IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 6, Ver. II (Nov.-Dec .2016), PP 67-80
www.iosrjournals.org

Simulation of Virtual LANs (VLANs) Using OPNET

Sarah Ali Abdullah
University of Information Technology and Communications, Baghdad, Iraq

Abstract: *Virtual LANs (VLANs) offer a method of dividing one physical network into multiple broadcast domains. This paper simulates a VLAN using OPNET. Different scenarios are designed and simulated, where a step by step procedure using the workspace of OPNET is given. The first scenario network is tested for the cases when the network composed of (10 PCs & 5 servers) and (24 PCs & 6 servers). This scenario is given for the purpose of comparison increased network size with no VLAN configuration. The second scenario is a 3_vlan configuration for the same network in the first scenario. The third scenario is a 6_vlan configuring. These scenarios are given for the purpose of comparison with and without VLAN, while the last scenario is given to explain VLAN interconnection which consists of one Cisco router, 4 PCs and 3servers. For VLAN inter communication, a Layer-3 router is required (e.g. Cisco 4700 router). The simulation is carried out for a total simulation time of 1 hour. The results obtained show a large reduction in traffic carried by the switch with more secure and efficient bandwidth utilization.*

Keywords: *LAN; VLAN; Switch; Router; traffic*

I. Introduction

Virtual LANs (VLANs) have recently developed into an integral feature of switched LAN solutions from every major LAN equipment vendor. Although end-user enthusiasm for VLAN implementation has yet to take off, most organizations have begun to look for vendors that have a well-articulated VLAN strategy, as well as VLAN functionality built into products today. One of the reasons for the attention placed on VLAN functionality now is the rapid deployment of LAN switching that began in 1994/1995 [1].

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2) [2]. This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through *tagging*, so that a single interconnect (*trunk*) may be used to transport data for various VLANs. Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design.

A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs. Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain [3].

This paper discusses these and other issues in greater detail, and attempts to determine the strategic implications that VLANs, pose for enterprise networks.

II. LAN & VLAN With Network Protocols And Design

To understand VLANs, it is first necessary to have an understanding of LANs. A Local Area Network (LAN) can generally be defined as a broadcast domain. Hubs, bridges or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Communications with devices on other LAN segments requires the use of a router.

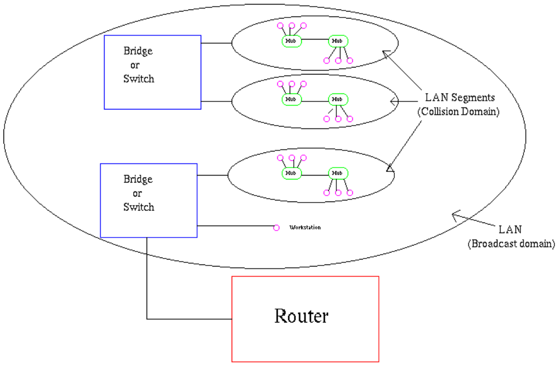
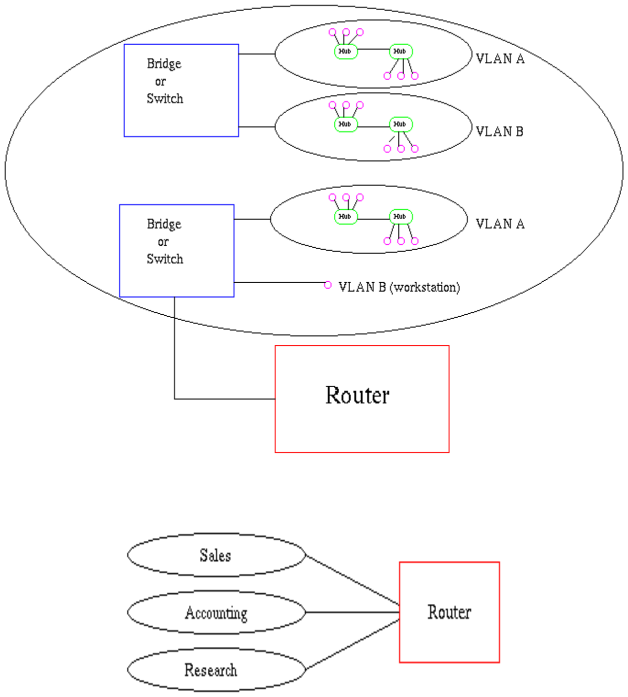


Figure 1: Physical view of a LAN.

Virtual LANs (VLANs) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment. Switches using VLANs create the same division of the network into separate broadcast domains but do not have the latency problems of a router. Switches are also a more cost effective solution [3].



Physical View

Logical View

Figure 2: Physical and logical view of a VLAN.

The protocol most commonly used today to configure VLANs is IEEE 802.1Q. The IEEE committee defined this method of multiplexing VLANs in an effort to provide multivendor VLAN support. Prior to the introduction of the 802.1Q standard, several proprietary protocols existed, such as Cisco's ISL (Inter-Switch Link) and 3Com's VLT (Virtual LAN Trunk). Cisco also implemented VLANs over FDDI by carrying VLAN information in an IEEE 802.10 frame header, contrary to the purpose of the IEEE 802.10 standard.

Both ISL and IEEE 802.1Q tagging is performed "explicit tagging" - the frame itself is tagged with VLAN information. ISL uses an external tagging process that does not modify the existing Ethernet frame, while 802.1Q uses a frame-internal field for tagging, and therefore does modify the Ethernet frame. This internal tagging is what allows IEEE 802.1Q to work on both access and trunk links: frames are standard Ethernet, and so can be handled by commodity hardware.

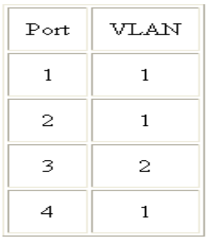
Under IEEE 802.1Q, the maximum number of VLANs on a given Ethernet network is 4,094 (the 4,096 provided for by the 12-bit VID field minus reserved values 0x000 and 0xFFF). This does not impose the same limit on the number of IP subnets in such a network, since a single VLAN can contain multiple IP subnets. The VLAN limit is expanded to 16 million with Shortest Path Bridging [4].

Early network designers often configured VLANs with the aim of reducing the size of the collision domain in a large single Ethernet segment and thus improving performance. When Ethernet switches made this a non-issue (because each switch port is a collision domain), attention turned to reducing the size of the broadcast domain at the MAC layer. A VLAN can also serve to restrict access to network resources without regard to physical topology of the network, although the strength of this method remains debatable as VLAN hopping [4] is a means of bypassing such security measures. VLAN hopping can be mitigated with proper switchport configuration.

III. VLAN TYPES, PROS and CONS

3.1 Type [5]:

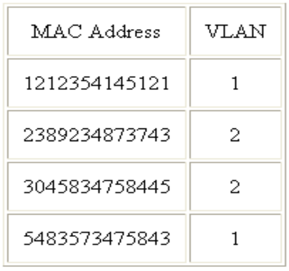
1. **VLAN Membership by Port number:** a VLAN can be defined based on the ports that belong to the VLAN. For example, in a bridge with four ports, ports 1, 2, and 4 belong to VLAN 1 and port 3 belongs to VLAN 2, see figure 3.



