# The Security Implications of Virtual Local Area Network (VLAN),Niger Mills, Calabar, Nigeria.

D. E. Bassey., B. E. Okon., R. Umunnah.

**ABSTRACT:** Virtual local area network (VLAN), is a logical grouping of network users and resources connected to administratively define the operation of activated ports on a switch. The creation of VLAN is saddled with the ability to develop smaller broadcast domain within a layer-2 switching router; by assigning different ports on the switch to different sub networks. The application was a re-design project carried out on the Niger-Mills' network to improve the operational short falls identified by the operators. Niger-Mills' LAN network covered a total of 5 departments:: marketing, sales, finance, engineering and management. Five (5) users were randomly sampled and selected from each department to constitute their individual LAN, making a total of 25 computers. The project successfully introduced this process in the Niger-mills LAN as a test run. It was further recommended that switch-model 2950/3560 be introduced to activate this function automatically. From the trouble shooting process, it was obvious that layer-2 switches only read frames for filtering. They don't access the network layer protocol, and by default, switch forward all broadcast. But the creation and implementation of VLAN, essentially activated a small broadcast domain at layer-2.

Based on this framework, the design was modified using six (6) core layer switches with 24 port Cisco catalyst 2950 switch. While the distribution and access switches were D-link switches, with link speed of 100Mb/s. The software, WIRESHARK, was also used to decode packet contents of the interface for readability. Its output was analyzed to verify that the security on the network was enhanced. The introduction of VLAN into Internet-circuit has been able to regulate these practices. Also, VLAN, advantageously built the LAN with multiple broadcast groups and allowed total control of each port and user.

**Key Words:** Broadcast domain, Ethernet, Host, LAN, Ports, VLAN

Electronics and Computer Technology Unit,
Department of Physics,
University of Calabar,
Calabar, Nigeria.



## 1.0 INTRODUCTION

Local Area Network (LAN) refers to a computer network covering a small physical area like a home, office, a small group of buildings or administrative location. It has the basic feature of higher data transfer rates in view of its small geographical coverage, and requires minimum telecommunications facility (Voelker, 2009).

Virtual local area network (VLAN), is a logical grouping of network users and resources connected to administratively define the operation of activated ports on a switch ((Bassey, D.E. et al. 2016).. The creation of VLAN is saddled with the ability to develop smaller broadcast domain within a layer-2 switching router; by assigning different ports on the switch to different sub networks. VLAN is usually treated like its own subnet or broadcast domain. That is, frames broadcast into the network are only logically switched between the ports that are grouped within the same VLAN.

Before delving into the VLAN security setup, it is pertinent to take a critical look at the basic VLAN structures and the setup.

## 2.0 BASIC STRUCTURAL SET-UP OF VLAN

### 2.1 Flat network structure

The structure of the network below (Fig.1) shows the design of a router (HOST-DEB) which allows broadcast to occur only from the originating network and switches forward the broadcast to all segments of the network. This type of network is called flat network because it has only one broadcast domain. Host- DEB is sending out broadcast to all ports through all the switches involved in forwarding the broadcast. Figure 1 is the router containing Host-DEB.

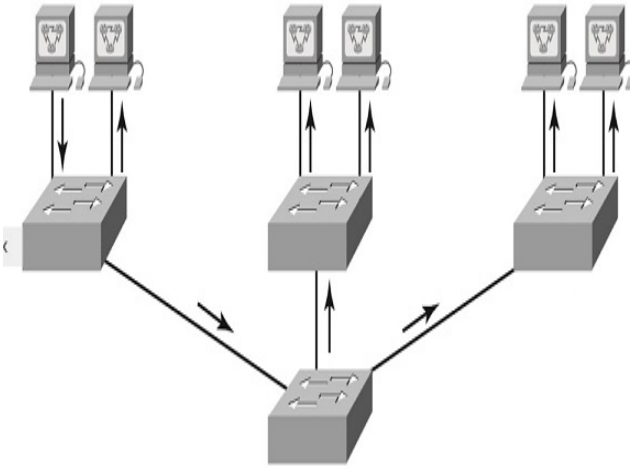

Fig. 1: Flat network structure showing the major host, Host-DEB.

