International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Design and Simulation of Secure Network for University Campus

Mon Mon Aye[1], Zar Chi Soe[2]

[1]Lecturer, Department of Electronic Engineering, Pyay Technological University, bago, Myanmar
[2]Lecturer, Department of Electronic Engineering, Technological University, Hinthata Myanmar

How to cite this paper: Mon Mon Aye | Zar Chi Soe "Design and Simulation of Secure Network for University Campus" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.1023-1027, **https://doi.org/10.31142/ijtsrd26568**

IJTSRD26568

ABSTRACT

Today's wireless network has come to stay as an essential tool of communication in education sector. These sectors have started deploying computers to perform their daily work such as studying and learning and access resources from their network. This technology has enabled to learn much faster and more conveniently. There are some problems still faced by the users such as poor network design by having large broadcast within the network and various security attacks. These problems can be solved by implementing VLAN (Virtual Local Area Network), PS (Port Security in switches) and ACL (Access Control List). They have been simulated in packet tracer 6.3 software.

KEYWORDS: *Education sector, Virtual Local Area Network, Port security, Access Control List*

I. INTRODUCTION

Network security is the process that information assets are protected [1]. Education sector network is set of virtual local area networks (VLAN), which are virtual divided for increasing the performance of network and increases campus network management with security. ACL is a set of commands grouped together to filter the traffic that enters and leaves the interface.

A. Virtual Local Area Network

VLAN is a logical partition of a layer 2 network. Multiple partitions can be created allowing for multiple VLANs to co-exist.

Each VLAN is a broadcast domain, usually with its own IP network. This technology is used to segment a complex network into smaller networks for better manageability, improved performance and security.

Implementing VLAN for any network will achieve the following benefits:

- Easily relocate PCs on LAN (Local Area Network)
- Easily modify configuration
- Easily add or remove hosts to or from the LAN
- Easily control network traffic between the LAN
- Improve network security
- Reduce the cost
- Easily manage the network administrations [6].

B. Port Security

Port security limits the number of valid Media Access Control (MAC) addresses allowed on a port. The MAC addresses of legitimate devices are allowed access, while other MAC addresses are denied. Any additional attempts to connect by unknown MAC addresses generate a security violation.

Follow these guidelines when port security configures:

- A secure port cannot be a trunk port.
- A secure port cannot be a destination port for Switch Port Analyzer.
- A secure port cannot belong to an Ether Channel port-channel interface.
- A secure port and static MAC address configuration are mutually exclusive.

C. Access Control List

ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface. It is a table that tells a computer operating system which gives access rights for each user to a particular system object. ACL can be used to prevent some packets flow through the network.

Implementing ACL will achieve the following:

- Prevent unwanted traffic in the network
- Protect critical devices existing in the network
- Prevent users from using systems [6].

II. VLAN IMPLEMENTATION

The requirements for new design are Cisco layer 2 switches and layer three devices to carry out the new setup. The organization need to purchase the managed switch which supports the VLAN interface. VLAN should be membership by using port number. All ports or interfaces in the switch are considered in one VLAN and one broadcast domain. The solution for this problem is by configuring VLAN in the switches and to put some ports into one broadcast domain and some into another broadcast within the same switch. So, this will segment hosts into smaller LAN to reduce overhead caused to each device. Administrator has created VLAN for each department then enabled the communication between

them by using layer three devices. Each switch can carry more than one VLAN as shown in Fig. 1. This network design has a total number of eight VLANs. The hosts in the same VLAN are able to communicate with each other but hosts from different VLANs are not. To achieve full connectivity, the router is connected. The router had one of its interface connected to the main switch and the other to the switch connected server firm representing DNS and Web. Each of them has its default gateway. Each VLAN can assign to each department according to the organization requirements shown in Table 1.