Port	VLAN
1	1
2	1
3	2
4	1

Figure 3: Assignment of ports to different VLAN's.

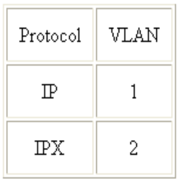
2. **Layer 2 VLAN Membership by MAC Address:** a VLAN is based on the MAC address of the workstation. The switch tracks the MAC addresses which belong to each VLAN, see figure 4.



MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

Figure 4: Assignment of MAC addresses to different VLAN's.

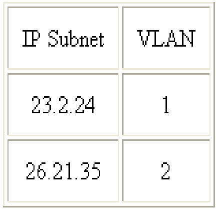
3. **Layer 2 VLAN Membership by Protocol Type:** a VLAN membership for Layer 2 VLAN's can also be based on the protocol type field found in the Layer 2 header, see figure 5.



Protocol	VLAN
IP	1
IPX	2

Figure 5: Assignment of protocols to different VLAN's.

4) Layer 3 VLAN Membership by IP Subnet Address: Membership is based on the Layer 3 header. The network IP subnet address can be used to classify the VLAN membership, see figure 6.



IP Subnet	VLAN
23.2.24	1
26.21.35	2

Figure 6: Assignment of IP subnet addresses to different VLAN's.

3.2 PROS [6]:

- **Performance:** routers that forward data in software become a bottleneck as LAN data rates increase. Doing away with the routers removes this bottleneck.
- **Formation of virtual workgroups:** Because workstations can be moved from one VLAN to another by changing the configuration of switches, it is relatively easy to put all the people working together on a particular project all into a single VLAN. They can then more easily share files and resources with each other. To be honest, though, virtual workgroups sound like a good idea in theory, but often do not work well in practice. It turns out that users are usually more interested in accessing company-wide resources (file servers, printers, etc.) than files on each other PC.
- **Greater flexibility:** If users move their desks, or just move around the place with their laptops, then, if the VLANs are set up the right way, they can plug their PC in at the new location, and still be within the same VLAN. This is much harder when a network is physically divided up by routers.
- **Ease of partitioning of resources:** If there are servers or other equipment to which the network administrator wishes to limit access, then they can be put off into their own VLAN. Then users in other VLANs can be given access selectively.

3.3 CONS [3]:

- VLANs limit - it is possible to create only 4094 different VLANs for the same network, because of the 12 bit VID identifier. Each VLAN has its own unique ID between 0 and 4096, whereby 0 and 4096 are reserved, thus the switch knows where to route the frame. This should be more than enough for today, in most companies, but could prove as a bottleneck in the future in the same manner IPV4 did.
- Managerial Overhead - when using hard configured VLANs, such as port based or MAC based its require quite a lot of managerial work to manage networks as they evolve and change with time (keeping track of port assignment or MAC assignment per VLANs is time consuming). On the other hand the usage of Subnet based VLANS requires stronger switches which cost more money, and also adds additional switching latency because it is required to decipher the layer 3 header partially.

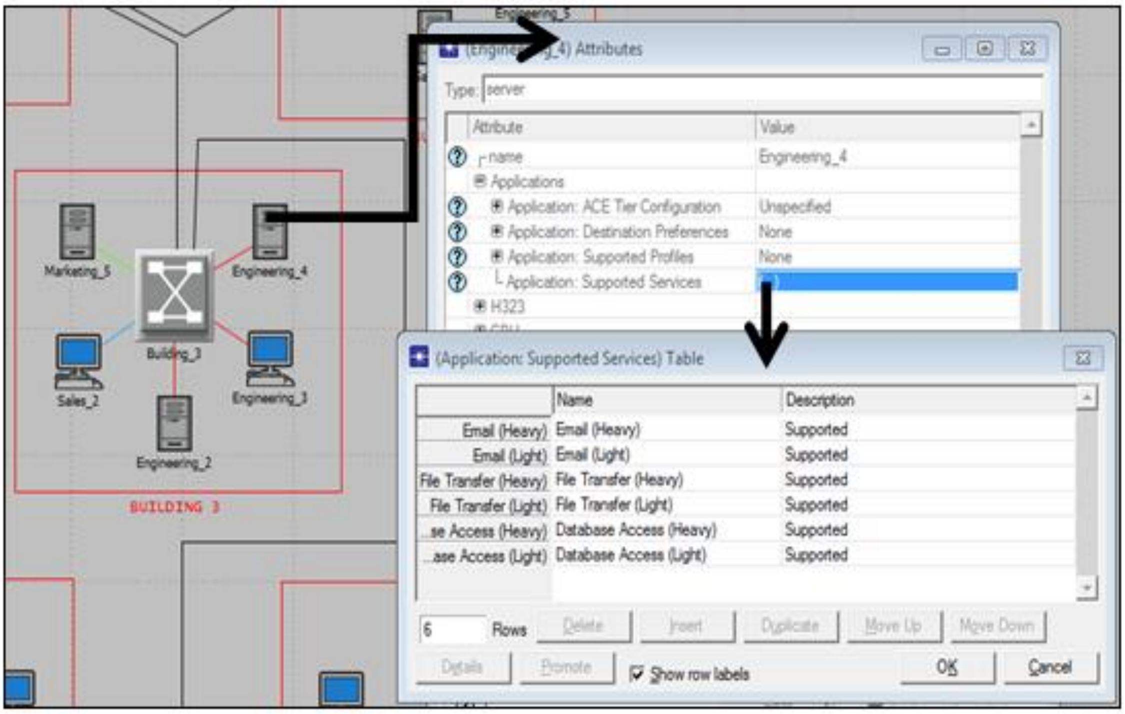
IV. Simulated Model Design

In this paper, the OPNET Modeler 14.5 is used to simulate VLAN with different application over the network. Three scenarios with NO_vlan, 3_vlans, 6_vlans and Inter-VLANs communication were tested and discussed in the following subsection.

4.1 Network Configuration Parameters:

Each object in the VLAN Model (server, node, and application) has a specific set of parameters. In general those parameters can be classified as follows:

- **Application Parameter:** Application Attribute definition is used to specify/choose the required application among the available applications such as FTP, HTTP, Video, Voices, and Print etc.,
- **Profile Parameter:** Profile Attribute definition will be used to create user profiles, these profiles can be specified on different nodes in a network designed to generate the application traffic.
- **Server Parameters:** In each server, supported services are based on the user profiles that may support FTP, HTTP, VoIP, Video, etc..., on the client as shown in figure 7.



