

DESIGN AND IMPLEMENTATION OF
INFRASTRUCTURE-BASED VLAN FOR SECURED
APPLICATIONS

SALIHU, ALHAJI BALA
M.ENG./SEET/2006/1577

DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING,
SCHOOL OF ENGINEERING AND ENGINEERING TECHNOLOGY,
FEDERAL UNIVERSITY OF TECHNOLOGY MINNA,
NIGER STATE.

JANUARY, 2011

DESIGN AND IMPLEMENTATION OF
INFRASTRUCTURE-BASED VLAN FOR SECURED
APPLICATIONS

SALIHU, ALHAJI BALA
M.ENG/SEET/2006/1577

A THESIS SUBMITTED TO THE POSTGRADUATE SCHOOL,
FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF
MASTER OF ENGINEERING (M. ENG.) DEGREE
IN ELECTRICAL AND COMPUTER ENGINEERING
(COMMUNICATION ENGINEERING OPTION).

JANUARY, 2011

DECLARATION

I, **SALIHU ALHAJI BALA** hereby declare that this work titled "Design and Implementation of Infrastructure-based VLAN for Secure Applications" was done by me in partial fulfillment of the requirements for the award of M.Eng. in Communication Engineering in the Department of Electrical and Computer Engineering, Federal University of Technology, Minna.

Saliyu, Alhaji Bala

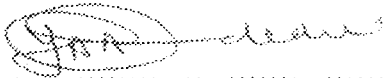


10/04/2011

(Signature and Date)

CERTIFICATION

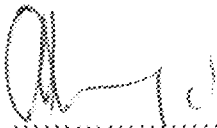
This thesis titled: Design and Implementation of Infrastructutre-based VLAN for Secured Application by Salihu, Alhaji Bala (M.Eng./SEET/2006/1577) meets the regulations governing the award of the degree of (M.Eng.) of the Federal University of Technology, Minna and is approved for its contribution to scientific knowledge and literary presentation.



ENGR. DR. Y. A. ADEDIRAN
SUPERVISOR

11/7/2011

DATE



ENGR. A. G. RAJI
HEAD OF DEPARTMENT
ELECTRICAL AND COMPUTER ENGINEERING

APRIL 11, 2011

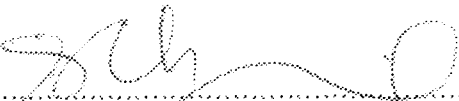
DATE



ENGR. PROF. M.S. ABOLARIN
DEAN, SEET

12/24/11

DATE



PROF. (MRS.) S.N. ZUBAIRU
DEAN, POSTGRADUATE SCHOOL

1/8/2011

DATE

Dedication

I dedicate this work to my parents

ACKNOWLEDGEMENTS

All praise and thanks are due to Allah the most exalted for making this work a reality. In putting together this work some individuals have contributed tremendously and I am grateful to them for their assistance. In this regard, my mentor Engr. Dr. Y. A. Adediran deserves a high level of appreciation for finding time to read through this work thoroughly, and for his suggestions which have assisted in improving the quality of this project. I would also like to acknowledge the contribution and encouragement of my H.O.D, Engr. A. G. Raji; the Dean of School of Engineering Prof. M.S Abolarin; the deputy Dean of School of Engineering Engr. Dr. O. Chukwu; the Dean, Postgraduate School, Prof. (Mrs.) S.N. Zubairu; the School Secretary, my colleagues in the department and all technical staff in the department. May Allah the exalted reward you all.

I cannot express my gratitude in words to my parents for their concern and constant prayers, my beloved wife Hafsat for all her love, support and encouragement, and to my brothers and sisters for their love, concern, support and prayers.

Special thanks go to Engr. (Mrs.) C. Alenoghena, Engr. J.G. Kolo , Engr. Dr. M.N. Nwohu, Engr. Dr. E. N. Onwuka whose counsel encouraged me to pursue this work to this end.

This acknowledgment will not be complete without acknowledging the encouragement and support of my brother and colleague Mallam Suleiman

Zubair, and finally, to all other well-wishers that are so numerous to mention.

Thank you all.

ABSTRACT

The objective of this work is to enhance the performance of an existing campus network (Ibrahim Badamasi Babangida University, Lapai, in this case) and to provide security measure for accessing important servers. This was accomplished by carrying out performance analysis of the existing network using analytical and simulation approach, then improving same by substituting the radio links with fiber optic link and incorporate Virtual Local Area Network (VLAN) into the design at a minimal cost and minimal change to existing network. The VLAN was implemented by enabling VLAN capability of the existing switches and configuring same for segmenting the network. An authentication server was also integrated to protect application servers. With this, we were able to improve the network performance, and also established that the VLAN can be implemented on the equipment already deployed in the Network and provide protection for secured application server.

TABLE OF CONTENTS

Title Page	ii
Declaration	iii
Certification	iv
Dedication	v
Acknowledgements	vi
Abstract	viii
Table of contents	ix
Abbreviation	xiii
List of Tables	xv
List of Figures	xvi
CHAPTER ONE	
1.0 INTRODUCTION	1
1.1 Background to the Study	1
1.2 Virtual Local Area Network	3
1.2.1 Broadcast Domain	4
1.2.2 Collision Domain	5
1.2.3 VLAN Identifications	6
1.3 VLAN Architectures	6
1.3.1 Service-based VLAN	7
1.3.2 Infrastructure-based VLAN	9
1.4 VLAN and Security Drives for Local Area Network	10
1.5 Problem Statement	12
1.6 Methodology	12

1.7 Aims and Objectives	13
1.8 Scope and Limitation	14
CHAPTER TWO	
2.0 LITERATURE REVIEW	15
2.1 Background of the review	15
2.2 Characterization of VLAN	15
2.3 Earlier motivations for VLAN in a network	17
2.4 History of some problems in setting up VLANs	22
2.4.1 Evolution of Standards and Proprietary concepts of VLANs	22
2.4.2 802.1 Internetworking subcommittee	23
2.4.3 802.10 VLAN standard	24
2.5 VLAN State-of-the-Art Design Alternatives	24
2.5.1 Customer VLAN model	25
2.5.2 Serviced-based VLAN Model	26
2.5.3 C-VLAN: Adding an Intermediate Aggregation Switch	26
2.5.4 Hybrid-Customer VLAN with multicast VLAN	27
CHAPTER THREE	
3.0 MATERIALS AND METHODS	33
3.1 Network Configuration	33
3.2 Network Performance Estimates	36
3.2.1 Performance estimates using standard formulae	36
3.2.2 Performance estimates using simulator	39
3.3 Network design	42
3.3.1 Topological design	43

3.3.2 VLAN design and implementation	51
3.4 VLAN Configuration	51
3.4.1 Network equipment for VLAN implementation	51
3.4.2 Switch configuration	52
3.4.3 VLAN database configuration	54
3.4.4 Ports configuration	55
3.4.5 Access link and trunk link	55
3.5 DHCP server configuration	58
3.6 Configuring inter-VLAN routing	60
3.7 Authentication scheme for secured application	61
3.7.1 Authentication server configuration	62
3.7.2 User verification procedure	63
CHAPTER FOUR	
4.0 RESULTS	66
4.1 Analytical result of the network dissection	66
4.2 Simulation result before VLAN implementation	68
4.3 Simulation result after VLAN implementation	72
4.4 Test for infrastructure-based VLAN	73
4.5 Test for secure application	73
CHAPTER FIVE	
5.0 DISCUSSION, CONCLUSION AND RECOMMENDATIONS	75
5.1 Discussion	75
5.1.1 Analytical results	75
5.1.2 Simulation results	76

5.2 Conclusion	76
5.3 Recommendations	78
REFERENCES	79

ABBREVIATIONS

ATM	Asynchronous Transfer Mode
BSR	Broadband Services Router
CATV	Cable Television
CoS	Class of Service
DMZ	Demilitarised Zone
DSCP	Differentiated Service Code Point
DSLAM	Digital Subscriber Line Access Multiplexor
IEEE	Institute of Electrical Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPSec	Internet Protocol security
IPv4	Internet Protocol Version 4
L2	Layer 2
LAN	Local Area Network
LANE	LAN Emulation
MAC	Media Access Control
MAVPN	Multiply Access Virtual Private Network
MIS	Management Information System
MPOA	Multiprotocol over ATM
MSANs	Multiservice Access Node
NAC	Network Access Control
OLT	Optical Line Termination

OS	Operating System
PVLAN	Private Virtual Local Area Network
QoS	Quality of Service
SSL	Secure Socket Layer
ToS	Type of Service
UDP	User Datagram Protocol
VID	VLAN Identification
VLAN	Virtual Local Area Network
VoD	Video on Demand
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

LIST OF TABLES

Table		Page
3.1	D _x Table, N _x = switch area x, d _{ij} = distance between Switch area i and switch area j.	45
3.2	D ₀ ; The initial starting distance matrix from the diagram in figure 3.6. (the distances are measured in kilometres)	46
3.3	S ₀ ; The initial sequence matrix from the diagram in figure 3.6	47
3.4	VLANs, users and server distribution	51
3.5	Switch ports configuration	56
4.1	Network properties before and after VLAN	67
4.2	Central switch interface IP addresses	70

LIST OF FIGURES

Figure	Page
1.1 Network layouts with two broadcast	4
1.2 VLAN segmentation	5
1.3 Service-Bases VLAN	8
1.4 Infrastructure VLAN paradigm	11
2.1 VLAN edge vs Trunk port	21
2.2 Customer VLAN model (a VLAN per customer)	25
2.3 Service VLAN Model	26
2.4 C-VLAN Ethernet frame with intermediate switch	27
2.5 Hybrid C-VLAN with M-VLAN Model	28
2.6 Logical network configuration of the prototype system	31
3.1 Ibrahim Badamasi Babangida University, Lapai main campus network layout	35
3.2 M/M/1 queue system of the entire network	36
3.3 Ping result between user 1 and Router 0 at ICT Centre	41
3.4 Ping result between user 91 and Router 0.	41
3.5 Network topology	44
3.6 Floyd's iterations 0 -3 result display	48
3.7 Floyd's iterations 3 -5 result display	49
3.8 spanning tree algorithm result display	50
3.9 Network symbol and properties of 2960-24TT switch	52

3.10	Physical appearances for 2960-24TT switch	52
3.11	configuration panels for switches	53
3.12	renaming area 1 switch	54
3.13	VLAN configuration for panel for switches	55
3.14	port configuration panel	58
3.15	DHCP server configuration panel	59
3.16	users IP configuration panel	60
3.17	RADIUS server configuration panel	62
3.18	RADIUS server configuration panel	60
3.19	RADIUS packet structure, request and response in computer	
	Network	64
4.1	Communications between users connected to different switches	68
4.2	Intra switch link test	69
4.3	Ping replies received at the user 1 terminal from router 0 (average time taken for reply is 39ms)	71
4.4	Ping replies received at the user 91 terminal from router 0 (average time taken for reply is 128ms)	71
4.5	Ping replies received at the user 159 terminal from router 0 (average time taken for reply is 113ms)	72
4.6	Intra and inter switch communication attempts	73
4.7	Communication links to test link to server from various network users	73
4.8	User login verification	74

CHAPTER ONE

1.0 INTRODUCTION

1.1 BACKGROUND TO THE STUDY

In any computing environment that supports multiple processes, there must be some mechanism for resource allocation among competing processes, as well as the enforcement of access control policies based on the privileges assigned to that process compared to the requirements of the resource. In a traditional timesharing operating system, these policies are enforced by kernel, such as when the application programme makes a system call. In the networking context, firewalls play a similar role in policy enforcement for sessions and/or individual datagram attempting to cross the boundary separating the "inside" and "outside" worlds (Minli *et al*, 2007).

The individual hosts often view the network as an untrustworthy resource. Hence, the host operating system has the primary responsibility for managing network resources, such as the configuration of the network interface to detect and block unauthorized remote accesses and while protecting the integrity of its own network traffic via encryption (e.g. IPsec, SSL, VPN.) or other means.

In recent years, researchers have advocated the need for concepts that model the fundamental design intent of a network manager's actions, and capture the ultimate network-wide performance, security, manageability and resilience objectives of the designer. While there has been tremendous attention and progress towards the design of network-wide abstractions in

certain domains, surprisingly little attention has been paid to the management of enterprise and campus networks. Despite their critical importance, and their striking differences and diversity compared to carrier networks, there is little systematic understanding of these networks in the community.

Large networks of any type are plagued by surges of traffic, which can lead to significantly degraded network performance as well as downtime (Prashant *et al*, 2007). These surges of traffic are frequently due to virus outbreaks, poor network management, misuse of network resources by the network users, among other factors.

A technique to easily and reliably control *access to network resources* for effective *management* would be a great value to a number of organisations. There had been a number of approaches to address these problems. Such include implementation of VLAN for virus containment (Aeron, 2009), Dynamic Access Control Scheme for Service-Based Multi-netted Asymmetric Virtual LAN (Wonwoo *et al*, 2005), design and implementation of Application-based Secured VLAN (Minli *et al*, 2007), and VLAN-based QoS control in mobile Networks (Minsato *et al*, 2006).

This work, considers an instance where a server operating system (OS) alone can enforce the desired resource allocation and access control policies, and change the scenario to have complete control over all the nodes within a network through switches at the edge of the network rather than depending on the server OS. Policy scheme and access control can be implemented in the networking hardware (like switches), without making any changes to the hosts

(nodes). This will be achieved using the standard techniques specified in VLAN 802.1Q, 802.1p and VLAN identification (VID).

IEEE 802.1Q (also known as VLAN Tagging) was a project in the IEEE 802 standards process to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between the networks. IEEE 802.1Q is also the name of the standard issued by this process, and in common usage, the name of the encapsulation protocol used to implement this mechanism over Ethernet networks. Due to the configuration parameter used by Cisco devices to enable 802.1Q, it is also commonly referred to as **dot1Q**.

IEEE 802.1p specification enables Layer-2 switches to prioritize traffic and perform dynamic multicast filtering. The prioritization specification works at the media access control (MAC) framing layer. The 802.1p standard also offers provisions to filter multicast traffic to ensure it does not proliferate over layer-2 switched networks.

VLAN Identifier (VID) is contained within each Ethernet frame of an Ethernet VLAN. It thus allows switches to separate traffic based on VID, hence creating separate VLAN.

1.2 Virtual Local Area Network

One of the common, though somewhat advanced, technologies that make designing and maintaining a LAN easier today than in previous years is the Virtual LANs. By default, switches break up collision domain and routers

break up broadcast domains. Breaking up broadcast domains in pure switch network could be achieved by creating a Virtual LAN.

Virtual Local Area Network (VLAN) is a logical grouping of network users and resources connected to administratively defined ports on a switch. When one creates VLANs, one is given the ability to create smaller broadcast domain within a layer 2 switch inter-networked by assigning different ports on the switch to different sub networks.

1.2.1 Broadcast Domain

A *broadcast domain* is everywhere a data-link level (e.g. Ethernet) broadcast frame would propagate to. This area is demarcated by routers, which signal the end of a layer-2 (data-link layer) network; to go further requires support at a higher layer, such as layer-3 (e.g. IP) to *route* the *packets* through the *inter-network*.

So, looking at the network layout in figure 1.1 we can see that there are two broadcast-domains, labelled A and B demarcated by a router.

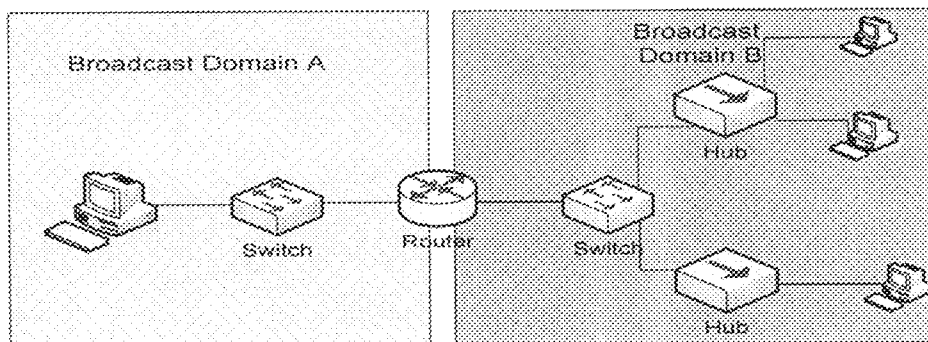


Figure 1.1: Network layouts with two broadcast

As shown in fig 1.2 a VLAN provides the ability to segregate a switch into separate broadcast-domains. This means that in order to get across between the different LANs, a router is not a must. In the olden days, when VLANs were still new, a *single router* was used, which had an interface on all VLANs; today such a configuration would be more likely to be called a "router on a stick". Today however, a high-speed router is embedded as part of the switch; this switch is then referred to as a *layer-3 switch*.

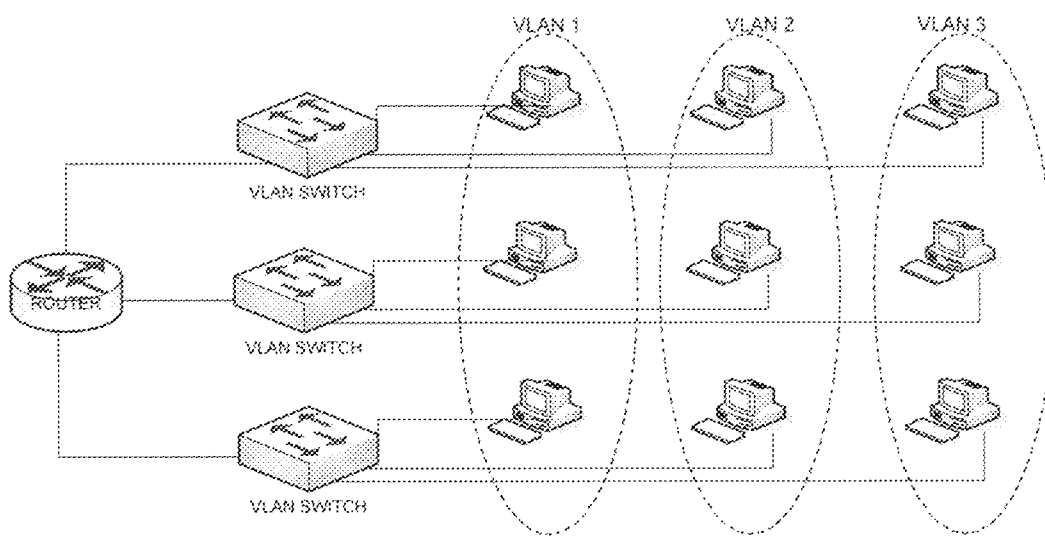


Figure 1.2. VLAN segmentation

1.2.2 Collision Domain

A collision domain is a physical network segment where data packets can "collide" with one another for being sent on a shared medium, in particular in the Ethernet networking protocol. A network collision is a scenario wherein one particular device sends a packet on a network segment, forcing every other device on that same segment to pay attention to it. Meanwhile, another

device does the same, and the two competing packets are discarded and resent one at a time. This becomes a source of inefficiency in the network.

