Faculty of Computing and Information Management
KCA University

DATA SECURITY IN GOVERNMENT NETWORK INFRASTRUCTURE

EUSTUS K.MUKIRI

Reg. No. 12/00293

A Masters Dissertation Submitted to

Faculty of computing and Information Management, KCA University

in partial fulfillment of the requirements

for the degree of Master of Science in Data Communications

NOVEMBER 2014

ABSTRACT

Most public organizations have deployed Local Area Networks in their buildings to enhance sharing of resources. These networks are poorly done such that security of data and information is compromised thereby exposing data to unauthorized users who may be within or outside the organization. To ensure data/information is well secured, organizations have decided to implement Virtual Local Area Networks (VLAN) whereby users are grouped according to departments to access resources associated with their department. This research project shows how to secure data in government network infrastructure by implementing secure VLANs.

Acknowledgements

First and foremost I offer my sincere gratitude to my supervisor, Prof Ddembe Williams, who has supported me throughout my research with his patience and knowledge whilst allowing me the room to work in my own way. I attribute the level of my Master's degree to his encouragement and effort and without him this Dissertation would not have been completed.

I would also like to acknowledge the support and guidance given by my classmates- January 2012 Cohorts in the research organization especially after loss of my wife during the period of research. Their persistent encouragement and relentless effort lead to timely completion of this thesis.

Table of Contents

Acknowledgements iii

LIST OF TABLES 1

CHAPTER ONE 2

1. INTRODUCTION 2

1.1. BACKGROUND 2

1.2. Sources of problems in Government Data Security 4

1.3. Definition of Terms 5

1.4. Problem Statement 6

1.5. Aims and Objectives 7

1.5.1. Aims 7

1.5.2. Specific Objectives 7

1.5.3. Significance of the Project 7

1.6. Scope of Project 7

1.7. Justification 8

1.1. CHAPTER'S SUMMARY 9

CHAPTER TWO 10

LITERATURE REVIEW 10

2. Introduction 10

2.1. State of the art in Government Data security 10

2.2. Vulnerabilities on government network infrastructure 13

2.3. State of practice in Government data Security 16

2.4. Technological Advancement in Government data security 17

2.4.1. Firewalls 17

2.4.2. Public Key Infrastructure (PKI) 18
2.4.3. Intrusion Prevention Systems (IPS) 20
2.4.4. Event Correlation Systems (ECS) 21
2.4.5. Virtual Private Networks (VPN) 21
2.4.6. Virtual local Area Network 22
2.4.7. Intrusion Detection and Analysis System 25
2.4.8. Anomaly Detection Systems (ADS) 25
2.4.9. Vulnerability Scanning Systems 26
2.4.10. Access control management (ACM) 27
2.5. The Open System Interconnected Model (OSI) 28
2.6. Critic of literature problems 30
2.7. CHAPTER'S SUMMARY 31
CHAPTER THREE 32
PROJECT PLANNING AND METHODOLOGY 32
3. INTRODUCTION 32
3.1. Research Methodologies 32
3.1.1. Exploratory Research 32
3.1.2. Descriptive research 33
3.1.3. Causal research (Explanatory) 33
3.1.4. System Development (SD) 34
3.1.5. Proposed methodology 39
CHAPTER FOUR 40
4. CONCEPTUAL MODELLING AND FIELD STUDIES 40
4.1. Introduction 40
4.2. Conceptual Model 40

4.3. Survey and planning stage 41
4.4. Project requirements 41
4.4.1. Project facilities 41
4.4.2. Software requirements 41
4.4.3. Hardware requirements 42
4.5. Simulation Tool (Cisco Packet Tracer) 43
4.6. Existing Network 44
4.7. LAN Topology 46
4.8. Configuration of Routers, Switches and Hosts 47
4.8.1. Naming of the network devices (Router and switches) 47
4.8.2. Router configuration: 47
4.8.3. Switch configuration: 48
4.8.4. Hosts Configuration: 49
4.9. Testing by simulation 49
4.9.1. Simulation analysis 50
CHAPTER FIVE 52
5. VLAN IMPLEMENTATION 52
5.1. INTRODUCTION 52
5.2. Implementation Model 53
5.3. Requirement analysis 53
5.4. Decision analysis 54
5.5. New VLANs Design 55
5.6. Configuration of VLANs, Routers, Switches and Hosts 57
5.6.1. Naming of network Devices (router and switches) 57
5.6.2. Router configuration: 58

5.6.3. Switch configuration: 58
5.6.4. Trunk configurations: 59
5.6.5. VLAN Configuration: 59
5.6.6. VTP Configuration: 60
5.6.7. Hosts Configuration: 60
5.6.8. Access control list configuration 60
5.7. Testing the designed VLANs 61
5.7.1. Host to host testing 61
5.8. Install and Implement the Network 63
5.9. Maintenance and support 63
5.10. Documentation 64
CHAPTER SIX 65
CONCLUSION AND FURTHER WORK 65
REFERENCES 66
APPENDIX: TEST RESULTS 85

LIST OF FIGURES

Figure 1: Multimethodological Approach to IS Research 35

Figure 2: Process of System Development Life Cycle.. 36

Figure 3: Current Logical LAN setup for Ground to 3rd floor 46

Figure 4: Logical representation of Designed VLANs 57

LIST OF TABLES

Table 1: evaluation of the methodologies 38

Table 2: software requirements 42

Table 3: hardware requirements 42

Table 4: Assigned IP Addresses 49

Table 5: Host to Host Testing 50

Table 6: VLAN to VLAN testing 51

Table 7: Assigned VLANs 55

Table 8: New IP Address Allocation 56

CHAPTER ONE

1. INTRODUCTION

This chapter gives a brief review which introduces the reader to the background of the research about data security in Government network infrastructure. Under the problem statement the foundation and the direction of the research is established. After problem statement the research affirm the fundamental objectives of the project, the scope and justification of the project.

1.1. BACKGROUND

According to Awondele et al.(2012), government networks are devoted infrastructures implemented to transmit data and information traffic inform of voice, video, and data from one network node/device to another. The network infrastructure comprise of various number of devices which are interconnected by either wireless or physical mode of transmission.

Data and information vulnerabilities which are associated with computer networks have increased rapidly and are among some of the concerns for those who manage and administer network infrastructure. This is because it continues to provide increased threats to the efficiency and integrity of companies and even public organizations, Curry et al., (2011).

Electronic Government is all about the use of Internet based information technologies and IT applications by the government for the delivery of smooth electronic services and information to the public, businesses or other government agencies by integrating processes. Moreover, it demands secure channels for information/data exchange without compromising security or exposing sensitive information between government agencies, citizens and structured organizations. In line with OECD (2005) the determinants for the success of E-Government are

‘available technologies and their interoperability, level of access that citizens and business will have, citizens’ attitude and awareness of e-Government services, the overall trust in electronic channels by citizens and business, and their expectations of the types of services that should be delivered and how they should be delivered.’

The rising threat of data and information in computers and also increasing threat to repository of information have stimulated much interest in technical safeguards to protect data (Denning Denning, 2009).

According to Alabady (2009), security of Local Area Networks is at the forefront of computer related issues. The emergence of new technologies has led to increased threat to data and information. Many of the threat are done in a sophisticated way, causing damage, theft or completely loss of information. As Government and business critical applications becomes available on the internet, a lot of threat to the application increase.

Data/information is an asset that must be secured (Kim et al., 2004). Rush to have Local area networks come at the expense of adequate data security. Without adequate protection or network security, governments, many individuals and even businesses are at risk of losing critical data in their organization. The main aims of security are to protect confidentiality, maintain integrity, and assure availability of the data. Bearing this in mind, it is important that all networks be protected from threats and vulnerabilities in order for businesses to achieve their fullest potential. Threats are persistent due to vulnerabilities, which can arise from poor Local area network design, mis-configured hardware or software or end-user carelessness.

Network security is a vital component when securing data because it is responsible for securing all information passed through networked computers (Kim, 2004). Network security

refers to all hardware and software functions, characteristics, features, operational procedures, access controls, administrative and management policy required to provide an acceptable level of protection for hardware, software, and information in a network. With this in mind the security of data will be enhanced

According to Rao and Choudhury (2010), Network can be physical or wireless interconnection of computers and communication devices that allow many users to share data or information or even resources within a defined geographical area, either a building or a group of buildings.

In this research the LAN, will be the independent interconnection of The Treasury building.

1.2. Sources of problems in Government Data Security

Information and Communication Technologies (ICTs) have increasingly become indispensable tools for development over the past few decades (Emanuel and Sife 2008).In terms of security issues, organizations experience threats such crushing of databases due to low security settings, and computers being attacked by viruses and worms. According to (OECD, 2003), Government organizations have the responsibility to build up a tradition and a norm for confidentiality, data protection and also data/information security. Information/data protection is not just a technical issue; it also involves issues such as training, sensitizing and educating staff and users for privacy , reducing or limiting access to user identifiable information (Fisser, 2001). Computers require up to date antivirus software, most of which are very expensive.

Public Key Infrastructure (PKI) can also be used as a countermeasure to safeguard data and information. Whether it would be integrated into an authentication system or part of a code signing system, the overall goal is to ensure Integrity (NIST, 2004). Additionally, PKI can serve in a capacity of ensuring that Confidentiality of data through trusted encryption mechanisms that

leverage trusted encryption materials. This technology is currently expensive to implement and very few governments have it in place.

1.3. Definition of Terms

E-government

According to the United Nation (2002) E-government is recognized as utilizing the NET and the (www) world wide web for the government to transact information and offer services to citizens.

Government

The Commonwealth of Nations (2005) identifies governments as a system by which a state or community is government.

ICT

As defined by the Information Technology Association of America (ITAA), ICT is the study, development, design, implementation, support or management of computer-based information systems, particularly software applications and computer hardware. IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit and retrieve information, securely.

Network

According to The Federal Networking Council (2011) a Network is a group of hardware components and computers interlinked by communication channels that allow exchange and sharing of data, information and resources.

System

According to Sun Microsystems (2011), a system is an orderly, purposeful structure regarded as a whole and consists of interrelated and interdependent elements (entities, factors ,components,

members, parts etc.). The entities, factors, components continue to influence one another (directly or indirectly) to maintain their activity and the continuous operation of the system, in order to attain the objective of the system.

Technology

IEEE defines technology as the use of scientific knowledge, experience and resources to create processes and products that fulfill human needs.

1.4. Problem Statement

According to most of the Organizations such as public and private sectors, they have deployed computers to their employees to perform their daily work and access resources from their network. Use of ICT has enabled organizations to operate their businesses much faster and more conveniently and also it make easy for the organization. While this has been done there are some problems still faced by the organizations such as poor network design by having large broadcasts within the network and inadequate data security Due to this, organizations have decided to implement VLAN (Virtual Local area Networks) to solve these problems (Shaffi and Al-Obaidy, 2012). Data and information are critical assets of the government, facilitating decision making process and stimulating economic growth. With the implementation of e-government, data sharing has been enhanced and can now be accessed and manipulated from any point. However, advancements in information communication technology (ICT) have raised concerns about the risks to data associated with weak ICT security. Lack of proper designed Local Area Network has contributed to vulnerability of data making it very easy for unauthorized people to locate and access the data (Kim et al., 2004). It's very important to have a well-planned and designed LAN which is grouped according to the users or the resources to ensure security of the data.

1.5. Aims and Objectives

1.5.1. Aims

This study aims at investigating the Local Area Network with intent of designing and simulating VLANs that will act as a pillar for implementing data security in the Government of Kenya National Treasury as the case study.

1.5.2. Specific Objectives

- Design VLANs that can be implemented to mitigate data security breaches in The National Treasury
- Test the VLANs using the simulation tool

1.5.3. Significance of the Project

- The research will be used to design VLANs to secure data in the with intent of being replicated in public and private organizations
- To help network administrators manage network resources and users centrally

1.6. Scope of Project

The scope of the project is to design National Treasury Building LAN with VLAN enhancements to assist in the security of Data and information. For simulation purposes, Cisco Packet Tracer will be used and various open protocols like ping, telnet will be used to test the connection of the different devices within the Local Area Network. The VLAN will be designed for the following departments in the National Treasury; ICT, Accounts, HRM, , Supply Chain Management and Admin. This will be replicated to other departments once the research is completed.

1.7. Justification

Volatile growth in ICT systems and networks has increased the dependence of both organizations and individuals on the information stored and communicated using these implemented systems. This creates the need to secure data and resources from any threat within and outside the networks (Stallings 2003).

Different levels of security are appropriate for different groups, organizations and even users. Organizations and individuals can ensure better security by using systematic approach that includes analysis, design, implementation and maintenance. The analysis phase requires that one to thoroughly investigate your entire network, both software and hardware, from inside and outside. This helps to establish if there are or may be vulnerabilities. The analysis will gives a clear picture of what is in place and what is required for future Ahmad and Habib (2010)

At the same time organizations must provide reliable and secure local area networks to access and share data/information. To ensure this, all servers should be placed in one Local area network for easier management, security and easier monitoring. This can be implemented through logically dividing the existing LAN to have VLAN for servers and for each department.

Following the last general elections held in Kenya, and the constitution created only twenty two Ministries, the Government in place reduced the Ministries from the existing forty two to only eighteen whereby this led to massive transfers of staff to the few ministries created.

