**Chapter 1: Introduction**

**1.0 Introduction**

Each of the past three centuries has been dominated by a distinct technology. The 18th century was the era of the great mechanical systems accompanying the Industrial Revolution. The 19th century was the age of the steam engine. During the 20th century, the key technology was information gathering, processing, and distribution. Among other developments, was the birth and unprecedented growth of the computer industry, and the launching of communication satellites; As a result of rapid technological progress, these areas are rapidly converging in the 21st century and the differences between collecting, transporting, storing, and processing information are quickly disappearing. Organizations with hundreds of offices spread over a wide geographical area routinely expect to be able to examine the current status of even at the push of a button. (Andrew S. and David J., 2011) As the ability to gather, process, and distribute information grows, the demand for more sophisticated information processing grows even faster. This give rise to what we know today as computer networks thus this is a collection of interconnected applications and device within an area that enable the processing and sharing of resources between different remote computer users. With the development of society, network information/resource is used by people more and more and its importance is becoming notable, thus making it becoming the most critical thing of a country's political, economic, and military resources. (Saadat M. as cited in Cuihang Wu ,2010)

**1.1 Background Information**

Computer network as part of information and communication technology (ICT) has become a significant component of the digital world today. Thus it has successfully presented us the need to adjust our culture and society to appropriately meet the challenges of this information age.

It can be inferred from Castells (1996), that ICT is one key factor responsible for metamorphosing our natural world to a global village thus enable the sharing and access of information resource from any geographical location in the world today. This is so, since ICT’s persistence brought about a rapid technological, social, political, and economic transformation. It is worthwhile to note that this rapid growth, has brought about network connectivity which has given rise to the establishment of what is known today as network of networks called the internet (the internet is a collection of different networks “local area network” infrastructure).

According to the SANS survey (2017), Network infrastructure is the key business asset for organizations that depend on geographically dispersed information for their line-of-business. This infrastructure is made up of different network applications, devices etc., that enable the sharing of information between distances user.

The Internet continues to grow exponentially. Personal, government, and business applications continue to multiply on the Internet, with immediate benefits to end users. However, these network-based applications and services can pose security risks to individuals and to the information resources of companies and governments. Information is an asset that must be protected. Without adequate network security, many individuals, businesses, and governments risk losing that asset. Network security is the process by which digital information assets are protected. The goals of network security are as follows: Protect confidentiality, maintain integrity and ensure availability; With this in mind, it is imperative that all networks be protected from threats and vulnerabilities for a business to achieve its fullest potential.

**1.2 Problem Area**

In recent years, as a result of the rapid development in information technology, the popularity of Internet has increasingly changed the style of living. Thus, security on the Internet and on Local Area Networks is now at the forefront of computer network related issues. With the evolution of networking and the Internet, the threats to information and networks have risen dramatically. Many of these threats have become cleverly exercised attacks causing damage or committing theft.

For example, the SANS-ICS, E-ISAC (SysAdmin Audit Network Security, Industrial Control System, Electricity Information Sharing and Analysis Center) in March 18th 2016 made a publication on an industrial attack on the Ukrainian Power Grid, which happen in December 23th, 2015. the attack; compromises about 3 distribution companies and over 30 sub-stations causing power blackout and denial of phone services to over 225,000 customers. And also, in April, 2017, there was another attack on internet applications and resources called WannaCry Ransomeware Attack that compromise host computer resources in worm-like manner, thus encrypting files and documents and demanding ransom from organizations. This affected about 105 countries.

Nowadays, to get connected comes at the expense of adequate network security, thus, information is an asset that must be protected. Typically, these threats are persistent due to vulnerabilities, which can arise from mis-configured hardware, outdated software licence, poor network design, inherent technology weaknesses, or end-user carelessness etc. The goal of any security design is to provide maximum security with minimum impact on user access and productivity. Some security measures, such as network data encryption, do not restrict access and productivity. On the other hand, cumbersome or unnecessarily redundant verification and authorization systems can frustrate users and prevent the much-needed access to critical network resources.

And also, since organizations are constantly subject to change, security policies must be systematically reviewed and updated to reflect new business directions, technological changes, and resource allocations. The project is model to provide more reliable and flexible security design amongst others; hence, attempt to obtain a cost effective, and a reliable security model that will protect confidentiality, maintain integrity, and Ensure availability of a network resources.

**1.3 Problem Statement**

There is a lack of reliable network security model for a cooperative network; taking a look at the university of Jos network (ict as case study).

**1.4 Research Question**

**Primary Question**

What should constitute a cooperative network security, that will enhance a flexible, reliable and a cost-effective protection to network asset?

**Secondary Questions**

* What influence does a network security have on cooperate network?
* What are the characteristics of the cooperate network security model?
* How can the cooperate network security model be designed?

**1.5 Research Objectives**

**Primary Objective**

The primary objective is to model a reliable and cost-effective network security for cooperation that will guard a network from vulnerabilities, threats, attacks, configuration weaknesses. Hence looking at the various causes and providing advice where necessary.

**Secondary Objectives**

* Identify the general effects of network security to a cooperative network.
* Identify the influence of network security to a cooperative asset.
* Identify the characteristics associated with the network security model.
* Establish and compose the necessary elements that should characterize the network security model.

**1.6 Research Methodology**

Through literature survey, the impact of network security to a cooperate network asset will be identified so as to answer the first and second sub-objectives.

Also, the review will go further to identify the characteristics of the network security, thereby answering the third sub-objective.

Furthermore, the last sub-objective will be answered through logical reasoning analysis and the use of already existing tools to build the components of network security model to enhance robust, flexible and a cost effective protective measure to cooperative network asset.

Also, a sampled opinion regarding network security will be obtained from network administrators and security analysis (if any) through a form of Interview/questionnaire for subsequent use in data analysis.

Consequently, results from the component model will be used to model a proof-of-concept prototype. At the end, the component model and the proof-of-concept prototype will be used to derive the conclusion on the flexibility, robust and cost effective of the network security model.

**1.7 Project Scope/Limitations**

The scope of this study is strictly on modelling a network security system that will enable protection of network resources (asset) with attention to vulnerability, configuration weakness, and poor security policies and how to mitigate them and most importantly having some intrusion detection capabilities. Thus, the model is design to prefer a better and a robust model that will reduce the threats and attacks posted by this security laps (i.e. vulnerability, configuration weakness, poor security policies)

Furthermore, this study will be using some already existing security tools to enable the modelling of the system; some of these tools include a virtual simulating environment, network security software, firewalls, identity servers etc. A model like this, will also have some essentials point of recommendation for security and network administrators

**1.8 Brief Chapter Outline**

**1.8.1 Chapter 1: Introduction**

This chapter provides an introduction to the research project. The direction of the project was expressed through the broad explanation given on the problem area, the scope, the significance of the project, the research objectives and the research methodology that would be followed to achieve the said objectives.

**1.8.2 Chapter 2: functionality of network security to cooperative network resources**

This chapter provides a detailed investigation into relevant literature and explores the current knowledge of the research area.

**1.8.3 Chapter 3: Data Collection and findings**

Chapter 3 will introduce the survey to be used in order to gather data pertaining to a specific population concerning their experience regarding network security.

**1.8.4 Chapter 4: Proposed solution**

In agreement with chapter 2 and the findings established chapter 3, a model for the network security will be established. The model will then be used to build a prototype to solve the problem stated at the start of this work.

**1.8.5 Chapter 5: Evaluation/Testing**

Activities aimed at evaluating the different attributes or capabilities of the system to determine if they met earlier specifications will be carried out in this chapter.

**1.8.6 Chapter 6: Conclusion**

This chapter will briefly conclude the research project by giving a holistic view to the mentioned problem in chapter one. A conclusion to this research project be established in this chapter. The chapter will re-state the problem statement together with the objectives from the previous chapters.

**1.9 Conclusion**

This chapter has provided a roadmap for the rest of this research document. Background of the problem was discussed and a problem statement formulated. Objectives for this study were defined together with the methodology for achieving the objectives. A scope was also set out to define certain limitations of this research. Finally, a brief outline was given of the chapters to follow. The next chapter will examine deeper into the topic.

**Chapter 2: Literature Review**

**2.0 Introduction**

As far back as Julius Caesar reign, security of information has been of much importance. Julius Caesar created the Caesar cipher. This cipher allowed him to send messages that could not be read if they were intercepted.

In our today society, there have been an increasing reliance on computer systems worldwide for data processing and information storage, the need for legitimate security of information and data cannot be overemphasized. Thus, un-authorized access, data can violate individual privacy and even threaten the existence of an organization; As many aspects of our lives rely on the Internet and computers, including communications, transportation, government, finance, medicine and education. With this in mind then, it is necessary to secure computer systems and the stored information *(MS-ISAC, 2010)*.

This chapter shall explore briefly, the relevance of network security to institutions. The first section shall present some important factors and tools necessary for network design and security setting for any institution. Subsequent sections shall identify some criterial and benefits derived by implement a good network security and conclude with a section to highlight the mode impact of security to institutions.

**2.1 What is network**

In many ways, network can be as the interconnection of computer or electronic device with the main aim of sharing information or resources. Today, computers are most useful if they are networked together to share information and resources, and companies that put their computers on a network need to take some simple precautions to reduce the risk of unauthorized access *(John E. 2001).*

Since the introduction of the personal computer in the early 1970s, businesses have found more uses and applications for technology in the workplace. With the introduction of local area networks, file sharing, and print sharing in the 1980s, it became obvious that distributed computing was no longer a passing fad.

**2.1.1 Type of network**

For any network security design there must be an already existing network design which could either be categories into:

*Local Area Network (LAN):* it’s a network situated within a single geographical location, such as office building, school etc. typically work with a High speed and cheaper connection. Thus, it’s Physical layer implementations vary, and all support various cabling structures. There are three main categories of the Ethernet LAN cabling include:

* Ethernet and IEEE 802.3 – Operate at 10 Mbps over coaxial cable, UTP, or fiber.
* 100 Mbps Ethernet (Fast Ethernet IEEE 802.3u) – Operates over UTP or fiber.
* 1000 Mbps Ethernet – Gigabit Ethernet that operates over fiber. Ethernet and IEEE 802.3 – Operate at 10 Mbps over coaxial cable, UTP, or fiber.

*LAN Specifications and Connections*: Ethernet has several LAN specifications, include:

* IEEE 802.3 (10Mbps), IEEE 802.3u (100 Mbps), and Gigabit Ethernet (1000 Mbps).
* UTP Category 5 is required for Fast Ethernet.
* Straight-through cables are typically used to connect different device types, such as a router and a switch. The exception is a switch-to-hub connection, which require a crossover cable.
* Crossover cables are typically used to connect similar devices, such as a switch and a switch.

*Wireless Local Area Network (WLAN):*A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. In 1997, 802.11 was implemented as the first WLAN standard. It is based on radio technology operating in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbps. thus, WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing, and warehousing.

According to a study by the Gartner Group, approximately 50 percent of company laptops around the world will be equipped for WLAN by 2006. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost-of-ownership, and scalability. There are three main types of WLAN architecture: Independent, Infrastructure, and Microcells and Roaming.

*Wide Area Networks (WAN):*Wide Area Networks can be seen as connection pipes that interconnect Local Area Networks. they are owned by service providers and their functionality-infrastructure is leased in order for LANs to be able to extend their expandability and make use of distant-remote services. A number of different WAN connection types exist today. Choosing the right WAN connection type is up to you this include:

* *Leased Line:* This is considered to be a dedicated point-to-point with the protocols of HDLC (High-Level Data Link Control) and PPP (Point-to-Point Protocol). When cost in not an issue, you should use this type of connection.
* *Circuit Switching:* is based on the typical telephone switching network. A connection needs to be established prior to be able to transfer data. With ISDN (Integrated Services Digital Network) protocol as it basically connection protocol type.
* *Packet Switching*: Always-on connection, where available bandwidth is shared between several users. No time-based charging. Charging is based on committed traffic rate. Frame Relay is a packet switching connection type.
* *High Level Data Link Control (HDLC):* HDLC is a data-link layer protocol with no standard way of identifying the type of network protocol carried within the HDLC encapsulation, each vendor uses its own proprietary HDLC protocol.

