Improving LAN Performance Based on IEEE802.1Q VLAN Switching Techniques

Dhurgham Abdulridha Jawad AL-Khaffaf
Dept. of Communication Techniques Engineering, Engineering Technical College/Najaf, Al-Furat Al-Awsat Technical University.
1337775@brunel.ac.uk

Abstract

VLAN is a set of users in different isolated logical LANs or broadcasting domains, they are communicated as a same LAN i.e. same broadcasting domain. Ethernet protocol is very popular over networks because it has a simple of implementation and ease of configuration. However, the support of Quality of Service (QoS) has become an essential merit of Ethernet network. In this context, the problems of large network and data transport delay have been regained significant importance. Alleviating the end to end delay by using the VLAN technology to enhance the network performance. In this paper, we analyze and evaluate the performance of LAN and VLAN networks in different scenarios. Measuring key performance indicators such as traffic sent, traffic received, average delay and throughput. The simulation was carried out by employing OPNET 17.5 Student Version. Two different scenarios are presented to observe the performance of LAN and VLAN networks. The simulation results illustrated that there is more existing traffic without VLAN technology. Hence, VLANs prohibit the access to the network resources of other departments. Also, VLAN has half average queuing delay compared with no VLAN scenario. Therefore, VLANs can improve bandwidth utilization, power, speed and security.

keyword:-VLAN; Ethernet network.

الخلاصه

الشبكة المحلية الافتراضية هيه تعمل على توزيع المستخدمين في شبكات محلية منطقية او نطاقات التي يمكن من خلالها ان تتصل على شكل شبكة محلية واحدة النطاق او نفس النطاقات لتعدد الارسال. بروتوكول الاثرنيت مشهور جدا في عالم الشبكات بسب سهولة التنفيذ والاعداد. على اي حال، دعم جودة الخدمة هو اصبح ميزه مهمة لشبكات الاثرنيت. في هذا السياق، مشاكل الشبكات الكبيرة وزمن تاخير نقل البيانات اصبح مهم جدا. تخيف زمن التاخير من نهاية الى نهاية بواسطة تكنلوجيا الشبكة المحلية الافتراضية لتحسين اداء الشبكة. في هذا البحث، نحن نحلل ونقييم اداء الشبكات المحلية والشبكات المحلية الافتراضية في مختلف السيناريوهات. مؤشرات قياس الاداء الرئيسية مثل مرور الارسال ومرور الاستلام ومعدل التاخير ومعدل ارسال البيانات. المحاكاة نفذة باستخدام برنامج الاوبنيت نسخة الطالب 17.5. اثنين من السيناريهات المختلفة هيه مستعرضة لملاحظة الاداء لشبكة محلية وشبكة محلية افتراضية. نتائج المحاكاة تبين ذالك هنالك مرور كبير للبيانات في الشبكة التي لا تستخدم تكنلوجيا الشبكة المحلية الافتراضية. من هذا المنطلق، تكنلوجيا الشبكات المحلية الافتراضية تمنع الوصول الى مصادر الشبكة والاقسام الاخرى. كذالك، الشبكة المحلية الافتراضية تمتلك نصف زمن تاخير الانتظار او الطابور مقارنتا مع سيناريو الشبكة المحلية. لذالك، الشبكات المحلية الافتراضية تستطيع تحسين استخدام عرض الحزمة او النطاق والقدرة والسرعة والامان.

الكلمات المفتاحية : شبكة محلية افتراضية ، شبكة الاثرنيت.

I. Introduction

Alocal Area Network can be defined as a group of users or workstations that are located in the same physical area and has the same broadcasting domain. Ethernet networks have been widely used in the past 15 years. Layer 2 switch depends on IEEE802.3 Ethernet protocol that retransmits broadcast packets, multicast packets and unknown unicast IP packets to the all ports. Broadcasts reach all workstations without need to send to the gateway. Some broadcasting frames are management frames, which are security frames. Broadcast packets are served Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), Internet Group Management Protocol (IGMP), Bootstrap Protocol (BOOTP) and Simple Network Management Protocol (SNMP). Broadcast and multicast packets are not blocked during the traditional switches, which degrade the network performance (Moldovansky, 2002; Kiravuo,

2013). It is well-known that the Ethernet network is insecure technology. One of the possible solution is creating logical separation between end hosts and switches (Kiravuo,2013). However, the large LAN suffers from huge traffic frames with less bandwidth utilization and security. Traditionally, the router can divide the big segment into small ones with lower traffic. Users can be classified dependent on them jobs. The router works to forward the packets between these small LANs but this has many disadvantages such as delay and power consumption because of the routers forwards packets based on routing protocols if they have the destination address. Otherwise, non-routable packets will be flooded by routers, which are consumed high power to aggregate and choose the best route dependent on computational algorithms. Since the switches are more spread than routers in the networks. Layer 2 switches have more simpler and faster configuration than routers. Also, switches deal with frame instead of packets that have a longer prefix than frames. Therefore, switches are faster than router to handle the traffic (Kiravuo, 2013; Nur, 2014). However, the VLAN approach implements at layer 2 in wired network. VLAN can employ a special treatment to data flow to identify the service based on VLAN ID, which uses rather than TCP/UDP ports, which allow or block TCP and UDP ports (Meddeb *et.al*., 2009).

