DEVELOPMENT OF ENHANCED DIFFERENTIATED SERVICES MODEL OF CAMPUS INTERNET NETWORK: A CASE STUDY OF AHMADU BELLO UNIVERSITY, ZARIA

BY

Julius Nyabvou PATRICK
M.Sc/ENG/36954/12-13

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES AHMADU BELLO UNIVERSITY ZARIA

IN PARTIAL FULFILLMENT FOR THE AWARD OF MASTER OF SCIENCE IN COMPUTER ENGINEERING

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

DECEMBER 2016

DECLARATION

I declare that the work in this dissertation entitled "Development of Enhanced Differentiated Services Model of Campus Internet Network; A Case Study of Ahmadu Bello University, Zaria" has been carried out by me in the Department of Electrical and Computer Engineering. The information derived from the literature has been duly acknowledged in the text and list of references provided. No part of this dissertation was previously presented for another degree or diploma at this University or any other institution

_____ _____

Julius Nyabvou Patrick Date

CERTIFICATION

This dissertation entitled "DEVELOPMENT OF ENHANCED DIFFERENTIATED SERVICES MODEL OF CAMPUS INTERNET NETWORK; A CASE STUDY OF AHMADU BELLO UNIVERSITY, ZARIA" by Julius Nyabvou PATRICK meets the regulations governing the award of the degree of Master of Science in Computer Engineering of the Ahmadu Bello University, and is approved for its contribution to knowledge and literary presentation.

_____ _____

Chairman, Supervisory Committee Date

(Dr. A. D. Usman)

_____ _____

Member, Supervisory Committee Date

(Dr. A.M.S. Tekanyi)

_____ _____

Head of Department Date

(Dr. Y. Jibril)

_____ _____

Dean, School of Postgraduate Studies Date

(Prof. Kabir Bala)

DEDICATION

To God Almighty, you are my All in All, the truth and source of all pure knowledge, and who in his munificence has granted humans both the desire and capacity to seek for the truth.

ACKNOWLEDGMENT

My perpetual gratitude goes to the Almighty God for Grace, love, Mercies revelations and faithfulness to me during this work. Thank you Lord; you are my All in All.

My profound gratitude and appreciation goes to my supervisors Dr. A. D. Usman and Dr. A.M.S. Tekanyi for their guidance, constant encouragement, constructive and objective criticism, inspiring motivations and for making necessary corrections during this work. God Bless you.

I sincerely thank Prof. M. B. Mu'azu and Dr. S. M. Sani for their constructive criticism and suggestions in improving the quality of this dissertation. Thank you for your patience.

I am thankful to these lecturers who in one way or the other have contributed by making necessary corrections to this work Dr. Y. Jibril, Dr. Kabir Ahmed Abu-Bilal, Dr. Sani Man-Yahaya, Dr. T. H. Sikiru, and all those whose names cannot be captured for want of space.

My heart warmly expresses my indebtedness and I bow in gratitude to my wife Ophelia Y. Patrick and daughter, Bernice Z. Patrick for love, understanding, patience, moral, financial and spiritual supports. Please accept my love.

I am extremely grateful to my parents Mrs Rosemary B. Patrick, Justice L.D Aba, Mrs. J.L.Aba, and late Mr. Patrick k. Badugu and; siblings, brother and sisters in-law Engr. Savior S. Patrick, Dr. Stephen S. Patrick, Rev. Fr. Christopher S. Patrick, Miss Esther B. Patrick, Miss Fidelia Aba, Barr. Cornelius Y. Aba, Engr. Emmanuel K. Patrick, Mr. Samuel Z. Patrick and Miss Angelina B. Patrick for their financial, moral support and encouragement.

I also recognize and appreciate Mr. T.M. Kunde and his wife Mrs. Cordelia Kunde, Mrs. Cecilia Ben, Mrs. Vera Peter and the rest too innumerable to mention, for their guidance and constant encouragement. You are so wonderful and acknowledged with no less gratitude for your contributions to my study.

TABLE OF CONTENTS

Page

Title Page i

Declaration ii

Certification iii

Dedication iv

Acknowledgement v

Table of Contents vi

List of Tables ix

List of Figures x

List of Abbreviations xi

List of Appendices xii

Abstract xiii

CHAPTER ONE: INTRODUCTION

1.0 Background 1

1.1.2 Ahmadu Bello University Internet Network 2

1.2 Motivation 4

1.3 Significance of Research 5

1.4 Statement of Problem 5

1.5 Aim and Objectives 6

1.6 Methodology 6

1.7 Dissertation Organisation 7

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction 8

2.2 Review of Fundamental Concepts 8

2.2.1 Campus Area Network 8

2.2.1.1 Features Campus Network 10

2.2.1.2 Campus Network Architecture 11

2.2.2 Performance Metrics in Computer Communication Networks . . 13

2.2.3 Need for Quality of Service 14
2.2.3.1 Factors which Determine Quality of Service 15
2.2.4 Network Services Models 16
2.2.4.1 Best-Effort Services Model 16
2.2.4.2 Integrated Services Model 17
2.2.4.3 Differentiated Services Model 18
2.2.4.4 Implementation of Differentiated Services 20
2.2.4.5 Analysis of Assured Forwarding 26
2.2.4.6 Limitations of Differentiated Services Architecture . . . 28
2.3 Review of Similar Research Works 29
2.3.1 Summary of Literature Review 34

CHAPTER THREE: MATERIALS AND METHODS

3.1 Introduction 35
3.2 Implementation of Differentiated Services Model Solution . . . 35
3.2.1 Implementation of Enhance Differentiated Services . . . 36
3.3 Simulation of Best-Effort and Developed Differentiated Services Model . 37
3.3.1 Best-Effort Network Service Model Simulation 37
3.3.2 Differentiated Services Models Simulation 39
3.3.3 Enhanced Differentiated Services Network Models Simulation . 43
3.4 Application and Validation of Enhanced Differentiated services model . 46
3.4.1 Best-Effort Service Model Validation 47
3.4.2 Differentiated Service Model Validation 48
3.4.3 Enhanced Differentiated Service Model Validation . . . 49

CHAPTER FOUR: RESULTS AND DISCUSSIONS

4.1 Introduction 51

4.2 Analysis of Results and Data Obtained using OPNET Simulator . . 51

4.2.1 Summary of Results Obtained using OPNET Simulator . . . 56

4.3 Results of Validation and Application of Enhanced Differentiated Model . 56

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary of findings 59

5.2 Conclusion 59

5.3 Limitation 60

5.4 Suggestion for Further Work 60

REFERENCES 61

LIST OF TABLES

Table 2.1:	QoS Requirements for Different Applications . . .	16
Table 2.2:	IP Precedence and DSCP Backward Compatibility . . .	25
Table 3.1:	Configuration Detail of Service Group Admission Control on a Router	50
Table 4.1	Delay of Best-Effort, Differentiated, and Enhanced Differentiated .	55
Table 4.2:	Best-Effort Service Model Validation Delay	57
Table 4.3:	Differentiated Service Model Validation Delay . . .	57
Table 4.4:	Differentiated Service Model Validation Delay . . .	58

LIST OF FIGURES

Figure 1.1: Topology Diagram of ABU Network 3
Figure 2.1: IP Headers 18
Figure 2.2: Differentiated Service Code-Point Field 19
Figure 2.3: Differentiated Services 20
Figure 2.4: Threshold of Dropping Queue of N Drop Precedence . . 26
Figure 3.1: Basic Differentiated Services Model 35
Figure 3.2: Proposed Enhance Differentiated Services Model . . . 36
Figure 3.3: OPNET Simulation of Best-Effort Services Model . . . 38
Figure 3.4: OPNET Simulation of Differentiated Services model . . 39
Figure 3.5: Flow Chart of OPNET Implemented of DSM . . . 40
Figure 3.6: OPNET Simulator Configuration of Packet Classifications . . 41
Figure 3.7: OPNET Simulator Configuration of Monitoring and Policing . 42
Figure 3.8: OPNET Simulation of Enhanced Differentiated Services Model . 43
Figure 3.9: Flow Chart OPNET Implementation of Enhanced Differentiated . 44
Figure 3.10: OPNET Simulator Setting-up of Admission Control . . 45
Figure 3.11: Validation Test-Bed Topology 46
Figure 3.12: Validation Setup at MKCL 47
Figure 3.13: Screenshot of Best-Effort Delay Obtained using Wireshark . 47
Figure 3.14: Screenshot of DSM Delay Obtained using Wireshark . . 48
Figure 3.15: Screenshot of EDSM Delay using Wireshark . . . 50
Figure 4.1: Delay in Seconds of Best-Effort Services Model Scenario . . 51
Figure 4.2: Delay of Differentiated Services Test Scenario . . . 52
Figure 4.3: Delay of Enhanced Differentiated Services Test Scenario . . 53
Figure 4.4: Delay of EDSM, DSM and ABU Test Scenario . . . 54

LIST OF ABBREVIATIONS

Acronym	Meaning
ABU . .	Ahmadu Bello University
DSM . .	Differentiated Services Model
EDSM . .	Enhanced Differentiated Services Model
CAN . .	Campus Area Network
QoS . .	Quality of Service
IP . .	Internet Protocol
IETF . .	Internet Engineering Task Force
FIFO . .	First in First out
PCQ . .	Per Connection Queuing
RFC . .	Request for Comment
LAN . .	Local Area Network
BRAS . .	Broadband Remote Access Server
RAS . .	Remote Access Server
VPN . .	Virtual Private Network
DSCP . .	Differentiated Service Code Point
DS . .	Differentiated Services
CoS . .	Class of Services
AcL . .	Access List
PBFS . .	Packet Based per Flow State
ToS . .	Type of Services
PHB . .	Per Hop Behaviors
EF . .	Expected Forwarding
AF . .	Assured Forwarding
ESD . .	Expected Scheduler Delay
CSFQ . .	Core State Fair Queuing

LIST OF APPENDICES

Appendix I:	Best-Effort Architecture Configuration on Routers . .	67
Appendix II:	DSM Configuration on Routers	70
Appendix III:	EDSM Configuration on Routers	74

ABSTRACT

Modern campus networks are designed for high-speed service with the capacity to handle many organization's bandwidth requirements, support data applications such as electronic-mail, web and files sharing services. These networks sometime lack the capacity to guarantee quality of service for voice, video and other interactive applications due to bandwidth requirement and high packet end-to-end delay. In some networks, voice, video and other interactive packets must be given priority in terms of bandwidth and delay over less-time-sensitive packets such as mail or file sharing for the networks to meet the QoS demand of these voices, video and other interactive applications. In this research, best-effort service model currently employed in Ahmadu Bello University (ABU) Internet network and differentiated services networking model define in RFC 2474 were analyzed. Enhanced differentiated services model was developed to improve and achieve better reduction in packet end-to-end delay of interactive traffic such as video conferencing and voice streaming in networks. The simulation results obtained of simulation of the three services model showed that enhanced differentiated services model with mean packet end-to-end of 0.10481s has 26% delay reduction as compared with differentiated services model with mean packet end-to-end of 0.10757s. The enhanced differentiated services model has 32% delay reduction as compared to the best-effort services model with mean packet end-to-end of 0.15417s. Similarly, validation results obtained of mean delay of the enhanced differentiated services model performed better than the differentiated services model by 40% and better than the best-effort services model by 83%. These results demonstrate the superiority of the enhanced differentiated service to differentiated service and best-effort services models in reduction of packet end-to-end delay of a network.

CHAPTER ONE

INTRODUCTION

1.1 Background

Information technology is strategically important to the goals and aspirations of business enterprises, government entities and educational institutions, particularly Universities. It is the cornerstone that enables the University's faculties, researchers, students, administrators, and staff to discover, learn, reach out, and serve humanity.

Campus Area Networks (CANs) such as ABU network transmit interactive and multimedia applications such as video and audio streaming for experimental, practical and other uses. The numbers of such interactive and multimedia applications on such networks are on the increase. Voice, video and data applications demand different types of performance assurance and so Quality of Service (QoS) provision is one of the important components in the design of such networks. Researchers have done considerable work in developing QoS models, mechanism and queuing disciplines to improve transmission of interactive and multimedia applications on IP networks. The challenge of implementation of the developed QoS models, and queuing mechanism on last mile networks of the internet and the inability and inappropriate implementation of most of the QoS models result in the degradation of the QoS in terms of packet loss, packet delays, and packet delay variation for messages transmitted over the networks.

Packet-based networks are networks in which packets sent from a source may traverse different paths to arrive at the final destination. The packets that are routed over separate paths are reassembled at the destination. Transmission rates of the various paths may vary depending upon the usage of the network paths over which the packets are being transmitted (Abaye *et al.*, 2006).

During heavy traffic conditions, packets may be delayed and lost. Packet delays and losses cause poor performance of the network and are more obvious with voice and other interactive streaming communications. Interactive streaming packets (voice, multimedia) in a network share the network bandwidth with conventional non-streaming packets (such as data associated with electronic mail, file transfer, web access, and other traffic). Voice data and other interactive packets that are lost or delayed due to inadequate or unavailable capacity of networks may result in gaps, silence, and clipping of audio at the receiving end, thus affecting the QoS of the network (Abaye *et al.*, 2006). One solution for this problem is the over provisioning of bandwidth. Howeve is an expensive option for service utilises and can be difficult to ensure in all cases. Another and a preferred solution is the use of QoS models. Two of such models that have been standardized by the Internet Engineering Task Force (IETF), are integrated services and differentiated services models. Due to scalability issue with integrated service model, differentiated services models is mostly preferred. The preferred differentiated services model also has the challenge of Packet being processed and eventually dropped during the last process, if threshold of queues are exceeded. This leads to added delay to incoming packet caused by the processing time of packets which are eventually dropped, hence the need to improve the differentiated services models for better performances.

1.7.2 Ahmadu Bello University Campus Network

The physical connectivity diagram of ABU network shown in Figure 1.1 illustrates how network devices are connected. Packets are transmitted between devices through a series of routers. Each intermediate router in the network may receive packets via multiple data streams that are routed simultaneously from their source devices to their respective destinations. In such conditions, packets may have to be stored at the intermediate routers for transmission at a later time due to reasons such as full buffers, packet loss or scheduling.

In ABU network, arriving internet packets are assigned on per connection queuing using first in first out (FIFO) queuing disciple.

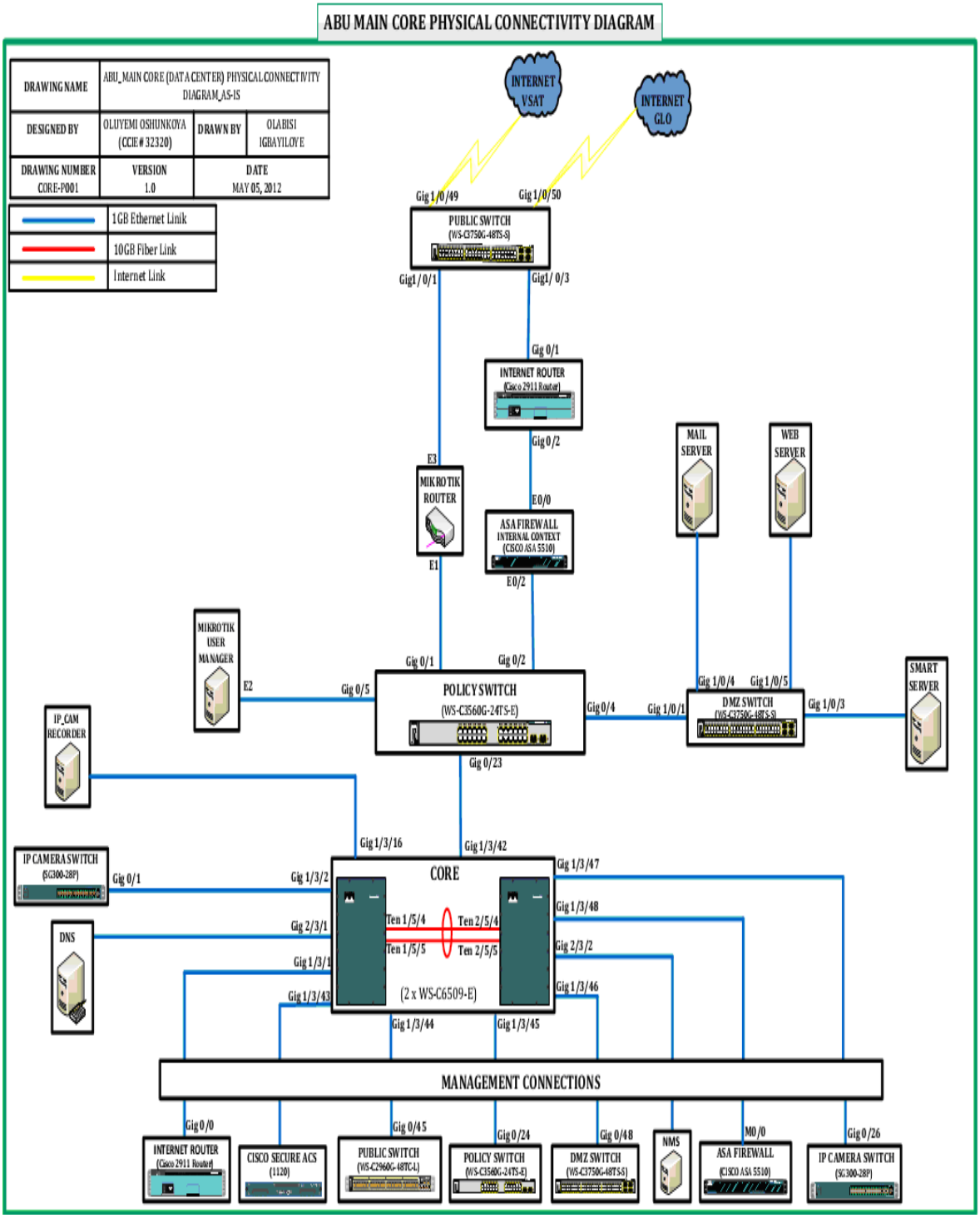


Figure 1.1: Topology Diagram of ABU Network (Tekanyi 2014)

The Per Connection Queuing (PCQ) is a method that can be used to dynamically equalize or shape traffic for multiple users. It is possible to divide PCQ scenarios into three major groups: equal bandwidth for a number of users, certain bandwidth equal distribution between users, and unknown bandwidth equal distribution between users. The ABU network uses PCQ with best-effort services model (without QoS), a staff is allotted 1Mbit/s bandwidth and a student allotted 50kbit/s bandwidth when there is congestion, while during light periods of traffic when there is no congestion at the interfaces, packet on arrival are served and dispatched. During heavy load periods of traffic in which packets arrival rate are faster than outgoings from the interface, congestion occurs and packets queue for services to avoid drop, once the interface is free they are serviced and transmitted based on their assigned priority employed at the interface. On such instances of congestion, transmission of multimedia and interactive traffic may suffer degradation of services across the network since such traffics has high bandwidth requirement and are delays sensitive. To avoid degradation of services of such multimedia and interactive traffics, service differentiation and priority will require being given to the multimedia and interactive traffic over non delay sensitive traffic at the interface with congestion.

Therefore there is a need to continuously improve the ABU network by evolving better QoS model to support and improve the transmission and deployment of interactive applications on the network.

1.8 Motivation

Transmission of voice, video and other interactive traffic may suffer degradation of services across a campus Internet network if there is congestion. Voice, video and data applications demand different types of performance assurance and QoS. Campus Internet network may require service differentiation and priority queuing at the interface in which congestion occurs to

give priority to delay sensitive traffic such as voice, video and other interactive traffic over non delay sensitive traffics such as file download and electronic mail traffic. The motivation for this dissertation is to develop and improve the differentiated services QoS architecture to reduce packet end to end delay and guarantee QoS for of delay sensitive traffic on campus Internet network.

1.9 Significance of Research

The contributions of this research are as follows:

i. Improve packet end to end delay by 32% compared with ABU current services model.
ii. Achieved 26% packet end to end delay reduction when compared with standard differentiated services model.

1.10 Statement of Problem

Due to the demand for new types of services, Universities' campuses are facing new challenges related to network infrastructure. The recent push to converge voice and video onto the data network has made QoS guarantee a critical factor in the design and engineering of campus area networks. Transmission of voice, video, and other interactive traffic may suffer degradation of services across the network if there is congestion and may require service differentiation and priority queuing at the interface where congestion occurs in order to give priority to delay sensitive over non delay sensitive traffic. Hence, the need to develop and continuously improve QoS architecture that can differentiate and give priority to delay sensitive video, voice and other interactive traffic during congestion periods in a campus network in order to reduce packet end to end delay of delay sensitive traffic.

