

**VIRTUAL LOCAL AREA NETWORK**

**DESIGN FOR A CAMPUS-WIDE**

**INTERNET TRANSPORT**

**[F.U.T MINNA, BOSSO CAMPUS AS A**

**CASE STUDY]**

**BY**

**ADAMU BIZUN YAMAI [99/8028EE]**

**DEPARTMENT OF ELECTRICAL AND**

**COMPUTER ENGINEERING**

**F.U.T. MINNA**

**NOVEMBER 2005**

**VIRTUAL LOCAL AREANETWORK  
[VLAN] DESIGN FOR A CAMPUS-WIDE  
INTERNET TRANSPORT[F.U.T MINNA,  
BOSSO CAMPUS AS A CASE STUDY]**

**BY**

**ADAMU BIZUN YAMAI [99/8028EE]**

**A THESIS**

**SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS  
FOR THE AWARD OF BACHELOR OF ENGINEERING [B.ENG] IN  
ELECTRICAL AND COMPUTER ENGINEERING**

**TO THE**

**DEPARTMENT OF ELECTRICAL AND COMPUTER  
ENGINEERING**

**SCHOOL OF ENGINEERING AND ENGINEERING TECHNOLOGY**

**FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA**

**NIGER STATE**

**NOVEMBER 2005**

## DECLARATION

I declare that this project was designed and written by me under the supervision of Engr. M.S. Ahmed, a lecturer in the Department of Electrical and Computer Engineering, Federal University of Technology, Minna



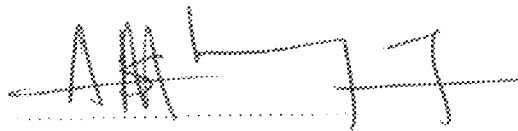
Adamu Bizun Yamai  
99/8028EE

8/12/2005

Date

## CERTIFICATION

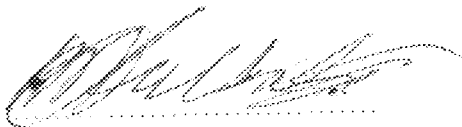
This is to certify that this work titled "Virtual Local Area Network (VLAN) design for a campus-wide internet transport (F.U.T. Minna, Bosso campus as a case study)" was carried out by Adamu Bizun Yamai under the supervision of Engr. M.S. Ahmed for the awards of Bachelor of Engineering (B.Eng) degree in Electrical/Computer Engineering of the Federal University Of Technology, Minna.



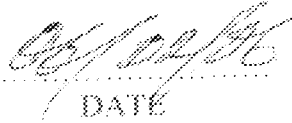
ENGR. M.S AHMED  
(PROJECT SUPERVISOR)



DATE



ENGR. M.D.ABDULLAHI  
(H.O.D)



DATE

.....  
EXTERNAL EXAMINER

.....  
DATE

## DEDICATION

To my parents: Mr. and Mrs. Adanu Bizun Kazabiriyind ,my brothers: Sheyin and Gideon, my sisters: Gloria, Damaris and Grace, and the NAVIGATOR family Minna

## ACKNOWLEDGEMENT

I want to acknowledge the giver and taker of life who has kept me this far

I also acknowledge the contributions of: my supervisor Engr. M. S. Ahmed, who was patient with me and also believed in what I was doing; my parents, who supported me morally, spiritually and financially to mention a few

I also acknowledge the support and encouragement I got from my friends and they are: Yerima, Yemi, George, Deola, Tolu, Drusilla, Dora, Kenny, Dan Onotu, Dan George, Okenwa, Ahmeh, Faith, and Ajingbe to mention a few.

I LOVE YOU ALL

## ABSTRACT

In a world where information is power and where information and communication technology [ICT] is the other of the day, there a need for an efficient means of communication[Virtual Local Area Network]], thus the need for decentralized computing

This project is a proposed design to establish an efficient network on campus via connecting all the Local Area Networks [LAN] using switches and routers . Optic fiber is used here for cabling because it can transport more information in much longer distance in less transmission time. This is because it has less attenuation and more bandwidth. Also it can't be affected by electromagnetic radiation. The network would be managed and kept secured by a network administrator

## TABLE OF CONTENT

Cover page	i
Title page	ii
Declaration	iii
Certification	iv
Dedication	v
Acknowledgement	vi
Abstract	vii
Table of content	viii
<u>Chapter One</u>	
1.0 Introduction	1
1.1 Data communication network	1
1.2 Aims and Objectives	1
1.3 Scope of study	2
1.4 Significance of study	3
<u>Chapter Two</u>	
2.0 Literature Review	4
2.1 Local Area Network	4
2.2 Wide Area Network	4



2.3 Full and Half Duplex Communication	4
2.4 Network Architecture	5
2.5 Peer-Peer Network	5
2.6 Client/Server Based Network	6
2.7 Advantages of Client/Server Network	7
2.8 Physical Topologies	8
2.9 Bus Topology	9
2.10 Star Topology	10
2.11 Ring Topology	10
2.12 Mesh	10
2.13 wireless	11
2.14 The OSI Reference Model	11
2.15 Common Network Connectivity Devices	14
2.16 Network Media	18
2.17 Cable Media	18
2.18 Wireless Media	19
2.19 LAN Architecture	19
2.20 LAN Adaptors, Drivers, and Protocols	22
2.21 LAN Adaptor Cards	22
2.22 LAN Adaptor Card Drivers	23
2.23 LAN Protocol	23
2.24 VLAN	24
2.25 Types of VLANs	25

2.26 Benefits of VLAN	27
2.27 How VLAN Works	29
2.28 VLAN Components	30
2.29 InterVLAN Routing	35
2.30 VLAN Standardization IEEE 802.1q	35
Chapter Three	
3.0 Design of a VLAN	37
3.1 Creating of VLAN	37
3.2 Membership of Port Group	37
3.3 Membership of MAC	37
3.4 Layer 3-Based VLAN	38
3.5 IP Multicast Group as VLAN	38
3.6 VTP	38
3.7 How VTP Works	39
3.8 VTP Version 2	40
3.9 Configuring VTP/VLAN	41
3.10 VTP Pruning	42
3.11 Configuring VTP Pruning	42
3.12 Dynamic Port VLAN Membership	43
3.13 How the VMPS works	43
3.14 Configuring Dynamic Ports	45
3.15 VMPS Configuring Files	45

Chapter Four	
4.0 Network Devices	51
4.1 Optic Fiber Switch	51
4.2 Optic Fiber Adaptors	52
4.3 Fiber Optic Terminologies	54
4.4 CISCO Offers	56
4.5 CISCO Routers	59
4.6 CISCO Switches	61
4.7 CISCO Security and VPN	63
Chapter Five	
5.0 Recommendation	65
5.1 Conclusion	66
REFERENCES	67

# CHAPTER ONE

## 1.0 INTRODUCTION

"The Campus Environment" is a name used here to identify a particular set of physical properties, geographical extent, data communication requirement, administrative relationships and need for flexibility that characterize our own university campus (i.e. Minna Bosso campus).

There are seven characteristics of this campus environment that provides a basis for design decisions for a data communication network. The seven are:

- i. Limited geographical extent
- ii. Up to several hundred (or thousand) nodes
- iii. Forces for both commonality and diversity
- iv. Multiple protocols and standards
- v. Confederated administration
- vi. Independently administered interconnections and
- vii. Routers and Gateways to other networks

## 1.1 DATA COMMUNICATION NETWORK

The need to share data is a compelling reason for interconnection. Individual users of computers do not work in isolation. A data communication network enables resources such as data, printer, internet connections, applications or combinations of all these to be shared amongst the devices in the network

## 1.2 AIMS AND OBJECTIVES

1) It will solve the problem of communication between offices, Departments, Schools and also between the administrative offices (senate)

- 2) It will reduce the task involved in organization of files, database for student and programmes.
- 3) It will reduce the cost involved in collecting, transmitting and sourcing information.
- 4) It will widen the sample space for research work by linking the institution to liable sources (i.e. the net if implemented).
- 5) It will ensure accurate delivery of data transmitted within and outside the institution by detecting and correcting any possible error on the packets of information being transmitted
- 6) It will provide efficiency in service for the staff and students of the institution through access to recent (current) and productive information.
- 7) It will adequately manage traffic on the network and also unite all Deans, H.O.D, departments, staff and students together via data collection transmission and storage. This project is carried out to establish a secured, economic, flexible, hierarchical and efficient means of communication on our campus knowing we are in the information age. Thus the need for decentralized computing and shared information which provides group of people [team, faculty, department etc] with the flexibility to handle their own specific information processing tasks, regardless of physical location

### **1.3 SCOPE OF STUDY**

This project is a design work that should be implemented by the institution, hence effort was made to design and configure with precision and accuracy (rooms have been

provided for expansion), an efficient and secured network. On this note I will like to state clearly that this project work is dynamic and cannot be totally exhausted within the scope of this write up. However, the information provided here is sufficient for the design work considering the time and financial constraint.

#### **1.4 SIGNIFICANCE OF STUDY**

The importance of this project work would be fully appreciated when implemented. It links the institution with the rest of the world, it eradicates traffic collision, and hence a cutting edge in technological development in data communication.

## **CHAPTER TWO**

### **2.0 LITERATURE REVIEW**

In the computer world, the term network describes two or more connected computers that can share resources such as data, a printer, an internet connection, applications, or a combination of all these. The simplest form of a computer network is the LAN [Local Area Network]

#### **2.1 LOCAL AREA NETWORK [LAN]**

By definition a LAN is limited to specific area, usually an office, and cannot extend beyond the boundaries of a single building.

Buildings with many LANS (like FUT MINNA Bosso campus) where everyone needs access to high-speed backbone LAN as well as a centralized data center with mainframe computers and application servers will need a VLAN.

#### **2.2 WIDE AREA NETWORK (WAN)**

A WAN is any network that crosses metropolitan, regional or national boundaries. Most professionals define a WAN as any network that uses routers and public network links. A WAN can either be centralized or distributed. The internet is actually a specific type of WAN. The internet is a collection of networks that are interconnected and thus it's technically an internetwork.

