Computer Science Department

Masters of Science Project

University of Fort Hare
Together in Excellence

AN ANALYSIS OF THE CORRELATION BETWEEN PACKET LOSS AND NETWORK DELAY ON THE PERFORMANCE OF CONGESTED NETWORKS AND THEIR IMPACT: CASE STUDY UNIVERSITY OF FORT HARE

Student:
Lutshete S. 200390813

Supervisor:
Dr K. Sibanda

December 2012

Dedications

I dedicate this work to my mom (Nancy), grandmother (Mamtshawe), grandfather (Tutu), aunts (Nontuthuzelo & Vuyelwa) and also to my cousins and friends.

Declaration

I, the undersigned declare that the work contained in this dissertation is my own original work and has not previously in its entirety or in part been submitted at any educational institution for a similar or any other degree awarded. I acknowledge that all references are accurately recorded and that, unless otherwise stated, all work herein is my own.

Signature..

Date...

Acknowledgements

I would like to thank the Eskom Holdings Limited for funding this research. Many thanks also go to the department of Computer Science, University of Fort Hare. In addition, I am truly grateful to my supervisor Dr. K. Sibanda and also Prof M. Thinyane whose doors were always open to me for guidance. Their guidance and support was invaluable.

Sincere gratitude also extends to Mr. M. Sibanda, Mr. C. Kika, and Miss S.M. Mabaso, all my colleagues from the Computer Science department, all members of the University of Fort Hare Technology and Support Centre (TSC) for the wealth of support they gave me during my studies. Thank you guys, your help is much appreciated, you all sacrificed your time. The combined contribution from all these parties is beyond measure. It made it all possible for the study.

To my parents, family members and relatives, thank you very much for the love and support. Throughout every milestone along the road, your encouragement kept me going until the end. To all my friends, too many to mention, I thank you for the moral support that you provided throughout the study period, I always had a family away from home. Above all, I would like to thank the Almighty for the wisdom, knowledge and understanding. All this is a manifestation of his love and grace.

Publication from this work

A Comparative Analysis of end to end Packet Delay and Loss rate at the University of Fort Hare network under stress

Lutshete Sizwe[1], Sibanda Khulumani[1], Sibanda Melusi[2]
1. Department of Computer Science
University of Fort Hare
Department of Computer Science
P. Bag X1314, Alice 5700
Tel: +27 40 602 2464, Fax +27 40 602 2464
email: {slutshete,ksibanda}@ufh.ac.za
2. Department of Economics and Extension
University of Fort Hare
P. Bag X1314, Alice 5700
Tel: +27 726473073,
email: sibandamelusi@yahoo.co.uk

Abstract- In this paper we study packet delay and loss rate at the University of Fort Hare network. The focus of this paper is to evaluate the information derived from a multipoint measurement of, University of Fort Hare network which will be collected for a duration of three Months during June 2011 to August 2011 at the TSC uplink and Ethernet hubs outside and inside relative to the Internet firewall host. The specific value of this data set lies in the end to end instrumentation of all devices operating at the packet level, combined with the duration of observation. We will provide measures for the normal day−to−day operation of the University of fort hare network both at off-peak and during peak hours. We expect to show the impact of delay and loss rate at the University of Fort Hare network. The data set will include a number of areas, where service quality (delay and packet loss) is extreme, moderate, good and we will examine the causes and impacts on network users.

***Index terms*−− packet delay, packet loss, multipoint measurement, end to end measurement**

INTRODUCTION

There has been a rapid rise in the use of Internet services worldwide. Subscriber growth seemingly has reached its saturation point and the ‘competition-of-volume’ between service providers has no more meanings in this market situation [1]. In this era, Internet users demand more refined quality of service (QoS), more diversified features of services and more enhanced performance, that is, ‘competition-of-quality’. Therefore, network performance management to provisioning QoS-guaranteed network is one of the significant issues for end to end network providers to survive in the Internet services market. An end-to-end network path consists of a sequence of store-and-forward links that transfer packets from the source host to the destination host at each end of the path. Most packet switched networks use store-and-forward transmission at the input of the link. A switch using store-and-forward transmission receives (save) the entire packet to the buffer and checks it for Cyclic Redundancy Check (CRC) errors or other problems before sending the first bit of the packet into the outbound link. Thus store-and-forward packet switches introduce a store-and-forward delay at the input to each link along the packet's route. Two commonly used throughput-related metrics of a path are the end-to-end capacity and the end-to-end available bandwidth [2]. Throughput is the amount of information (in bits, bytes, packets, etc) that can go or be sent through a connection, that is, the actual bandwidth that is available to a network. An end-to-end capacity is the maximum possible end-to-end throughput and an end-to-end available bandwidth is the maximum end-to-end throughput without reducing cross traffic rate. This study will focus at the University of Fort hare Network. It will examine end-to-end connection for Client-Server communications.

PROBLEM DOMAIN

In recent years, network users are demanding anytime and anywhere access to high-speed internet services [3]. Therefore various challenges to provide the end-to-end QoS guaranteed services through (Wide Local Area Network) WLAN have arisen that include QoS parameters and bottleneck generated due to the limited capacity and the overload at a gateway linked with backbone network. Nowadays, internet is the main source to access information. According to [4], the Internet offers great opportunities for educational purposes. The web is a cost effective technology to facilitate the development of educational applications [5]. On the other hand, there has been much debate on the usefulness of the Internet for educational purposes; however it is still argued that the web is still not suitable for teaching probably because of network congestion [6]. The main problem at hand say at Fort Hare University is the network traffic congestion that results in high loss and delay rates of data packets. The network performance is not stable as a result of known and unknown bottlenecks. A bottleneck is a phenomenon where the performance or capacity of an entire network system is limited by a single or limited number of components or resources. One of the known bottlenecks is congestion; as a result, the network performance has been degraded, making it very difficult to access the Internet and other network applications. Therefore, the poor performance of Internet access can have a huge impact on academic results. This study will enable us to propose new network management techniques so as to monitor, control and determine how network resources are utilized.

Research Objectives

This study will analyze QoS (packet loss, delay, jitter, etc) an end-to-end delay and loss rate of different available bandwidth of an Internet path at Fort Hare University

The specific objectives are to:

- To investigate the delay characteristics of different available bandwidth services through bandwidth measuring tools such as ping, packet tracer and packet sniffer.
- To determine whether the delay is stable through the analysis of bandwidth characteristics obtained from the use of bandwidth measuring tools
- To investigate the loss rate of data packets at the University of fort hare network
- To investigate the critical bottlenecks across the whole network
- To asses what factors are affecting the delay through literature survey

Measurements

We will study the University of Fort Hare network by collecting network data traffic using bandwidth measuring tools. In order to analyze and model the characteristics of loss and delay rate, there is a need to find a measurement tool to gather the data. We classify measurements tools as those that take round-trip, or two-way measurements, and those that can take one-way measurements. A brief discussion of these methods and their examples follows. For a two way measurement, the most commonly used method for measuring delay and packet loss characteristics are the Internet Control Message Protocol (ICMP) tools, ping and trace route, which send probe packets to the destination and gather information about the network path from the response [7]. One-way measurements are more valuable as they give information as to the direction in which the observed behavior occurs, unlike two-way measurements which offer the aggregate measurements. For example, by noting the exact arrival and departure time of packets at both hosts, it is trivial to isolate the different components which contribute to the round trip delay. However for this study the one way measurement method will not be employed because such approaches are not widely deployed and they require installation of software at both the source and destination, which is difficult and thus severely limit the number of potential hosts that can be used in measurements [7]. Measurements are necessary for understanding the current system behavior and also inform the implementation of the new system.

Experiments

After gathering data, experiments will be conducted by simulating University of fort hare network traffic using scilab as our simulation tool. Following the topology construction of the University of Fort Hare network, network traffic is simulated. This is done on the condition that the network is observed 8 hours a day. The reason for choosing "8 hours" is because it is the most common number of business hours.

Data Analysis

This will be the comparison of the data from simulation experiments with the data from the actual network (one collected from TSC). Then after propose changes on the performance of the current network setup. The purpose of analysis is for creating recommendations for network performance improvement.

CONCLUSION

With this study we expect to find major reason for data packet loss and delays and also investigate the critical bottlenecks across the University of Fort Hare network. To achieve this, a two way measurement method will be employed.

ACKNOWLEDGEMENTS

We would to thank ESKOM who offered me bursary to undertake the research. Also Telkom Center of Excellence in ICT for Development at the University of Fort Hare, with funding from Telkom, Tellabs, Saab Grintek Technologies, Easttel and THRIP.

REFERENCES

[1] Kang, K.C., Nam, K., Jeon, D.J., & Kim, S.Y., 2002. Delay Characteristics of High-Speed Internet Access Network: One Case Study

[2] Tan, W., Zhanikeev, M. & Tanaka, Y., 2006. "Rate-Based and Gap-Based Available Bandwidth "Estimation Techniques in Cross-Traffic Context. Conference paper presented at the 9th Asia-Pacific Network Operations and Management Symposium. Busan, Korea.

[3] Kim, Y. & Takano, M., 2006. "Management of Convergence Networks and Services", Conference paper presented at the 9th Asia-Pacific Network Operations and Management Symposium. Busan, Korea.

[4] Fong, A.C.M. & Hui, S.C., 2002. "An end to end solution for Internet lecture delivery". *Campus wide information systems* 19(2): 45-51.

[5] Tian, S., 2001. ``The World Wide Web: a vehicle to interactive learning and teaching applications", *Internet Research: Electronic Networking and Policy*, Vol. 11 No. 1, pp. 74-83.

[6] Bork, A. & Britton, D.R., 1998. ``The Web is not yet suitable for learning", *IEEE Computer*, Vol. 31 No. 6, pp. 115-116.

[7]Savage, S., 1999. "Sting: a TCP-based Network Measurement Tool," In Proceedings of the 1999 USENIX Symposium on Internet Technologies and Systems".

Lutshete Sizwe completed a B.Sc degree in 2007 and Honours in Computer Science in 2008, at the University Of Fort Hare and currently an MSc researcher at the University Of Fort Hare. His research interests include networking technologies.

Abstract

Effective network management is essential in supporting business processes and operations; however, little evidence provide empirical information on current network management practices to assist IT personnel to identify the weaknesses of their networks and to plan for improvement. This research is an initiative towards improving University of Fort Hare's (UFH) network performance. To accomplish that we have illustrated and highlighted the correlation between packet delay and loss rate in relation to network performance at the UFH network. The research focuses on measuring and analysing the relationship between end-to-end network delay and loss rate, network performance behaviours that both affect delay and packet loss. A review of background study on the correlation of delay and packet loss and how the end-to-end network parameters collectively affect network performance was conducted. End-to-end Network delay and loss rate behaviour were measured, monitored and modelled using Optimized Network Engineering Tool software (OPNET) modeller, Orion NPM and Cacti. The findings showed that the UFH network is highly congested and as a result the network experiences unaccepted delays leading to high packet loss. We developed an improved network architecture with the main aim of improving its efficiency, performance and behaviour of the future UFH network. This was using measurements and computer simulation; as well as data gathered from a questionnaire that was administered to a focus group set up at UFH.

Key words—End to end packet delay, loss rate, congestion, network performance, network management, OPNET, Orion NPM

Table of contents

Dedications ii

Declaration iii

Acknowledgements iv

Publication from this work v

ACKNOWLEDGEMENTS vii

Abstract viii

Table of contents ix

List of Tables xii

List of Figures xiii

List of Acronyms xiv

Chapter one: Introduction 1

1.0 Introduction 1

1.1 Background and motivation 1

1.1.1 UFH network Infrastructure 5

1.2 Problem Statement 10

1.3 Research Objectives 11

1.3 Research Questions 12

1.4 Justification 12

1.5 Methodology 13

1.5.1 Experiments 13

1.5.2 Data analysis 13

1.6 Outline of The dissertation 13

Chapter two: Literature review 15

2.0 Introduction 15

2.1 Network Performance 15

2.1.1 The need to measure network performance 16

2.1.2 QoS Parameters for Network Service 18

2.1.3 Network performance metrics 19

2.1.4 Network performance management 22
2.1.5 Network traffic management 30
2.1.6 Network Congestion 36
2.1.6.1 Network bottlenecks related to congestion 36
2.1.7 End user experience on Network performance 40
2.1.8 Network management techniques employed at the University of Fort Hare network 41
2.1.9 Current trends in network performance management and monitoring 44
Chapter three: End-to-End packet delay and packet loss in switched networks 47
3.0 Introduction 47
3.1 Delay and Loss in Packet-Switched Networks 47
3.1.1Queuing Delay 50
3.1.2 Packet Loss 52
3.2 Summary 52
Chapter four: Network Management Techniques 53
4.0 Introduction 53
4.1 Techniques used for network performance evaluation 53
4.1.1 Mathematical analysis 53
4.1.2 Measurements 54
4.1.3 Computer simulations 57
4.2 Chosen methods 57
4.3 Summary 57
Chapter five: Methodology and implementation 59
5.0 Introduction 59
5.1 Phase 1 59
5.1.2 Deployment of cacti as performance monitoring tool 63
5.1.3 Investigation of network performance metrics 64
5.2 Phase 2 65
5.2.1 Identification of network management 65
5.2.2 Data collection 66

5.2.3 Evaluation of network management techniques ...66
5.3 Phase 3...66
5.3.1 Network Model Framework...67
5.3.2 Modelling Topology...69
5.3.3 Configuring Applications ...74
5.3.4 Configuring Profiles ...75
5.3.5 Configuring Web (HTTP) applications ...76
5.3.6 Configuring e-mail APPLICATIONS...77
5.3.7 Configuring FTP applications ...78
5.3.8 Simulation Tool...79
5.4 Summary...80
Chapter six: Results and analysis...82
6.0 Introduction ...82
6.1 Packet Loss and delay...82
6.2 Modelled delay and loss rate traffic ...88
6.3 Correlation between delay and loss...91
Chapter 7: Conclusions and recommendations...94
7.0 Introduction ...94
7.1 Summary and conclusion ...94
7.2 Recommendations...96
7.3 Future work ...97
References ...99
Appendix 1 ...107
UFH Internet disruption messages (emails) ...107
Appendix 2 ...110
Bandwidth usage ...110
END-TOE-END WEEKLY(HOUR) PACKET LOSS ...111
END-TOE-END MONTHLY(WEEKLY) PACKET LOSS...112
UFH NETWORK MAP ...113

List of Tables

TABLE 6. 1 : Correlation between delay and packet loss 91

List of Figures

Figure 1. 1: UFH total headcounts……………………………………………………………..4
Figure 1. 2: Network infrastructure of UFH…………………………………………………7
Figure 1. 3: Catalyst 6509 switch……………………………………………………………8
Figure 1. 4: Great hall stackable switch…………………………………………………..9
Figure 1. 5: Stackable switch………………………………………………………………10
Figure 2. 1: Common network performance metrics…………………..........................18
Figure 2. 2: DIagrammatic example of a simulation of a study... 28
Figure 2. 3: Cacti end to end delay graph 35
Figure 2. 4: Cacti end to loss graph 35
Figure 2. 5: Current ufh orion network management tool 43
Figure 3. 1 : Delay in packet switched networks ………………………………………. 48
Figure 5. 1 : Discovered snmp and icmp enabled nodes……………………………….60
Figure 5. 2 : Network availability 63
Figure 5. 3 : Network framework 67
Figure 5. 4 : Project editor 68
Figure 5. 5 : Node model 70
Figure 5. 6 : Switch node model 71
Figure 5. 7 : Link model 72
Figure 5. 8 : Probe model 73
Figure 5. 9 : Entire University of Fort Hare network topology model 74
Figure 5. 10 : Configuring a web application in opnet 77
FIGURE 5. 11 : Configuring an e-mail application in opnet.. 78
Figure 5. 11 : Configuring an e-mail application in opnet 79
Figure 5. 12 : Simulation tool... 80
Figure 6. 1 : End to end daily (hour) packet delay and loss………………………………82
Figure 6. 2 : End to end weekly (daily) packet delay and loss 83
Figure 6. 3 : End to end monthly (weekly) packet delay and loss 84
Figure 6. 4 : Packet loss and delay rate from 1/3/2012 to 30/3/2012 85
Figure 6. 5 : Packet loss and delay rate from 1/1/2012 to 10/23/2012............................. 86
Figure 6. 6 : Modelled delay and loss packet behaviour.. 89
Figure 6. 7 : Delay and loss of ufh live network... 90
Figure 6. 8 : Delay and loss of modelled ufh network 90
Figure 6. 9 : Correlation between loss and delay... 92
Figure 7. 1 : Proposed network architecture 98

List of Acronyms

ACK	Acknowledgement
ART	Application Response Time
ATM	Asynchronous Transfer Mode
CAC	Connection Admission Control
Cat	Category
DSR	Dynamic Source Routing
FTP	File Transfer Protocol
GoS	Grade of Service
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IEEE	Institution of Electrical and Electronics Engineering
IP	Internet Protocol
IPFIX	Internet Flow information Export
IT	Information Technology
KPI	Key Performance Monitor
LFN	Long Fat Network
M2M	Machine to Machine
MPLS	Multi-Protocol Label Switching

MRTG	Multi Router Traffic Grapher
MTBF	Mean Time Between Failures
MTRS	Mean Time to Restore Service
NPM	Network Performance Monitor
NPM	Network Performance Metric
OPNET	Optimised Network Engineering Tool
OSI	Open Systems Interconnection
OTT	One-way Transit Time
PHP	Hypertext Preprocessor
PRTG	Paessler Router Traffic Grapher
QoS	Quality of Service
RMON	Remote Network Monitoring
RRDTool	Round Robin Database Tool
RTT	Round Trip Time
SAP	Service Access Point
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSL	Secure Socket layer
TCP	Transport Control Protocol
TSC	Technology Support Centre
UFH	University of Fort Hare

UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Chapter one: Introduction

1.0 Introduction

The study analysed end-to-end packet delay and loss rate behaviour in line with network performance at the University of Fort Hare. This chapter introduces the study and the main objectives of the study.

1.1 Background and motivation

Network management techniques have long been of interest to the networking research community and network administrators. A key factor of network management is to increase utilisation of the network and its performance while ensuring availability of services to network users. Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provision of an ideal network system (Clemm, 2006). Network management deals with keeping and maintaining a healthy state of the network. This includes network monitoring so as to identify problems that might affect network performance, reliability, security and smooth business operations. Packet delivery and network reliability are two of the most important aspects in network performance. Several factors affect network performance. These include packet loss, delay rate, throughput, latency and bandwidth utilisation. They all affect the effective performance of a network. In some cases, the network may not work at all; in others, it may be slow or unusable. As a result, applications running over the network suffer thus poor service delivery.

Several studies have dealt with network performance (Jan, 2010; Bubley, 2011 and IDATE & UMTS Forum, 2011) and indicated that data volumes are growing explosively, stimulated by smartphones and attractive flat-rate data services. With social media and other new services gaining attraction, such as cloud computing and machine to-machine (M2M) communication, the resulting deluge of data traffic will pose a challenge and risk to administrators in offering a compelling customer service unless they manage networks properly (Lee, 2011). While pressured to exercise lean network management methods, network administrators have to approach this management mode wisely, as cutting costs and resources at the expense of service quality can backfire and result in poor service delivery. Previous researchers considered the impact that network metrics such as packet loss, delay, and jitter have on network performance (Shah, Harris & Gutierrez, 2002). They analysed the degradation of the quality that network traffic experience by monitoring each individual network metric separately. They observed that in some scenarios (off peak and peak hours), different network metrics change simultaneously and consequently, their combined effect has a specific bearing on network performance. Some network metrics such as packet loss and network delay change simultaneously when networking devices (routers, switches etc.) that interconnect different networks start experiencing increased levels of congestion. Consequencely, to account for these conditions it is sometimes necessary to go beyond the individual variation analysis of each metric and analyse the impact of the simultaneous variations caused for example by packet loss and delay. Therefore it is important to understand and analyse the level of correlation that exists between packet loss and network delay as a consequence of congestion and to study the impact of this correlation. Stevens (1998) analysed the correlation between packet loss and network delay taking into account that such events occur in sequence (for example delay precedes packet loss and packet loss precedes delay). In this approach, Moon (2000) establishes the analysis considering that from an event perspective, when a packet is dropped from the buffer (for example the packet is lost) then its delay cannot be determined. Therefore it is necessary to quantify the correlation between packet loss and delay using a metric that conditions network delay to the occurrence of packet loss. Based on the previous work that has been done by the researchers as singled out above, this study identified possible factors and bottlenecks affecting the network performance at the University Fort Hare and proposed possible network management techniques to improve its performance.

UFH network is faced with high bandwidth usage see appendix 2. Even though a bandwidth control mechanism was deployed at UFH (Forefront Threat Management Gateway of 2010), students still manage to bypass such mechanisms and access blocked sites to download movies, music and games. From our on-going observation we observed that students make use of BitTorrent, Gnutella, eDonkey, and other file sharing programs to download and share files. Such programs come with high bandwidth implications. Literature shows that (Enterasys Networks, 2011) torrents traffic is estimated to account for 17.9% of all internet traffic. Nearly two-thirds of this traffic is estimated to be non-pornographic copyrighted content shared illegitimately. Such traffic largely consists of films, television episodes, music, and computer games and software (about 63.7% of all bittorrent traffic or 11.4% of all internet traffic). Hence there is need to deploy other mechanisms deployed to counter illegal access to blocked sites. Such mechanisms should involve the use of more than one bandwidth control mechanisms. This kind of setup will help to contain any kind of loopholes that might be available. In addition, a quota system should be alongside the bandwidth control mechanisms. The quota system should strictly allocate each student a specific amount of bandwidth for a period of two weeks. Our investigation revealed that the student population at UFH has been increasing faster than the network's bandwidth.

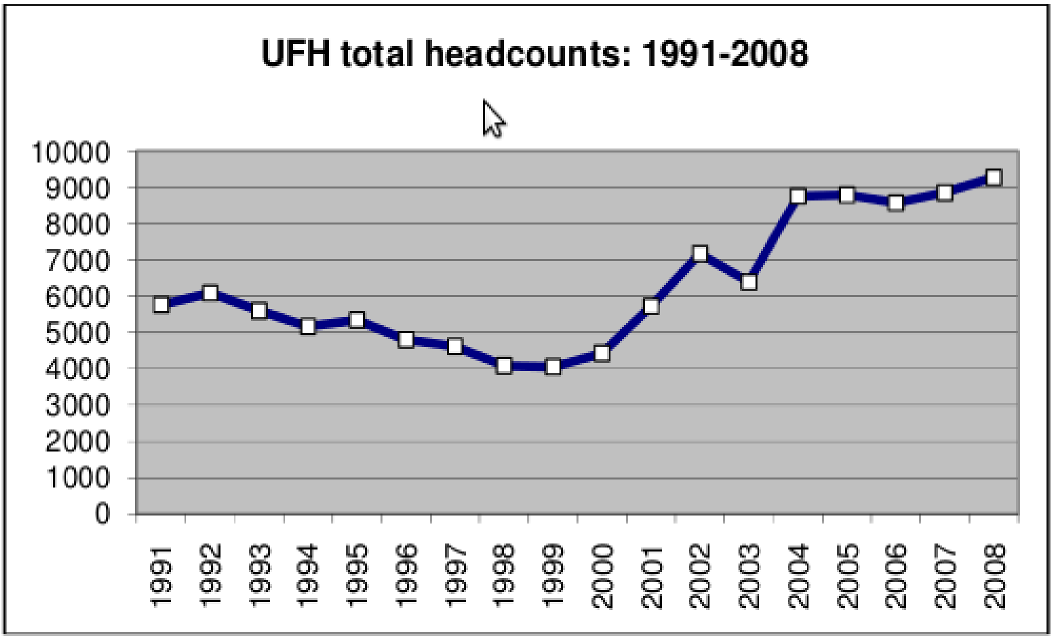


Figure 1. 1: UFH total headcounts

Figure 1.1 shows a gradual increase in the learner numbers at the University of Fort Hare over the past 10 years. It is implied that such a trend can have congestion implications on the university network devices, which have not been expanding. UFH network for example lacks a distribution layer that can be a limiting factor on expanding the current network system. This design of the network compromises modularity and it disallows replicating design elements as the network grows. Literature suggests (Enterasys Networks, 2011) that availability can be increased through redundant implementations with hierarchical networks. Having a distribution layer can allow UFH's current access layer devices to connect to different distribution layer switches and thus ensure path redundancy, which is lacking at UFH. Redundancy helps to ensure that when the distribution layer switch fails, the access layer switch can connect to the other distribution layer switch as an alternative path.

1.1.1 UFH network Infrastructure

The UFH network consists of the following layers:

1.1.1.1 The Core layer

Figure 1.2 illustrate current hierarchical network design model of University of Fort Hare, which consist of core and access layers. This section discusses how the core layer of the UFH network is structured. A core layer is considered as a backbone of the network and ideally it includes the high-end switches and high-speed cables such as fibre cables. It is called backbone only because all other layers rely upon it. This layer is capable of regulating several network functionalities even though it does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed, ensures reliable delivery of packets and it is important for the core to be highly available and redundant. Figure 1.2 illustrates how various departments, administration offices and computer labs at UFH are interconnected using a core layer. In this figure, the core switch with device name UFH-ACOREC1S1 serves as the backbone for the University of Fort Hare network. Figure 1.3 represent a Catalyst 6509 switch that provides a variety of high density ports that support many different wiring technologies, distribution, and core network as well as data centre deployments. This device belongs to Cisco Catalyst 6500 Series end-to-end operational consistency benefits. It supports all Cisco Catalyst 6500 Series modules, including:

- Supervisor engines
- Fast Ethernet modules (with IEEE 802.3af Power over Ethernet [PoE])
- Gigabit Ethernet modules (with IEEE 802.3af PoE)
- 10 Gigabit Ethernet modules
- Flex WAN modules
- Shared Port Adaptors/SPA Interface Processors

- Multi-Gigabit services modules (content services ,firewall, intrusion detection, IP Security [IPSec], VPN, network analysis, and Secure Sockets Layer [SSL] acceleration)

In addition, Cisco Catalyst 6509 provides maximum uptime with redundancy and rapid (1 to 3 seconds) state full failover across supervisor engines. It supports modular Cisco IOS Software to minimize unplanned downtime through self-healing processes and simplifies software changes through subsystem in-service software upgrades.

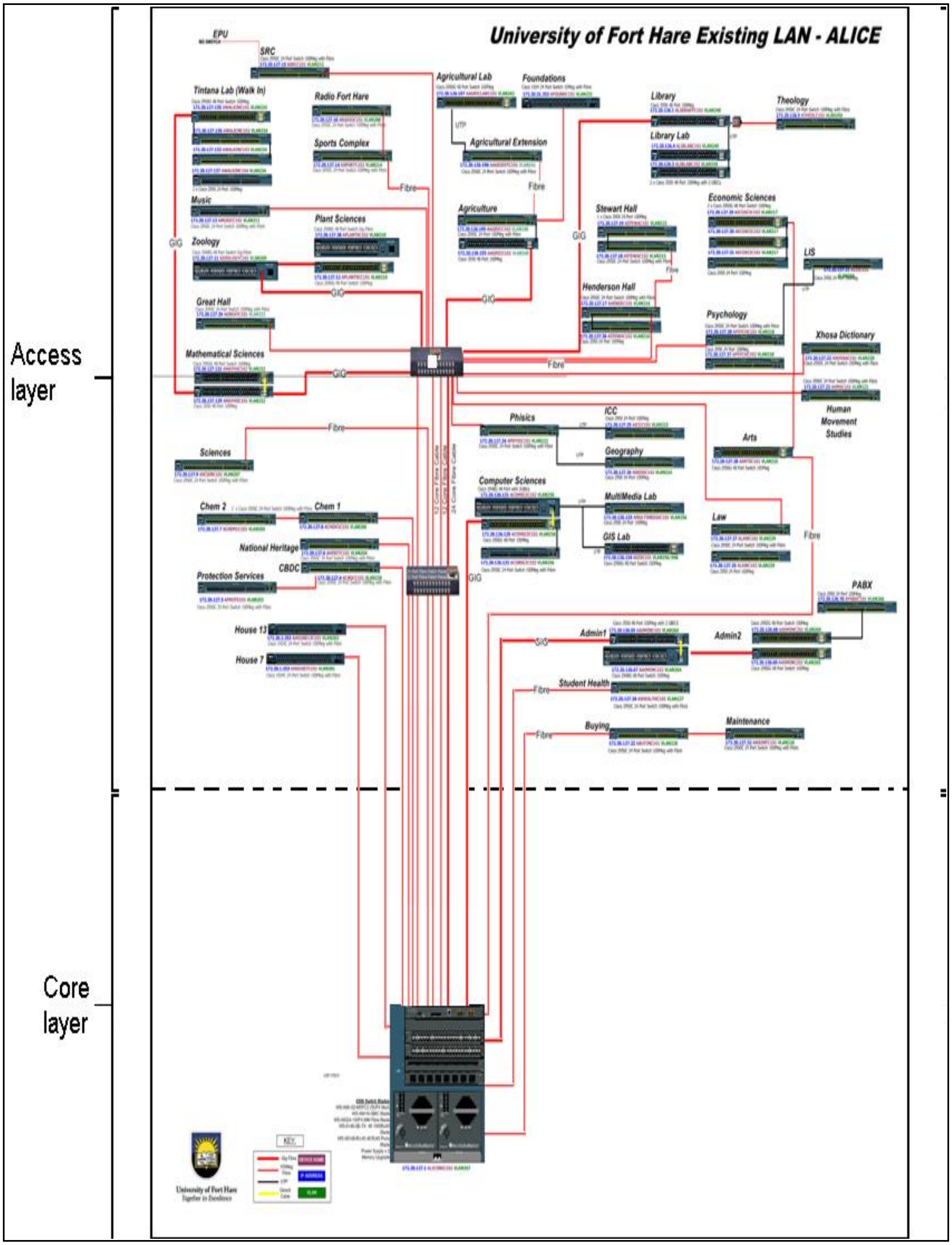


Figure 1. 2: Network infrastructure of UFH Source: UFH TSC

In order for this device to serve the University of Fort Hare network in its daily operations it needs to be fast and extremely resilient because every department, administration office and computer lab depend on it for connectivity.

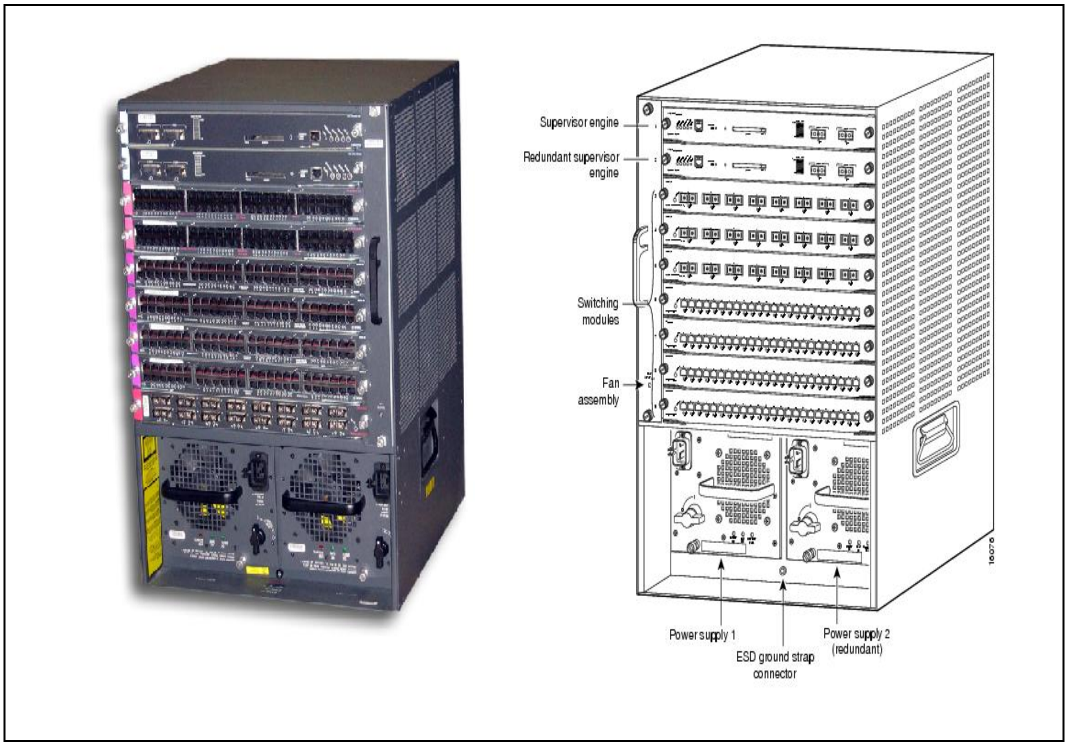


Figure 1. 3: Catalyst 6509 switch Source: University of Fort Hare TSC

1.1.1.2 The Access layer

The access layer is the first point of entry into the network for edge devices, end stations, and IP phones as shown in Figure 1.2. Ideally switches in the access layer are supposed to be connected to distribution layer switches for redundancy. If a connection between the distribution layer switches consists of an L3 connections, then there are no loops and all uplinks actively forward traffic.

