014)

The main Terminologies of MPLS technology are explained as follows:

a) **Label Switch Router (LSR) Provider Router (P Router)** - Any router which is located in the MPLS domain and forwards the packets based on label switching is called LSR. When an LSR receives a packet, it checks the look-up table and determines the next hop. However, before forwarding the packet to next hop, it removes the old label from the header and attaches new label.

b) **Label Edge Router (LER) or Provider Edge (PE)** – A packet enters into MPLS domain through LER which is called Ingress router. Packet leaves the MPLS domain through LER which is called Egress router. LER has an ability to handle L3 lookups and is responsible for adding or removing the labels from the packets as they enter or leave the MPLS domain.

c) **Customer Edge (CE)** - A CE router is a router located on the customer premises that provides an Ethernet interface between the customer's LAN and the provider's core network.

d) **Label Distribution Protocol (LDP**) - It is a protocol in which the label mapping information is exchanged between LSRs. It is responsible in establishing and maintaining labels.

e) **Forward Equivalence Class (FEC)** – It is considered as the set of packets which have related characteristics and are forwarded with the same priority in the same path. This set of packets is bounded to the same MPLS label. Each packet in MPLS network is assigned with FEC only once at the Ingress router.

f) **Label Switched path (LSP)** – LSP is the path set by the signaling protocols in MPLS domain. In MPLS domain there exists number of LSPs that originate at Ingress router and traverses one or more core LSRs and terminates at Egress router.

2.2.3.3 MPLS Operation

The devices on a campus network running MPLS technology separate the operation into three main blocks as; Control Plane components, Forwarding Plane (Data Plane)component, and Label-Swapping Forwarding algorithms (Minei, 2011).

a) Control Plane and Forwarding Plane (Data Plane) components

The Control Plane component maintains and controls the forwarding table by learning the network topology from the routing protocols such as OSPF, IS-IS and BGP, it is responsible for building the MPLS IP routing control by updating the label bindings which are exchanged between the routers. When MPLS packet arrives at the router's interface, the forwarding decision is taken by the Data Plane (forwarding component) by consulting the forwarding table, which is maintained by control plane, the packets are then forwarded towards the appropriate node based on the forwarding decision(Jim, 2014).

The control plane depends on the IP infrastructure in establishing or maintaining the paths, in MPLS network, each router maintains a label information table that is used for updating the forwarding table, based on this forwarding table the forwarding decision is done, in MPLS routers, control plane and data plane are separated entities, this separation allows the deployment of a single algorithm that is used for multiple services and traffic types as in Figure 2.4 (Jim, 2014).

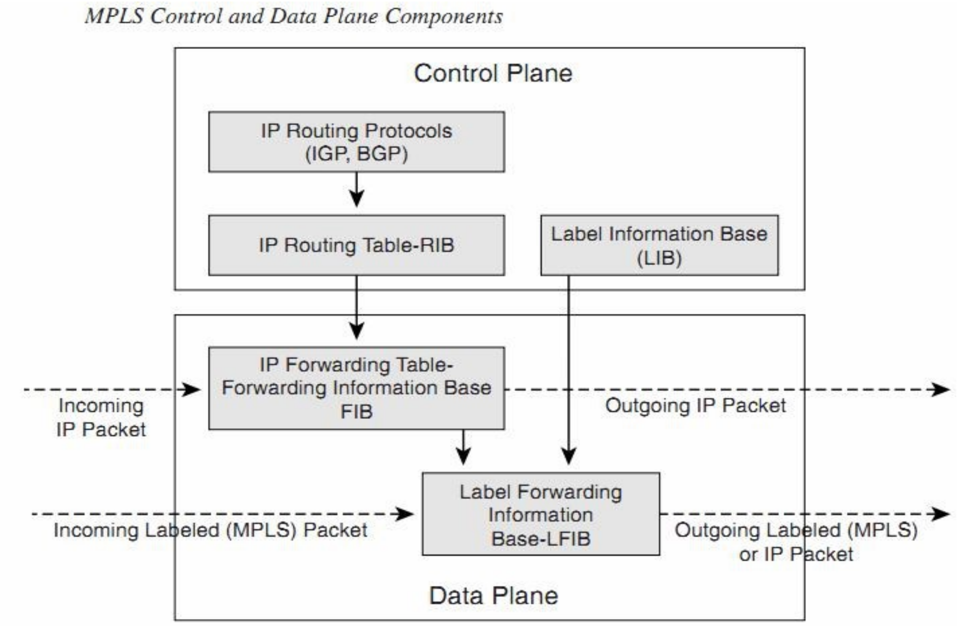

MPLS Control and Data Plane Components
Control Plane
IP Routing Protocols (IGP, BGP)
IP Routing Table-RIB
Label Information Base (LIB)
IP Forwarding Table-Forwarding Information Base FIB
Incoming IP Packet
Outgoing IP Packet
Label Forwarding Information Base-LFIB
Incoming Labeled (MPLS) Packet
Outgoing Labeled (MPLS) or IP Packet
Data Plane

Figure 2.4: Label Switch Router (Minei, 2011)

b) Label-Swapping Forwarding Algorithm

The label-swapping forwarding algorithm explains how the packets are routed in the MPLS domain which is described in the following steps (Jim, 2014).

i) When a packet enters the MPLS domain a label of short fixed-length is inserted in the packet header by the Ingress router, FEC is identified from the label.

ii) The packets belonging to one particular FEC are forwarded through the same path through the MPLS network even though all the packets do not have the same destination address.

iii) The path on which the packets are forwarded to the next hop in the network is LSP.

iv) Every hop in MPLS network forwards the packets based on the label but not on IP address. This is done until the packets reach the final hop in the MPLS network and then the label is removed by the Egress router and normal IP forwarding resumes.

v) Here the Ingress and Egress routers are the LER"s and the hops within the MPLS domain are LSR"s which is shown in Figure 2.5

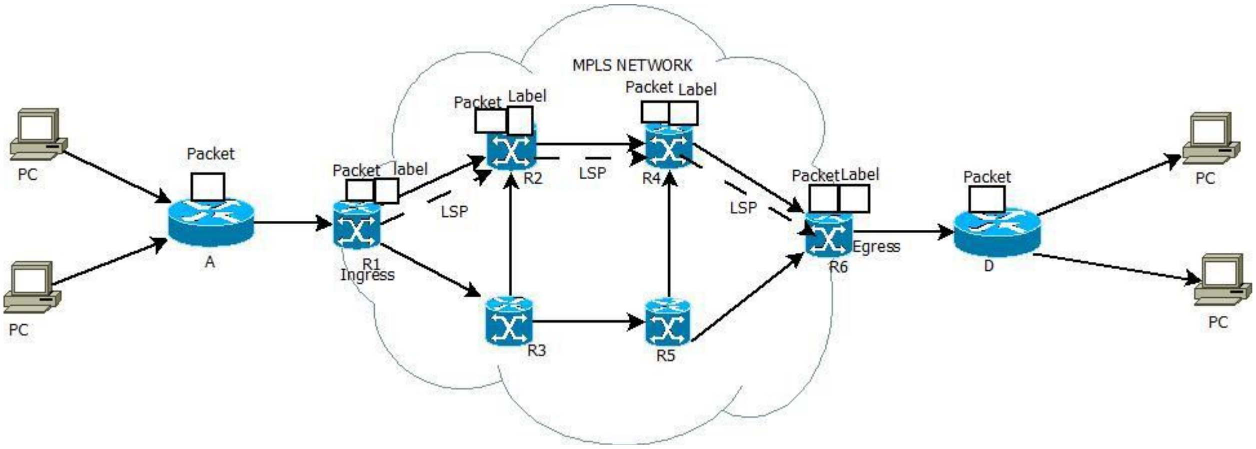


Figure 2.5 MPLS Network (Jim, 2014)

MPLS uses signaling protocols to establish the paths, Label Distribution Protocol (LDP) is the signaling protocol and the paths established are called Label Switched Path (LSP), all the packets enter or exit the MPLS domain through LERs. In Fig.2.5; R1 and R6 are the LERs, R1 is the Ingress router which maps the incoming traffic into the MPLS domain, R6 is the Egress router through which the packets exit from the MPLS domain, An LSP originates at Ingress router and travels through one or more LSRs and terminates at Egress router.

When packets enter the MPLS domain, labels are inserted in their headers by Ingress router and the packets are mapped on to the LSP using Forwarding Equivalence class (FEC), all the packets which match a Particular FEC are forwarded on the same LSP, the FEC is described by the set of attributes such as destination IP address, Type of Service etc. The core LSRs (which are R2, R3, R4, and R5 in Figure 2.5) forward the packets based on label information but not on the IP address, when the router receives the packet, it checks Label Information Base (LIB) instead of routing table and determines the next hop in MPLS domain. Finally, the Egress router R6 removes the label from the packet header and forwards the packet to the next hop based on IP address and from here the conventional IP forwarding of packets continues (Minei, 2011; Jim, 2014)

2.2.4 Network Performance Metrics

The performance parameters considered in the cause of this research work are defined as follows (Narbik, 2015):

I. **Throughput:** Throughput or network throughput is the average rate of successful data transfer over a network, it is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (bps or pps) or data packets per time slot.

II. **End-to-End Delay**: Delay is a measure of time a packet takes to traverse a route, End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination and back to the source.

III. **Queuing Delay:** Delay is a measure of time a packet takes to traverse a route, Queuing delay is the time spends in the routing queue.

IV. **Jitter:** Jitter or Packet Delay Variation (PDV) is the difference in end-to-end delay between selected packets in a traffic flow with any lost packets being ignored.

V. **Server Load:** Load is a measure of the amount of computational work that a computer system performs, or is the amount of traffic utilizing the links along the path. The best path is the one with the lowest load.

2.2.5 Graphical Network Simulator (GNS3)

Graphical Network Simulator (GNS3) is a software emulator for networks, it allows the combination of virtual devices and real devices, and so can be used to simulate complex networks, to provide complete and accurate simulations, GNS3 is strongly linked with: Dynamips, a Cisco IOS emulator, Dynagen, a text-based front end for Dynamips, Qemu, a generic and open source machine emulator and virtualizer and VirtualBox, a free and powerful virtualization software. GNS3 is an excellent complementary tool to real labs for network engineers and administrators, it can also be used to experiment features of Cisco IOS, Juniper JunOS or to check configurations that need to be deployed later on real routers. GNS3 project is an open source, free program that may be used on multiple operating systems, including Windows, Linux, and MacOS X (Mike, 2013).

2.2.6 OPNET Modeler

Optimized Network Performance (OPNET) is a discrete event simulation tool; it provides a comprehensive development environment supporting the modeling and simulation of communication networks, this contains data collection and data analysis utilities. It provides several modules for the simulation comprising a vast universe of the protocols and network elements, it has gained popularity due to its easy handling in networking research, the user does not require programming knowledge in order to use OPNET; the user can directly concentrate in building and analyzing models from simulation. The main feature of OPNET is that it provides various real-life network configuration capabilities that make the simulation environment close to reality (Adarshpal, 2013).The advantages of OPNET compared to other simulators include GUI interface, comprehensive library of network protocols and models, graphical interface to view the results, availability of documentation for the user to develop the network models etc. In this thesis, OPNET Modeler 16.5 was used to design, simulate and generate data for analysis for ABU campus network with the following object configuration models from the OPNET library;

I. **ethernet_wkstn:** Ethernet workstation OPNET element is used to simulate the network users; it consists of single Ethernet connection at a selected rate, directed by the underlying medium used to connect to an Ethernet switch.

II. **Dell_PowerEgde_8450_700_8CPU server:** Dell server used in the research to configure the network services.

III. **CS_C6506_6S_ae32_a2 router:** Multi-Layer Switch (MLS/Router) model capable of supporting Routing and MPLS

IV. **10Gbps fibre link:** This is a full duplex fibre link used to connect active devices.

V. **1Gbps fibre link:** This is a full duplex fibre used to connect distribution and access devices.

VI. **1000Basex:** This is a full duplex Ethernet link operating at 1GBps to connect end devices.

VII. **MPLS_E-LSP_STATIC:** Static LSP are not signaled during the startup. They allow more routing control

VIII. **Application Config:** This element is used to tell OPNET which application is going to be modeled upon the underlying network, a single Application Config. is used to instruct OPNET for multiple network applications, application parameters for different application types being observed are configured in this element.

IX. **Profile Config:** Profiles describe the activity patterns of a user or group of users in terms of the applications used over a period of (simulation) time, there can be several different profiles running on a given network under observation. User profiles have diverse properties, so configuring a certain profile with a specific application was done here, the configured profiles are then assigned to the network users.

X. **mpls_config_object:** Configuring MPLS FEC and Traffic Trunk is done under this element configuration, the configured specification is used at the Ingress Edge router to direct the traffic flows and assign different LSP to different application traffic (Adarshpal, 2013).

The function of the network model is to standardize system from the higher layer equipment, the node model is to standardize the function of the node from the application, process and the communication interface. The function of the process model is to standardize process behavior of node which is inside the system, including the decision-making process and arithmetic.

2.3 REVIEW OF SIMILAR WORKS

The following literature were consulted and critically reviewed in order to have the knowledge on the extent of the research on this problem being studied.

Jun *et al;* (2006) conducted a research on OSPF performance and stability, and proposed an evaluation method based on white-box measurements compared with the black-box measurement. The measurement of internal parameters would help to know the performance limitation on a specific hardware. The aimed was to introduce a new method of network design as the implementation performance and stability limitation can be calculated based on the parameters measured. The result showed that the number of adjacencies on a given router in a network is coefficient in determining the router's CPU utilization as a function of internal processing time. The research did not show how the network designs and topology could be achieved using the proposed solution.

Jing-bo *et al;* (2008) conducted a research on disadvantages of conventional "Special line" networking such as IP Networks, Frame Relay and the ATM networks with the aim of suggesting a solution to their scalability issues. The research was modeled and simulated using OPNET modeler and it was able to show that Multi-Protocol Label Switching Virtual Private Network (MPLS VPN) networks provided significant improvement compared to conventional "Special line" networks. None of the network services such as FTP or web were configured to justify the research findings. The simulation was carried out only for a short period of time which will not give the full picture of the research. The research recommended upgrades in real equipment with no defined guidelines.

Nuuti ***et al;*** **(2009)** conducted a research to address the scalability issues of Ethernet technology due to growing interest in using Ethernet technology in access and carrier backbone networks. The research proposed RBridges design and TRILL routing protocol, RBridges are a step forward for Ethernet switching technology, offering better scaling characteristics than conventional STP bridges. The proof of concept prototype was implemented using Click and Quagga and was in the process of testing in various network size and traffic models. The major issue with RBridges is that they did not take into account mobile Ethernet devices and mobility events directly on top of the link layer. Additionally, RBridges relied on flooding Ethernet frames across the network when the frames are destined to unknown end-stations or sent using a broadcast Ethernet address. The research concentrated on validating the functionality of the distributed index to eliminate broadcast traffic on Ethernet network such as ARP request using the engineered software but no rigorous test was carried out to test the TRILL routing protocol and performance parameters.

Berzuk ***et al;*** **(2010)** conducted a research to compare the characteristics of unicast routing protocol such as RIP, OSPF, ad AntNet and multicast routing protocol such as DVMRP, MOSPF, PIM-DM, CBT, and PIM-SM with the aim to provide recommendation of their practical applications as well as technology and ways of organizing Multipath routing. Two data networks models for unicast and multicast were created to investigate the protocols. Unicast data network model was designed and modeled using MathCAD to analyse the mechanisms of traffics control and efficiency of routing algorithms, sixteen network nodes were selected in the model to form the flow of information which was calculated based on the number of population and statistics, internet load was also calculated per user, and for all protocols routing tables were constructed. In Multicast data network model, comparative analysis of routing protocols was carried out in software package network simulator, two hundred routers with varying number of users in the group were used to show different data transfer and number of packets transmitted per second. Multipath routing involves optimizing the use of network resources in terms of distribution network load and as consequences – to prevent overloads as well as increases fault tolerance. The comparative analysis did not show which protocol was the best or most prepared in terms of practical applications.

Mangla *et al;* (2010) proposed a framework to evaluate the potential financial impact of network optimization services such as network assessment, network support, network resources sharing in an organization; due to increase in user demand of the network services that may likely cause congestions and bottleneck on popular network services. The research suggested Distributed Content Delivery Network (DCDN) architectural model which will help an organization to reduce cost and improve scalability by making resources such as storage capacity, processing power, bandwidth, internet availability common to end users, by increasing the overall quality of services experience to end users. DCDN architecture will allow the organization have a cluster of servers with varying functionality, DCDN servers basically redirect the end user request to where the content is without the knowledge of the end user. In a DCDN, content or network services can be stored on surrogated servers, each server have replica of contents. Border gateway Protocols (BGP) is suggested as the routing protocol between devices because of its flexibility in using its attributes to influence traffic flow. Quagga software tool was proposed to model and test the framework. The concept was not modeled or simulated using any of the standard simulation tools.

Arshad *et al;* (2010) conducted a research to highlight the drawback such as speed, scalability, and security issues of traditional IP-based virtual private networks (VPNs) with aim of addressing them. Layer-2 VPNs are efficient but not intelligent and scalable; layer-3 VPNs are intelligent and scalable but not efficient. A survey was carried out and a new design scheme was proposed for MPLS/BGP-VPNs in such way that the features of layer-3 as scalability and intelligence are merged with the efficiency of layer-2 to deal with the evolving demand of speed, scalability and security. The proposed design of optimized data networks through MPLS/BGP-VPNs is implemented in Dynagen simulator for better understanding; five routers were configured in the research and only ICMP traffic was generated for testing. The technical challenges of merging layer-2 and layer-3 VPNs were not taking care of, and features such as traffic engineering TE, end-to-end performance, security and path management were left for future work. Also, five routers are not enough to test any proposed design of the size of the internet or large and complex campus network, also no any network service configured to justify the survey. A more rigorous survey using a complex design with some network services configured need to be conducted and validation need to be carried out after the findings.

Hock *et al;* (2010) conducted a research on comparative analysis to address the redundancy issues in IP network where several equal-cost shortest paths exist between two nodes in IP networks. Intra-domain routing in IP networks follows shortest paths according to administrative link costs. When several equal-cost shortest paths exist, routers that use equal-cost multipath (ECMP) distribute the traffic over the entire domain. In the cause of the research, Single Shortest path (SSP) and Unique Shortest Path (USP) were proposed; where tie-breakers decide which of the paths is chosen for SSP. However, the tie-breakers are not clearly defined and do not work in a deterministic way because the information change over time, which makes SSP routing unpredictable, that can lead to unexpected high link loads in the network in spite of routing optimization. Fifty optimizations were run for each of the various routing options and select the link cost setting with the lowest maximum link utilization for analysis. The comparative analysis was carried out using heuristic algorithm, and showed that USP routing provide high link optimization than SSP in all failure protected scenarios for classic IP networks, not-via IP fast reroute, and MPLS network with facility or one-to-one backup. The research also showed that Fast Re-Route (FRR) mechanisms could repair failures faster than conventional IP rerouting by pre-computing shortest backup paths around failed network elements.

Jialei *et al;* (2010) proposed a layered architecture for Multi-protocol Label Switching (MPLS) technology to be integrated into IP network with the aim of improving performance and reduce bottleneck arises in delivering high speed and QoS (Quality of Service) guaranteed network services in an IP network, and future Next Generation Network (NGN) environment. MPLS technology is independent from upper layer network protocols as such provide many features and benefits such as unicasting, multicasting, VPN services, Traffic Engineering (TE) with the help of resource reservation protocol (RSVP). The proposed layered MPLS architecture has some limitations such as specific implementation of core routers situated between core layer and merging layer of the MPLS architectural domain, job sequence during initialization phase, support for multicasting services and the integration with pure IPv6 network in NGN environment which to need to be resolve in the future research. However, no experiment was carried out on the MPLS architecture in both IPv4 and IPv6 networks using network simulation tools to verify the proposed solution.

Zhao ***et al;*** **(2010)** carried out a survey from network operator's perspective to address the routing scalability issues of active hardware's components on the internet such as control engine, forwarding engine or line cards, and switch fabric. The internet and global routing table continue to grow with time, and in the near future the routing infrastructure will not be able to sustain such growth. The internet routing table growth has been mainly driven by the growth of internet services configured, and implemented and de-aggregation of the network address space. In searching for the solution of the routing scalability problems; few basic requirement were provided to help in design a more deployable and practical solution. The requirements were group in three main categories as business support, compatibility, and OPEX reduction. MPLS technology and other advanced features of existing technologies were proposed as a measure to address some of the scalability issues. Based on the operational experiences, the survey identified several requirements for potential solutions and provides brief comments on the existing solutions, such as business model change, routing architecture re-design, network design optimization, and software optimization. The survey was theoretically based and no simulation was carried out to generate data for analysis.

Tokalic ***et al;*** **(2011)** conducted a research on the performance of devices on routing of packets based on their global IP addresses as the number of hosts keeps growing. MultibitTrie Lookup Table Update (MLTU) algorithms was proposed and implemented for classical lookup table according to the network topology changes reported by OSPF protocol. The MLTU algorithm was implemented through two functions, **insert** for adding the entry to the lookup table or modifying the existing entry, and **removal** for removing the entry from the lookup table. It is connected with OSPF source code, using method *net*, *mask*, and *ifc* of the class *INrte* that calculate the network address (i.e prefix), mask, and the output port address. This is aimed at optimizing the speed and memory requires in routing of IP packets. The performance of the algorithm was analyzed in a real network and the result showed that update speed is satisfactory if the updates were triggered by the changes of the network topology. However, if the updates are triggered by other services (e.g bandwidth reservations), typical update algorithms become a bottleneck, and the speed needs improvement to take care of the other services. In that case, the IP lookup algorithms that imply fast updates, such as the PFL algorithm need to be deployed for future research. The research was modeled and simulated using single area OSPF with more than 51 routers> However, the design is susceptible to serious scalability issues on a complex network due to the way OSPF responds to topology changes.

Modhar *et al;* (2011) conducted a research to analyze the traffic behavior in a campus network, University of Mosul campus network was modeled and simulated as a case study. File transfer Protocols (FTP), HTTP (Web), and VoIP network services were designed, configured and simulated in an OPNET modeler environment. The research network model was made up of two CISCO routers (2600), core switch (cisco6509), two servers, ip32 cloud and 37 VLANs, 1000BaseX fiber optic simulation cables. The simulation results showed that the network model have a positive efficiency on designing and managing the targeted network and can be used to view data flow. Also, the simulation results showed that the maximum number of VoIP service users could be raised up to 5000 users when working under IP Telephony, this means that the ability to utilize VoIP service in the network can be maintained and is better when subjected to IP telephony scheme. The Mosul campus network was modeled and simulated in OPNET modeler using conventional layer-2 switched network. Although many devices were connected to represent the topology in question but the network layer and data link layer technologies were not considered in configuring and running the simulation.

Akinsipe *et al;* (2012) conducted a research on modeling of conventional IP network, MPLS, and MPLS RSVP-TE (with path reserved for voice traffic) networks and the performance parameters of the networks such as throughput, utilization, and voice jitter were compared. Different applications have been put in place to enhance application services in a network. MPLS is one of such technologies, and it provides a reliable delivery of application services. It delivers services with low delays, low losses, and high speed of transmission. Due to the Traffic Engineering of MPLS, it can also be used to efficiently utilize networks resources as well as implement real-time applications (voice and video). Signaling protocols such as RSVP-TE and CR-LDP are used for traffic engineering in MPLS. The research results showed that IP network have higher throughput than both MPLS, and MPLS RSVP-TE followed by MPLS network, but the overall simulation results showed that MPLS network performs better than both IP and MPLS RSVP-TE networks in terms of utilization while the MPLS RSVP-TE network has the best performance for voice traffic due to the reserved path and the MPLS network has a better performance for voice traffic than IP network. The research network topology did not reflect the real life design as the standard network hierarchical structure was not followed.