Since there was no enough space to host the different cadres of staff being transferred from various other government agencies, they were allocated offices haphazardly on different floors. This led to having many departments hosted per floor while else the various networks were designed per floor.

This has led to The National Treasury network experiencing challenges on scalability and data security thereby compromising its availability, integrity and reliability. Due to staff sharing the available resources on the one network per floor, staff can view and even access resources for other departments of which they are not supposed to do.

Applications like Integrated Financial Management Information Management (IFMIS) and integrated personnel Payroll Database (IPPD) which is accessed by Government institutions should be safeguarded by ensuring it's accessed by the right users.

To mitigate the security of the different departments and their resources, this research is going to design and create various VLANs for use per department and even recommend various methods which can be used to improve the security of the information.

1.1. CHAPTER'S SUMMARY

This chapter gives a general introduction to the project, statement of the problem, aim, objectives of the project, justification, scope and significance of the study.

CHAPTER TWO

LITERATURE REVIEW

2. Introduction

The chapter presents the theoretical framework and reviews existing literature related to this study. According to Fraenkel and Wallen (2003), a literature review helps researchers learn what others have written about a topic. It also lets researchers see what have been the results of other related studies. It includes examining documents such as journals, magazines and dissertations that have a bearing on the research being conducted (Kombo and Tromp, 2006).

The literature reviews analyze several themes related to data security in government. The chapter addresses the issues contained in the research problem and objectives of the project.

2.1. State of the art in Government Data security

According to (Khidzir , Mohamed and Arshad, 2013) information and Data security involves the activities, processes, controls and efforts that aim to protect information and data, and their underlying infrastructures. It continues to explain that confidentiality; integrity and availability are the core principles of information and data security and broadly used in most study fields.

Federal Bureau of Investigation (FBI) said "identity theft have emerged as one of the dominant white collar crime problem of the 21st Century. Estimate vary regarding of the two impact of the problem but agreement exists that it is pervasive and growing (Deybach 2008)".

Elssied et al.,(2011) explains that increase in use of electronic government have led to loopholes and unintended data or information security breaches and created new vulnerabilities to cyber

threat .To face these new challenges, governments all over the world should come up with effective cyber security strategies to mitigate the security breaches.

Elssied, et al.,(2011) also explains that users in a secured system should have reasonable anticipations that their data is well protected against unauthorized access or modification, and data is still available. As explained some of the security attributes are;

Confidentiality: the data or the information transacted by the governments is only accesses by authorized users and no one can see it unless authorized to do so..

Integrity's: information or data transacted through the e-government cannot be altered/ modified during the transmission.

Non-repudiation: the e-government information cannot be denied

Controllability: The dissemination of the Internet information can be controlled.

Efficiency: is a measure of speed and cost or is getting all you're testing done in the least time possible with the small amount of resources,

Effectiveness: it concern with high quality regardless of speed or is doing the job right. Efficiency means "doing the thing right," Effectiveness means "doing the right thing."

Vagueness: these are things that are not clearly, precisely, or even definitely expressed or stated or not precisely determined or known also means uncertain.

Accuracy :The state of being exact to what is required; freedom from mistakes, this exemption arises from carefulness; exact conformity to truth, or to a model or rule; precision; exactness; nicety; correctness; as, the value of testimony depends on its accuracy.

Dealing with e-Government in a comprehensive view is a big challenge and quite a complex task Upadhyaya et al (2009). He explains the three model layers of security that are readily available to address issues of compress system as;;

- Application layer security
- Network layer security
- Data security

The issues that are to be managed in Application layer are authentication, data integrity, trust, and user anonymity and security dependences. He continues to explain that TCP/IP in the network layer security can be secured by cryptographic method and protocols that have been made to secure communication channels. Since government data or information may contain secrets, personal data about staff, suppliers, clients, or even the organization's financial records, information/data security measures must be implemented to safeguard them.

He further explains that Data security means protecting a database from destructive forces and the unwanted actions of unauthorized users. This mechanism incorporates measures like Back up early and often, Use file-level and share-level security, Password-protect documents, Use EFS encryption, Use disk encryption, make use of a public key infrastructure, Hide data with steganography, Protect data in transit with IP security, Secure wireless transmissions and user rights management to retain control.

2.2. Vulnerabilities on government network infrastructure

According to Mbowe et al.., (2014), technology advancement has led to data or information becoming more valuable thereby making organizations have a lot of challenges in safeguarding it from attackers whether inside or outside the organization. The advancement in technology have brought new tools used by attackers to penetrate networks or even any repository of data or information.

Pfleeger C.P and Pfleeger S.L. (2003) state that vulnerability is a software or hardware defect or weakness in securing a system which may lead to unauthorized entry by a malicious user or attacker thereby causing loss of data or information.

According to Curry et al., (2011), prior to a hacker getting unauthorized access to an organization data or information, security of the institution is very important for those managing the network to determine the network's security threats and vulnerabilities. Since there are many challenges arising from this, it is very necessary for the institutions to adequately invest in measures that will safeguard the security of their information within their network infrastructure.

The importance of secure networks will continue to be of very importance to anyone designing ,implementing or managing a network infrastructure. Securing of the network includes security of data and information and also security of the infrastructure on which there can be theft, tampering of devices hence the disruption of information and services is kept to the minimum, Kuhn et al., (2005).A secure local area network is one that has acceptable integrity, confidentiality and is available to the intended users. In case a hacker wants log into a system or network as sometimes the case is, sometimes there is nothing one

can do to stop it since they have advanced tools in their hands but what can be done is to reduce all areas by making it harder for the intruder to breach the system's security.

Some of the various vulnerabilities on network infrastructures are;

- Easy access to information

  This can be attributed by having data/information that is not secured and any user can access and modify the data /information

- poor network designs.

  Having networks that are not hardened to counter external attack or even internal attack can lead to loss , unavailability or even disclosure of that information

- Poor firewall deployment.

  If firewall fails to counter what is designed to do, it may lead to spending a lot of resources without achieving security objective

- Insecure/exposed Ports.

  Good ports configuration dictates one to disable all ports then open those that are to be used for a specific reason. But if not implanted well, it can allow attackers inside systems thereby making the data, resource or the information insecure

- Indiscriminate enabling of services.

  If some services in a system are not required, the rule don't run. Attacks can use specific services, which open some port thereby endangering data or information to loss.

- Improper system configuration.

  Any system/ device must be well coded or configured to ensure no faults are left which can increase threats to a system.

- Poor intrusion detection system (IDS) setups.

All IDS must be well configured and alarms should be well set to ensure system/network are safeguarded.

- Disgruntled employees.

Not all employees are satisfied in what they undertake hence it's very imperative to implement even basic mechanisms to ensure security of data. Authentication of users is a good tool ensure auditing of whoever did access a system.

- Lack of efficient physical security

Use of biometric to access resource location improve the security of information held there. Some organizations deploy CCTVs or even watchmen to ensure security of premises holding vital information thereby increasing security of the data.

- Corporate Espionage.
- Indiscriminate enabling of services.
- Weak password implementation

System require strong passwords which make it hard for any attacker or software to crack it. Strong hashing should be implemented and any encryptions tools should be implemented make systems more secure

- Poor anti-virus implementation.

Not all antivirus software are secure. Some can't identify the various malwares, spywares released each and every day on the internet. Other systems don't have any antivirus thereby increasing the chances of data/information loss.

2.3. State of practice in Government data Security

Information and technology can help manage the risks facing government agencies. It is imperative for government organizations and agencies to strengthen privacy protection and security programs through the implementation of policy and improvement of technology (Lin, 2013). He further explains how system should be secured with Public Key Infrastructure (PKI) for both data encryption and digital certification.

The security breaches of confidential data or information have continued to be hard to solve due to increased spyware and malware programs and also due to unauthorized access to information or any data kept within network infrastructure Mbowe et al..,(2014).

According to Davies (2002) different sources of data or information insecurity need to be considered whenever designing new networks. This enable one to put up to data mitigation techniques to safeguard the security of the information or the data. Some of these sources are; Message hijacking by unauthorized people, transmission disruption which can be caused by attacks like DDoS and DoS and also rerouting of data or information to fake or non-existing network devices or systems.

For protection of malicious applications, many organizations be it public or private use anti-viruses to detect, identify and even remove a known virus or a malicious code. Antivirus are cost effective depending with financial repercussions. Some are cheap, others free and other free and available from the internet.

Physical security is a key issue to safeguard data and information. Government and even private organizations are employing armed personnel to their premises to safeguard access of

premises by the right people. This may deter those with intentions of accessing a premise and tamper with the information. Use of closed circuit cameras (CCTV) is also detrimental in securing premises housing data.

2.4. Technological Advancement in Government data security

The confidentiality, the availability and integrity of data/information is at risk from being accessed by unauthorized users, hacker/sniffers listening in on the network, and also internal users giving away the access keys to the information / data store. With emergence of new technologies organizations continue adopting the best and readily available technologies (Denning Denning, 2009). This has continued to ensure government is up to date with new technologies.

Some of the technologies are;

2.4.1. Firewalls

According to (Zwicky et al, 2000) A firewall is given as a "device/software or set of components that restricts access between a secured network and the Internet, or between different networks." Public and private organizations use the firewalls to regulate the flow of data and information between different networks. They restrict the movement of network traffic and also act as a route that performs further processing on the traffic beyond simple choking restrictions.

A firewall is a device or a system that is used to regulate flow of data/information traffic between different interconnected networks by using different security rules, Sachin et al (2012). The traffic flow is regulated or controlled by a policy created on the firewall. The filtering of the traffic flow by the firewall policy is implemented by network administrator. There may be more

than one rule within a firewall to filter different network traffic. The network packet, arriving on the firewall are checked against the set firewall rules policy. Depending on the packet, and the type of policy they are allowed or discarded or denied the access to the network. Network Packet filtering on the firewall allows one to explicitly restrict or allow packets by port number, network IP address, or both IP address and port number. An example is one restricting all packets headed to port 80 which is (WWW) on all computers on the local area network except computer 1 and 2 .

Firewall protect internal network from external network. Firewall follows some of the following parameters;

- Service control

To ensure firewall works accordingly, it control services which are running in the system and passing through the firewall

- Direction control

Firewall are used to control direction of traffic as set in its configurations

- User control

Authentication can also be configured in the firewall allowing different users to access the only set resources

- Behavior control

User behavior together with how they access a system can be set within a firewall. Users can be given full or partial rights to a system or a resource through the firewall.

2.4.2. Public Key Infrastructure (PKI)

The main role of PKI as a countermeasure is to defend against any attacks and compromise.

Whether it be included into an authentication system or even part of a code signing system, the main goal is to ensure there is Integrity (NIST,2004). Additionally, PKI can serve in a capacity of ensuring that Confidentiality of data through trusted and recognized encryption mechanisms that leverage trusted encryption materials.

According to Clarke (2004), a Public Key Infrastructure is "an arrangement, usually carried out by software at a central location together with other coordinated software at distributed locations, which provides for third party (often termed a trusted third party) vetting of and vouching for user identities and for binding of public keys to users (typically in certificates) and vice versa."

One of the most common PKI being used today is Secure socket layer (SSL) which is being used through the internet in securing web browsers especially web browsers which are transactional or have private information being exchanged. Companies like VeriSign provide the facilities through the internet for organizations to secure their information using the SSL certificates. PKI can also be implemented within organizations internally to secure internal communication also to provide encryption service to the data/ information and the systems, digital code signing, allow users to digitally sign their communication and also secure identity of the users. Use of PKI have been limited due to its associated cost and also the complex involved during the deployment. Most deployments revolve around SSL in the internet but recently PKI has started to evolve such that those big companies have initiated process of deploying the PKI e.g. AOL has implemented PKI and use it to generate SSL certificates.

2.4.3. Intrusion Prevention Systems (IPS)

According to Desai (2003), Intrusion Detection System (IPS) is any device either software or hardware that is implemented to detect any attack which is known or unknown and mitigate the attack to safeguard data and information. Intrusion Prevention system (IPS) combine the use of intrusion detection system capability on data inspection with the blocking technology which is used by the firewalls. The capability to block is also referred also as active response and allow implementation of a policy to detect any violation which is again translated in time to a policy based action for stopping or impeding a violation.

IPS has a number of variations but most common are the inline network based systems. Also there are those IPS that have Denial of Service (DoS) and Distributed Denial of Service (DDoS) detection and mitigation variations. Their detection is based on awareness of the traffic on the application layer of the Open System Interconnect (OSI) Model. Firewalls which are host based are usually integrated with IDS detection capabilities to ensure application based specific response on an implemented policy instead of using signature set.

The different IPS variations have some things in common. These are; they generate alert based on policy or signature and also they initiate a response the way it's programmed in the system. Alerts occur as a result of signature matching or security policy setup for an application being violated. The response vary from either blocking the traffic , chocking flow the affected traffic to even terminating the traffic.

The limitations to IPS include;

- Accurate detection

If traffic is not well analyzed and incorrect response initiated as a violation to the set policy, known and required traffic may be terminated or blocked resulting to a negative impact within an organization

- Ability to scan full throughput of a LAN
- Ability to generate accurate response and in time
- IPS must be able to select right responses based on set policy and also ensure it is able to issue alert while the offense is still in progress

2.4.4. Event Correlation Systems (ECS)

Event correlation systems improves the successes of IDS since it provide more superior mechanisms for managing, aggregating and Correlating IDS events which are generated through policy violations or signature detections.