1.11 Aim and Objectives

The aim of this research is to develop an enhanced differentiated services model to improve the differentiated services model define in RFC 2474. This is with the view to reduce packet delay of sensitive traffic on a campus Internet network.

The objectives of this research are:

i. Develop an enhance differentiated services model for a Campus Area Network (CAN)
ii. Compare the proposed enhanced differentiated services with best-effort and differentiated service model using Riverbed Modeller Academic Edition 17.5 (OPNET)
iii. Validate the developed enhanced differentiated services model using live routers on a test-best network to establish the improvement achieved by the developed model.

1.12 Methodology

The research methodology is as follows:

i. Implementation of differentiated services model and its simulation using OPNET simulator.
ii. Development of enhanced differentiated services model and its simulation using OPNET simulator.
iii. Comparison of performance of best-effort, differentiated services model with that of the developed enhanced differentiated services model.
iv. Validation of the developed enhanced differentiated services model using live routers and switches on a developed Test-bed network.

1.13 Dissertation Organisation

The summary of how the rest of the chapters are organised is presented thus:

Having presented the introduction with the general background of the dissertation in chapter one, chapter two presents the literature review consisting of systematic review of some fundamental concepts theories relevant to differentiated services model and the developed enhanced differentiated service model. Also in this chapter is a comprehensive review of work similar to this dissertation. Development of the enhanced differentiated services model is analysed in chapter three. Prior to this, the general structure of the differentiated services model defined in RFC 2474 and it shortcoming is briefly highlighted in the chapter. Chapter four presents the results of simulation and validation of the developed differentiated services model. A test bed using live router and switches was developed and the best-effort, differentiated and the developed enhanced differentiated service were configured and the end to end delay measured using Wireshark network analyser. Chapter five presented the conclusion of the study. Also in the chapter are the summary of finding and the suggestion for further work. Finally, all cited references are presented at the end of this dissertation work.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

This chapter present literature review, this provides the background knowledge related to the proposed topic and similar research works conducted by other researchers in that area in order to provide the basis for the approach taken to resolve congestion problem of campus networks. This is provided in two perspectives: a discussion of fundamental concepts and the review of similar works on the research topic.

2.2 Review of Fundamental Concepts

In discussing fundamental concepts, campus area networks performance metrics used in communications networks such as packet delay and packet delay variance of a network, network services models, as well as network topology and routing in packet switch network are discuss. Issues affecting these performance metrics, such as QoS, traffic management and congestion control are also studied.

2.2.1 Campus Area Network

Campus area network is a computer network interconnecting a few to several Local Area Networks (LANs) within a University campus. Campus area network may link a variety of campus buildings, including colleges, departments, student halls of residence, library, etc.

Characteristics such as scalability, flexibility, QoS, topology, etc are very important requirements in the design process of a network. Therefore, many design models, such as hierarchical model that exists can be followed to simplify network design process.

Hierarchical model simplifies the design through the methodology of breaking the network into three main components which are: access network, distribution network (convergence / aggregation network) and core network (backbone network) in order to make the network

smaller and more manageable (Academy 2014). That of a CAN is supported by different layers each rendering specific functions. These layers are:

i. Core layer.
ii. Distribution layer
iii. Access layer

Core Layer: The core layer provides a high-speed backbone for forwarding all traffic in the network. It also provides very strong routing and forwarding capabilities and wide bandwidth. Functions and attributes of the core layer include the following (Academy 2014):

i. Providing a high speed, highly reliable, and available backbone. This is accomplished by implementing redundancy in both devices and links, so that no single point of failure exists.
ii. It provides quick adaptation to network changes by implementing quick-converging routing protocols. The routing protocol is designed with fault tolerance. Only physical route should implement redundant link so that the extra capacity can be used when failures exist.

Distribution Layer: The distribution layer interface is between the core and access layer. Its functions include:

i. Implementing policies of filtering, prioritizing, and queuing traffic through broadband equipment, such as Broadband Remote Access Server (BRAS).
ii. Routing traffic between the access and core layers.
iii. Providing redundant connections, both to access and core devices.

Access Layer: Access layer is the point of entrance of the users to the network. Users can be local or remote. Local users typically access the network through connections to a LAN switch.

Remote users might access the network through the Internet or Remote Access Server (RAS) using Virtual Private Network (VPN) connections. Access layer functions include:

i. Authentication of the users by ensuring that only users who are authorized to access the network are admitted (Security-Network Access Server).
ii. Guarantying that users are charged according to accounting policies implemented.
iii. Implementing QoS mechanism that reduces network delay time and packet delay variance

2.2.1.1 Features of Campus Network

Campus networks characteristics are different from other types of networks, such as governmental or enterprises networks. The government networks have very high security and high-availability requirements. An enterprise network has several criteria that determine different network requirements according to specific cases. It depends on the business field, such as financial/bank institutions, business sales, and service provision. Regarding those criteria demands for high-availability and scalability, security services such as intrusion detection/prevention and manageability can be important requirements to be met by the network. In summary, for government and financial institutions, data security and network reliability are of vital concern.

University campus network core mission is research and build knowledge through teaching. Hence, campus networks are designed to support specific requirements and characteristics. Some important characteristics and requirements of a campus network include the following (Ustares 2010):

i. Large-scale networks with active and different user groups.
ii. Multiple and integrated access network system.

iii. Complex network system management.

iv. Open and flexible network environment and in continuous development.

v. Multitude of network activities, including researches, laboratories experiments and simulations, electronic learning (e-learning), etc.

vi. Security limitations.

vii. Need for availability and high-performance network design to improve collaboration among researchers, faculty, staff, and students and to support the deployment of new applications and services.

2.2.1.2 Campus Network Architecture

Networks are evolving from two separate networks – that is voice oriented network developed by International Telecommunication Union (ITU) and data oriented network developed by Internet Engineering Task Force (IETF). Furthermore, the converged next generation network allows a set of new emerging services, where both data and multimedia traffic are sent using the single IP network with the advantages of offering integrated multi-services to the users. These two different kinds of traffic have different characteristics and QoS requirements. An important challenge for today's network is to properly design an infrastructure that can meet the requirements of different types of traffic and provide different QoS to a wide variety of applications.

A network architecture model provides a framework and technological foundation for designing, building, and managing a communication network (Dannewitz, et al. 2013). A layered model divides the communication tasks into a number of components and each component provides a set of functions and interacts with each other. Network architecture is a set of functions and abstract design principles. Each of these functions becomes an important component above

which a network is built. There are four components that make up network architecture, which are:

i. Services and network management
ii. Network control,
iii. Switching
iv. Edge access

Services and Network Management: Providing multimedia services in a university environment are important since it facilitates faculties, departments, staff and students work collaboration and communication as well as researches and other related applications. They also improve the quality of distance learning (e-learning) based on a broad range of converged communications infrastructure access. Network management system carries out fault management, configuration management, accounting management, performance management and security management for all devices. Network management ensures monitoring and management services and a variety of components of the entire network infrastructure of campus network. Managing networks deals with monitoring the network in a way to detect and prevent failure, analyse and improve networks performance and respond to demands of services in a shorter time.

Network Control: Networks are evolving towards the convergence of voice, video, data, and mobile network technology over an IP-based infrastructure. However, Multimedia stream have different characteristics and QoS requirements from data stream and hence, it needs different protocols from the original TCP/IP protocols. Thus, news protocols are emerging like the Real-Time Protocol (RTP) and Resource ReSerVation Protocol (RSVP) for improving support to applications like video, audio, and interactive multimedia conferencing. Therefore, network

administration provides critical functions to integrate all those services and support these different protocols.

Core Switching: It is usually the constitution of Layer 2 and Layer 3 switches and routers. Ethernet is widely adopted at campus networks due to its excellent cost/performance ratio and its configuration convenience. The core technology for the campus network can be hybrid technology consisting of fiber optic and wireless technologies. The hybrid technology has advantages, such as high bandwidth facilities and mobility.

Edge Access: Edge access is the part of network responsible to connect subscribers and equipment through different access technologies and provides information conversion to a format suitable to be transported over the network.

2.2.2 Performance Metrics in Computer Communication Networks

Performance metric is a standard definition of a measurable quantity that indicates some aspect of performance. Performance metrics are the criteria used to evaluate the performance of a system. There are a number of metrics applicable to computer networks, but the focus of this research will be on packet delay metric which is of greatest relevance to the development and efficient running of multi-media application in any communication network. Computer network performance metrics include (Obiniyi *et al.,* 2014):

Availability: Availability metric assesses how robust the network is. It presents the percentage of time the network is running without any failure of specific network element or any problem affecting the availability of services.

Throughput: This refers to the average rate of successful data or message delivery over a communication link or system and is usually measured in bits per second (bit/s or bps).

Latency: Latency refers to the amount of time it takes data to travel from one location to another across a network. It is usually measured in milliseconds (ms). It is sometimes referred to as delay because the software may often wait to execute some functions while data travels back and forth across the network.

Delay: The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. Delay metric also assess the network congestion condition or effect of routing change.

Packet Delay variance/Jitter: Jitter is often used as a measure of variability over time of the packet latency across a network. A network with constant latency has no variation (or jitter). Packet jitter is expressed as an average of the deviation from the network mean latency. It is usually referred to as Packet Delay Variation (PDV).

Bandwidth: Bandwidth means the used capacity or available capacity of a network, link or route. It may also refer to the consumed bandwidth, corresponding to the achieve throughput, which is the average rate of successful data transfer through a communication path. Bandwidth metric, in practice, assess the amount of data that a user can transfer through the network in a time unit and may be dependent or independent of the existing network traffic.

Packet Loss: Packet loss and error metrics are indicative of the network congestion conditions and/or transmission errors and/or equipment malfunctioning. They basically measure the fraction of packets lost in a network due to buffer overflows, link error, or other reasons.

2.2.3 Need for Quality of Service

The concept of QoS is a generic term that defines the level or measure of service that is provided for a particular application or network service. It also refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies (Tavares,

2011). Modern switched networks are high-speed networks that are capable of handling many organization's bandwidth requirements. With the recent push to converge voice and video onto the data network, QoS has moved from being a Wide-Area Network (WAN)–only feature (where the links are relatively slow) to a feature that is required throughout the WAN and LAN. Due to the demands for new types of service, universities' campuses are facing new challenges related to network infrastructure, voice traffic is not bandwidth-consuming, but it is delay and delay variance-sensitive. A CAN and LAN must be able to provide minimal delay and delay variance to meet the required QoS. These requirements make QoS on such networks a real challenge. Therefore, the need to design networks which have the following functionalities (Tavares, 2011).

i. Can deliver multiple classes of service – that is they should be QoS conscious.
ii. Is scalable – so that network traffic can increase without affecting network performance.
iii. Can support emerging network intensive, mission critical applications.

In order to meet these functionalities the network should implement service models so that services are specific to the traffic they service.

2.2.3.1 Factors which Determine Quality of Service

Four important parameters used to measure QoS (Tavares, 2011) include:

i. Packet delay.
ii. Packet delay variance.
iii. Packet loss.
iv. Bandwidth.

The guidelines for ensuring acceptable QoS for different traffic types are displayed in Table 2.1 (Hutcheson, 2008).

Table 2.1: QoS Requirements for Different Applications

Traffic type	Bandwidth	Loss (max)	Delay (max)	Delay variance (max)
Interactive voice (G.711)	12-106 kbit/s	1%	150 ms	30 ms
Streamed video (MPEG-4)	0.005-10 Mbit/s	2%	5000 ms	Insensitive
Streamed audio (MP3)	32-320 kbit/s	2%	5000 ms	Insensitive
Data	Variable	Sensitive	Insensitive	Insensitive

IETF developed two QoS service models: integrated service and differentiated service models to improve the best-effort service network.

2.2.4 Network Services Models

The commonly implemented network services models are three which are:

i. Best-effort service model.

ii. Integrated service model.

iii. Differentiated service model.

2.2.4.1 Best-Effort Services Model

Best-effort is the service provided to all kinds of traffic for their transportation. It is a network policy where no special QoS model is implemented and all traffic is treated equally. This model delivers the entire packet to the destination without guarantees of its delay, delay variance, loss, etc. There is no differentiation between the kinds of traffic, no classification or prioritization, and all packets receive the same treatment independent of their contents (Tavares, 2011).

Best effort is the treatment that packets get when no predetermined preference is specified for them. If there is congestion on the medium, the caching function can be used to store packets temporarily and when the situation is resolved, packets are forwarded. In the event of extreme congestion when the network devices cannot handle the packets coming to such devices, packets are dropped indiscriminately irrespective of their levels of importance (Tavares, 2011).

For packet loss, the retransmission model is one of the alternative methods used. This model is well suited for services such as web mail, file transfer, web access, etc. However, for real-time services such as video conferencing, different models that can guarantee QoS are preferable used. Best-effort service is not suitable to guarantee end-to-end QoS for all kind of traffic (Tavares, 2011). To provide end-to-end QoS, two models are deployed: integrated services and differentiated services models. End-to-end QoS means that the network provides the level of service required by traffic throughout the entire network, from one end to the other.

2.2.4.2 Integrated Services Model

The basic concept behind integrated services is that network resources are apportioned according to application request and subject to bandwidth management policy. Integrated services use an explicit signalling mechanism from applications to network devices to reserve and release resources in the network. The application requests a specific service level, for example, its bandwidth and delay requirements. After the network devices have confirmed that it can meet these requirements, the application is assumed to only send data that requires that level of service.

Applications in an integrated services environment use the RSVP to indicate their requirements to the network devices. The network devices keep information about the flow of packets, and ensure that the flow gets the resources it needs by using appropriate queuing (prioritizing traffic) and policing (selectively dropping other packets) methods. Two types of services provided in an integrated services environment are as follows (Tavares, 2011):

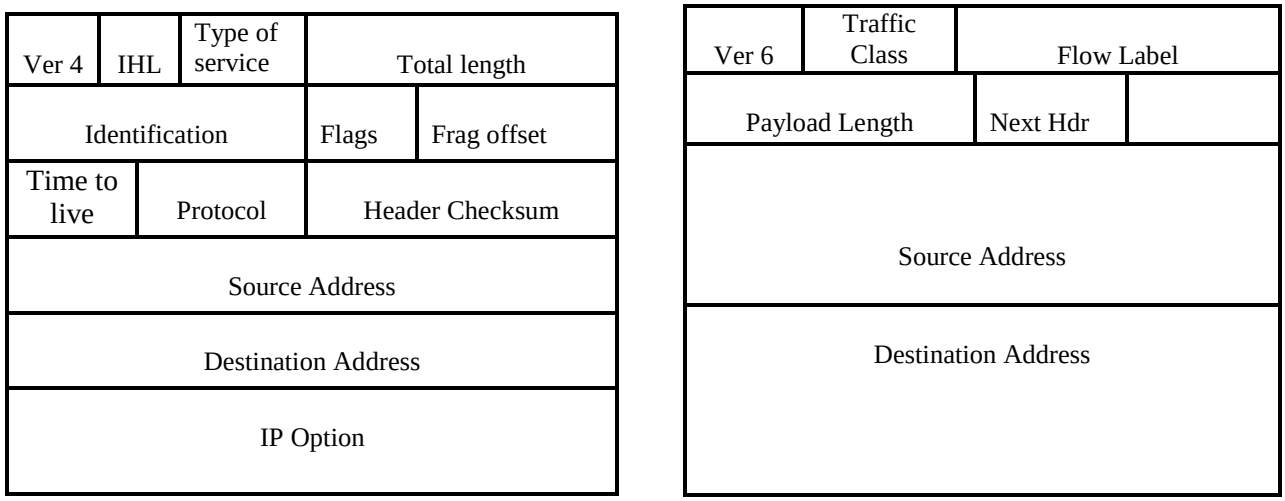
i. **Guaranteed Rate Service** - This service allows applications to reserve bandwidth to meet their requirements. The network uses Weighted Fair Queuing (WFQ) with RSVP to provide this service.

ii. **Controlled Load Service** - This service allows applications to request low delay and high throughput, even during times of congestion. The network uses RSVP with Weighted Random Early Detection (WRED) to provide this kind of service.

Integrated services model provisions resources for network traffic and requires RSVP on all network devices. This characteristic makes it not used currently as much as differentiated services.

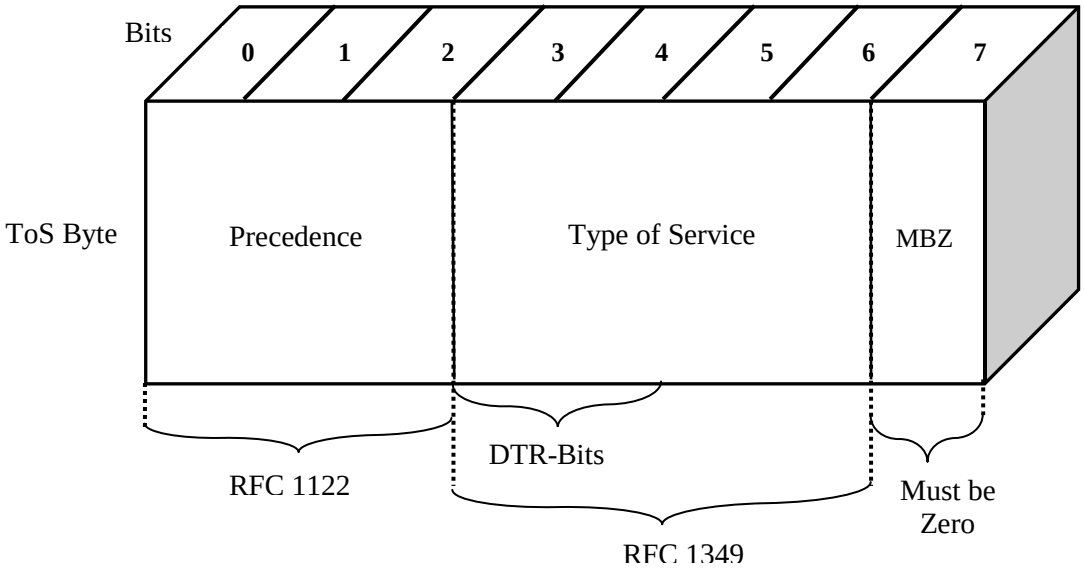
2.2.4.3 Differentiated Services Model

Differentiated services mechanism technique treats packets with different level of requirements depending on their source, destination, and/or the kind of traffic they are carrying. To accomplish this, packets are first divided into classes by marking the Type of Service (ToS) byte in the IP header. A 6-bit bit-pattern, called the Differentiated Services Code Point (DSCP) in the Internet Protocol version 4 (IPv4) ToS octet or the Internet Protocol version 6 (IPv6) traffic class octets, are used as shown in Figures 2.1 and 2.2 respectively.



(a) Version Four (b) Version Six

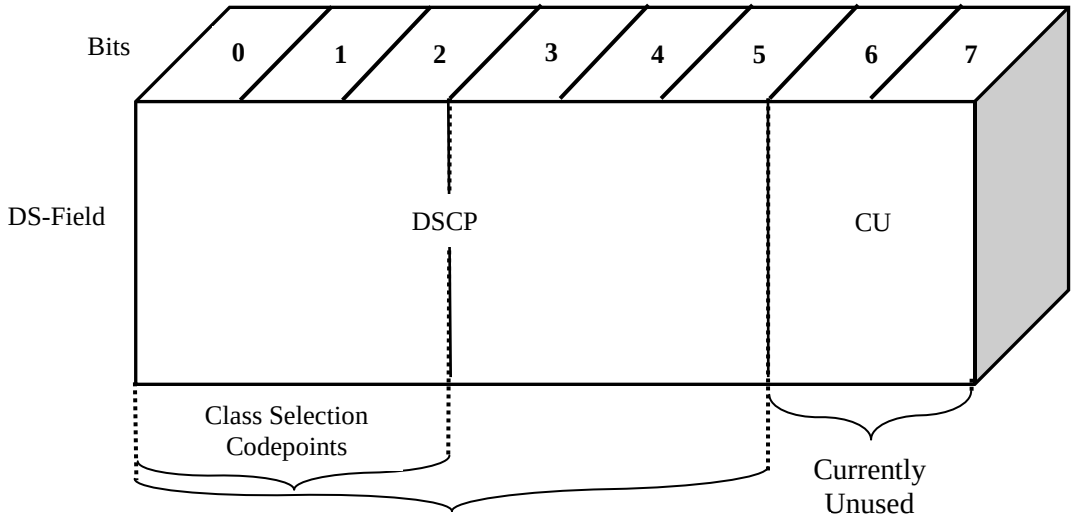
Figure 2.1: IP Headers (Cisco Systems, 2006)



Bits (0-2): IP-Precedence Defined
111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 - Flash
101 - Immediate
001 - Priority
000 - Routine

Bits (3-6): The Type of Service Defined
0000 - [all normal]
1000 – [minimize delay]
0100 – [maximize throughput]
0010 – [maximize reliability]
0001 – [minimize monetary cost]

(a) IPv4 Type of Service Byte



(b) Differentiated Service Code Point

Figure 2.2: Differentiated Service Code-Point Field (Cisco System, 2005)

The network tries to provide the level of service based on the QoS defined in the header of each packet. Packets are usually classified or marked by edge network devices according to previous defined criteria such as source, destination, and kind of traffic. Classification and marking are the fundamental bases of differentiated services as they help implement priority in the network. At first, packet is identified and depending on that identification it is given priority over other packets or different treatment from them.