Goyal *et al;* (2012) conducted a comprehensive survey on how to improve OSPF convergence speed, scalability as well as extension of OSPF protocol to provide routing functionality in MANETs due to high level of service availability and ever-growing size of routing domain. Modern routing domains need to maintain a very high level of service availability. Hence, OSPF needs to achieve fast convergence to topology changes. The survey showed that the link state routing protocols such as OSPF are an essential component of today's network and will continue to serve this role in the foreseeable future. But due to the complexity of the SPF algorithm, link state protocols are still facing scalability issues. The survey suggested that the area-level organization of the routing domain need to be examine, small area sizes are good from convergence speed and scalability perspective but may be difficult to achieve in a large routing domain. The survey was not implemented on any simulator.

Atayero ***et al;*** **(2012)** conducted a research on modeling and simulation of a Local Area Network in OPNET modeler. The simulation and analysis of the Covenant University campus LAN in the OPNET Modeler environment was used as a case study. The main purpose of a campus network is efficient resource sharing and access to information among its users. A key issue with designing and implementing such LAN is its performance under ever increasing network traffic, and how this is affected by various network metrics such as latency and end-to-end delay. The research showed that implementing network in complex environment is a challenging task, hence the need for proper network design and analysis using simulator before implementation. The network was designed and configured using hubs and switches, which will not give the actual behavior of traffic as compared to current network design, and it was not validated using real equipment.

Fatigau ***et al;*** **(2013)** conducted a research on the analysis of performance impact of File Transfer Protocol (FTP) and Video traffics for MPLS network and Conventional IP network, using OPNET Modeler simulator. The research results showed that MPLS network performed better in real time application such as video conferencing, where traditional IP networks encounter high packet loss and more delays which are unacceptable for this kind of applications. But the simulation was carried out using non-realistic topology using hubs and no any routing protocols configured on the routers. This would not give the actual optimization accuracy needed in real life design. As future work the research will concentrate on simulations with more realistic topologies.

Mishra *et al;* (2014) conducted a research on performance analysis of VoIP application over conventional IP network and MPLS network. The performance comparison is based on the performance metrics such as Voice packet jitter, Voice packet end-to-end delay, voice delay variation, voice packet send and received. The research was simulated using OPNET modeler and the simulation results it can be concluded that MPLS provides best solution in implementing the VoIP application as compared to conventional IP networks because of the following reasons; MPLS takes less processing time in forwarding the packets which is more suitable for the applications like VoIP, Implementing of MPLS with TE minimizes the congestion in the network, and MPLS suffers minimum delay and provides high throughput compared to conventional IP network. The result showed that MPLS network performed better than conventional IP network. The topology has not emulated any real life design and the devices used in the design have no longer being used in real life design, and the devices were connected without following the hierarchical model. A more realistic network designed showing core, distribution an access layer device is needed to test, simulate and analyse the actual behavior of the protocols.

Abdul-Bary *et al;* (2014) conducted a research on performance analysis of multimedia applications over conventional IP network and MPLS communication network with traffic engineering. The performance comparison is based on the performance metrics such as delay variation, delay, page response time, throughput, and packet drop for different types of traffic (voice, video, data) in their movement in a congested network for both MPLS-TE and conventional IP network. The main objective of the research is based on the performance analysis of conventional IP network and MPLS TE network in respect of multimedia applications (VoIP, Video Conferencing) and Non Real Time application (FTP). The research was modeled and simulated using OPNET modeler, and based on the simulation results it can be concluded that MPLSTE provides best solution in implementing such applications compared to conventional IP networks. Also the research explained poor link utilization in conventional IP networks. The study showed that networks configured with OSPF routing techniques are not capable of handling the incoming traffic efficiently. When the network traffic increased, shortest path from source node to destination node became heavily congested and led to loss of transmission data.

Oyeleke *et al;* (2015) conducted a research to test the performance of IP, MPLS and MPLS-TE technologies with path reserved for voice traffic using OPNET modeler, performance metrics such as voice packet delay variation, video packet end-to-end delay variation, and voice packet reception rate were compared. The simulated results collected were analyzed and showed that MPLS network performed better than both the IP and MPLS-TE networks in terms of Video packet end-to-end delay i.e it has lower packet delay, while the MPLS-TE network performed better than both IP and MPLS networks in terms of voice packet delay variation due to reserved. In addition, the simulated topology doesn't reflect a real life designed as it doesn't follow the approved standard hierarchical model, also only delay variation was analysed other performance metric need to critically be analyzsd and conclude which technology is more preferred in any campus network design.

Divya *et al;* (2015) conducted a research to test the performance of traditional IP network and MPLS network using VoIP traffic, the growing number of internet services users and real-time network services is a critical task for traditional IP network as it utilizes best-effort services which doesn't offer guarantee of services, and also provide least predictability of services which is unacceptable in today's network. The performance measurement is carried out using OPNET modeler to calculate the least number of VoIP calls that can be kept in the IP and MPLS networks, the performance measurement in both networks is done using performance metrics i.e delay, jitter, and packet sends and receive. The simulation result showed that MPLS network provides lower delay, and jitter compared to traditional IP network. but the topology adopted illustrated a simple network designed with fewer routers and obsolete devices like hubs, that is not enough to predict a complex network running many real time traffics and thousands of users, also no validation using real device to validate the findings.

Most of the literature reviewed, addressed the scalability issues of campus network using few performance parameters, some did not follow the standard and approved hierarchical model in real life network design, and using very old network devices which are no more in the market such as hubs. Some literature used simulation tools without proper analysis of the collected data and no validation carried out, also some carried out their research on small campus networks which will not give the real picture of what is happening in real life nowadays. This research work will emulate and simulate a complex network model using GNS3 and OPNET to identify some scalability issues affecting hardware's performance such as CPU, memory, and link utilization due to the type of design and routing protocol running on the network. The performance of the hardware will be tested and improved using data generated and analysed on performance metrics such as; End-to-End delay, queuing delay, jitter, throughput, and load during the simulations. A suitable designed solution will then be proposed, configured, simulated and validated using active equipment.

CHAPTER THREE

MATERIALS AND METHODS

3.1 INTRODUCTION

This section provided the detailed descriptions of the case study and guides in the designed, configurations, and simulations of the methodology followed in the cause of the research.

3.2.1 The Ahmadu Bello University Network

The ABU Campus Network is designed based on optical fiber backbone comprising of three rings: Samaru, Kongo and Shika. The fibre backbone connects all Faculties, Departments and other Units of the University to the Data Center. The data center houses the core infrastructure hosting the network services and the Internet link connectivity. The University has two Internet Service Providers (ISPs): STM-1 fibre link from GLO-I and STM-1 microwave link from Nigerian Research and Education Network (NgREN) providing the University with two 155Mbps full duplex bandwidth links.

The ABU campus network runs almost entirely on Cisco devices and was designed following the standard 3 layer hierarchical models with core, distribution and access layers in order to provide scalable and reliable network.

3.2.1.1 The Core layer

The core provides a high-speed path (backbone) for moving data packets as efficiently and quickly as possible between distribution layer devices (Lammle, 2014). It was designed and configured with minimal configurations for fast and efficient switching of traffic in and out of the network. All traffic from the Internet or any external network has to pass through a Unified Threat Management (UTM) for inspection before reaching the demilitarized zone (DMZ) where

ABU mail server, web server, students/staff portal, video conferencing and voice call manager is located. Traffic from any external network or DMZ is not allowed to reach the LAN but traffic from the LAN can reach anywhere as shown in Figure 3.1. The core also, has two CISCO 6509 switches that connect all the distribution switches to the entire network, there are also call manager for voice and video conferencing server.

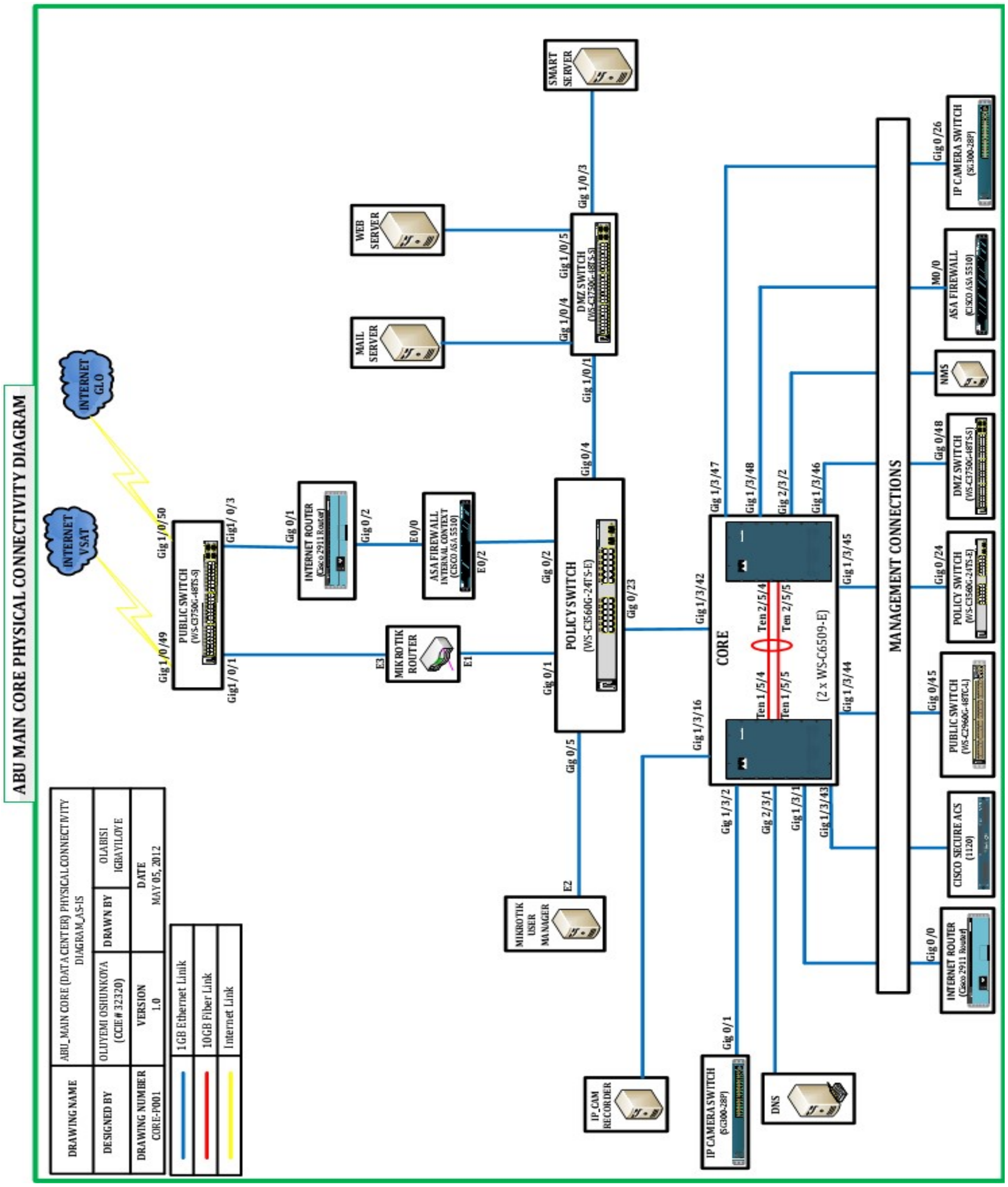


Figure 3.1: Physical Diagram of Core Layer of the ABU Network (ABU Network, 2012)

3.2.1.2 Distribution layer

The distribution layer is sometimes referred to as workgroup layer and is communication point between core and access layer. The primary functions of the distribution layer are to provide routing, filtering, and to determine how packets can reach the core for access or vice visa, this is where all the traffic manipulation typically happens, all local routing decisions and policies are configured (Lammle, 2014).

The distribution layer of the ABU network interconnects Faculties, Departments and other Units of the University to the core layer as in Figure 3.2, the design was implemented with partial redundancy between the distribution and core layer devices; Open Shortest Path First Protocols (OSPF) was configured as the network layer routing protocol, OSPF is probably the best routing protocol to deploy as compared with other routing protocols like Routing Information Protocol (RIP) or Enhanced Interior Gateway Routing Protocol (EIGRP) in a network of this size, but OSPF does not scale well in terms redundancy because it allow some of the active links on the network to be over utilized while others underutilized.

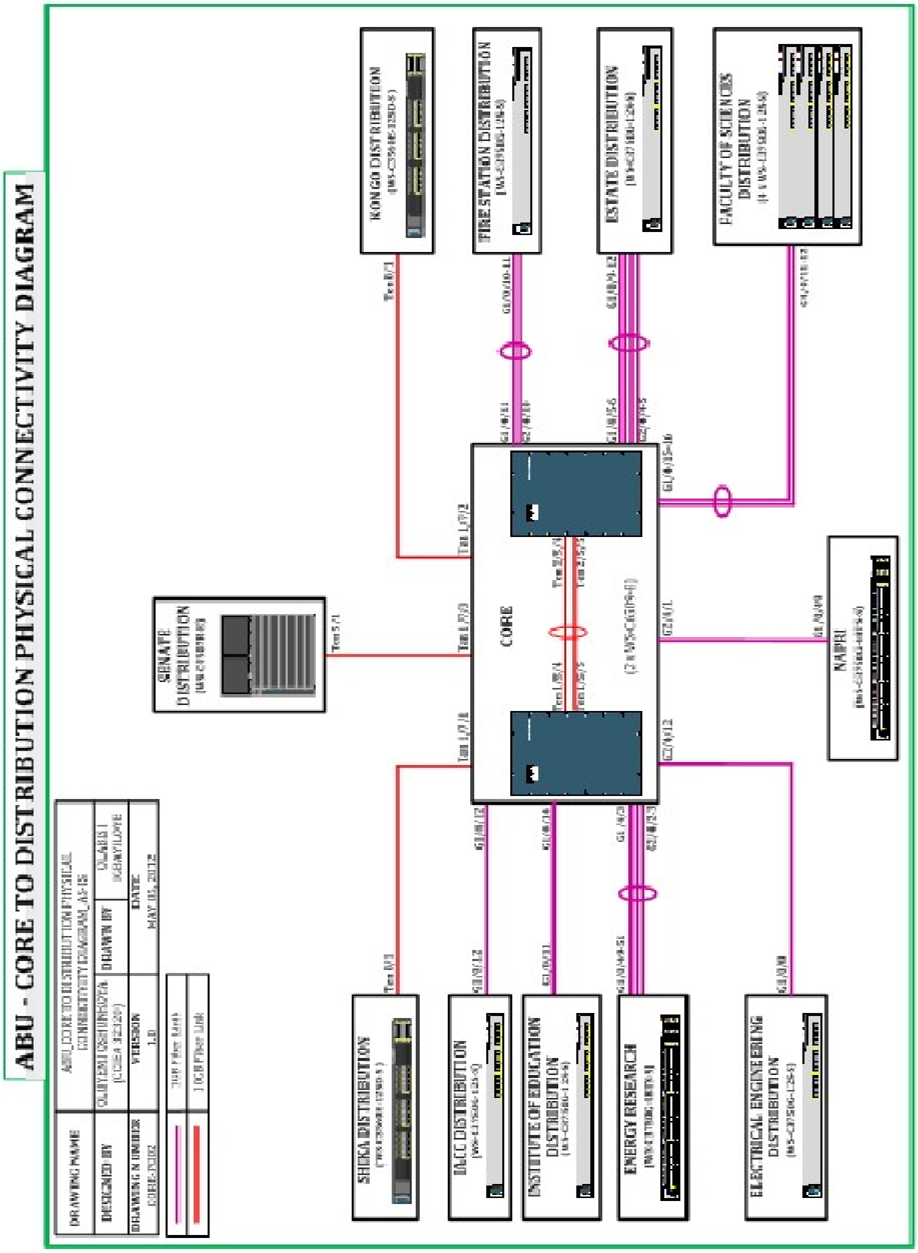
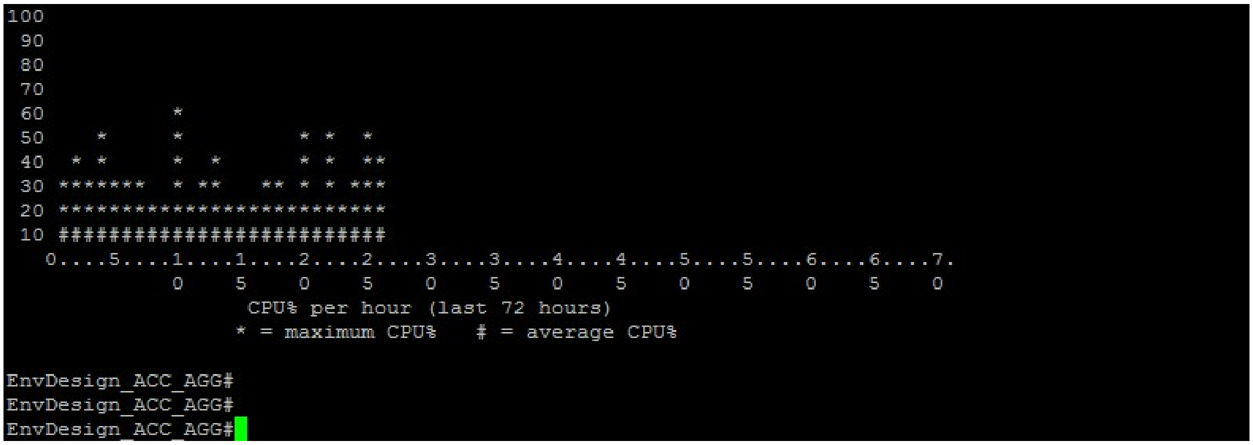


Figure 3.2: Physical Diagram of the Core and Distribution Layer of the ABU Network

Figure 3.3 is a screen shot of CPU utilization of Faculty of environmental design access aggregate switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 60% within 10hrs of browsing the network services on the network and the Internet.

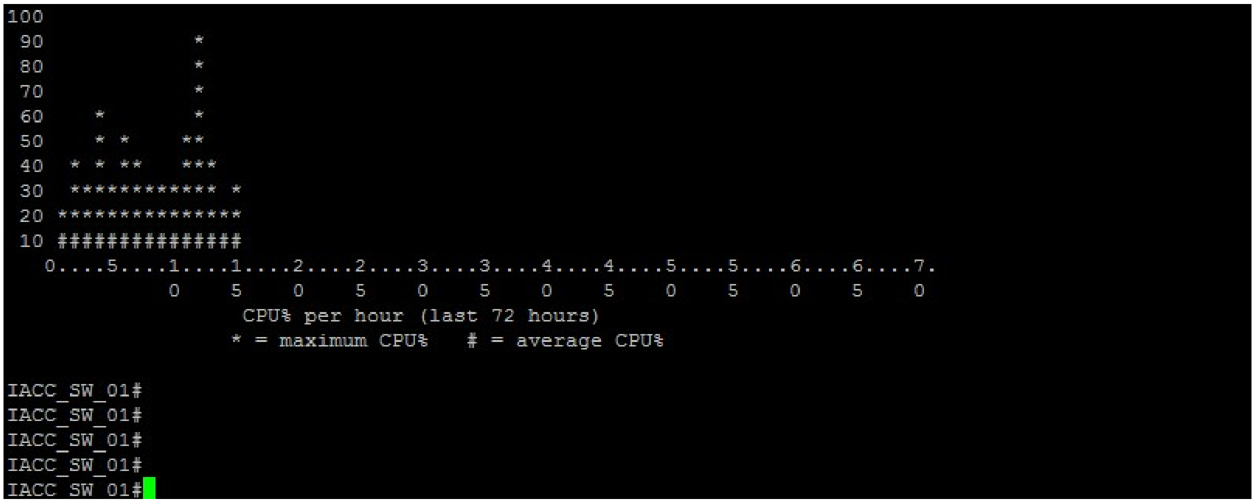


```
100
 90
 80
 70
 60          *
 50    *     *         * *  *
 40  * *     *  *      * *  **
 30 *******  * **   ** * * ***
 20 **************************
 10 ##########################
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%

EnvDesign_ACC_AGG#
EnvDesign_ACC_AGG#
EnvDesign_ACC_AGG#
```

Figure 3.3: Environmental Design Access Aggregate Switch

Figure 3.4 is a screen shot of CPU utilization of Iya Abubakar Computer Centre access aggregate switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 90% within 12hrs of browsing the network services on the network and the Internet.

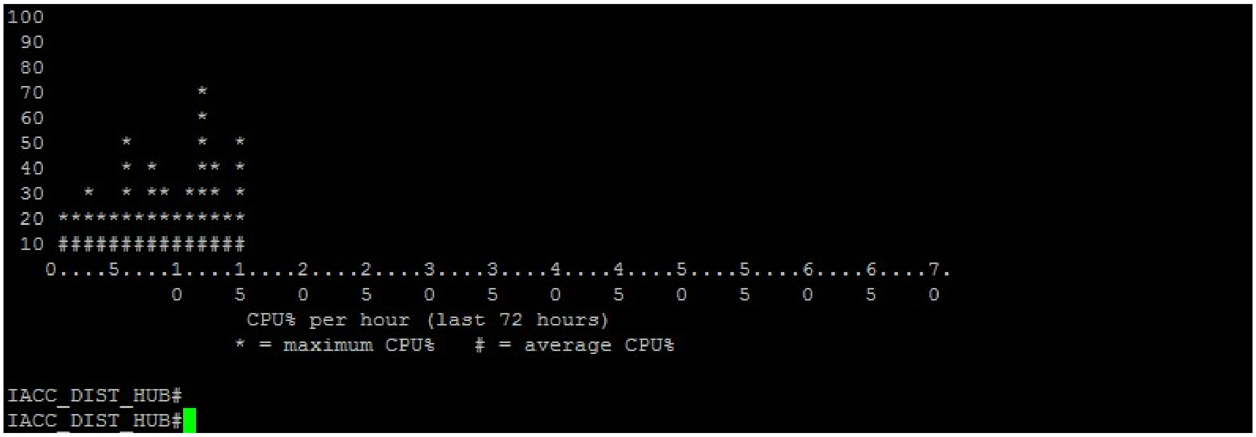


```
100
 90            *
 80            *
 70            *
 60    *       *
 50    * *    **
 40  * * **   ***
 30  ************ *
 20 ***************
 10 ###############
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%

IACC_SW_01#
IACC_SW_01#
IACC_SW_01#
IACC_SW_01#
IACC_SW_01#
```

Figure 3.4: IACC Access Switch

Figure 3.5 is a screen shot of CPU utilization of Iya Abubakar Computer Center distribution switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 70% within 12hrs of browsing the network services on the network and the Internet.