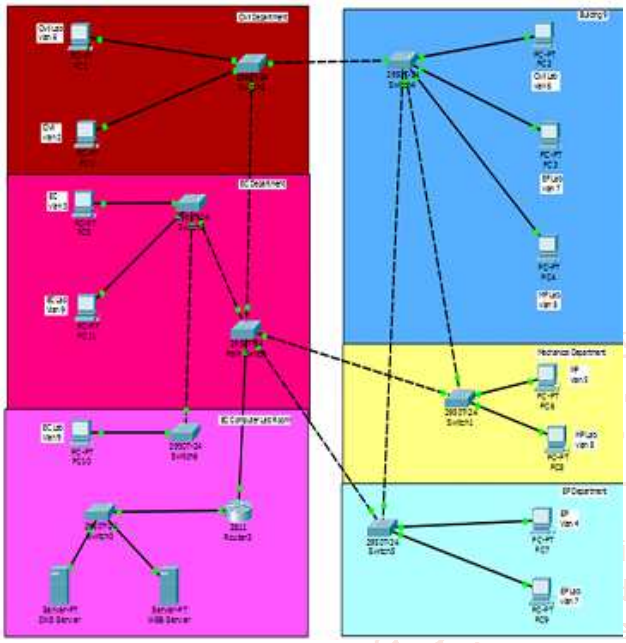

Figure1. Implementation of VLAN

Table1. Assigning Switch Port to VLANs

VLAN, Device, Interface	IP Address	Subnet Mask
VLAN 2(Civil Dep)	192.168.2.0	255.255.255.0
VLAN 3(EC Dep)	192.168.3.0	255.255.255.0
VLAN 4(EP Dep)	192.168.4.0	255.255.255.0
VLAN 5(MP Dep)	192.168.5.0	255.255.255.0
VLAN 6(Civil Lab)	192.168.6.0	255.255.255.0
VLAN 7(EC Lab)	192.168.7.0	255.255.255.0
VLAN 8(EP Lab)	192.168.8.0	255.255.255.0
VLAN 9(MP Lab)	192.168.9.0	255.255.255.0
Fa0/0.2	192.168.2.1	255.255.255.0
Fa0/0.3	192.168.3.1	255.255.255.0
Fa0/0.4	192.168.4.1	255.255.255.0
Fa0/0.5	192.168.5.1	255.255.255.0
DNS Server	192.168.10.2	255.255.255.0
Web Server	192.168.10.3	255.255.255.0
Ethernet1/0	192.168.10.1	255.255.255.0

III. VLAN CONFIGURATION

First of all, four VLANs are created on main switch and named. Fig. 2 shows commands for VLAN. In this section will be configured in access mode to all the interfaces of the switches that are connected to end devices such as computers and will be allowed the access of a single VLAN per interface. Fig. 3 shows the switch port command.