1.1.1.3 Great Hall Overview

1.1.1.3.1 Great Hall Network Components

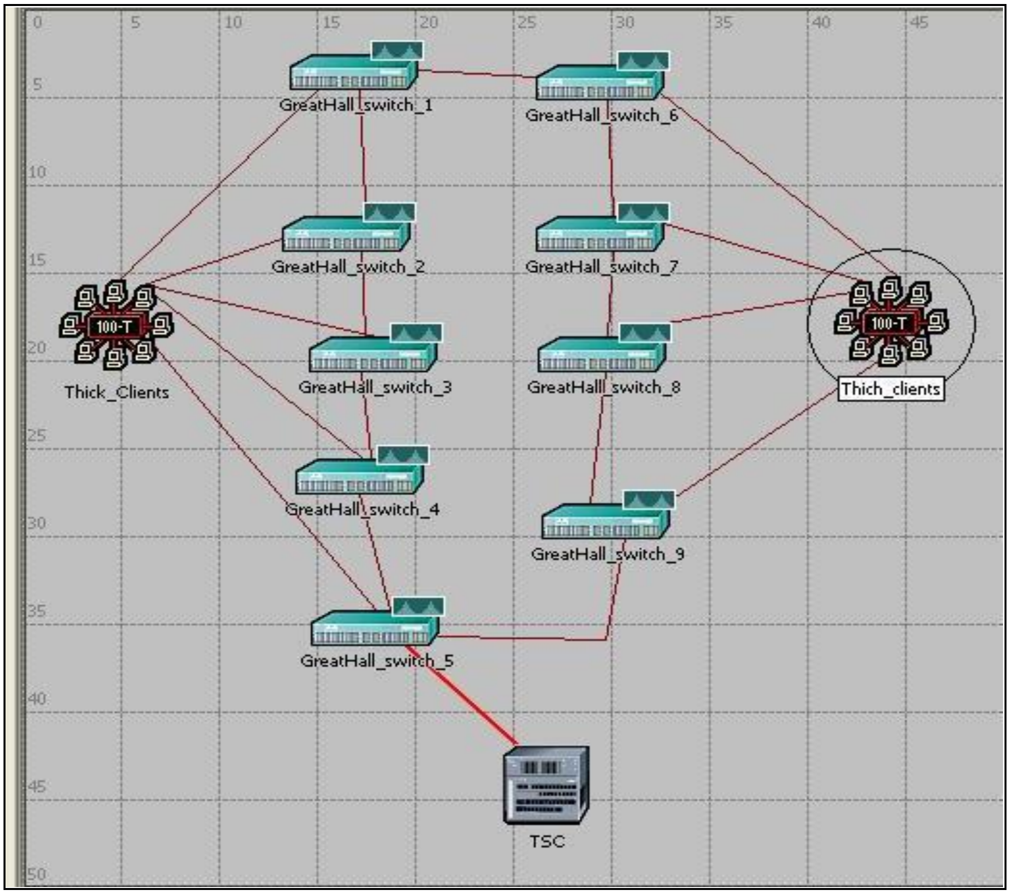


Figure 1. 4: Great Hall stackable switch

The Great Hall is the University's building that houses many computers. It contains 350 thick client computers connected to the stack switches using Cat 6 Unshielded Twisted Pair (UTP) cable. Cat 6 cables are mainly designed for gigabit rated networks. GreatHall_switch_1 to GreatHall_switch_9 represent a stackable switch, which is of machine type Catalyst 37xx stack. This stackable switch represents a group of 9 individual switches functioning as a single switch that assumes the port capacity of all the 9 switches combined. Figure 1.5 shows the physical structure of the traditional stackable switch representing GreatHall_switch_1 to GreatHall_switch_9 combined.

Figure 1. 5: Stackable switch

Communication between Great Hall and TSC is through a 1 gigabit link, ideally Great Hall is supposed to be Gigabit Ethernet. Cat 6 communication channels are much faster than other channels used in most of the labs and administration offices around campus. Instead they happen to use Cat 5 UTP cables with a maximum speed of 100Mb/s. The connections in the labs and offices operating at a speed of 100MB/s are referred to as fast Ethernet. Cat 6 is far much better than Cat 5 because of its structural difference in a form of longitudinal separator. This longitudinal separator is the difference between Cat 5 and Cat 6 cable. Longitudinal separator decreases crosstalk, allows faster data transfer and it gives Cat 6 cable twice the bandwidth of Cat 5.

1.2 Problem Statement

In recent years, network users are demanding anytime and anywhere access to high-speed internet services. On the other hand, network management has become more sophisticated as more and more network management techniques are developed. Network administrators are dedicated to offering an efficient network system that can provide a stable end-to-end network QoS (Quality of service). Despite the network management efforts, various challenges to provide the end-to-end QoS requires advanced or special knowledge and management techniques to monitor computer networks (Foster *et al.*, 2004). This is because of rapid change in network bottlenecks. One of the known bottlenecks is congestion. As a result of congestion, the network performance becomes degraded, making it very difficult to access the Internet and other network resources. Network congestion occurs when a link or node is transporting too much traffic such that its quality of service is compromised **(**Moon *et al.*, 1998). Typical effects from congestion include network delay and packet loss that could result in poor Internet services or collapsing of the entire network. From our initial investigation, the main problem at Fort Hare University is that the network is highly congested. This results in high packet loss and delay rates. A constrained network performance has major implications on access to information. Network availability is of great concern at University of Fort Hare community. Reliability and network efficiency are other network performance problems that are of great interest to the UFH community. These problems are caused by minimal knowledge of network management, frequent power cuts, poorly structured networks, and use of old network infrastructure. It is therefore necessary to review the University of Fort Hare network infrastructure, investigate and analyse specific performance metrics so as to propose new network management techniques, which will control and determine how network resources are utilised. Improved network performance at the University of Fort Hare will go a long way in improving the academic performance of the students as students will be using a reliable Internet services as an alternative source of information.

1.3 Research Objectives

This research aimed at investigating the correlation between packet delay and loss rate in relation to network performance at the UFH network.

The specific objectives:

I. To investigate the network performance metrics and factors affecting network performance in order to find out how network services can be fully utilised on the University of Fort Hare Network;

II. To identify and evaluate the current network management techniques being used to improve network performance
III. To recommend on how to improve the current network performance management techniques.

1.4 Research Questions

In pursuing our research we considered the following research questions:

I. What are the network performance metrics and factors affecting network performance at the University of Fort Hare?
II. What are the current network management techniques being used to improve network performance at the University of Fort Hare?
III. What needs to be done in order to improve the current network performance management techniques at the University of Fort Hare?

1.5 Justification

An analysis of end-to-end packet delay and loss rate gives an understanding of the network dynamics for many real-time and nonreal-time applications, especially for QoS provisioning and congestion control. It is therefore important in the provision of a more accurate prediction of the end-to-end delay distributions and loss rate characteristics. Understanding end-to-end packet delay and loss rate dimensions will improve the network management techniques and hence network performance and service delivery. We believe that generating information on network performance and identifying bottlenecks can improve UFH's network performance. As a result academic performance can be enhanced since the Internet will increase the volumes of information available to students.

1.6 Methodology

This study collected network data traffic at the University of Fort Hare's network using network-monitoring tools. The following network measuring tools were used: a case study approach method was used employing cacti and Orion as data collection tools. This was followed by empirical approach method of gathering data where scientific decisions were made based on the data derived from direct observation and experimentation. Experiments were carried out in the third phase where the entire network was modelled in order to provide a platform where changes to enhance the network performance can be made. Measurements are necessary for understanding the current system behaviour and also inform the implementation of the new system.

1.6.1 Experiments

After gathering data, experiments were conducted by simulating University of fort hare network traffic using OPNET as our simulation tool. The simulated network was supposed to be observed 8 hours a day. The reason for choosing "8 hours" was because it is the most common number of business hours.

1.6.2 Data analysis

Data from network management tools and data from informal interviews with TSC administrator was analysed and discussed. Recommendations on the changes to be made on the current network setup are given with the hope of enhancing the performance of the current network.

1.7 Outline of The dissertation

The dissertation is structured as follows: Chapter 1 has presented the background to the study and problem statement, objectives, research questions, motivation and research methodology. Chapter 2 presents literature review; that is theory related to end-to-end delay and loss, outlining various methods used to model these parameters. Chapter 3 presents an overview of end-to-end packet delay and packet loss in switched networks. In Chapter 4, we present a discussion of the various network management techniques and subsequently chapter 5 presents the methodology and implementation of the project. Results and analysis of the study are presented in chapter 6. The dissertation ends with conclusions and recommendations in chapter 7.

Chapter two: Literature review

2.0 Introduction

This chapter reviews on the Internet network performance behaviours of both delay and packet loss. It also reviews how delay and packet loss have been modelled and analysed. In addition, the correlation of delay and packet loss, a review of how the end-to-end network parameters collectively affect network performance is also presented. The commonly used network performance characteristics are latency, throughput, response time, arrival rate, utilization, bandwidth, loss and reliability. These metrics are presented in this chapter and we also make an overview of the current research trends in the field of network performance monitoring.

2.1 Network Performance

According to SolarWinds (2010) network performance focuses on the availability of a network to the network users. However availability on its own does not fully portray network performance. It can therefore be noted that network availability falls under the network performance umbrella, i.e. the degree in which the network is operable and also how it is conveyed through network metrics (Liotine, 2003). The overall Network performance is affected by a number of factors to which consistency stands out as a major factor. Consistency refers to the provision or to maintain a same network performance over a given period. It enables network administrators to foresee and respond to various network behaviours (Liotine, 2003).

Network behaviour is monitored by collecting and storing baselines. Network baselining is the process of measuring and evaluating the performance of a network in real-time (El-Hassany et al., 2010). The moment this information is collected, it is used as a benchmark to compare and analyse with other network traffic scenarios (El-Hassany et al., 2010). This is achieved by the use of network analysis tools that are used to develop a baseline for a network. Examples of such tools are Paessler Router Traffic Grapher (PRTG) and Multi Router Traffic Grapher (MRTG). By so doing, network baselining offers network administrators with insight into anticipated behaviour of the network and most importantly, awareness to the environment changes. Generally, it is thought that when there is high-quality traffic, it is assumed that everything is running perfectly. This assumption may be in actual fact incorrect (El-Hassany et al., 2010). Initial understanding of the network behaviour is therefore important in offering immediate solutions to problems that arise. Henceforth, baselining seems fit as a way that makes it easier to identify causes of abnormal network behaviour.

2.1.1 The need to measure network performance

As a tool, network performance measurement is a standalone factor when it comes to collecting information for the following purposes:

- Network performance analysis of throughput, Quality of Service (QoS) performance metrics and testing of new technologies and applications.
- Review of network properties such as traffic, path, and link characteristics.
- Developing network monitoring and fault detection mechanisms.
- Decision-making schemes – e.g. future expanding of networks, traffic engineering, routing, Connection Admission Control (CAC) (Calyam, 2005).

The necessity for measuring network performance metrics to support operations, management and planning of networks has become network administrator's nightmare (Calyam, 2005). This is because managed Internet Protocol (IP) networks are dominating in the way information is conveyed to users on a worldwide scale. IP networks are no longer confined to transferring data but are also the carrier for multi service operations (Hasib & Schormans. 2003).

Most of the latest applications require massive data throughput (bandwidth) with specific performance requirements (Moon, 2000; Dahal & Saikia, 2003; Martin et al., 2000);

(Ramakrishnan et al., 2001). As a result, without measurements, there will be no benchmark of how a network performs. Measurements therefore show whether deviations improve or reduce the network's performance, and by how much (Floyd and Henderson, 1999). When QoS declines, the following questions give the network administrator and users headaches (Garcia-Luna-Acevesand Parsa, 1999):

- Why is/are application(s) responding slowly?
- Why there is loss of data?
- What measures to take to improve performance?
- Will an increase of bandwidth be of use?

With such questions in mind, there is a need to collect network data with the use of network measuring tools in order to provide solutions to these questions. With the help of collected network data network administrators can take necessary precautions, in order to avoid congestion in the network. Reduction in performance may cause long packet delay time, jitter or larger packet loss ratio. Network measurement is essential to keep track of the network performance and thus analyse, identify and fix any errors that are or might occur. Figure 2.1 illustrates the common network performance metrics.

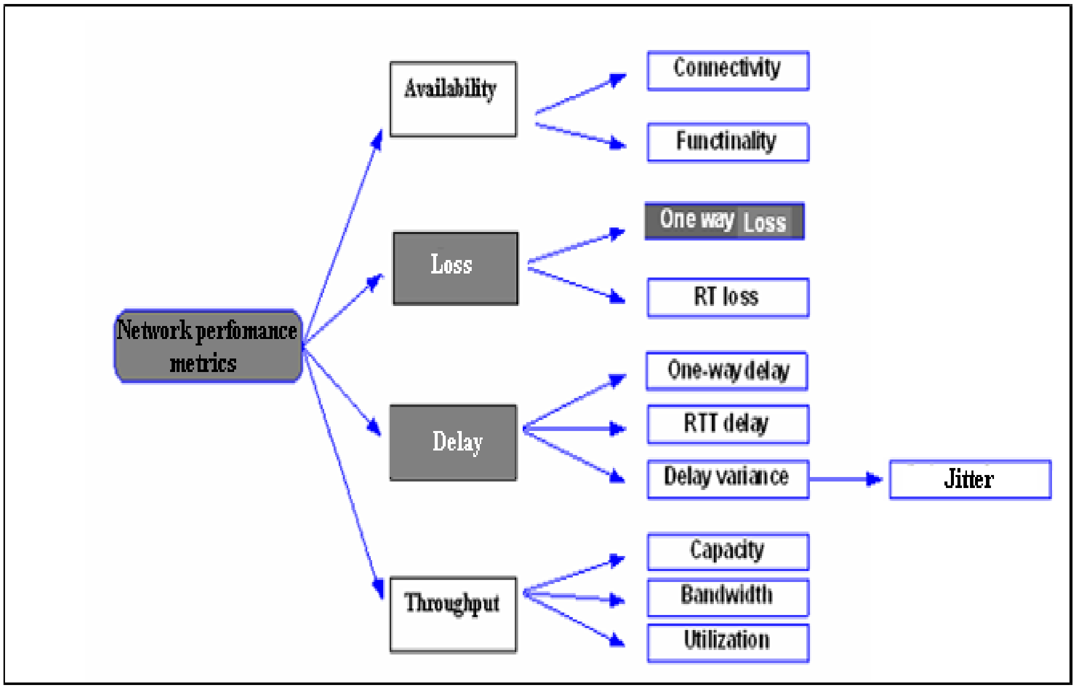


Figure 2. 1: Common network performance metrics.   Source: Maheen, 2006

These metrics are availability, packet loss, delay and throughput. Network performance measurement may be collected in order to analyse such metrics.

2.1.2 QoS Parameters for Network Service

QoS metrics represent the quality of service to network users. It enables users to understand the degree of assurance to service. QoS metrics are different according to the type of services they provide. The following are the general QoS metrics required in network service: availability, delivery, latency, bandwidth, mean time between Failures (MTBF) and Mean-Time to Restore Service (MTRS) (Hong et al., 2001). In a data network environment, availability is the ratio of the feasibility of service in every specific service request (Hong et al., 2001). Hong et al., (2001) defines availability of service as the key metric that users are focused on; in other terms users demand availability/presence of service all times when required. Delivery is the opposite of packet loss, which means that a percentage of each service is delivered without packet loss (Hong et al., 2001). Some service such as QoS and GoS etc. define delivery as packet delay. This type of service lies on how individual service providers define delivery (Hong et al., 2001). Latency would be the time taken for a packet to travel from a Service Access Point (SAP) to a distant target and back (Hong et al., 2001). This usually involves the time it takes to transmit the service and queuing delay. Bandwidth refers to the Network Performance Metric (NPM) which is the core metric of performance measurement in the Network Management (Hong et al., 2001). It includes values such as availability, loss, delay and utilization. Availability is the connectivity and functionality in the network management layer. By connectivity we refer to the physical connectivity of network elements and by functionality we refer to whether the associated network devices work well or not. Loss is the rate of packets lost in transit from sender to receiver during a specific time interval, loss is expressed in percentages. Delay consists of three kinds of factors: one-way delay, round trip delay and delay variance. Utilization is the throughput for the link expressed as a percentage of the access rate.

2.1.3 Network performance metrics

Two important parameters which are affected by network behaviour are end-to-end delay and packet loss (Bolot, 1993). Since the Internet is a “best effort” network which does not provide any guarantee on delay and loss, transport protocols typically use these parameters to monitor the network in order to determine the congestion status.

A “best-effort” network relies on certain principles which are: there is no traffic that is denied entry to the network, all packets are treated in the same fashion, and the only guarantee given by the network is to deliver every packet as quickly as it can, without undertaking to treat any class of packets preferentially to any other given the available resources (Lehman et al., 2006). This means, there are no artificial delays that will be created, and no unnecessary losses will be experienced. The best-effort service is sufficient as long as the applications using the network are not responsive to jitter (packet variations in delay) and loss rates.

2.1.3.1 Packet delay

Delay variation which is best known as jitter is the most vital and complicated element of network behaviour to examine as noted by Pathak et al., (2008). In delay there are many possibilities in the time required for a packet to complete the path from the source to destination. In addition, delay variation is the core source of information about the network. The time taken for a packet to be transmitted from the source to the destination is defined as the One-way Transit Time (OTT) and is given by:

$$OTT = \Sigma\ (Tn + Pn + D\ n + Q\ n) \qquad (1)$$

In equation (1), T denotes the transmission delay, P is the propagation delay, D is the processing delay, Q is the queuing delay and n is the number of nodes from the source to the destination. Transmission delay is the time taken for the whole packet to be transmitted across the path. This also relies on factors such as the link's bandwidth and the packet size (Zeitoun et al., 2003). Demichelis (2000) defines propagation delay as the time taken to transmit bits along a communication link; this is affected by the link's length and the speed of propagation. For example bits transmitted over a fiber link will be faster than those transmitted over copper link.

Processing delay is the time taken to process each packet and prepare it for transmission, whereas queuing delay is the time a packet spends queued in the router's buffer before being transmitted to the destination or next hop. The transmission and propagation delay are influenced by the primary network infrastructure and have least variation. The smallest time for the end-to-end transmission of the packet, the inherent delay, consists primarily of these two deterministic components and is usually very close to their sum (Demichelis, 2000).

Moreover, these metrics are determined more by the network topology than the network load (Zeitoun et al., 2003). Overall, the variation in delay is primarily a result of the processing and queuing delay. Between processing delay and queuing delay, queuing delay is mostly influenced by network conditions; hence it contributes most to delay variation. A delay measurement used in TCP and other similar transport protocols for congestion control and retransmission mechanisms is the RTT. RTT values are taken per segment and segment RTT is defined as (Corner, 2000):

$$SegmentRTT = Fdelay + Ddelay + Adelay \qquad (2)$$

Fdelay represents OTT resulting from a packet travelling from the source to the destination. Ddelay is the processing delay at the destination. A-delay is OTT arising from acknowledgement (ACK) travelling back from destination to source. According to Acharya & Saltz (1996) Internet round trip delays can be either temporal or spatial variations in RTT. Delay behaviour varies a lot, influenced by factors like; the time of the day as well as the physical or geographical distance between the communicating parties. RTT values have been shown to follow a unimodal asymmetrical distribution which is skewed towards the right.

2.1.3.2 Packet Loss

Packet loss happens when one or more packets of data being transmitted through a computer networks do not reach their intended destination (Arai et al., 1996). Packet loss usually arises from: 1) a buffer overflow at intermediary nodes which might result in congestion, and 2) bit errors, like those caused by interference such as noise (corrupted packets rejected in-transient (Arai et al., 1996), 3) faulty networking hardware, 4) faulty network drivers or normal routing routines (such as Dynamic Source Routing (DSR) in ad-hoc networks) and also 5) distance between the transmitter and receiver (Allman et al., 1999). Though, packet losses caused by bit errors such as noise are not a norm on high bandwidth and wireless networks. Packet loss recognition is typically used as a feedback mechanism to show congestion on the network link. Such event is triggered by transport protocols to request the sender to adapt its sending rate accordingly (Biaz & Vaidya, 2003).Transport Control Protocol (TCP) and its variants are designed in a manner where they assume that all losses are result of congestion (Allman et al., 1999), and adapt their transmission rate to suite the required rate. In case of congestion, not only does the sender have to decrease its sending rate in order not to prolong the congestion, it also has to resend the lost packet. Apart from loss event occurrence, packet loss can be characterized by loss distance and loss length (Koodli & Ravikanth, 2002). Loss distance denotes the amount of packets between consecutive loss events, while loss length is the number of packets lost per event. From the loss distance, it can be witnessed how often loss events occur. A small loss distance shows that losses are close to each other and occur after short intervals, which might suggest possible congestion (Koodli & Ravikanth, 2002). The loss length, on the other hand, indicates the nature of the loss event that is whether it is a single-packet or a bursty loss. Single-packet losses generally occur to link or transmission errors, however bursty losses are expected to be congestion-related.

2.1.4 Network performance management

Computer networks are different according to the user or client day to day services, operations and business needs. Though, they follow the same approach when it comes to end-to-end transmission of data. As data is broken into component parts called segments, packets, and frames respectively to their Open Systems Interconnection (OSI) layer of belonging for transmission according to Saltzer et al., (1984) delivery depends or may be affected by a number of factors such as:

- Delay - where packets take longer to be delivered from the other end to the other end of interconnected networks. In an environment with reliable protocols in place where a destination host acknowledges delivery of data, it becomes possible to measure such RTT round-trip time events.
- Packet loss - in other network scenarios, network devices will lose packets. This happen as a result of errors, network devices becoming congested, due to deliberate discarding of traffic in order to enforce a particular service level.
- Retransmission - when packets are lost in an efficient network environment, retransmission occurs to counter act lost packets. This invokes two delays which

are: firstly the delay from retransmission of data; and secondly, the delay caused by waiting for data to be received in the correct order before forwarding it up the protocol stack.

- Throughput - which is the amount of traffic a network can carry, usually measured in kilobits per second. Throughput follows the same idea as road network, where one can picture it as the number of lanes on a highway, whereas latency is similar to its speed limit.

The above highlighted factors and others such as network signal strength on the end user devices, compression, encryption and concurrency, etc. affect the efficiency and consistency of network performance. In some circumstances, the network may not function completely, or it may be slow or unusable. Since applications run over these networks, application performance may suffer. Numerous intelligent solutions are available to make certain that traffic over the network is effectively managed to enhance performance for all users. Solutions such as International Business Machines (IBM) Solution that tracks and enhances network performance for customer's needs and Savvis solution that lighten customer network resource load and keep user information flowing by providing network solutions that enhance application performance and deliver the flexibility that users need to increase network capabilities as they grow.

Network performance management comprises of measuring, modelling, planning, analysing, and improving networks giving assurance that network will deliver speed, reliability, and capacity that is suitable for the nature of the application and satisfactory user experience. Various applications warrant different blends of capacity, latency, and reliability. For instance: streaming video or voice can be unreliable but needs to have very low latency so that holdups don't occur. Big file transfer or e-mail must be reliable and have high volume, but doesn't need to be instantaneous. Instant messaging doesn't consume much bandwidth, but should be fast and reliable.

2.1.4.1 Network performance management tasks and classes of tools

Network Performance management enables the network administrators to proactively prepare for degradations in their infrastructure and eventually improve the end-user experience. Network administrators accomplish many tasks; these include performance measurement, forensic analysis, capacity planning and load-testing or load generation (Frey, 2009). They also work hand in hand with application developers and Information Technology (IT) departments who rely on them to deliver underlying network services.

For performance measurement, administrators normally measure network performance at different levels. They either use per-port metrics which is the amount of traffic on port 80 sent between a client and a server and how long did it take; or they rely on end-user metrics such as the response time on login page load. Per-port metrics are collected using flow-based monitoring and protocols such as netflow standardized as Internet Protocol Flow Information Export (IPFIX) or Remote Network Monitoring (RMON). End-user metrics are collected by means of web logs, synthetic monitoring, or real user monitoring. Such an example is application response time (ART) which provides end to end statistics that measure QoS. For network troubleshoot purposes, administrators regularly depend on sniffers that break down the transactions by their protocols and can locate problems such as retransmissions or protocol negotiations. For performance ability planning, modelling tools such as Optimized Network Engineering Tool (OPNET), MATLAB, PacketTrap, Zyrion Traverse, Riverbed Cascade, Scrutinizer NetFlow and sFlow Analyser, or NetQoS that simulate current network setup behaviour and contributes to network performance enhancement decision making are used (Frey, 2009).

2.1.4.2 The role of network management tools

Network management first approach to managing network performance requires an understanding of the relationship between network utilization and application performance. Network Performance tools give administrators insight into this relationship with an integrated view of performance metrics that include end-to-end performance such as loss and delay, traffic analysis, Voice over Internet Protocol (VoIP) quality, and device performance from this intuitive, web-based network performance management console such as Cacti which is currently employed at University of Fort Hare. By using *Cacti* and other network management tools network administrators can access a top-down view of all applications such as data, video, and voice of the entire network (Hewlett-Packard Development Company, 2005).

According to (Hewlett-Packard Development Company, 2005) network performance tools offer network-specific views for different subnets in an organization, such as network engineering, operations, and voice management to enable administrators at all levels to:

- Measure end-user application response times
- Track VoIP quality metrics to ensure VoIP quality of experience
- Understand how changes affect network and application performance
- Isolate performance problems to the application, server, or network
- Identify the applications and users consuming bandwidth
- Avoid unnecessary Wide Area Network (WAN) costs
- Manage the convergence of voice, video, and data
- Identify virus or denial of service attacks

Network Performance tools also provide an integration platform that works with other third-party applications. Administrators can export any network Performance view to any third-party Web-based application with just a few mouse clicks. In addition, network performance tools contain a publishing platform to display data from any third-party application (Hewlett-Packard Development Company, 2005).

With Network performance tools, network administrators can make more informed decisions based on precise usage of data from a network. They also minimize cost through staff efficiency and collaboration by deploying a single tool to resolve performance issues rapidly. Network performance tools allow reduction of risks resulting from changes on networks such as VoIP deployments, multiprotocol label switching (MPLS) migrations, QoS policy implementations, and application roll-outs.

In this study major focus shall be emphasized on the *Cacti* platform, the reason being that *Cacti* is the network performance monitoring tool that is currently used at UFH where the case study is done.

2.1.4.3 Importance of modelling performance

Performance is about user satisfactory provisioning. To deliver ideal network performance, network administrators should have a clear view of how the network will perform and behave prior the implementation of new changes. In order for these new implementations to become a success, efficient network modelling techniques have to be put in place. In addition, network administrators need to know the importance of network modelling for the success of the proposed network system.

Network modelling is the process of producing a network model; a network model represents the construction and working of the current network setup (Güne et al., 2010). It can be noted that a network model is not the real world operational network but a man-made representation of the real world network to help us better comprehend real world network systems (Güne et al., 2010).

A network model scenario is similar to but with much less complexities than the actual network it represents. A major objective of a network model is to enable network engineers to foresee what would be the effect of changes to the current or proposed network system (Güne et al., 2010). In addition, a network model should give a clear view, a mirror like image to the real world system and it should include most of the real world network's prominent features. Furthermore, its design should not be difficult as it makes it impossible to understand and experiment with it. A good model contains a sensible adjustment between realism and simplicity. In order for network engineers to master the modelling process it is recommended that they increase the complexity of a model iteratively (Güne et al., 2010). A key issue that network engineers should take note of in modelling networks is model validity. Model validation methods include simulating the model under known input conditions and comparing model output with system output (Güne et al., 2010). Generally, a network model designed for a simulation study is developed with the help of network simulator software such as OPNET, ns2/ns3 and NetSim.

There are two forms of simulation; which are discrete event simulation and continuous simulation (Güne et al., 2010). Discrete event simulation is much simpler to implement and hence it is an ideal choice for this study. Furthermore, it is used in a wide variety of situations. In a discrete simulation study, network administrator decision making is essential at all stages, that is, model development, experiment design, output analysis, conclusion formulation, and making decisions to change the network system under study. The only stage where the administrator's input is not necessary is when running the simulation, if OPNET simulation software packages perform efficiently. A network simulator is a piece of software or hardware that predicts the behaviour of a network, without an actual network being present (Güne et al., 2010).

The key point is that powerful simulation software is hardly a destructive factor - its absence can hurt a simulation study but its presence will not ensure success. Experienced problem formulators, simulation modellers and analysts are crucial for a successful simulation study. Figure 2.2 is a diagrammatic illustration depicting how a simulation of a particular event being studied can be done.

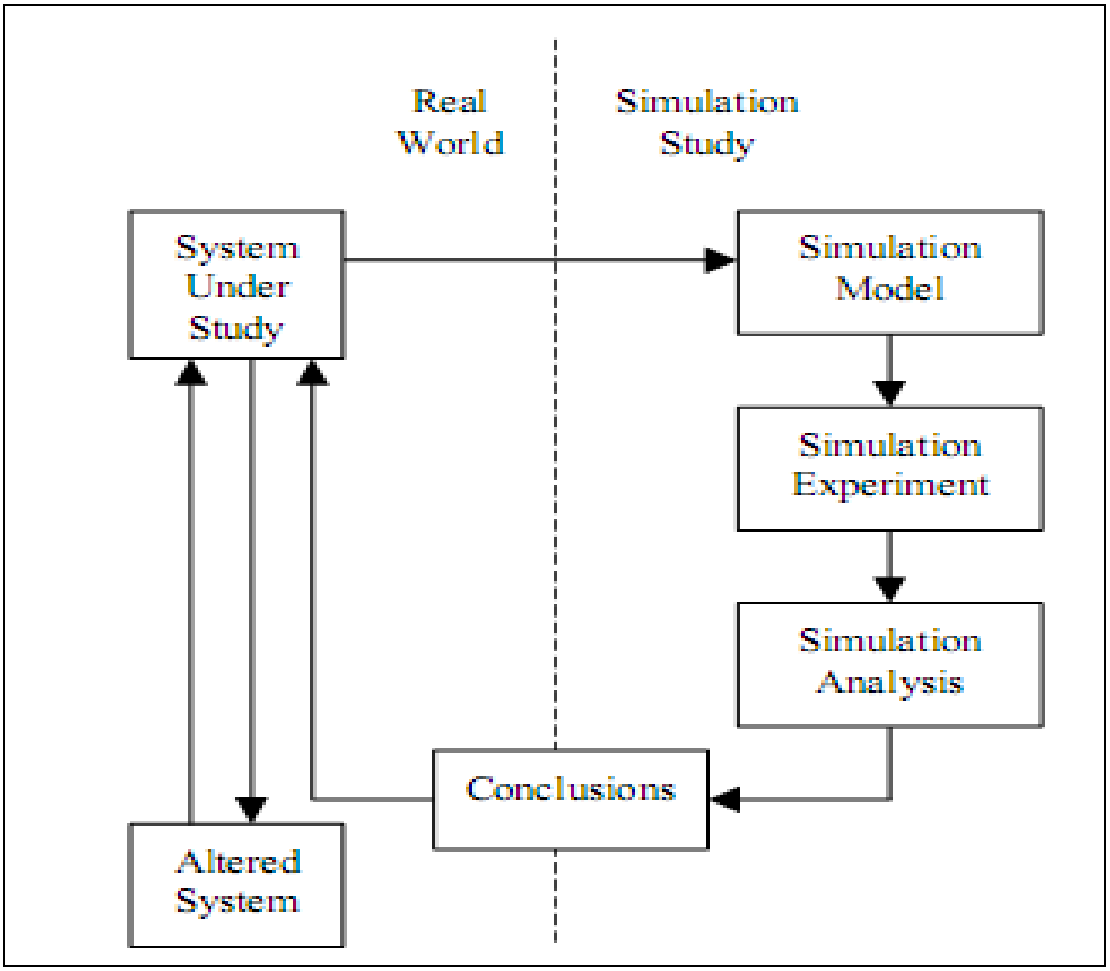


Figure 2. 2: Diagrammatic example of a simulation of a study. Source: Maria, 1997

Network Modelling is the viable method as far as network management and network performance is concerned. This has been noted on previous network studies (Maria, 1997). This study also focuses on similar modelling process so as to build the University of Fort Hare Network Model.

