Designing a secure campus network and simulating it using Cisco packet tracer

Alaa H. Ahmed¹, Mokhaled N. A. Al-Hamadani²

¹Network Department, Computer Science and Information Technology College. University of Kirkuk, Iraq ²Department of Elecronic Techniques, Al-Hawija Technical Institute, Northern Technical University, Iraq

Article Info

Article history:

Received Apr 18, 2021 Revised Jun 1, 2021 Accepted Jun 6, 2021

Keywords:

IP addresses Network Security Trunk VLAN

ABSTRACT

The network is a massive part of life today. It participates not only on one side of life but in nearly every station, especially in educational organizations. The key aim of education is to share data and knowledge, making the network important for education. In particular, it is essential to ensure the exchange of information; thus, no one can corrupt it. To safe and trustworthy transfers between users, integrity and reliability are crucial questions in all data transfer problems. Therefore, we have developed a secure campus network (SCN) for sending and receiving information among high-security end-users. We created a topology for a campus of multi networks and virtual local area networks (VLANs') using cisco packet tracer. We also introduced the most critical security configurations, the networking used in our architecture. We used a large number of protocols to protect and accommodate the users of the SCN scheme.

This is an open access article under the <u>CC BY-SA</u> license.



Corresponding Author:

Mokhaled N. A. Al-Hamadani Department of Electrnoic Techniques Northern Technical University 36001, Adan, Kirkuk, Iraq Email: Mokhaled_hwj@ntu.edu.iq

1. INTRODUCTION

Nowadays, the network has become the need of most people, especially science seekers. A lot of researchers and scientists are depending excessively on networks to get more information. Students' also involved in the case of network-dependent for a lot of reasons like sharing information, and knowledge between themselves. Thus, the network is an important demand of each community and organization [1]-[3]. Nevertheless, the network can fall under many threats and intrusions; and the reason behind that is the development of web technologies and services [4]-[6]. Those attacks can occur in many different ways either physically damaging the devices or logically hacking the codes. That type of intrusion can cause a lot of problems because of the lack of veracity. Therefore, security has a significant effect in protecting the network from those types of attacks. Network security can be applied in many aspects of the network in order to keep it from unauthorized access. Thus, network security is now one of the essential issues in many firms like universities.

As consequence, we designed a secure campus network (SCN) which includes many networks and each network consists of many VLANs'. Those networks are supported by a security system that prevents outside access without authentication. Also, it protects the sanctity and privacy of each user, so no one can attack their private information. In section 1, we explained the technologies that we used to implement SCN which is packet tracer. Also, we explained the SCN structure and the required resources that we used to create the SCN topology. In section 2, we explained internet protocol (IP) addressing methods, and the connectivity between the devices in entire network. Whereas, virtual local area network (VLAN) explanation and simulation has been taking part in section 3. After that in section 4, there is a detailed illustration about security and configurations that we applied in the campus topology using packet tracer. Finally, in section 5 a secure network campus scenario will be conclude.

2. METHODOLGY

Cisco packet tracer (CPT) is the main technology that we depended on designing and simulating a secure campus network. CPT is a visual simulation tool that has been created and designed by cisco system. CPT has been used as an effective tool to teach and learn network communication in realistic way [7], [8]. It offers a realistic visualization and simulation tool for learning [9], [10]. That what help the users especially students to create, design, configure, and troubleshoot different type of networks such as LAN and WAN. Also, it helps with the security problems by using security protocols. For example, qualifying the use of some protocols like spanning tree protocol which helps with the looping problems; especially when there are three switches connected to each other.

2.1. Implementation

In order to design a secure campus network (SCN), we used different devices wired and wireless. Also, we used different types of communication media to connect the devices. After connecting the devices, we implemented many important configurations as VLANs, dynamic host configuration protocol (DHCP), and routing information protocol (RIP). Moreover, we applied security and management techniques in the main devices of the network; to make the campus network safer and to protect it from interior and exterior attackers. So, the sanctity and the privacy of the user will be granted.

2.2. SCN topology

The topology that is designed for the secure campus network consists of four main parts or buildings. Each part contains different devices as switches, computers, laptops, smartphones, phones, printers, access point, wireless router, and servers. All of those devices are connected with a switch that connects them directly with a router. The routers in the campus are connected with each other dynamically as it's shown in Figure 1.



Figure 1. Topology of secure campus network

2.3. Required resources

We used different types of devices in our work to show different connectivity cases. Most of the devices are connected using cables like PCs. However, some of them connected by wireless such as smartphones. As a wireless connection provider, we used two devices in different networks such as wireless routers and access points. The descriptions of the devices are:

- 4 Router (Cisco 8211)
- 1 wireless router (WRT300N)
- 9 Switches (Cisco 2960)
- 1 server(server-PT)
- Access point (Accesspoint-PT)
- 17 PCs (Pc-PT)
- 3 laptops (Laptop-PT)
- 1IP phone(7960)
- 2 smart phones(Smartphone-PT)
- 2 printer (Printer-PT)

- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology
- Copper straight through cables to connect most of the end devices with switches, and switches with routers.
- Serial DTE cables to connect routers with each other dynamically
- Copper cross-over cables to connect the three switches with each other.

3. IP ADRESSES

An IP address is an internet protocol address that assigns to each device in the network [11]-[13]. Each device assigns a unique IP address to be recognizable and visible by other devices in the network so that it can send and receive data easily without any missing. Each one consists of 32-bit number which is in the format of four-octet numbers separated by a dot as 192.168.1.0. The IP address has two versions IPv4 and IPv6 [14], [15]. Where IPv4 has five classes A, B, C, D, and E each one has a different range of capacity. For example, class A has a range from 1 to 127 network addresses [16]-[18]. This can be written as 1.0.0.0 to 126.255.255.255. Thus, Class A provides a few very large sizes of networks. In our work, we used IP addresses with class c to connect end devices, however for the router's port that has a connection with other router's we used IP addresses of class A.