*WAN specification and connection*: There are several ways to carry traffic across the WAN. The implementation depends on distance, speed, and the type of service required. The speeds of connections vary from 56 Kbps to T1/E1 (1.544/2.048 Mbps).

**2.1.2 Network component**

For any network design each component that is to be on a network is categorized according to its’ mode of operation and design; thus, have different physical or logical connectivity. This modularity enables flexibility in network design. It facilitates implementation and troubleshooting. Three areas of focus in segmental network design are as follows:

*Enterprise component*: This area contains the network elements required for independent operation within a single campus or branch location. This is where the building access, building distribution, and campus core are located thus the device located at this level include the pc, switches (access, distribution layer) etc.

*Server farm*: A component of the enterprise campus, the data centre server farm protects the server resources and provides redundant, reliable high-speed connectivity, thus the device located at this level include various servers, and other network resources.

*Enterprise edge*: As traffic comes into the campus network, this area filters traffic from the external resources and routes it into the enterprise network. It contains all the elements required for efficient and secure communication between the enterprise campus and remote locations, remote users, and the Internet. Such device includes routers, gateway device, firewall ids/ips etc.

**2.1.3 network design model**

network design model can the categorized into:

*Hierarchical Network Design:* In networking, a hierarchical design is used to group devices into multiple networks. The networks are organized in a layered approach. The hierarchical design model has three basic layers:

*Core layer*: Connects distribution layer devices e.g. Routers, ids, firewall, switches etc.

*Distribution layer*: Interconnects the smaller local networks e.g. switches, etc.

*Access layer:* Provides connectivity for network hosts and end devices e.g. pc, tabulate etc.

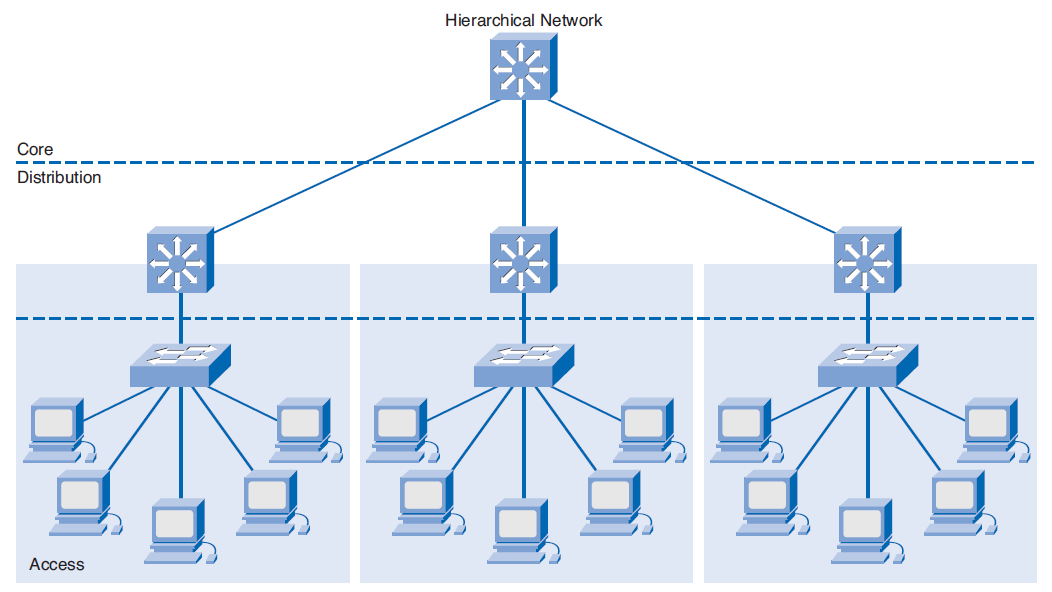


Fig 2.1: Hierarchical Network Design

*Flat network design:* is a computer design approach that aim to reduce cost, maintenance, and administration. Thus, flat network is design to reduce the number of routers and switches on a computer network by connecting devices to a single switch instead of separate switches thus in flat network design all device is on the same broadcast example include star, ring, mesh etc.

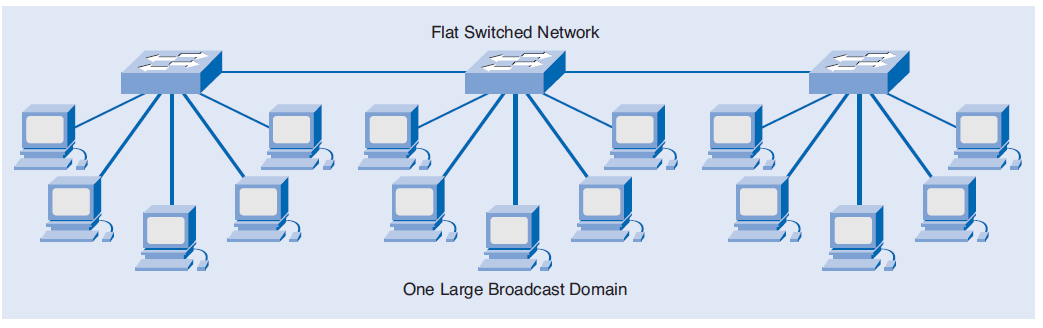


Fig 2.2: flat network design

**2.1.4 Characteristic of a network architectures**

Networks must support a wide range of applications and services, as well as operate over many different types of physical infrastructures. The term network architecture, in this context, refers to both the technologies that support the infrastructure and the programmed services and protocols that move the messages across that infrastructure. Thus, there are some basic characteristics that underlying architectures need to address in order to meet user expectations this include:

* *Scalability*: Scalable network designs can grow to include new user groups and remote sites and can support new applications without impacting the level of service delivered to existing users
* *Fault Tolerance:*A fault tolerant network is one that limits the impact of a hardware or software failure and can recover quickly when such a failure occurs. These networks depend on redundant links, or paths, between the source and destination of a message. Both the physical infrastructures and the logical processes that direct the messages through the network are designed to accommodate this redundancy.
* *Security:* Security is a feature that must be designed into the network, not added on after the network is complete. Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources.
* *Quality of Service (QoS):* Applications available to users over internetworks create higher expectations for the quality of the delivered services. Voice and live video transmissions require a level of consistent quality and uninterrupted delivery that was not necessary for traditional computer applications. Quality of these services is measured against the quality of experiencing the same audio or video presentation in person. Thus, new requirements to support this quality of service over a converged network are changing the way network architectures are designed and implemented.
* *Manageability:* No matter how good the initial network design is, the available network staff must be able to manage and support the network. A network that is too complex or difficult to maintain cannot function effectively and efficiently.

**2.1.5 Network Requirements**

Most businesses actually have only a few requirements for their network:

The network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions. The network should reliably deliver applications and provide reasonable response times from any host to any host. The network should be secure. It should protect the data that is transmitted over it and data stored on the devices that connect to it. The network should be easy to modify to adapt to network growth and general business changes. Because failures occasionally occur, troubleshooting should be easy. Finding and fixing a problem should not be too time-consuming.

**2.2 network threats, vulnerabilities and attacks**

When discussing network security, there are some common terms used to describe network breach this include:

**2.2.1 network threats**

*Network Threats:*A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. There are different categories of threats. There are natural threats,occurrences such as floods, earthquakes, and storms. There are also unintentional threats that are the result of accidents and stupidity. Finally, there are intentional threats that are the result of malicious intent. Each type of threat can be deadly to a network.

*Network Vulnerabilities***:** A vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat. Most vulnerabilities can usually be traced back to one of three sources:

* *Poor design:* Hardware and software systems that contain design flaws that can be exploited. In essence, the systems are created with security holes. An example of this type of vulnerability would be the "sendmail" flaws in early versions of Unix. The sendmail flaws allowed hackers to gain privileged "root" access to Unix systems. These flaws were exploited on numerous occasions.
* *Poor implementation:* Systems that are incorrectly configured, and therefore vulnerable to attack. This type of vulnerability usually results from inexperience, insufficient training, or sloppy work. An example of this type of vulnerability would be a system that does not have restricted-access privileges on critical executable files, thereby allowing these files to be altered by unauthorized users.
* *Poor management:* Inadequate procedures and insufficient checks and balances. Security measures cannot operate in a vacuum; they need to be documented and monitored. Even something as simple as the daily backup of a system needs to be verified.

**2.3.2 Network Attacks**

Unauthorized access can happen to an organization’s information or computer systems in many ways. Some of these could be done on purpose (maliciously) and others occur by accident. No matter why the event occurs, damage is done to the organization.

An attack is a specific technique used to exploit a vulnerability. For example, a threat could be a denial of service. A vulnerability is in the design of the operating system, and an attack could be a "ping of death." Attacks may occur through technical means (a vulnerability in a computer system) or they may occur through social engineering (non-technical means to gain unauthorized access). Regardless of whether there was malicious intent or not. Attacks on a network can be categorizes as:

* *Passive:*an attack is said to be passive when a network intruder intercepts data traveling through the network. some passive attacks included the following traffic analysis, Eavesdropping, Monitoring etc.
* *Active:* an attack is said to be active when an intruder initiates commands to disrupt the network's normal operation. Some active attacks include spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole etc.
* *Black hole attack:* Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it wants to intercept. A hacker uses the flooding based protocol for listing the request for a route from the initiator, then hacker create a reply message he has the shortest path to the receiver. As this message from the hacker reached to the initiator before the reply from the actual node, then initiator wills consider that, it is the shortest path to the receiver. So that a malicious fake route is create.

**2.2.3 Common network security vulnerability and attack**

When discussing network security, they common terms used are vulnerability and attack. Vulnerability is a weakness, which is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves*.* There are three primary vulnerabilities or weaknesses:

1. Technology weaknesses
2. Configuration weaknesses
3. Security policy weaknesses

*Technological Weaknesses*: Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

*Configuration Weaknesses*: Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate. Some common configuration weaknesses are listed in Table 2.0.

Table: 2.0 configuration weakness

|  |  |
| --- | --- |
| **Weakness** | **How the weakness is exploited** |
| Unsecured user accounts | User account information may be transmitted insecurely across the network exposing usernames and password to snoopers |
| Misconfigured internet services | A common problem is to turn on javascript in web browser enabling attacks by way of hostile javascript when accessing untrusted sites, IIS, FTP, and terminal services also pose problem |
| Unsecured default setting within products | Many products have default settings that enable security holes |

*Sources: (Design and Implementation of a Network Security Model for Cooperative Network, 2009)*

*Security Policy Weaknesses*: Security policy weaknesses can create unforeseen security threats. The network may pose security risks to the network if users do not follow the security policy. Some common Security Policy Weaknesses are listed in table 2.1 Threats are the people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses. Finally, the threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices.