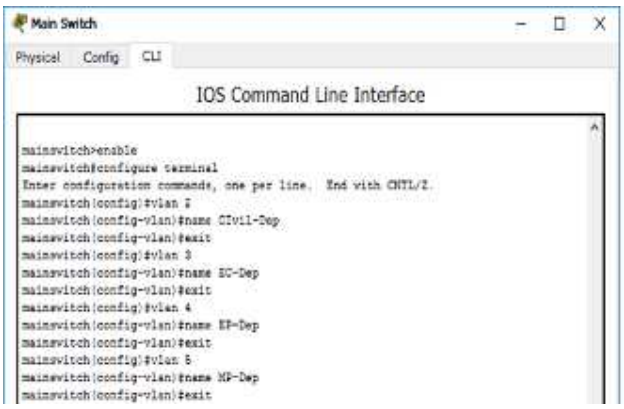

Figure2. Creating VLAN in Main Switch

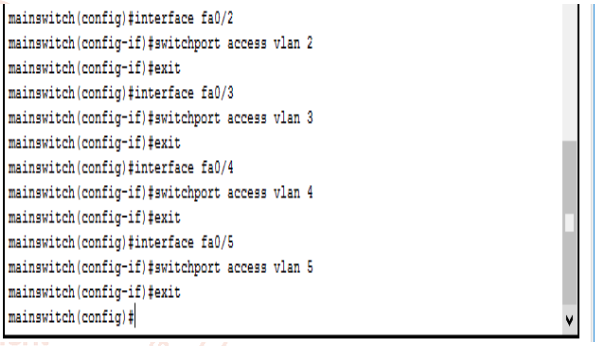

Figure3. Assigning Ports in Main Switch

After all configuration of the network design is complete, it is time to test all network connections are already successfully connected by typing ping the destination IP address in the Command Prompt window.

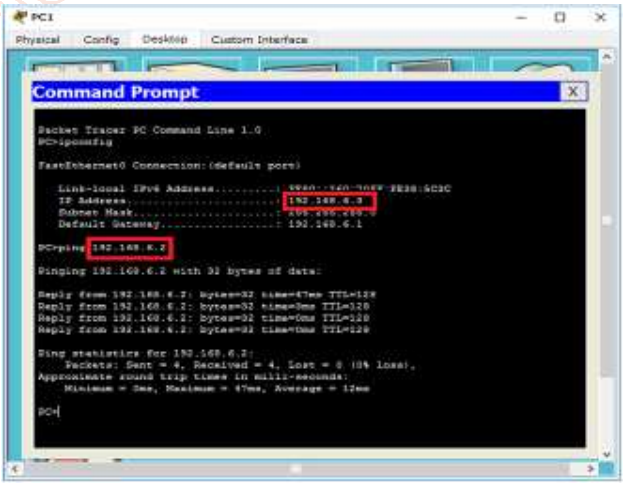

Figure4. Testing for Same VLAN

If after pinging, it says Reply from destination IP address then the network has been successfully connected. To verify, the computers that are in the same VLAN have communication. A ping test will be done. Fig. 4 is the result for same VLAN from PC1 to PC2 in the VLAN 6.