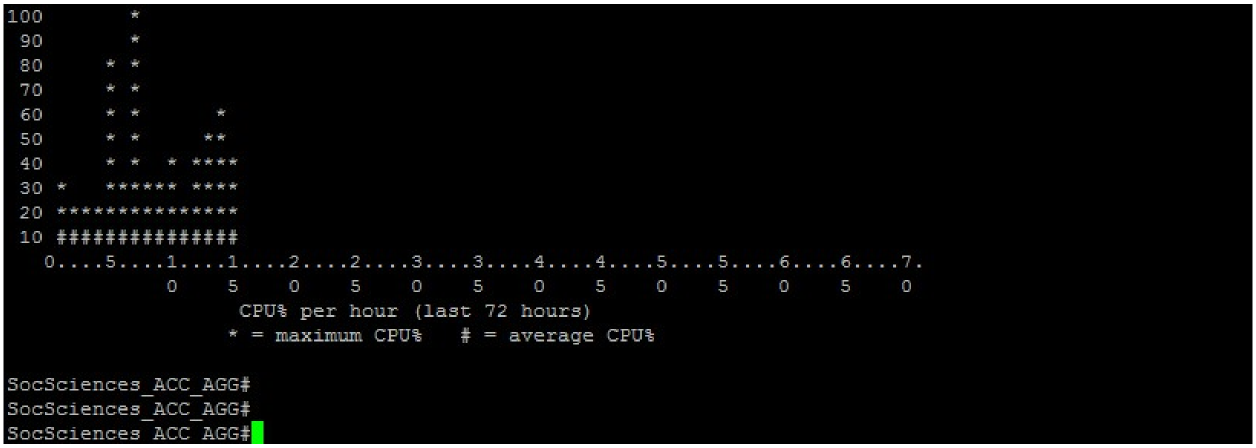


```
100
 90
 80
 70            *
 60            *
 50      *     *  *
 40      * *   ** *
 30   *  * ** *** *
 20 ***************
 10 ###############
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%

IACC_DIST_HUB#
IACC_DIST_HUB#
```

Figure 3.5: IACC Distribution Switch

Figure 3.6 is a screen shot of CPU utilization of Faculty of social science access aggregate switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 100% within 8hrs of browsing the network services on the network and the Internet

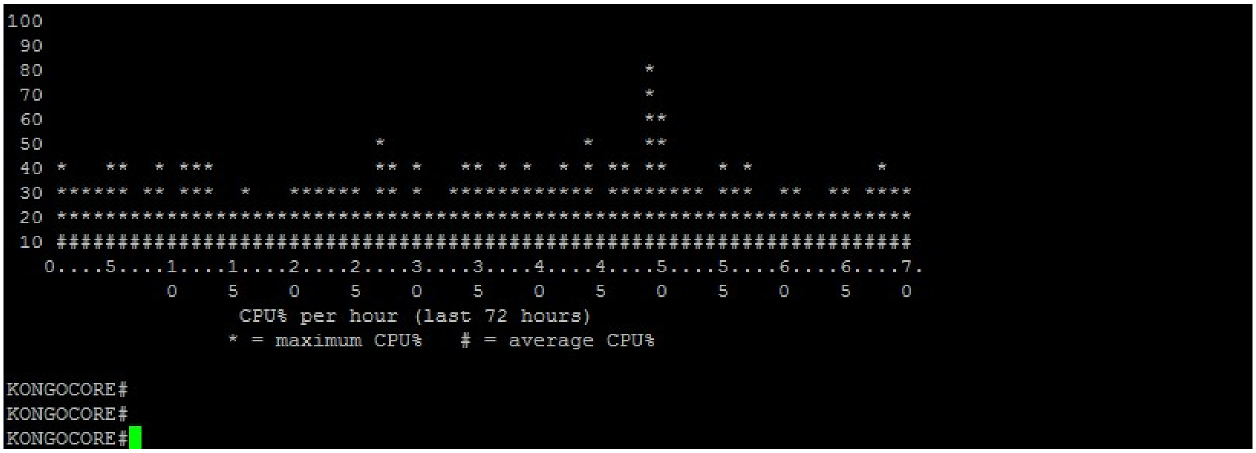


```
100       *
 90       *
 80     * *
 70     * *
 60     * *      *
 50     * *     **
 40     * *  * ****
 30 *   ****** ****
 20 ***************
 10 ###############
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%

SocSciences_ACC_AGG#
SocSciences_ACC_AGG#
SocSciences_ACC_AGG#
```

Figure 3.6: Social Science Access Aggregate Switch

Figure 3.7 is a screen shot of CPU utilization of Institute of administration kongo distribution switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 80% within 49hrs of browsing the network services on the network and the Internet.

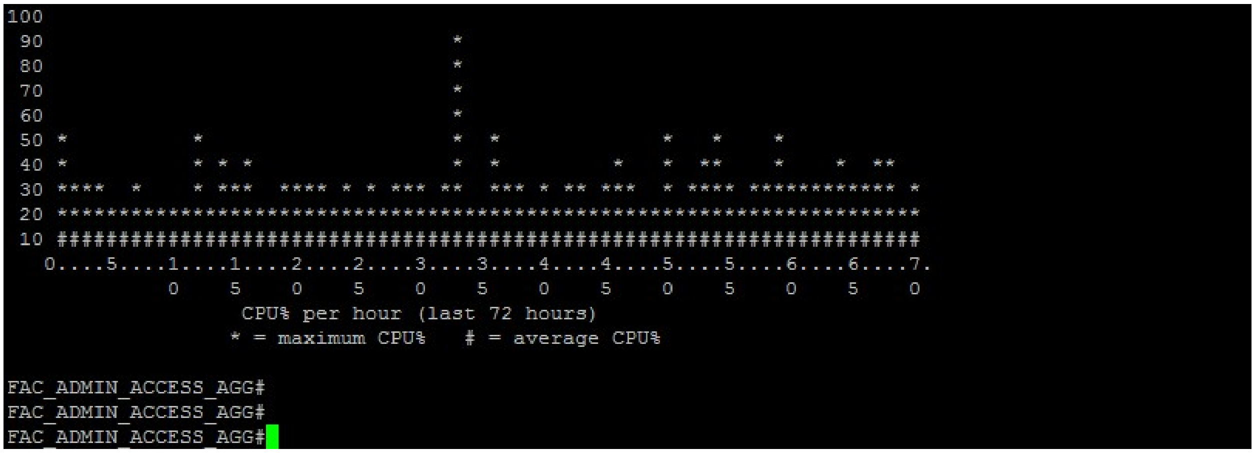


```
100
 90
 80                                                 *
 70                                                 *
 60                                                 **
 50                           *                *    **
 40 *   **  * ***             ** *   ** * *  * * ** **    * *          *
 30 ****** ** ***  *   ****** ** *  ************ ******** ***  **  ** ****
 20 **********************************************************************
 10 ######################################################################
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%

KONGOCORE#
KONGOCORE#
KONGOCORE#
```

Figure 3.7: Kongo Campus Core Switch

Figure 3.8 is a screen shot of CPU utilization of Faculty of Administration access aggregate switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 90% within 33hrs of browsing the network services on the network and the Internet.

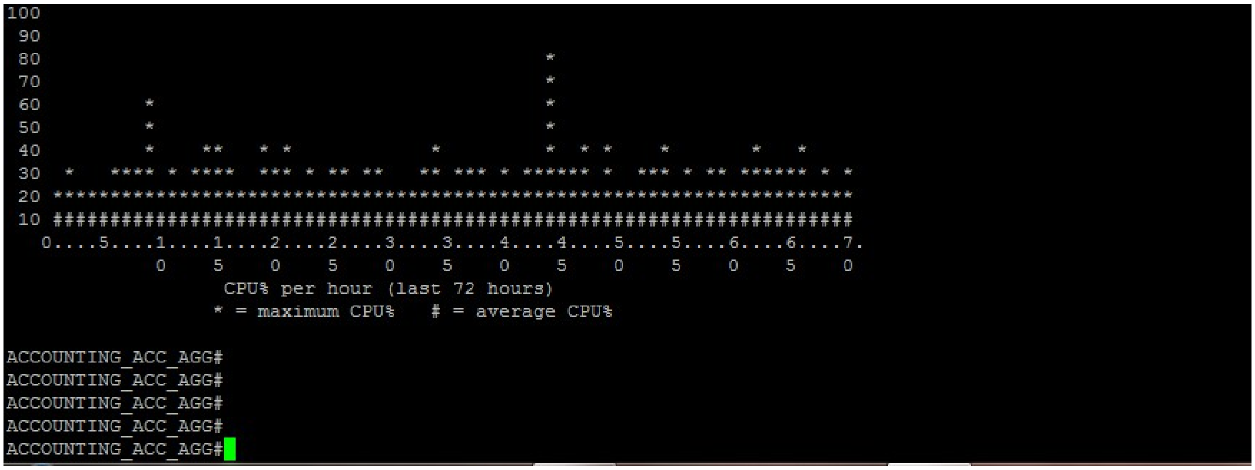


```
100
 90                                 *
 80                                 *
 70                                 *
 60                                 *
 50 *          *                    *  *             *   *    *
 40 *          * * *                *  *         *   *  **    *    *  **
 30 ****  *    * ***  **** * * *** **  *** * ** ***  * **** ************ *
 20 **********************************************************************
 10 ######################################################################
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%

FAC_ADMIN_ACCESS_AGG#
FAC_ADMIN_ACCESS_AGG#
FAC_ADMIN_ACCESS_AGG#
```

Figure 3.8: Faculty of Administration Access Aggregate Switch

Figure 3.9 is a screen shot of CPU utilization of Department of Accounting access aggregate switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 80% within 44hrs of browsing the network services on the network and the Internet.



```
100
 90
 80                                            *
 70                                            *
 60          *                                 *
 50          *                                 *
 40          *    **   * *            *         *  *  *    *       *   *
 30  *   **** * ****  *** * ** **   ** *** * ****** *  *** * ** ****** * *
 20 **********************************************************************
 10 ######################################################################
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
               CPU% per hour (last 72 hours)
              * = maximum CPU%   # = average CPU%

ACCOUNTING_ACC_AGG#
ACCOUNTING_ACC_AGG#
ACCOUNTING_ACC_AGG#
ACCOUNTING_ACC_AGG#
ACCOUNTING_ACC_AGG#
```

Figure 3.9: Department of Accounting Access Aggregate Switch

The screen shots as in Figure 3.3 to Figure 3.9 show some of the findings about the scalability issues on the ABU network active devices. At peak periods, there is very high CPU, RAM and link utilization, which is not ideal for a large and complex campus network. Also, it has been observed that the devices have many numbers of routes in their routing table, which inevitably affects the performance of the hardware's RAM and CPU due to the complexity of running the Shortest Path First (SPF) algorithm per topology changes. If proper IP address planning is implemented on the network, it would help in the redesign of the OSPF routing protocol to reduce the size of the routing table as such increase the processing power and faster lookup.

3.3.1.3 Access layer

The access layer controls user and workgroup access to the internetwork resources, it is sometime referred to as desktop layer, network resources most users needed will be available locally, end user devices such as Laptop, Mobile Phones, and Printers etc access the network through this layer (Lammle, 2014).

Several ABU campus network access layer devices in many Departments and other Units of the University have a flat design, all the access switches runs the default Spanning Tree Protocol (STP) processes allowing only the best candidate switch to be the root for a segment, this will result in many network scalability issues such as layer 2 forwarding loops, frame duplications and excessive flooding due to a high rate of STP Topology Changes (TC). This has been discovered with the addition of more active devices at the Iya Abubakar Computer Center (IACC) node as described in Figures 3.10 and 3.11.

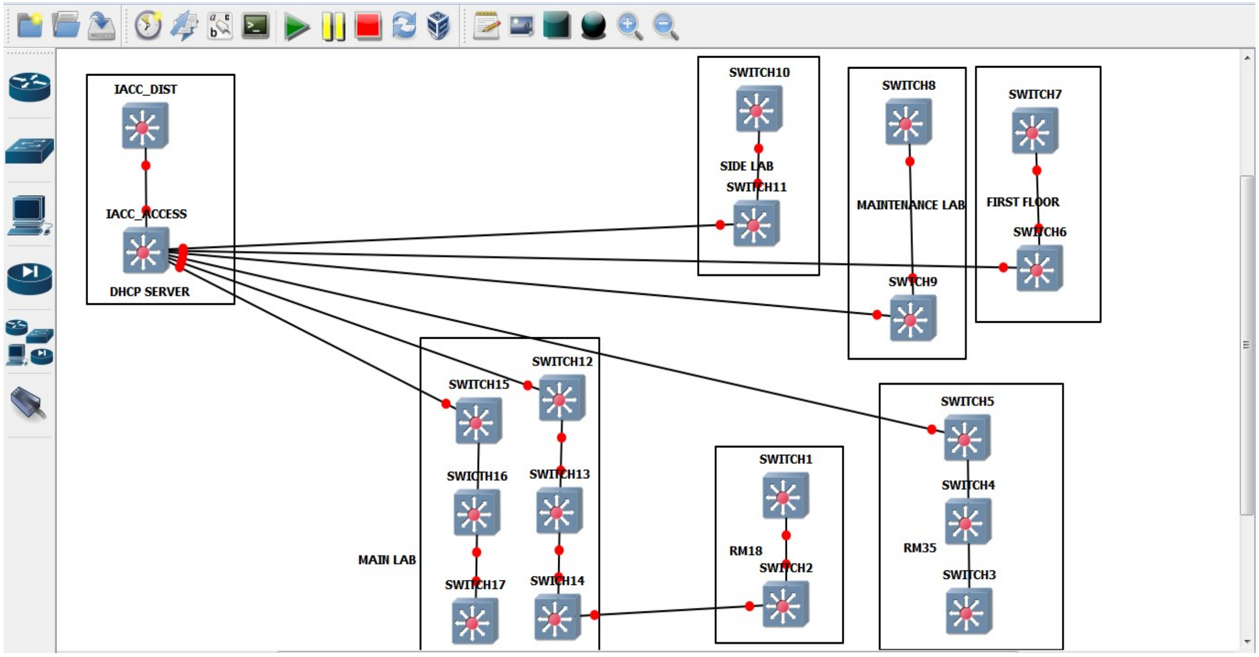
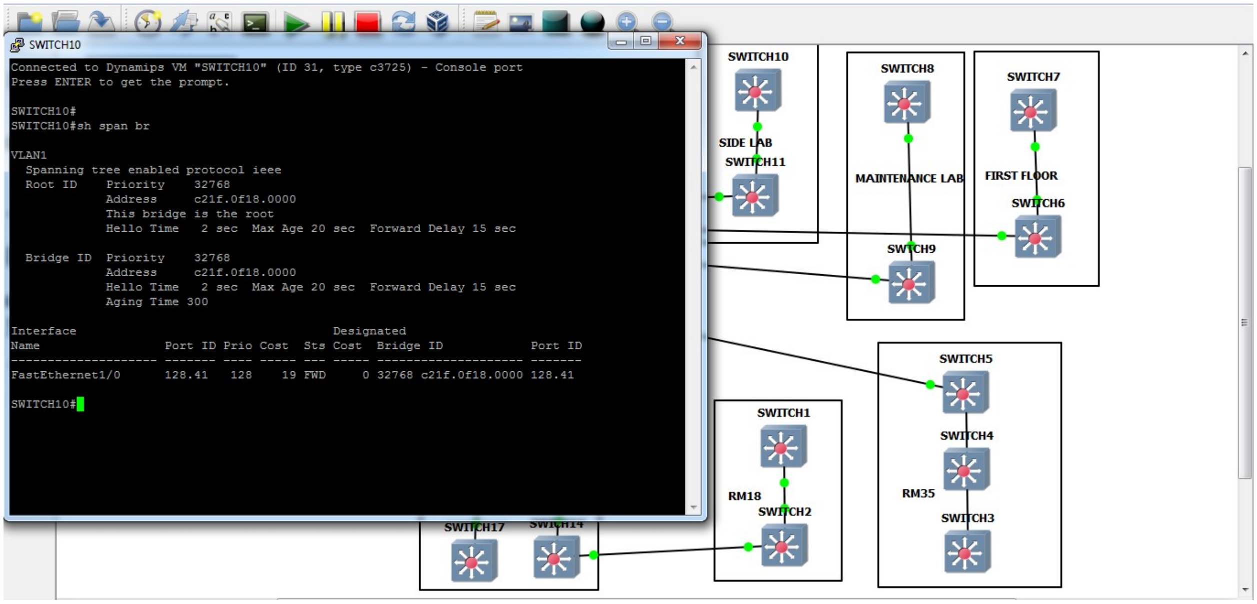


Figure 3.10: IACC Access Layer Devices



```
Connected to Dynamips VM "SWITCH10" (ID 31, type c3725) - Console port
Press ENTER to get the prompt.

SWITCH10#
SWITCH10#sh span br

VLAN1
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     c21f.0f18.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     c21f.0f18.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128    19 FWD     0 32768 c21f.0f18.0000 128.41

SWITCH10#
```

Figure 3.11: IACC Access Layer with STP Root Bridge

From the IACC access layer topology in Figure 3.11, a switch10 in the Side Lab happened to be the root switch on the network because it has the best bridge ID. It means that the layer-2 switch is the root of the STP and all layer-2 frames, Bridge Protocol Data Units (BPDUs) must pass through switch10. Access Aggregate Switch provides the Dynamic Host Configuration Protocol (DHCP) services which will bring a lot of frame duplication and high CPU utilization on the hardware and since layer-2 switching is hardware specific, it will eventually affect the network performance (Rich, 2008). If the STP is well configured, some access aggregate and distribution switches of the ABU campus network ought to be configured as the root switch since they are responsible for DHCP and other services. This will help the end nodes to have a predefined path for both network and data link layer of the Open System Interconnect (OSI) model.

The network scalability issues on the ABU campus network are as a result of poor IP address planning, routing protocol design and configuration, underutilization of the redundant links and spanning tree design and configuration issues which resulted in high CPU, Memory and Link utilization on active devices. The network design can be improved to have higher throughput, minimize delays, and jitter if any of following techniques were properly designed and implemented:

a) Rapid Per VLAN Spanning Tree Plus (RPVST+), or Multiple Spanning Tree Protocol (MST) to optimize spanning tree protocol

b) Advanced Open Shortest Path First Protocol to address to the complexity of the SPF Algorithm.

c) Multi-Protocol Level Switching(MPLS), or Virtual Private LAN Service (VPLS) to address OSPF redundancy issues

d) Efficient IP address planning to address high CPU, memory, and Link utilization.

This research is aimed at utilizing the Multi-Protocol Label Switching (MPLS) to address the scalability issues of a complex network due the following reasons: (Goyal, 2012; Kok-Keong, 2012).

a) Effective route aggregation on the active devices which will results in having smaller routing and faster lookup.
b) Routing lookup based-on label binding in the Forward Information Based (FIB) table rather IP addresses in the routing table
c) Increased in security by segregating physical resources (i.e traffic isolation and separation), configuration and management into independent domains.
d) Flexibility, simplified management and network efficiency.
e) IP Address Re-Use

3.3 METHODOLOGY

The methodology adopted is based on the designed, configurations, and simulations of ABU campus network to identify areas vulnerable to scalability issues, GNS3 and OPNET modeler simulators were used to configure the network with network services such as web server, email server, FTP server, voice and video server, and performance parameters such as throughput, delay (end-to-end, queuing), jitter, and server load were configured to test the performance of the active devices at the access, distribution, and core layers. The proposed designed solution (MPLS technology) was also adopted with some justifiable reasons and simulated; the result output showed some significant improvement of the active devices performance which showed MPLS technology performed better in a complex campus network even with frequent addition of more services and end users.

3.3.1 ABU Campus Network Modeling and Emulation using GNS3

ABU campus network (as in Figure 3.12) was modeled and designed in GNS3 emulation environment with IOS release 15.2 (4) S3 and termed Scenario 1, the routers in the topology were configured to run OSPF routing protocol to emulate the real live ABU network design and configuration, the network was hierarchically configured having basic intra area and inter area routes. From Figure 3.12, the redundant links between Electrical Engineering department distribution switch and Iya Abubakar Computer Center distribution and any other redundant links on the network were not utilized at all as the default OSPF configuration allows selection of best shortest path to destination alone.

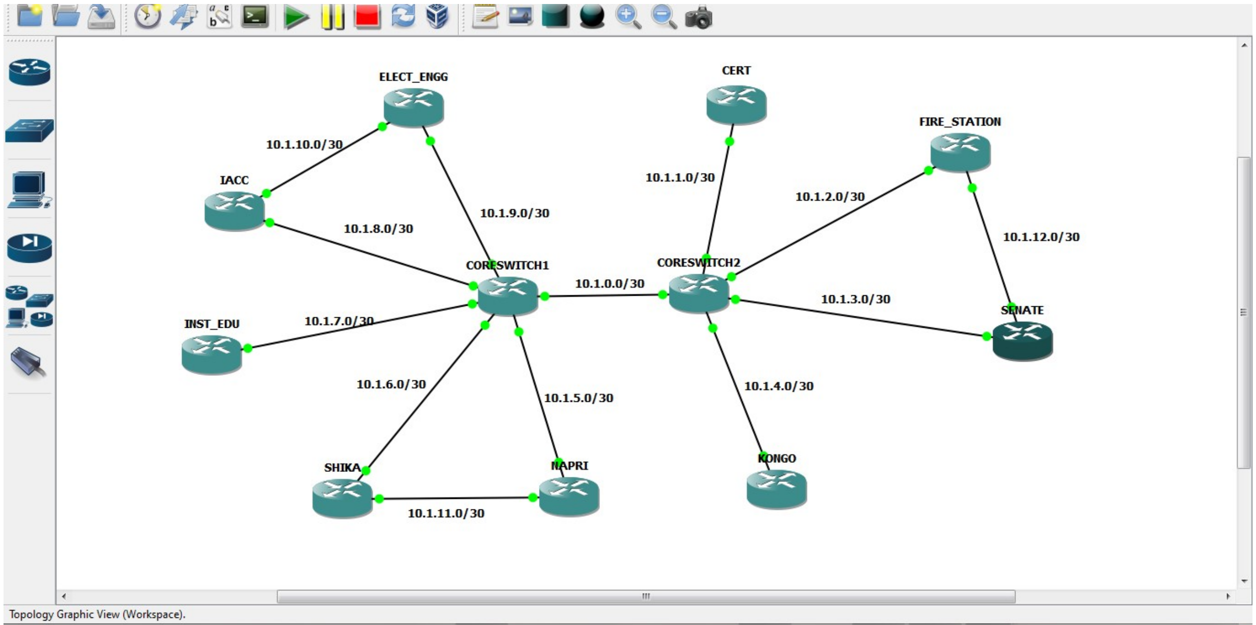
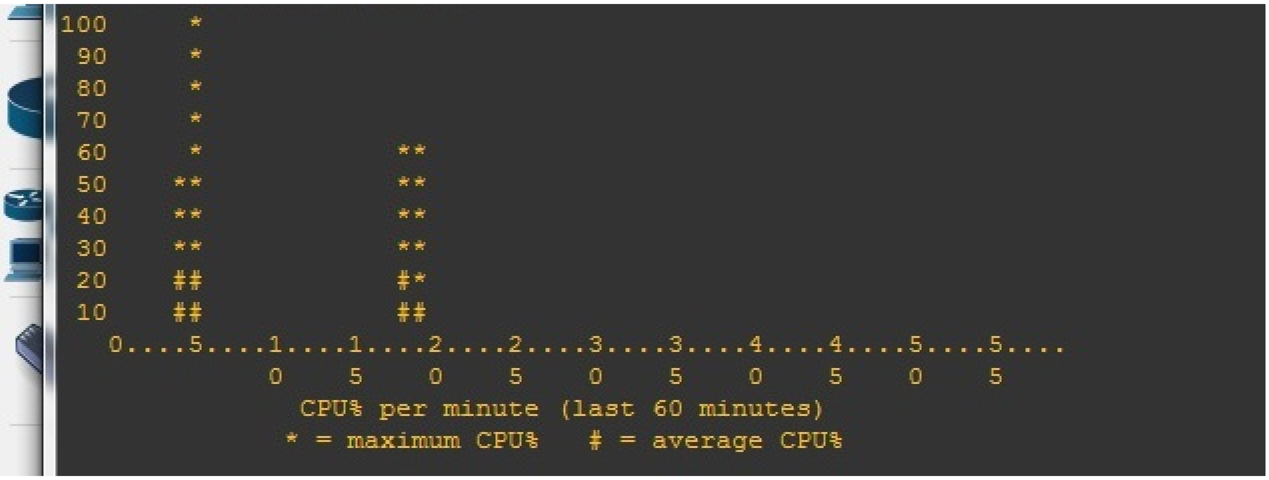


Figure 3.12 Scenario 1: ABU Campus Network Design Model

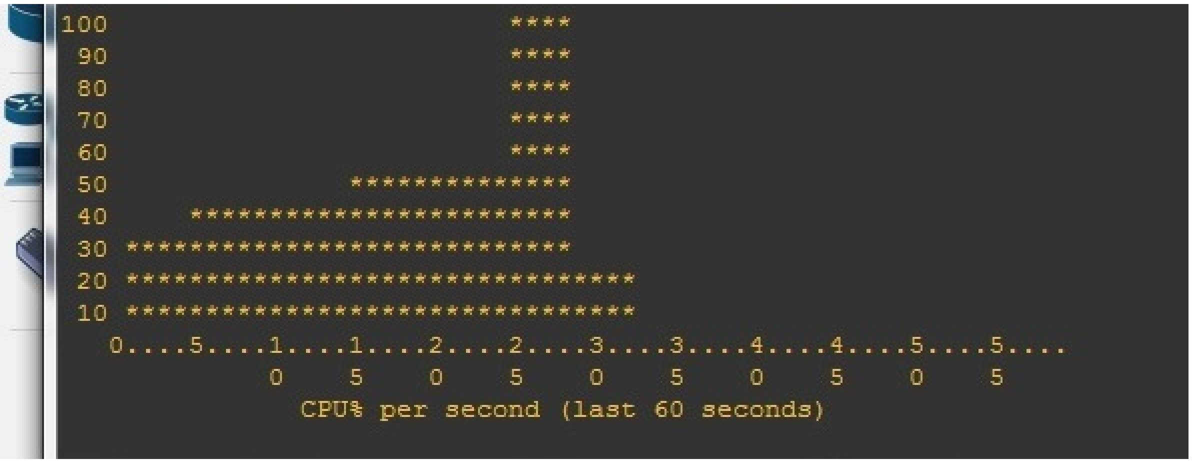
Figure 3.13 shows the screen shot of CPU utilization of the Senate building distribution switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 100% within the emulation process time.



```
100     *
 90     *
 80     *
 70     *
 60     *            **
 50    **            **
 40    **            **
 30    **            **
 20    ##            #*
 10    ##            ##
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 3.13: Senate Building Distribution Switch

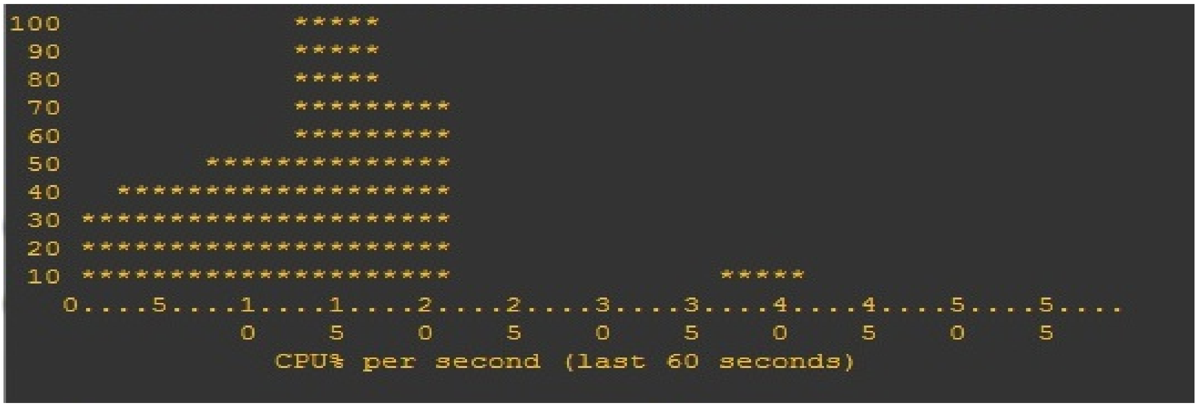
Figure 3.14 shows the screen shot of CPU utilization of the Senate building distribution switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 100% within the emulation process time.



