Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

OPEN ACCESS Journal of Applied Sciences

ISSN 1812-5654
DOI: 10.3923/jas.2016.517.525

Research Article
Analysis of Virtual Local Area Network (VLAN) with Physical Network Security Implementation

Mohammed F. Alsharekh

Department of Electrical Engineering, Unaizah College of Engineering, Qassim University, Saudi Arabia

Abstract

Background: High throughput, minimum delay of final demand, require from any network. Traffic congestion is in a given network performance and reduce the main problem. Although, a switch to help greatly improve the transport efficiency, but this is not a large network, which in the case of WAN. **Objectives:** Virtual lAN (VLAN) switches play an important role, to further improve network performance. Available types are based on the port number and the new version is based on the Media Access Control (MAC) address. A design analysis is carried out to prove that VLAN switch techniques improve the throughput of a network as the graphical results using different network metrics backs this statement. **Methodology:** The design and analysis is done on OPNET IT Guru software which has been proven to be very efficient real time network simulator software by other researchers. **Results:** The results obtained from the simulations and testing of the security lock is successful. A password based electronic combination lock is proposed as the physical security measure implemented to boost the network security as it allows for only authorized personnel access to the room or office depending on where it is installed on the infrastructure. **Conclusion:** The security of a network topology of an organization irrespective of its size is not only dependent only on the virtual configuration but also on the physical security measure implemented to prevent unauthorized personnel access to the network facilities especially its main server room and other very important rooms or offices.

Key words: Management security, network security, OPNET IT, traffic congestion, VLAN

Received: August 29, 2016 Accepted: September 20, 2016 Published: October 15, 2016

Citation: Mohammed F. Alsharekh, 2016. Analysis of Virtual Local Area Network (VLAN) with physical network security implementation. J. Applied Sci., 16: 517-525.

Corresponding Author: Mohammed F. Alsharekh, Department of Electrical Engineering, Unaizah College of Engineering, Qassim University, Saudi Arabia

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

With the increase in computer and network systems in today's world, the need to increase and strong computer and network security has become increasingly necessary and important[1]. In the computer network system has exposed many networks increase the variety of internet threats and exposure, one can see the need to improve network security is crucial, every organization[2,3]. Security, including identification, authentication and authorization, as well as surveillance cameras, to protect the computer hardware or network device[4] the integrity, availability, accountability and authenticity. There is no procedure laid down to design a secure network.

Virtualization of hardware in computer systems is a technique used to separate and make physical resources of hardware available to logical machines[5], which provide services to their users the same way a physical machine does. Virtualization introduces a new layer of implementation to our traditional computer networks, which introduces new security issues in the network[6,7].

The VLAN technology network, which is usually defined as a broadcast domain can be considered as a group of one of the regions of the terminal station. Perhaps in multiple physical LAN segment, this is not the limit of their physical location, you can communicate if they have a common LAN[8,9]. The analysis of the throughput of a VLAN network makes it possible to know the effectiveness of the network. The OPNET IT Guru provides for a real network scenario design implementation and gathering of results using different metrics.

Research has focused on the accuracy of the simulation more realistic network packet level analysis. Currently the popular network simulator that can perform this type of analysis modeling OPNET and NS-2 from the virtual gateway test-bed projects VINT two. These were selected because they are in academia, business and industry visibility. In this study, two network simulator, the network test bed. From OPNET NS-2 and modeling accuracy compared using CBR data traffic and FTP sessions. Several programs have been evaluated and regeneration of simulation tools and network test bed[10]. Results networking researchers provide interesting guidelines in network simulation tools of choice[11]. From the researcher's point of view, NS-2 provides very similar results compared to the OPNET Modeler, but the "Free" version of the NS-2 makes it more attractive to researchers[12]. However, a complete set of OPNET Modeler module provides more functionality than the NS-2, therefore, the network operators will be more attractive. The OPNET has a good design with the mainstream software and operating system user interface.

A research closely similar was conducted by Begg *et al.*[13], from the department of computer science and software engineering from the University of Canterbury research simulator next generation network service availability and flexibility. This study is done to find the best network simulator software for discrete-event simulation. The evaluation criteria used in this survey was modeling capabilities, credibility of simulation models and simulation results, extendibility, usability and costs of licenses. Simulation models are said to be credible if they are valid and verified. If a model represents a given system accurately at the required level of details then it's said to be valid. The credibility of a final result which a simulator using a simulation model produces depends on the quality of its sources of randomness and statistical accuracy of the final simulation results. The extendibility of a simulator means its ability to be expanded[14]. The amount of work/time needed to extend the existing simulation models is an important factor. The usability of a given simulator is measured by the level of its user-friendliness. The final results of the research show that simulation studies of service availability and resilience by using various simulations are feasible and can be done relatively easily. It is seen that some bugs were detected in a software patch when applying NS2. This hinders the comparison of OPNET and NS2. Not with standing, a conclusion was made practically justifying OPNET as the tool for the next stage of network research projects[15]. The OPNET proved to be relatively easy to use and there was no problem obtaining the required results.