Table: 2.1: security policies weakness

|  |  |
| --- | --- |
| **Weakness** | **How the weakness is exploited** |
| Lack of written security policy | An unwritten policy cannot be consistently or enforced. |
| Lack of continuity | Frequent replacement of personnel can lead to an erratic approach to security |
| Logic access control not applied | Poorly chosen, easily cracked or default password can allow unauthorized access to the network. |
| Software and hardware installation and change do not follow policy | Unauthorized changes to network topology or installation of unapproved application create security holes |
| Disaster recovery plan is non-existent | The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when someone attacks the enterprise |

*Sources: (Design and Implementation of a Network Security Model for Cooperative Network, 2009)*

*Common daily attack network:*As the LAN, WLAN and WAN networks are used for researches also the network administrator at each level of this network try to control the resources and information that transverse in the network. Thus, here will discuss on some of the common security issues suffered by network administrators on a daily basis:

* *Viruses:* A virus, a parasitic program that cannot function independently, is a program or code fragment that is self-propagating. A virus is usually spread by executing an infected program or by sending an infected file to someone else, usually in the form of an e-mail attachment.
* *Trojan Horses:* A Trojan horse is a program or code fragment that hides within another program or disguises itself as a legitimate program. The Trojan horse program functions much the same way as the legitimate program, but usually it also performs some other function, such as recording sensitive information or providing a trap door. An example would be a *password grabber* program.
* *Port Scanning*: One of the tools that hackers often use for this type of reconnaissance is a port scanner. A port scanner is a program that listens to well-known port numbers to detect services running on a system that can be exploited to break into the system.
* *Spoofs:* Spoofs cover a broad category of threats. In general terms, a spoof entails falsifying one's identity or masquerading as some other individual or entity to gain access to a system or network or to gain information for some other unauthorized purpose. There are many different kinds of spoofs, including, among many others, IP address spoofing, session highjacking, domain name service (DNS) spoofing, sequence number spoofing, and replay attacks.
* *DNS Poisoning:*Another method that can be used to launch this attack is to compromise a DNS server. One method for doing so is known as DNS poisoning. DNS poisoning exploits a vulnerability in early versions of the Berkeley Internet Name Daemon (BIND). BIND, the most commonly deployed DNS software on the Internet, was developed for BSD UNIX.
* *Password Cracking:*Password cracking is sometimes called a dictionary-based attack. Password crackers are programs that decipher password files. They are able to decipher password files by utilizing the same algorithm used to create the encrypted password.
* *Sniffing:*Network sniffing or packet sniffing is the process of monitoring a network in an attempt to gather information that may be useful in an attack. With the proper tools a hacker can monitor the network packets to obtain passwords or IP addresses.
* *Denial of Service:*Denial-of-service attacks are designed to shut down or render inoperable a system or network. The goal of the denial-of-service attack is not to gain access or information but to make a network or system unavailable for use by other users. It is called a denial-of-service attack, because the end result is to deny legitimate users access to network services.

**2.3 Network Security solutions**

Network security is important for the protection company assets. Thus; network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies.

Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on a network. a simple definition for information security: Information security = confidentiality + integrity + availability + authentication

Thus, we will be looking at what network security is, it’s characteristic and how-to setup a good and secured network. (John E., 2001)

**2.3.1 network security**

network security deal with the protection of information on network from un-authorized users (i.e. insuring confidentiality, integrity, and accessibility of such information to authorized user). Thus, network security is a mind-set of examining the threats and vulnerabilities of an organization and managing them appropriately.

securing any information on a network, either by a cooperative or government there is no laid-down procedure for designing a secure network. Thus, Network security has to be designed to fit the needs of one organization network and not anyone else’s *(MS-ISAC, 2010).*

*Network security tools operation:* Network security combines multiple layers of defences at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats. Hence network security consists of the following tools which include: Access control, Antivirus and antimalware software, application security, behavioural analytics, intrusion prevention system, mobile device system, vpn etc.

*Characteristics of a network security:* network security is being characterized by procedures and policies that protect information from accidents, incompetence, and natural disasters. Such policies and procedures characterized a network security. Hence, there can be no information security without

*Confidentiality*: this ensures that unauthorized users do not intercept, copy, or replicate information. At the same time,

*Integrity*: this is necessary so that organizations have enough confidence in the accuracy of the information to act upon it. Moreover, information security requires organizations to be able to retrieve data; security measures are worthless if organizations cannot gain access to the vital information they need to operate when they need it.

*Authentication*: information is not secure without authentication determining whether the end user is authorized to have access etc.

**2.3.2 Importance of security**

*In cooperation:* Computers control functions at many utilities including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas network

Today, cooperate networks require access to the internet and public networks. It’s common for cooperate network to have several access points to public and other private networks. Thus, securing open network of such is extremely important.

For the survival of many business, it’s necessary to allow open access to network resources and to ensure that data and resource are secured as possible. The internet has created an enabling environment for companies and cooperatives to build stronger relationship with customers, suppliers, partners, employees, etc. thus, this relationship require a mission-critical network that can accommodate the ever-increasing constituencies as well as the ever-increasing demands on capacity and performance. These networks also need to process voice, video and data traffic as network coverage into multiservice environment.

*in higher institution of learning:* In today’s computing environment, protection of intellectual property and data, including research data, clinical data, and business and personal information is paramount for administrators of higher education institutions.

Thus; Academic environments must protect their communications infrastructures from a growing number of threats that include viruses, worms, information theft, and data sabotage.

A higher education institution’s network has become a critical resource that supports education, research, administrative services, and campus communications. Faculty, students, and staff depend on the reliability and capability of this network and on the associated applications, data resources, services, and online communities of colleagues for much of what they do. Maximum network reliability has become mandatory. *(cisco-inshedi, 2004)*

**2.3.3 LAN/WAN network Security**

Threats will continue to be a major issue in the global world network as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with these attacks. This include the following:

*Controlling End User Access:* Creating an account and assigning a password are only small parts of giving someone access to the network. A network administrator also has to determine other account parameters such as when an end user can access the network, what groups the user is associated with, what files he or she can access, and limitations on network and server resources.

*Restrictions to Location or Workstation:* Consideration should be given to restricting, to a specific workstation, end users who are authorized to enter sensitive transactions or who perform particularly sensitive and/or confidential work. It is preferable to locate the station in a restricted area. Obviously, access to the server itself should be restricted to the LAN administrator and his/her backup.

*Time/Day Restrictions:* Consideration should be given to restricting end user access to business hours only, especially for those employees who are authorized to access and use sensitive and/or confidential data. If an employee does not normally work in the evenings and on the weekends, then the ability to access the network should be restricted for that time period. Most every operating system and NOS has the capability to restrict an account's access to specific time periods.

*Remove Inactive Accounts:* Organizations should review network user accounts on a regular basis and delete any accounts that are no longer required. Accounts for users or employees no longer with the organization should be deleted. Firms should also delete inactive accounts, removing or disabling username accounts that have not been accessed in the last three to six months. Hackers frequently try to exploit inactive accounts for the initial break into a system or as a means to gain access to a network again.

*Segmenting LAN Traffic:* Network segmentation is a process of separating a large network into several smaller networks. This can be accomplished by grouping associated users together on a hub or similar network device. A hub is a network device with multiple ports into which other network devices are plugged. Whenever possible, organizations should segment their networks for both security and performance purposes. Segmenting networks prevents packets from traversing the entire network.\

*Secure Socket Layer (SSL):* is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel

* + 1. **Risks Assessment, Policies**

*Risk assessment:* The concept of risk assessment is crucial to developing proportionate defences. To perform a risk analysis, organizations need to understand possible threats and vulnerabilities. Risk is the probability that a vulnerability will be exploited. The basic steps for risk assessment are listed as follows: Identifying and prioritizing assets; Identifying vulnerabilities; Identifying threats and their probabilities; Identifying countermeasures; Developing a cost benefit analysis; Developing security policies and procedures.

Furthermore, assigning a threat rating to each portion of a network and apply an appropriate level of security is helpful to maintain a workable balance between security and required network access. Assign each network resource one of the following three risk levels:

*Low Risk*: Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.

*Medium Risk:*Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.

*High Risk:* Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems. Once you've assigned a risk level, it's necessary to identify the types of users of that system. The five most common types of users are:

* *Administrators*: Internal users responsible for network resources.
* *Privileged:* Internal users with a need for greater access.
* *Users*: Internal users with general access.
* *Partners:* External users with a need to access some resources.
* *Others*: External users or customers.

table 2:3 risk assessment table

|  |  |  |  |
| --- | --- | --- | --- |
| **System** | **Description** | **Risk level** | **Type of users** |
| Network routers | Distribution network device | High | Administrators for Device configuration (support staff only); All others for use as a transport |
| Closet switches | Access network  Device | Medium | Administrators for device configuration (support staff only); All others for use as a transport |
| Firewall | Access network  Device | High | Administrators for device configuration (support staff only); All others for use as a transport |
| Internal e−mail server | Network  Application | Medium | Administrators for Configuration; All other |
| DNS and DHCP servers | Network  Applications | Medium | Administrators for configuration; General and privileged users for use |

*Sources: (Network Security Policy: Best Practices White Paper, 2005)*

*Network security policies:* this can be thought of as the documents that spell out the *what* and *why* of information security for an organization. There are various reasons for an organization to develop network and system security policies and procedures. Some are obvious, while others are not so obvious. Some reasons concern the direct benefit that an organization gains from having policies and procedures, such as preventing or detecting fraud or deterring hackers. Other benefits are indirect in that the policies protect the organization from potential liability or save it from possible embarrassment.

Furthermore, network security policy design must be in accordance with organization laydown polices. Thus, it’s design so as to meet some of the objectives generally associated with network security policies, this include managing risk, ensuring business continuity, Protecting the organization from liability, defining responsibilities, expectations, and acceptable behaviours ensuring information integrity and confidentiality etc.

**2.3.5 Network Security Model**

There are different approaches used to develop a network security model. Usually, organizations employ some combination of this approaches to achieve security. These approaches include: security by obscurity, the perimeter defence model, and the defence in depth model, Open Access Security Model, Closed Access Security Model.

*Security by Obscurity:* The concept behind this model is that if no one knows that a network or system is there, then it won't be subject to attack. The basic hope is that hiding a network or at least not advertising its existence will serve as sufficient security.

The problem with this approach is that it never works in the long term, and once detected, a network is completely vulnerable.

*The Perimeter Defence:*The perimeter defence model is analogous to a castle surrounded by a moat. When using this model in network security, organizations harden or strengthen perimeter systems and border routers, or an organization might "hide" its network behind a firewall that separates the protected network from an untrusted network. Not much is done to secure the other systems on the network.

The assumption is that perimeter defences are sufficient to stop any intruders so that the internal systems will be secure. There are several flaws in this concept: First, this model does nothing to protect internal systems from an inside attack. Second, the perimeter defence almost always fails eventually. Once it does, the internal systems are left wide open to attack.

*The Defence in Depth:*The most robust approach to use is the defence in depth model. The defence in depth approach strives for security by hardening and monitoring each system; each system is an island that defends itself. Extra measures are still taken on the perimeter systems, but the security of the internal network does not rest solely on the perimeter systems.

This approach is more difficult to achieve and requires that all systems and network administrators do their part.

*Open Access Security Model*: this model assumes that the protected assets are minimal, users are trusted, and threats are minimal. This type of network security design gives users free access to all areas. When security breaches occur, they are likely to result in great damage and loss.

*Closed Access Security Model:* closed model assumes that the protected assets are premium, all users are not trustworthy, and that threats are frequent. User access is difficult and cumbersome; furthermore, this model also requires that network security departments must clarify that they only implement the policy, which is designed, written, and approved by the corporation

**2.4 Characteristics of Network Security**

Network security has some fundamental important features that are really helpful for the protection of the confidential data from leaking and also help to protect from hacking. Some important characteristics of the information security are as follows

* 1. Integrity and Confidentiality
  2. Authentication and Management of Risk

**2.4.1 Network security architecture**

*Prevention:*The foundation of security is prevention. To provide some level of security, it is necessary to implement measures to prevent the exploitation of vulnerabilities. In developing network security schemes, organizations should emphasize preventative measures over detection and response. Remember that it is impossible to devise a security scheme that will prevent all vulnerabilities from being exploited, but companies should ensure that their preventative measures are strong enough to discourage potential criminals-so they go to an easier target.

*Detection:*Once preventative measures are implemented, procedures need to be put in place to detect potential problems or security breaches, in the event preventative measures fail. The sooner a problem is detected the easier it is to correct and cleanup.

*Response:*Organizations need to develop a plan that identifies the appropriate response to a security breach. The plan should be in writing and should identify who is responsible for what actions and the varying responses and levels of escalation. Thus; network security is not a technical problem; it is a business and people problem. The technology is the easy part. The difficult part is developing a security plan that fits the organization's business operation and getting people to comply with the plan.