In order to assign IPs for each device we did some of them manually and some of them by using DHCP protocol. The DHCP protocol is a dynamic host configuration protocol that assigns an IP address to end devices depending on the configuration that makes on some devices like a server or router. A DHCP server allows computers to request IP addresses and networking parameters from their Internet service provider (ISP) automatically, eliminating the need for a network administrator or user to assign IP addresses to all network devices manually. In a secure campus network, we configured a server to provide the PCs with the IP addresses as it is shown in Figure 2. We put 192.168.4.6 as a start IP address and also we determined the maximum number of 25 for end devices.

SERVICES -					DHCP					
HTTP					o ner					
DHCP	Interface	Fost	Ihernelli		 Servi 	ce 🖲 On		Oom		
DHCPv6	Paol Name				arry	erPeol				
TFTP	Defect Determine				100	100 4 4				
DNS	Delaw Galeway				1164	100.4.1				
SYSLOG	DNS Server				0.0.0	0.0				
AAA	Start P'Address	192		105 4		6				
NUP	Subort Mask	955	265			946		10	10	
ENALL	- sector many	200	_	leve leve						
TOT	Heximum Number of	of Uniers			20					
M Management	TFTP Server:				0.0.0	0.0				
Badus FAP	WLC Address				0.0.0	10				
Transfer Low		3043			1.4.4.4			0-2/4/6		
	1	Add			Save	1.1		Raterow	\$	
	Psol Name	Defast Gateway	. D Se	DNS STVBC J	Start P ddress	Subnet Mask	Max User	TFTP Server	WLC Address	
	aarverPaal	192.168.4.1	0.0.0.0	192	168.4.6	255.255.255.0	25	0.0.0.0	0.0.0.0	
	1.20									

Figure 2. Server configuration to provide DHCP

Designing a secure campus network and simulating it using Cisco packet tracer (Alaa H. Ahmed)

3.1. Connectivity

The connectivity between the same networks happens directly since there are switch connections between the devices. In the parts that have two or three switches, we used trunks to connect them together. Where Trunks is a channel that allows connectivity between the VLANs' that are connected to a switch. However, the connectivity between routers will need network routing protocols static or dynamic such as RIP. RIP is a router information protocol that is responsible for finding the best path for data to be transmitted [19]-[21]. Also, it prevents routing loops by limiting the number of paths from source devices to destination devices. Therefore, we used RIP to connect the entire network with each other; so the end devices can send and receive information from different networks with the shortest and simplest path. After that, we checked the connectivity between the end devices as is shown in Figures 3 and 4.

	1		
GLOBAL		RIP Routing	
Settings	Network	1 (FATTHON	
Algorithm Settings		<u>م</u>	dd
ROUTING	Network Address		^
Static			
RIP	130.10.0.0		
INTERFACE	172,16.0.0		
FastEthernet0/0			
FastEthernet1/0	192.168.1.0		
Serial2/0	192 168 2 0		
Senal3/0	102.100.2.0		4
FastEthernet4/0			Remove
FastEthernet5/0			
quivalent IOS Commands			
Router>enable Router# Router#configure te	erminal		
Enter configuration	commands, one per	line. End with CNTL	/z.
Router(config) #rout	er rip		

Figure 3. Routing information protocol (RIP)



Figure 4. Connectivity between devices (continue)

 \times

R PC6

Physical Config Desktop Programming Attributes	
Command Prompt X	
Pinging 192.160.2.2 with 32 bytes of data:	•
Request timed out. Reply from 192.160.2.2: bytes=32 time=24ms TTL=125 Reply from 192.168.2.2: bytes=32 time=22ms TTL=125 Reply from 192.168.2.2: bytes=32 time=13ms TTL=125	
<pre>Ping statistics for 192.168.2.2: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 13ms, Maximum = 24ms, Average = 19ms</pre>	
C:\>ping 192.160.3.2	
Pinging 192.168.3.2 with 32 bytes of data:	
Reply from 192.168.3.2: bytes=32 time <lms ttl="128<br">Reply from 192.168.3.2: bytes=32 time<lms ttl="128<br">Reply from 192.168.3.2: bytes=32 time<lms ttl="120<br">Reply from 192.168.3.2: bytes=32 time<lms ttl="128</td"><td></td></lms></lms></lms></lms>	
<pre>Ping statistics for 192.168.3.2: Dackets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms</pre>	
G:\\s	,

🗌 Тор



Figure 4. Connectivity between devices

4. VLAN

VLAN or virtual local area network is a group of local area networks (LAN) that are connected to each other to add more security and manage broadcast domain into the LANs [22]-[24]. Therefore, in secure campus network, we used VLANs in some parts to separate the end devices into different VLANs' for many reasons. Firstly, it will put the student, lecturers, employees, managers, and other staff in different VLANs', so it will reduce the traffic. Secondly, for security reasons, VLAN will restrict access to the ports by non-authorized people [25]. VLAN has five types default, management, voice, data, and native VLAN; where default VLAN is already available in every switch and all ports are assigned to it. So, it is easy to attack those ports by outsider or insider attackers. Therefore, changing all ports to another VLAN rather than the default VLAN which will be more secure.