ECS pulls together logs found in IDS and allow aggregation of the log data from different sources which include firewalls, applications and even hosts.

2.4.5. Virtual Private Networks (VPN)

According to (Moskowitz, 2004) Virtual Private Network (VPN) is a private intercommunications network that uses public networks, for communication between different public or private organizations. The VPN is often seen as a low cost solution for deploying a secure private network than use of private leased-lines. They are used to protect and safeguard the integrity of communications and also safeguard the confidentiality during the transmission of data and information while utilizing encryption.

VPN can also be defined as combination of both software and hardware devices to provide users with transmission of data and information through unsecured network by establishing a

secure private network within the unsecured network. e.g. creating a private network on shared networks like the internet, Lo (2010). VPN provide institutions an easy, inexpensive and most secure way of sending and receiving data across the world. Due to this Government institutions and their clients can communicate securely on a cost effective transmission

VPN is classified to three architectures;

- Site to site intranet VPN

  This is where a number of LAN in the different geographical locations in the same institution are connected using VPN

- Remote Access VPN

  This is where a single network device, either a laptop or computer is connected to the organization network using a telephone or a modem.it mostly used by law enforcers to access their system remotely. The VPN solution deployed ensure security of the information by authentication, data encryption and even digital signature of information.

- Extranet VPN

  This type of VPN is where resources of one government department are opened for access to another. The access spans a number of domains and different types of resources for different agencies.

2.4.6. Virtual local Area Network

Pal and Pal (2013) define a virtual local area network as a logical grouping of network hosts and resources which are defined administratively on a switch port. VLAN break up broadcast domains in a switched internetwork. VLANs within a Local area network help create small broadcast domains within the layer 2 of the OSI reference model. This is done through assigning

switch ports to different sub networks. Frames broadcasted within a VLAN are logically grouped within that VLAN only

Membership of a given VLAN can be based on

- Port numbers
- MAC addresses
- IP Addresses
- IP Multicast addresses
- Or combination of all features

VLANs are also used as an extra measure of security, used to reduce network traffic and are easy and cost effective to implement

VLAN are grouped into two types;

- Static VLAN

  These are type of VLANs created and updated by a network administrator. Switch ports are mapped to a VLAN and one can only re assign the port manually. It is considered to be more secure. This kind of VLAN is considered easy design and configure.

- Dynamic VLAN

  This is where VLANs are automatically assigned based either on MAC address, protocols and applications

A switch can have more than one VLAN but a switch port can only belong to one VLAN. Pal and Pal (2013) explains that a switch port can only be in all VLANs if it is a trunk port but one vlan if it's an access port.

In a switched network there are two types of links. These are;

- Access port

Belong to only one VLAN and carries traffic for its only VLAN. Any type of network device attached to access link is not aware of VLAN membership since it just assume its same broadcast domain. access link devices don't communicate with other devices which are outside their vlan unless they are routed

Some switches allow addition of an extra vlan on top of the access port for voice traffic. This vlan is called a voice VLAN which is only allowed to run on top of data vlan hence allowing the two types of traffic to run concurrently.

- Trunk port

  This type of ports can carry more than one VLAN at a time. It give 100/1000mbps point to point connection between two switches or between switch and a router or between switch and server. A trunk port carries traffic of between 1-4094 VLANs at a time.

VLAN identification ensure that the switches and routers keep a record/track of how packet frames are being transmitted. There are two types of trunking methods;

- Inter switch Link (ISL)

  This is where vlan information is tagged on Ethernet frame. This ensure VLAN are multiplexed through the trunk by using ISL encapsulation method. This form of encapsulation is done on layer 2 and encapsulate data frame with a new header and cyclic redundancy check.

- IEEE 801.1q

  This is a method of encapsulation which was created by IEEE for frame tagging. This technology insert a field to identify a VLAN and it the best to be used between different models of network devices.

2.4.7. Intrusion Detection and Analysis System

The concept of intrusion detection has been around since 1980 (Innella, 2004). Intrusion detection is designed to detect misuse or abuse of network or system resources and report that occurrence. The security industry has greatly expanded intrusion detection over the past years to incorporate several advanced concepts. Beyond basic detection and alerting, most systems today bill themselves as having "intrusion prevention" capabilities; otherwise known as active response. The concept of intrusion prevention is that an activity can be detected reliably and then stopped, either at the host or network level, by the detecting system.

2.4.8. Anomaly Detection Systems (ADS)

This is similar to intrusion Detection System (IDS), Chung (2004). It's a key element in intrusion detection and other various detection elements and part of it behavior is to detect presence of intentional or unintentional attacks, defects or faults in a system. The detection is based on rules and predictability of the logged data availed from the multiple sources. When the rules are applied on the predictability of the logs, it generate the best rule to whether it's a an attack, misuse or abuse which is occurring.

ADS calculate it rules from the aggregate logged data and evaluate whether it current performance deviates from the expected level.

According to Jyothsna and Prasad (2011), The main advantage of ADS over signature based detections is that a simple attack which does not exist in signature based detection can be detected in case it fall out of normal traffic pattern.

This is most identified whenever they ADS detect a new worm. The moment it's infected with a worm, it scans looking for any vulnerability within the system at faster rate thereby filling the LAN with malicious traffic causing traffic abnormality

2.4.9. Vulnerability Scanning Systems

According to Cook (2004) Vulnerability scanning is the "automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened." The vulnerability scanning mostly relies on a number of tools that can identify users/hosts and continue applying the test on them for any known vulnerability. The processes of automated scanning include three levels which are;

- Authority to scan
- Determine scope of program
- Establish security baseline depending on the number of vulnerabilities of the host scanned.

Vulnerability scanning program safeguards and secures the scan results and have a plan and a process in store instead of a remediation of the found vulnerabilities. It is recommended that vulnerability scanning be done at a risk management process but not as a standalone security measure. vulnerability scanning is a useful measure and a cheap way since some of the tools are readily available as open sources. Regular vulnerability canning provides more information on all the risk areas within the available technologies in an organization.

It's very important especially for those resources having access the internet to ensure the security of the devices before deployment

2.4.10. Access control management (ACM)

According to Rotchke (2004) access control management system enforce use of identification, authentication and authorization to safeguard access to data/information in a system. Users of the system are limited to what he or she can do to the resource by restricting the type of access (either write, modify, read, execute, etc.). standard access control management gives a user an interface to self-identify then provide a mechanism for the system to challenge and confirm the identity of the user and again it must provide a way of giving the correct rights to access the resource as per the user.

Access control management have the following security models;

- Discretionary access control (DAC)

  Under this security model, the resource owner directly manage the access controls

- Mandatory access control (MAC)

  Under this model it is the system that gives and assigns the level of access to a resource

- Role based access control (RBAC)

  Unser this model, access to a resource is given depending on the rights of a group or user within the system

ACM system gives the foundation for data and information security in organizations. One of the primary functions of ACM is to categorize data or information systems according to the assigned values and provide protective mechanisms depending with the values of a given type of resource. Rights are given to users or system objects and which are again provided with way of authorizing the access to the said resources Tripton and Krause (2000). Depending on the magnitude of implemented systems, ACM vary in prices. Also the type of the secucity model implemented also determine how expensive ACM can be. It advised to

implement the ACM before all other safeguards on data and information security since its main aim is to control who and what one accesses in a system.

2.5. The Open System Interconnected Model (OSI)

The International Standard Organization (ISO) derived an international framework on standard communication for heterogeneous systems or infrastructure in a network.

As a standard of transmission system in open world, this system is referred to as Open System Interconnection Model (OSI). The OSI standard model provides a system to filter complex inter-networks into small components or technologies that can be understood easily while being used.

The main aim of the Open Standard interconnect (OSI) is to ensure all network nodes or devices all over the world communicate with other, as long as they all use the OSI standards model, Stallings (2003). The OSI reference model is categorized to seven levels where each and every level in OSI Model works according to its functionality. The levels communicate to each other since they have a communication functionality properly sequenced between them. The functionality of each OSI layer is different from each. Each OSI layer has different level and labels.

The OSI Layers are;

- Application layer

  This is the last layer of the OSI model. It is used to organize all the systems level applications .e.g. FTP

- Presentation layer

This is the sixth layer of the OSI model and it is responsible for the transmission and receiving of data and information in the mode of graphic.it undertakes the compression and decompression of the data during the encryption process.

- Session layer

  This is the fifth layer of the OSI model and it manages the end and start sessions between the end user applications. It is mostly used in TV, video conferencing and VOIP where user first establish multiple sessions with receiver prior to sending of the data.

- Transport layer

  This is the fourth layer of the OSI reference model and it involves transport control protocol (TCP) which is a connection type protocol, and user datagram protocol (UDP) which is a connectionless type of protocol.

- Network layer

  This is the third layer in OSI model and is responsible in making logical transmissions/ connection between the source and the destination. The type of data in the layer is usually in the form of network packets. The network layer protocol offer two services; connection mode where its either connectionless communication or connection oriented communication, and IP addressing where every network node has a unique identifiers which ensure the send and receive make the right connections.

- Data link layer

  This is the second layer in the OSI model and ensure control methods to ensure proper data format and can also access data flow error in the physical layer. The data format in this layer is called frames.

- Physical layer

This is the first layer or the lowest layer in the OSI model. It ensures the connectivity between the physical mediums and the system interface cards. The layer transform electrical signals to bits forms

According to Stalling (2003), there are three level of abstraction in the system architecture of the OSI model. These are;

- The OSI architecture

  This the combination of OSI service specification and the OSI protocol specification

- The OSI service specifications

  They ensure communication between user and system in each and every layer

- The OSI protocol specification

  They ensure the type of protocol to be used and running on a specific communication service

2.6. Critic of literature problems

According to Selil (2010) there is a lot of talk in the federal government about how hard/expensive it is to have good information security. That narrative is also part of the cyber warfare discussion currently seeking rampant funding. When the politics are used to finds a ways of building kingdoms the actual solutions are sometimes hidden by the blatant profiteering. Solving the information security problem is fairly inexpensive but the solutions take some thinking.

Data and information access and sharing involve their movement from one point to another (Brown and Magill (1994).). During data transmission, threats are likely to be experienced causing the data and/or information to be vulnerable to unauthorized people. This theory

highlights potential security breaches that may hinder data and information when being shared or accessed by different categories of people, hence, use of different networks need to be deployed to ensure access of resources is by the right people.

Tripton and Krause (2000). Advise organization to implement the ACM before all other safeguards on data and information security since its main aim is to control who and what one accesses in a system. This technology is easy to implement but cost of the technology leads to organization going for other security models readily available and less costly.

2.7. CHAPTER'S SUMMARY

This chapter presented the theories from which this project is based and critical concepts relating to this study.

CHAPTER THREE

PROJECT PLANNING AND METHODOLOGY

3. INTRODUCTION

This chapter describes the methodologies and the techniques that are available for research. Various methodologies will be identified and discussed and then all the methodologies will be evaluated to select the best method to be used for this project.

3.1. Research Methodologies

Researches can be classified according to their purpose or function "to understand how the nature of the problem influences the choice of research method" (Zikmund, 2000). Every researcher has his/her own motivation to perform a scientific study with an aim of find a result to solve the intended purpose. According to Yin (2003), McNabb (2008) the research purpose can be grouped in three categories; exploratory research, descriptive research and explanatory (or casual) research. In each of the above mentioned approach one or more of a variety of statistical tools are used during the test of ideas or concepts and to communicate research findings.

3.1.1. Exploratory Research

According to Saunders et al, (2000), exploratory research is used to clarify an understanding of a problem. The goal is to explore something and is appropriate for when the research problem is difficult to delimit. Yin 2003, Saunders et al, (2000) and McNabb (2008) explains that exploratory approach should be applied when the researcher is not sure about the correct model to use and the kind of relations and characteristics that are more suitable. It is very

helpful to analyze “the general nature of the problem, the possible decision alternatives, and relevant variables that need to be considered” (Aaker et al., 2004, p.75). The main goal of exploratory research is to provide background information, “the production of inductively derived generalizations about the group, process, activity, or situation under study” (Given, 2008, p.327). He further explained that exploratory studies are variable ways of researching “What is happening; to seek new insights; to ask questions and to assess phenomenon in a new light”. So an explorative research is suitable when a problem is difficult to demarcate and when you have not gotten a clear apprehension about what model to use and which characteristics and relation are important

3.1.2. Descriptive research

McNabb (2008) explains that the object of descriptive research is to provide a description of diverse phenomenon’s connected to individuals. It focuses on the accurate description of the variable in the problem model. It gives a description of an event or defines a set of attitudes, opinions, or behaviors that are observed or measured at a specified time and environment. Descriptive research in contrast to exploratory research, stem from substantial knowledge of variables in question and for this type of research to be productive questions should be designed to secure specific kinds of information related. Cross-Sectional Study and Longitudinal Study are the main types of descriptive study.

3.1.3. Causal research (Explanatory)

The research is said to be explanatory when the focus is on because effect relationships explain what causes produced what effect according to (Yin 2003). The explanatory research seeks to find cause and effects relationship between variables. It accomplishes this through

laboratory and field experiment. This research help in developing a theory that could be used to explained the empirical generalization that is developed in the descriptive stage according to Roynolds (1971).