**2.4.2 Why security is not a point product but a process**

Obviously, we cannot just rely on a single type of security to provide protection to an organization’s information. Likewise, we cannot rely on a single product to provide all of the necessary security for our computer and network systems. Unfortunately, some vendors (in their zeal to sell their products) have implied that such was actually true *(Eric Maiwald, 2001).* The reality of the situation is that no one product will provide total security for an organization. Many different products and types of products are necessary to fully protect an organization’s information assets. Thus, some of this product include anti-virus software, access control, firewall, intrusion dictation, policy management, encryption, etc.

**2.4.3 Benefit of network security**

As we know that network security plays a very important role in defending the information from different types of disclosure. There, it has several benefits that really encourage us to use information security technology. One of the big and the major advantage of the information security is that it can take steps to prevent different tope of data from leakage and increase the reliability of the information. Another benefit of the information security is that it can increase the confidentiality of a document.

**2.5 Conclusion**

Computer and networking have brought considerable change in capacity and globality for accessing and using information as well as communication, both of which have impacted on world and different institution such as the Education, cooperate world etc. positively. Thus, this advancement is described based on the devices used or based on content or services provided by this technology. However, this chapter has laid the necessary background to network and information security, thus given us the key issue in security such that it not just a point product but it a process that keep going because no design or model is good enough to solve the problem it can only minimized the rate of occurrence and time taking for it to occur but in most cases, it will occur. Hence from the chapter also we see that if good policies and risk measures are properly taken it will help in mitigating some of this cyber and network security challenge. So, in the next chapter we will see the difference existing model and it requirement and how to design a better model for such a network. Thus, taking university of Jos network security as case study.

**Chapter 3: Proposed Solution**

**3.0 Introduction**

The previous chapter has formed the foundation of knowledge, needed to fully understand this research. Now taking a proper look into the problem statement defined earlier, “There is need for improvement in the network security, policies design and implementation in University of Jos (main-campus) network”. Thus; based on what has been discussed in the previous chapter, the importance of a good network security cannot be over emphasis; especially in an academic environment like University of Jos.

The purpose of this chapter is to determine design methodology of the network of the school particularly main campus Bauchi road, it security state and the level of policy implementation on the network. Hence; the chapter will look at how the sample data will be collected and evaluated after which results will be given.

**3.1 Data Collection**

A research work being carried out will usually dictate the kinds of research methodologies to be employed in order to collect data. Two types of research methods exist: qualitative and quantitative. (Sheldon, 2014) explains that qualitative research is an in-depth exploration of what people think, feel or do and why - intangibles. On the other hand, he says that quantitative research provides a measure of how many people think, feel or behave in a certain way and uses statistical analysis to determine the results. So, apparently, qualitative is about people and quantitative is about numbers.

It is worthwhile to note that any method employed can give us quantitative data which is used to measure variables and verify existing theories or hypotheses or to question them. The data is then used to generate new hypotheses based on the results of data collected about the different variables.

For the purpose of this research, a survey will be taken for qualitative data gathering through interview, and documentation. The following sub-sections will take a look at the specifics interview and the process that was followed in gathering responses from respondents.

**3.1.1 Population of the Study**

The study population is made up of some principal staff in charge of the network of university of Jos. Undoubtedly, these staff are familiar with the system and especially the University network design and it security. Hence, constituting the most preferred population of interest.

**3.1.2 sampling and Instrument Design**

During the process of sampling; respondents were carefully selected from the members of the technical staff. Thus, the inclusion criterion for respondents, is that he/she must be member of the ICT network staff. Hence, an interview can be seen as a formal meeting at which someone is asking questions in order to find out if something is suitable or not; thus, it can say to be structured, semi-structured or un-structured.

In this research, one on one conversation with some member of the ICT staff was made, of which responses were made by each one of them thus the questions are structured such that:

Firstly, it concerned with the network design model. Thus, the question is aimed at determining the network design module and how it operate and also the various disaster prevention mechanism and also it connection to the internet service providers and the kind of resources/service on the network.

Secondly, is focused at understand whether or not there exist a security policy that govern the network resources usage also looking also at the kind of security implemented so far on the network. Furthermore, it also takes note of the risk management policy on the network.

Thirdly, it tries to investigate the various challenges (i.e. both security and network in general) face by the network administrators and member of staff. Which include security policy, security mechanism deployed on the network, utilization of the network resources (bandwidth) etc.

Here are some of the sample question used and the various responses:

1. what kind of network design model is the network running on?
2. What are the different kind of resources that can be found within the intranet.
3. How is the network connected to the internet?
4. What are the risk and disaster recovery plans for the network?
5. What are the security policy?
6. What are the different challenges encounter with the network.
7. What kind of design and security model will you like to be implemented on the network

From the interview carried out among approximately three to four members of staff, the following responses were gotten:

* Concerning network design model; one of the responder said that the network was using flat model before the current upgrade to a hierarchal model design reason was due to the increase in the school population and also for flexibility in managing the network. And the network runs from the main campus to the naraguta campus.
* Concerning the intranet resources some of the respondent said that there are no intranet resources within the school (i.e. resources like mail servers, ftp servers, internal application service servers etc.), must of the resources are hosted in the cloud. Thus, the school only provide internet services to it users.
* Concerning the internet connection, the school is connected the internet via the internet service provider using STM1 line that run 155mb/sec. the connection to the internet services provider is at the main campus.
* Risk assessment and disaster recovery plans, one of the respondent said that in terms of fire disaster management, a modern fire alarm system (fm-200) has been install and more so, its running an auto backup recovery procedure between the two campuses and also in the cloud.
* Security policy and implementation, some of the respondent said that basically there are no policy documentation, that guide the implementation any policy on the network. But so far it has been implementation without any confidential documentation that guide such policies.
* Challenges within the network, some of the respondent said that the key issue facing the network is the used of unlicensed software been used in the network, and also no documented policy that guide the implementation of policy on the network, furthermore, some the respondent said that some other challenges include include user challenges (i.e. users not oriented to the various network resources such as e-library for the school), technical staff challenge (i.e. lack of man power and also introduction of new device into the network that will require more knowledge to handle), and administration challenge (i.e. lack of policy implementation and release of funds).
* Concerning views of the various respondent a new network model and security design; some respondents, want the network to be able monitor and block unlicensed software, protection of users, provide a productive network for academic research rather than social chart with unnecessary download of firms and large files. Block of some site, quality traffic control, and also having some monitoring device to check activities on the network. In general, also have a system that will control usage of different devices in the network, and having a documented policy that will guide the implementation of any policy or rules on the network.

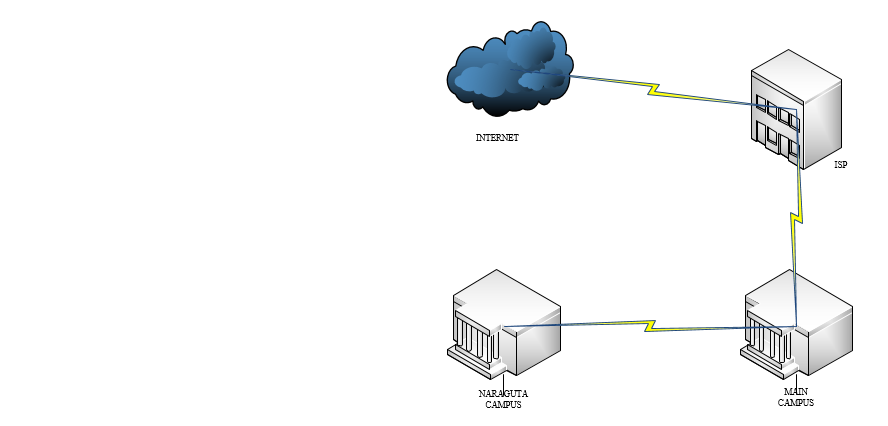
**3.2 Findings**

From the previous section, the result from the interview and some documentation gotten has led to several key findings. Looking at what was set out at the start, these findings will be unveiled subsequently.

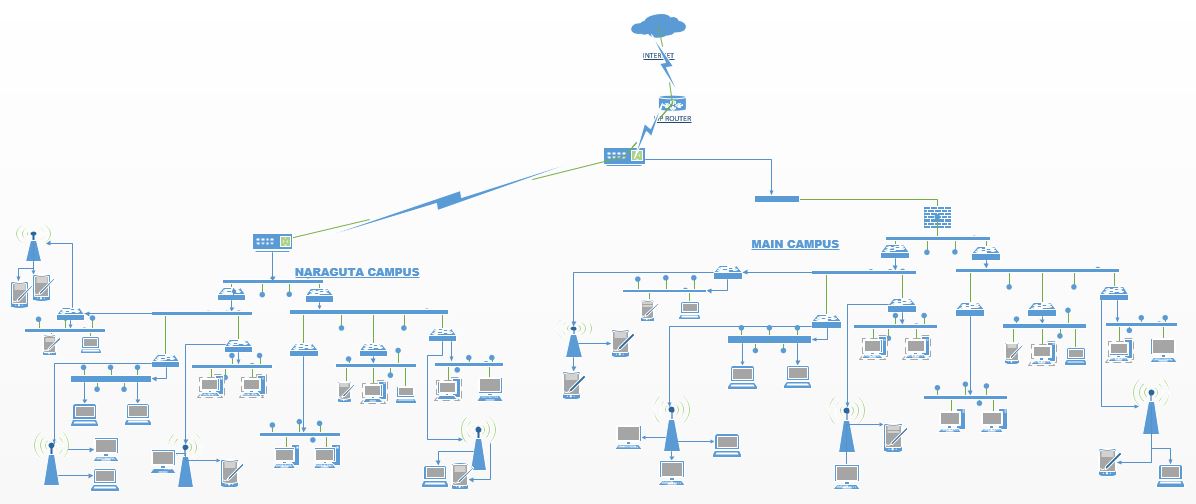
**3.2.1 Network Layout and Design Model:** Looking at the first part of the question which focus on the network design model. It was discovered that the network primarily was build on a flat design model. Thus, the design model seems not suitable and reliable due to increase in student, network user, more computer connecting device, student computer labs extinction, with huge bandwidth investment, erratic and poor internet connectivity and control.

Recently due to the increase in network users ranging from student to staff, it has been changed to a hierarchical design model with connection running between main and naraguta campus, and a connection to the internet service providers from main campus. In terms of resources within the network such as web application, database and email servers etc., they are hosted externally on the cloud (i.e. network cloud), with only internet services running within the campus; this was due to the incident that happen some year back.

The network model design on ground: with this new development on the network, thus the network hence; the network consists of WLAN, LAN and a WAN. For the network WLAN it consists of access-point at the end point for user. For the LAN it consists of switches, patch panels, cables (cat 5). For the WAN, this wan can be seen as a MAN network that runs between the two campuses of the school (i.e. from main campus to naraguta campus) it resources consist of routers, wan cables (fibre). And a connection to the ISP using a boarder gateway protocol. Below is a design of the network between the two campuses.



*Fig 3.0: school network layout*

*Fig 3.1: detailed network design of the school*

**3.2.2 Network Security Design and Policy Implementation:** Secondly, in terms of security design and policy implementation from the finding made, there is virtually no security policies for the network optimisation. Due to Poor administrative control and management; thus, this poor policy implementation has led to a high security risk causing massive virus ridden on the network. Furthermore, causing huge bandwidth investment with poor internet connectivity and control. But at the time of compiling this report, some important policies have been put in place such as bandwidth consumption rate to monitor in the network and also a recovery system for the network.

**3.2.3 Challenges of the Existing System:** Thirdly, the issue of challenges faces on a day to day base, include user challenges (i.e. users not oriented to the various network resources such as e-library for the school), technical staff challenge (i.e. lack of man power and also introduction of new device into the network that will require more knowledge to handle), and administration challenge (i.e. lack of policy implementation and release of funds). Furthermore, no ICT or security policy to form legal framework and upgrade policy, used of unlicensed software, and network abuse by users which include:

*Service disruption*: Disruption of the administrative infrastructure and learning resources such as computer labs caused by botnets, worms, malware, adware, spyware, viruses, DoS attacks.