The process of classification of packet is the process of analysing and sorting packets according to their contents between different categories. It means that each packet is designate as belonging to voice category, data category or multimedia category, etc.

Each category has different level of QoS requirements. Marking process will check the category that the packet belong to and therefore put a mark or level of priority within the head of packet. Packets belonging to voice categories can be marked as high priority because of their high QoS requirement.

2.2.4.4 Implementation of Differentiated Services

The following actions are undertaken when implementing differentiated services and they include classifying packet, marking, metering, and scheduling (shaping or dropping) of packet:

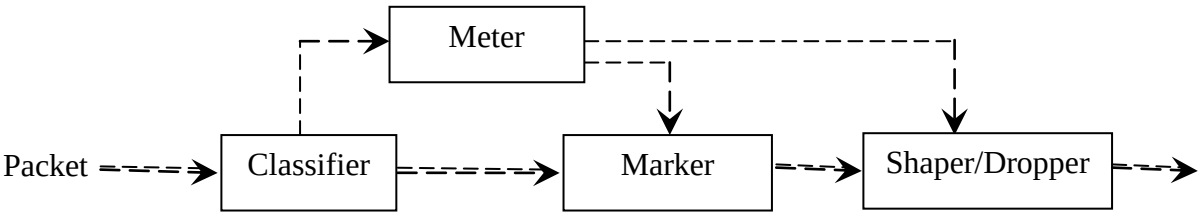


Figure 2.3: Basic Differentiated Services (RFC 2474)

Traffic Classification: Traffic classification distinguishes one traffic type from another. The process generates Differentiated Services Code Point (DSCP) for each packet, which identifies all the future QoS actions to be performed on this packet. Packet classification involves using a

traffic descriptor (such as packet source interface, packet destination media access control, packet protocol type etc.) to categorize packet within a specific group and to make the packet accessible for QoS handling in the network. Using packet classification, network traffic can be partition into multiple priority levels or Class of Service (CoS). Traffic classification can be achieved using either Access Lists (ACLs) or the match command. This describes how to set the DSCP values when configuring QoS on a Cisco router. To create a traffic class, the *class-map* command can be used. The syntax of the *class-map* command is as follows: *class-map [match-any | match-all] class-name no class-map [match-any | match-all] class-name*

An ACL refers to rules that are applied to port numbers or IP addresses that are available on a host or other layer 3, each with a list of hosts and/or networks permitted to use the service. According to Shaikh and Harkut (2015), Access control lists ACLs method typically utilizes the basic payload-based (based on port number, protocol, source address and destination address) classification technique. Classification is on a per-packet basis. Packet-Based per Flow State (PBFS) method is based on flows. A flow is defined as a sequence of packets from a sending application to a receiving application. In this method, a table to track each session based on the source address, destination address, source port, destination port, and the transport protocol is maintained for each flow. Since a flow has multiple packets, once a packet is marked as belonging to an application all subsequent packets in the flow need to be marked as such. For example, in a typical VoIP call, H.323 is used for setting up the call and then RTP/RTCP is used for carrying the actual voice traffic. Once a H.323 flow is identified and marked, subsequent RTP/RTCP flows to the same source IP/destination IP pair are tagged with the same parameters.

The *match-all* and *match-any* keywords need to be specified only if more than one match criterion is configured in the traffic class. *The match-all* keyword is used when all of the match

criteria in the traffic class must be met in order for a packet to be placed in the specified traffic class. The *match-any* keyword is used when only one of the match criterions in the traffic class must be met in order for a packet to be placed in the specified traffic class. If neither the *match-all* nor *match-any* keyword is specified, the traffic class will behave in a manner consistent with match-all keyword.

Marking: Packet markers set the Differentiated Services (DS) field of a packet to a particular code point, adding the marked packet to a particular DS behaviour aggregate. The marker may be configured to mark all packets which are steered to it to a single code point, or may be configured to mark a packet to one of a set of code points used to select a Per - Hop Behaviour (PHB) in a PHB group, according to the state of a meter. When the marker changes the code point in a packet it is said to have "re-marked" the packet

Implementing differentiated services QoS requires using the following markers for each packet or frame transmitted (Cisco System, 2011):

i. Type of service (applies to IP traffic)
ii. Class of service (applies to Layer 2 traffic)
iii. Differentiated Services Code Point (Applies to IP traffic)

Type of Service: The most common form of QoS marking present in IP networks today is the use of the Type of Service (ToS) field. Interpreted by routers, the ToS field is a part of the IP header and allows for a QoS marking to be applied on a per-packet basis.

Two subfields exist within the ToS field as shown in Figure 2.2 (a). The ToS subfield is not used, with the precedence subfield being the only portion of the ToS field actually used today. The IP precedence value is simply a 3-bit binary value, which in decimal terms represents a value of 0 through 7. The value indicates the relative priority of the packet, with 0 representing

the lowest priority and 7 representing the highest priority. Each priority level is also assigned a name, for example, an IP precedence value of 6 that represents internetwork control traffic.

Class of Service: Class of Service (CoS) refers to the marking of Layer 2 frames that indicates the QoS requirements of the frame. CoS is required for Layer 2 devices to apply QoS within a Layer 2 network if Ethernet is considered the Layer 2 technology. A CoS field is created on tagged traffic, where the tag is primarily used to identify the VLAN that the tagged frame belongs to. Two major tagging techniques (trunking protocols) are supported by Cisco switches today—IEEE 802.1Q and ISL.

Differentiated Services Code Point: The IP precedence marking mechanism provides up to eight different indications of QoS. Eight levels of QoS are not sufficient for many large networks, thus resulting in scalability issues. Recently, the IETF has developed a new standard as highlighted in RFC 2474 that defines a differentiated services (DS) Field that obsoletes the old ToS and precedence fields and uses the first six high-order bits (up to 64 levels of QoS) for QoS marking. The value defined in the DS Field is known as the DSCP and is designed to be backward compatible with older routers that only understand IP precedence.

In the differentiated services model, each device that can provide QoS is able to provide PHB for different classes of traffic. The PHB is simply the way in which the queuing and scheduling mechanisms on a forwarding device are implemented for a particular class of traffic. Differentiated services-compliant networks support the following PHBs (RFC 2474):

i. **Default PHB**: Defined in RFC 2474, this defines that traditional best-effort service (first-in, first-out) should be applied. RFC 2474 states that a DSCP value of 0 should be used to indicate that the default PHB be applied to a packet.

ii. **Class-Selector PHB**: Defined in RFC 2474, this is used to preserve backward compatibility with IP precedence, by setting the three low-order bits to 000 (DSCP values are in the format xxx000, where xxx is equivalent to IP precedence). With this PHB, forwarding devices must apply queuing and scheduling in the same fashion as IP precedence is applied. For example, a packet with a DSCP value of 111000 (equivalent IP precedence of 7) is provided preferential treatment over a packet with a DSCP value of 101000 (equivalent IP precedence of 5).

iii. **Expedited Forwarding PHB**: This PHB is designed for applications that required guaranteed bandwidth, low latency, and low jitter, such as voice and video. To provide this service, a forwarding device will typically place packets into a priority queue that is serviced before any other queues. RFC 2598 defines a DSCP value of 46 to indicate that the expedited forwarding PHB is required.

iv. **Assured Forwarding PHB**: Defined in RFC 2597, this defines four classes of traffic called AF1, AF2, AF3 and AF4, each of which can be assigned a different level of QoS. For example, a forwarding device might allocate 10%, 20%, 30% and 40% of a link bandwidth to the AF1, AF2, AF3 and AF4 classes, respectively. Within each class, three sub-classes exist (AFx1, AFx2 and AFx3), with each sub-class defining a relative drop precedence, which is used to determine which packets should be dropped first if a queue is full. For example, in the AF3 class, traffic assigned to the AF33 sub-class will be discarded before traffic in the AF32 sub-class, which in turn will be discarded before traffic in the AF31 sub-class

Table 2.2: IP Precedence and DSCP Backward Compatibility (Cisco, 2011)

Drop Precedence	**Class 1 (AF1)**	**Class 2 (AF2)**	**Class 3 (AF3)**	**Class 4 (AF4)**
Low Drop Precedence	AF11 DSCP = 10	AF21 DSCP = 18	AF31 DSCP = 26	AF41 DSCP = 34
Medium Drop Precedence	AF12 DSCP = 12	AF22 DSCP = 20	AF32 DSCP = 28	AF42 DSCP = 36
High Drop Precedence	AF13 DSCP = 14	AF23 DSCP = 22	AF33 DSCP = 30	AF43 DSCP = 38

In Table 2.2, each class of traffic is allocated a specific amount of bandwidth; for example, class 1 might be allocated 10% of the available bandwidth, whilst class 4 might be allocated 50% of the available bandwidth depending on the level of importance and network resource demand of each class. Within each class, if the queue that services the class becomes full, packets are discarded according to their drop precedence. For example, packets with a DSCP value of 10, 12, or 14 are assigned to class 1. If the queue in which these packets are placed into is full, packets in the class with high drop precedence (for example, AF13 or DSCP 14) are discarded first, before packets with medium and low drop precedence.

Metering: Traffic meters measure the temporal properties of the stream of packets selected by a classifier against a traffic profile specified in an agreement specifying classifier rules, agreement, and any corresponding traffic profiles. They are responsible for metering, marking, discarding, and /or shaping rules which are applied to the traffic streams selected by the classifier. A meter passes state information to other conditioning functions to trigger a particular action for each packet which is either in- or out-of-profile (to some extent).

Shapers: Shapers delay some or all of the packets in a traffic stream in order to bring the stream into compliance with a traffic profile. A shaper usually has a finite-size buffer and packets may be discarded if there is no sufficient buffer space to hold the delayed packets.

Droppers: Droppers discard some or all of the packets in a traffic stream in order to bring the stream into compliance with a traffic profile. This process is known as "policing" the stream. Note that a dropper can be implemented as a special case of a shaper by setting the shaper buffer size to zero (or a few) packets.

2.2.4.5 Analysis of Assured Forwarding

Nguyen *et al.,* (2000) presented the assured forwarding analytical approach as an N drop-precedence threshold dropping queue with Poisson arrivals case, an extension of Bolot *et al.,* (1999) loss probability and expected delay calculations for AF mechanisms.

In an N drop-precedence threshold queue as shown in Figure 2.4, there are N flows (each flow corresponds to a level of drop precedence) arriving at the queue. A packet is discarded at its arrival when its corresponding buffer threshold has been reached or exceeded.

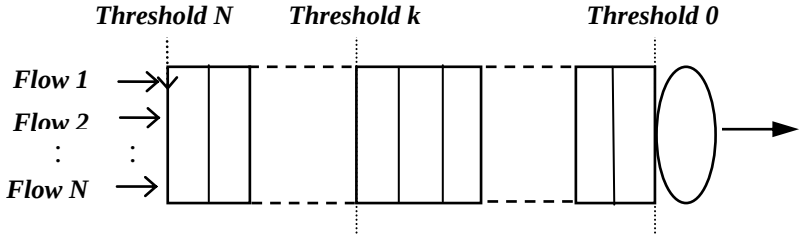


Figure 2.4:Threshold Dropping Queue of N Drop Precedence (Nguyen *et al.,* 2000)

Introducing the following terms (Nguyen *et al.,* 2000):

i. The arrival rate of the i^{th} priority flow is λ_i.
ii. The packet service times are exponentially distributed service times with mean $1/\mu$.
iii. The loads of the i^{th} priority flow and the aggregation are ρ_i and ρ, respectively
iv. The buffer threshold of the i^{th} priority flow is L_i, packets (L_o is 0)
v. At steady-state, the probability that there are n packets in the system is $\Pi(n)$
vi. $\alpha(n)$ is the acceptance probability of a packet which arrives to the queue with n other packets already in the system
vii. $\alpha_i(n)$ is the acceptance probability of an i^{th} priority packet which arrives to the queue seeing n other packets already in the system. For a threshold queue, this probability can be determined as(Nguyen, et al. 2000):

$$\alpha_k(n)= \begin{cases} 1 \text{ if } n < l_k \\ 0 \text{ if } l_k \leq n \end{cases} \quad (2.1)$$

viii. p_i is the ratio of the i[th] priority flow's load to the overall load. Hence, p_i is the ratio of λ, over the sum of all arrival rates.

It is important to notice that the lower the drop precedence of a flow, the higher the priority of the flow (for example the first priority flow has the lowest drop precedence and a buffer threshold of L_N, which is the buffer size of the queue). From the definition of $\alpha(n)$ and $\alpha_i(n)$ (Nguyen *et al.*, 2000):

$$\alpha(n) = \sum_{i=1}^{N} p_i \alpha_i (n) \quad (2.2)$$

$$\alpha(n) = \begin{cases} P_1 + \ldots + P_N \; if & n < L_1 \\ P_2 + \ldots + P_N \quad if & L_1 \leq n < L_2 \\ \quad \ldots\ldots \quad \ldots\ldots & \quad \ldots\ldots \\ P_k + \ldots + P_N \quad if & L_{K-1} \leq n < L_k \\ \quad \ldots\ldots \quad \ldots\ldots & \quad \ldots\ldots \\ P_N \quad if & L_{N-1} \leq n < L_N \\ 0 \quad if & L_N = n \end{cases} \quad (2.3)$$

It can be seen that this threshold queue can be modelled as a birth-death process. Packets receive at the queue for processing can be referred to as birth process and the packet served and transmitted away from the queue is referred to as death process. For a state n, the birth rate is p*p*α(n) while the death rate is μ. The steady-state distribution of buffer content is (Nguyen *et al.*, 2000):

$$\Pi(n) = \Pi(0)\rho^n \prod_{i=0}^{n-1} \alpha(i) \quad (2.4)$$

With the probability that the buffer is empty, Π(0) is given as:

$$\Pi(0) = \left[\sum_{n=0}^{L_N} \rho^n \prod_{i=0}^{n-1} \alpha(i)\right]^{-1} \quad (2.5)$$

$$\Pi(0) = \left[1 + \sum_{i=1}^{n} [\prod_{j=1}^{i-1} (\rho_j + \cdots + \rho_n)^{L_J - L_{J-I}} \sum_{K=1}^{L_J - L_{J-I}} (\rho_j + \cdots + \rho_n)^K]\right]^{-1} \quad (2.6)$$

From (3.3) and (3.4), Π(n) becomes:

$$\Pi(n) = \Pi(0) \prod_{j=1}^{k-1} \left[\sum_{i=j}^{N} p_i\right]^{L_j - L_{j-1}} \left[\sum_{i=k}^{N} p_i\right]^{n - L_{k-1}} \text{ if } L_{K-1} < n \leq L_k \quad (2.7)$$

The loss probability of the i[th] priority flow is determined as (Nguyen *et al.*, 2000):

$$Loss_i = 1 - \sum_{n=0}^{L_N} \Pi(n) \alpha i(n) \quad (2.8)$$

Clearly, when a packet arrives at the queue which already has n packets, it has a delay of n packets service times plus its own service time. Therefore, the mean delay of the i[th] priority flow (excluding rejected packets) is (Nguyen *et al.*, 2000):

$$Delay_i = \frac{1}{\mu} \frac{\sum_{n=0}^{L_N - 1} (n+1)\Pi(n)}{\sum_{n=0}^{L_N - 1} \Pi(n)} \quad (2.9)$$

Resolving the following $\sum_{n=0}^{L_N - 1} (n+1)\Pi(n)$ and $\sum_{n=0}^{L_N - 1} \Pi(n)$ in term of ρ (loads priority flow)

$$Delay_i = \frac{1}{\mu} \frac{1 + \sum_{k=1}^{i} \left[\prod_{j=0}^{k-1} (\rho_j + \cdots + \rho_n)^{L_J - L_{J-I}} \sum_{K=1}^{L_J - L_{J-I}} (\rho_j + \cdots + \rho_n)^K\right]}{1 + \sum_{i=1}^{n} [\prod_{j=1}^{i-1} (\rho_j + \cdots + \rho_n)^{L_J - L_{J-I}} \sum_{K=1}^{L_J - L_{J-I}} (\rho_j + \cdots + \rho_n)^K]} \quad (2.10)$$

From equation (2.9) and (2.10), the mean delay of the i[th] priority flow is affected by the packet service time 1/μ and delay of n packets service times at the queue which already has n packets.

2.2.4.6 Limitations of Differentiated Services Architecture

The differentiated services model as define in RFC 2474 has the following limitations

i. Packet can be processed and eventually dropped during the last process of scheduling and queuing if the threshold of the queue is exceeded, which result to added delay for incoming packet due to the processing time of packets that are eventually dropped (Headquarters 2003).
ii. Differentiated services model do not cater for the changing demand for network resources by various network traffic

To address these limitations of the differentiated services model, an admission controller is proposed to drop packet early if accepting the packet will eventually cause threshold of queues to be exceeded during the process of queuing and scheduling. The admission decision is based on

the comparison of the available and the requested resources to ensure that only packet that will be accepted by the scheduling and queuing systems will be accommodated and process by the network. However, only high priority packet achieves highest possible loss protection over others.

2.3 REVIEW OF SIMILAR RESEACH WORKS

The review of research works conducted by other researchers in the areas related to this proposed work provides the background knowledge of establishing the basis for the approach taken to resolve delay and delay variance of CAN network. Considerable work has been done by many researchers in developing QoS architectures, mechanisms, and queuing disciplines to improve transmission of interactive and multimedia applications on IP networks. The key ones are critically reviewed as presented hereunder:

In their work to improve measurement based classification of traffic for QoS guarantees to traffic from different applications, **Roughan *et al.*, (2004)** developed a traffic classification scheme to give priority to delay sensitive traffic. The develop scheme classify traffic based on the way in which an application is used rather than the measurement based automated CoS mapping. The developed traffic classification scheme was able to classify a new application, for which they did not have any specific training data, except from similar applications in the same class. However, added complexity in the traffic classification scheme which will require more network resources and the inability to significantly address the traffic delay need of interactive and multimedia application is the drawback of the work.

Bhakta *et al.*, (2011) developed differentiated service architecture for QoS support and routing for delay-sensitive and best-effort services in IEEE 802.16 mesh network. They developed new cross-layer routing metric, namely, Expected Scheduler Delay (ESD) using efficient distributed

scheme to calculate ESD and routed the packets using source routing mechanism. This scheme was capable of differentiating between delay sensitive and best-effort traffic and routed packets accordingly. The work was able to establish that ESD metric was better compared to hop count metric in terms of delay for the service model that contained both delay sensitive and best effort service. The issue with this work was added complexity in routers designed for the routers to be able to calculate ESD and routed the packets using source routing mechanism and that the level of improvement of the architecture depended on how the expected scheduler delay performed.

Olawoyin *et al.*, (2011) presented queue management and scheduling in network performance, by analysing the performance bottleneck of different queuing policies. They proposed the use of Active Queue Management (AQM) to replace drop-tail queue management in order to improve network performance in terms of delay, link utilization, as well as packet loss rate and system fairness. The work showed that AQM improved network performance by reducing packet loss rate. Their work indicated a major drawback of added complexity in queuing management and scheduling mechanism for it's to be able to efficiently manage and schedules traffic to their respective queues.

