EVALUATION OF NETWORK PERFORMANCE FOR SINGLE VLAN AND SIX VLANs NETWORK

Ogar-abang, M. O., Fischer, G. A. Akpama, E. J.
[1]Department of Physics Engineering, Arthur Jarvis University, Calabar, Nigeria.
[2,3]Department of Elect/Elect Engineering, CRUTECH, Calabar, Nigeria.
mikeogar@arthurjarvisuniversity.edu.ng
gertrudefischer42@gmail.com
ekoakpama2004@yahoo.com

Abstract
The customer's interest is quality service. Network performance for single and multiple VLANs is investigated with an attempt to evaluate and compare the performance of the two in terms of quality of service. Ease of segmentation of network traffic, congestion control, and improved security by segmenting a single broadcast network using virtual Local Area Network (VLANs) is the main objective of this paper. An evaluation of a network with single VLAN was carried out to determine the waiting time (W_q), Network utilization (ρ) and mean service time (T_s) using Markov/ Markov Single (*M/M/1)* queue model. After which, a Six VLAN model was implemented representing an *MM/6* model. With the *MM/6* model, the evaluation of network properties in comparison to that of a single VLAN is carried out. The evaluation is done analytically and the results therefrom, is validated with simulated results using packet tracer network tool and MATLAB. The result showed that; implementation of VLANs in a network with *M/M/1* server, T_s= 1.412sec, was above 70.6% and W_q=3.391 as compared to T_s=0.235 sec, = below 11.8% and W_q=0.0314 sec for *MM/c* where c= (6) number of VLANs. The result shows that VLANs break a single Broadcast domain into multiple smaller broadcast domains, this in turn increases the network performance such as mean service time, waiting time and reduces network utilization. Users Priority, Access control, and other security policies can be implemented at the Data Link layer using multiple VLANs.
Keyword- *VLANs, Congestion Control, Broadcast Domain, Collision Domain.*

1.0 INTRODUCTION

In any computing environment that supports processes, there must be some mechanism for resource allocation among competing processes, as well as the enforcement of access control policies based on the privileges assigned to that process compared to the requirements of the resources. In a traditional time-sharing operating system, these policies are enforced by the kernel, such as when the application program makes a system call. In the networking context, firewalls play a similar role in policy enforcement for a session and/or individual datagram attempting to cross the boundary separating the "inside" and "outside" worlds [1]. The individual hosts often view the network as an untrustworthy resource. Hence the operating system has the primary responsibility of managing network resources, such as the configuration of the network interface to detect and block unauthorized remote access, while protecting the integrity of its network traffic via encryption (e.g. IPsec, SSL, and VPN) or other means. recently researcher have proposed a concepts that model the fundamental design intent of a network administrators actions and capture the ultimate network-wide performance, security, and manageability and resilience objectives of the designer. There is no doubt that the progress toward the design of network-wide abstraction in certain domains, surprisingly not very much attention is being paid on the management of enterprise and campus networks. Despite their critical importance, and their striking differences and diversity compared to carrier networks, there is little systematic understanding of this network in the community.

Large networks of any type are plagued by surges of traffic, which lead to significantly degraded network performance as well as downtime [1, 2]. These surges of traffic are frequently due to virus outbreaks, poor network management, and misuse of network resources by the network users among other factors. A technique to easily and reliably control access to network resources for effective management would be of great value to many organizations. There had been several approaches to address these problems. Such include implementing of VLAN for service-based multi-netted Asymmetric virtual LAN [3], design and implementation of Application-based secured VLAN [1] and VLAN-based Quality of Service (QoS) control in mobile networks [4, 10].

This work considers an instance where the server Operating System (OS) alone can enforce the desired resources allocation and access control policies by braking single broadcast domain into smaller domains carrying different traffic and changes the scenario to have complete control over all the nodes within a network through switches at the edge of the network rather than depending on the server OS. Policy scheme and access control can be implemented in the host networking hardware (like switches), without making any changes to the hosts (nodes), this will be achieved using the standard techniques specified in VLAN 802.1q and VLAN Identification (VID). In IEEE 802 standard process a mechanism developed to allow multiple switch networks and to transparently share the same physical network link without compromising data integrity between the networks, [5]. IEEE 802.1q also became the name of the encapsulation protocol used to implement this VLAN mechanism over Ethernet networks. Due to the configuration parameter used by Cisco devices to enable 802.1q, it is also commonly referred to as dot1q.

