**DESIGN OF A VIRTUAL LOCAL AREA NETWORK (VLAN)**

**(CASE STUDY OF DEPARTMENT OF MATHEMATICS, USMANU DANFODIYO UNIVERSITY, SOKOTO.)**

**BY**

**AHMAD, Ibrahim Dogondaji**

**ADM. NO: 1011310014**

**A RESEARCH WORK SUBMITTED TO THE DEPARTMENT OF MATHEMATICS, COMPUTER SCIENCE UNIT, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF SCIENCE (B.Sc. Hons) DEGREE IN COMPUTER SCIENCE, USMANU DANFODIYO UNIVERSITY, SOKOTO.**

**NOVEMBER, 2015.**

# APPROVAL PAGE

This is to certify that this research carried out by IBRAHIM AHMAD DOGONDAJI with Admission Number 1011310014 under the supervision of Dr. Ahmed Yusuf Tambuwal of Computer Science Unit, Department of Mathematics, Usmanu Danfodiyo University, Sokoto is fully adequate in scope for the reward of Bachelor of Science Degree (B.Sc. Hons) in Computer Science.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dr. A Y Tambuwal Date

Project Supervisor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prof. I. J. Uwanta Date

Head of Department

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

External Examiner Date

# DEDICATION

This report is dedicated to the Almighty Allah for his protection, wisdom, knowledge and understanding throughout the period of the project.

Besides, it is dedicated to my caring parents, Mr. and Mrs. Ahmad Aliyu Dogondaji for their solely contribution towards the success of this program.

# ACKNOWLEDGEMENTS

I wish to acknowledge and express my sincere gratitude to Allah (S.W.T) for giving me the ability, gifts, and privilege to make this report possible and making the entire project a successful one.

I wish to extend my profound and sincere gratitude to my supervisor Dr. Ahmed Yusuf Tambuwal for his guidance, encouragement and motivation which provide me with initiation to write this project.

This acknowledgement would not end without commending effort of all my lecturers whom through their help and assistance I was able to reach the stage I am now.

I would also like to thank the staffs of UDUNET and Cisco for their help and support, especially Mal. Bello Big Man and Mal. Aliyu Cisco.

My sincere gratitude goes to my parents, Late Engr. Ahmad Aliyu Dogondaji and my Mother Hajiya Halimat Ahmad Dogondaji for their moral support and guidance, May Allah, have mercy upon them as they brought me up (when I was) small.

I also wish to thanks my brothers and sisters. Specials thanks goes to my friends and well-wishers especially Abdulrahman Aliyu, Abdulmalik Yusuf, Faruk Ibrahim, Sulaiman Bunza and Faisal Sulaiman, for their support, assistance and encouragement.

TABLE OF CONTENTS

[APPROVAL PAGE ii](#_Toc435268548)

[DEDICATION iii](#_Toc435268549)

[ACKNOLEDMENT iv](#_Toc435268550)

[ABSTRACT vii](#_Toc435268551)

[CHAPTER ONE: INTRODUCTION 1](#_Toc435268552)

[1.1 BACKGROUND STUDY 1](#_Toc435268553)

[1.2 PROBLEM STATEMENT 1](#_Toc435268554)

[1.3 AIM AND OBJECTIVES 2](#_Toc435268555)

[1.4 MOTIVATION 3](#_Toc435268556)

[1.5 SCOPE OF THE PROJECT 3](#_Toc435268557)

[1.6 LIMITATION OF THE PROJECT 3](#_Toc435268558)

[CHAPTER TWO: LITERATURE REVIEW 4](#_Toc435268559)

[2.1 INTRODUCTION 4](#_Toc435268560)

[2.2 VLAN AND NETWORKING 4](#_Toc435268561)

[2.2.1 Network Types 4](#_Toc435268562)

[2.2.2 Network Architecture 5](#_Toc435268563)

[2.2.3 Networking Devices 6](#_Toc435268564)

[2.2.4 Common Network Cables 8](#_Toc435268565)

[2.2.5 IP Address 8](#_Toc435268566)

[2.2.6 Cisco Packet Tracer. 10](#_Toc435268567)

[2.3 VLAN (VIRTUAL LOCAL AREA NETWORK) 10](#_Toc435268568)

[2.4 CONFIGURING SWITCHES AND ROUTER 12](#_Toc435268569)

[2.4.1 Configuring Vlans 12](#_Toc435268570)

[2.4.2 Trunking and Inter-VLAN Routing 15](#_Toc435268571)

[CHAPTER THREE: SYSTEM ANALYSIS AND DESIGN 20](#_Toc435268572)

[3.1 INTRODUCTION 20](#_Toc435268573)

[3.2 ANALYSIS OF THE CURRENT NETWORK 20](#_Toc435268574)

[3.2.1 Problems of the current network 22](#_Toc435268575)

[3.2.2 Feasibility Study 23](#_Toc435268576)

[3.3 NEW DESIGNS 24](#_Toc435268577)

[3.3.1 Proposed Network Design 1 25](#_Toc435268578)

[3.3.2 Proposed Network Design 2 28](#_Toc435268579)

[CHAPTER FOUR: SYSTEM IMPLEMENTATION AND TESTING 31](#_Toc435268580)

[4.1 SYSTEM IMPLEMENTATION AND TESTING OF DESIGN 1 31](#_Toc435268581)

[4.2 SYSTEM IMPLEMENTATION AND TESTING OF DESIGN TWO 40](#_Toc435268582)

[CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS. 43](#_Toc435268583)

[5.1 SUMMARY 43](#_Toc435268584)

[5.2 CONCLUSION 44](#_Toc435268585)

[5.3 RECOMMENDATIONS 44](#_Toc435268586)

[REFERENCES 46](#_Toc435268587)

[GLOSSORY 47](#_Toc435268588)

# ABSTRACT

Computer networks in organization have evolve over time. Most large organization have a complex and wide range of different networks configurations, operating systems and strategy. The network technology that handle our internet communications come in many different forms.

In this research project, the problems of the current LAN network in Department of Mathematics, Usmanu Danfodiyo University, Sokoto have been analyzed and documented. These problems includes: All host are in one broadcast domain which causes more traffic on the segment and may slow the network performance, Switches flood broadcasts out all ports, which consumes unnecessary bandwidth. As the number of devices connected to a switch increases, more broadcast traffic is generated and more bandwidth is wasted, Every device that is attached to a switch can forward and receive frames from every other device on that switch, so when users from mixed departments share a segment, undesirable information captures can occur, which may result to network security problem.

Hence the design of Virtual LAN for the department will solve the problems associated to the current network by creation of various logical groups to provide more security and more broadcast domains. As for bandwidth issues, VLANs, can offer more bandwidth to users than is inherent in a shared network. The new network was designed with Unshielded Twisted Pair cable (Fast Ethernet Network). The Fast Ethernet Network has a higher cost of installation but will deliver a network with much higher performance.

# CHAPTER ONE: INTRODUCTION

## 1.1 BACKGROUND STUDY

Good network administration is the backbone of today's technology-dependent enterprises. Network administrators are charged with keeping expansive networks and numerous applications running smoothly, and the job can seem overwhelming at times.

We live in a truly connected society. We can communicate almost instantaneously with others worldwide; changing events from the smallest of countries and places are immediately broadcast to the world; our email messages are delivered to handheld devices; cars access the internet to receive driving instruction and solved mechanical problems. Even household appliances can connect to the internet and be remotely controlled, so as campus and universities. The communication and information option we have at our fingertips have changed how we react and relate to the world around us.

As powerful and flexibility of our communication systems have expanded, the sophistication of the networks that support these systems has become increasingly critical and complex. The network technologies that handle our internet communication come in many different forms. Satellites, broadcast towers, telephone lines, even buried cables and fiber optics carry our telephone messages, emails and text messages. These different networks must be able to efficiently and effectively integrate with one another.

A computer network is a communication system that connects two or more computers so that they can exchange information and share resources. Networks can be set up in different arrangement to suit user’s needs.

As corporations grow, network administrators find themselves deep in frustration. Management wants more users on the network, whereas users want more Bandwidth. Segmenting LANs is another approach to provide users additional bandwidth without replacing all user equipment. By segmenting LANs, the administrator breaks a Network into smaller portions and connects them with some type of internetworking Equipment.

## 1.2 PROBLEM STATEMENT

The staff offices in the Department of Mathematics, Usmanu Danfodiyo University Sokoto, Nigeria, are located in the new Mathematics department building (i.e. old Management Sciences building) of the university. The offices located within the building, do have a LAN (Local Area Network) communication network that connects them, to enable sharing of resources, data transfer and information circulation.

1. Hosts and servers that are connected to Layer 2 switch are part of the same network segment. This arrangement poses some significant problems, which include:
2. All host are in one broadcast domain, which causes more traffic on the segment and may slow the network performance.
3. Switches flood broadcasts out all ports, which consumes unnecessary bandwidth. As the number of devices connected to a switch increases, more broadcast traffic is generated and more bandwidth is wasted.
4. Every device that is attached to a switch can forward and receive frames from every other device on that switch, so when users from mixed departments share a segment, undesirable information captures can occur, which may result to network security problem.
5. LANs require physical administration as the location of the user changes, the need for re-cabling, addressing the new station, reconfiguration of routers and hubs arises. The mobility of the users in a network results in network costs.

## 1.3 AIM AND OBJECTIVES OF THE STUDY

This research project is aimed at designing a virtual LAN (VLAN) network that will connect all the staff offices in Department of Mathematics for efficient resource sharing, fast information circulation and reduce congestion on the current network to enhance the performance and to create different groups in order to secure information. The research has the following objectives:

1. To identify the networking media that best suits the network.
2. To determine the best network architecture that would enable effective resource sharing between all staff offices of the Mathematics Department.
3. To design respective VLANs for different units
4. To configure network addresses for each units
5. To identify configurations required on Cisco router and switches to create VLAN’s and Inter VLAN routing

## 1.4 MOTIVATION

In a LAN network, users were assigned to networks based on geography and were limited by physical topologies and distances and are also in one broadcast domain VLANs can logically group networks so that the network location of users is no longer so tightly coupled to their physical location and provide multiple broadcast domain.

There are some official reasons why certain hosts access each other while others do not. As an example, members of a particular VLAN may be the only users who need to access the VLAN’s server.

## 1.5 SCOPE OF THE PROJECT

To design and configure a network for Department of Mathematics which includes: Mathematics unit, Computer unit and Statistics unit, where all the users in the department receive appropriate individual IP address. Each Units uses different network address. The Department uses Cisco switches and router.

The project is to understand the advantages of using VLAN in a network, how broadcasting is controlled. Understand the configuration which is required to set up a vlan based network using Cisco routers and switches and how inter-vlan is achieved.

## 1.6 LIMITATION OF THE PROJECT

Networking covers not only local, regional, national or international boundaries but the whole world at large. This research project therefore, centers only to the VLAN network of Department of mathematics, Faculty of Science, Usmanu Danfodiyo University Sokoto, Nigeria.

The Vlan designs cannot show how broadcast message is passed across the network, but broadcast group and broadcast address for various groups where created.

# CHAPTER TWO: LITERATURE REVIEW

## 2.1 INTRODUCTION

Ugomma (2004), designed a Local Area Network for the previous location of department of Mathematics UDUS on her project, which was then located at the faculty of sciences building. Her project was limited to the LAN network that connected the offices of that department, which by designing a VLAN will enhance the performance of the network and security.