#### **2.3 FULL AND HALF DUPLEX COMMUNICATION**

All network communications [LAN, MAN, WAN communications] can be classified as half duplex or full duplex. With half duplex, communication happens in both directions,

but in one direction at a time. A full duplex on the other hand allows communications in both directions simultaneously

## **2.4 NETWORK ARCHITECTURE**

The two most common types are

- Peer-to – peer network
- Client/Server network

The difference between the two is determined by the following factors

- Size of organization
- Level of security
- Amount of traffic
- Network budget
- Needs of Network users e.t.c

## **2.5 Peer-to-peer Networks**

In this type of network the computers connected have no centralized authority. From an authority view point all these are equal and therefore are known as peers

This type of network is appropriate for an environment where:

- 1) There are ten computers on the network or fewer.
- 2) Security of files is not important
- 3) The distance apart from each computer to the other is small.
- 4) Growth of the networks is limited



## PEER-PEER NETWORK

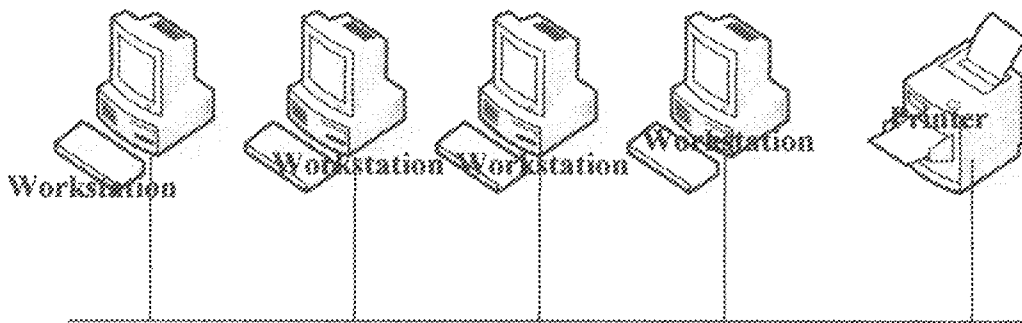


Fig 2.0 PEER --PEER NETWORK

## 2.6 CLIENT/SERVER-BASED NETWORK

This is a type of NETWORK which uses a network operating system designed to manage the entire network from a centralized point, which is the server. This type of network is necessary where security of files and directories cannot be overemphasized. There is an administrator that manages the network and keeps it secured with security policies. As the size of the network increases, the server becomes specialized in function, hence, on a server-based network; there can be specialized server such as:

- File and print servers:** - which manage users' access and use of files and printer resources. They are used for file and data storage.
- **Application servers:** - this makes the server side of client/server application, as well as the data. available to clients.
- Mail server:** - it manages electronic messaging between network users.

## CLIENT/SERVER BASED NETWORK

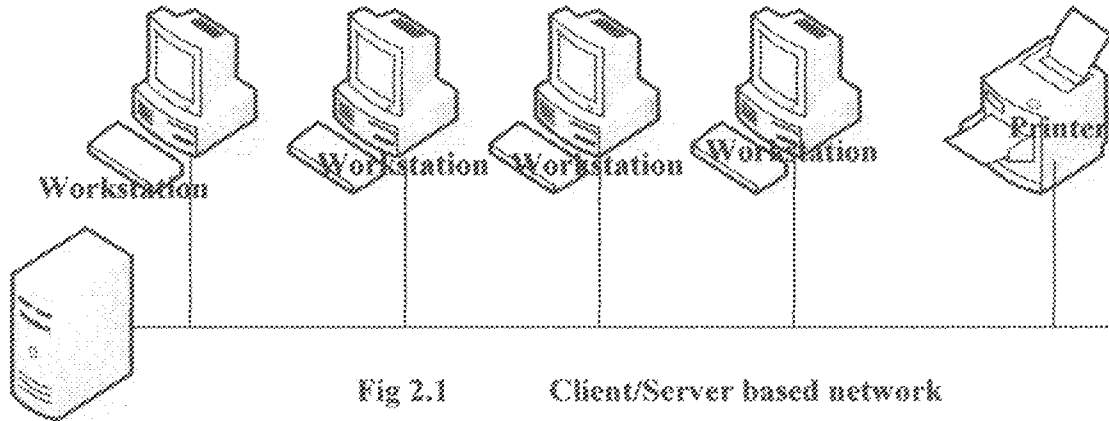


Fig 2.1 Client/Server based network

Main server

### 2.7 ADVANTAGES OF SERVER-BASED NETWORK

The advantages of client/server-based network are:

#### Sharing resources

A server is designed to provide access to many files and printers while maintaining performance and security to user. Server based sharing of data can be centrally administered and controlled.

#### Security

Security is most often the primary reason for choosing a server based approach to networking.

### **Backup**

There is a back up of important information on regular schedules, because it's centralized.

### **Number of User**

It supports thousand of users. The future expansion capability of such network is feasible due to its design.

## **2.8 PHYSICAL TOPOLOGIES**

A topology is basically a map of the network. The physical topology of a network describes the layout of the cable and workstations and the location of all the network components. The cables or connections in a physical topology are often referred to as network/physical media. A network topology implies a number of conditions. For example, a particular topology can determine not only the type of cable used, but how the cabling is run through floors, ceilings and walls. Topology also determines how computers communicate on the network.

The five most common topologies are:

- \*Bus Topology
- \*Star Topology
- \*Ring Topology
- \*Mesh Topology
- \*Wireless

## 2.9 Bus Topology

In a bus topology, all computers are attached to a single continuous cable that terminates at both ends, which is the simplest way to create a physical network. It consists of a single cable called a trunk that connects all of the computers in the network in a single-line. Only one computer at a time can send messages, hence the number of computers on the bus affects the overall performance of the network. The bus is a passive topology. Computers on a bus only listen for data being sent on the network. They are not responsible for moving data from one computer to the next.

The failure of one computer, does not affect the rest of the network.

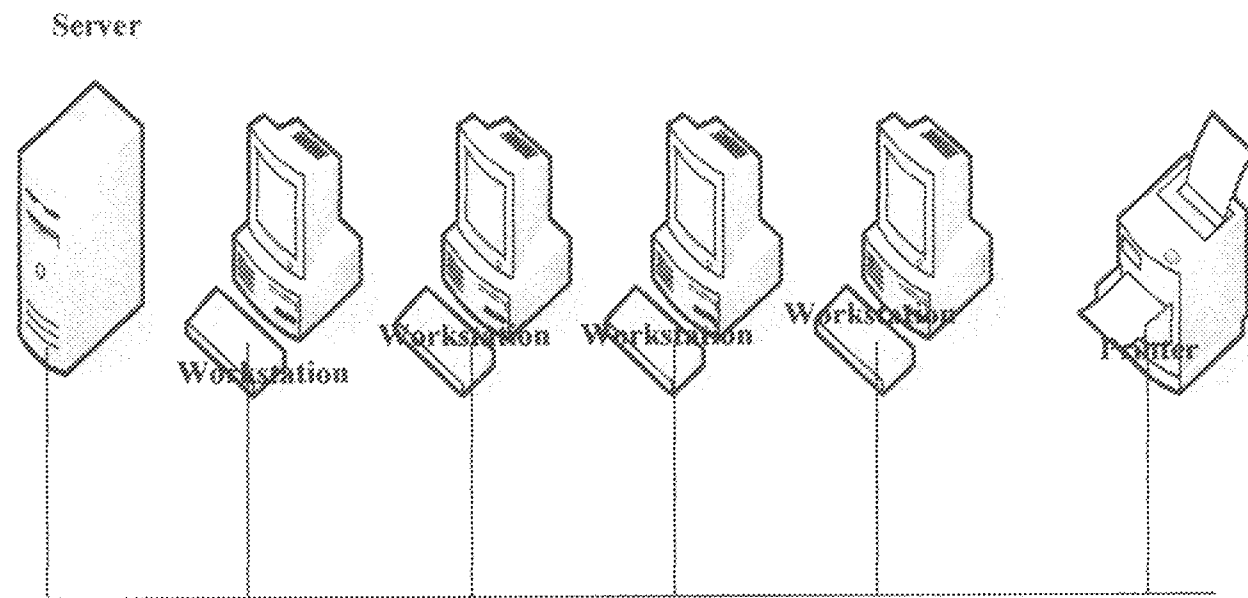


Fig 2.2 Bus Topology

## **2.10 STAR TOPOLOGY**

In this topology, the computers are connected by a cable segment to a centralized component, called a HUB. Signals are transmitted from the sending computer through the hub to all computers on the network. The star network offers centralized resources and management; if the central point fails, the entire network goes down. It is much fault tolerant than the bus topology

## **2.11 RING TOPOLOGY**

This type of topology connects computers on a single circle of cable. There are no terminal ends. The signals travel around the loop in one direction and passes through each computer. In this case, each computer acts like a repeater to boost the signal and send it onto the next computer.

The failure of one of the computers on this type of topology causes the entire network to fail. Token passing is a method used in transmitting data around the ring. The token is passed from the source computer to the to the destination computer

The source computer modifies the token, put an electronic address on the data and sends it around the ring. The data passes each computer until it finds the one with the address that matches the address on the data. The receiving computer indicates that he data has been received. After verification; the sending computer creates a new token and releases it on the network.

## **2.12 MESH.**

In a mesh topology, a path exists from each station to every other station in the network. A mesh topology can become quite complex as wiring and connections increases

exponentially. For every  $n$  stations you have  $n(n-1)/2$  connections. This topology is expensive.

### **2.13 WIRELESS**

Radio Frequency [RF] systems are being used in our world today. The RF networking hardware available today makes it easy for people to connect wirelessly to their corporate network as well as the Internet.

### **2.14 THE OSI (OPEN SYSTEM INTERCONNECT) MODEL**

The OSI model was developed in 1977 by the INTERNATIONAL ORGANISATION OF STANDARDISATION [ISO] to provide "common ground" when describing any network protocol and promote interoperability by providing a guideline for network data transmission between computers that have different hardware vendors, software, operating systems, and protocols. Network data transmission is performed via the use of a protocol suite/stack. A protocol suite is most easily defined as a set of rules used to determine how computers communicate with each other. The OSI model is used to describe what tasks a protocol suite performs as you explore how data moves across a network.

The OSI reference model consists of seven layers that build from the wire (Physical) to the software (Application). These are

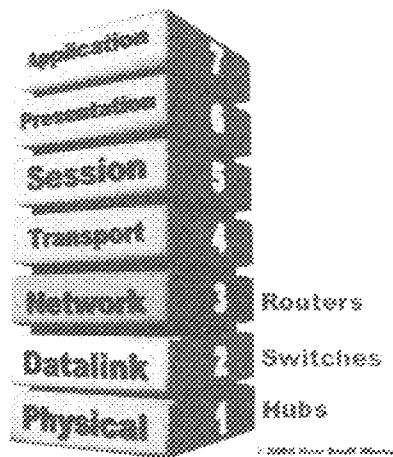


Fig 2.3

**APPLICATION LAYER:**

This layer is responsible for defining how interactions occur between network services and the network. It may also support error-recovery

**PRESENTATION LAYER:**

This layer is responsible for formatting data exchange. Also character sets are converted, and data is encrypted here. Data may also be compressed in this layer, thus handling the redirection of data streams.