If a group of Ethernet or fast Ethernet devices in a CSMA LAN are connected by repeaters they will compete for access on the network. This situation is typically found in a hub environment where each host segment connects to a hub that represents only one collision domain and only one broadcast domain. Only one device in the collision domain may transmit at any time, and the other devices in the collision domain listen to the network in order to avoid data collisions. Collisions decrease network efficiency. VLAN, in the contrary, segments collision domain thereby allowing many hosts within Ethernet network to transmit without collision. Both computers that attempt to transmit must back off; wait for a random period of time, which is generated independently by each computer, and then retransmit.

1.2.3 VLAN Identifications

VLANs are identified by a 12-bit number (i.e. 4096 different VLAN IDs are possible). A switch-port may be a member of a number of VLANs; in the case of multiple VLAN assignments to a port, *trunking* must be used, which is to say that the frames are *tagged* with their VLAN identifier so that the neighbourhood device (typically a switch or a router) can know which network it belongs to.

1.3 VLAN ARCHITECTURES

Due to the trends toward server centralization, enterprise-wide e-mail, and collaborative applications, various network resources will need to be made available to users regardless of their VLAN membership. Ideally, this access

should be provided without most user traffic having to traverse a router. Organisations that implement VLANs recognise the need for certain logical end-stations (for example, centralized servers) to communicate with multiple VLANs on a regular basis, either through overlapping VLANs (in which network-attached end-stations simultaneously belong to more than one VLAN) or via integrated routing that can process inter-VLAN packets at wire speed. From a strategic standpoint, these organisations have two ways to deploy VLANs: a "service-based" VLAN implementation or an "infrastructure-based" VLAN implementation. The choice of approach will have a substantial impact on the overall network architecture, and may even affect the management structure and business model of the organisation.

1.3.1 Service-Based VLANs

A service-based approach to VLAN implementation looks, not at organisational or functional groups, but at individual user access to servers and applications—that is, network resources. In this model depicted in fig 1.3, each VLAN corresponds to a server or service on the network. Servers do not belong to multiple VLANs but groups of users do. In a typical organization, all users would belong to the e-mail server's VLAN, while only a specified group, such as the accounting department plus top-level executives, would be members of the accounting database server's VLAN. By its nature, the service-based approach creates a much more complex set of VLAN membership relationships to be managed.

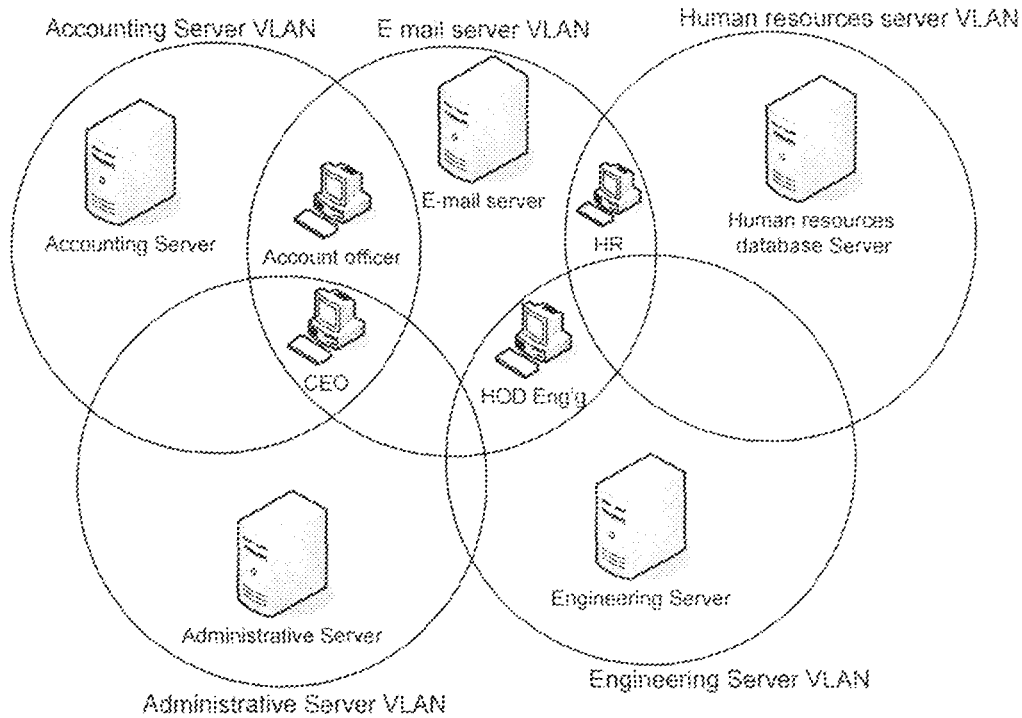


Figure 1.3: Service-Base VLAN

Given the level of most VLAN visualization tools presently available, a large number of overlapping VLANs using the service-based approach could generate incomprehensible multilevel network diagrams at a management console. Therefore, to be practical, service-based VLAN solutions must include a high level of automatic configuration features.

However, in response to the types of applications that organisations want to deploy in the future, as well as the shift away from traditional and more rigid organisational structures, the trend in VLAN implementation will be toward the service-based approach. As bandwidth to the desktop increases and as vendor solutions become available to better manage greater VLAN overlap, the size of the groups that belong to a particular set of VLANs may become smaller and smaller.

At the same time, the number of these groups may increase, to the point where each individual could have a customized mix of services delivered to his or her workstation. Taking that concept a step further, control over what services are delivered at a given time could be left up to each individual user. At that point, the network structure begins to take on the multiple-channel characteristics of a cable TV (CATV) network. In fact, at this stage, this model finds the greatest degree of similarity in VLANs defined by IP multicast group, where each workstation has the choice of which IP multicast or "channel" it wants to belong to. In such a future environment, VLANs lose the characteristics of static or semistatic broadcast domains defined by the network manager, and become channels to which users subscribe.

Users simply sign up for the applications they need delivered to them at a particular time. Nevertheless, application use could be accounted for, by enabling precise and automated chargeback for network services. Network managers could also retain control in order to block access to specific channels by certain users for security purposes.

1.3.2 Infrastructure-based VLANs

An infrastructural approach to VLANs is based on the functional groups (that is, the departments, workgroups, sections, etc.) that make up the organisation. Each functional group, such as accounting, management and information system (MIS), and engineering, is assigned to its own uniquely defined VLAN. Based on the 80/20 rule, the majority of network traffic is assumed to be within these functional groups, and thus within each VLAN. In

this model, VLAN overlap occurs at network resources that must be shared by multiple workgroups. These resources are normally servers, but could also include printers, routers providing WAN access, workstations functioning as gateways, and so forth.

The amount of VLAN overlap in the infrastructural model is minimal, involving only servers rather than workstations—making VLAN administration relatively straightforward. In general, this approach fits well in those organizations that maintain clean, discrete organisational boundaries. The infrastructural model is also the approach most easily enabled by presently available solutions and fits more easily with networks deployed today. Moreover, this approach does not require network administrators to alter how they view the network, and entails a lower cost of deployment. For these reasons, most organisations should begin with an infrastructural approach to VLAN implementation.

As can be seen in the example in Figure 1.4, the e-mail server is a member of all of the departments' VLANs, while the accounting database server, Engineering server and MIS server are only a member of their respective VLAN only.

1.4 VLAN and security drives for Local area networks

As VLANs are driven by the need to create security in depth, many organisations are beginning to realise that traditional security-firewalls, intrusion detection, antivirus, and content filtering are not enough. They realise that security must exist at all levels of information exchange/sharing environment.

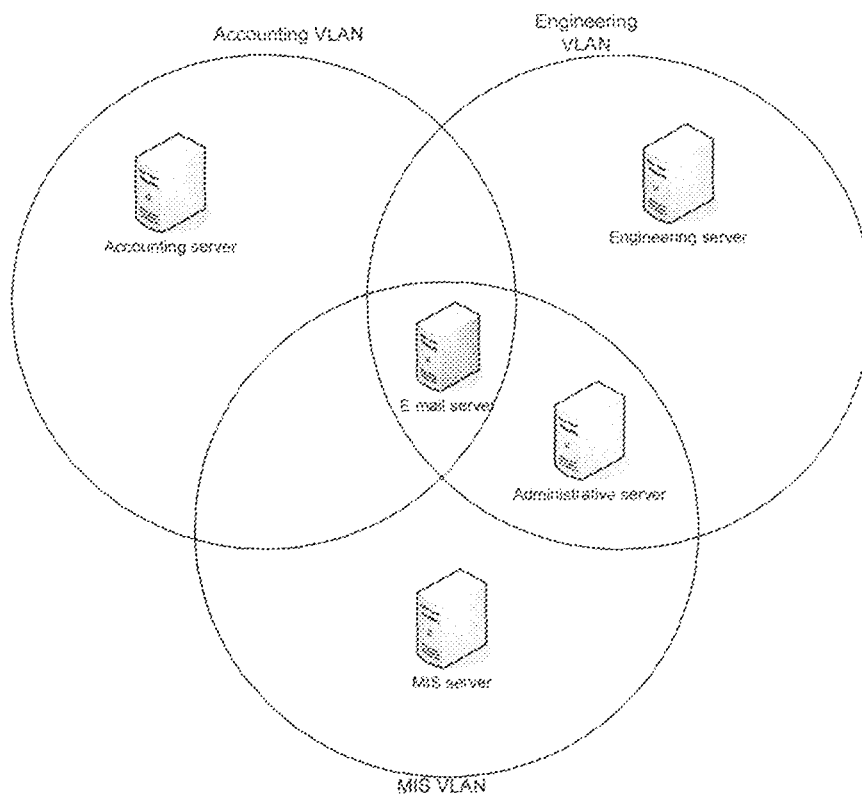


Figure 1.4: Infrastructure VLAN paradigm

Securing access to LAN switch ports in an organisation is not about an employer not trusting its employees. Rather it is about securing communications between different logical layers of a network. It is also about implementing rational security policies.

Progress requires change. Change requires critical thinking-an objective look at what is possible. Anytime a new technology is introduced, there is resistance, and for good reason. Technologies need to be streamlined, audited, simplified before they gain general acceptance. VLANs are no different. When introduced in 1998, only a few organisations were bold enough to try and deploy the technology. Years later, the wrinkles are ironed out. It is now acceptable in the mainstream. VLANs are poised to be as

ubiquitous as firewalls. VLANs usage could provide good security policy. They are ideal for those environments that have mobile users in a campus setting. Good examples of this include higher institutions in Nigeria, government complexes, hospitals and healthcare facilities. The technology can enhance wireless LAN security through segregation and strong authentication. VLANs are also used in telecommunications carrier provisioning services where each VLAN can be defined for each of the carrier's unique customers or for service classifications.

1.5 PROBLEM STATEMENT

Intrusion into secured application/database within an enterprise network by unauthorised users has been a common challenge that hinders the information privacy/ security within an organisation. Total or physical isolation of the secured application/server from the hypothetical LAN will pose the challenge of buying more switches or routers, and make the server out of reach for the authorised users within the LAN. However, proper integration of the secured server with the existing network could be achieved with implementation of VLAN. More to the VLAN implementation is ability to secure the server by defining policy for all the network users. This work is therefore aimed at design and implementation of Infrastructure-based VLAN for Secure application for an enterprise network.

1.6 METHODOLOGY

The implementation of this scheme (*Design and Implementation of Infrastructure-based VLAN for Secure Applications*) is to be carried out in the following order:

- I. Evaluating the performance of the existing Local Area Network (LAN) of Ibrahim Badamasi Babangida University, Lapai main campus using standard formulae and simulator;
- II. Effecting the necessary changes (equipment and link media) and proposing a new architecture for the campus network;
- III. Optimising the proposed architecture and configuring VLAN on the switches to segment the hosts into required number of VLANs;
- IV. Identifying each host within various VLANs by tagging using VLAN ID techniques;
- V. Choosing a VLAN for the application server to be secured;
- VI. Defining encryption algorithm for accessing the application server for authorised users.

1.7 Aim and objectives

The implementation of the infrastructure-based VLAN will provide the following benefits for the network.

- **Quality of Service:** Three 802.1p bits are used to form layer-2 class of service (CoS) bits that enable traffic differentiation. Traffic differentiation includes congestion management, the basis of QoS-aware service provisioning in packet-switched networks
- **Security:** VLAN ensures improved security, work group management and traffic control.
- **Simplified administration.** : Seventy percent of network costs are as result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, re-cabling, new station addressing, and reconfiguration of hubs and routers become necessary. Some of

these tasks can be simplified with the use of VLANs. If a user is moved within a VLAN, reconfiguration of routers is unnecessary. In addition, depending on the type of VLAN, other administrative work can be reduced or eliminated. However, the full power of VLANs will only really be felt when good management tools are created which can allow network managers to drag and drop users into different VLANs or to set up aliases.

- **Reduced Cost:** VLANs can be used to create broadcast domains which eliminate the need for expensive routers.
- Safe guarding an application server against unauthorised user within a network.
- Identifying each user/terminal within a network.

1.8 Scope and Limitation

This project is limited to implementation of VLAN for securing an application in a given server, and optimizing the campus network. Other security and counter-security measures were not considered. The effort is totally geared towards achieving distinct isolation of secured-server using VLAN 802.1Q segmentation techniques and enabling access to only certified hosts.

CHAPTER TWO

2.0

LITERATURE REVIEW

This chapter presents the review which guides the study of VLAN capability in enhancing network performance and discusses specific findings that provide insights in formulating the research problem, methodology, design, and implementation. The search for relevant literature was extended to include VLAN implementation for security, network optimization, access control, quality of service (QoS) and various combinations of these.

The review is divided into parts which include characterisation of VLAN, desires/motivations for VLAN implementation, problem in setting up effective VLAN, how to use VLAN to optimize network and other researchers' overview on similar topics.

2.1 CHARACTERIZATION OF VLAN

The first industry conference devoted entirely to virtual LANs (VLANs) was held in Santa Clara, CA. Nearly 350 attendees had discussion about all the possible definitions of what a VLAN is- or what a VLAN should be and about vendor products and strategies, user experience with VLAN implementation and the latest about the asynchronous transfer mode (ATM) forum's initiatives on LAN Emulation, Multiprotocol over ATM (MPOA) and network management (John *et al*, 1996)

One way to understand the essence and nature of implementing VLAN is to analyse some definitions accredited to it. The *Virtual Local Area Network* (VLAN) has been defined by many researchers and network developers. For

(VLAN) has been defined by many researchers and network developers. For example, Cisco defines VLAN as a logical grouping of network users and resources connected to administratively defined ports on a switch (Cisco, 2006). A very basic definition of the term VLAN is based on the meaning of broadcast domain. However, according to Decisys (1996), defining precisely what VLANs are, has become a contentious issue. Yet, most people would agree that VLAN can be roughly equated to a broadcast domain. More specifically, VLANs can be seen as analogous to a group of end-stations, perhaps on multiple physical LAN segments, that are not constrained by their physical location and can communicate as if they were on a common LAN.

However, issues such as the extent to which end-stations are not constrained by physical location, the way VLAN membership is defined, the relationship between VLANs and routing, the relationship between VLANs and ATM have been left up to each vendor. To a certain extent these are tactical issues, but how they are resolved has important strategic implications.

In the same vein, a VLAN is also defined as a logical grouping of end stations such that all end stations in the VLAN appear to be on the same physical segment even though they may be geographically separated (Wonwoo *et al*, 2005). Most definitions of VLAN by different researchers, network equipment manufacturing companies and authors build up their definition(s) by either considering VLAN to be logical grouping or separation of broadcast domain. Thus, from these definitions, a generalised meaning of VLAN could be formulated as: A VLAN is a logical grouping of end stations with each group

having separate broadcast domain with inter-communication ability among different groups.

2.2 Earlier Motivations for VLAN In a Network

Since VLANs were introduced in February 1993 two major benefits –reducing management cost associated with moves, adds and changes and performance improvements for client-server applications have been used to quantify and justify VLAN implementation. The management benefits are totally attributed to the nature of VLAN service itself. VLAN technology proposes to solve three problems in switched LAN networks. First is to improve efficiency and performance by constraining broadcast (including multicast). Second is to promote security by erecting firewalls that can be used to enforce access control policies. Third is to ease management of end-station moves and changes, ensuring that traffic from a given subnet is always delivered to intended host(s) (John *et al.*, 1996).

Because VLAN permits hosts connected to LAN switch to be organised into logical groups as a function of some administrative strategy, it is flexible for user/host management, bandwidth allocation and resource optimization (Misato *et al.*, 2006). This manageability and logical grouping advantage of VLAN paves way for its application and implementation in areas like network security, bandwidth management, network resource control and ensuring quality of service (QoS) in a given Ethernet network.

Examples of VLAN for network security is found in the implementation of

VLAN for Virus containment (Aeron, 2004). VLAN was implemented to curb the spread of virus within a Local Area Network by tracking and quarantining the infected host(s) until disinfected. Similarly, (Minli Zhu *et al*, 2006) designed and implemented application-based secured VLAN (AS-VLAN), a prototype system. This application-based S-VLAN architecture is suitable for hotspots, university and enterprise LANs, and can efficiently prevent intruders from interrupting secured applications. The Application-based Secure VLAN (ASVLAN) is simpler and more efficient than IPsec in LAN environment as it conforms to Layer-2 semantics, and it is cost-efficient to real-time applications such as VoIP. VLAN is also used to improve security by isolating groups. High-security users can be grouped into a VLAN, not necessarily on the same physical segment, and no users outside that VLAN can communicate with them.

According to Oizak (2006), VLANs are ideal for restricting traffic. For example, a logical Demilitarized Zone (DMZ) can be created by using a VLAN. Packets entering the DMZ are assigned a restricted VLAN ID that allows access only to devices on the DMZ. So far, this is not different from a standard physical DMZ; the difference is the flexibility of the VLAN approach. DMZ devices on a VLAN don't have to be physically located together. DMZ servers can be located anywhere on the enterprise network—as long as they all share the same VLAN ID.

Carrying VLANs a step further, restricted network segments can be created for workstations that are identified as infected with malware (harmful

softwares such as viruses, Trojans designed to cause damage or disruption to a computer system) or that fail to meet specific security requirements. Because of the distributed nature of VLANs, endpoint devices from anywhere on the enterprise network can reside on a single restricted segment.