*Harmful or inappropriate content*: Pornography, adult, aggressive, offensive and other type of content that could put the physical and psychological well-being of minors at risk.

*Network abuse:* Peer-to-peer file sharing and instant messaging abuse, use of non-approved applications by students, staff, and faculty.

*Unauthorized access*: Intrusions, unauthorized users, escalation of privileges, and unauthorized access to learning and administrative resources.

General form the research and survey made thus far some staff are of the opinion that security policy should form legal framework and upgrade policy so as to enable proper implementation of security policy and also the monitoring of the network for software legitimacy. Furthermore, some are also of the opinion orientation should be made to student on the different functional and resources available locally within the school and also outside.

**3.3 Proposed solution**

From the find made so far is has shown that the ICT unijos need serious improvement in terms of security policy implementation and security implementation. So, in line with that these new model prototype is to model a hieratical network design model with a defence in depth security model.

The hieratical network model helps in enable easy expansion of network, easy troubleshooting of network, and also reliability of network. while the defence in depth design models will improve the level of security on the network and help in checking and keeping track of users on the network and what they are doing. Also, the new proposed model should be able to check the legitimacy of application that are on the network so as to ensure more reliable security.

**3.4 Conclusion**

This chapter has investigated by means of one on one conversation survey which gathers the opinion some staffs regarding certain behaviors the network and it security design. These findings will serve as a basis constructing the model of the prototype to address the problem stated at the start of this research. Chapter 4 will present this model and will go further to implement the prototype.

**CHAPTER 4: Design and Implementation**

**4.0 Introduction**

The previous chapter discussed on the survey and finding from the field from different participant; of which from the survey and finding thus far, one could see that there exists a correlation between the stated problem in the early chapters. The findings have established that the chosen population would welcome desire improvement on the network security so as the enable them control the traffic, minimized cost, and ensure reliability of network to users and most importantly promote research and intellectual enhancement within the school.

This chapter will discuss the prosed solution to the identified problem which is poor network security design and implementation. However, the proposed solution will only serve as a proof of concept to further the cause of a good security model and policy implementation. Thus, starting with the highlight of requirements of the system, design, and implementation. At the end, solution model will be given to illustrate how the proposed solution would work.

**4.1 Requirement Specification**

Every system need to provide some service; hence this prototype was implemented base on a hieratical network model design architecture that enhances and enforces scalability of network and also a defence in depth security model to ensure confidentiality, and promote quality research work within the institution. thus, to implement this system a simulator (cisco packet tracer) was used which consist of the following: router (1941, 2620xm, 2911,1891), switch (2960, 2560-24ps), firewall (ASA 5505), sniffer, servers, PC, wireless access point, wireless end device and the finding in chapter 3 were also used to come up with the network security model requirement.

*Cisco packet tracer*: Packet Tracer is a simulator, for visualization, collaboration, and assessment tool for teaching networking, allowing users to experiment with network behavior, build models. Packet Tracer is based on three learning principles: learning is active, learning is social, and learning is contextual. Thus; this simulator is general give a platform for the design and simulation of the new system.

Furthermore, this system consists of the WLAN, LAN and WAN (i.e. MAN) of which all of them have their own. Component thus this include:

**Local Area Network Requirement (LAN) and Wireless LAN:** a LAN network as mention in the previous chapter consist of switches, personal computer, printers, cabling, and basically is a network that span within an office, small area. A hierarchical design model, as stated in the previous chapter, has some key factor in it that make it flexible and scalability, that’s its ability to arrange the LAN network into layer which include access layer, distribution layer, and the core:

An Access layer of a network is way the end user is sited, that is way the pc, wireless end devices and small switches are located while the distribution layer also consist of switches, but with some redundancy capabilities in it. While the core layer is the layer were the core device that hold the network together layer this include layer three devices, the servicers, the switches, sniffers and routers are. So, for this design the following were used within the LAN network:

*Switches:* switches unlike router are used by default to break up collision domain but enabling broadcast domain and enable switching of frames from one port to another within the switched network. Thus; they’re employed to add functionality to a network LAN. The main purpose of a switch is to make a LAN work better by optimizing its performance providing more bandwidth for the LAN’s users. So, for this project am used the 2960, 2560-24ps switches.

*Adaptive Security Appliance (ASA):*A firewall is in essence a portal through which information enters and exits. On one side of the portal is the internal network that must remain secure, and on the other is the information needed from the outside world combined with the undesirable threats of external networks. Thus, for the project the 5505 ASA model was used.

*Sniffer:* this an end device or application that is used to monitor traffic flow and packets within a network.

*Wireless Access Points*: An access point is modeled as a repeater with one wireless port and one Ethernet port. In the settings for the wireless port, you can toggle the **Port Status**, set the **SSID**, **Channel**, and **Authentication**.

*Personal computers (PC):* this is an end point device that a user uses to access the internet, thus it can be a computer system, a phone, etc.

*Server:* this is a system that used to provide service to the end users in terms of web services, email services, etc. thus this server are seen as the critical area of any network because it houses tons of information about the organization, it staffs, and confidential resources of a company.

**Wide Area Network Requirement:** a WAN network as mentioned in the previous chapter is a network that span within a large region of area, which can be categories Metropolitan Area Network (i.e. a network that span within a city or small region like Jos etc.) regional Area network (i.e. a network that span within area large geographical area like between two country region) thus for such a network to be achievable some equipment are need which include the service provider, wan cabling, satellite, and routers. So, for this project work we will be using the routers, the internet service providers and also simulate the internet also.

*Service providers:* these are companies that come together to provide internet services to local network users. These services include application services, network services, internet services, management services, storage services etc. this companies can be group into three which include the tier 1 network service providers (this network service provider can be seen as the backbone for network service some of the provide at this level include AT&T United State, Global Telecom and Technology etc.). tier 2 network service providers (this network service provider tap from the tier 1 some of this company include cogent communication united stated, hurricane electric etc.), tier 3 network service providers (this network services providers are seen as the local service provider that provide access to the local network user).

*Router:* routers this is a layer 3 device (switch) that uses logical addressing and provide what is called packet switching; and can also provide packet filtering by using access lists, and when routers connect two or more networks together and use logical addressing (IP or IPv6), this is called an internetwork. Thus, it uses a routing table (map of the internetwork) to make path selections and to forward packets to remote networks. routers are known for breaking up broadcast domains by default, it’s important to remember that they break up collision domains as well. Show in this project I make used the 1941, 2620xm, 2911 router series.

**4.1.2 Available operation:**

* Restrict management device access to authorized parties and for the authorized ports and protocols.
* Authorize actions and log all administrative access and display legal notification banners. Ensure confidentiality by using secure protocols like SSH and HTTPS.
* Enforce route filters to ensure that only legitimate networks are advertised, and networks that are not supposed to be propagated are never advertised. Also Uses access control lists (ACLs) to control resource access by users on the network.
* Implement a hierarchical design, segmenting the LAN into multiple IP subnets and VLANS to reduce the size of broadcast domains.
* Disable VLAN dynamic trunk negotiation on user ports and disable unused ports and put them into an unused VLAN and also Implement port security, Dynamic ARP Inspection, and DHCP snooping.
* Use a dedicated VLAN ID for all trunk port with an explicitly configure trunk on infrastructure ports.
* Provide secure in-band management access for systems residing at the institution sites by deploying firewalls and ACLs to enforce access controls, using Network Address Translation (NAT) to hide management addresses, and use secure protocols like SSH and HTTPS; and so on.

**4.1.2 Functional Requirement**

* The system shall allow specific traffic to the server on the network through the used DMZ within the network.
* The system shall allow VLAN within the network to segment the LAN into multiple IP subnets or VLANS to reduce the size of broadcast domains.
* The system shall control DNS remoted access
* They system shall keep track of packets coming in and going out of the network.
* The system shall keep a syslog of all band traffic that access the network.
* The system shall enable password and port security on router and switches
* System shall control user access to various resource on the network locally and on the internet

**4.1.3 Non-Functional Requirements**

* Service availability and resiliency
* Prevent unauthorized access, network abuse, intrusions, data leak, and fraud
* Ensure data confidentiality, integrity, and availability
* Ensure user segmentation and also enforce access control
* Protect the endpoints infrastructural devices etc.

**2.2 System Design**

For any good network security design model to be implemented in a network it must have a blueprint (i.e. a layout structured) that define it such policy design and implementation; thus, this policy must be design according to the organization policies. Hence, for a good network security policy there are some key things that must be put in place (i.e. network resources/assets). Here is a sample blueprint procedure:

**2.2.1 Network Security Policy Design Template**

network security policy design, it can be categories in terms of: preparation, prevention, and response.

***Preparation:*** this deals with setting up of the necessary policy statements, risk assessment thus, in general setting up a security policy structure. Prior to implementing a security policy, you must do the following:Create usage policy statements, conduct a risk analysis, establish a security team structure.

* *Create Usage Policy Statements:* this provides the general user community with an understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities.
* *Conduct a Risk Analysis:* this identify the risks within a network, network resources, and data. The intent of a risk analysis is to identify portions of a network, assign a threat rating to each portion, and apply an appropriate level of security. Assign a risk level to each of the following: core network devices, distribution network devices, access network devices, network security devices, e-mail systems, network file servers etc.
* *Establish a Security Team Structure:* this deals with the Creation of a cross−functional security team led by a Security Manager with participants from each of your company's operational areas. The security team has three areas of responsibilities: policy development, practice, and response.

***Prevention*:** this deals with the prevention of this network devices as mention earlier, thus; Prevention can be broken into two parts: approving security changes and monitoring security of a network.

* *Approving Security Changes:* can be seen as changes to network equipment that have a possible impact on the overall security of the network.
* *Monitoring Security:*Security monitoring is similar to network monitoring, except it focuses on detecting changes in the network that indicate a security violation.

***Response:*** Response can be broken into three parts: security violations, restoration, and review.

* *Security Violations:* When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having these decisions made ahead of time makes responding to an intrusion much more manageable.
* *Restoration:* Restoration of normal network operations is the final goal of any security violation response. Define in the security policy how you conduct, secure, and make available normal backups.
* *Review:*The review process is the final effort in creating and maintaining a security policy. There are three things you'll need to review: policy, posture, and practice.

**2.2.2 policy design for the new system**

For this security implementation, from the sample shown above we define our own policy as follows:

*Risk assessment***:** From the above template: we group the users of the network into student, staffs (academic, non-academic) and technical staff as the users of the university of Jos network. For the resources of the network; we have internal and external servers, switches, routers, firewall, wireless devices, Risk assessment on this resource include:

Table 4.1: systems risk assessment rate level

|  |  |  |  |
| --- | --- | --- | --- |
| **System** | **Description** | **Risk level** | **Type of users** |
| Router | Core network device | High | Technical staffs for Device configuration (support staff only); All others for use as a transport |
| Switches | Access network  Device | Medium | Technical staff for device configuration (support staff only); All others for use as a transport |
| Firewall | Access network  Device | High | Administrators for device configuration (support staff only); All others for use as a transport |
| Internal server (ftp, email, internet) | Network  Application | Medium | Technical staff for Configuration; staffs for use |
| DNS and DHCP servers | Network  Applications | Medium | Technical staff for configuration; General and privileged users for use |
| Wireless devices | Access network  Device | Low | Technical staff for device configuration (support staff only); All others for use as a transport |

*Sources: (this project work, 2018)*

*Policy Creation:*

*Purpose:* The purpose of this policy is to secure and protect the information assets owned by university of Jos. university of Jos provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. university of Jos grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that all network infrastructure devices must satisfy to connect to university of Jos network. Only those network infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a university of Jos network

*Scope:* All student, staff, administrator must adhere to this policy. This policy applies to all network infrastructure devices that connect to university of Jos network or reside on university of Jos site that provide network connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of communication device capable of transmitting packet data.

