American Journal of Computer Science and Information Engineering
2014; 1(2): 10-23
Published online November 20, 2014 (http://www.aascit.org/journal/ajcsie)

Keywords
Standards,
Architecture,
Security,
Models,
Evaluation,
VLAN,
Utilization,
Throughput

Received: October 10, 2014
Revised: October 28, 2014
Accepted: October 29, 2014

Online service computing using VLAN design architecture

Okafor Anthony Chinedu[1], Okafor Kennedy Chinedu[2], Ugwoke Fidelia Ndidi[3], Osuesu Blessing Obianuju[1], Ogbu Vincent Ikechukwu[4]

[1]Dept. of Electronics and Computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria
[2]Dept. of Electrical and Electronic Engineering, Federal University of Technology, Owerri, FUTO, Nigeria
[3]Dept. of Computer Science, Michael Okpara University of Agriculture, Umudike, Umuahia, Nigeria
[4]Dept. of Electrical and Electronic Engineering, Anambra State University, Uli, Anambra State, Nigeria

Email address

thoned2002@yahoo.co.uk (Okafor A. C.),arissyncline@yahoo.com(Okafor K. C.), ugwoke.ndidi@gmail.com(Ugwoke F. N.),1oby_grey@yahoo.com(OsuesuB. O.), ikechukwu_ogbu@yahoo.com (Ogbu V. I.)

Citation

Okafor Anthony Chinedu, Okafor Kennedy Chinedu, Ugwoke Fidelia Ndidi, Osuesu Blessing Obianuju, Ogbu Vincent Ikechukwu. Online Service Computing Using VLAN Design Architecture. *American Journal of Computer Science and Information Engineering.* Vol. 1, No. 2, 2014, pp. 10-23.

Abstract

For a good design, security trust in Online Service Computing can effectively improve the underlying design architecture. This paper reviewed various contributions for OSC in the context of existing web services architecture. Though various security models have been proposed in literature, we observed that online stores application integration on a Secured-tier VLAN offers an extended advantage over other schemes. In this regard, validating the overall online web architecture for optimality considering the secured-tier VLAN is the focus of this paper. A comparison as well as performance evaluation was carried out on OSC VLAN implementations yielding a satisfactory security measure on the part of end users, merchants and vendors, but showed no significant impact on the network utilization, throughput and queuing delays as similarity pattern was observed. We conclude that the security of OSC network can be improved through the logical isolation of users and the end servers in such designs. As such, a secured network with accepted performance metrics can drive any online application with little administrative overhead.

1. Introduction

In a distributed networked environment like the internet, data logic integration on the web constitutes a security challenge, because of the extreme heterogeneity of data sources involved, and the complexity of communication patterns which can arise [1].

In a typical e-commerce domain, the issue of security will always constitute enormous constraint for numerous users. This has prompted the need for a robust encryption algorithm that will protect the users and the administrators on a secured service network application. Whether exchanging financial, business or personal information, people want to know with whom they are communicating (authentication) and they wish to ensure that the information is neither modified (data integrity) nor disclosed (confidentiality) in transit [1]. Since, secure communication is an intrinsic requirement of today's world of on-line transactions, Secure Sockets Layer (SSL) protocol [2], SHH [3],

SET [4], HTTP [5], [6], TLS [7], etc are the most popular choice for achieving security goals on the web. For most online applications, on the application layer, SSL is trusted to secure transactions for sensitive applications ranging from web banking, to stock trading, to e-commerce, but unfortunately, the use of SSL imposes a significant performance penalty on web servers.

Again, in any computing environment that supports multiple processes such as OSC, 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 resource [8].

In the networking context, Intrusion Detection System (IDS), firewalls, routers etc can be used to enforcement policy for boundary separation considering the "inside" and "outside" worlds. But in this paper, we consider a somewhat different view of security integration for OSC environment as opined in [8] and [9].

For OSC environment, we cannot rely on the host operating systems and the e-commerce applications to enforce the desired resource allocation and access control policies, but by using VLAN integration so as to have complete control and trust at the edge of the network, a logical isolation implemented in the networking hardware, without making any changes to (or trusting) the hosts could further strength the system security.

To motivate this work, we provide two possible experimental domains. First, we consider the problem of attaching unlimited functional computers to the OSC without VLAN. In the second instance, we then considered an OSC VLAN design. Rather than assuming that the individual hosts are in need of protection by the network, our second scenario considers the case where the individual hosts are simply trusted by network administrator. With the review and evaluation studies of the proposed network context for OSC, this work seek to further encourage the use of VLAN for all forms of Online computing systems.

The rest of the paper is organized as follows. In Section II we provide an exhaustive literature review and the research gaps in the existing work. In Section III we state our proposed framework as part of the methodology. In Section IV, we describe the design principles for our OSC VLAN integration, which are the key component in our approach while detailing our implementation considerations. In Section V, we show the experiment results from our proof-of-concept prototype test bed and make the discussion according to experiment results. Finally in Section VII, we make a conclusion, showing a summary of achievements.

2. Related Works

In this section, we shall exhaustively review works comprising of online platforms and the VLAN contributions. This will facilitate the development and evaluation of our experimental scenarios.

The paper in [8], developed a new approach for customer to business owner transactions securely by implementing a novel 3 – Tier E-Commerce Management portal. This makes online business very flexible and secured on the part of business owners and customers. Their proposed system seeks to replace the conventional E-commerce models on the internet today using Secured Software Development Life Cycle (SSDLCM) on Ecommerce platform. Their security scheme aims at eradicating SQL injection possibilities as well as exploiting Software as a service in a dynamic Ecommerce domain. The work also developed a new encryption scheme based on XAMP MD5 Random Curve Cryptography (XMD5 – RCC) running on Secure Socket Layer (SSL) which protects the user and administrators on the Ecommerce platform.

The work in [9] developed a general purpose e-commerce store where any product (such as books, CDs, computers, mobile phones, electronic items, and home appliances) can be bought from the comfort of home through the Internet. The work defined an online store as a virtual store on the Internet where customers can browse the catalogue and select products of interest. We observed that the vulnerabilities in the design is very high.

The author in [10] explained that e-commerce operates as either business to customer (B2C) or business to business (B2B), but the model of discretionary access control model, Mandatory Access Control (MAC) model, Role-based Access Control (RBAC) model, and Access control Tasks/Workflow are used to analyze the access control functions [11]. By applying these models, designers can offer different features and describe the perspective from different points of view to understand, clarify and solve the security problems [10].

Trust Modelling in [12] showed that the trust level of an E-Commerce system is the summary of the contribution made by five events viz: the communication technology advances, social and commercial value awareness, cultural background and economical changes. In their work, the ERC2G Trust Model was used to show that the trust level can be dynamically measured as shown in figure 1.

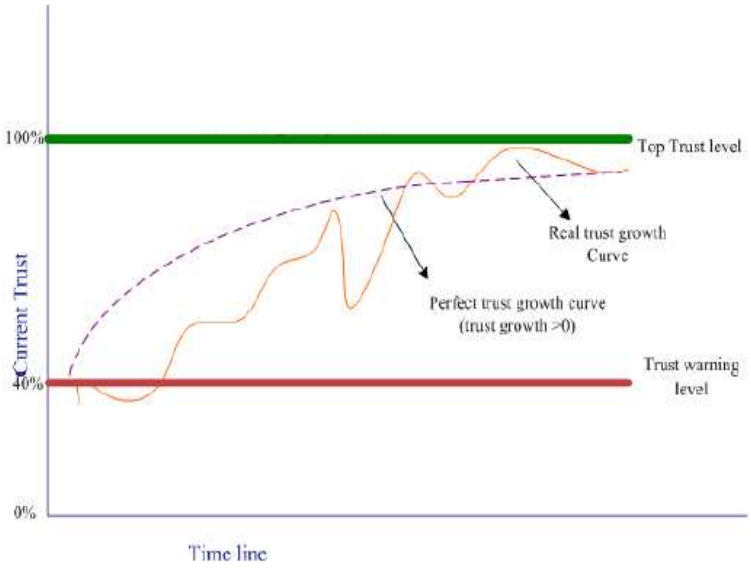

Figure 1. *Curves of trust level computed by ERC²G Trust Model [12]*

Several works have studied VLAN design in enterprise networks. The paper in [13], focused on infrastructure-based active mechanisms such as boundary firewalls adapted by private enterprise networks, to effectively filter malicious traffic from Internet. In their, architectural design, the S-VLAN setup comprise of user authentication at the network boundary, trusted edge switches, core switches and other edge switches. But the application interaction on the computing model was not discussed.