**SESSION LAYER:**

This layer defines how two computers establish, synchronize, maintain, and end a session. Security authentication, data transfer, acknowledgements, and connection release takes place here.

**TRANSPORT LAYER:**

It is responsible for checking that the data was delivered error-free. It is used to divide a message into smaller segments called packets for ease of transmission. Also it handles logical address/name resolution. This layer is also responsible for the majority of error and flow control in network communications.

### **NETWORK LAYER:**

The network layer is responsible for logical addressing and translating logical names into physical addresses. Also it controls congestions, routes data from source to destination, and builds and tears down packets. Most routing protocols function in this layer

### **DATA-LINK LAYER:**

It takes raw data from the physical layer and gives it a logical structure. It also controls functions of logical network topologies and physical addressing as well as data transmission synchronization and connection. It is made up of two sub-layers:

-Media access control [MAC]

-Logical link control [LLC]

The Hardware [MAC] Address:

Every NIC [network interface card] has an address, typically assigned at the factory. This address is protocol-independent and is often called the **HARDWARE ADDRESS**. MAC address is a 12-digit hexadecimal number

Logical Topology:

Logical Topology dictates the way the information flows. These are Peer-Peer network and Client/Server network

### **PHYSICAL LAYER:**

This layer deals with the physical concept of a network. It receives information from upper layers , translates all the data into signals that can be transmitted on a transmission medium[signal encoding]. It also specifies how much of the media will be used during data transmission. Finally this layer specifies the layout of the transmission media[ its topology]. Physical topologies include the following: bus, star, ring, and mesh.



## **2.15 COMMON NETWORK CONNECTIVITY DEVICES**

These devices include:

- Network interface card [NIC]
- Hub
- Switch
- Repeater
- Bridge
- Router
- Gateway

### **NETWORK INTERFACE CARD [NIC]:**

This is an expansion card you install in your computer to connect, or interface your computer to the network.

### **HUBS**

These are physical layer devices that operate principally at layer 1 of the OSI reference model. This is a central component in the star topology. Every device in the network connects directly to the Hub via single cable

### **SWITCHES**

Switches are a fundamental part of most networks. Switches enable several users to send information over a network. Users can send the information at the same time and do not slow each other down. Just like routers allow different networks to communicate with each other, switches allow different nodes of a network to communicate directly with

each other. A node is a network connection point, typically a computer. Switches allow the nodes to communicate in a smooth and efficient manner.

Illustration of a Cisco Catalyst switch.

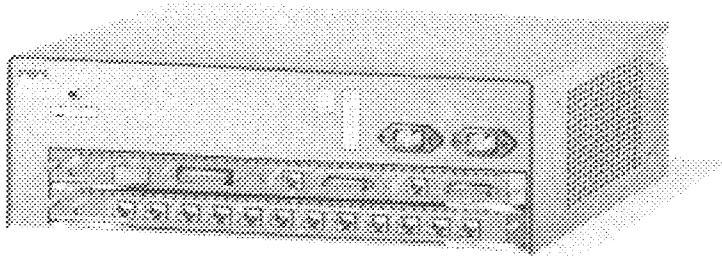


Fig 2.4

### Switch Technologies

A switch has the potential to radically change the way nodes can communicate with each other. But what makes a switch different from a router? Switches usually work at Layer 2 (Data link) of the Open System Interconnection (OSI) reference model with use of MAC addresses. Routers work at Layer 3 (Network) with Layer 3 addresses. The routers use IP, Internetwork Packet Exchange (IPX), or Appletalk, which depends on the Layer 3 protocols that are in use

Switches use one of three methods for routing traffic:

Cut-through

Store and forward

Fragment-free

Switches can provide a high-speed backbone for hubs. They offer speed that is up to 155 Mbps to more than 2Gbps. It equally uses transport protocol, such as TCP/IP. It can be used with any cable type (ranging from coaxial cable to optic fiber).

## **REPEATER**

A repeater works at the physical layer of the OSI and it regenerate the network's signal and resends them out on other segment. It takes a weak signal from one segments, regenerates it, and passes it on to the next segment, in other words, it works within the same architecture.

It does not translate or filter anything and for it to function properly, it is used to connect networks with the same access method

## **BRIDGES**

Bridges are data communications devices that operate principally at Layer 2 of the OSI reference model. Bridges controls data flow, handles transmission errors, provides physical (as opposed to logical) addressing, and manages access to the physical medium. Bridges are generally used to segment a LAN into a couple of smaller segments. Bridges work like repeaters but can as well isolate traffic or problems on networks

## **ROUTERS**

While most switches operate at the Data layer (Layer 2) of the OSI reference model, the router operates at the Network layer (Layer 3) .In fact, a Layer 3 switch is incredibly similar to a router. Like routers, Layer 3 switches actually work at the Network layer. When a router receives a packet, the router looks at the Layer 3, or Network layer, source and destination addresses to determine the path for the packet to take. This activity is Layer 3 (Network) networking activity. A standard switch relies on the MAC addresses to determine the source and destination of a packet. This activity is Layer 2 (Data) networking. The fundamental difference between a router and a Layer 3 switch is that

Layer 3 switches have optimized hardware to pass data as fast as Layer 2 switches. Yet Layer 3 switches make decisions on how to transmit traffic at Layer 3, just like a router. Current Layer 3 switches like the Cisco Catalyst 6500/6000 switches use the information from the routing protocols to update the hardware caching tables.

Note: Routers are necessary for communication between two VLANs.

### GATEWAYS

A gateway is any hardware and software combination that connects dissimilar network environment. Gateways are the most complex of network devices because they perform translations at multiple layers of the OSI model

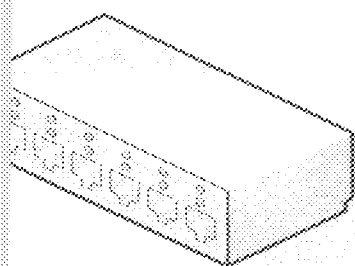


Fig 2.5 10-Port Hub

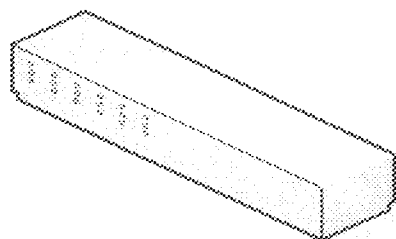


Fig 2.6 8-Port Switch

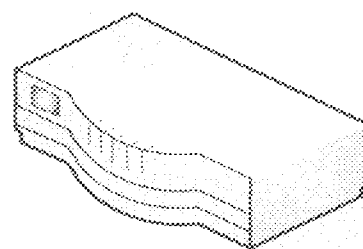


Fig 2.7 8-Port Switch

## **2.16 NETWORK MEDIA**

Most networks today are connected by some sort wire or wireless, which acts as a medium of transmission carrying signals between computers.

The two major network media in used are:

- Cable media [physical/wired media]
- Wireless media

## **2.17 CABLE MEDIA**

The three types of cable media used in local area network area are:

### **-TWISTED-PAIR CABLE:-**

This consists of multiple, individually insulated wires that are twisted together in pairs. Sometimes a metallic shield is placed around the twisted pair, hence the name shielded twisted pair (STP). More commonly, you see cable without outer shielding; it's called unshielded twisted pair (UTP)

### **-COAXIALCABLE:-**

This contains a center conductor, made of copper surrounded by a plastic jacket, with a braided shield over the jacket. This can either be Thinnet coaxial cable (with small copper core) or thicknet cable (with large copper core).

### **-OPTICAL FIBRE CABLE**

It transmits digital signals using light pulses rather than electricity. It is immune to EMI and RFI. It carries more data through longer distances within a short transmission time. It is good for every high-speed, high capacity data transmission because of its low attenuation and the high bandwidth.

## **2.18 WIRELESS MEDIA**

Wireless mediums include:

Infrared

Laser

Narrow band (single frequency) radio

Spread spectrum radio.

Advantages over cable media are:

- It provides a degree of portability
- Extend networks beyond limits of copper.

## **2.19 LOCAL AREA NETWORK ARCHITECTURE**

LAN architecture includes its overall structure and all components that make it functional including hardware and system software. Some of them are:

- IEEE 802.3 Ethernet standard, which is the most popular
- IEEE 802.5 token ring standard
- Apple talk architecture
- Arc Net architecture
- The most popular and commonly used architecture is the Ethernet standard defined by IEEE 802.3

## **ETHERNET**

Eihernet is a base architecture that uses a bus topology, usually transmits at 10 Mbps and relies on CSMA/CD to regulate traffic on the main cable segment. The Ethernet media is

passive, which means it draws power from the computer and thus will not fail unless the media is physically out of place.

### Ethernet Basics

Ethernet features are summarized as follows:

- Traditional Topology: Linear bus
- Other Topology: Star bus
- Type of architecture: Base band
- Specifications: CSMA or 100Mbps
- Transfer speed: 10 Mbps or 100Mbps
- Cable Type: Thicknet, Thinnet, UTP.

Ethernet breaks down data into a frame format for transmission. A frame is a packet of information transmitted as a single unit, it can be between 64 and 1,518 bytes long where the frame occupies 18 bytes and the data itself takes up to 46 to 1,500 bytes.

A typical frame used for TCP/IP, Ethernet II frame has the following sections;

<b>FRAME FIELD</b>	<b>DESCRIPTION</b>
Preamble	marks the start of the frame
Destination and source	The origin and destination address
Type	used to identify network layer
Cyclic redundancy check (CRC)	error checking field to determine if the frame arrived error-free

There are four different 10 Mbps Ethernet topologies, namely;

- 10 Base T
- 10 Base 2

-10 Base 5

-10 Base FL

X Base Y IN Ethernet topology implies:

X is the transmission rate (speed of transmission); Base as the base band architecture and Y as the medium of transmission

### 10 base T

It is standard for Ethernet running over twisted-pair. The following summarizes its features:

<u>Category</u>	<u>Note</u>
Cable	Category 3, 5, UTP
Connectors	RJ 45 at cable ends
Transceiver	Each computer should have one on its NIC
Transceiver to hub distance	100 meters maximum
Back bones for hubs	coaxial or fiber optic to join a layer LAN

### 10 Base 2

It is a standard for Ethernet running over thinnest coaxial cable. It transmits at 10 Mbps over a base band wire and can carry a signal roughly two time 100 Mbps Thinnest cabling components include:

BNC barrel connectors

BNC T connectors

BNC terminal

### 10 Base 5



The IEEE specification for this topology is 10Mbps, base band, and 500-meter segments. It makes use of thick coaxial cable or thicknet. Thicknet generally uses a bus topology and can support as many as 100 nodes per backbone segments.