Policy: *Requirements:*

All network infrastructure devices that reside at university of Jos site and connect to a university of Jos network, or provide access to information classified as university of Jos Confidential, or above must abide by the standards specified:

1. *Network requirement:*

Ensure that cabling, plugs and other wires are protected from foot traffic. And Having a UPS (Uninterruptible Power Supply).

Develop and maintain an asset control system that will keep records of all computing and networking equipment and software.

Check network configurations regularly; and maintain logs of all network transactions and review daily.

Backups should be automated and be performed nightly. At a minimum, a weekly incremental and a full monthly backup should be considered.

Backups should be tested to ensure that when needed, recovery could be performed.

Several generations of backups should be maintained with the latest copy kept on site and the others off-site.

The enable password on the router or switch must be kept in a secure encrypted form; thus, the router or switch must have the enable password set to the current production router/switch password.

Use approved authentication protocols and infrastructure, and encryption protocols.

Auditing software should be run periodically and compared to security policies and procedures for discrepancies. These should be corrected immediately

Periodic training of users on updates should be performed.

Not interfere with wireless access deployments maintained by other support organizations.

All wireless access point within the university are made student and All personal computer should be on the wireless access points.

Maintain a hardware address (MAC address) that can be registered and tracked.

1. *Internet requirement:*

General access to the Internet for recreational use through the university network is strictly limited to students, administrators and technical staff (hereafter referred to as “Authorized Users”).

Access to some site will be limited for staff and will only be allowed parodically, so as to enhance research and productivity.

Student are allowed full access to research site like public library, google library etc. with a youtube access for 70 magabyte download; and a total denial to social media and movie site.

Protect network from outside entities and also enable secure transmissions sent over the Internet.

1. *Security requirement:*

Servers should be in limited access locked rooms.

Passwords must not be shared. And for any password transmission, it should be encrypted and not transmitted in clear text format

Passwords should be a minimum of 6 alpha and numeric characters. And Password history should not be allowed.

local user accounts should be configured on the router as backup. But routers and switches must use TACACS+ for all user authentication.

Any breach to systems or the network should be investigated. And intruder alert facilities should be activated and all alerts should be acted on.

Users should be made aware of security policies and procedures. Especially of the consequences to violations of these policies.

Ensure that security related events are immediately posted and acted on in time; furthermore, record and report all network malfunctions and document it appropriately.

1. *Host requirement:*

Performance of illegal activities through the network by any user (Authorized or otherwise) is prohibited.

Personal equipment used to connect to the networks must meet with the acceptable required standard as stated in the Hardware, software and product licensing for Accessing the Networks.

Terminal workstations (computer systems) will be installed and maintained by an approved support operating system for all member of staffs.

All unauthorized copies of software should be removed from computers.

Policy: *The following services must be configured:*

* Password-encryption and all routing updates shall be done using secure routing updates.
* Access control lists must be used to limit the source and type of traffic that can terminate on the device itself. And with Network segmentation
* The router must be included in the corporate enterprise management system with a designated point of contact.
* Each router must have the following statement presented for all forms of login whether remote or local:
* *"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. "*
* Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
* The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

1. IP access list accounting
2. Device logging
3. Packet filtering at the router level
4. Router console and modem access must be restricted by additional security controls

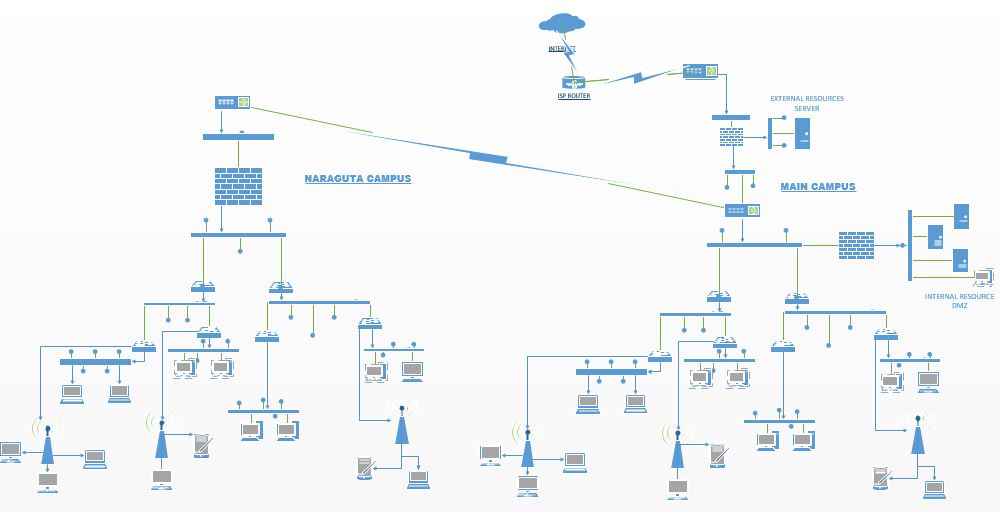
Policy Compliance: *Compliance Measurement*

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, packet monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Policy: *Exceptions:* Any exception to the policy must be approved by the Infosec team in advance.

Policy: *Non-Compliance:*Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, blocking of such devices.

**2.2.3 System Model:** More so, using the above stated policy strategy we have the following design that will suite such as policy, as shown below:

*fig 4.1: new design layerout*

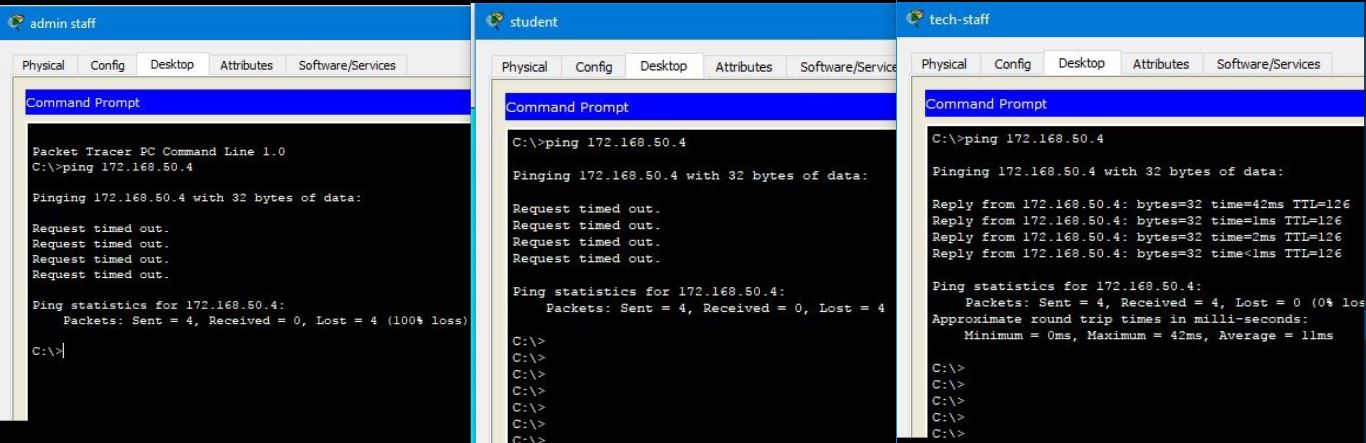
This will enable more robust network in term of security and protection of intellectual property of the school as well.

**4.3 System implementation operation**

The requirement and information obtained from the previous chapters has enable the design of a new prototype which is design to give an up to date security to the network with optimal performance and also enhance research and intellectual growth among student and staff. Thus, this implementation is carried out using cisco packet tracer 7.0 and here are some of the implementation which include:

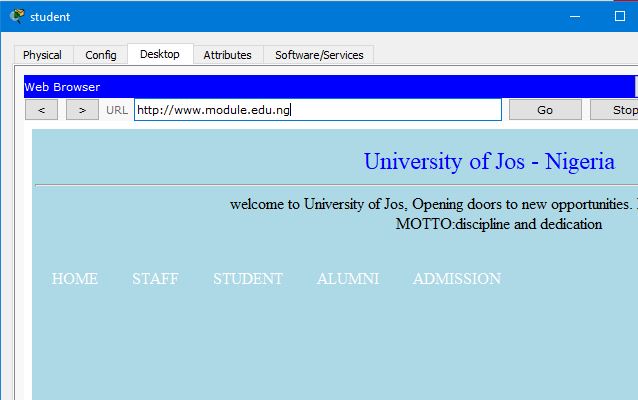
*Internal resources and traffic/protocol enable:*

For the existing system there is no internal resources (i.e. internal school servers for library works, local DNS-servers, email-servers etc.), but with the new system model it gives room for such resources and it been protected by a dmz (de-militarized zone) configuration that enable the following traffic/protocol to pass through which include:

*Ping traffic/icmp protocol:* the ping/icmp protocol is mostly used by attackers to cause denial of service with what is now as ping of death thereby cause ligemated users access to the need resources, but it also used for testing connnectivity so with which only the technical staff are allow access to such protocol. Which enable them to run tested to these internal servers.

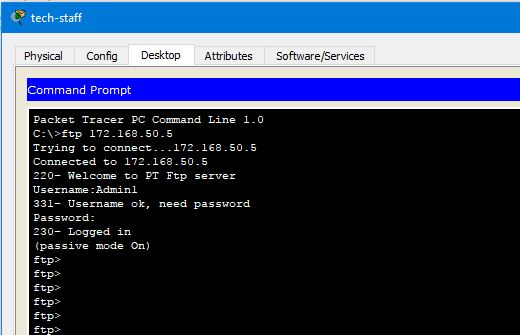
*Fig 4.2: ping to the dns-server by admin staff, student and tech-staff*

*Web traffic/www protocol:* This protocol/traffic operate at port 80 and 433 is enable to all users of the network; the server that has this traffic house on also have library material and student project that will enhance quality productivity among student and staff but the protocol.



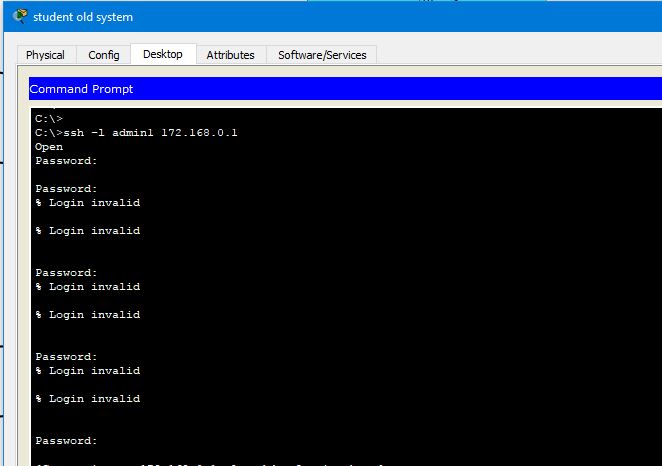
*Fig 4.3: Access to internal web server*

*File transfer protocol (ftp) traffic:* This protocol is used to enable transfer of files between users to servers as backup thus most of which are the system configuration (like routers, switches, firewall etc.) and some sensitive files that is only for confidential purpose only. So, for that only the technical staff are allowed access to this particular protocol.