The authors in [14] presented S-VLAN performance evaluation using Congestion Management in DataCenter internet Network as a case study. Their work developed a stable candidate scheme for congestion control for Data centre Network (DCNs). The approach used is based on the measurement of QoS parameters with variation of load intensities alongside with the buffer sizes of the core switch. The S-VLAN scheme was able to control link utilisation by assigning tags to high priority end systems running different services, hence logically reducing the amount of queuing delay in the DCN networks as well as traffic overhead, thereby improving network performance for online applications.

The work in [15] made three contributions in a cost-benefit framework for enterprise network redesign by discussing a model to capture VLAN redesign costs while demonstrating the effectiveness of their approach using data obtained from a large-scale campus network. In their work, the considerations for VLAN redesign includes: the correctness criterion, resource constraints and VLAN performance criterion considering the broadcast traffic associated with a VLAN. This in turn depends on (i) the number of hosts in the VLAN; and (ii) the span of the VLAN, i.e., how spread out the hosts of the VLAN are in the underlying network topology.

The authors in [19] characterized VLAN usage in one operational network and expose several degenerate designs. The work in [20] shows the feasibility of adopting a systematic approach in the VLAN design of greenfield networks that are yet to be deployed. Other works include the use of traffic data [21],[22] to expose degenerate design patterns, understand VLAN traffic patterns, and correlate cross-layer faults. By contrast, this work focuses on designing systematic algorithms for automating common VLAN operational tasks.

Furthermore, the experience of designing and implementing the VLAN configuration toolkit, and the insight from its initial deployment are also unique. There also exists industry efforts like the Cisco VLAN Trunk Protocol [23] to manage VLANs, however such efforts are limited in functionality. For instance, VLANs that span multiple VTP domains still require manual configuration of trunk links. Our work complements these industry efforts by not only automating the trunk link configuration tasks for OSC applications, and also validating their effects and impact of the tasks.

Existing works made great efforts in discussing VLAN applications and its operational mechanisms but not in the context of Online Service computing and front end user interaction security. Online Service Computing using VLAN infrastructure has numerous advantages such as viz:

1 Redefining security integration
2 Ease management even though they are spread over physically disparate locations [16], [17].
3 Supports evolutions such as Software defined Networking SDN [18] according to its layers
4 Proper identification of individuals on the OSC platform from a remote server while restructuring the communication pattern between users and the servers.
5 Offers flexibility and low cost economy

2.1. Our Contributions

This research seeks to propose an OSC model that is very efficient with respect to network security application integration, service-oriented, and responsive to business needs, with rapid service delivery. In context, the security of

the proposed OSC network will be improved through a logical isolation of users and the backend severs simultaneously.

Again, this paper will investigate the feasibility of using the OSC VLAN to enforce these policies that will protect end users activities on the web platform. First, we describe an application-based secure VLAN architecture that can be used to completely secure a particular network service from unauthorized access, without making any changes to the hosts and requiring only minimal changes to existing standardized LAN components. Second, we present a case study to show how our approach can be applied to IP Telephony. Finally, we describe our experiences from a prototype implementation of the S-VLAN concept.

3. Methodology

3.1. OSC Framework

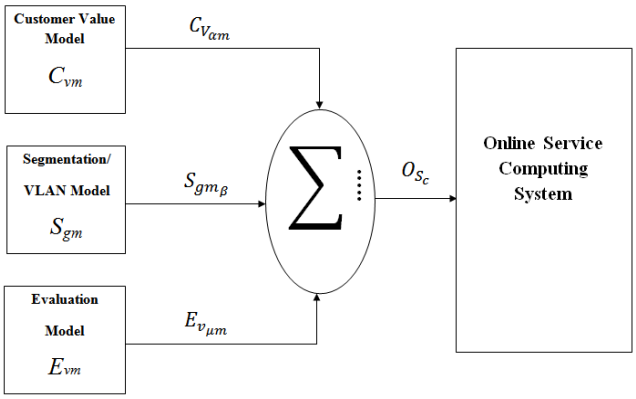

Figure 2. *Proposed Online Service Computing Model*

Figure 2 shows the Online Service Computing model. In our proposed model, when a business owner migrates the business template online, legitimate customers must login with their VLAN names and link IDs for the transaction to be consummated. The customer value model, the segmentation VLAN model on the network and the evaluation model constitutes the functional components that characterize the proposed OSC.

The OSC model equation could be represented as:

$$O_{S_c}=C_{V_{\alpha m}}+S_{gm_\beta}+E_{v_\mu m}. \quad (3.1)$$

where, $C_{V_{\alpha m}}, S_{gm_\beta}, E_{v_\mu m}$ are the combinations of several internal and external design models for the OSC.

From *Equ*.3.1, we shall only focus on the segmented VLAN model; $S_{gm_\beta,}$ This work will now discuss the OSC communication network platform with the VLAN controller leveraging *Equ*.3.1

3.2. OSC Communication Network Platform with VLAN Controller

This paper leveraged the underlying principles of VLAN mapping to further strengthen the security layout of the OSC platform discussed in this research. Figure 3 shows a proposed OSC VLAN layered architecture where the application web servers are tied to the end user VLAN tags. As such once a user registers into the application, the user is automatically logged to a unit VLAN, making the system to be secured. There could be W_{n+1} VLAN users on the VLAN switching controller mapped with the web server as shown in figure 3. In the next section, an OSC VLAN controller block and the scheduling architectural model is presented.

Figure 3 shows the proposed OSC VLAN architecture while figure 4 shows the flow algorithm of OSC scheduling of buffer for VLAN tagging while figure 5 shows the functional block diagram of the VLAN switching unit which controls the switch fabric unit S_f and the trunk traffic T_f. In the case of a packet popped from the input trunk buffer, the packet processing unit will check whether it is directed to a user within the ports of the same switch or it is directed to a user within ports of another switch.

In the first case, a tag remover unit will remove the tag information and checks the address of the destination user and the port location associated with this address will be taken from the lookup table. After that, the packet processing unit will apply the following algorithm:

a) If the packet is directed to a node within the same VLAN, then the processing unit will close the proper crossbar switch to forward the packet to the required destination output buffer.
b) If the packet is not within the same VLAN, the packet processing unit will add the tag information and direct it to the output trunk buffer. Figure 6 shows a detailed internal OSC VLAN architecture block diagram leveraged in this research.

The network system design for the OSC network is a distributed enterprise model with a core catalyst switch, based on the principles of separation of control and forwarding, and with the design goal to support heterogeneity of enterprise server modules within a single network system. These were implemented in

Resources are allocated in the backplane by setting up the VLANs` in a way that matches the anticipated traffic and its requirements. The VLAN information is stored in the forwarding tables in incoming forwarding elements (FEs), as part of the next-hop information. The IP forwarding table follows the submitted table valid host ranges for the user nodes. The derived IP subnet is mapped into the core VLAN switch backbone configured to optimize its general performance as shown in Appendix I, and II.

The main goals of OSC system security are confidentiality or secrecy, integrity, availability, accountability, and assurance. The goal of confidentiality is to ensure the information is not accessed by an unauthorized person. The goal of information integrity is to protect information from unauthorized modification. Information availability ensures the information is available when needed and is not made inaccessible by malicious data-denial activities. In our model, information accountability ensures that every action of an entity can be uniquely traced back to the entity while security assurance is the degree of confidence in the security of the

system with respect to predefined security goals. In the next chapter, the process model analysis and results are presented.

We shall now present the application tier of the OSC system.