In this paper, OPNET simulator is used to provide comprehensive environment to implement the proposed paradigm. The simulation model for the suggested network is a special network for a company with three buildings as departments. The key performance indicators are traffic sent, traffic received, average queuing delay, throughput and time delay. A comparison was carried out on the proposed model of two different scenarios with LAN and VLAN technologies.

The reminder of this paper is organized as follows. In section II briefly reviews the related work. Section III presents the VLAN technology. Section IV discusses the main benefits of using VLAN concept. The designed network model and configuration networks are introduced in section V and section VI respectively. Section VII presents the simulation results and its analysis. Finally, section VIII summarizes the paper.

II. Related Work

Our research benefits of related work on VLAN model that tries to address the LAN problems. VLAN can be used to protect, monitor, control and manage the data traffic. The authors combine VLAN and virtual desktops to enhance management of operating system over network domain (Daryabar *et.al.*, 2011). As (Leischner and Tews ,2007) pointed out, using a new topology that integrates VPN and VLAN technologies with Supervisory Control And Data Acquisition (SCADA) implementations, which aims to overcome on the security vulnerabilities by adding more resistant to cryptanalysts. VLAN technique offers virtual isolated LAN from others network. VPN technique provides a secured communication channel that supports privacy and confidentiality for transmitted data. The authors combine these technologies to make a hard task against attacker. (Otsuka *et.al*.,2007) argued that VLAN cannot be used for raising network throughput, but for segregating host into many sets. However, VLAN can be also support multiple paths between hosts to raise throughput as follows: whole hosts are included in VLAN groups, which have different link groups to support the communication between VLAN groups. Each pair of hosts can use different links for communication. (Meddeb *et.al.*,2009) assess the performance of layer 2 security concept and they try to prove the layer 2 security better than higher layer security for sensitive delay applications such as VoIP and videoconferencing stream.

III. Virtual Local Area Network Technology

The underlying reason that makes routers cannot be used to divide the broadcast domain instead of switches because of routers require more time than switches to process incoming data (Cisco, 2016). Routers must recalculate checksum, decreases the time to live value and looks at longest-prefix that matches the destination address in header of the packet for forwarding. All these processes take time to process in routers. Alternatively, VLAN technology can be employed in switches for segmenting the broadcast domain (Kiravuo *et.al.*, 2013). However, primary driver behind VLAN is to reduce the congestion on the large LAN. VLANs can break the large physical LANs into small logical LANs to address the high traffic problem. VLAN can group hosts even though they are not in the same physical segment. The motivation of VLAN technology is to increase the network efficiency by reducing the broadcasting domain size. Thus, the host at different VLANs cannot directly communicate each other's. Moreover, VLAN can be used for security reasons (Kiravuo *et.al*., 2013; Nur, 2014). VLANs have higher flexibility than LAN to organize the devices/users into groups with logical LAN, they can communicate each other as if they are on the same wired LAN dependent on the logical connection rather than physical one. VLAN can be defined by IEEE802.1Q standard in 1998. VLAN attaches extra 4-bytes to traditional Ethernet frame header also known as VLAN tag as illustrated in Fig. 1.

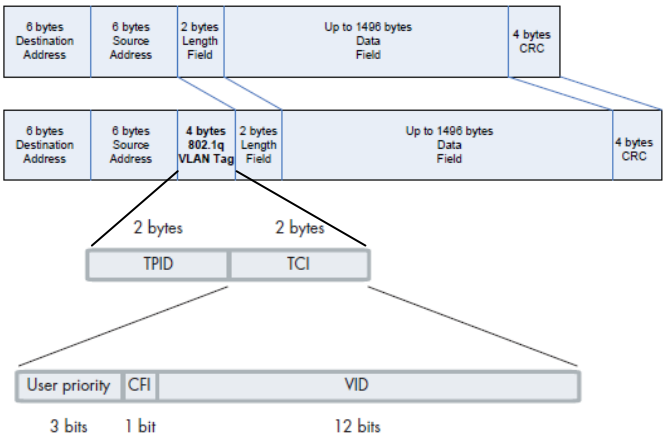

Figure 1: LAN and VLAN frame formats (Leischaer and Tews, 2007).

