**BONUS LAB ASSIGNMENT**

**(FIND THE IMPOSTER)**

Akshit Puri

Cyber Security, Loyalist College of Applied Arts and Technology

CYSE2001: Secure Network Infrastructure

Instructor: Peter Wheeler

28th September 2022

Firstly, we will keep all the Switch MAC address tables populated by typing "ping -t 10.9.9.255" on PC0's Command Prompt

Graphical user interface, application

Description automatically generated

Starting from Switch0, using ‘show mac address-table to trace the location of each

Malicious acting MAC addresses.

Graphical user interface, application

Description automatically generated

We have been informed that the following three MAC addresses are acting maliciously:

- 0006.2a55.34de

- 0000.0c07.be8e

- 0001.9666.3d1b

And by looking at the mac-address-table of Switch 0 we will get to know that all these maliciously acting mac addresses are connected to **Fast Ethernet 0/1.**

The Switch0’s FastEthernet0/1 is connected to Switch1

Now we must check the mac-address-table of Switch1 to trace the location of the suspicious mac-address.

Graphical user interface, application

Description automatically generated

by looking at the mac-address-table of Switch 1 we will get to know that all these maliciously acting mac addresses are connected to **Fast Ethernet 0/2.**

The Switch1’s FastEthernet0/2 is connected to Switch4

Now we must check the mac-address-table of Switch4 to trace the location of the suspicious mac-address.

Graphical user interface, application

Description automatically generated

From this mac-address table, we can see that the malicious mac-address is connected to which Fast Ethernet Port.

- 0006.2a55.34de = FastEthernet 0/5

- 0000.0c07.be8e = FastEthernet 0/3

- 0001.9666.3d1b = FastEthernet 0/2

The Switch4’s FastEthernet0/5 is connected to Switch12

The Switch4’s FastEthernet0/3 is connected to Switch10

The Switch4’s FastEthernet0/2 is connected to Switch9

Now we must check the mac-address-table of Switch9, Switch10 & Switch12 to trace the location of the suspicious mac-address.