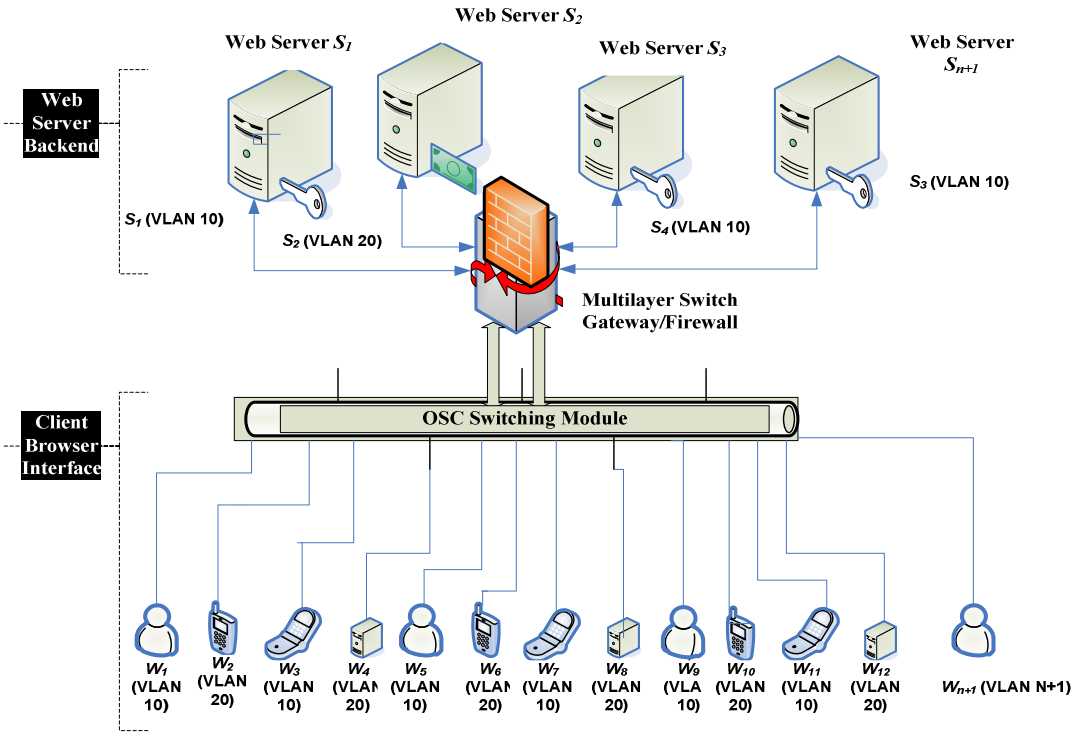

Figure 3. *A Proposed OSC VLAN layered Architecture*

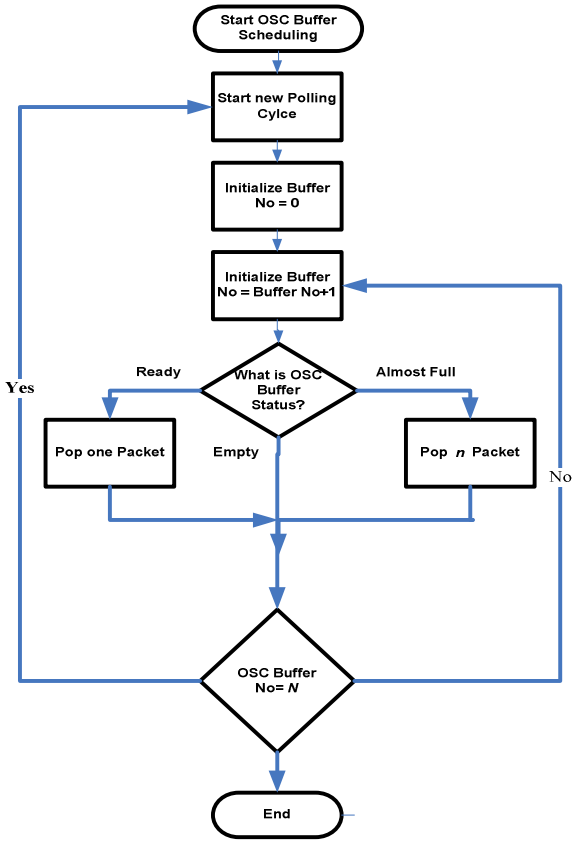

Figure 4. *A FlowChart of OSC Scheduler polling cycle.*

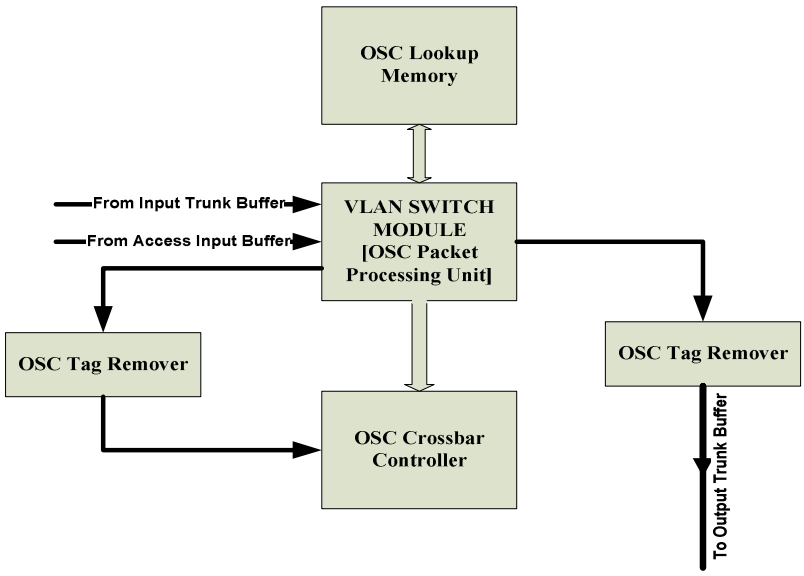

Figure 5. *VLAN Controller block diagram.*

3.3. OSC Flowchart Designs

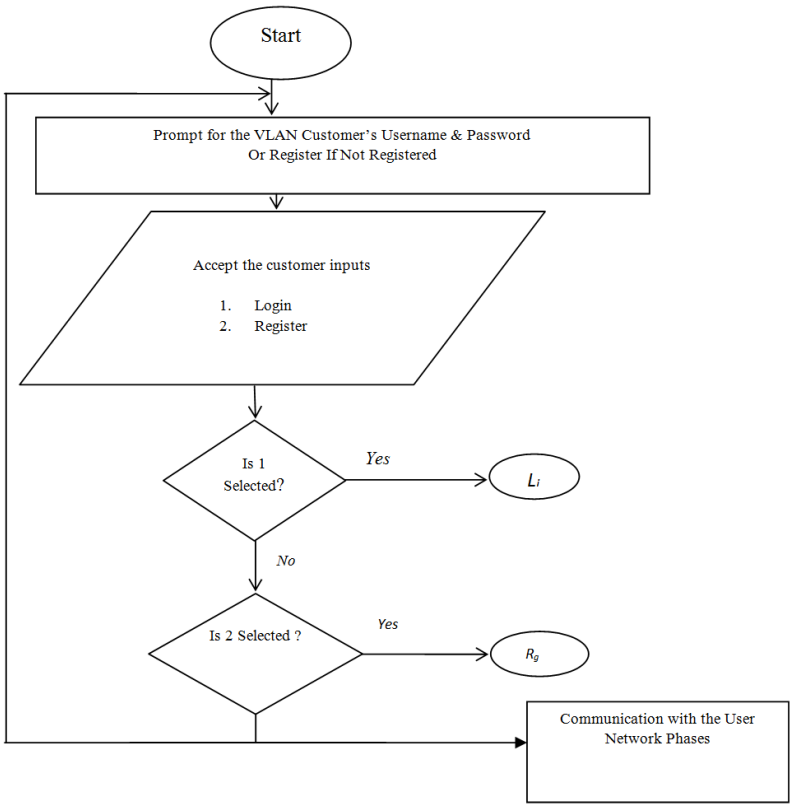

Figure 6. *OSC Portal (User Interface) with network Communication*

Figure 6 shows OSC user interface algorithm. The system accepts new registration or prompts for a new registration. Essentially, it is either a customer logs in or register before initiating any transaction on the OSC. In figure 7 and figure 8,the transaction completion based on VLAN id, billing and server processing is accomplished.

The VLAN backbone in this work considered the following network design issues: Loops traffic, Convergence, Broadcasts, Subnetworking, Security, and Media Dependence. Two factors were considered with regard to mixed-media scenario in this work. Firstly, the maximum transfer unit (MTU) differs for various network media. When VLANs media are switched, nodes must use the MTU specified for the scenario setup.. Secondly, because they operate at Layer 2 (data link layer), the OSC VLAN backbone must use a translation function to switch between dissimilar media types.

The translation function handles MAC and IP addresses as well as media format conversions. The maximum packet size used in this work is 1024bytes and the traffic metrics implemented in the VLAN backbone shown in Appendix I, II.