Similarly, the ability of VLANs to create firewalls can also satisfy more stringent security requirements and thus replace much of the functionality of routers in this regard. This is primarily true when VLANs are implemented in conjunction with private port switching. The only broadcast traffic on a single-user segment would be from that user's VLAN (that is, traffic intended for that user). Conversely, it would be impossible to listen to broadcast or unicast traffic not intended for that user (even by putting the workstation's network adapter in wanton mode), because such traffic does not physically traverse that segment (Decisys, 1996).

In the same vein, VLAN segregation is a coarse-grained access control technique, which may be perfectly acceptable in a network address control (NAC) deployment. In addition, VLAN segregation is attractive because it is widely standardised and widely implemented. This makes it easy for someone to design a network access control (NAC) architecture, and easy for everyone to understand the details of the deployment (Interop Lab, 2006).

In another perspective, private VLANs (PVLANS) are tools that allow segregating traffic at Layer-2 (L2), turning a broadcast segment into a non-broadcast multi-access-like segment. Traffic that comes to a switch

from a loose port (that is, a port that is capable of forwarding both primary and secondary VLANs) is able to go out on all the ports that belong to the same primary VLAN. Traffic that comes to a switch from a port mapped to a secondary VLAN can be forwarded to a loose port or a port belonging to the same community VLAN. Multiple ports mapped to the same isolated VLAN cannot exchange any traffic (Cisco, 2005).

Provisioning of QoS supported model in mobile environment using VLAN could be found in the work of Sasaki *et al* (2006). In their proposal, the performance of the proposed method was evaluated through experiments using mobile IP networks. The results obtained by experiment showed the effectiveness of the adaptive control method. By adopting the priority control using VLAN defined in IEEE802.1p, end-to-end priority control was realised.

Trend (2008) identified one of the advantages of the 802.1Q VLAN as its ability to offer quality of service (QoS) by means of three 802.1p bits. These bits are used to form the layer-2 class of service (CoS) bits that enable traffic differentiation. Traffic differentiation includes congestion management, the basis of QoS-aware service provisioning in packet-switched networks.

Again Quality of Service, as defined in IEEE standard 802.1p, use the VLAN 3-bit priority fields to provide eight unique traffic priorities (Tom, 2001). Typically, highest priority QoS tags are utilized for critical time-sensitive traffic such as protection and routing information. Historically, QoS technology has

provided switches and routers the ability to prioritize bandwidth allocation. QoS now enables them to prioritize VLAN traffic. By implementing VLANs, one can configure a switch to allow a given edge device to only talk to other devices on the same VLAN or on other trusted VLANs. As Fig. 2.1 illustrates, use of traditional technology would have required a unique physical infrastructure for each bridged network.

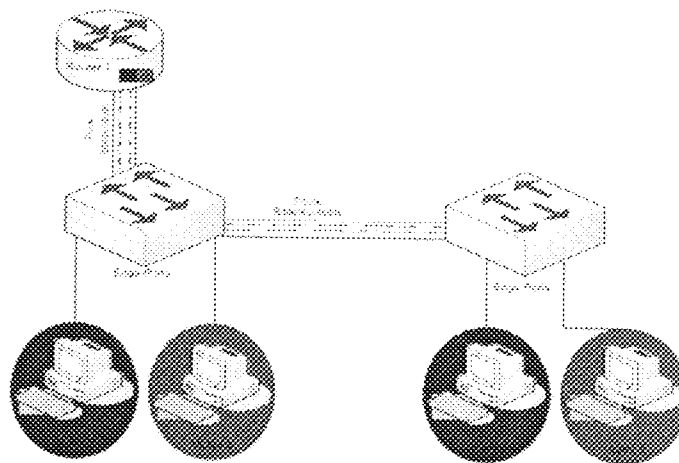


Figure 2.1: VLAN edge vs Trunk port

Marking identifies certain packets belonging to a particular service or subscriber. In IP, marks are carried in the IP precedence/ type of service (ToS) bits or in the differentiated Services Code Points (DSCPs). The Ethernet CoS bits allow for full mapping of the IPv4 precedence field, or partial mapping of the 6-bit DSCP. These mappings are used to extend the IP QoS mechanisms in Ethernet. A good example of this is the provision of QoS-aware services based on the Internet Engineering Task Force (IETF) Differentiated Services framework within a carrier-grade Ethernet network (Trend, 2008).

2.3 HISTORY OF SOME PROBLEMS IN SETTING UP VLANS

There are a number of challenges facing the growth/ wide acceptance of VLAN in enterprise networks, though more techniques to overcome such pitfalls have been proposed by many researchers and network developers. One of the earlier and common challenges that faced the development of VLAN implementation was proprietary products.

2.3.1 Evolution of Standards and Proprietary Concepts of VLANS

Given the variety of types of VLAN definitions and the variety of ways that switches can communicate VLAN information, it should not be surprising that each vendor has developed its own unique and proprietary VLAN solutions and products. The fact that switches from one vendor will not interoperate entirely with VLANs from other vendors force customers to buy from a single vendor for VLAN deployment across a network. An exception to this rule arises when VLANs are implemented in conjunction with an ATM backbone and LAN Emulation (LANE)

The fact that single-vendor VLAN solutions in the LAN backbone will be the rule for the foreseeable future contributes to the recommendation that VLANs should not be deployed indiscriminately throughout the enterprise. It also implies that purchase decisions should be more highly centralised or coordinated than they may traditionally have been. Thus, from both procurement and technological perspective, VLANs should be considered as elements of a strategic approach.

The following two VLAN standards have been proposed by IEEE to subvert the interoperability problems among VLAN equipment:

- i. 802.1 Internetworking Subcommittee
- ii. 802.10 VLAN standard

2.3.2 802.1 Internetworking Subcommittee

In March 1996, the IEEE 802.1 Internetworking Subcommittee completed the initial phase of investigation for developing a VLAN standard, and passed resolutions concerning three issues: the architectural approach to VLANs; a standardized format for frame tagging to communicate VLAN membership information across multiple, multi vendor devices; and the future direction of VLAN standardisation. The standardised format for frame tagging in particular, known as 802.1Q, represents a major milestone in enabling VLANs to be implemented using equipment from several vendors, and will be satisfactory in encouraging more rapid deployment of VLANs (Behrouz, 2007). Moreover, establishment of a frame format specification allows vendors to immediately begin incorporating this standard into their switches. All major switch vendors, including 3Com, Alantec, FORE, Bay Networks, Cisco, and IBM voted in favour of this proposal. However, due to the lag time necessary for some vendors to incorporate the frame format specification and the desire on the part of most organisations to have a unified VLAN management platform, VLANs, in practice, continue to retain characteristics of a single-vendor solution for some time. This has significant ramifications for deployment and procurement of VLANs. Department-level procurement for LAN equipment, particularly in the backbone, is not practical for organisations

deploying VLANs. Purchasing decisions and standardization on a particular vendor's solution throughout the enterprise will become the norm, and price-based product competition will decrease. The structure of the industry itself may also shift in favour of the larger networking vendors that can furnish a complete solution across a wide range of components.

2.3.3 802.1Q VLAN Standard

In 1995, Cisco Systems proposed the use of IEEE 802.1Q, which was originally established to address LAN security for VLANs. Cisco attempted to take the optional 802.1Q frame header format and "reuse" it to convey VLAN frame tagging instead of security information. Although this can be made to work technically, most members of the 802 committee have been strongly opposed to using one standard for two discrete purposes. In addition, this solution would be based on variable-length fields, which make implementation of ASIC-based frame processing more difficult and thus slower and/or more expensive (Decisys, 1996).

2.4 VLAN STATE-OF-THE-ART DESIGN ALTERNATIVES

In recent times VLAN application can be found in the areas of broadband service provisioning (e.g. in broadband networks). There are different techniques/models used to provide VLAN design alternatives (Juniper, 2009).

The following are examples:

- a. *Customer VLAN*: Also called the 1:1 model, in which model there is a dedicated VLAN for each subscriber.
- b. *Service VLAN*: In this model a dedicated VLAN allocated for each

- c. C-VLAN: Adding an Intermediate Aggregation Switch.
- d. Hybrid: Customer VLAN (C-VLAN) with Multicast VLAN (M-VLAN)

2.4.1 Customer VLANs

The customer VLAN (C-VLAN) model, as depicted in Figure 2.2, uses a separate dedicated VLAN for each subscriber. This C-VLAN carries all traffic between the multi-service access nodes (MSANs), such as an optical line termination (OLT) or digital subscriber line access multiplexor (DSLAM) and the broadband services router (BSR). This model mirrors the deployed edge architecture used in many carrier environments for dial, private line, Metro Ethernet and Frame/ATM aggregation, and is deployed by many of the world's largest IP-based broadcast television (IPTV) providers.

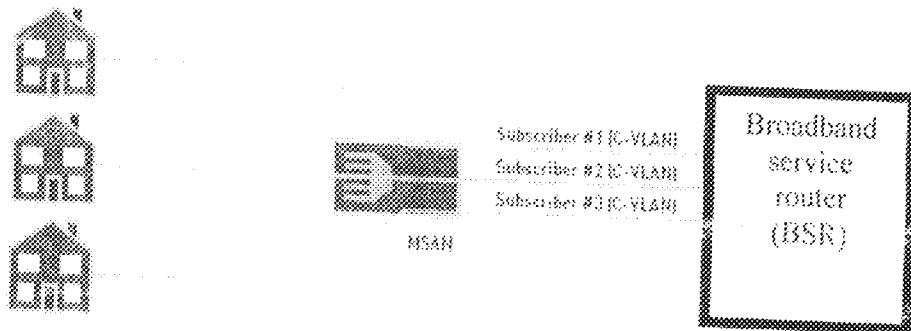


Figure 2.2: Customer VLAN model (a VLAN per customer)

In a "pure" C-VLAN model, the edge router performs channel replication and sends the broadcast television traffic to the subscriber via a unicast session. IPTV traffic, for example, is forwarded to each subscriber across the C-VLAN. A pure C-VLAN model works well if most television traffic is expected to be unicast to each subscriber (VoD or internet-based video downloads), or if

there is sufficient bandwidth available to send a unique video stream to each subscriber.

2.4.2 Service VLAN (S-VLAN) Model

In the service VLAN model, there is a separate VLAN for each service such as Internet access, Voice over IP (VoIP), IP-based broadcast television (IPTV) and Video on Demand (VoD). Internet Group Management Protocol (IGMP) packets always travel on the same S-VLAN as the associated IPTV. Figure 2.3 shows a simple example with three service VLANs.

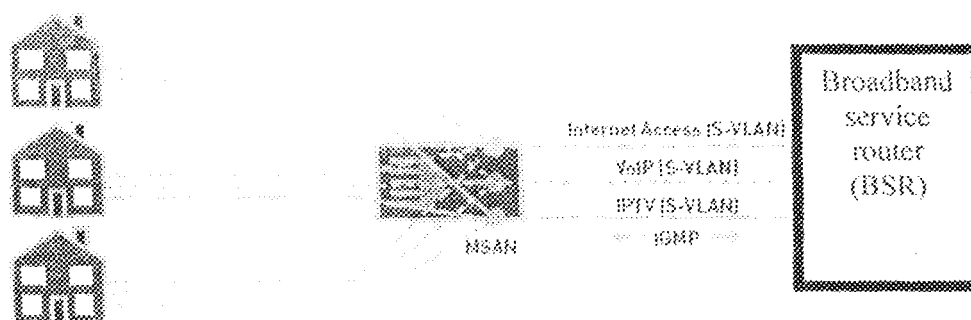


Figure 2.3 Service VLAN Model

The big challenge to service VLANs is that no network element can look at all traffic destined for each specific subscriber to determine whether there is sufficient bandwidth. Instead, a fixed amount of bandwidth must be "carved-out" for each service.

2.4.3 C-VLAN: Adding an Intermediate Aggregation Switch

Multi service access nodes (MSANs) are often connected to the edge router via an intermediate Ethernet aggregation switch. One way to support this is by assigning a unique VLAN ID to each subscriber connected to the same edge router port. However, since a single VLAN tag supports only 4,096 subscribers, it is possible to exhaust this pool

As depicted in Figure 2.4, the solution is to use multiple VLAN tags—an “outer” tag and “inner” tag. The outer VLAN tag identifies the MSAN and is used by the switch to forward traffic to it. In addition, the switch removes this tag. The inner tag identifies the subscriber connected to this MSAN and is used to identify the individual subscriber. This technique is defined in the IEEE 802.1ad supplement to the IEEE 802.1Q VLAN Bridging standard, and is commonly called “Q-in-Q” or “stacked VLANs”.

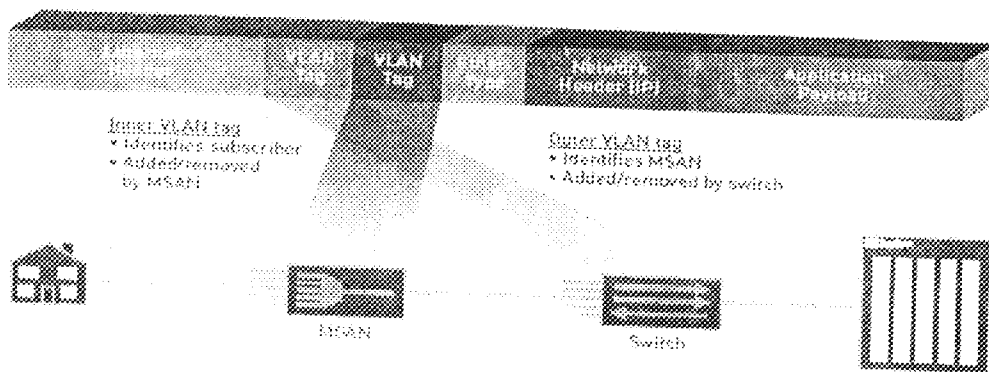


Figure 2.4: C-VLAN Ethernet frame with intermediate switch

2.4.4 Hybrid: Customer VLAN (C-VLAN) with Multicast VLAN (M-VLAN)

The hybrid model leverages the strengths of both (C-VLAN and M-VLAN) architectures, creating a single policy enforcement point while providing efficient multicast delivery. The hybrid model as depicted in Figure 2.5, leverages multiple VLANs as follows:

- ✓ A subscriber-dedicated C-VLAN carries unicast traffic such as Internet Access and Voice over IP between the access node and the BSR.
- ✓ A service VLAN carries broadcast television traffic to each MSAN. Because the S-VLAN carries multicast IPTV traffic exclusively, it is

often referred to as a Multicast VLAN (M-VLAN).

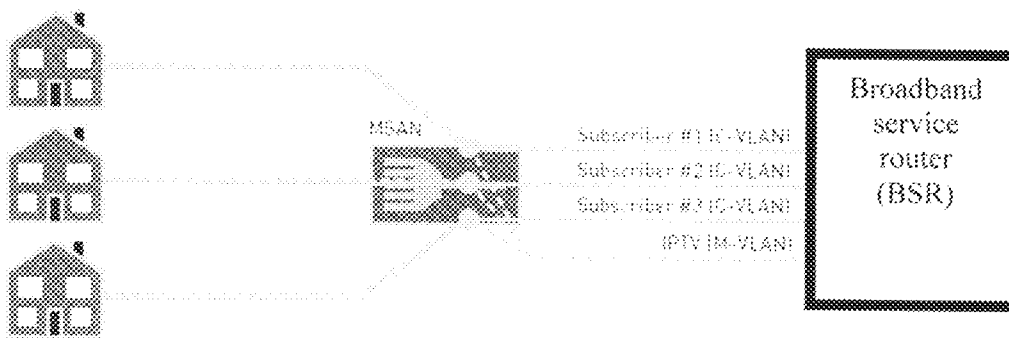


Figure 2.5: Hybrid C-VLAN with M-VLAN Model

✓ often referred to as a Multicast VLAN (M-VLAN).

In hybrid model, there is one "customer VLAN" per subscriber which carries all unicast traffic (Internet access, VoIP, VoD). In addition, one VLAN carries multicast traffic to all subscribers. Therefore, if there are N subscribers, the network supports $(N+1)$ VLANs. At the MSAN, the separate VLANs are often merged onto a single VLAN. IGMP and VoD traffic can flow on either the C-VLAN or the M-VLAN. IGMP forking can also be used to forward IGMP requests on either VLANs or ATM virtual circuits.

In conclusion, all the three (3) basic topologies described are deployed today. For a standard retail broadband network with a large amount of broadcast, the S-VLAN model works well and is often used. In addition, the service VLAN model is typically more appealing for service providers looking to build a multi-edge network or provide wholesaler-based service, since VLANs carrying different services can easily be forwarded to different endpoints. For networks with a heavy focus on offering diverse services or heavy VoD penetration, the

C-VLAN model is preferred. A separate M-VLAN is deployed if dictated by bandwidth requirements.

In addition, VLAN technology is also being used in cooperation with other network technologies like VPN (Virtual Private Network) to realise some new technologies for modeling in Ethernet networking alternatives. An example of such is the work of Honda *et al* (2004) titled "a prototype implementation of VPN enabling user-based Multiple associations". This prototype implementation uses such an architectural framework. To be more specific, the Ethernet is used for the base network, IEEE 802.1Q VLAN is used for establishing VPNs, and IP is used for controlling user access to VPNs. The VPN to be offered to users ("User VPN") was implemented by IEEE 802.1QVLAN. IEEE 802.1Q technology uses a tag containing a 12-bit VLAN ID attached to an Ethernet frame to virtually divide Ethernet connections. In order to simplify this prototype implementation, each VLAN was configured so as to have only one IP subnet so that no duplication can occur between IP address spaces.

The user host is connected to the VLAN via a device called an "MAVPN gateway," (multiply association VPN). The access lines between the hosts and the MAVPN gateway are multiplexed using the IEEE 802.1Q; that is, the MAVPN gateway bridges the access circuits to VPNs that are implemented with IEEE 802.1Q VLAN. In this way, the hosts can use multiple layer-2 VPNs. The MAVPN gateway also has a function to authenticate users; only the access lines from the user host that may be granted for association with

the target VPNs can be connected. In the initial condition where the host does not yet belong to any VPNs, communication is allowed only within the site, as shown in Figure 2.6. To represent this initial condition, such an initial site is referred to as "Default VPN. The IP address of the user terminal is assigned by the DHCP server installed within each VLAN from the IP address spaces of the respective VLANs. IP addresses for servers are statically assigned from the respective VLAN IP address spaces.

User account information to be used for authentication purposes will be provided to every MAVPN gateway from the RADIUS server, as shown in Figure 2.6. The RADIUS server will be installed within a special "Management VPN" system. User account information to be stored in the RADIUS server will include user IDs, VPN names for which association is granted, and passwords. As such, a user can have as many accounts as the number of VPNs for which he/she is granted association.