Observed with respect to both send and receive frames network performance and results. When the frame size of 1500 bytes is constant, then the received traffic, high latency and collisions. However, reduce the 1500-256 bytes of frame size, the performance is improved. Delay, transportation tank, traffic sources, collisions and packet sizes are used in this study performance index. The simulation results show that performance data traffic in an Ethernet environment observed a good approximation[16].

Many architectures using virtual LANs, in its switch, the same network infrastructure independent of each subnet. Generally, completely isolated virtual LANs. In 2002 the Black Hat conference, introduction, from: Convery Sean (CISCO) shows how inter-VLAN packets. Obviously, this is possible because, VLAN design is not safe, it is used to force[17].

The European Research magazine published a performance appraisal in 2009 different Ethernet LAN switch and hub. The purpose of this study is in an Ethernet environment to measure latency and throughput performance. The OPNET's specification, simulation and performance analysis of various communication networks to provide a comprehensive development environment. There are so many factors, such as a heavy load on the network generate higher traffic, resulting in congestion of the network interface. Network security is that people always thought it was, malware, viruses, trojans, hackers and sometimes even exceeded. Network security may be an unintentional human error, which can damage a person's nature, as well[18].

In a LAN network of organizations now-a-days, consists of many workstations, network printers, servers and router which are used primarily to transmit incoming data throughout the network. At times, if two individuals were to send data simultaneously, a collision would occur resulting in loss of all data transmitted. The original data would have to be sent again as the coalition continues to propagate throughout the network by the switches. Switches form LAN segments with workstation and are commonly known as collision domains because collisions remain within that segment. The physical connection between workstations, switches[19] and routers[20] determines broadcast and collision[21] domains which mean that all participants in the LAN must to be in the same location. This results to busy traffic which is often a problem of large LAN networks.

In the LAN, if the mobile device from one to another hub, the network address is no longer true and from the network group must go to the machine and then corrected. This is not much work if it rarely occurs, but in a larger network workstation with a high percentage is increasing every year, this process can take a lot of time and the machine cannot communicate until the update is complete[20]. In the hub network[22], there is a certain amount of bandwidth limits, users can share. Sacrificing performance is difficult to accommodate the case of a significant increase. Today more than ever, the application needs more band width. In many cases, the entire network must undergo a periodic re-designed to adapt to economic growth.

The performance, privacy (security) and management of a single LAN is no more regarded highly reliable[23]. Let us consider a multiple LANs across campus or college, it is notice that there are too much broadcast traffic (not filtered by switches), so many hubs and routers thereby incurring so much cost, the need to enhance data security, the need to improve network manageability.

The security of a network is not only limited to virtual configuration but also physical implementation to ensure only authorized users get access to the main network infrastructure i.e., server room. Safes and vaults access control, security engineering design of today's most interesting and elegant example is the use of a mechanical combination lock.The basic internal structure of the modern safe lock long predates computers and networks and yet a careful study of these devices reveals a rich history of threats and countermeasures that mimic the familiar cycles of attacks and patches that irk practitioners of computer and network security[24]. The electronic combinational lock system is implemented to provide a form of physical security to the network especially its server room as it boosts the overall network security and as well as its performance.

A network topology can only be said to be secure when the virtual security configuration is implemented as well as physical security[25]. The need for a physical security measure for a network and its server room are very essential as unauthorized persons having access to the main server or other confidential hosts can lead to loss of vital important data and bridge of security. In this study, the VLAN is designed using the OPNET simulator for analysis the throughput of a network. The performance of the network is evaluated by using different network metrics such as traffic received, traffic forwarded and link delay. The electronic combination lock is implemented on the physical network to provide a security measure. Therefore, only authorized personnel with the password combination can access the server.

MATERIALS AND METHODS

System design and description: A proposed block diagram is used to analyze the hardware description as well as software design. Also discusses the major components of the system description information.

System block diagram for inter-VLAN routing: Figure 1 shows the proposed VLAN implementation on a small scale level in the Cisco laboratory using two Cisco switches, 5 PC's, 1 Cisco router and a main server where applicable. The switches are connected to each other with PC's connected their ports. A main server and router are connected to switch 1. The two switches are connected together to enable the IEEE 802.1Q protocol for VLAN Trunking which makes it possible for two switches to interact. Two VLANs cannot interact except there is a layer 3 device (e.g., router, layer 3 switches) connected. So, the router is connected to enable two or more VLANs interact with one another.