In the field of Information System (IS) a variety of research methodologies has been explored by researchers, each being appropriate for different aspects of research study depending on the domain and the philosophical position of the researchers. Nunamaker et al. (1990-91) see systems development as a research methodology that fits comfortably into the category of applied science, which belong to the engineering, development and formulative types of research.

3.1.4. System Development (SD)

According to (Nunemaker et al,.1991),objectives of IS research clearly demonstrates the legitimacy of and necessity of system development as a research methodology.
IS research leads to the development of a prototype system with the intention of illustrating the theoretical framework. In some more organization or society-oriented studies the role of such a system can be played by an existing piece of technology or the process of technology transfer. systems development becomes a natural intermediate step linking basic and applied research. Nunamaker et al. (1990-91) continue to prove that systems development represents a central part of a multi-methodological IS research cycle (see Figure 1).

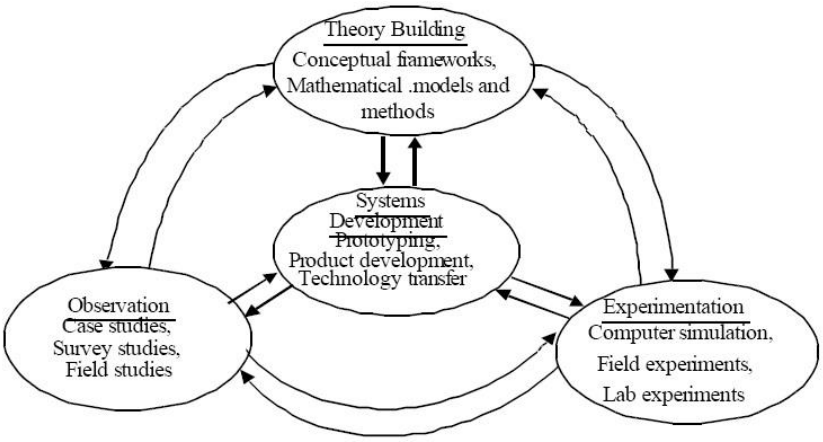


Figure 1: A multimethodological approach to IS Research (adapted from Nunamaker et al. 1990-91, p.94).

Figure 1: Multimethodological Approach to IS Research

According to Nunamaker et al. (1990-91), the principle parts of a system development life cycles are;

- Construct a conceptual framework
- Develop a system architecture
- Analyze and design the system
- Build the system
- Experiment, observe and evaluate the system

The principle parts can be represents as a hierarchy of identifiable “super -methodologies” as shown below;

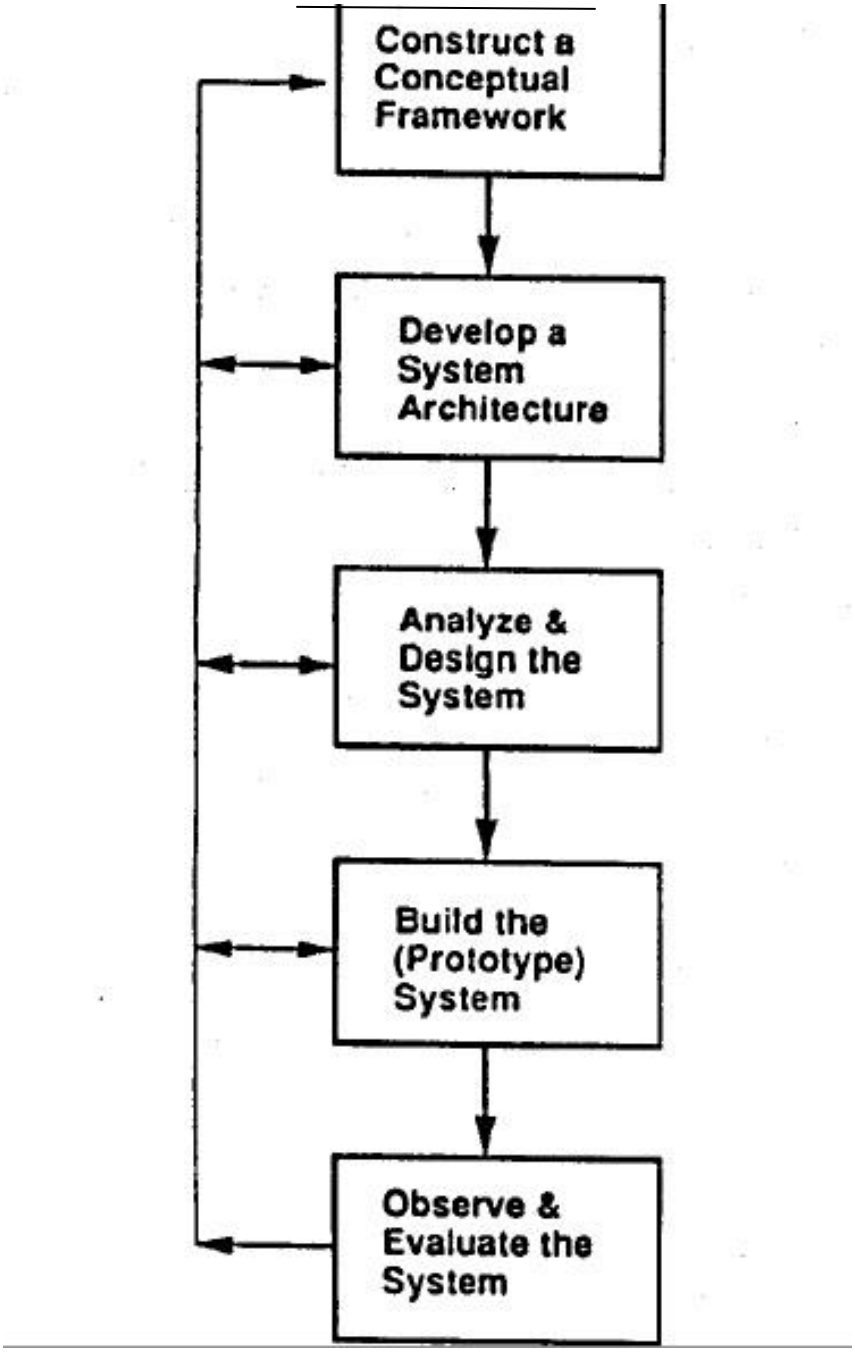


Figure 2: Process of System Development Life Cycle (Adapted from Nanumaker et al 1990-91 pg. 98)

Miles and Huberman (1994) proposed some criterion to be used for evaluation of the best methodology to use. The criteria are;

- Significance: The study must be significant, either theoretically, practically, or both. Yin (1994 p.147) when discussing case studies says that "the individual case or cases are unusual and of general public interest. The following query was used in this criteria" Does the study have practical significance? Will it contribute to the building of "better" systems?".
- External validity: Cook and Campbell (1979 p. 39) define the external validity as " approximate validity with which conclusions are drawn about the generalizability of a casual relationship to and across populations or persons, settings, and times. The following query was used in this criteria " Are the methods, processes and outcomes described in conclusions generic enough to be applicable in other settings?".

Since the objectives of the project are to investigate the Local Area Network and then design VLAN,, the following comparison proposes the best methodology to use using the above criterion;

Table 1: evaluation of the methodologies

Attribute	**Methodologies**			
	Exploratory Research	**Descriptive research**	**Causal research (Explanatory**	**System Development**
Significance	There will be only explanations with reports.	There will be only explanations without any testing	There will be only explanations without any testing	The project is of significant and will make the contribution for a better network
External validity	Can't be applied to other settings	Can't be applied to other settings	Can't be applied to other settings	Since it will be tested and implemented, it can be implemented in other settings

3.1.5. Proposed methodology

As seen from the table 4, System development methodology is the best suited for this project since the methodology will be tested, simulated and implemented.

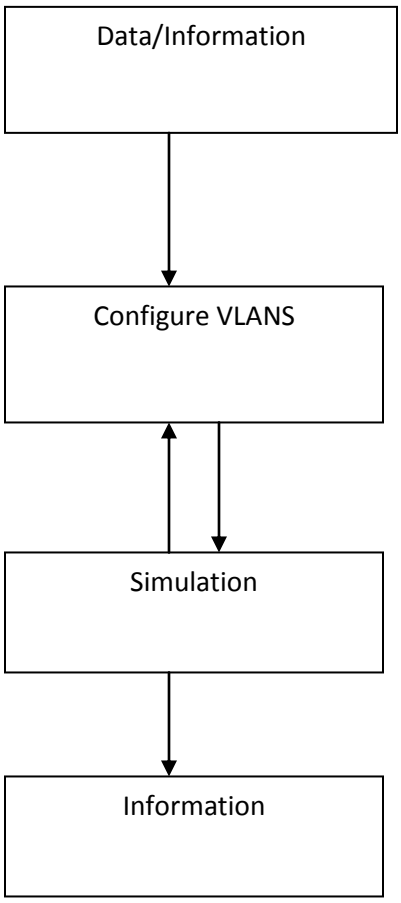
CHAPTER FOUR

4. CONCEPTUAL MODELLING AND FIELD STUDIES

4.1. Introduction

This chapter describes the status of The National Treasury Local Area Network (LAN). It explains the various devices used in the network and how the network is logically segmented. Different users of different departments share the network and users are not grouped per departments but are housed in any of the floors . Using the System development approach according to (Nunemaker et al,.1991), the National Treasury Network will be analyzed, tested and implemented using Cisco Packet Tracer as the simulation tool.

4.2. Conceptual Model



4.3. Survey and planning stage

A key important stage of project development is survey and planning stage. Always a well-planned project ensures the objective of a project is attained completely. A well planned project always makes sure everything run smoothly. During the planning phase, all issues are considered hence time is very important to ensure one leaves room for unforeseeable event and this makes the process easier. Project planning involves the following steps: Evaluate current state, evaluate the future of the project and also ensure one completes the gap in between. However, there are many steps involved during an IT project development.

During the project research/survey one should be concerned on the objective of the project, aim of having the project and also the scope of the project. They should all be clear and ensure they all meet the user requirements.

4.4. Project requirements

The high level projects requirements are project facilities, software requirements and hardware requirements.

4.4.1. Project facilities

These are the equipment and required infrastructure to be used by the project. For this research, a laptop was required which would be installed with the required software and simulation tool.

4.4.2. Software requirements

These are software or programs required either by the equipment being used in the project or even any program or software being run on user end devices or and testing and simulation software.

The software requirements for the project are as tabulated below;

Table 2: software requirements

Software requirement	**Type/category**
Cisco packet tracer	Free ware
Windows family	Buy
Ping utility	Free ware
telnet utility	Free ware

4.4.3. Hardware requirements

The following are the hardware requirements for the proposed LAN;

Table 3: hardware requirements

Item	**Requirement**
Router	As for simulation purposes to use the high end router provided by Cisco packet tracer
Switch	As for simulation purposes to use the high end switch provided by Cisco packet tracer
Laptops	As for simulation purposes to use the high end laptop provided by Cisco packet tracer
Desktops	As for simulation purposes to use the high end desktop provided by Cisco packet tracer
Cables	As for simulation purposes to use the high end cables provided by Cisco packet tracer

Wireless devices	As for simulation purposes to use the high end wireless devices provided by Cisco packet tracer
Servers	As for simulation purposes to use the high end server provided by Cisco packet tracer
Connections	As for simulation purposes to use the high end cables provided by Cisco packet tracer as per the required type of cable required for each type of connection

4.5. Simulation Tool (Cisco Packet Tracer)

Cisco Packet tracer is a network simulation tool provided by CISCO Systems to student and administrators to experiment. It can be used for simulation purposes, visualization purposes and even collaboration capabilities. It helps to understand any complex network technology concepts.

It can also be used to design and simulate any network by interconnecting various networking equipment and also one can run the various network tests to ensure the connectivity and communication between different networking devices is as per the set requirements.

Various protocols e.g. Telnet, secure socket later (SSL), ftp e.tc can be used and run on the Cisco packet tracer simulation tool.

This tool is provided by CISCO through either being a student, Cisco professional or a Cisco trainer. It is downloaded from the Cisco study guide. One has to be conversant with its use because some commands are proprietary. For this research, Cisco Packet tracer version 5.3.0088

will be used. The tool will be installed in a window operating system family with Basic requirements.

For this research, ping utility which uses Internet Control Message protocol (ICMP) will be used. This will be used to provide echo request with timestamps and receive echo reply also with timestamps.

Cisco packet tracer allow the use of ICMP protocol by dragging “add simple PDU” on the sending device and taping on the destination host and will give automatic results on the right hand side corner. Another way is by using ping command on the host by opening the command prompt and practically timing the ping commands to the ip address of the destination. This is a bit cumbersome noting that one has to know the ip addresses of the sender and the destination hosts. Results of a ping are immediately displayed on the result panel on the right hand side of the packet tracer.

If the result area is completely filled with simulation results, one can erase those results by using the delete button on the results to be deleted.

Connection of the devices can be noted with the green signals on the packet tracer, where the green color indicates there is a good connection between the devices but amber signifies either the wrong cable or bad configurations hence the devices can’t exchange information

4.6. Existing Network

System development approach which is most commonly used approach in network implementation will be used to design and simulate the National Treasury LAN with the current

VLAN enhancements. The approach will be used to analyses the network diagram based on modeling where modeling is the act of drawing one or more graphical representation.