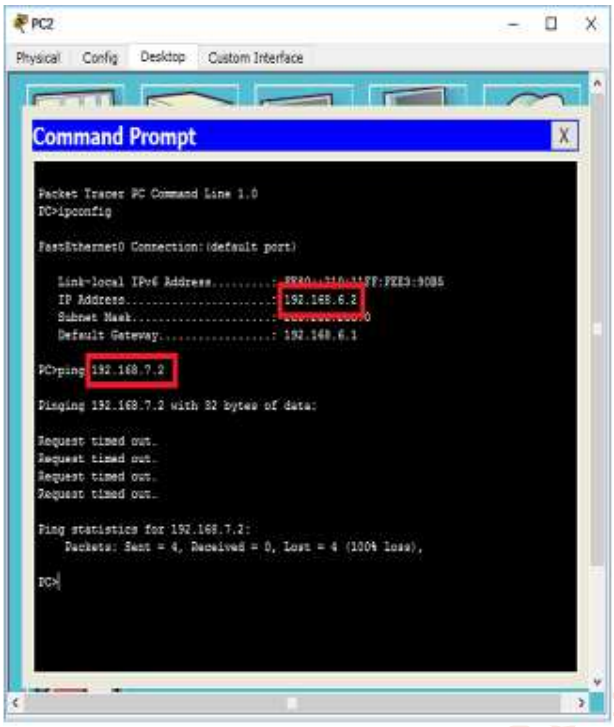

Figure5. Testing for Different VLANs

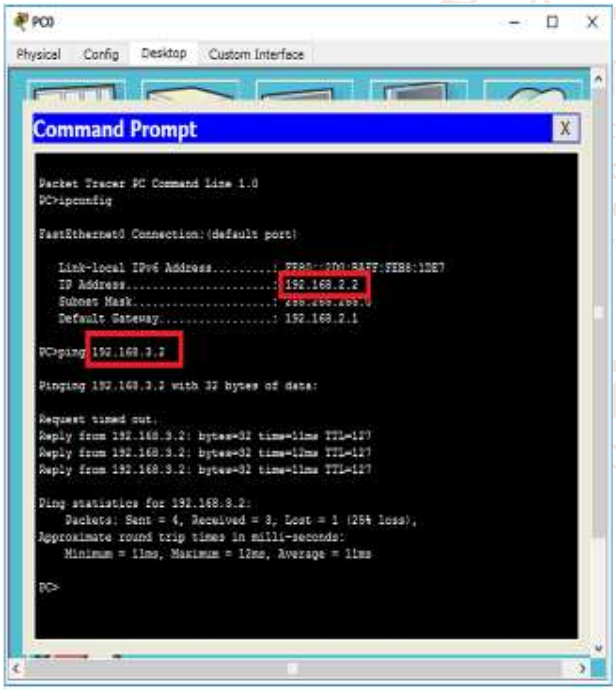

Figure6. Testing for Inter VLANs

Fig. 5 is the result that test in different VLANs which is from VLAN 6 to VLAN 7. Fig. 6 is the result of the inter VLAN from Civil Department to EC Department. It is the testing from VLAN 2 to VLAN 3.

IV. PS IMPLEMENTATION AND TESTING

All switches can be secured by not allowing other devices to connect to the ports already in use. If unauthorized PC or laptops try to connect with the switch, data will be gotten the unauthorized PC or laptops. To prevent this condition, all interfaces of all switches can be configured the port security commands. After configuration, the switch associates that port with the device's MAC address and any other device will be denied. When unauthorized PC or laptop connects, the port will be turn off. Fig. 7 illustrates commands for port security. The fourth command actually indicates that only one device is allowed to be connected to that specific port and the third command indicates the allowed device. The switch associates that port with the device's MAC-address. After configuration of the port security, Fig. 8 is the result that the unauthorized PC or laptop cannot connect to the switch.