**SWITCH 12:**

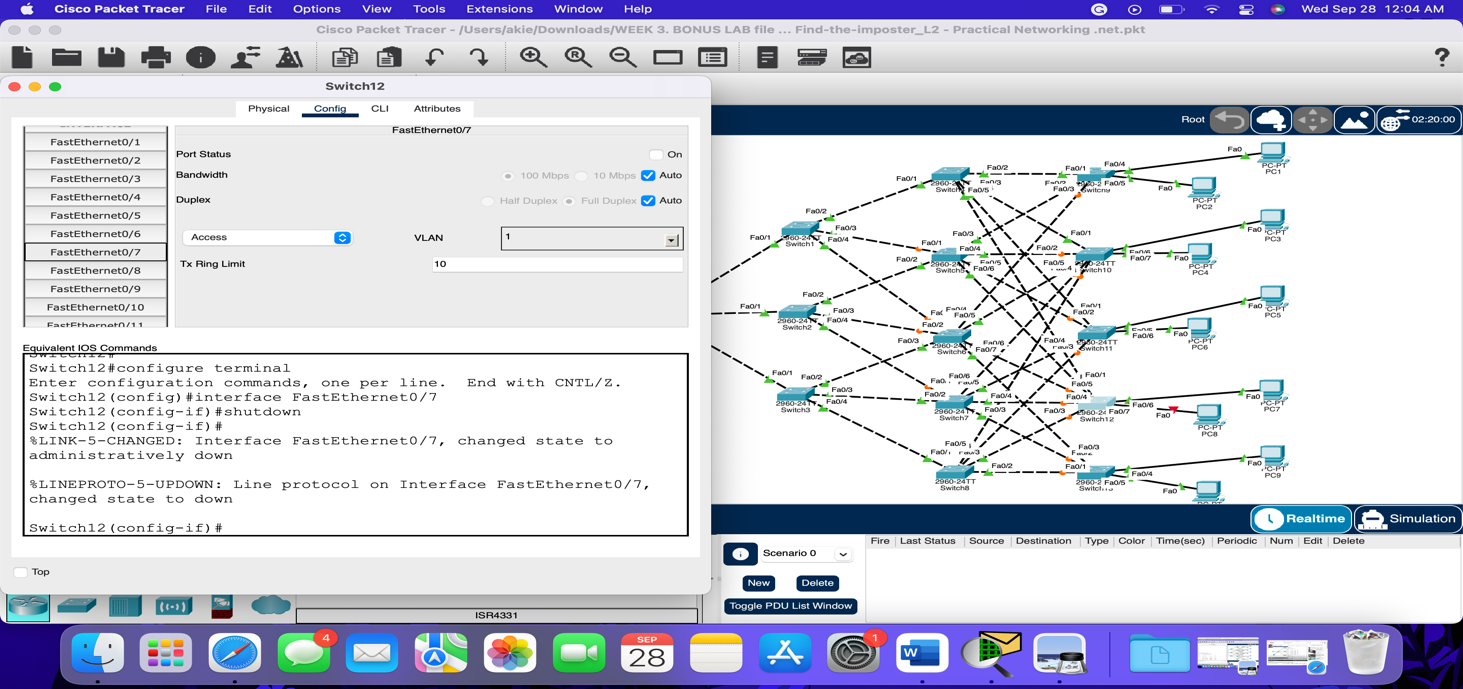
**Graphical user interface, application

Description automatically generated**

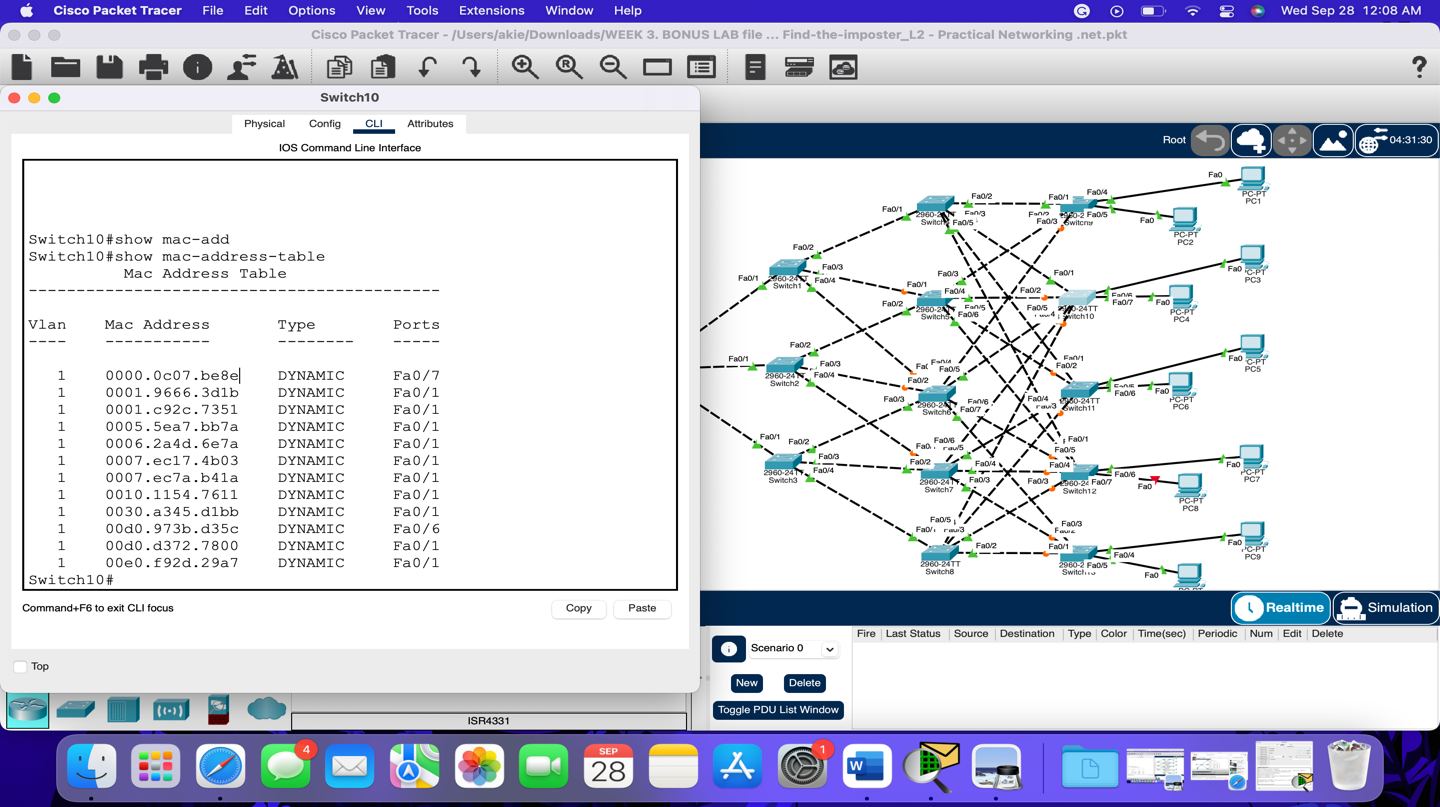
by looking at the mac-address-table of Switch 12 we will get to know that the “0006.2a55.34de “ maliciously acting mac address is connected to **Fast Ethernet 0/7.**

The Switch12’s FastEthernet0/7 is connected to PC8

Now we shut down the port Fa0/7 of Switch 12 to disconnect from the ***0006.2a55.34de*** maliciously acting mac-address.

