COMPUTER NETWORK DESIGN FOR NIGERIAN UNIVERSITIES

Ebinimi John Abiama

Department of information and communication Technology, Bayelsa Medical University,
Amara, Yenagoa
Email: nimiolotu@gmail.com Phone No:08060644536

ABSTRACT

Computer Networks are integral parts of everyday social and professional life, in the 21st century and it has a lot of positive impact on society at large. With increasing dependence on and usage of information and communication Technology (ICT) in tertiary institutions worldwide, it has become very imperative for computer systems been used in Nigeria Universities to be linked together to enhanced interconnectivity and access to information. The Objective of this project is to design a suitable network system for Nigerian universities. The target is to design a network with high-quality security and low cost, in such a way that the network devices of the university will meet standards associated with universities in developed countries. The developed system is an integration of network systems configured with IP addresses to all the devices incorporated. The network consists of routers, switches, backups, firewalls, and servers. The incorporation of the firewall device helps to prevent any unfavourable data from entering the network. All devices in the network are secured by passwords and these passwords are encrypted to be more secured. Additionally, each computer in the network is secured by antivirus programs and a backup system. The servers used for this network design are DHCP servers and DNS servers. The Nigeria university communities stand to benefit from the project as the project will enhance education, interconnectivity and information accessibility in Nigerian universities. Conclusively, the general productivity, development and stability of any University, depend so much on the Network Infrastructure as the backbone of its operations, therefore this project will be a veritable tool for the smooth educational operation of Bayelsa Medical University.

Keywords: Computer, network, design Nigeria and universities.

1. 0 INTRODUCTION

University Campus Networks play a pivotal role in the learning, management, research and other dayto-day activities of Universities. in today's Nigerian Universities where there is development in infrastructure, student increasing population, computer network plays vital role as backbone to enhance and sustain Administration, Collaborative and Digital educational system, as well as communication, access to resources and research platforms. The university communities need the computer Network to deliver quality and secure resource utilization; hence the need for a University Campus-wide Network can never be overemphasized. The increasing demand for high performance network has challenged network researchers to design network architectures that can deliver high quality service to end users (Sarkar., Bymer and Al Qirim, 2005;
Magus,2011).

A Network is a combination of devices, Computers, phones, sensors and any other equipment, interlinked together to function, share Information and resources, communicate and collaborate and store Information. Ramaya (2023) defined computer network as a system that connects two or more computing devices to transmit and share information. Computer networking is the practice of transporting and exchanging data between nodes over a shared medium in an information system (Scarpati, 2023). Computer network node is any physical device within a network of other tools that is able to send, receive or forward information (Tim, 2021). A University Campus Network
Infrastructure is a combination of devices within a University campus environment, for Administration, Teaching, Learning and Communication.

The functionality of a University Network
Infrastructure is to serve a variety of purposes such as sharing University resources. Most often, the software resources like the University portal, Electronic Library, Human Resource System and Educational Platforms are stored in a centralised location and members of staff and student within

and outside the campus environment might at some point in time require to use these resources. The ability of members of the university to optimally utilize such resources depends on the kind of network infrastructure and policies that are inherent in the University.

Students sometimes would want to access library resources or might have to submit assignments on the learning platforms, and staff of the different departments would also want to carry out the specific task from outside their office locations, all of these are factors that must be considered in the planning of a University computer network system. Computer networking in tertiary institutions provides students with access to educational resources as well as enable staff to share information effectively, thereby increasing their productivity, efficiency, reduce cost, enhance flexibility. Many institutions in Nigeria, like the Bayelsa Medical University, are looking for solutions to integrate networks with security, backup, and other elements found in a developed country's university network. The objective of this project was to offer a local area network design suited for universities in Nigeria in Bayelsa Medical University.

2.0. EQUIPMENT AND DESIGN SELECTION 2.1 Network Topology

Network topology defines the structure of the network of how all the components are interconnected to each other (ww.javapoint.com). There are different network topologies for computer networking. A network topology determines how hosts are connected to a computer network. It characterizes how the personal computer (PCs) and other hosts are organized, and linked to each other. Available network topologies include Point-to-Point, Bus, Star, Ring, and Mesh topology. Each type has a different set of advantages and disadvantages. However, for this project, the star network topology was selected because it is best suited for the purpose of the project.