To abridge this work, one could observe that network hosts can use transparently multiple VPNs system on an individual user basis. It was also confirmed that host access can be controlled individually by way of an authentication mechanism.

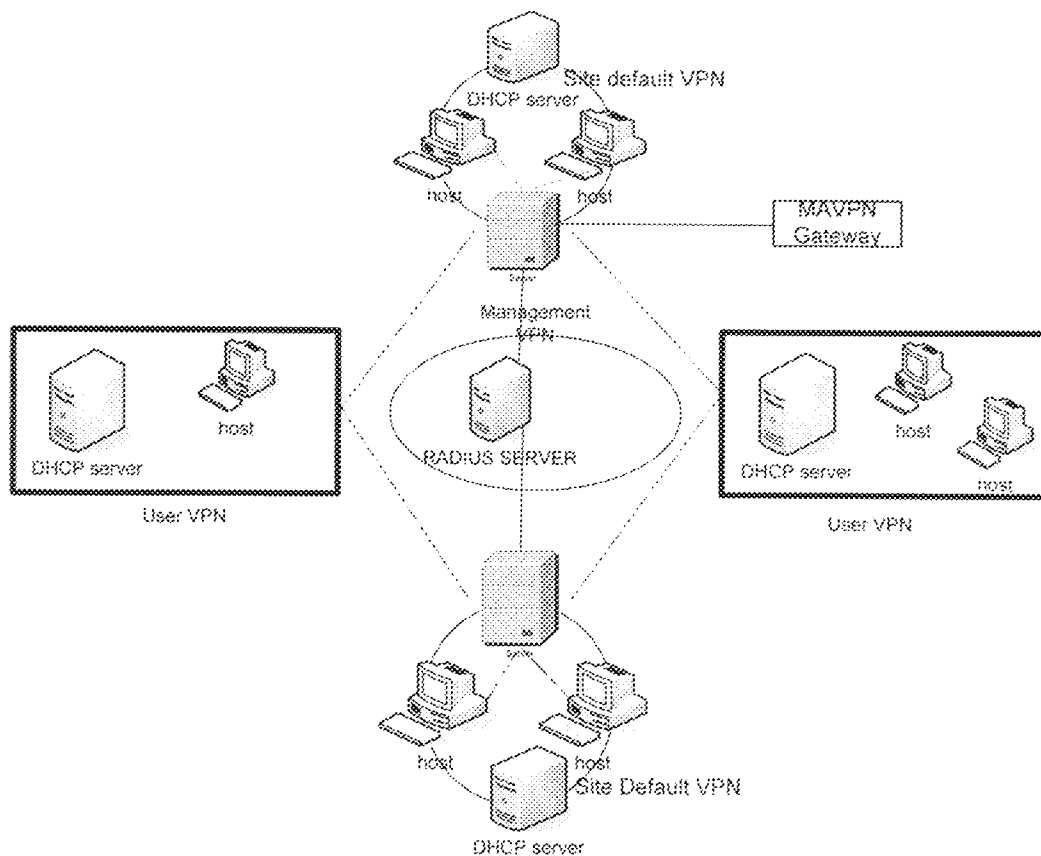


Fig. 2.6: Logical network configuration of the prototype system

Conversely, the use of VLAN for security measures in a switch network, some researchers found it inadequate. For example, Apani: a software developing company based in Southern California in the United States developed an application to proffer solution to how network security administrators can reduce the complexities of firewall and VLAN management in an enterprise network. In an attempt to drive home this point, the company presented EpiForce security software that is designed to deliver access control and policy-based encryption, both based on identity, to protect critical data and communications from intruders (Apani, 2009).

CHAPTER THREE

3.0

MATERIALS AND METHODS

This chapter describes the network configuration for Ibrahim Badamasi Babangida University Lapai, the performance estimate of the network using standard formulae and Simulator (Cisco packet Tracer) with the aim of obtaining the true behaviour of the network. The chapter later, gives the highlights for new network design and procedure for VLAN implementation.

3.1 NETWORK CONFIGURATION

Towards realisation of the goals for this project as stated in Chapter One, the Ibrahim Badamasi Babangida University's Lapai campus network is considered. The network is a demonstration of a common LAN implemented in enterprise networks. Such networks could also be found in banks, schools, local internet service providers (cyber cafes), etc. Fig 3.1 depicts a layout of the network without VLAN. This network comprises seven (7) areas with a switch in each area linked to router 0 at the ICT centre via a radio link.

To bring home the need for VLAN implementation in an enterprise network like this (figure 3.1), the performance of the existing network would be estimated using network simulator and known mathematical model equations that can support the demonstration of all the functions performed by the network. Cisco Packet Tracer network simulator is chosen for modeling and simulating the performance of the network. However, another simulator called *Tora* is also

incorporated for some instances to achieve excellent results in our analysis and design.

Cisco Packet Tracer is a comprehensive networking technology teaching and learning programme that offers a unique combination of realistic simulation and visualisation experiences, assessment and activity authoring capabilities, and opportunities for multi user collaboration and competition. Innovative features of the **Packet Tracer** can help students and teachers collaborate, solve problems, and learn concepts in an engaging and dynamic social environment. Some reasons for choosing Packet Tracer are as follows:

- It provides a realistic simulation and visualization learning environment that imitates laboratory equipment for network design.
- It enables authoring and localisation of structured learning activities such as labs, demonstrations, quizzes, exams, and games.
- It empowers students to explore concepts, conduct experiments, and test their understanding.
- It allows students and teachers to design, build, configure, and troubleshoot networks using virtual equipment.
- It supports a variety of teaching and learning opportunities such as lectures, group and individual labs, homework, and competitions.

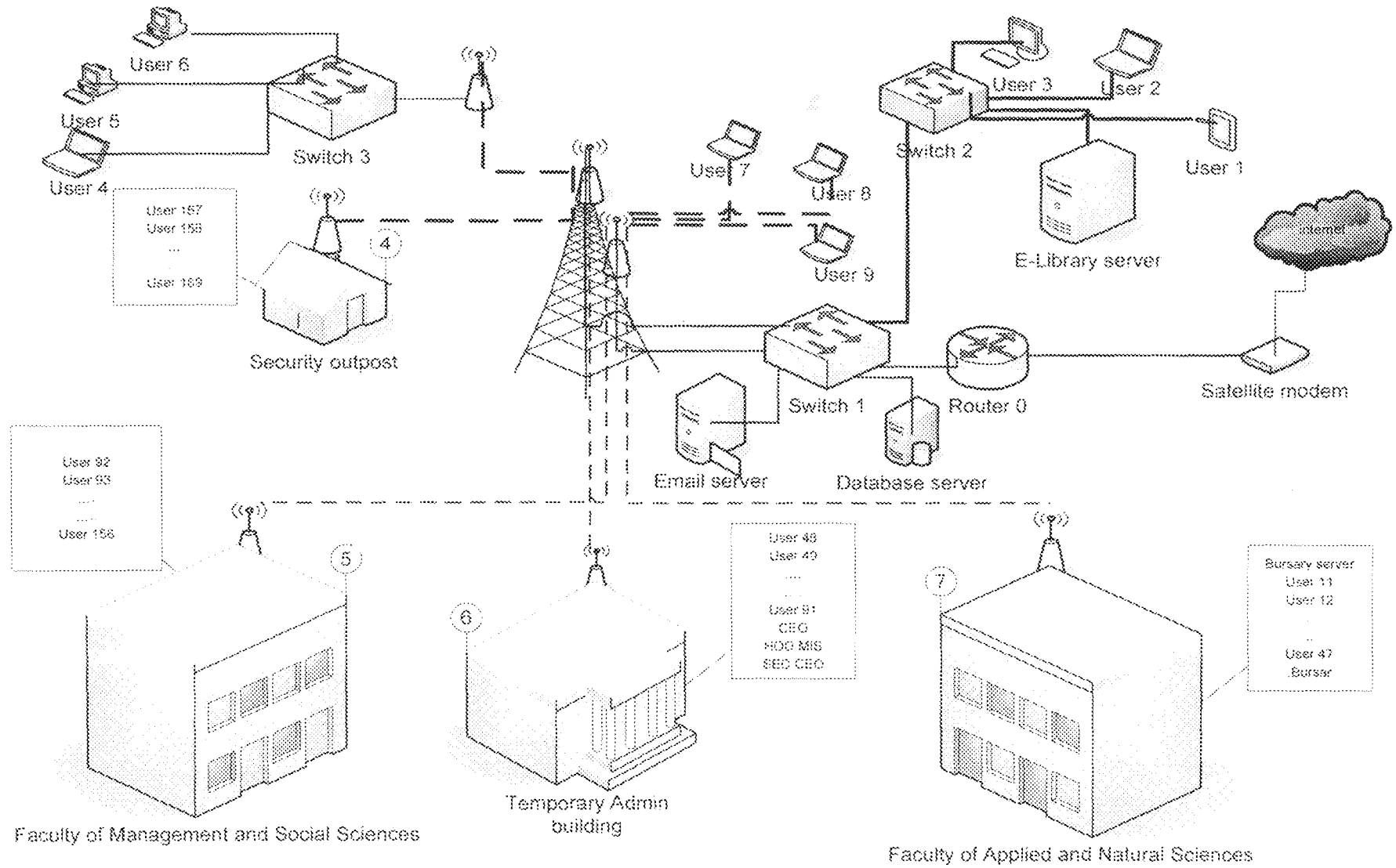


Figure 3.1 Ibrahim Badamasi Babangida University, Lapai main campus network layout

As illustrated in figure 3.1 the structure of the network consists of seven areas with a switch in each area, except area 2 (library complex) that is connected to switch 1 via cable link for onward connection to the router 0, every other switch is connected to switch 1 via radio link. Router 0 is Cisco 2611 configured as DHCP server for the entire network. At area 6 (temporary administrative building) is a server meant for bursary department. However, both the server and the host around area 6 are configured to use the same subnet. Also at area 2 (E-library) there is a server for library services.

3.2 Network Performance Estimates

3.2.1 Performance Estimate Using Standard Formulae

The network performance measures of interest are network delay, network utilisation and service time for the network users. We first conduct analysis of the existing network to estimate its performance. The entire system/network (figure 3.1) to be analysed conforms to a simple M/M/1 queuing system; this is because the entire network forms a single broadcast domain (assumed to be the queue) as illustrated in figure 3.2.

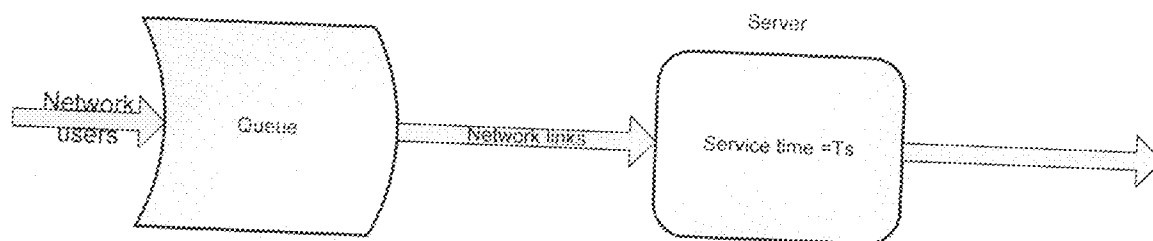


Figure 3.2: M/M/1 queue system of the entire network

Assume random request by network users from the router 0 which is the sole link to internet, the random request could be matched with **Poisson distribution**. Which states that, the probability that there are k arrivals in t seconds is given by;

$$P_k = \frac{e^{-\lambda t} (\lambda t)^k}{k!} \quad (3.1)$$

where λ is the average number of arrivals per second. For $k = 0$, the above probability reduces to $e^{-\lambda t}$. Thus, the probability that there are one or more arrivals in time t is = 1- (probability that there is no arrival)

$$p_0 = 1 - e^{-\lambda t} \quad (3.2)$$

By random service, we imply that the time to service an arrival is given by the exponential distribution function. That is,

$$P_r(\text{service time} < t) = 1 - e^{-\frac{t}{T_s}} \quad (3.3)$$

where T_s is the service time.

The queue size for the network users is given by

$$p_k = p_0 (\lambda T_s)^k \quad (3.4)$$

where p_k is the total number of broadcast in the network, λ is the mean arrival rate per second, T_s is the mean service time in seconds and p_0 is the probability that the queue is empty, we can determine p_0 by simplifying the equation (3.4) for p_k and the fact that the sum of p_k , for $k= 0,1,2,\dots,\infty$, must be 1, so,

$$\sum_{k=0}^{\infty} p_k = \sum_{k=0}^{\infty} p_0 (\lambda T_s)^k = 1 \quad (3.5)$$

Thus,

$$1 = p_0 \sum_{k=0}^{\infty} (\lambda T_s)^k \quad (3.6)$$

Equation 3.6 is a typical geometric series with common ratio λT_s , solution of infinite geometric series in equation 3.5 is

$$= p_0 \frac{1}{1 - \lambda T_s} \text{ (assuming } \lambda T_s < 1 \text{) (Stroud, 2001)}$$

$$\text{or } p_0 = 1 - \lambda T_s \quad (3.7)$$

Network utilization Ψ can now be found from the probability that the queue is not empty, or

$$\Psi = 1 - p_0 = \lambda T_s \quad (3.8)$$

The queue size distribution can be described in term of server utilization

$$p_k = p_0 (\lambda T_s)^k \quad (3.9)$$

or,

$$p_k = (1 - \lambda T_s) (\lambda T_s)^k = (1 - \Psi) \Psi^k \quad (3.10)$$

But from above λT_s is assumed to be less than 1. According to Little's formula the mean queue size in a network is given by

$$\sum_{k=0}^{\infty} k p_k = \frac{\Psi}{1 - \Psi} \quad (3.11)$$

(Vijay, 1987)

The above derived equations can now be used to determine the behaviour of our network.

The mean arrival rate within the network (rate of broadcast by network users) = 0.05Mbps as given by the internet service provider (ISP)

i.e $\lambda_s = 0.5\text{Mbps}$

Average link speed = 85Mbps (Ethernet 802.3 are designed with link speed of 10/100 Mbps. However, the 85 Mbps is assumed to take care of loss and cable properties)

Average message length broadcasted within the network = 120 Mb (assumed)

Thus, the mean service time $T_s = \frac{120\text{Mb}}{85\text{Mbps}} = 1.412\text{sec}$

Average network utilisation = $\Psi = \lambda T_s = 0.5 \times 1.412 = 0.706 = 70.6\%$ (from equ. 3.8)

The mean waiting time is given by service time multiplied by the mean queue

size. Thus, mean waiting time = $\frac{\Psi T_s}{1 - \Psi} = \frac{0.706 \times 1.412}{1 - 0.706} = 3.391\text{sec} \approx 3.4\text{sec}$

This waiting time is required before a given broadcast is serviced.

3.2.2 Performance Estimate Using Simulator

To further ascertain the network's true behaviour, simulation of the network was conducted. Figures 3.3 and 3.4 show the results obtained for pinging router 0 from user 1 terminal connected to switch 1, and user 91 connected to switch 3 at Faculty of Management And Social Sciences. The "PING" is a tool of the Internet Control Message Protocol (ICMP); it is a TCP/IP protocol that enables computers on a network to share error and status information. ICMP is often used for troubleshooting/ verification of connectivity test (Tom, 2008). From simulation results of the network (refer to fig 3.1) it was observed that the time taken by any host to access the router is inversely proportional to its distance away. This phenomenon makes the network to be distance-biased.

Similarly, the ping result for pinging router 0 from user 234 is as shown in figure 3.4

Other drawbacks in this network include;

- i. Bandwidth wastage because too many users are placed within the same broadcast domain.
- ii. Segregation of the hosts that are not connected to the same switch to share network resources that are not meant for all users will not be possible. The network resources are opened (unsecured), no restriction. Thus any network user can intrude into important servers within the network.
- iii. The Database server load was also found to be soaring.
- iv. Arbitrary delay was also observed in traversing the network

To restrain the problems highlighted above, VLAN is to be implemented with logical configuration that will be done on the switches. VLAN can help break up broadcast domain to the required number. In the same vein, it could be used to isolate important servers, and cut down the database server load and the network service time.

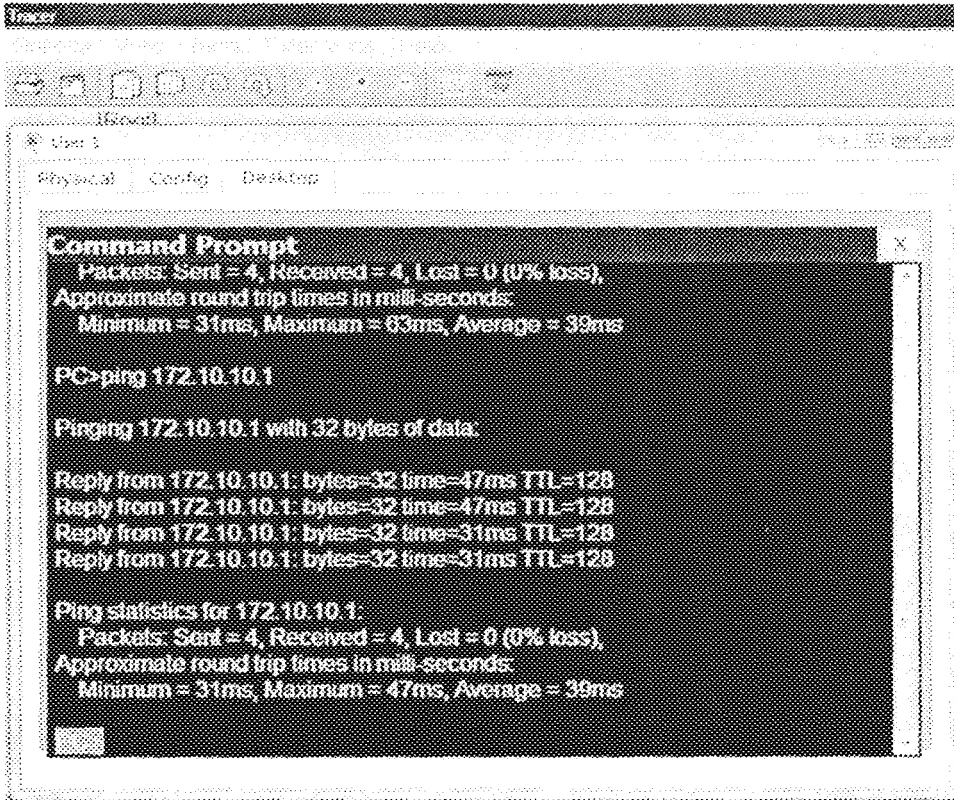


Figure 3.3: Ping result between user 1 and Router 0 at ICT Centre

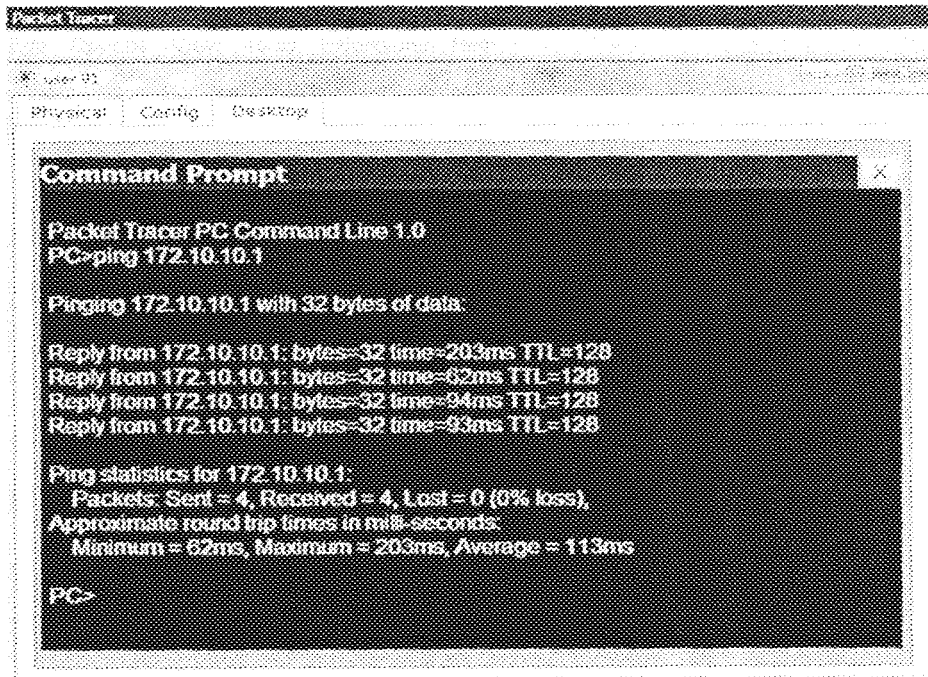


Figure 3.4: Ping result between user 91 and Router 0.