```
100                         ****
 90                         ****
 80                         ****
 70                         ****
 60                         ****
 50               **************
 40     ************************
 30 ****************************
 20 ********************************
 10 ********************************
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)
```

Figure 3.14: Senate Building Distribution Switch

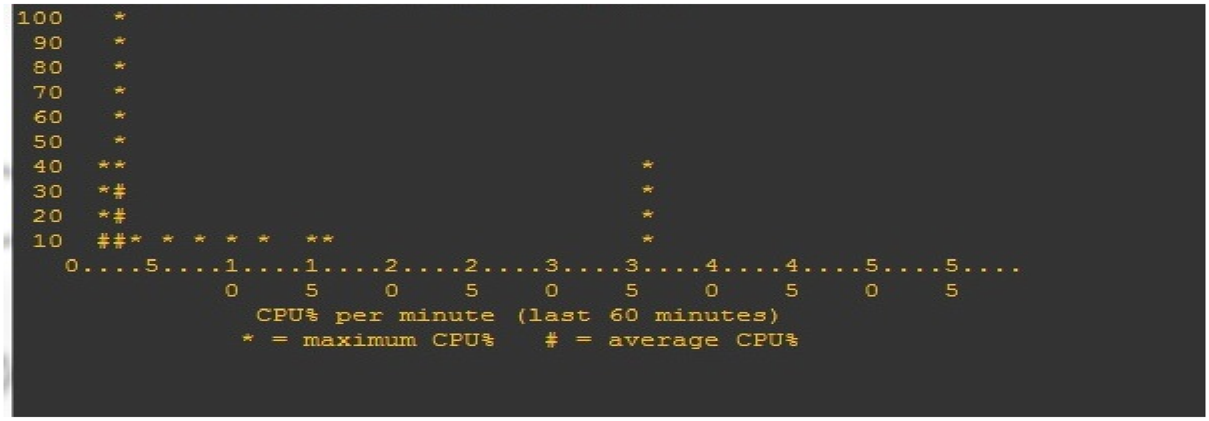
Figure 3.15 shows the screen shot of CPU utilization of Iya Abubakar Computer Center distribution switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 100% within the emulation process time.



```
100             *****
 90             *****
 80             *****
 70             *********
 60             *********
 50        **************
 40   *******************
 30 *********************
 20 *********************
 10 *********************               *****
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)
```

Figure 3.15: IACC Distribution Switch

Figure 3.16 shows the screen shot of CPU utilization of Institute of Administration (Kongo campus) distribution switch, the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be shown that the CPU utilization reached 100% within the emulation process time.



```
100   *
 90   *
 80   *
 70   *
 60   *
 50   *
 40  **                                *
 30  *#                                *
 20  *#                                *
 10  ##* * * * *  **                   *
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 3.16: Kongo Campus Distribution Switch

Figure 3.13 to Figure 3.16 show the emulated output of the some of the devices on the ABU campus network and the way they behave at peak period. It can be deduced that there is significant increase in the CPU, RAM and link utilization on the network hardware, affected largely by the poor design of STP and OSPF protocols. There is need to address the design issues which would help to achieve a scalable design and provide optimum network resources utilization.

3.3.2 ABU MPLS Network Modeling and Emulation using GNS3

ABU Campus network (as in Figure 3.17) was modeled and designed in GNS3 emulation environment with IOS release 15.2 (4) S3 and termed Scenario 2, the routers in the topology were configured to run OSPF and MPLS technology. This is the proposed design solution to address the scalability issues of the network by providing logical redundant paths across the entire domain provided there is at least one physical path to any given destination. Routing functionality is based on “label" not IP address as in the case of OSPF and this is to address the problem of hop-by-hop destination based routing that processes packets based on the IP header, which will result in faster routing lookup.

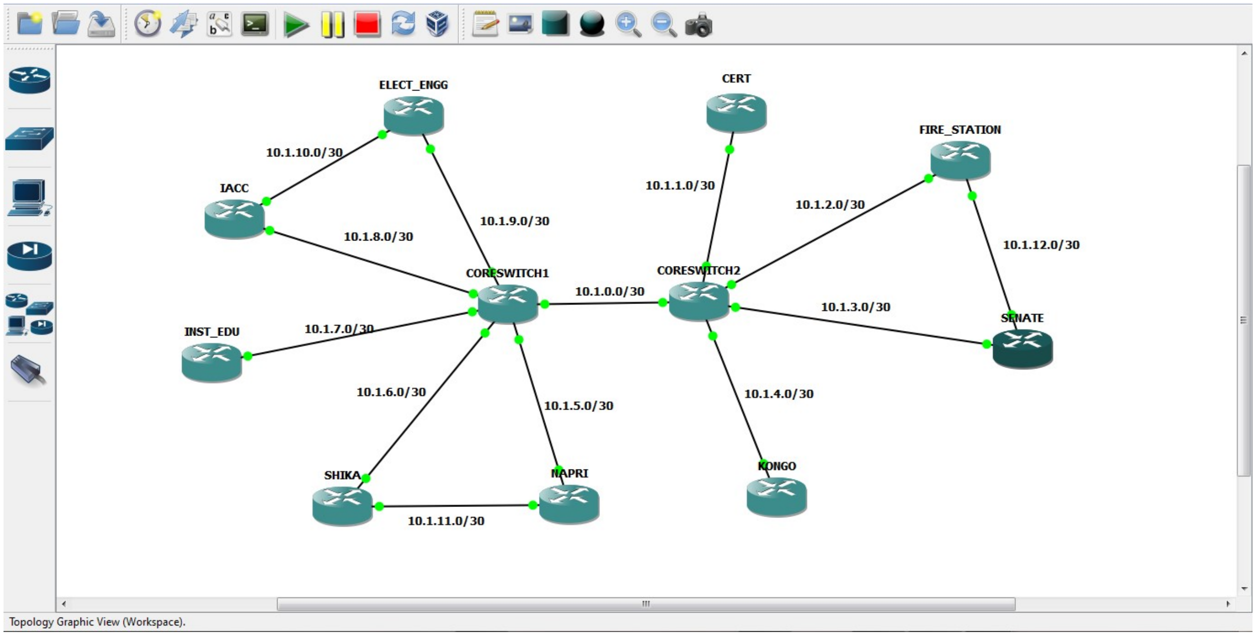
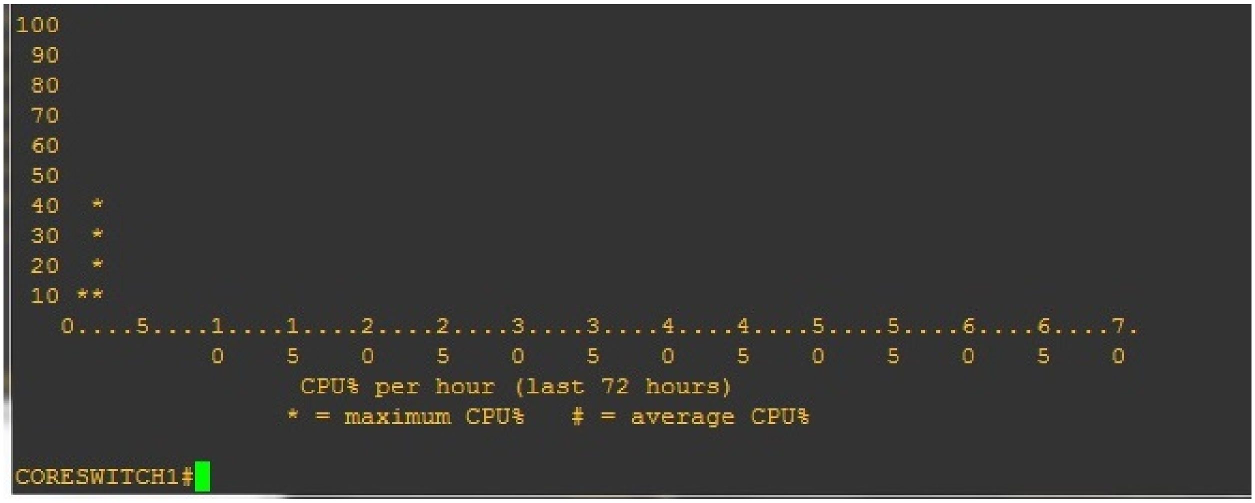


Figure 3.17 Scenario 2: MPLS-Enabled ABU Campus Network Design Model

Figure 3.18 shows the screen shot of CPU utilization of Core switch at the datacenter; the vertical axis represents the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 40% within the first 2hrs of the emulation process.

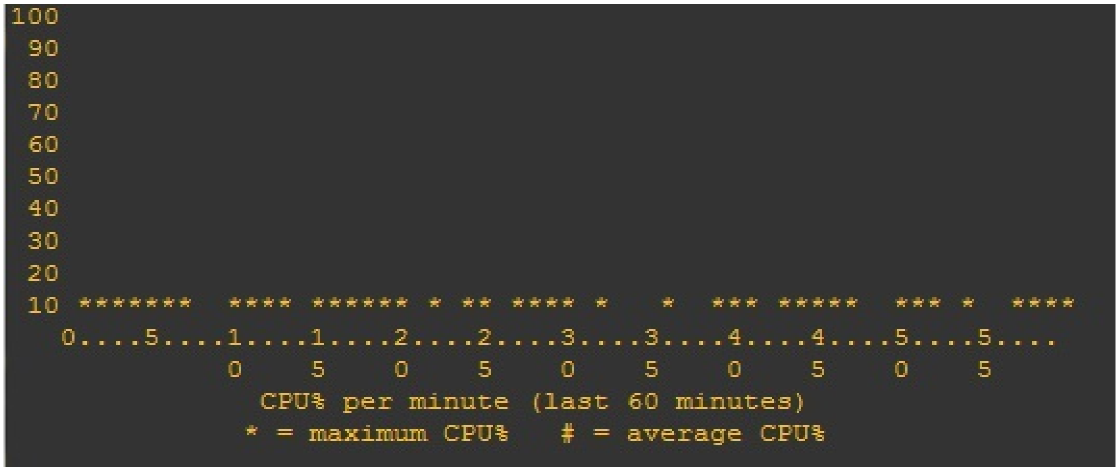


```
100
 90
 80
 70
 60
 50
 40  *
 30  *
 20  *
 10 **
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%

CORESWITCH1#
```

Figure 3.18: Datacenter Core Switch

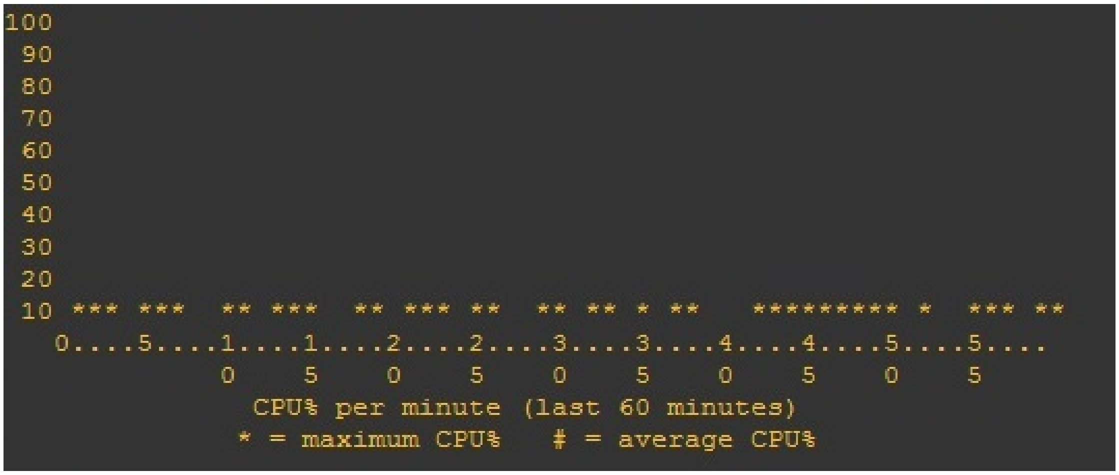
Figure 3.19 shows the screen shot of CPU utilization of Department of Electrical and Computer Engineering distribution switch; the vertical axis represent the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 10% within 60hrs of the emulation process.



```
100
 90
 80
 70
 60
 50
 40
 30
 20
 10 *******  **** ****** * ** **** *   *  *** *****  *** *  ****
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 3.19: Electrical and Computer Engineering Department Distribution Switch

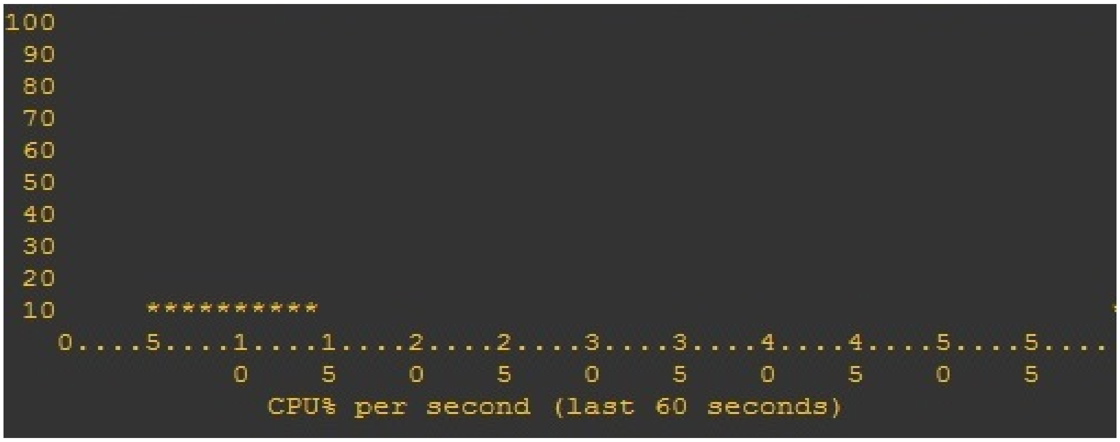
Figure 3.20 shows the screen shot of CPU utilization of Iya Abubakar Computer Center distribution switch; the vertical axis represents the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 10% within 60hrs of the emulation process.



```
100
 90
 80
 70
 60
 50
 40
 30
 20
 10 *** ***  ** ***  ** *** **  ** ** * **   ********* *  *** **
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
                CPU% per minute (last 60 minutes)
               * = maximum CPU%   # = average CPU%
```

Figure 3.20: IACC Distribution Switch

Figure 3.21 shows the screen shot of CPU utilization of institute of Administration distribution switch; the vertical axis represents the utilization in percentage while the horizontal represent the time. It can be seen that the CPU utilization reached 10% within 15hrs of the emulation process.