Baswaraj and Tomar, (2011) worked on modelling packet switched network over TCP/IP to achieve reduction of end to end delay and packet loss rate of packet. The works suggested modified routing to reduce congestion by developing network architecture and an algorithm called Core-Stateless Fair Queuing (CSFQ). The developed architecture significantly reduced the implementation complexity of Fair Queuing (FQ) algorithm and still achieved approximately fair allocations of congestion control. The developed model reduced the chances of tail drop by selectively dropping packets when the output interface began to show signs of congestion. By dropping some packets early, rather than waiting until the buffer was full the model avoided

dropping large numbers of packets at once. Their challenge was the inability to address the network need of delay sensitive data.

In their work to improve transport-layer performance in order to improve the transmission of interactive traffic across a network, **Cai *et al.*, (2011)** developed packet pacing as an alternative that changed traffic characteristics favourably by adding intentional delay in packet transmissions. They presented a Queue Length Based Pacing (QLBP) algorithm that paced network traffic using a single queue, which could be implemented with small computational and memory overhead. Results showed that, pacing improved transport layer performance, providing a trade-off where small amounts of additional delay could significantly increase connection bandwidth. The problem of their research was an increase of the overall transmission delay which was not good for real-time and other multimedia traffic.

Zheng *et al.*, (2012) In their work to address the issue of limited available resources and degree of traffic aggregation at the radio access level of a IEEE 802.11 WLAN, which render the differentiated services principles less effective and affect the transmission of delay sensitive traffic, implemented a hybrid QoS architecture framework. The developed hybrid QoS architecture ensured that session-based applications were admitted according to the traffic profile they require and Fair Intelligent Congestion Control (FICC) algorithm was applied to provide fairness among traffic aggregates and control congestion at the bottleneck interface between the wireless link and the network core via mechanisms of packet scheduling, buffer management, feedback, and adjustments. Added complexity in buffer management and packet scheduler so as to be able to provide fairness among traffic aggregates and control congestion at the bottleneck interface are the disadvantages of this work.

In their work of comparing traffic conditioners to manage throughput, packet loss and delay of a network, **Kaur *et al.*, (2012)** designed ways of choosing the best traffic conditioner to apply from source to destination pair so that QoS could be guaranteed. Traffic classification and traffic conditioning were important functions of differentiated services also known as admission control. There was no convincing evidence to suggest that the choice of traffic conditioner affected a source's achieved rate, which was the major limitation of this research

Sonawane and Varalaxmi, (2013) developed an application that would improve performance of the network by controlling packet loss using techniques to control network congestion. They implemented the Stable Token-Limited Congestion Control (STLCC) mechanism for controlling inter-domain congestion and improved network performance. The results revealed that the application was able to control network congestion by controlling packet loss, thus improving the performance of the network. The work did not consider packet delay which was also a key network performance indicator and this was a setback in this study.

Mukherjee and Khanna, (2013), in their work of developing a scheduling discipline for resources allocation to improve the QoS for any network carrying various types of traffic, evaluated the performance of First-In-First-Out (FIFO), Priority Queuing (PQ), and Weighted Fair Queuing (WFQ) scheduling discipline. The work was able to establish that WFQ when merged with DSCP was a better method of queuing. This work can be improved by addressing the issue of packet end to end delay, which was the major limitation of their work.

In his work based on modelling and analysis of the performance of networks in finite-buffer regime, **Torabkhani, (2014)** presented the effects of finite buffer sizes on the throughput, packet losses, and packet delay in different networks. They used the established effect of finite buffer sizes to analytically characterize network throughput, packet losses, and packet delay to estimate

and model the performance measures of a network. The work capture the vital trends of the network, yielded better estimates of the throughput, packet losses and delay performance measures. The work also established that finite-buffers created dependencies which could not be captured directly using the classical queuing theoretical models. However, large buffers had an adverse effect on the latency, which was the regret in this research.

Dantas *et al.*, (2014) designed a differentiated service methodology that implemented constrained resource allocation according to demand's priority level for wavelength division multiplexing networks. The differentiated services mechanism higher priority connections were guaranteed a larger amount of resources and still, lower priority demands were guaranteed a minimum level of service. The problem of their research was an increase of the network control complexity in terms of network scheduling and queuing mechanism.

Liu *et al.*, (2014) presented an approach of traffic engineering with Forward Fault Correction (FFC) in a network to promote the transmission of multimedia traffic. By developing FFC using sorting networks, a proactive approach for handling network faults, such as link failures and high switch configuration delays were implemented. The work showed that with negligible loss in overall network throughput, FFC could reduce data loss by a factor of 7–130 in well-provisioned networks and reduce the loss of high-priority traffic in well utilized networks. The limitation of their work was evident in the increase design complexity of routers, which need to infuse FFC mechanism in the router design.

Wan, (2015), in his work to develop a multiple video streaming priority based enhanced schemes using standard differentiated services architecture, evaluate the performance of standard differentiated services architecture and two developed priority based enhanced schemes namely,

Inner-Priority (IP) based scheme and Cross-Class Priority (CCP) based scheme. The work was able to establish that IP based scheme outperformed CCP based scheme and standard differentiated services in reducing packet loss rate and bandwidth utilization. However, the work did not consider the effect of packet end to end delay which is the restriction of their endeavour. Packet delay affects QoS of streaming packet.

2.3.1 Summary of Literature Review

Based on all literatures reviewed, it is ascertain that conventional packet network cannot guarantee QoS for the transmission of delay sensitive traffic, there is need to develop QoS architecture to guarantee good QoS for interactive applications on networks. The review has also given a lead way of the work by other researchers to resolve the issue related to transmission of delay sensitive traffic across a network, problems encountered, and their solutions to different related issues on QoS. From the knowledge gained, the approach of enhancing the differentiated services architecture will guarantee good QoS for interactive applications on CAN.

CHAPTER THREE
MATERIALS AND METHODS

3.1 Introduction

This chapter focuses on development of an enhanced differentiated services model solution. Differentiated services model solution is highlighted and addressed in the development of the enhanced differentiated services architecture for improved performance. Performance analysis through simulation of best-effort and developed differentiated services model solutions are presented along with their simulation setting and the data flow diagram. Finally application and validation of the Enhanced differentiated service model was presented.

3.2 Implementation of Differentiated Services Model Solution

This section describes how to implement differentiated services model as defined in RFC 2474. Differentiated services QoS allows for the selection of specific network traffic such as delay sensitive traffic, prioritizing it according to its relative importance and giving it preference over others.

Developing differentiated services model involves expanding on the basic differentiated services model shown in Figure 3.1

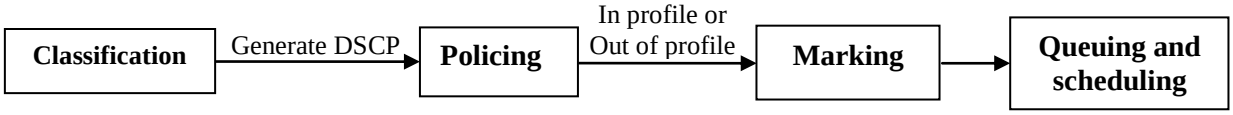


Figure 3.1: Basic Differentiated Services Model (RFC 2474)

Classification: Packet classification is implemented by configuring and defining the DSCP for each application using the traffic descriptor such as Packet source interface, packet destination Media Access Control, packet Protocol type of each traffic (for this research packet destination is used). Using packet classification, network traffic is partition into multiple priority levels or CoS.

Policing: Packet monitoring and policing are implemented by defining and specifying policy details (Bandwidth, Peak information rate etc) for each DSCP, using the IP QoS parameters

attribute of the router. Monitoring involves, comparing DSCP to the configured policies and determines if the packet is in profile or out of profile.

Queuing and Scheduling: To determine into which of the queues to place the packet, based on the CoS, mechanisms in the routers involve schedulers are used. For this work WFQ and RED buffer management algorithms are used.

To address these limitations of the differentiated services model, an admission controller is proposed to drop packet early if accepting the packet will eventually cause threshold of queues to be exceeded during the process of queuing and scheduling. The admission decision is based on the comparison of the available and the requested resources to ensure that only packet that will be accepted by the scheduling and queuing systems will be accommodated and process by the network. However, only high priority packet achieves highest possible loss protection over others.

3.2.1 Implementation of Enhance Differentiated Services

This section describes how to implement the enhanced differentiated services model. The logical view of the architecture is shown in Figure 3.2

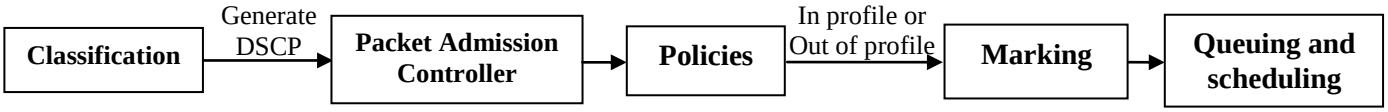


Figure 3.2: Proposed Enhance Differentiated Services Model

The improvement of the proposed enhances differentiated services Model over the differentiated services Model, is the inclusion of admission control. The admission control is to ensure that only packet that can be accommodated and processed by the network is accepted after the packet is classified, thereby avoiding the situation in which packets are processed and eventually drop during the last process (scheduling and queuing). Also packet admission control regulates and

prioritizes the acceptance of packet into the differentiated services domain which caters for the changing demand of the network resources by various class of traffic.

3.3 Simulation of Best-Effort and Developed Differentiated Services Model

Each of the differentiated services and best-effort solutions are modelled using the OPNET simulator. The methodology adopted in this modelling and simulation is presented below:

Step1. Create a project
Step2. Create a baseline scenario
Step3. Develop architecture using topology diagram of ABU network shown in Figure 1.1
Step4. Import or create traffic
Step5. Choose statistics to be collected
Step6. Run the simulation
Step7. View the results
Step8. Duplicate the scenario
Step9. Configure other architecture
Step10. Re-run the simulation
Step11. Compare the obtained results

Steps for settings up simulation for each model solution include:

File → New → Project →Ok
Scenario name = 'enter scenario name' →Ok
Initial Topology = create empty scenario → Next
Network Scale = campus → Next
Select Network Technology = do not select any →Next
Set Preview → Finish
Setup Network
Run Simulation =DES → Configure/Run Discrete Event Simulation
View Result = DES →View Result →Global Statistic →Voice →Packet end – end delay

3.3.1 Best-Effort Network Service Model Simulation

The best-effort services model network simulated scenario is setup to determine how the network handles large internet traffic without any special QoS implemented.

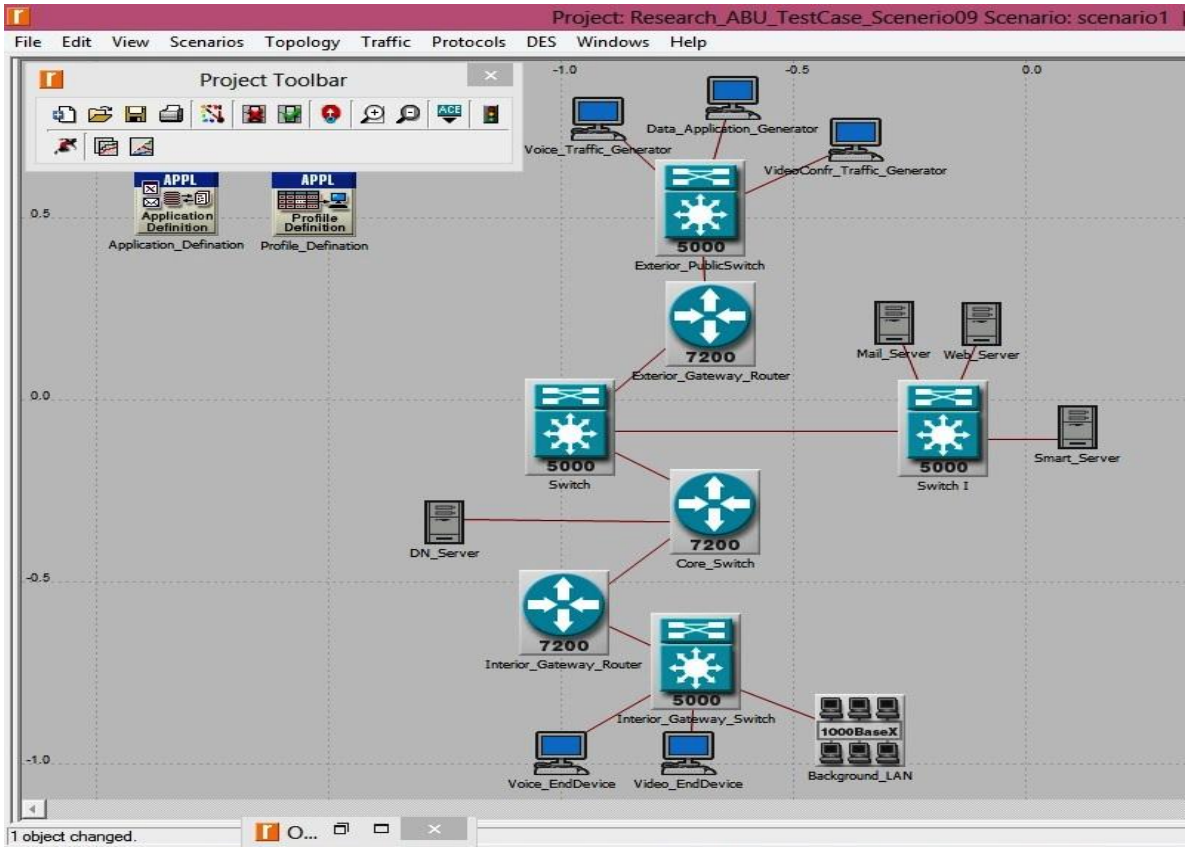


Figure 3.3: OPNET Simulation of Best-Effort Services Model Internet Network

The best-effort services model was setup based on topology diagram of ABU network shown in figure 1.1. Network Equipment where implemented on the OPNET simulator as it is on the topology diagram of ABU network, with the exception of the mikrotik exterior router where Cisco 7204 router was adopted for the simulation. Other equipment on the network include Cisco 6500 router used as core switch and Cisco 2911 router as internet interior gateway, Figure 3.3 shows the simulated scenario of the best-effort services model.

Application definition and profile definition tools were used on the OPNET simulator to set and define applications and profile of users on the network. The applications defined includes; Http Ftp, Database, email, files sharing, video conferencing and voice over IP. Three users profile were define and configure, which include Group 1 profile which run applications such as Http,

ftp, email and file sharing, Group 2 profile run video conferencing, file sharing and emails while Group 3 profile run voice call, Http, file sharing and email applications.

3.3.2 Differentiated Services Models Simulation

Differentiated services model was setup using the simulation setting of the OPNET simulator.

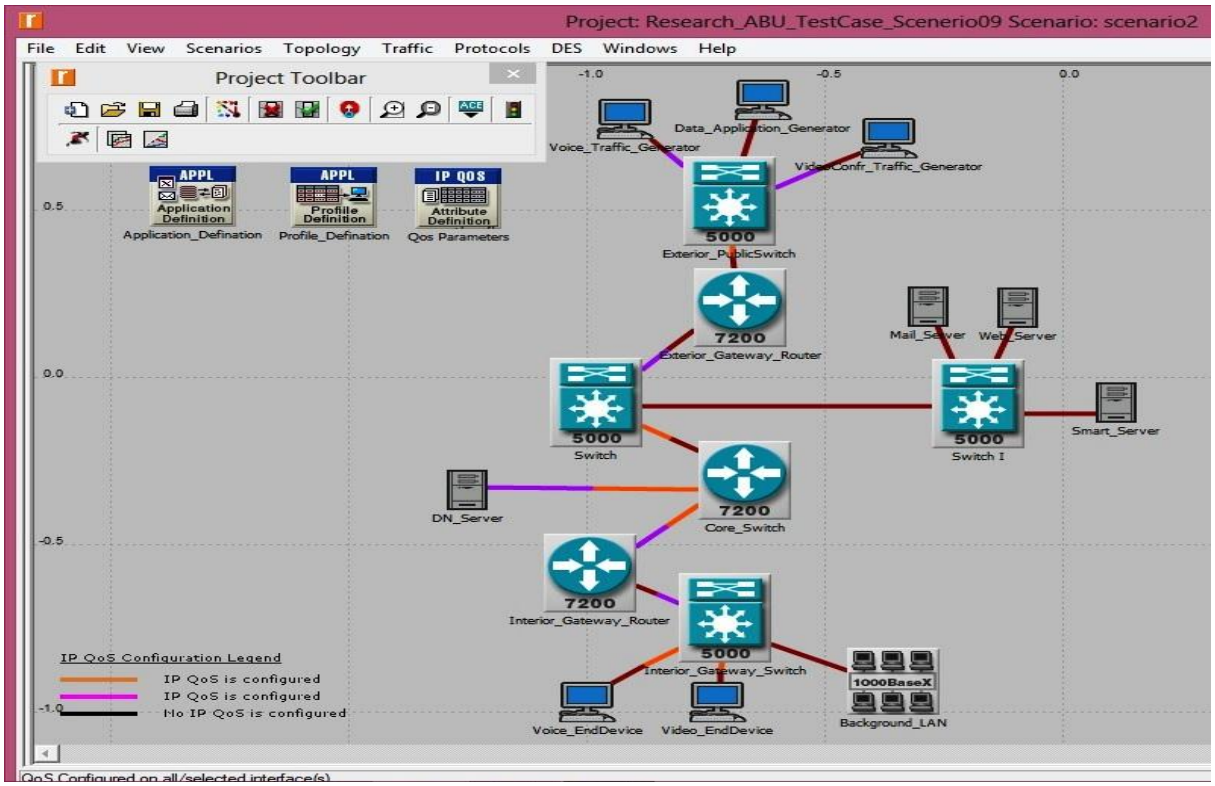


Figure 3.4: OPNET Simulation of Differentiated Services model

Applications and users profile definition of best-effort services model simulated scenario were maintained, devices and links where configured and enable with differentiate services QoS. Figure 3.4 shows the simulated scenario of differentiated services model. To implement the differentiated services scheme in routers and other devices we modify existing OPNET model of routers, because most components needed for our differentiated services-enabled router exist in the Cisco 7204 and other router models used for this work.

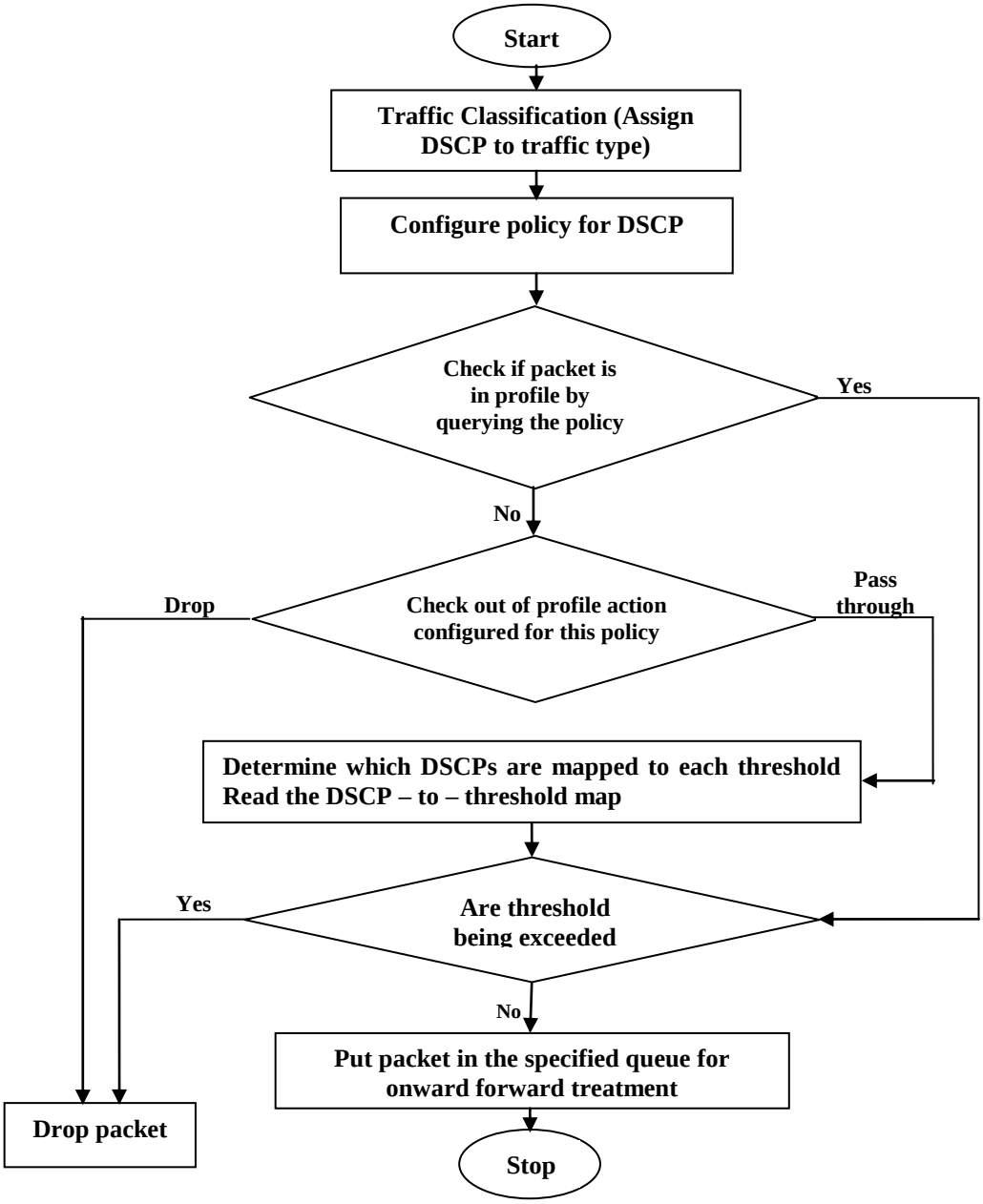


Figure 3.5: Flow Chart of OPNET Implemented Differentiated Service Model

To implement the differentiated services scheme on the routers, the IP QoS process model was modified, enable and configured with differentiated services so as to handle and give priority to some classes of traffic. The flow chart for the implemented differentiated services model is shown in Figure 3.5.

