Design and Simulation of Secure Network for University Campus

Mon Mon Aye¹, Zar Chi Soe²

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



2019, pp.1023-1027, https://doi.org/10.31142/ijtsrd26568

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed

under the terms of the Creative Commons Attribution



License (CC BY 4.0) (http://creativecommons.org/licenses/by /4.0)

improved performance and security.

Easily modify configuration

Improve network security

ABSTRACT

I.

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

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 > A secure port and static MAC address configuration are network. This technology is used to segment a complex 2456-64 mutually exclusive. network into smaller networks for better manageability,

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

B. Port Security

Reduce the cost

following benefits:

≻

≻

≻

≻

۶

⊳

≻

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.

Implementing VLAN for any network will achieve the

Easily relocate PCs on LAN (Local Area Network)

Easily add or remove hosts to or from the LAN

Easily control network traffic between the LAN

Easily manage the network administrations [6].

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 portchannel interface.

International Journal of Trend in Scientific Research and Development (IJTSRD) @ www.ijtsrd.com eISSN: 2456-6470

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.



Figure 1. Implementation of VLAN

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

Table1. As	ssigning	Switch	Port to	VLANs	
------------	----------	--------	---------	-------	--

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.

Main S	witch											=			X
Physical	Config	CLI													
			105 Comma	nd i	ŭ	ne	. In	iter	fac						
			100 commu	ing :	-	170	-	PLC.	102	č –				_	
mainsvi mainsvi Inter o mainsvi mainsvi mainsvi mainsvi mainsvi mainsvi mainsvi mainsvi mainsvi mainsvi mainsvi	tch>ensb tch ensb tch ensf tch conf tch conf	le igure 5 tion co ig)tvlan ig-vlan ig-vlan ig-vlan ig-vlan ig-vlan ig-vlan ig-vlan ig-vlan	erminel mmands, one per 1: 0+name OTVII-Dep 0+east 0+name SC-Dep 0+east 0+name SE-Dep 0+east 0+name MD-Dep 0+east	ine.		Ind	i vi	sh (/2.	G				•
	rig	gurez	2. Ci eatilig	; v	L	A	IN	111	1.1	am	30	nun	L		
mainsw	itch(con	fig)‡int	terface fa0/2												
mainsw	itch (con:	fig-if)‡	<pre>#switchport access</pre>	vla	n 2	2									
mainsw	itch (con:	fig-if)‡	‡exit												
mainsw	itch (con:	fig)‡int	terface fa0/3												
mainsw	itch (con:	fig-if)‡	#switchport access	vlar	n 3	3									
mainsw	itch (con	fig-if)±	texit.												
mainey	itch (con	fia)tint	terface fa0/4												
maingu	itch (con	Fig_if)#	tevitchnort access	vlar		۵									
mainaw	itch (con	11y 11/4 Fig_if\4	*switchpoit access	VIG		-									
mainsw	itch/con	g/#	terfore fo0/5												
mainsw	uten (con:	rid) tiur	CELLACE ISU/5												
mainsw	itch (con:	[1g-1])	#switchport access	via	n t	5									

Figure 3. Assigning Ports in Main Switch

mainswitch(config-if) #exit
mainswitch(config) #

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.

				-	- C2	×
hysical Co	nfig Deski	op Custom Interface			-	
-				-	~	1
Comma	nd Prom	pt			x]
					-	
PC-ipoint	acer PC Com	mand Line 1.0				
TastIther	net0 Connec	tion:(default port)				
Link-1	acal TRvé A	ddimes	Inter Plan Scac			
Dabret	Hask	ADD. 400. 40				
Defaul	E QADEMAY	192.168.6.				
PCrping 1	12 345 842					
Pinging 1	92.169.612	with 31 bytes of data:				
Replay Con	- 192 188 C	7: Sylass32 simestime Tile	128			
Reply fro	n 192.160.6	.2: bytes=02 time=(ms TTL=1) .2: bytes=03 time=thms TTL=1;	20			
Find stat	Lating for	192.568.6.2+				
Fecke	ta: Sent -	F. Received = 4, Lost = 8 ()	14 Lossi.			
Minia	um - Sme, 10	animum = 47ms, Average = 120				
804						

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. International Journal of Trend in Scientific Research and Development (IJTSRD) @ www.ijtsrd.com eISSN: 2456-6470





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.



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.

International Journal of Trend in Scientific Research and Development (IJTSRD) @ www.iitsrd.com eISSN: 2456-6470

💐 Router	3			_		Х
Physical	Config	CLI				
			IOS Command Line Interface			
						^
Router>	enable					
Router#	configure	termi	nal			
Enter c	onrigurat config)ta	10n co	mmands, one per line. End with CNTL/2. List 120 denv ton host 192 168 2 2 host 192 168 10 :	3 67		
Router (config) #a	ccess-	list 120 deny top host 192.168.4.2 host 192.168.10.3	3 eq	WWW	
Router (config)‡a	ccess-	list 120 deny tcp host 192.168.5.2 host 192.168.10.	3 eq	WWW	
Router (config)‡a	ccess-	list 120 permit ip any any			
Router (config)‡i	nterfa	ce ethernet1/0			
Router (config-if) #ip a) #evit	ccess-group 120 out			
Router (config) #e	nd				
Router#						
SYS-5-	CONFIG_I:	Confi	gured from console by console			
						~
			Сору	1	Paste	в

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.

DNS Se	rver								-		\times
hysical	Config	Se	rvices	Desktop	Custom	Interface					
SER	/ICES	\land				DNC					
HT	ГТР					DNS					
DH	ICP		DNS 5	Service	۲	On		Ooff			
DHO	CPv6										
TF	TP		Resou	rce Records	1						
D	NS		Name	[Туре	A Rec	ord	-
SYS	SLOG										_
A	AA		Addre	ss							
N	TP			Add		Save			Remov	e	
EM	AIL									-	
F	TP		No.	N	ame	Тур	be	0)etail		



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.

PC0						7	D	
sysical Config	Desktop	Custom Interfa	C#		_	_	_	
COLUMN A	-	- 1-				0	-	٦
Web Brows	ar						3	5
< > URL	http://192.96	8.10.3			-60		Stop	
		Cisco Pa	cket Trac	er				1
Welcome to Cise	o Packet Tr	rscer. Opening	doors to new a	opportunities	Mind Wi	ide O	pen.	
Onlink Links								
A small page								
Copyrights								
Image page								
anothing a								
								÷
4								

Figure 12. Testing Result for Before Configuration of ACL



Figure 13. Testing Result for After Configuration of ACL

CONCLUSION VI.

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.

International Journal of Trend in Scientific Research and Development (IJTSRD) @ www.ijtsrd.com eISSN: 2456-6470

- [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.