VLAN tag field contains the following bits: 3-bits known as Priority Code Point (PCP) to support 8 priority levels for user frame; 12-bits indicate VLAN ID to identify 4069 possible VLANs; 1-bit points out to Drop Eligible Indication (DEI) also known as Canonical Format Indicator (CFI) for control frame and 2-bytes Tag Protocol Identifier (TPID). PCP uses to determine Quality of Service (QoS) in the intermediate devices such as routers and switches (Kiravuo *et.al.*, 2013; Leischaer and Tews, 2007; Otsuka *et.al*.,2011). VLAN feature is supported in internetworking switches that allows administrators to segment the users into groups or VLANs according to applications, functions, etc. Each VLAN work as an independent network with separated logical broadcast domain even though it has share the same infrastructure of other VLANs. However, VLANs can enhance the LAN performance by dividing the single large broadcast domain into many smaller ones (Kiravuo *et.al.*, 2013; Cisco, 2016). The switches have a trunk port to carry frames among VLANs over multiple physical switches. IEEE802.1Q protocol adds/removes extra header fields for frames that are forwarded across trunk ports (Leischaer and Tews, 2007). The following section provides the primary benefits of VLAN

technology that aims to improve network performance.

IV. VLAN Benefits

The main advantages of using VLANs to organize the users/devices into large LAN. For the sake of brevity, we will list here some of the more main features that offer significant benefits to networks and users:

1) Security: grouping the users/devices that have the sensitive information from others in order to reduce the chance of breaching confidential data.
2) Saving cost: reducing the unnecessary transmission of available bandwidth and power. Switches that support VLANs can minimize the load on network devices.
3) Shrink broadcast domain: segmenting the large LAN into small VLANs diminishes the number of devices/users in the broadcast domain.
4) Simpler enterprise and application management: VLANs organize network devices/users based on business, geographic requirement, etc. The network has been become easy to manage and develop.
5) Improve IT staff efficiency: VLANs gather users dependent on similar functions. However, IT staff have no difficulties to configure particular switch (Moldovansky, 2002; Kiravuo *et.al.*, 2013; Cisco, 2016).

V. Network Model Description

A. Simulation of switched LAN(NO_VLAN)

The first scenario is designed to visualize the implementation of switched LAN network. However, there are three main switching devices used for buildings. A switch forwards the incoming packet to the output ports based on the destination address. In this scenario, there is one broadcasting domain/single network only. In this way, users allow to access to management confidential servers and share all resources. All nodes can communicate each other's without restrictions. Thus, there are high traffic requests on administrative server.

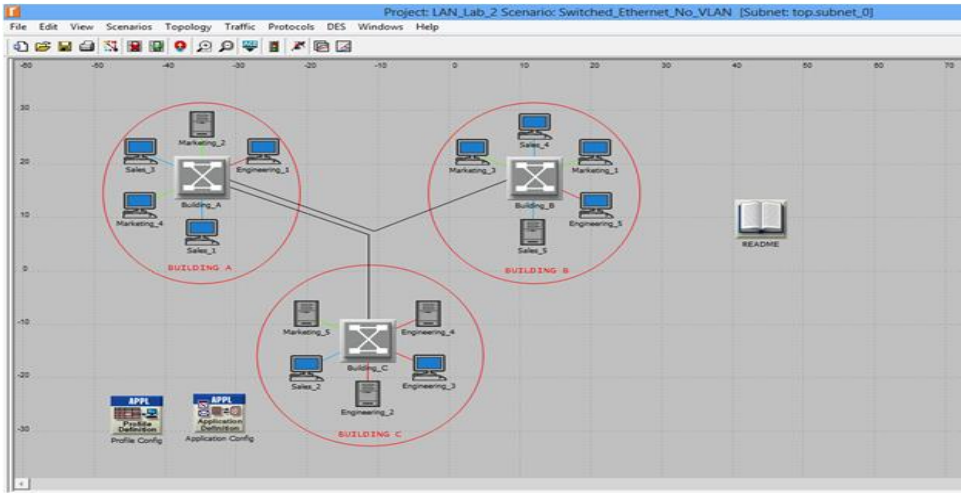

Figure 2: Switched Ethernet network scenario without VLANs.

Fig. 2 shows that there are three buildings A, B and C, they have different hosts and servers classified as marketing, sales and engineering respectively.

B. Simulation of VLAN network

In this section, VLAN scenario is considered with three logical group of users, which are found in different buildings. These users are logically segregated for security reason by using

different VLANs such as marketing, sales and engineering, which are defined in scenarios as depicted in Table I.

TABLE I
VLAN'S GROUPS CONFIGURATION

	Color	Server	VLAN Name	VLAN ID
Engineering	Red	Admin server	VLAN 30	30
Marketing	Green	Marketing server	VLAN 20	20
Sales	Blue	Sealing server	VLAN 10	10

Hosts and servers are distributed in three buildings as shown in Fig. 3.