```
100
 90
 80
 70
 60
 50
 40
 30
 20
 10     **********                                              *
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
                CPU% per second (last 60 seconds)
```

Figure 3.21: Kongo Campus Distribution Switch

The improved design, using MPLS in the campus network showed significant improvement in CPU, RAM and Link utilization, which has been shown in Figure 3.18 to Figure 3.21.

3.3.3 ABU Campus Network Design and Configuration Using OPNET Modeler

The ABU campus network design was adopted from GNS3 emulator tools to allow testing of additional features, and network services such as File Transfer Protocol (FTP), Web, Email, Voice and video traffic, the services were configured and data geneated using performance parameter; end-to-end delay, queuing delay, jitter, throughput, and server load, the steps adopted in modeling and simulation in the OPNET evironment is presented in the OPNET architecture algorithmic decribed in the flow diagram in Figure 3.22.

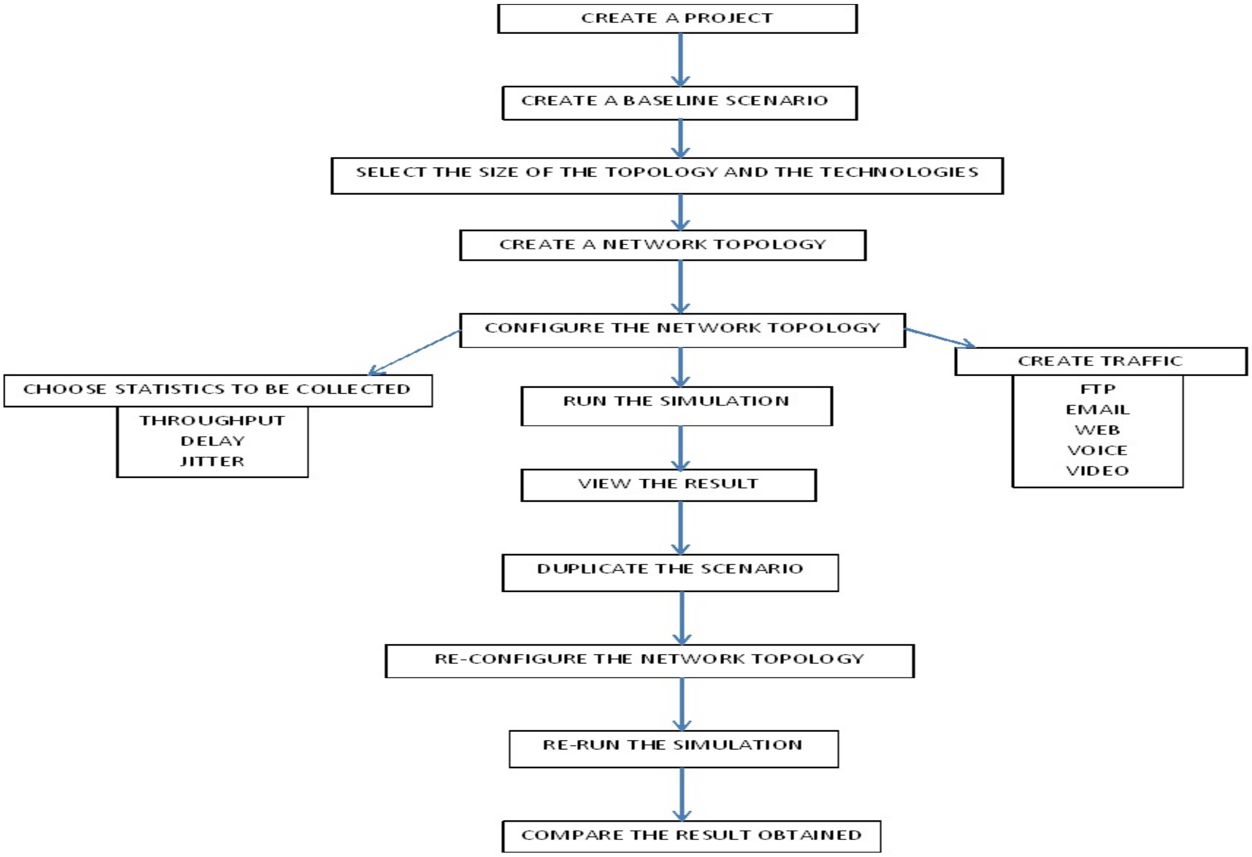

CREATE A PROJECT
CREATE A BASELINE SCENARIO
SELECT THE SIZE OF THE TOPOLOGY AND THE TECHNOLOGIES
CREATE A NETWORK TOPOLOGY
CONFIGURE THE NETWORK TOPOLOGY
CHOOSE STATISTICS TO BE COLLECTED
THROUGHPUT
DELAY
JITTER
CREATE TRAFFIC
FTP
EMAIL
WEB
VOICE
VIDEO
RUN THE SIMULATION
VIEW THE RESULT
DUPLICATE THE SCENARIO
RE-CONFIGURE THE NETWORK TOPOLOGY
RE-RUN THE SIMULATION
COMPARE THE RESULT OBTAINED

Figure 3.22: OPNET Flow diagram

Scenario 1 as in Figure 3.23 shows the ABU Campus network as it is being implemented; running OSPF routing protocols to exchange information between the devices. The OSPF was configured with basic features such as; subnets, normal areas, authentications, etc. to establish adjacency and update the link state topological database. Network services such as FTP, Web, Mail, Voice, and Video services were configured to subject the network's hardware on a traffic flow.

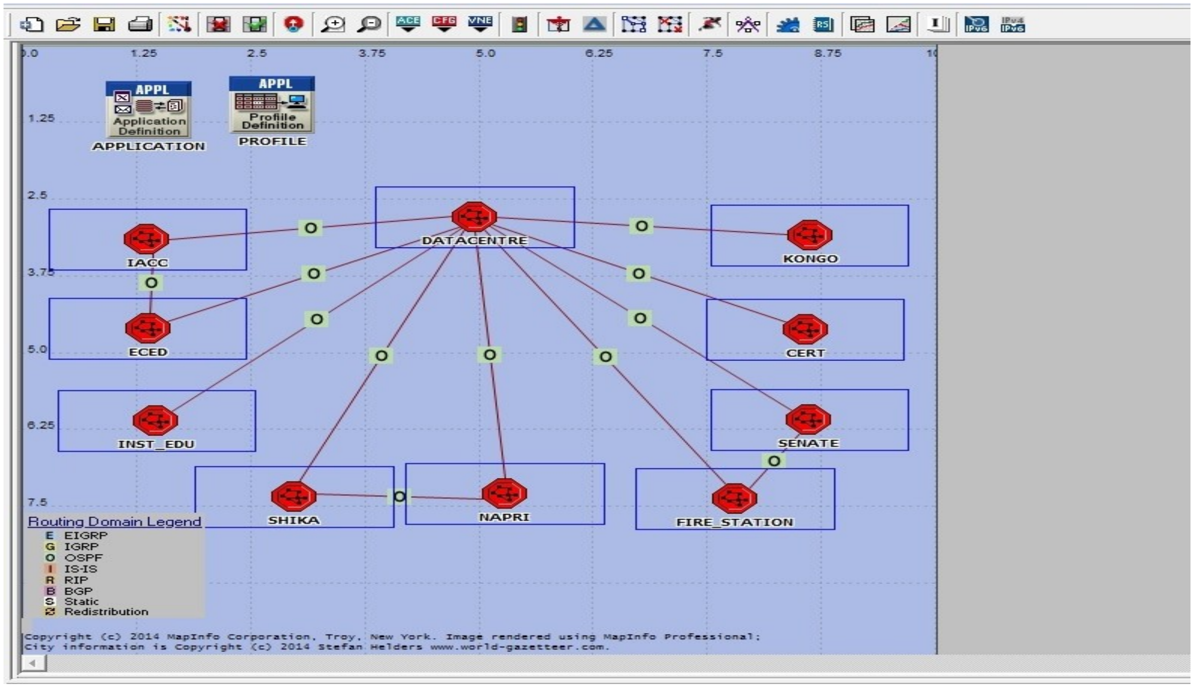


Figure 3.23: Scenario 1: ABU Campus Network Simulation Model

Scenario 2 as in Figure 3.24 shows the ABU Campus network configured with MPLS technology, the simulation model was used as an imrprovement in addressing the scabalilty issues in conventional OSPF network. Network services such as FTP, web, mail, voice and video services were configured (the configuration steps are shown in Figure 3.14 to Figure 3.16). Data was generated and collected from both conventional OSPF network and MPLS network.

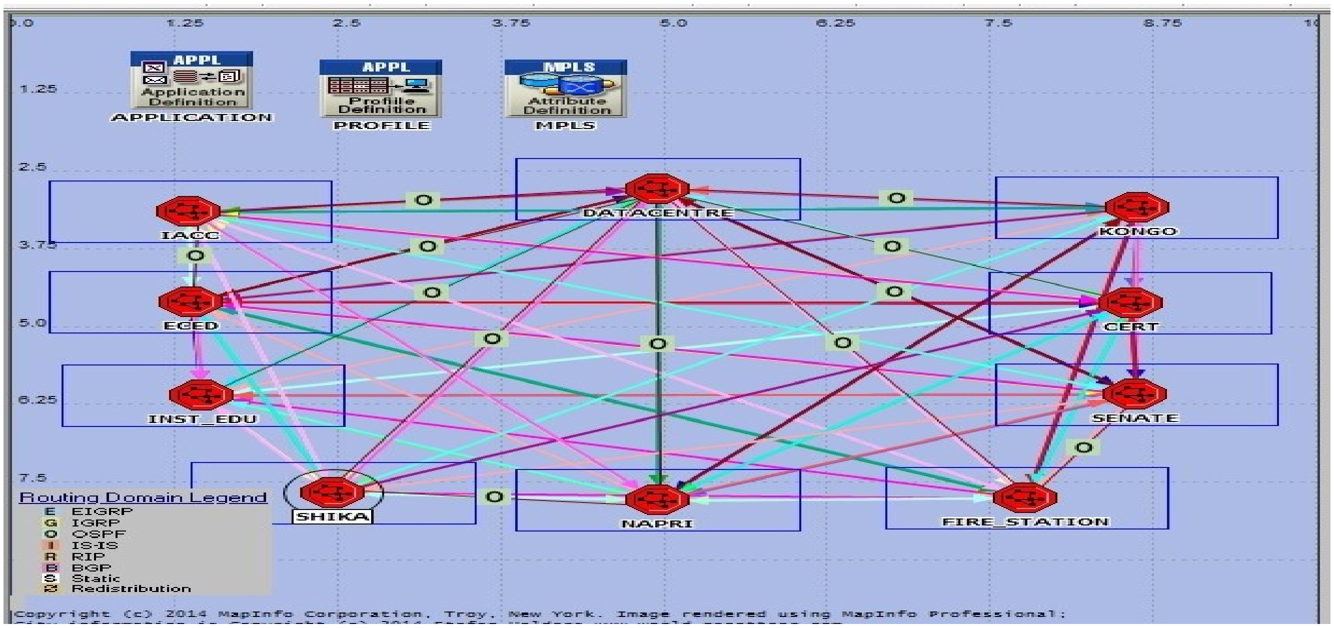
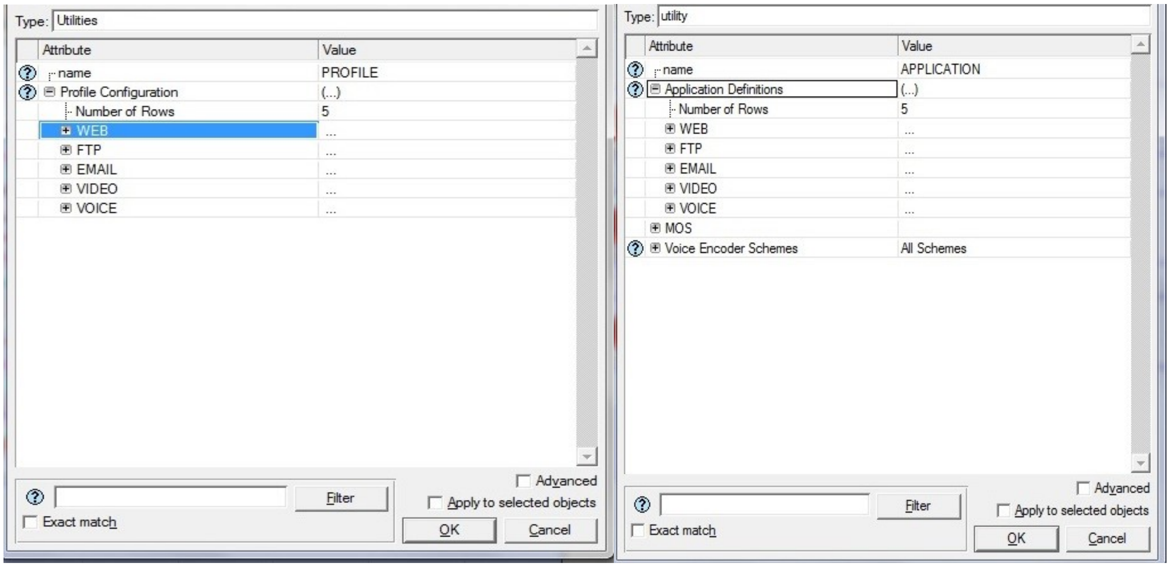


Figure 3.24: Scenario 2: MPLS-Enabled ABU Campus Network Simulation Model



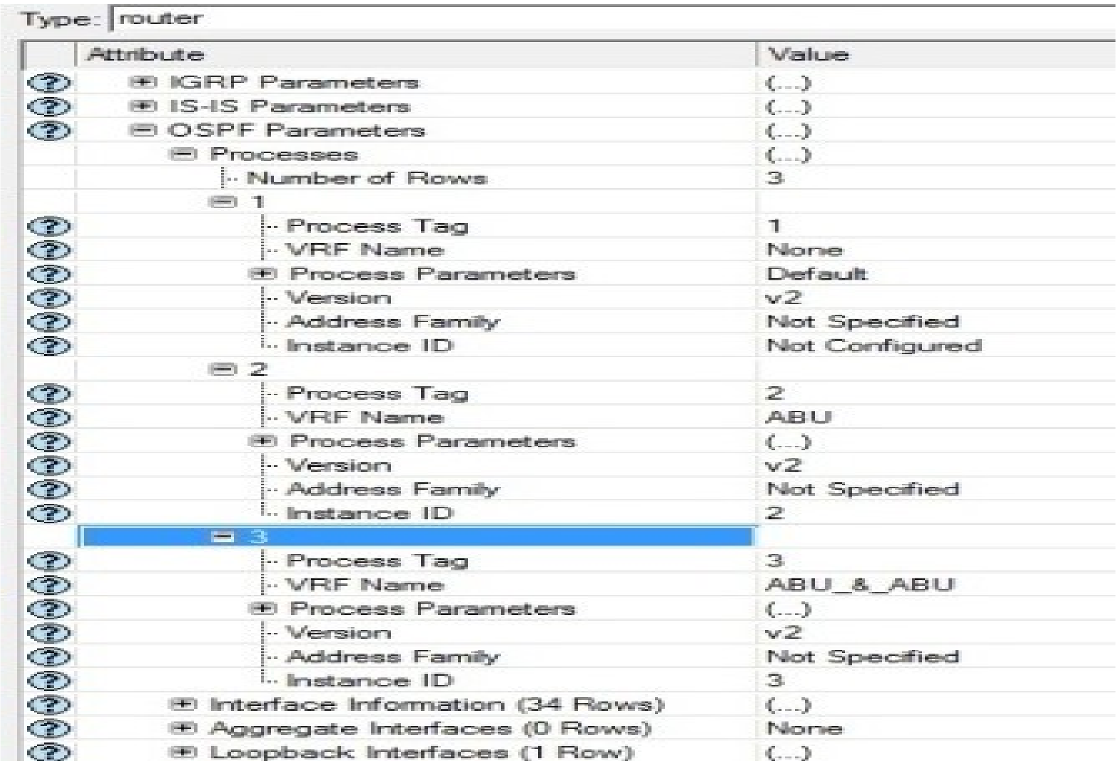
Type: Utilities

Attribute	Value
name	PROFILE
⊟ Profile Configuration	(...)
Number of Rows	5
⊞ WEB	...
⊞ FTP	...
⊞ EMAIL	...
⊞ VIDEO	...
⊞ VOICE	...

Type: utility

Attribute	Value
name	APPLICATION
⊟ Application Definitions	(...)
Number of Rows	5
⊞ WEB	...
⊞ FTP	...
⊞ EMAIL	...
⊞ VIDEO	...
⊞ VOICE	...
⊞ MOS	
⊞ Voice Encoder Schemes	All Schemes

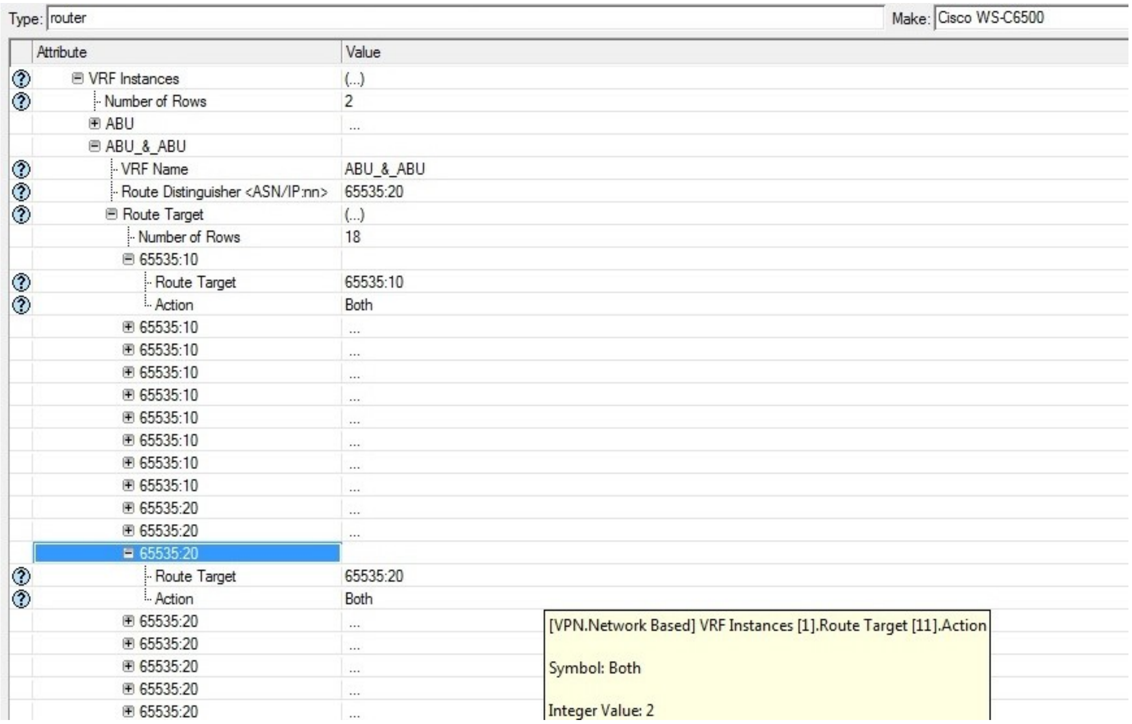
Figure 3.25: Profile and Application Attributes of the Services Configured



Type: router

Attribute	Value
⊞ IGRP Parameters	(...)
⊞ IS-IS Parameters	(...)
⊟ OSPF Parameters	(...)
⊟ Processes	(...)
Number of Rows	3
⊟ 1	
Process Tag	1
VRF Name	None
⊞ Process Parameters	Default
Version	v2
Address Family	Not Specified
Instance ID	Not Configured
⊟ 2	
Process Tag	2
VRF Name	ABU
⊞ Process Parameters	(...)
Version	v2
Address Family	Not Specified
Instance ID	2
⊟ 3	
Process Tag	3
VRF Name	ABU_&_ABU
⊞ Process Parameters	(...)
Version	v2
Address Family	Not Specified
Instance ID	3
⊞ Interface Information (34 Rows)	(...)
⊞ Aggregate Interfaces (0 Rows)	None
⊞ Loopback Interfaces (1 Row)	(...)

Figure 3.26: MPLS Configuration 1



Type: router Make: Cisco WS-C6500

Attribute	Value
⊟ VRF Instances	(...)
Number of Rows	2
⊞ ABU	...
⊟ ABU_&_ABU	
VRF Name	ABU_&_ABU
Route Distinguisher <ASN/IP:nn>	65535:20
⊟ Route Target	(...)
Number of Rows	18
⊟ 65535:10	
Route Target	65535:10
Action	Both
⊞ 65535:10	...
⊞ 65535:10	...
⊞ 65535:10	...
⊞ 65535:10	...
⊞ 65535:10	...
⊞ 65535:10	...
⊞ 65535:10	...
⊞ 65535:10	...
⊞ 65535:20	...
⊞ 65535:20	...
⊟ 65535:20	
Route Target	65535:20
Action	Both
⊞ 65535:20	...
⊞ 65535:20	...
⊞ 65535:20	...
⊞ 65535:20	...
⊞ 65535:20	...

[VPN.Network Based] VRF Instances [1].Route Target [11].Action

Symbol: Both

Integer Value: 2

Figure 3.27: MPLS Configuration 2

Figure 3.28 shows the MPLS design and configuration flowchart algorithms as an improved campus network design in OPNET Modeler.

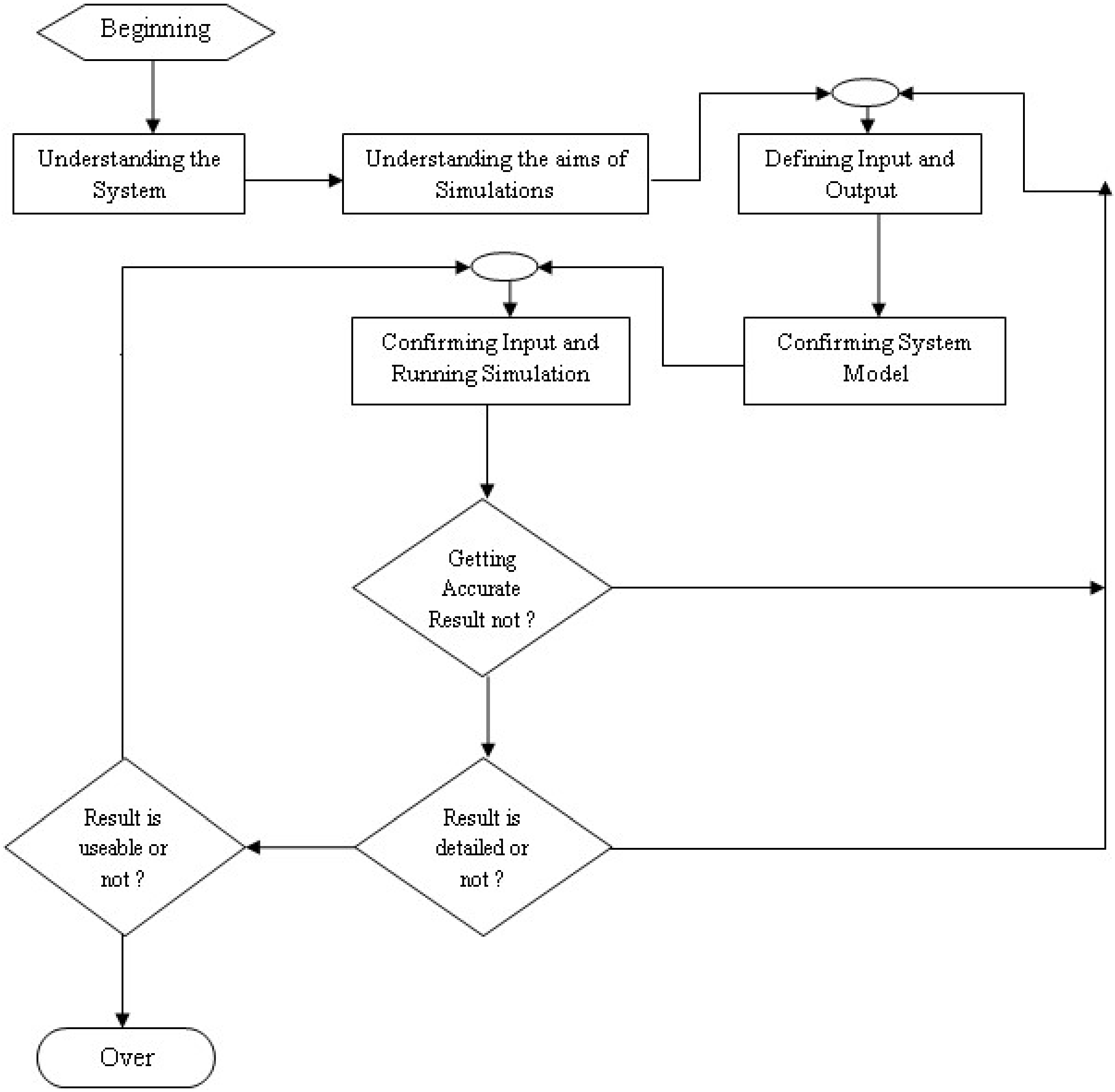

Beginning
Understanding the System
Understanding the aims of Simulations
Defining Input and Output
Confirming Input and Running Simulation
Confirming System Model
Getting Accurate Result not ?
Result is useable or not ?
Result is detailed or not ?
Over

Figure 3.28: MPLS Design and Configuration Processing Flowchart

CHAPTER FOUR

RESULTS AND DISCUSSIONS

4.1 INTRODUCTION

This chapter discusses the result obtained for performance metrics; throughput, end-to-end delay, queuing delay, jitter, and server load in the cause of simulation process, and CPU utilization, RAM utilization and link utilization in the cause of validation processes.

4.2 DATA COLLECTION AND ANALYSIS

The modeled ABU campus network in OPNET modeler environment is simulated for three hours averagely to represent the peak period, data was generated and collected using the performance parameters such as; Throughput, Jitter, Delay (End-to-end, Queuing), and server load.

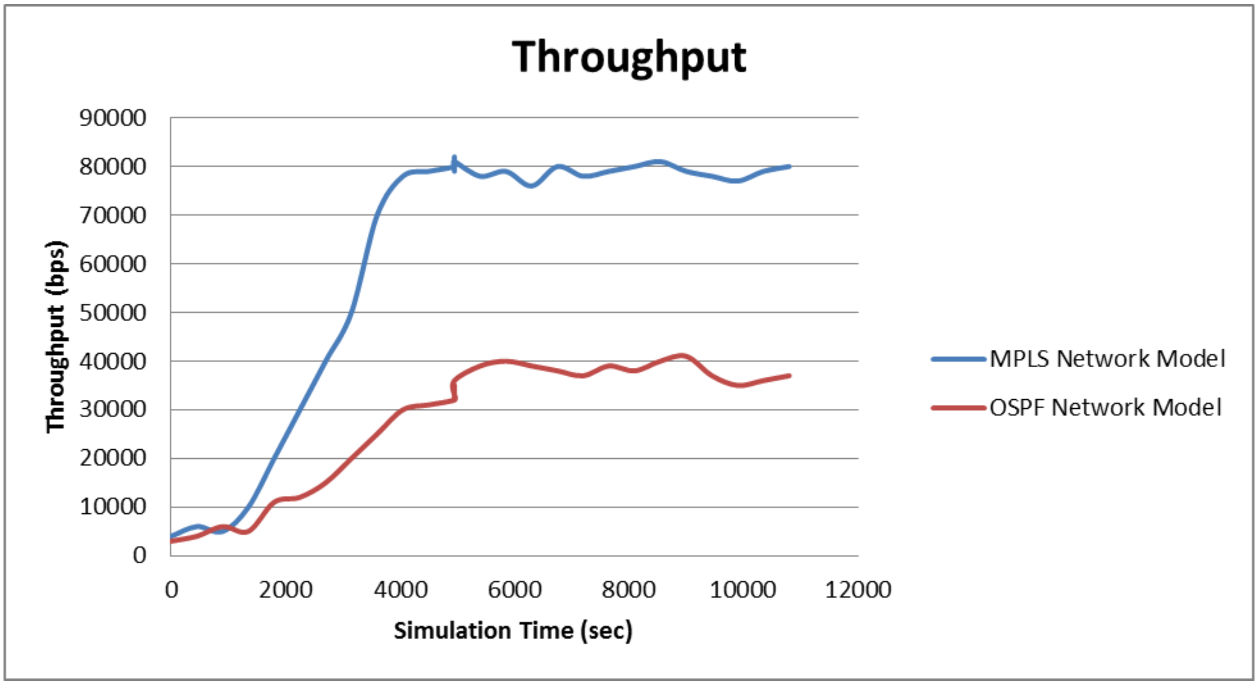


Figure 4.1: Throughput

In Figure 4.1 the throughput for incoming and outgoing traffic was measured, and it can be seen that the throughput for the existing ABU campus network design and configuration (i.e default

OSPF network) increased rapidly throughout the simulation period from 4,000 (bps) to 81,000 (bps) respectively, it can also be seen that the throughput for MPLS-Enabled ABU campus network design and configuration increased rapidly throughout the simulation from 3,000 (bps) to 41,000 bps respectively at the end of the simulation period. It can be deduced from Figure 4.1 that ABU campus network with existing design have a lower throughput for both incoming and outgoing traffic compared with MPLS-Enabled ABU Campus network.

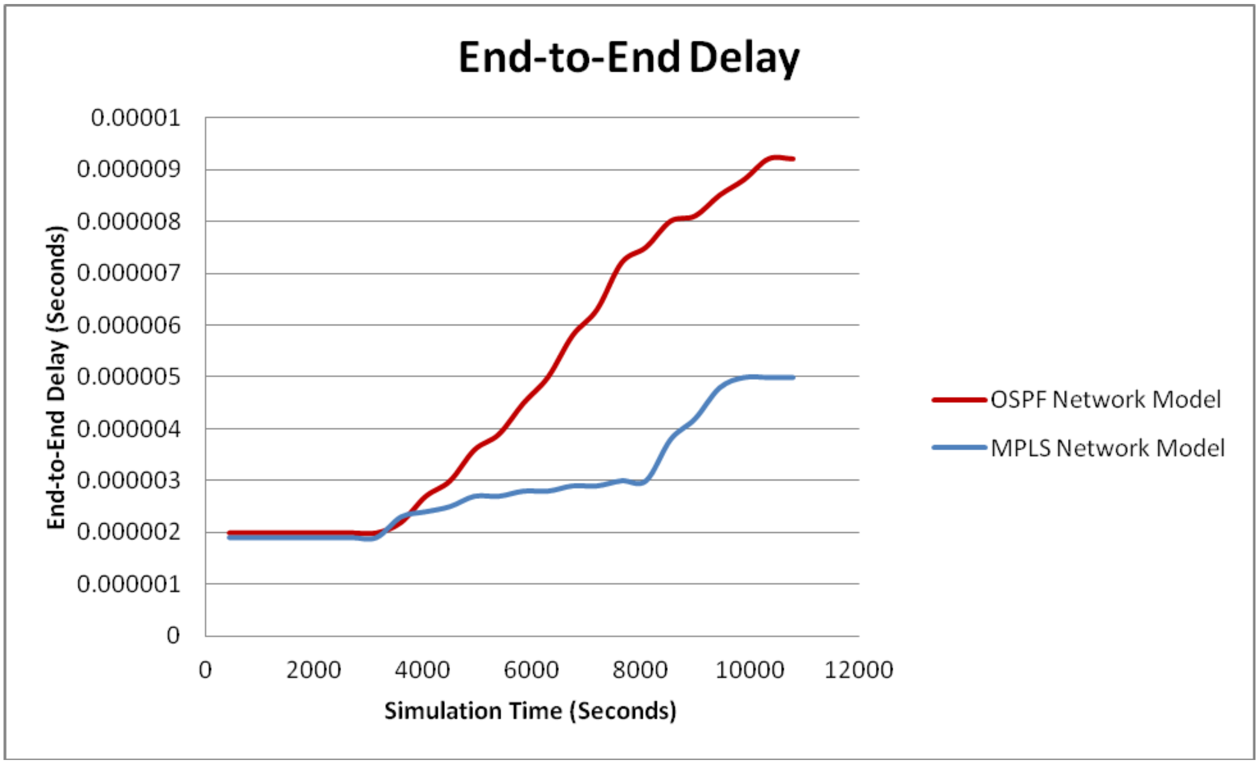


Figure 4.2 End-to-end Delay

Figure 4.2 showed the end-to-end delay of the LAN traffic, it can be seen that ABU network with existing design (i.e default OSPF network) have higher delay from 0.000002s to 0.0000092s during the simulation period as compared to that of MPLS-Enabled ABU network which has delay from 0.0000019 to 0.0000050s. It can be deduced from Figure 4.2 that ABU campus network with existing design have very high end-to-end delay compared with ABU campus network running MPLS technology.

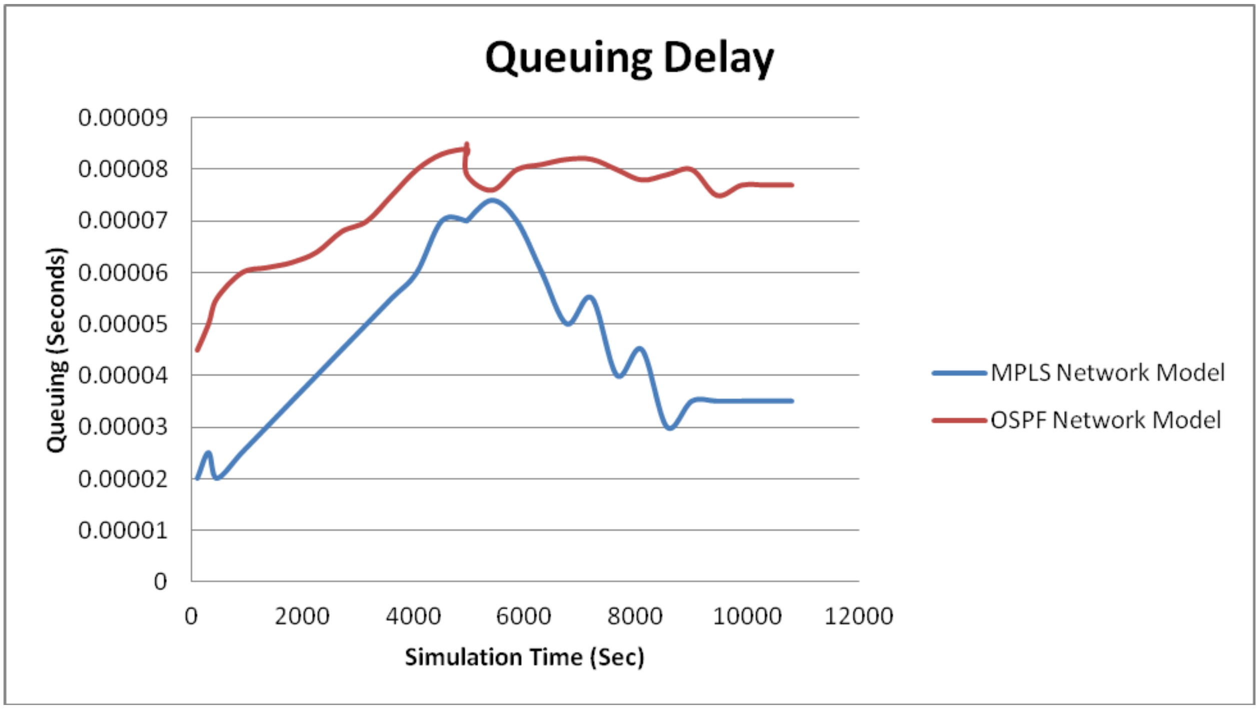


Figure 4.3: Queuing Delay

Figure 4.3 showed the queuing delay of the LAN traffic at the transmit ring of the network hardware interface, it can be seen that ABU network with existing design (i.e default OSPF network) have higher queuing delay from 0.000045s to 0.000084s compared with MPLS-Enabled ABU network which has delay from 0.00002s to 0.000074s. It can be deduced from Figure 4.3 that ABU campus network with existing design have very high queuing delay compared with ABU campus network running MPLS technology.

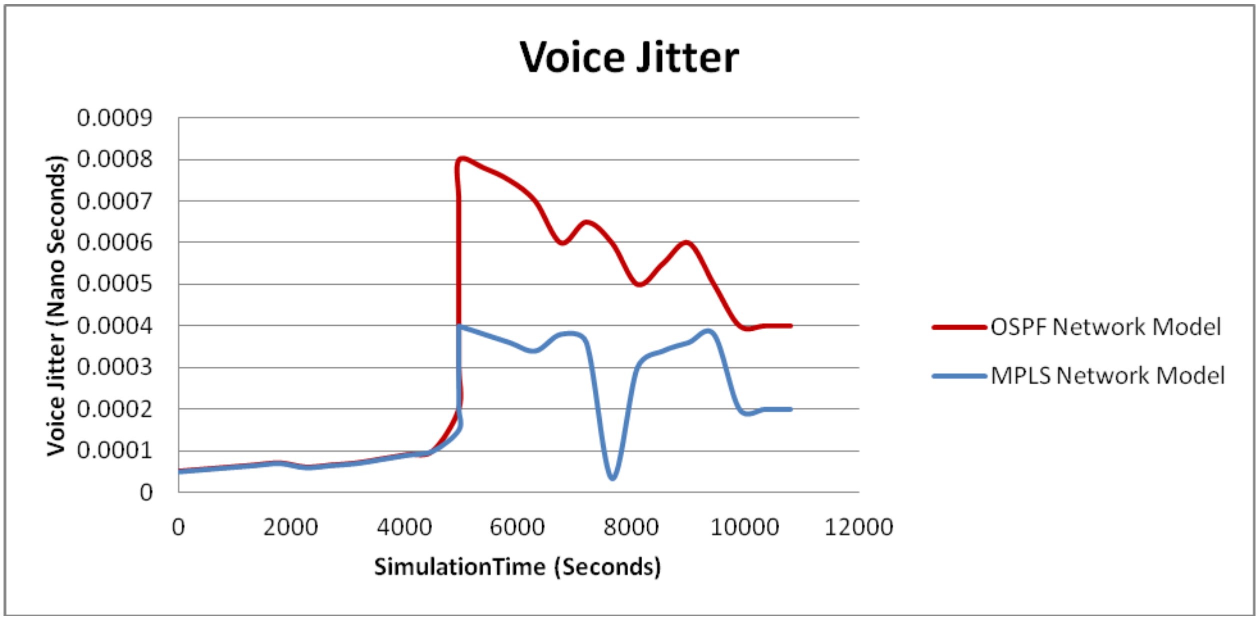


Figure 4.4: Jitter

Figure 4.4 showed voice traffic jitter on the network, it can be seen that the voice jitter for ABU campus network with existing design (i.e default OSPF network) increased rapidly from 0.00005s to 0.00080s after some minute to the start of the simulation then later started to drop with fluctuations. For MPLS-enabled ABU campus is from 0.00005s to 0.0004s with fluctuations throughout the simulation period. It can be deduced from Figure 4.4 that ABU Campus Network has very high Jitter because it has higher delay compared with ABU campus network running MPLS technology

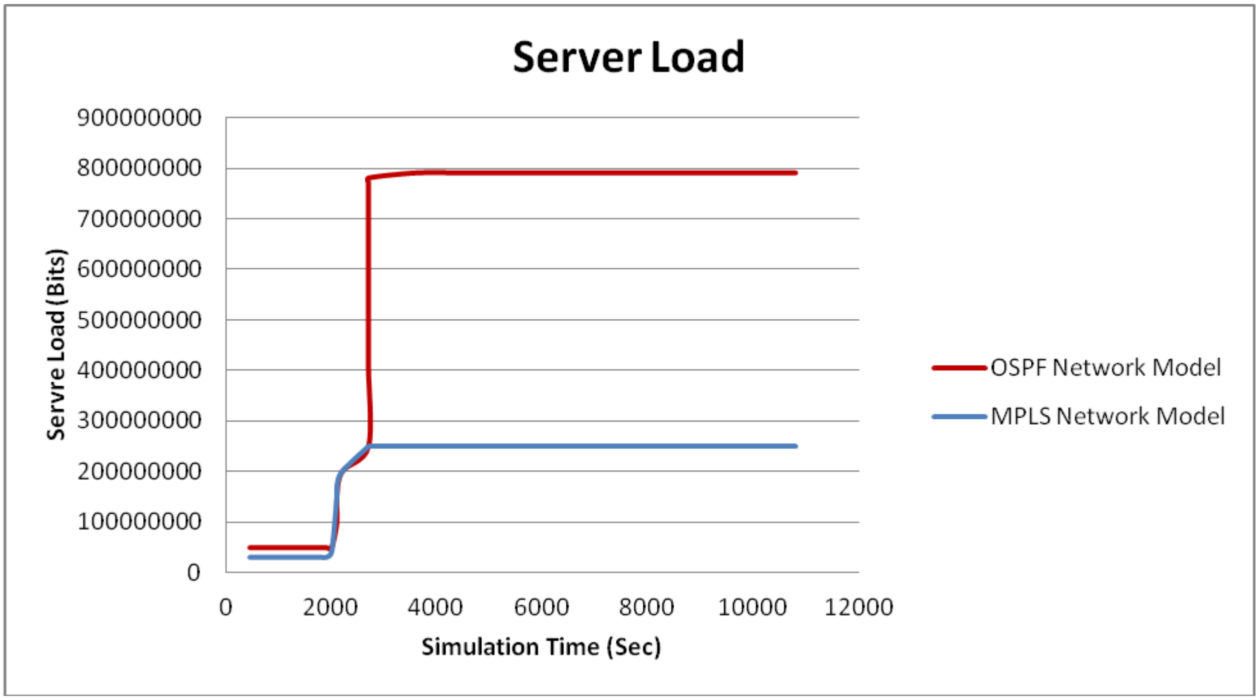


Figure 4.5: Server Load

Figure 4.5 showed that the ABU network with existing design (i.e default OSPF network) have very high server load of 790,000,000 (bits/sec) during the simulation period compared with the MPLS-Enabled ABU campus network of about 250,000,000 (bits/sec).

From the results output in the two scenarios shown in Figure 4.1 to Figure 4.5, it can be deduced that campus network; designed, configured, and implemented using MPLS technology provides a more scalable, flexible, secured, and efficient network with higher throughput, lower delay, lower jitter and lower server load.

4.3 VALIDATION

The GNS3 simulation configurations models from the simulation environment were adopted and configured on live routers and switches to validate the simulation results. Figure 4.6 depicts the schematic diagram of the topology adopted for the validation, while Plate 4.1 depicts the picture of the experimental test-bed used for the validation process in Mamman Kontagora Computer Laboratory (MKCL) of the Department of Electrical and Computer Engineering, A.B.U. Zaria. Two Cisco 2911 routers were configured as core devices while two 2911 and two 2901 Cisco routers respectively were configured as distribution devices, two Cisco catalyst 3560 v2 series PoE-24 and two catalyst 2960 switches were configured as access devices. Figures 4.7 to Figure 4.13 showed the screenshots of CPU utilizations of some of the hardware configured in the validation processes.

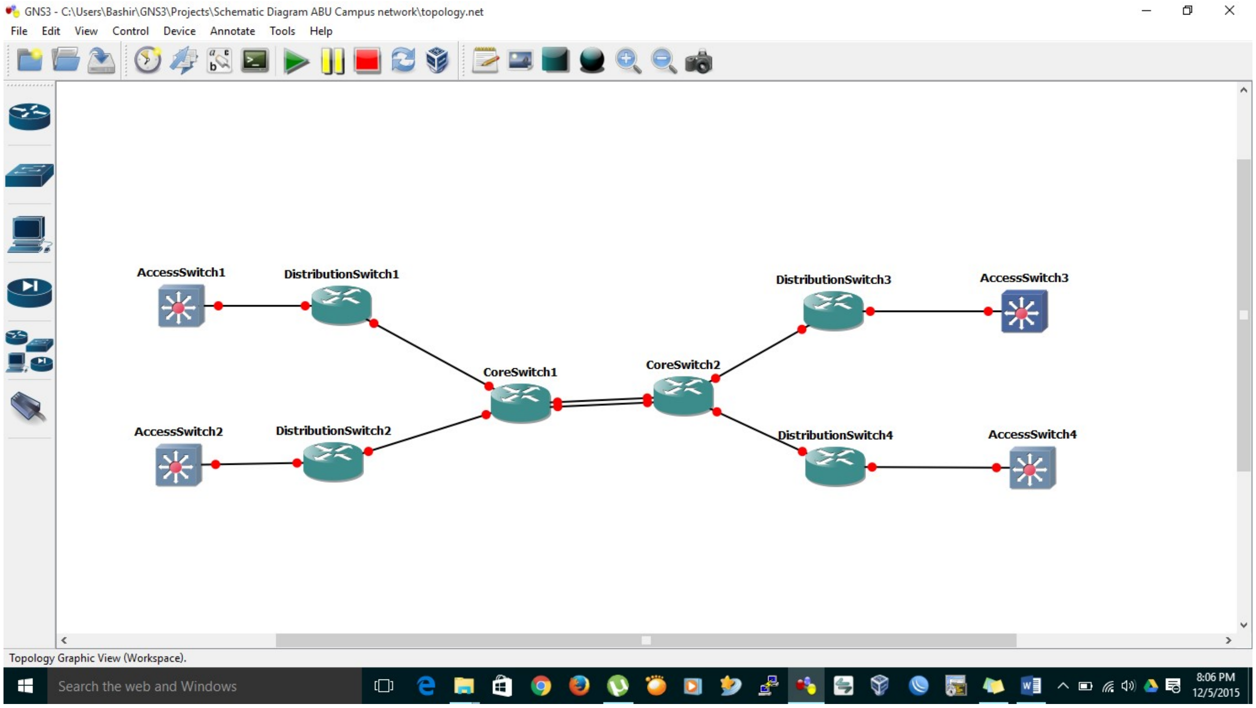
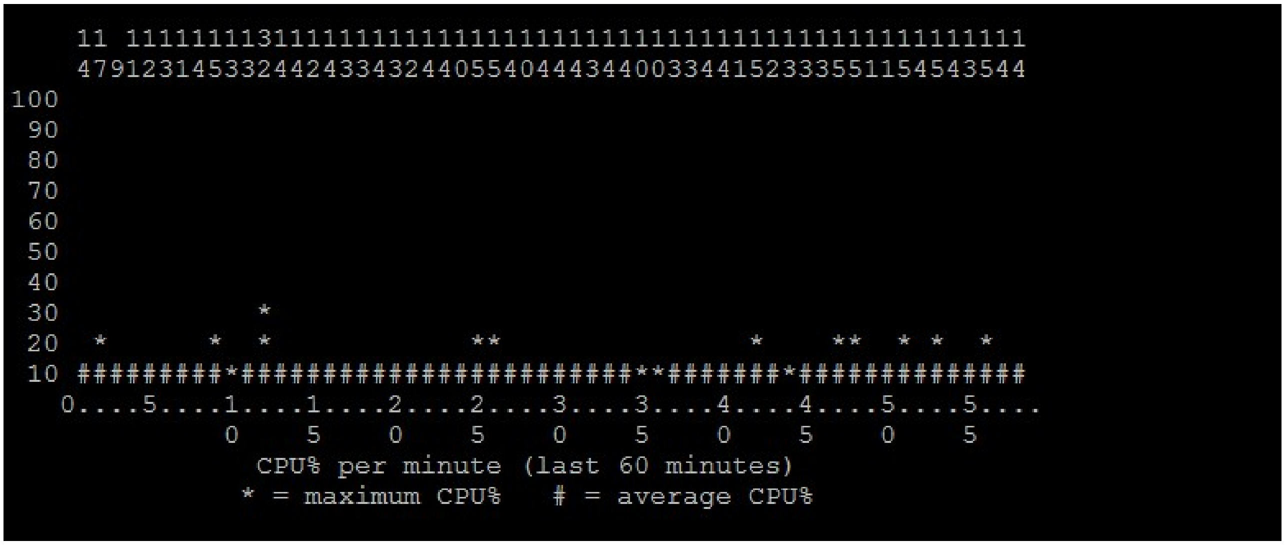

GNS3 - C:\Users\Bashir\GNS3\Projects\Schematic Diagram ABU Campus network\topology.net
File Edit View Control Device Annotate Tools Help
AccessSwitch1
DistributionSwitch1
DistributionSwitch3
AccessSwitch3
CoreSwitch1
CoreSwitch2
AccessSwitch2
DistributionSwitch2
DistributionSwitch4
AccessSwitch4
Topology Graphic View (Workspace).
Search the web and Windows
8:06 PM
12/5/2015

Figure 4.6: Schematic Diagram of the Validation Topology Setup

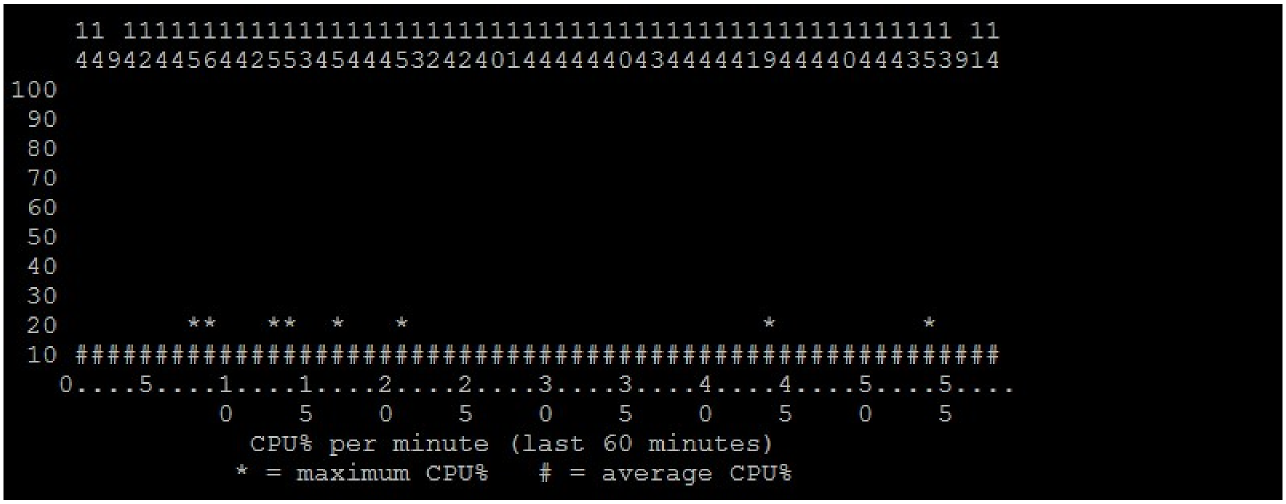
Plate 4.1: Live Validation Experimental Setup at the MKCL