This technique will be used since the new logical presentation of National Treasury Network diagram will help figure out and analyze problems, define all requirements and design the new network with VLAN enhancements.

The National treasury has the following departments; Administration. Accounts, Human Resource Management (HRM), human resource Development (HRD), Supply chain Management (SCM), Information Communication Technology (ICT), Planning and Monitoring, external audit, Finance, Internal Audit, Debt Management, Budget, External resources, Integrated Financial management Information System (IFMIS) and Macroeconomic. Some of these departments run specific Applications or systems to be accessed by only those departments. Examples of these Systems are; Integrated Personnel Payroll database (IPPD) which is run by the HRM department, Integrated Financial management Information system (IFMIS) which is run by the IFMIS and accessed by specific users in all other departments, Government Payment Services (G-PAY) run by accounts, Email System, Web service, Domain name service e.t.c.

The National treasury has an existing network which is in a star topology. The network is sub netted to 14 VLANS which are represented per floor. The staff are distributed across the floors where by some staff on one department are distributed across different floors. This has led to some users have to walk to floor whereby they specific certain systems are located since the VLANs are designed in such a way one cannot access any resource in a different VLAN. E.g. Accounts staff are located in 2nd and 3rd floor which are represented by VLAN 3 and 4

respectively. The following is the current logical LAN setup for the ground to 3rd floor (Sketch using Packet tracer

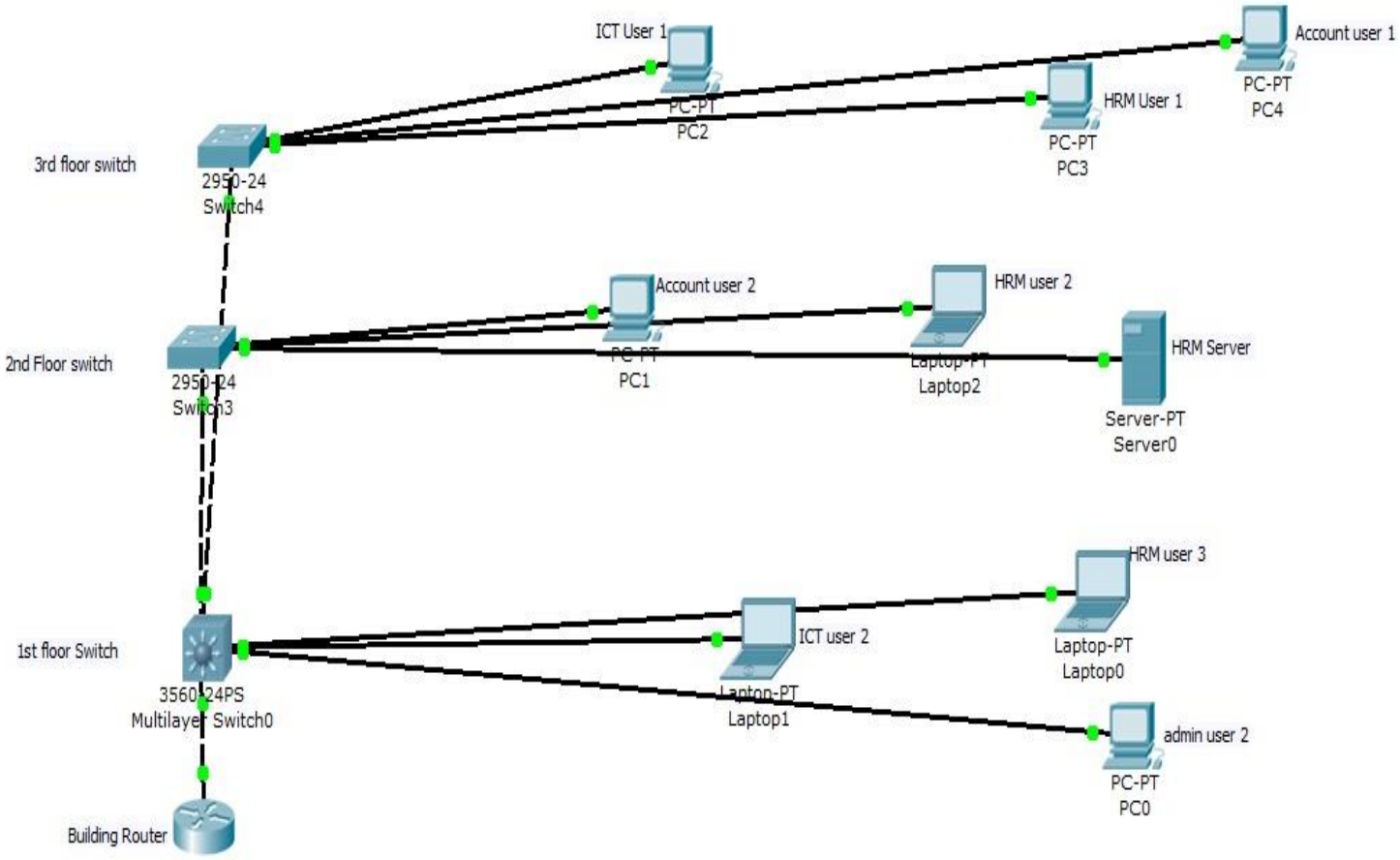


Figure 3: Current Logical LAN setup for Ground to 3rd floor

4.7. LAN Topology

As shown from the logical LAN setup of the Treasury Building, it can be seen that the LAN is in Star topology since each and every host/user connects to the floor switch. Communication from one user to another has to pass through the floor switch.

The Network is a class A network with IP 10.118.0.0 and subnet 255.255.255.0. The first floor network is 10.118.1.x where x is any number between 1 to 254. Second floor network is

10.118.2.x and third floor network is 10.118.3.x. (x is any number between 1 to 254).The gateway for VLAN 2 is 10.118.1.254, VLAN 3 is 10.118.2.254 and VLAN 4 is 10.118.3.254.

4.8. Configuration of Routers, Switches and Hosts

4.8.1. Naming of the network devices (Router and switches)

To ensure all the network devices i.e. routers and switches had to be given right names for the purpose of identification. Since switches were distributed on all the floors, the name of the switches was given as SWTCH MODEL-FLOOR NUMBER-NAME OF FLOOR WING-S NUMBER (Where S means switch).example; The switch model on first floor on northern wing is Cisco 3750. The hostname configuration is 3750-01-N-S1 on the configuration setup of the switch.

4.8.2. Router configuration:

Security of data, information and even the network is a vital component in an organization, Akin (2002). Access control list can be deployed in a router to provide for the security of any resource within the network. Cisco IOS enables network administrators to implement security for the network using the Access control list (ACL). The feature of using ACL prevents some network packets from passing through the network to a destined network or host.

Access control list has the following benefits;

- Prevents traffic which is unwanted to access the LAN
- Its used to block users or host from accessing some systems or devices
- It can block some devices or host from existing in the LAN

In the case of The National Treasury network, it has one Router (CISCO 6506) where Sub interfaces for each VLAN are created and this limits each VLAN to a specific IP Address as per the floor VLAN. Access control List is implemented to ensure communication to other networks is filtered and blocked as per the network administrator configuration.

The configuration is as shown in the appendix.

4.8.3. Switch configuration:

According to Shaffi and Obaidy (2012), Virtual local Area networks (VLAN) enable network administrators and network engineers to create logical LANs from physical LAN. This is a type of technology that is used to subdivide complex networks to smaller networks so that they can be managed well, they can also be secured in an understandable manner and to improve performance of the network. VLAN logically subdivide the switch to segments based on an institution function like geographical location or even the organization unit like a department.

VLANs in any network have some of the following benefits;

- it is easy to relocate a host within the VLAN
- It becomes easier to make changes on the LAN configurations
- Network traffic between the VLANs is easily controlled
- Its becomes easily to safeguard and improve the security of data, information and resources within a VLAN

In the case of the National Treasury physical network, each floor is served by at least two Cisco 3750 switches depending on the number of network ports per floor. The setup need for this device is to create VLAN as per the floor. All switch ports are assigned to the floor VLAN. Each switch has a trunk configured on it giganet port to the first floor switch which is the Core switch

for the network and all trunk ports of the switches terminate on the modular ports of the Cisco 4506 core switch. From the network, fiber cable is used as the backbone to connect to the core switch. The network is designed to provide 1000mbps backbone speed. For security of the switches passwords are enabled to ensure one has to log in the device. The configurations are as shown in the appendix.

4.8.4. Hosts Configuration:

Each host has a network Interface card (NIC) connected to the floor switch with Untwisted pair of category 6 cable. The NIC cards gives 10/100 mbps speed to the host. Each host is assigned an IP Address, Subnet mask and gateway as per the VLAN the host is attached to. The IP Addresses are manually assigned to the hosts.

4.9. Testing by simulation

The following are list of IP Addresses on the identified hosts (users) and Resources for use during the simulation;

Table 4: Assigned IP Addresses

User	**Department**	**IP Address**	**VLAN No.**
ICT USER 1	ICT	10.118.3.1	4
HRM USER 1	HRM	10.118.3.2	4
ACCOUNT USER 1	Account	10.118.3.3	4
HRM USER 2	HRM	10.118.2.1	3
ACCOUNT USER 2	ACCOUNT	10.118.2.2	3

HRM SERVER	HRM	10.118.2.3	3
ICT USER 2	ICT	10.118.1.1	2
HRM USER 3	HRM	10.118.1.2	2
ADMIN USER 1	ADMIN	10.118.1.3	2

4.9.1. Simulation analysis

After successfully logically simulating the network setup on the Cisco packet tracer and running the tests using ping utility, it was found that, users can access resources in their floor (VLAN) but cannot access resources in the other floors or VLANs. This was a problem since users in the same department e.g. Account or HRM are unable to access resources in the other VLANs.

This can be explained through the following test results from Cisco Packet Tracer;

Table 5: Host to Host Testing

HOST TO HOST TESTING	
Test Name	Host to host
Test Target	To test communication between hosts in VLAN 4 (3rd Floor)
Source IP Address	10.118.3.2
Destination IP Address	10.118.3.3
Technique	Send packets from packet tracer
Expected Result	Pass
Actual Result	Successful. There is communication between hosts in VLAN 4

From the results, it can be explained that all host within same VLAN can communicate. i.e. ICT, HRM and Account users can communicate since they are on same VLAN.

To test communication between VLANs, the following simulation was done using Cisco Packet Tracer;

Table 6: VLAN to VLAN testing

VLAN to VLAN TESTING	
Test Target	To test communication between VLAN 4 and VLAN 3
Source IP Address	10.118.3.1
Destination IP Address	10.118.2.1
Technique	Send packets from packet tracer
Expected Result	FAIL
Actual Result	FAILED. There is no communication between hosts in VLAN 2 and hosts in VLAN 3.

From the results, it can be explained that host in VLAN 4 cannot communicate with hosts in VLAN 3. i.e. Accounts User 1 in VLAN 4 cannot communicate with Accounts User 2 in VLAN 3. The implemented access control list (ACL) helps to filter the floor networks from accessing the others.

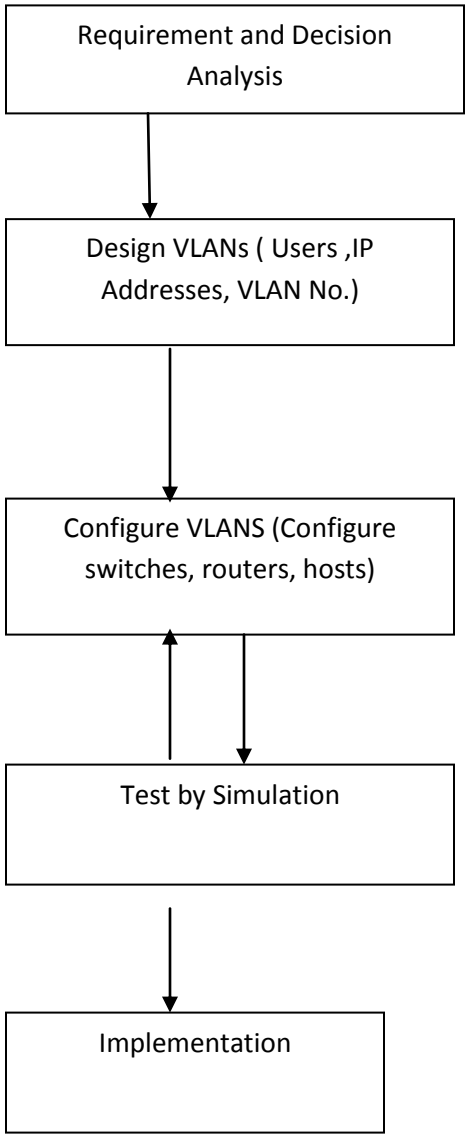
CHAPTER FIVE

5. VLAN IMPLEMENTATION

5.1. INTRODUCTION

This chapter provides the real logical LAN of the Treasury building after the analysis of the existing network. New VLANs will be designed, users migrated to the new VLANs and before the implementation, testing of the VLANs will be done to ensure they work appropriately. Since each floor has more than fifty users, only three users per floor will be used to test and simulate the designed network. Also since the building floors are similar, this implementation plan will consider only first, second and third floors.