In [5] IEEE 802.1Q specification enable layer-2 switches to prioritize traffic and perform dynamic multicast filtering. The specification works at the Media Access Control (MAC) framing layer. The 802.1q standard stops the proliferation of multicast traffic over the data-link layer. VLAN identifier (VID) is contained within each Ethernet frame of an Ethernet VLAN. This makes it possible for switches to separate traffic based on VID, hence creating different VLAN.

II. Virtual Local Area Network

The first industry conference devoted entirely to virtual local area networks (VLANs) was held in Santa Clara, CA. nearly 350 attendees discussed all the possible definitions of what a VLAN is or what a VLAN should be and about vendor products and strategies, user experience with VLAN implementation [3]. One way to understand the essence and nature of implementing VLAN is to analyses some definitions accredited to it. The Virtual Local Area Network (VLAN) has been defined by many researchers and network developers as a logical grouping of network users and resources connected to administratively defined ports on a switch [3]. Also a very basic definition of the term VLAN is based on the meaning of Broadcast Domain. However, according to [4-6], defining VLAN precisely what VLANs are has become a contentious issue. Yet, most people would agrees that VLAN can be seen as a grouping of end-stations, perhaps on several physical LAN segments, that are not determine by their physical location and can communicate as if they were on a common LAN.

Furthermore, issues such as the extent to which end-stations are not constrained by physical location, the way VLAN membership is defined, the relationship between VLANs and routing have been left up to each vendor. To a certain extent these are tactical issues, but how they are resolved has important strategic implications.

In the same vein, a VLAN is defined as a logical grouping of end stations such that all end stations in the VLAN appear to be on the same physical segment even though they may be geographically separated [4]. Most definitions of VLANs by different researchers, network equipment manufacturing companies and authors build up their definition(s) by considering VLAN to be logical grouping or separation of the broadcast domain. Thus, from these definitions, a generalized meaning of VLAN could be formulated as A VLAN is a logical grouping of end stations with each group having a separate broadcast domain with inter-communication ability among different groups.

4. Collision versus Broadcast Domain

By default, switches break up collision domain and routers break up broadcast domains. Breaking up broadcast domains in pure switch network could be achieved by creating Virtual LAN [6]. When a VLANs is created, smaller broadcast domain are created within a layer 2 switch inter-networked by assigning different ports on the switch to different sub networks. A broadcast domain is everywhere a data-link level broadcast frame would propagate to. A router demarcate this area, which signal the end of a layer-2 network; to go further requires support at a higher layer, such as layer-3 (e.g. IP) to route the packets through the inter-network [2]. So, looking at the network layout in Fig. 1 we can see that there are two broadcast-domains, demarcated by a router.

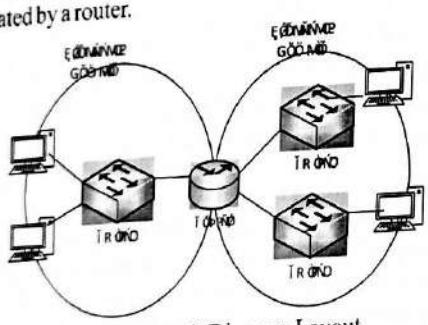

Fig. 1. Network Diagram Layout

As shown in Fig. 2. VLAN provides the ability to segregate a switch into separate broadcast-domains. This means that in order to get across between the different LANs, a router is not a must [8]. In the olden days, such a configuration would be more likely to be called a "router on a stick" Today however, a high-speed router is embedded as part of the switch; this switch is then referred to as a layer-3 switch. While a collision domain is a physical network segment where data packets can "collide" with one another for being sent on a shared medium, in particular in the Ethernet networking protocol. A network collision is a scenario wherein one particular device sends a packet on a network segment to pay attention to it. Meanwhile, other device does the same, and the two competing packets are discarded and resent one at a time. This becomes a source of in the efficiency network.