Tanenbaum (2003:1) identified that each of the past three centuries were dominated by a single topology. 18th century was the era of great mechanical systems, 19th century was the age of steam engines and 20th century’s key technology was information gathering, processing as well as distribution. As the key technology of 20th century grows, then the need for more sophisticated information processing system increases.

Leon-Garcia and Widjaja (2000:1) exclaimed that the operation of modern communication networks is a very complicated process involving the interaction of many systems. This is due to the very many protocols embedded therein, each performing specified function as well as the overall function of the network. Forouzan (2004 and 2007) therefore, clarified that research in data communications and networking has resulted in new technologies, whose first goal is to enable the exchange of data in forms as text, audio, images and video from all points in the world.

## 2.2 VLAN AND NETWORKING

Timothy J. O’Leary (2005) defines a computer network is a communication system that connects two or more computers so that they can exchange information and share resources. Networks can be set up in different arrangement to suit users’ needs.

### 2.2.1 Network Types

Clearly, different types of channels – wired or wireless – allow different kinds of networks to be formed. Network may be within home, citywide and even international, using both cable and wireless connections. These include:

1. **Personal Area Networks**

A personal area network (PAN) is a type of wireless network that works within a very small area – your immediate surroundings. PANs connect cell phones to headsets, PDAs to other PDAs, keyboards to cell phones, and so on. The most popular PAN technology is Bluetooth, with a maximum range of around 33 feet.

1. **Local Area Networks**

Networks with nodes that are in close physical proximity – within the same building, for instance – are called local area networks (LANs). Typically, LANs span distances less than a mile and are owned and operate by individual organizations under single administrative control. LANs are widely used by colleges, universities and other types of organizations to link personal computer and to share printers and other resources.

1. **Metropolitan Area Networks**

Metropolitan area networks (MAN) span distances up to 100 miles these networks are frequently used as links between office buildings that are located throughout the city.

Unlike a LAN, a MAN is typically not owned by a single organization. Rather it is owned by group of organizations or by a single network service provider that provides network services for a fee.

1. **Wide Area Networks**

Wide area networks (WANs) are countrywide and worldwide networks. These networks provide access the regional service (MAN) providers and typically span distance greater than 100 miles. They use microwave relays and satellites to reach users over a long distances.

### 2.2.2 Network Architecture

Network architecture describes how a network is arranged and how resources are coordinated and shared. It encompasses a variety of different network specifics, including network topologies and strategies. Network topology describes the physical arrangement of the network. Network strategies defines how information and resources are shared.

**1. Topology**

A network can be arrange and configure in several different ways. This arrangement is called the network’s topology. The most common topologies are:

1. **Bus network –** each device is connected to a common cable called a bus or backbone, and all communications travel along this bus.
2. **Ring network –** each devices is connected to two other devices, forming a ring. When a message is sent, it passed around the ring until it reaches the intended destination.
3. **Star network –** each device is connected directly to the central network switch. Whenever a node sends a message, it is routed to the switch, which then passes the message along to the intended recipient. Star topology is the most widely used network topology today.
4. **Tree network –** each device is connected to a central node, either directly or through one or more other devices. The central node is connected to two or more subordinate nodes that in turn are connected to other subordinate nodes and so forth, forming a tree like structure.
5. **Mesh network –** this topology is the newest type and does not use a specific physical layout (such as star or tree). Rather, the mesh network requires that each node have more than one connection to the other nodes. The resulting pattern forms the appearance of a mesh.

**2. Strategies**

Every network has a strategy, or a way of sharing information and resources. Common network strategies include:

1. **Client/server (Hierarchical) network –** central computer coordinate and supply services to other nodes; based on specialization of nodes; widely used on the internet; able to handle very large networks efficiently; powerful network management software available.
2. **Peer-to-peer network –** nodes have equal authority and act as both clients and servers; widely used to share games, movies, and music over the internet; easy to set up and use; lacks security controls.

### Networking Devices

1. **Hub**

Tambuwal (2015) defines a Hub as a physical layer device. It’s used to extent a network and strength of a signal. A Hub is one of the network devices that is installed at the Access layer of an Ethernet Network. Hubs contain multiple ports that are used to connect hosts to the network. Hub does not decode message sent b/t host on the network. Hubs cannot determine which host should get any particular message, so it regenerates the same message out of the other post.

Only one message can be sent through be Ethernet hub at a time, when two or more host connected to a hub attempt to send a message at the same time, the electronic signals that make up the messages collide with each other at the hub. A collusion causes the message to become garbled and unreadable by the hosts.

1. **Switch**

Tambuwal (2015) defines a switch as a data link layer device and can deliver packets to a particular part of network that understand MAC address.

An Ethernet switch is a device that is used at the access layer. Like a hub, a switch connect multiple host to the network. Unlike host, a switch can forward a message to a specific host.

When a host sent a message to another host on a switch, the switch accept and decode the frames to read the physical MAC address portion of the message.

A table on the switch called a MAC address table, contains a list of all of the active ports and host MAC address that are attached to them. When a message is sent b/w hosts, the switch checks to see if the destination MAC address is in the table. If it’s the switch build a temporary connection called circuit between the sources and destination ports.

1. **Router**

Dr. A. Y Tambuwal (2015) defines a router as a network device that connect from one network to another and can understand IP address.

A router is a networking device that connects a local network to other local networks. Routers, like switches, are able to decode and read the messages that are sent to them. Unlike switches, which only decode (Un-encapsulate) the frame containing the MAC address information, routers decode the packet that is encapsulated within the frame.

The packet format contains the IP addresses of the destination and source hosts, as well as the message data being sent between them. Each port, or interface, on a router connects to a different local network.

### 2.2.4 Common Network Cables

Many different types of cables exist to interconnect the various devices in a NOC or local network.

There are two kinds of physical cable. Metal cables, usually copper, have electrical impulses applied to them to convey information. Fiber optic cables, made of glass or plastic, use flashes of light to convey information.

1. **Twisted Pair (TP)**

TP cable is one of most commonly used cables type in networking. Wires are grouped in pairs and twisted together to reduce inference. The pairs of wires are colored so that you can identify the same wire at each end.

Typically in each pair, one of the wires is solid color and its partiner is the same color striped onto a white background.

1. **Coaxial Cable**

Coaxial was one of the earliest types of network cabling developed. Coaxial cable is the kind of copper cable used by cable TV companies. Coaxial has a single rigid copper core that conduct the signal.

The core is typically surrounded by a layer of insulation, braided metal shielding and protective jacket.

It is used as a high-frequency transmission line to carry a high-frequency or broadband signals

1. **Fiber Optic Cable**

Fiber Optic cables can be either glass or plastic with a diameter about the same as a human hair that carry digital information at very high speed over a long distance.

Since they used light instead of electricity, electrical inference does not affect the signal. Fiber Optic cables have many uses as well as communications. They are also used in medical imagine, medical treatment and mechanical engineering inspection.

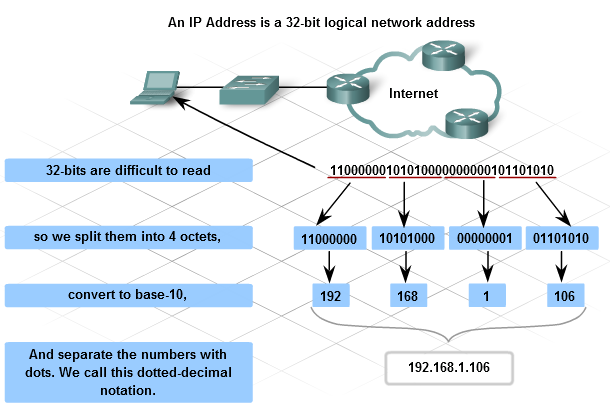
### 2.2.5 IP Address

One of the most important aspects of communications on an Internetwork is the logical addressing scheme.

IP addressing is the method used to identify hosts and network devices. The number of hosts connected to the Internet continues to grow, and the IP addressing scheme has had to be adapted to cope with this growth.

In order to send and receive messages on an IP network, every network host must be assigned a unique 32 bit IP address. Because large binary numbers are difficult for humans to read and understand, IP addresses are usually displayed in dotted-decimal notation. In dotted-decimal notation, each of the four octets is converted to a decimal number separated by a decimal point. For example, the IP address:

11000000.10101000.00000001.01101010 is represented as 192.168.1.106 in dotted decimal notation.



**Figure 2-1 IP Address**

### 2.2.6 Cisco Packet Tracer.

Packet Tracer is a medium fidelity, network-capable, simulation-based learning environment for networking novices to design, configure, and troubleshoot computer networks at a CCNA-level of complexity. Packet Tracer is an integrated simulation, visualization, collaboration, and assessment environment. Packet Tracer supports student and instructor creation of simulations, visualizations, and animations of networking phenomena. Like any simulation, Packet Tracer relies on a simplified model of networking devices and protocols. Real computer networks, experienced both in-person/hands-on and remotely, remain the benchmark for understanding network behavior and developing networking skills. Packet Tracer was created to help address the Digital Divide in networking education, where many students and teachers lack access to equipment, bandwidth, and interactive modes of learning networking

## 2.3 VLAN (VIRTUAL LOCAL AREA NETWORK)

Hosts and servers that are connected to Layer 2 switches are part of the same network segment. This arrangement poses two significant problems:

Switches flood broadcasts out all ports, which consumes unnecessary bandwidth. As the number of devices connected to a switch increases, more broadcast traffic is generated and more bandwidth is wasted.

Every device that is attached to a switch can forward and receive frames from every other device on that switch.

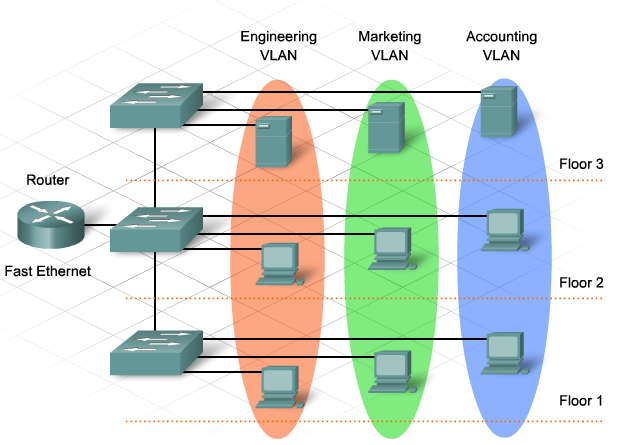
As a network design best practice, broadcast traffic is contained to the area of the network in which it is required. There are business reasons why certain hosts access each other while others do not. As an example, members of the accounting department may be the only users who need to access the accounting server. In a switched network, virtual local area networks (VLANs) are created to contain broadcasts and group hosts together in communities of interest.

Kennedy Clark & Kavin Hamilton (1999) defines VLAN Technically, as set forth by IEEE, VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the extent that a broadcast frame propagates through a network.

Cisco (2009) defines a VLAN as a logical broadcast domain that can span multiple physical LAN segments. It allows an administrator to group together stations by logical function, by project teams, or by applications, without regard to physical location of the users.

The difference between a physical network and a virtual, or logical, network can be shown in the following example:

The students in a school are divided into two groups. In the first group, each student is given a red card, for identification. In the second group, each student is given a blue card. The principal announces that students with red cards can only speak to other students with red cards and that students with blue cards can only speak to other students with blue cards. The students are now logically separated into two virtual groups, or VLANs.



**Figure 2-2 VLAN**

Using this logical grouping, a broadcast goes out only to the red card group, even though both the red card group and the blue card group are physically located within the same school.