2.1.4.3.1 OPNET simulation and services

Alain Cohen, in collaboration with his brothers Marc and Steven Baraniuk, initiated MIL 3, Inc. in 1986 (OPNET 1.1) In 2000, MIL 3, Inc. evolved its name to OPNET Technologies, Inc. (OPNET 7.0). Currently, OPNET Technologies, Inc. is a supplier of software products and services renowned for (Dunaytsev, 2010):

- Network planning and engineering
- Application performance management
- Network research and development

OPNET Modeller refined stylish tool that offers analysis and modelling of network performance. The most popular version is OPNET modeller 11.5 in particular which was used on this study can simulate a wide variety of different networks, which are interlinked (Informer Technologies, 2012). Network engineers can work from their PC to simulate different networks and study visually the behaviour and impact of various factors such as end-to-to delay, loss rate, bandwidth, data rate, etc. on the network (OPNET Technologies, 2012). OPNET modeller has a very user-friendly and easy to understand graphic interface. OPNET Support a variety of platforms which are: Microsoft: Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows 7 and Linux: Red Hat Enterprise and Fedora.

OPNET enable network administrators to anticipate network management issues and allow administrators to enhance the performance and reduce the availability of communication networks and networked applications. OPNET combines predictive simulations and a comprehensive understanding of networking behaviour to enable network experts to effectively design and deploy networks, diagnose network and application performance problems, and foretell the impact of proposed network modifications.

2.1.5 Network traffic management

As University of Fort Hare will have future expansion of the network, there will always be a need to add new network applications, support remote users, implement different types of network traffic, and extend to more campuses, having complete view into an infrastructure's behaviour becomes ever more important and challenging. More than ever, straightforward and effective traffic management from the network core to the network access layer is critical to the University of Fort Hare’s network success.

2.1.5.1 The Importance of network traffic management

Networks have evolved from a transport mechanism to a strategic business tool for many organization including universities. This evolution has been brought into life by components such as the Internet, an increasingly mobile workforce, and the ability of multiple types of data traffic running through the same network (Hewlett-Packard Development Company, 2005). As a result, networks are becoming more public, more extended, and more complex. Network administrators are being forced to understand and create a supporting environment for new applications. In today’s connected business environment, straightforward and effective network management from the network core to the network access layer is essential (Hewlett-Packard Development Company, 2005). Network users need a network infrastructure that scales to meet their changing needs and network that manages addition of network services in an effective manner. In addition, network administrators are expected to control the network in such a way that it is transparent to users. Essential information need to be instantly available around the clock. However, it is impossible to achieve this without the right management tools to make well-informed decisions. Most network administrators do not have simple, affordable tools that can quickly answer the following questions, regardless of the size of the network:

- Is network performance reducing or becoming congested?
- What is the current network utilization, and what has it been in the past hour?
- Which network routers are most active or over-utilized?

- Why is a server slow or inaccessible?
- Which users and applications are driving network traffic?
- Which users and applications are starving for bandwidth?
- How much bandwidth is required for new applications?

2.1.5.2 Types of Network Traffic

Nowadays networks are required to accommodate a variety of complex data traffic. Network traffic management tools allow network administrators to pinpoint different types of network traffic, a variety of requests from users and traffic from a wide range demanding network applications. In addition, network management tools facilitate network optimization and enable network components to interact appropriately. In order for network administrators to achieve network optimization they have to understand where inefficiencies and problems are occurring, and what causes such occurrence. The integration of various standards and technologies, such as RMON and sFlow combined with effective traffic management software tools, such as ProCurve Manager Plus, *Cacti*, netFlow, enable administrators to effectively support various traffic types with optimum fault occurrence, performance management, and capacity planning on all ports. The following highlights and illustrates several types of network traffic that need to be managed, considered and supported: Bursty traffic which might result from large file downloads such as FTP, multimedia content that includes .wmv, .swf, .mov file format and graphic content that contain .jpg, .gif file format. Problems associated with such data traffic would result from spikes in bandwidth consumption (Hewlett-Packard Development Company, 2005), effectively starving other applications of bandwidth for a brief period of time but if such starving persist it will result in congestion (Hewlett-Packard Development Company, 2005). Interactive traffic and latency sensitive traffic are vulnerable to problems caused by bursty traffic. To counteract such problems network administrators need to set a maximum restriction that limit access to bandwidth usage.

Interactive traffic with instances such as Secure Socket Layer (SSL) transactions, Instant Messenger and Telnet sessions which all constitute relatively short request/response events, and generally they support real-time interaction with end users. Such traffic is susceptible to competition for bandwidth, which can result in poor and unpredictable application response time. They need to be given a high priority over less essential traffic and traffic that is less dependent on real-time response such as e-mail.

Latency sensitive traffic which includes Streaming applications, VoIP, and video conferencing all generate a steady stream of traffic which utilizes a significant amount of bandwidth. Their problems would be a weakness to competition for bandwidth, which might result in poor and unpredictable application response time (Hewlett-Packard Development Company, 2005). These applications can also easily use available bandwidth, effectively starving other applications (Hewlett-Packard Development Company, 2005). Network administrators could take measures such as configuring minimum guarantees of access to bandwidth prioritizing using business need and objectives, and also configure maximums to avoid any application from consuming too much bandwidth.

Non-real time traffic for Instance, E-mail and Batch Processing Applications are the main sources of non-real time traffic within the network. Problems that may rise can consume bandwidth that might be used by more business-critical applications. Therefore to eliminate such problems administrators need to schedule bandwidth allocation for off-peak hours; configure a maximum bandwidth restriction and low prioritization during peak hours.

2.1.5.3 Network management tools

There are lots of network management tools to choose from ranging from: Open Source and Commercial, Linux/Unix-based and Windows-based Network tools (Cisco, Juniper, Orion, and others) unfortunately there is no precise combination of tools to use for your network. That is why network administrators need to know about most of these network management tools and understand their network needs so as to shape their individual choices of tools. In this study we focused on cacti and Orion as our network management tools.

2.1.5.3.1 Cacti Network Management Tool

Cacti is a frontend Round Robin Database Tool (RRDTool) that stores all the necessary network data. Cacti enables administrators to generate graphs and fill them with data stored in MySQL database. It is a Hypertext Pre-processor (PHP) based platform. In addition to generating graphs, Cacti also handles data sources and Round Robin Archives in a database. Cacti contain Simple Network Management Protocol (SNMP) support for those network administrators that use MRTG to create traffic graphs (The Cacti Group, 2012). In handling data sources/gathering, Cacti will direct the paths to any external script/command along with any data that the user will need to "fill in". Cacti will then collect this data in a cron-job and fill a MySQL database/the round robin archives. Data sources are also created, that match to the actual data on the graph. For example, in a case were administrators may want to plot the ping times to a host, *Cacti* enables creation of a data source utilizing a script that pings a host and returns its value in milliseconds. Having defined options for RRDTool such as how to store the data, administrators become enabled to define any additional information that the data input source requires, such as a host to ping in that particular case. Once a data source is created, it is automatically maintained at 5 minute intervals.

Having created data sources, with the use of RRDTool, graphs can be created using the data sources. Cacti enables administrators to create imaginable RRDTool graph using all of the standard RRDTool graph capabilities and consolidation functions. These graphs can then be customized by a colour selection area and automatic text padding function in Cacti to make the process easier.

Cacti is not only used for the creation of RRDTool based graphs, but it can be used in many ways to display them. Cacti allow for a "list view" and a "preview mode", which resembles the RRDTool user interface. In addition, there is a "tree view", which allows administrators to put graphs onto a hierarchical tree for administrative purposes.

In addition to many functions of Cacti, it has a built in network performance based management tool so administrators can add accounts and give them rights and limitations to certain areas of the tool itself according to their discipline and operations. This then allows them to create user accounts that can change graph parameters, while others can only view graphs (read only accounts). Therefore each user maintains their own settings when it comes to viewing graphs.

At fixing this management process, Cacti is also capable of scaling large number of data sources and graphs by means of templates. This enables the creation of a single graph or data source template which defines any graph or data source associated with it. A host template enables administrators to define the capabilities of a host so *Cacti* can poll it for information upon the addition of a new host (The Cacti Group, 2012). Figure 2.3 shows the Cacti end to end delay graph and Figure 2.4 shows the Cacti end to loss graph

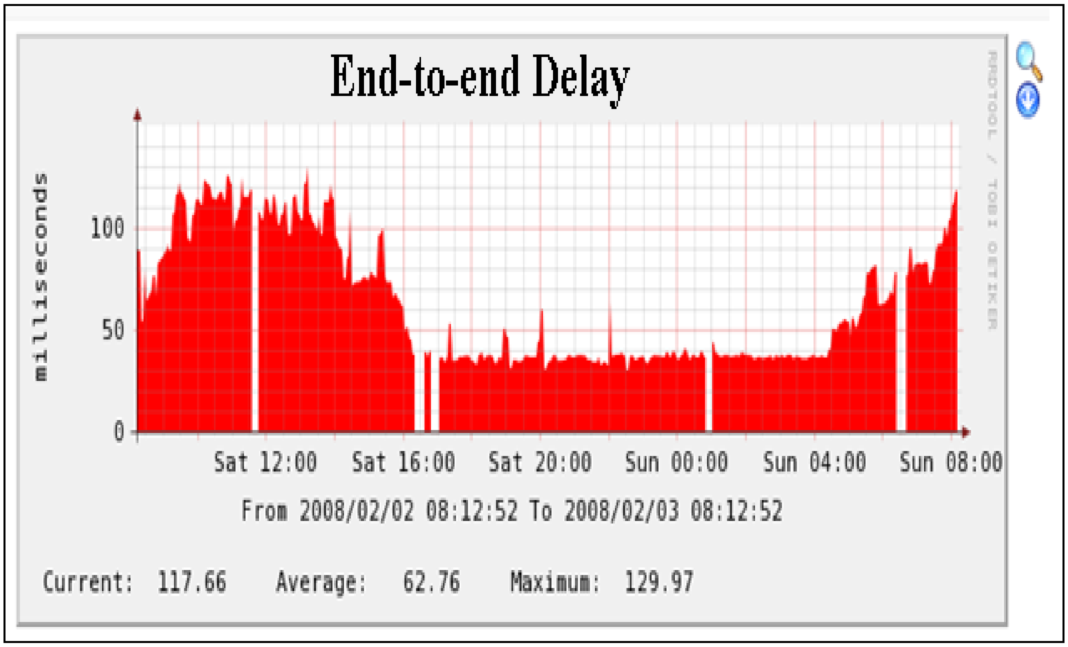


Figure 2. 3: Cacti end to end delay graph Source: The Cacti Group, 2012

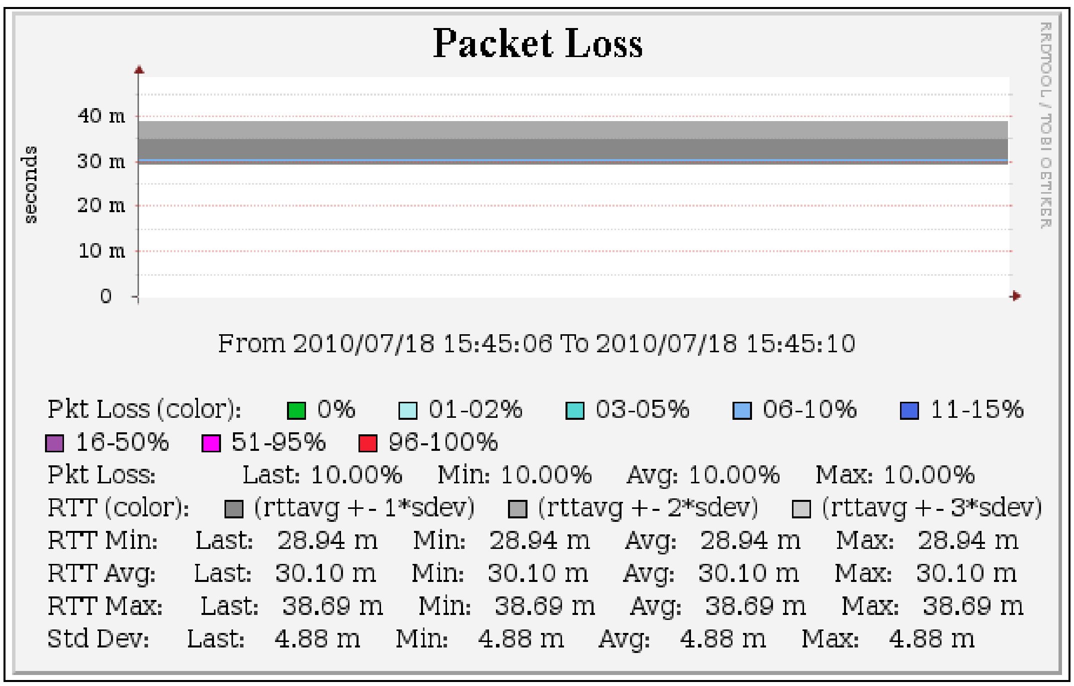


Figure 2. 4: Cacti end to loss graph Source: The Cacti Group, 2012

2.1.6 Network Congestion

A congested network is when the amount of traffic injected into the network links exceeds the available transmission capacity of the network resources (Herranz & Sanchez Cidoncha, 2010). As a result, packets that cannot be transmitted instead they are queued in the router's buffer until resources become available for them to be sent (Moon, 2000). As a result, the network gets overloaded. If this situation is not rectified, the entire network may collapse. A network collapse is when the network load is very high, but throughput is lessened to almost zero (Herranz & Sanchez Cidoncha, 2010). Two of the essential characteristics of a packet switched network which are affected by network conditions are end-to-end delay and packet loss (Bolot, 1993).

2.1.6.1 Network bottlenecks related to congestion

A bottleneck is a scenario where the performance or capacity of the entire network is limited by a single or limited number of components or resources. The term bottleneck initiated from a pouring of water from a bottle mechanism, where the rate of outbound traffic is limited by the width of the channel of exit that is, bottleneck. By increasing the width of the bottleneck one can increase the rate at which the water flows out of the neck at different rates. So the same is true for data network. In relation to congestion, network congestion arises when a link or node is carrying so much data, resulting in quality of service deteriorating. Typical effects include delay and packet loss. These two performance metrics can play a major role on increasing load that can lead either to small increase in network throughput, or to an actual reduction in network performance.

Network administrators can eliminate network bottlenecks in various ways; for example by increasing the bandwidth or by traffic prioritization. As network bottleneck persist they can cause frustrating amounts of network congestion on a network. It is advisable for network administrators to replace or upgrade network links so that they can have the same bandwidth capabilities as the neighbouring links to eliminate network bottleneck.

2.1.6.2 End to End Packet loss and Delay concerns

Probably you are asking yourself; why is packet loss and delay important? Explanation lies on the importance of end-to-end packet loss and delay. When packet loss results from network problems, lost or dropped packets can result in highly noticeable performance issues such as scary delay variation. This might cause streaming technologies, VoIP, online gaming and videoconferencing to go AWOL and that will affect all other network applications to a degree whereby the network becomes unstable. However, it is important to note that packet loss does not always indicate a problem. If the delay and the packet loss at the destination hop are satisfactory then the hops before that one do not matter (Nessoft Knowledge Base, 2011).

2.1.6.2.1 Measuring and analysing end-to-end loss importance

IP and MPLS (Multiprotocol Label Switching) packet network contains a mixture of traffic, with a vast difference in QoS requirements. The service model of emerging multi-service packet networks, including the packet backbone networks, packet loss is based on the network's potential assurance of QoS to user applications. End-to-end packet loss is a worth noting QoS performance metric available in Service Level Agreement SLA. The reason being a number of applications such as VoIP and videoconference etc. degrades network performance severely if the end-to-end loss exceeds a certain limit, and the network will become unusable under excessive loss.

A network with a high traffic delay product is commonly known as a long fat network (LFN) and often pronounced "elephant". As defined in RFC 1072, a network is said to be LFN if its traffic delay product is meaningfully greater than 10^5 bits (12500 bytes).

A well performing network may fall into this category, where protocol tuning is critical for achieving peak throughput, on account of their extremely high bandwidth, even though their delay is not great (Welzl, M., 2005).

Where end-to-end packet delay is very high and link throughput may also be high. The high end-to-end packet delivery time makes life difficult for those protocols that use stop-and-wait approach and applications that assume rapid end-to-end response prior transmission (Welzl, M., 2005).

A high traffic delay output is an important problem in the design and functioning of protocols such as TCP in respect of network performance. Here the protocol can only attain its ideal throughput if a source transmits an adequate amount of data before being required to stop and wait until an acknowledgement is received from the destination, acknowledging successful arrival of that data. If the amount of data sent is inadequate as compared with the bandwidth-delay product, then the link is not being kept busy and the protocol is operating below the peak of the link. Protocols that hope to thrive in this respect need carefully designed self-monitoring, self-tuning algorithms (Welzl, M., 2005).

2.1.6.2 End to End Packet loss and Delay users' point of view

Two major essentials of network performance are loss and delay. Network users are more familiar with the concept of bandwidth as it is often advertised by network service providers of data bundles. However, delay and loss matters equally to the end user experience as the behaviour of IP networks illustrates. Businesses use the term "QoS" to refer to steady network performance by measuring and analysing both packet loss and delay in a correlation manner (Enterprise QoS Solution Reference Network Design Guide, 2012).

QoS is a major issue in network performance implementation. The issue is on assuring that packet traffic or other media connections will not be delayed or dropped due interference from other lower priority traffic. For the end user, large delays are troublesome. It becomes hard for users to operate on a network with too large delays.

For instance on VoiP configured network, users keep interrupting one another. Such interruption “delay” causes strange sound effects, even though there are VoIP solution software integrated with jitter buffers that can handle delays, to some degree (Enterprise QoS Solution Reference Network Design Guide, 2012).

2.1.6.3 Correlation between Packet loss and delay

Previous studies suggest that delays and losses share many properties and are correlated, particularly on high network load (Kurose et al., 1998; Bolot, 1993; Jiang & Schulzrinne, 2000). Kurose et al. (1998), claims that congestive losses and packet delays are mostly due to buffering within the network. Packets transmitted on the network are temporally stored in queuing buffers while waiting to be routed to the advancing hop, which is closer to their destination. If these packets are not forwarded in time or the buffers filled up with large packets, the buffers might be filled to capacity. This results in buffer overflows and the discarding of all arriving packets. In such an event, when the packets are queued in the buffer, their queuing delay rises, so the succeeding (congestive) loss is indeed preceded by high RTT values. In addition, even after packets are dropped, the buffer remains full because some packets are still queuing up, and these packets will also suffer from a high delay.

As congestion is increasing, due to adaptation at the TCP sender, for instance, buffered packets begin to de-queue from the queue, so that the queue becomes smaller, resulting in a decline in the RTT values. Therefore, we expect to see an increase in delay prior to congestive loss; the delay remains high for a short period after the loss before decreasing. Nevertheless, the reverse is not true; when a loss burst occurs, delays just prior and after this loss burst are likely to be high, whereas losses do not necessarily follow when delays are high (Moon, 2000). This most likely occurs because routers have large buffers that can hold all incoming packets until congestion clears, causing high delays without dropping packets. It can therefore be noted that even though a string of high delay values might indicate congestion, packets are not always lost, especially if routers have enough buffer space to handle the influx of arriving packets (Moon, 2000). Moreover, the increase in RTT prior to packet loss is usually short-lived. Empirical studies have found that the degree of correlation between increase in RTT and packet loss is less influential on the performance of network, it was found that on average only 7-18% of observed loss events were preceded by a noticeable increase in RTT (Martin, et al., 2000). Another interesting observation is that the rate of inherent RTT also tends to diminish with increasing loss rate, a behaviour which can be explained by congestive losses. Increase in loss rate is normally due to congestive losses, which are by definition, due to buffer overflows. This means that packets are queued at the routers buffer; hence there is a high queuing delay. This ensures that inherent RTT occurs less frequently, if at all, during congestive losses (Martin, et al., 2000).

2.1.7 End user experience on Network performance

In battle with the growth of the network utilizing devices, end user satisfaction is also becoming the top priority for network administrators and the importance of measurement of user satisfaction is becoming higher than ever. With the complexity of networks and service offerings, the understanding of user experience and satisfaction is getting more and more complicated with time.

The traditional method of measuring user experience via key performance indicator (KPI) is no longer an ideal choice for user satisfactory provision as KPI alone cannot represent the user experience across different network services available today (Kok Ho, 2011). The following shows the loop holes that KPI have: 1) Current KPI measures the performance of each network element independently, resulting in neglection of cases of failures or bad performances due to other network elements. Hence, network performance is expected to be lower than those recorded in the scorecard (Kok Ho, 2011). 2) In measuring network service and application performance: KPI tend to measure network performance from the network point of view, like connection success rate, packet loss rate, end-to-end packet rate etc., but what really matters to users are questions like “Can I open a web page? How long does it take to open the web page?

What is the quality of the streaming media? How fast is the buffering time?" which means network performance measurement method is unable to measure the performance of services at the application level.

It is worth noting that the best way to understand the end user experience is directly from user's point of view. Nevertheless it is critical to deploy different methods of network management to enhance network performance so as to provide a comfortable user experience.

2.1.8 Network management techniques employed at the University of Fort Hare network

Effective network management is essential in supporting business processes and operations; however, few studies provide empirical information on current network management practices to assist IT personnel to identify the weaknesses of their networks and to plan for improvement. Gartner Inc. developed a five-phase network maturity model to assist network teams to improve their networks. However, network teams need specific practices in each of the phases to guide their improvement processes (Chen, 2005). Chen (2005) uses online questionnaire to gather data to be mapped into the maturity model to assist network teams to identify areas that need improvements and to provide best practices in various industries and in organization of various sizes to guide the planning of network management improvements.

To support normal day to day operations, effective network management techniques are vital; however, studies have to be done to provide experimental information on current network management methods to assist the University of Fort Hare to identify the weaknesses of their network and plan for network improvements.

2.1.8.1 Visualized University Fort Hare Orion network management

SolarWinds Network Performance Monitor (NPM) is a tool that brings about complete fault detection and network performance management solution that can adapt in rapid network growth and its functionality grows proportionally as the network monitoring needs grow. Thus enabling network administrators to gather and view network performance metrics data through the use of web browsers. Concurrently; monitoring, collecting, and analysing data from network devices such as routers, switches, firewalls, servers, and any other SNMP, Internet Control Message Protocol (ICMP), or WMI-enabled devices is necessary. SolarWinds NPM effectively offers a user friendly and scalable network monitoring solution for network professionals. SolarWinds NPM reduces cost in terms of the number of personnel managing the network because it requires fewer personnel to take advantage of its functionality and its use (SolarWinds, 2010). From a business point of view SolarWinds NPM does not require a team of consultants and months of unpleasant surprises and running it up because the NPM experience is far more intuitive than conventional complex enterprise network management systems (SolarWinds, 2010). Because it can take less than an hour to deploy and no consultants are needed, NPM provides quick and cost-effective visibility into the health of network devices, servers, and applications on your network, ensuring that you have the real-time information you need to keep your systems running at peak (SolarWinds, 2010).

SolarWinds NPM monitors the following valuable performance metrics for physical and virtual devices on the network:

- Network availability
- Bandwidth capacity utilization
- Buffer usage and errors
- CPU and memory utilization
- Interface errors and discards
- Network latency
- Node, interface, and volume status

- Volume usage

These monitoring functionalities, together with web-based interface that can allow network administrators to customize the interface according to their network needs, alerting, reporting engines, and flexible growth capabilities, make SolarWinds Orion Network Performance Monitor the ideal choice at the University of Fort Hare network performance monitoring needs. Figure 2.5 illustrates the current University Fort Hare Orion network management tool. There are two network monitoring tools currently deployed at the University of Fort hare. This setup is motivated by the fact that any technology contains loopholes. So the use of two network monitoring tools such as Cacti and Orion help to bridge any gaps that each might have.

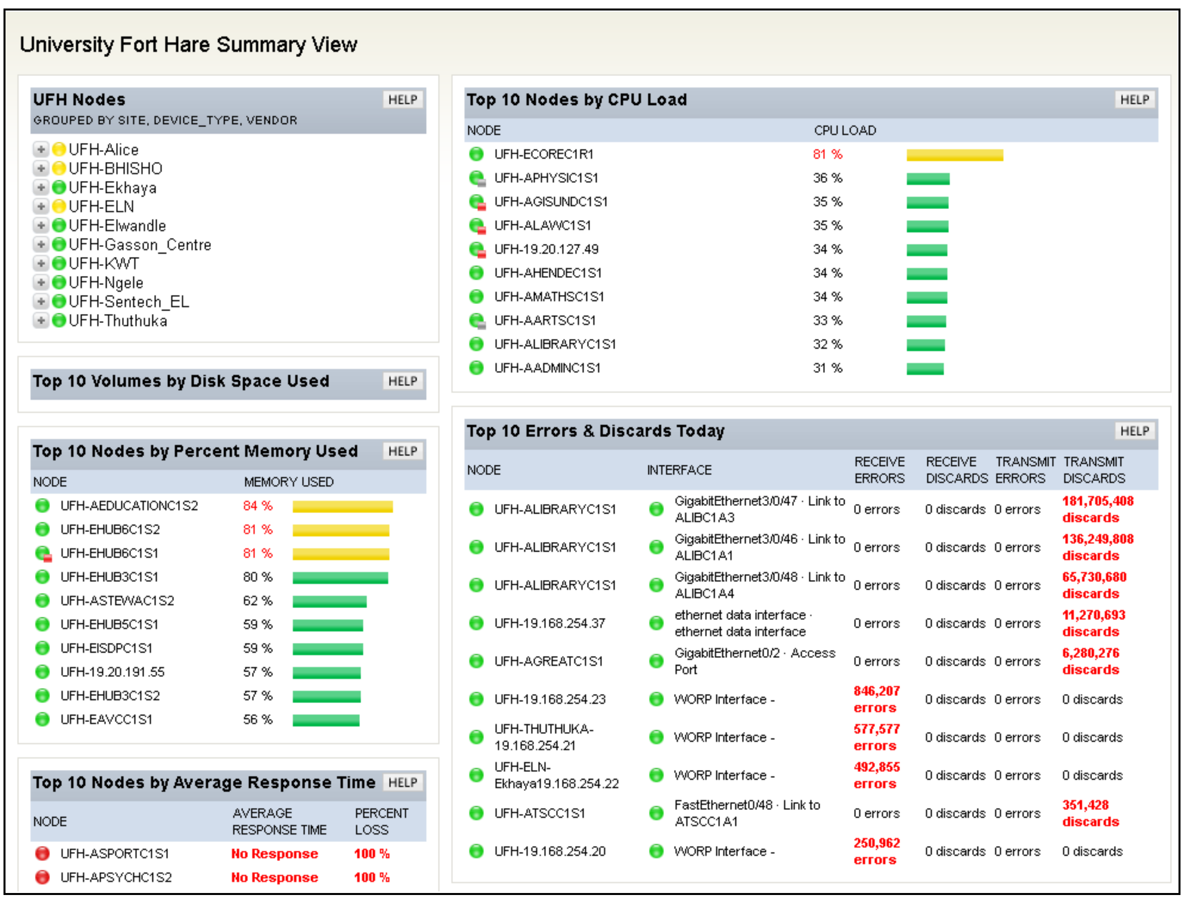


Figure 2. 5: Current UFH Orion network management tool Source: University of Fort Hare, 2012.

2.1.8.2 Benefits of Orion Network Performance Monitor

Orion network performance monitor comes very handy to network administrators due to its benefits such as automatic discovery and wizard-driven configuration. Which means immediately after installing SolarWinds NPM tool, network administrators can be able to monitor critical network devices, making it easy to understand and use. Because of its design which caters for network administrators which also have other responsibilities, it is worth noting that SolarWinds NPM is proprietary software. Nevertheless, it is of affordable value in comparison to its superior and limitless functionalities and scalability**.** By adding individual polling engines, one can scale SolarWinds NPM installation to any environment size. By sharing the same database, it is also possible to share a unified user interface, making the addition of polling engines transparent to the staff members.

2.1.9 Current trends in network performance management and monitoring

Back in the days managing network performance used to be really easy. It was a matter of simple adding bandwidth when the response time is getting slow. Well, that used to be one of the “paradigm” way back, network applications started to migrate to WAN and the term "paradigm" was not in use as frequently as it is now. Is this approach still working? Well, if it is, only in very few and marginal networks. Simply, because bandwidth is an important factor of network performance, nonetheless certainly not the only factor affecting network performance.

Network performance management means how well the network serves its users. It requires analysis and management of network performance metrics. Network performance management includes the processes of measuring, reporting, and controlling of responsiveness, availability, and utilization for the different network components. It's important to emphasize that network performance has to be measured end-to-end. What truly matters is how well the performance is as seen by end users. The performance of each of the individual network components, while important, is less critical to measure than end-to-end network behaviour.

Most of network performance tools are SNMP based. However, not all network performance management tools are SNMP based. EcoNET from Compuware (Farmington Hills, MI), is using a proprietary protocol for collecting data from distributed single monitors (Rabinovitch, 2012). In contrast to the specialized hardware based RMON probes, super monitors are windows-based applications. Super monitors are communicating with windows-based Single View central data visualization and reporting console. Single View correlates and merges data from typically 5-10 Super monitor agents and then stores it into a relational database (Rabinovitch, 2012). Data collected by one Single View can be shared with additional Single View consoles and the relational database is ODBC compliant. EcoNET also includes powerful reporting capabilities, with numerous standard reports (Rabinovitch, 2012). The most impressive feature offered by EcoNET is the ability to measure and track network performance across the entire networks, measuring the network load cost (Santa Clara, CA) previously announces transcendWare architecture allows monitoring and managing networks end-to-end. Transcend networking is a three-part framework for (Rabinovitch, 2012):

- Scaling performance of the campus network;
- Extending the reach to remote sites and users on the WANs;
- Managing the growth of enterprise networks.

The framework stipulates constructive ways for networks that provide a satisfactory user service, as well as simpler and more cost effective to design and manage. TranscendWare modules are the software that powers the Transcend Networking framework.

Network performance management is one of the critical and challenging tasks in managing modern networks. Since most network administrators follow the simple rule of "better safe than sorry", quite often network administrators are expensive to find and, obviously, expensive network infrastructures. However, network performance management seems to have gained momentum lately, and some tools, as described above, can be used today to help network administrators to manage performance and capacity planning not only of their hierarchical legacy, but also modern distributed networks.

2.2 Summary

In this chapter, various network performance management and monitoring techniques, network performance metrics with more focus on end-to-end packet delay and loss rate were explained. The chapter focused on the importance of network performance management in respect to end user satisfactory service provisioning. Different end-to-end packet delay and loss rate measurements, modelling and analysis studies, similar to this research, were explored to help to understand and analyse the core of this research. The importance of measuring and modelling end-to-end packet delay and loss rate to enhance network performance was also highlighted. To deliver an ideal network performance network modelling need to be considered when deploying network changes or planning for future changes; these will help network administrators to understand the current behaviour of the network. However, understanding the current network behaviour does not only lie on network modelling, network management and monitoring tools need to be used to enable administrators have a clear view of the network behaviour. Since the main focus of this research was to analyse and model end-to-end packet delay and loss rate, various network monitoring and modelling tools needed to be considered. In the next chapter the modelling and measuring methods of University of Fort Hare network are presented along with a discussion of how they can be merged to enhance University of Fort Hare network performance.

Chapter three: End-to-end packet delay and packet loss in switched networks

3.0 Introduction

In this chapter an end-to-end packet delay and packet loss in switched networks were discussed. We looked at how a packet experience various kind of delay as it travels through the network. We then highlighted how packet loss generally occurs in switched networks.

3.1 Delay and Loss in Packet-Switched Networks

Having briefly highlighted the University of Fort Hare network architecture, we then look at what happens when a packet travels through from source to destination taking delay and loss into consideration. As packet travels through the network from source to host, it passes through a sequence of network devices. The packet experiences or suffers several types of delays. The most important of these delays are processing delay, queuing delay, transmission delay, and propagation delay (Burmeister, 2008). Adding up these delays they give rise to what is referred to as total nodal delay. Understanding the nature of packet delay helps in understanding how networks behave as far as performance is concerned.