Physical security lock block diagram: The physical network security system block diagram which is an electronic combination lock is shown in Fig. 2. The electronic combination lock system block diagram implemented as a physical security measure for the network. The system is made up of 5 main parts: Power source, microcontroller, keypad, LCD, buzzer, LED. The microcontroller acts as the main control unit of the system as it is programmed to carry out various functions. There are two inputs and 3 outputs. The power source (5 V) and the keypad are the inputs. The keypad is the main input which is used to key the password into the system. The LCD, buzzer and LED are the outputs.

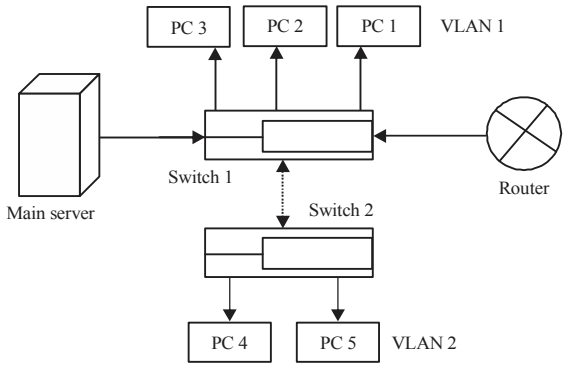

Fig. 1: Inter-VLAN routing block diagram for virtual local area network

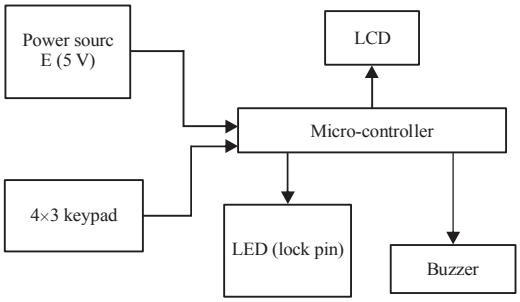

Fig. 2: Physical security lock block diagram for virtual local area network

VLAN design using OPNET IT Guru: Figure 3 shows the VLAN design using OPNET IT Guru. The design is based on a college or university block setting. The main aim here as a network engineer is to get the maximum out of their current infrastructure by implementing VLANs to reduce cost and LAN traffic. In this design, there are two scenarios.

The first scenario is called CollegeNetwork_NO_VLAN where the switch performance in a wired switched Ethernet network is studied. The second scenario is called CollegeNetwork_With_VLANs were the switch performance is improved by configuring VLANs. There are different faculties existing in the various blocks. The faculty of Social Science highlighted with the blue color exists in one VLAN (VLAN 10) and as such can share ideas. The faculty of Information Technology with the lemon green color exists in one VLAN (VLAN 20) and as such they can share ideas. The faculty of Engineering highlighted with the red color exists in one VLAN (VLAN 30) and as such can share ideas. Faculties existing in the same VLANs share ideas with each other notwithstanding their physical location. There are a number of software required to facilitate the hardware of the VLAN to successfully operate in the completion of this project, which is shown in Table 1.