(Engineering_4) Attributes

Type: server

Attribute	Value
name	Engineering_4
Applications	
Application: ACE Tier Configuration	Unspecified
Application: Destination Preferences	None
Application: Supported Profiles	None
Application: Supported Services	(...)
H323	

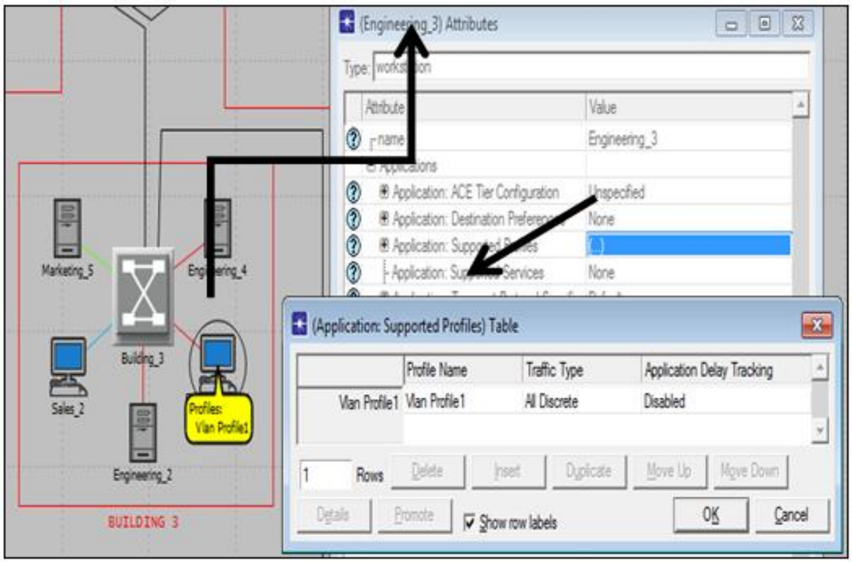
(Application: Supported Services) Table

	Name	Description
Email (Heavy)	Email (Heavy)	Supported
Email (Light)	Email (Light)	Supported
File Transfer (Heavy)	File Transfer (Heavy)	Supported
File Transfer (Light)	File Transfer (Light)	Supported
...se Access (Heavy)	Database Access (Heavy)	Supported
...ase Access (Light)	Database Access (Light)	Supported

6 Rows

Figure 7: Configuration server with different applications

- **Nodes Parameters (PC):** Network parameters are set for all nodes, such as workstations, and PC with client server applications as shown in figure 8.



(Engineering_3) Attributes

Type: workstation

Attribute	Value
name	Engineering_3
Applications	
Application: ACE Tier Configuration	Unspecified
Application: Destination Preferences	None
Application: Supported Profiles	(...)
Application: Supported Services	None

(Application: Supported Profiles) Table

	Profile Name	Traffic Type	Application Delay Tracking
Vlan Profile1	Vlan Profile1	All Discrete	Disabled

1 Rows Delete Insert Duplicate Move Up Move Down

Details Promote ☑ Show row labels OK Cancel

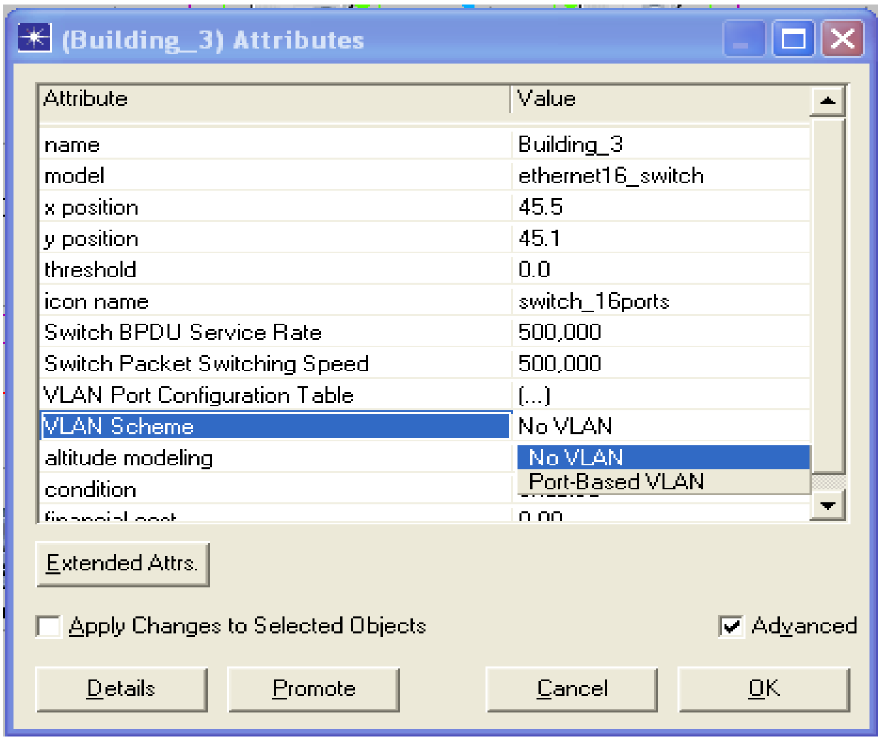
Figure 8: Configuration PC nodes with applications

4.2 Scenarios:

This paper provides three scenarios. The objective of these scenarios is to compare the performance of the VLAN model with different applications.

- **Scenario #1: "NO_vlan"**

This scenario generates network traffic without any separation between departments (classical network). To configure no VLANs, specify "NO_vlan" as the value for the "VLAN scheme" attribute on the switch devices which support VLANs as shown in figure 9. Switch devices, connected to gather by 100baseT links and each port in switch connection with several PC and the server. In the first case three network department is shown in figure 10. The total number of available hosts in this scenario are 12 PCs and 3 servers. Then when increased network departments to six departments with 24 PCs and 6 servers connected as one broadcast domain to increased traffic greater than first case shows the complete network diagram in figure 11.


(Building_3) Attributes

Attribute	Value
name	Building_3
model	ethernet16_switch
x position	45.5
y position	45.1
threshold	0.0
icon name	switch_16ports
Switch BPDU Service Rate	500,000
Switch Packet Switching Speed	500,000
VLAN Port Configuration Table	(...)
VLAN Scheme	No VLAN
altitude modeling	No VLAN Port-Based VLAN
condition	
financial cost	0.00

Extended Attrs.

☐ Apply Changes to Selected Objects ☑ Advanced

Details Promote Cancel OK

Figure 9: VLAN Scheme Options

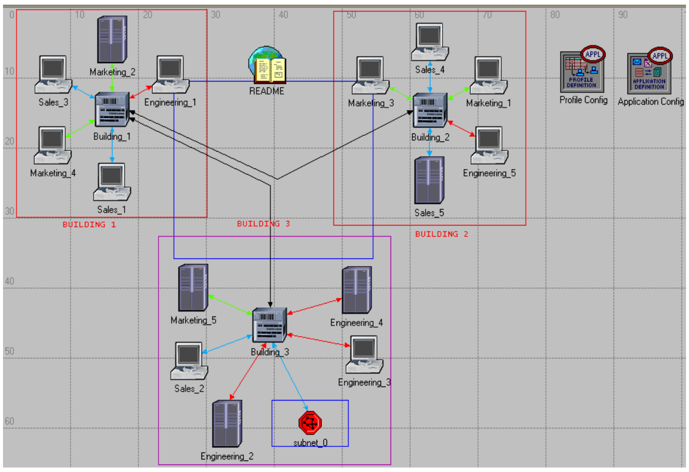


Figure 10: First scenario "No_vlan" with three departments.