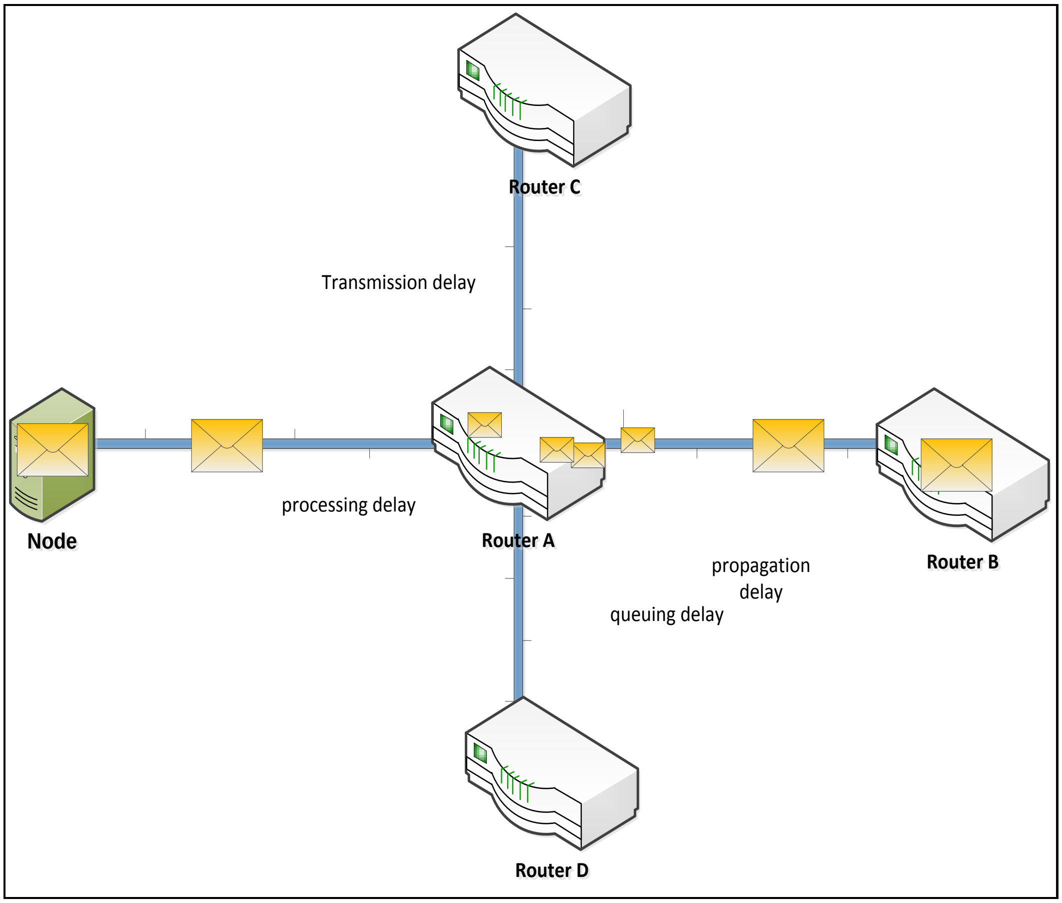


Figure 3. 1 : Delay in packet switched networks

Figure 3.1 illustrates how a packet is sent from the upstream node through router A to router B, as part of its end-to-end route between source and destination. Figure 3.1 shows how a packet is characterized as it adds up to nodal delay at router A. Router A has three outbound links, one leading to router B, another leading to router C, and another leading to router D. Each link is led by a queue (also known as a buffer). When the packet from the upstream node arrives at router A, its header is examined by router A to determine the appropriate outbound link for the packet, and then directed to the link. In figure 3.1 the outbound link for the packet is the one that leads to router B. A packet can only be transmitted on a link if:

- There is no other packet currently being transmitted on the link
- There are no other packets preceding it in the queue;

- The link is currently busy or if there are other packets already queued for the link, then the newly arriving packet will join the queue.

Processing delay can include:

- The time required to examine the packet's header and determine where to direct the packet.
- The time needed to check for bit-level errors in the packet that occurred in transmitting the packet's bits from the upstream router to router A.

After this nodal processing, the router directs the packet to the queue that leads the link to router B. As the packet is waiting to be transmitted onto the link; it experiences a queuing delay at the queue. The queuing delay of a specific packet depends on the number of other, earlier-arriving packets that are queued and waiting for transmission across the link (Burmeister, 2008). If there are no other packets currently being transmitted and the queue is empty, then the packet's queuing delay is zero. In contrast, if there is heavy traffic and several other packets are awaiting transmission, the queuing delay will be long. Assuming that packets are transmitted in first-come-first-serve manner, the packet can only be transmitted once all the packets that arrived before it have been transmitted.

Denoting the length of the packet by *L* bits and denoting the transmission rate of the link (from router A to router B) by *R* bits/sec, the rate *R* is determined by transmission rate of the link to router B. For example, for a 100 Mbps Ethernet link, the rate is *R*=100 Mbps. The transmission delay illustrated in figure 3.1 is defined by L/R. This is the amount of time required to transmit all of the packet's bits into the link.

Once a bit is pushed onto the link, it needs to propagate to router B. This is called propagation delay i.e. the time required to propagate from the beginning of the link to router B. The bit propagates at the propagation speed of the link. The propagation speed depends on the physical medium of the link (i.e., multimode fiber, single modefiber, twisted-pair copper wire, etc.) and is in the range of 2*108 meters/sec to 3*108 meters/sec, which is equivalent to the speed of light. Looking at figure 3.1 the propagation delay is the distance between router A and router B divided by the propagation speed of the link. That is, the propagation delay is d/s, where d is the distance between router A and router B and *s* is the propagation speed of the link. Once the last bit of the packet propagates to node B, that packet and the rest of the packets are stored in router B. The whole process then continues with router B now performing the forwarding.

The transmission delay does not involve distance between two routers; it is a function of the packet's length and the transmission rate of the link. On the other hand, the propagation delay, is a function of the distance between the two routers, but has nothing to do with the packet's length or the transmission rate of the link.

3.1.1 Queuing Delay

Queuing delay is in contrast to other delays; that is, transmission, propagation and processing. The queuing delay can differ from packet to packet. Take for example in a scenario where ten packets arrive to an empty queue at the same time, the first packet transmitted will suffer no queuing delay, while the last packet transmitted will suffer a relatively large queuing delay while it is waiting for the other nine packets to be transmitted (Burmeister, 2008). Hence, queuing delay is characterized by using statistical measures, such as average queuing delay, variance of queuing delay and the probability that the queuing delay exceeds some specified value.

Measuring the significance of queuing delay (i.e. is it big or insignificant) mostly depends on the rate at which traffic arrives to the queue, the transmission rate of the link, and the nature of the arriving traffic, i.e., whether the traffic arrives periodically or whether it arrives in bursts. To gain some insight here, we let *a* represent the average rate at which packets arrive to the queue. Recall that *R* is the transmission rate, i.e., it is the rate (in bits/sec) at which bits are pushed out of the queue. Also suppose, for simplicity, that all packets consist of *L* bits. Then the average rate at which bits arrive to the queue is *La* bits/sec. Finally, assume that the queue is very big, so that it can hold essentially an infinite number of bits. The ratio *La/R,* called the traffic intensity, often plays an important role in estimating the extent of the queuing delay. If $La/R > 1$, then the average rate at which bits arrive to the queue exceeds the rate at which the bits can be transmitted from the queue, resulting in queue that tends to increase without bound and the queuing delay will approach infinity (Burmeister, 2008).

In the case of $La/R =< 1$. Here, the nature of the arriving traffic impacts the queuing delay. For example, if packets arrive periodically, i.e., one packet arrives every L/R seconds, then every packet will arrive to an empty queue and there will be no queuing delay. On the other hand, if packets arrive in bursts but periodically, there can be a significant average queuing delay. For example, suppose N packets arrive at the same time every $(L/R)\ N$ seconds. Then the first packet transmitted has no queuing delay; the second packet transmitted has a queuing delay of L/R seconds; and more generally, the nth packet transmitted has a queuing delay of $(n\text{-}1)L/R$ seconds. We leave it as an exercise for the reader to calculate the average queuing delay in this example.

The scenarios described above of periodic arrivals are a bit theoretical. Typically the arrival process to a queue is random, i.e., the arrivals do not follow any pattern; packets are spaced apart by random amounts of time. In this more realistic case, the quantity La/R is not usually sufficient to fully characterize the delay statistics. Nonetheless, it is useful in gaining an intuitive understanding of the extent of the queuing delay. In particular, if traffic intensity is close to zero, then packets are pushed out at a rate much higher than the packet arrival rate; therefore, the average queuing delay will be close to zero. On the other hand, when the traffic intensity is close to 1, there will be intervals of time when the arrival rate exceeds the transmission capacity due to the burstiness of arrivals, and a queue will form (Burmeister, 2008). As the traffic intensity approaches 1, the average queue length gets bigger and bigger.

3.1.2 Packet Loss

Due to the fact that the queue capacity is finite, packet delays do not really approach infinity as the traffic intensity approaches one. Alternatively, a packet can arrive to find a full queue. The packet will be lost if there is no place to store it resulting in router dropping the packet (Burmeister, 2008). From an end-to-end network viewpoint, it will look like a packet have been transmitted into the network core, but never emerging from the network at the destination. The fraction of lost packets increases as the traffic intensity increases. Thus, performance at a node is often measured in terms of both delay and in terms of the packet loss.

3.2 Summary

This chapter presents end-to-end packet delay and packet loss in switched networks. We look at how delay and loss generally occur on packet switched networks. We discussed how a packet travels through the network from source to host, we highlighted that as it travels it passes through a sequence of network devices. We also looked at different types of delays experienced by a packet. Discussed delays were processing delay, queuing delay, transmission delay, and propagation delay. Finally we look at packet loss on switched networks. Highlighting that a packet will be lost if there is no place to store it resulting in router dropping the packet. In order to analyse packet loss and packet delay in packet switched networks one has to use various network management technique. These are presented in the next chapter.

Chapter four: Network Management Techniques

4.0 Introduction

This chapter discusses different network management techniques used for network performance evaluation. These include the mathematical analysis, measurements and computer simulations. An overview of each of these techniques is given and a motivation for the chosen method is briefly highlighted.

4.1 Techniques used for network performance evaluation

In general there are three different methods for network performance evaluation: mathematical analysis, measurements, and computer simulation (Mondragon *et al*., 2008). In this research however measurements and computer simulation were used. These methods were ideal for the study because of a number of factors which are dissected in the following sections. Literature shows that there are plenty of discussions about when and how to use which method. It is worth noting, performance evaluation comes with concern whether to use the real network or a model. Such consent arises from the fact that measurements require real network system to be available. Such concern will also be discussed.

4.1.1 Mathematical analysis

Previous studies have shown that the packet delays follow the Pareto as well as the Gamma distribution depending on the current network conditions (Vardi, 1996). To mention a few; Weibull distribution, Markov Chains etc. are some of the types of mathematical analysis method for performance evaluation. Mathematical analysis was however left out of this study due to its complex nature to understand and a highly intensive statistical and mathematical background requirement. Furthermore, mathematical analysis often provides a limited insight for the system being studied (Vardi, 1996).

4.1.2 Measurements

Network performance includes a description of speed, capacity, and distortion of events that are carried across the network (Lehpamer, 2002). This description of what is included in the network performance can only be valid if network administrators can measure network performance metrics; end-to-end delay and loss rate, available bandwidth as well as the characteristics of the network behaviour. It can only then be possible to make reasonable recommendations relating to network performance. In this study focus was on measurement of end-to-end delay and loss rate, simply because these two metrics are the ones that affect network congestion mostly thereby eventually deteriorating the network performance.

By studying and understanding network performance metrics, network administrators can determine how these metrics may be measured and analysed, and how the resulting measurements can be meaningfully interpreted. In this work numerous popular network management and measurement tools were tested and their ability to provide useful measurements as network performance evaluation methods was examined. Imperatively we viewed basic approach of measurements which include: collecting end-to-end delay and loss rate data from the active University of Fort Hare network using Cacti, Orion (preferred network management tools). Henceforth, information gathered was then used to evaluate and make recommendations about network performance in the third phase. We refer to this method as a passive approach to performance measurement evaluation, the reason being the approach attempts to measure the performance of the network without disturbing its operation (Lehpamer, 2002).

4.1.2.1 Types of network measuring tools

Network administrators have long been challenged with enhancing their network performance to respond to changing demands of the network services and users. But now more than ever the end-user experience is something network administrators must capture to prove their network is delivering services as it should if not what could be done to accomplish a user satisfactory network performance. The following (Cacti and Orion) are different types of network measuring tools that were used in this study to analyse and recommend future changes on the quest to enhance network performance, which was one of the specific objective of our research.

4.1.2.1.1 Cacti

The use of Cacti was motivated by a number of factors. First of all Cacti is an open source tool. Classically, it can graph network performance metrics which are SNMP enabled. In Cacti configured environment lots of different graphing can be done with SNMP, Perl, or Shell scripts. There are several important reasons that come with the use of Cacti as a network monitoring tool such as: Cacti is by far the best RRDTool front-end network monitoring tool. Cacti provide an easy to use user interface (The Cacti Group, 2012). Cacti is easy to install and you don't need to be an expert or spend much time to configure it, Cacti eliminate the need of pre-requisite tools which is the case with other tools, Furthermore Cacti has a very flexible web interface built with PHP/MySQL. It has a very active large community in the form of public forum to get support and updates. Forums enable the sharing of Cacti templates with other Cacti users on the forum, which will save a lot of time, rather than design all the templates from scratch. It allows the addition of plug-ins to Cacti packages and enables integration of other free tools such as Ntop and PHP Weathermap.

4.1.2.1.2 Orion

The Orion network performance monitor (often referred to as Orion NPM or ONPM) is a web-enabled performance management solution that has a number of important features that make it a valuable tool for any network administrator's toolkit (SolarWinds, Inc., 2008). Orion NPM provides a comprehensive fault and performance management platform that allows for the intuitive collection and viewing of the network availability and real-time and historical statistics from a web browser (SolarWinds, Inc., 2008). Importantly, by leveraging the features of the tool, network administrators are allowed to detect, diagnose, and resolve network performance problems which may allow them to avoid outages or dramatically reduce the impact time of a network related issue for the end users.

Orion network performance monitor is the current tool being used to monitor and analyse in detail the network performance statistics for the University of Fort Hare network routers, switches, wireless access points, servers, and any other SNMP-enabled devices in real time.

It allows collection of all of the details that might be needed when working on any network issue through the use of the drill down maps and top 10 views of the network. Orion NPM is geared to detecting network outages caused by broken links and faulty equipment. Because it produces network-centric views, it's intuitive to navigate and easy to see what's working and what's not. However, Orion NPM is easy to setup even for a network beginner. In addition an inexperienced network administrator will have no or little trouble installing Orion. Again, using Orion, it is readily easy to get support from SolarWinds expert forums. Use of Orion NPM eliminates amateur mistakes such as blaming the network for latency problems, when it's really an application on a server that is underlying cause. The tool can also leverage the advanced alerting capabilities of the tool for correlated events or other sustained network conditions.

4.1.3 Computer simulations

Computer simulation is often applied either for comparing different design alternatives or for optimizing a certain design. In this study a computer simulation method was employed to model the University of Fort Hare network. In this research computer simulation imitates a real-world system behaviour which our case study is UFH network. Computer simulations are actually applied in many different fields and there are several deferent types of computer simulations, like discrete-event simulation, continuous simulation, Monte Carlo simulation, spread sheet simulation, trace-driven simulation etc. In the field of computer networks the dominant simulation technique is discrete-event simulation which is the one employed in this study. The key property of discrete-event simulations is that the state of the simulation model can only change at discrete points in time which are referred to as events (Abdul Majid, 2011).

4.2 Chosen methods

Often the most efficient way to get the ideal solution for our research questions; is to create a model of the existing network and study possible scenarios of the network expansion via software simulation and measure these performance metrics through the use of network monitoring tools such as Cacti and Orion etc. Hence computer simulation and measurements were the chosen techniques for our research. In parallel to literature our choice was motivated by technical expertise in studying network performance and identifying the cause of problems in the network.

4.3 Summary

This chapter discussed different network management techniques used for network performance evaluations. The following techniques were discussed; mathematical analysis, measurements and computer simulations. There are a number of mathematical analyses for performance evaluation; they include the Weibull distribution, Markov Chains etc. However in this study, those were left out due to their complexity to understand and a highly intensive statistical and mathematical background. On measurement, this study focused on end-to-end delay and loss rate, because these two metrics are the ones that affect network congestion mostly. The measurement approach involved collecting end-to-end delay and loss rate data from the active University of Fort Hare network using Cacti and Orion network management tools. Cacti provides an easy to use user interface and is easy to install. Furthermore Cacti has a very flexible web interface built with PHP/MySQL. With Orion NPM, it provides a comprehensive fault and performance management platform that allows for the intuitive collection and viewing of the network availability and real-time and historical statistics from a web browser. For these reasons, this measurement approach was used in our study.

Chapter five: Methodology and implementation

5.0 Introduction

This chapter is divided into three sections which seek to address the following tasks: 1) Investigation of network performance metrics and factors affecting network performance in order to find out how network services can be fully utilised on the University of Fort Hare network; 2) identifying and evaluating the current network management techniques being used to improve network performance 3) formulating ways to improve the current network performance management techniques currently in use.

In phase one a case study approach method was used employing Cacti and Orion as data collection tools. This was followed by empirical approach method of gathering data were scientific decisions are made based on the data derived from direct observation and experimentation. The type of data gathered using this method was from the current network management techniques being used to improve network performance. Experiments were carried out in the third phase where the entire network was modelled in order to provide a platform where changes to enhance the network performance can be made. From the outcomes of phase three, recommendations were made. We divided our approach into three phases.

5.1 Phase 1

In this phase of the research, investigation of network performance metrics and factors affecting network performance was done. The above mentioned tools; Cacti and Orion were used to obtain the results. The following description illustrates how the tools were used to obtain the required results.

Orion NPM network management tool was used to identify, monitor, measure and manage the network performance. This tool was used for performing network discovery and monitoring for determining performance degradation.

We discovered network subnets by employing Orion NPM IP Network Browser function. This was done by scanning for all IP addresses being used within the subnet address of 172.20.0.0 and subnet mask of 255.255.255.0. In this case, only SNMP and ICMP supporting devices were found. Only 53 SNMP and ICMP enabled devices were found and these consisted routers, switches and servers. The snapshot illustrated in Figure 5.1 Indicate the SNMP and ICMP IP Addresses and System Name of the SNMP and ICMP capable equipment by a plus sign (+) prior to the IP Address. Selecting the plus sign (+) expands the selection in order to observe greater detail of the item.

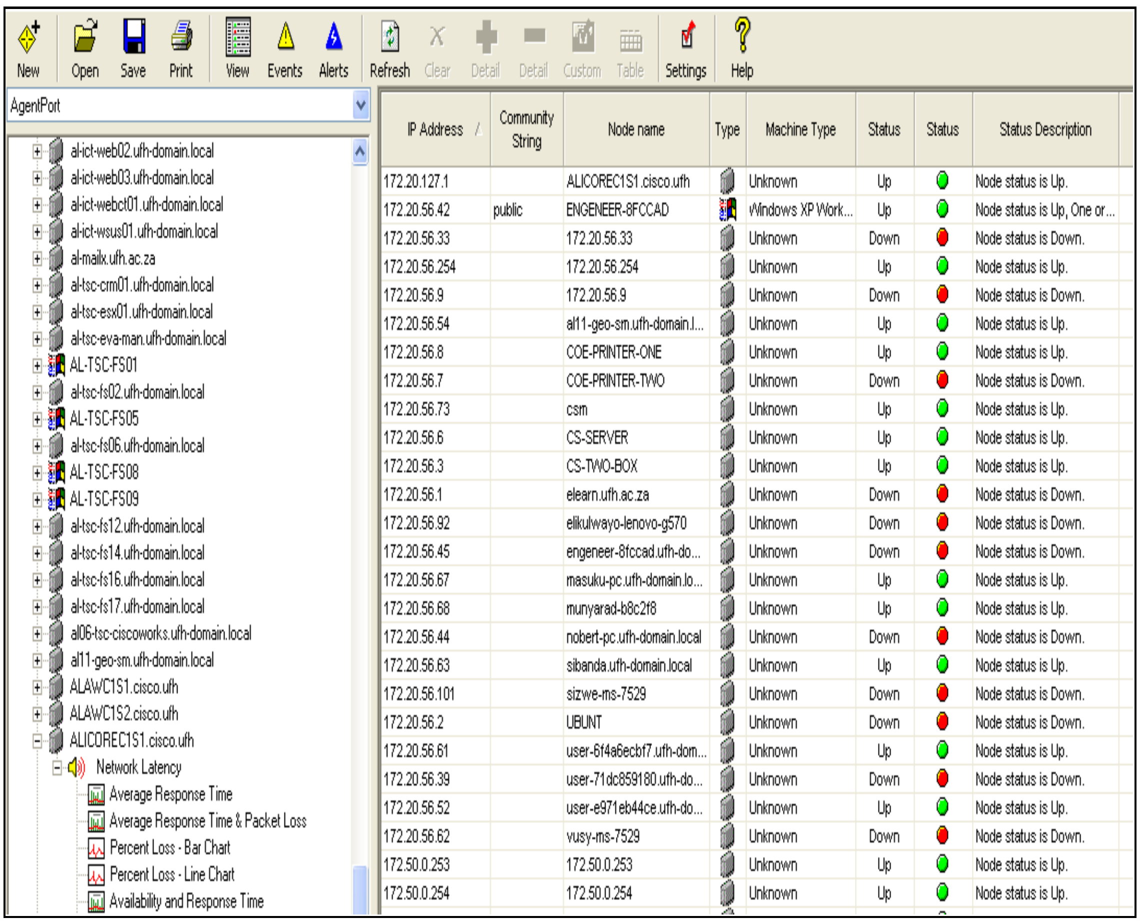


Figure 5. 1 : Discovered SNMP and ICMP enabled nodes

The Network Discovery Wizard was used to provide a subnet list of University of Fort Hare network as illustrated in Figure 5.1. Then, a subnet address was selected to perform a discovery of all nodes on all networks by network address. This function provided us with additional network information such as the mask, the class of the network, the subnet mask, the IP address and the description

The snapshot in Figure 5.1 illustrates a subnet discovery query provided by Orion NPM. The SNMP Sweep function enabled us to select a range of IP addresses to be scanned; the information obtained by this Sweep function provided us with similar results and provides the same detailed information as provided by network subnet discovery query.

In addition, routers on the network were able to be identified using the Router Query and with the use of the MAC Addresses Discovery tool to identify equipment such as routers and switches on the network. Both queries provided detailed information about the queried items to include key elements such as IP addresses, domain name server (DNS), Response Times, System Descriptions, Physical Addresses and IP Addresses.

The Orion NPM was also used to observe the up/down status of nodes, again with special interest in monitoring the SNMP and ICMP enabled devices and the default gateway. The snapshot illustrated in Figure 5.1 was taken at a time when the network had just recovered from a hit (degraded connection) where the network experienced an approximately 80% packet loss at the several network devices, indicated by the Red peak in the lower right quadrant. By examining the details shown in Figure 5.1 more closely, the Orion NPM also indicated a reduction in the average response times from approximately 1500 to 1250 milliseconds, showing an improvement in the network response times as the network recovered.

The Orion NPM IP network browser function was used to scan for all IP addresses within the subnet address of 172.20.0.0 and subnet mask of 255.255.255.0.The results of the IP network browser are illustrated in Figure 5.1. While the IP network browser was performing the network scan, the snapshot illustrated in Figure 5.1 was also taken off the Orion bandwidth gauge tool performing transmits and receive bandwidth usage. By capturing IP Address transmit and receive bandwidth, it was possible to capture the usage of the nodes that are connected to the University of Fort Hare network and visually monitor the live node status.

The Orion NPM was used to observe the performance of nodes, with special interest in monitoring the network core devices. The NPM tool illustrated in Figure 5.1 was configured to monitor the University of Fort Hare network devices 24 hours per day in order to capture continuous network average response time (Blue), % packet loss (red), and peak minimum and maximum response times (green). The snapshot illustrated in Figure 5.1 indicates a network connection outage.

The Orion SNMP Real-Time Graph was used to observe the up/down status of network devices. This network monitoring tool was configured to capture continuous packet flow coming in and out of the University of Fort Hare network devices 24 hours per day in order to monitor the network status. Figure 5.2 illustrates a loss of network connectivity at all times. Real-time network performance monitoring should not be restricted to just monitoring the network devices, but also the links that provides external connectivity to the network and their system fault monitoring capability as well.

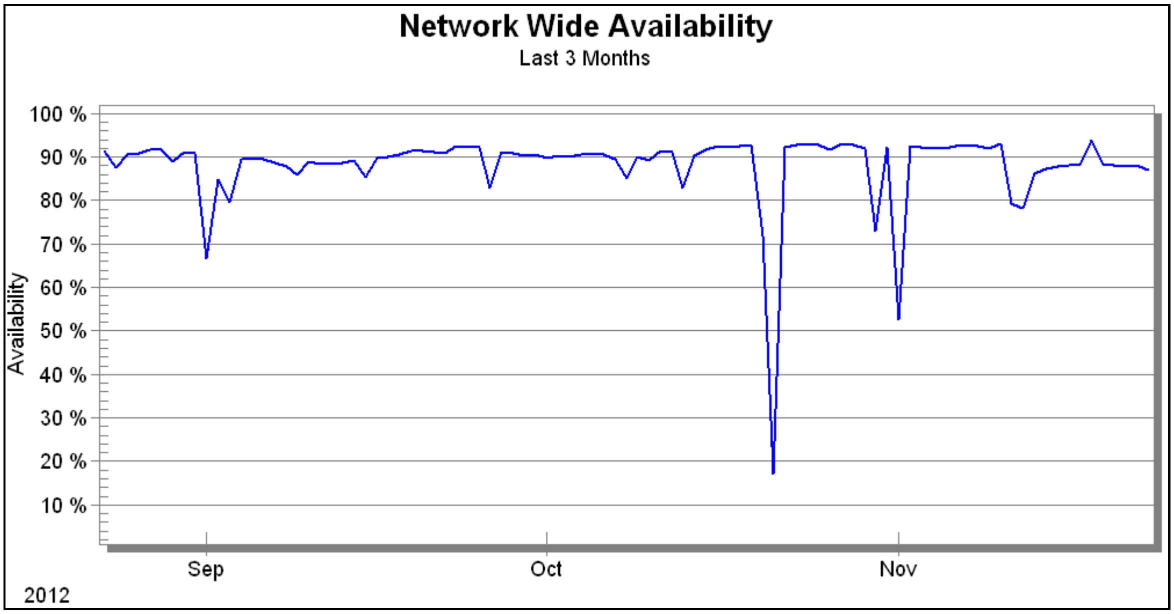


Figure 5. 2 : Network availability

5.1.2 Deployment of cacti as performance monitoring tool

We used Cacti as our second performance monitoring tool. We used two network monitoring tools in order to counteract any disadvantages that each might contain. In addition to get different views of network behaviour so that we can clearly understand the needs of UFH network. Alongside Cacti we used Apache/MySQL/PHP) and RRD Round Robin Database. Which enabled us to collect, manage and display graphs of collected data. We took advantage of RRD and MySQL database to store the University of Fort Hare network data. MySQL and PHP were used to provide a graphical, web-based interface to the RRD databases. RRD database is widely known as the functionality of MRTG graphing. The decision of using Cacti as our network monitoring was highly motivated by the fact that cacti took MRTG configuration to a whole new level. In addition, Cacti provide a click-and-point interface to RRD's. That helped us to easily define, graph, and track many different network devices without editing a configuration file using an editor. We used Cacti to collect I/O statistics of the University of Fort Hare network devices. For each network devices we were monitoring we created graph for it.

5.1.3 Investigation of network performance metrics

Orion NPM provided us with a comprehensive performance, fault management, and network availability tools to ensure that the investigation of network performance metrics run smoothly. Our investigation of metrics were done using Orion NMP web interface, which gave us a unified view into the performance of a number of nodes, network devices and interfaces on the University of Fort Hare network. From a single web page, we managed to monitor performance metrics from any SNMP-enabled devices, including routers, switches and servers. Commonly monitored performance metrics include packet delay and loss rate, latency, errors, and discards. Using Orion NPM as our network management tool, we managed to collect information about above mentioned monitored performance metrics.

Orion NPM was deployed at the University of Fort Hare server which is running Windows Server 2008 R2 and also we installed and configured Orion NPM at our testing machine which is running Microsoft Windows XP. On deploying Orion NPM we firstly installed and configured Orion NPM using a simple wizard interface. Next, we configured Orion NPM to automatically discover our network. Finally, we began monitoring the network for fault, performance issues and investigated network performance metrics.

Orion NPM comes with different modules such as MIB database that covers the vast majority of common network devices. Through the use of Management Information Base (MIB) we collected valuable and highly detailed management data. In addition, Orion NPM poller function enabled us to create a custom poller to monitor any SNMP-enabled device values that had a MIB, including virtually any statistic that a network device recorded.

5.2 Phase 2

In this section of the research an in-depth identification and evaluation of the current network management techniques being used was carried out.

5.2.1 Identification of network management

The second stage was the survey being conducted whereby data was collected from Fort Hare network administrators. This was done in the period from February 2011 to June 2012. The survey sought information on the current network management techniques. An informal interview schedule (questionnaire) was used as the data collection instrument. A structured interview was selected so as to standardize the order in which questions were asked to respondents, and to ensure that questions were answered within the same context.

A questionnaire was used and administered in person to a focus group. In a focus group, questions are asked in an interactive group setting where participants are free to talk with other group members (Marshall and Rossman. 1999). Group discussions produce insights that would be less accessible without the type interaction found in a group setting. This is because listening to others' verbalized experiences stimulates memories and ideas (Lindlofts & Taylor, 2002). In addition, a consultation method was used so as to get administrators and network users' input on current network management techniques employed at the University of Fort Hare and certain network performance issues. The data collected by consultation was analysed and used to identify and evaluate current network management techniques being used at the University of Fort Hare. Such understanding of management techniques and evaluation enabled us to make informed decisions on proposing changes that will enhance network performance. The advantage for using consultation is that it is the qualitative exercise to seek evidence to help deliver the most effective and efficient decision making.

5.2.2 Data collection

The questionnaire captured information on what were the current network management techniques employed, current congestion management techniques at work, whether the network management changed over time? Such kinds of information were asked. These questionnaire generated data that was used to identify and to evaluate current network management techniques.

5.2.3 Evaluation of network management techniques

On evaluating these network management techniques experiments in the form of observation and desktop approach were used to evaluate the current management techniques. Desktop approach and experiments were done in a form of measurements and computer simulations. These experiments were carried so as to conclude whether such techniques are ideal to produce the projected network performance.

In addition to observation and desktop approach on the evaluation of the network management techniques, the study reviewed relevant literature and web-based resources on current trends and past experiences. Literature reviews can generate information for evaluating and understanding network management techniques at low cost and minimize the time frame for project delivery basis. Sources of information such as journals, books, internet, and other documents such as user manuals and network tools experiments manuals were used.

5.3 Phase 3

This section dealt with formulation of ways to improve the current network performance by using the modelling technique. To develop a simulation model of the University of Fort Hare network, we examined and studied the physical topology and the behaviour of the local area network of University of Fort Hare. This model was designed using

OPNET to highlight and point out the need for implementing new changes on the network.

5.3.1 Network Model Framework

The simulation models were organized in a hierarchy consisting of three main levels: the simulation network, node models and process models. The top level refers to the simulation scenario or simulation network. It defines the network layout, the nodes and the configuration of attributes of the nodes comprising the scenario. The node models are at the second level in the hierarchy and consist of an organized set of modules describing the various functions of the node. The modules in the nodes were implemented using process models, the lowest level in the hierarchy. Process models consist of finite state machines, definitions of model functions, and a process interface that defines the parameters for interfacing with other process models and configuring attributes.

Network model was built in a manner where the workflow centred on the Project Editor. This was used to create network models, collect statistics directly from each network object or from the network as a hole, execute a simulation and view results. See Figure 5.2.

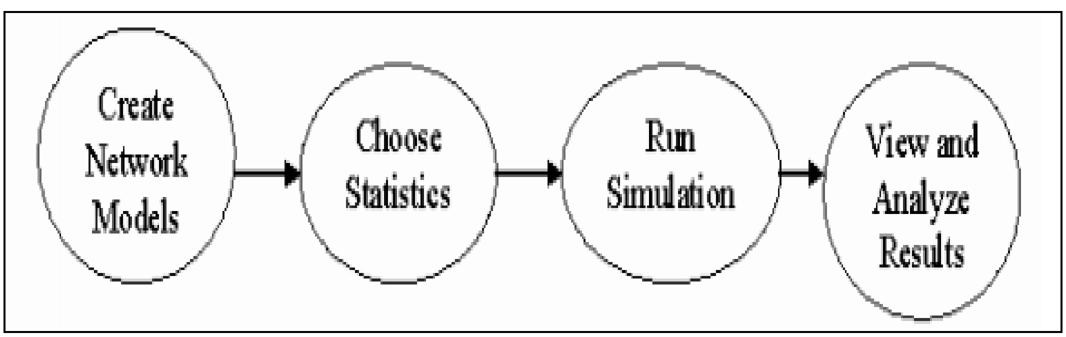


Figure 5. 3 : Network framework

The main staging area of our model for creating the simulated network was done in Project Editor as shown in Figure 5.3. This was used to create a network model using models from the standard library, collect statistics about the network, run the simulation and view the results. Using specialized editors accessible from the Project Editor via

File -> **New** we created node and process models, build packet formats and created filters and parameters.