### 2.2 Switched network structure

Figure 2 below, illustrates Host-DEB, sending a frame to a destination, Host-SAM. The frame is only forwarded to the port where Host-SAM is located. This is a huge improvement over the old hub network that differs from the conventional design where a network will have only one collision domain.

The advantage of having a layer-2 switch is the creation of an individual collision domain segment for each device to plug into each port on the switch. Thereby, setting the stage to surpass the Ethernet constraints, as larger networks can now be built using this platform (James et al.,2000).

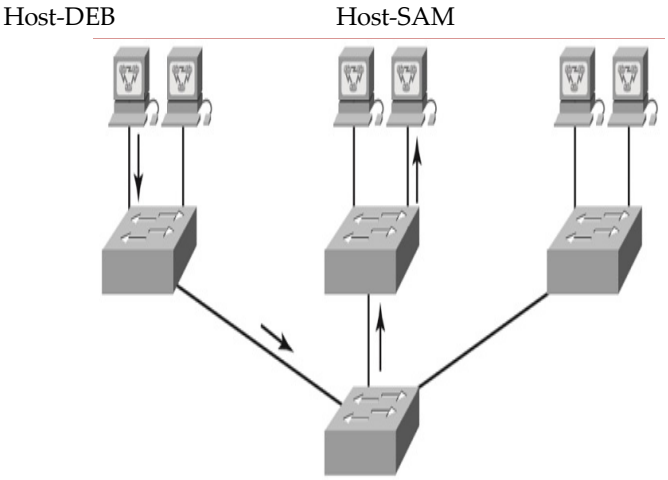


Fig.2: Switch network structure

### 2.3 VLAN and Security

The security issues in flat inter-network illustrated in Fig.1 was tackled by connecting hubs and switches together with routers. In this scenario, it was basically the router's job to maintain security. However, from operational point of view, this arrangement was ineffective. The reasons were obvious: firstly, any subscriber connecting to the physical network could access the network resources located on that particular LAN. Secondly, subscribers were expected to observe all traffic in that network by simply plugging a network analyzer into the hub. Users could also join a work-group by just plugging their work-stations into the existing hub. These media created a very high rate of insecurity within the entire network resources. To arrest the unwholesome drift, VLAN was introduced into the internet-work to regulate these practices. This was done by building another LAN and creating multiple broadcast groups; thereby configuring full control over each port and user (Wright and Joe, 2009). The idea of anyone just plugging their workstation into any switch port and gaining access to the network resources was eradicated. The administrator can now control each port and resources accessed by every port. This study successfully introduced this process in the Niger-mills LAN as a test run. It was further recommended that switch-model 2950/3560 be introduced to activate this function automatically.

VLAN can be created based on the particular resources required by any operator. In addition, the switches can be configured to alert network management station of any unauthorized access to the network resources; and through the VLAN hub, restrictions can be implemented on the router. Such restrictions can be extended to hardware addresses, protocols and applications.

### 2.4 Flexibility and Scalability

From what have been discussed so far, it is obvious that layer-2 switches only read frames for filtering. They don't access the network layer protocol and by default, switch forward all broadcast. But the creation and implementation of VLAN, essentially activates a small broadcast domain at layer-2.

Broadcast sent out from a node in one VLAN shall not be forwarded to the port configured for a different VLAN. So, by assigning switch ports or users to VLAN groups on a switch or groups of connected switches, flexibility was gained to add only the users needed into the broadcast domain, irrespective of their physical locations. This setup also worked to block broadcast storms caused by a faulty network interface card (NIC), as well as prevented an intermediate device from propagating broadcast storms throughout the entire stations. These problems can occur in a network built with VLAN. Incidentally too, VLAN has the capacity to quarantine the problem.

Another advantage of VLAN is that as the station gets bigger, additional VLANs can be created from within to reduce the high bandwidth requirement of the broadcast. Invariably, the fewer the users in a VLAN, the lesser the problems the users may likely encounter while accessing the VLAN.