Star Topology

The star topology is generally used for all networks whereby each device or computer is connected to a central hub by a direct line. The centre hub can be a switch, router, or server. Each computer connects directly to the centre device such as the hub, router, and server. A star topology is designed with each node connected directly to a central network hub, switch, or concentrator. It is easy to add and remove a computer from the network without affecting the network. It is easy to replace, install or remove hosts or other devices. A problem in the network can be easily detected, t is easier to modify or add a new computer without disturbing the rest of the network by simply running a new line from the computer to the central location and plugging it to the hub. Furthermore, the cost of this network topology is less. The star topology network connection was used for this design because each computer is independent of other computers in the network, and it is less expensive than mesh and ring topology and easy to install.

Star Topology

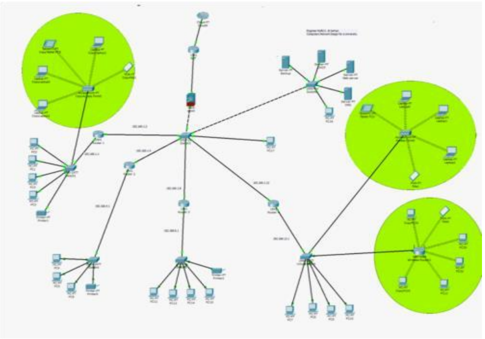


Fig 2.1: Star topology

Figure 2.1: The access point is star topology

2.2 Choice of network connection

Wireless

There are different methods of equipment connection for computer networking. However, for this project, the wireless connection is adopted. Wireless is used to depict media communications in which electromagnetic waves transfer the signal over part or most of the transmission path, so there is less need for a cable. There are many advantages of wireless transmission when compared to wire. The advantages of wireless connection include easy network installation, increase accessibility, wide reach, flexibility, efficiency and cost effectiveness (Prasanna, 2023). The wireless that is used in this network design is (802.11). The 802.11 is an advanced group of details for WLANs developed by a group in the Institute of Electrical and Electronics Engineers (IEEE). Mobility is less limited and can provide wide coverage over a long distance. Thus, making use of wireless is of great benefit to users of this network design. All Wi-Fi devices are secured by a password. The password prevents unauthorized users to connect to the WiFi network. This is because the network could easily be hacked when it is open to all users, especially unauthorized users who can overcrowd the network, making it work very slowly. Also, a limited number of IP addresses that are reserved for the real users of the network can be taken by unauthorized users. To connect the wireless, Cisco access point is used, and at least one access point is installed in each building. The number of access point Installations depends on the size of the building.

Connection Setup

The obvious way, given the constraints, to connect devices is for all computers to be connected to switches, and then switches must be connected to the routers. After that, all routers connect to the last switch to link with the edge switch, in which various servers, such as the DHCP server and DNS server, are connected. The last switch is also connected to a firewall device. The firewall device links to the NAT router and then to the external networks or internet. The Fig 2.3 below shows the connection setup of all devices.

Fig 2.3: Integration network system

Devices Used

The devices used, in this project are routers, switches, servers, etc. All were chosen from the Cisco Company. This is because the quality of Cisco devices is much better than other devices. According to the Cisco website, With Cisco network systems, intelligent network services, such as quality of service (QoS) and encryption, are consistently supported and preserved across the entire network, enabling the security, and highquality service delivery regardless of whether the user is at the main campus or in a satellite campus. The number of hosts used is 5075 for the network and is distributed among various sections in the university.

2.3 Features of the Network Infrastructure

Infrastructure

Infrastructure powers all functions on the network. Network infrastructure is the backbone that connects people and business to each other (Ron, 2022). The network infrastructure includes all base devices in the network. When all base devices are protected, the network system will be secured. This is because the data passing from the outside of the local network must pass through those devices into the local network. The devices used for infrastructure in this network design are a virtual switch, backup systems, firewalls, and DNS.