```
    11 1111111131111111111111111111111111111111111111111111111
    4791231453324424334324405540444344003344152333551154543544
100
 90
 80
 70
 60
 50
 40
 30            *
 20  *      *  *            **               *    **  * *  *
 10 #########*########################**#######*##############
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 4.7: Core Switch 1

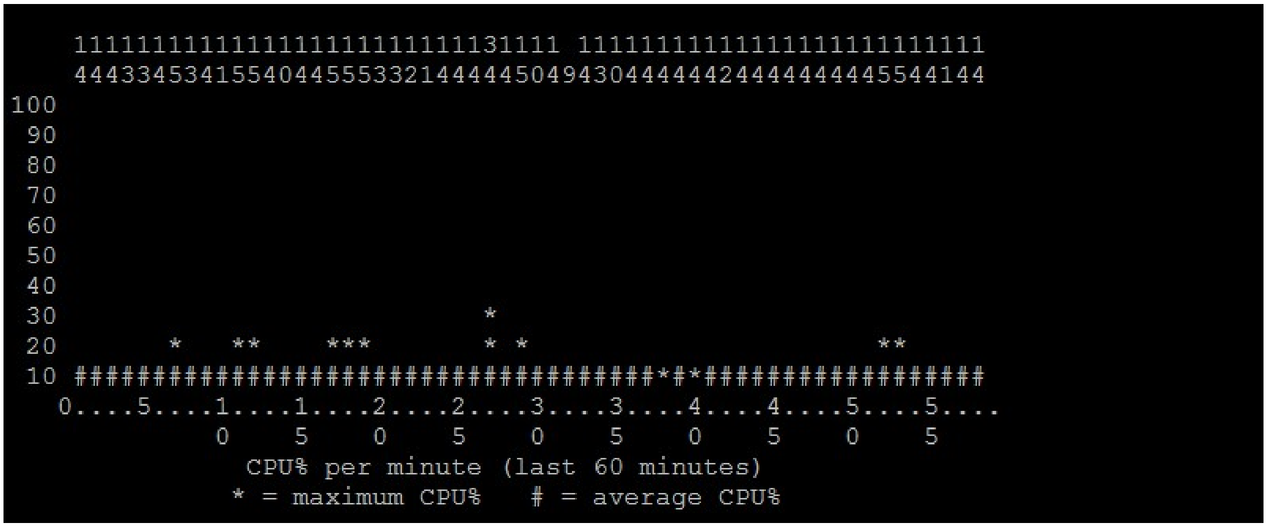
Figure 4.7 shows the CPU utilization of the live switch configured as the first core switch. It shows the CPU utilization from between 9% to 15% within the first hour of the simulation, which is a significant improvement compared with the conventional OSPF network with up to 100% CPU utilization.



```
    11 1111111111111111111111111111111111111111111111111111 11
    4494244564425534544453242401444444043444441944440444353914
100
 90
 80
 70
 60
 50
 40
 30
 20        **   **  *   *                      *          *
 10 ##########################################################
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 4.8: Core Switch 2

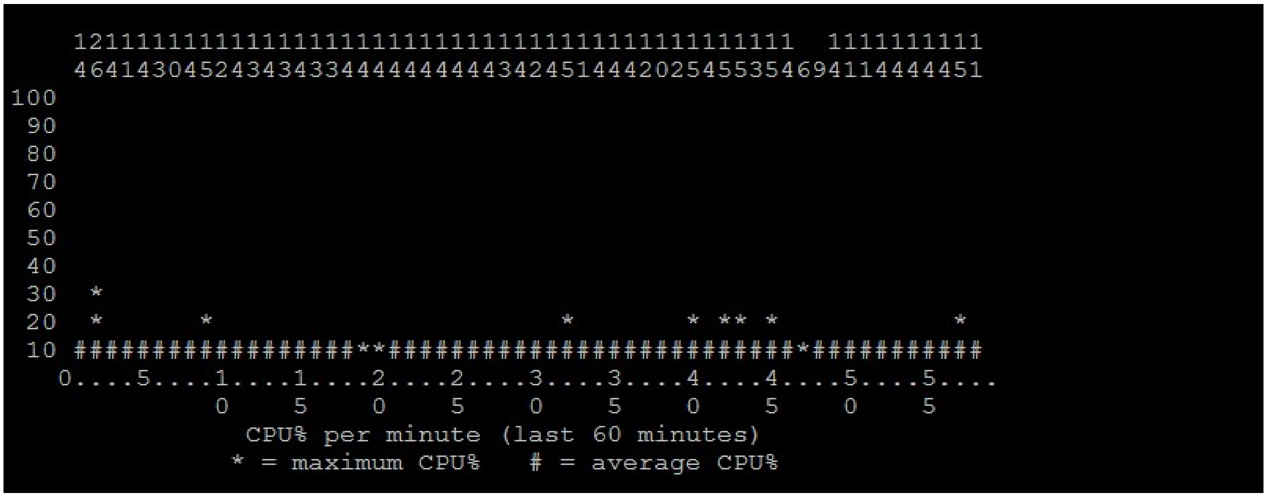
Figure 4.8 shows the CPU utilization of the live switch configured as the second core switch. It shows the CPU utilization from between 9% to 14% within the first hour of the simulation, which is a significant improvement compared with the conventional OSPF network with up to 100% CPU utilization.