Packet Classification: The packet classification is implemented by configuring and defining the DSCP for each application using the application definition tool of each traffic generator on the OPNET simulator as shown in Figure 3.6.

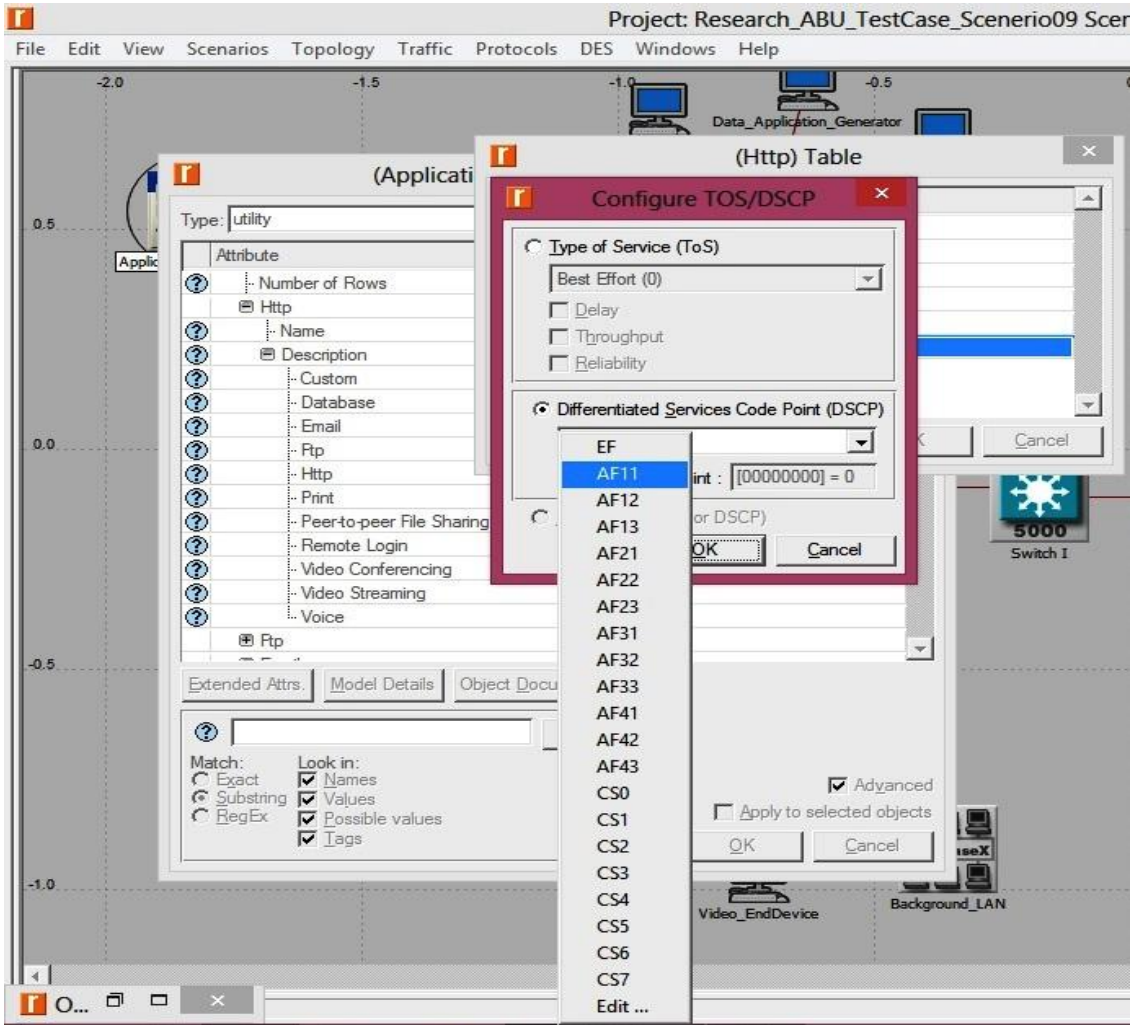


Figure 3.6: OPNET Simulator Configuration of Packet Classifications

Http was classify with DSCP of AF33, Ftp with AF32, Database with AF31, email with AF13, files sharing with AF12, video conferencing with EF and voice over IP with AF43

Packet monitoring and Policing: After a packet is being classified, is monitored and policed according to the class it belongs, it is schedule and queued for onward forwarding. Packet

monitoring and policing are implemented by defining and specifying policy details (Bandwidth, Peak information rate etc) for each DSCP, using the IP QoS parameters attribute of the router on the OPNET simulator.

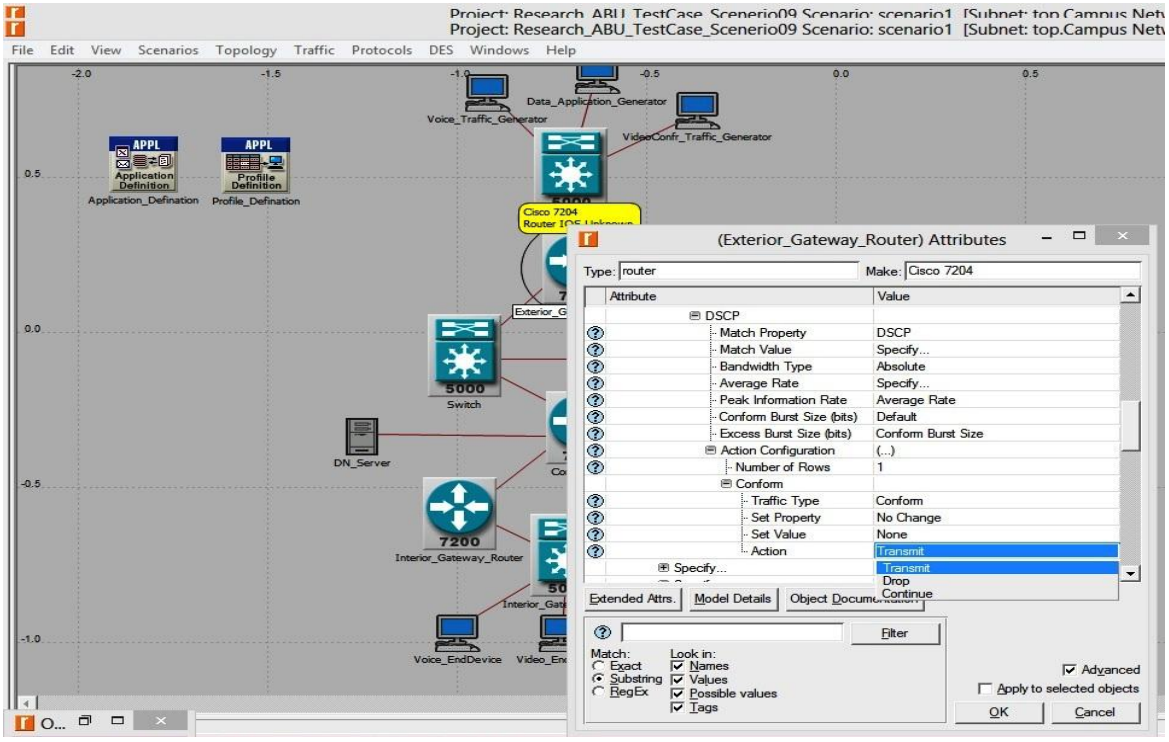


Figure 3.7: OPNET Simulator Configuration of Packets Monitoring and Policing

The monitoring which depict decision box 1 and box 2 on the flow chart was implemented on the exterior router by defining under the IP QoS parameters attribute, action to be taken for conform and non-conform packet. How to setup policy is shown in Figure 3.7.

Packet Routing and Forwarding: After classification and conformance check, the packet enters the regular IP forwarding process, which is implemented at Core Switch. Packets are forward based on the routing algorithm used, for our network it is the Open Shortest Path First (OSPF).

Packet Scheduling Mechanisms: The QoS mechanisms in the routers involve schedulers, for this work WFQ and RED buffer management algorithms, were configured using the QoS attribute setting of the interior gateway router to schedule each traffic class.

3.3.3 Enhanced Differentiated Services Network Models Simulation

The Enhanced differentiated services model was setup using the simulation setting of the OPNET simulator. Application and users profile definition of best-effort services model simulated scenario were maintained.

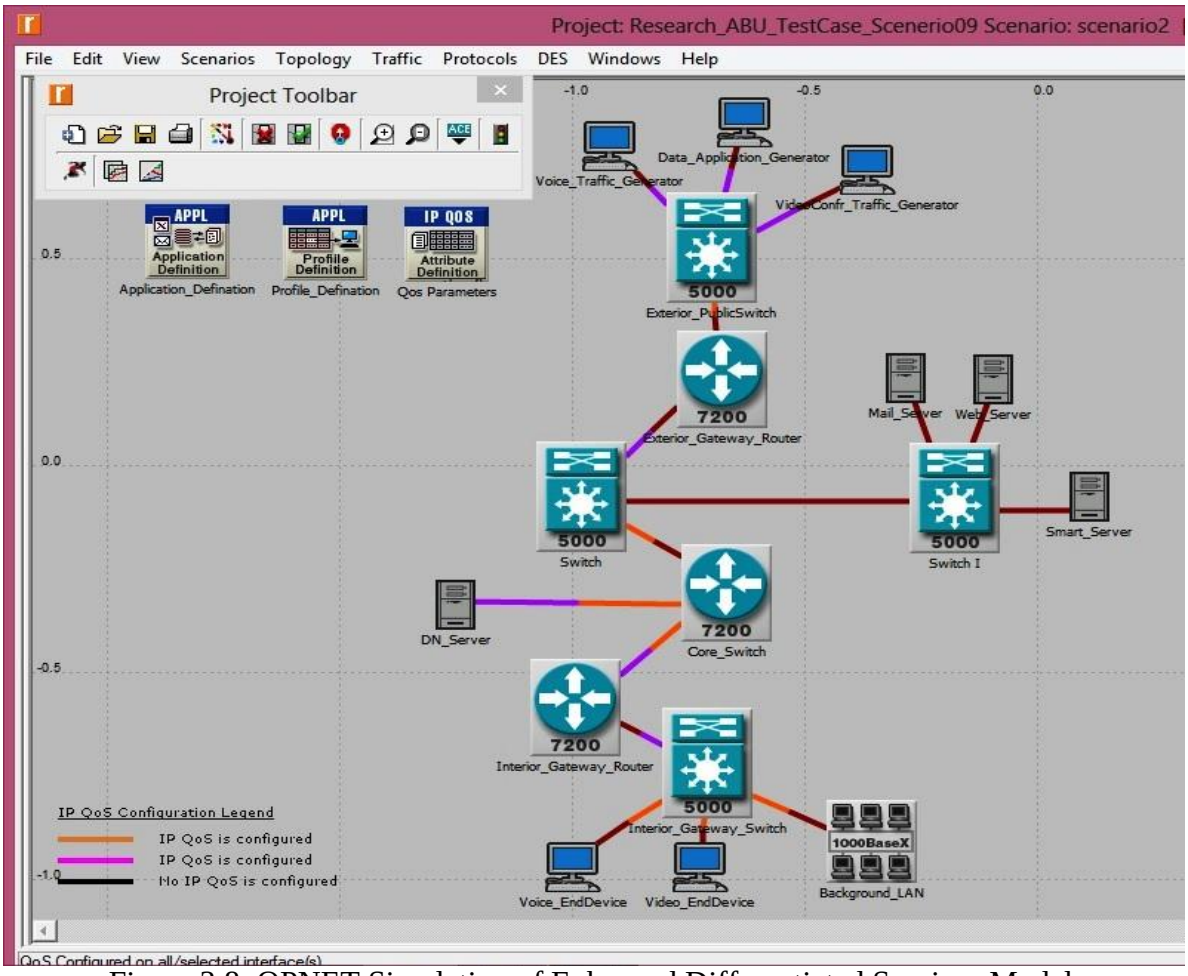


Figure 3.8: OPNET Simulation of Enhanced Differentiated Services Model

Differentiated services QoS was configure and enable as was done setting-up for differentiated services model, with the addition of admission control to ensure that only packet that can be accommodated and process by the network is accepted into the network. Figure 3.8 shows the simulated scenario of the Enhanced differentiated services model.

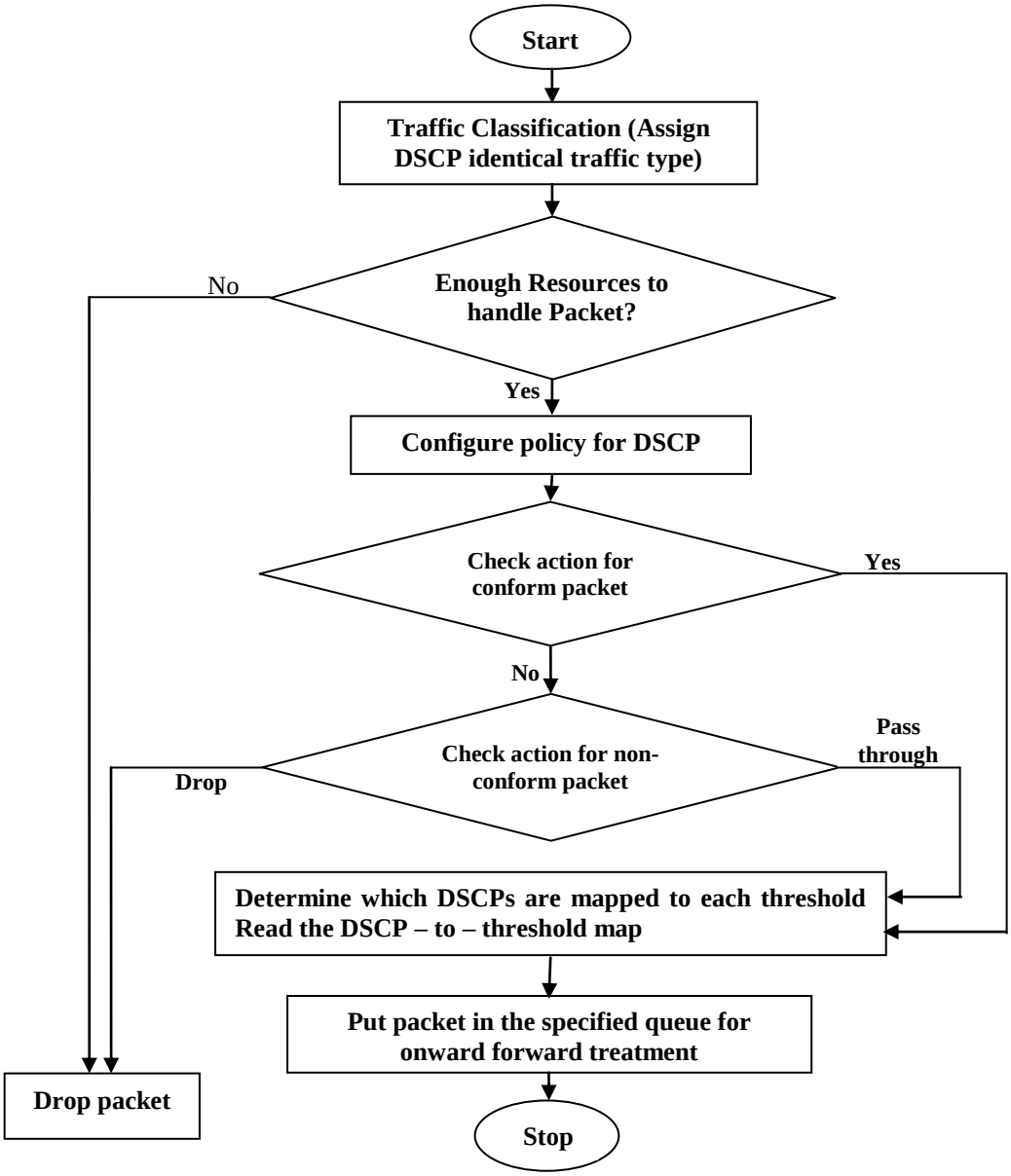


Figure 3.9: Flow Chart OPNET Implementation of Enhanced Differentiated

The flow chart of OPNET implementation of enhanced differentiated services model is shown in Figure 3.9.

Implementation of Admission Control: The admission control was implemented by configuring queuing fill level range and it drop probability range of QoS mechanisms in the traffic generators connected to the exterior Gateway router. Only traffic that can be handled by the router is admitted, and those packets such as video conferencing that are delay sensitive are given priority over other during the dropped process.

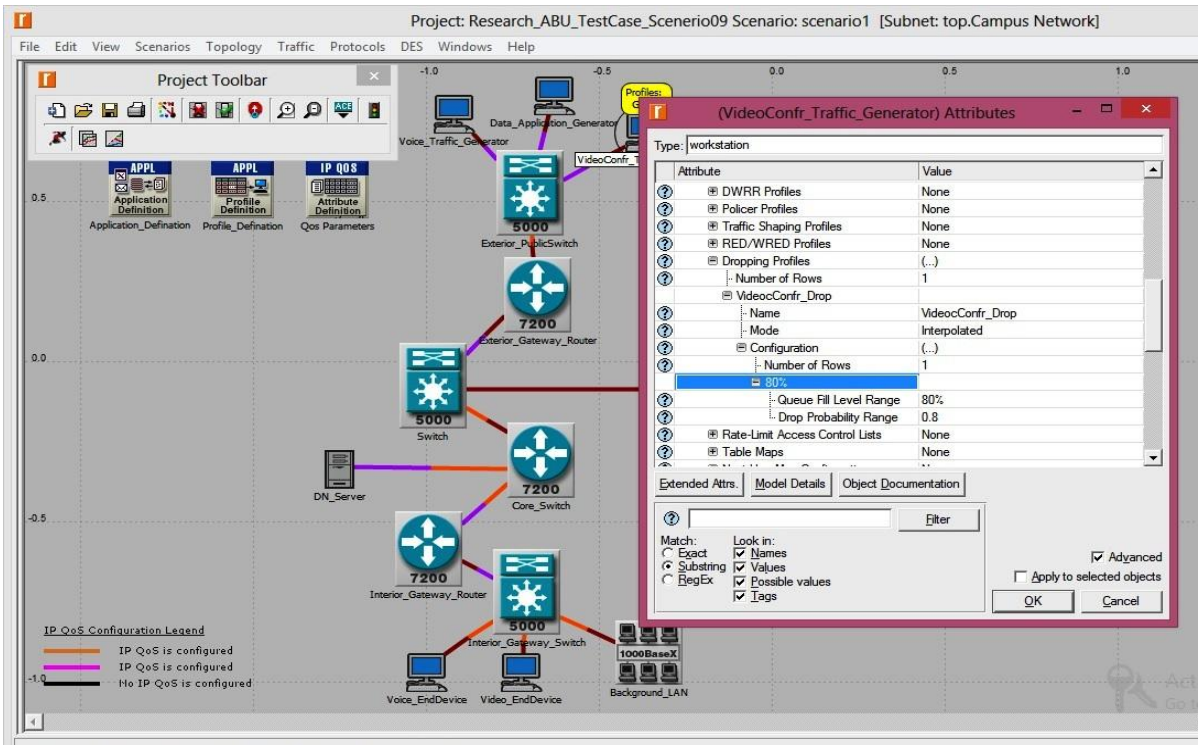


Figure 3.10: OPNET Simulator Setting-up of Admission Control

This was achieved as shown in Figure 3.10, by setting the queue filled level and it drop probability range such that non delay sensitive packet (email, file sharing etc) are dropped before delay sensitive packet (video-conferencing and voice streaming) to ensure QoS guarantee for delay sensitive packet and also because non delay sensitive packet can be retransmitted if a packet is drop before its destination. For this work, queue fill level and it drop probability range for data applications are (25%-0.5, 50%-0.6 and 75%-0.8), videoconferencing is (25%-0.1, 50%-0.1 and 75%-0.1) and for voice is (25%-0.4, 50%-0.3 and 75%-0.1). Queue fill level indicated the ration of packers in a queue against the size of queue (the total packet a queue can take at a time). While drop probability implies drop preference of packets in case the queue cannot accommodate the total packet in the queue. An application with high drop probability is dropped before an application with low drop probability.