3.3 Network Design

Based on the hardware requirement for deploying VLAN a new router would have to replace router 0 in the existing network. VLAN-aware switch cable of inter-VLAN routing will be required for the replacement. Also, as a network design issue, an appropriate node placement is required for the switches.

The topological design of a network assigns the links and link capacities for connecting the nodes. This is among the critical aspect of a network design because the routing, the flow control and other behavioural design algorithms rest largely on the given network topology. The location of the switches, link connections and link speeds directly determine the transit time through the network. The topological design helps in selecting appropriate locations for the network concentrators (switches and routers). In this work, *Floyd's Algorithm* and *Minimal Spanning Tree algorithm* were applied to determine how best to link our switches to ensure optimal performance for the network and reduce cost.

Floyd's algorithm is one of the general algorithms that is used to determine the shortest route between any two nodes in a network (Taha, 2006). The algorithm represents an n -node network as a square matrix with n rows and n columns. Entry (i, j) of the matrix gives the distance D_{ij} from node i to node j , which is finite if i is linked directly to j and infinite otherwise. Similarly, it deals with linking the nodes of a network, directly or indirectly, using shortest length of connecting branches.

3.3.1 Topological Design

Given the locations of the network users in their various areas as depicted in fig 3.1 the optimal location for the switches is highly desirable. We replace all the radio links with fiber links; this is because the existing radio links use IEEE 80211b DSSS. DSSS is the high-rate direct sequence spread spectrum (HR-DSSS) method for signal generation in 2.4 GHz unlicensed industrial, scientific, and medical (ISM) Band (Behrouz, 2007). The ISM band can be competitive. Another reason for replacing the wireless link is to avoid delay as propagation delay depends upon the transmission media and direct distance between the source and the destination device. For wired media, propagation delay is negligible (Sanjay, 2005). To begin the design the physical area to be covered by the network is considered while the seven (7) switches within the area are distributed to initialize the switch placement, after which Floyd's algorithm is applied to select appropriate connections for the switches based on distances between the nodes. Floyd's algorithm is applied with the aid of TORA primer software to optimize the location of the switches. The TORA primer optimisation system is a windows-based software designed for use with many of the techniques presented in operations research text books. An important feature of the software is that it can be used to solve problems in an automated mode, thus relieving one of the burdens of the continuous computations that generally characterise Operations Research (OR) algorithms (Taha, 2006). Figure 3.5 illustrates the initial switch distributions while initial Floyd's matrices obtained from the switch positions are as shown in Table 3.1 and 3.2.

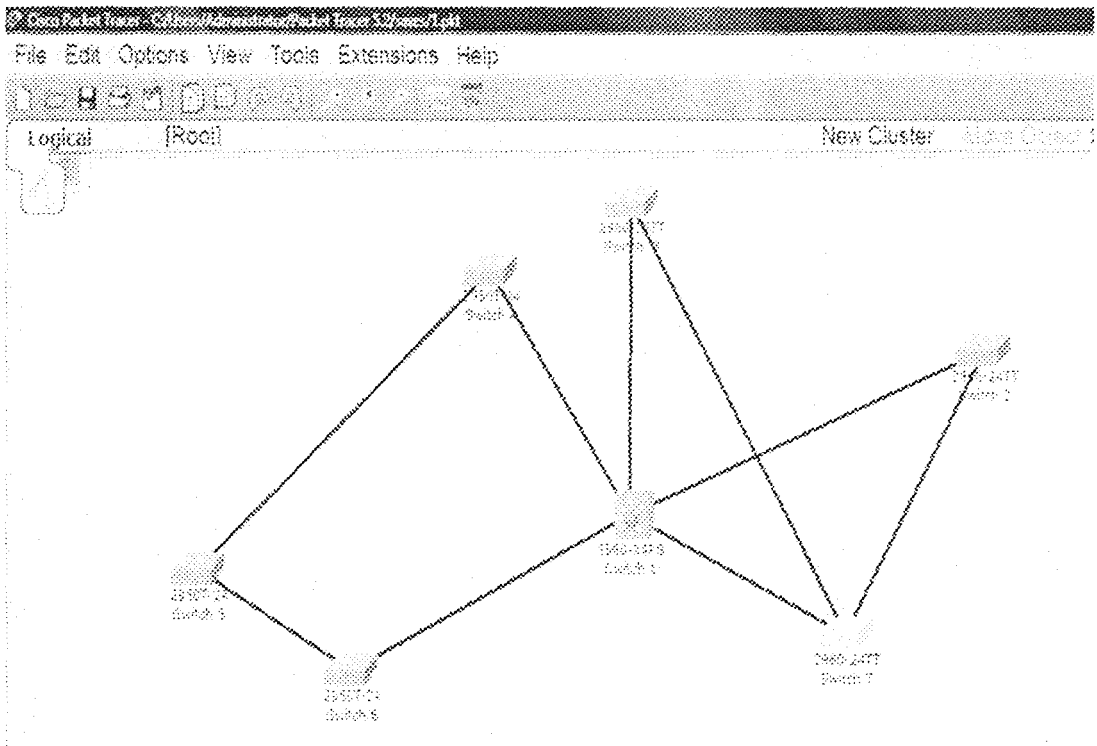


Figure 3.5: Network topology

The approximate link distances is as shown in tables 3.2

Table 3.1: Dx Table, N_x = switch area x , d_{ij} = distance between Switch area i and switch area j .

	N1	N2	N3	N4	N5	N6	N7
N1		d_{12}	d_{13}	d_{14}	d_{15}	d_{16}	d_{17}
N2	d_{21}		d_{23}	d_{24}	d_{25}	d_{26}	d_{27}
N3	d_{31}	d_{32}		d_{34}	d_{35}	d_{36}	d_{37}
N4	d_{41}	d_{42}	d_{43}		d_{45}	d_{46}	d_{47}
N5	d_{51}	d_{52}	d_{53}	d_{54}		d_{56}	d_{57}
N6	d_{61}	d_{62}	d_{63}	d_{64}	d_{65}		d_{67}
N7	d_{71}	d_{72}	d_{73}	d_{74}	d_{75}	d_{76}	

Table 3.2: D_0 ; The initial starting distance matrix from the diagram in figure 3.6. (the approximate distances are measured in kilometers)

	N1	N2	N3	N4	N5	N6	N7
N1	—	1	13	3	∞	7	2
N2	1	—	∞	∞	∞	∞	5
N3	3	∞	—	∞	∞	∞	8
N4	3	∞	∞	—	6	∞	∞
N5	∞	∞	∞	6	—	4	∞
N6	7	∞	∞	∞	4	—	∞
N7	2	5	8	∞	∞	∞	—

Table 3.3: S_0 : The initial sequence matrix from the diagram in figure 3.6.

	N1	N2	N3	N4	N5	N6	N7
N1	—	2	3	4	5	6	7
N2	1	—	3	4	5	6	7
N3	1	2	—	4	5	6	7
N4	1	2	3	—	5	6	7
N5	1	2	3	4	—	6	7
N6	1	2	3	4	5	—	7
N7	1	2	3	4	5	6	—

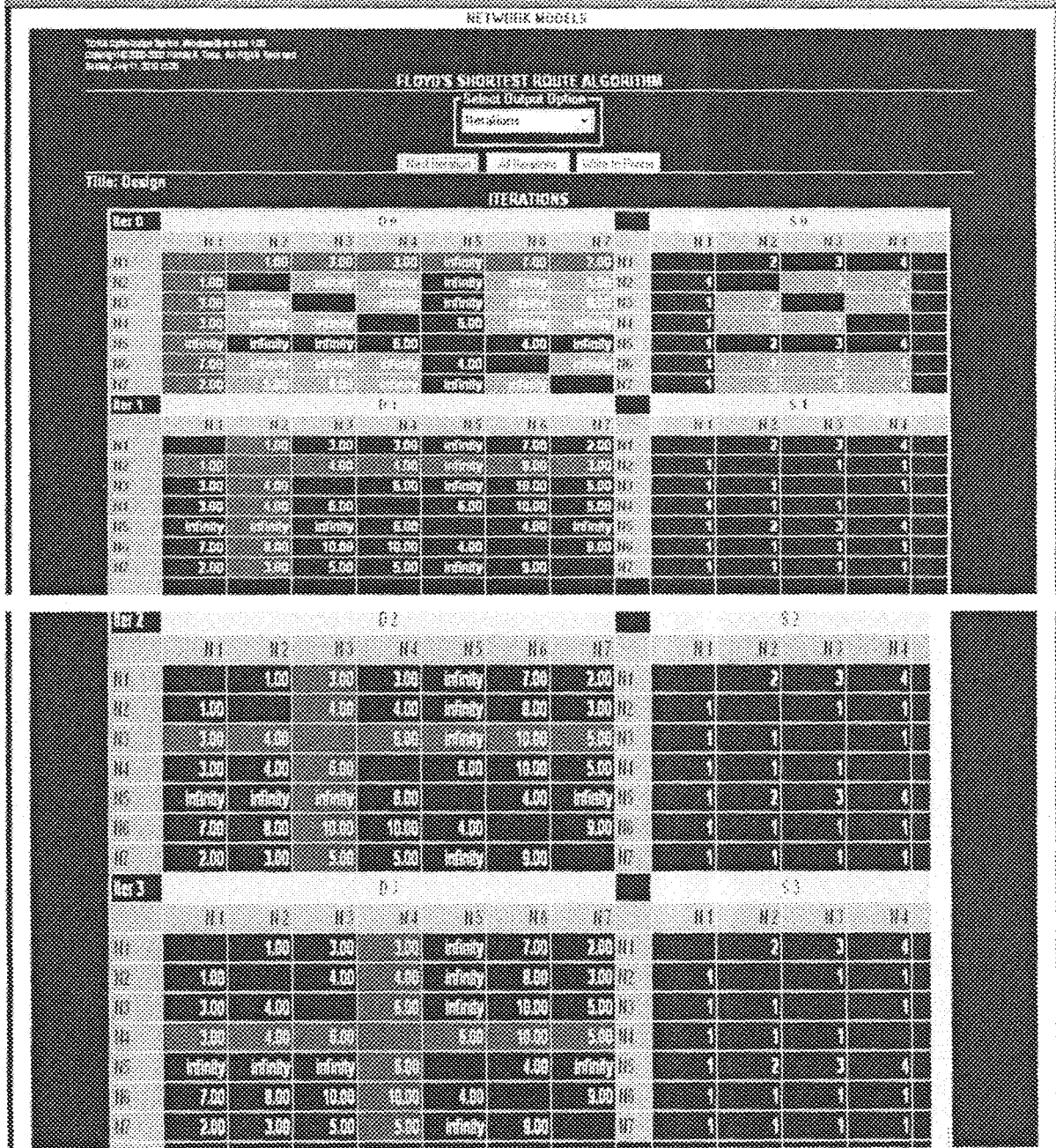


Figure 3.6: Floyd's iterations 0 -3 result display

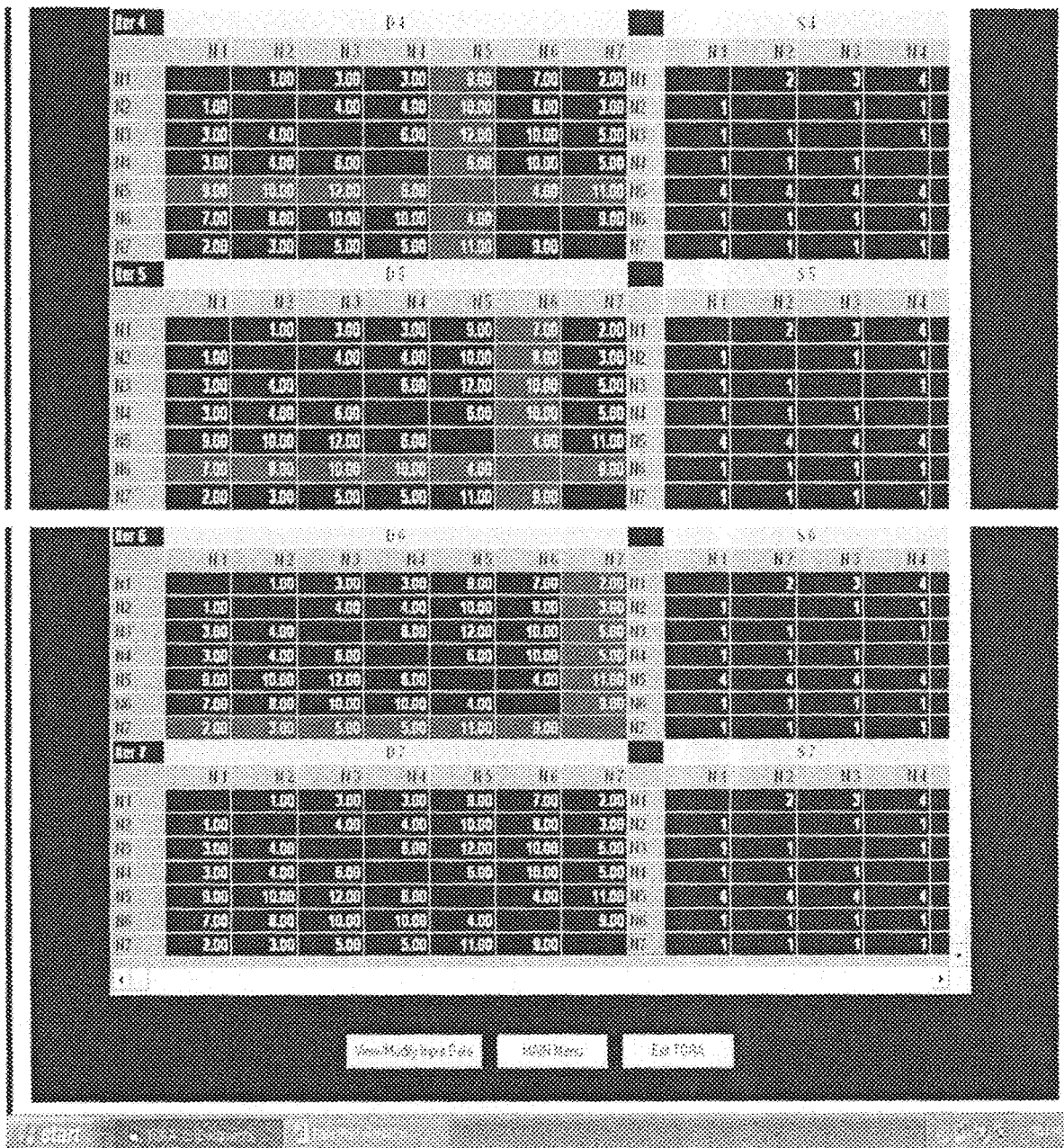


Figure 3.7: Floyd's iterations 3 -5 result display

The results obtained using the Tora software (for Floyd's algorithm), show that after 5 iterations the optimal shortest routes were determined for the switches. The iteration tables from the software are as displayed in figures 3.6 and 3.7. To conclude the topological design, the final matrices D_5 and S_5 contain all the information needed to determine the shortest route between any two nodes in the

network, we now apply **Minimal Spanning Tree algorithm** to the final iteration table of Floyd's algorithm to determine the best way to link the shortest possible length of connecting the switches starting from switch 1. Figure 3.8 display the result for the spanning tree algorithm. The minimal spanning tree algorithm deals with linking the nodes of a network either directly or indirectly, using the shortest length of connecting branches. The unwanted links were replaced by new link. (Direct links $D_{1,5}$ and $D_{2,4}$ were removed and direct link $D_{2,4}$ was introduced) following the result of the spanning tree algorithm.