5.2. Implementation Model



5.3. Requirement analysis

This requires identifying the departments and Users in the National Treasury building and where they are located. This is to assist in knowing the Data or information they share and how well it should be secured. The purpose for this requirement analysis is to identify data (application servers), process and interface users to the right VLAN which will improve data

security. There exist the following departments in the National Treasury; Administration. Accounts, Human Resource Management (HRM), human resource Development (HRD), Supply chain Management (SCM), Information Communication Technology (ICT), Planning and Monitoring, external audit, Finance, Internal Audit, Debt Management, Budget, External resources, Integrated Financial management Information System (IFMIS) and Macroeconomic. Since only first, second and third floor were of important for this research since what was to be designed for the three floors would be replicated to the rest of the floors.

For simulation purposes, only three users or hosts were to be used per floor.

The following were the hosts to be used per floor;

- Third floor: ICT User 1, Account user 1, HRM user 1
- Second floor: Account user 2, HRM user 2, HRM server
- First floor: ICT User 1, HRM user 3, Admin User 2

The network devices already on the existing network were found to be the right devices for the new network design. This requirement was very important to check since it was imperative to have the right devices to ensure they can support the configurations and also to have the right security of the device as per the recommendations from the manufacturer's (CISCO).

5.4. Decision analysis

After the analysis of all the requirements, a decision is made for the right network design with the VLAN enhancements. Departments/users will be grouped as per the assigned VLAN. This was after a decision to let users of same department access same resources and be able to communicate to another.

The following are the VLAN grouping for the users according to departments;

Table 7: Assigned VLANs

User	Department	VLAN NAME	VLAN No.
ICT USER 1	ICT	ICT	2
HRM USER 1	HRM	HRM	3
ACCOUNT USER 1	ACCOUNT	ACCOUNT	4
HRM USER 2	HRM	HRM	3
ACCOUNT USER 2	ACCOUNT	ACCOUNT	4
HRM SERVER	HRM	HRM	3
ICT USER 2	ICT	ICT	2
HRM USER 3	HRM	HRM	3
ADMIN USER 2	ADMINISTRATION	ADMINISTRATION	5

5.5. New VLANs Design

This is a phase where the graphical/logical drawing of the LAN is established according to the requirements from analysis in order to fulfill the scope and objective of the project. VLAN numbers and their networks was decided to be made simple to ensure that that network administrator can easily remember how the network is designed without referring on a documentation always. The Network is a class A network with IP 10.118.0.0 and subnet 255.255.255.0. VLANs are designed to have the following networks; VLAN 2 network is 10.118.2.x where x is any number between 1 to 254, VLAN 3 network is 10.118.3.x , VLAN 4 network is 10.118.4.x and VLAN 5 is 10.118.5.x. (x is any number between 1 to 254).

The gateway for VLAN 2 is 10.118.2.254, VLAN 3 is 10.118.3.254, VLAN 4 is 10.118.4.254 and VLAN 5 is 10.118.5.254.

To ensure all the users were in the right VLANs, the following IP Addresses were assigned to the users;

Table 8: New IP Address Allocation

User	**Department**	**IP Address**	**VLAN No.**
ICT USER 1	ICT	10.118.2.1	2
ICT USER 2	ICT	10.118.2.2	
HRM USER 1	HRM	10.118.3.1	3
HRM USER 2	HRM	10.118.3.2	
HRM SERVER	HRM	10.118.3.3	
HRM USER 3	HRM	10.118.3.4	
ACCOUNT USER 1	Account	10.118.4.1	4
ACCOUNT USER 2	ACCOUNT	10.118.4.2	
ADMIN USER 1	ADMIN	10.118.5.1	5

The logical representation of the network is prepared using Cisco Packet tracer

Diagram: Logical Representation of Designed VLANs

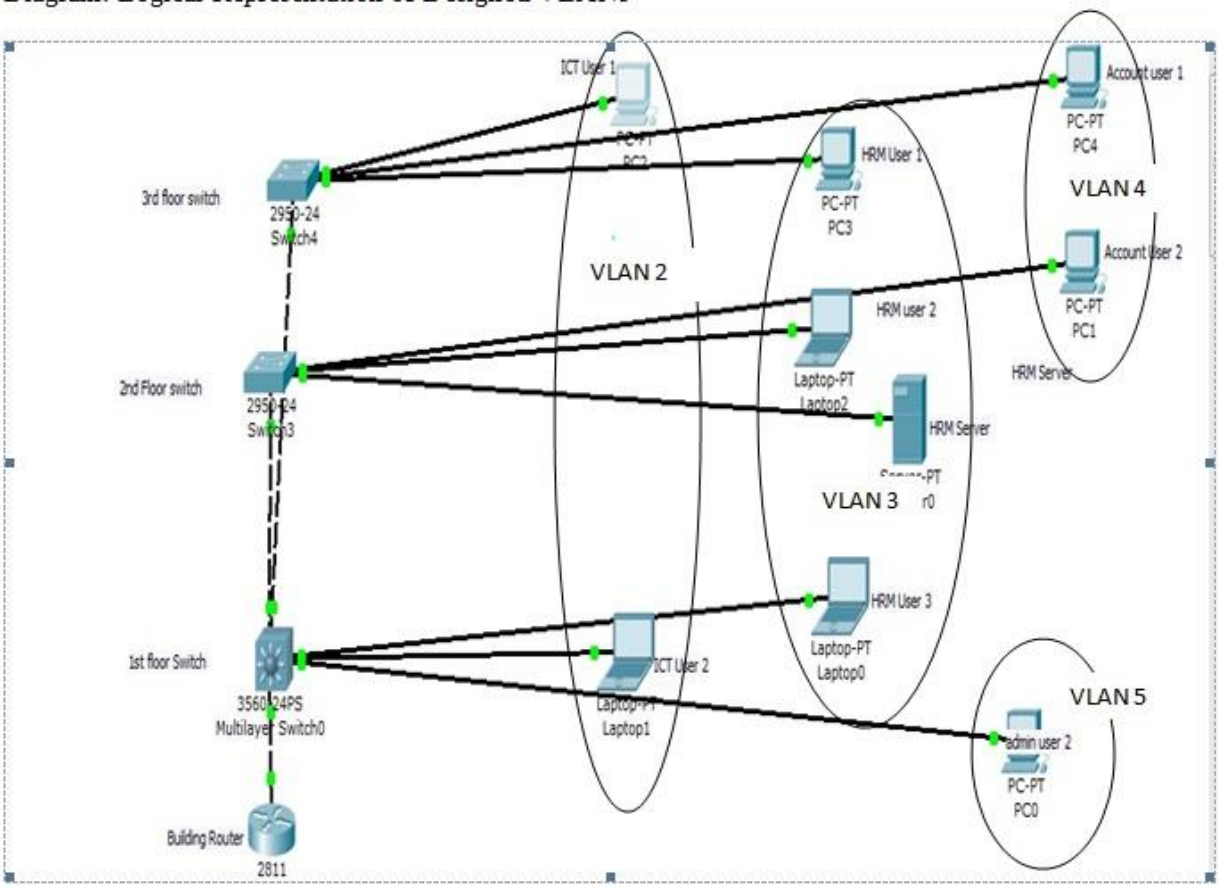


Figure 4: Logical representation of Designed VLANs

5.6. Configuration of VLANs, Routers, Switches and Hosts

5.6.1. Naming of network Devices (router and switches)

To ensure all the network devices i.e. routers and switches had to be given right names for the purpose of identification. Since switches were distributed on all the floors, the name of the switches was given as SWTCH MODEL-FLOOR NUMBER-NAME OF FLOOR WING-S NUMBER (Where S means switch).Example; The switch model on first floor on northern wing is Cisco 3750. The hostname configuration is 3750-01-N-S1 on the configuration setup of the switch.

5.6.2. Router configuration:

Security of data, information and even the network is a vital component in an organization, Akin (2002). Access control list can be deployed in a router to provide for the security of any resource within the network. Cisco IOS enables network administrators to implement security for the network using the Access control list (ACL). Using ACL in the new designed VLANs will prevent network packets from passing through the network to a destined network or host.

Access control list implementation will have the following benefits;

- Prevents traffic which is unwanted to access a VLAN
- Its used to block users or host from accessing some systems or devices in another VLAN
- It can block some devices or host from existing in the LAN

Sub interfaces for each VLAN are created and this will limit each VLAN to a specific IP Address as per the VLAN. This act as the gateways for each VLAN. Since the existing Router (CISCO 6506) was capable to perform all the required operations, it was recommended not to be replaced since the Manufacturer (CISCO) was still supporting it.

The configurations of the router are as shown in the appendix.

5.6.3. Switch configuration:

The setup need for this device is to create VLAN as per the floor. The switch ports are assigned to the right VLAN. The existing Switches (CISCO 3750) are intelligent switches, there was no need to replace them since they could perform the desired operations and could support more broadcast domains. The floor switches could also accommodate more than one VLANs. For security of the switches passwords are enabled to ensure one has to log in the device. To ensure the VLAN information was propagated to other switches in the Treasury Building, Each floor

switch was interconnected to the first floor core switch (CISCO 4506) using a trunk which allowed the VLANs configured to pass through.

The configurations are as shown in the appendix.

5.6.4. Trunk configurations:

Trunk ports can carry more than one VLAN at a time. It gives 100/1000mbps point to point connection between two switches or between switch and a router or between switch and server. A trunk port carries traffic of between 1-4094 VLANs at a time.

To ensure the VLANs are propagated between the switches and even the router, encapsulation IEEE 801.Q protocol was used.

The configuration are as indicated on the appendix.

5.6.5. VLAN Configuration:

The VLANs are created in one of the switches which act as the server. VLAN names and VLAN Number are assigned and their corresponding IP Addresses. The first floor switch is identified as the server switch where the VLANs will be created. VLAN Trunk protocol is implemented to help in the propagating of the VLAN information to the other switches in the building thereby reducing the workload to create in each switch and also to help in the administration of the VLANs. All the other switches except the first floor were configured to client vtp status to ensure there was only one VTP server to propagate VLAN information on the Local Area Network.

The configurations are as indicated on the appendix.

5.6.6. VTP Configuration:

VLAN Trunk Protocol (VTP) reduces administration in a switched network, Steele (2012). When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst series products and it was best to implement it in the National treasury Building since all the available network devices were all from CISCO. First floor switch which acted as the core switch and the server to the VTP domain was configured and these was propagated to the other floor switches which were configured as clients on the vtp domain.

The configurations are as indicated on the appendix.

5.6.7. Hosts Configuration:

All hosts i.e. computers and servers were manually configured for the purpose of this simulation. Each host is assigned an IP Address, Subnet mask and gateway as per the VLAN the host is attached to. For this research, IP Addresses will be manually assigned and was recommended if the simulation was successful, to ensure IP Address were allocated dynamically since the National treasury was a big network with many hosts.

5.6.8. Access control list configuration

To ensure filtering traffic of the unwanted networks, ACL is configured on the router sub interfaces. The different extended access groups are created then the access list defined per interface depending on the VLANs being filtered.

The configurations are as per the appendix.

5.7. Testing the designed VLANs

The main purpose of this stage is to;

- Build the VLANs and test whether security of Applications and users is enhanced and to see whether the design is working as required. This will be constructed and tested using the Cisco Packet Tracer which will simulate the topology and even the packet movements during testing.
- Test plan: this defines all the testing required to ensure all the VLANs are working as designed. If design passes the tests it declared complete for full implementation

  Using the Cisco Packet Tracer to construct and test, the following test results were achieved and their configurations are as shown on the appendix.

5.7.1. Host to host testing

Since Users of same Departments are designed to be in the same VLAN, the following test for Users in the same VLAN was simulated on the Cisco packet Tracer.

Table 9: Host to host testing on Designed VLANs

HOST TO HOST TESTING	
Test Name	Host to host
Test Target	To test communication between host in VLAN 2
Source IP Address	10.118.2.1
Destination IP Address	10.118.2.2
Technique	Send packets from packet tracer

Expected Result	Pass
Actual Result	Successful. There is communication between hosts in VLAN 2

From the results above, it can be proved that users in the same VLAN can communicate and share resources even if they are located in different floors. This shows that resources can be shared within the VLAN without hosts of other VLANs accessing it.

Table 10: VLAN to VLAN testing on Designed VLANs

VLAN to VLAN TESTING	
Test Target	To test communication between VLAN 4 and VLAN 3
Source IP Address	10.118.4.1
Destination IP Address	10.118.3.1
Technique	Send packets from packet tracer
Expected Result	FAIL
Actual Result	FAILED. There is no communication between hosts in VLAN 2 and hosts in VLAN 3.

From the results above, it can be seen that, host of different VLANs cannot communicate since the access control list was configured not to allow traffic to other networks hence this safeguards data/information or resources from being accessed. The use of access control lists (ACL) helps to filter unwanted network.

5.8. Install and Implement the Network

This stages is very critical since its derived from the testing done on the simulation. If the test failed to meet the required results, it could not be implemented. As for this research, it was found that the designed VLANs were successfully tested hence the process of implementation was to be done as per the simulation on the Cisco packet tracer. Since the Cisco router and the switches already on the network was up to date, there was no need of procuring others hence they were ready to be configured as per the simulation. Then the Users and Servers hosting the Data to be secured are migrated to the right and respective VLANs. Various protocols to be used on the LAN are implemented as per the hardware available since they could support.