3.4 Application and Validation of Enhanced Differentiated Services Model

This section presents the validation of the developed enhanced differentiated service model with existing differentiated service model and its application on live routers. The area of validation considered here is the improvements in reduction of delay by the developed enhanced differentiated service model on the test-bed network develop for the validation. To demonstrate this, each of the differentiated services and best-effort services solutions modelled using the OPNET simulator were adopted and configured on live routers and switches. Figure 3.11 shows the topology of the developed test bed adopted for the validation. Figure 3.12 presents the picture of the test-bed used for the validation in Mamman Kontagora Computer Laboratory (MKCL) of the Department of Electrical and Computer Engineering, Ahmadu Bello University, Zaria.

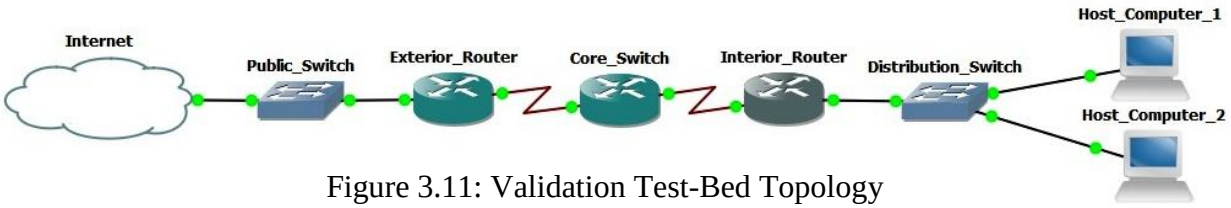
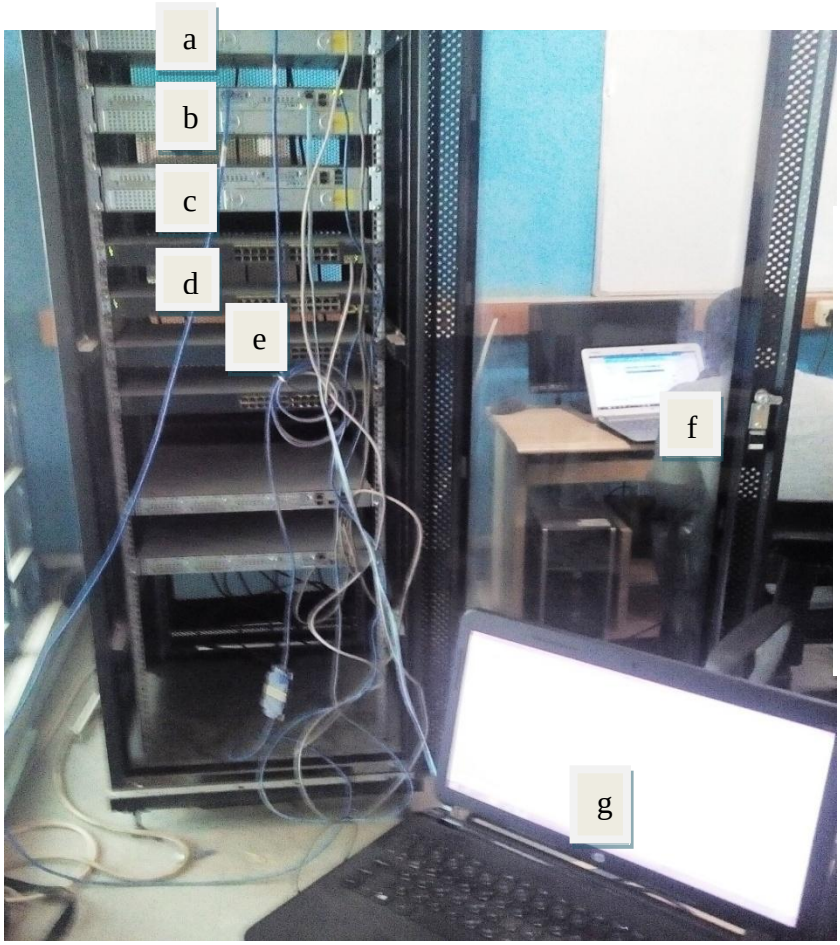


Figure 3.11: Validation Test-Bed Topology

Cisco 2911 routers and Cisco catalyst 2960 switches were used for the setup of the validation test-bed. The Internet traffic coming into the MKCL was used as input traffic for the validation. Two Cisco catalyst 2960 switches were configured and used one as policy switch connecting the exterior router with the core switch and the other configured as distribution switch. The switch situated at the laboratory was adapted as public switch connecting the test-bed network through the exterior router with Internet traffic. Three Cisco 2911 routers were configured and used as exterior, core switch, and interior router.



List of Devices

a - Exterior Router (Cisco 2911 Router)
b - Core Switch (Cisco 2911 Router)
c - Interior Router (Cisco 2911 Router)
d - Policy Switch (Catalyst 2960 switch)
e - Distribution Switch (2960 switch)
f - End Device (HP Laptop Computer)
g - End Device (HP Laptop Computer)

Figure 3.12: Validation Setup at MKCL

Two computers were used as end devices one running data and multimedia streaming (live streaming of Channels New and file download), the other computer was running video streaming (Streaming Skype). Best-effort, differentiated services, and enhanced differentiated service model were separately configured on the test-bed setup and at each instant the time of processing a packet and the processed time of each packet across the setup are determined using Wireshark network analyser. This was done to determine the packet delay, of the three QoS models.

3.4.1 Best-Effort Service Model Validation

Setting up best-effort services model was achieved by configuring the validation setup without QoS, configuration on routers of best-effort services model on the test-bed setup is illustrated on Appendix 1

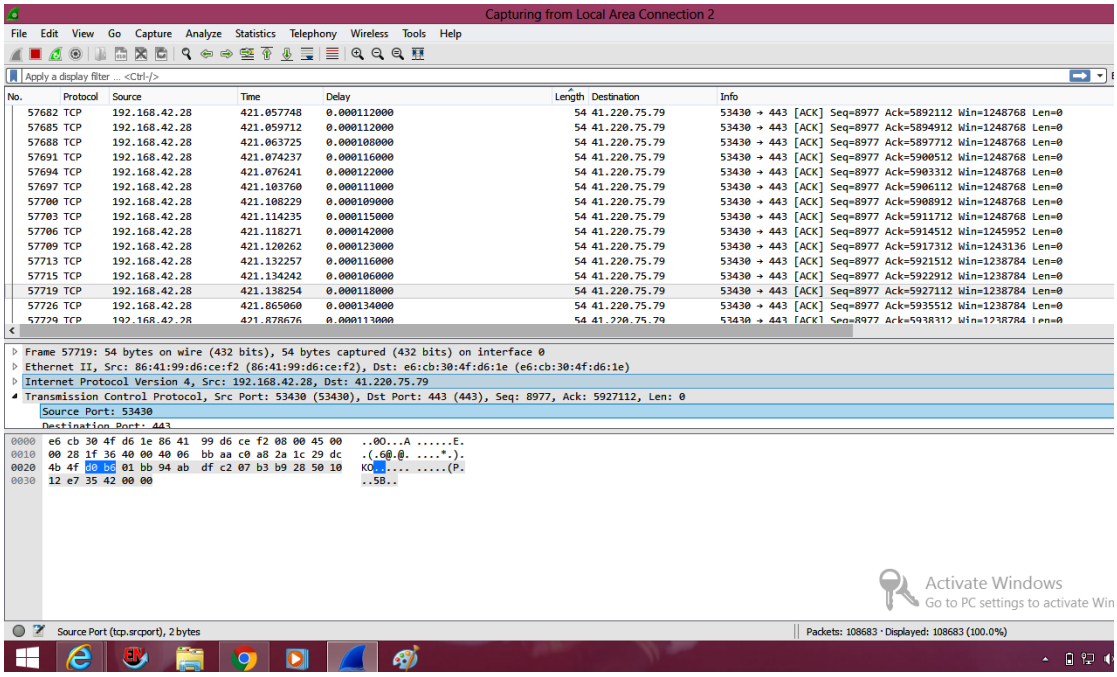


Figure 3.13: Screenshot of Best-Effort Delay Obtained using Wireshark

Figure 3.13 shows the screenshot of delay, time of processing packet and the processed time of packet etc across the test-bed. The first column shows the packet number which help in identifying packets analysed by the Wireshark network analyser. The second, third, sixth and seventh column indicate the protocol, the source, the length and destination of the packets respectively. The fourth column register the time a packet is processed, which is a measure of the total time it takes to process a packet from source to destination. The fifth column indicates delay, which is the processing time of the network (the actual time it takes the network to process packet but not including the time it takes the packet to wait for network resources)

3.4.2 Differentiated Services Model Validation

Validation of the differentiated service network model was achieved by configuring the validation setup with differentiated service. The exterior router was configured to classify and policy traffic based on source information of each application, the core switch was configured to mark traffic, while the interior router was configured to schedule the traffic. The configuration

on routers of differentiated service network architecture on the test-bed setup is illustrated in Appendix II.

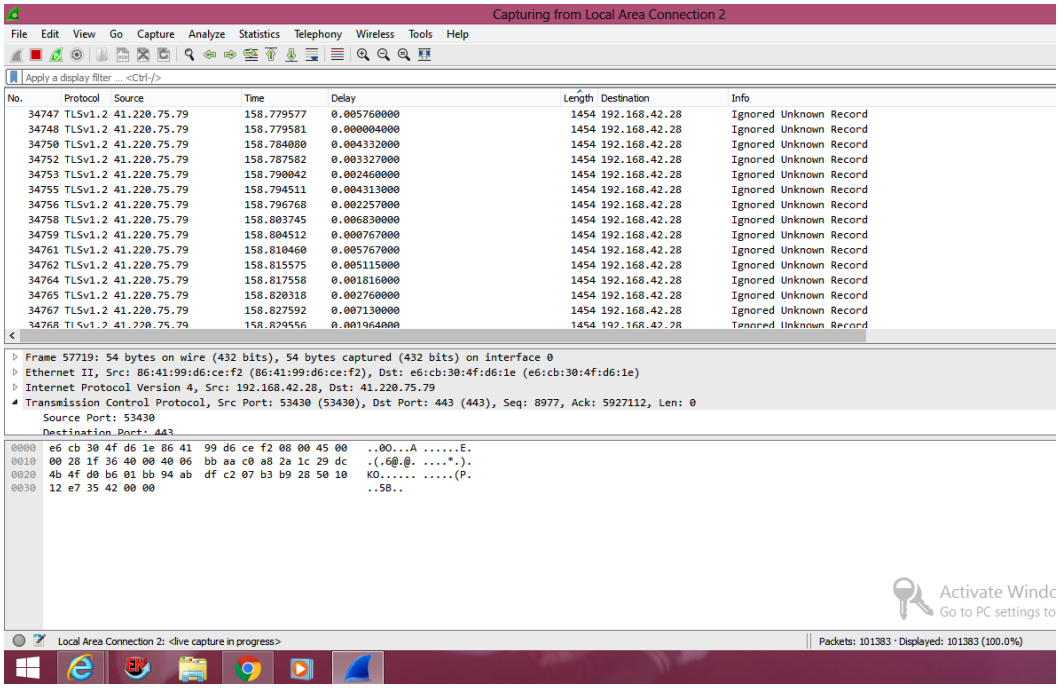


Figure 3.14: Screenshot of Differentiated Services Data Obtained using Wireshark

Figure 3.14 shows the screenshot of delay, time of processing a packet and the processed time of packet obtained from the test bed after configuring the devices with differentiated service model.

3.4.3 Enhanced Differentiated Services Model Validation

The validation of enhanced differentiated service network model was achieved by configuring differentiated service architecture and then setting up an admission control on the exterior router. The admission control was to ensure that only packet that can be accommodated and processed by the network was accepted. The exterior router was configured with admission controller, to classify, and to policy traffic based on source information of each application. The core switch was configured to mark the traffic. The interior router was configured to schedule the traffic. The steps taken to configure admission control are detailed in Table 3.1.

Table 3.1: Configuration Detail of Service Group Admission Control on a Router

Steps	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode
Step 2	configure terminal	Enters global configuration mode
Step 3	cable application-type *n* include service-class service-class-name	For service class parameters, this command variation applies a service class name to the service flows, and applies corresponding QoS parameters.
Step 4	cable application-type n name bucket-name	Assigns an alpha-numeric name for the specified bucket
Step 5	admission-control application-type n ds-bandwidth pct	Enables SGAC checking for the specified application-type
Step 6	Ctrl-Z	Returns to Privileged EXEC mode.

Configuration on routers of enhanced differentiated service network architecture on the test-bet setup is illustrated in Appendix III.

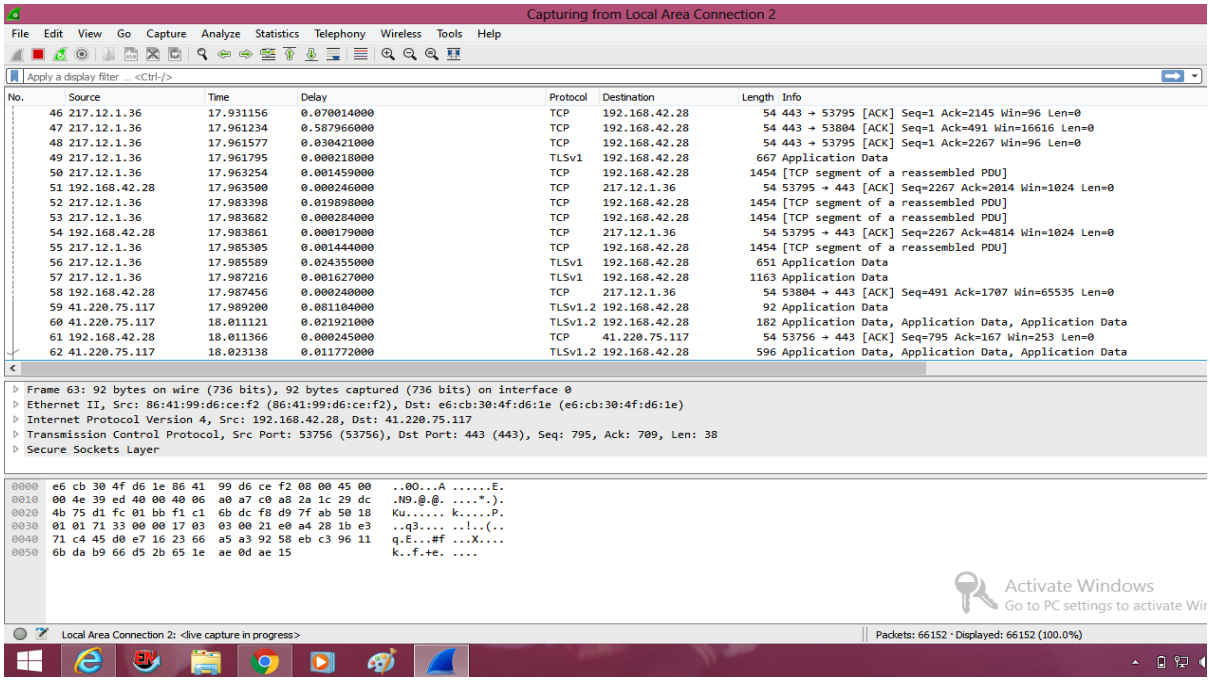


Figure 3.15: Screenshot of Enhance Differentiated Services Delay Obtained using Wireshark

Figure 3.15 shows the screenshot of delay, time of processing a packet and the processed time of packet obtained from the test bed setup after configuring the devices with enhanced differentiated service model.

CHAPTER FOUR
RESULTS AND DISCUSSIONS

4.1 Introduction

The network service models were implemented and simulated using OPNET simulator in order to establish how viable the work is. This chapter presents the analysis of the results obtain of simulation of the three services model and the results obtain using the develop test bed for application and validation of the three services model.

4.2 Analysis of Results and Data Obtained using OPNET Simulator

OPNET simulator is capable of generating plots from the simulation performed, and this is achieved using the following commands:

DES ⟶ Results ⟶ View Results (Enter)

The plots of end to end delay obtained for best-effort, differentiated and enhanced differentiated services model are shown in Figure 4.1 to Figure 4.5. The horizontal (X) axis indicate the simulation time in seconds while the vertical (Y) axis indicates the packet delay time in minutes.

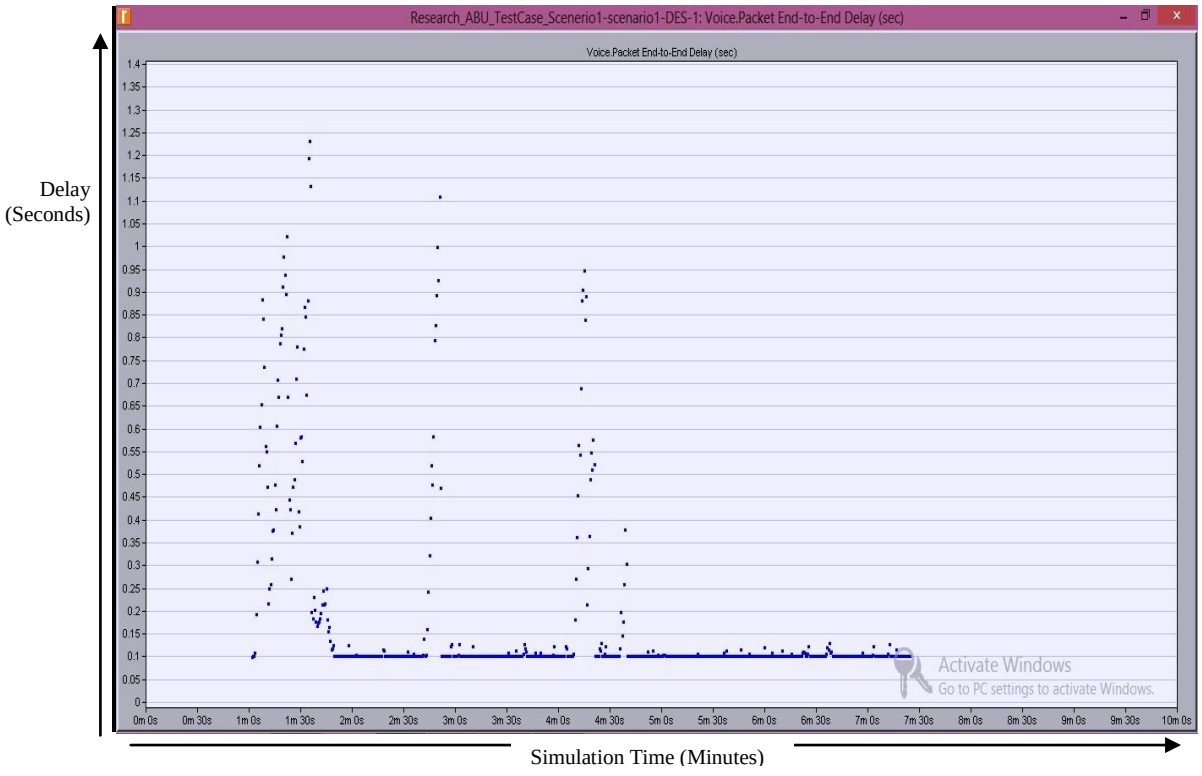


Figure 4.1: Delay in Seconds of Best-Effort Services Model Scenario

Figure 4.1 shows a plot of packet end to end delay in seconds generated after configuring best-effort services model on the OPNET Simulated network. The plot which is a scatter plot indicates packet end to end delay of events (i.e. transmission of a packet from source to destination) at various instants of time from 00s to 600s (indicated on the plot as 0 minutes (m) 0 second(s) to 10m 0s). The packet end to end delay is dependent on the processing time of the network and the time taking in processing other packets in the network before the packet to be processed. Hence the plot of the packet end to end delay reflected the processing time of the network and the time wasted in waiting due to lack of network resource to process the packet. The peaks in delay on the plot such as time 90s, 145s and 255s (indicated on the plot as 1m 30s, 4m 45s, and 4m 15s) are times of high congestion at the interfaces of the network during the simulation since the processing time and the traffic coming into the network varies depending on the number and nature of application running on the network at any given time.