Thicknet cabling components include:

- Transceiver
- Transceiver cables
- DIX or AUI connector

#### 10 Base FL

It's a standard that uses fiber optics as medium of communication between computers and repeaters. The maximum distance for a 10 Base FL segment is 2000 meters.

### **2.20 LAN ADAPTERS, DRIVERS AND PROTOCOLS**

The Network adapter cards are the only interface or connection between the computer and the network cable. Since it's impossible for an installed network adapter card to work without its driver been installed, there should be adequate preparation for computers on local area network to be able to communicate with each other and other peripherals.

#### **2.21 LAN ADAPTERS CARDS**

The only interface or connection between the computers on a network and the network cable is called the network adapter card. It's installed in an expansion slot in each computer and the server on the network.

**The functions of the network adapter cards are:**

- Prepare data from the computer for the network cable
- Send the data to another computer

- Control the flow of data between computer and the cabling system
- Receiving incoming data from the cable and translate into bytes
- It converts the data to be sent to byte. It restructures data traveling in parallel so that it will flow through 1-bit mode serial path of the network cable.

The network adapter card can only sends data over network to the adapter card at the receiving end, after it has confirmed its consent to receive such data.

**To enhance the network adapter card functionality, the adapter card must:**

- Fit with the computer's internal structure(data bus-architecture)
- Have the right type of cable connector for the cabling.

### **2.22 LAN ADAPTER CARD'S DRIVER**

A driver is software that enables the computer to work with a particular device, in this case, an adapter card. The operating system of a computer cannot communicate with the device (Adapter card) until the driver for that adapter card has been fully installed and configured. The manufacturers of the adapter cards are responsible for supplying the configured. The manufacturers of the adapter cards are responsible for supplying the driver.

### **2.23 LAN PROTOCOL**

Protocols are rules and procedures for communicating when several computers are on network. The rules and technical procedures governing their communication are called protocols.

### **How Protocols work:**

**At the source computer, the protocol does the following:**

- Breaks the data into packets
- Add addressing information to the packets
- Prepare the data for transmission

**At the destination computer, it does these:**

- Takes the data packets off the cable
- Brings the data through the NIC to the computer
- Gets the information added by the sending computer

### **2.24 VIRTUAL LOCAL AREA NETWORK (VLAN).**

As networks grow in size and complexity, many organizations turn to Virtual Local Area Networks (VLANs) to provide some way to structure this growth logically. Basically, a VLAN is a collection of nodes that group together in a single broadcast domain also Virtual LAN (VLAN) is a group of devices on one or more LANs that are Configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. A broadcast domain is a network or portion of a network that receives a broadcast packet from any node within that network. In a typical network, everything on the same side of the router is part of the same broadcast domain. A switch on which you have implemented VLANs now has multiple broadcast domains, which is similar to a router. But you still need a router to route from

one VLAN to another. The switch alone cannot perform this routing. While you can have more than one VLAN on a switch, the VLANs cannot communicate directly with each other. Communication between VLANs requires the use of a router.

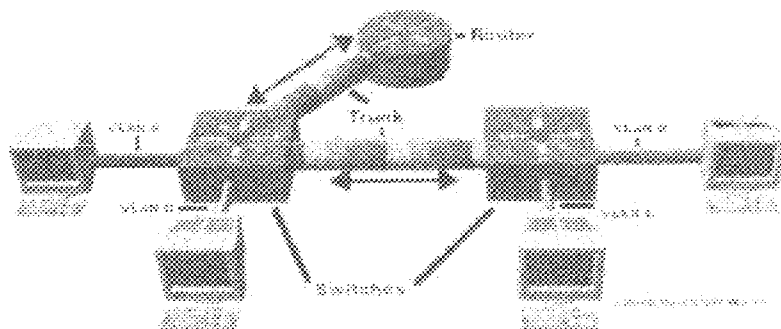


Fig 2.8

## 2.25 TYPES OF VLAN

Each VLAN is of a particular type, and has its own maximum transmission unit (MTU) size. Types of VLANs are defined:

- Ethernet/802.3 VLANs
- Token Ring/802.5 VLANs

Switches will allow a VLAN of one of these types to be assigned to a static/dynamic port for which the physical MAC layer is of the corresponding type; for example, allow a VLAN of type Ethernet/802.3 to be assigned to a physical 10BaseT port. Others are

- Port-Based VLAN: each physical switch port is configured with an access list specifying membership in a set of VLANs.
- MAC-based VLAN: a switch is configured with an access list mapping individual MAC addresses to VLAN membership, i.e. for maintaining a full list of all VLANs everywhere within the VTP domain. This information is stored in nonvolatile RAM (NVRAM). The VTP server can add, delete, and rename VLANs.

-Protocol-based VLAN: a switch is configured with a list of mapping layer 3 protocol types to VLAN membership - thereby filtering IP traffic from nearby end-stations using a particular protocol such as IPX.

-ATM VLAN - using LAN Emulation (LANE) protocol to map Ethernet packets into ATM cells and deliver them to their destination by converting an Ethernet MAC address into an ATM address.

**A VLAN has two important concepts:**

- Logical segmentation of a switched network and
- One broadcast domain.

A VLAN is a switched network that is logically segmented by functions, project teams, or applications, without regard to the physical location of users. For example, several end stations might be grouped as a department, having the same attributes as a LAN even though they are not all on the same physical LAN segment.

To accomplish this logical grouping, a VLAN-capable switching device must be used. Each switch port can be assigned to a VLAN. Ports in a VLAN share broadcast traffic in one VLAN and are not transmitted outside that VLAN. This segmentation improves the overall performance of the networks.

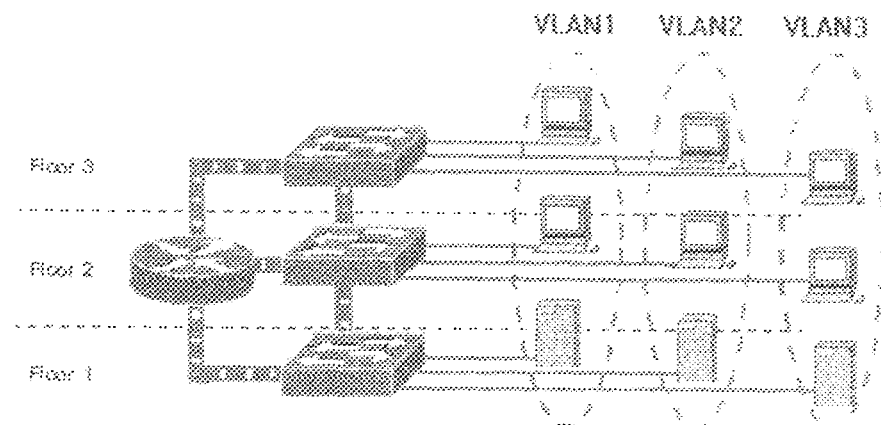


Fig 2.9

## 2.26 BENEFITS OF A VLAN

VLANs provide the following benefits:

- 1) Reduced administration costs associated with moves, adds, and changes
- 2) Controlled broadcast activity and better network security
- 4) Flexible and scalable segmentation
- 5) Security— A separation of systems with sensitive data from the rest of the network provides security. This system separation decreases the chance that someone can gain access to information that the person does not have authorization to see.
- 6) Projects/special applications—You can simplify the management of a project or work with a special application with the use of a VLAN. Because the VLAN brings all the necessary nodes together, project management can be simpler.
- 7) Performance/bandwidth—The careful monitor of network use allows the network administrator to create VLANs that reduce the number of router hops. The VLANs can also increase the apparent bandwidth for network users.

8) Broadcasts/traffic flow—Since VLANs do not pass broadcast traffic to nodes that are not part of the VLAN, a VLAN automatically reduces broadcasts. Access lists provide the network administrator with a way to control who sees particular network traffic. An access list is a table that the network administrator creates. The table lists the addresses that have access to that network

9) Departments/specific job types—Universities can set up VLANs for departments that are heavy network users. A campus can also set up a VLAN across departments and dedicate the VLAN to specific types of employees, such as the Vice Chancellor, Deans, or HODs

As an organization grows there arises a need for moves, adds and changes in its network structure. These moves, adds, and changes are one of the greatest expenses in managing a network. VLANs provide an effective mechanism to control these changes and reduce much of the cost of hub and router reconfiguration. If a group of VLAN users move but remain in the same VLAN connected to a switch port, their network addresses do not change. Router configuration is left intact; a simple move for a user from one location to another does not create any configuration changes in the router if the user stays in the same VLAN.

Similar to routers, VLANs offer an effective mechanism for setting up firewalls in a switch fabric, protecting the network against broadcast problems that are potentially dangerous, and maintaining all the performance benefits of switching. You can create these firewalls by assigning switch ports or users to specific VLAN groups in single switches and across multiple connected switches, thus increasing security easily and inexpensively by segmenting the network into distinct broadcast groups.

Broadcast traffic in one VLAN is not transmitted outside that VLAN. This type of configuration substantially reduces overall broadcast traffic, frees bandwidth for real user traffic, and lowers the overall vulnerability of the network to broadcast storms. You can take advantage of existing hub investments by assigning each hub segment connected to a switch port to a VLAN. All the stations that share a hub segment are assigned to the same VLAN. If an individual station must be reassigned to another VLAN, the station is relocated to the appropriate corresponding hub module. The interconnected switch fabric handles communication between the switching ports and automatically determines the appropriate receiving segments. You can also assign VLANs based on the application type and the amount of application broadcasts. You can place users sharing a broadcast-intensive application in the same VLAN group and distribute the application across the campus.

## 2.27 HOW VLAN WORKS

VLANs allow ports on the same or different switches to be grouped so that traffic is confined to members of that group only. This feature restricts broadcast, unicast, and multicast traffic (flooding) to ports included only in a certain VLAN. You can set up VLANs for an entire management domain from a single Catalyst® 2950 Series Switch. The VLANs on a Catalyst 2950 Series Switch simplify adding and moving end stations on a network. For example, when an end station is physically moved to a new location, its attributes can be reassigned from a network management station via Simple Network Management Protocol (SNMP) or the command-line interface (CLI). When an end



station is moved within the same VLAN, it retains its previously assigned attributes in its new location.