### 2.5 Understanding the working of VLANs

To understand how a VLAN is configured to the ports in a switch, it is imperative to take a look at the working of the traditional network as shown in Fig.3 below:

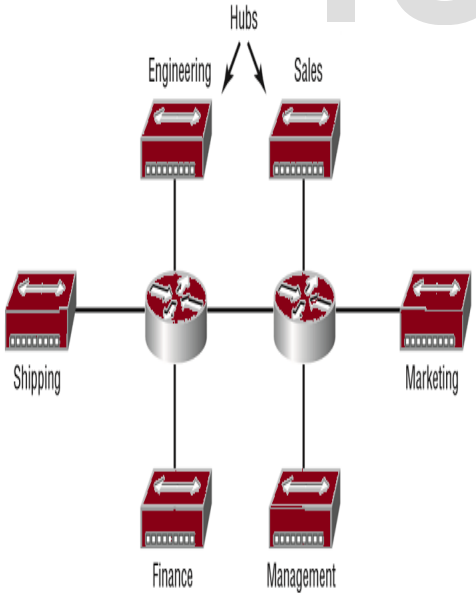


Fig.3: Physical LANs connected to routers

In Fig. 3 above, each network is attached with a hub to a router. Each node attached to a particular physical network must match the network's number in order to be able to communicate on the internet circuit. Each department has its own LAN, so if you need to add new users to engineering department, you would just plug them into the engineering LAN and they will automatically be part of the engineering rear-ender and broadcast domain. This design was recognized for many years without identifying and modifying the defect in the design. Once the hubs for the engineering LAN are fully engaged and new users are to be added to the engineering LAN, the user cannot access the internet-circuit of the engineering department. However, when there are extra spaces in the LAN of the marketing department, the engineering staff can be transferred to the marketing unit through which he is connected to the LAN of the marketing unit. This obviously means that the new user is now part of the marketing LAN, instead of the engineering LAN. This model created a breach of security because the new engineering employee is now a member of the marketing broadcast domain and he can see all the servers and access all network services that the marketing staff can see and access. Secondly, for this very user to access the engineering network services, the administrator needs to get their job done by going through the router to log into the engineering server. This was not very efficient.

However with the advent of switches, the physical boundaries in the network can be removed as shown in Fig.4 below. From the illustration below, staff from the engineering unit cannot see and access the resources in any other unit of the company even when he is connected through the router of a different unit. He can only communicate with the VLAN that he is configured to interact with.(If VLAN-2 is representing engineering, VLAN-2 can communicate with VLAN-2 anywhere irrespective of their position/location in the company).

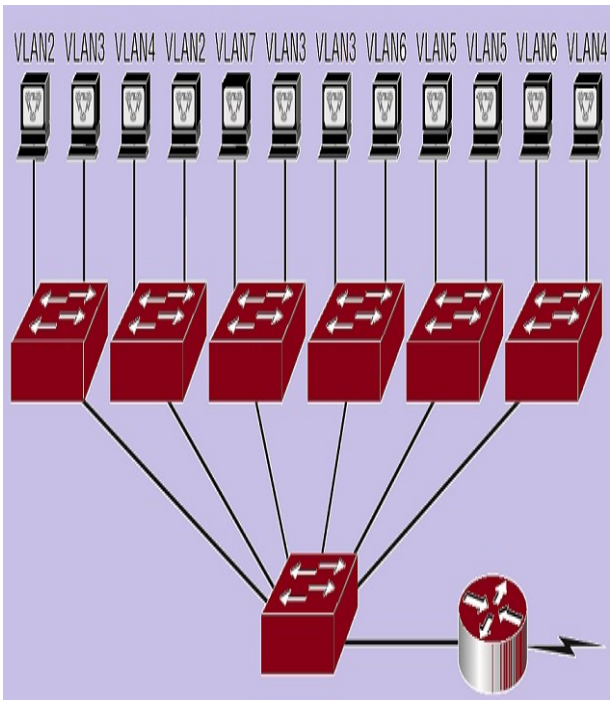


Fig.4: Switches removing the physical boundary

## 3.0 RESEARCH METHODOLOGY

### 3.1 Simulation details

Network communication among the VLANS was made possible using a Cisco 3600 router. Based on this framework, the design was made using six (6) core layer switches with 24 port Cisco catalyst 2950 switch (Hooke, 2000). While the distribution and access switches were D-link switches, with the link speed being 100Mb/s. The LAN network covered a total of 5 departments which include: marketing, sales, finance, engineering and management. Five (5) users were randomly sampled and selected from each department to constitute their individual LAN, making a total of 25 computers as shown in table 1 below.