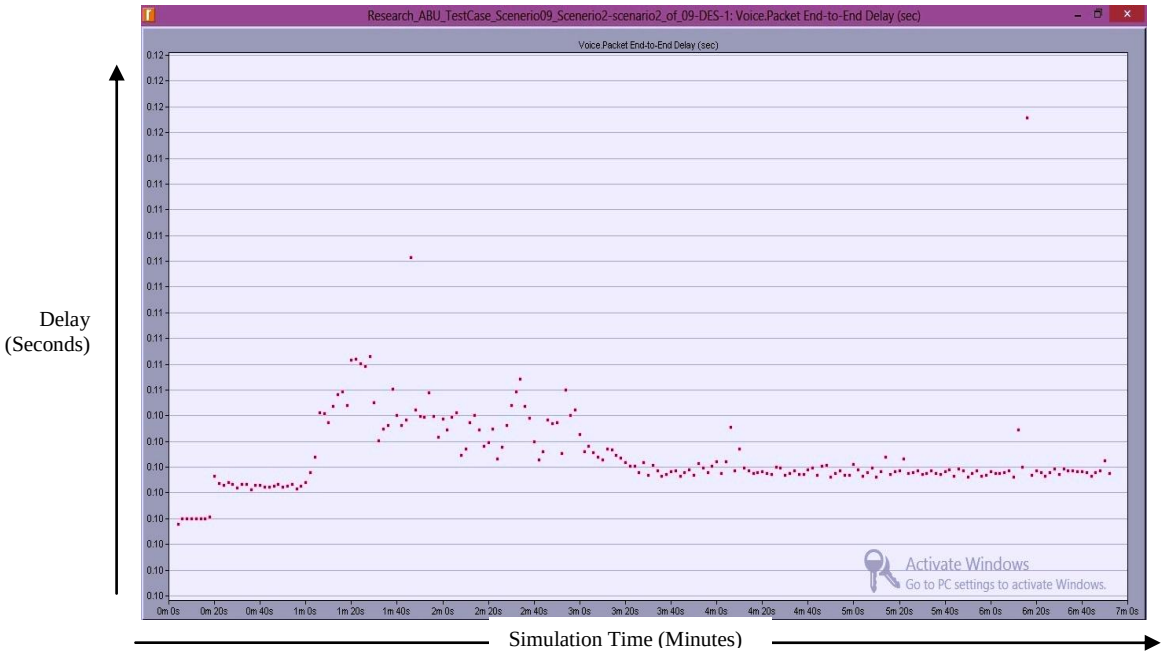


Figure 4.2: Delay of Differentiated Services Test Scenario

Figure 4.2 shows plots of packet end-to-end delay generated after configuring the OPNET Simulated network with differentiated services model. The plot is a scatter graph; the value of

end to end delay in seconds on the plot indicates the level of congestion at the interfaces of the simulated network with differentiated services QoS configured.

The plots of packet end-to-end delay shown in Figure 4.3, is generated from the OPNET Simulated network after configuring it with the developed enhanced differentiated services model.

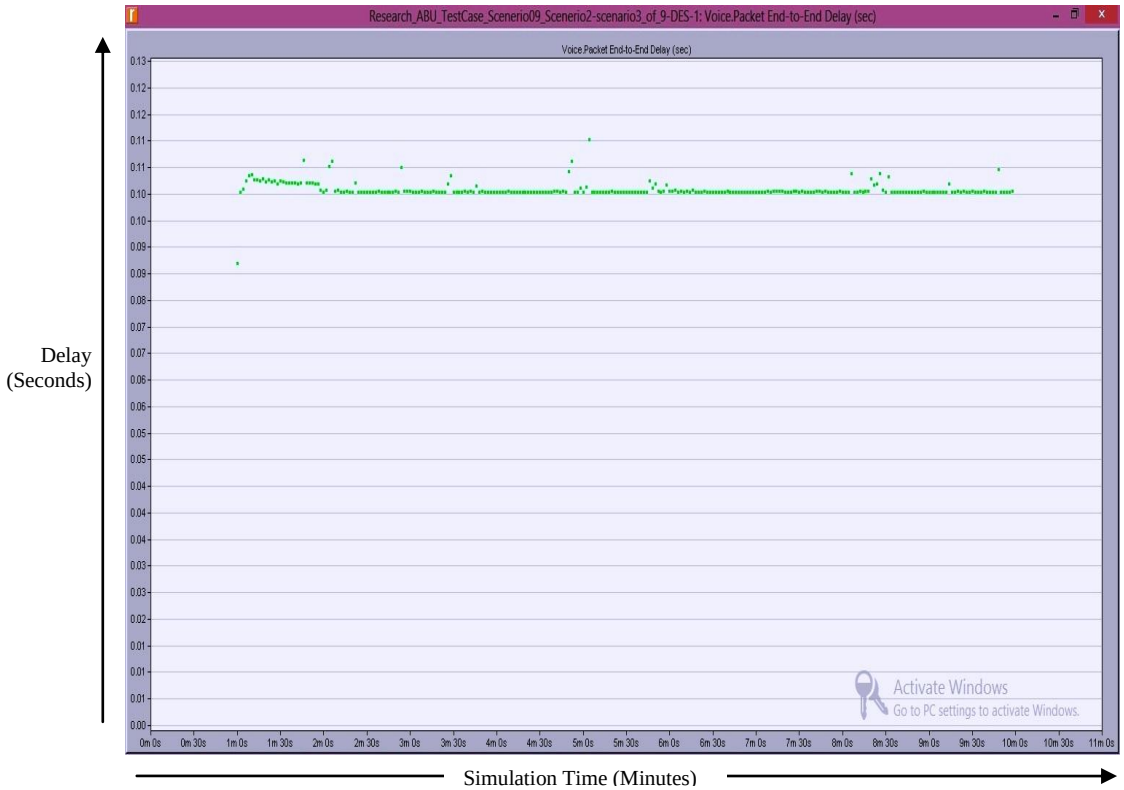


Figure 4.3: Delay of Enhanced Differentiated Services Test Scenario

The plot indicates the packet end-to-end delay at instants of time during the simulation of enhanced differentiated services model.

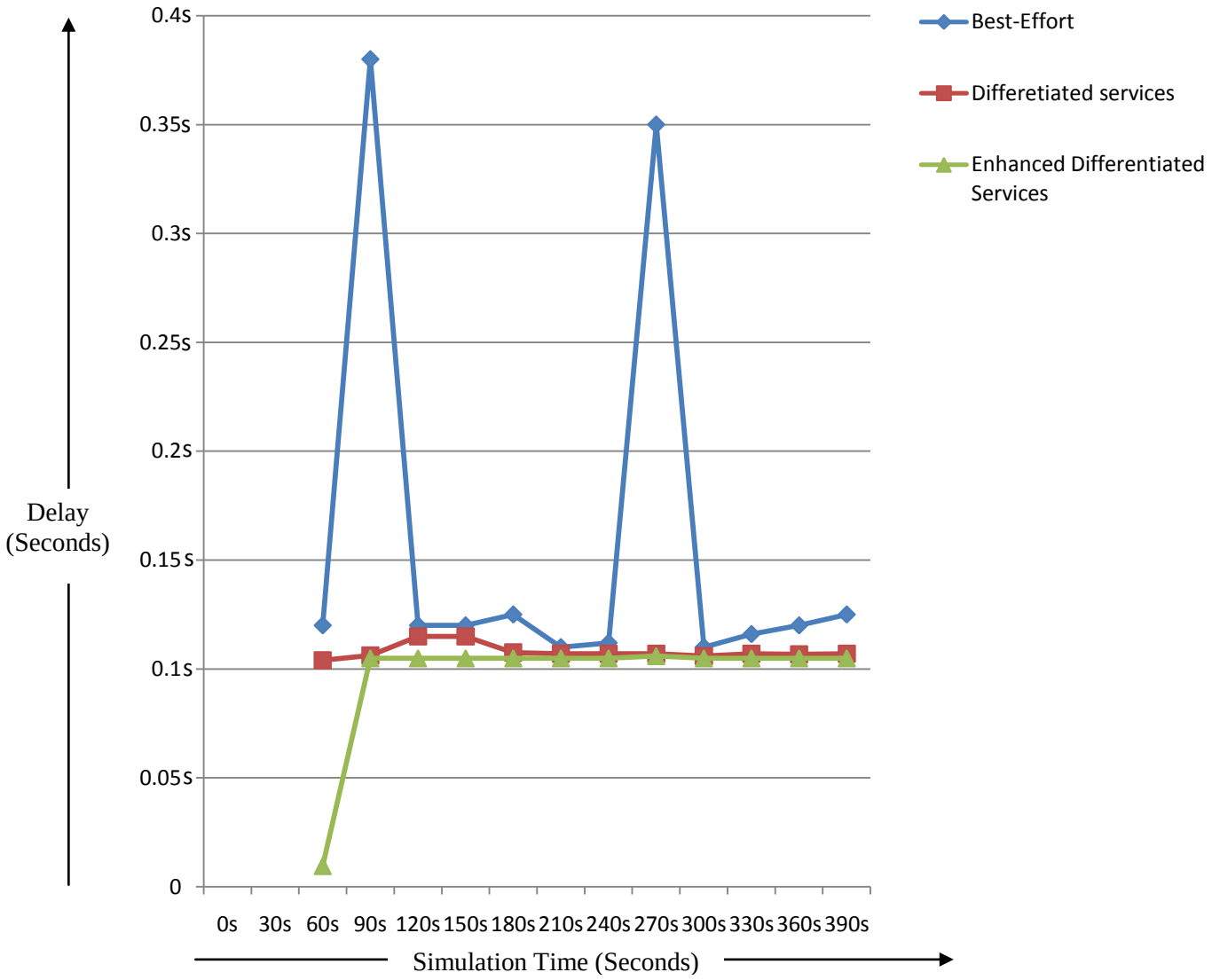


Figure 4.4: Delay of Enhanced, Differentiated Services and Best-Effort Test Scenario

Figure 4.4 shows overlaid plot of best-effort, differentiated services and enhanced differentiated services network scenarios of packet end to end delay at various simulation times. The plot in green indicates the packet end to end delay of enhances differentiated services, the plot in red indicates the packet end-to-end delay of differentiated services, and the plot in blue the packet end to end delay of best-effort at various simulation time. The actual packet end-to-end delay and the rate of fluctuation of the packet end-to-end delay at some instant of time reduces for the plot of differentiated services when compared to the best-effort test case and for the plot of the

enhanced differentiated services when compared to the differentiated services and best-effort test case. These are indications of the level of improvement achieve by the implementation of differentiated services and enhanced differentiated services.

Table 4.1: Delay Time of Best-Effort, Differentiated, and Enhanced Differentiated Services Model

Simulation Time (Seconds)	**Delay Best-Effort (Seconds)**	**Delay Differentiated Services (Seconds)**	**Delay Enhance Differentiated Services (Seconds)**
60	0.12000	0.10400	0.09570
90	0.38000	0.10620	0.10600
120	0.11500	0.10900	0.11000
150	0.12000	0.11500	0.10500
180	0.12500	0.10760	0.10500
210	0.11000	0.10700	0.10500
240	0.10000	0.10720	0.10500
270	0.35000	0.10700	0.10500
300	0.11000	0.10680	0.10600
330	0.10000	0.10720	0.10500
360	0.12000	0.10680	0.10500
390	0.10000	0.10700	0.10500
Mean (Seconds)	0.15417	0.10757	0.10481

The extrapolated data obtain from the plot of best-effort, differentiated, and enhanced differentiated services networks is shown in Table 4.1. From the calculated means, the proposed enhance differentiated service model has better performance with mean packet end to end delay of 0.10481s as compared with the differentiated services packet end to end delay of 0.10757s, and best-effort services network packet end to end delay of 0.15417s.

The level of improve achieve by the differentiated services model compare with the best-effort services model can be elaborated using the equation for percentage improvement.

Percentage Improvement (PI) = $\frac{(Initial\ value - New\ value)}{Initial\ value}\ X\ 100$ 4.1

PI of enhanced over differentiated services = $\frac{(0.10757-0.10481)}{0.10757}\ X\ 100 = 26\%$

PI of Enhance differentiated over best-effort = $\frac{(0.15417-0.10481)}{0.15417}\ X\ 100 = 32\%$

4.2.1 Summary of Simulated Results Obtain using OPNET Simulator

Plots of packet end to end delay of best-effort services model and that of differentiated services model at various simulation times shows the superiority of enhance differentiated services model. Its mean packet end to end delay of 0.10481s is better than the differentiated services mean packet end to end delay by 26%. It is also better than the best-effort services model mean packet end to end delay of 0.15417s by 32%. Hence enhance differentiated services model will guarantee and assure QoS for the transmission of interactive and other multimedia traffic across the network better then the services model currently deployed

4.3 Results of Validation and Application of Enhanced Differentiated services Model

On three instants each of the three service model were configured on the test-bed network and connected to the Internet. The two end devices (computers) were use to check email, stream Channels News and stream Skype. Wireshark network analyser is used to determine packet number, source, and length, destination of packets and time of processing a packet for each of the services model.

The delay and the total time it takes a packet from source to destination can be determined using time of processing a packet and the processed time of each packet. The time it take a packet from source to destination (indicated on table 4.2 to 4.4 as End to End Time) can be calculated using equation 4.2.

End to End Time = Time of processing a packet – Time of processing previous Packet 4.2

Also the delay of each packet across the network can be calculated by subtracting the obtained processing time of each packet from the time it take a packet from source to destination hence the values on table 4.2, 4.3 and 4.4

Table 4.2: Best-Effort Service Model Validation Delay

Time of Processing Packet	End to End Time	Processed Time	Delay
421.057748	0.001964	0.001210	0.001843
421.059712	0.004013	0.000121	0.003892
421.063725	0.010512	0.000108	0.010405
421.074237	0.002004	0.001160	0.001888
421.076241	0.027519	0.001220	0.027397
421.103760	0.004469	0.001011	0.004358
421.108226	0.006006	0.000109	0.005897
421.114235	0.004036	0.000115	0.003921
421.118271	0.001991	0.000142	0.001849
421.132257	0.011995	0.000123	0.011872
Mean	0.0074509	0.0005319	0.007332

Table 4.2 shows the result obtained using Wireshark network analyser to determine the delay of the validation setup test-bed configured with best-effort service model. On the table the mean processed time of 0.0005319s indicated the average duration it takes to process a packet. The mean end to end time of 0.0074509 indicated the average duration it takes a packet to be transmitted from source to destination. While Delay of 0.007332 illustrated the average time a packet spend within the network due to lack of network resource to process the packet.

Table 4.3: Differentiated Service Model Validation Delay

Time of Processing Packet	Total Delay	Process Time	Delay
158.779581	0.000004	0.000004	0.000000
158.784080	0.004499	0.004332	0.000167
158.787582	0.003502	0.003327	0.000175
158.790042	0.002460	0.002460	0.000000
158.794511	0.004469	0.004313	0.000156
158.796765	0.002254	0.002250	0.000004
158.803745	0.006980	0.006830	0.000150
158.810460	0.006715	0.000767	0.005948
158.82038	0.002760	0.001816	0.000944
158.827592	0.007274	0.007274	0.004514
Mean	0.004092	0.003337	0.001206

Table 4.4: Enhanced Differentiated Service Model Validation Delay

Time of Processing Packet	Total Delay	Process Time	Delay
17.961577	0.000218	0.000218	0.000000
17.961795	0.001467	0.001459	0.001321
17.963254	0.002490	0.000246	0.000030
17.963500	0.019898	0.019890	0.000008
17.983398	0.000284	0.000272	0.000012
17.983682	0.000179	0.000170	0.000009
17.983861	0.001444	0.001444	0.000000
17.985305	0.002840	0.002435	0.004045
17.985559	0.001627	0.001627	0.000000
17.987456	0.010984	0.009193	0.001791
Mean	0.043042	0.003886	0.000722

Table 4.3 and 4.4 indicate the average duration it takes to process a packet, average duration it takes a packet to be transmitted from source to destination over the network and the average time a packet spend within the network due to lack of network resource of differentiated services and enhanced differentiated service model. Table 4.3 mean delay values of 0.001206s show improvement in delay reduction over table 4.2 mean delay values of 0.007332. Also table 4.4 mean delay values of 0.000722 shows improvement in delay reduction over that of table 4.3 and table 4.2.

The level of improvement achieved by the enhanced differentiated services model compared with the differentiated services model and with the best-effort service model architecture can be elaborated using equation (4.1) for Percentage Improvement (PI).

Therefore the percentage improvements were computer for enhanced differentiated services over differentiated services and best-effort services model as follows:

PI of enhanced over differentiated services = $\frac{(\ 0.001206 - 0.000722\ )}{0.001203}\ X\ 100 = 40\%$

PI of Enhance differentiated service over best-effort = $\frac{(0.004332 - 0.000722\ )}{0.004332}\ X\ 100 = 83\%$

Hence the enhanced differentiated services model performed better than the differentiated services model by 40% and better than the best-effort services model by 83%.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary of findings

Here are the summary of this research findings,

i. Use of QoS model improves the performance of network.

ii. Due to scalability issue with integrated service model, differentiated services model is mostly preferred for QoS assurances in networks.

iii. Differentiated services model has limitations which include the challenge of Packet being processed and eventually dropped during the last process if threshold of queues are exceeded. This will result to added delay to incoming packet caused by the processed time of packets which are eventually dropped.

iv. To enhance the differentiated services model an admission controller was developed to drop packet early if accepting the packet will eventually cause threshold of queues to be exceeded during the process of queuing and scheduling. The admission decision is based on the comparison of the available and the requested resources to ensure that only packet that will be accepted by the scheduling and queuing systems will be accommodated and process by the network

v. Results and validation of delay of enhance differentiated services model, best-effort services model and that of differentiated services model at various simulation times shows the superiority of enhance differentiated services model.

5.2 Conclusions

i. The use of QoS models such as differentiated services model improves the performance of network in term of packet end to end delay.

ii. The enhancement of the differentiated services model by inclusion of admission control had further improve the performance of network in term of packet end to end delay reduction. This is illustrated by the percentage improvement of the enhanced differentiated services model of 26% over the differentiated service architecture and percentage improvement of the enhanced differentiated services model of 32% over the ABU architecture.

5.3 Limitations

These are the limitations of the research work:

i. The basic limitation of this work is the assumption the interactive traffic such as video conference and voice streaming which are delay sensitive are more important in campus network over non delay sensitive traffic such as file download

ii. In studying the performance of the three models best-effort, differentiated service and develop enhance differentiated service model, the simulated network is approximate network.

5.4 Suggestions for Further Work

The following suggestion are made as to the improvement of research in this area

i. In addition to improving reduction of delay for interactive traffic, efficient bandwidth utilization scheme should be consider. This will greatly improve the overall performance of network.

ii. Because of the effect of delay in QoS of interactive traffic on a network, further research may look at better ways to further reduce delay of networks.

REFERECES

Abaye, A., Lo, W. F., Carsten, R. R., Robertson, B. and Briere, D. (2006). Performance Model*ing of a Communications System. Proceedings of IEEE 29th Conf. on Local Computer Networks, pp. 1-13,*

Academy, Cisco Networking (2014). Scaling Networks Companion Guide: Pearson Education.

Alberto, L.-G., and Indra, W. (2000). Communication networks: fundamental concepts and key architectures. *Mc GrawHill*.