3.4. Network Model IP Assignment (192.168.10.0/29)

Considering figure 3 whose VLAN Controller block diagram is shown in Figure 5, there are two workgroups considered in this work for the OSC VLAN integration mapping. The corresponding valid host ranges were computed from Table 1, thus:

- Location A= VLAN10 on Subnet 0. (Host-Range = 192.168.10.1 ---192.168.10.8).
- Location B= VLAN20 on Subnet 8. (Host-Range=192.168.10.9 ---192.168.10.14).

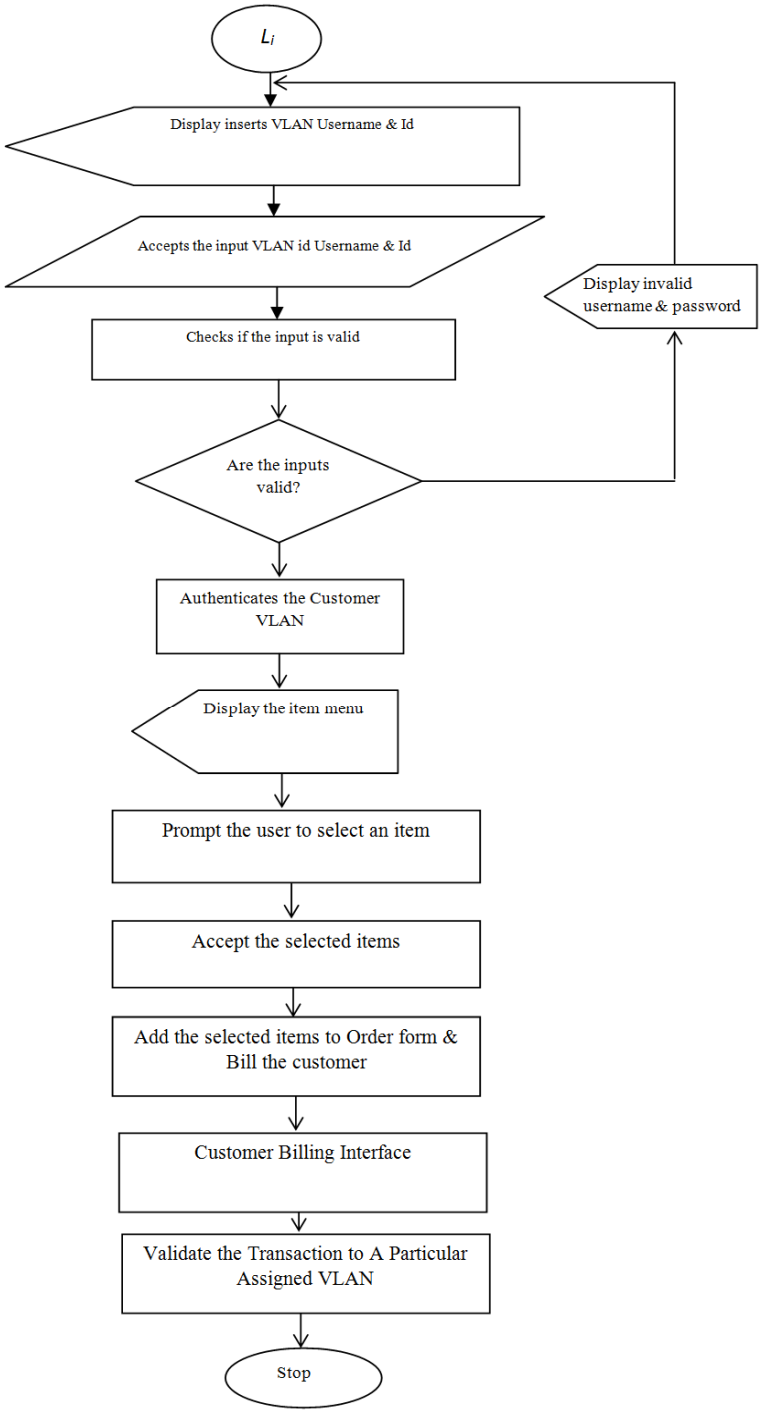

Figure 7. *OSC Portal (Login Interface)*

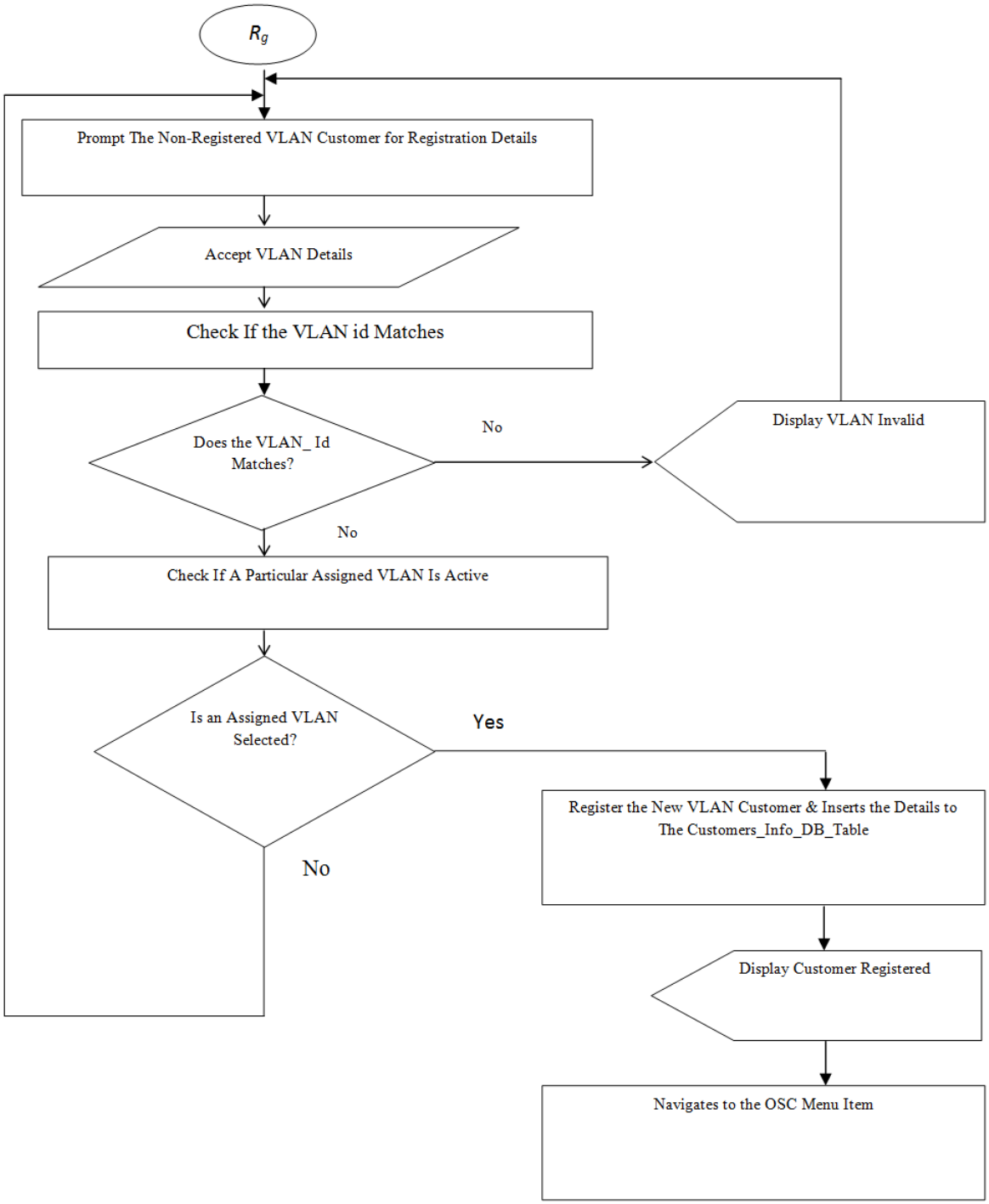

Figure 8. *OSC Portal (Registration Interface)*

Table 1. *Switch lookup table for OSC Synthesis VLAN table mapping.*

PORT INTERFACES	MAC ADDRESSES	VLAN LOCATONS/NAMES	VLAN PRIORITY TAG ID
Fa0/1, Gig/1,	Nil	Location A	10
Fa0/2,Fa0/3, Fa0/4, Fa0/5,	0010.1158.BCB7, 0002.160D.1A8E, 0060.2F80.8374, 0060.4735.BA61	Location-B	20
Fa0/6,Fa0/7, Fa0/8, Fa0/9,	0009.7C6A.8B1D, 0006.2ABB.E5CA, 0001.97A1.D537, 00D0.D33B.E204	Location-C	30
Fa0/10,Fa0/11, Fa0/12, Fa0/13	0007.ECB3.CC53, 0007.EC67.7D56, 00E0.B029.0625, 0006.2A2B.52E8	Location-D	40
Fa0/14,Fa0/15, Fa0/16, Fa0/17	0060.3EBA.11A9, 0000.0C2D.9548, 00E0.F7D6.BD0A, 0060.47D1.387A,	Location-E	50
Fa0/18,Fa0/19, Fa0/20, Fa0/21		Location-F	60