Virtual switch

A virtual switch accomplishes more than simply forward information bundles. It keenly coordinates the correspondence on a network by checking information parcels before moving them to a destination.

Backup

Backup creates duplicates, and this is a greater degree of protection. It is through creating backup copies saved both in the same workplace or another location, updated on a regular basis, that ensure the least amount of losses in the case of the original data loss. Backup helps to reduce human error (www.nordic.backup).

Firewall

The firewall prevents external users from gaining access to the network resources and local data and thereby securing the network and its resources from external threats.

Domain Name System (DNS) Domain Name System (DNS) device directs local and Internet movement to the proper target by performing real-time look-ups of Internet addresses with different DNS servers situated on the Internet. Prior to a local computer to sending a DNS server.

Encryption Passwords

Encryption Passwords**.** Each host must have its own password for authentication control. Encryption of Passwords is the only authorization process to gain access to the information in the network. The password must be different from one device to another, depending on the user of the device.

Individual Hosts

The number of attacks worldwide has risen in recent times due to the constant development of sophisticated software. Each person or host must have his/her security to protect their data from hackers. Every host must secure their data from attack and protect their information from being stolen. A professor preparing questions for an exam to administer to his students should be able to ensure the exam remains confidential on the network under consideration. If the exam questions are not private, all students will see the exam questions. This will cause a serious academic integrity problem. So, each professor must secure their data. Also, students must secure their grades and assignments from other students. Security is very important in preventing others from seeing their personal information. There is much software to secure each host device, such as antiviruses, update and patching tools, basic support and server room.

Antivirus:

Antivirus is dedicated computer software's that help in detecting cyber threats such as malicious, spywares and phishing program in the system (intellipaat, 2023). The antivirus prevents viruses from been active in computers in the network to make the network become fully protected from threats.

Switches

Switches are devices used on the network to transmit and receive data from one device to another or many devices, depending on the message intended. A switch provides the full bandwidth of the network to each port, thereby reducing collisions on the network. Switches also perform functions from the Data Link Layer (Layer 2 on the OSI [Open Systems Interconnection] Model

Routers

A router is a networking device that forwards data packets between computer networks. The router chooses the best path to transfer data packets to their destination in the most efficient manner. Think of a router as a traffic cop at a busy intersection. This traffic cop determines which vehicles get through, which vehicles are not permitted on the path and the destination that the vehicles may take. Since the network must connect many computers to many switches, the router is an important component of the network. The router will control switches in a hyper-star topology.

NAT System

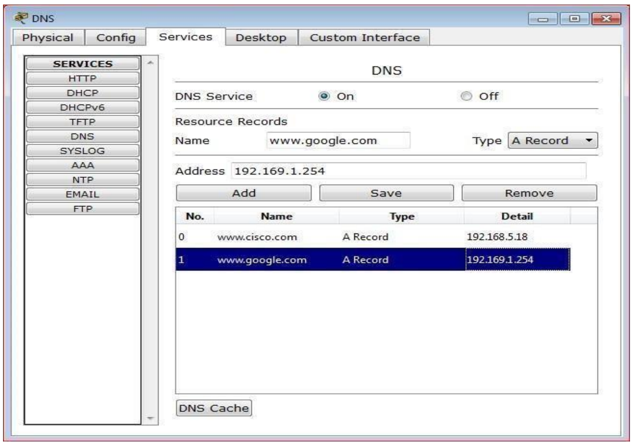
NAT stands for Network Address Translation. It is a software tool that translates numerous private IP addresses from the LAN to one public IP address that is required for access to the Internetwork (Internet or WAN: Wide Area Network). NAT devices are used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses.

Wireless Access Point

An access point is a wireless service device used for networks. Wireless access point service plays a significant role in this design and is very important for educational institutions. The Access point devices connect to the router directly. Each access point device is placed in an area to distribute the internet for that particular area.