```
    1111111111111111111111111131111 111111111111111111111111111
    44433453415540445553321444445049430444444244444444445544144
100
 90
 80
 70
 60
 50
 40
 30                           *
 20       *   **    ***       * *                      **
 10 #####################################*#*###################
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 4.9: Distribution Switch 1

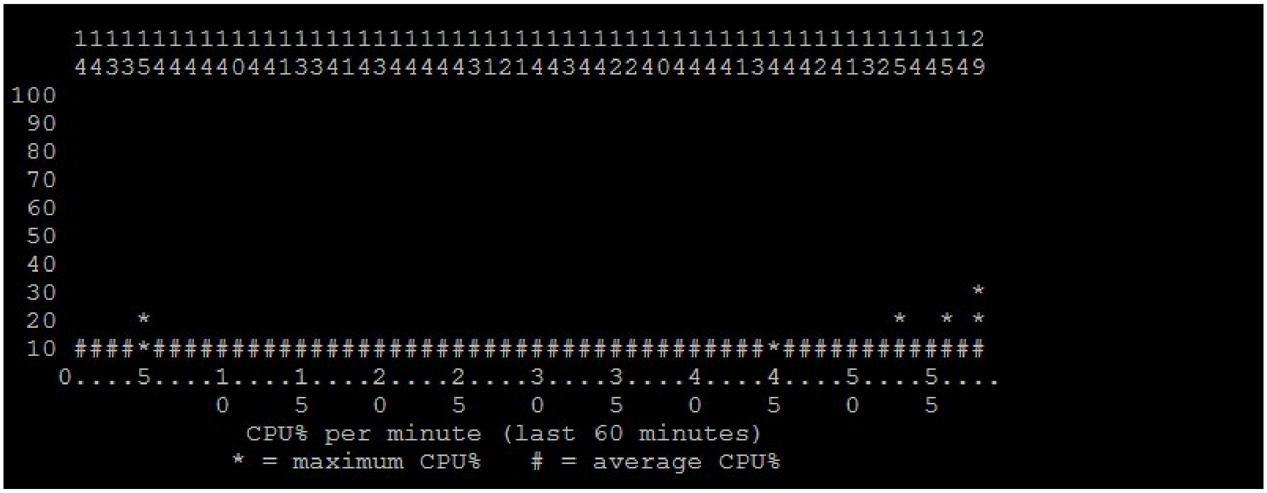
Figure 4.9 shows the CPU utilization of the live switch configured as the first distribution switch. It shows the CPU utilization from between 9% to 34% within the first hour of the simulation, which shows a significant improvement compared with the conventional OSPF network with up to 100% CPU utilization.



```
    1211111111111111111111111111111111111111111111  1111111111
    4641430452434343344444444443424514442025455354694114444451
100
 90
 80
 70
 60
 50
 40
 30  *
 20  *      *                      *       * ** *           *
 10 ##################**##########################*###########
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 4.10: Distribution Switch 2

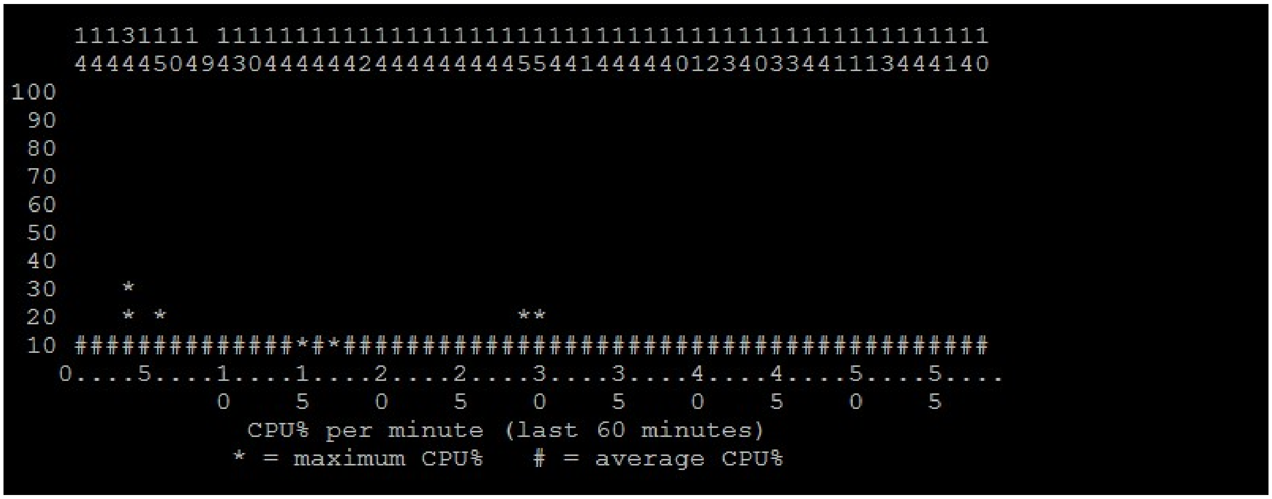
Figure 4.10 shows the CPU utilization of the live switch configured as the second distribution switch. It shows the CPU utilization from between 6% to 15% within the first hour of the simulation, which shows a significant improvement compared with the conventional OSPF network with up to 100% CPU utilization.



```
    1111111111111111111111111111111111111111111111111111111112
    4433544444044133414344444312144344224044441344424132544549
100
 90
 80
 70
 60
 50
 40
 30                                                          *
 20     *                                               *  * *
 10 ####*#######################################*#############
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 4.11: Distribution Switch 3

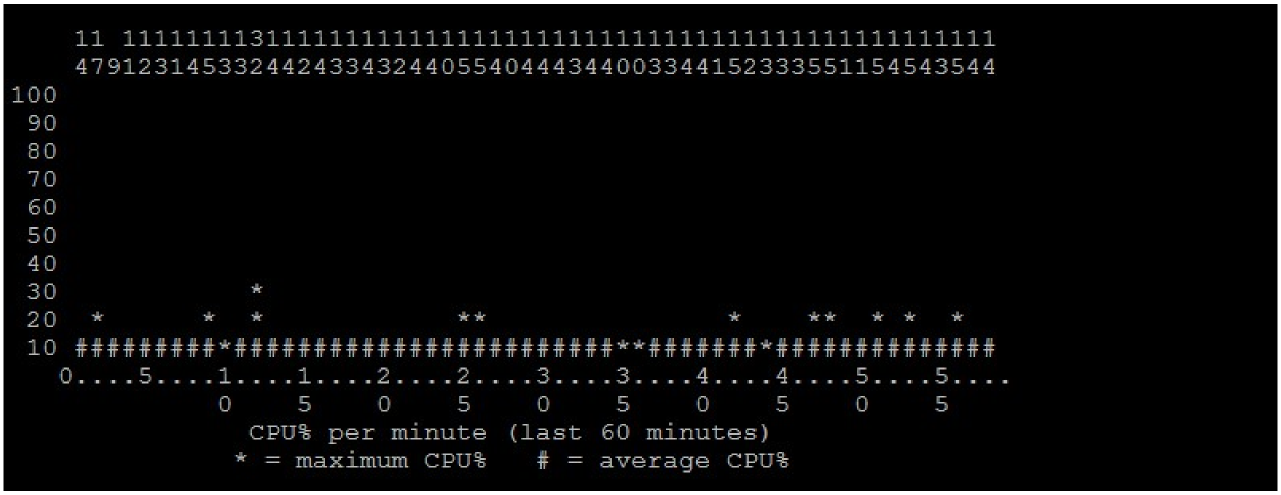
Figure 4.11 shows the CPU utilization of the live switch configured as the third distribution Switch. It shows the CPU utilization from between 10% to 29% within the first hour of the simulation, which shows a significant improvement compared with the conventional OSPF network with up to 100% CPU utilization.



```
    11131111 1111111111111111111111111111111111111111111111111
    4444450494304444442444444444554414444401234033441113444140
100
 90
 80
 70
 60
 50
 40
 30    *
 20    * *                      **
 10 ##############*#*#########################################
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 4.12: Access Aggregate Switch 1

Figure 4.12 shows the CPU utilization of the live switch configured as the first access aggregate switch. It shows the CPU utilization from between 9% to 15% within the first hour of the simulation, which shows a significant improvement compared with the conventional OSPF network with up to 100% CPU utilization.



```
    11 1111111131111111111111111111111111111111111111111111111
    4791231453324424334324405540444344003344152333551154543544
100
 90
 80
 70
 60
 50
 40
 30            *
 20  *      *  *            **               *    **  * *  *
 10 #########*########################**#######*##############
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

Figure 4.13: Access Aggregate Switch 2

Figure 4.13 shows the CPU utilization of the live switch configured as the second access aggregate switch. It shows the CPU utilization from between 9% to 32% within the first hour of the simulation, which shows a significant improvement compared with the conventional OSPF network with up to 100% CPU utilization.

Figures 4.7 to Figure 4.13 showed an average of 9% to 32% CPU utilization when MPLS technology was implemented on a campus network compared with 90% to 100% CPU utilization when conventional OSPF is implemented on the network. This shows that the MPLS technology provides more scalability than the OSPF network.

4.3.1 Validation Result

The GNS3 simulated configuration model was adopted and configured on live routers and switches the Mamman Kontagora Computer Laboratory (MKCL) of the Department of Electrical and Computer Engineering, A.B.U. Zaria in order to validate the simulation results. CPU utilization, RAM utilization, and Link utilization were taken into consideration in the course of the validation as shown in Figure 4.13 to Figure 4.15.

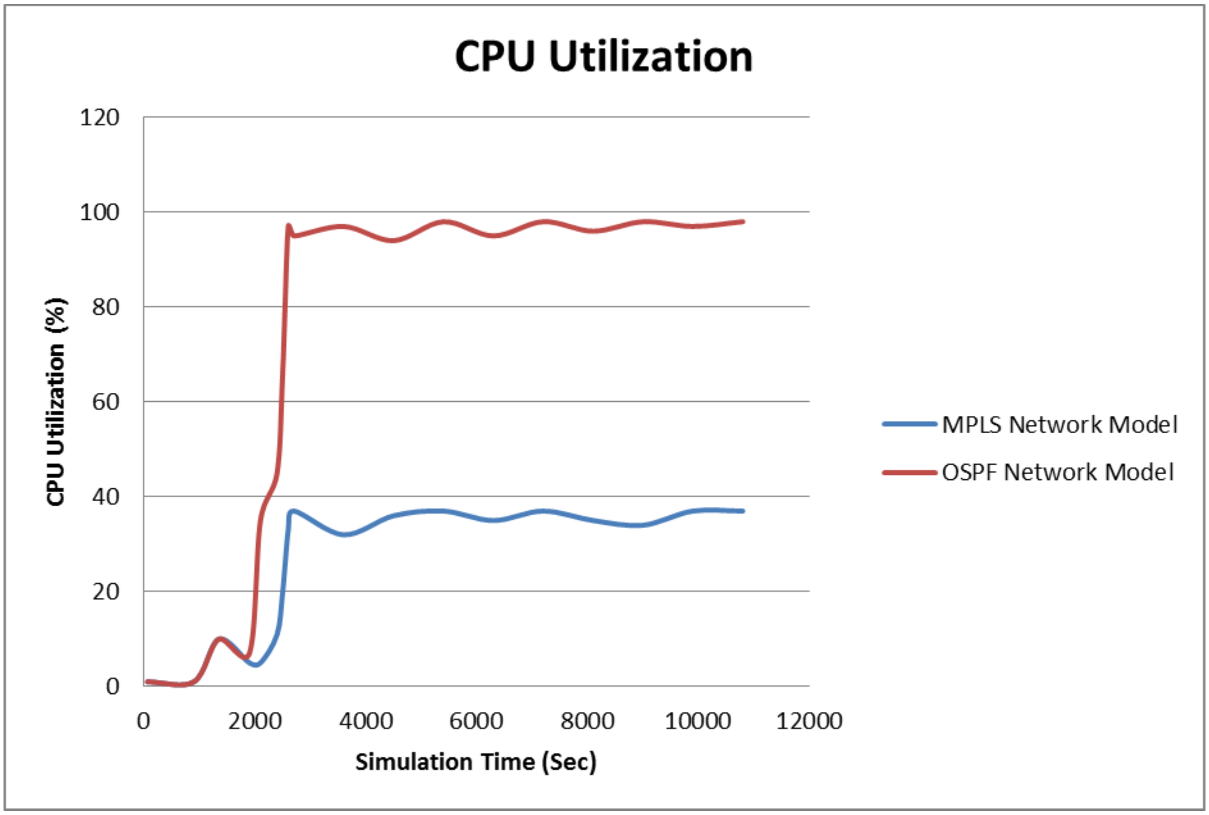


Figure 4.14: CPU Utilization

Figure 4.14 showed the average CPU utilization of the core switch measured in percentages, it can be seen that the CPU utilization for ABU campus network with existing design (OSPF network) steadied at about 99% while that of MPLS-Enabled Campus network steadied at about 37%. High CPU utilization causes route flapping and sub-optimal routing which can result in scalability issues like higher end-to-end and queuing delays.

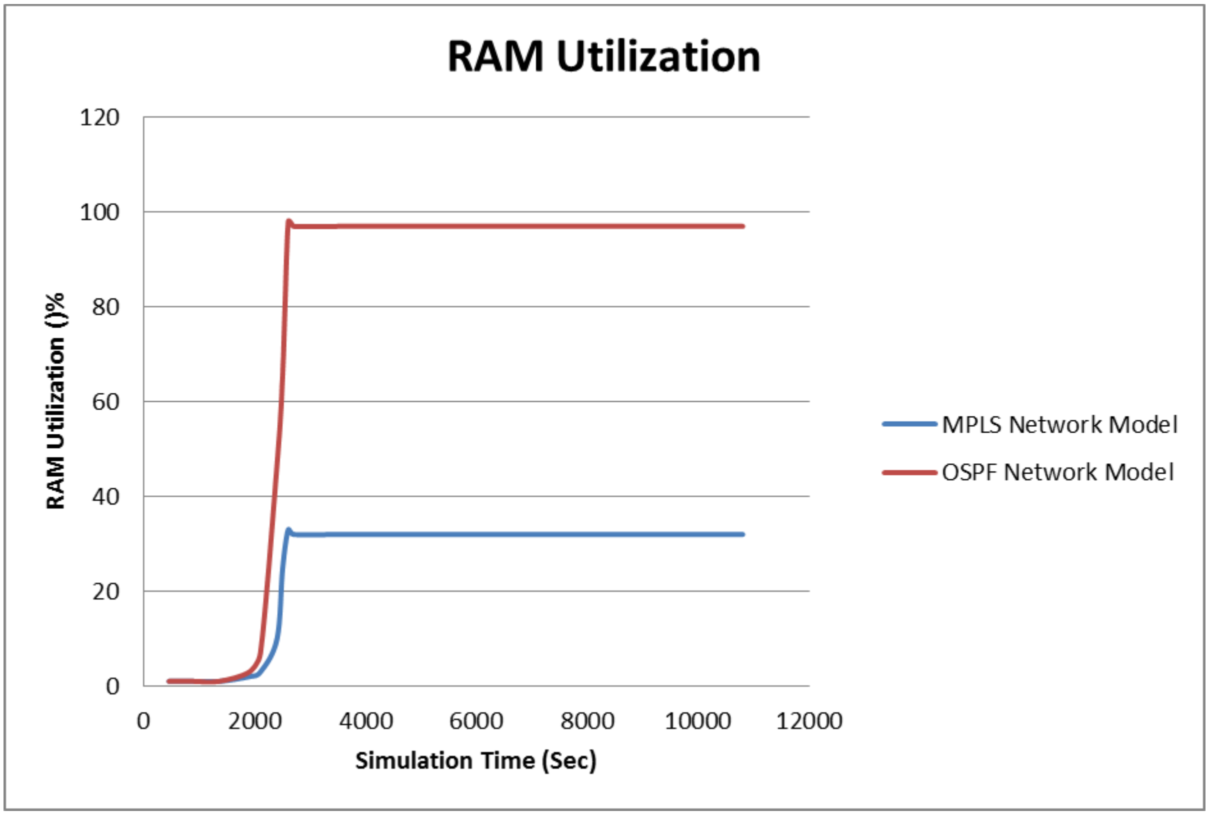


Figure 4.15: RAM Utilization

Figure 4.15 shows the average utilization of the RAM of the core switch, which stores the entire routes to all the possible destinations on the network. If conventional OSPF is implemented on a large and complex network, there will be a lot of routes which will virtually fill the RAM and cause a slow lookup process. From Figure 4.14, there is about 97% RAM utilization using the OSPF network design, while it is about 32% RAM utilization when MPLS is implemented. This is because the size of the routing table is reduced thus leading to a faster lookup process.

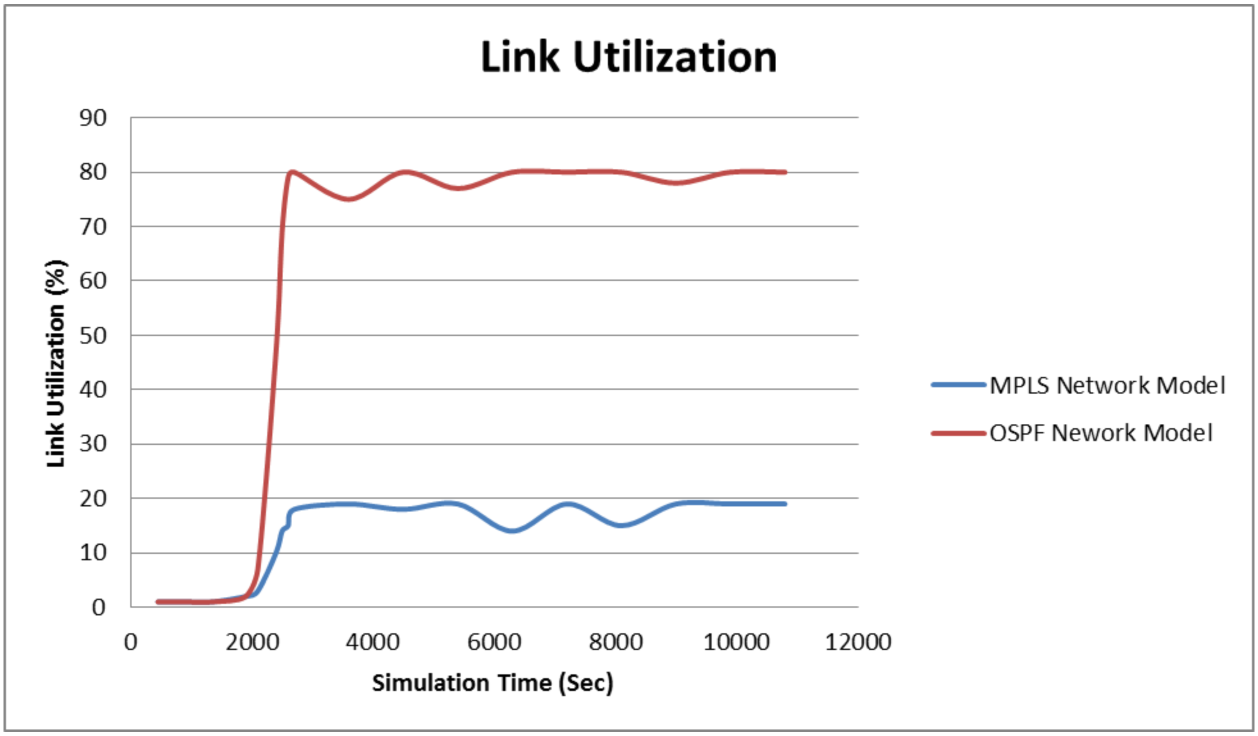


Figure 4.16: Link Utilization

Figure 4.16 showed the link utilization of the core switch measured in percentages, it can be seen that the link utilization based on the OSPF network design is about 80% as compared to 19% with the MPLS-based design. This shows that MPLS-based design is more efficient than the conventional OSPF-based design as high link utilization causes network congestion, routing queue delays, higher throughput and sub-optimal routing. From the results output in the two scenarios as in Figure 4.14 to Figure 4.16, it can be deduced that campus network; designed, configured, and implemented using MPLS technology provide a more scalable network and flexible network.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

The sub-section presents the summary of the research, limitation, conclusion, recommendations, and further work.

5.2 SUMMARY

This research work presents the scalability evaluation of a large and complex campus network configured and implemented using default layer-2 (STP) and layer-3 (OSPF) technologies, areas vulnerable to scalability issues were identified when some of the physical devices of ABU campus network were checked for several days at pick period and also the ABU network model was emulated using GNS3 simulator, this resulted in affecting the performance of active devices CPU, RAM, and link utilizations as well as network performance. Proposed improved designed solution was adopted with view of improving network performance, ABU network was designed and simulated in OPNET modeler environment, network services were configured, and performance metric; throughput, end-to-end delay, queuing delay, jitter, and server load were configured to compare the result out of the existing design and the improved designed solution. The proposed solution using MPLS technology showed significant improvement compared with the existing design with active devices performance increase CPU 37% compare 99%, RAM 32% compare 80%, link utilization 30% compare 90%.

5.3 SIGNIFICANT CONTRIBUTION

The conventional campus network designs use a mix of switching (layer-2) technologies at the network edge (access layer) and routing (layer-3) technologies at the core (Distribution and Core layers). At layer-2, the network design is achieved by means of Virtual Local Area Networks (VLANs) and STP protocols, and layer-3 by means of routing protocols such as OSPF or EIGRP. Therefore, the significant contributions of this research work are itemized as follows:

a) Developed a network design solution to achieve maximum utilization of network hardware as it achieved significant improvement in hardware utilizations up to 37% for CPU, 32% for RAM and, 19% for link utilization as compared with conventional design of 97.5%, 97% and 80% utilization respectively

b) Developed a more scalable network design solution using MPLS technology that provides flexible support for wide ranges of applications and services and simplified network architecture to overcome some of the limitations of conventional network design using OSPF, MPLS-based network have higher throughput from 4,000 (bps) to 81,000 (bps) compared with OSPF network from 3,000 (bps) to 41,000 bps, lower end-to-end delay from 0.0000019 to 0.0000050s compared with 0.000002s to 0.0000092s, lower queuing delay from 0.00002s to 0.000074s compared with 0.000045s to 0.000080s, lower jitter from 0.00005s to 0.0004s compared with 0.00005s to 0.00080s, lower server load of 250,000,000 (bits/sec) compared with 790,000,000 (bits/sec).

c) Provided a frame work that enabled maximum utilization of IP addresses using IP address re-use and more efficient route aggregations.

5.4 CONCLUSION

As the demands placed on campus network have grown in complexity, so has the need for scalable solutions to provide multiple solutions for centralizing services and security policies while preserving the high-availability, manageability, security, and scalability benefits of existing campus design. The output of the research results showed that MPLS campus network is the most preferred design over the conventional OSPF network design, as it provides a significant improvement in the efficiency and performance of networks.

5.5 LIMITATIONS

During the course of this research work, certain limitations were observed which are itemized as follows:

a) GNS3 emulator consumes a lot of computer resources during simulation; a computer system with very high specs is required.

b) MPLS technology requires more recent Internetwork Operating System (IOS) on the routers and switches to be implemented.

5.6 RECOMMENDATION AND FUTURE WORK

Future works should consider the following areas:

a) The design and implementation of scalable and flexible campus network using seamless MPLS network technology solution.

b) The design and implementation of campus network using MPLS over IPv6 technology.

References

Abdul-Bary, R. S., & Alhafidh, O. K. (2014). "Performance Analysis of Multimedia Traffic over MPLS Communication Networks with Traffic Engineering". *IJCNCS VOL.2, NO.3*, 93–101.

Adarshpal, S. S., & Vasil, Y. H. (2013). *"The Practical OPNET® User Guide for Computer Network Simulation".* 6000 Broken Sound Parkway NW, Suite 300: CRC Press "Taylor & Francis Group".

Akinsipe, O., Goodarzi, F., & Li, M. (2012). "Comparison of IP, MPLS and MPLS RSVP-TE Networks using OPNET". *International Journal of Computer Applications (0975-8887) Vol.58-No.2*.