If a group of Ethernet or Fast Ethernet devices in a Carrier Sense Multiple Access (CSMA) LAN are connected by repeaters they will compete for access on the network. This is typically found in a hub network where each host segment connects to a hub that representing one collision and broadcast domain respectively. In this environment, one device transmit at any time, and the other devices within the domain listens to the network in order to avoid data collisions.

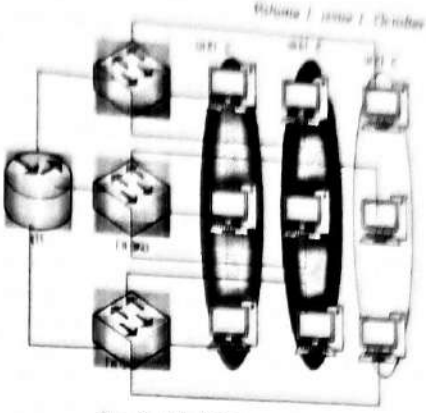

Fig. 2. VLAN Segmentation

These Collisions decrease network efficiency, on the contrary, VLANs segments collision domain thereby allowing many hosts within Ethernet network to transmit without collision. Both computers that attempt to transmit must back off, wait for a random period of time, which is generated independently by each computer, and then retransmit [7]. This is made possible through VLANs Identification. VLANs are identified by a 12-bit number (i.e. 4096 different VLAN IDs; in the case of multiple VLANs assignment to a port, trucking must be used, which implies that the frames are tagged with their VLAN identifier so that the neighborhood device (typically a switch or a router) can know which network it belongs to [13, 14].

B. VLAN Architectures

Due to the trends toward server centralization, enterprise-wide E-mail, and collective applications, various network resources will need to be made available to users regardless of their VLAN membership. Ideally, this access should be provided without most user traffic having to transverse a router [3]. Organizations that implement VLANs recognize the need for certain logical end-stations (for example, centralized servers) to communicate with multiple VLANs regularly, either through overlapping VLANs (in which network-attached end-stations simultaneously belong to more than one VLAN) or via integrated routing that can process inter-VLAN packets at wire speed. From a strategic standpoint, these organizations have two ways to deploy VLANs; a "service-based VLAN implementation or an infrastructure-based" VLAN implementation as shown in figure 3 [8-10]. The choice of approach will have a substantial impact on the overall network architecture, and may even affect the management structure and business model of the organization. A serviced-based approach to VLAN implementation looks, not at organizational or functional groups, but at individual user access to servers and applications. In terms of infrastructure-based, Approach to VLANs is based on the functional group that is, the department, workgroups, sections, etc. that make up the organization.

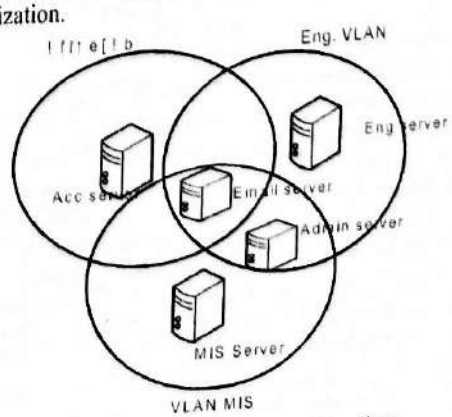

Fig. 3. Infrastructure VLAN Paradigm

Furthermore, issues such as the extent to which end-stations are not constrained by physical location, the way VLAN membership is defined, the relationship between VLANs and routing have been left up to each vendor. To a certain extent these are tactical issues, but how they are resolved has important strategic implications.

Each functional group, such as Accounting Department, Management and Information System (MIS), and Engineering, are assigned a uniquely defined VLAN. Based on the 80/20 rule [11], the majority of network traffic is assumed to be within these functional groups, and thus within each VLAN. In this model, VLAN overlap occurs at network resources that must be shared by multiple workgroups.