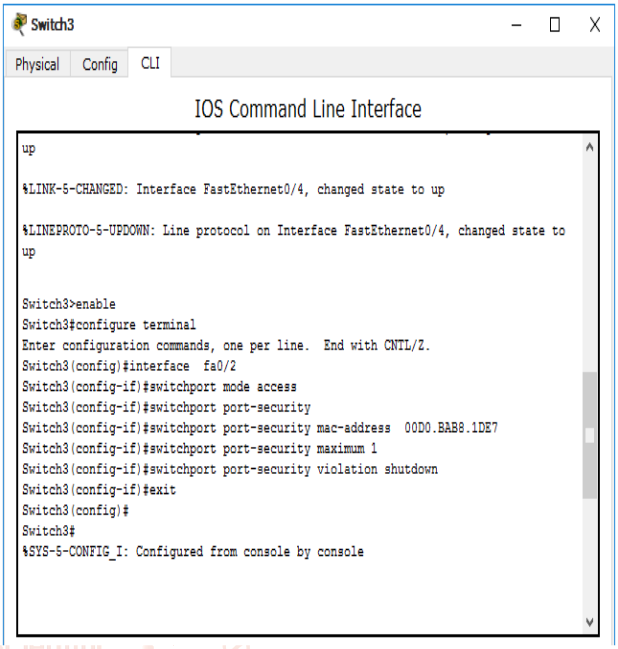

Figure7. Configuration Port Security

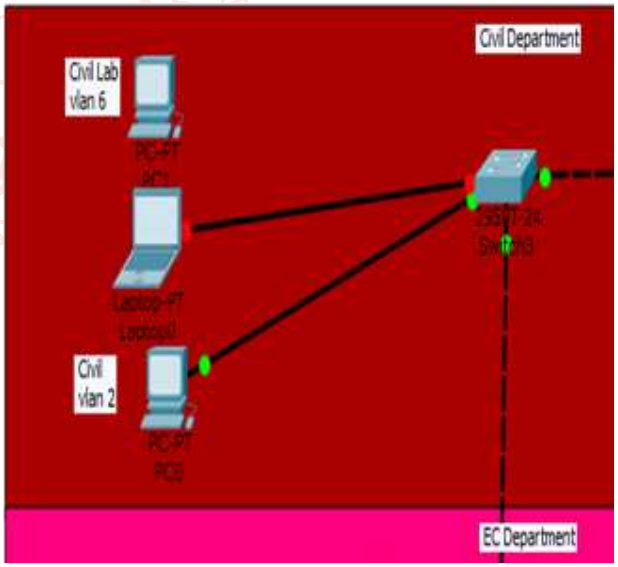

Figure8. Testing for Port Security

V. ACL IMPLEMENTATION AND TESTING

To control and secure the network, the access control list was configure. Access lists have to configure the router that connected the web server. In access list configuration, two basic steps require to be accomplished. The first step is to create an access list definition and the second step is to apply the access list to an interface. In the router, access lists was created, then configure the router's interface connected to the Web server. Fig. 9 is the creating the access list and the applying the access list to an interface Ethernet 1/0.

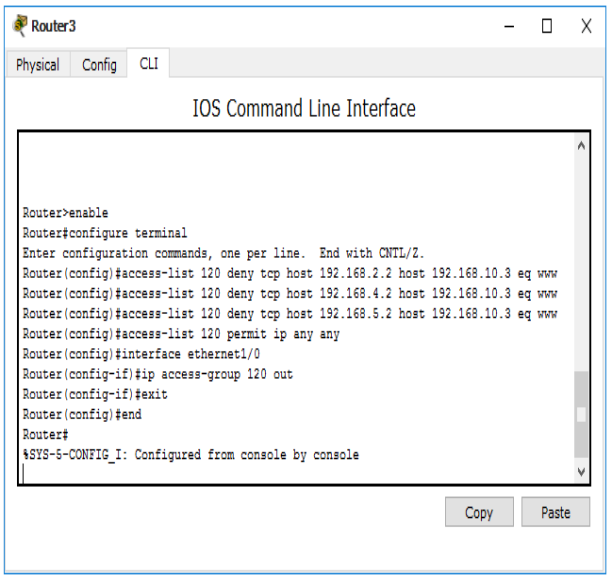

Figure9. Creating and Applying Access List

Each server must be responsible for only one job. DNS server is responsible for resolving a name to an IP address. Web server is only responsible for http services. Fig. 10 is the configuration of the DNS Server. Fig. 11 is the configuration of the web server.