Andrew, S. T., & Watherall, D. J. (2011). *Computer Networks (5th Edition).* Pearson.

Arshad, M. J., Tauqir, A., & Amjad, F. (2010). "Data Networks' Design and Optimization through MPLS VPNs using BGP". *Journal of American Science*, 6(12).

Atayero, A., Alatishe, A., & Iruemi, J. (2012). "Modeling and Simulation of a University LAN in OPNET Modeler Environment". *IJETAE, ISSN 2250–2459*.

Berzuk, V., & Varich, V. (2010). "The Analysis of the Characteristics of Routing Protocols in IP Networks". *TCSET'2010*, 23-27.

Bezruk, V., & Varich, V. (2010). "The Analysis of the Characteristics of Routing Protocols in IP Networks". *TCSET'2010, Lviv-Slavske, Ukraine*, 23-27.

Denise, D. (2014). *"CCNP Routing and Switching SWITCH 300-115 Quick Reference".* CISCO Press.

Dhirendra, S., Vikram, K., Marco, Z., & Vikram, S. (2011). "A Study of Efficiency- Campus Networks in Western Himalayan Universities of India". *IEEE Computer Society '2011 Workshops of International Conference on Advanced Information Networking and Applications'*.

Dijkstra, E. W. (1959). "A Note on Two Problems in Connection with Graphs." Numerische Math. 1,. 269-271.

Divya, S., & Renu, S. (2015). "Performance Measure of MPLS and Traditional IP Network through VoIP Traffic". *International Journal of Science, Engineering and Technology Research (IJSETR), VOl 4, ISSN: 2278-7798*, 2118-2122.

Douglas, E. C. (2009). *"Computer Networks and Internet" 5th edition.* Pearson Prentice Hall.

Douglas, E. C. (2013). *"Internetworking with TCP/IP, Principles, Protocols and Architecture" 6th edition Vol.1.* Pearson Prentice Hall.

Faraz, S., Zaheer, A., Johnson, L., & Abe, M. (2012). *Troubleshooting IP Routing Protocols (CCIE Professional Development Series).* CISCO Press.

Fitigau, I., & Toderean, G. (2013). "Opnet Analyze for FTP and Video Network traffic using IP over MPLS Protocol". *ANUL XX, NR. 2, ISSN 1453 - 7397*.

Goyal, M., Soperi, M., Baccelli, E., Choudhury, G., Shaikh, A., Hosseini, H., & Trivedi, K. (2012). "Improving Convergence Speed and Scalability in OSPF: A Survey". *IEEE Communications Surveys & Tutorials Vol.14 No2*.

Hock, D., Matthias, H., Michael, M., & Christian, S. (2010). "Optimizing Unique Shortest Paths for Resilient Routing and Fast Reroute in IP-Based". *IEEE/IFIP Network Operations and Management Symposium - MOMS 2010*, 309-316.

Jeff, D., & Jennifer, C. (2009). *Routing TCP/IP, Volume I (CCIE Professional Development) 2nd Edition.* CISCO Press.

Jialei, W., & Yuanping, Z. (2010). "A layered MPLS Network Architecture". *IEEE 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, 1-4.

Jim, G., Ivan, P., & Jeff, A. (2014). *"MPLS and VPN Architecture" Vol. 2.* CISCO Press.

Jing-bo, X., Ming-hui, L., & Lu-Jun, W. (2008). "Research on MPLS VPN Networking Application Based on OPNET". *IEEE International Symposium on Information Science and Engineering*, 404 - 408.

John, T. (2011). *"Designing Cisco Network Service Architectures (ARCH): Developing an Optimum Design for Layer 3 (CCDP)".* CISCO Press.

Jun, B., Xiaoxiang, L., & Jianping, W. (2006). "OSPF Performance Measurements and Scalability Study". *IEEE*. '*Proceeding in Wireless and Optical Commnication Networks'*

Kenneth, H. R. (2012). *"Discrete Mathematics and Its Applications" 7th Edition.* McGraw-Hill.

Kevin, R. F., & Richard, W. S. (2011). *"TCP/IP Illustrated Vol.1 The Protocols" 2nd Edition.* Addison-Wesley Professional Computing Series.

Kok-Keong, L., & Fung, L. B.-H. (2012). *"Building a Resilient IP Networks".* Indianapolis, IN 46240 USA: CISCO Press.

Lammle, T. (2012). *"Cisco Certified Network Associate Study Guide 7th edition".* Sybex.

Lammle, T. (2014). *"CCNA Routing and Switching Review Guide".* Sybex.

Luc, D. G. (2006). *"MPLS Fundamentals".* CISCO Press.

Mangla, N., & Khola, R. K. (2010). "Optimization of IP routing with Content Delivery Network". *IEEE International Conference on Networking and Information Technology*, 424-428.

Mike, F. (2013). *"Graphical Network Simulator GNS3 ver1.0"*. Retrieved April 5th, 2015, from http://www.csd.uoc.gr/~hy435/material/GNS3-0.5-tutorial.pdf

Minei, I., & Julian, L. (2011). *MPLS-Enabled Applications: Emerging Developments and New Technologies, 3rd Edition.* John Wiley & Sons Ltd.

Ming-hui, L., & XIA, J.-b. (2008). "Research and Simulation on VPN Networking Based on MPLS". *IEEE 'The 4th International Conference on Wireless, Networking and Mobile Computing'.*

Mishra, R., & Ahmad, H. (2014). "Comparative Analysis of Conventional IP Network and MPLS Network over VoIP Application". *IJCSIT Vol.5(3)* , 4496-4499.

Modhar, A. H. (2011). "Building Model for the University of Mosul Computer Network Using OPNET Simulator". *Tikrit Journal of Eng. Science Vol.18 No.2*, 34-44.

Naoum, R. S., & Maswady, M. (2012). "Performance Evaluation for VOIP over IP and MPLS". *WCSIT Vol.2 No.3*, 110-114.

Narbik, K., Peter, P., & Vinson, T. (2015). *CCIE Routing and Switching v5.0 Official Cert Guide Library, 5th Edition* . CISCO Press.

Nuuti, V., & Jukka, M. (2009). "Minimizing ARP broadcasting in TRILL". *IEEE GLOBECOM Workshops*, 1-6.

Oyeleke, G. A., & Oluwatosin, O. A. (2015). "Evaluating IP, MPLS and MPLS-TE Network". *Communications on Applied Electronics (CAE) - ISSN:2394-4714, Vol 3 - No.1*, 28-31.

Ranjbar, A. (2015). *"Troubleshooting Methods for Cisco IP Networks".* CISCO Press.

Rich, S., & Jim, E. (2008). *"The All-New Switch Book" Second Edition.* Wiley Publishing Inc.

Richard, F., Balaji, S., & Erum, F. (2010). *"Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Foundation learning for SWITCH 642-813".* CISCO Press.

Rick, G., & Allan, J. (2008). *"Routing protocols and concepts: CCNA exploration companion guide".* London: Pearson Education.

Ruhani, R., Farah, A. A., Murizah, K., Mat, Y., & Hashim, H. (2015). "Implementation of High Availability Concept Based On Traffic Segregation Over MPLS-TE". *Asian Research Publishing Network (ARPN) ISSN:1819-6608*, 1295-1301.

Russ, W., Alvaro, R., & Don, S. (2005). *"Optimal Routing Design".* CISCO Press.

Stallings, W. (2007). *"Data and Computer Communicatons" 8th edition.* Prince Hall.

Tokalic, A., Zoran, C., & Aleksandra, S. (2011). "Performance Analysis of the IP lookup table updating". *IEEE TELSIKS*.

Wang, W. (2003). "The OPNET Modeler and Network Simulation". *Beijing: People's Posts and Telecommunication Press*, 61-77.

Wendell, O., Rus, H., & Denise, D. (2009). *"CCIE Routing and Switching Exam Certification guide" 4th Edition.* CISCO Press.

Zhao. (2007). "Research and Simulation on Network based on MPLS" . *Chong Qing Engineering College Journal Vol 21*, 36-38.

Zhao, X., & Dante J. Pacella, J. S. (2010). Routing Scalability: An Operator's View. *IEEE Journal on Selected Areas in Communications, Vol. 28 No. 8*.

APPENDIX I

THE MPLS IDP PROCESS MODEL PROCEDURE OF THE SIMULATION SCENE

```
own_objid = op_id_self ();
own_node_objid = op_topo_parent (own_objid);
own_prohandle = op_pro_self ();
op_ima_obj_attr_get (own_objid, "process model",
proc_model_name);
process_record_handle= (OmsT_Pr_Handle)
oms_pr_process_register (own_node_objid, own_objid,
own_prohandle, proc_model_name);
oms_pr_attr_set (process_record_handle, "protocol",
OMSC_PR_STRING, "ip_encap", OPC_NIL);
if (ip_encap_ici_print_procs_set == OPC_FALSE)
{
op_ici_format_print_proc_set ("inet_encap_ind",
"src_addr", inet_address_ici_field_print);
op_ici_format_print_proc_set ("inet_encap_ind",
"dest_addr", inet_address_ici_field_print);
op_ici_format_print_proc_set ("inet_encap_ind",
"interface_received", inet_address_ici_field_print);
op_ici_format_print_proc_set ("inet_encap_req",
"src_addr", inet_address_ici_field_print);
op_ici_format_print_proc_set ("inet_encap_req",
"dest_addr", inet_address_ici_field_print);
}
```

APPENDIX II

MPLS CONFIGURATIONS ON THE ROUTERS

```
CORESWITCH1(config)#do sh run
Building configuration...
Current configuration : 2949 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname CORESWITCH1
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
ipcef
iptcpsynwait-time 5
ipvrf ABU_MPLS
rd 1:1
 route-target export 1:1
 route-target import 1:1
no ip domain lookup
mpls label protocol ldp
interface Loopback1
ip address 192.168.1.1 255.255.255.0
interface Loopback2
ip address 192.168.2.1 255.255.255.0
interface Loopback3
ip address 192.168.3.1 255.255.255.0
interface Loopback4
ip address 192.168.4.1 255.255.255.0
interface Loopback5
ip address 192.168.5.1 255.255.255.0
interface Loopback6
ip address 192.168.6.1 255.255.255.0
interface Loopback7
ip address 192.168.7.1 255.255.255.0
interface Loopback8
ip address 192.168.8.1 255.255.255.0
interface Loopback9
ip address 192.168.9.1 255.255.255.0
```

```
interface Loopback10
ip address 192.168.10.1 255.255.255.0
interface FastEthernet0/0
ipvrf forwarding ABU_MPLS
ip address 10.1.0.1 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet0/1
ipvrf forwarding ABU_MPLS
ip address 10.1.5.1 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet1/0
ipvrf forwarding ABU_MPLS
ip address 10.1.9.1 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet2/0
ipvrf forwarding ABU_MPLS
ip address 10.1.8.1 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet3/0
ipvrf forwarding ABU_MPLS
ip address 10.1.7.1 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet4/0
ipvrf forwarding ABU_MPLS
ip address 10.1.6.1 255.255.255.252
 duplex auto
 speed auto
mplsip
router ospf 2 vrf ABU_MPLS
 router-id 192.168.1.1
 log-adjacency-changes
 redistribute bgp 65535 subnets
 network 0.0.0.0 255.255.255.255 area 0
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
```

```
router bgp 65535
 no synchronization
bgp router-id 192.168.1.1
bgp log-neighbor-changes
 neighbor 192.168.11.1 remote-as 65535
 neighbor 192.168.11.1 update-source Loopback1
 no auto-summary
 address-family vpnv4
 neighbor 192.168.11.1 activate
 neighbor 192.168.11.1 send-community both
 neighbor 192.168.11.1 next-hop-self
 exit-address-family
 address-family ipv4 vrf ABU_MPLS
 redistribute ospf 2 vrf ABU_MPLS match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
no ip http server
no ip http secure-server
mplsldp router-id Loopback1 force
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
CORESWITCH1(config)#

CORESWITCH2#sh run
Building configuration...
Current configuration : 2880 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname CORESWITCH2
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
```

```
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
ipcef
iptcpsynwait-time 5
ipvrf ABU_MPLS
rd 1:1
 route-target export 1:1
 route-target import 1:1
no ip domain lookup
mpls label protocol ldp
interface Loopback11
ip address 192.168.11.1 255.255.255.0
interface Loopback12
ip address 192.168.12.1 255.255.255.0
interface Loopback13
ip address 192.168.13.1 255.255.255.0
interface Loopback14
ip address 192.168.14.1 255.255.255.0
interface Loopback15
ip address 192.168.15.1 255.255.255.0
interface Loopback16
ip address 192.168.16.1 255.255.255.0
interface Loopback17
ip address 192.168.17.1 255.255.255.0
interface Loopback18
ip address 192.168.18.1 255.255.255.0
interface Loopback19
ip address 192.168.19.1 255.255.255.0
interface Loopback20
ip address 192.168.20.1 255.255.255.0
interface FastEthernet0/0
ipvrf forwarding ABU_MPLS
ip address 10.1.0.2 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
ipvrf forwarding ABU_MPLS
ip address 10.1.1.1 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet2/0
ipvrf forwarding ABU_MPLS
ip address 10.1.2.1 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet3/0
ipvrf forwarding ABU_MPLS
ip address 10.1.3.1 255.255.255.252
 duplex auto
 speed auto
mplsip
interface FastEthernet4/0
ipvrf forwarding ABU_MPLS
ip address 10.1.4.1 255.255.255.252
 duplex auto
 speed auto
mplsip
router ospf 2 vrf ABU_MPLS
 router-id 192.168.11.1
 log-adjacency-changes
 redistribute bgp 65535 subnets
 network 0.0.0.0 255.255.255.255 area 0
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
router bgp 65535
 no synchronization
bgp router-id 192.168.11.1
bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 65535
 neighbor 192.168.1.1 update-source Loopback11
 no auto-summary
 address-family vpnv4
 neighbor 192.168.1.1 activate
 neighbor 192.168.1.1 send-community both
 neighbor 192.168.1.1 next-hop-self
 exit-address-family
 address-family ipv4 vrf ABU_MPLS
 redistribute ospf 2 vrf ABU_MPLS match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
ip classless
```

```
no ip http server
no ip http secure-server
mplsldp router-id Loopback11 force
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
CORESWITCH2#
```

```
ELECT_ENGG>en
ELECT_ENGG#sh run
Building configuration...
Current configuration : 1769 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname ELECT_ENGG
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
ipcef
interface Loopback30
ip address 192.168.30.1 255.255.255.0
interface Loopback31
ip address 192.168.31.1 255.255.255.252
interface Loopback32
ip address 192.168.32.1 255.255.255.0
interface Loopback33
ip address 192.168.33.1 255.255.255.0
interface Loopback34
ip address 192.168.34.1 255.255.255.0
interface Loopback35
ip address 192.168.35.1 255.255.255.0
```

```
interface Loopback36
ip address 192.168.36.1 255.255.255.0
interface Loopback37
ip address 192.168.37.1 255.255.255.0
interface Loopback38
ip address 192.168.38.1 255.255.255.0
interface Loopback39
ip address 192.168.39.1 255.255.255.0
interface Loopback40
 no ip address
interface FastEthernet0/0
ip address 10.1.10.1 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
ip address 10.1.9.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 log-adjacency-changes
 network 10.1.9.2 0.0.0.0 area 0
 network 10.1.10.1 0.0.0.0 area 0
 network 192.168.0.0 0.0.255.255 area 3
ip classless
ip http server
no ip http secure-server
```

```
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
ELECT_ENGG#

IACC>en
IACC#sh run
Building configuration...
Current configuration : 1723 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname IACC
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
ipcef
interface Loopback40
ip address 192.168.40.1 255.255.255.0
interface Loopback41
ip address 192.168.41.1 255.255.255.0
interface Loopback42
ip address 192.168.42.1 255.255.255.0
interface Loopback43
ip address 192.168.43.1 255.255.255.0
interface Loopback44
ip address 192.168.44.1 255.255.255.0
interface Loopback45
ip address 192.168.45.1 255.255.255.0
interface Loopback46
ip address 192.168.46.1 255.255.255.0
interface Loopback47
ip address 192.168.47.1 255.255.255.0
interface Loopback48
ip address 192.168.48.1 255.255.255.0
interface Loopback49
ip address 192.168.49.1 255.255.255.0
interface FastEthernet0/0
ip address 10.1.10.2 255.255.255.252
```

```
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0
ip address 10.1.8.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 log-adjacency-changes
 network 10.1.8.2 0.0.0.0 area 0
 network 10.1.10.2 0.0.0.0 area 0
 network 192.168.0.0 0.0.255.255 area 4
ip classless
ip http server
no ip http secure-server
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
IACC#
INST_EDU#sh run
Building configuration...
Current configuration : 1877 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname INST_EDU
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
ipcef
iptcpsynwait-time 5
no ip domain lookup
interface Loopback50
ip address 192.168.50.1 255.255.255.0
interface Loopback51
ip address 192.168.51.1 255.255.255.0
interface Loopback52
ip address 192.168.52.1 255.255.255.0
interface Loopback53
ip address 192.168.53.1 255.255.255.0
interface Loopback54
ip address 192.168.54.1 255.255.255.0
interface Loopback55
ip address 192.168.55.1 255.255.255.0
interface Loopback56
ip address 192.168.56.1 255.255.255.0
interface Loopback57
ip address 192.168.57.1 255.255.255.0
interface Loopback58
ip address 192.168.58.1 255.255.255.0
interface Loopback59
ip address 192.168.59.1 255.255.255.0
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto

interface FastEthernet3/0
ip address 10.1.7.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 log-adjacency-changes
 network 10.1.7.2 0.0.0.0 area 0
 network 192.168.0.0 0.0.255.255 area 0
ip classless
no ip http server
no ip http secure-server
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
INST_EDU#
SHIKA#sh run
Building configuration...
Current configuration : 1854 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname SHIKA
boot-start-marker
boot-end-marker
```

```
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
ipcef
iptcpsynwait-time 5
no ip domain lookup
interface Loopback60
ip address 192.168.60.1 255.255.255.0
interface Loopback61
ip address 192.168.61.1 255.255.255.0
interface Loopback62
ip address 192.168.62.1 255.255.255.0
interface Loopback63
ip address 192.168.63.1 255.255.255.0
interface Loopback64
ip address 192.168.64.1 255.255.255.0
interface Loopback65
ip address 192.168.65.1 255.255.255.0
interface Loopback66
ip address 192.168.66.1 255.255.255.0
interface Loopback67
ip address 192.168.67.1 255.255.255.0
interface Loopback68
ip address 192.168.68.1 255.255.255.0
interface Loopback69
ip address 192.168.69.1 255.255.255.0
interface FastEthernet0/0
ip address 10.1.11.1 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet4/0
ip address 10.1.6.2 255.255.255.252
 duplex auto
 speed auto
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
ip classless
no ip http server
no ip http secure-server
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
SHIKA#


NAPRI#sh run
Building configuration...
Current configuration : 1854 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname NAPRI
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
```

```
ipcef
iptcpsynwait-time 5
no ip domain lookup
interface Loopback70
ip address 192.168.70.1 255.255.255.0
interface Loopback71
ip address 192.168.71.1 255.255.255.0
interface Loopback72
ip address 192.168.72.1 255.255.255.0
interface Loopback73
ip address 192.168.73.1 255.255.255.0
interface Loopback74
ip address 192.168.74.1 255.255.255.0
interface Loopback75
ip address 192.168.75.1 255.255.255.0
interface Loopback76
ip address 192.168.76.1 255.255.255.0
interface Loopback77
ip address 192.168.77.1 255.255.255.0
interface Loopback78
ip address 192.168.78.1 255.255.255.0
interface Loopback79
ip address 192.168.79.1 255.255.255.0
interface FastEthernet0/0
ip address 10.1.11.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
ip address 10.1.5.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
ip classless
no ip http server
no ip http secure-server
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
NAPRI#

KONGO#sh run
Building configuration...
Current configuration : 1894 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname KONGO
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
ipcef
iptcpsynwait-time 5
no ip domain lookup
interface Loopback80
ip address 192.168.80.1 255.255.255.252
interface Loopback81
```

```
ip address 192.168.81.1 255.255.255.252
interface Loopback82
ip address 192.168.82.1 255.255.255.252
interface Loopback83
ip address 192.168.83.1 255.255.255.252
interface Loopback84
ip address 192.168.84.1 255.255.255.252
interface Loopback85
ip address 192.168.85.1 255.255.255.252
interface Loopback86
ip address 192.168.86.1 255.255.255.252
interface Loopback87
ip address 192.168.87.1 255.255.255.252
interface Loopback88
ip address 192.168.88.1 255.255.255.252
interface Loopback89
ip address 192.168.89.1 255.255.255.252
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet4/0
ip address 10.1.4.2 255.255.255.252
 duplex auto
 speed auto
```

```
router ospf 1
 log-adjacency-changes
 network 10.1.4.2 0.0.0.0 area 0
 network 192.168.0.0 0.0.255.255 area 1
ip classless
no ip http server
no ip http secure-server
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
KONGO#
SENATE#sh run
Building configuration...

Current configuration : 1855 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname SENATE
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
ipcef
iptcpsynwait-time 5
no ip domain lookup
interface Loopback90
ip address 192.168.90.1 255.255.255.0
interface Loopback91
ip address 192.168.91.1 255.255.255.0
interface Loopback92
ip address 192.168.92.1 255.255.255.0
interface Loopback93
```

```
ip address 192.168.93.1 255.255.255.0
interface Loopback94
ip address 192.168.94.1 255.255.255.0
interface Loopback95
ip address 192.168.95.1 255.255.255.0
interface Loopback96
ip address 192.168.96.1 255.255.255.0
interface Loopback97
ip address 192.168.97.1 255.255.255.0
interface Loopback98
ip address 192.168.98.1 255.255.255.0
interface Loopback99
ip address 192.168.99.1 255.255.255.0
interface FastEthernet0/0
ip address 10.1.12.1 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet3/0
ip address 10.1.3.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
ip classless
no ip http server
no ip http secure-server
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end

SENATE#
FIRE_STATION#sh run
Building configuration...
Current configuration : 1901 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname FIRE_STATION
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
ipcef
iptcpsynwait-time 5
no ip domain lookup
interface Loopback100
ip address 192.168.100.1 255.255.255.252
interface Loopback101
ip address 192.168.101.1 255.255.255.252
interface Loopback102
ip address 192.168.102.1 255.255.255.252
interface Loopback103
ip address 192.168.103.1 255.255.255.252
interface Loopback104
ip address 192.168.104.1 255.255.255.252
interface Loopback105
ip address 192.168.105.1 255.255.255.252
interface Loopback106
```

```
ip address 192.168.106.1 255.255.255.252
interface Loopback107
ip address 192.168.107.1 255.255.255.252
interface Loopback108
ip address 192.168.108.1 255.255.255.252
interface Loopback109
ip address 192.168.109.1 255.255.255.252
interface FastEthernet0/0
ip address 10.1.12.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0
ip address 10.1.2.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
ip classless
no ip http server
no ip http secure-server
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
```

```
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end

FIRE_STATION#

CERT#sh run
Building configuration...
Current configuration : 1893 bytes
version 15.2
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
hostname CERT
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 5
ip subnet-zero
no ipicmp rate-limit unreachable
ipcef
iptcpsynwait-time 5
no ip domain lookup
interface Loopback110
ip address 192.168.110.1 255.255.255.0
interface Loopback111
ip address 192.168.111.1 255.255.255.0
interface Loopback112
ip address 192.168.112.1 255.255.255.0
interface Loopback113
ip address 192.168.113.1 255.255.255.0
interface Loopback114
ip address 192.168.114.1 255.255.255.0
interface Loopback115
ip address 192.168.115.1 255.255.255.0
interface Loopback116
ip address 192.168.116.1 255.255.255.0
interface Loopback117
ip address 192.168.117.1 255.255.255.0
interface Loopback118
ip address 192.168.118.1 255.255.255.0
```

```
interface Loopback119
ip address 192.168.119.1 255.255.255.0
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
ip address 10.1.1.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 log-adjacency-changes
 network 10.1.1.2 0.0.0.0 area 0
 network 192.168.0.0 0.0.255.255 area 2
ip classless
no ip http server
no ip http secure-server
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
CERT#
```