- Switch configuration for VLANs
- We created three VLANs 10, 20, and 30; and then we assigned fa0/2, fa0/3, and fa0/4 respectively, one port for each one of them
- We moved all the other FastEthernet ports fa0/5 fa0/24 from default VLAN to new VLAN which we assigned as a VLAN 40 to be a saver.
- We changed the two remaining ports GigabitEthernet 0/1 and 0/2 to be in static trunk mode as is shown in the configuration below.

Switch(config)#hostname sw1 sw1(config)# vlan 10 sw1(config-vlan)# name Lecturer sw1(config)# vlan 20 sw1(config-vlan)# name employee sw1(config)# vlan 30 sw1(config-vlan)# name Student sw1(config)# vlan 40 sw1(config)#int range fa0/5-24 sw1(config-if-range)#switchport mode access sw1(config-if-range)#switchport access vlan 40 sw1(config)#int range gig0/1-2 sw1(config-if-range)#switchport mode trunk

- Since $\frac{fa0}{1}$ connects the root switch with the router, we changed its mode to be trunk too.

	sw1(config-if-range)#switchport trunk
sw1(config-if)#int fa0/2	allowed vlan 10,20,30
sw1(config-if)#switchport access vlan 10	sw1(config-if-range)#
sw1(config-if)#no shut	sw1(config)#int range gig0/1-2
sw1(config-if)#int fa0/3	sw1(config-if-range)#switchport mode trunk
sw1(config-if)#switchport access vlan 20	sw1(config-if-range)#switchport trunk
sw1(config-if)#no shut	allowed vlan 10,20,30
sw1(config-if)#int fa0/4	sw1(config-if)#int fa0/1
sw1(config-if)#switchport access vlan 30	sw1(config-if)#switchport mode trunk
sw1(config-if)#no shut	sw1(config-if)#switchport trubk allowed vlan
	10,20,30

4.1. Network security

There are a lot of techniques to protect the network from interior and exterior attackers. Attacking could be physical by sabotaging, ruining, or stealing the devices; or it can be by hacking the system and accessing without authorization. Thus, in order to protect the network from those types of attacks, we need a strong security system. Network security is a set of policies and procedures that monitor the entire network continuously to secure and prevent it from unauthorized access. Consequently, in SCN we used a high level of security in the main devices like routers and switches. We secured all the ports so those devices would not accept any access without authentication.

In the routers' case, we secured VTY lines and console lines by adding passwords to require authentication from the user; as it is clear in the following router configuration. In the switch's case, we also secured all ports; also, we disabled some protocols that show the information of the devices to others such as cisco discovery protocol (CDP). At the same time, we enabled other protocols like spanning tree protocol (STP) in order to prevent looping between switches.

- a. Router configuration for security
- We start the security process by putting a password for the line console in order to prevent remote access by others.
- We put a password for line VTY 0 4 to restrict the telnet and SSH unauthorized access.
- We used the message-digest algorithm MD5 to encrypt passwords as shown in Figure 5.
- Finally, we put some restricted features in creating new passwords such as minimum length, and the number of attempts. For example, we verified restriction by entering new user with weak password and the router rejected it as it is shown in the Figure 6.

Indonesian J Elec Eng & Comp Sci

ISSN: 2502-4752

485

×

ndonesian 5 Lice Ling & Comp Ber	15511. 2502	1752			
outorting	L'esmania: alas				
outerfeel	Deserved				
conterfectuation consola 0	Passworu. Bentarbanabla				
conter(county)/rime consore o	Router-chaole				
couter(config-line)//password network	Passworg:				
touter(config-line)#login	Router#conf t	27 52			
touter(config-line)#line vty 0 4	Router(config)#security passwords mi	in-length			
touter(config-line)#password network	10				
touter(config-line)#login	Router(config)#line console 0				
touter(config)#exit	Router(config-line)#exec-timeout 2				
	Router(config-line)#end				
	Router(config)#line vtv 0.4				
couter>enaoue	Router(config-line)#exec-timeout 2				
assword	Router(config line)#and				
Router#conf t	Protoconfig-ture/read	increase 2			
Router(config)#enable secret network1	Router(conng)=togin block-tor 120 as	tempts 5			
Router(config)#usemame alaa secret alaa	within 60				
Router(config)#	Router(config)#login on-failure log				
Router#exit	Router(config)#login on-success log				
MCHINE: NAME	Router(config)#end				
P Router0					×
and the second				A COLOR	103
Discolaria Config	and the second				
Physical Config	LI Attributes				
	IOS Command Line Interface				
	contrantes trom compete al cons	020			1271
show run	25072255033503070120100508050000000000000000000000000000	18-33-34 L			*
Building configur	ation				
Current configura	- CCT homes				
t to the second second second	cion : ce/ pyres				
version 12.4					
no service timest.	amps log datetime msec				
ho service timest	amps debug datetime msec				
service password-	encryption				
hostname Router					
The second s					
1					
enable secret b y	1\$mERr\$20d5Wotdefhb5Vvnhxnxau				
8					100
10 A					
10000					
ip cer					
1 to the second se					
					Y
Ctrl+F6 to exit CLI focus		Copy		Paste	11
		(T)(T)(T)		T MARE	
Router0			_	Ē.	×
The second second			14	1000	- 22
	NAMES IN THE REAL PROPERTY OF				
Physical Config	Attributes				
	the second second second second second				
	IOS Command Line Interface				
SYS-5-CONFIG_I; C	Configured from console by cons	ole			~
show run	ST WARDSHAUSS II I STATE IN AN AND AND A STRATE AND AND AN AND AND AND AND AND AND AND				
Building configura	stion				
Conservation and the second	A NEW MILLION				
Current configurat	tion : soo bytes				
version 12.4					
no service timesta					
no service timesta	umps log datetime msec				
the second cameses	amps log datetime msec amps debug datetime msec				
service password-e	amps log datetime msec amps debug datetime msec ancryption				
service password-e security passwords	amps log datetime msec amps debug datetime msec ncryption 9 min-length 10				