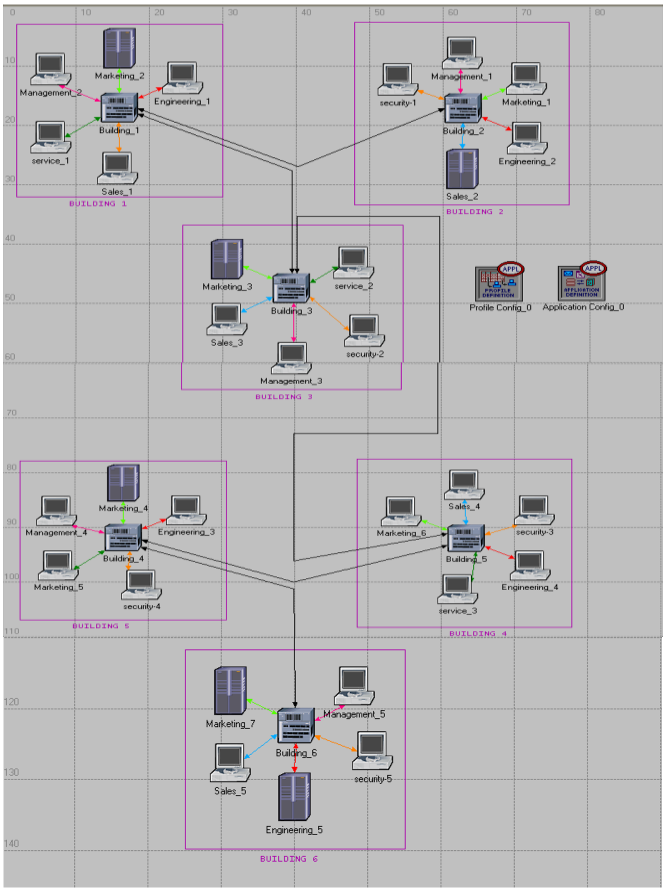
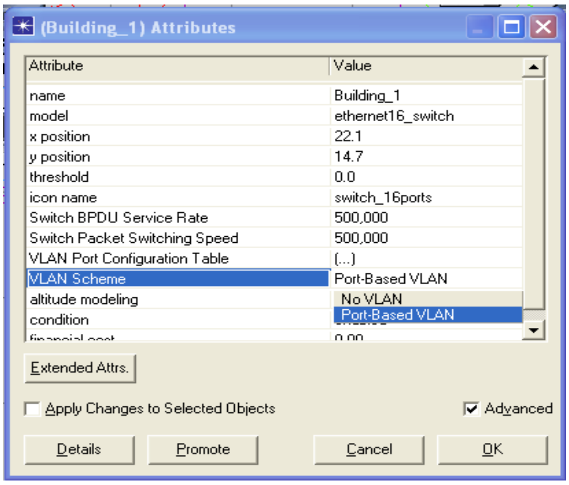


Figure 11: First scenario "No_vlan" with six Departments.

- **Scenario #2:"3_vlans"**

The previous network has been modified and configured in order to generate three VLAN (10, 20, and 30) as shown in figure 15. The procedure configuring VLAN is as follows:

1. Specify "Port-Based VLAN" as the value for the "VLAN scheme" attribute on the switch devices which support VLANs. Then choose Port-Based VLAN as shown in figure 12.

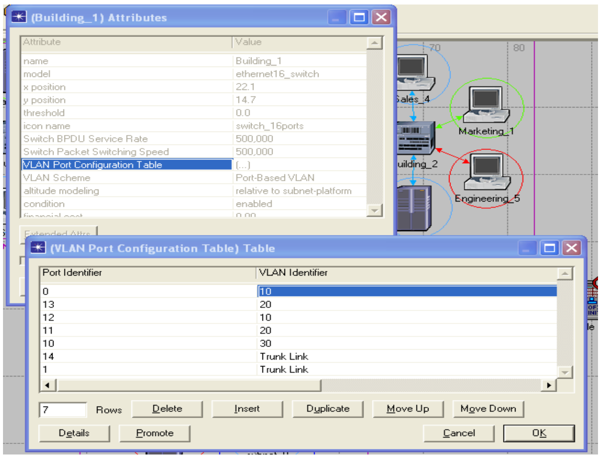


(Building_1) Attributes

Attribute	Value
name	Building_1
model	ethernet16_switch
x position	22.1
y position	14.7
threshold	0.0
icon name	switch_16ports
Switch BPDU Service Rate	500,000
Switch Packet Switching Speed	500,000
VLAN Port Configuration Table	(...)
VLAN Scheme	Port-Based VLAN
altitude modeling	No VLAN Port-Based VLAN
condition	

Figure 12: VLAN Scheme option Port-Based VLAN.

2. Additionally, you can populate the "VLAN Port Configuration Table" to associate VLAN identifiers, such as switch of building _1 allocated port 0 for VLAN10, port 13 to VLAN 20, port 12 to VLAN 10, port 11 to VLAN 20, port 10 to VLAN 30, port 14 to trunk link, and port 1to trunk link to specific ports as shown in figure 13.



(Building_1) Attributes

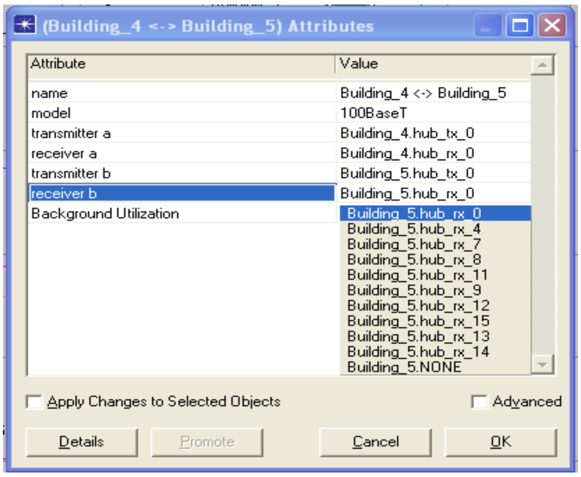
Attribute	Value
name	Building_1
model	ethernet16_switch
x position	22.1
y position	14.7
threshold	0.0
icon name	switch_16ports
Switch BPDU Service Rate	500,000
Switch Packet Switching Speed	500,000
VLAN Port Configuration Table	(...)
VLAN Scheme	Port-Based VLAN
altitude modeling	relative to subnet-platform
condition	enabled

(VLAN Port Configuration Table) Table

Port Identifier	VLAN Identifier
0	10
13	20
12	10
11	20
10	30
14	Trunk Link
1	Trunk Link

Figure 13: VLAN Scheme option Port-Based VLAN

3. Port numbers corresponding to an associated link can be found using the "link interfaces" option from the "Link Attributes (advanced)" dialog box. Then select link interface option into each interface link and identifiers to specific ports as shown in figure 14.