4. Implementation

As for the simulation testbed (Experimental Test Bed) used for the application network simulation, a generic template for running two network scenarios was developed using event driven OPNET tool, [6]. We implemented a proof-of-concept testbed for our application based Secure VLAN architecture design using the parameters in [24],[25]. We used linux computers to represent the end hosts, although any network devices could have been used. We used some Server PCs running Linux Mandrake 9.1, kernel 2.6.0 with bridging enabled and built-in layer 2 firewall support, to represent the trusted edge switches. We extended switches as a multilayer firewall and revised one of targets to do VLAN processing as described in table 1. We emulate a manually bootstrap process. The encryption algorithm used is advanced encryption standard as it is suitable for hardware implementation later on real switches. Of course, for real implementation, it would be better to use a commercial switch with reprogramming capability, such as the Nortel Passport 4000, in combination with hardware support for encryption/decryption at the ports. In the testbed, we used an Extreme Networks Summit 48i to represent the core network.

This is a high performance commercial switch with 48 ports and support for 802.1Q VLAN tagging. The impact of VLAN mapping on traffic workload in an OSC platform was investigated in the simulation study.

Now, the OSC VLAN offers high bandwidth optimization with low latency and consequent high throughput in a congested link. A star topology was used in the model with the *N* VLANs assigned to end system/workgroups locations as shown in figure 3. The simulation deals with two different cases; the first one is devoted to the case in which all the workstations (nodes) are connected to VLAN 10 , the second case defines VLAN 20 membership (by port and MAC), Also, only VLAN tag 10 and 20 was assigned to the OSC servers. Figure 9 shows the network setup with 7 loads (for scenario-I) where the following metrics were studied- Utililization, Throughput and queuing delay for the OSC http traffic. The traffic data for figures 9 to figure 12 is shown in appendix I for a seven load points.