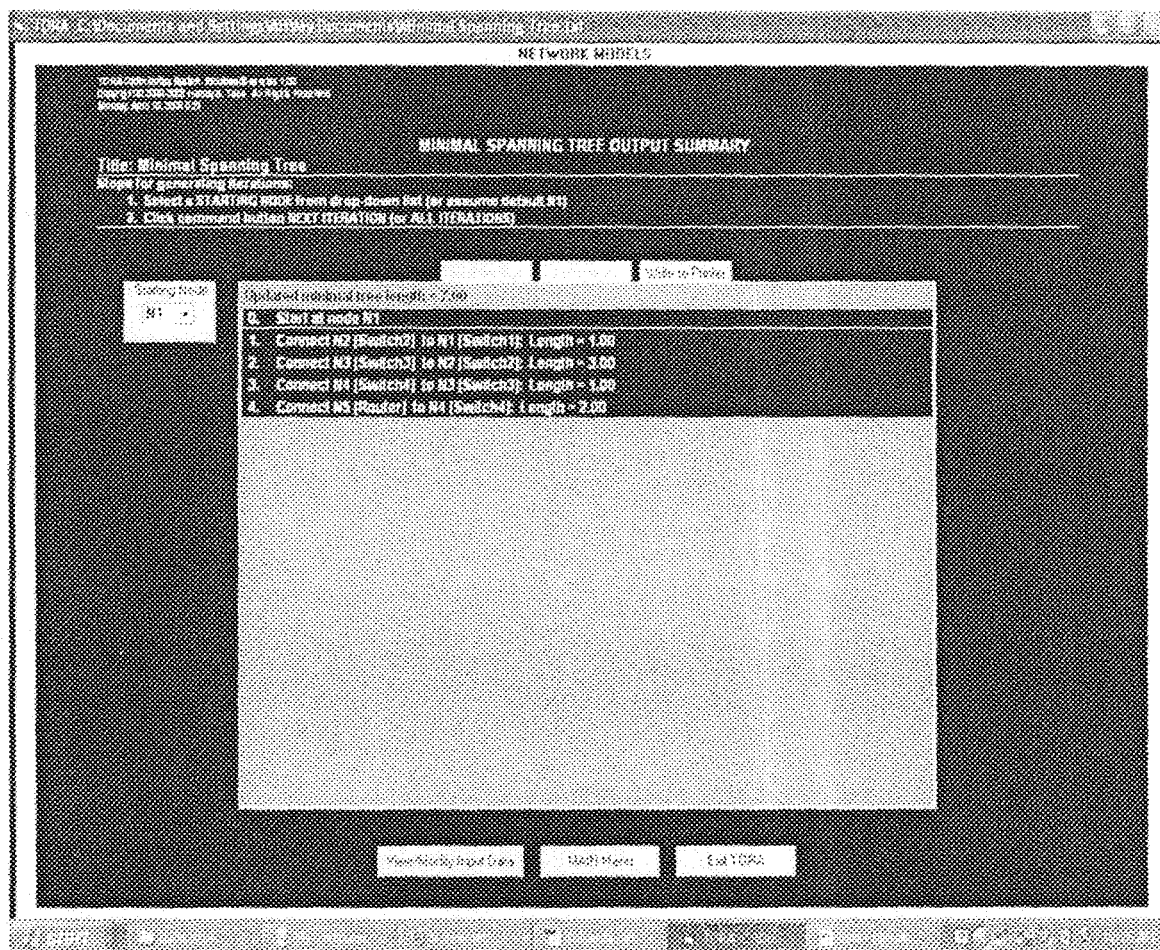


Figure 3.8: Spanning tree algorithm result display

3.3.2 Vlan Design and Implementation

In order to simplify this implementation, all users were categorised into six groups and distributed within 6 VLANs. Table 3.4 shows the users' distribution for various VLANs to be implemented. Table 3.4 forms the basis for our VLAN segregation. Each VLAN is configured so as to have only one IP subnet to avoid IP conflicts. Users within each VLAN are assigned IP automatically by a DHCP server located in the same VLAN.

Table 3.4: VLANs, users and server distribution

VLAN No.	VLAN Names	Members
1	Default	Email server
2	Bursary	Email server, CEO, Bursar, all HODs and principal staff, Bursary server, all Deans
3	Sciences	FAAN staff
4	Visitors	Visitors
5	MIS	Email server, MIS server, HOD MIS, Data base server
6	Admin	University principal staff

3.4 Vlan Configuration

3.4.1 Network Equipment for VLAN Implementation

The proposed VLAN will be implemented by IEEE 802.1QVLAN techniques using Cisco Packet Tracer 5.2. Cisco Catalyst 2960-24TT switches were incorporated to support IEEE 802.1Q technology that uses a tag containing a 12-bit VLAN ID attached to an Ethernet frame to virtually divide Ethernet connections. The Cisco Catalyst 2960-24TT is a member of the Catalyst 2960 Series Intelligent Ethernet

Switch family. It is a fixed-configuration, standalone switch that provides wire-speed Fast Ethernet and Gigabit Ethernet connectivity for mid-sized networks.

3.4.2 Switch Configuration

By default the Cisco 2960-24TT switch is designed to create a primary VLAN called "default VLAN" before any configuration for multiple VLANs. Figure 3.11 shows the inherent properties of the switch before configuration and connection.

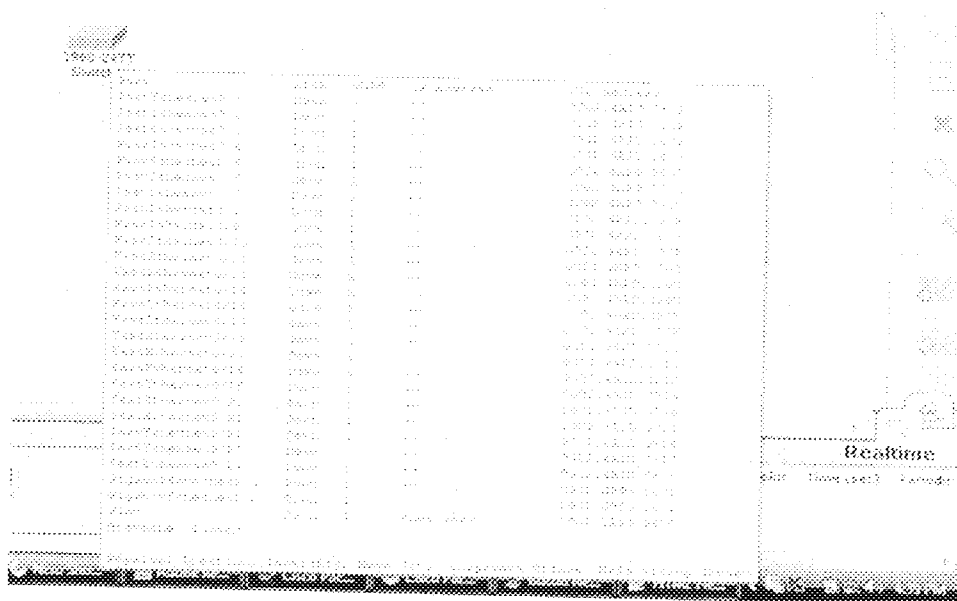


Figure 3.9: Network symbol and properties menu of 2960-24TT switch

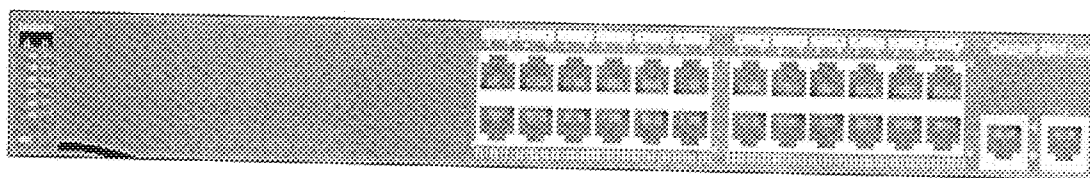


Figure 3.10: Physical appearances for 2960-24TT switch

From Properties menu shown in figure 3.8, each port has different MAC address, and could be connected to either different or similar link types. Each switch within

the network is configured to support only the VLANs traffic that is allowed to traverse the switch. Figure 3.9 depicts the configuration panel for a switch.

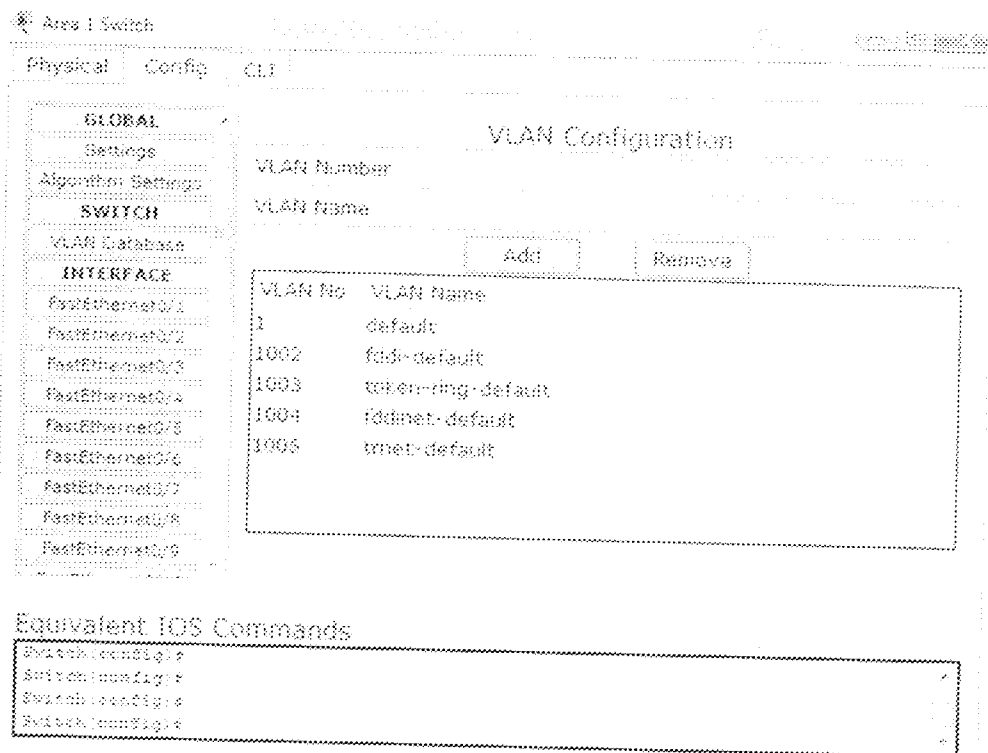


Figure 3.11: Configuration panels for switches

The **Config** tab (figure 3.11) for the switch offers three general levels of configuration: global, switching, and interface. In global settings, the switch display name was changed as it appears on the workspace and the hostname as it appears in the Cisco IOS. Figure 3.12 illustrates change of name for area 1 switch. One could also manipulate the switch configuration files in any of the following ways:

- Erase the NVRAM (where the startup configuration is stored).
- Save the current running configuration to the NVRAM.
- Export the startup and running configuration to an external text file.

- Load an existing configuration file (in .txt format) into the startup configuration.
- Merge the current running configuration with another configuration file.

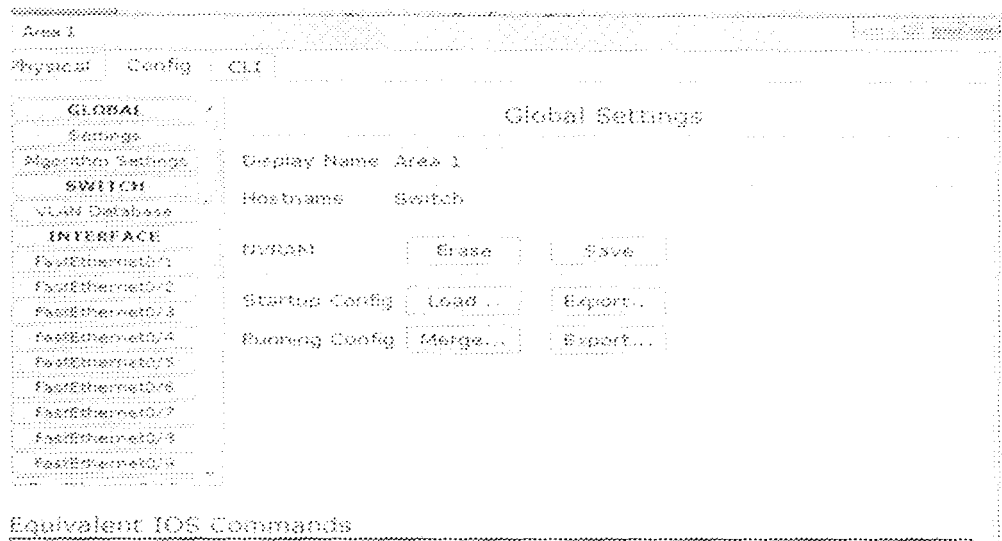


Figure 3.12: Renaming area 1 switch

3.4.3 VLAN Database Configuration

To configure switching, **SWITCHING** button was expanded to gain access to the VLAN Database button. The switching level, however, is where we managed the VLAN database of the switch.

VLANs 2, 3, 4, 5 and 6 were configured on the switches from the **VLAN Database** sub-panel. Each VLAN was added by entering a name and a VLAN number and pressing the **Add** button. As depicted in fig 3.13 all the configured VLAN entries are displayed.

3.4.4 Ports Configuration

As frames are switched throughout the network, switches are meant to keep track of all the different types, including understanding what to do with them depending on the hardware address. Frames are handled differently according to the type of link they are traversing. There are two different types of links in a switched environment; Access links and Trunk links.

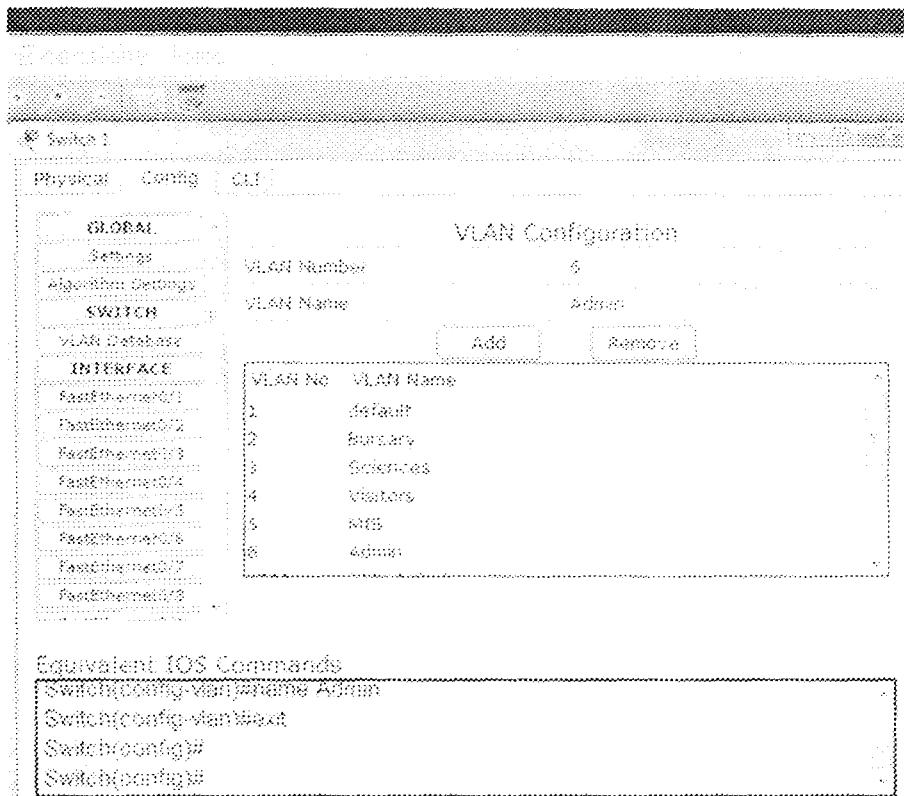


Figure 3.13: VLAN configuration for panel for switches

3.4.5 Access links and Trunk links

Access Link: this type of link is only part of one VLAN, and it is referred to as the *native VLAN* of the port. Any device attached to an *access link* is unaware of a VLAN membership—the device just assumes its part of a broadcast domain,

Table 3.5: Switch ports configuration that carry multiple telephone conversations.

Switch	port	Type of link configured	VLAN membership
Area 1	FastEthernet 0/2	Trunk	All VLANs
	FastEthernet 0/3	Access	VLAN3
	FastEthernet 0/4	Access	VLAN2
	FastEthernet 0/5	Access	VLAN2
	FastEthernet 0/6	Trunk	
	Area 2	FastEthernet 0/1	Trunk
FastEthernet 0/2		Access	
FastEthernet 0/3		Access	
FastEthernet 0/4		Access	VLAN3
FastEthernet 0/5		Access	VLAN4
FastEthernet 0/6		Access	
Area 3	GigabitEthernet 1/1	Trunk	All VLANs
	FastEthernet 0/1	Access	
	FastEthernet 0/2	Trunk	All VLANs
	FastEthernet 0/4	Access	VLAN4
	FastEthernet 0/5	Access	VLAN3
	FastEthernet 0/6	Access	VLAN4
Area 4	FastEthernet 0/21	Access	
	GigabitEthernet 1/1	Trunk	All VLANs
	FastEthernet 0/1	Trunk	All VLANs
	FastEthernet 0/2	Trunk	All VLANs
	FastEthernet 0/3	Trunk	All VLANs
	FastEthernet 0/4	Trunk	All VLANs
	FastEthernet 0/5	Trunk	All VLANs
	GigabitEthernet 1/1		
	GigabitEthernet 1/2		

but it has no understanding of the physical network. In contrast, a trunk link can carry multiple VLANs and originally gained its name after the telephone system

Trunking allows us to make a single port part of multiple VLANs at the same time. All the user ports were configured as "access link" whilst servers' ports and printer were configured as "trunk links". Table 3.5 gives the summary for ports configuration for various switches.

Switches have only Ethernet-type interfaces (ports). For each interface, the **Port Status** (on or off), **Bandwidth**, **Duplex** setting, **VLAN Switch Mode**, and **Transmission Ring Limit** were set. By default, an interface is a VLAN access link assigned to default VLAN (VLAN 1). Figure 3.14 shows the configuration panels for port 1 known as FastEthernet 0/1 before changes were made.

We use the drop-down menu on the right side to reassign the port to another configured VLAN supported by the switch. We could also change an interface into a VLAN trunk port by using the drop-down menu on the right to select the VLANs that trunk is to handle. Ports within a switch can only support one of the VLAN preconfigured in the switch.

Throughout configurations in the **Config** tab, the lower window will display the equivalent Cisco IOS commands for all one's actions.