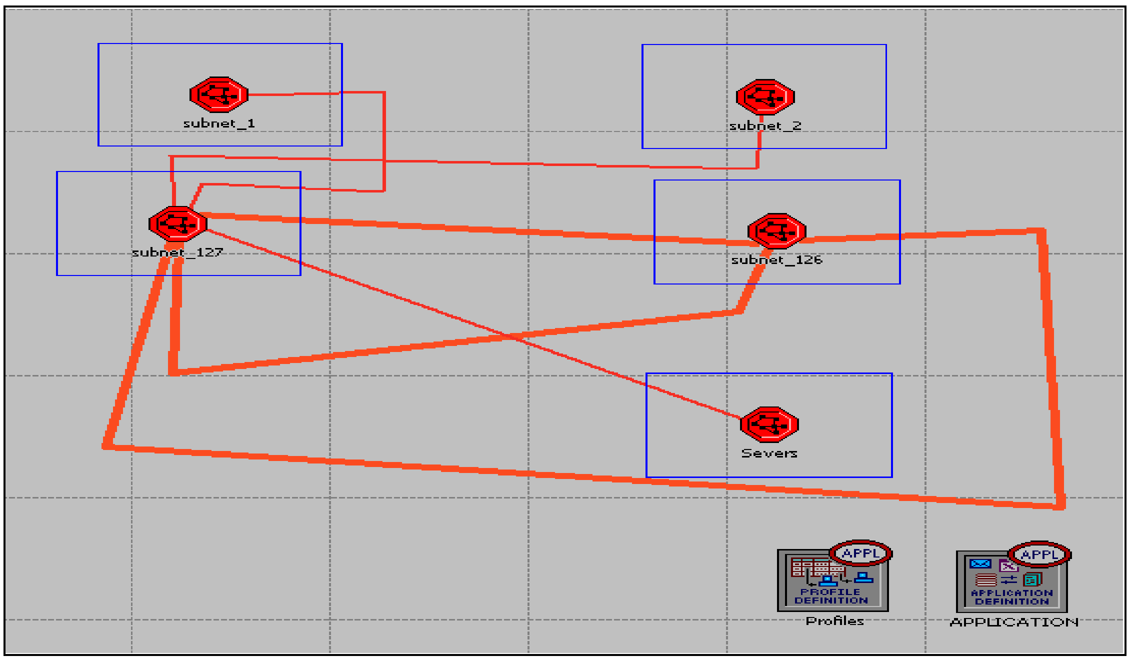


Figure 5. 4 : Project editor

Enhancing the design of University of Fort network is a major issue. Reason being we are dealing with a very complex network. Nevertheless, simulations were used to analyse the conceptual design of the network. The objective is to have a network setup that maximizes the network performance, taking into consideration the cost constraints and the required services to be offered to different types of users. Our simulation show that even after being implemented, network optimization should be performed periodically throughout the lifetime of the network to ensure maximum performance of the network and to monitor the utilization of the network resources. Figure 5.8 shows the experiments design of the network of Fort Hare University which has several departments: 30 departments including academic departments and administration departments. We utilised LAN model that allows us to simulate multiple clients and servers in one simulation object. Even though, this model dramatically increases both the amount of configuration work we needed to perform and the amount of memory needed to execute the simulation. We were able to define a profile that specifies the pattern of applications employed by the users of University of Fort Hare network.

Figure 5.3 shows that we designed a 100BaseT_LAN which was our access layer with a number of nodes varying according to departments, labs and administration. In contrast with the real network we used a 24 and 48 ports Gigabit Ethernet (GbE)10/100/1000 access switches to connect the nodes. We used 100BaseT Ethernet (Unshielded Twisted Pair) UTP cables. For instance, in the Great Hall, 300 nodes were assigned. It was noted that the Great hall has the most number of nodes. This number is equivalent to the real current operational network. On the core layer we used Cisco 3700 Series Routers which is Cisco3745. To interconnect access layer and the core layer we used a 1 Gb/sec fibre-optic. The performance of the modelled network and real network mentioned above were then compared and details compiled in chapter six.

5.3.2 Modelling Topology

After creating our new scenario we designed network topology as follows:

5.3.2.1 Node Model

The Node Editor was used to create models of nodes see Figure 5.4. The node models were then used to create node instances within University of Fort Hare network model. OPNET node models have a modular structure. We define each node by connecting various modules with packet streams and statistic wires. This enabled connections between modules and also allowed packets and status information to be exchanged between modules. Each and every module that we placed in a node served a specific purpose, which was generating, queuing, processing, or transmitting and receiving packets. We proceeded with the following steps:

1. Routers: Select Object Palette → Internet_toolbox→Cisco. From the drop-down menu choose and drag Cisco3745 to the project editor.

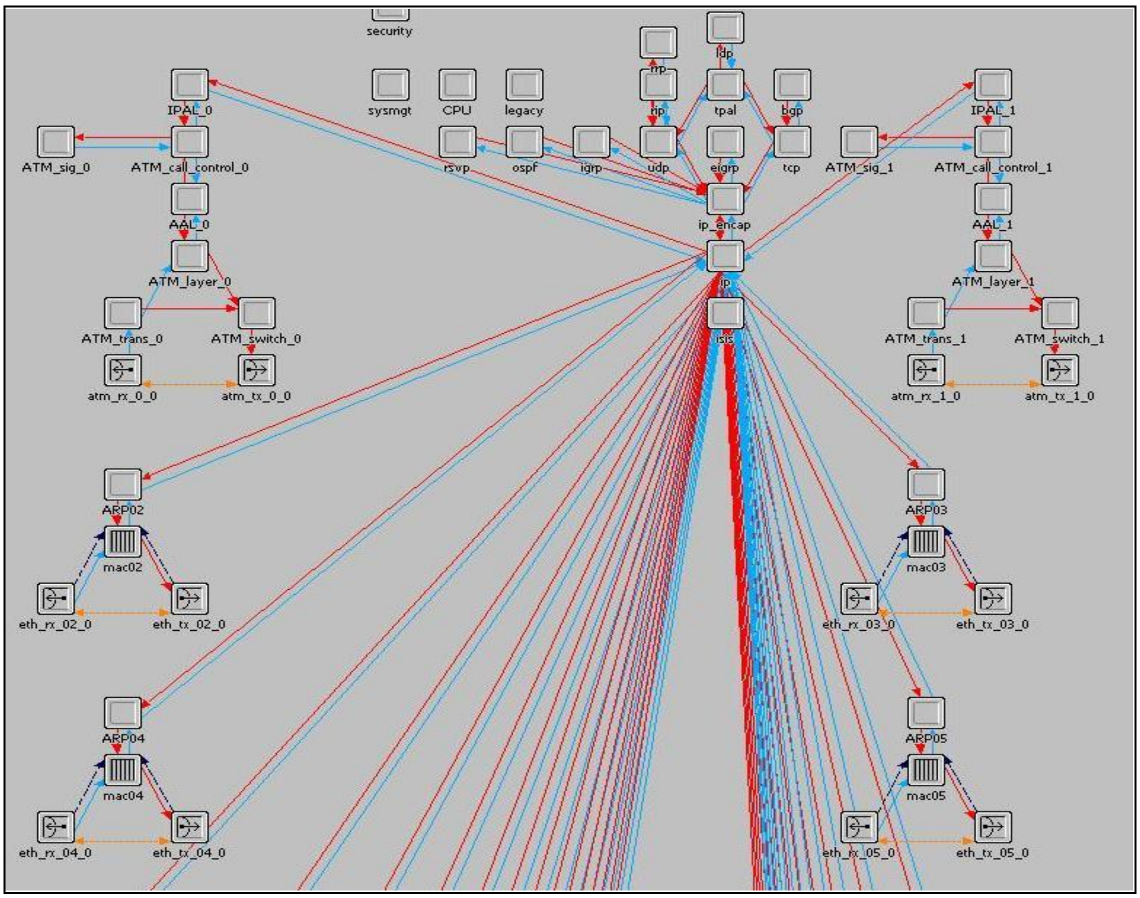


Figure 5. 5 : Node model

2. Switches: Select Object Palette → Internet_toolbox →Cisco. From the drop-down menus choose and drag Cisco catalyst 2960 to the project editor (Figure 5.5).

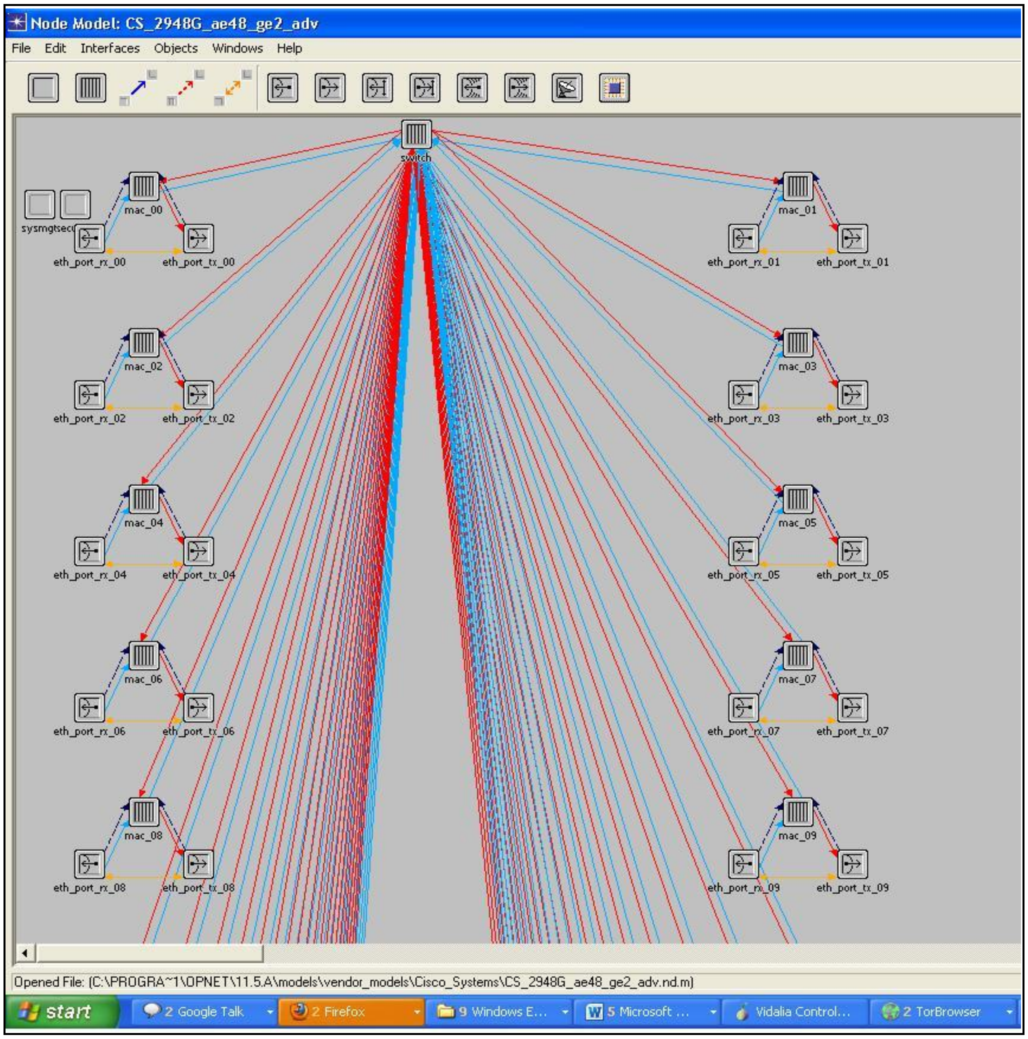


Figure 5. 6 : Switch node model

3. Nodes: Select Object Pallete → Internet_toolbox →Node. From the drop-down menu

   Choose and drag 100 Base T_LAN to the project editor. To interconnect all the network devices; (Figure 5.6).

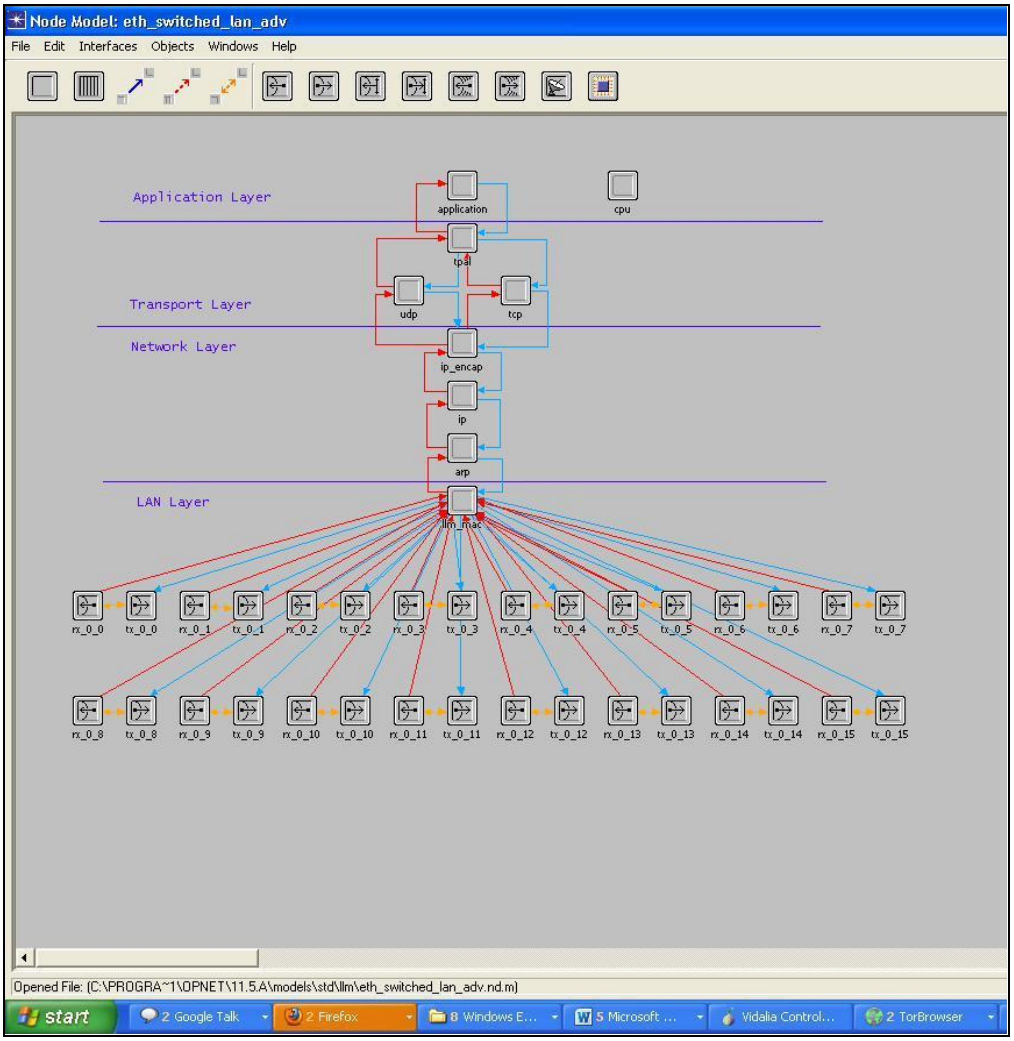


Figure 5. 7 : Link model

5.3.2.2 The Link Model

Figure 5.6 shows the link model. The link model enables to create new types of link objects that have different attributes, interfaces and representations.

4. Links: Select Object Pallete → Internet_toolbox →Link models. From the drop-down

   menu choose and drag 100BaseT and 1Gbps_Ethernet to the project editor.

5.3.2.3 Probe Model

The probe model was used to model the statistics to be collected. Different probes were used and that enabled us to model several different types of statistics that could be collected including global statistics, link statistics, node statistics, attribute statistics, and several types of animation statistics.

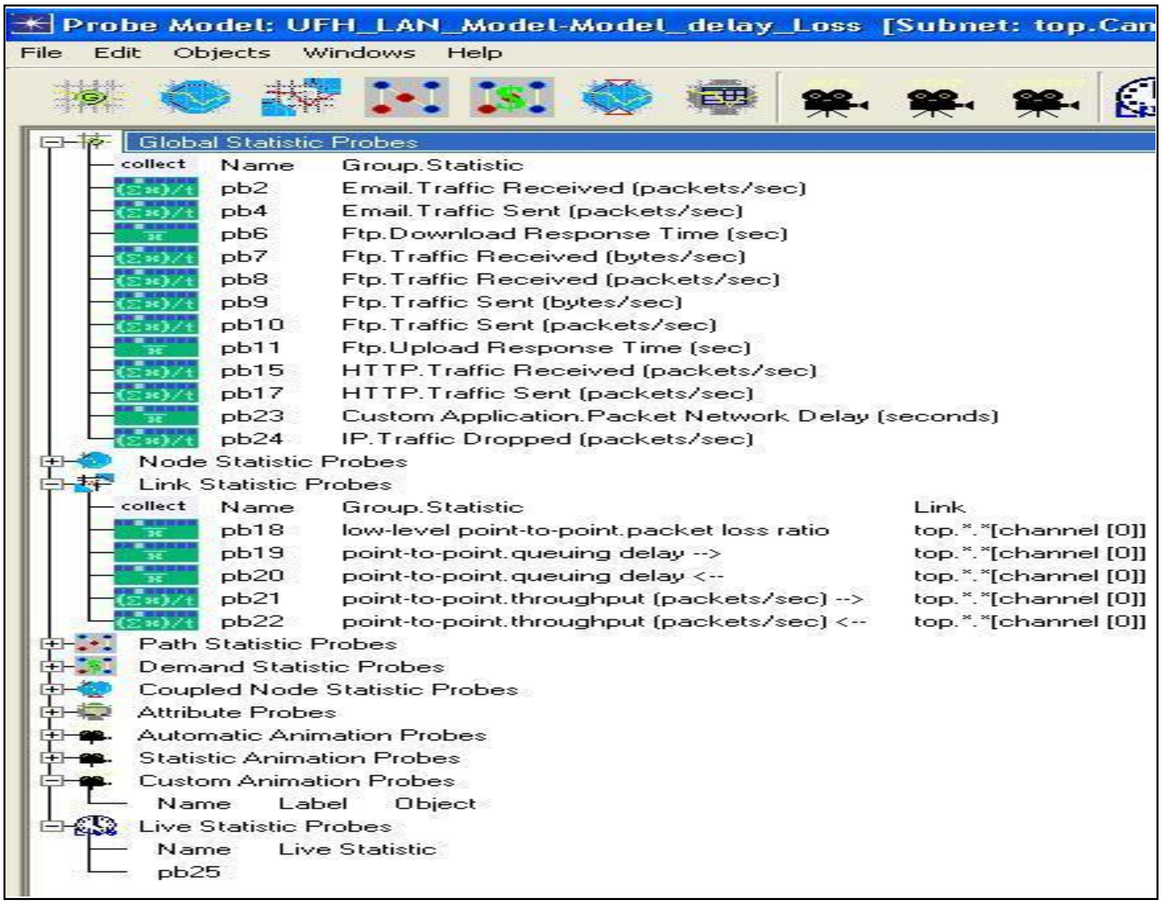


Figure 5. 8 : Probe model

To configure traffic generated by the nodes we right-clicked on any of the nodes then selected similar nodes. All stations in the network were selected (Figure 5.7). We also right-clicked on any of the nodes then we selected Edit Attributes. We checked the *Apply Changes* to *Selected Objects* check box. This is important to avoid reconfiguring each node individually. Figure 5.8 shows the entire University of Fort Hare network topology model.

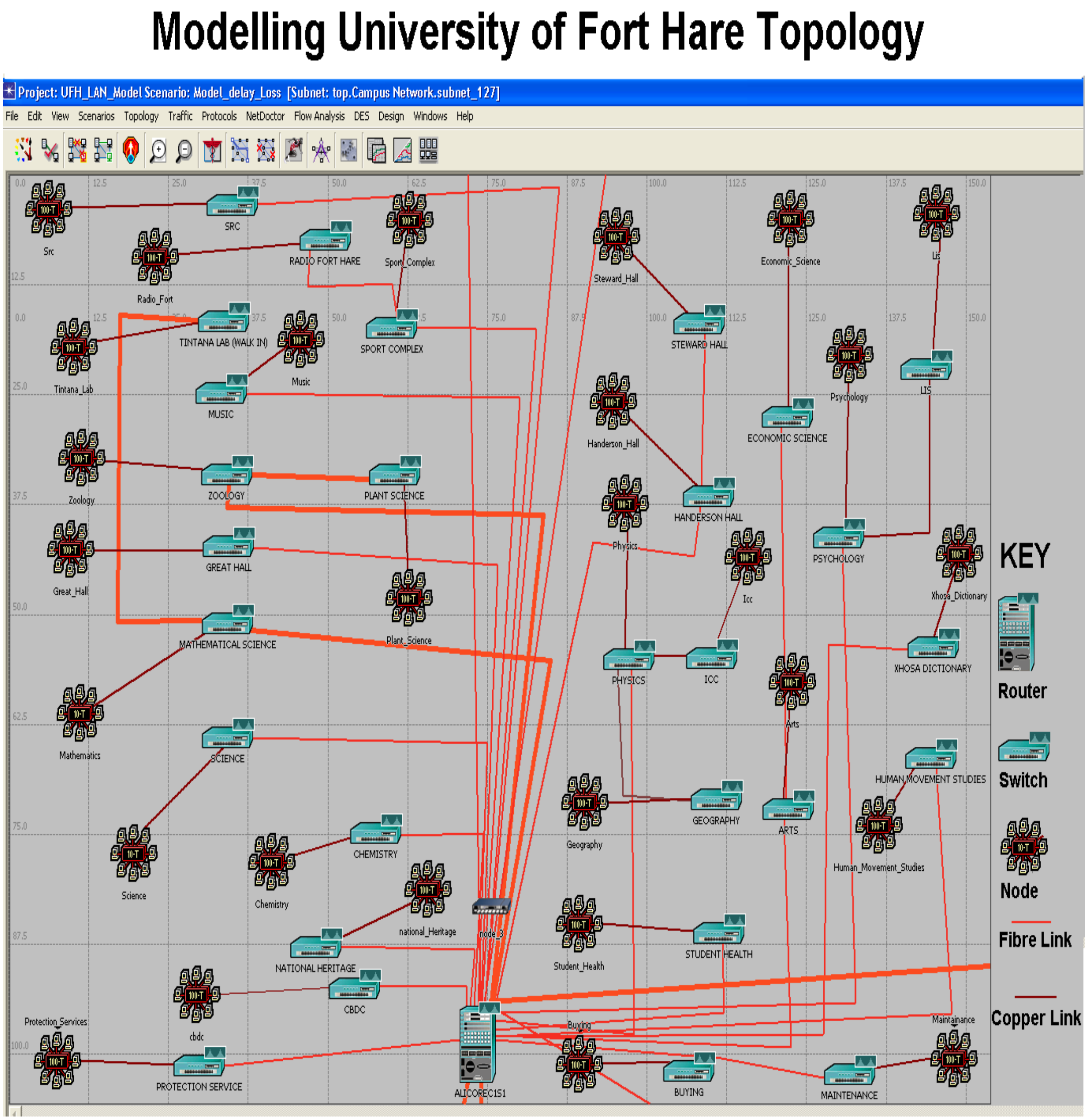


Figure 5. 9 : Entire University of Fort Hare network topology model

5.3.3 Configuring Applications

We identified the frequently used applications that required network access. More focus was given to those that required Internet access, which we termed APPLICATIONS. Internet application traffic must travel via the University of Fort Hare Internet gateway-the proxy-subsequently passing through the web Servers gateway to reach the Internet. The APPLICATIONS were http, emails and File Transfer Protocol (FTP). FTP APPLICATIONS were used to access local University of Fort Hare FTP servers to complete various operations or save data on the network drives. Since Students and staff needed to read their daily e-mails, email servers were enabled. HTTP service was used for general internet browsing.

5.3.4 Configuring Profiles

We described the activity patterns of network user or group of users in terms of the applications they used over a period of time. We defined the applications using the Application Configuration object before making use of the profiles object.

The above mentioned APPLICATIONS were further classified into two broad categories: peak and off peak. We further divided each category into additional sub-classes as follows:

- Peak: staff and administration hours– which were between 8:00-16:30 where they were assumed to be busy accessing emails and the Internet.
- Peak: students – between 17:00-00:00 where students were browsing Internet and doing their homework and saving them on network drives.
- Off-peak: started from 00:00-8:00 when labs and administration offices were closed and we assumed that there in no one who is using the internet.
- 0ff-peak: during school vacation whereby 90% of the students had gone home.

5.3.4.1 User profiles

The model was constructed based on the user profiles to determine how the network APPLICATIONS were being used at University of Fort Hare. These user profiles were sectioned over a period of 3 months into: the vacation, weekdays, and weekends. These categories determined lab and administration occupancy and the APPLICATION usage. The vacation in these three months happened two times during the January period and Easter vacation. During this time, the labs were mostly empty since most students would have gone home. The weekday's time period section modelled student and administration activities from Monday to Friday. During this time period, the laboratories were mostly occupied as students worked on their homework and assignments via the internet. Finally, the weekends time period included Saturday and Sunday, when the labs were mostly empty. On weekends students mostly browsed Internet and occasionally worked on assignments. We further divided each user profile based on the time of the day into four sub-categories: morning, day, evening and night.

The reason for this dissection of network usage during different times was to obtain the behaviour of the overall network performance under different constraints.

5.3.5 Configuring Web (HTTP) applications

To enable application configuration, the Application Configuration and Profile Configuration modules were added in the project editor. The Application Configuration module holds the application definitions, while the Profile Configuration module takes care of the user profile behaviour (how the users make use of the applications defined in the Application Configuration module). To configure http applications, the application named Hypertext Transfer Protocol (HTTP) should be selected from the list of built-in models. These were chosen from the existing configurations such as: Light Browsing, Heavy Browsing, Searching, or Image Browsing. In addition, OPNET enabled us to configure web applications via parameters such as: HTTP Specification which outlined the version of HTTP protocol, Page Interarrival Time which specified time in seconds between successive webpage downloads, Page Properties which modelled properties of the webpage by specifying the number and the type of objects. Figure 5.9 illustrates steps for configuring a web application in OPNET.

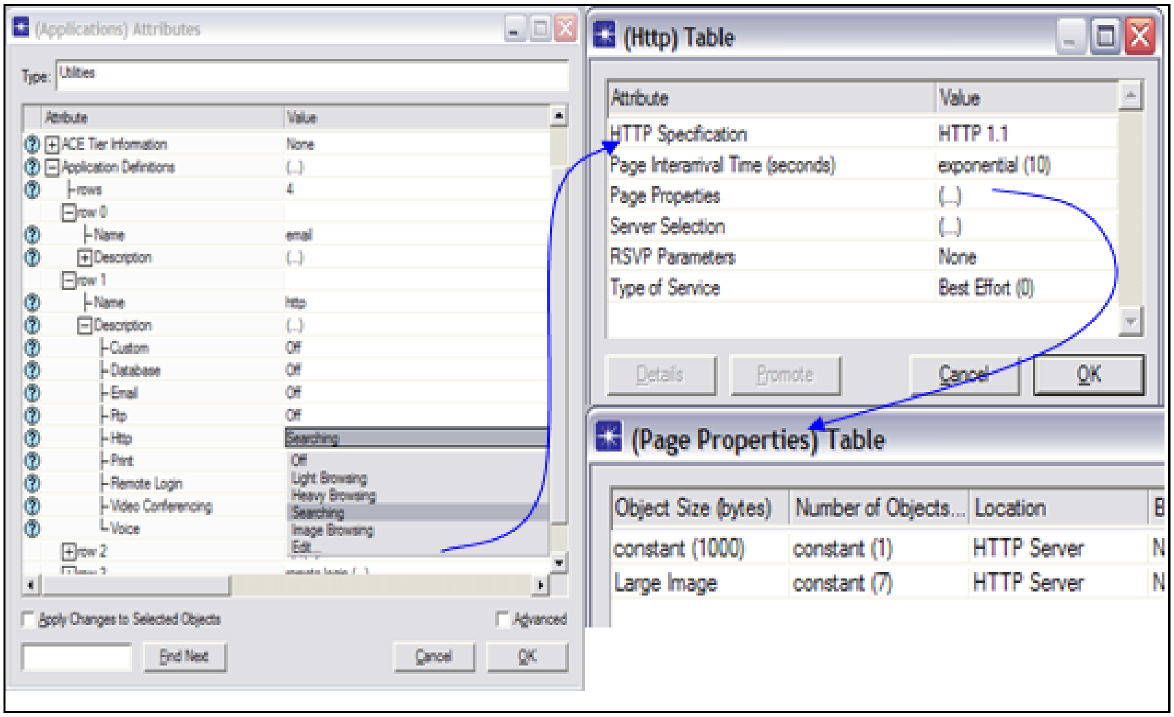


Figure 5. 10 : Configuring a web application in OPNET

5.3.6 Configuring e-mail APPLICATIONS

The e-mail applications were configured as follows:

1) The E-mail services gave options such Low Load, Medium Load, and High Load as shown in Figure 5.10.

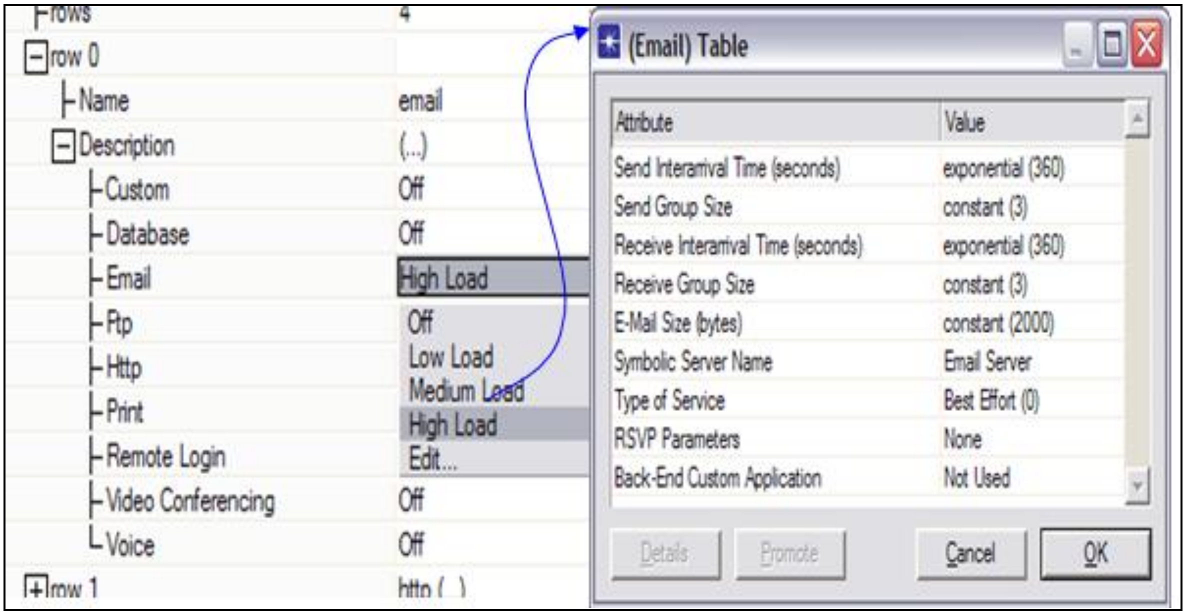


Figure 5. 11 : Configuring an e-mail application in OPNET

2) E-mail Send and receive were configured setting the Interarrival Time which stipulated the amount of time in seconds between successive sent and received operations. It also set Send and receive Size which determined the number of e-mail messages per single sent (receive) operation. Then finally set the E-Mail Size which defined the size of e-mail message in bytes.

5.3.7 Configuring FTP applications

FTP configurations include Low Load, Medium Load, and High Load as shown in Figure 5.11.