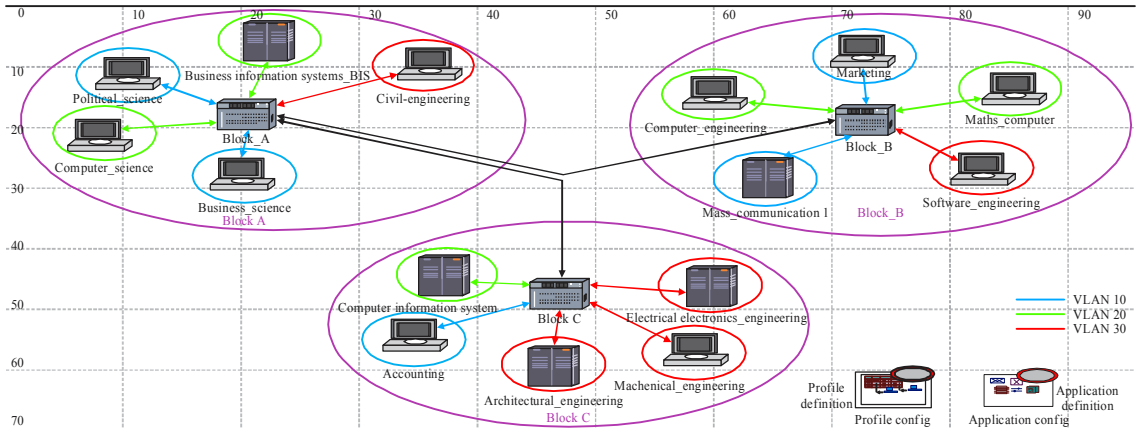

Fig. 3: VLAN design using OPNET IT Guru

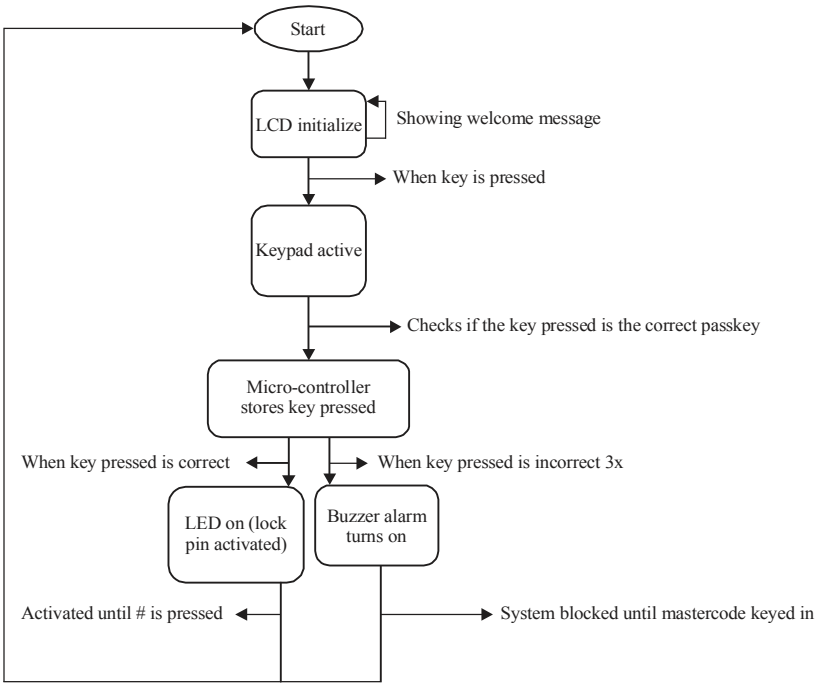

Fig. 4: System flowchart of data in the electronic lock security system

Table 1: Software requirement

Items	Software environment	Category
Design simulator software	OPNET IT Guru Academic Version	Free license
Inter-VLAN implementation design	Cisco Packet Tracer	Freeware
Circuit design and simulation	Proteus 7 Professional	License file
Power circuit design and simulation	Multism 10	License file
Source code (embedded C language)	Keil u Vision 4	License file

Implementation of software and hardware: The design hardware for the electronic combination lock security system consists the fundamental components such as AT89C51 microcontroller, 4×3 keypad, 2×16 LCD module, LED and buzzer. Numeric key is used to enter a password number. The '*' is used for the cancel key when a wrong key is pressed. The '#' is used for the enter key when the right password key is pressed to activate the lock pin, which is shown by the LED lighting. When the password is wrong for three times the system displays "BLOCKED" on the LCD whilst also activating the alarm and only the master code can be used to unblock it.

The password can be changed by inputting the password changed key and then the system asks for the master code to be entered. Once it's entered, the system asks for the new password to be inputted and saves the new password. Figure 4 show the flowchart drawn for the interpretation of the flow of data in the electronic combination lock security system gives an easier understanding of the working of the project. The code for the microcontroller is written in C language. The hex file is burnt into the controller with the burner.

RESULTS

The results shown in Fig. 5-8 are the graphical comparison of the VLAN design scenarios. The blue color indicates the CollegeNetwork_No_VLAN scenario while the red indicates the CollegeNetwork_With_VLAN scenario. The results are compared to the previous study carried out as detailed in the literature review background study. The results have shown considerably prove to back up this study on VLAN implementation in networks using different performance metrics.

Block_A (Switch 1): Figure 5a and b shows the traffic received and forwarded (bits sec^{-1}) on Block_A (Switch 1). The graph shows a significant difference in the traffic received and forwarded for both scenarios. The X-axis represents the time, the position in the Y-axis represents. An average of 1,500 bits is received over a period of about 8 h on the network were VLAN is not configured while an average of 500 bits is received at the same time in the network were VLAN configured. The average traffic forwarded is seen in Fig. 5b which is the same