Figure 5. Router security configuration

hostname Router

-More-

Ctrl+F6 to exit CLI focus

login block-for 120 attempts 3 within 60 login on-failure log login on-success log

enable secret 5 \$1\$mERr\$20dSWotdefhb5VvnBXMxa0

Designing a secure campus network and simulating it using Cisco packet tracer (Alaa H. Ahmed)

Copy

Paste

KOUDEL#	
Router#	
Router#	
Router#	
Router#conf t	
Enter configuration command	per line. End with CNTL/Z.
Router(config) #username ahm	ret computer
% Password too short - must	least 10 characters. Password not
configured.	
· ·	

Figure 6. Password restriction

- b. Switch configuration for security
- We disabled the CDP protocol from all the devices, and the reason is that CDP gives information about the devices that are adjacency to a specific device.
- We allowed the spanning tree protocol to get rid of the looping that can happen when there is a cycle of switches in the topology.
- After that, we did port security for used ports. We determined a maximum of 2 devices and a broadcast level to be 80% as is shown in Figure 7 and the configuration.
- We verified the security configurations of ports fa0/1, fa0/2, and fa0/3 as its shown in the Figure 8.

sw1(config)#int range fa0/1-24	sw1(config)#int range gig0/1-2
sw1(config-if-range)#no cdp enable	sw1(config-if-range)#switchport mode trunk
sw1(config-if-range)#spanning-tree bpduguard	sw1(config-if-range)#switchport trunk allowed vlan
enable	10,20,30
sw1(config-if-range)#shutdown	sw1(config-if-range)#
sw1(config-if)#exit	sw1#
sw1(config)#int range fa0/1-3 sw1(config-if-range)#switchport port-security sw1(config-if-range)#switchport port-security maximum 2 sw1(config-if-range)#switchport port-security violation shutdown sw1(config-if-range)#switchport port-security mac-address sticky sw1(config-if-range)#storm-control broadcast level 80 sw1(config-if-range)# sw1#	

Attributes		
IOS Command Line Interfac	ce	
spanning-tree mode pvst. spanning-tree extend system-id interface FastEthernet0/1 switchport access vian 10 switchport port-security no cdp enable spanning-tree bpduguard enable storm-control broadcast level 80 interface FastEthernet0/2 switchport port-security switchport port-security switchport port-security no cdp enable switchport port-security no cdp enable switchport port-security no cdp enable switchport bord-access switchport port-security no cdp enable storm-control broadcast level 60 interface FastEthernet0/3 switchport access vian 30 More		()
tri+E6 to exit CLI focus	Copy	Paste

Figure 7. Switch security configuration

	3.26	20.200.00000						
	101	S Comman	d Line Inte	erface				
							8	in.
1 enet 100001 1	500	-	-			-	0	
10 enet 100010 1	500		-	-	-	-	0	
0	7.5.7						10	
Switchsshow port-securi	sy in	nerface	e fa0/1					
Port Security		Enable	ed					
Port Status		Secure	a-rib					
Violation Mode		Shusde	DWEL					
Aging Time		0 mine						
Aging Type	5000 E	Absolu	128					
SecureStatic Address Ag	ing :	Disabl	Lect					
Maximum MAC Addresses		- <u>-</u>						
Total MAC Addresses	-00 E	1						
Configured MAC Addresse	8 2	0						
STICKY MAC Addresses	80 B	in the second		2012/07/2025				
Last Source Address: Via	n	0090.2	2170.163	6C:10				
Security Violation Coun-	e :	0						
Switch#								-
Switchs								
Switche								

Figure 8. Port security verification (continue)