****

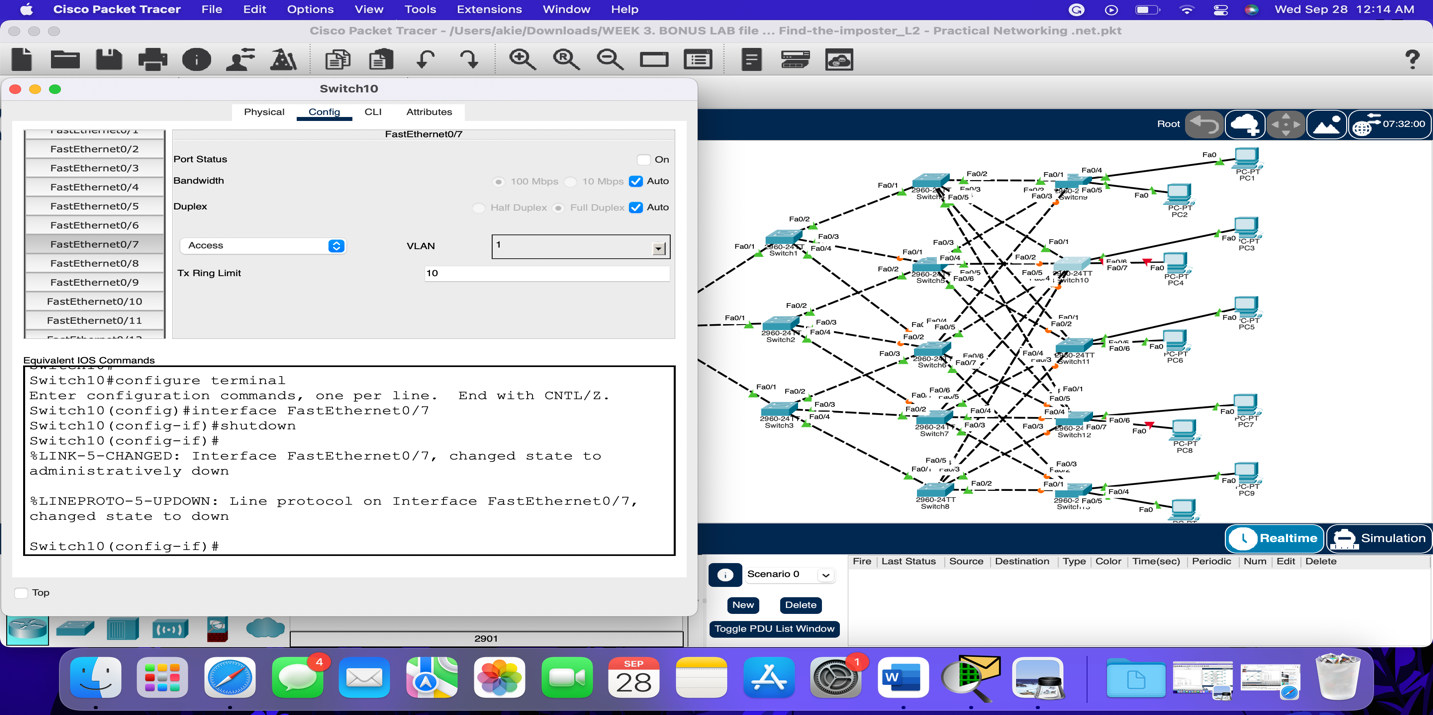
**SWITCH 10:**



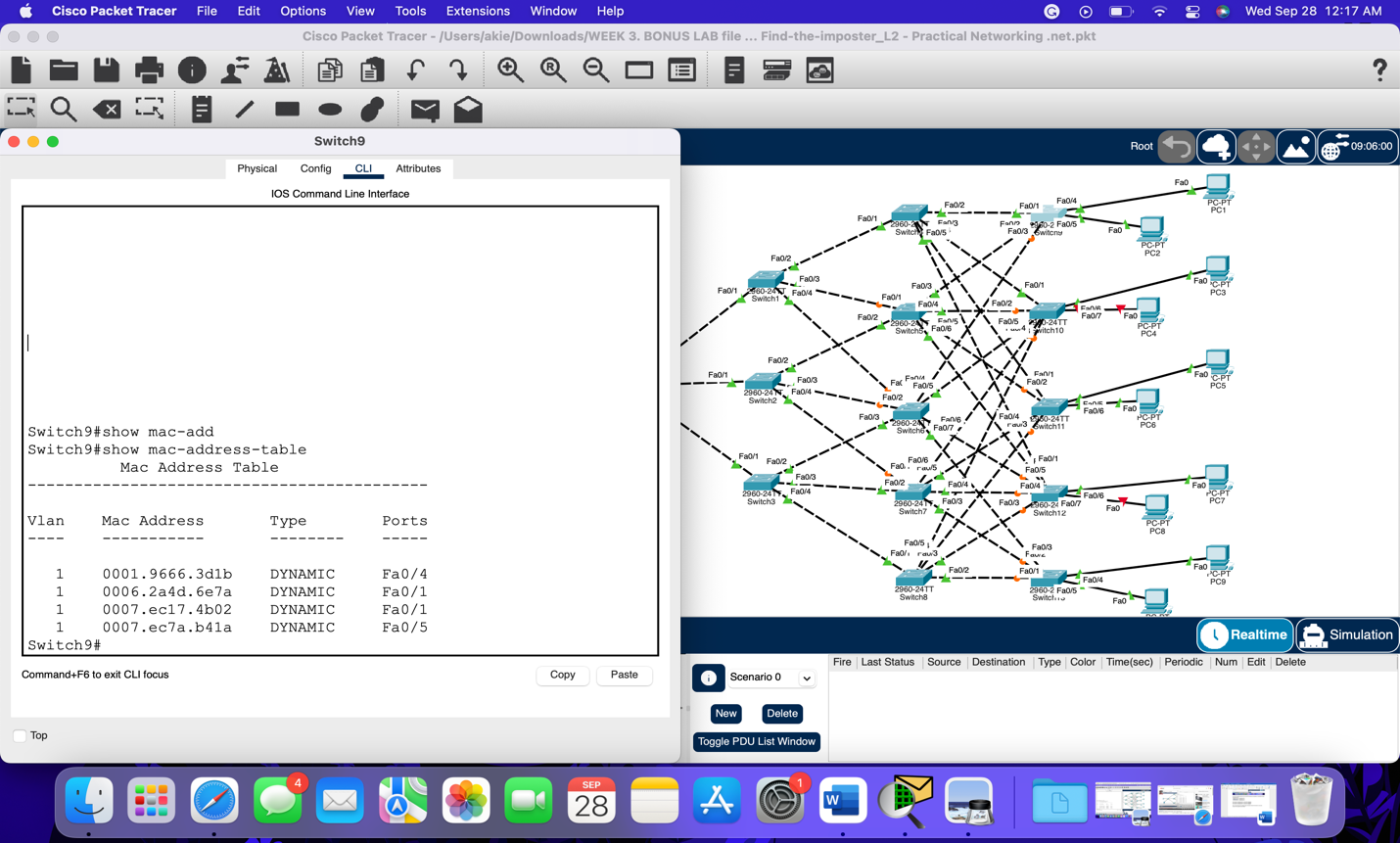
by looking at the mac-address-table of Switch 10 we will get to know that “0000.0c07.be8e” maliciously acting mac address is connected to **Fast Ethernet 0/7.**

The Switch10’s FastEthernet0/7 is connected to PC4

Now we shut down the port Fa0/7 of Switch 10 to disconnect from the ***0000.0c07.be8e*** maliciously acting mac-address.



**SWITCH 9:**

****

by looking at the mac-address-table of Switch 9 we will get to know that the “0001.9666.3d1b” maliciously acting mac address is connected to **Fast Ethernet 0/4.**

The Switch9’s FastEthernet0/4 is connected to PC1

Now we shut down the port Fa0/1 of Switch 9 to disconnect from the ***0001.9666.3d1b*** maliciously acting mac-address.

**Graphical user interface, text, application

Description automatically generated**

**Thus, the imposters are PC1, PC4 & PC8**. At Last, we can ping again from PC0.

Graphical user interface, application

Description automatically generated

Previously we are getting 11 ping responses in PC0 Command Prompt but now only 8 ping responses because 3 maliciously acting ports and disabled.

Also, the Mac-address table of Switch0 is not showing any Maliciously acting mac addresses.

Graphical user interface, application

Description automatically generated