This method involved the use of a packet application called Wire-shark. The application was used on the Niger-mills network to capture packets on the network Interface card (NIC) of some users on the network in order to monitor their activities on the network (Bassey, D.E. et al. 2016,), based on the protocols they are using at that time. The software (WIRESHARK) decoded packet contents of the interface for readability. Its output was analyzed to verify if the security on the network was enhanced through the injection of WIRESHARK (Patterson, 2008).

Table 1

Proposed network profile of Niger mills company, Calabar

| S/N | Department | VLAN | no of users |
|---|---|---|---|
| 1 | Sales | 4 | 5 |
| 2 | Marketing | 2 | 5 |
| 3 | Finance | 4 | 5 |
| 4 | Management | 3 | 5 |
| 5 | Engineering | 6 | 5 |
| | **TOTAL** | | **25** |

### 3.2 Hardware Configurations

All networks require four components so that the nodes within it can communicate with each other and exchange information. These are components transmission media, hardware devices, rules and standards or protocols and software (components in form of network operating systems and applications). In this work, some network hard-wares like the router was configured using the command line interface, while Class-C type IP addresses were assigned to end users' devices like printer, PCs and server as shown below

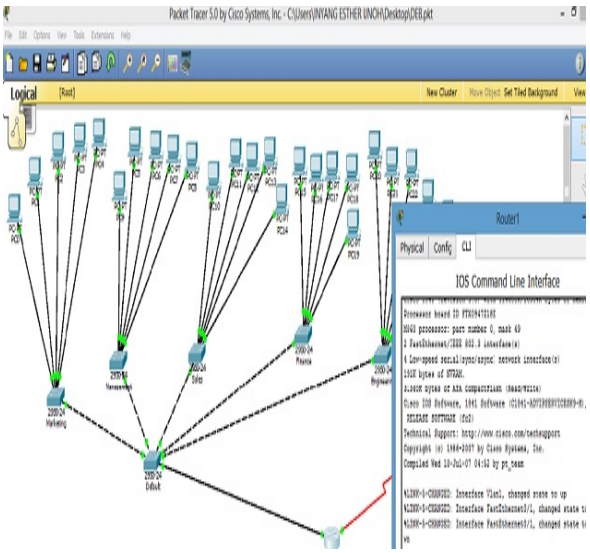

Fig 5: Showing router fully configured to perform its action

### 3.2.1 Router Configuration

| | |
|---|---|
| Router | enable |
| Router | configure terminal |
| Router (configure) | Hostname DEB-LAN |
| DEB-LAN (configure) | line console 0 |
| DEB-LAN (configure-line) | password pass-word |
| DEB-LAN (configure-line) | login |
| DEB-LAN (configure-line) | line Vty 0 4 |
| DEB-LAN (configure-line) | password pass-word |
| DEB-LAN (configure-line) | login |
| DEB-LAN (configure-line) | exit |
| DEB-LAN (config-line) | interface fastEthernet 0/0 |
| DEB-LAN (config- line) | ip address 192.168.10.1 255. 255.255.0 |
| DEB-LAN (config) | no shutdown |
| DEB-LAN (config) | interface se 0/1/0 |
| DEB-LAN (config) | ip address 192.152.10.1 255.255.255.0 |
| DEB-LAN (config-if) | # exit |

### 3.2.2 IP Addressing

The computer systems of the LAN were assigned corresponding IP addresses based on their logical groupings (VLAN). Below is a picture showing the IP address configuration of PC-marketing 1 in the marketing VLAN.