III. Materials and Method

In this section, a comparative performance analysis of a single VLAN and the proposed Six VLANs model is carried out using M/M/c queuing theory for c= 1 and c = 6. The existing network is assumed to be a single queue network that is simulated using (Cisco packet tracer 6.1) to obtain the true behavior of the network. The section later gives the highlights for new network design and procedure for VLAN implementation.

A. VLANs Models

Analysis of Single VLAN Model

The network performance measures of interest are *network delay, network utilization and service time* for the network users. We first conduct an analysis of the existing network to estimate its performance. The entire network with a single VLAN conforms to an *M/M/C queuing model*; this is because the entire network forms a single broadcast domain (assumed to be the queue). Where C represents the number server or sub-processor in a switch. Assume a random request from a network user from router which is the sole link to the internet, the request follow a **Poisson distribution** which state that, the probability that there *k* arrival in time *t* seconds is given by [15 - 17];

$$p_k = \frac{e^{-\lambda t}}{k}(\lambda t)^k \qquad (1)$$

Where λ *is the average arrival per sec.* for k_0, (k = number of arrival) the above probability reduces to $e^{-\lambda t}$ Thus the probability that there are no more arrivals in time t =1- (probability that there is no 1 arrival)

$$p_o = 1 - e^{-\lambda t} \qquad (2)$$

By random service, it imply that the time to service an arrival is given by the exponential distribution function [13], this is, T_s(service time<t) $= 1 - e^{-\left(\frac{\lambda}{T_s}\right)}$ (3)

Where T_s = service time.

The queue size for the network users is given by $p_k = p_o(\lambda T_s)^k$ (4)

Where P_k is the mean service time and P_o is the probability that the queue is empty, we can determine P_o by simplifying the (4) for P_k and the find the sum of P_k, for 0,1,2 ..... ∞, must be 1, so

$$\sum_{k=0}^{\infty} p_k \sum_{k=0}^{\infty} p_o(\lambda T_s)^k = 1 \qquad (5)$$

Or

$$p_k = (1-\lambda T_s)(\lambda T_s)^k = (1-\rho)\rho^k \qquad (6)$$

Where ρ is the network utilization.

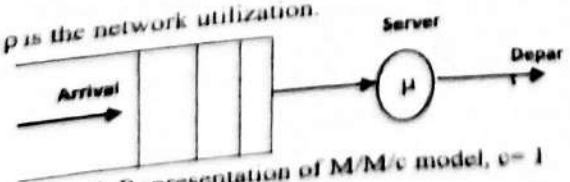

Fig 4 Representation of M/M/c model, c= 1

From the above λTs is assumed to be less than 1. According to Latte's formula, the mean queue size in a network is given by

$$p_k = \sum_{k=1}^{\infty} k p_k \frac{\rho}{1-\rho} \qquad (7)$$

Equation (7) is used to determine the behavior of a Single VLAN network.

- Six VLANs Model

In the six VLANs, an analytical model for such VLANs is proposed here. The M/M/C queuing system can similarly be modeled as in the single VLAN case, except that the number of servers is greater than one bus, that is, has a maximum of $c = 6$ buses. Figure 5, is an M/M/c queue model with c representing server or processors in a single switch. c = 6. The network utilization ρ is given as

$$\rho = \frac{\lambda}{\mu} = \frac{\lambda}{\min\ (\mu_c)} < 1$$

For c=1.....6

Where λ = average arrival rate of frames

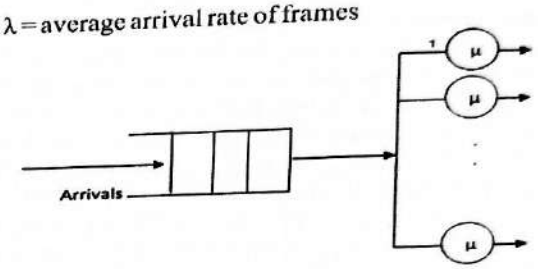

Fig. 5. ***MM/c server Model***

The model above is an M/M/c queue with c representing server or processors in a single switch. c = 6. The network utilization ρ is given as

$$\rho = \frac{\lambda}{\mu} = \frac{\lambda}{\min\ (\mu_c)} < 1$$

For c=1.....6

Where λ = average arrival rate of frames

Mean processing time of $VLAN \Rightarrow 1 = \frac{1}{\mu_1}$, $VLANs \Rightarrow 2 = \frac{1}{\mu 2}$, $VLANs \Rightarrow 6 = \frac{1}{\mu_6}$