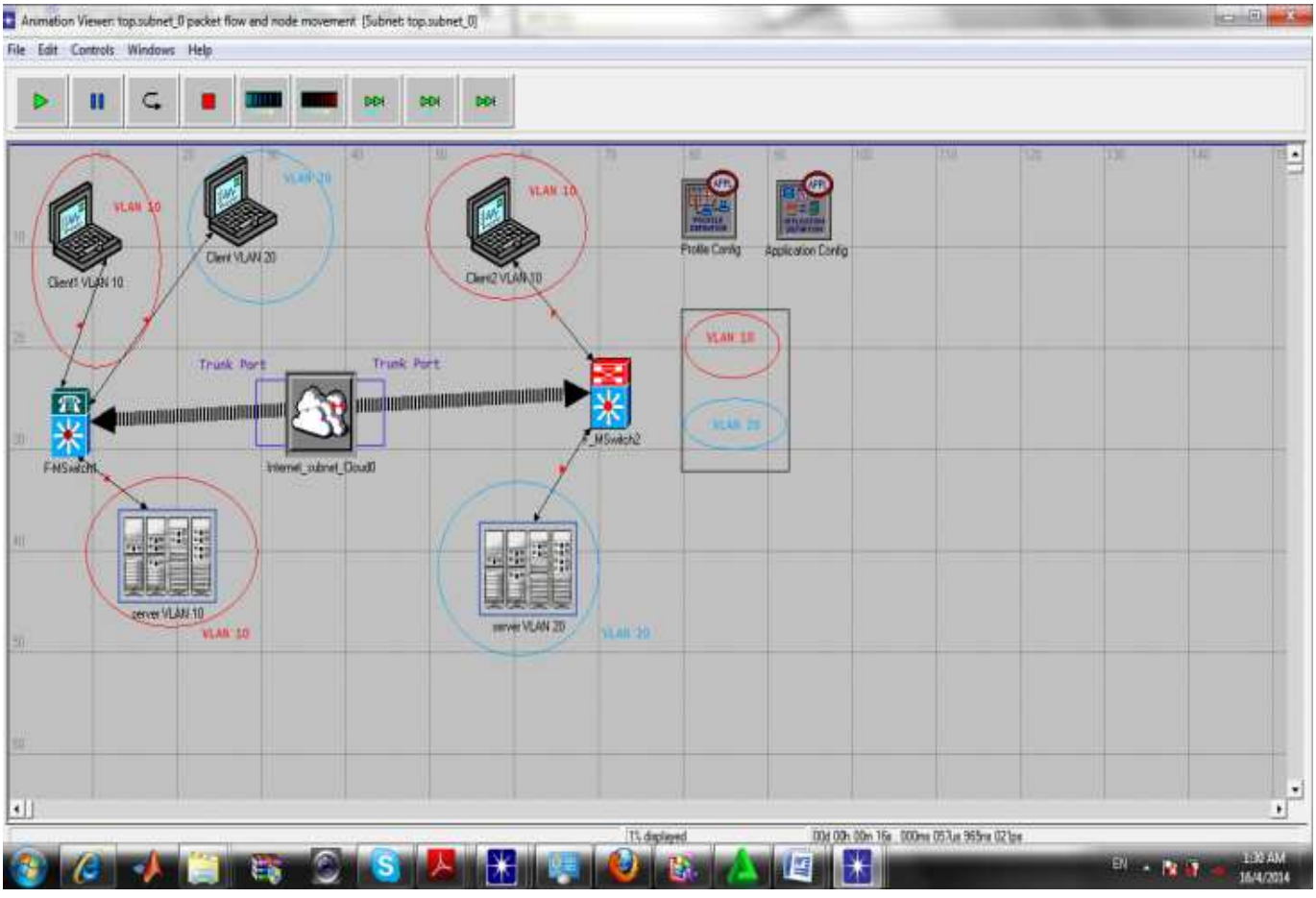

Figure 9. *OSC VLAN simulation with 7 loads (scenario-I)*

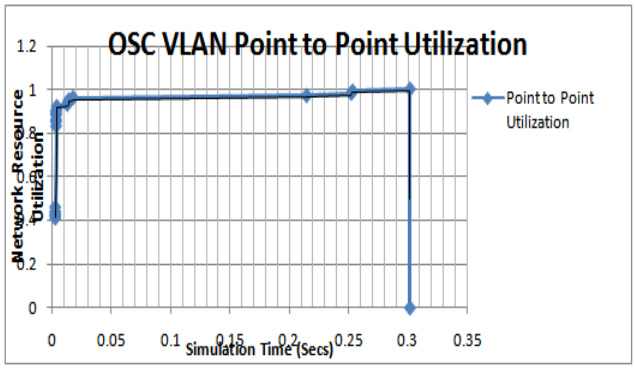

Figure 10. *OSC VLAN Network resource Utilization with 7 loads*

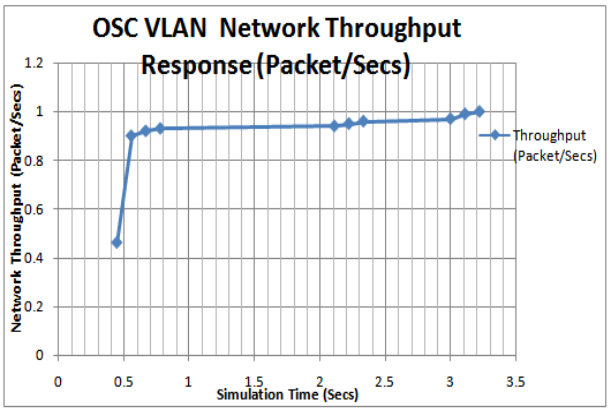

Figure 11a. *OSC VLAN Network Throughput response with 7 loads (packet/secs)*

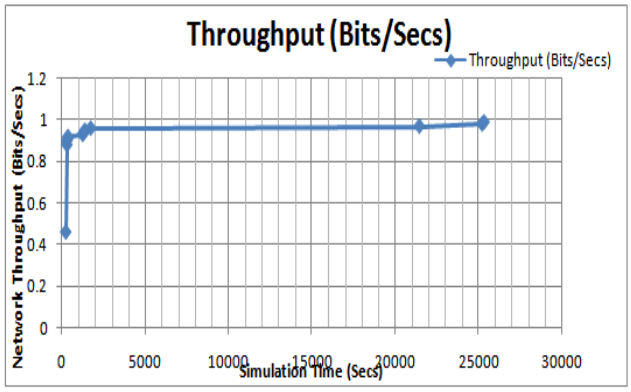

Figure 11b. *OSC VLAN Network Throughput response with 7 loads (Bits/secs)*

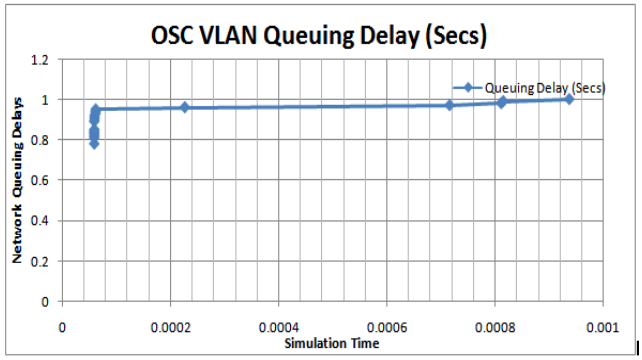

Figure 12. *OSC VLAN Network Queuing delay response with 7 loads (packet/secs)*

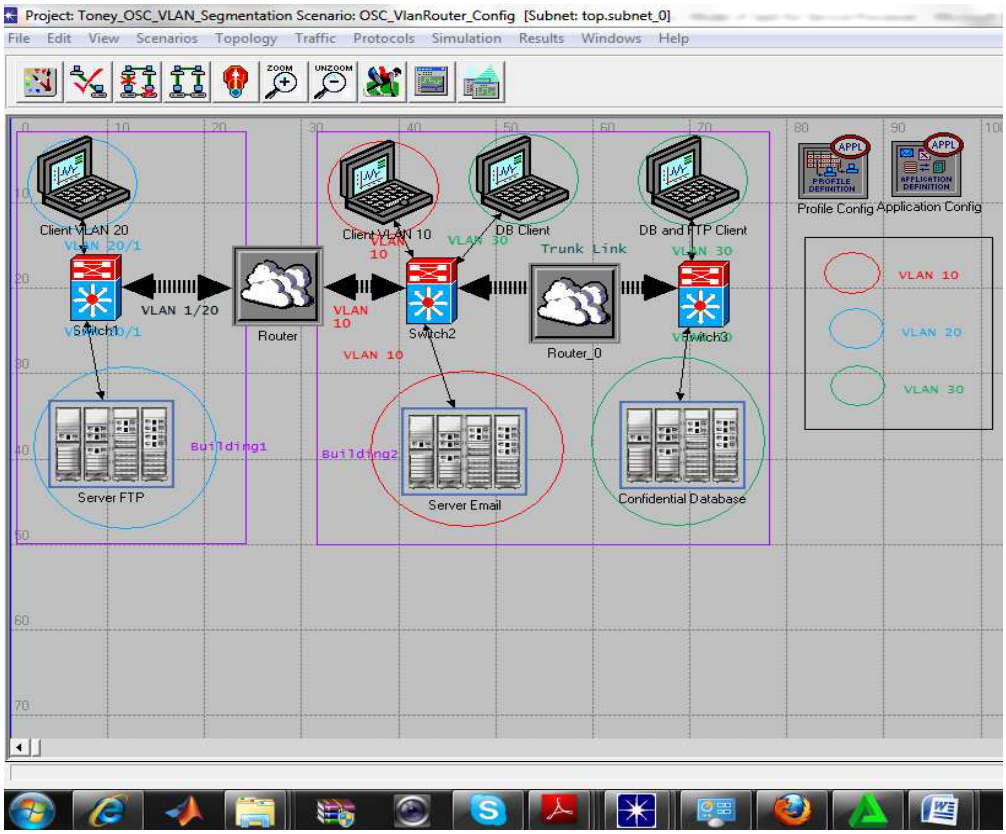

Figure 13. *OSC VLAN setup with 10 loads*

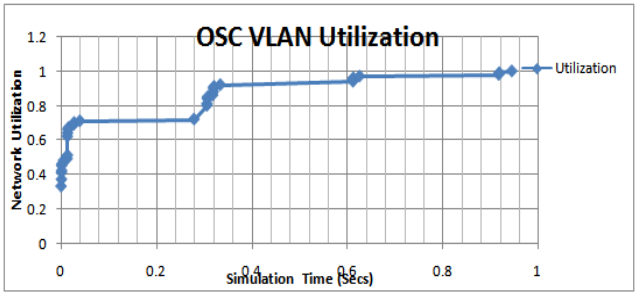

Figure 14. *A Plot of OSC VLAN Utilization setup response with 10 loads*

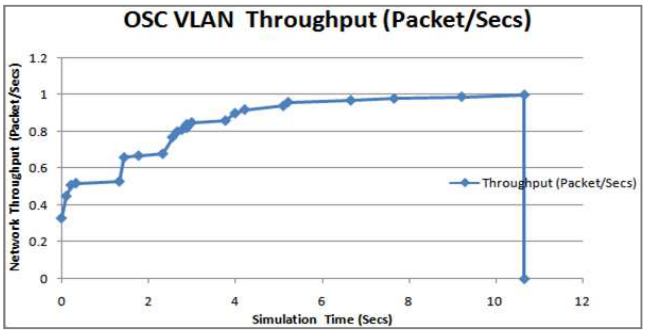

Figure 15a. *A Plot of OSC VLAN Throughput setup response (Packet/Secs) with 10 loads*

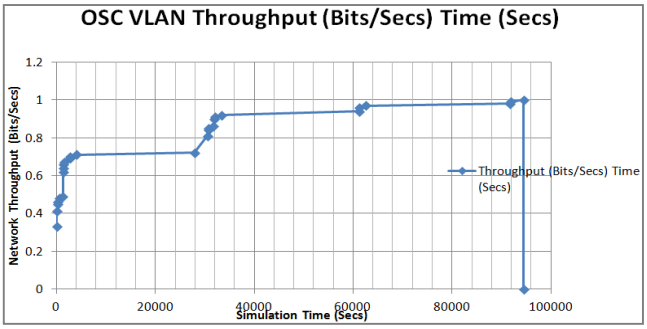

Figure 15b. *A Plot of OSC VLAN Throughput setup response (Bits/Secs) with 10 loads*

Appendix II shows the OSC VLAN (Scenario-II) ie second scenario where an investigation on the performance metrics of Utililization, Throughput and queuing delay for the OSC http traffic was carried out. Figure 13 shows the OSC VLAN setup with 10 loads.