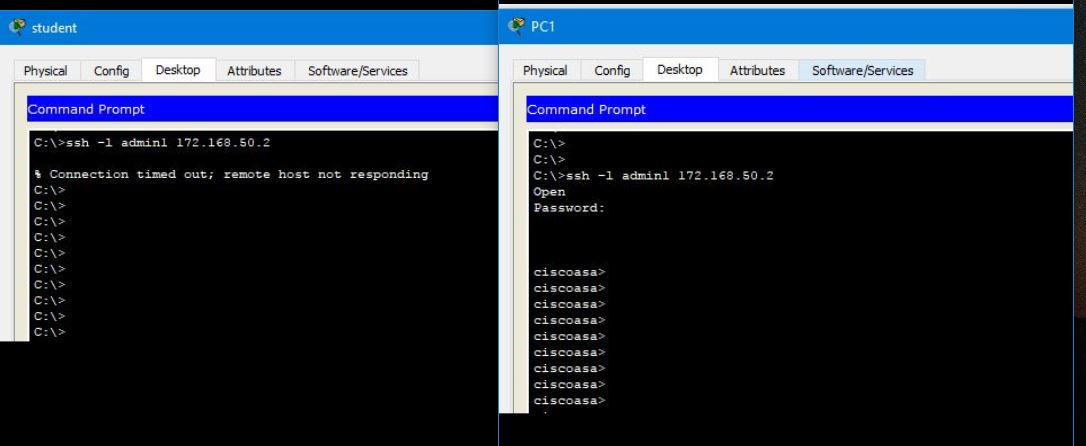


*Fig 4.4: ftp access by admin staff*

*Secured shell (ssh) traffic/protocol:* This protocol/ traffic is used to opened a secured connection over a remoted network to either remoted resources and devices on the network. For the old system design, anyone can have the ability to test the password and username of the remoted devices like routers and servers, this give the remoted devices a high chance of been brute force. For the new system design it only allow three members of the technical staff to be able to carry out ssh to remote devices and resources.

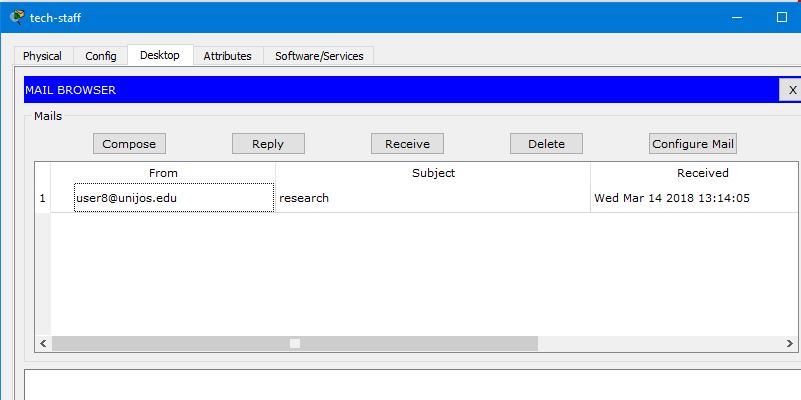


*Fig 4.5.1: ssh from the old system*



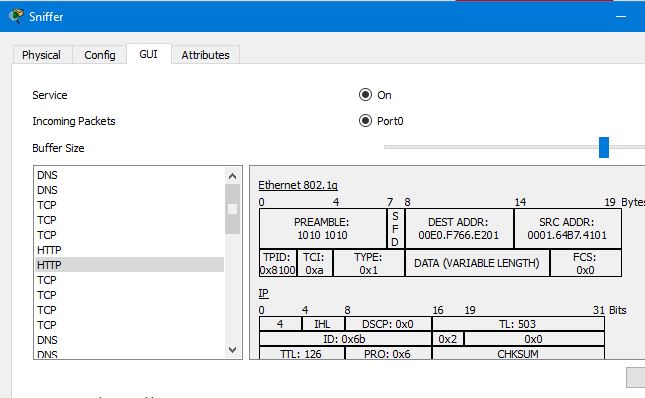
*Fig 4.5.2: ssh into device by student and tech-staff from new system model*

*Mail traffic/ smtp & pop3 protocol*: This protocol enables mail services between clients, but it requires a server. This protocol is only enable or members of staff only without the student. This enable staff to share resources and ideas on a particular research.



*Fig 4.6: mail transfer between users*

*Traffic monitoring:*



*Fig 4.7: monitoring of traffic into dmz zone*

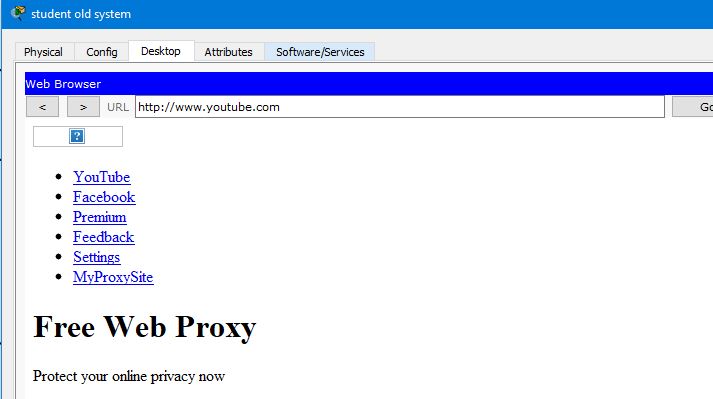
This above figure monitors all traffic going in and out of the internal dmz so as to ensure a real-time check of traffic

In general, all this protocol enable are been inspected at the dmz level to ensure that they did not carry any malicious contents and to also ensure that the actual the standard of transmission.

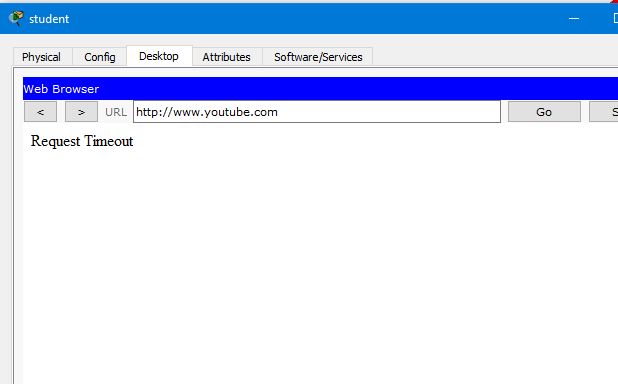
*External resources and traffic/protocol enable*

In institution like university of Jos, research and intellectual enhancement is key; so, with the existing system, there are some protocol and site that have been disable but not fully so with the new system, it tries to ensure that such protocols are disable and only site that are can enable search and intellectual enhancement are enable. Some of this protocol/site include:

*Web/www protocol*: this protocol enable access to internet resources such web site, etc. inthe existing system student cannot visit site like facebook, with little or full access to youtube and movie download. But in the new system student, admin staff have not access to youtube or facebook but the admin staff have access to online newspaper site. While staff (academic) have access to youtube, online newspaper site but not facebook.

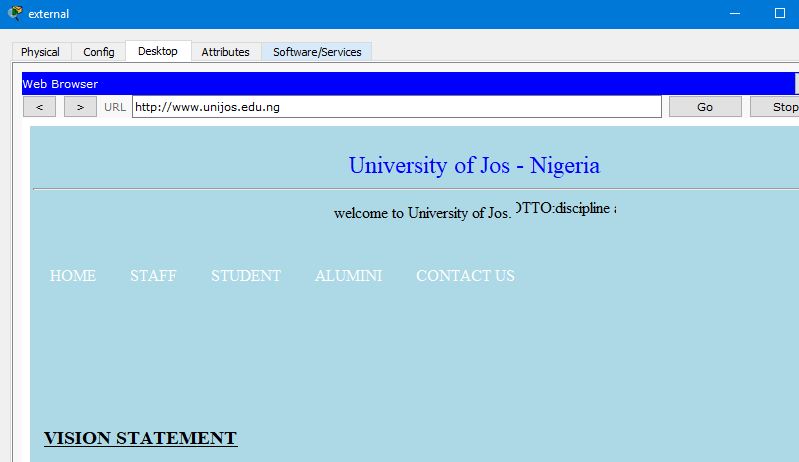


*Fig 4.8.1: old system external resources access*



*Fig 4.8.2: new system external resource acess*

*External users access:* the new system has the school external webserver within the school, which allowed external users to access the school website, with only http protocol enable to the web server.



*Fig 4.9: external user accessing unijos site*

In general, for all traffic coming into the network are been inspected at the edge router as they coming

**4.4 Conclusion**

This chapter discussed the requirements, structure and functionalities of the proposed

solution. The chapter made use of visual representations to present the system’s design, as

well as how it would look and function. Furthermore, give a security policy suitable for the network design and security

The chapter focused on demonstrating a proof of concept to assist towards solving the

problem stated at the start of this research. The next chapter will test and evaluate the prototype against the requirements outlined earlier.

**Chapter 5: Evaluation/Testing**

**5.0 Introduction**

Looking at the problem stated in previous chapters, and the model developed to serve as a solution to the problem identified. This chapter is concerned with testing the model in terms of performance, and policy guidelines.

**5.1 Testing**

Testing refers to the critical examination of the model design, to see if it works or has any bugs or errors within it. Testing was being conducted from start to finish of the program. During testing, a prototype’s activities, characteristics, and outcomes are usually collected and analyzed so as to make judgments about the prototype, to improve its effectiveness and/or to inform programming decisions (Patton, 1987).

**The different tests carried out on this model include the following:**

*Integrity testing* – this involve testing the system to see how trust worth the system is in terms of service quality, time, efficient, redundancy fallback etc.

*Accessibility testing* – this involve testing the system to see whether or not it actually allows the right access to the right users.

*Reliability test* – this involve testing the system to see whether or not is actual dependable for resources access and availability to authorized users at the required time.

*Confidentiality testing* – this deals with how the system enable high top secret to be access by the right user without interference by a third party.

*Regression testing* – involves testing the system after you have made significant changes to ensure that new bugs, not present in previously working parts of the system, have not crept in as a consequence of the change.

*Acceptance testing* – by the user/client with or without you present. They will be interested in how the system operates in its live environment, with real data and performing in real time under normal working pressures.

**5.2 People involved in the testing**

The developed model was tested by different people through alpha testing. These people

include my supervisor, client (some of my course mates), and myself.

**5.3 Test design for the model**

|  |  |  |  |
| --- | --- | --- | --- |
| **Task Section** | **Old System** | **New System** | **Remark** |
| Internal resources access | No | * Student have access to internal web server * Admin/academic Staff access to internal webserver, and mail server * Technical staff access to web, mail, and ftp servers | Passed |
| Internal protocol enabled | No | * Student have web protocol, DNS services enable for internal web service * Admin/academic staff have web, smtp, pop3, DNS protocol services enable. * Technical staff have web, smtp, pop3, DNS, ftp protocol enabled. |
| Internet user access to internal resources | No | * Only internal public server, that is enabled for public access using the web protocol |
| Internal security device enabled | General fire wall | * General firewall, and another internal for internal resources. |
| External resources access | Have a general block to social media like face-book etc. | * Students are given web access to internet library resources * Administrative staff are given web access to internet library, newpaper headline only. * Academic staff are given access to internet library, newpaper headlines, and youtube only. * Technical staff are given general access | * Student are supposed to have access to youtube but with the download capacity of 70mb only. * Staff (both admin and academic) are supposed to have a periodic time of access youtube, facebook etc. |
| External protocol enabled | All protocol is enabled to internet. | * Web protocol is enabled for all staff and student * All protocol is enabled for technical staff. | Passed |
| Remote access enabled network devices | Restricted but both within an outside the network | * Restricted to only three members of the technical staff |
| Traffic enable for inside network users (from ping, ssh, nmap) | All traffic | -student, staffs, and admin staff are given only web service traffic only while technical staff are given all privileges. | For nmap traffic in the new system is only disable for student. |
| Broadcast domain control using vlan | Yes | Yes | Passed |
| Real time monitoring | No | Yes |
| Syslog of all band traffic | No | No |

**5.4 Conclusion**

This chapter takes a Look at the evaluation test result of the model prototype developed, against the existing system, thus; the result shown above have clearly shown that the new model system if implemented on a production network will increase the level of productivity, reliability and efficiency among users of such a system. furthermore, for any system developed and tested there will always be a weak area or an area that have not been touch. Looking at which such area can be looked into for further modification of this new system. the next chapter will showcase some this weak spot.

**Chapter 6: Conclusion and Future Work**

**6.0 Introduction**

This chapter will form the conclusion of this research project. The chapter will re-state the

problem statement together with the objectives from the previous chapters.

In chapter one the problem statement is as follows: that “there is a lack reliable network security with a considerable cost within the cooperate organization” due to some fact which include weakness in term of technology, human and misconfiguration of network and security devices thus looking at the university of Jos network security system and the resources available to promote research work among student and staff.