This example also shows another feature of VLANs. Broadcasts do not forward between VLANs, they are contained within the VLAN.

Each VLAN functions as a separate LAN. A VLAN spans one or more switches, which allows host devices to behave as if they were on the same network segment.

A VLAN has two major functions:

* A VLAN contains broadcasts.
* A VLAN groups devices. Devices located on one VLAN are not visible to devices located on another VLAN.

Traffic requires a Layer 3 device to move between VLANs.

In a switched network, a device can be assigned to a VLAN based on its location, MAC address, IP address, or the applications that the device most frequently uses. Administrators assign membership in a VLAN either statically or dynamically.

1. **Static VLAN –** membership requires an administrator to manually assign each switch port to a specific VLAN. As an example, port fa0/3 may be assigned to VLAN 20. Any device that plugs into port fa0/3 automatically becomes a member of VLAN 20.
2. **Dynamic VLAN** – membership requires a VLAN management policy server (VMPS). The VMPS contains a database that maps MAC addresses to VLAN assignments. When a device plugs into a switch port, the VMPS searches the database for a match of the MAC address and temporarily assigns that port to the appropriate VLAN.

Dynamic VLAN membership requires more organization and configuration but creates a structure with much more flexibility than static VLAN membership. In dynamic VLAN, moves, adds, and changes are automated and do not require intervention from the administrator.

## 2.4 CONFIGURING SWITCHES AND ROUTER

### 2.4.1 Configuring Vlans

Cisco (2009) Whether VLANs are created statically or dynamically, the maximum number of VLANs depends on the type of switch and the IOS. By default, VLAN1 is the management VLAN.

An administrator will use the IP address of the management VLAN to configure the switch remotely. When accessing the switch remotely, the network administrator can configure and maintain all VLAN configurations.

When a VLAN is created, it is assigned a number and a name. The VLAN number is any number from the range available on the switch, except for VLAN1. Naming a VLAN is considered a network management best practice.

1. **Use the following commands to create a VLAN using global configuration mode:**

Switch(config)#vlan vlan\_number

Switch(config-vlan)#name vlan\_name

Switch(config-vlan)#exit

Assign ports to be members of the VLAN. By default, all ports are initially members of VLAN1. Assign ports one at a time or as a range.

1. **Use the following commands to assign individual ports to VLANs:**

Switch(config)#interface fa#/#

Switch(config-if)#switchport access vlan vlan\_number

Switch(config-if)# exit

1. **Use the following commands to assign a range ports to VLANs:**

Switch(config)#interface range fa#/start\_of\_range - end\_of\_range

Switch(config-if)#switchport access vlan vlan\_number

Switch(config-if)#exit

The removal of VLANs and the reassignment of ports to different VLANs are two separate and distinct functions. When a port is disassociated from a specific VLAN, it returns to VLAN1.

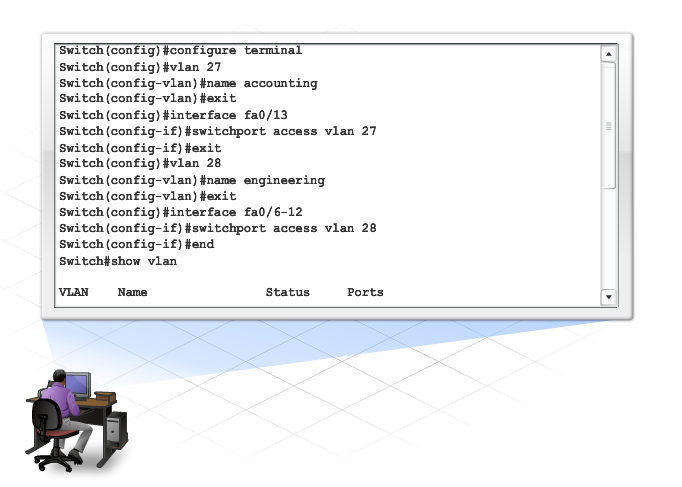
1. **To delete a VLAN:**

Switch(config)#no vlan vlan\_number

1. **To disassociate a port from a specific VLAN:**

Switch(config)#interface fa#/#

Switch(config-if)#no switchport access vlan vlan\_number



**Figure 2-3 Configuration Codes**

To verify, maintain, and troubleshoot VLANs, it is important to understand the key show commands that are available in the Cisco IOS.

1. **The following commands are used to verify and maintain VLANs:**

show vlan

* Displays a detailed list of all of the VLAN numbers and names currently active on the switch, along with the ports associated with each one
* Displays STP statistics if configured on a per VLAN basis

show vlan brief

* Displays a summarized list showing only the active VLANs and the ports associated with each one

show vlan id id\_number

* Displays information pertaining to a specific VLAN, based on ID number

show vlan name vlan\_name

* Displays information pertaining to a specific VLAN, based on name

### 2.4.2 Trunking and Inter-VLAN Routing

**Trunking**

A VLAN has three major functions:

* Limits the size of broadcast domains
* Improves network performance
* Provides a level of security

To take full advantage of the benefits of VLANs, they are extended across multiple switches.

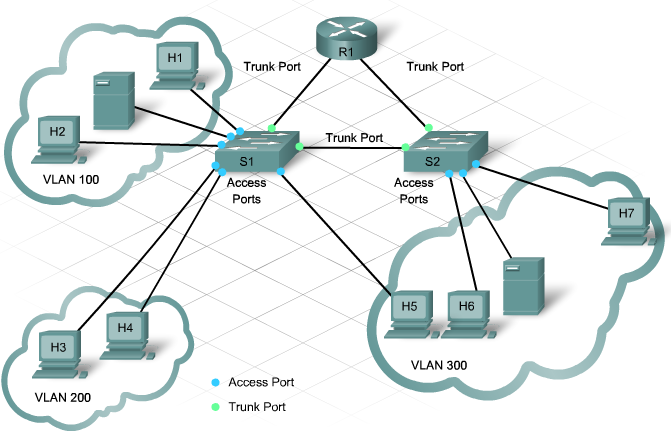
Switch ports can be configured for two different roles. A port is classified as either an access port or a trunk port.

1. **Access Port**

An access port belongs to only one VLAN. Typically, single devices such as PCs or servers connect to this type of port. If a hub connects multiple PCs to the single access port, each device connected to the hub is a member of the same VLAN.

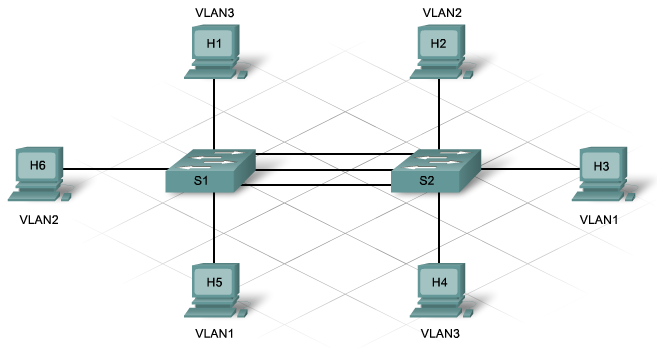
1. **Trunk Port**

A trunk port is a point-to-point link between the switch and another networking device. Trunks carry the traffic of multiple VLANs over a single link and allow VLANs to reach across an entire network. Trunk ports are necessary to carry the traffic from multiple VLANs between devices when connecting either two switches together, a switch to a router, or a host NIC that supports 802.1Q trunking.

****

**Figure 2-4 Access and Trunk Ports**

Without trunk ports, each VLAN requires a separate connection between switches. For example, an enterprise with 100 VLANs requires 100 connecting links. This type of arrangement does not scale well and is very expensive. Trunk links provide a solution to this problem by transporting traffic from multiple VLANs on the same link. When multiple VLANs travel on the same link, they need VLAN identification. A trunk port supports frame tagging. Frame tagging adds VLAN information to the frame.



**Figure 2-5 without trunk port**

Switch ports are access ports by default.

1. **To configure a switch port as a trunk port, use the following commands:**

Switch(config)#interface fa(controler # / port #)

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation {dot1q | isl | negotiate}

Switches that support both 802.1Q and ISL require the last configuration statement. The 2960 does not require that statement because it only supports 802.1Q.

1. **To return a trunk port to an access port, issue either of the following commands:**

Switch(config)#interface fa(controler # / port #)

Switch(config-if)#no switchport mode trunk

or

Switch(config-if)#switchport mode access

**Inter-VLAN Routing**

Although VLANs extend to span multiple switches, only members of the same VLAN can communicate.

A Layer 3 device provides connectivity between different VLANs. This arrangement enables the network administrator to strictly control the type of traffic that flows from one VLAN to another.

One method of accomplishing the inter-VLAN routing requires a separate interface connection to the Layer 3 device for each VLAN.

Another method for providing connectivity between different VLANs requires a feature called subinterfaces. Subinterfaces logically divide one physical interface into multiple logical pathways. Configure one pathway or subinterface for each VLAN.

To support inter-VLAN communication using subinterfaces requires configuration on both the switch and the router.

1. Switch:

Configure the switch interface as an 802.1Q trunk link.

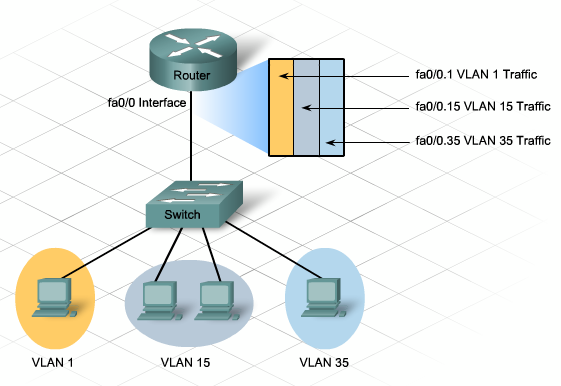
1. Router:

Select a router interface with a minimum of a 100Mbps FastEthernet.

Configure subinterfaces that support 802.1Q encapsulation.

Configure one subinterface for each VLAN.

A subinterface allows each VLAN to have its own logical pathway and default gateway into the router.



**Figure 2-6 Inter-VLAN routing**

The host from the sending VLAN forwards traffic to the router using the default gateway. The subinterface for the VLAN specifies the default gateway for all hosts in that VLAN. The router locates the destination IP address and does a routing table lookup.

If the destination VLAN is on the same switch as the source VLAN, the router forwards the traffic back down to the source switch using the subinterface parameters of the destination VLAN ID. This type of configuration is often referred to as a router-on-a-stick.

To configure inter-VLAN routing, use the following steps:

Configure a trunk port on the switch.

Switch(config)#interface fa0/2

Switch(config-if)#switchport mode trunk

On the router, configure a FastEthernet interface with no IP address or subnet mask.

Router(config)#interface fa0/1

Router(config-if)#no ip address

Router(config-if)#no shutdown

On the router, configure one subinterface with an IP address and subnet mask for each VLAN. Each subinterface has an 802.1Q encapsulation.

Router(config)#interface fa0/0.10

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 192.168.10.1 255.255.255.0

Use the following commands to verify the inter-VLAN routing configuration and functionality.

Switch#show trunk

Router#show ip interfaces

Router#show ip interfaces brief

Router#show ip route

# CHAPTER THREE: SYSTEM ANALYSIS AND DESIGN

## 3.1 INTRODUCTION

Whitten *et al*. (2001:13) defined system analysis as the study of a business problem domain to recommend improvements and specify the business requirement for the solution. It is a technique that decomposes a system into its component pieces for the purpose of studying how well those component parts work and interact to accomplish their purpose (Whitten *et al*., 2001).