(Building_4 <-> Building_5) Attributes

Attribute	Value
name	Building_4 <-> Building_5
model	100BaseT
transmitter a	Building_4.hub_tx_0
receiver a	Building_4.hub_rx_0
transmitter b	Building_5.hub_tx_0
receiver b	Building_5.hub_rx_0
Background Utilization	Building_5.hub_rx_0 Building_5.hub_rx_4 Building_5.hub_rx_7 Building_5.hub_rx_8 Building_5.hub_rx_11 Building_5.hub_rx_9 Building_5.hub_rx_12 Building_5.hub_rx_15 Building_5.hub_rx_13 Building_5.hub_rx_14 Building_5.NONE

Figure 14: VLAN Scheme option Port-Based VLAN.

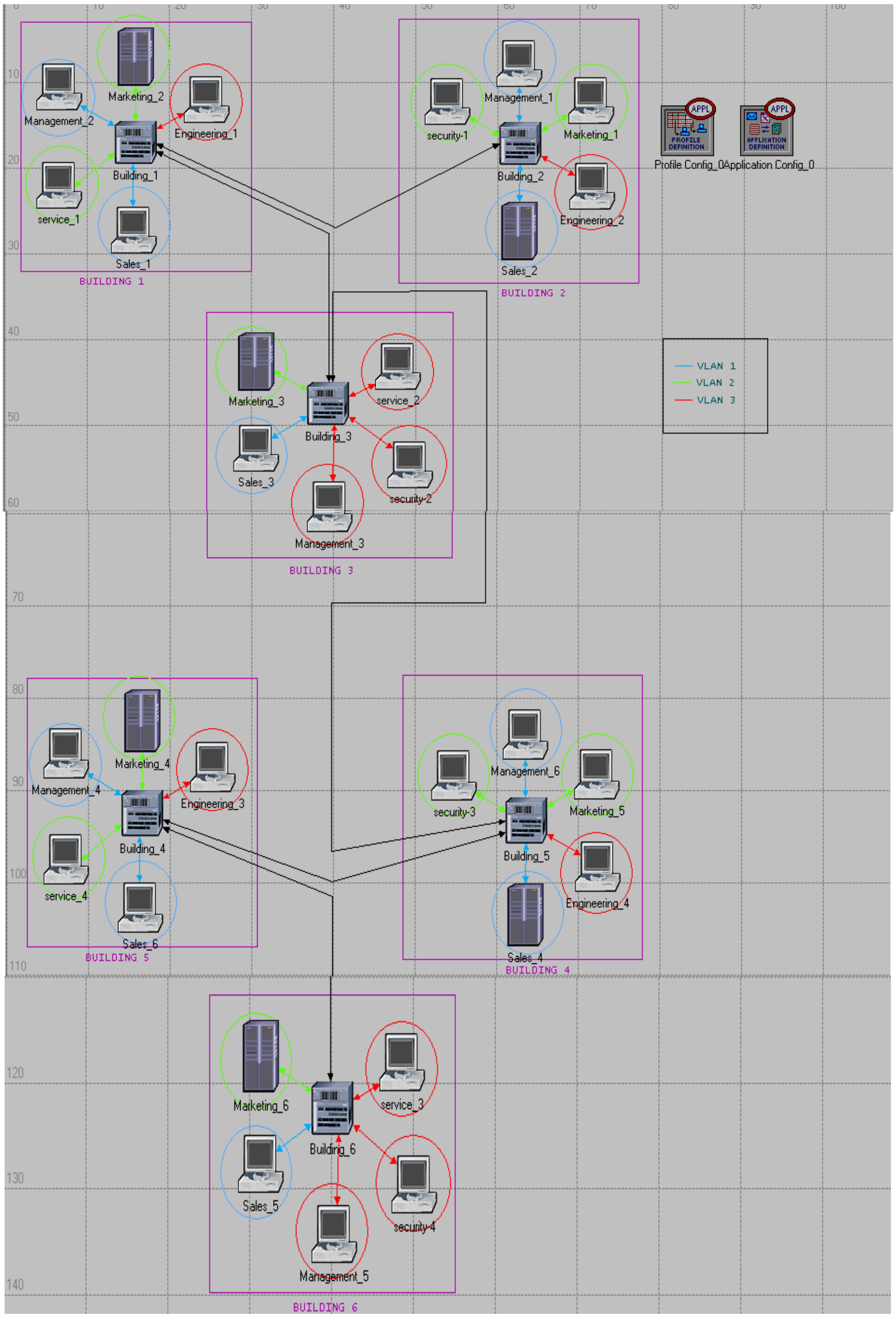


Figure 15: Second scenario "3_vlan" with six departments.

- **Scenario#3: "6_vlan"**

This scenario generated network traffic with VLAN configuration. A network composed of six departments. These departments are logically separated by using a six VLAN for each of them. Divided network into six VLAN (1, 2, 3, 4, 5, and 6) as shown in figure 16. The purpose of this scenario to show what do when increased the network component with increased VLAN.

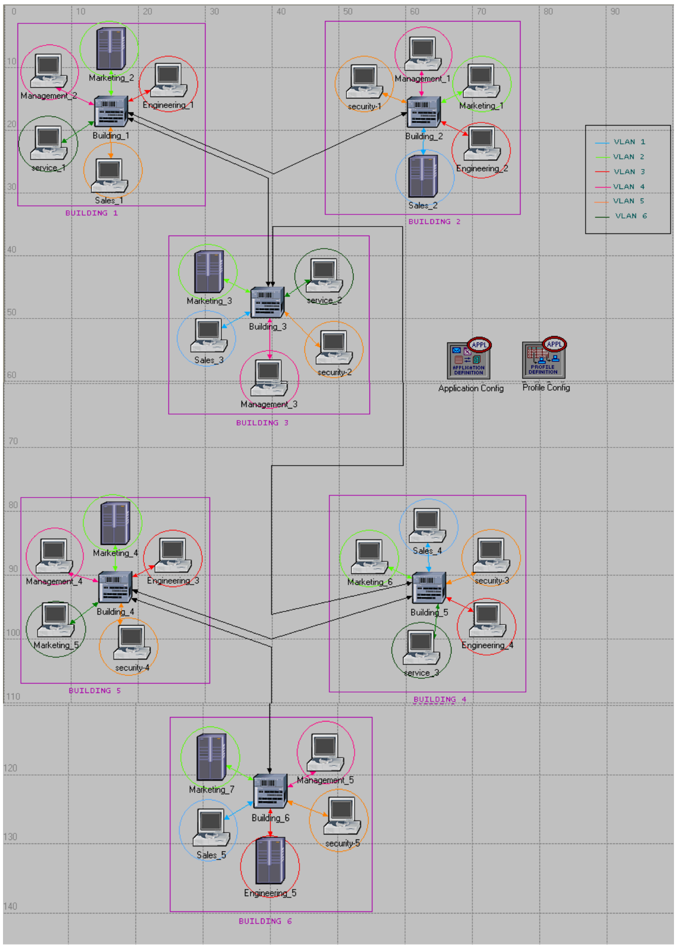


Figure 16: Second scenario "6_vlan" with six departments.