Servers

The term server refers to a device or a computer program that supports other devices or programs called clients. This is known as the client-server model; one server can support many clients and give different functionalities or characteristics to different clients. The few servers used in this project are the DHCP and DNS servers. The Domain Name System (DNS) is a server service that maps a domain name to IP addresses. The DNS server translates a domain name to the IP address. IP address contains 32 bits. Since people cannot easily memorise all numbers of IP addresses, it is easier for them to memorize the domain names of IP addresses. The DNS server is connected to the switch and then to the router. The IP address for the DNS server is static, and the IP address used is 199.8.8.8. The configuration of the DNS server is shown in the Fig 2.4 below.



DNS

DNS Service ● On ○ Off

Resource Records

Name www.google.com Type A Record

Address 192.169.1.254

No.	Name	Type	Detail
0	www.cisco.com	A Record	192.168.5.18
1	www.google.com	A Record	192.169.1.254

Figure 2.4: DNA configuration

Server Room

Server Room is a room where all major devices (servers, routers, firewall, DNS… etc...) are securely placed. All the devices are placed in a standard way in a rack in the server room. Only authorized personnel who have permission to maintain, install, protect, secure, design, and monitor network devices are allowed into the server room.

Update and Patching Tools

All devices in the network are programmed by software such as the operating system (OS). Over time, this software loses some characteristics which make it vulnerable to attacks. Sometimes, companies make software for devices. Then, that company might want to develop that software or test it to see if there are some problems with that software. If there is any problem with the software, the company will publish a new or higher version of the software, usually with a patch to fix the old problems to make it more secure. The important thing that companies focus on is security when updating the software to a new version. All devices in the network need a software update for the security of the network devices and data.

2.4 Basic Support

All universities have specialised technicians for managing the network devices. The Bayelsa Medical University must have specialised technicians for managing the network devices. These specialists must have skills in networking. If they do not have experience, it will affect the whole network system. For example, when a device such as a router does not work or breaks down, and if a person does not have enough experience to fix that problem, it may affect the whole network. So, network technicians must take networking courses to gain enough experience on how to fix the problem of the network system.

3. 0 IMPLEMENTATION

The first step is to configure all the personal computers. Each personal computer must be connected to a switch. Each computer needs a unique Internet Protocol (IP) address.

3.1 Expectations and ongoing Challenges, Options, and Possible Future Evolution

An operating network will face challenges over its lifespan. One big challenge this design will face is economic problems. This is because a key requirement has been cost on making reduction suitable for Bayelsa Medical University. As a result, robust materials and fewer numbers of complex devices, such as servers, will be used. If there are improvements in the economy in the future, the network materials and the number of devices used will be upgraded or extended. For example, in the future, more servers can be added to the already existing three servers as a form of system-wide upgrade.

Furthermore, more than one backup device can be added to save the network's data. Accordingly, it is necessary to include room for future development plans. For instance, this project's network design has an extra number of IP addresses for the future. The network needs 5075 hosts while it has 8190 hosts. In the future, the Bayelsa Medical University can connect 3115 additional hosts, which can be included without exhausting available IP addresses.

3.2 Scenarios and Issued to be should be considered for the optimal functioning of the network

Quality of Devices

The quality of the network device is vital for the network. When the device has good quality, the number of issues in the network will be reduced. Cisco Company is known for their good quality network devices. According to the Cisco website, "With Cisco network systems, intelligent network services, such as quality of service (QoS) and encryption, are consistently supported and preserved across the entire network, enabling the same secure, high-quality service delivery regardless of whether the user is at headquarters or in a local branch." As a result, all devices used for this research are Cisco devices, such as routers, switches, access points, services, and firewalls. One reason for patronising Cisco devices is the high protection service that its devices provide, which will be highly relevant to important information of the University. It is important for a network to continue working all the time and should never stop for any reason. A network failure can disrupt academic activities. All staff, professors, and students need the network most of the time. For example, suppose a network stops for any reason. In that case, the students cannot submit their assignments, exams can be halted, and every other student's academic activities that use the network will be stopped. Also, professors will not be able to attend online class sessions until the network starts working again. Cisco devices are very strong at withstanding such network failures. Therefore, using Cisco devices will minimise possible network failures for this project's implementation.