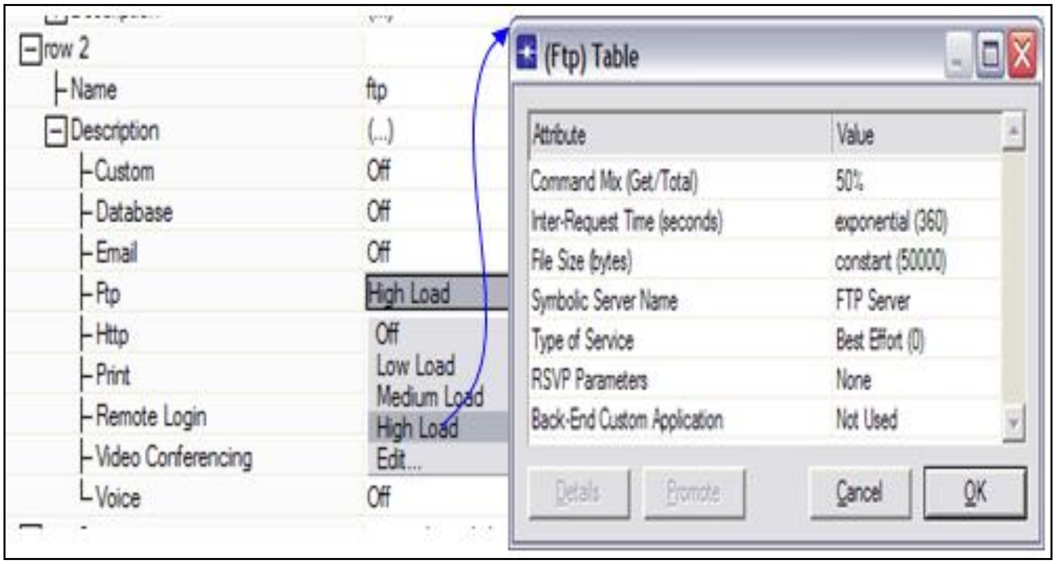


Figure 5. 12 : Configuring an e-mail application in OPNET

5.3.8 Simulation Tool

In the simulation tool (Figure 5.12) we specified a number of simulations constrains. Furthermore, we characterized simulation sequences by simulation icons, which contained a set of attributes that controlled the simulation’s run-time characteristics.

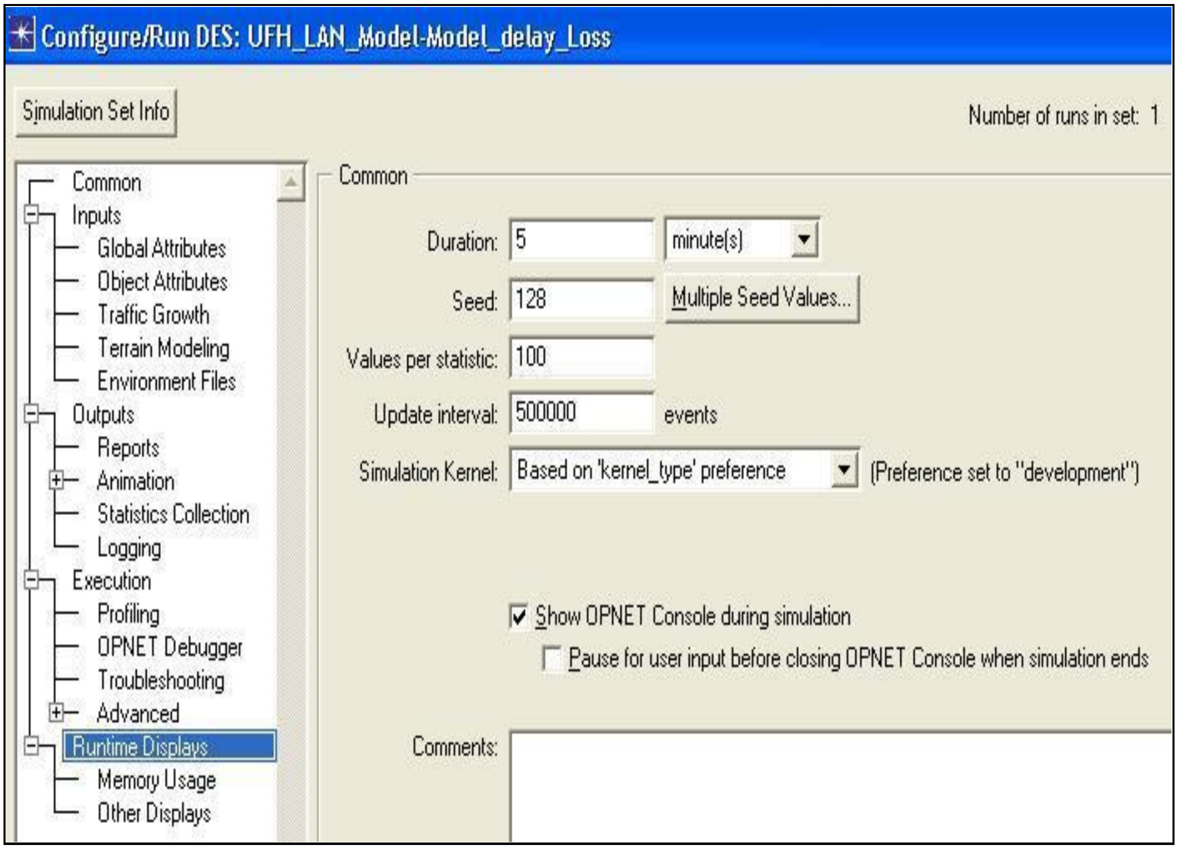


Figure 5. 13 : Simulation tool

5.4 Summary

This section discussed several data collection methods e.g. network measuring and monitoring tools for measuring performance metrics. The main focus was on Cacti, Orion and OPNET as our network monitoring and measuring tools. Orion NPM provided us with a comprehensive performance, fault management, and network availability tools to ensure that the investigation of network performance metrics run smoothly. We used Cacti as our second performance monitoring tool. We used two network monitoring tools in order to overlap any disadvantages that each might contain. The second stage was the survey being conducted whereby data was collected from Fort Hare network administrators and to get different views of network behaviour so that we can clearly understand the needs of UFH network. This chapter also dealt with formulating ways to improve the current network performance by using the modelling technique. The

Simulation models were organized in a hierarchy consisting of three main levels: the simulation network, node models and process models. We identified the frequently used applications that required network access. More focus was given to those that required Internet access, which we termed APPLICATIONS. We also described the activity patterns of network user or group of users in terms of the applications they used over a period of time. In the next chapter we presented the results of our investigation and also make an analysis of those results.

Chapter six: Results and analysis

6.0 Introduction

Experiments and measurements were carried out on the university of Fort Hare network. In carrying out experiments and measurements Cacti and Orion tools were employed. Network performance metrics and factors affecting network performance were investigated together with current network management techniques being used at UFH with the aim of improving network performance. The results are presented and discussed in this chapter.

6.1 Packet Loss and delay

Since the packet delay is measured in microseconds while packet loss is measured in percentages the natural logarithm was used.

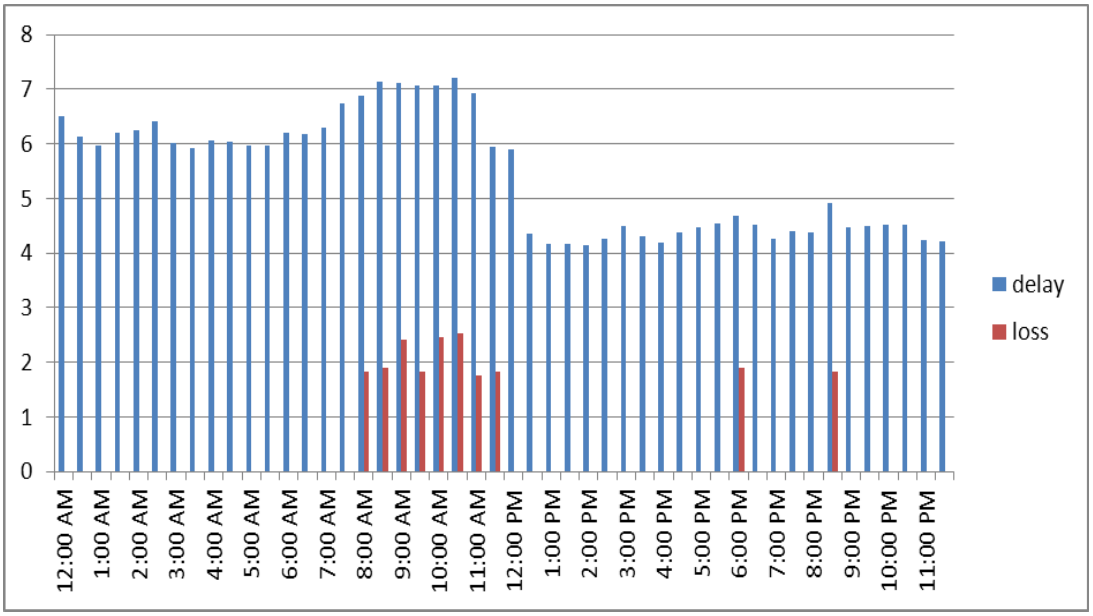


Figure 6. 1 : End to end daily (hour) packet delay and loss

Figure 6.1 represent a normal day of how students make use of network. According to the results represented in this figure the network is mostly busy starting from 8:00 AM to 11:00 AM. This is the time when most of the computer labs and offices are opened. Looking at figure 6.1 we observed that the network is less busy from 12:00 PM to 17:00 PM when students and staff members are going for lunch breaks, attending lectures and going for practical sessions. Then from 6:00 PM, the network gets congested as students are finished with their lectures. At this time students tend to occupy the labs in numbers to work on their assignments and daily routine of Internet browsing. As the network gets congested the packet delay tends to increase resulting in increased packet losses, which eventually impact network performance.

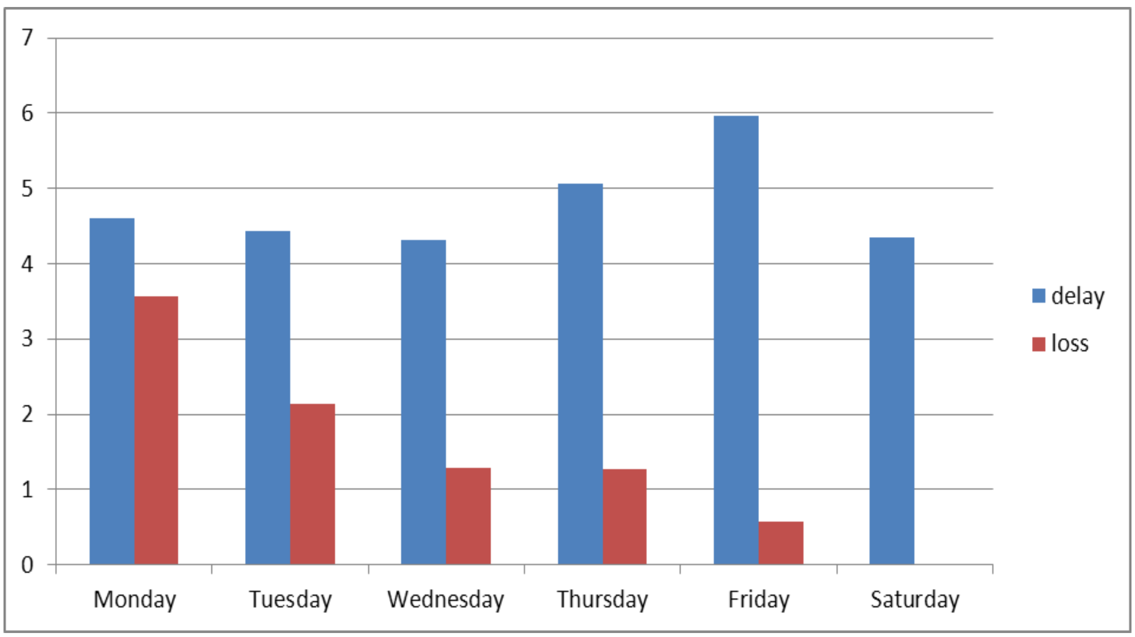


Figure 6. 2 : End to end weekly (daily) packet delay and loss

According to figure 6.2, Monday is when the network is heavily congested with high packet losses. Our assumption is that students and staff use this day to get update on their e-mails, online news and many more. Also this is the day when network administrators often update the network security software and other programs. Basically Monday is the busiest day of the week as far as students and staff are concerned and that puts pressure on the network resources. Students and staff members rely on network to do their daily businesses. As the week progresses the network gets lesser and lesser congested as students and staff get done with most of their work and turn their attention to other activities or leisure. On weekends most students leave the campus and that relieves the network.

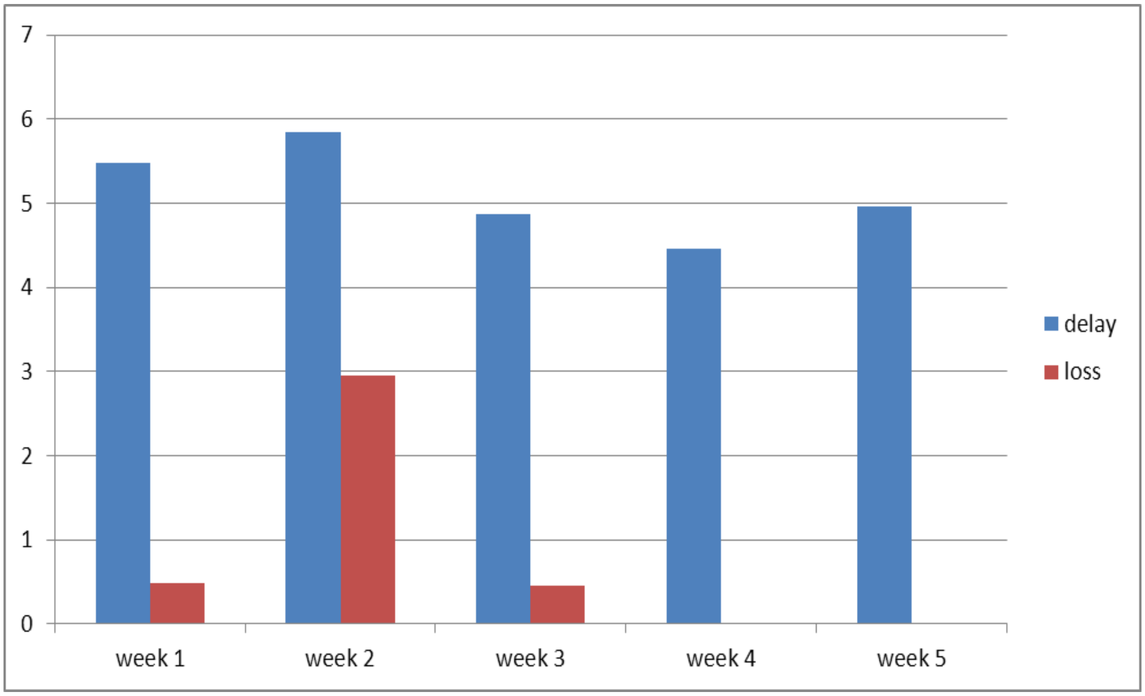


Figure 6. 3 : End to end weekly packet delay and loss for november

Figure 6.3 presents monthly end-to-end delay and packet loss collected on weekly basis. Looking at figure 6.3 one can see that in week 1 of the month of November there was less packet losses as student had already started writing their exams. At this time students were mostly found in the library preparing for their exams. On week 2 of November most students were done with writing their exams and they had less to do as far as academics are concerned. This resulted in students occupying the labs in large numbers thereby congesting the network as it is illustrated by high packet loss and delay in figure 6.3. On the 4th and 5th weeks the student were going home and that had a huge relief on the network.

Figure 6.4 shows the packet loss and delay from 1/3/2012 to 30/3/2012. From this figure we could see that the packet loss rate changed as the traffic load changes. As load increased, it was possible that packet loss rate increased since buffers might have begun to populate on the path between the senders and receivers.

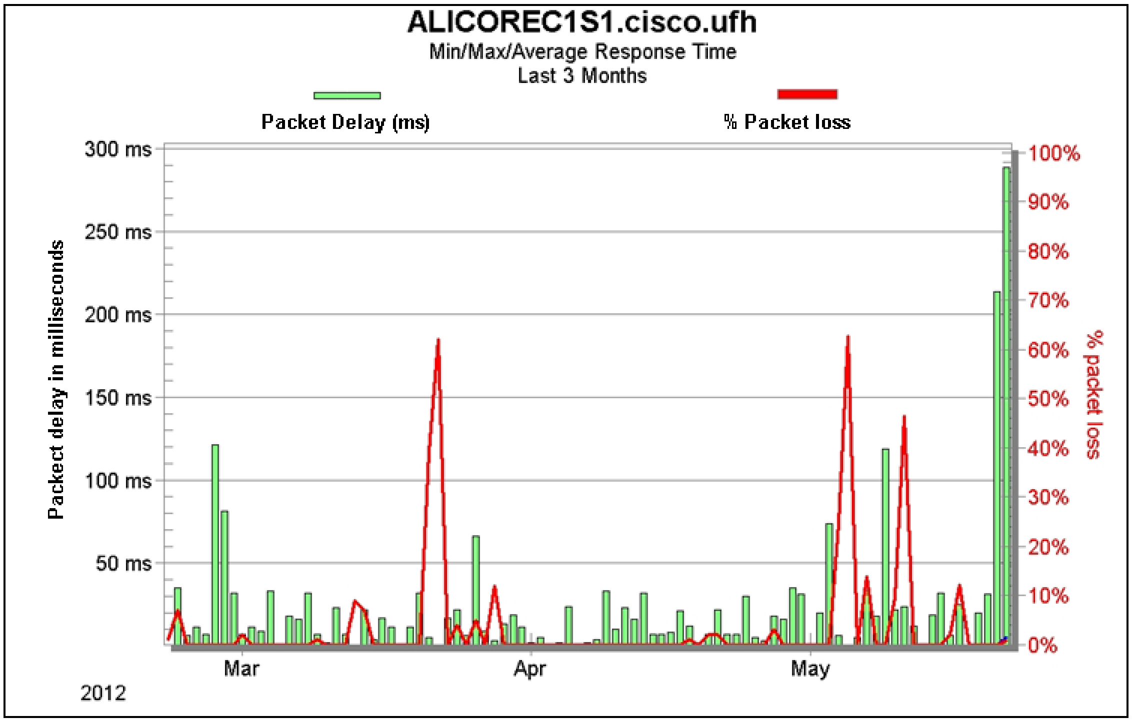


Figure 6. 4 : Packet loss and delay rate from 1/3/2012 to 30/3/2012

Results show that sometimes there was high packet losses experienced when packet delay was very low. This could be a result of out of date equipment being used and also misconfigurations. Out of date equipment and misconfigured network may not be able to handle the network load.

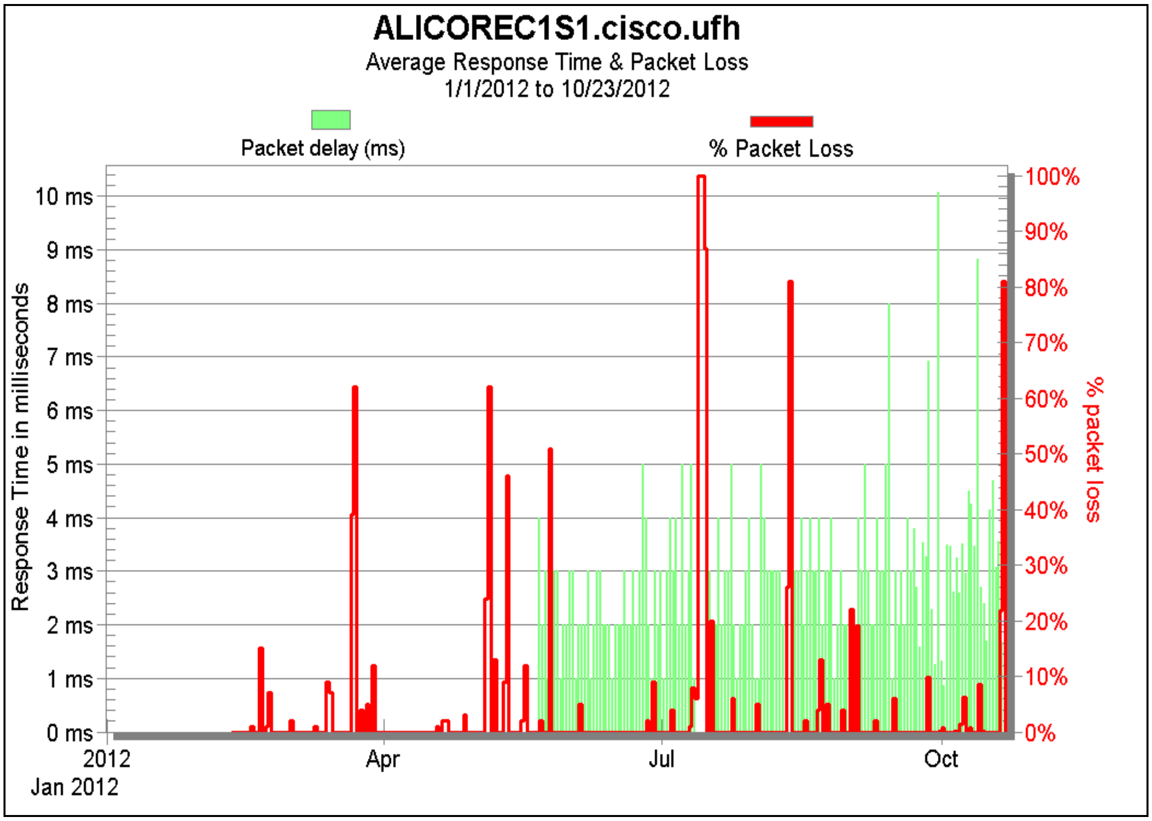


Figure 6. 5 : Packet loss and delay rate from 1/1/2012 to 10/23/2012

Figure 6.4 and Figure 6.5 illustrate the delay (green) and loss rate (red) of packets for the periods 1/3/2012 to 30/3/2012 and 1/1/2012 to 10/23/2012 respectively. The data used to graph this behaviour was collected at ALICORECS1.cisco.ufh core device using Orion network monitoring tool. ALICORECS1.cisco.ufh network device was responsible for distributing packets across the network. Figure 6.4 indicates that during the beginning of March there was less packet loss because students were busy with their registration process, hence most of the labs were free. This included the Great Hall which plays a major role in the network congestion. The above scenario indicates that; congestion is unlikely to occur due to the idleness or minimal usage of the network. Congestion is a problem that normally occurs on shared networks when multiple users contend for access to the same resources. Normally congested networks result to unacceptable packet loss. Ideally packet loss is a metric where anything greater than 0% should be cause for concern.

Figure 6.4 also shows that during mid-March, the network started to experience traffic losses below 20% as students started to attend lectures and occupying the labs in numbers browsing the Internet and spending time on websites like Facebook, YouTube etc. It was observed that students often occupied labs starting at 17:00 when the lectures were over to 00:00 when the labs were being closed. This explains the high potential traffic loss indicated at these times due to congested state of the network. The two high peaks indicated on figure 6.4 were probably caused by power cut or bad weather. Power cuts are a norm at the University of Fort Hare. During the end of March repairs and services on transformers started, hence there was abnormality in traffic loss rate.

On vacations and public holidays, it was observed that most students go home which resulted in less occupancy of the labs. For example, in early April it was Easter and end of June it was end of semester vacation (figure 6.5) there was minimal loss close to 0 %. As from the end of April to May daily business went to normal for academics and that resulted in more Internet usage by students, who were accessing the network looking for their emails and data stored in the network. Such events caused the loss average to go as far as above 10% for the Month of May. A bad weather condition plays a major role to inconsistencies in traffic loss behaviour. Another factor that resulted in inconsistency of traffic loss behaviour was the use of old network devices such as routers, switches and cables.

Figure 6.4 also indicates measurements of live network delay. It demonstrates that other significant factors beyond the physics factors affected delay. The following round trip delays were reported using the Internet Control Message Protocol (ICMP) packet. The data provided in the figure 6.5 shows that, the reported round packets delays in May were much longer than in March and in April due to more lab occupancy in May. For example the delay from May was twice more than March and April which averaged 150 milliseconds in comparing with 50 milliseconds delay of March and April. It is worth noting that delay behaviour was following the same trend as loss as they happened concurrently since they were being influenced by more or less the same factors.

6.2 Modelled delay and loss rate traffic

The results shown in figure 6.6 presents the end-to-end delay and loss obtained from UFH modelled network. From the graph it is observed that there is an increase in the performance when the traffic is transmitted using our improved UFH network model. In our simulation the packet loss indicates that it is almost impossible for IP networks not to experience packet loss. However this packet loss should be minimized as much as possible. As little as a 3% packet loss rate can drive a 75% performance loss (Q Factor Communications, 2012). For this simulation end-to-end packet loss was less that 3% implying that delay has decreased resulting in increase in overall network performance. The decrease in packet loss and delay in modelled network is due to the fact that our simulated network transmits packets with high transmission speed with low delays and moreover hierarchal layer design and latest network components were used in the modelled network, which temporarily reduced the congestion. As explained in the section above the end-to-end delay in a network should not be above 3% in order to have an ideal network performance. If the UFH network can employ such a scenario as our modeled network, this will relieve pressure to the entire network and improve its performance.

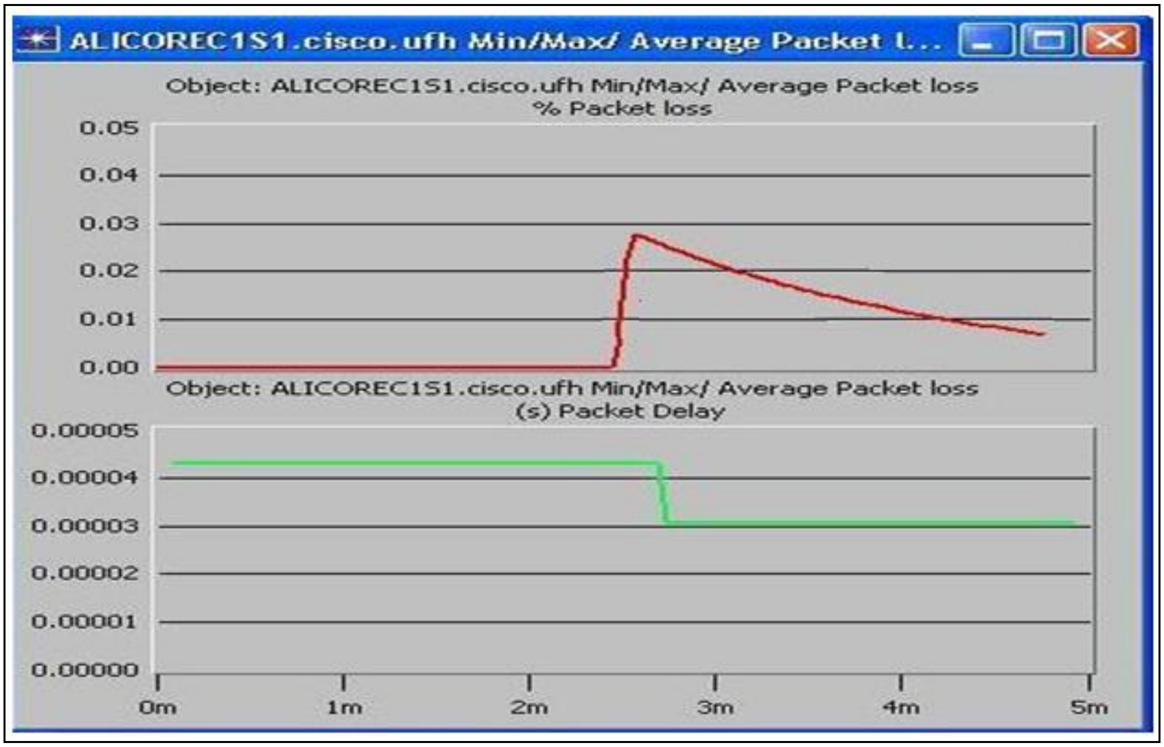


Figure 6. 6 : Modelled delay and loss packet behaviour

Figure 6.7 and figure 6.8 is the comparison of delay and loss rate between modelled networks and live UFH network. Figure 6.7 and figure 6.8 shows packet loss and delay result in different network behaviours. To illustrate the difference between them, the delay and loss rate were taken from modelled network and from Live UFH network with old network equipment and high congestion resulting in high delay and loss. Figure 6.8 is simply delay and loss data taken from UFH modelled network that have changes as far as equipment and configuration is concerned. While these figures might be afflicted with packet loss, nevertheless their behavioural characteristics are very different. Figure 6.8 depicts reduced packet loss, an average interval of roughly 2%, while the congested live UFH network represented by figure 6.7 have high packet loss. Although both networks have packet loss, modelled network exhibit a high level of reliability as far as performance is concerned, nevertheless a technique designed to address the type of packet loss behaviour in UFH network helps to in address the packet loss in our modelled network.

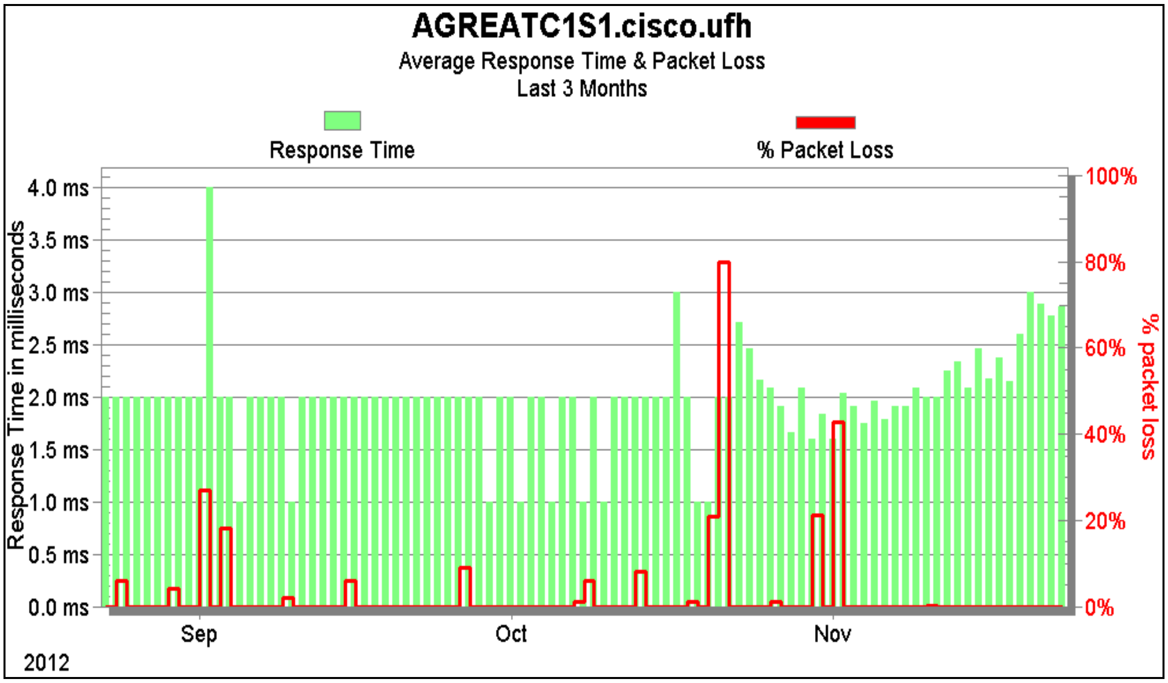


Figure 6. 7 : Delay and loss of UFH Live network

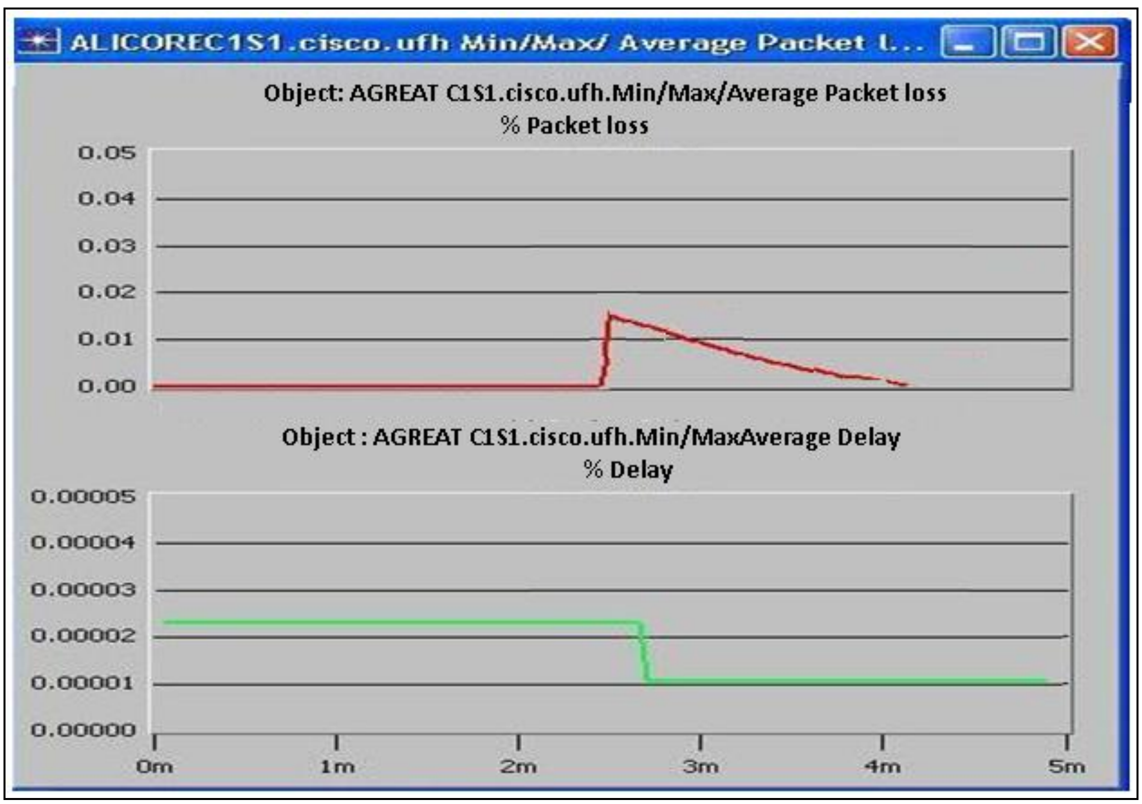


Figure 6. 8 : Delay and loss of modelled UFH network

6.3 Correlation between delay and loss

This section presents the results of the correlation between delay and loss obtained from a linear regression model.