- **Scenario#4: "Inter-VLANs communication"**

In this scenario different VLANs can communicate with each other via a router, because the VLAN information is not carried when going through the IP. If a router is connected to a VLAN-aware bridged-network via an access port with PVID 1 (Default VLAN), then packets arriving from this router will be associated with VLAN 1. Hence, they will be forwarded to any port in the bridged-network along their path to their destinations as long as these ports are also a member of VLAN 1 (please note that VLAN 1 doesn't have to be used for such a configuration, any other valid VID can be used for the same purpose). Complete network diagram as shown in figure 17.

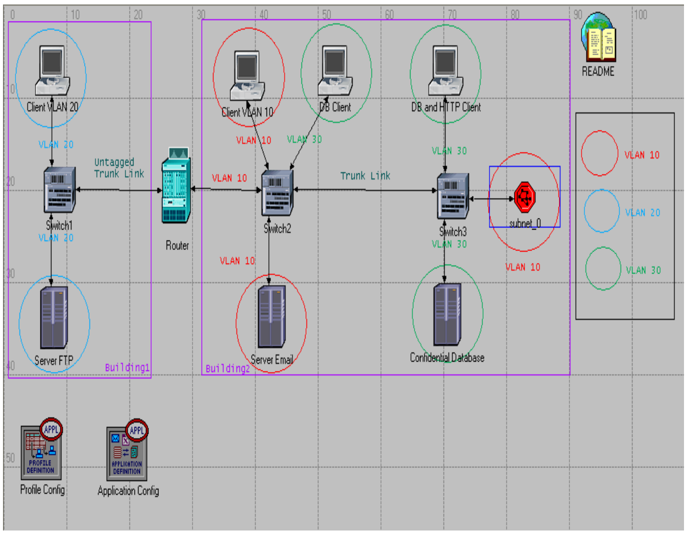


Figure 17: Scenario for "Inter-VLANs communication"

V. Results – Evaluation

This section introduces the results for the scenarios that highlight comparison between with and without VLAN mechanism on the network have different types of traffic which presented in the section 4.2. The results related to these scenarios are presented and analyzed in the following subsections.

Scenario #1: The results obtained from this scenario are more traffic exists in the network without VLANs in both cases three and six departments, since any communication between departments is allowed. The total time simulation scenario measured on duration 1.0 hour.
Figure 18 and figure 19 show objects response time for switch traffic received in (bit/sec) with three and six departments. This statistic is updated only when the packet enters a VLAN for the first time. If the same packet traverses through the same VLAN or trunk links, this statistic is not redundantly updated.

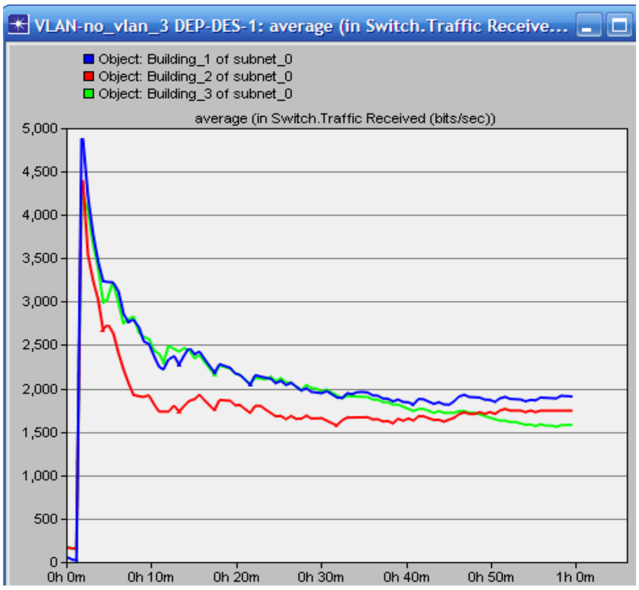


Figure 18: Traffic received in switch (bit/sec) for first scenario "NO_vlan" with three departments.

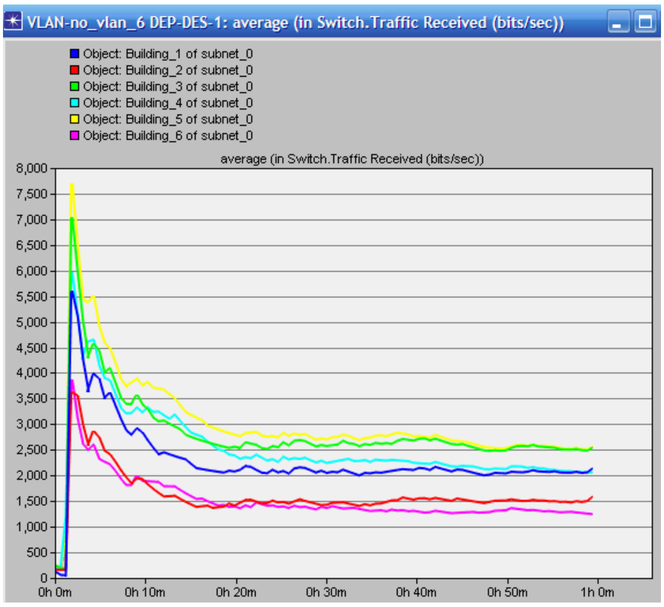


Figure 19: Traffic received in switch (bit/sec) for first scenario "NO_vlan" with six departments.

Scenario #2: The results obtained from this scenario are large reduction in traffic carried by the switch. When using VLANs, it is no more possible to send traffic in other department than one's. It improves the bandwidth utilization, security and the administration by supporting a virtual organization. The total time simulation during this scenario measured on duration 1.0 hour.

Figure 20 shows object response times for switch traffic received in (bit/sec), It is clear from the results that the high decreased traffic value compare the previous result that obtain from without VLAN scenario.