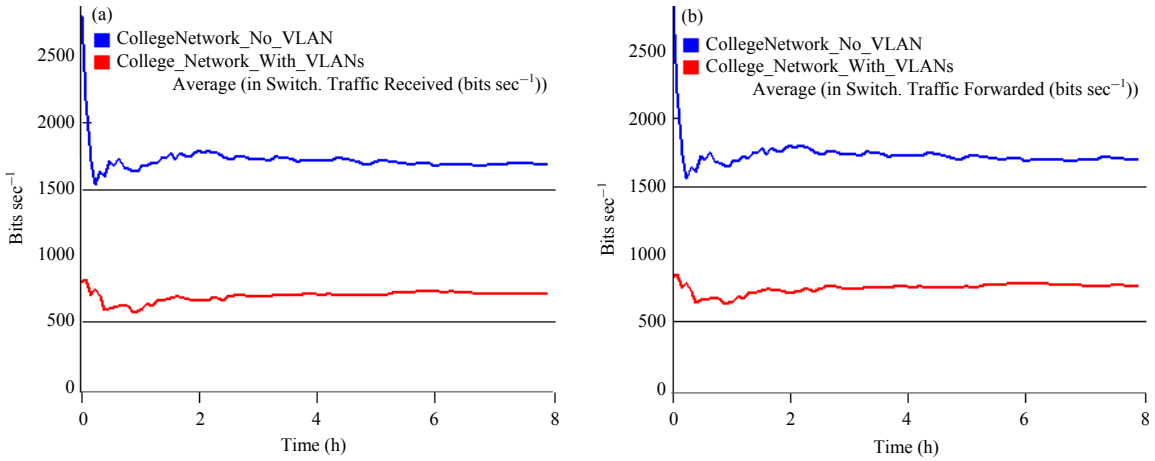

Fig. 5(a-b): Traffic (a) Received and (b) Forwarded on Block_A of subnet_0

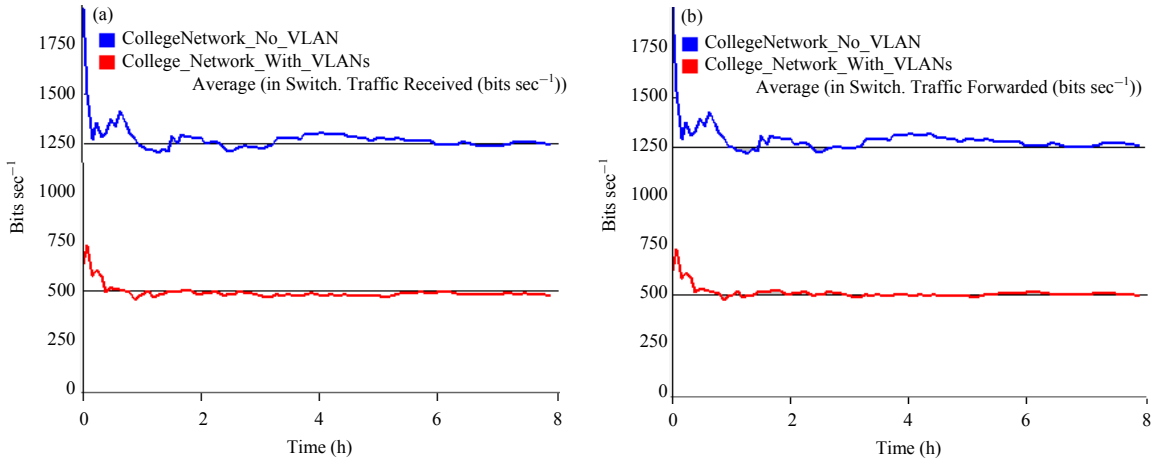

Fig. 6(a-b): (a) Traffic (a) Received and (b) Forwarded on Block_B of subnet_0

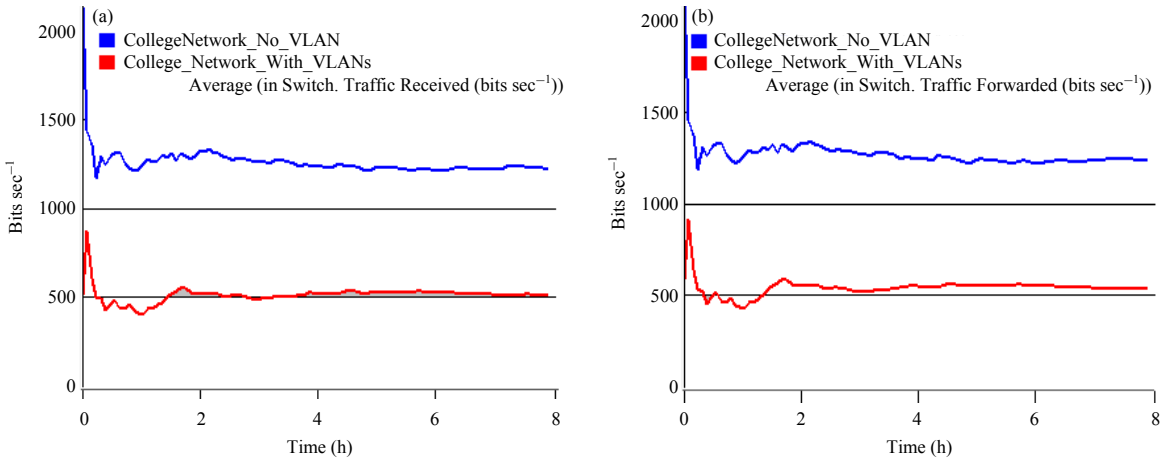

Fig. 7(a-b): Traffic (a) Received and (b) Forwarded on Block_C of subnet_0

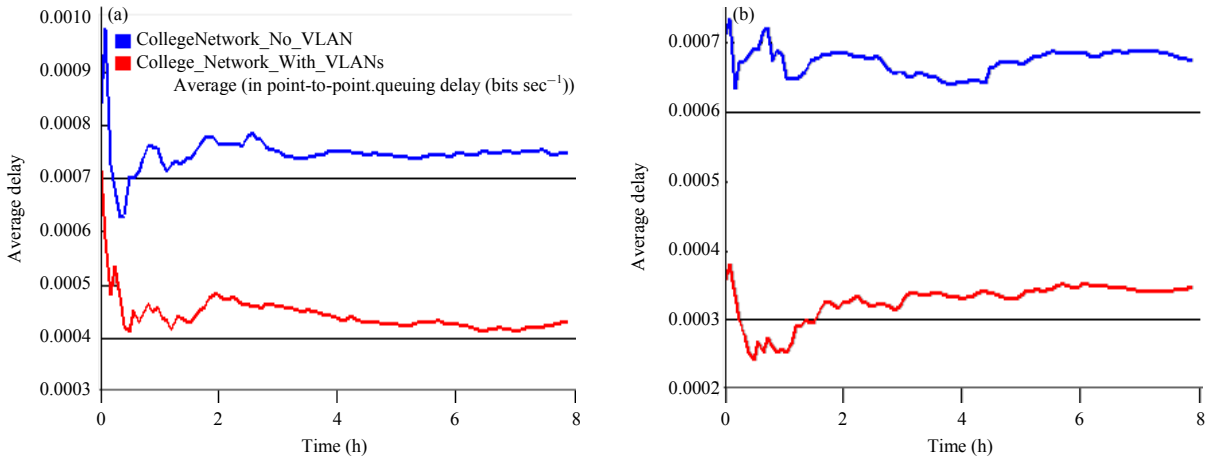

Fig. 8(a-b): (a) Average link delays of (a) Block_A to Block_B of subnet_0 and (b) Block_C to Block_A of subnet_0

value as the traffic received. The traffic received and forwarded in the scenario With_VLAN is much lesser than that of No_VLAN. This justifies the fact that VLANs help reduce network traffic.

Block_B (Switch 2): Figure 6a and b shows the traffic received and forwarded on Block_B (Switch 2) in bits sec^{-1}. The graph shows a significant difference in the traffic received and forwarded for both scenarios. The traffic received and forwarded in the scenario With_VLAN is much lesser than that of No_VLAN. This result agrees with the results of Block_A (Switch 1) further helping to prove that the network with VLAN is better than network with no VLAN as it helps reduce traffic.

Block_C (Switch 3): Figure 7a and b shows the traffic received and forwarded on Block_C (Switch 3). The graph shows a significant difference in the traffic received and forwarded for both scenarios as the bits received and forwarded to the network with VLAN is less compared to the network with no VLAN. The traffic received and forwarded in the scenario With_VLAN is much lesser than that of No_VLAN. This further justifies the fact that VLANs help reduce network traffic.

This type of delays falls within the congestion delay category. Figure 8a and b show the average queuing delays of the links connecting the blocks (Switches). The queuing delays here are small because the switches are not filled up to cause packet dropping. If the queue levels (hence queuing delays) were large, then having VLAN configuration would make a greater impact on the network response time in addition to reducing switch throughput according to Faheem[26].