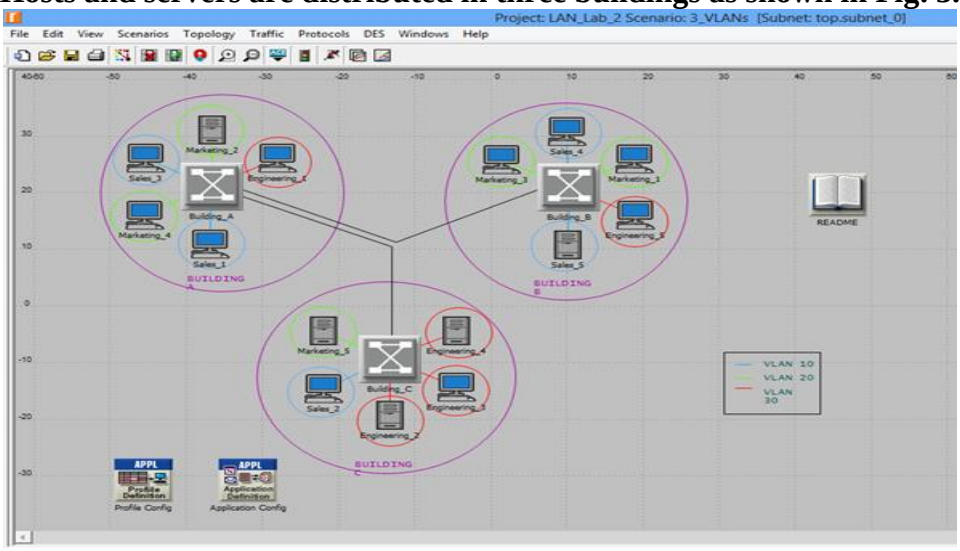

Figure 3: Switched Ethernet network scenario with three VLANs.

As in Fig. 3 shows that the network with VLANs, the red circles indicate the administration servers and workstations, the green circles represent the marketing network servers and workstations, and blue circles are sealing network servers and workstations.

VI. Application and Profile Configurations

Application definition can be defined as applications that are created to generate the traffic on the network. There are two applications in each scenario such as Email application and FTP (File Transfer Protocol) application. Applications performance have been checked with both VLAN and NO_VLAN scenarios. Profile configuration can be described as the activity of application which used by users throughout a time period. FTP profile and Email profile were used FTP application and Email application respectively. All profiles are configured to run together to allow more than one application to work at same time.

VII. Simulation Results

The network has been executed with different scenarios. The performance parameters that have been considered in this work are traffic sent and received, average delay analysis, throughput and application performance. The simulation results are obtained by using OPNET 17.5 Modeler student version available by Brunel University London/ United Kingdom. Both scenarios are using different data link layer protocol such as IEEE802.3 Ethernet LAN protocol

and IEEE802.1Q VLAN protocol. The results visualize the impact of different protocol on traffic sent and received, throughput and application performance.

A. Traffic sent

Traffic forwarded are measured in bits per second which are composed by traffic sources across all nodes. Fig. 4, 5 and 6 show the traffic sent for switch traffic forward of buildings in both NO_VLAN and VLAN scenarios.

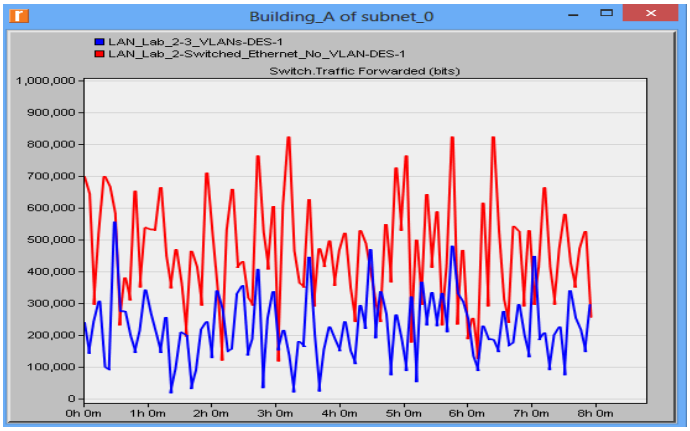

Figure 4: Traffic forwarded of building A (bits/sec).

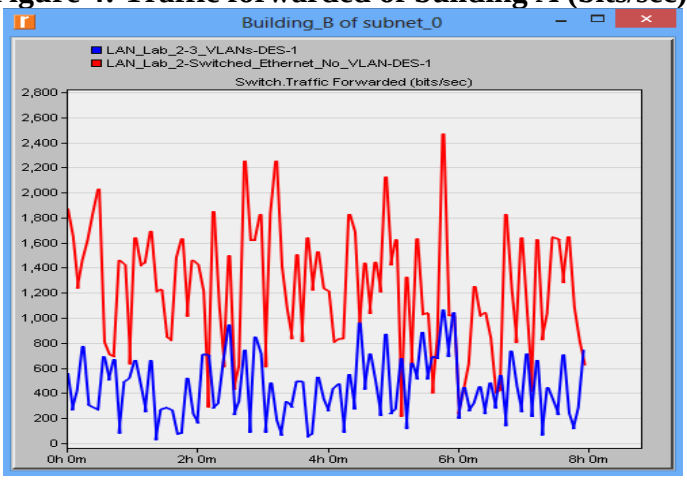

Figure 5: Traffic forwarded of building B (bits/sec).