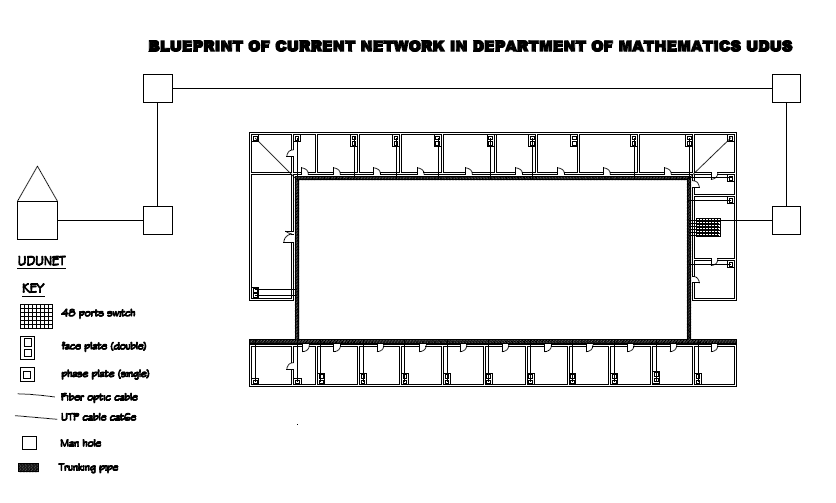
The key facilitator or player of the information system development game and computer application is called the System Analyst. A variety of system solving approaches is used by different system analysts due to the difference in problem domain under consideration and choice

This chapter focuses on the problem domain of this research topic- Design of Virtual Local Area Network (VLAN) for Mathematics Department, Usmanu Danfodiyo University Sokoto, Nigeria. It provides specification of what the new network would accomplish based upon requirements.

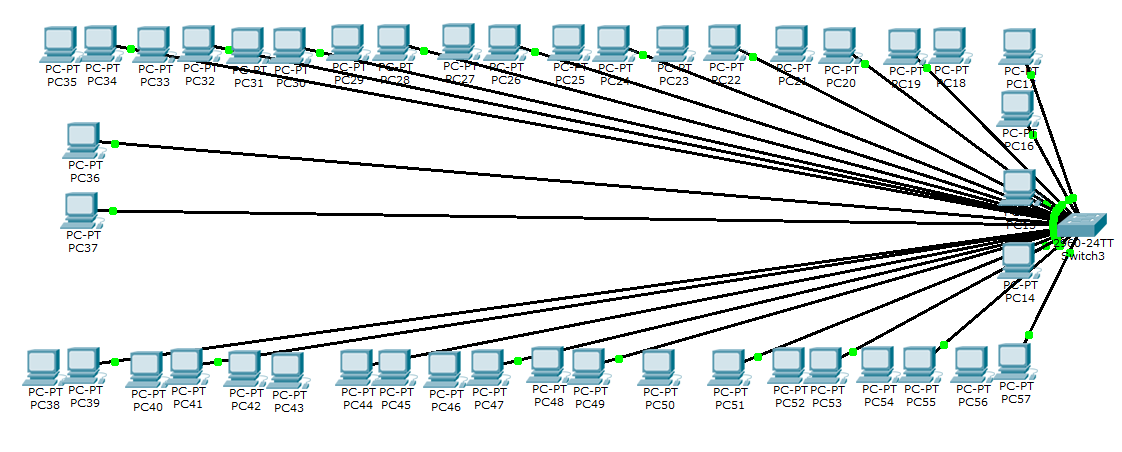
## 3.2 ANALYSIS OF THE CURRENT NETWORK

In the department of mathematics, there is one existing LAN network. The network has a switch called Access switch that is connected to the Core switch at UDUNET network, with a fiber optic cable for wireless connection.

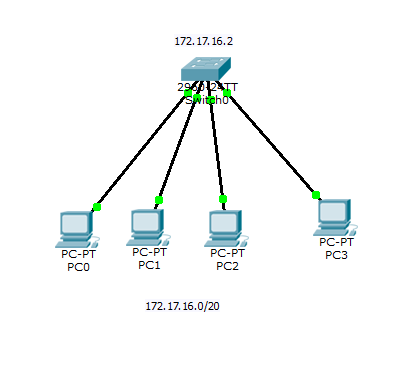
The network has its 48 port switch in the HOD office, which consists of a rank, a switch and a patch panel. A group Cat-5 cable (twisted pair cable for carrying signals) is connected to the switch ports using RJ-45 connector, and it is taken to every offices through the Trunking pipe where it is connected to the face plate available in that room in order to make the network available for the users in the room, instead of waiting for a particular user to disconnect his or her computer from the network.



**Figure 3-1 Blueprint of the current network**



**Figure 3-2 Physical topology of the current network**



**Figure 3-3 logical topology of the current network**

### 3.2.1 Problems of the current network

A network supposed to have a blueprint of its design for easy retrace when connection problem occurs but there is nothing like blueprint of the these current networks’ design which will make identification of the particular switch port to which an office link is connected to a difficult task in case a port of the faceplate in that office is disconnected from the network

Placing all host in one local network segment also has its own disadvantages. This include:

All host are in one broadcast domain which causes more traffic on the segment and may slow the network performance.

For security issues of the shared media nature of LAN networks. Whenever a station transmits in a *shared* network, all stations attached to the segment receive a copy of the frame, even if they are not the intended recipient. If the users on the network belong to the same department, this might not be disastrous, but when users from mixed departments share a segment, undesirable information captures can occur.

When users attach to the same shared segment, they share the bandwidth of the segment. The more users that attach to the shared cable means less average bandwidth for each user. If the sharing becomes too great, user applications start to suffer.

Based on results obtained from the system studies, an overall analysis of the current network is thoroughly made in a detailed manner leading to the specification of the new network. Here, task to be accomplished by separate elements of the new network are identified.

The importance of resource sharing and data communication over a network can never be over emphasized. In fact, the essence of networking derived from the origin was to disallow unnecessary duplication of same knowledge and to encourage sharing of knowledge centering on various aspect. It is therefore necessary to state that with the implementation of a Virtual Local Area Network in Mathematics Department, effective resource sharing and communication will be achieved.

### 3.2.2 Feasibility Study

Feasibility is the measure of how beneficial the development of information system would be to the organization (Whittte *et al*., 2001). This made Whitte *et al*. (2001:42) to define feasibility study as the activity by which feasibility is measured and assessed. The main goal of feasibility study is not to solve a problem, but to accurately achieve its scope.

The principal work area for this research project is the Offices of Mathematics Department Lecturers, Usmanu Danfodiyo University Sokoto, Nigeria. The offices are currently connected to the LAN network, the aim of this research is very much necessary and must be realized to achieve a standard network that other departments within the university will desire.

However, the question of realizing the aim of this project is assessed here. Because the benefit and importance of this research work outweigh its cost, the research work is deemed economically feasible. The research work is further deemed operationally feasible for once all installation works are completed; the proposed network will operate as required. Other feasibility measures as schedule and risk have been assessed and deemed fit for this research work.

This research work stresses the need to network the staff offices of Mathematics Department and having installed this network according to the design proposed in this research work, the overall performance of Mathematics Department will move to a greater height as the efficiency relies heavily on the accuracy of the Network Engineer and the Administrator.

The benefits and improvements of the new network design if installed include:

1. The network, having connects all the staff offices of Mathematics Department, will enable sharing of a single hardware devices like a printer or scanner, instead of installing one in each of the offices.
2. Creation of various logical groups to provide more security and more broadcast domain to the network.
3. Information circulation and communication through broadcast messages, emails etc. instead of going from office to office just to pass information.
4. Enable Remote login, desktop sharing and file sharing like submission of students’ result to the Examination Officer and other related documents across the network for effective use.
5. Easy detection and fixing of faulty port in case of any room that is disconnected from the network since the network design has a blue print for easy tracing.
6. The network devices and their connections are highly protected from abuse and interruption respectively since the Head of Department’s office which has some level off restrictions is used as the networking devices room

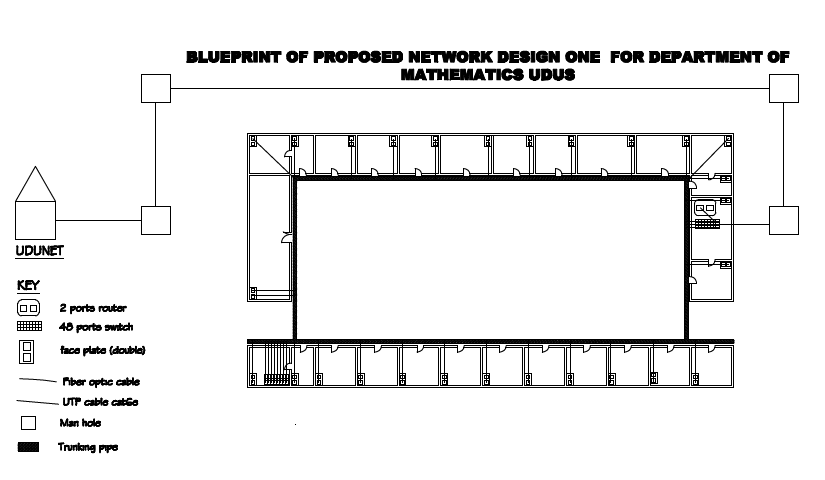
## 3.3 NEW DESIGNS

The process involved in the building of a new system by utilizing the information gained or collected during system analysis is known as System Design.

System design defines the architecture, components, modules, interface and data of the new system. It must therefore, produce a complete picture of the input, processing, storage and output requirement of the new system (Waites and Knott, 1996).

Here, the system design focuses on the implementation of the ‘new network’ under consideration, by identifying and installing the best fitting networking medium and devices.