Physical Config CL Attributes IOS Command Line Interface Configured MAC Addresses 1 0 Sticky MAC Addresses 1 1 Last Source Address VI 1 1 0090.2170.14RC:10 Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Configured MAC Addresses 2 1 Configured MAC Addresses Tobal MAC Addresses 1 Last Source Addresses Configured MAC Addresses 1 Last Source Addresses Switch# Sw				<u>.</u>	
IOS Command Line Interface Configured MAC Addresses : 0 Sticky MAC Addresses : 0 Security Violation Count : 0 Switch# : 0090.3170.16RC:10 Switch# : 0090.3170.16RC:10 Switch# : 0 Switch# : 0 Switch# : 0 Switch# : Shutdown Aging Time : 0 Aging Type : Shutdown Aging Type : 1 Configured MAC Addresses : 2 Total MAC Addresses : 1 Configured MAC Addresses : 1 Configured MAC Addresses : 0 Sticky MAC Addresses : 1 Last Source Address:Vian : 0000C.0576.20RD:20 Switch# : 0	Physical Config <u>CLI</u> Attrib	outes			
Configured MAC Addresses : 0 Bticky MAC Addresses : 1 Last Source Address:Vian : 0090.2170.16RC:10 Security Violation Count : 0 Switch# Switch# Switch# Switch# Switch# Switch# Source address 2 Violation Mode : Shutdown Aging Type : Absolute SecureStatic Addresses : 1 Configured MAC Addresses : 1 Configured MAC Addresses : 1 Cast Source Addresses : 1 Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Sticky MAC Addresses : 1 Configured MAC Addresses : 0 Sticky MAC Addresses : 0 Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Sticky MAC Addresses : 1 Configured MAC Addresses : 0 Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Sticky MAC Addresses : 1 Configured MAC Addresses : 0 Switch#		IOS Command Line Interface			
<pre>sticky NAC Addresses : 1 Last Source Address:Vian : 0090.3170.16EC:10 Switchs Switchs Switchs Switchs Switchs Switchs Switchs Aging Time : 2 Enabled Port Status : Secure-up Violation Mode : Shutdown Aging Time : 0 mins Aging Type : Absolute BecureStatic Addresses : 1 Configured MAC Addresses : 1 Configured MAC Addresses : 1 Last Source Addresses : 1 Last Source Addresses : 1 Switchs Switchs Switchs Switchs Switchs Switchs Sticky MAC Addresses : 1 Config CU Attributes Sticky MAC Addresses : 1 Last Source Address Vian : 000C.0576.20BD:20 Switchs Switchs Switchs Switchs Switchs Switchs Sticky MAC Addresses : 1 Last Source Address Vian : 000C.0576.20BD:20 Sticky MAC Addresses : 1 Last Source Address Vian : 0 Switchs</pre>	Configured MAC Addresses	: 0			~
Last Source Address:Vlan : 0090.2170.16EC:10 Switchs Switchs Switchs Switchs Switchs Switchs Switchs Switchs Switchs Switchs Switchs Secure Status : Secure-up Violation Mode : Shutdown Aging Type : Absolute SecureStatic Address Aging : Disabled Maximum MAC Addresses : 2 Configured MAC Addresses : 1 Last Source Address:Vlan : 000C.9576.20BD:20 Security Violation Count : 0 Switchs Switchs Switchs Switchs Switchs Switchs Switchs Staty MAC Addresses : 1 Config CL Attributes Staty Violation Count : 0 Switchs Switchs Switchs Staty MAC Addresses : 1 Config CL Attributes Staty MAC Addresses : 1 DS Command Line Interface Staty MAC Addresses : 1 Source Addresses : 1 Switchs S	Sticky MAC Addresses	 Langersteinen erstellter 			
Security Violation Count : 0 Switchs Switchs Switchs Switchs Switchs Switchs Switchs Switchs Switchs Solute Secures Se	Last Source Address:Vlan	: 0090.2170.16EC:10			
Switchs Swi	Security Violation Count	: 0			
Switchs Switchs Switchs Switchs Switchs Switchs Switchs Secures Secures Secures Secures Secures Secures Secures Secures Secures Secures Switch Switchs Swit	Switch#				
Switch# Switch# Switch#show port-security interface fa0/2 Port Security : Knabled Port Status : Secure-up Violation Mode : Shutdown Aging Time : 0 mins Aging Type : Absolute SecureStatic Address Aging : Disabled Maximum MAC Addresses : 1 Configured MAC Addresses : 1 Last Source Addresses : 1 Last Source Addresses : 1 Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# State Source Addresses : 1 Last Source Addresses : 1 Copy Paste Switch#	Switchs				
Switch#show port-security interface fa0/3 Port Status I Secure-up Violation Mode I Shutdown Aging Time I 0 mins Aging Type I 0 mins Aging Type I 1 Sabled Maximum MAC Addresses I 2 Configured MAC Addresses I 1 Last Source Addresses I 1 Last Source Addresses I 1 Switch# Switch# Config CLI Attributes Switch0 - Physical Config CLI Attributes Sticky MAC Addresses I 1 Last Source Addresse I 1 Last Source Addresse I 1 Last Source Addresse I 1 Switch# Switch# Switch# Switch# Sticky MAC Addresses I 1 Last Source Addresse I 1 Last Source Addresse I 1 Last Source Addresse I 1 Switch# S	Switch#				
Port Security : Knabled Port Status : Secure-up Violation Mode : Shutdown Aging Type : Absolute SecureStatic Address Aging : Disabled Maximu RAC Addresses : 1 Configured MAC Addresses : 1 Last Source Address: 1 Switchs Switchs Switchs Switchs Ctrl+P6 to ext CU focus Copy Paste Switchol Physical Config CU Attributes Switchill : 0 Switchill	Surreptsyon bore-security	interface fa0/2			
Port Status : Secure-up Violation Mode : Shutdown Aging Time : 0 mins Aging Time : 0 bisoled Maximu MAC Addresses : 1 Configured MAC Addresses : 1 Last Source Addresses : 1 Last Source Address:Vian : 000C.0576.20BD:20 Switch# Switch# Switch# Switch# Switch# Switch# Switch# Story MAC Addresses : 1 Last Source Address:Vian : 000C.0576.20BD:20 Switch# Switch# Switch# Switch# Switch# Switch# Switch# Switch# Story MAC Addresses : 1 Last Source Address:Vian : 000C.9576.20BD:20 Switch# Swit	Port Security	: Enabled			
Violation Mode : Shutdown Aging Time : O mins Aging Type : Absolute SecureStatic Addresses : 2 Total MAC Addresses : 2 Configured MAC Addresses : 0 Sticky MAC Addresses : 1 Last Source Address: 1 Switch: Switch: Switch: Ctrl+F6 to ext CLI focus Copy Paste Switch: Ctrl+F6 to ext CLI focus Copy Paste Switch: Switch: Switch: Switch: Copy Copy Paste Copy Paste Switch: Swi	Port Status	: Secure-up			
Aging Time : 0 mins Aging Time : Absolute SecureStatic Addresses : 1 Configured MAC Addresses : 1 Configured MAC Addresses : 1 Last Source Addresses : 1 Security Violation Count : 0 Switch# Switch# Switch# Copy Paste Copy Paste Copy Paste Copy Paste Copy Copy Paste Copy Copy Copy Copy Copy Copy Copy Copy	Violation Mode	: Shutdown			
Aging Type : Absolute SecureStatic Addresses ging : Disabled Maximum MAC Addresses : 2 Configured MAC Addresses : 1 Configured MAC Addresses : 1 Last Source Address : 1 Switch# Switch# Switch# Switch# Switch# Switch# Enclose Config Attributes Book Command Line Interface Sticky MAC Addresses : 1 Last Source Address : 0 Switch#	Aging Time	: O mins			
Switch0 - Copy Paste Switch0 Config CLI Attributes Switch0 - Copy Paste Switch8 Starte Addresses : 1 Last Source Addresse : 1 Switch8 Switch8 Switch8 Switch4 Switch	Aging Type	: Absolute			