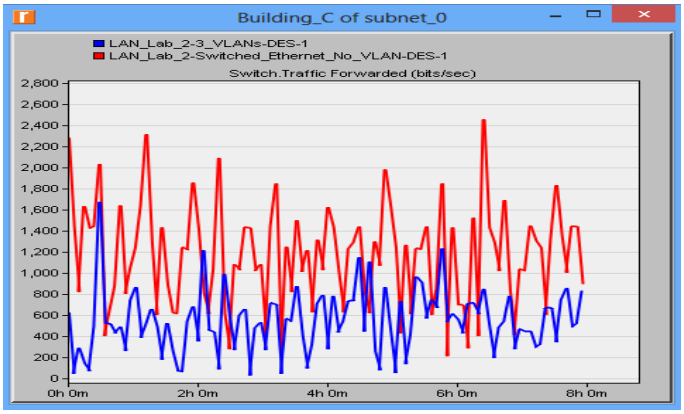

Figure 6: Traffic forwarded of building C (bits/sec).

It is clearly seen that there is different traffic forwarded in switches of buildings between two NO_VLAN and VLAN scenarios over all buildings A, B and C. VLAN scenario has lower traffic forwarded than NO_VLAN scenario because VLAN scenario has segmented a single large broadcasting domain into three broadcasting domains in order to reduce and control traffic forwarded of the network. VLAN technology can be used to mitigate vulnerability surface for attackers by reducing the traffic request to servers. On the other hand, VLAN achieves the power reduction in switches by reducing the required power to forward unnecessary traffic. This has affected the bandwidth utilization.

B. Traffic received

The traffic received of switched buildings for both NO_VLAN and VLAN scenarios is measured in bits per second as shown in Fig. 7, 8 and 9 across all nodes.

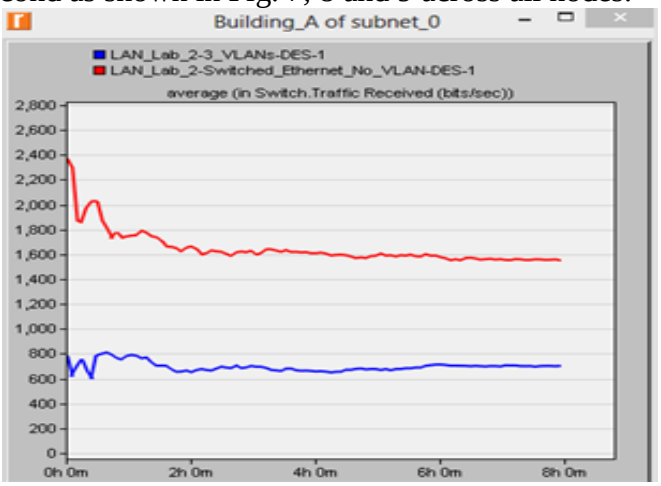

Figure 7: Traffic received of building A (bits/sec).

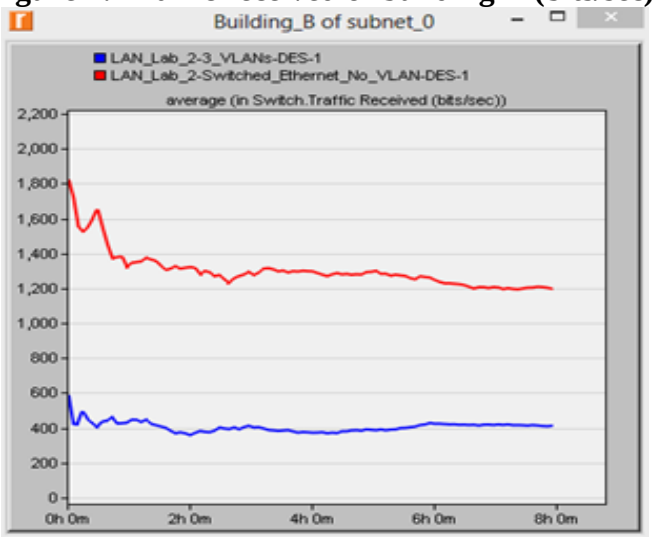

Figure 8: Traffic received of building B (bits/sec).