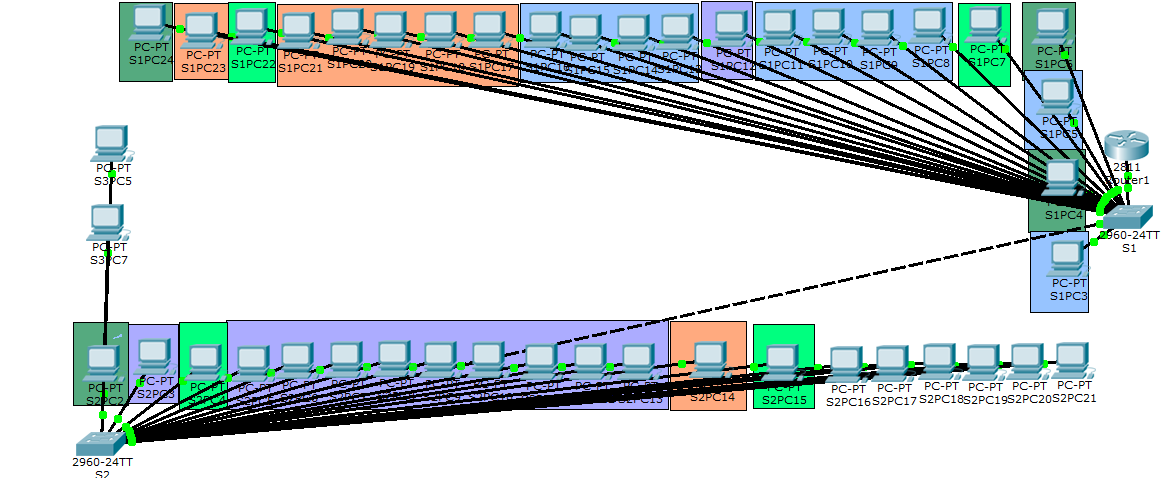
### 3.3.1 Proposed Network Design 1



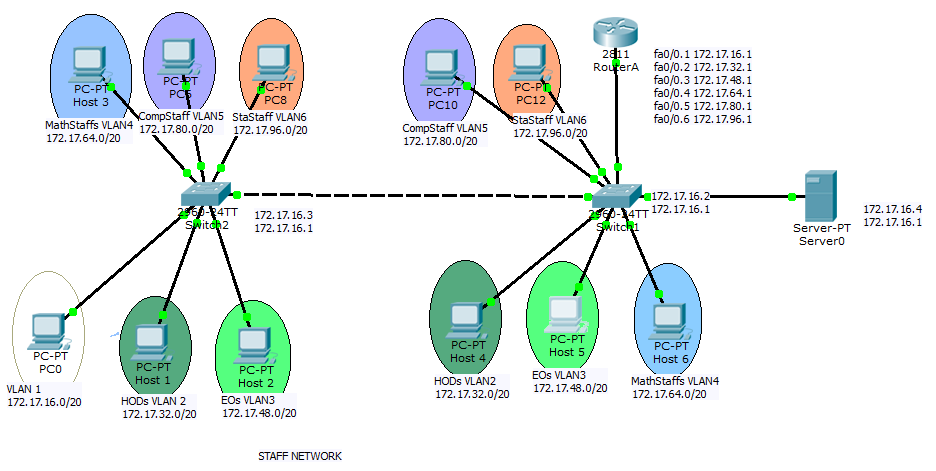
**Figure 3-4 blueprint of network desing1**

The network above consist of two 48 - ports switches (switch 1 and switch 2). Switch1 is connected to the Core switch at UDUNET network, with a fiber optic cable for wireless connection.

The network has its switch1 in the HOD office, which consists of a rack cabinet, and a patch panel. A group Cat-6 cable (twisted pair cable for carrying signals) is connected to the switch ports using RJ-45 connector, and it is taken to offices M1 to M12 through the trunking pipe where it is connected to the face plate available in that room and switch2 located in the HOU Computer office, which also consist of a rack cabinet, and a patch panel. A group Cat-6e cable (twisted pair cable for carrying signals) is connected to the switch ports using RJ-45 connector, and it is taken to offices M13 to M23 through the trunking pipe where it is connected to the face plate available in that room. The network is grouped into VLAN1 (default), VLAN2 (for H.O.D’s), VLAN3 (for Exams Officers), VLAN4 (for Mathematics Staff), VLAN5 (for Computer Staff) andVLAN6 (for Statistics Staff), providing 6 different broadcast domain. A good procedure was used while assigning each host to it respective switch and respective port for easy retrace when connection problem occurs and makes identification of the particular switch port to which an office link is connected to in case a port of the faceplate in that office is disconnected from the network. For example: a host with name PC-PT S”x”PC”y” belongs to Switch”x” port”y”.



**Figure 3-5 physical topology of design1**



**Figure 3-6 logical topology of design1**

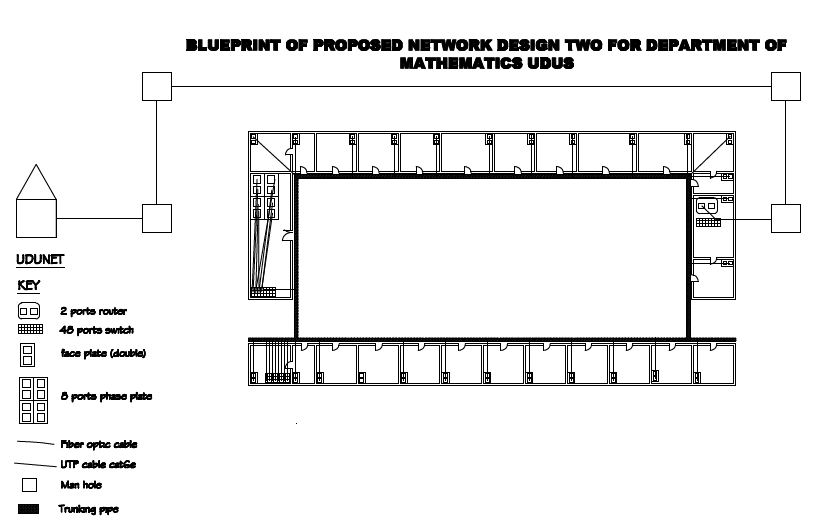
The advantages of placing host in remote network segment are:

1. More appropriate for large, more complex networks
2. Splits up broadcast domains and decreases traffic
3. Can improve performance on each segment
4. Makes the machines invisible to those on other local network segment
5. Can provide increased security
6. Can improve network organization

Some of the disadvantages of placing host in remote network segment include:

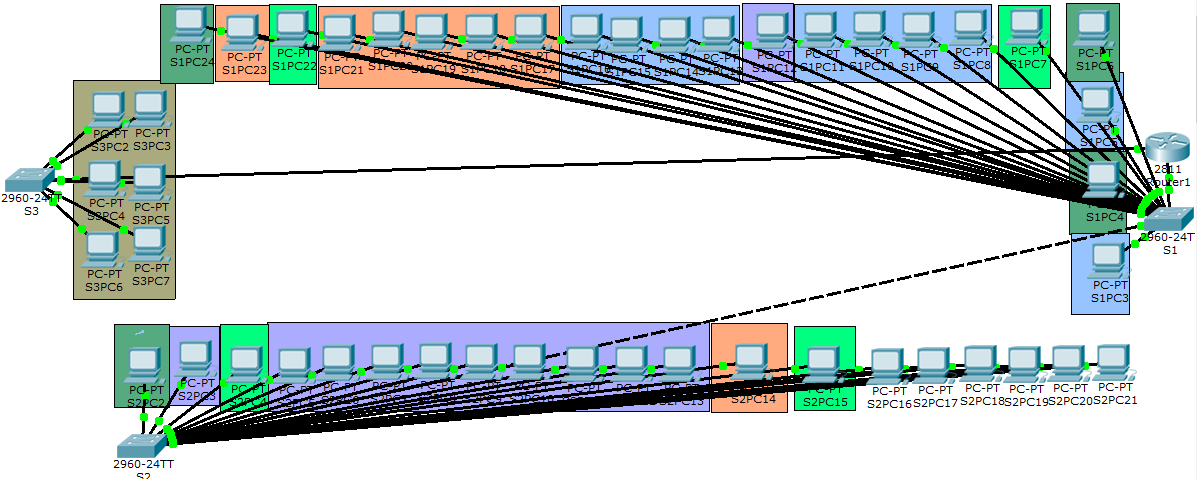
1. Requires the use of Routing (distribution layer)
2. Router can slow traffic between segments
3. More complexity and expense (requires Router)

### 3.3.2 Proposed Network Design 2

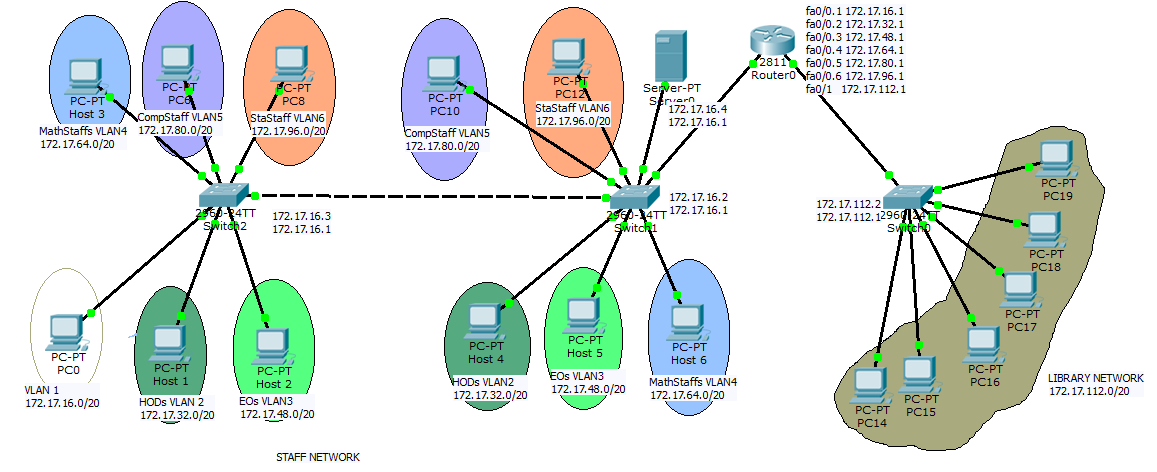


**Figure 3-7 Blueprint of design2**

This network is similar to the proposed design 1 network with the additional of library network for future when the library will be used as a computer lab for the use of students of mathematics department. The room is provided with a 24 port switch which will enable up to 23 host to be connected to it using a group Cat-6e cable (twisted pair cable for carrying signals) which is connected to the switch ports using RJ-45 connector. A good procedure was used while assigning each host to it respective switch and respective port for easy retrace when connection problem occurs and makes identification of the particular switch port to which an office link is connected to in case a port of the faceplate in that office is disconnected from the network. For example: a host with name PC-PT S”x”PC”y” belongs to Switch”x” port”y”



**Figure 3-8 physical topology of design2**

**Figure 3-9 Logical topology of design2**

Advantages of the network of the design are

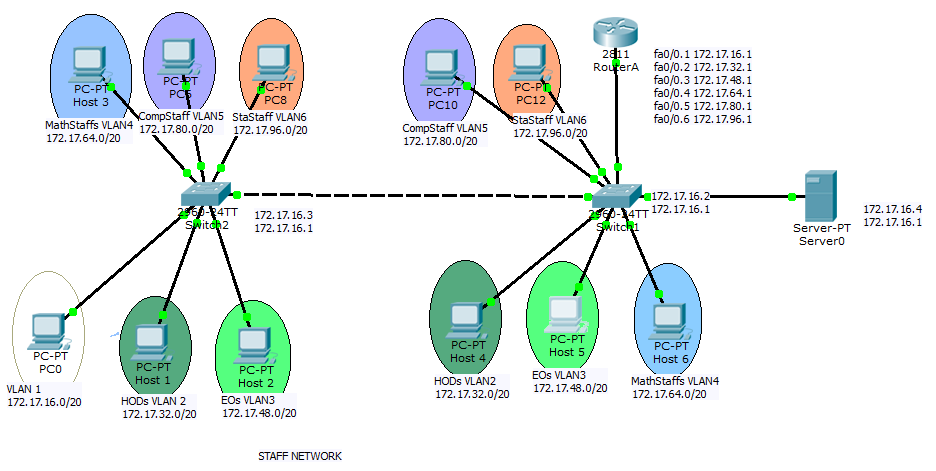
1. All the advantages of design1
2. Additional of students network (broadcast domain)

Disadvantages of the network are:

1. All the disadvantages of the network design1
2. Additional cost of networking materials.

# CHAPTER FOUR: SYSTEM IMPLEMENTATION AND TESTING

## 4.1 SYSTEM IMPLEMENTATION AND TESTING OF DESIGN 1



|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Host name | VLAN2 | VLAN3 | VLAN4 | VLAN5 | VLAN6 | VLAN1 | IP Address | Trunk | password | Secret |
| RouterA |  |  |  |  |  |  |  | Fa0/0 | mathdept | Units |
| Switch1 | Fa0/4 Fa0/22 | Fa0/7 Fa0/22 | Fa0/3, Fa0/5, Fa0/8-11,  Fa0/13-16 | Fa0/12 | Fa0/17-21  Fa0/23 | All remaining ports | 172.17.16.3/20 | Fa0/1  Fa0/2 | mathdept | Units |
| Switch2 | Fa0/2 | Fa0/4  Fa0/15 | Fa0/24 | Fa0/3  Fa0/5-13 | Fa0/14 | All remaining ports | 172.17.16.4/20 | Fa0/1 | mathept | Units |

**Figure 4.1 Logical Desing1**

**Table4.1 Table of contents for Design 1**

**Objectives**

1. Configure two switches, one as a VTP server and the other as a VTP client.
2. Configure six VLANs on the VTP server switch and propagate this information to the VTP client.
3. Configure VLAN configuration on Router A.
4. Configure inter-VLAN routing using a router-on-a-stick configuration.
5. Verify connectivity between the VLANs.