The simulation was tested and re-tested again to ensure all the required parameters were in place. After the analysis of the results, it was found that the VLANs could be implemented in the National Treasury Network and it would give more benefits to the network administrator since all departments would be on their own network.

5.9. Maintenance and support

After the implementation the network requires maintenance and support to ensure any hitches reported are rectified. Also due to emergence of new technologies like implementing new VLAN protocols, support is necessary where specific professionals in Network Administration and Security together with Application Developers will have continuous training for any support necessitated. Software update for the devices also ensure loophole are sealed to secure the devices as required by the Manufacturer of the Devices.

5.10. Documentation

For the purpose of later reviews and if there was change management for the network administrator of the network, all the configurations were to be documented, labeling of the network devices (router and switches) were to be done accordingly and the name of VLANs, their networks, VTP configurations and any use of password was to be documented and kept in a safe location.

CHAPTER SIX

CONCLUSION AND FURTHER WORK

This research is helpful to the organization for the effective data security by implementing VLANs to ensure staffs are in the right network when accessing resources. Other benefits are;

- Improve the manageability of users per department instead of per floor management. This assists the movement of the users to any floor since the port a user connects is migrated to the right VLAN.
- Reduce cost of procuring Routers since one router is enough. A router can be configured to have more than one interface hence one router is enough to create all the routing interfaces.
- To have many broadcast domain since once can create more than one VLAN in one switch. Since one switch host many users from different departments, moving users to specific VLAN helps to create the different networks in a switch hence reduce traffic collisions.

Further Work

Since there were more than one applications being run in the Government of Kenya National Treasury network, it is recommended that all the Application Servers be moved to their own VLAN where the network administrator, network security and the application developers could access them and enforce or configure more security to them. It would be also easier to monitor this specific network since it would be the business core of the National Treasury. This VLAN would be in a Demilitarized zone (DMZ) to enable implement data and information security centrally.

REFERENCES

Akin (2002) Hardening Cisco Routers

Alabady (2008), "Design and Implementation of a Network Security Model using static VLAN and AAA Server," In Proceedings International Conference on Information & Communication Technologies: from Theory to Applications, ICTTA'2008

Awondele et al.,()2012) Proceedings of Informing Science & IT Education Conference (InSITE)

Rotchke (2004), Access Control Systems & Methodology (New York: SecurityDocs.com, 2004, accessed 06 November 2004)

Brown, C.V. & Magill, S.L. (1994). Alignment of the IS functions with the enterprise: Toward a model of antecedents. MIS Quarterly, December, pp.371-403.

Froehlich, A., S. (2005): CCNA Voice: Study Guide Exam 640-460

Lammle, T., S. (2005): Certified Network Associate Review Guide (640-802):

Ciborra, C.U. (1993). Teams, Markets and Systems: Business innovation and information technology. Cambridge, Cambridge University Press.

Lammle (2005) CISCO: Cisco Certified Network Associate study guide, 5th edition,

Clarke, R. (2008) Conventional Public Key Infrastructure: An Artefact Ill-Fitted to the Needs of the Information Society.

Desai, N. (2004) Intrusion Prevention Systems: the Next Step in the Evolution of IDS.

Davies (2002), Tutorial: The Security of Data in Networks,

Daft, R.L. (1998). Organization Theory and Design, 6th Edition. South Western College Publishing.

Sharfman, F.,(1991). Strategic Decision-making: a multiple-context framework, Advances in Information Processing in Organizations, Vol. 4, pp. 77-110.

Sawy, Malhotra, Gosain, and Young(1999). IT-intensive value innovation in the electronic economy: insights from Marshall industries, MIS Quarterly, Vol. 23, No. 3, pp. 305-335.

Zwicky et al.,(2002) Building Internet Firewalls, 2nd Edition

Emanuel and Sife (2008) International Journal of Education and Development using Information and Communication Technology; (IJEDICT), 2008, Vol. 4, Issue 3, pp. 137-142.

Farrow (2003). VLANs: Virtually insecure? Network Magazine, 18(3), 62-63.

Froom, R., Sivasubramanian, B., Frahim, E., & Houston, T. (2007). Authorized self-Study guide: Building Cisco Multilayer Switched Networks (BCMSN) (4th ed.).Indianapolis: Cisco Press.

Fadl N, Ibrahim O, A.alaziz and Yousif A. (2011) International Journal of Advanced Science and Technology, Vol. 37, December, 2011

Given, L. M. (2008). The Sage encyclopedia of qualitative research methods. Los Angeles, Calif: Sage Publications.

Galliers, R.D. (1993). Towards Flexible Information Architecture: Integrating Business Strategies Information Systems Strategies and Business Process Redesign. Journal of Information Systems, 3, pp.199-213.

Tipton and Krause (2000), Information Security Management Handbook, 4th Edition (Boca Raton: Auerbach, 2000),

IEEE (2002) Computer Society Press, Los Angeles

IBM: Network Planning Products: Planning (1984) SC27-0658- 1, IBM Corporation, Research Triangle Park, North Carolina, pp. 28 – 30

Shaffi and Obaidy (2012)Effective Implementation of VLAN And ACL In Local Area Network, International Journal of Information Technology and Business Management 29th August 2012. Vol.4 No. 1

Day and Zimmermann (1983)The OS1 Reference Model in proc. THE IEFJ2, VOL. 71, NO. 12, Dec. 1983

Jyothsna and Prasad (2011) International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, September 2011

Steele (2012) Beyond Virtual Local Area Networks (VLANs)

Khidzir , Mohamed and Arshad 2013; Journal of Industrial and Intelligent Information Vol. 1, No. 4, December 2013

Kothari C. R., (2004)Research Methodology: Methods & Techniques; New Dheli: New Age

Kim J., Lee K., Lee C., (2004) Design and Implementation of Integrated Security Engine for Secure Networking, In Proceedings International Conference on Advanced Communication Technology

Kim (2004), "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, February 2004

Kuhn, D. R., Walsh, J. T., and Fries (2005). Security considerations for Voice over IP Systems (Jan. 2005); NIST Special Publication 800-58.

Lin (2004) Information and Data Security Best Practices, 12 October 2004

Lederer, A.L. and Salmela, H. (1996). Towards a theory of strategic information systems planning, Journal of Strategic Information Systems, Vol. 5, pp. 237-253.

Lo (2012) Journal of Theoretical and Applied Information Technology, electron government affairs system based on VPN technology

Manu (2004) Firewall Basics

Mbowe et..al (2014) Journal of Information Security, 2014, 5, 166-177

Miller (1987). The structural and environmental correlates of business strategy, Strategic Management Journal, Vol. 8, pp. 55-76.

Miller (1988). Relating Porter's business strategies to environment and structure: analysis and performance implications, Academy of Management Journal, Vol. 31, No. 2, pp. 280-308.

Mugenda M. Olive & Mugenda G. Abel (2003): Research Methods: Quantitative and Qualitative Approaches; Nairobi: ACTS Press.

NIST (2004)National Institute of Standards and Technology. NIST PKI Program. Washington

Nanumaker J., JR., Chen M., Purdin T., (2001); Systems development in Information Research

Organization de coope ration et de developpement e conomiques. (2005). OECD e-government studies: Mexico. Paris: Organization for Economic Co-operation and Development.

Orodho A. J and Kombo (2002) research methods Nairobi: KU Institute of Open Learning

Innella (2004)The Evolution of Intrusion Detection Systems, 12 October 2004); available from http://www.securityfocus.com/infocus/1514; Internet

Rao and Choudhury (2010), international Journal of Library Science, Vol 01, Issue J10, year 2010

Stallings (2003) Network Security Essentials Applications and Standards, 2nd ed., New Jersey: Pearson Education, 2003, pp. 123-128

Stallings (2003) Network Security Essentials Applications and Standards, 2nd ed., New Jersey

Ehta, Singh, Upadhyaya , Subarna , Shakya and Pokharel (2012) Information Security Framework for E-Government Implementation in Nepal, Journal of Emerging Trends in Computing and Information Sciences, vol. 3, no.7, July 2012 pg. 1074-1078

Vyncke and Paggen (2008) LAN switch security: what hackers know about your switches (pp. 54-64). Indianapolis, IN: Cisco Press.

Zikmund (2000) Business Research methods. Fort Worth: Dryden

APPENDIX 1: Device Configurations

Switch configurations

To Create VLAN ICT

Switch>en

Switch#config

Switch(config)#vlan 2

Switch(config-vlan)#name ict

Switch(config-vlan)#exit

Switch#

To Create VLAN HRM

Switch#config

Switch(config)#vlan 3

Switch(config-vlan)#name HRM

Switch(config-vlan)#exit

Switch#

To Create VLAN ACCOUNT

Switch#config

Switch(config)#vlan 4

Switch(config-vlan)#name ACCOUNT

Switch(config-vlan)#exit

Switch#

To Create VLAN ADMIN

Switch#config

Switch(config)#vlan 5

Switch(config-vlan)#name ADMIN

Switch(config-vlan)#exit

Switch#wr

Switch#

To configure VTP on server switch

Switch#conf t

Switch(config)#vtp mode server

Switch(config)#vtp domain treasury

Switch(config)#vtp password ******** (where ****** is the designated password for the VTP)

Switch(config)#do wr

Switch(config)#

To configure VTP on all client switches

Switch#conf t

Switch(config)#vtp mode client

Switch(config)#vtp domain treasury

Switch(config)#vtp password ******** (where ****** is the designated password for the VTP)

Switch(config)#do wr

Switch(config)#

3rd Floor Switch Configurations

To Configure ICT User 1 to access VLAN 2

Switch#conf t

Switch(config)#int fa0/5

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

To Configure HRM User 1 to access VLAN 3

Switch#conf t

Switch(config)#int fa0/4

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

To Configure Account User 1 to access VLAN 4

Switch#conf t

Switch(config)#int fa0/3

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 4

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

2ND FLOOR SWITCH CONFIGURATIONS

To Configure Account User 2 to access VLAN 4

Switch#conf t

Switch(config)#int fa0/2

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 4

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

To Configure HRM User 2 to access VLAN 3

Switch#conf t

Switch(config)#int fa0/3

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

To Configure HRM Server to access VLAN 3

Switch#conf t

Switch(config)#int fa0/4

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

1ST FLOOR SWITCH CONFIGURATIONS

To Configure ICT User 2 to access VLAN 2

Switch#conf t

Switch(config)#int fa0/3

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

To Configure Admin User 2 to access VLAN 5

Switch#conf t

Switch(config)#int fa0/5

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 5

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

To Configure HRM User 3 to access VLAN 3

Switch#conf t

Switch(config)#int fa0/4

Switch(config-if)#switchport ac

Switch(config-if)#switchport access vlan 3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport nonegotiate

Switch(config-if)#do wr

Switch(config-if)#no shutdown

Switch(config-if)#

ROUTER CONFIGURATIONS

To Configure VLAN 2 sub-interface

Router#conf t

Router(config)#int fa0/0

Router(config-if)#int fa0/0.2

Router(config-subif)#encapsulation dot1Q 2

Router(config-subif)#ip address 10.118.2.254 255.255.255.0

Router(config-subif)#no shutdown

Router(config-subif)#do wr

Router(config-subif)#

Router#

To Configure VLAN 3 sub-interface

Router#conf t

Router(config)#int fa0/0

Router(config-if)#int fa0/0.3

Router(config-subif)#encapsulation dot1Q 3

Router(config-subif)#ip address 10.118.3.254 255.255.255.0

Router(config-subif)#no shutdown

Router(config-subif)#do wr

Router(config-subif)#

Router#

To Configure VLAN 4 sub-interface

Router#conf t

Router(config)#int fa0/0

Router(config-if)#int fa0/0.4

Router(config-subif)#encapsulation dot1Q 4

Router(config-subif)#ip address 10.118.4.254 255.255.255.0

Router(config-subif)#no shutdown

Router(config-subif)#do wr

Router(config-subif)#

Router#

To Configure VLAN 5 sub-interface

Router#conf t

Router(config)#int fa0/0

Router(config-if)#int fa0/0.5

Router(config-subif)#encapsulation dot1Q 5

Router(config-subif)#ip address 10.118.5.254 255.255.255.0

Router(config-subif)#no shutdown

Router(config-subif)#do wr

Router(config-subif)#

Router#

To configure router name

Router#conf t

Router(config)#hostname 6506-00-R1

6506-00-R1(config-if)#do wr

6506-00-R1(config-if)#exit

6506-00-R1#

To configure Switch name

Switch#conf t

Switch(config)#hostname 3750-01-N-S1

3750-01-N-S1(config-if)#do wr

3750-01-N-S1#

To configure Access Control Lists (ACL)

6506-00-R1#config t

6506-00-R1(config)# int fa0/0.2

6506-00-R1(config-if)# access group 102 in

6506-00-R1(config-if)#exit

6506-00-R1(config)# access list 102 deny icmp 10.118.3.0 0.0.0.255 10.118.2.0 0.0.0.255

6506-00-R1(config)# access list 102 deny icmp 10.118.4.0 0.0.0.255 10.118.2.0 0.0.0.255

6506-00-R1(config)# access list 102 deny icmp 10.118.5.0 0.0.0.255 10.118.2.0 0.0.0.255