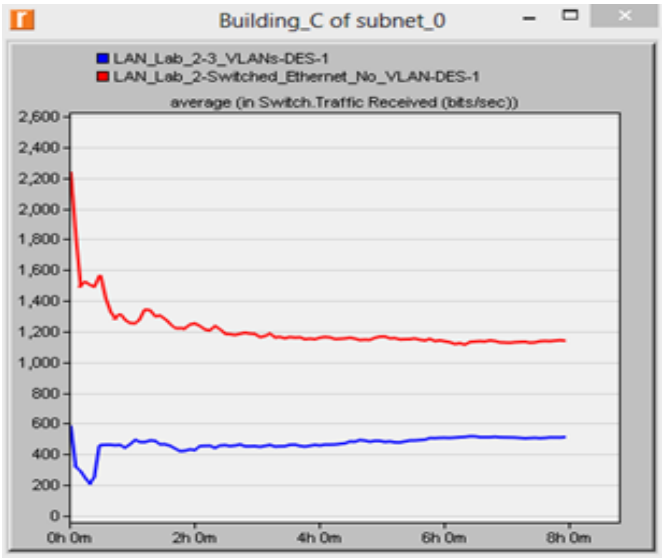

Figure 9: Traffic received of building C (bits/sec).

From the above three graphs in Fig. 7, 8 and 9 it can conclude that the VLAN curve (blue curve) has lower values of traffic received than NO_VLAN curve (red curve) across all nodes in three buildings. However, the traffic sent and received in switches have highly reduced with VLAN technology compared with NO_VLAN because the network broadcasting domain has divided into three logical networks in order to distribute users. Thus, VLAN scenario divides the total users by three; VLAN mitigates the risk of broadcasting storm by reducing attacking surface. Under VLAN scenario, sales are prohibited to access other departments. Therefore, VLAN can reduce the congestion level in networks with more bandwidth utilization.

C. ***Average queuing delay analysis***

The end-to-end queuing delay of all frames by nodes is measured in second for both building A to building B link and building A to building C link as shown in figures below.

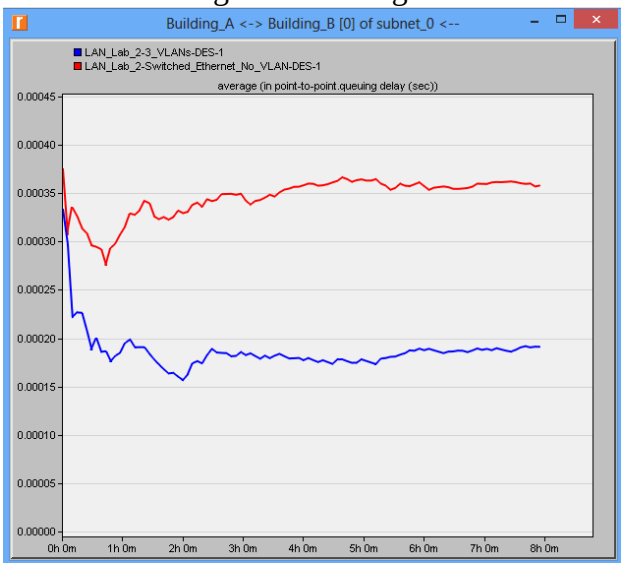

Figure 10: Average Queuing delay of A-B link.

TABLE II Average queuing delay of A-B link

	Minimum	Maximum	Average
NO_VLAN Scenario	0.000276	0.000376	0.000346
VLAN Scenario	0.000157	0.000334	0.000186

The presented results in Fig. 10 and Table II for A-B link indicate that VLAN scenario has less queuing delay than NO_VLAN scenario because of VLAN has less traffic flow over the time of simulation. However, the maximum value of queuing delay is approximately same for link building A-B in both cases, but the average and minimum queuing delay of VLAN are mostly half compared with NO_VLAN.

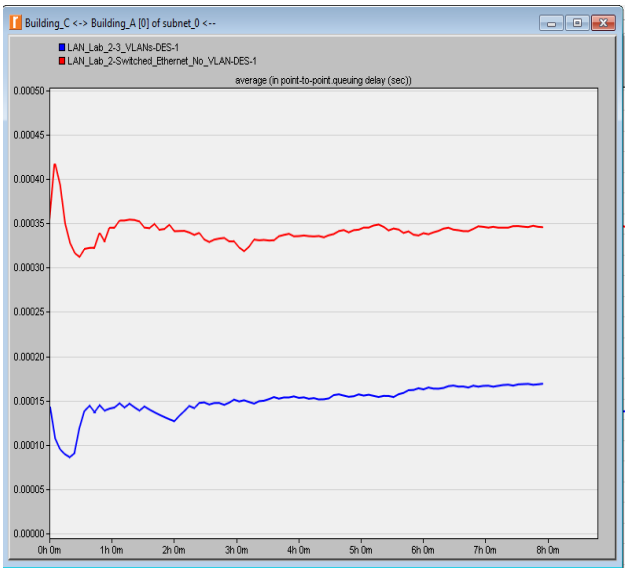

Figure 11: Average Queuing delay of C-A link.

It is clearly seen that in Fig. 11, the VLAN technology can minimize the average queuing delay for links between buildings as expected because of VLAN scenario has less forwarded and received traffic. VLAN works to distribute users over several logical broadcasting domains, the performance is improved.