**Step 1: Connect the equipment**

a. Connect the router Fa0/0 interface with a straight-through cable to Switch 1 Fa0/2 interface.

b. Connect Switch 1 Fa0/1 port to the Fa0/1 port on Switch 2 using a crossover cable.

c. Connect a PC with a console cable to perform configurations on the router and switches.

**Step 2: Perform basic configurations on the router**

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. Configure Router A with a hostname and console, Telnet, and privileged passwords according to the table diagram.

Router(config)#hostname RouterA

RouterA(config)#

RouterA(config)#enable password mathdept

RouterA(config)#enable secret units

RouterA(config)#

RouterA(config)#line console 0

RouterA(config-line)#password mathdept

RouterA(config-line)#login

RouterA(config-line)#line vty 0 15

RouterA(config-line)#password mathdept

RouterA(config-line)#login

RouterA(config-line)#end

**Step 3: Configure VLAN trunking on the router**

Configure Router a Fa0/0 interface to trunk for VLAN 1, VLAN 2 VLAN3, VLAN 4, VLAN5, and VLAN6 with 802.1Q encapsulation.

RouterA(config)#interface fa0/0

RouterA(config-if)#**no shutdown**

RouterA(config-if)#**interface fa0/0.1**

RouterA(config-subif)#**encapsulation dot1Q 1**

RouterA(config-subif)#ip address 172.17.16.1 255.255.240.0

RouterA(config-subif)#**exit**

RouterA(config)#interface fa0/0.2

RouterA(config-subif)#**encapsulation dot1Q 2**

RouterA(config-subif)#ip address 172.17.33.1 255.255.240.0

RouterA(config-subif)#**exit**

RouterA(config)#interface fa0/0.3

RouterA(config-subif)#**encapsulation dot1Q 3**

RouterA(config-subif)#ip address 172.17.48.1 255.255.240.0

RouterA(config-subif)#**end**

RouterA(config)#interface fa0/0.4

RouterA(config-subif)#**encapsulation dot1Q 4**

RouterA(config-subif)#ip address 172.17.64.1 255.255.240.0

RouterA(config-subif)#**end**

RouterA(config)#interface fa0/0.5

RouterA(config-subif)#**encapsulation dot1Q 5**

RouterA(config-subif)#ip address 172.17.80.1 255.255.240.0

RouterA(config-subif)#**end**

RouterA(config)#interface fa0/0.6

RouterA(config-subif)#**encapsulation dot1Q 6**

RouterA(config-subif)#ip address 172.17.96.1 255.255.240.0

RouterA(config-subif)#**end**

**Step 4: .Configure Switch 1**

1. Configure Switch 1 with a hostname and console, Telnet, and privileged passwords according to the table diagram.

Switch(config)#hostname Switch1

Switch1(config)#

Switch1(config)#exit

Switch1(config)#enable password mathdept

Switch1(config)#

Switch1(config)#enable secret units

Switch1(config)#

b. Configure Switch 1 with the VLAN 1 IP address of 172.17.16.2/20.

Switch1(config)#**interface vlan 1**

Switch1(config-if)#**ip address 172.17.16.2 255.255.240**

Switch1(config-if)#**no shutdown**

Switch1(config-if)#**end**

c. On Switch 1, create VLAN 2 named HODs, VLAN 3, named Eos, VLAN 4 named MathUnitStaffs, VLAN 5 named CmpUnitStaffs, VLAN 6 named StaUnitStaffs,

Switch1(config)#**vlan 2**

Switch1(config-vlan)#**name HODs**

Switch1(config-vlan)#**exit**

Switch1(config)#**vlan 3**

Switch1(config-vlan)#**name EOs**

Switch1(config-vlan)#**exit**

Switch1(config)#

Switch1(config)#**vlan 4**

Switch1(config-vlan)#**name MathUnitStaffs**

Switch1(config-vlan)#**exit**

#Switch1(config)#**vlan 5**

Switch1(config-vlan)#**name CmpUnitStaffs**

Switch1(config-vlan)#**exit**

Switch1(config)#

Switch1(config)#**vlan 6**

Switch1(config-vlan)#**name StaUnitStaffs**

Switch1(config-vlan)#**exit**

d. Configure Switch 1 with the default gateway address of 172.17.16.1.

Switch1(config)#ip default-gateway 172.17.16.1

Switch1(config)#end

e. Configure Switch 1 with the interfaces

Switch1(config)#interface fa0/4

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 2

Switch1(config-if)#exit

Switch1(config)#interface fa0/6

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 2

Switch1(config-if)#exit

Switch1(config)#

Switch1(config)#interface fa0/24

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 2

Switch1(config-if)#exit

Switch1(config)#

Switch1(config)#interface fa0/7

Switch1(config-if)#switchport mode access

Switch1(config-if)#swit

Switch1(config-if)#switchport access vlan 3

Switch1(config-if)#exit

Switch1(config)#

Switch1(config)#interface fa0/22

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 3

Switch1(config-if)#exit

Switch1(config)#

Switch1(config)#interface fa0/3

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 4

Switch1(config-if)#exit

Switch1(config)#

Switch1(config)#interface fa0/5

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 4

Switch1(config-if)#exit

Switch1(config)#

Switch1(config)#interface range fa0/8-11

Switch1(config-if-range)#switchport mode access

Switch1(config-if-range)#switchport access vlan 4

Switch1(config-if-range)#exit

Switch1(config)#

Switch1(config)#interface range fa0/13-16

Switch1(config-if-range)#switchport mode access

Switch1(config-if-range)#switchport access vlan 4

Switch1(config-if-range)#exit

Switch1(config)#

Switch1(config)#exit

Switch1(config)#interface fa0/12

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 5

Switch1(config-if)#exit

Switch1(config)#

Switch1(config)#interface range fa0/17-21

Switch1(config-if-range)#switchport mode access

Switch1(config-if-range)#switchport access vlan 6

Switch1(config-if-range)#exit

Switch1(config)#

Switch1(config)#interface fa0/23

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 6

Switch1(config-if)#exit.

f. Configure all other interfaces on Switch 1 in VLAN 1. By default, there is only a single VLAN for all ports. You cannot rename or delete VLAN 1. Therefore, no further configuration is necessary. To prove this, issue the command **show vlan brief**.

**Step 5: Configure VLAN trunking on Switch 1**

a. Configure trunking between Switch 1 and Switch 2 with 802.1 encapsulation using port Fa0/2 on both switches.

Switch1(config)#intertacw fa0/2

Switch1(config-if)#switchport mode trunk

Switch1(config-if)#exit

b. Configure trunking between Switch 1 and Router A with 802.1 encapsulation using port Fa0/1 on Switch 1.

Switch1(config)#int fa0/1

Switch1(config-if)#switchport mode trunk

Switch1(config-if)#end

Switch1#

**Step 6: Configure VTP on Switch 1**

a. Configure Switch 1 as part of VTP domain Group 1.

Switch1(config)#vtp domain Group1

Changing VTP domain name from NULL to Group1

b. Configure Switch 1 as the VTP server and Switch 2 as the VTP client.

Switch1(config)#**vtp mode server**

Device mode already VTP SERVER.