ICT in general, is actually an indispensable tool in today’s educational growth and research growth. After background information with regards to the specific information was given, chapter two started with an in-depth review of literature works concerning network design and security. Certain findings were stated and chapter two combined with chapter three lead to chapter four (the proposed solution). The solution chapter discussed the proposed solution to the identified problem in chapter one. The model is intended to serve as proof of concept. In chapter 5, tests and evaluation of the solution was carried out and discussed fully.

**6.1 Brief summary of findings**

Looking at the search project at hand, from chapter one to five different findings were made concerning computer networking and network security; starting off from chapter one where the general introduction into the project work was made clearly by stating what network security is and it numerous benefit to our society today; more so not forgetting the different challenge faces over the years with network and security. Going into chapter two, it’s clearly outline what network is and it impact to the cooperate world especially our day to day life thus looking at some of the modern design of network and security architectures.

From the literatures review from chapter two, a collusion was drawn that for a cooperate world like the higher institution where research work is key to it establishment, there is a lack of network security for intellectual properties and research material access for student especially in terms of project search and access to need material rather the institution have become a place for social media chat and movie download. This fact led to the proposed solution in subsequent chapters. Solution was proposed and tested were carried out to see if actually the solution state was actually possible and true.

It can now clearly be seen that all the chapters form a holistic view in the problem statement in chapter one. The next section will show the accomplishment of all the objectives as discussed in chapter one.

**6.2 Accomplishment of objectives**

This section will briefly discuss how the objectives was accomplished. Thus, it will further mention how the primary objective, in turn, comprehensively addressed the problem statement found in chapter one.

*Objectives:* As mentioned in chapter one, the primary objective is to model a network security that will be reliable, cost efficient, and guard against weakness and exposed of resources. Thus, also consisting of these secondary objectives became necessary:

* Identify the general effects of network security to a cooperative network.
* Identify the influence of network security to a cooperative asset.
* Identify the characteristics associated with the network security model.
* Establish and compose the necessary elements that should characterize the network security model.

From the objectives stated above, we can see that the effect of network security was extensive exploited in review of literatures that show how important network security can be to an organization either a cooperate or higher institution. Furthermore, look at the influence of network security to a cooperative asset; from the previous chapters we can see how information security is key to any organization growth in terms of providing confidentiality, and integrity to authorized users in terms of sharing information.

Looking at the different perimeter that characterized a network, and network security; this objective was also exploited in the previous chapters; thus, showing the different element that define a network and network security etc.

Generally, the model discourse in the chapter four try to justify the fact that a more reliable and cost-efficient network security system can be achievable reasons been that network security is not just about the technologically system involve in network design but also the people using the system are key to making a more secured system. Users of a network decide whether a network can be vulnerable or not; of which is only possible that way if there is no policy put in place to govern the implementation and usage of network. So, the chapter given a clear inside of what a network security model should possessed especially in a school environment like the university of Jos where research and intellectual resources are to enhance.

**6.3 Suggestions for further research**

This section will mention any suggestions one could use to further these studies in this

particular field.

As mentioned throughout the chapters, network security is not a static system but a dynamic system that evolves every day due to the desire to showcase skills by hacker and some for financial benefit; while some just help the growth of technology, all these reasons show that a network security cannot be said to be 100 percent efficient, but the layer of policies implemented and the number of integrated system determine how fast or slow a network can be crack.

Looking at the case study for this project which is the university of Jos network, it can be seen that intellectual enhancement and research is important; the model design, have shown that there is room for future studies, in areas like, provide periodic access to social media platform for staff, also look at how to block access to unlicensed software on the network to reduce the possibility of attacks, given student access to video tutorial but with limited download capacity, and more so, periodic review of security policies etc.

**6.4 Conclusion**

This project has identified the critical aspects needed to develop a good network security model for higher institution like University of Jos. The network and security model of the study area was sample and finally a model that served as a proof of concept was designed and showcased. Therefore, the research can be said to have achieved it target objective. It is hoped that this model will be appended to a production system.

**REFERENCE**

Alabady S., 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’

Ali Q., and Alabady S. 2007, "*Design and Implementation of a Secured Remotely Administrated Network,*" In Proceedings International Arab Conference on Information Technology, ACIT.

Andrew S. Tanenbaum, David J. Wetherall (2011), *“Computer Networks, Fifth Edition Pearson*” Education Inc. pg. 1

Barbara Filkins (2017) “*sans Network Security Infrastructure and Best Practices: A SANS Survey”*

Castells, M. (1996). “*The Rise of the Network Society (vol. 2)”*. Oxford: Blackwell Publishers.

Cisco-inshedi *“cisco integrated network security in higher education institutions”* (1992-2004) cisco system, inc pg1-3

Cisco (Oct 04, 2005), “*Network Security Policy**: Best Practices White Paper*” Document ID: 13601 Cisco Systems, Inc. pg 1-7

Cuihong Wu (2010), “*The problems in Campus Network Information Security and Its Solutions,”* School of Computer and information, Shanghai Second Polytechnic University, pg 261

Christensson, P. (2010, January 4). ICT Definition. Retrieved 2015, Sep 8, from http://techterms.com

Eric Maiwald 2001, “*network security a beginner’s guide*”, McGraw-Hill companies, inc. pg 36-44

John E. 2001, “*Canavan Fundamentals of Network Security*”, Artech House Boston London inc. pg3

Multi-State Information Sharing and Analysis Center *(MS-ISAC)*, (2010) *“Why Cyber Security Is Important?”*, Center.inc

*"Network Security 1 "*, Cisco system,Inc. 2006

Shastry Y., Klotz S., and Russell R., 2005 *“Evaluating the effect of iSCSI protocol parameters on performance,”* In Proceedings of the Parallel and Distributed Computing and Networks,

SANS-ICS, E-ISAC (2016) “*WhiteAnalysis of theCyberAttack on theUkrainian Power Grid,”* 1235 G street NW Suite 600 Washington, DC 20005 pg iv

SAN- CPRC (Consensus Policy Resource Community) (2014), “*Acquisition Assessment Policy”,* SANS Institute. Pg 1-3

SAN- CPRC (Consensus Policy Resource Community) (2014), “*Router and Switch Security Policy”*, SANS Institute. Pg 1-3

Salah Alabady (2009), “*Design and Implementation of a Network Security Model for Cooperative Network*”, International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009, pg 9

saulaimon adeniji adebayo, (2012), *“network security bachelor’s thesis*” turum ammattikorkeakoulu

Steven M. Helwig, (2005), “*Security Policy for Higher Educational Institutions*” SANS Institute 2000 – 2005 pg 6-8

**Appendix a: dmz and router configuration**

***Dmz Configuration***

hostname DMZ-WALL

interface Vlan2

nameif outside

security-level 0

ip address 172.168.50.2 255.255.255.248

interface Vlan3

no forward interface Vlan1

nameif dmz

security-level 90

ip address 172.168.51.1 255.255.255.248

object network EMAIL

host 172.168.51.6

description email ip mapping

object network FTP/AAA

host 172.168.51.5

description ftp ip mapping

object network INTERNAL/DNS

host 172.168.51.4

description internal/dns ip mapping

route outside 0.0.0.0 0.0.0.0 172.168.50.1 1

access-list INTERNAL-DNS extended permit tcp any host 172.168.50.4 eq www

access-list INTERNAL-DNS extended permit tcp 192.168.20.0 255.255.255.0 host 172.168.50.6 eq pop3

access-list INTERNAL-DNS extended permit tcp 192.168.20.0 255.255.255.0 host 172.168.50.6 eq smtp

access-list INTERNAL-DNS extended permit tcp 192.168.40.0 255.255.255.0 host 172.168.50.6 eq ftp

access-list INTERNAL-DNS extended permit tcp 192.168.30.0 255.255.255.0 host 172.168.50.6 eq pop3

access-list INTERNAL-DNS extended permit tcp 192.168.30.0 255.255.255.0 host 172.168.50.6 eq smtp

access-list INTERNAL-DNS extended permit tcp 192.168.40.0 255.255.255.0 host 172.168.50.6 eq smtp

access-list INTERNAL-DNS extended permit tcp 192.168.40.0 255.255.255.0 host 172.168.50.6 eq pop3

access-list INTERNAL-DNS extended permit udp any host 172.168.50.4 eq domain

access-list INTERNAL-DNS extended permit udp any host 172.168.50.4 eq 514

access-list INTERNAL-DNS extended permit tcp 192.168.40.0 255.255.255.0 host 172.168.50.5 eq ftp

access-list INTERNAL-DNS extended permit tcp host 172.168.50.1 host 172.168.50.5 eq ftp

access-list INTERNAL-DNS extended permit icmp 192.168.40.0 255.255.255.0 host 172.168.50.4

access-list INTERNAL-DNS extended permit icmp 192.168.2.0 255.255.255.252 any

access-list INTERNAL-DNS extended permit ip 192.168.1.0 255.255.255.252 any

access-group INTERNAL-DNS in interface outside

object network EMAIL

nat (dmz,outside) static 172.168.50.6

object network FTP/AAA

nat (dmz,outside) static 172.168.50.5

object network INTERNAL/DNS

nat (dmz,outside) static 172.168.50.4

aaa authentication ssh console LOCAL

username admin1 password 89YenYLlCYftnmxP encrypted

class-map inspection\_default

match default-inspection-traffic

policy-map global\_policy

class inspection\_default

inspect dns

inspect ftp

inspect http

inspect icmp

service-policy global\_policy global

telnet timeout 5

ssh 172.168.51.3 255.255.255.255 dmz

ssh 192.168.40.250 255.255.255.255 outside

ssh 192.168.40.251 255.255.255.255 outside

ssh timeout 20

***Router Configuration***

hostname EDGE

login block-for 30 attempts 3 within 60

enable secret 5 $1$mERr$tKAvQPi4nwql8vUTe8ogt/

no ip cef

no ipv6 cef

no ip domain-lookup

spanning-tree mode pvst

class-map type inspect match-any INSIDE\_PROTOCOLS

match protocol http

match protocol dns

match protocol bgp

match protocol udp

match protocol tcp

match protocol icmp

match protocol ssh

match protocol syslog

policy-map type inspect INSIDE\_TO\_INTERNET

class type inspect INSIDE\_PROTOCOLS

inspect

zone security UNIJOS-INSIDE

zone security INTERNET

zone security INSIDE

zone-pair security IN\_TO\_OUT\_ZONE source UNIJOS-INSIDE destination INTERNET

service-policy type inspect INSIDE\_TO\_INTERNET

zone-pair security INTERNET\_TO\_INSIDE source INTERNET destination UNIJOS-INSIDE

service-policy type inspect INSIDE\_TO\_INTERNET

interface FastEthernet0/0

ip address 209.165.200.1 255.255.255.248

zone-member security UNIJOS-INSIDE

duplex auto

speed auto

interface Serial0/0/0

ip address 209.165.200.9 255.255.255.252

zone-member security INTERNET

no cdp enable

router ospf 1

router-id 20.20.20.20

log-adjacency-changes

passive-interface FastEthernet0/0

passive-interface FastEthernet0/1

network 209.165.200.8 0.0.0.3 area 2

network 209.165.200.0 0.0.0.7 area 2

router bgp 25

bgp log-neighbor-changes

no synchronization

neighbor 209.165.200.10 remote-as 50

network 209.165.200.8 mask 255.255.255.252

ip classless

ip route 0.0.0.0 0.0.0.0 209.165.200.10

ip route 192.168.2.8 255.255.255.252 209.165.200.2

ip route 172.168.50.0 255.255.255.248 209.165.200.2

ip flow-export version 9

ip access-list extended sl\_def\_acl

deny tcp any any eq telnet

deny tcp any any eq www

deny tcp any any eq 22

permit tcp any any eq 22

no cdp run

logging 172.168.50.5

logging 209.165.200.6

line vty 0 4

login