Backup

As a form of best practice, organisations and companies always place Backup server offsite. A backup system is a mechanism for storing data in the network, allowing storage and recovery if needed. Network backup is an integral part of the backup and recovery process in an IT environment (Rouse, 1014). The data in the backup are updated periodically depending on how the backup schedule is configured. The data stored in this platform are very important and must be protected from any loss. To protect these data, more than one backup server is strongly preferred, and the location of the backup server must be far away from the location of the original data. However, the cost will be high when the backup device is placed in another location. If a budget allows, more than one backup server device and the backup server will be placed in other continents, separate from the location of the local area. As an extreme example, if the local area network is in the Asian continent, the backup device can be placed in another continent, such as the North or South American continent or the Australian continent. This is because if natural disasters such as earthquakes, floods, hurricanes, volcanoes, etc., occur in the location of the local network, the backup data will not be affected since its location is far away from the disaster.

Evolution/ Optional Additions

Budget plays a significant role in the design of the network in terms of quality, device selection, and network security. The budget for this network design is limited. When the budget is limited for designing the network, the designer must utilise specific devices that the available budget can afford. Therefore, if the budget is high, devices that could be used include optical fibres, firewalls, backup devices, two networks for security and many servers.

Optical Fiber

Optical fibre cable is a medium for transferring information. Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of infrared or visible radiation through an optical fiber (Macintosh, 2014 and www.thefoa.org). This cable is more expensive than other cable types, less noisy than twisted pair cable, faster, and mostly used for long-distance transmissions. However, "from around 2005, the development of the continuous extrusion techniques began in earnest, and by 2008 40-Gb transmission was developed. This was the world's fastest transmission speed, surpassing the GI type silica optical fibre. These results were achieved through joint research with Asahi Glass.

4.0 CONCLUSION AND RECOMMENDATIONS

4.1 Conclusion

All networks need many servers to do their work. For this research, the use of servers was minimized because of cost, hence only few but very important servers such as DNS and DHCP were used in the project. These servers help the network to perform their functions smoothly. This Research has proven that a standard network system can be designed with less cost. We used the cheapest devices in designing the network, the security of this network turned out to be very strong. This is because the firewall and backup devices used in this network are of good quality. This design allows for future expansion, as universities can connect 3115 additional hosts, allowing for perhost costs, like cabling. The additional hosts can be included without exhausting the available IP address. Also, if there are high budgets, they can develop the network system to become more powerful and have a high level of security, and many servers can be added to the network.

4.2 Recommendation

The design allows for future expansion therefore the researcher recommends that the University management should work toward expanding the network as the university community expand.

REFERENCES

Bagus Mulyawn (2011): Campus Network Design and Implementation Using Top Down Approach. Proceedings of the 1st International Conference on information Systems for Business Competitiveness (CISBC, 2011).

Jessica Scarpati (2023). Computer networking. Retrieved on 28 September, 2023 from. www.techtarget.com/search

Margaret Rouse (2014). Network backup: What does network Backup mean? Available atwww.technopedia.com/defin

Mcintosh Jane., Chrisp Peter., Parker Philip., Gibson Carrie., Grant R. G., and Regan Sally (2014). History of the world in 1000. object. New York.DK and the Smithson. P. 382

Prasanna Venkatesan (2014) Wireless network; Advantages and disadvantages. https://www.aplustopper.com/wire

Ramaya Mohanakrishnan (2023). What is a computer network? Definition, Objectives, Components, Types and Best Practices. Retrieved on20 September, 2023 from, www.spiceworks.com/tech

Ron Herman (2022). Network infrastructure: Knowing what it is and why it is important.httpps://www.bccs.com/network-inf

Sarkar, N. I., Bymer, C and Al Qirim, N.A.Y (2005). Upgrading to Gigabit Ethernet: The case of a large New Zealand Organization. available at **http://citeseerx.ist.psu.edu/viewdoc/download**

Tim Fisher (2021). What is a Node in a Computer Network? www.lifewire.com/whatis.aUnderstnding wavelength in FiberOptics. www.thefoa.or.

What is antivirus software.? Available at httP://intellipaat.com.blog/what

What is Network topology? www.javapoint.com/comp

Why Network Backup is Essential for Your

Business. Available at https://www.nordic.backup.com/blog