IV. Result

The result of standard formulas derived above (queuing theory formulas) for analyzing the network performance provides an explicit way of analyzing the network properties. Similarly, the Cisco packet tracer simulator offers the test bed for modeling and evaluating the newly designed network. The results of the analysis and the properties of the modeled network are presented in this section.

A. Analytical Result of the Network Dissection

Following the earlier assumptions of an M/M/c system for the entire network model, the modeled network with six VLANs has been segmented into six broadcast domains, each of the domain-independent of the other for their intercommunication. Thus, the network delay for each domain is calculated using the same M/M/c, where c = 6. Assuming equal distribution of the messages being sent to the network by the users, the length of the messages per VLAN will now be equal to one-sixth of the mean message length into the network. Thus the network arrival rate within the network is (rate broadcast by network users) = 0.5Mps as given by the internet service provider (ISP).

That is, λ = 0.5Mbps

B. Analytical Result for M/M/c for c = 1

Average link speed = 85Mbps (Ethernet 802.3 are designed with link speed 10/100Mbps. But 85Mbps is assume to take care of the loss and cable properties). Average message length broadcast within the network = 120Mb (Assumed). From (7), the network characteristics for a single VLAN and that of the Six VLAN

model were generated as shown in Table 1.

Table 1. Network Characteristics

No of Segment	Network Performance	$\bar{n}$	ρ	w_s
1	M/M/1	1.412s	70.6%	3.391 s
2	M/M/2	0.706 s	35.5%	0.385 s
3	M/M/3	0.471 s	23.5 %	0.173 s
4	M/M/4	0.353 s	17.6%	0.095 s
5	M/M/5	0.282 s	14.1	0.055 s
6	M/M/6	0.235 s	11.8%	0.0314 s

From the above analysis, it is glaring that the mean service time T_s for the networking users and the waiting time w_s have reduced arithmetically as the numbers of VLANs increase, while network utilization also reduced as VLANs increases as shown in table 1 and Fig. 6. Thus, more broadcast can be accommodated without saturation.

V. Discussion of Result

The entire network was assumed to be a typical M/M/c model. This was because all the users within the network tend to compete or share the network resources with no segmentation or preference for any user within the network. Thus, every user possesses an equal probability to access the network facilities. The result obtained shows that *the network utilization was above 70.6%* which implies that any upsurge in the number of users or number of requests within the network, particularly during peak hours cause network congestion.

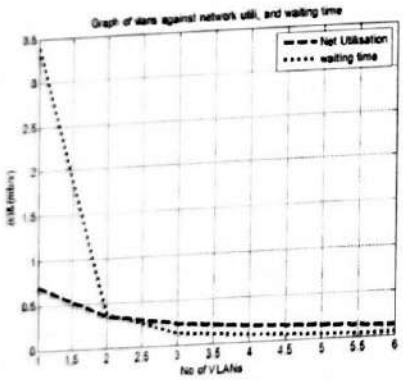

Fig. 6. *Graph of Network Utilization, Waiting Time against VLANs*

This circumstance reduces the network throughput to almost zero, which means no user enjoys the service of the network at that particular period. Comparing it to M/M/1 and M/M/6 VLANs models, *the network average utilization reduces to 11.8%*. At this value, the tendency of congestion is highly reduced even at peak hours. Similarly, *the mean service time and waiting time* is also reduced from 1.412 seconds and 3.391 seconds to 0.235 and 0.036 seconds respectively, thereby making the network more robust for all users.