Switch1(config)#**end**

**Step 7: Configure Switch 2**

1. Configure Switch 2 with a hostname and console, Telnet, and privileged passwords according to the table diagram.

Switch(config)#hostname Switch2

Switch2(config)#end

Switch2(config)#enable password mathdept

Switch2(config)#

Switch2(config)#enable secret units

Switch2(config)#

1. Configure Switch 2 with the VLAN 1 IP address of 172.17.16.3/20.

Switch2(config)#**interface vlan 1**

Switch2(config-if)#**ip address 172.17.16.3 255.255.240**

Switch2(config-if)#**no shutdown**

Switch2(config-if)#**end**

1. Configure Switch 2 with the default gateway address of 172.17.16.1.

Switch2(config)#ip default-gateway 172.17.16.1

Switch2(config)#end

d. Configure Switch 2 with the interfaces

Switch2(config)#interface fa0/2

Switch2(config-if)#switchport mode access

Switch2(config-if)#switchport access vlan 2

Switch2(config-if)#exit

Switch2(config)#interface fa0/4

Switch2(config-if)#switchport mode access

Switch2(config-if)#switchport access vlan 3

Switch2(config-if)#exit

Switch2(config)#

Switch2(config)#interface fa0/15

Switch2(config-if)#switchport mode access

Switch2(config-if)#switchport access vlan 3

Switch2(config-if)#exit

Switch2(config)#

Switch2(config)#interface fa0/24

Switch2(config-if)#switchport mode access

Switch2(config-if)#switch access vlan 4

Switch2(config)#interface fa0/3

Switch2(config-if)#swit

Switch2(config-if)#switchport mode access

Switch2(config-if)#swit

Switch2(config-if)#switchport access vlan 5

Switch2(config-if)#exit

Switch2(config)#

Switch2(config)#interface range fa0/5-13

Switch2(config-if-range)#switchport mode access

Switch2(config-if-range)#switchport access vlan 5

Switch2(config-if-range)#exit

Switch2(config)#

Switch2(config)#interface fa0/14

Switch2(config-if)#switchport mode access

Switch2(config-if)#switchport access vlan 6

Switch2(config-if)#exit

**Step 8: Configure VLAN trunking on Switch 2**

Switch2(config)#int fa0/1

Switch2(config-if)#switchport mode trunk

Switch2(config-if)#exit

**Step 9: Configure VTP on Switch 2**

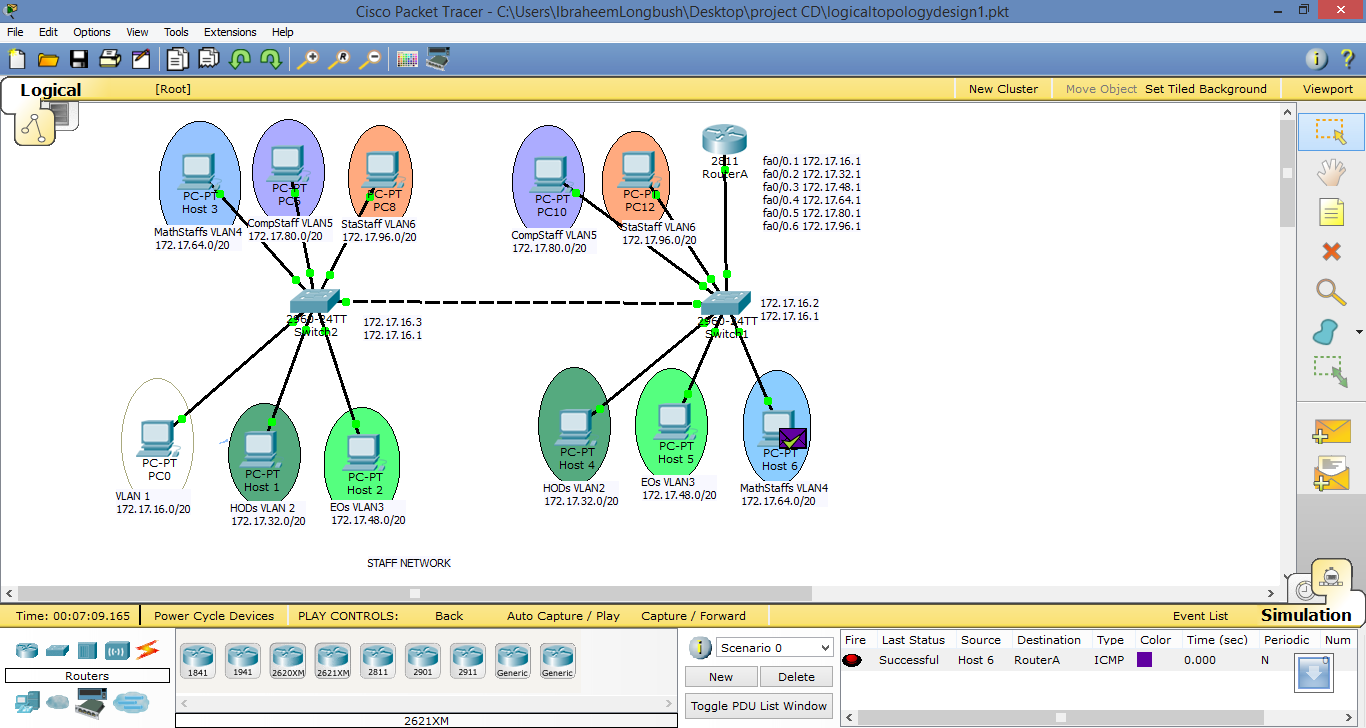
Switch2(config)#**vtp mode client**

**Testing**

The router and switches should be able to ping the interfaces of the other devices.

1. From each device, issue a ping to all interfaces.

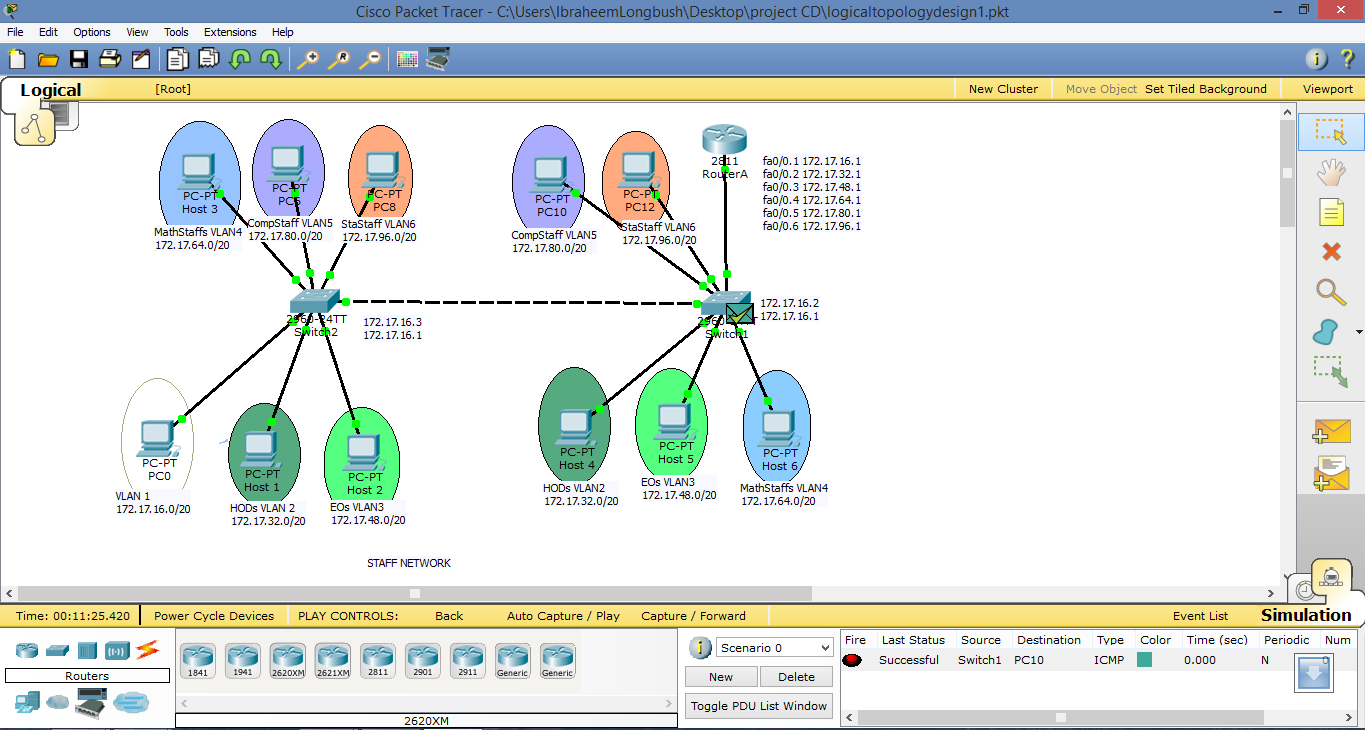
Each device should be able to ping each other in the network. The figure 4-2 below shows host 6 pings to router0. The ping is successful. But it the ping failed, try sending again. If the problem persist check the IP address of the host and default gateway.



**Figure 4-2 Ping from Host 6 to Router0**

1. From Switch 1, ping to all other devices.

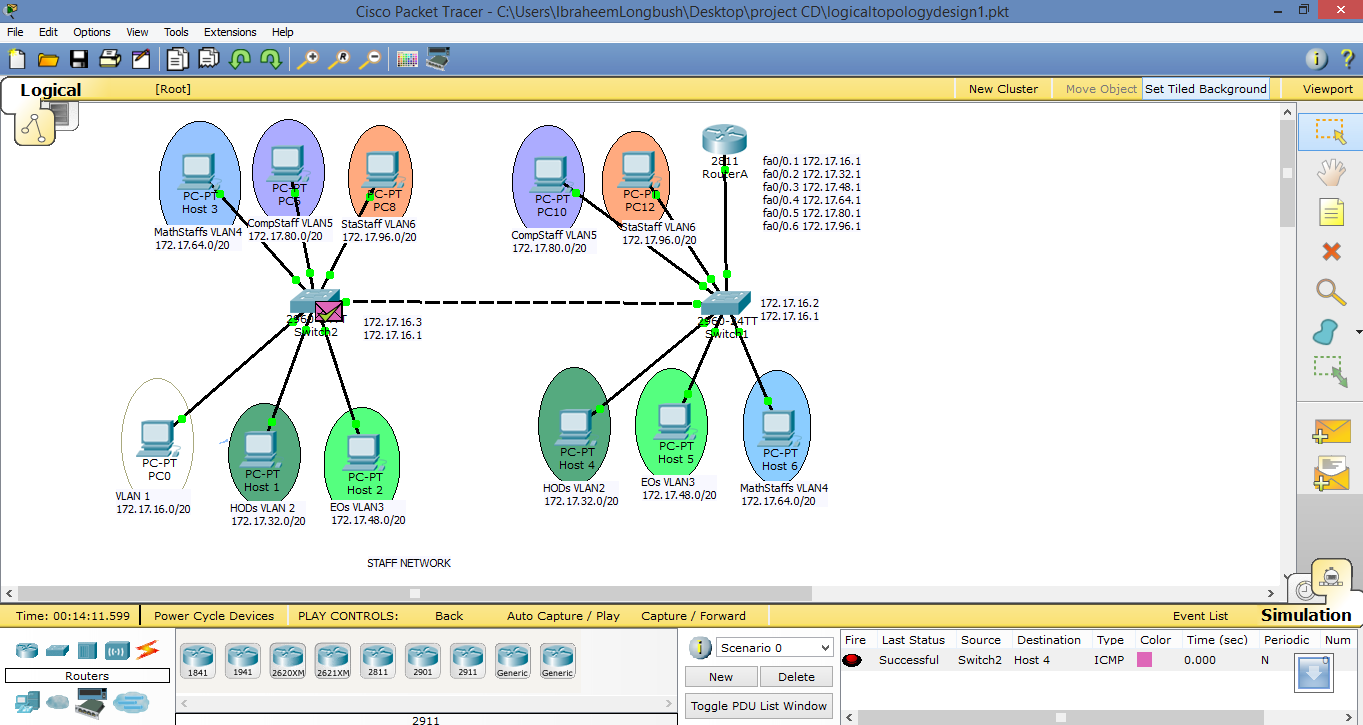
All the devices should be able to send a ping to switch 1 successfully. If the ping failed, resend it again may be it’s due to the connection failure. If the problem persist, check if the host is connected to the switch port properly. The figure 4-3 shows switch 1 pings PC 10 successfully and vice versa.



**Figure 4-3 Ping from Switch1 to PC10**

1. From Switch 2, ping to all other devices.

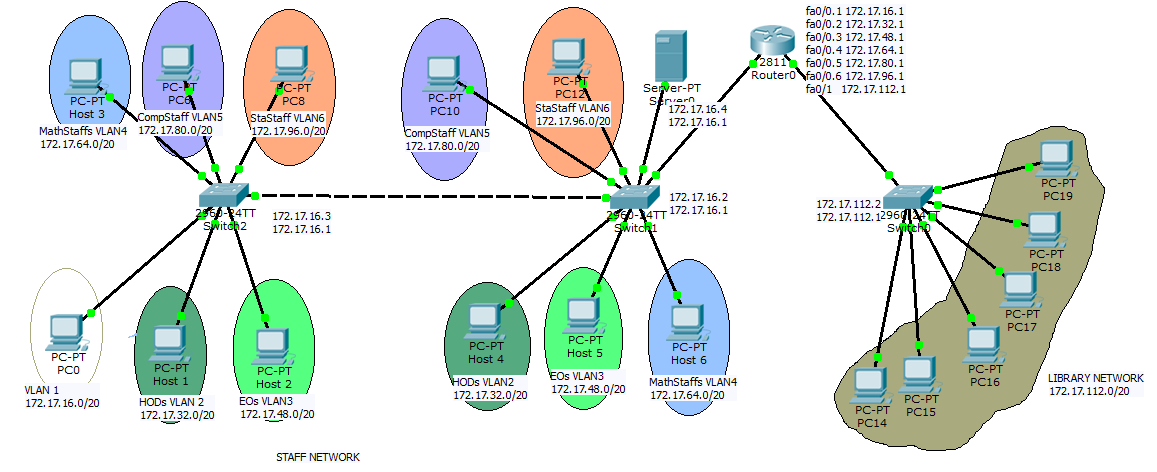
So also all the devices should be able to send a ping to switch 2 successfully. If the ping failed, resend it again maybe it’s due to the connection failure. If the problem persist, check if the host is connected to the switch port properly. The figure 4-4 shows switch 2 pings Host 4 successfully and vice versa.



**Figure 4-4 Ping from Switch2 to Host 4**

If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the router and switch configurations.