MAX.Mum PAC Addresses : 2 Configured MAC Addresses : 1 Last Source Addresses : 1 Last Source Address:Vian : 000C.9576.20BD:20 Switch# Switch# Switch# Switch# Switch# Switch# Switch# End Config Cil Attributes IOS Command Line Interface Sticky MAC Address:Vian : 1 Source Address:Vian : 1 Switch#	SecureStatic Address Agin	g : Disabled			
Tobal HAC Addresses : 1 Configured MAC Addresses : 0 Sticky MAC Addresses : 1 Last Source Address Vian : 000C.9576.20BD:20 Switch# Switch# Switch# Switch# Switch0	HAXIMUM HAC Addresses				
Switch0 - Command Line Interface Sticky MAC Addresses : 1 Last Source Addresses : 1 Copy Paste Switch8 Switch8 Switch0 - C Physical Config CL Attributes IOS Command Line Interface Sticky MAC Addresses : 1 Last Source Addresses : 1 Last Source Addresses : 1 Switch8 Command Line Interface fa0/3 Switch8	Total MAC Addresses	1 1			
Switch0 - O Physical Config CLI Attributes Switch2 Sticky MAC Addresses 1 L Last Source Addresses 1 Copy Paste Switch0 - O Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses 1 L Last Source Addresses 1 L Last Source Addresses 2 Copy Copy Copy Copy Copy Copy Copy Copy	Configured MAC Addresses	5 Y			
Switchs Switch0 Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses I I Last Source Addresses I I Switchs	Dolcky HAU Addresses	: 1 : 0000 0536 2020-20			
Switch# Switch# Switch# Switch# Switch0 — Physical Config Cli Attributes IOS Command Line Interface Sticky MAC Addresses : 1 Last Source Addresses : 1 Last Source Addresses : 000C.9576.208D:20 Security Violetion Count : 0 Switch# Swi	Requested Violation Count	. 0000.100/0.20RD120			
Switch# Switch# Switch# Switch0	security aroteriou conue	3 B			12
Switchs Switchs Switchs Switch0 - Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses Sticky MAC Addresses I 1 Last Source Address Vian I 000C.9576.208D:20 Security Violation Count I 0 Switchs Swit					
Switchs Switch0 - Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses : 1 Last Source Address:Vian : 000C.9576.208D:20 Security Violation Count : 0 Switch# Switch	Switch#				
Copy Paste Switch0 — Physical Config Clinet IOS Command Line Interface Sticky MAC Addresses : Last Source Address Vian : Switch18 Switch18 Switch18 Switch18 Switch18 Switch18 Switch18 Switch18 Switch18 Switch19 Switch19 Switch19 Switch18 Switch19 Switch18 Switch19 Switch19 Switch19 Switch19 Switch19 Switch19 Switch20 Switch19 Switch20 <	Switch#				
Switch0 - Copy Paste Switch0 - C Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses : 1 Last Source Address Vian : 000C.9576.20BD:20 Security Violation Count : 0 Switch# Switch# Switch# Switch# Show port-security interface fa0/3 Port Security : Enabled	Switch# Switch# Switch#				4
Switch0 - Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses I 1 Last Source Address VIan I 0000.9576.208D:20 Security Violation Count I 0 Svitch# Switch#Show port-security interface fa0/3 Port Security I Enabled	Switch# Switch# Switch#				
Switch0 - Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses I I Last Source Address Vian I 000C.9576.20BD:20 Security Violation Count I 0 Svitch# Switch# Switch# Switch#Show port=security interface fa0/3 Port Security I E Enabled	Switch# Switch# Switch# Stri+F6 to exit CLI focus		Сору	Past	
Switch0 - C	Switch# Switch# Switch# Ctrl+F6 to exit CLI focus		Сору	Past	
Switch0 — Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses : 1 Last Source Address:Vian : 000C.9576.20BD:20 Switch# Switch# Switch# Switch# Switch# Switch#Show port=security interface fa0/3 Port Security : Enabled	Switch# Switch# Switch# Ctrl+F6 to exit CU focus		Сору	Past	
Physical Config CLI Attributes IOS Command Line Interface Sticky MAC Addresses I I Last Source Address:Vlan I 000C.2576.20BD:20 Security Violation Count I 0 Svitch# Switch#Show port=security interface fa0/3 Port Security I Snabled	Switch# Switch# Switch#		Сору	Past	2
IOS Command Line Interface Sticky MAC Addresses I L Last Source Address:Vian I 000C.9576.20BD:20 Security Violation Count I 0 Svitch# Switch# Switch#show port-security interface fa0/3 Port Security I Interface fa0/3	Switch# Switch# Switch# Switch0		Copy	Past	
IOS Command Line Interface Sticky MAC Addresses : 1 Last Source Address:Vian : 000C.9576.20BD:20 Security Violation Count : 0 Svitch# Svitch# Svitch# Svitch#show port-security interface fa0/3 Port Security : Enabled	Switch# Switch# Switch# Switch0 Physical Confin CLI Attem		Copy —	Past	a 2
Sticky MAC Addresses : 1 Last Source Address:Vian : 000C.9576.20BD:20 Security Violation Count : 0 Switch# Switch# Switch# Switch#show port-security interface fa0/3 Port Security : Enabled	Switch# Switch# Etri+F6 to exit CLI focus Switch0 Physical Config CLI Attrib	utes	Copy —	Past	2
Last Source Address Vian : 000C.9576.20BD:20 Security Violation Count : 0 Switch# Switch# Switch#show port-security interface fa0/3 Port Security : Enabled	Switchs Switchs Switch0 Physical Config <u>CLI</u> Attrib	outes IOS Command Line Interface	Серу	Past	*
Security Violation Count : 0 Switch# Switch# Switch#show port-security interface fa0/3 Port Security : Enabled	Switch# Switch# Evitch# Switch0 Physical Config <u>CLI</u> Attrit Sticky MAC Addresses	ioutes IOS Command Line Interface 2 1	Сору —	Past	2 ×
Switch# Switch# Switch#show port-security interface fa0/3 Port Security : Enabled	Switch# Switch# Switch# Switch0 Physical Config <u>CLI</u> Attric Sticky MAC Addresses Last Source Address Vian	Nutes IOS Command Line Interface 2 2 2 000C - 9576 - 208D : 20	Copy —	Past	2 C
aviton: Switch: Switch#show port-security interface fa0/3 Port Security : Enabled	Switch# Switch# Evitch# Ctrl+F6 to exit CLI focus Switch0 Physical Config <u>CLI</u> Attrit Sticky MAC Addresses Last Source AddressesUlan Security Violation Count	005 Command Line Interface 2 1 2 000C.9576.208D:20 2 0	Серу	Past	
evitch#show port-security interface fa0/3 Port Security : Enabled	Switchs Switchs Switchs Switch0 Physical Config <u>CLI</u> Attrit Sticky MAC Addresses Last Source Address Vian Security Violation Count	Utes IOS Command Line Interface : 1 : 000C.957€.208D:20 : 0	Сору	Past	
Port Security : Enabled	Switchs Switchs Switchs Switch0 Physical Config <u>CLI</u> Attric Sticky MAC Addresses Last Source Address Vian Security Violation Count Switchs	Nutes IOS Command Line Interface = 1 = 0000C.957€.208D:20 = 0	Серу	Past	
RAPE BRANTERS	Switchs Switchs Switchs Switch0 Physical Config <u>CU</u> Attrib Sticky MAC Addresses Last Source Address Vian Security Violation Count Switchs Switchs	105 Command Line Interface 2 1 2 000C.9576.20BD:20 2 0	Сору —	Past	
Down Original Commention	Switchs Switchs Switchs Switch0 Switch0 Physical Config <u>CLI</u> Attric Sticky MAC Addresses Last Source Address(Vlan Security Violation Count Switchs Switchs Switchs	Nutes IOS Command Line Interface 1 1 1 000C.9576.20BD:20 2 0 Interface 5a0/3	Серу —	Past	×