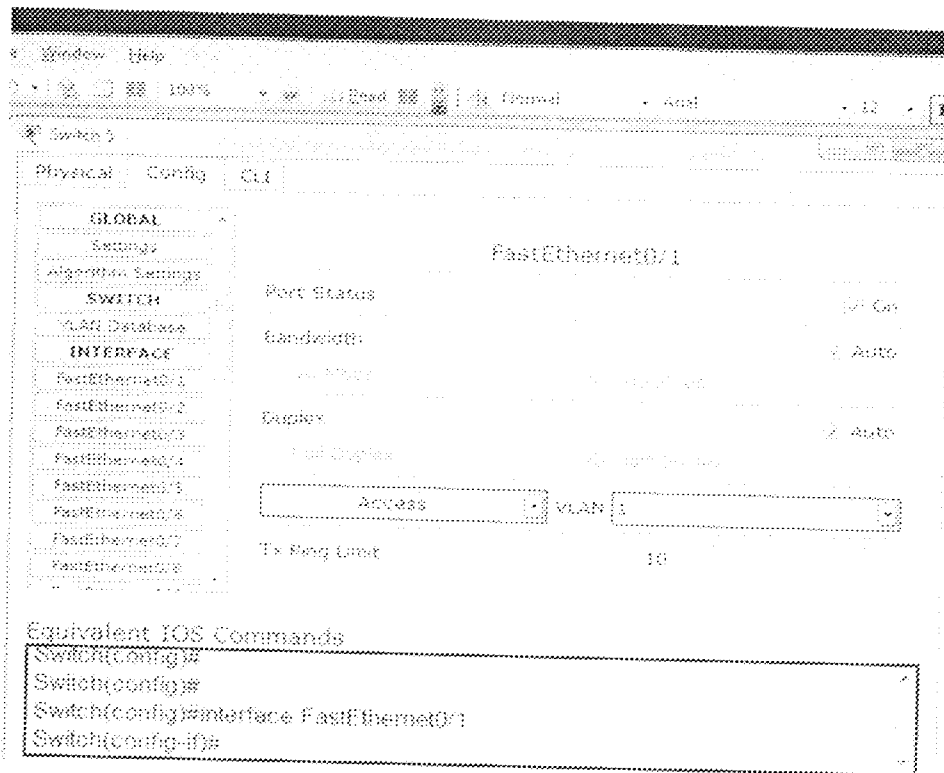


Figure 3.14: Port configuration panel

3.5 Dhcp Server Configuration

The DHCP property of the server is configured from the services sub-tab, the start IP address and subnet mask were configured as 172.10.10.10 and 255.255.0.0 respectively. Figure 3.15 illustrates configuration of DHCP server to automatically allocate IP addresses to users.

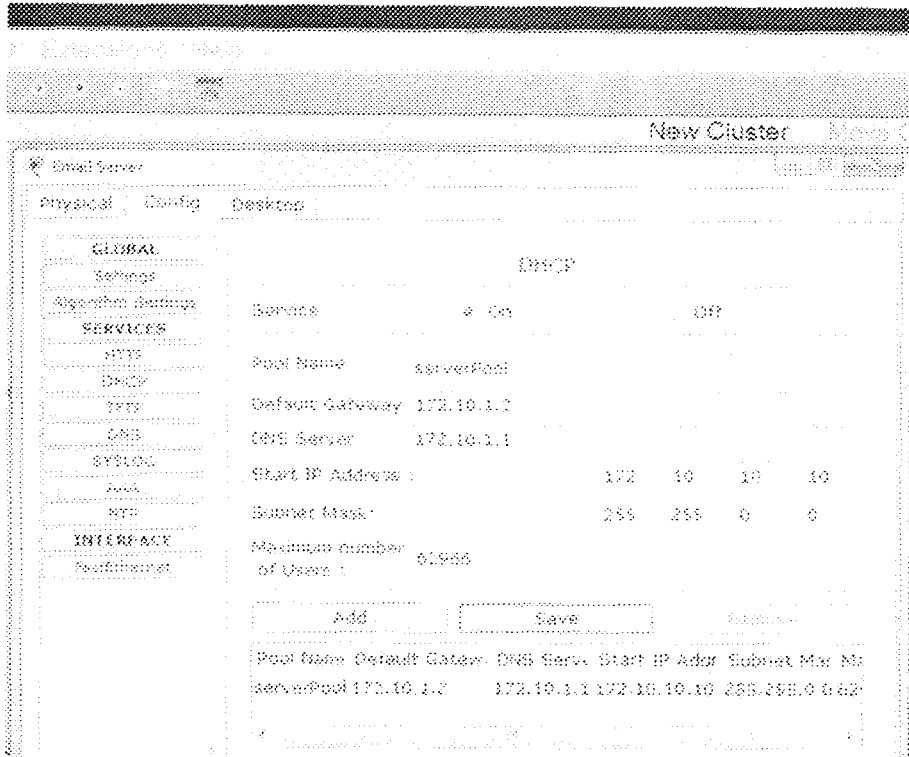
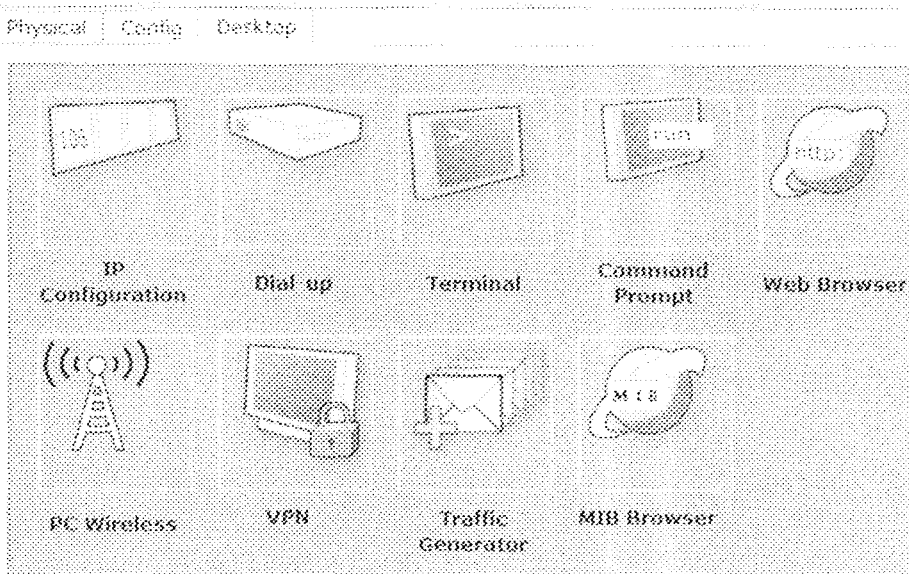


Figure 3.15: DHCP server configuration panel

Similarly, figure 3.16 illustrates configuration of desktop user to automatically acquire IP address from DHCP server.



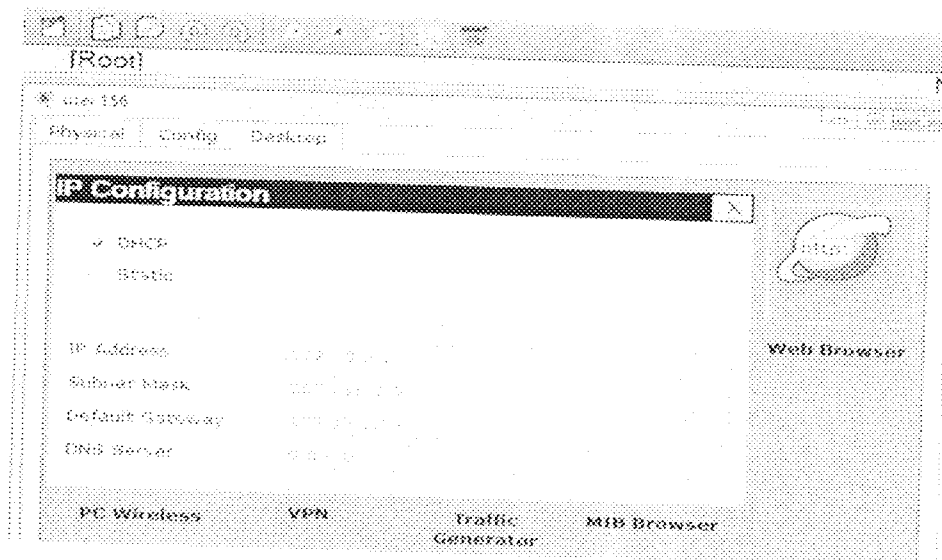


Figure 3.16: users IP configuration panel

3.6 Configuring inter-VLAN Routing

Network devices in different VLANs cannot communicate with one another without a router to route traffic between the VLANs. In most network environments, VLANs are associated with individual networks or subnetworks. For example, in an IP network, each subnetwork is mapped to an individual VLAN. In a Novell IPX network, each VLAN is mapped to an IPX network number. In an AppleTalk network, each VLAN is associated with a cable range and AppleTalk zone name.

Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, when an end station in one VLAN needs to communicate with an end station in another VLAN, inter-VLAN communication is required. This communication is supported by inter-VLAN routing.

The inter-VLAN was implemented at the central switch at ICT Centre to allow the members of other VLANs that are not in the same VLAN with the application server but possess authentication key to access the application server. To curb

others that do not have the authentication key to access the application server, an authentication scheme is incorporated. The mechanism used by the scheme is discussed in Section 3.7

3.7 Authentication Scheme for Secured Application

Login access presents a challenge to network managers entrusted with network security. Our authentication scheme to be implemented is designed to authenticate, authorise, and account every user that requests service from the application server. Authentication, Authorisation and Accounting (AAA) technologies are based on Cisco product capabilities (Cisco, 2009). For the purposes of this design, the following generic definitions apply:

- *Authentication*: The process of validating the claimed identity of an end user or a device, such as a host, server, switch, router, and so on.
- *Authorization*: The act of granting access rights to a user, groups of users, system, or a process.
- *Accounting*: The methods to establish who, or what, performed a certain action, such as tracking user connection and logging system users.

Depending on the conventions and requirements of particular design, one could select a security environment which utilizes *Terminal Access Controller Access Control System Plus (TACACS+)* or *Remote Authentication Dial-in User Service (RADIUS)*.

3.7.1 Authentication Server Configuration

In the AAA service configuration, we set up the server to be a RADIUS server. The Radius was configured as AAA server. In addition to configuring the AAA server, we also need to add authorised users. To add authorised users, we enter the **UserName** and **Password** for the user and click on the + button. The configuration panel is as shown in figure 3.17, device R1 is a router that grants all the users access to the application server. It is being configured to use AAA authentication on the VTY lines using authentication list telnet_lines. The authentication list uses RADIUS as its source for login information which is configured to poll the Radius_Server device on 192.168.10.2 using the key.

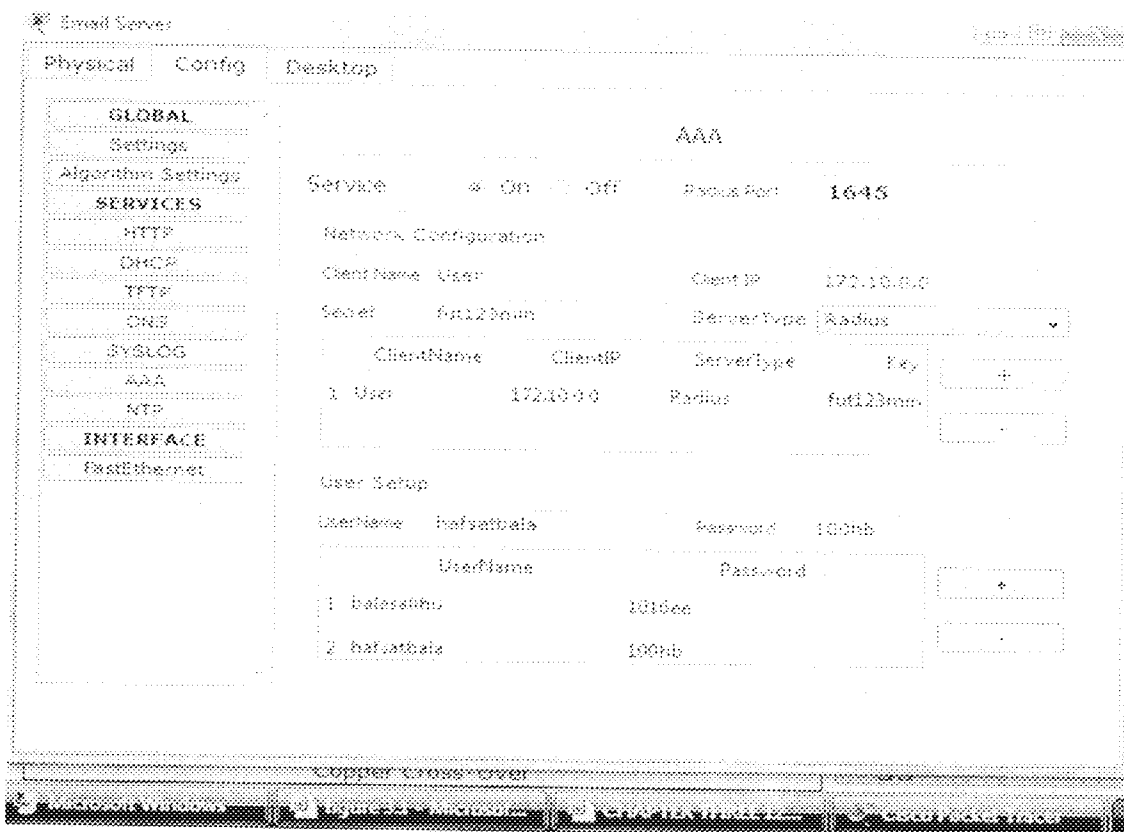


Figure 3.17: RADIUS server configuration panel

Figure 3.18 shows the network layout for securing the Application server. The switch could be any of the area switches within the network.

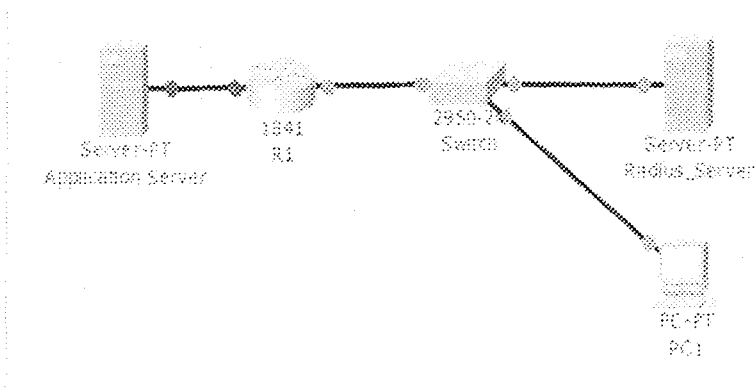


Figure 3.18: Network layout for securing application server

3.7.2 User Verification Procedure

- a) As shown in figure 3.17, the network user at PC1 terminal performs the request to access application server by entering his/her user ID and password.
- b) This information is passed to a Network Access Server R1 device, then to RADIUS server over the RADIUS protocol.
- c) The RADIUS server checks that the information is correct using authentication schemes. If accepted, the server will then authorise access; if otherwise access is denied.

Interaction protocol between client and server utilizes UDP transport protocol.

RADIUS packet structure in computer network is as displayed in Figure 3.19

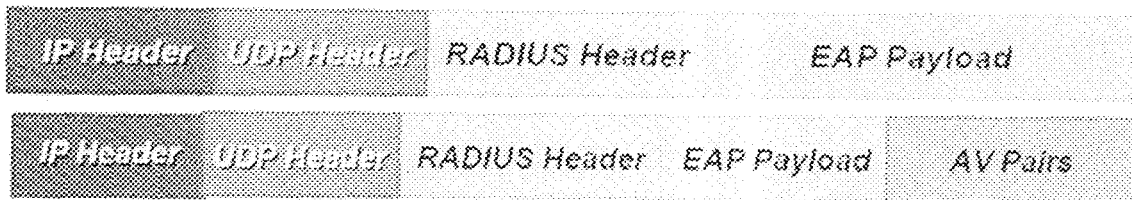


Figure 3.19 RADIUS packet structure, request and response in computer network.

Password protection is based on following principle;

$$C_1 = P_1 \oplus \text{MD5}(S+RA)$$

$$C_2 = P_2 \oplus \text{MD5}(S+C_1)$$

$$C_n = P_n \oplus \text{MD5}(S+C_{n-1})$$

where

RA= Request Authenticator

C_1 ----- C_n = cipher text block

P_1 ----- P_n = password broken into 16-octet blocks

MD5= hash 1 encryption algorithm

The client and server share a secret. That shared secret (S), followed by the Request Authenticator (RA), is put through an MD5 hash to create a 16 octet value which is XORed with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the Request Authenticator. The User-password attribute contains $C_1+C_2+\dots+C_n$, where + denotes concatenation. After the server receives the RADIUS access-request packet, authenticator device is

verified through address and secret password stored on server. If server does not possess a shared secret for the authenticator, the request is silently dropped. Because the server also possesses the shared secret, it can obtain the unprotected password through reverse algorithm and, using its authentication database, validates the username and password. If the password is valid, the server creates an Access-Accept packet to send back to the authenticator. If the password is invalid, the server creates an Access-Reject packet. If authenticator receives a response packet, it attempts to match it with an outstanding request using the identifier field. If the client receives a verified packet, with correct login information, user computer is authenticated (Liberios, 2004).

CHAPTER FOUR

4.0

RESULTS

The result of standard formulas derived in Chapter 3 (queuing theory formulas) for analysing the network performance provide explicit way of representing the network properties analytically. Similarly, Cisco packet tracer simulator offers the test bed for modeling and evaluating the newly designed network. The results of the analysis and the properties of the modeled network are presented in this chapter.

4.1 Analytical Result of the Network Dissection

Following the earlier assumptions of an M/M/1 system for the entire network in Chapter 3, the modeled network with six VLANs has been segmented into 6 different broadcast domains, each of the domain independent of the others for their intra communication. Thus, the network delay for each domain is calculated using same M/M/1 equations. Assuming equal distribution of the messages being sent to the network by the users, the message length per VLAN will now be equal to one-sixth of the mean message length into the network. Thus,

$$\text{message length per VLAN} = \frac{1}{6} \times 120 \text{ Mb/sec} = 20 \text{ Mb/ sec.}$$

Hence, mean service time per VLAN

$$T_s = \frac{20}{85} = 0.235 \text{ sec}$$

Network utilization per VLAN

$$\Psi = \lambda T_s = 0.5 \times 0.235 = 0.118 \approx 11.8\%$$

and, mean waiting time

$$w_t = \frac{\Psi T_s}{1 - \Psi} = \frac{0.118 \times 0.235}{1 - 0.118} = 0.0314 \text{ sec}$$

From the above analysis, it is glaring that the mean service time T_s for the network users and the waiting time w_t have reduced (improved), while network utilisation has also reduced as shown in Table 4.1. Thus, more users or broadcast can be accommodated without saturation.

Table 4.1: Network properties before and after VLAN

s/ no.	Network properties	Before VLAN	After VLAN	inference
1	Mean service time T_s	1.412 sec.	0.235 sec.	Reduced by 83.36%
2	Network utilisation	70.6%	11.8 %	Improved 83.29%
3	Mean waiting time	3.391 sec.	0.0314sec.	Reduced by 106.86%

4.2 Simulation Results Before VLAN Implementation

The simulation of the IBBU Lapai network considered in fig 3.1 shows that grouping of network users that were not connected to the same switch was not feasible. The proof of this weakness within the network was obtained by trying to establish communication across switches. Figure 4.1 shows the analysis of such attempts.