The IP address of a Catalyst 2950 Series Switch Supervisor Engine module can be assigned to any VLAN. This mobility allows a network management station and workstations on any Catalyst 2950 VLAN to directly access another Catalyst 2950 Series Switch on the same VLAN, without using a router. Only one IP address can be assigned to a Catalyst 2950 Series Switch; if the IP address is reassigned to a different VLAN, the previous IP address assignment to a VLAN becomes invalid.

## 2.28 VLAN COMPONENTS

Some of the major components and concepts related to VLANs include switches, routers, inter-operability concerns, transport protocols, and VLAN management

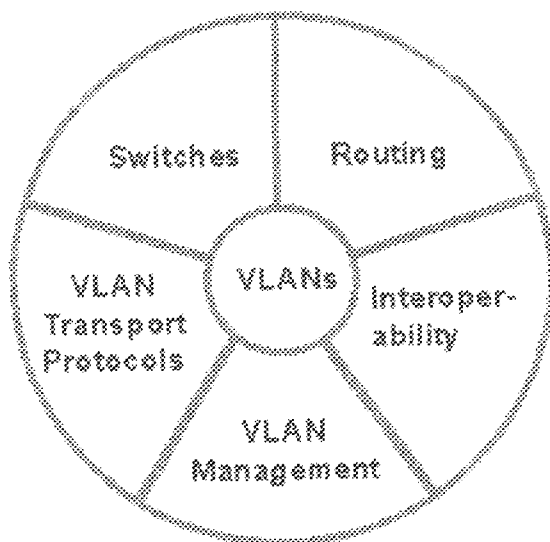


Fig 2.10

## SWITCHES—THE CORE OF VLANs

Switches are a primary component of VLAN communication. They perform critical VLAN functions by acting as the entry point for end-station devices into the switched fabric, facilitating communication across the organization, and providing the intelligence to group users, ports, or logical addresses into common communities of interest. They enable multiple physical LAN segments to be interconnected in a single larger network. Each switch has the intelligence to do filtering and forwarding decisions by frame, based on VLAN metrics defined by network managers, and to communicate this information to other switches and routers within the network.

The criteria used to define the logical grouping of nodes into a VLAN are based on a technique known as frame tagging. There are two types of frame tagging—implicit and explicit. Implicit tagging enables a packet to belong to a VLAN based on the Media Access Control (MAC) address, protocol, the receiving port of a switch, or another parameter into which nodes can be logically grouped. Explicit tagging requires the addition of a field into a frame or packet header that serves to classify the VLAN association of the frame. Frame tagging functions at Layer 2 and requires little processing or administrative overhead.

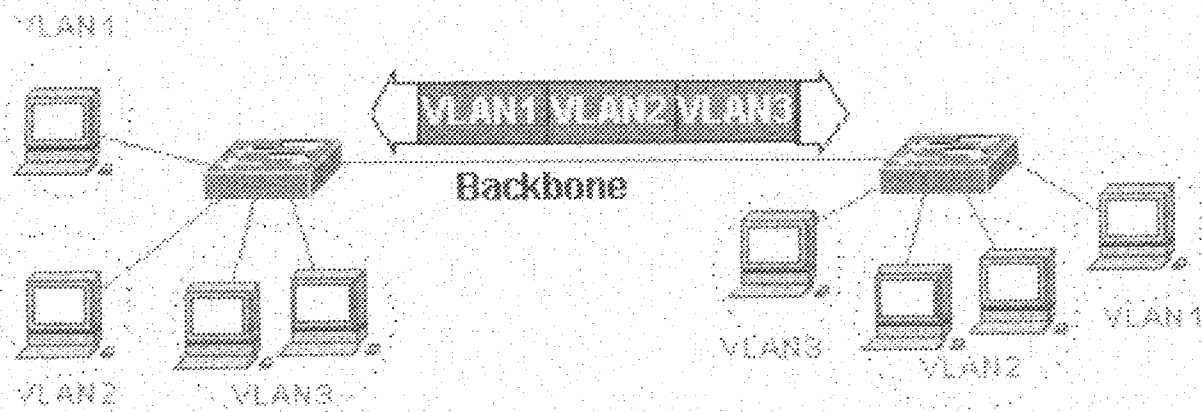


Fig 2.11

## ROUTERS

For inter-VLAN communication, you must use routers that extend VLAN communications between workgroups. Routers provide policy-based control, broadcast management, and route processing and distribution. They also provide the communication between VLANs and VLAN access to shared resources such as servers and hosts. Routers connect to other parts of the network that are either logically segmented into subnets or require access to remote sites across wide-area links. Consolidating the overall number of physical router ports required for communication between VLANs, routers use high-speed backbone connections over Fast Ethernet, Fiber Distributed Data Interface (FDDI), or ATM for higher throughput between switches and routers.

### **Interoperability with Previously Installed LAN Systems**

VLANs provide system compatibility with previously installed systems, such as shared hubs and stackable devices. Although many of these devices are being replaced with newer switching technologies, previously installed concentrators still perform useful functions. With VLANs, you can configure devices such as shared hubs as a part of the VLAN architecture and can share traffic and network resources that directly attach to switching ports with VLAN designations.

### **Transport Protocols that Carry VLAN Traffic across Shared LAN and ATM**

#### **Backbones**

The VLAN transport enables information exchange between interconnected switches and routers residing on the corporate backbone. Transport capabilities remove physical boundaries, increase flexibility of a VLAN solution, and provide mechanisms for interoperability between backbone system components. The backbone acts as the aggregation point for large volumes of traffic. It also carries end-user VLAN information and identification between switches, routers, and directly attached servers. Within the backbone, high-bandwidth, high-capacity links carry the traffic throughout the enterprise. Three high-bandwidth options include Fast Ethernet, Fiber/Copper Distributed Data Interfaces (FDDIs/CDDIs), and ATM.

#### **VLAN Management**

Network management solutions offer centralized control, configuration

## More about Token Ring VLANs

A Token Ring VLAN is slightly more complex than an Ethernet VLAN. In transparent bridging, there is only one type of broadcast frame and, therefore, only one level of broadcast domain, but in source routing there are multiple types of broadcast frames that fall into two categories:

Those that are confined to a single ring

Those that traverse a bridged domain

These two categories of broadcast frames result in a broadcast domain that is hierarchical in nature, because a local ring domain can exist only within a domain of all the interconnected rings. In a Token Ring VLAN, logical ring domains are formed by defining groups of ports that have the same ring number. The IEEE calls such a port group a concentrator relay function (CRF). On Catalyst Switches, such a grouping of Token Ring ports is called a Token Ring CRF (TrCRF).

The domain of interconnected rings is formed using an internal multiport bridge function that the IEEE calls a bridge relay function (BRF). On Catalyst Switches, such a grouping of logical rings is called a Token Ring BRF (TrBRF).

The following figure illustrates TrCRFs and a TrBRF within a Catalyst Token Ring Switch or Module.

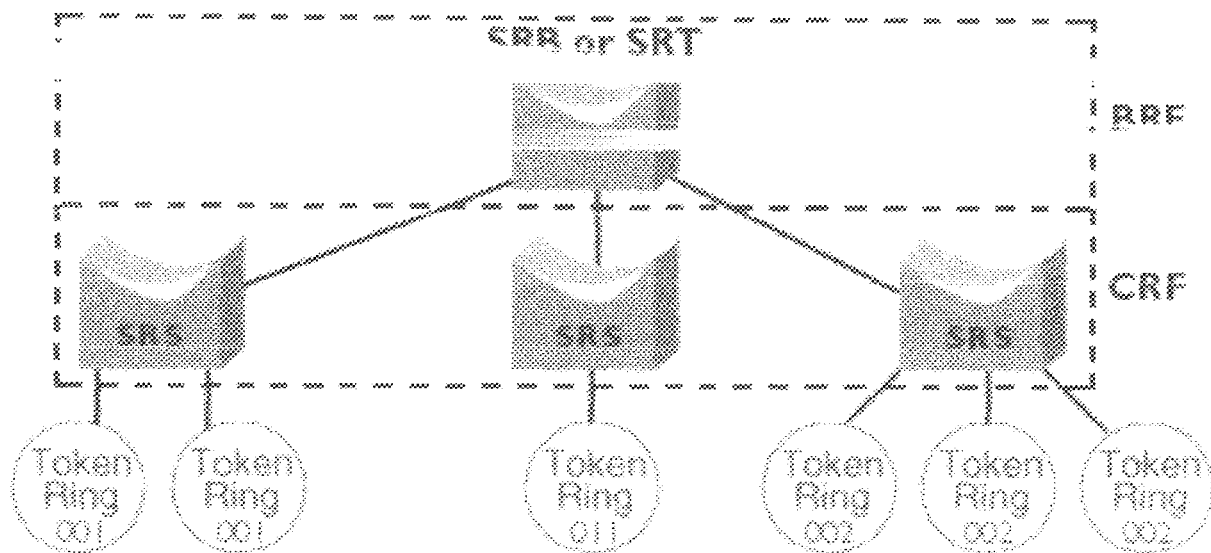


Fig 2.12

### 2.29 INTER-VLANROUTING

By definition, VLANs perform traffic separation within a shared network environment. Communication between VLANs is performed through routing functionality and, for non-routable protocols, switching. This integrated solution of high-speed, scalable VLAN switching of local traffic and efficient routing and switching of inter-VLAN traffic is becoming increasingly attractive in large networks. Cisco routers address this requirement with their ability to connect 802.10, Inter-Switch Link (ISL), and ATM LAN Emulation (LANE)-based VLANs.

### 2.30 VLAN STANDARDIZATION-IEEE 802.1q

IEEE 802.1q provides for the standardization of VLANs based on a three-layer approach. Though the IEEE 802.1q draft provides for both explicit (for example, standard IEEE 802.1q, IEEE 802.10, ISL, and so on) and implicit tagging (identification by filter), no support is provided for the implicit tagging in Revision 1. Revision 1 of the IEEE 802.1q

draft supports only one-level tagging. The one-level tagging allows the insertion of Ethertype and VLAN-ID information in the frame after the source MAC address (or Routing Information Field [RIF]), but before the original Ethertype/Length (or Logical Link Control [LLC]) field. The one-level tagging also includes a Token Ring encapsulation bit so that Token Ring frames can be carried across Ethernet backbones without IEEE 802.1b translation of data contents. Currently, several different transport mechanisms are used for communicating VLAN information across high-performance backbones. Among them are the LANE standard that has been approved by the ATM Forum, the Cisco ISL for Fast Ethernet, and the IEEE 802.10 protocol, which provides VLAN communication across shared FDDI backbones. All these VLAN technologies are supported on the Catalyst 5000 Series Switches. Each allows a single link to carry information from multiple VLANs. You will learn more about ISL, IEEE 802.10, and LANE in this module

## CHAPTER THREE

### 3.0 DESIGN OF A VIRTUAL LOCAL AREA NETWORK

#### 3.1 CREATING OF V LAN

The common virtual LAN (VLAN) configuration options implemented today are as follows:

- By port group
- By Media Access Control (MAC) address
- By network-layer information
- By IP3.0 multicast groups

#### 3.2 MEMBERSHIP OF PORT GROUP

VLAN membership is defined by assigning a specific VLAN to a port or a group of ports. Still the most common way of defining VLAN membership, this type does not allow multiple VLANs to be assigned to the same switch port or group of ports. The main disadvantage of defining VLANs by port is that the network manager must reconfigure VLAN membership when a user moves from one port to another.