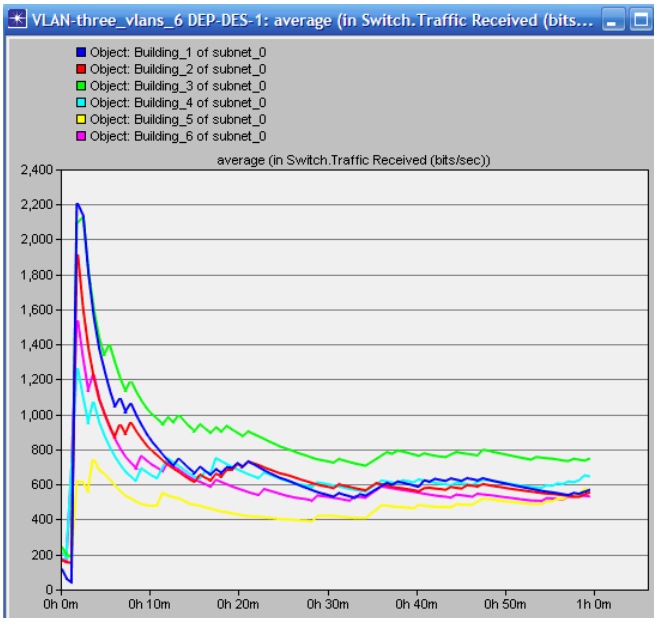


Figure 20: Traffic received in switch (bit/sec) for second scenario "3_vlan" with six departments.

Scenario#3: In this section what is understood from these results is that the average switch value of traffic received in (bit/Sec) is decreased on the network when divided network into multiple VLAN (6_vlan) that shown in figure 21.

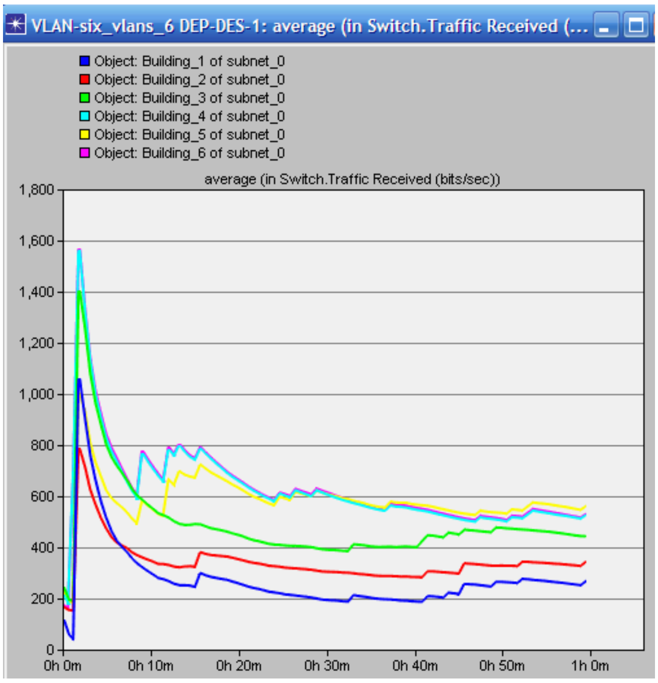


Figure 21: Traffic received in switch (bit/sec) for second scenario "6_vlan" with six departments.

Ethernet delay and traffic forward in (bit/sec) are the next performance metrics used to quantify VLAN mechanism over the network in the scenarios# 1, 2, 3. The results (Global statistics) of three scenarios have been collected and grouped together for the same number of departments as shown in figure 22 and 23.

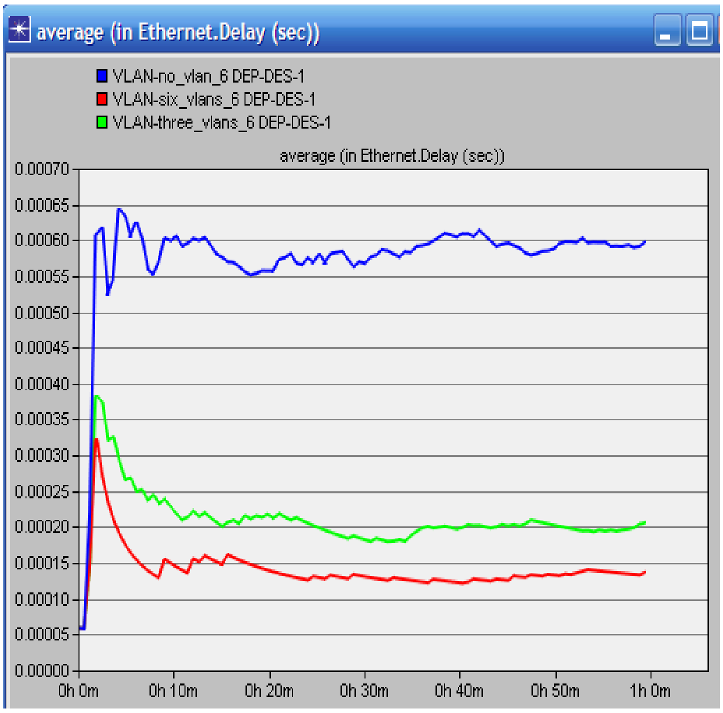


Figure 22: Ethernet Delay (sec).

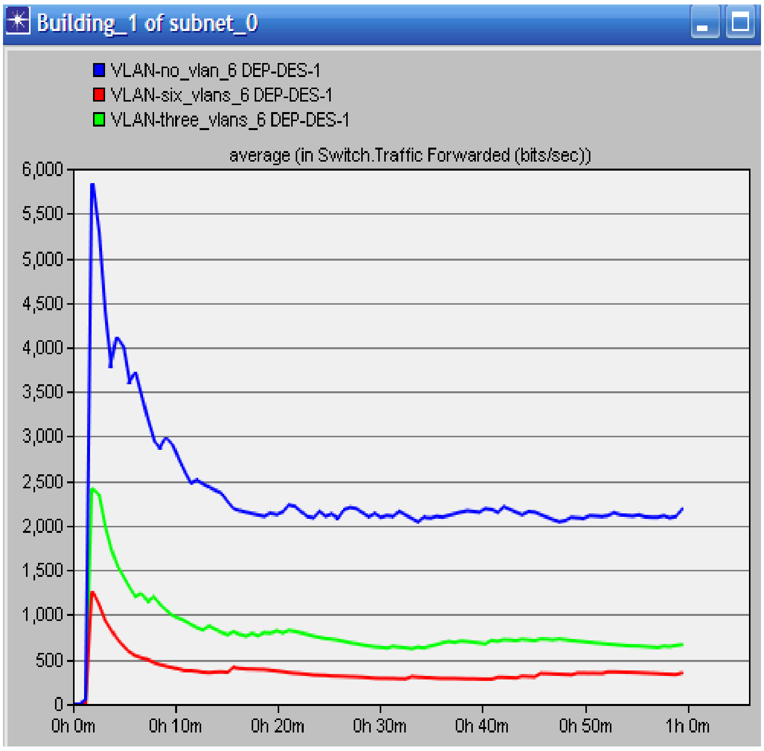


Figure 23: Average switch of building 1 traffic forwarded (bit/sec).

Scenario #4: The results obtained on duration 1.0 hour. "Building1" can get emails from the email server in "Building2" even though the email server doesn't belong to the same VLAN as the client in "Building1", since the connection is established via a router and the ports of these clients support the PVID of the access port to the router figure 24 shows email download for client VLAN 20.