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
●	Failed	User 2	Email Server	ICMP	■	0.000	N	0	(edit)	(delete)
●	Failed	user 4	E Library server	ICMP	■	0.000	N	1	(edit)	(delete)
●	Failed	user 5	user 7	ICMP	■	0.000	N	2	(edit)	(delete)
●	Failed	user 6	user 9	ICMP	■	0.000	N	3	(edit)	(delete)

Time: 00:26:31 | Power Cycle Devices

Figure 4.1: Communications between users connected to different switches

In figure 3.1 the communication request sent from user 2 connected to switch 2, to E-mail Server connected to switch 1, failed because the frame could not traverse the network links to the expected destination. Similarly, communication request from user 4, User 5 and user 6, to E-Library server, user 7 and user 9 respectively also failed as depicted in figure 4.1 regardless of the fact that all the nodes use the same IP subnet. This is because they are not in the same VLAN.

In contrast, communication between user 1 and the E-Library server was successful because the two communicating devices were connected to the same switch and share the same IP subnet. Figure 4.2 shows the details of

how echo request sent from user1 traverses through the network links and devices to the E-Library server. Similarly, communication link from wireless user 7, user 70, and user 134 to user 9, Bursary server and user 240 respectively were all successful because all the pair communicating devices were connected to the same switch.

File	Last Status	Source	Destination	Type	Collis	Time (sec)	Periodic	Item	Edit	Delete
	Successful	User 1	E-Library Server	ICMP		0.000	N	0	(edit)	(delete)
	Successful	user 7	User 9	ICMP		0.000	N	1	(edit)	(delete)
	Successful	user 70	Bursary Server	ICMP		0.000	N	2	(edit)	(delete)
	Successful	user 134	user 100	ICMP		0.000	N	3	(edit)	(delete)

Time: 02/27/20 | Power Cycle Devices

Figure 4.2: Intra switch link test

However, every host can reach the router successfully. This means that every network user can access the internet service via the router irrespective of its location within the network. The ping tests from user 1, wireless user 9 and user 300 to the router were all successful as shown in figure 4.2. Each Ethernet interface of the router is configured with different subnet as indicated in Table 4.2.

Table 4.2: Central switch interface IP addresses

S/no.	FastEthernet interface	IP address	Subnet	Link to network
1	1/0	172.10.10.30	255.255.0.0	Switch 3
2	0/0	172.10.20.30	255.255.0.0	Switch 2
3	0/1	172.10.30.30	255.255.0.0	Switch 4

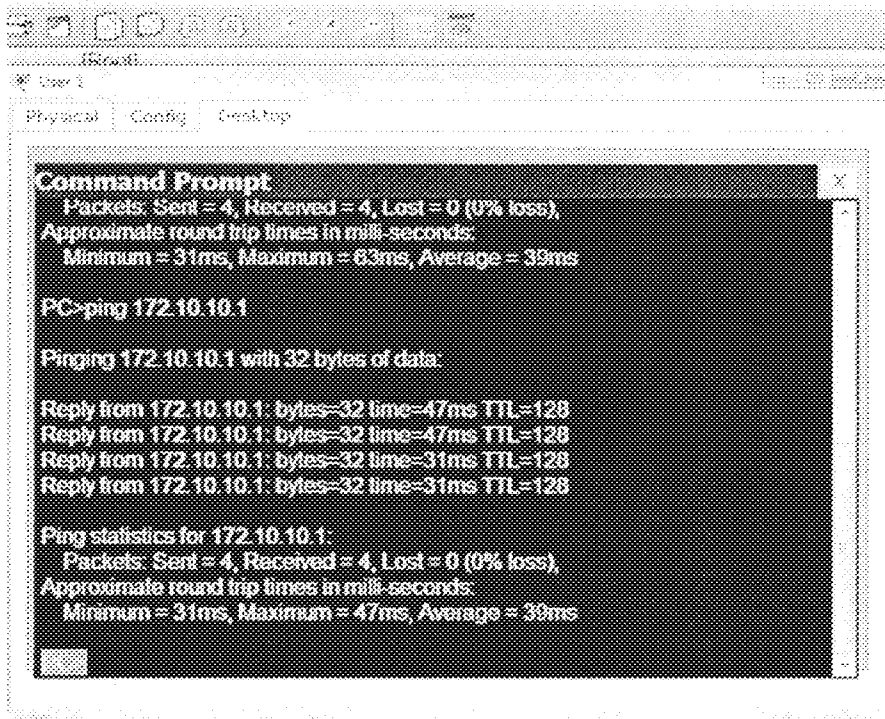


Figure 4.3: Ping replies received at the user 1 terminal from router 0 (average time taken for reply is 39ms)

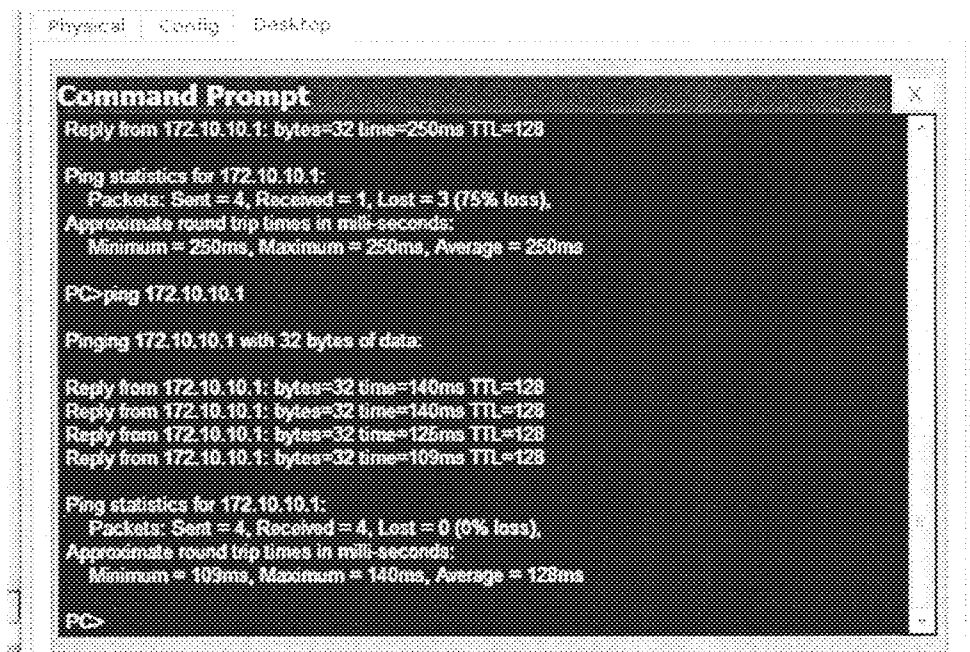


Figure 4.4: Ping replies received at the user 91 terminal from router 0 (average time taken for reply is 128ms)

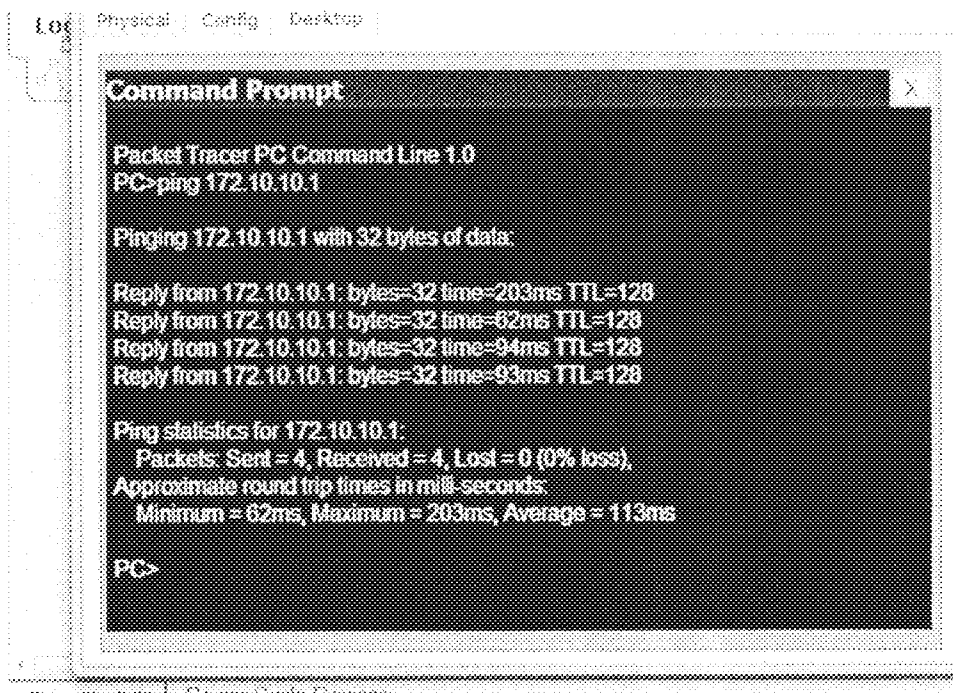


Figure 4.5: Ping replies received at the user 159 terminal from router 0 (average time taken for reply is 113ms)

Comparing the successful ping test shown in figures 4.3, 4.4 and 4.5 it could be observed that the reply time is inversely proportional to the distance away from the Router 0 in figure 3.1. Thus, the network is distance biased.

4.3 Simulation Results Obtained After VLAN Implementation

Subsequent to implementation of 6 VLANs, inter-switch communication was established which was not possible in the existing network. In figure 4.7 it is confirmed that the only successful communications were intra-VLAN, which was practicable because trunk links exist between adjacent switches.

File	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit
	Successful	Bursar	HOD MIS	ICMP	White	0.000	N	0	(edit)
	Successful	HOD MIS	Database server	ICMP	Black	0.000	N	1	(edit)
	Failed	user 4	Database server	ICMP	Grey	0.000	N	2	(edit)
	Successful	SEC CEO	Database server	ICMP	Light Grey	0.000	N	3	(edit)
	Successful	SEC CEO	Email Server	ICMP	Dark Grey	0.000	N	4	(edit)

Figure 4.6: Intra and inter switch communication attempts

4.4 Test for Infrastructure-Based VLAN

From figure 4.7 ping request from user 48 in VLAN5 and CEO in VLAN2 to Mail server were successful. These scenarios confirm that both servers belong to more than one VLAN which implies that the VLAN implemented is infrastructure-based.

File	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit
	Successful	User 48	Email Server	ICMP	Black	0.000	N	0	(edit)
	Successful	user CEO	Database server	ICMP	White	0.000	N	1	(edit)
	Successful	user 4	Email Server	ICMP	Light Grey	0.000	N	2	(edit)
	Successful	HOD MIS	Library Server	ICMP	Dark Grey	0.000	N	3	(edit)

Figure 4.7: Communication links to test link to server from various network users.

4.5 Tests for Secured Application

Intrusion into secure application server was impracticable for unauthorised users. Fig 4.9 shows two unsuccessful attempts by unauthorised network users. However, at the third attempt the correct user name and password

were provided by authorised user and access was granted after successful authentication.

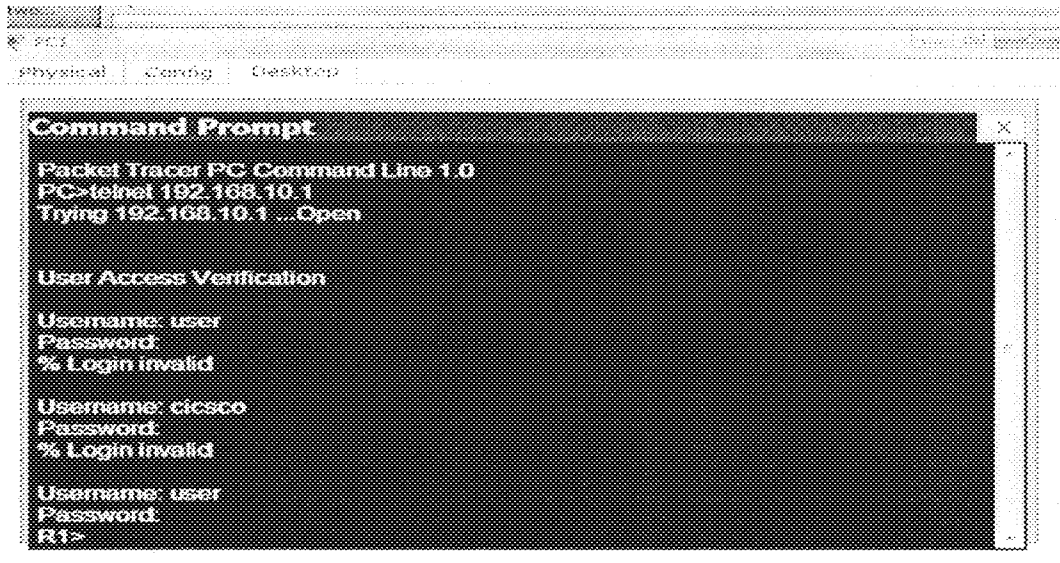


Figure 4.8: User login verification

CHAPTER FIVE

5.0 DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1 Discussion

The design and implementation of infrastructure-based VLAN for secure applications which is the focus of this project work yielded results. Our case study, the Ibrahim Badamasi Babangida University (IBBU) Lapai Main campus network was analytically dissected to evaluate the network performance and behaviours. Both analytical and simulation results obtained provide the bases for our design and subsequent prototype implementation.

5.1.1 Analytical Results

The entire network was assumed to be a typical M/M/1 scenario. This is because all the users within the network tend to compete or share the network resources with no segregation or preference for any user within the network. Thus, every user possesses equal probability to access the network facilities. The result obtained shows that the network utilisation was 70.6% which implies that any upsurge in the number of users or number of requests within the network, particularly during peak hours cause network congestion. This circumstance reduces the network throughput to almost zero, which means no user enjoys the service of the network at that particular period. After redesigning the network, the network average utilisation was reduced to 11.8%. At this value the tendency of congestion is highly reduced even at peak hours.

Similarly, the mean service time and the mean waiting time reduced from 1.412 seconds and 3.391 seconds to 0.235 seconds and 0.036seconds respectively, thereby making the network more robust for all users.

5.1.2 Simulation Results

From simulations it was observed that users that were not within the same location (switch) cannot communicate directly. This situation makes it impossible for logical grouping of network users. Subsequent to implementation of our design of VLANs, inter-switch communication was established. Thus, the network users could be grouped logically to exchange information (e.g among committee members). Also, the VLAN implemented reduced the migration cost of stations going from one group to another. Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by using software. We were also able to provide an extra measure of security, people belonging to the same group (VLAN) can send broadcast messages with guaranteed assurance that users in other groups will not receive these messages.

5.2 Conclusion

The success recorded in this work was not hitch-free, some of these problems were overcome through consultations. However, some of the underlying problems are mentioned here

- i. The information collected from the operators and the administrators of the IBBU Lapai network were verified before use, particularly information about the network equipment in use. We thus, result to collect the information and find a way of verifying same by seeking access to such equipment.

- ii. We always tried to compare our result with real life behaviour of the network. However, at most times we have to liaise with the network users to grant us access to their computers. Some of our results were based on mathematical analysis and software simulation. Though, we were able to make up to about 65% of such comparison. The comparisons we made aid us in obtaining better results.

- iii. Equipment like radios and the switches and routers within the network were not configured by the network administrators; they were mostly installed and configured by the contractors. Hence, we could not login into the equipment to access the configuration file. Nonetheless, we made assumptions from those that were accessible.

- iv. Lack of equipped network laboratory in the department. If such laboratory exists we would have been able to simulate the real network scenario.

5.3 Recommendations

- i. The department of Electrical and Computer Engineering should set up a well equipped network laboratory with practical laboratory manuals to serve as teaching aid for data communication network and related courses.

- ii. The Department should purchase full versions of simulation softwares (e.g ns-2 , OmNet++ , OpNet etc) with their respective detailed manuals. All the versions used to implement this work were free educational versions which restrict users' access to some important features needed for proper network analysis.

REFERENCES

- Aaron, S.M. (2004): *Implementation of Virtual LAN for virus containment*, New Mexico Tech, Socorro, NM, infohost.nmt.edu/~sfs/Students/AaronSolo/Papers/seniorproj.pdf
- Behrouz, A.F. (2007): *Data Communication and Networking*, fourth edition, McGraw-Hill International edition, pp. 434.
- Cisco Systems, Inc. (2002), *Cisco Certified Network Associate study Guide*, fourth edition, pp. 348.
- Cisco Systems, Inc. (2002): *Virtual LAN Security Best Practices*, www.cisco.com/warp/public/cc/pd/si/casi/ca6000/.../vlnwp_wp.pdf
- Decisys Inc., (1996): *The Virtual LAN technology Report*
<http://www.3com.com/nsc/200374.html#aaaa>
- Honda, O., Ohsaki H. and Imase, M. (2005): *A Prototype Implementation of VPN Enabling User-based Multiple association*,
<http://cifeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.80.5599>
- John, M. and Tony, T. (1996): *Do VLANs Make Sense in Your Network?*, Business Communications review.
- Juniper Networks, (2009): *VLAN Design for IPTV/MULTIPLAY NETWORKS*, White paper, www.juniper.net/us/en/local/pdf/whitepapers/2000186-en.pdf
- Minli, Z., Mart, M. and Bala, B. (2007): *Design and implementation of Application-Based Secured VLAN*, <http://eeexplore.ieee.org/iel5/9433/29935/01367248.pdf>
- Prashaunt, G., Nan, Z., Yu-wei S., and Sanjay R , (2007): *Characterizing VLAN usage in an Operational Network* , purdue University publication.
<http://docs.lib.purdue/ece/tr/362>

- Sheldon, T. (2001): *Encyclopedia of Networking and Telecommunications*, Network management protocols, TATA McGraw-Hill edition, pp 603, 271.
- Sasaki, M., Yokota H. and Akira I. (2009): *VLAN-based QoS Control in Mobile*. <http://www.icmu.org/icmu2006/pdf/ICMU2006-1568990697.pdf>
- Sanjay, P. (2005) *The complete Reference Data Communications and Computer networks* A.K Jain, Second Edition, pp. 33.
- Taha, H. A. (2006): *Operations Research an Introduction*, 7th edition, Pearson Education Inc. pp.233-236, 246-251.
- Trend communications.(2008): *Scalable Ethernet Using VLAN Stacking*. www.trendcomms.com/.../Scalable+Ethernet+Using+VLAN+Stacking/.../an.tango.gbe.qig.pdf
- Vijay, A. (1987): *Design and Analysis of computer Communications Networks*, McGraw Hill Inc. 117 pp, 271-275
- White paper: **Authenticated VLANs**,(2002): Secure Network Access at Layer 2 November2002,<http://www.alcatellucentbusinessportal.com/support/.../doc/link.cfm?id...>