VI. Conclusion

VLANs implementation reduces the migration cost of stations going from one group to another. Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by deploying VLANs. With VLANs, some level of security at layer 2, people belonging to the same group of (VLAN) can send broadcast messages with guaranteed assurance that users in other groups will not receive these message. The analyses have proved that it is possible to configure any VLAN switch as many parallel sub-processors according to the number of used VLANs. Such an idea can be extended to model VLAN switches

dynamically to manage a variable number of VLANs with variable traffics. It has been shown that network utilization can be increased with the minimization of the average number of frames in the buffer. Network congestion can be reduced by minimization of time delay in the buffer. This is because the offered load is equally-distributed on the six servers in the M/M/6 VLANs topology.

References

[1]. Z. Minli, M. Mart, and B. Bala, "Design and implementation of application-Based Secured VLAN" in *proc of 29th Annual international IEEE Conference on local computer Network (LCN' 04)*, pp. 407-408, Nov. 2004.

[2]. G. Prashant, Z. Nan, S. Yu-Wei, and R. Sanjay, "Characterizing VLAN usage in operational network" Aug. 22, 2007 [July 10, 2015].

[3]. M. John and T. Tony, *Do VLANs make sense in your network?*" white paper, (1996),

[4]. White Paper: Authenticated VLANs, Secured Network Access at Layer 2, Nov. 2002[Dec. 10, 2015]

[5]. A. J. Dhurghan, "Improving LAN perf romance based on IEEE 802.1Q VLAN switching technique ", *Journal of University of Babylon, Engineering Science*, Vol. 26, No. 1, pp. 287, 2018.

[6]. A. I. Isaika and O. M. Akeem, "Enhancement of network performance of an enterprises network with VLAN", *American Journal of mobile System, Application, and service*, Vol. 1, No. 2, PP 84-86, 2015.

[7]. J. Raff, "Efficiency of four virtual LANs switches with equal processing times", *journal of Mathematics and computer*, Vol. 8, No. 1, Mosul University, pp. 4-10, 2011.

[8]. S. M. Aaron, "Implementation of virtual LAN for Virus containment".9 Dec. 2004 [Feb. 7, 2014].

[9]. H. A. Taha, "*Operations Research an introduction*",7th edition, Pearson Education Inc. 2006 pp.233-236, 246-2512

[10]. Decisys, Inc., "The Virtual LAN security best practices", June 1996 [Oct. 7, 2015]

[11]. L. Todd, "*Cisco certified network associate study guide*", Indianapolis Indiana, Wiley Publishing, Inc., Sixth edition, pp. 555-602, 2007.

[12]. Sasaki, M, Yokota, H, and Akira I., "VLAN based QoS control in Mobile." [Oct. 7, 2015] 2006

[13]. Odom V. and Nottingham H., "*Cisco switching black book*", Arizona: The Coriolis Group. 2001.

[14]. V. Mancuso and L. Monica, "Controlled VLANs switching using VLANs to counteract the Effect of topology changes in Quasi-Static mesh access networks", *Proceeding of the Sixth IEEE International Conference on Computer and Information Technology (CIT'06), IEEE Computer Society*, 2006.

[15]. W. Arbaugh and A. Mishra, "An Initial Security Analysis of the IEEE 802.1X standard". Internet: http://www.cs.umd.edu/ waa/1x.pdf, 6 Feb. 2002. [Sep.10, 2016]

[16]. B. Mohammed Al-Bazzaz, "*Analysis, design and enhancement of Switches for virtual Computer networks*", Ph.D thesis, Electrical Eng. Dept., Mosul University, Iraq. 2007.

[17]. A. Vijay, "*Design and Analysis of computer communications Networks*", New York: McGraw Hill Inc., pp. 271-275, 1987.

[18]. I. Adan and J. Resing, "Queuing Theory", Netherlands: Eindhoven University Technology, pp.180, 2001.

[19]. K. E. Medhi J., "Queuing System: general concept", *Stochastic Models in Queueing Theory*, 2nd edition, New York: Academic publishers Inc., pp. 53-67, 2007