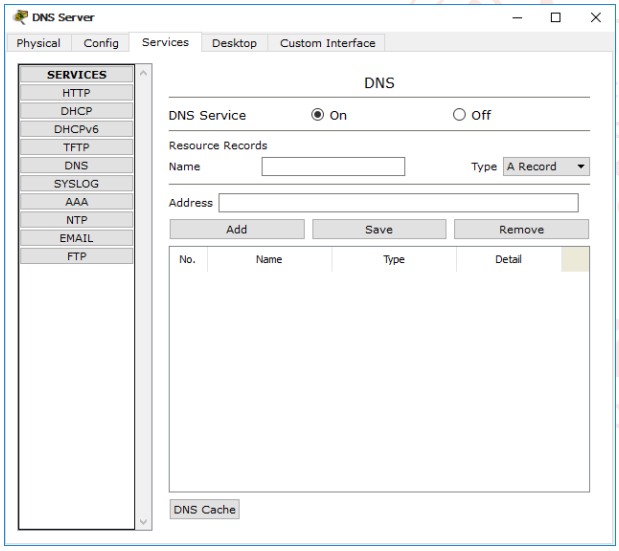

Figure10. DNS Server Configuration

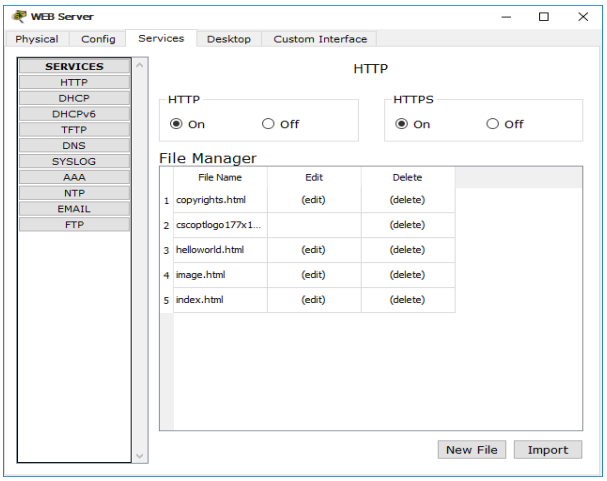

Figure11. Web Server Configuration

Fig. 12 and Fig. 13 are results that PC0 (VLAN2) ping the web server before and after configuration of the access control list.

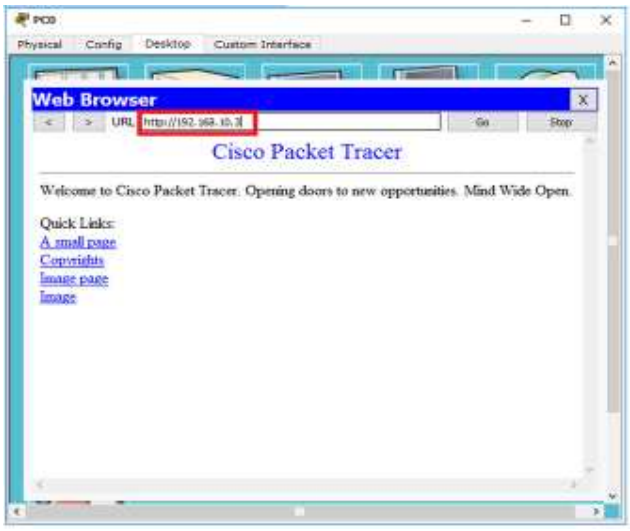

Figure12. Testing Result for Before Configuration of ACL

Figure13. Testing Result for After Configuration of ACL

VI. CONCLUSION

Network architecture and its security are important any organization. VLANs are also used as a means of providing WAN (Wide Area Network) and MAN (Metropolitan Area Network) services. Access Control List has been used to enforce better security and to filter unwanted packets.

ACKNOWLEDGEMENT

I would wish to acknowledge the many colleagues at Pyay Technological University who have contributed to the passing this research paper.

REFERENCES

[1] Kim J., Lee K., Lee C., "Design and Implementation of Integrated Security Engine for Secure Networking", In Proceedings International Conference on Advnaced Communication Technology, 2004.

[2] Computer Networks, 4th Edition Tanenbaum, A. S. Prentice Hall 2004.

[3] A. Velte and T. Velte. "Cisco: A Beginner's Guide", McGraw-Hill Inc. 3rd edition, 2004.

[4] Alabady S., "Design and Implementation of a Network Security Model using Static VLAN and AAA Server", In Proceedings International Conference on Information & Communication Technologies: from Theory to Applications, ICTTA, 2008.

[5] Computer and Network Technology: Proceedings of the International Conference on ICCNT 2009: Zhou, Jianhong Mahadevan, Venkatesh, World Scientific Publishing Co.

[6] CCNA Security Study Guide: Exam 640-553, Boyles, Tim, Sybex.

[7] Abubucker Samsudeen Shaffi, "Effective Implementation of VLAN and ACL in Local Area Network" In Proceedings JITBM & ARF, 2012.

[8] Cisco Systems Inc. http://www.cisco.com

[9] Sharat Kaushik, Anita Tomar, Poonam, "Access Control List Implementation in a Private Network", International Journal of Information & Computation Technology, Vol. 4, No. 14, 2014, pp. 1361-1366.