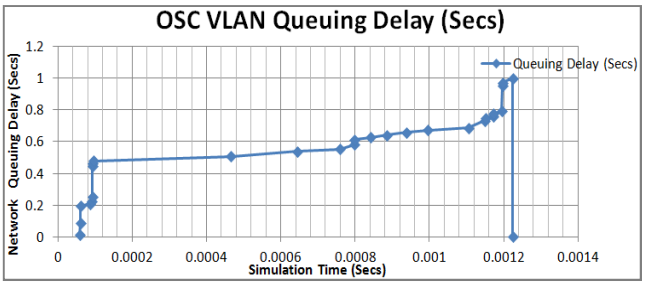

Figure 16. *A Plot of OSC VLAN queuing delay setup response (Packet/Secs) with 10 loads*

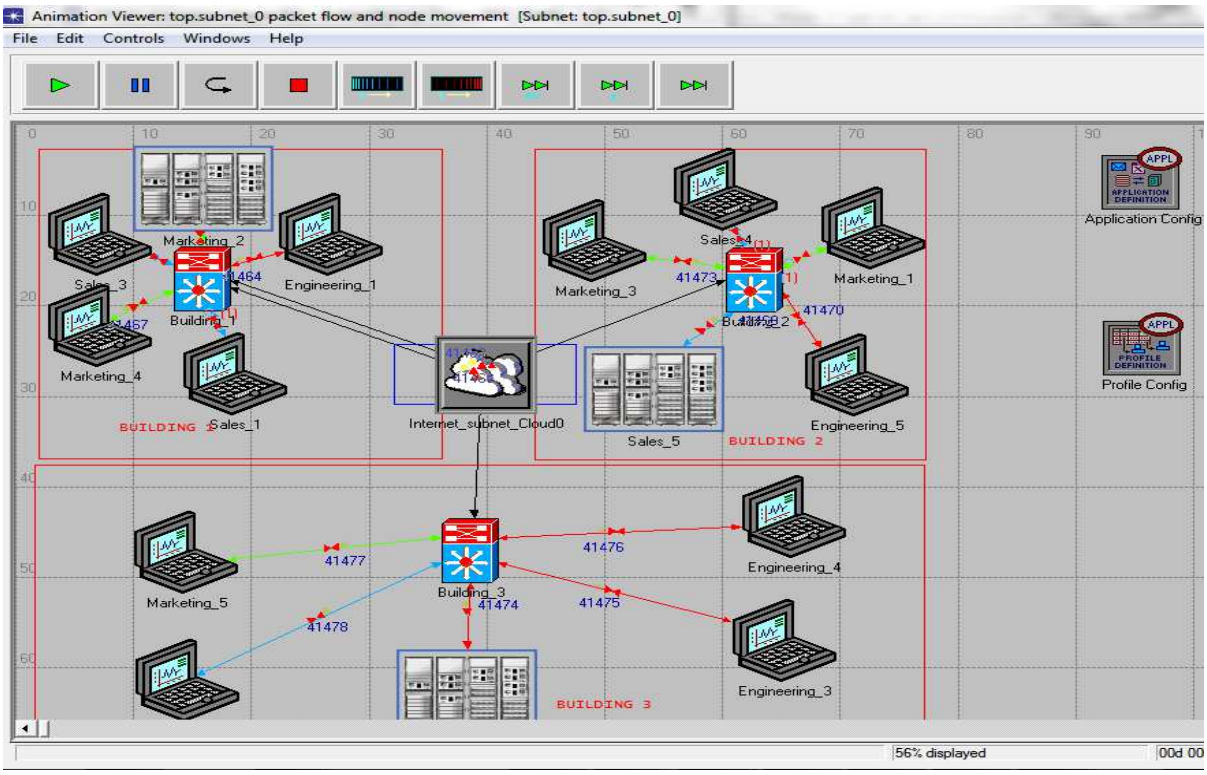

Figure 17. *Network simulation for OSC No VLAN setup with 17 loads (Scenario-II).*

Appendix II shows the OSC No VLAN (Scenario-II) i.e. second scenario where an investigation on the performance metrics of Utililization, Throughput and queuing delay for the OSC http traffic was carried out. Figure 17 shows OSC scenario for No VLAN setup with 17 loads. This resulted in figures 18a to figure 18c for the selected metrics

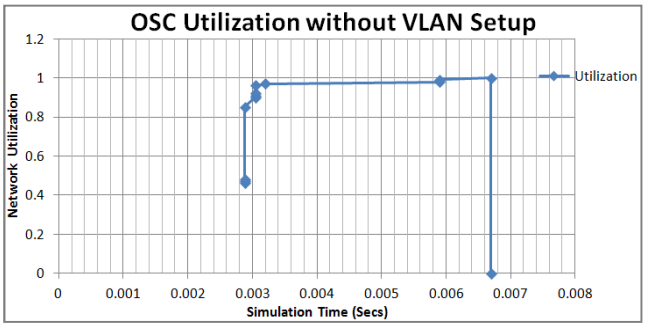

Figure 18a. *Plot OSC No VLAN setup Utilization with 17 loads.*

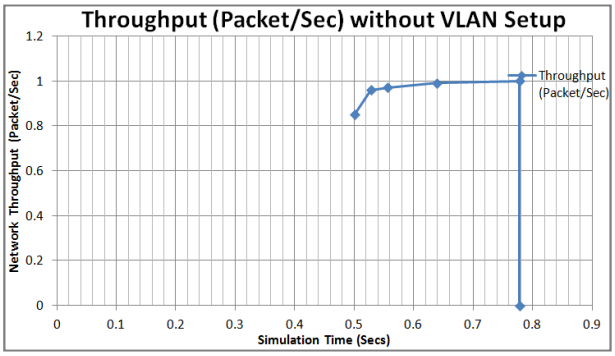

Figure 18b. *A Plot OSC No VLAN setup Throughput (packets/Sec) with 17 loads*

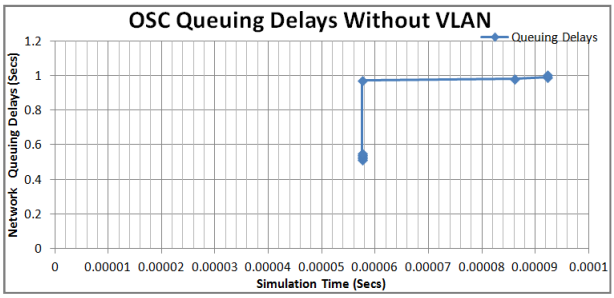

Figure 18c. *A Plot OSC No VLAN setup Queuing delays with 17 loads*

5. Analysis of Results

The simulation was run for several times while keeping other parameters constant in the first two cases while varying VLAN and the load intensities for different packet generation rates (arrival rates). Figure 9 to figure 16 shows that OSC with VLAN segmentation for the both the users and the application servers have no significant impact on the traffic performance metrics, but rather offers a robust point to point security layout for the terminal devices and users. Considering the various VLAN loads intensities, the maximum utilization, throughput and queuing is similarly same. As shown in figure 13, the OSC VLAN was observed to significantly regulate broadcasts and improve security mapping i.e. it accurately handles traffic segmentation as shown in figure 3. With increase in load intensities, bandwidth optimization on the core switch is maintained by VLAN generally.

From the simulated testbed, the FIFO Queues of figure 4, holds packets based on service policy of VLAN, hence the switch is capable of determining the number of bits in each of the incoming buffers at the beginning of service of each packet arrival.

6. Conclusion and Summary of Achievements

In this research work, we had presented an online service computing system for e-commerce transactions while showing the feasibility of encouraging business owners to migrate their businesses online via a simulation evaluation. This research has shown the network architecture for supporting OSC systems and has verified that OSC VLAN can improve the overall system security but does not affect the performance quality. A generic mathematical model for customer value chain, logical isolation and performance evaluation were some of the key design attributes of our model. Using the experimental test data gathered from our experimental testbed, we simulated an OSC network scenario using heavy http traffic with OPNET IT guru while comparing the results in the context of utilization, throughput and queuing delays for loads on the network. As such a case for VLAN and NO VLAN scenarios were studied (See Appendixes I, and II). Our discovery showed that OSC VLAN model under heavy traffic achieves good security isolation compared with the case with No VLAN mapping on the network setup. The results of simulation showed that networks for e-commerce services with VLANs will handle web application integration efficiently.

In summary, we have designed an application-based secure VLAN architecture and implemented a prototype system. Our application based VLAN architecture (OSC) is suitable for hotspots, university and enterprises LANs and can efficiently prevent inside security problems from interrupting secured applications. Our Application based Secure VLAN (SVLAN) is simpler and more efficient than IPSec in LAN environment as it conforms to Layer 2 semantics, and it is cost effective to real-time applications such as VoIP.

Our future work includes implement the real A VLAN architecture in commercial programmable switches and move crypto algorithms to be implemented by hardware to achieve wire-speed performance.