Baswaraj, D. M., & Tomar, D. (2011). Modeling of Packet Switched Network over TCP/IP to Suggest Modified Routing to Reduce Congestion. *Int. J. on Recent Trends in Engineering and Technology, 6*(1).

Bhakta, I., Chakraborty, S., Mitra, B., Sanyal, D. K., Chattopadhyay, S., & Chattopadhyay, M. (2011). A diffServ architecture for QoS-aware routing for delay-sensitive and best-effort services in IEEE 802.16 mesh networks. *Journal of Computer Networks and Communications, 2011*. *25*(9), 34-65.

Bolot J.C., May M., Jean-Marie A., Diot C., (1999) Simple Performance Models of Differentiated Services Schemes for theInternet. Proceedings of IEEE INFOCOM, March 1999

Cai, Y., Wolf, T., & Gong, W. (2011). Delaying transmissions in data communication networks to improve transport-layer performance. *Selected Areas in Communications, IEEE Journal on, 29*(5), 916-927.

Comer, Douglas E.,(2008) Computer networks and internets: Prentice Hall Press.

Dannewitz, Christian, et al.2013 Network of Information (NetInf)–An information-centric networking architecture. Computer Communications 36(7):721-735.

Freeman, R. L. (2009). Introductory Concepts. *Fundamentals of Telecommunications*, 1-19.

Hanuliak, M. (2014). Modeling of parallel computers based on network of computing. *American Journal of Networks and Communications, 3*(1), 43-56.

Headquarters, Corporate (2003) Catalyst 3550 Multilayer Switch Software Configuration Guide. Cisco IOS Release 12:13.

Hutcheson, L. (2008). FTTx: Current status and the future. *Communications Magazine, IEEE, 46*(7), 90-95.

J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, (1999) Assured forwarding PHB group, RFC 2597, Internet Engineering Task Force,June.

Kausha, S., and Sharma, R. (2007). Modeling and analysis of adaptive buffer sharing scheme for consecutive packet loss reduction in broadband networks. *International Journal of Computer Systems Science and Engineering, 4*(1), 8-15.

Kurose, J., and Ross K., (2005), Computer Networking – A Top-Down Approach Featuring the Internet, 3rd Edition -2005 pp 734-736.

Leon-Garcia, A., and Widjaja, I. (2000). Communication Networks: Fundamental Concepts and Key Architectures, 2000: McGraw-Hill Companies Inc., USA.

Liu, H. H., Kandula, S., Mahajan, R., Zhang, M., and Gelernter, D. (2014). Traffic engineering with forward fault correction. Paper presented at the Proceedings of the 2014 ACM conference on SIGCOMM. *9*(2), 216-227.

Nguyen, Long V, Tony Eyers, and Joe F Chichar, (2000) Differentiated service performance analysis. Computers and Communications, 2000. Proceedings. ISCC 2000. Fifth IEEE Symposium on, 2000, pp. 328-333. IEEE.

Obiniyi, A., Soroyewun, M., and Abur, M. (2014). New Innovations in Performance Analysis of Computer Networks: A Review.

Olawoyin, L., Faruk, N., and Akanbi, L. (2011). Queue management in network performance analysis. *Int. J. Sci. Technol, 1*, 215-218.

Pokorný, Martin, et al.(2014).The Impact of Traffic Management Tools Application on the Business Computer Network Performance. Procedia Economics and Finance 12:539-548.

Rakheja, P., Kaur, P., Gupta, A., and Sharma, A. (2012). Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network. *International Journal of Computer Applications, 48*(18), 6-11.

Shaikh, Z. A., andHarkut, D.G.,(2015). An Overview of Network Traffic Classification Methods.*International Journal on Recent and Innovation Trends in Computing and Communication* ISSN: 2321-8169 Volume: 3 Issue: 2 482-488

Sonawane, R. R., and Varalaxmi, G. (2013). A Novel Token Based Approach Towards Packet Loss Control. *Communications Magazine, IEEE, 36*(1), 70-75.

Tavares, Á. S. (2011). Major: Electronics and Communication Engineering, 5th ed. Pp 24-58.

Torabkhani, N. (2014). Modeling and Analysis of the Performance of Networks in Finite-Buffer Regime. *Journal of Computer Networks and Communications, 2014*. *5*(2), 424-445.

Ustares, Jose Javier Escobar(2010)A Forensic Analysis Of Network Security Logs On A Virtual Environment, Texas A and M University-Corpus Christi.

Vaid, Aseem, Sanjeev Putta, and Gregory Rakoshitz(2002) Directory enabled policy management tool for intelligent traffic management: Google Patents.

Wang, Y., Krishnamurthy, A., Qian, L., Dauchy, P., and Conte, A. (2004). A-Serv: a novel architecture providing scalable quality of service [Internet applications]. Paper presented at the Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE.

Wooldridge, M. (1997). Agents as a Rorschach test: A response to Franklin and Graesser Intelligent Agents III Agent Theories, Architectures, and Languages (pp. 47-48): Springer.

my, Cisco Networking (2014). Scaling Networks Companion Guide: Pearson Education.

Dannewitz, Christian. (2013) Network of Information (NetInf)–An information-centric networking architecture. Computer Communications 36(7):721-735.

Mukherjee, Sabyasachi, and OS Khanna (2013) Fairness Evaluation of a DSCP Based Scheduling Algorithm for Real-Time Traffic in Differentiated Service Networks. International Journal of Information and Electronics Engineering 3(4):423.

Nguyen, Long V, Tony Eyers, and Joe F Chicharo, (2000). Differentiated service performance analysis. Computers and Communications. Proceedings of ISCC 2000 Fifth IEEE Symposium 2000, pp. 328-333. IEEE.

Roughan, Matthew, (2004) Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification. Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, 2004, pp. 135-148. ACM.

Ustares, Jose Javier Escobar, (2010) A Forensic Analysis Of Network Security Logs On A Virtual Environment, Texas A&M University-Corpus Christi.

Wan, Zheng, (2015). Evaluation on Inner-priority and Cross-class Priority based Multiple Video Streaming under DiffServ Architecture. International Journal of Future Generation Communication and Networking 8(4):275-286.

Zheng, Li, Doan B Hoang, and Ming Li, (2012) Wireless Hybrid QoS Architecture with an Enhancement of Fair Intelligent Congestion Control. *International Journal of Computer Applications, 8*(12), 56-61.

APPENDIX I

Best-Effort Services Model Configuration on the Routers

EXTERIOR ROUTER

```
Router>enable
Router#config t
Router(config)#hostname Exterior_Router
Exterior_Router(config)#interface fastEthernet 0/0
Exterior_Router(config-if)#ip address 192.168.40.10 255.255.255.0
Exterior_Router(config-if)#no shutdown
FastEthernet0/0
IP address 192.168.40.10
Status manual up
Exterior_Router(config-if)#exit
Exterior_Router(config)#interface fastEthernet 1/0
Exterior_Router(config-if)#ip address 192.168.30.10 255.255.255.0
Exterior_Router(config-if)#no shutdown
FastEthernet1/0
IP address 192.168.30.11
Status manual up
Exterior_Router(config-if)#
Exterior_Router(config-if)#^Z
Exterior_Router#
Exterior_Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.30.11
Exterior_Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.40.10
Exterior_Router(config)#ip route 192.168.10.0 255.255.255.0 192.168.40.10
Exterior_Router(config)#ip route 0.0.0.0 0.0.0.0 10.255.4.1
Exterior_Router(config)#exit
```

CORE SWITCH

```
Router>enable
Router#config t
Router(config)#hostname Core_Switch
Core_Switch(config)#interface serial 2/0
Core_Switch(config-if)#ip address 192.168.20.10 255.255.255.0
Core_Switch(config-if)#no shutdown
Serial2/0
IP address 192.168.20.10
Status manual up
Core_Switch(config-if)#exit
Core_Switch(config)#interface fastEthernet 0/0
Core_Switch(config-if)#ip address 192.168.40.1 255.255.255.0
Core_Switch(config-if)#no shutdown
```

FastEthernet0/0
IP address 192.168.40.1
Status manual up
Core_Switch(config-if)#exit
Core_Switch(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.1
Core_Switch(config)#ip route 192.168.10.1 255.255.255.0 192.168.30.1
Core_Switch(config)#ip route 192.168.30.10 255.255.255.0 192.168.40.10
Core_Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.40.10
Core_Switch(config)#exit

INTERIOR ROUTER

Router>enable
Router#config t
Router(config)#hostname Interior Router
Interior_Router(config)#interface fastEthernet 0/0
Interior_Router(config-if)#ip address 192.168.10.1 255.255.255.0
Interior_Router(config-if)#no shutdown
FastEthernet0/0
IP address 192.168.10.1
Status manual up
Interior_Router(config)#interface serial 2/0
Interior_Router(config-if)#ip address 192.168.30.1 255.255.255.0
Interior_Router(config-if)#no shutdown
Serial2/0 192.168.30.1
Status manual up
Interior_Router(config-if)#exit
Interior_Switch(config)#ip route 192.168.20.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 192.168.40.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 192.168.30.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.10
Interior_Switch(config)#exit
Interior_Switch#

POLICY SWITCH

Switch>enable
Switch#config t
Switch(config)#hostname Policy_Switch
Policy_Switch(config)#interface vlan1
Policy_Switch(config-if)#ip address 192.168.40.10 255.255.255.0
Policy_Switch(config-if)#no shutdown
Vlan1
IP address 192.168.40.10
Status manual up

DISTRIBUTION SWITCH

Switch>enable
Switch#config t
Switch(config)#hostname Distribution_Switch
Distribution_Switch(config)#
Distribution_Switch(config)#interface vlan1
Distribution_Switch(config-if)#ip address 192.168.10.10 255.255.255.0
Distribution_Switch(config-if)#show ip interface brief
Vlan1
IP address 192.168.10.10
Status manual up

APPENDIX II

Differentiated Services Architecture Configuration on the Routers

EXTERIOR ROUTER

```
Router>enable
Router#config t
Exterior_Router(config-if)#ip address 192.168.40.10 255.255.255.0
Exterior_Router(config-if)#no shutdown
FastEthernet0/0
IP address 192.168.40.10
Status manual up
Exterior_Router(config-if)#exit
Exterior_Router(config)#interface fastEthernet 1/0
Exterior_Router(config-if)#ip address 192.168.30.10 255.255.255.0
Exterior_Router(config-if)#no shutdown
FastEthernet1/0
IP address 192.168.30.11
Status manual up
Exterior_Router(config-if)#
Exterior_Router(config-if)#^Z
Exterior_Router#
Exterior_Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.30.11
Exterior_Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.40.10
Exterior_Router(config)#ip route 192.168.10.0 255.255.255.0 192.168.40.10
Exterior_Router(config)#ip route 0.0.0.0 0.0.0.0 10.255.4.1
Exterior_Router(config)#class-map EF
Exterior_Router(config-cmap)#match all
Exterior_Router(config-cmap)#match EF starting-port-number 443
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF1
Exterior_Router(config-cmap)#match all
Exterior_Router(config-cmap)#match AF1 starting-port-number 25
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF2
Exterior_Router(config-cmap)#match all
Exterior_Router(config-cmap)#match AF2 starting-port-number 80
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF3
Exterior_Router(config-cmap)#match all
Exterior_Router(config-cmap)#match AF3 starting-port-number 1090
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#policy-map EF
Exterior_Router(config-pmap)#bandwidth-percent 40
Exterior_Router(config-cmap)#exit
```

Exterior_Router(config)#policy-map AF1
Exterior_Router(config-pmap)#bandwidth-percent 20
Exterior_Router(config-cmap)#exit
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#policy-map AF2
Exterior_Router(config-pmap)#bandwidth-percent 15
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#policy-map AF3
Exterior_Router(config-pmap)#bandwidth-percent 25
Exterior_Router(config-cmap)#exit

CORE SWITCH

Router>enable
Router#config t
Router(config)#hostname Core_Switch
Core_Switch(config)#interface serial 2/0
Core_Switch(config-if)#ip address 192.168.20.10 255.255.255.0
Core_Switch(config-if)#no shutdown
Serial2/0
IP address 192.168.20.10
Status manual up
Core_Switch(config-if)#exit
Core_Switch(config)#interface fastEthernet 0/0
Core_Switch(config-if)#ip address 192.168.40.1 255.255.255.0
Core_Switch(config-if)#no shutdown
FastEthernet0/0
IP address 192.168.40.1
Status manual up
Core_Switch(config-if)#exit
Core_Switch(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.1
Core_Switch(config)#ip route 192.168.10.1 255.255.255.0 192.168.30.1
Core_Switch(config)#ip route 192.168.30.10 255.255.255.0 192.168.40.10
Core_Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.40.10
Core_Switch(config)#
Core_Switch(config)#policy-map ET

INTERIOR ROUTER

Router>enable
Router#config t
Router(config)#hostname Interior Router
Interior_Router(config)#interface fastEthernet 0/0
Interior_Router(config-if)#ip address 192.168.10.1 255.255.255.0
Interior_Router(config-if)#no shutdown

FastEthernet0/0
IP address 192.168.10.1
Status manual up
Interior_Router(config)#interface serial 2/0
Interior_Router(config-if)#ip address 192.168.30.1 255.255.255.0
Interior_Router(config-if)#no shutdown
Serial2/0 192.168.30.1
Status manual up
Interior_Router(config-if)#exit
Interior_Switch(config)#ip route 192.168.20.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 192.168.40.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 192.168.30.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.10
Interior_Switch(config)#exit
Interior_Switch#

POLICY SWITCH

Switch>enable
Switch#config t
Switch(config)#hostname Policy_Switch
Policy_Switch(config)#interface vlan1
Policy_Switch(config-if)#ip address 192.168.40.10 255.255.255.0
Policy_Switch(config-if)#no shutdown
Vlan1
IP address 192.168.40.10
Status manual up

DISTRIBUTION SWITCH

Switch>enable
Switch#config t
Switch(config)#hostname Distribution_Switch
Distribution_Switch(config)#
Distribution_Switch(config)#interface vlan1
Distribution_Switch(config-if)#ip address 192.168.10.10 255.255.255.0
Distribution_Switch(config-if)#show ip interface brief
Vlan1
IP address 192.168.10.10
Status manual up
Distribution_Switch>enable
Distribution_Switch#config t
Distribution_Switch(config)#interface fastEthernet 0/1
Distribution_Switch(config-if)#fair-queue
Distribution_Switch(config-if)#congestive-discard-threshold 80

```
Distribution_Switch(config-if)#exit
Distribution_Switch(config)#interface fastEthernet 1/1
Distribution_Switch(config-if)#fair-queue
Distribution_Switch(config-if)#congestive-discard-threshold 90
Distribution_Switch(config-if)#exit
Distribution_Switch(config)#interface fastEthernet 2/1
Distribution_Switch(config-if)#fair-queue
Distribution_Switch(config-if)#congestive-discard-threshold 100
Distribution_Switch(config-if)#exit
```

APPENDIX III

Enhanced Differentiated Services Architecture Configuration on the Routers

EXTERIOR ROUTER

```
Router>enable
Router#config t
Router(config)#hostname Exterior_Router
Exterior_Router(config)#interface fastEthernet 0/0
Exterior_Router(config-if)#ip address 192.168.40.10 255.255.255.0
Exterior_Router(config-if)#no shutdown
FastEthernet0/0
IP address 192.168.40.10
Status manual up
Exterior_Router(config-if)#exit
Exterior_Router(config)#interface fastEthernet 1/0
Exterior_Router(config-if)#ip address 192.168.30.10 255.255.255.0
Exterior_Router(config-if)#no shutdown
FastEthernet1/0
IP address 192.168.30.11
Status manual up
Exterior_Router(config-if)#
Exterior_Router(config-if)#^Z
Exterior_Router#
Exterior_Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.30.11
Exterior_Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.40.10
Exterior_Router(config)#ip route 192.168.10.0 255.255.255.0 192.168.40.10
Exterior_Router(config)#ip route 0.0.0.0 0.0.0.0 10.255.4.1
Exterior_Router(config)#class-map EF
Exterior_Router(config-cmap)#match all
Exterior_Router(config-cmap)#match EF starting-port-number 443
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF1
Exterior_Router(config-cmap)#match all
Exterior_Router(config-cmap)#match AF1 starting-port-number 25
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF2
Exterior_Router(config-cmap)#match all
Exterior_Router(config-cmap)#match AF2 starting-port-number 80
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF3
Exterior_Router(config-cmap)#match all
Exterior_Router(config-cmap)#match AF3 starting-port-number 1090
Exterior_Router(config-cmap)#exit
```

Exterior_Router(config)#policy-map EF
Exterior_Router(config-pmap)#bandwidth-percent 40
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#policy-map AF1
Exterior_Router(config-pmap)#bandwidth-percent 20
Exterior_Router(config-cmap)#exit
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#policy-map AF2
Exterior_Router(config-pmap)#bandwidth-percent 15
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#policy-map AF3
Exterior_Router(config-pmap)#bandwidth-percent 25
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map EF
Exterior_Router(config-cmap)#admission-control bandwidth_pct 100
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF1
Exterior_Router(config-cmap)#admission-control bandwidth_pct 90
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF2
Exterior_Router(config-cmap)#admission-control bandwidth_pct 80
Exterior_Router(config-cmap)#exit
Exterior_Router(config)#class-map AF3
Exterior_Router(config-cmap)#admission-control bandwidth_pct 90

CORE SWITCH

Router>enable
Router#config t
Router(config)#hostname Core_Switch
Core_Switch(config)#interface serial 2/0
Core_Switch(config-if)#ip address 192.168.20.10 255.255.255.0
Core_Switch(config-if)#no shutdown
Serial2/0
IP address 192.168.20.10
Status manual up
Core_Switch(config-if)#exit
Core_Switch(config)#interface fastEthernet 0/0
Core_Switch(config-if)#ip address 192.168.40.1 255.255.255.0
Core_Switch(config-if)#no shutdown
FastEthernet0/0
IP address 192.168.40.1
Status manual up
Core_Switch(config-if)#exit
Core_Switch(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.1

Core_Switch(config)#ip route 192.168.10.1 255.255.255.0 192.168.30.1
Core_Switch(config)#ip route 192.168.30.10 255.255.255.0 192.168.40.10
Core_Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.40.10
Core_Switch(config)#
Core_Switch(config)#policy-map ET

INTERIOR ROUTER

Router>enable
Router#config t
Router(config)#hostname Interior Router
Interior_Router(config)#interface fastEthernet 0/0
Interior_Router(config-if)#ip address 192.168.10.1 255.255.255.0
Interior_Router(config-if)#no shutdown
FastEthernet0/0
IP address 192.168.10.1
Status manual up
Interior_Router(config)#interface serial 2/0
Interior_Router(config-if)#ip address 192.168.30.1 255.255.255.0
Interior_Router(config-if)#no shutdown
Serial2/0 192.168.30.1
Status manual up
Interior_Router(config-if)#exit
Interior_Switch(config)#ip route 192.168.20.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 192.168.40.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 192.168.30.0 255.255.255.0 192.168.20.10
Interior_Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.10Interior_Switch(config)#exit
Interior_Switch#

POLICY SWITCH

Switch>enable
Switch#config t
Switch(config)#hostname Policy_Switch
Policy_Switch(config)#interface vlan1
Policy_Switch(config-if)#ip address 192.168.40.10 255.255.255.0
Policy_Switch(config-if)#no shutdown
Vlan1
IP address 192.168.40.10
Status manual up

DISTRIBUTION SWITCH

```
Switch>enable
Switch#config t
Switch(config)#hostname Distribution_Switch
Distribution_Switch(config)#
Distribution_Switch(config)#interface vlan1
Distribution_Switch(config-if)#ip address 192.168.10.10 255.255.255.0
Distribution_Switch(config-if)#show ip interface brief
Vlan1
IP address 192.168.10.10
Status manual up
Distribution_Switch>enable
Distribution_Switch#config t
Distribution_Switch(config)#interface fastEthernet 0/1
Distribution_Switch(config-if)#fair-queue
Distribution_Switch(config-if)#congestive-discard-threshold 80
Distribution_Switch(config-if)#exit
Distribution_Switch(config)#interface fastEthernet 1/1
Distribution_Switch(config-if)#fair-queue
Distribution_Switch(config-if)#congestive-discard-threshold 90
Distribution_Switch(config-if)#exit
Distribution_Switch(config)#interface fastEthernet 2/1
Distribution_Switch(config-if)#fair-queue
Distribution_Switch(config-if)#congestive-discard-threshold 100
Distribution_Switch(config-if)#exit
```