Ctrl+F6 to exit CLI focus			Сору	Paste
Switch#	_			Y
Switch#				15
Switch#				
Switch#				1.00
Switch#				
Security Viclation Count	4	0		
Last Source Address:Vlan	Ŧ	0002.4AAL.64D5:30		
Sticky MAC Addresses	7			
Configured MAC Addresses	1	0		
Total MAC Addresses	÷	1		
Maximum MAC Addresses	+	Description of the second s		
SecureStatic Address Aging	1	Disabled		
Aging Type	- 21	Absolute		
Aging Time	1	0 mins		
Violation Mode	1	Shutdown		
and the last and the state of the state of		and one of the set of a set we we		

Figure 8. Port security verfication

Designing a secure campus network and simulating it using Cisco packet tracer (Alaa H. Ahmed)

5. CONCLUSION

To increase the security level in the network's system especially on campuses, we proposed a secure campus network (SCN) scenario designing and simulating using the cisco packet tracer program. This paper presents a topology that contains four-building, with different networks and different types of devices. In each building, we separate the end devices into different VLANs for security purposes. Also, we applied security techniques for the routers that connect the networks and for switches that connect the end devices with each other to prevent outside or unauthorized accesses. Moreover, this paper shows the real weight of some protocols in connecting and securing the entire campus system.