Appendix I. OSC VLAN (Scenario-1)

Time (Secs)	OSC VLAN Senario-1						
	Point to Point Utilization	Time (P/S)	Time (B/S)	Throughput (Packet/Secs)	Throughput (Bits/Secs)	Time (Secs)	Queuing Delay (Secs)
0.00256	0.41	0.444444444	256	0.46	0.46	0.0000576	0.78
0.00256	0.42	0.555555556	320	0.9	0.88	0.0000576	0.81
0.00256	0.43	0.666666667	323.5555556	0.92	0.9	0.0000576	0.82
0.00256	0.44	0.777777778	384	0.93	0.91	0.0000576	0.83
0.00256	0.46	2.111111111	387.5555556	0.94	0.92	0.0000576	0.84
0.0032	0.83	2.222222222	1267.555556	0.95	0.93	0.0000576	0.85
0.0032	0.85	2.333333333	1338.666667	0.96	0.94	0.0000576	0.89
0.0032	0.86	3.000000000	1402.666667	0.97	0.95	5.81333E-05	0.9
0.0032	0.88	3.111111111	1751.111111	0.99	0.96	0.00005824	0.91
0.003235556	0.89	3.222222222	21455.11111	1.00	0.97	0.00005824	0.92
0.003235556	0.9	3.222222222	25216.88889	0.00	0.98	6.00421E-05	0.93
0.00384	0.91	3.222222222	25337.77778	0.00	0.99	6.01143E-05	0.94
0.003875556	0.92	3.222222222	30178.66667	0.00	1.00	0.00006024	0.95
0.012675556	0.93	3.222222222	30178.66667	0.00	0.00	0.000225143	0.96
0.013386667	0.94	3.222222222	30178.66667	0.00	0.00	0.00071517	0.97
0.014026667	0.95	3.222222222	30178.66667	0.00	0.00	0.000810543	0.98
0.017511111	0.96	3.222222222	30178.66667	0.00	0.00	0.000814429	0.99
0.214551111	0.97	3.222222222	30178.66667	0.00	0.00	0.000936579	1
0.252168889	0.98	3.222222222	30178.66667	0.00	0.00	0.000936579	0
0.253377778	0.99	3.222222222	30178.66667	0.00	0.00	0.000936579	0
0.301786667	1.00	3.222222222	30178.66667	0.00	0.00	0.000936579	0
0.301786667	0.00	3.222222222	30178.66667	0.00	0.00	0.000936579	0

Appendix II. OSC NO VLAN (Scenario-3)

Time (Secs)	Utilization	Time (P/S)	Throughput (Packet/Sec)	Time (B/S)	Throughput (Bits/Sec)	Time (Secs)	Queuing Delays
0.00288	0.46	0.5	0.85	288	0.85	0.0000576	0.51
0.00288	0.47	0.527777778	0.96	304	0.96	0.0000576	0.52
0.00288	0.48	0.555555556	0.97	320	0.97	0.0000576	0.53
0.00288	0.85	0.638888889	0.99	589.333333	0.99	0.0000576	0.54
0.00304	0.9	0.777777778	1	669.333333	1	0.0000576	0.55
0.00304	0.91	0.777777778	0	669.333333	0	0.0000576	0.97
0.00304	0.92	0.777777778	0	669.333333	0	8.60571E-05	0.98
0.00304	0.96	0.777777778	0	669.333333	0	9.22435E-05	0.99
0.0032	0.97	0.777777778	0	669.333333	0	9.22435E-05	1
0.005893333	0.98	0.777777778	0	669.333333	0	9.22435E-05	0
0.005893333	0.99	0.777777778	0	669.333333	0	9.22435E-05	0
0.006693333	1	0.777777778	0	669.333333	0	9.22435E-05	0

References

[1] Okafor, Anthony, Chinedu, "A Model for Online Service Process Computing; A Case for VLAN Online Shop Integration", M.Sc Thesis, Department of Electrical and Electronic Engineering, Nnamdi Azikiwe University, Awka, Unpublished, 2014

[2] A. Frier, P. Karlton and P. Kocher, "The SSL3.0 Protocol Version 3.0", Available Online: http://home.netscape.com/eng/ssl3/

[3] T. Ylonen, T. Kivinen, M. Saarinen, T. Rinne, S. Lehtinen "SSH Protocol Architecture", IETF Internet draft, work in progress, Jul. 2003.

[4] MasterCard International and Visa International, "Secure Electronic Transaction Specification, Version 1.0", http://www.setco.org/, May 1997.

[5] R. Fielding et al., "Hypertext Transfer Protocol –HTTP/1.1", RFC 2616, Jun. 1999.

[6] D. Wagner, B. Schneier, "Analysis of the SSL 3.0 protocol", 2nd USENIX Workshop on Electronic Commerce, Nov. 1996.

[7] C. Coarfa, P. Druschel, D. Wallach, "Performance Analysis of TLS Web Servers", Network and Distributed Systems Security Symposium '02, San Diego, California, Feb. 2002.

[8] Okafor Nneka I.,Okafor K.C, Ugwoke F. N, Udeze,C.C "3-Tier E-ComP: *A Novel E-Commerce Management Portal Based on Secured SDLC Approach*", Computing, Information Systems, Development Informatics & Allied Research Vol. 4 No. 4 December, 2013, Pp.1-11

[9] Swapna Kodali, "The Design and Implementation of an E-Commerce Site For Online Book Sales", M.Sc thesis for the Department of Computer and Information Sciences, Indiana University South Bend, May 2007

[10] Han Zhang, "A Formal Security Modeling and Analysis in B2B e-commerce, A thesis submitted in partial fulfillment of the requirements of Doctor of Philosophy in Computer Science, University of Auckland July 2006,

[11] James Joshi, Walid G. Aref, Arif Ghafoor, and Eugene H. Spafford. Security models for web-based applications. Commun. ACM, 44(2):38–44, 2001.

[12] Zhongwei Zhang and Zhen Wang, "Assessing and Assuring Trust in E-Commerce Systems",

[13] Minli Zhu, Mart Molle, "Design and Implementation of Application-based Secure VLAN",

[14] Okafor K.C and Dr. T.A Nwaodo: " A Synthesis VLAN Approach to Congestion Management in Datacenter internet Networks", International Journal of Electronics and Telecommunication System Research, Volume 5, Number 6, May 2012 pp. 86 – 92, electroscopejournal.org/wa6.php or www.electroscopejournal.org.ng/j11t6.html.

[15] Xin Sun and Sanjay G. Rao, "A Cost-Benefit Framework for Judicious Enterprise Network Redesign", In Proc. IEEE INFOCOM, 2011.pp.216-220

[16] P. Garimella, Y.-W. E. Sung, N. Zhang, and S. Rao. Characterizing VLAN usage in an operational network. In *ACM SIGCOMM workshop on Internet Network Management (INM'07), Kyoto, Japan*, 2007.

[17] S. K. Sadhukhan and D. Saha. Auditing campus-wide local area networks (LANs) for Virtual LAN configurations using a simple network manager. Technical report, Indian Institute of Management (IIM).

[18] Okafor, K.C, Achumba I,Ezeh G.N,Diala, U.H, " OpenFlow Virtual Appliance: An Efficient Security Interface For Cloud Forensic Spyware Robot", (Accepted)

[19] P. Garimella, Y.-W. E. Sung, N. Zhang, and S. Rao. Characterizing VLAN usage in an operational network. In *ACM SIGCOMM workshop on Internet Network Management (INM'07), Kyoto, Japan*, 2007.

[20] Y.-W. E. Sung, S. G. Rao, G. G. Xie, and D. A. Maltz. Towards systematic design of enterprise networks. In *Proc. of the ACM CoNEXT Conference*, 2008.

[21] A. Mansy, M. B. Tariq, N. Feamster, and M. Ammar. Measuring VLAN-induced dependencies on a campus network. In *Proc. ACM SIGCOMM IMC*, 2009

[22] K. Sripanidkulchai, C. Issariyapat, and K. Meesublak. Inference of network-wide VLAN usage in small enterprise networks. In *Proc. of IEEE Workshop on Automated Network Management*, 2008.

[23] Cisco. Understanding vlan trunk protocol (VTP). Online: document.http://www.cisco.com/application/pdf/paws/10558/21.pdf, 2007

[24] Udeze C.C., Okafor K.C, C.C.Okezie, Okeke O., "Performance Evaluation of Openflow VLAN Strategy in DataCenter Switched Ethernet, African Journal of Computing & ICT, IEEE. Vol 6. No 2. September 2013. pp 63-72. Online: http://www.ajocict.net.

[25] C.C. Okezie, Okafor K.C, Udeze C.C "*Open Flow Virtualization: a Declarative Infrastructure Optimization Scheme for High Performance Computing" Academic Research International,* Vol.4, Number 4, July 2013, Pp. 232-244

[26] *Riverbed Modeler Academic Edition* release17.5 PL6.*https://splash.riverbed.com/.../riverbed-modeler-academic-edition-release, June 11, 2014*