#### 3.3 MEMBERSHIP OF MAC

VLANs are defined based on the source MAC address of the hosts connected to the switch port. VLANs based on MAC addresses enable users to move to a different physical location on the network and have their workstation automatically retain its



VLAN membership because MAC-layer addresses are hardwired into the network interface card (NIC) of the workstation.

### 3.4 LAYER 3-BASED VLAN

VLANs are defined based on information contained in the network-layer header of the packet, such as the protocol type or the network layer address. A major advantage of defining a VLAN based on Layer 3 information is that it enables partitioning by protocol type. Also, there is no need to reconfigure the network address of each workstation when a user moves to a new location.

### 3.5 IP MULTICAST GROUP AS VLAN

VLAN membership is defined based on IP multicast groups. All workstations that join an IP multicast group are members of the same VLAN. The fundamental concept of VLANs as broadcast domains still applies here. The main advantage of multicast group-based VLANs is the high degree of flexibility due to the dynamic nature of the VLANs because workstations can join different multicast groups at different times.

### 3.6 VLAN TRUNK PROTOCOL

VLAN Trunk Protocol (VTP) is a proprietary Layer 2 messaging protocol that maintains virtual LAN (VLAN) configuration consistency throughout the network. VTP manages the addition, deletion, and renaming of VLANs at the system level. This protocol allows you to manage VLANs on a network-wide basis and make central changes that are automatically communicated to all the other switches in the network without requiring manual intervention at each switch.

### 3.7 HOW VTP WORKS

A VTP domain is made up of one or more interconnected devices that share the same VTP domain name. A switch can be configured to be in one and only one VTP domain.

Catalyst® Switches configured as VTP servers and clients maintain all VLANs everywhere within the VTP domain. A VTP domain defines the boundary of the specified VLAN. Using VTP, each Catalyst 5000 Series Switch advertises its management domain, its configuration revision number, and its known VLANs and their specific parameters on its trunk ports.

VTP establishes global configuration values and distributes the following global configuration information:

- VLAN name
- VLAN IDs
- Emulated LAN names
- 802.10 security association identifier (SAID) values
- Maximum transmission unit (MTU) size for a VLAN
- Frame format

Catalyst 2950 Series Switches can be configured to operate in any one of the three VTP modes:

*VTP server*—VTP server is responsible for maintaining a full list of all VLANs, but will not store the information in NVRAM. VTP Client cannot add, delete, or rename VLANs. Any changes made must be received from server advertisement.

*VTP transparent*—A switch configured in the VTP transparent mode does not participate in VTP; however, it will pass on the VTP advertisements. A VLAN defined on the switch is local only to the switch and is stored in NVRAM.

VTP servers and clients transmit information through trunks to other attached switches and receive updates from those trunks. Using VTP servers, the global VLAN information can be modified through the VTP Management Information Base (MIB) or the command-line interface (CLI).

The advertisement frames are sent to a multicast address so that they can be received by all neighboring devices, but they are not forwarded by normal bridging procedures. All switches in the same management domain learn about any new VLANs configured in the transmitting switch.

Using periodic advertisements, VTP tracks configuration changes and communicates them to other switches in the network. The configuration is updated and propagated to the other switches by a higher VTP-advertisement revision number. The switch ignores VTP advertisements with a lower revision number. When new switches are added to the network, the added devices receive updates from VTP and automatically configure existing VLANs within the network.

### **3.8 VTP VERSION 2**

Catalyst 2950 Series Software Release 3.1 supports VTP Version 2, an extension to VTP that supports Token Ring LAN switching. VTP Version 2 must be enabled to support Token Ring switching. VTP Version 1 and 2 are not interoperable on switches in the same VTP domain.

### 3.9 CONFIGURING VTP AND VLAN

The `set vtp` and `set vlan` commands use VTP to set up VLANs across an entire management domain. Initially, all switched Ethernet, Ethernet repeater, and FDDI ports are in the default VLAN defined as VLAN 1.

By default, the Catalyst 5000 Series Switch is in the no-management domain state until it is configured with a management domain or it receives an advertisement for a domain. If a switch receives an advertisement, it inherits the management domain name and configuration revision number. The switch ignores advertisements with different management domains or earlier configuration revision numbers and checks all received advertisements with the same domain for consistency.

The `set vtp` command sets up the management domain, including establishing the management domain name, the VTP mode of operation (server, client, or transparent), and the password value. There is no default domain name (the value is set to null). The default advertisement interval is five minutes. The default VTP mode of operation is set to server.

By default, the management domain is set to nonsecure mode without a password. A password sets the management domain to secure mode. You must configure a password on each Catalyst 2950 Series Switch in the management domain when in secure mode, otherwise the switch would ignore the VTP advertisements when the configured password does not match the password in the VTP advertisement.

VTP Version 2 is disabled by default. VTP Version 2 must be manually enabled using the `set vtp v2 {enable | disable}` command. All switches in a VTP domain must be running the same version of VTP.

VTP is transmitted on all trunk connections, including Inter-Switch Link (ISL), 802.1Q, and LAN Emulation (LANE).

## 2.10 VTP PRUNING

The VTP pruning feature detects when a switch does not need the traffic for a particular VLAN and restricts flooded traffic to only those trunk links that the traffic must use to access the appropriate network devices. VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, which includes broadcast, multicast, unknown, and flooded unicast packets.

## 3.11 CONFIGURING VTP PRUNING

By default, VTP pruning is disabled in a management domain. The pruning enable option of the set vtp command enables pruning in the entire management domain. Make sure that all devices in the management domain support VTP pruning before enabling it. VTP pruning, even if enabled, does not take effect on a VLAN that is not pruning eligible. By default, VLAN 1 is not pruning eligible, while VLANs 2 through 1000 are pruning eligible.

To enable pruning eligibility, the set vtp pruneeligible command is used.

```
console> set vtp pruneeligible 120,150
```

Vlans 4-5,9-99,120,150,201-1000 eligible for pruning on  
this device.

This command specifies VLANs 120 and 150 as eligible for pruning. It also displays all pruning-eligible VLANs.

To disable pruning eligibility, the clear vtp pruneeligible command is used.

```
Console> clear vtp pruneeligible 2,3,6-8,100-200
```

Vlans 1-3,6-8,100-200 will not be pruned on this device.

Pruning eligibility resides on the local device only.

### 3.12 DYNAMIC PORT VLAN MEMBERSHIP

You can configure the virtual LAN (VLAN) membership for a port to be static or dynamic. Dynamic ports are assigned to a VLAN based on the source Media Access Control (MAC) address of the hosts connected to that port. One advantage of dynamic ports is that you can move a device from a port on one switch to a port on another switch in the network without changing the VLAN assignment.

To configure dynamic port VLAN membership, the following tasks have to be completed:

Configure the VLAN Membership Policy Server (VMPS)

Configure dynamic ports on clients

The VMPS has a database of MAC-address-to-VLAN mappings necessary for setting up dynamic ports.

### 3.13 HOW THE VMPS WORKS

After you enable VMPS by entering the set vmps state enable command, the configuration information is downloaded from a Trivial File Transfer Protocol (TFTP) server. After the VMPS successfully downloads the ASCII configuration file, it parses the file and builds a database and begins to accept requests from clients.

The VMPS opens a User Datagram Protocol (UDP) socket to communicate with clients and listen to client requests. As shown in the following figure, upon receiving a valid

request from a client, the VMPS searches its database for a MAC-address-to-VLAN mapping.

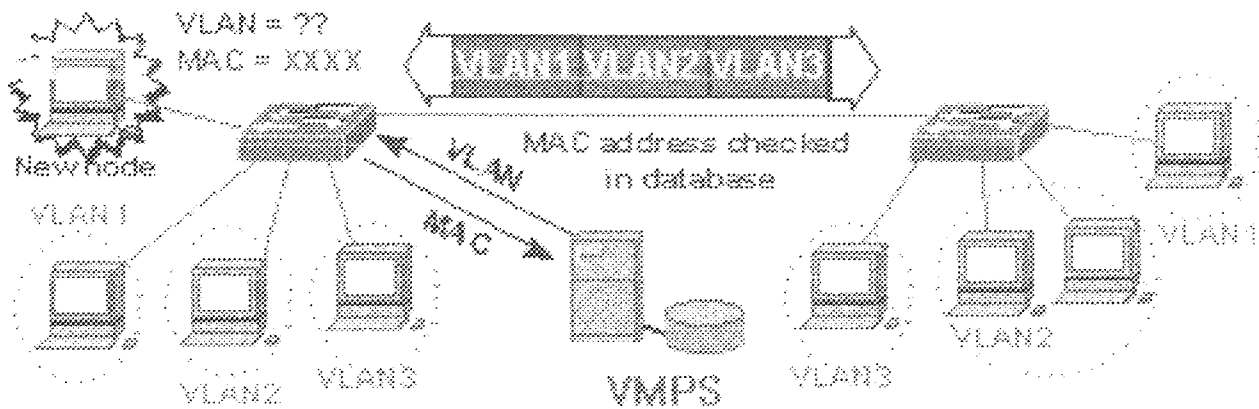


Fig 3.0

The assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group. If the VLAN is legal on this port, the VLAN name is passed in the response. If the VLAN is illegal on that port and the VMPS is not in secure mode, it sends an access-denied response. If the VMPS is in secure mode, it sends a port-shutdown response.

If the VLAN from the table does not match the current VLAN on the port and there are active hosts on the port, the VMPS sends an access-denied or a port-shutdown response based on the secure mode of the VMPS.