TABLE III **Average queuing delay of C-A link**

	Minimum	Maximum	Average
NO_VLAN Scenario	0.000312	0.000418	0.000341
VLAN Scenario	0.0000860 2015	0.000169	0.00015

The data analysis of C-A link in Table III for both scenarios shows that VLAN scenario has approximately half average queuing delay than NO_VLAN scenario. This means that VLAN is an advantageous tool to reduce the queuing delay of communicating users for fast transmission.

D. ***Throughput***

The average throughput of links between buildings is measured in bits per second for both NO_VLAN scenario and VLAN scenario.

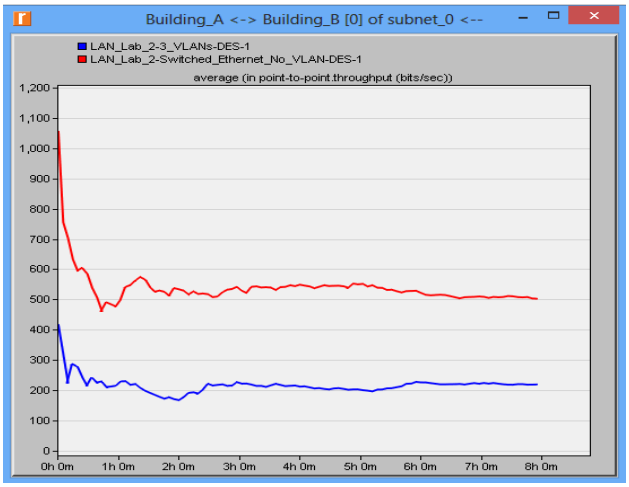

Figure 12: An average Throughput of A-B link.

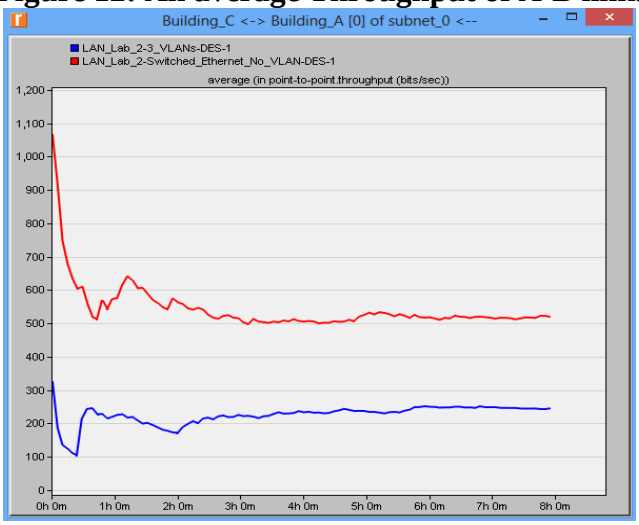

Figure 13: An average Throughput of C-A link.

It found that VLAN has less throughput compared to NO_VLAN scenario. That is because the NO_VLAN scenario has higher traffic than VLAN scenario due to a single broadcast domain. The traffic is exactly related to throughput. The traffic received and forwarded has a positive relationship with throughput. Therefore, VLAN cannot raise network throughput, but it works to segment single large network domain into three broadcast domains to achieve higher utilization of bandwidth with less traffic level. Moreover, VLANs can reinforce multiple paths between users to raise throughput.

*E. **Time delay***

There are two applications in both scenarios such as Email application and FTP (File Transfer Protocol) application. Applications performance have been evaluated with both VLAN and NO_VLAN scenarios. The time delay is the key performance indicator for upload and download in such applications.

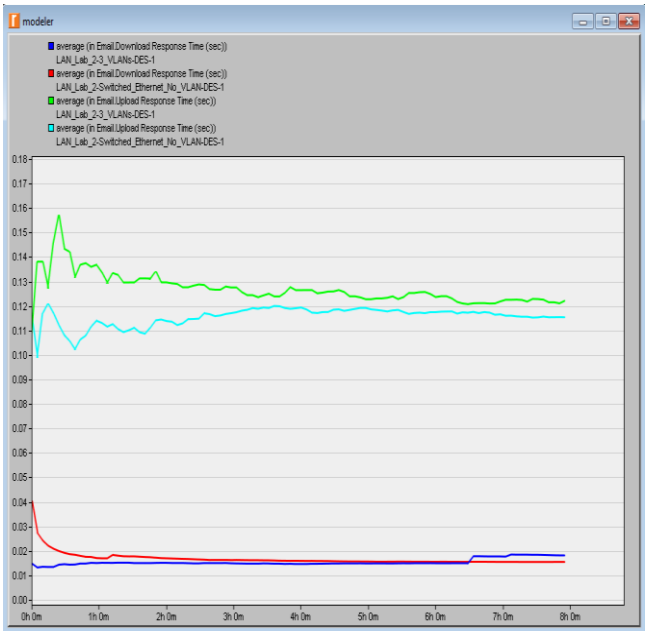

Figure 14: The response Time for both VLAN and switched Ethernet without VLAN (NO_VLAN) for Email application.