6.3.1 Linear Regression

Linear regression attempts to model the relationship between two variables (delay and packet loss) by fitting a linear equation to observed data. One variable in this case, delay is considered to be an explanatory variable, and the other is considered to be a dependent variable (loss). A linear regression line has an equation of the form

$$Y = a + bX \qquad (3)$$

Where X is the explanatory variable and Y is the dependent variable. The slope of the line is b, and a is the intercept (the value of y when x = 0).

6.3.2 Linear Regression Results (correlation between delay and packet loss)

Table 6. 1 : Correlation between delay and packet loss

Variable	**Beta**	**Standard error**	**sig**
Constant	2.759	1.438	0.000
delay	0.907**	0.013	0.003

a. Dependent Variable: loss ** Significant at 5% significance level
$R^2 = 0.640$

R-squared is interpreted as the proportion of the total variability in the response variable Y (loss) that can be accountable for by the predictor variable X (delay). Since R-squared is 0.64, this value is above 0.5 showing that the variation of loss is accountable for by delay. In other words, the data best fitted the model. The results show that there is some positive significant association between the two variables (delay and loss). Delay is significantly affecting loss at 5% significance level with a value of 0.003. A valuable numerical measure of association between two variables is the correlation coefficient, which is a value between -1 and 1 indicating the strength of the association of the observed data for the two variables. As highlighted in section 6.1 there is congestion in the UFH network. This has an impact on the co-rrelation of delay and loss. As delay increases over a period of time due to congestion, there is increasing loss at intervals of high delay as illustrated in the scatterplot in figure 6.9.

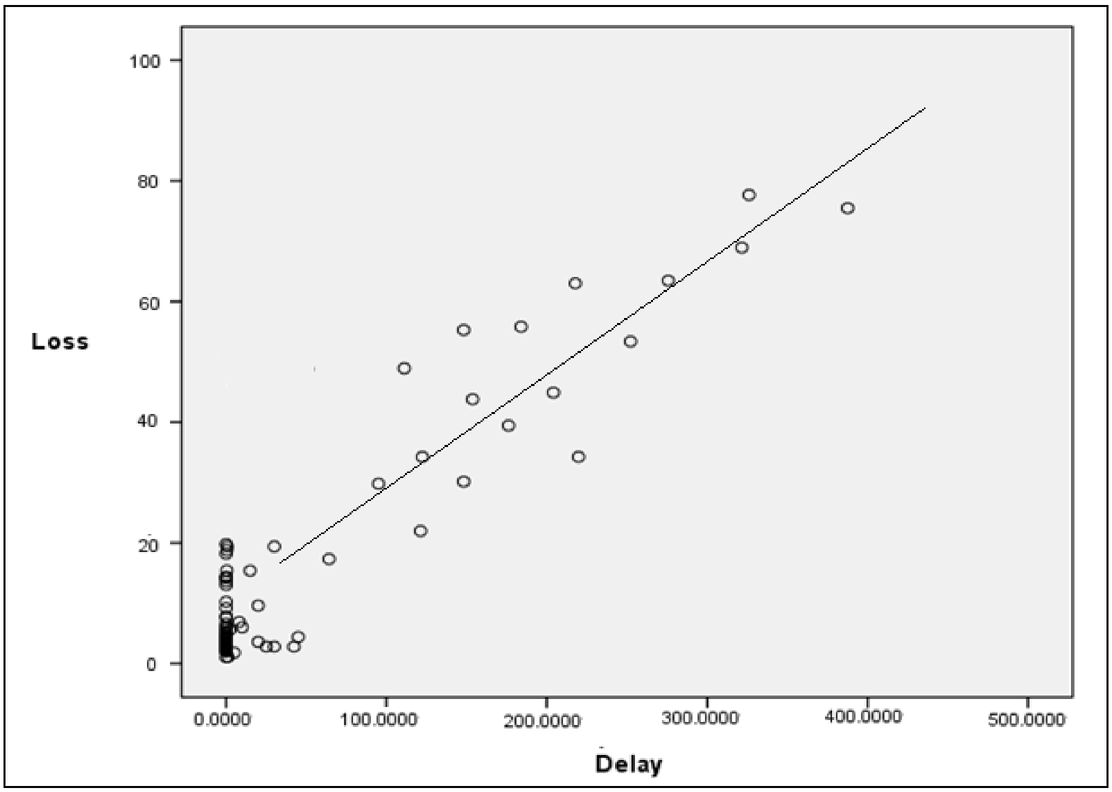


Figure 6. 9 : correlation between loss and delay

6.5 Summary

This chapter presented the results of our investigation. The results of the study revealed that generally congestion is a problem that normally occurs on UFH network as students and staff members contend for access to the same resources. Normally congested networks result to unacceptable packet loss and high delay rates. From the modelled network, there was a decrease in packet loss and in packet delay behaviour due to changes made on the model. Simulation results were discussed focussing on network performance, capacity, efficiency and predictability of key performance areas. We also highlighted a set of results (Linear Regression) which indicates that, under the specific conditions imposed by different scenarios, quite different responses of the network are possible, and that loss sometimes correlate with delay. The next chapter will recommend and conclude our work.

Chapter 7: Conclusions and recommendations

7.0 Introduction

This chapter presents conclusions of the research findings and makes recommendations based on the results of the study anticipated to improve the UFH network if implemented.

7.1 Summary and conclusion

From our initial investigation, the main problem at Fort Hare University was that the network was highly congested. This resulted in high packet loss and delay rates. With a constrained network performance, there are major implications on access to information. In addition network availability is a great concern at University of Fort Hare due to frequently loss of connection to Internet link. Reliability and network efficiency are other network performance degrading factors.

The goal of this research was to enhance UFH network performance where the solutions and results were to benefit those studying and working at UFH and to the network management community at large. The main specific objectives were 1) to investigate the network performance metrics and factors affecting network performance at the University of Fort Hare network, 2) to identify and evaluate the current network management techniques being used to improve network performance and 3) to formulate ways to improve the current network performance management techniques currently in use.

Experiments and measurements were carried out on the UFH network through which Cacti and Orion tools were employed. These experiments and measurements form parts of different network performance evaluation techniques that were used. Measurements and computer simulations techniques were chosen as our performance evaluation methods. Network performance metrics and factors affecting network performance were investigated through the use of Cacti and Orion NPM. These tools were deployed at UFH. Furthermore, a survey was conducted whereby data was collected from Fort Hare's network. Based on the data we collected from this survey we managed to recommend solutions that will improve network performance. Then we formulated ways to improve the current network performance by modelling UFH network using OPNET. The model was developed based on 1) the current infrastructure, 2) the survey carried out, and 3) the information obtained from network monitoring tools .The results of the network behaviour were taken into huge consideration on recommending the restructuring and enhancement of the UFH overall network performance.

The research proved to be a success in a number of key ways. Firstly, the research produced a number of findings that have helped to generate a deeper understanding of how to implement and sustain high performing networks. For the first objective, the results revealed that generally; congestion is a problem at UFH networks. This is due to the high number of users that contend for network access through old network equipment. This resulted to unacceptable packet loss and high delay rates. It was noted that there was high loss and delay rates when students often occupied the labs particularly at 17:00 hours. This explained the high potential traffic loss indicated at those times (17:00-00:00) due to congested state of the network. Again high loss and delay rates were also caused by frequent power cut and bad weather. Power cuts are a norm at the University of Fort Hare. From these results we can conclude that the more there is congestion in a network, the performance degrades resulting in high loss and delay.

In achieving objective 2, we had a clear view and understanding of the current network management techniques employed and current congestion management techniques at work. It was noted that the UFH network is faced with high bandwidth usage despite bandwidth control mechanisms deployed at UFH in a form of Forefront Threat Management Gateway 2010. Students still managed to bypass such mechanisms and accessed blocked sites to download movies, music and games. There is need for other mechanisms to be deployed to counter this misuse of the network. For example, a quota system if used in parallel to bandwidth control mechanisms whereby students are allocated a strict number of bandwidth per period say weekly or fortnightly. Such kind of network management setup will help to overlap any kind of loopholes that might be there from various kinds of bandwidth control mechanisms.

For objective 3, the computer simulation model (modelled network), showed a decrease in packet loss and in packet delay behaviour. This was because of changes made on the model that included cabling, network devices and the use of hierarchal model. Through this objective we achieved methods to formulate ways to enhance or improve the current UFH network. If the changes that we performed on the model can be adopted and implemented UFH network system, the congestion problem can be eased resulting in an ideal network performance.

7.2 Recommendations

The current network system lacks a distribution layer that supports the existing core and access layer and thus limits scalability. We therefore propose having a properly designed network that follow the hierarchical layer model approach to achieve an ideal network performance. This means that the current network system should add a redistribution layer to the existing core and access layer. This will lead to the core and distribution layers performing their operations at very high speeds, resulting in no contention for network bandwidth access layer. As a result, UFH networks can achieve near wire speed between all devices. To properly enhance UFH network performance; UFH network architecture designers should make it a point that they avoid the transmission of data through low performing intermediary switches. Having this design in place, manageability of UFH network will be relatively simple. This will be able to counteract network management problem highlighted in objective 2 as well. Where by each layer of the newly improved architecture design will perform specific functions relevant to that layer. Objective 3 motivated us to propose a properly designed network architecture that contains a fibre optic that interconnect 3 campuses and also a 10 Gig fibre optic link as shown in figure 7.1. Again, instead of having a wireless network infrastructure originating from the very same wired network susceptible to high percentage packet loss rate, dilapidating network performance and efficiency; a separate parallel wireless network where each and every department have its own wireless network would be ideal.

Provision of a reliable and constant network performance was the ultimate goal of this research. Therefore, in this research we have taken into consideration different factors, techniques and methods which could enable this. Throughput from this research helped us to recommend solutions that can enhance UFH network performance and help UFH network to reach world class standards. We expect UFH TSC department together with management to adopt our recommendation and solutions. In so doing UFH community will have a better network service that can help reach new heights as far as academic and daily business is concerned.

7.3 Future work

This study was only limited to measurements and computer simulations. It did not make much use of statistical methods and mathematical techniques to evaluate network performance. Such techniques could have helped us show the correlation between network packet loss and delay or vise-versa. Future studies may make use of statistical methods and mathematical techniques to improve studies on network performance.

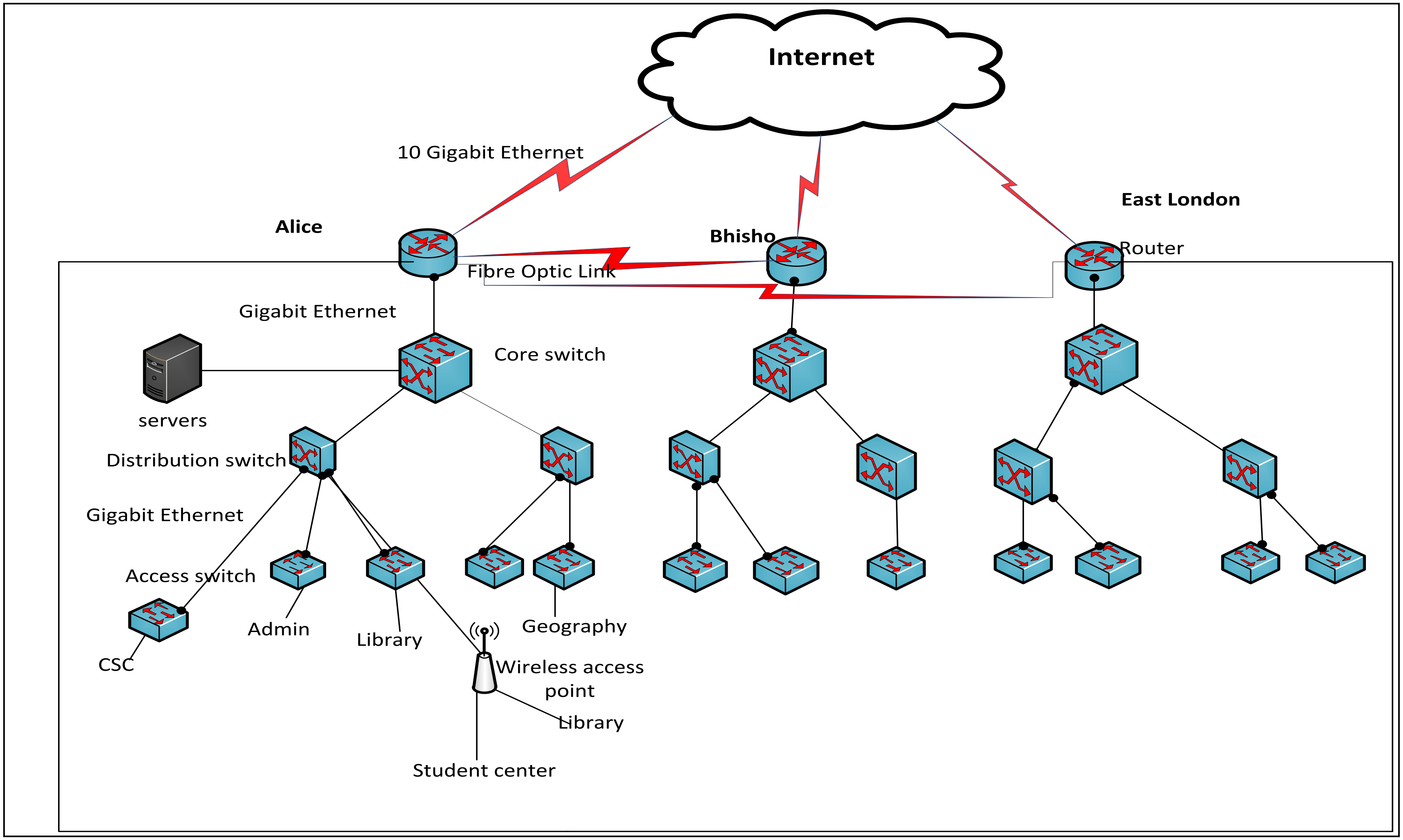


Figure 7. 1 : Proposed network architecture

References

Abdul, M., 2011. Human behaviour modelling: an investigation using traditional discrete event and combined discrete event and agent-based simulation. PhD Thesis submitted to the University of Nottingham for the degree of Doctor of Philosophy, Nottingham.

Acharya, A., & Saltz, J., 1996. A Study of internet round-trip delay, Technical Report CS-TR-3736, University of Maryland.

Allman, M., Paxson, V., & Stevens, W., 1999. TCP Congestion Control, RFC 2581,

Arai, M., Chiba, A., Iwasaki, K., 1999 Measurement and modelling of burst packet losses in Internet end-to-end communications, Proceedings of the Pacific Rim International Symposium on Dependable Computing, P. 260-267.

Biaz, S., & Vaidya, N.H., 2003. Is the round trip time correlated with the number of packets in flight, Proceedings of the ACM SIGCOMM conference on Internet measurement.

Black, D., Floyd, S. & Ramakrishnan, K., 2001. The Addition of Explicit Congestion Notification (ECN) to IP, RFC3168.

Bolot, J., 1993. Characterizing end-to-end packet delay and loss in the Internet, Journal of High Speed Networks. vol. 2. (no. 3). P. 289-298.

Bork, A. & Britton, D.R., 1998. ``The Web is not yet suitable for learning'', IEEE Computer, Vol. 31 No. 6, pp. 115-116.

Bubley, D., 2011. Carrier WiFi Opportunities Enabling offload, onload and roaming A Disruptive Analysis thought-leadership paper. Available online: https://wifimobilize.com/pdf/whitepaper.pdf Accessed on 17 July 2012.

Burmeister,E.F., 2008. Integrated Optical Buffers for Packet-Switched Networks. PhD Thesis, university of California, Santa Barbara.

Calyam, P., Krymskiy, D., Sridharan, M., & Schopis, P., 2005. Active and Passive Measurements on Campus. Regional and National Network Backbone Paths, Proceedings of IEEE ICCCN.

Castro, R., Coates, M., Liang, G., Nowak, R.D. and Yu, B., 2004. Network tomography: recent developments, *Statistical Science*, 19, 499-517.

Chen, C., 2005. Computer Network Management: Best Practices. Available online: http://www.osra.org/2006/chen.pdf Accessed on 04 June 2012.
Clemm, 2006: Network Management Fundamentals. CiscoPress.

Coates, M.J., Castro, R., Gadhiok, M., King, R., Tsang Y., and Nowak, R. (2002).

Comer, D., 2000. Internetworking with TCP/IP. Upper Saddle River, N.J.: Prentice Hall.

Dahal, M. & Saikia,D., 2003. Packet loss free congestion control in TCP for controlled packet latency and optimal throughput, Proceedings of Asia-Pacific Region Conference on Convergent Technologies for, vol. 1.

Demichelis, C., 2000. Improvement of the Instantaneous Packet Delay Variation (IPDV) Concept and Applications, World Telecommunications Congress 2000.

Dunaytsev, R., 2010. Network Simulators: OPNET Overview and Examples, Available online: http://www.cs.tut.fi/kurssit/TLT-2707/lecture12.pdf Accessed on 02 June 2012.

El-Hassany, A.,Kissel, E., Fernandesy, F., Swany, M., Gunter, D., Samak, T., & Schopf M.J., 2010. Scalable Integrated Performance Analysis of Multi-Gigabit Networks, Available online: http://damsl.cs.indiana.edu//projects/phoebus/xsp_monitoring.pdf Accessed on 02 June 2012.

Enterasys Networks, 2011. Data Center Networking –Connectivity and Topology Design Guide. Available online: http://www.enterasys.com/company/literature/datacenter-design-guide-wp.pdf Accessed on 02 June 2012.

Lawrence, E., 2005. End-to-end delay tomography, *Proceedings Large Scale Network Inference Workshop,*Banff, Canada and also to appear in *Performance Evaluation Review.*

Enterprise QoS Solution Reference Network Design Guide, 2012. Quality of Service Design Overview, Available online: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSIntro.pdf Accessed on 04 June 2012.

Floyd, S. & Henderson, T., 1999. The New Reno Modification to TCP's Fast Recovery, Available online: http://tools.ietf.org/html/rfc3782 Accessed on 06 June 2012.

Fong, A.C.M. & Hui, S.C., 2002. "An end to end solution for Internet lecture delivery". Campus wide information systems 19(2): 45-51.

Foster, I., Fidler, M., Roy, A., Sander &Winkler, L., 2004. End-to-end quality of service for high-end applications. Computer Networks, Volume 34, Issue 6, December 2000, Pages 915–929

Frey, J., 2009. ROI for Network Performance Management, Available online: http://www.networkinstruments.com/assets/pdf/EMA_ROI_wp.pdf Accessed on 02 June 2012.

Garcia-Luna-Aceves J.J. & Parsa, C., 1999. Improving TCP congestion control over Internets with heterogeneous transmission media, Proceedings of the Seventh international conference on network protocols, Santa *Cruz, CA.*

Güne, S., Gross, J., & Wehrle, K., 2010. Modelling and Tools for Network Simulation, Springer Heidelberg Dordrecht London NewYork, London NewYork.

Hasib, M. & Schormans, J.A., 2003. Limitations of Passive and Active Measurement Methods in Packet Networks, London Communications Symposium.

Herranz, R., &Sanchez Cidoncha M., 2010. Network Congestion 2030, Congested Network Response Assessment, Vol 2. Available online: http://www.eurocontrol.int/eec/gallery/content/public/document/eec/report/2010/Strategy_Network_Congestion%202030_2_final.pdf Accessed on 02 June 2012.

Hewlett-Packard Development Company, 2005. Traffic Management for the Enterprise, Available online: http://www.hp.com/rnd/pdfs/traffic_management_paper.pdf Accessed on 04 June 2012.

Hong, J.W., Kim, M. S. & Lee, H. J., 2002. QoS Parameters to Network Performance Metrics Mappingfor SLA Monitoring, KNOM Review 5(2).

IDATE & UMTS Forum, 2011. Mobile traffic forecasts 2010-2020 report. IDATE - UMTS Forum 2011 Report No. 44. Available online: http://www.umtsforum.org/component/option,com_docman/task,doc_download/gid,2537/Itemid,213/ Accessed on 17 July 2012.

Informer Technologies, 2012. OPNET Modeller Documentation, Available online: http://opnet-modeller-documentation.software.informer.com/ Accessed on 02 June 2012.

Jan, W., 2010. Revenue requirements for mobile operators with ultra-high mobile broadband data traffic growth. Paper presented at 21st European Regional ITS Conference, Copenhagen 2010.

Jiang, W., & Schulzrinne, H., 2000. Modelling of packet Loss and Delay and Their effect on Real Time Multimedia Service Quality, Department of Computer Science. Columbia University.

Kevin, L., 2011. Toward a customer-centric organization. *Huawei technologies COMMUNICATE, beyond technology.* (60) 3.

Kok Ho, Y., 2011. Managing user experience for MBB, Available online: http://www.huawei.com/in/static/hw-093297.pdf Accessed on 05 June 2012.

Koodli, R., & Ravikanth, R., 2002. One-way Loss pattern Sample Metrics, RFC 3357.

Kurose J, Moon, B.S., & Towsley, D., 1998. Correlation of Packet Delay and Loss in the Internet, Technical Report , Department of Computer Science, University of Massachusetts, Amherst.

Lawrence, E., Michailidis, G. and Nair, V.N., 2005, Local area network analysis using

Lehman, T., Jabari, B & Sobieski, J., 2006. DRAGON. A Framework for Service Provisioning in Heterogenous Grid Networks, IEEE Communications, 44(3).

Lehpamer, H., 2002. Transmission Systems Design Handbook for Wireless Networks, Nor-
wood, MA: Artech House.

Lobo, A.F., Bashkirtsev, P., DeDomenico, R., Fabian, A., Gramatges, G., Hnatyshin, V., Metting, J., Simmons, M., & Stiefel, M., 2005. Modelling a University Computer Laboratory using OPNET Software, Available online: http://users.rowan.edu/~hnatyshin/Publications/ICTSMA_06.doc Accessed on 01 June 2012.

Maria, A., 1997. Introduction to modelling and simulation, Proceedings of the 1997 Winter Simulation Conference, Atlanta,Georgia.

Martin, J., Nilsson, A. & Rhee, I., 2000 .The incremental deployability of RTT-based congestion avoidance for high speed TCP Internet connections, Proceedings of the 2000 ACM SIGMETRICS international conference on Measurement and modelling of computer systems, p.134-144, June 18-21, 2000, Santa Clara, California, United States.

Shah, A., Harris, D. & Gutierrez, D., 2002. Performance of Remote Anatomy and Surgical Training Applications Under Varied Network Conditions. In P. Barker & S. Rebelsky (Eds.), Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2002 (pp. 662-667). Chesapeake, VA: AACE.

Matthew, L., 2003. Mission-Critical Network Planning, Artech House Telecommunications Library, Artech House Publishers.

Maximum likelihood network topology identification from edge-based unicast measurements,*ACM Sigmetrics Proceedings*, Marina Del Rey, CA.

Moon, S. B., Jim Kurose & Don Towsley, 1998 Correlation of Packet Delay and Loss in the Internet. Technical Report 98-11, Department of Computer Science, University of Massachusetts, Amherst, MA 01003.

Mondragon, R., Moore, A., Pitts, J. & Schormans, J., 2008. Analysis, simulation and measurement in large-scale packet networks. Published in IET Communications.

Moon, S., 2000. Measurement and analysis of end to end delay and loss in the Internet, Ph.D. thesis, University of Massachusetts, Armhest.

Nessoft Knowledge Base, 2011. Packet loss or latency at intermediate hops, Available online: http://www.nessoft.com/kb/24 Accessed on 04 June 2012.

OPNET Technologies, 2012. High Definition IT Performance Management, Available online: http://www.opnet.com/ Accessed on 02 June 2012.

Pathak, A., Pucha, H., Mao, Z.M., Hu, Y.C.A., & Zhang, Y., 2008. Measurement Study of Internet Delay Asymmetry, PAM.

Rabinovitch, E., 2012. Network Management Performance -Tips and Tools, Available online: http://www.uniforum.org/web/pubs/uninews/970411/feature2.html Accessed 06 June 2012.

Saltzer, J.H., Reed, D.P., & Clark, D.D., 1984. End-to-end arguments in system design, ACM Transactions on Computer Systems (TOCS).

Savage, S., 1999. “Sting: a TCP-based Network Measurement Tool,” In Proceedings of the 1999 USENIX Symposium on Internet Technologies and Systems”.

SolarWinds, Inc, 2008. Orion Network Performance Monitor: fault & performance management. Available online: http://www.solarwinds.com/resources/datasheets/OrionDatasheet.pdf Accessed on 04 June 2012.

SolarWinds, 2010. Orion Network Performance Monitor availability & performance management for your data center network, Available online: http://www.solarwinds.com/resources/datasheets/SolarWinds_OrionNPM_Datasheet.pdf Accessed on 04 June 2012.

Stevens, W. 1998."Unix Network Programming". 2 edition. Vol. 1. pp 85-110, Prentice Hall. NJ, USA

Suryawanshi, P., 2010. Internet Traffic Management, Available online: http://sit.iitkgp.ernet.in/research/aut04seminar1/8r.pdf Accessed on 04 June 2012.

The Cacti Group, 2012. Cacti Manual 0.8.7, Available online: http://docs.cacti.net/manual:087 Accessed on 04 June 2012.

Tian, S., 2001. ``The World Wide Web: a vehicle to interactive learning and teaching applications", Internet Research: Electronic Networking and Policy, Vol. 11 No. 1, pp. 74-83.

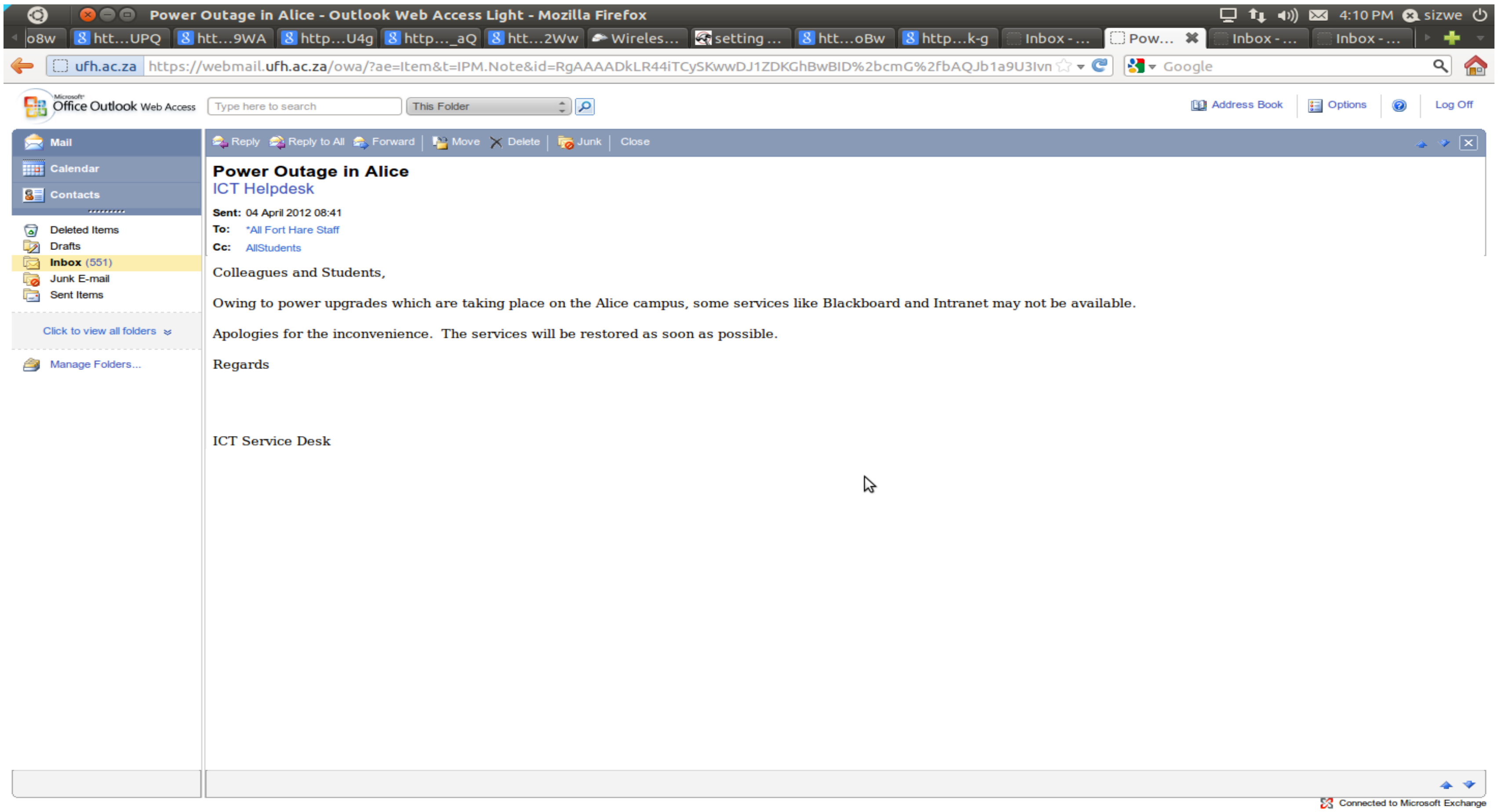
Vardi, Y., 1996. Estimating source-destination traffic intensities from link data, *Journal of the American Statistical Association*, 91, 365-377.

Welzl, M., 2005. Network Congestion Control: Managing Internet Traffic, Wiley Series on Communications Networking & Distributed Systems), John Wiley & Sons.

Zeitoun. A., Jamin. S., & Wang Z., 2003. Challenges and Lessons Learned in Measuring Path RTT for Proximity-based Applications, Proceedings of the Passive and Active Measurement Workshop, La Jolla, CA, USA, P. 181-191.