You can configure a fallback VLAN name into the VMPS. If the requested MAC address is not in the table, the VMPS sends the fallback VLAN name in response. If you do not configure a fallback VLAN and the MAC address does not exist in the table, the VMPS sends an access-denied response. If the VMPS is in secure mode, it sends a port-shutdown response. Upon subsequent resets of the Catalyst® 5000 Series Switches, the

configuration information is downloaded automatically from a TFTP server, and the VMPS is enabled.

### 3.14 CONFIGURING DYNAMIC PORTS

Dynamic ports work in conjunction with the VMPS. You must configure the VMPS before configuring dynamic ports. The VMPS must be active and accessible to the Catalyst 5000 Series Switch. On the current Catalyst 5000 Series Switch hardware platform, a dynamic (nontrunking) port can belong to only one VLAN at a time. Upon link-up, a dynamic port is isolated from its static VLAN. The source MAC address from the first packet of a new host on the dynamic port is sent to the VMPS, which provides the VLAN number to which this port must be assigned.

Multiple hosts (MAC addresses) can be active on a dynamic port, provided they are all in the same VLAN.

**Note:** When a port becomes dynamic, the spanning-tree PortFast feature is automatically enabled for that port. This prevents applications on the host from timing out and entering loops caused by incorrect configurations.

Static ports that are trunking cannot become dynamic ports. You must first turn off trunking on the trunk port before changing it from static to dynamic.

### 3.15 VMPS CONFIGURING FILES

The following describes the parameters in the configuration file:

You must define the VMPS domain in the file. It corresponds to the VTP domain name of the switch. The mode defines the VMPS to be either in *open* or *secure* mode. The fallback VLAN is assigned to the MAC addresses not defined in the database.



"MAC addresses" define the MAC address and the corresponding VLAN table. The keyword `NONE` specifies that the MAC address should be denied connectivity. A port is identified by the IP address of the switch and the module/port number of the port, in the form `mod_num/port_num`.

"Port group" defines a logical group of ports. The keyword `all-ports` specifies all the ports in the specified switch.

"VLAN group" defines a logical group of VLANs. These logical groups define the VLAN port policies in the next section.

"VLAN port policies" define the ports associated with a restricted VLAN. You can configure a restricted VLAN by defining the set of dynamic ports on which it can exist.

The VMPS parser is a line-based parser. Start each entry in the file on a new line. Ranges are not allowed for the port numbers.

**A sample VMPS configuration file is shown below:**

```
!vmmps domain
```

```
<domain-name>
```

```
! The VMPS domain must be defined.
```

```
!vmmps mode {
```

```
open | secure }
```

```
! The default mode is open.
```

```
!vmmps fallback
```

```
<vlan-name>
```

```
!vmmps no-domain-req { allow | deny }
```

```
!  
!  
! The default  
value is allow.  
vmps domain WBU  
vmps mode open  
vmps fallback  
default  
vmps no-domain-req deny  
!  
!  
!MAC  
Addresses  
!  
vmps-mac-addr  
!  
! address <addr> vlan-name  
<vlan_name>  
!  
address 0012.2233.4455 vlan-name hardware  
address  
0000.6509.a080 vlan-name hardware  
address aabb ccdd.eeff vlan-name
```

```

Green
address 1323.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654
vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port
Groups
!
!vmps-port-group <group-name>
! device <device-id>
{ port <port-name> | all-ports }
!
vmps-port-group
WiringCloset1
device 198.92.30.32 port 3/2
device 172.20.26.141 port
2/8
vmps-port-group "Executive Row"
device 198.4.254.222 port
1/2
device 198.4.254.222 port 1/3
device 198.4.254.223

```

```

all-ports
!
!
!VLAN groups
!
!vmps-vlan-group
<group-name>
! vlan-name <vlan-name>
!
!
vmps-vlan-group
Engineering
vlan-name hardware
vlan-name software
!
!
!VLAN port
Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group
<group-name> }
! { port-group <group-name> | device

```

```
<device-id> port <port-name> ]  
{  
vmps-port-policies vlan-group  
Engineering  
port-group WiringCloset1  
vmps-port-policies vlan-name  
Green  
device 198.92.30.32 port 4/8  
vmps-port-policies vlan-name  
Purple  
device 198.4.254.22 port 1/2  
port-group "Executive  
Row"
```

## CHAPTER 4

### 4.0 NETWORK DEVICES: NAMES, MODELS, TERMINOLOGIES,

#### FUNCTIONS AND PRICES

##### 4.1 OPTIC FIBRE SWITCH

###### Fiber Optic Switch - 4 Port Ethernet

Opterna Model 5100S Price: \$295.00

Sale price: \$250.75

Fiber Optic Connectors: sc

Mounting: desk/floor

Power Supply: universal w/IEC320 connector

###### Fiber Optic Switch - 8 Port Ethernet

Opterna Model 9100S Price: \$345.00

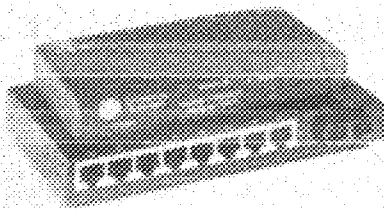
Sale price: \$293.25

Fiber Optic Connectors: sc

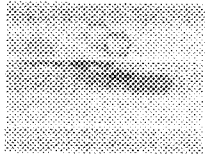
Mounting: desk/floor

Power Supply: universal IEC320 connector

Fig 4 0

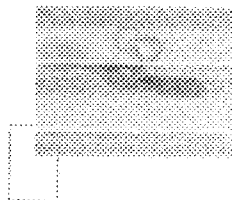


## 4.2 FIBRE OPTIC ADAPTORS



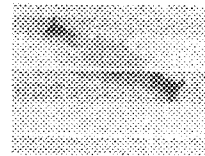
Fiber Optic Adapter-  
SC-SC- Multi Mode-  
Duplex

FA-SCSC2-MM \$7.00



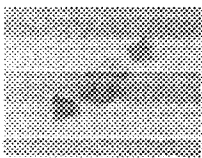
Fiber Optic Adapter- SC-SC-  
Single Mode-Duplex

FA-SCSC2-SM \$9.75



Fiber Optic Adapter- ST-SC-  
Multi Mode-Simplex

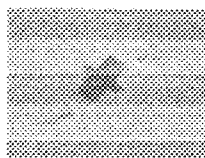
FA-STSC-MM \$10.50



F/O Adapter, SC/APC-  
SC/APC- Single Mode-  
Simplex

FA-SCA/SCA-SM

\$14.00



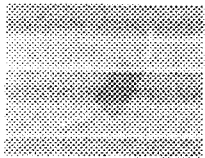
F/O Adapter--- MTRJ-  
MTRJ--- Multi Mode-Duplex

FA-MTMT-MM \$4.20



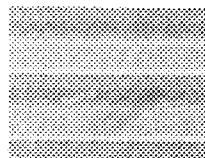
Fiber Optic Adapter--- FC-FC-  
-- Multi Mode-Simplex

FA-FCFC \$6.50



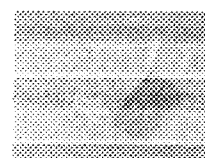
Fiber Optic Adapter-  
LC-LC- Multi Mode-  
Simplex

FA-LCLC-MM \$5.50



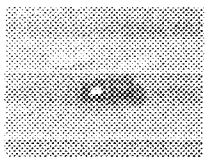
Fiber Optic Adapter- LC-  
LC- Single Mode-Simplex

FA-LCLC-SM \$13.50



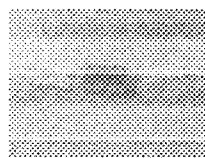
Fiber Optic Adapter--- LC-  
LC- Multi Mode-Duplex

FA-LCLC2-MM \$9.00



Fiber Optic Adapter,  
MU-MU, Single Mode-  
Simplex

FA-MUMU-SM  
 \$16.00



Fiber Optic Adapter, MU-  
MU, Single Mode-Duplex

FA-MUMU2-SM \$20.00



### 4.3 FIBER OPTIC TERMINOLOGIES

**Absorption:** One cause of attenuation where light signal is absorbed into the glass during transmission

**Adaptor:** A device used to interconnect two different connector types

**Attenuation:** Optical loss of power , attenuation is measured in dB per length of cable.

Attenuation is usually caused by absorption and scattering.

**Attenuator:** A device used to attenuate an optic signal

**Bandwidth:** The range of signal frequencies that an optic fiber cable will transmit

**Buffer:** The protective coating over the fiber

**Coupler:** A device used to connect two similar connector types

**Fusion Splice:** A permanent splice where the two fiber ends are welded together.

**Insertion Loss:** The attenuation caused by the insertion of a device [such as splice or connection point to a cable.

**Link:** The entire span between two optical devices. Includes all cables, connections, and splices.

**Loss Budget:** The maximum amount of power that is allowed to be lost per optical length.

**Jack:** The female receptacle-usually found in equipment.

**Mandrel:** A fiber wrapping device used to cause attenuation within a fiber cable.

**Mechanical splice:** A mechanical means of connecting two fibers.

**Multimode:** A type of fiber optic cable where the core diameter is much larger than the wavelength of light transmitted. Two common multimode fiber types are 50/125 and 62.5/125.