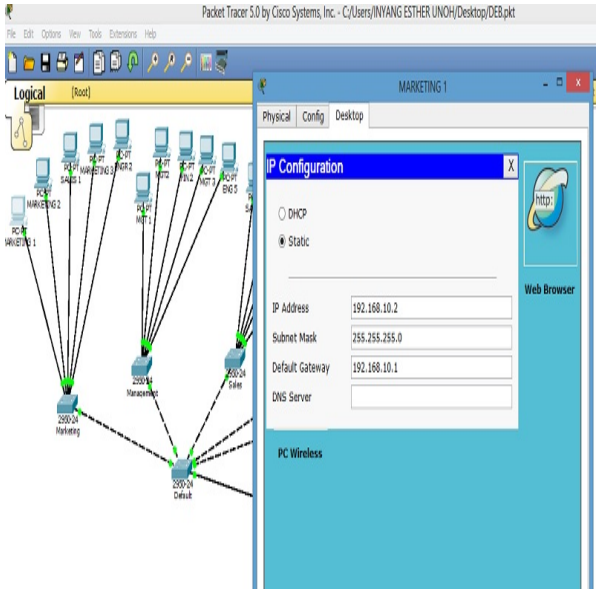


Fig.6: IP addresses of computer systems (marketing-1)

Below is a table showing the names and the IP addresses of each node on the LAN

### 3.2.3 VLAN configuration

Switch-model 2950 was configured for this study. Since this switch can perform this task under auto mode conveniently, the exercise was not time consuming.

## 4.0 RESULTS AND DISCUSSIONS

### 4.1 Results

The advantages of designing a network with VLAN are tremendous as the users can be restricted from having unauthorized access to the network resources and web pages. Fig. 7 below shows a complete configuration of the networks with VLAN.

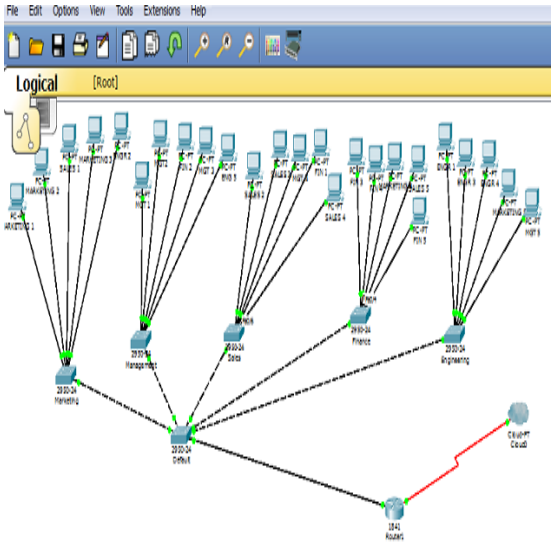


Fig.7: LAN simulation with VLANs

Tables 2-6 show the IP addresses of the nodes in the 5 VLANs of the 5 selected units of Niger mills, Nigeria Ltd.

TABLE 2

Nodes of IP addresses and arrangement

on VLAN-2 (marketing VLAN)

| Nodes Arrangement | IP Addresses |
|---|---|
| Marketing 1 | 192.168.10.2/24 |
| Marketing 2 | 192.168.10.3/24 |
| Sales 1 | 192.168.10.4/24 |
| Marketing 3 | 192.168.10.5/24 |
| Engineering 2 | 192.168.10.6/24 |

TABLE 3

Nodes of IP addresses and arrangement

on VLAN-3 (Management-MGT) VLAN)

| Nodes Arrangement | IP Addresses |
|---|---|
| MGT 1 | 192.168.10.7/24 |
| MGT 2 | 192.168.10.8/24 |
| FIN 2 | 192.168.10.9/24 |
| MGT 3 | 192.168.10.10/24 |
| ENGR 5 | 192.168.10.11/24 |

TABLE 4

Nodes of IP addresses and

arrangement on VLAN-4 (Sales VLAN)

| Nodes Arrangement | IP Addresses |
|---|---|
| Sales 2 | 192.168.10.12/24 |
| Sales 3 | 192.168.10.13/24 |
| MGT 4 | 192.168.10.14/24 |
| FIN 1 | 192.168.10.15/24 |
| Sales 4 | 192.168.10.16/24 |

TABLE 5

Nodes of IP addresses and

arrangement on VLAN-5 (Finance VLAN)

| Nodes Arrangement | IP Addresses |
|---|---|
| FIN 3 | 192.168.10.17/24 |
| FIN 4 | 192.168.10.18/24 |
| MKT 4 | 192.168.10.19/24 |
| FIN 1 | 192.168.10.20/24 |
| Sales 4 | 192.168.10.21/24 |