Appendix 1

UFH Internet disruption messages (emails)



Power Outage in Alice

ICT Helpdesk

Sent: 04 April 2012 08:41

To: *All Fort Hare Staff

Cc: AllStudents

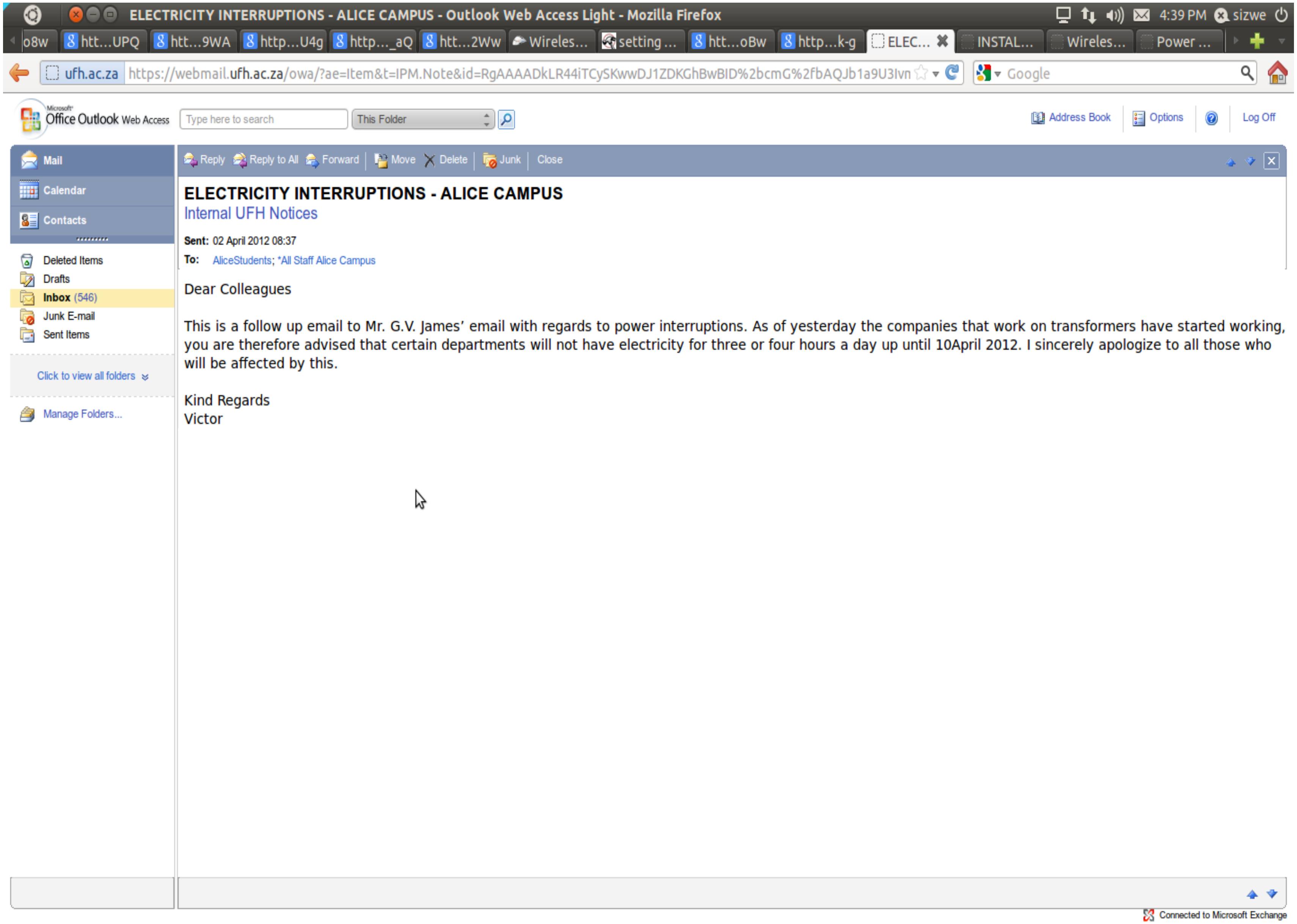
Colleagues and Students,

Owing to power upgrades which are taking place on the Alice campus, some services like Blackboard and Intranet may not be available.

Apologies for the inconvenience. The services will be restored as soon as possible.

Regards

ICT Service Desk


ELECTRICITY INTERRUPTIONS - ALICE CAMPUS - Outlook Web Access Light - Mozilla Firefox

https://webmail.ufh.ac.za/owa/?ae=Item&t=IPM.Note&id=RgAAAADkLR44iTCySKwwDJ1ZDKGhBwBID%2bcmG%2fbAQJb1a9U3Ivn

Mail
Calendar
Contacts
Deleted Items
Drafts
Inbox (546)
Junk E-mail
Sent Items
Click to view all folders
Manage Folders...

Reply | Reply to All | Forward | Move | Delete | Junk | Close

ELECTRICITY INTERRUPTIONS - ALICE CAMPUS

Internal UFH Notices

Sent: 02 April 2012 08:37

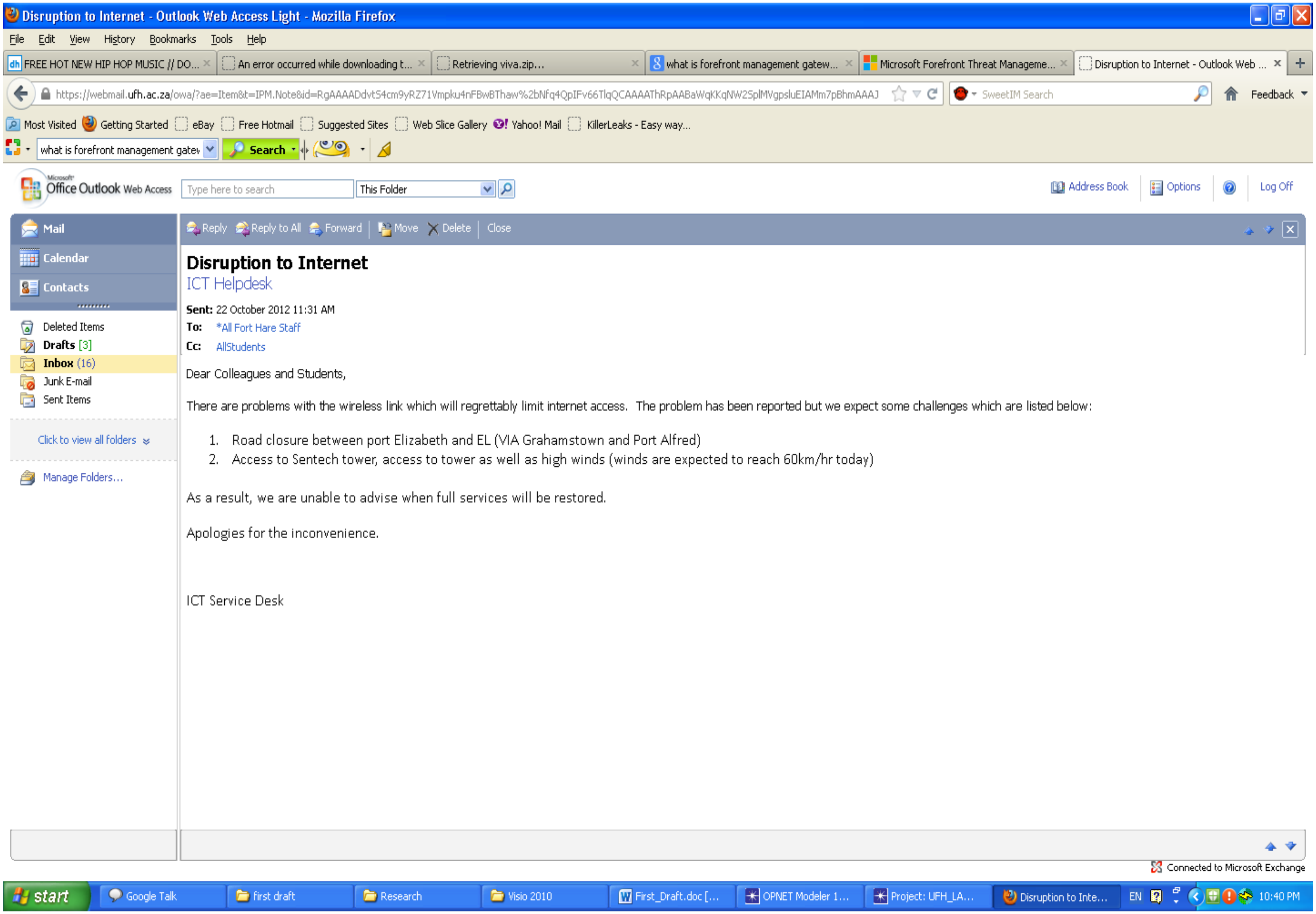
To: AliceStudents; *All Staff Alice Campus

Dear Colleagues

This is a follow up email to Mr. G.V. James' email with regards to power interruptions. As of yesterday the companies that work on transformers have started working, you are therefore advised that certain departments will not have electricity for three or four hours a day up until 10April 2012. I sincerely apologize to all those who will be affected by this.

Kind Regards
Victor

Connected to Microsoft Exchange



Disruption to Internet

ICT Helpdesk

Sent: 22 October 2012 11:31 AM

To: *All Fort Hare Staff

Cc: AllStudents

Dear Colleagues and Students,

There are problems with the wireless link which will regrettably limit internet access. The problem has been reported but we expect some challenges which are listed below:

1. Road closure between port Elizabeth and EL (VIA Grahamstown and Port Alfred)
2. Access to Sentech tower, access to tower as well as high winds (winds are expected to reach 60km/hr today)

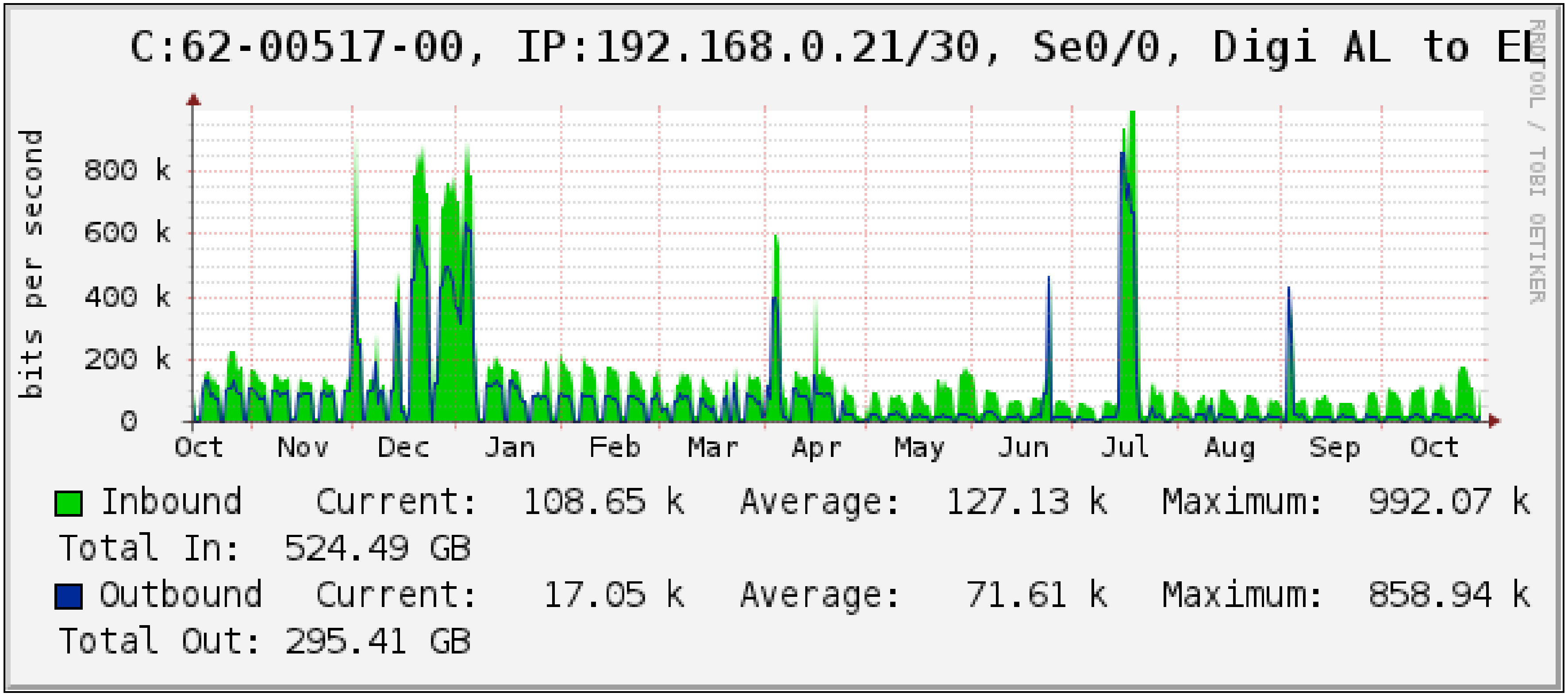
As a result, we are unable to advise when full services will be restored.

Apologies for the inconvenience.

ICT Service Desk

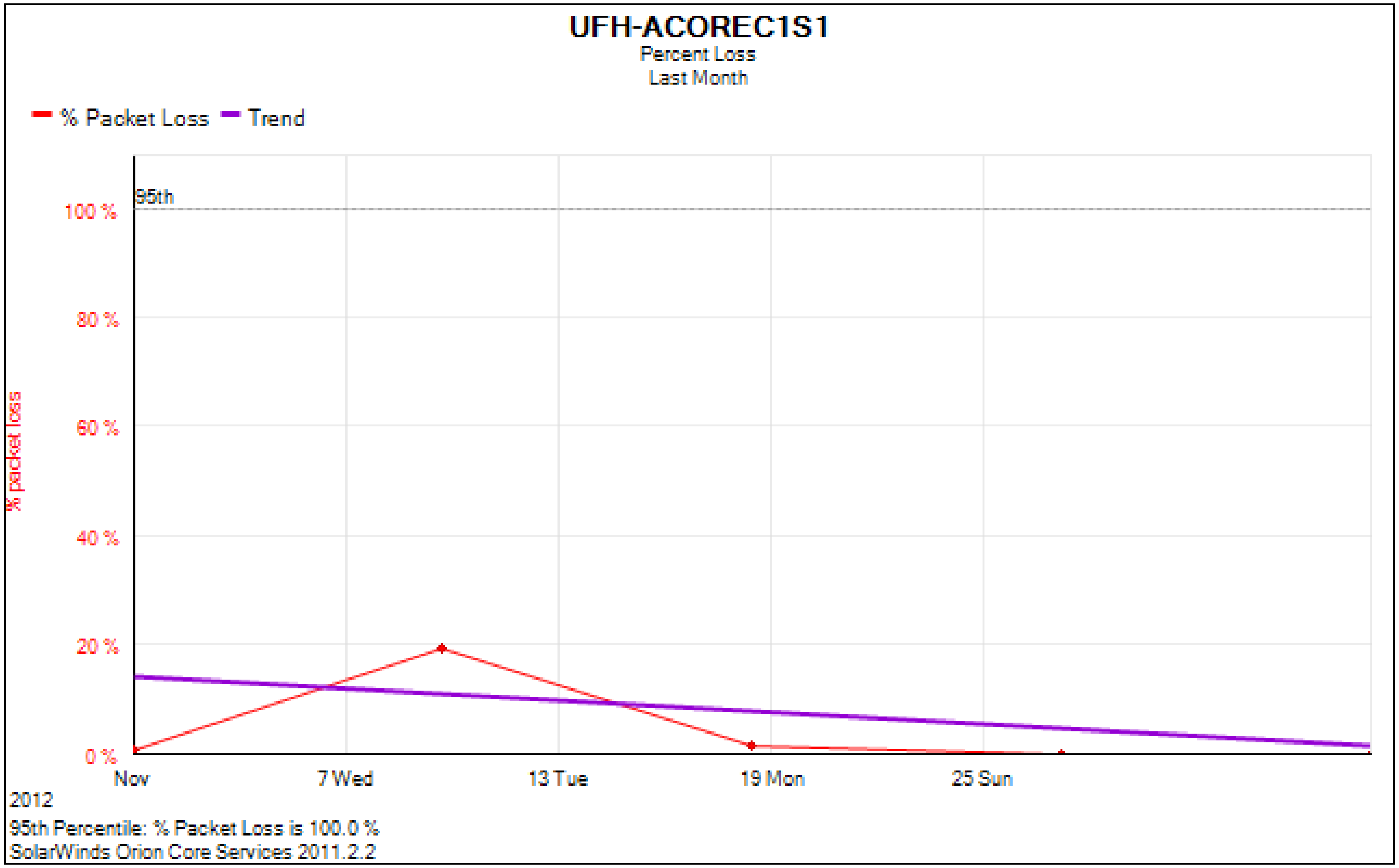
Appendix 2

Bandwidth usage

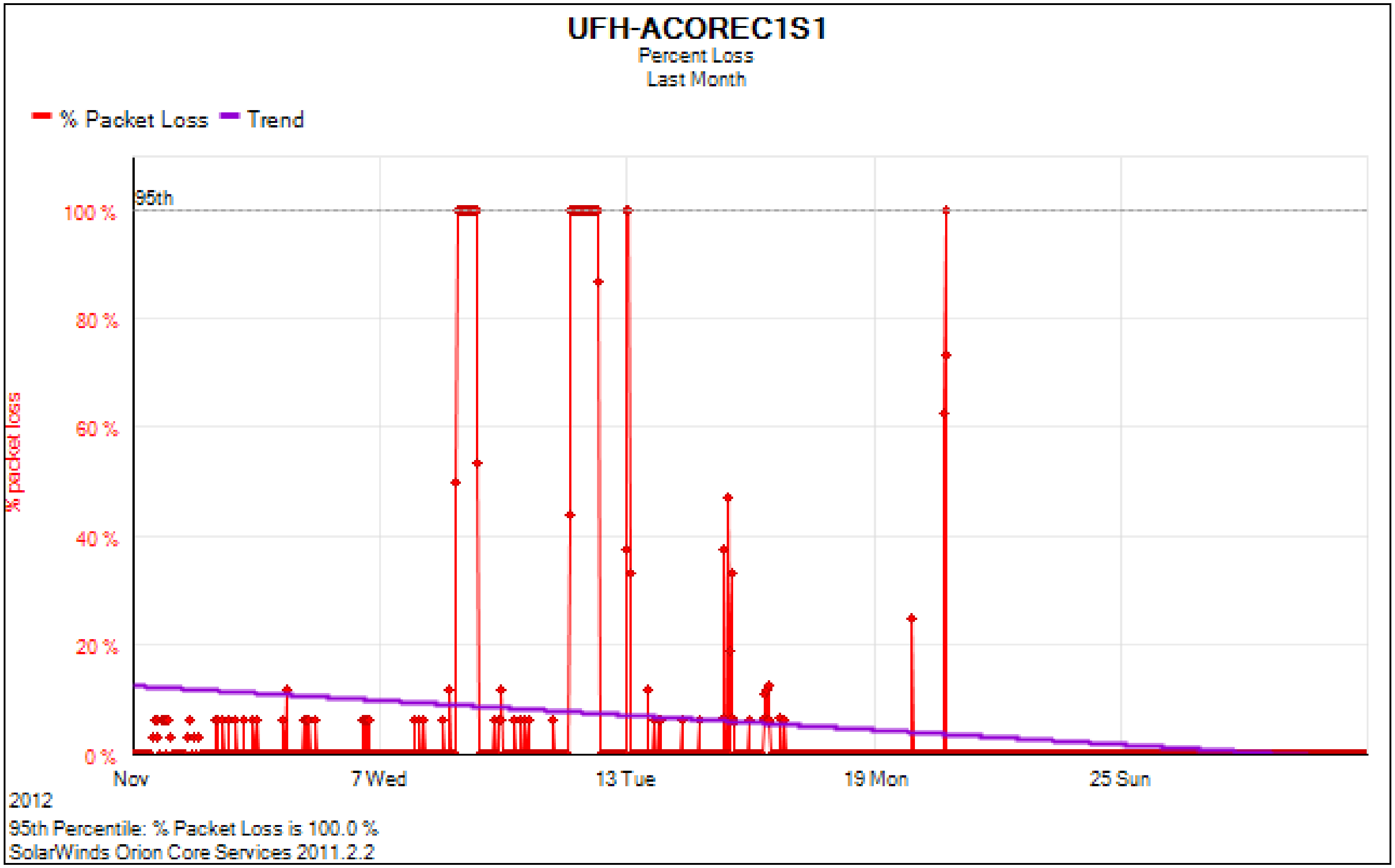


Yearly (1 Day Average)

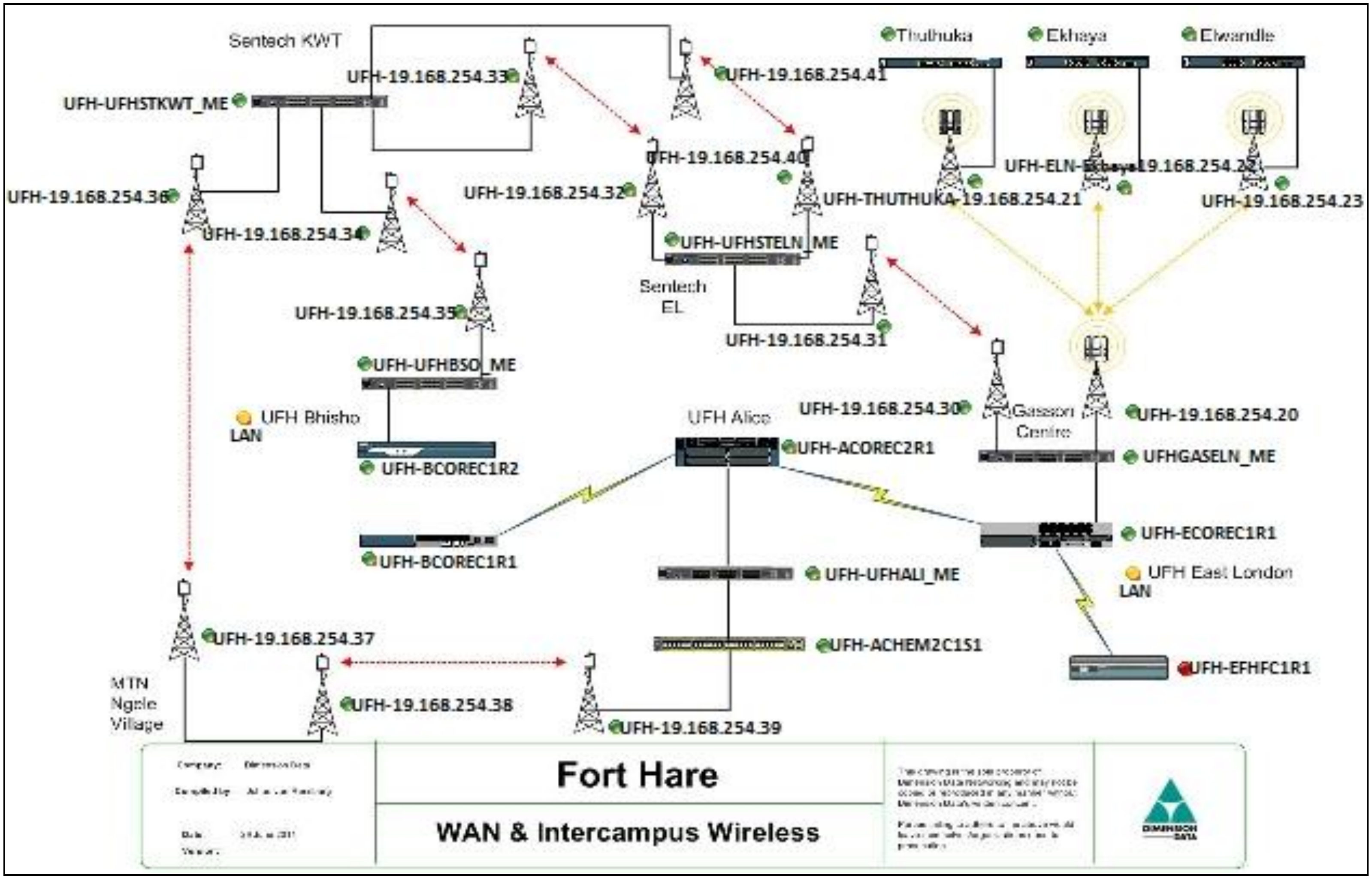
END-TOE-END WEEKLY(HOUR) PACKET LOSS



END-TOE-END MONTHLY(WEEKLY) PACKET LOSS



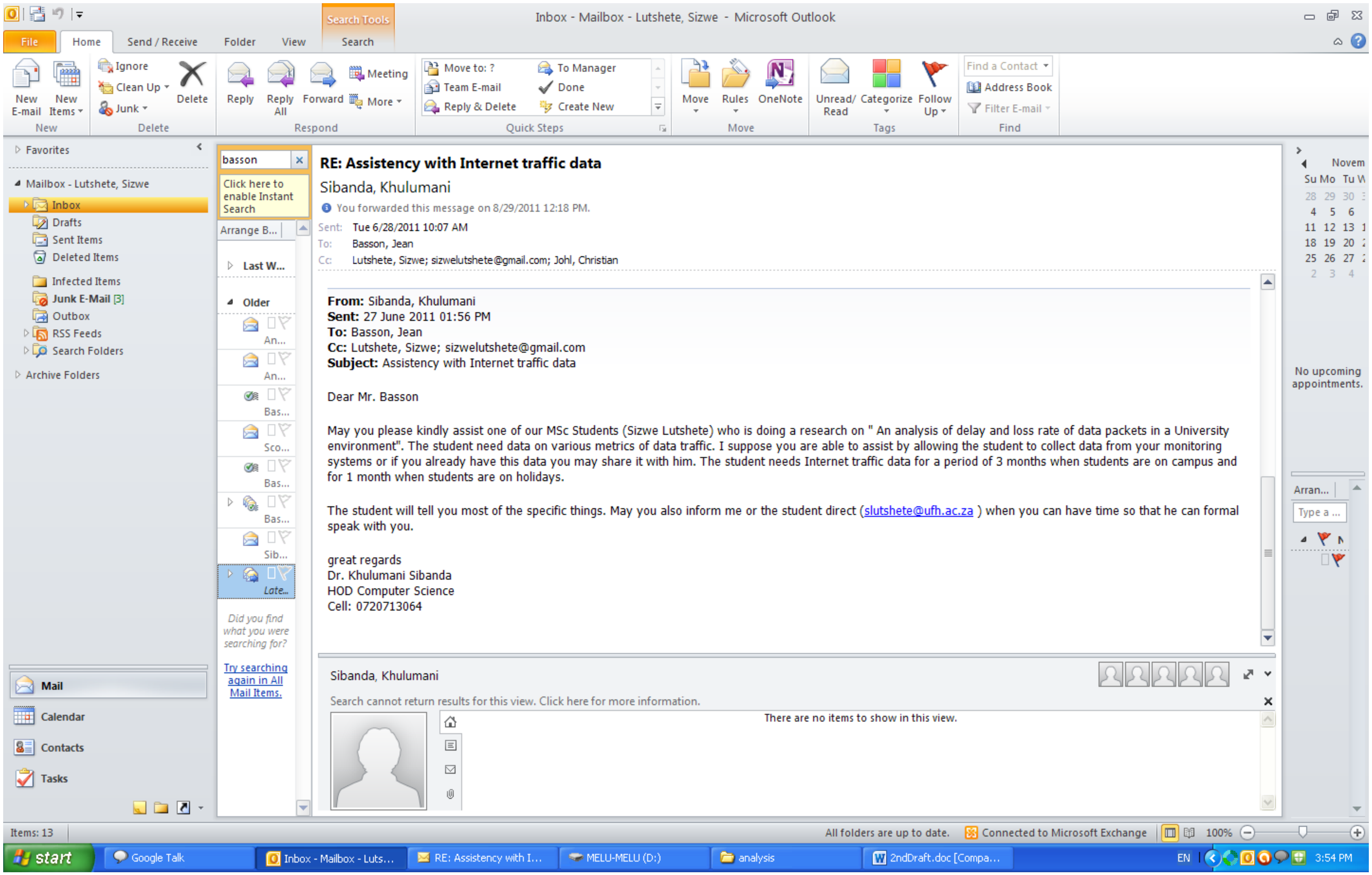
UFH NETWORK MAP



UFH Network Map

Appendix 3

Permision to undertake research



RE: Assistency with Internet traffic data

Sibanda, Khulumani

You forwarded this message on 8/29/2011 12:18 PM.

Sent: Tue 6/28/2011 10:07 AM

To: Basson, Jean

Cc: Lutshete, Sizwe; sizwelutshete@gmail.com; Johl, Christian

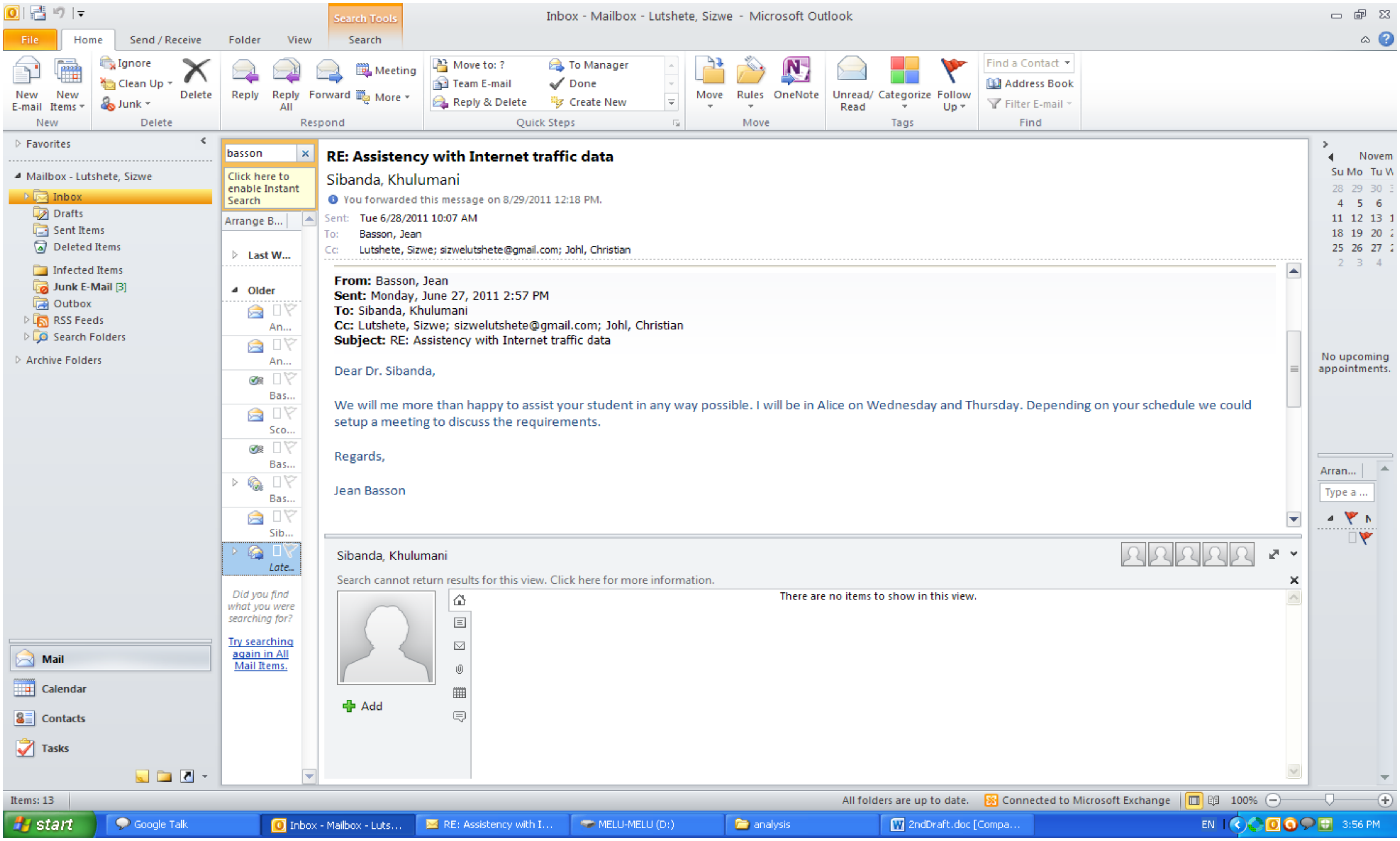
From: Sibanda, Khulumani
Sent: 27 June 2011 01:56 PM
To: Basson, Jean
Cc: Lutshete, Sizwe; sizwelutshete@gmail.com
Subject: Assistency with Internet traffic data

Dear Mr. Basson

May you please kindly assist one of our MSc Students (Sizwe Lutshete) who is doing a research on " An analysis of delay and loss rate of data packets in a University environment". The student need data on various metrics of data traffic. I suppose you are able to assist by allowing the student to collect data from your monitoring systems or if you already have this data you may share it with him. The student needs Internet traffic data for a period of 3 months when students are on campus and for 1 month when students are on holidays.

The student will tell you most of the specific things. May you also inform me or the student direct (slutshete@ufh.ac.za) when you can have time so that he can formal speak with you.

great regards
Dr. Khulumani Sibanda
HOD Computer Science
Cell: 0720713064


Inbox - Mailbox - Lutshete, Sizwe - Microsoft Outlook
RE: Assistency with Internet traffic data
Sibanda, Khulumani
You forwarded this message on 8/29/2011 12:18 PM.
Sent: Tue 6/28/2011 10:07 AM
To: Basson, Jean
Cc: Lutshete, Sizwe; sizwelutshete@gmail.com; Johl, Christian
From: Basson, Jean
Sent: Monday, June 27, 2011 2:57 PM
To: Sibanda, Khulumani
Cc: Lutshete, Sizwe; sizwelutshete@gmail.com; Johl, Christian
Subject: RE: Assistency with Internet traffic data
Dear Dr. Sibanda,
We will me more than happy to assist your student in any way possible. I will be in Alice on Wednesday and Thursday. Depending on your schedule we could setup a meeting to discuss the requirements.
Regards,
Jean Basson
Search cannot return results for this view. Click here for more information.
There are no items to show in this view.
All folders are up to date.
Connected to Microsoft Exchange