**Plug:** A male connector.

**Return Loss:** The ratio of the power launched into a cable and the power of the light returned down the fiber. This measurement is expressed in positive decibel units [dB]. A higher number is better.  $\text{Return loss} = 10 \log[\text{incident power}/\text{returned power}]$

**Scattering:** A second cause of attenuation. Scattering occurs when light collides with individual atoms in the glass.

**Termination:** The process of mechanically installing a connector onto a fiber cable.

**Wavelength:** A means of measuring light color. Expressed in nanometer[nm]

#### 4.4 CISCO OFFERS

Part Number	Item Description	List	
		RRP	Sale Price

#### SWITCHES

WS-C2950- 12	12-port 10,100 Switch	£615	£298
WS-C3550- 24-SMI	24-pt 10,100+2-pt. GBIC SMI SW,	£2,060	£1,042
WS-C2970G- 24T-E	Catalyst 2970, 24 10/100/1000T Enhanced Image	£2,745	£1,295
WS-C3750- 24TS-S	Catalyst 3750 24 10/100 + 2 SFP Standard Multilayer Image	£2,745	£1,349

#### Upgrades

for the

above

system

WS-X3500- XL	GigaStack GBIC Module	£175	£86
-----------------	-----------------------	------	-----

WS-G5483=	1000BASE-T GBIC	£275	£94
-----------	-----------------	------	-----

## ROUTERS

CISCO1701-	Cisco 1701 ADSL Security Access Router	£1,032	£559
------------	--	--------	------

K9

Upgrades

for the

above

system

PVDM-	Cisco PVDM PVDM/4 - Voice DSP module - 4	£275	£150
-------	--	------	------

256K-4= ports

PVDM2-32=	Cisco voice fax module Voice, fax module Plug-	£1,100	£605
-----------	--	--------	------

in module G.711 Cisco IOS 12.3(7)T

CISCO2612	Cisco 2612 - router, External - modular,44,5 cm	£2,060	£1,122
-----------	---	--------	--------

x 30 cm x 4.3 cm,1 x Motorola MPC860 40

MHz,32 MB,8 MB,Ethernet, Token Ring,AC

100/240 V ( 50/60 Hz )

CISCO2801	Cisco 2801 Integrated Services Router - router,	£1,390	£749
	External - modular - 1 U, 128 MB (installed) /		
	384 MB (max), Cisco IOS , hardware encryption,		
	MPLS support		

## SECURITY

### & VPN

PIX-515E- FO-FE-BUN	PIX 515E-FO-FE Bundle (Chassis, Failover SW, 6 FE, VAC+)	£2,405	£1,329
PIX-515E-R- BUN	Restricted SW Bundle 2FE pt	£2,400	£1,386
PIX-506E- BUN-K9	PIX 506E 3DES/AES Bundle (Chassis, SW, 2 FE Ports, 3DES/AES)	£960	£532
PIX-506E	Firewall Chassis, 2-pt Eth 10BT, Software	£960	£532

## **4.5 CISCO ROUTERS**

### **Cisco SP Routers**

#### **Cisco 7200 Series**

Industry's most widely deployed universal services router for Enterprise and Service Provider edge applications. The Cisco 7200 combines exceptional price/performance with the widest range of connectivity options and unmatched feature support.

#### **Cisco 7300 Series**

The Cisco 7300 Series is optimized for flexible, feature rich IP/MPLS services at the network edge, where service providers and enterprises link together. The Cisco 7300 Series can be used for enterprise campus Internet gateway applications or be deployed by service providers as a high-end CPE router for enterprise-class managed service offering.

#### **Cisco 7400 Series**

The Cisco 7400 series are compact, single-rack unit (RU) routers ideal for application specific routing deployments in service provider and enterprise networks.

#### **Cisco 7500 Series**

Service providers and enterprise customers need solutions that optimize network density, bandwidth aggregation, availability, serviceability, and operational costs. The high-performance Cisco 7500 Series Routers remain the market leaders due to their breadth of advanced support for LAN/WAN services, redundancy, reliability, and performance.

#### **Cisco 7600 Series**

The Cisco 7600 Series Router delivers robust, high-performance IP/MPLS features for service

provider edge and enterprise MAN/WAN applications. Coupled with various interfaces and innovative adaptive network processing technology, the Cisco 7600 Series provides integrated Ethernet, private line, and subscriber aggregation capabilities

### **Cisco 10000 Series**

The Cisco 10000 Series is the industry's only edge router that delivers consistent, high performance features for carriers deploying IP/MPLS services to broadband and private line customers

### **Cisco 10700 Series**

The Cisco 10700 Series Internet Routers are the only metro edge access routers designed to optimize optical transport with Dynamic Packet Transport (DPT), Cisco's market leading Resilient Packet Ring (RPR) technology, to integrate full IP routing and services and to deliver intelligent Ethernet subscriber interfaces for simple, scalable, and reliable networks.

### **Cisco 12000 Series**

The Cisco 12000 Series routers make up a portfolio of intelligent routing solutions that scale from 2.5 Gbps/slot to 40 Gbps/slot capacity, enabling carrier-class IP/MPLS core and edge networks.

## **4.6 CISCO SWITCHES**

### **Cisco Distribution Switches**

#### **Cisco Catalyst 3550 Switch**

The Cisco Catalyst 3550 Series Intelligent Ethernet Switch is a line of stackable, multilayer switches that provide high availability, quality of service (QoS), and security to enhance network operations.

#### **Cisco Catalyst 3560 Switch**

The Cisco Catalyst 3560 Series switches is a line of fixed configuration, enterprise-class, IEEE 802.3af and Cisco prestandard Power over Ethernet (PoE) switches in Fast Ethernet configurations that provide availability, security, and quality of service (QoS) to enhance network operations.

#### **Cisco Catalyst 3750 Switch**

The Cisco Catalyst 3750 Series is an innovative product line for mid-sized organizations and enterprise branch offices. Featuring Cisco StackWise technology, the products improve LAN operating efficiency by combining industry-leading ease of use and the highest resiliency available for stackable switches.

#### **Cisco Catalyst 3750 Metro Switch**

The Cisco Catalyst 3750 Metro Series switches are a new line of premier multilayer switches that bring greater intelligence to the metro Ethernet edge, enabling the delivery of more differentiated metro Ethernet services.



### **Cisco Catalyst 4000/4500 Chassis Switch**

The Cisco Catalyst 4000/4500 Series extends control from the backbone to the network edge with intelligent network services including advanced quality of service (QoS), scalable performance, comprehensive security, and simple manageability.

### **Cisco Access Switches**

#### **Cisco Catalyst 2900 Switch**

The Catalyst 2900 family has the industry's highest density, small form factor fixed configuration switches, offering feature-rich end-to-end software and solutions for workgroup and wiring closets.

#### **Cisco Catalyst 2940 Switch**

The Cisco Catalyst 2940 Series Switches are small, standalone, managed switches with 8 Fast Ethernet ports and a single integrated Fast Ethernet or Gigabit Ethernet uplink.

#### **Cisco Catalyst 2950 Switch**

The Cisco Catalyst 2950 Series is a line of fixed-configuration, stackable, and standalone switches that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity.

#### **Cisco Catalyst 2970 Switch**

The Cisco Catalyst 2970 Series Switches are affordable Gigabit Ethernet switches that deliver wire-speed intelligent services for small and medium businesses and enterprise branch offices.

## **Cisco Catalyst 3500 XL Switch**

The Cisco Catalyst 3500 Series XL is a scalable line of stackable 10/100 and Gigabit Ethernet switches that deliver premium performance, manageability, and flexibility, with excellent investment protection.

## **4.7 CISCO SECURITY AND VPN**

### **Cisco Security and VPN**

#### **Cisco ASA 5500 Series Adaptive Security Appliance**

The Cisco ASA 5500 Series Adaptive Security Appliance is a high-performance, multifunction security appliance family delivering converged firewall, IPS, network anti-virus and VPN services. As a key component of the Cisco Self-Defending Network, it provides proactive threat mitigation that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity while remaining cost-effective and easy-to-manage.

#### **Cisco Secure PIX Firewall**

The world-leading Cisco PIX Firewall and Security Appliance Series provides robust, enterprise-class, integrated network security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN), in-line intrusion protection, and rich multimedia and voice security in cost-effective, easy-to-deploy solutions.

## **Cisco IDS**

As part of the market-leading Cisco IDS Intrusion Detection System (IDS), the Cisco IDS 4200 sensors provide pervasive protection against unauthorized or malicious activity traversing the network, such as attacks by hackers.

## **Cisco VPN 3000 Series Concentrators**

Cisco VPN 3000 Series Concentrators is a family of purpose-built, remote access Virtual Private Network (VPN) platforms and client software that incorporates high availability, high performance and scalability with the most advanced encryption and authentication techniques available today. Supported connectivity mechanisms include IPSec and WebVPN (Clientless SSL web browser-based connectivity).

## **Cisco Security Software**

Pricing and information on the Cisco Security Software range of products, including: Cisco Secure Access Control Server, Cisco VPN Client and the new Cisco Security Agent.

## **Cisco Security Monitoring, Analysis and Response System (CS-MARS)**

The Cisco Security Monitoring, Analysis and Response System (CS-MARS) extends the portfolio of security management products for the Cisco Self-Defending Network initiative. A result of the Protego acquisition, Cisco CS-MARS offers a family of high-performance, scalable appliances for threat management, monitoring, and mitigation, enabling customers to make more effective use of network and security devices.

## CHAPTER 5

### RECOMMENDATION AND CONCLUSION

#### RECOMMENDATION

In order to solve data communication problems faced on our campus today, especially file transfer, lack of good students' database and records, illegal access to delicate information, I strongly recommend that a Virtual Local Area Network [VLAN] be implemented in FUT Minna, Bosso Campus, Starting with a Local Area Network [LAN] in each department, then all these can be connected via VLAN. Thus enabling an efficient communication on campus irrespective of geographical location.

The network [VLAN] can be programmed to utilize the Net [Internet], Thus enabling a communication medium / access with other universities in the country and the world at large that are also connected to the net [Internet].

Regulatory bodies like NUC [Nigerian University Commission] would also have access to the university.

## CONCLUSION

The project is carried out to establish a secured / cheap, flexible, hierarchical and efficient means of communication on our campus knowing we are in the information age. The emergence of information and communication technology [ICT] attempts to solve this problem. Thus the need for a decentralized computing and shared information which provides group of people [ schools (Faculties), departments, teams e.t.c ] with the flexibility to handle their own specific information processing tasks, regardless of physical location. It also eradicates traffic collision and hence the cutting edge for technological development in data communication networks.

## REFERENCES

1. <http://www.arin.net>
2. <http://www.cisco.com>
3. <http://www.google.com>
4. Interconnecting Cisco devices by Steve Mc Querry, Copyright 2002.  
Cisco system inc. [ISBN: 1-57870-111-2]
5. Farber, D.J, and Vitta J.J , " Extendability considerations in the design of the distributed computer system ( CS )," Proc. Nat. Telecomm. Conf., (November 1973)  
Atlanta, Georgia, pp.15E
6. David Growth, Network + Study Guide , Third Edition  
William Stallings, Local and Metropolitan Area Network, fifth edition.
7. Sunshine , Carl A., " Source Routing in Computer Networks, " Computer  
Communication Review 1, 7, (January 1977) pp.29-33
8. Metcalfe, R.M , and Boggs, D.R., "Ethernet: Distributed Packet Switching for  
Local Computer Network," Comm ACM 19,7 (July, 1976), pp.395-404
9. Clark. D.D, Pograd K.T., and Reed. D.P., "An Introduction to Local Area Network. "  
Proc. IEEE 66, 11 (November, 1978),. Pp. 1497-1517
10. International Organization for Standardization, Open System Interconnection  
Reference Model of Open Systems Architecture,"
11. Association Francaise de Normalization Tour Europe, Paris, France, November,  
1978
12. Todd Lammle, CCNA study guide fifth edition
13. Todd Lammle, CCNA study guide fifth edition