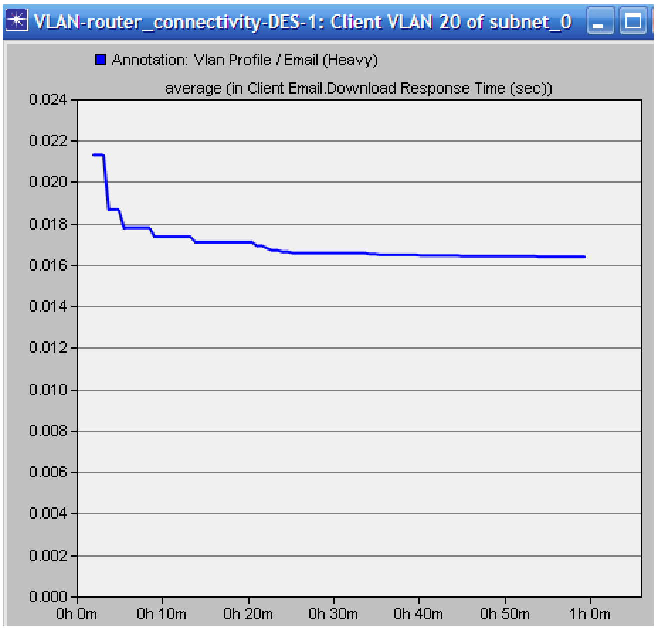


Figure 24: Email downloads response time for client VLAN_20.

However, packets coming from the router in "Building2" are given the VLAN membership 10. It means that clients and servers with VLAN membership 30 in "Building2" can never communicate with stations outside the "Building2" and vice-versa. For instance, the request of the FTP client in "Building2" are dropped by "Switch2" from the FTP server resides in "Building1"that can show in figure 25.

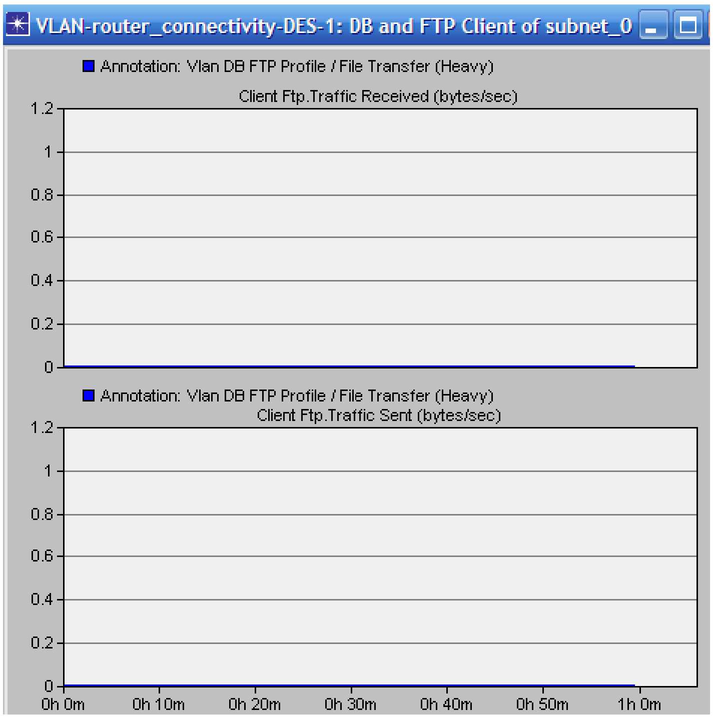


Figure 25: Traffic received and send for FTP client.

In "Building2", stations with VLAN membership 10 or 20 will never be able to connect to the server "Confidential Database", because the server belongs to the VLAN 30. That's why "Switch3" is dropping the VLAN 10 packets it receives, as shown in figure 26, which convey connection requests to the database server from clients that belong to VLAN 10 or 20. Traffic dropped is the final metrics used in the quantification system performance over VLANs communicated with each other via a router.

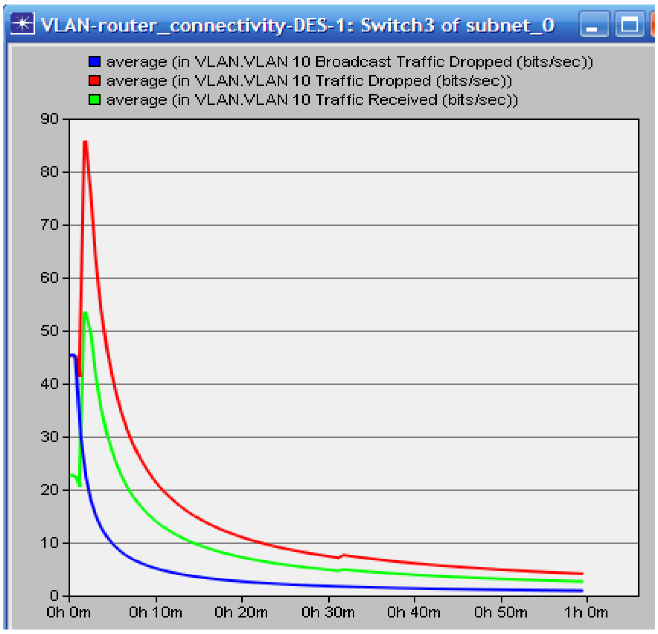


Figure 26: Traffic dropped and received for switch3.

VI. Conclusion

When the number of PCs increased in a local area network, the need for configuring VLANs becomes necessary in order to reduce the traffic handled by the main switch. As it had been shown in the analysis performed in this paper, increasing the number of VLANs reduce the traffic rapidly, can also control the size and composition of the broadcast domain by controlling the size and composition of a VLAN.

This is due to the fact that VLANs creates many broadcast domains. The other conclusion is related to security. VLAN groups, many PCs into multiples LANs as if they are physically separated. The reduction in traffic using 3_vlans is around 50% with NO-vlan and increase reduced when moving to 6_vlans 60% with NO-VLAN. This means that a gain of an extra can be added to overall network. Finally, the results also show that, a device on a VLAN is restricted to only communicate with devices that are on their own VLAN. Just as a router provides connectivity between different VLAN segments.

Reference

[1]. David Passmore, John Freeman, "The Virtual LAN Technology Report", March 7, 1997 http://www.3com.com /nsc/200374.html.

[2]. Patricia Thaler, Norman Finn, Don Fedyk, Glenn Parsons, Eric Gray, "IEEE 802.1Q", March 10, 2013.

[3]. Komal Sharma, Meenu Yadav, Megha Pundir, Isha Malhotra, and Jaskaran Singh," VLAN & Its Implementation over ATM by using IP: a communication ", Discovery Engineering, Volume 2, Number 8, November 2013.

[4]. Rik Farrow, "VLAN INSECURITY", on 2014-04-21http:// rikfarrow.com/Network/net0103.html.

[5]. Mathias Hein, David Griffiths, Orna Berry, “Switching Technology in the Local Network: From LAN to Switched LAN to Virtual LAN”, February 1997.

[6]. AlliedWare Plus™ OS, "Overview of |VLANs (Virtual LANs)", 2008 Allied T ele sis, Inc.