DISCUSSION

There have been several efforts to provide security in virtual network. Wei *et al.*[27] and Cabuk *et al.*[28] implemented a prototype of their framework based on a para-virtualization platform, while Huang *et al.*[29] considered an underlying network based on programmable routers. Although the majority of publications do not target specific network virtualization techniques, different types of platforms have their own sets of benefits, which is similar to the sHype security model. The sHype[29] is a security model which add isolation enforcement and policy defined resource to monitor mandatory access control policies on VLAN communication. This perspective is important to understand how a VLAN implementation works, especially because there are no standards for VLAN implementation. The implementation described in this study is a design model of an existing security kernel (Turaya)[30]. The Turaya security kernel comprises two layers: A hypervisor layer basedon an L4 microkernel[31,32] and resource management services (memory management, I/O drivers) and the trusted software layer providing the security services to achieve security model. As the specific implementation described by Tiwari *et al.*[33] and Kikuta *et al.*[34] should be possible to generalize VLAN models from other systems. The VLAN model is a set of general methods or techniques that should be useful in evaluation and comparing the various proprietary standards in delays. Previous study results show a network, by increasing and reducing inter-hub fixed frame size reduces collision or switched network. These results from this VLAN design now justify that irrespective of the frame size in a network where a VLAN is configured on the

switches; the network performance of the network is improved. The traffic forwarded and received and the link queuing delay is all better for the network with VLAN.

CONCLUSION

A physical network security measure was implemented in the form of an electronic combination lock of which a circuit was finally built that had the ability to open three different doors using a password and activate an alarm when the password is inputted wrongly 3 times. The password can be changed when there is a breach of security depending on the program written. This project can be used to improve network security in general as implementing VLANs improves the network performance and electronic combination lock provides physical security to the organization's network such as banks, hospitals, rooms or offices has any confidential information on their systems especially the server room of the network topology.

ACKNOWLEDGMENTS

The author would like to acknowledge this study for significant advances field of networks in the form of VLAN's which allow the better security formation of physical network security implementation to improved VLAN performance and simplified the administration, which was supported by Unaizah Engineering College.

REFERENCES

1. Wei, W. and Y. Qi, 2011. Information potential fields navigation in wireless Ad-Hoc sensor networks. Sensors, 11: 4794-4807.
2. Chen, S., J. Xu, R.K. Iyer and K. Whisnant, 2002. Evaluating the security threat of firewall data corruption caused by instruction transient errors. Proceedings of the International Conference on Dependable Systems and Network, June 23-26, 2002, Washington, DC., pp: 495-504.
3. Kim, H.W. and S. Lee, 2004. Design and implementation of a private and public key crypto processor and its application to a security system. IEEE Trans. Consum. Electron., 50: 214-224.
4. Skorin-Kapov, N., J. Chen and L. Wosinska, 2010. A new approach to optical networks security: Attack-aware routing and wavelength assignment. IEEE/ACM Trans. Networking, 18: 750-760.
5. Li, P. and T. Mohammed, 2008. Integration of virtualization technology into network security laboratory. Proceedings of the 38th Annual Frontiers in Education Conference, October 22-25, 2008, Saratoga Springs, NY., pp: S2A-7-S2A-12.
6. Bleikertz, S., 2010. Automated security analysis of infrastructure clouds. M.Sc. Thesis, Technical University of Denmark, Denmark.
7. Song, H. and M. Brandt-Pearce, 2013. Range of influence and impact of physical impairments in long-haul DWDM systems. J. Lightwave Technol., 31: 846-854.
8. Wang, T.I., C.H. Yeh and Y.M. Huang, 2005. A secure VLAN construction protocol in wireless AD HOC networks. Proceedings of the 3rd International Conference on Information Technology: Research and Education, June 27-30, 2005, Taiwan, pp: 68-72.
9. Song, H. and M. Brandt-Pearce, 2013. Model-centric nonlinear equalizer for coherent long-haul fiber-optic communication systems. Proceedings of the IEEE Global Communications Conference, December 9-13, 2013, Atlanta, Georgia, USA., pp: 2394-2399.
10. Lucio, G.F., M. Paredes-Farrera, E. Jammeh, M. Fleury and M.J. Reed, 2003. OPNET modeler and Ns-2: comparing the accuracy of network simulators for packet-level analysis using a network testbed. WSEAS Trans. Comput., 2: 700-707.
11. Lucio, G.F., M.P. Farrera, E. Jammeh, M. Fleury, M.J. Reed and M. Ghanbari, 2006. Packet by packet analysis in contemporary network simulators. IEEE Latin Am. Trans., 4: 299-307.
12. Zhu, C., O.W.W. Yang, J. Aweya, M. Ouellette and D.Y. Montuno, 2002. A comparison of active queue management algorithms using the OPNET modeler. IEEE Commun. Magaz., 40: 158-167.
13. Begg, L., W. Lui, K. Pawlikowski, S. Perera and H. Sirisena, 2006. Survey of simulators of next generation networks for studying availability and resilience. Technical Report TR-COCS 05/06, Department of Computer Science and Software Engineering, Univeristy of Canterbury, Christchurch, New Zealand.
14. Heidemann, J., K. Mills and S. Kumar, 2001. Expanding confidence in network simulations. IEEE Network, 15: 58-63.
15. Makris, P., D.N. Skoutas and C. Skianis, 2013. A survey on context-aware mobile and wireless networking: On networking and computing environment's integration. IEEE Commun. Surveys Tutorials, 15: 362-386.
16. Bansal, R.K., V. Gupta and R. Malhotra, 2010. Performance analysis of wired and wireless LAN using soft computing techniques-a review. Global J. Comput. Sci. Technol., 10: 67-71.
17. Sean, C., 2002. Hacking layer 2: Fun with ethernet switches. Cisco Systems. https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf
18. Din, I.U., S. Mahfooz and M. Adnan, 2009. Performance evaluation of different Ethernet LANs connected by switches and hubs. Eur. J. Scient. Res., 37: 461-470.
19. Nadarajah, N., E. Wong, M. Attygalle and A. Nirmalathas, 2006. Protection switching and local area network emulation in passive optical networks. J. Lightwave Technol., 24: 1955-1967.