TABLE 6

Nodes of IP addresses and arrangements

on VLAN-6 (Engineering (ENGR) VLAN)

| Nodes Arrangement | IP Addresses |
|---|---|
| ENGR 1 | 192.168.10.22/24 |
| ENGR 3 | 192.168.10.23/24 |
| ENGR 4 | 192.168.10.24/24 |
| MKT 5 | 192.168.10.25/24 |
| MGT 5 | 192.168.10.26/24 |

**4.2 Discussion**

The internet circuit is made up of five broadcast domains or VLANs as shown in Fig. 7 above. The broadcast domains were labeled in accordance with the 5 selected departments of the company.

From Fig. 7 and Table 2 above, Sales 1 and ENG-2 nodes were plugged into the Marketing VLAN (VLAN-2) to ascertain if the VLAN configuration has enhanced effective security in the internetwork. A positive result was achieved as the physical location of Sales-1 and ENGR-2 did not signify that they were communicating with Marketing 1, 2 and 3. They were logically separated and redirected to their respective departments as Sales 1 was assigned VLAN-4, and ENGR-2 was assigned VLAN-6. Though they were connected to a port on a switch in the Marketing VLAN, they did not interconnect or share resources. Also, in Table 3, FIN-2 and ENGR-5 were plugged into the management broadcast domain (VLAN-3). Unexpectedly, they did not share the network resources with the Management VLAN. Rather, they were logically configured to communicate with their traditional VLANs which are VLAN-5 and VLAN-6 respectively.

This process was repeated for VLAN-4, VLAN-5 and VLAN-6, and the result was awesome. Furthermore, a casual plug-in into the extra port VLAN-5 switch indicated that all unused ports in the internetwork were assigned VLAN-1, which was meant to be basically for work-group and administrative purposes. This was not operationally good; as anyone who plugs into the unused ports can access the admin resources and could use all site without any limitation. An attempt to assign individual ports to different VLAN numbers was futile and protracted. However, to regulate unnecessary and unauthorized access to the internetwork, firewall security device were configured automatically to those ports to ward-off any illegal access to the company's resources and unofficial sites.

**5.0 CONCLUSION**

From the deductions made from the project, it is obvious that nodes within the same VLAN cannot communicate with each other except they are assigned to the same broadcast domain. This claim is in congruence with what Wood (2010) asserted in his lecture on network security attack. This theory has been empirically reviewed by this work. Accordingly, VLAN helps in the effective enhancement of network security in corporate LAN. This simply implies that the activation of VLAN in an organization enriches confidentiality, security and the removal of physical boundaries.

In addition, the switches were configured to inform the network management station of any unauthorized access to the network resources; in order to investigate and place restrictions on such hardware addresses, protocols and applications. From the study, VLAN has the benefits of enhancing security greatly. In addition, it increases the number of broadcast domain while decreasing their sizes. It also helps in grouping users and resources logically.

**REFERENCES**

1..Bassey, D. E., Ogbulejie, J.C., Okon, B. E (2016) Modelling a Low Latency IP Network in Nigeria. IJSETR, Vol.15, Issue 3, 830 - 834.

2. Bassey, D. E., Okon, B.E., Effiom, E.E...(2016). Pilot Case-study of GSM-Network Load Measurement in Ikeja, Nigeria, IJSETR,Vol.5,Issue3,824-829.. ..

3..David A. Patterson (2008). Computer Organization: Hardware / Software Interface, 4th Edition.

4. Geoffrey M. Voelker (2009). Characterizing user Behavior and Network Performance in a Public Wireless LAN. Proceedings of the 2009 IEEE International Conference on Communication, 1287-1291

5..Hooke, A. (2000). Interplanetary Internet, Third Annual International Symposium on Advanced Radio

Technologies. Retrieved 2011-11-12

6. James F.K, and Keith W.R. (2000). High Speed Networking: A Systematic Approach to High Bandwidth Low-Latency Communication. Computer Networking. The Internet (5th Edition).

7. Wood, J. (2010). "The Darknet: A Digital Copyright Revolution". Richmond Journal of Law and Technology 16 (4). Retrieved 25 October 2011.