## 4.2 SYSTEM IMPLEMENTATION AND TESTING OF DESIGN TWO



**Figure 4-5 Logical design 2**

**Table 4-2 Table of contents for Design 2**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Host name | VLAN2 | VLAN3 | VLAN4 | VLAN5 | VLAN6 | VLAN1 | IP Address | Trunk | password | Secret |
| RouterA |  |  |  |  |  |  |  | Fa0/0  Fa0/2 | mathdept | Units |
| Switch1 | Fa0/4 Fa0/22 | Fa0/7 Fa0/22 | Fa0/3, Fa0/5, Fa0/8-11,  Fa0/13-16 | Fa0/12 | Fa0/17-21  Fa0/23 | All remaining ports | 172.17.16.3/20 | Fa0/1  Fa0/2 | mathdept | Units |
| Switch2 | Fa0/2 | Fa0/4  Fa0/15 | Fa0/24 | Fa0/3  Fa0/5-13 | Fa0/14 | All remaining ports | 172.17.16.4/20 | Fa0/1 | mathdept | Units |
| Switch3 |  |  |  |  |  | All ports | 172.17.112.2/20 | Fa0/1 | mathdept | Units |

**Perform all the configuration from Step 1 to 10 in Design 1**

**Step 11: Configure on Router**

Add the following configurations to the router

RouterA(config)#interface fa0/1

RouterA(config-if)#**ip address 172.17.112.1 255.255.240.0**

RouterA(config-if)#**no shutdown**

RouterA(config-if)#**exit**

**Step 12: Configure Switch 3**

1. Configure Switch 3 with a hostname and console, Telnet, and privileged passwords according to the table diagram.

Switch(config)#hostname Switch3

Switch3(config)#end

Switch3(config)#enable password mathdept

Switch3(config)#

Switch3(config)#enable secret units

Switch3(config)#

Switch3(config)#line console 0

Switch3(config-line)#password mathdept

Switch3(config-line)#login

Switch3(config-line)#line vty 0 15

Switch3(config-line)#password mathdept

Switch3(config-line)#login

Switch3(config-line)#end

1. Configure Switch 2 with the VLAN 1 IP address of 172.17.112.2/20.

Switch3(config)#**interface vlan 1**

Switch3(config-if)#**ip address 172.17.112.2 255.255.240**

Switch3(config-if)#**no shutdown**

Switch3(config-if)#**end**

1. Configure Switch 3 with the default gateway address of 172.17.112.1.

Switch3(config)#ip default-gateway 172.17.112.1

Switch3(config)#end

1. Configure all other interfaces on Switch 1 in VLAN 1. By default, there is only a single VLAN for all ports. You cannot rename or delete VLAN 1. Therefore, no further configuration is necessary. To prove this, issue the command **show vlan brief**.
2. Configure VLAN trunking on Switch

Configure trunking between Switch 3 and Router with 802.1 encapsulation using port Fa0/1 on switch 3

Switch3(config)#intertacw fa0/1

Switch3(config-if)#switchport mode trunk

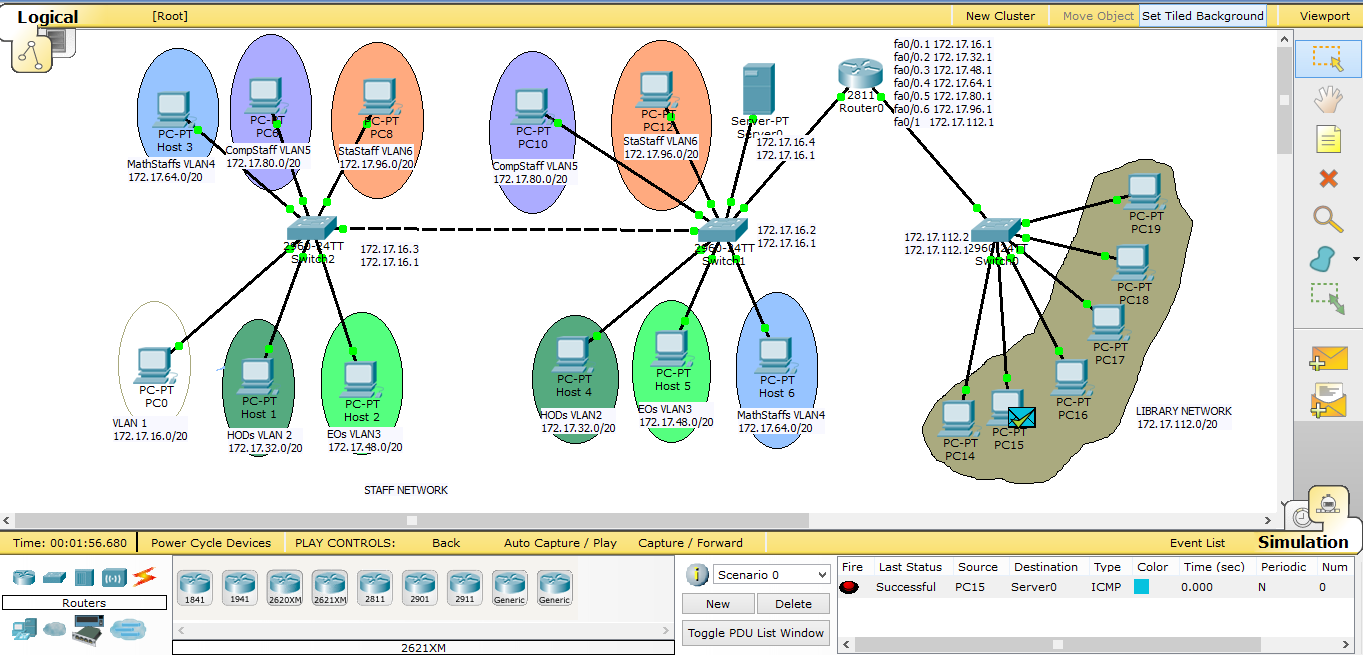
Switch3(config-if)#exit

**Testing**

The router and switches should be able to ping the interfaces of the other devices. All the testing in design 1 should also be successful in this design 2, and also:

From each device in library network, issue a ping to all interfaces. The Host in library network should be able to send a ping to all devices in staff network and also to the department’s server.

If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the router and switch configurations



**Figure 4-6 PC 15 pings Server and forwarded back**

# CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS.

## 5.1 SUMMARY

In this research project, an attempt has been made to network the offices of Mathematics Department staff of Usmanu Danfodiyo University, Sokoto. A study of the problem domain was conducted by studying the existing networks in the above Department and the observed setbacks are well documented. The problems of that domain include:

1. The networks not having a blue print of the design for easy maintenance.
2. All host are in one broadcast domain which causes more traffic on the segment and may slow the network performance.
3. Switches flood broadcasts out all ports, which consumes unnecessary bandwidth. As the number of devices connected to a switch increases, more broadcast traffic is generated and more bandwidth is wasted.
4. Every device that is attached to a switch can forward and receive frames from every other device on that switch, so when users from mixed departments share a segment, undesirable information captures can occur, which may result to network security problem.
5. LANs require physical administration as the location of the user changes, the need for recabling, addressing the new station, reconfiguration of routers and hubs arises. The mobility of the users in a network results in network costs.

It was based on these setbacks that this research study among other issues was carried out to reduce (or completely eliminated) the above problems especially the problem of one broadcast domain by creating multiple broadcast domain and the amount of stress associated in finding the particular switch port each of the connected offices is being connected to.

Further, analysis on the current functionality of the new network design was achieved by gathering domain requirements using information-gathering techniques. While subsequently refurnishing them, they finally resulted into what is called system requirements.

Therefore, the installation that will be carried out is entirely dependent upon the identified system requirements.

The new network was designed using Unshielded Twisted Pair (UTP) cable even though more cost is required for its installation.

## 5.2 CONCLUSION

As far as we live in the age and world of technology, the use of computer for information and communication processing is a welcome development.

With the deployment large number of switch ports, VLAN has become an indispensable tool for the network administration to segment the network to increase bandwidth per user, provide security and provision multimedia service. The evolution of VLAN as a simple broadcast containment device to a necessary function in the network, propel VLAN to be the number 1 tool in an IT professional’s bag of trick.

Networking as emphasized throughout this research work primarily enables the good culture of ‘sharing’. It is therefore necessary to state that with the implementation of a Virtual Local Area Network in Mathematics Department, effective resource sharing and communication will be achieved. Hence, implementation of this study is practically cost effective.

## 5.3 RECOMMENDATIONS

Regarding the conducted study, I recommend the following:

1. This research work should be fully implemented in the problem domain under consideration – the offices of Mathematics Department Lecturers, Usmanu Danfodiyo University Sokoto, Nigeria. This would surely be in the best interest of the lecturers and the entirety of the University in a bid to taking Mathematics department to a very high standard.
2. A modification of this study should be carried out by intending Network Administrators and Engineers so as to bring forth a befitting network for better network performance.
3. Security should be strictly enforced as stated while configuring the router and switches
4. In order to acquaint students with practicalities involved in Networking, the complete implementation of this study should be carried out in the company of all students of the Computer Science Unit if the school is on session. This will serve practical to Networking course.

# REFERENCES

CCNA Discovery 3 (2009). *Switching in an Enterprise Network.* Version 4.0.0.0. Cisco

Dr. A. Y Tambuwal (2015). Lecture Note: Data Communications and Networking. Usmanu Danfodiyo University, Sokoto.

Forouzan, B.A. (2004). *Data Communication and Networking*. 3rd edition. New Delhi: McGraw Hill Publishing Company.

Forouzan, B.A. (2007). *Data Communication and Networking*. 4rd edition. New Delhi:

Kennedy Clark & Kavin Hamilton (1999). *Cisco LAN Switching*. Cisco Press

Leon-Garcia, A. and Widjaja, I., (2000) *Communication Networks.* USA, McGraw Hill Companies.

Nnonyelum Ugomma Martha (2004). Design of a Local Area Network. Project

Timothy J. O’Leary (2005). *Computing Essentials 2005*: McGraw-Hill International Edition

Tanenbaum, A. S. (2003). *Computer Networks*. 4th edition. New Delhi: Prentice Hall.

Waites, N. and Knott, G. (1996). *Computing*. 2nd edition. Durham: Business Education Publishers Limited.

Whitten, J. L., Bentley, L. D. and Dittman, K C. (2001) *Systems Analysis and Design Methods.* 5th edition. New York: McGraw Hill Companies.

# GLOSSORY

**Node –** any device that is connected to a network. It could be computer, printer or data storage device.

**Client –** a node that request and uses resources available from other nodes. Typically, a client is a user’s personal computer.

**Server –** a node that shares resources with other nodes. Dedicated servers specialize in performing specific tasks. Depending on the task, they may be called an application server, database server, web server etc.

**Host –** any computer system that can be accessed over a network.

**Router –** a node that forwards or routes data packets from one network to their destination in another network.

**Switch –** central node that coordinates the flow of data by sending messages directly between sender and receiver nodes.

**Network operating systems (NOS) –** control and coordinate the activities of all computers and other devices on a network.

**Network administrator –** a computer specialist responsible for different network operation and implementation of new networks

**Bandwidth –** is a measurement of the width or capacity of the communication channel. Effectively, it means how much information can move across the communication channel in a given amount of time.

**Broadcast domain –** set of devices that receive broadcast frames originating from any devices within the set.

**Collision –** result when two or more devices transmit frames simultaneously which impact and become damage when they meet on the physical media

**Frame –** logical grouping of information sent over a transmission medium as a data link layer unit