20. Decasper, D., Z. Dittia, G. Parulkar and B. Platter, 2000. Router plugins: A software architecture for next-generation routers. IEEE ACM Trans. Network., 8: 2-15.
21. Peng, J., 2007. A new scheme to avoid collisions for broadcast packets in wireless LANs. IEEE Commun. Lett., 11: 762-764.
22. Joseph, V. and S. Mulugu, 2012. Deploying next generation multicast-enabled applications: Label switched multicast for MPLS VPNs, VPLS and wholesale ethernet (Joseph, V. and Mulugu, S.)[Book review]. IEEE Commun. Magaz., 50: s8-s8.
23. Chen, X. and X. Chen, 2012. Study on layout strategy of transit hub network. Proceedings of the International Conference on Industrial Control and Electronics Engineering, August 23-25, 2012, Xi'an, China, pp: 258-261.
24. Wu, J., H.P. Shiang, K.T. Chen and H.W. Tsao, 2002. Delay and throughput analysis of the high speed variable length self-routing packet switch. Proceedings of the Workshop on High Performance Switching and Routing, Merging Optical and IP Technologies, May 29, 2002, Kobe, Japan, pp: 314-318.
25. Wei, W., Q. Xu, L. Wang, X.H. Hei, P. Shen, W. Shi and L. Shan, 2014. GI/Geom/1 queue based on communication model for mesh networks. Int. J. Commun. Syst., 27: 3013-3029.
26. Faheem, H.M., 2005. Multiagent-based security for the wireless LAN. IEEE Potentials, 24: 19-22.
27. Wei, W., X.L. Yang, P.Y. Shen and B. Zhou, 2012. Holes detection in anisotropic sensornets: Topological methods. Int. J. Distrib. Sensor Networks. 10.1155/2012/135054.
28. Cabuk, S., C.I. Dalton, H. Ramasamy and M. Schunter, 2007. Towards automated provisioning of secure virtualized networks. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 29-November 2, 2007, Alexandria, VA., USA., pp: 235-245.
29. Huang, D., S. Ata and D. Medhi, 2010. Establishing secure virtual trust routing and provisioning domains for future internet. Proceedings of the IEEE Conference on Global Telecommunications, December 6-10, 2010, Miami, USA., pp: 1-6.
30. Song, H. and M. Brandt-Pearce, 2012. A 2-D discrete-time model of physical impairments in wavelength-division multiplexing systems. J. Lightwave Technol., 30: 713-726.
31. Vaishnavi, R.A. and R. Rajalakshmi, 2012. Shype to maintain the ATM system stability. Proceedings of the International Conference on Computer Communication and Informatics, January 10-12, 2012, Coimbatore, India, pp: 1-6.
32. EMSCB., 2008. Towards trustworthy systems with open standards and trusted computing. European Multilaterally Secure Computing Base (EMSCB) Project. http://www.emscb.com/content/pages/opentc.htm
33. Tiwari, M., J.K. Oberg, X. Li, J. Valamehr and T. Levin *et al*., 2011. Crafting a usable microkernel, processor and I/O system with strict and provable information flow security. Proceedings of the 38th Annual International Symposium on Timothy Sherwood Computer Architecture, June 4-8, 2011, San Jose, CA., USA., pp: 189-199.
34. Kikuta, K., D. Ishii, S. Okamoto and N. Yamanaka, 2010. Point-to-multipoint VLAN path signaling demonstration on the GMPLS controlled Ethernet test network. Proceedings of the Conference on (OFC/NFOEC), Optical Fiber Communication (OFC), collocated National Fiber Optic Engineers Conference, March 21-25, 2010, San Diego, California, pp: 1-3.