REFERENCES

- [1] S. Pandey, "Modern Network Security: Issues and Challenges," *International Journal of Engineering Science and Technology (IJEST)*, vol. 3, no. 5, 2011.
- [2] M. N. Abdullah, I. A. Satam, R. W. Daoud, S. N. Shihab, and H. A. Kamel, "Design and implement a self-managed computer network for electronic exams and sharing," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 1, pp. 466-475, 2020, doi: 10.11591/ijeecs.v19.i1.pp466-475.
- [3] M. Naagas, E. Mique, and T. D. Palaoag, "Defense-through-deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack," *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 4, pp. 593600, 2018, doi: 10.11591/eei.v7i4.1349.
- [4] M. Jahanirad, A. L. N. Yahya, and R. M. Noor, "Comprehensive Network Security Approach: Security Breaches at Retail company-A Case Study," *IJCSNS International Journal of Computer Science and Network Security*, vol. 12, no. 8, 2012
- [5] X. Zhou, B. Li, Y. Qi, and W. Dong, "Mimic Encryption Box for Network Multimedia Data Security," *Hindawi* Security and Communication Networks, 2020.
- [6] L. T. Monther Aldwairi, "Security techniques for intelligent spam sensing and anomaly detection in online social platforms," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 275-287, 2020, doi: 10.11591/ijece.v10i1.pp275-287.
- [7] S. Liangxu, I. Wu, Y. Zhang, and H. Yin, "Comparison between physical devices and simulator software for Cisco network technology teaching," *omputer Science & Education (ICCSE), 2013 8th International Conference IEEE*, 2013, doi: 10.1109/ICCSE.2013.6554134.
- [8] N. Sanam, "Performance Evaluation of Wide Area Network using Cisco Packet Tracer," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, pp. 2915-2919, 2019, doi: 10.30534/ijatcse/2019/38862019.
- [9] I. Shemsi, "Boosting Campus Network Design Using Cisco Packet Tracer," *International Journal of Innovative Science and Research Technology*, vol. 2, no. 11, 2017.
- [10] S. Nagendram, K. Ramchand, and H. Rao, "Hybrid Security and Energy Aware Routing for Wireless Ad hoc Networks," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 2, 2019, doi: 10.35940/ijrte.b3659.078219.
- [11] P. Pathak, S. Majunder, C. Mondal, and M. K., "College Network Scenario Implementation by using Cisco Packet Tracer," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, no. 1, pp. 299-304, 2018.
- [12] Z. A. Jaaz, S. S. Oleiwi, S. A. Sahy, and I. A. Barazanchi, "Database techniques for resilient network monitoring and inspection," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no. 5, pp. 2412-2420, 2020, doi: 10.12928/TELKOMNIKA.v18i5.14305.
- [13] S. N. Sisat, "IP Subnetting," International Journal of Electronics, Communication & Soft Computing Science and Engineering, vol. 2, no. 5, pp. 5-9, 2013.
- [14] Md. A. Hossain, and M. Zannat, "Simulation and Design of University Area Network Scenario(UANS) using Cisco Packet Tracer," *Global Journal of Computer Science and Technology: G Interdisciplinary*, vol. 19, no. 3, 2019, doi: 10.34257/GJCSTGVOL19IS3PG7.
- [15] M. J. Arshad, A. Farooq, S. Ahsan, and M. Shahbaz, "A Path Towards IP-V6 Transition Strategies for Scientific Research: An Overview," *Life Science Journal*, vol. 9, no. 1, pp. 599-602, 2012.
- [16] J. D. McCabe, "Network Analysis, Design and Architecture," Elsevier Inc., 2007.
- [17] S. Isaac and J. Abdu, "Comparative Analysis Between IPv4 AND IPv6," International Journal of Information Systems and Engineering, vol. 3, no. 2, 2015, doi: 10.24924/ijise/2016.11/v4.iss2/20.26.
- [18] Z. Hamid and S. Daud, "A Comparative Study between IPv4 and IPv6," in *International Conference on Engineering, Technology & Vocational Education*, 2020.
- [19] O. K. Sulaiman, A. M. Siregar, K. Nasution, and T. Haramaini, "Bellman Ford algorithm in Routing Information Protocol (RIP)," in *Journal of Physics Conference Series*, 2018, doi:10.1088/1742-6596/1007/1/012009.
- [20] D. Liu, B. Barber, and L.Digrande, "Implementing RIP, Version 2," in Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit, Syngress, 2009, pp. 197-232.
- [21] V. Baggan, A. K. Sahoo, P. K. Sarangi, and S. P. Chaturvendi, "A comprehensive analysis and experimental evaluation of routing information protocol: An elucidation," *Materials Today: Proceedings*, 2020, doi: 10.1016/j.matpr.2020.10.676

- [22] C. Agwu, N. Nwogbaga, and O. Chukwuka, "The Proposed Roles of VLAN and Inter-VLAN Routing in Effective Distribution of Network Services in Ebonyi State University," *International Journal of Science and Research* (*IJSR*), vol. 4, no. 7, pp. 2608-2615, 2015.
- [23] S. S. Tambe, "Understanding Virtual Local Area Networks," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 25, no. 4, pp. 174-6, 2015.
- [24] Z. Zhang, "Analysis of Virtual Local Area Networking Technology," in 2016 6th International Conference on Machinery, Materials, Environment, Biotechnology and Computer, 2016.
- [25] M. Sudha, A. K., A. K., J. T., and J. Nelson, "Implementation of VLAN AND Inter VLAN in Corporate Networks," International Journal of Advanced Research (IJAR), vol. 8, no. 2, pp. 1074-1078, 2020, doi: 10.21474/IJAR01/10548.

BIOGRAPHIES OF AUTHORS



Alaa H. Ahmed, B. Sc Computer Science-College of Science-University of Kirkuk-Iraq. M.Sc Comuter Science-College of Arts and Sciences- The University of North Carolina at Greensboro-USA. Assistant lecturer-University of Kirkuk-Iraq. Research interest. Data Mining, Darta Fusion, Database, Machine Learning, Networking, and any new techniques and subjects in computer science.



Mokhaled N. A. Al-Hamadani, B. Sc Computer Science-College of Science-University of Kirkuk-Iraq. M.Sc Comuter Science-College of Arts and Sciences-The University of North Carolina at Greensboro-USA. Assistant lecturer-Northern Technical University-Iraq. Research interest. Big Data, Deep Learning, Machine Learning, Database, Networking, and any new techniques and subjects in computer science.