6506-00-R1(config)# int fa0/0.3

6506-00-R1(config-if)# access group 103 in

6506-00-R1(config-if)#exit

6506-00-R1(config)# access list 103 deny icmp 10.118.2.0 0.0.0.255 10.118.3.0 0.0.0.255

6506-00-R1(config)# access list 103 deny icmp 10.118.4.0 0.0.0.255 10.118.3.0 0.0.0.255

6506-00-R1(config)# access list 103 deny icmp 10.118.5.0 0.0.0.255 10.118.3.0 0.0.0.255

6506-00-R1(config)# int fa0/0.4

6506-00-R1(config-if)# access group 104 in

6506-00-R1(config-if)#exit

6506-00-R1(config)# access list 104 deny icmp 10.118.2.0 0.0.0.255 10.118.4.0 0.0.0.255

6506-00-R1(config)# access list 104 deny icmp 10.118.3.0 0.0.0.255 10.118.4.0 0.0.0.255

6506-00-R1(config)# access list 104 deny icmp 10.118.5.0 0.0.0.255 10.118.4.0 0.0.0.255

6506-00-R1(config)# int fa0/0.5

6506-00-R1(config-if)# access group 105 in

6506-00-R1(config-if)#exit

6506-00-R1(config)# access list 105 deny icmp 10.118.2.0 0.0.0.255 10.118.5.0 0.0.0.255

6506-00-R1(config)# access list 105 deny icmp 10.118.3.0 0.0.0.255 10.118.5.0 0.0.0.255

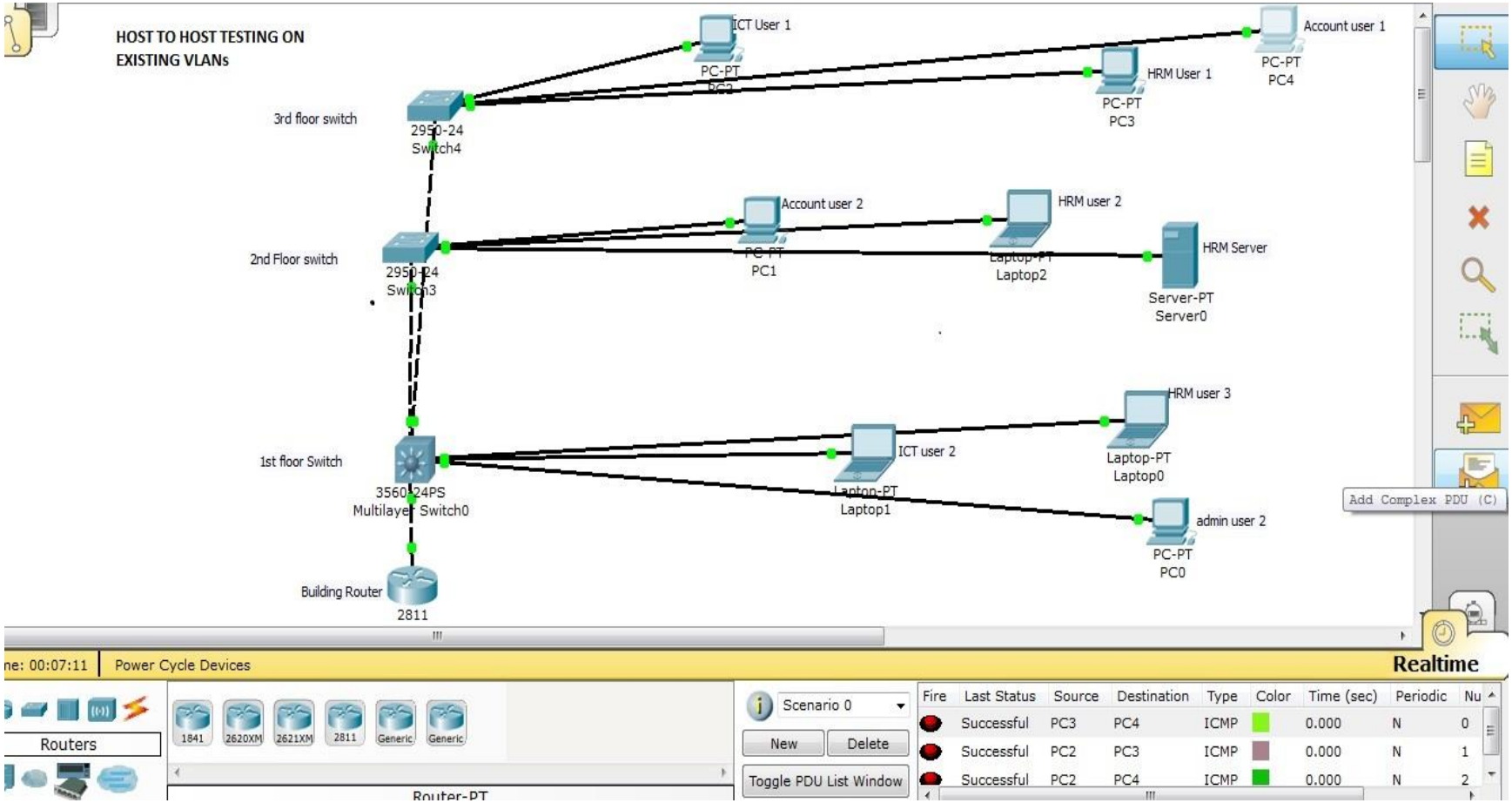
6506-00-R1(config)# access list 105 deny icmp 10.118.4.0 0.0.0.255 10.118.5.0 0.0.0.255

6506-00-R1(config)#wr

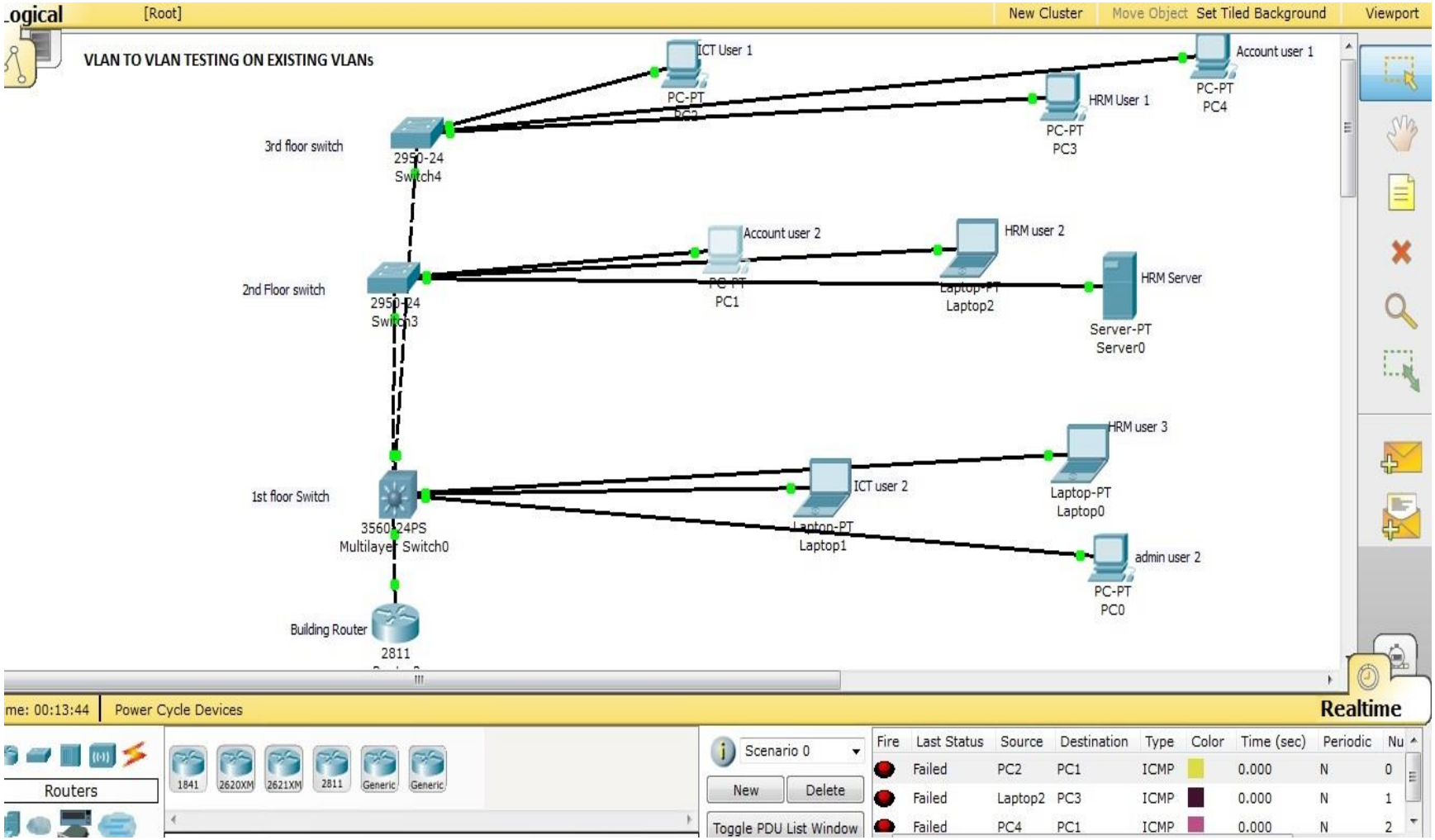
6506-00-R1(config)#

APPENDIX: TEST RESULTS

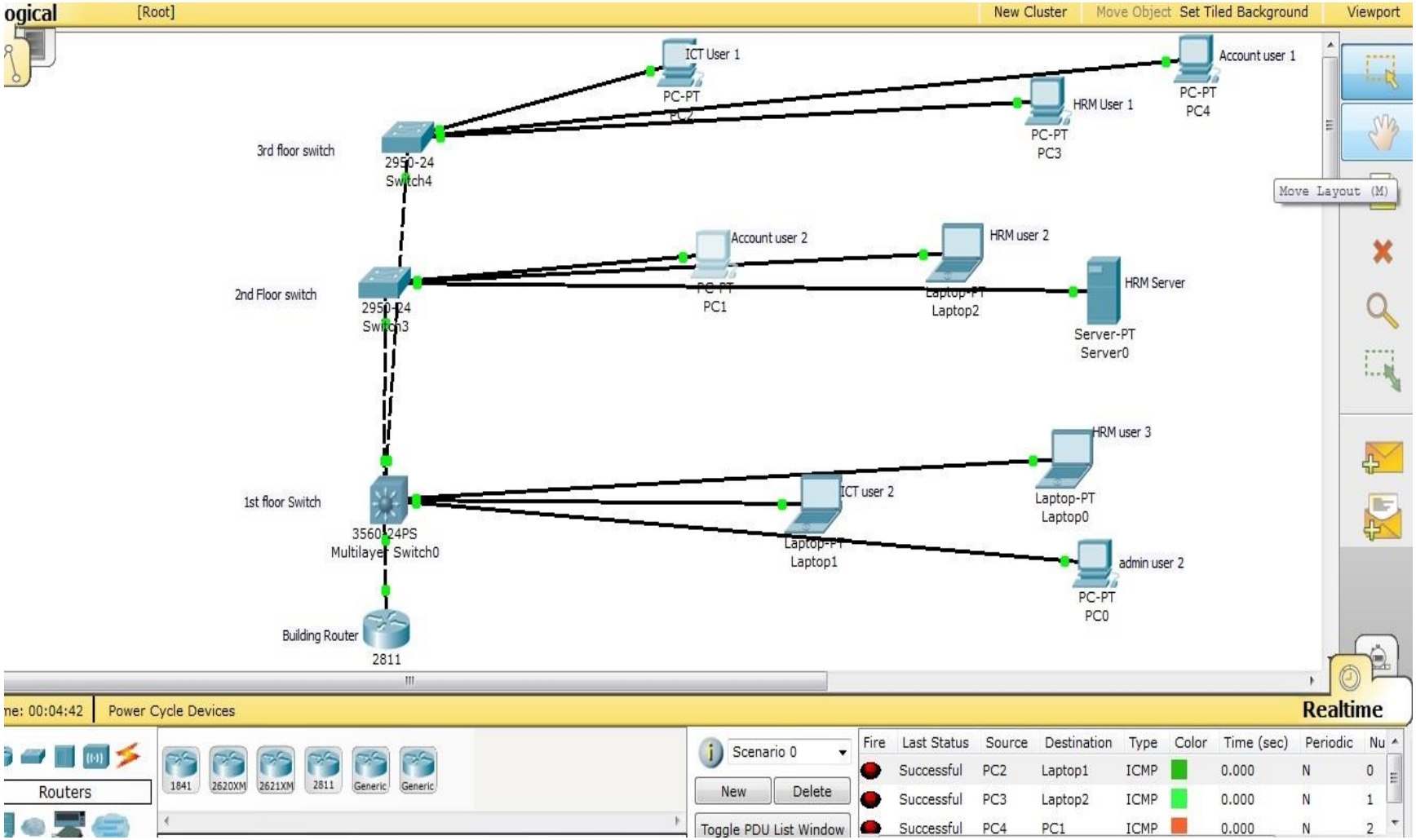
HOST TO HOST TESTING ON EXISTING VLANS



VLAN TO VLAN TESTING ON EXISTING VLANS



HOST TO HOST TESTING ON NEW DESIGNED VLANS



VLAN TO VLAN TESTING ON NEW DESIGNED VLANS