The graphs in Fig. 14 describe that VLAN scenario has a higher upload response time (green curve) and lower download response time (blue curve) compared to NO_VLAN scenario to Email application throughout the simulation. In case NO_VLAN, the Email application has given a better upload time delay (cyan curve), but slight higher download time delay (red curve) versus VLAN at the beginning of simulation. Then, download response time for both scenarios have approximately same and constant over the simulation. VLAN download response time has little bit lower than NO_VLAN at the end of simulation. Thus, NO_VLAN has better upload response time than VLAN with Email application.

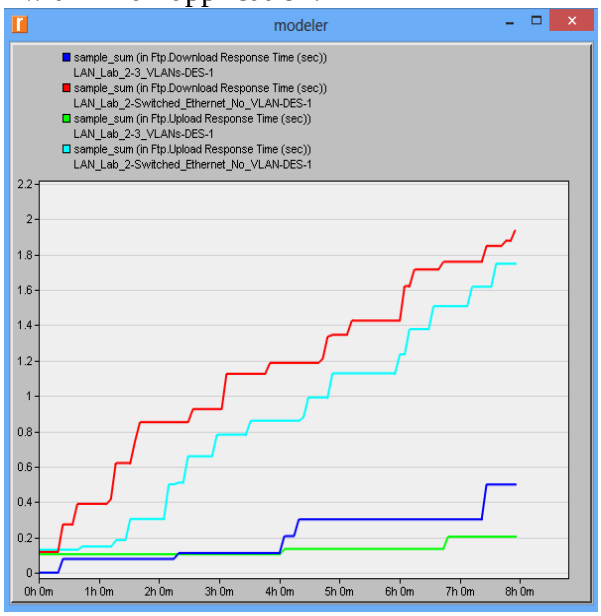

Figure 15: The response Time for both VLAN and switched Ethernet without VLAN (NO_VLAN) for FTP application.

Upload and download response time in both scenarios for FTP application are presented in Fig. 15. It is clearly seen that the VLAN scenario has a better performance in terms of upload and download response time (green and blue curves) compared with NO_VLAN scenario with heavy load FTP application. The difference between two scenarios is becoming large during the simulation. As a result, VLAN technology has considered as a best tool for heavy load applications such as multi-media applications, video streaming data, HTTP, FTP, and etc.

VIII. Conclusion

This work has been aimed to improve LAN performance by using VLAN technology, which have many merits in terms of power, throughput, delay and bandwidth. MAC layer protocol is very important in the implementation of the network. Choosing the technology effects the security and bandwidth utilization. We have evaluated the performance of the network by using two data link layer protocols such as IEEE802.3 and IEEE802.1Q. Different network departments have been considered employing OPNET modeler. Traffic sent, traffic received, throughput and average response time for links and applications are been the key performance indicators. VLAN was proved that it has limited access to the confidential server files by controlling traffic and achieving better security and less level of congestion. The comparative results give a clear picture about selection of VLAN technique for heavy load applications gives a significant result for the performance of the network. In the future, it can introduce other cost effective functions to control further computing-related resources.

References

Cisco , 2016, "Cisco Networking Academy's Introduction to VLANs", Cisco Press, 2014. [Online]. Available: http://www.ciscopress.com. Accessed: Oct. 23.

Daryabar F., Dehghantanha, A., Norouzi, F. and Mahmoodi, F. , 2011, "Analysis of virtual honeynet and VLAN-based virtual networks". International Symposium on Humanities, Science and Engineering Research. IEEE. pp. 73-77.

Kiravuo T., Sarela, M. and Manner, J. , 2013 ,"A survey of ethernet lan security". IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, pp.1477-1491.

Leischner G. and Tews, C., 2007 ,"Security through VLAN segmentation: Isolating and securing critical assets without loss of usability". In proceedings of the 9th Annual Western Power Delivery and Automation Conference, Spokane, WA.

Meddeb A., Elgueder E., Harrathi I. and Youssef H. , 2009,"Benefits of a pure layer 2 security approach in Metro Ethernet". In *Computers and* Communications, ISCC.IEEE Symposium. pp. 48-49.

Moldovansky A. , 2002, "Utilization of modern switching technology in ethernet/IP networks". *In Proccedings of 1st Workshop on Real-Time LANs in the Internet Age*, pp. 25-27.

Nur, A.M.H. , 2014 ,"Performance Analysis of LAN and VLAN Using Soft Computing Techniques." *IOSR Journal of Electronic and Communication Engineering*. Vol. 9, No. 6. pp. 10-16.

Otsuka T., Koibuchi M., Jouraku A. and Amano H. , 2005 , "VLAN-based minimal paths in PC cluster with Ethernet on mesh and torus". International Conference on Parallel Processing (ICPP'05). IEEE, pp. 567-576.