Imposter Assignment

=== To Start the lab:
1. Fast Forward time a few minutes (or just wait)
2. Open PC0's Command Prompt
3. Type "ping -t 10.9.9.255"
(You should receive 11 ping responses)
4. This will keep all the Switch MAC address tables populated

=== LAB Task:

You have been informed that the following three MAC addresses are acting maliciously:
- 0006.2a55.34de
- 0000.0c07.be8e
- 0001.9666.3d1b

Starting from Switch0, use `show mac address-table` to trace the location of each MAC address above and shutdown their port.

I will be performing the below steps to find the 3 MAC addresses which are acting maliciously.

Summary of the Solution -:

I will be going to each Switch and find the interface and MAC addresses and then find the next switch.

So, by using below two commands we will find the imposter MAC address.

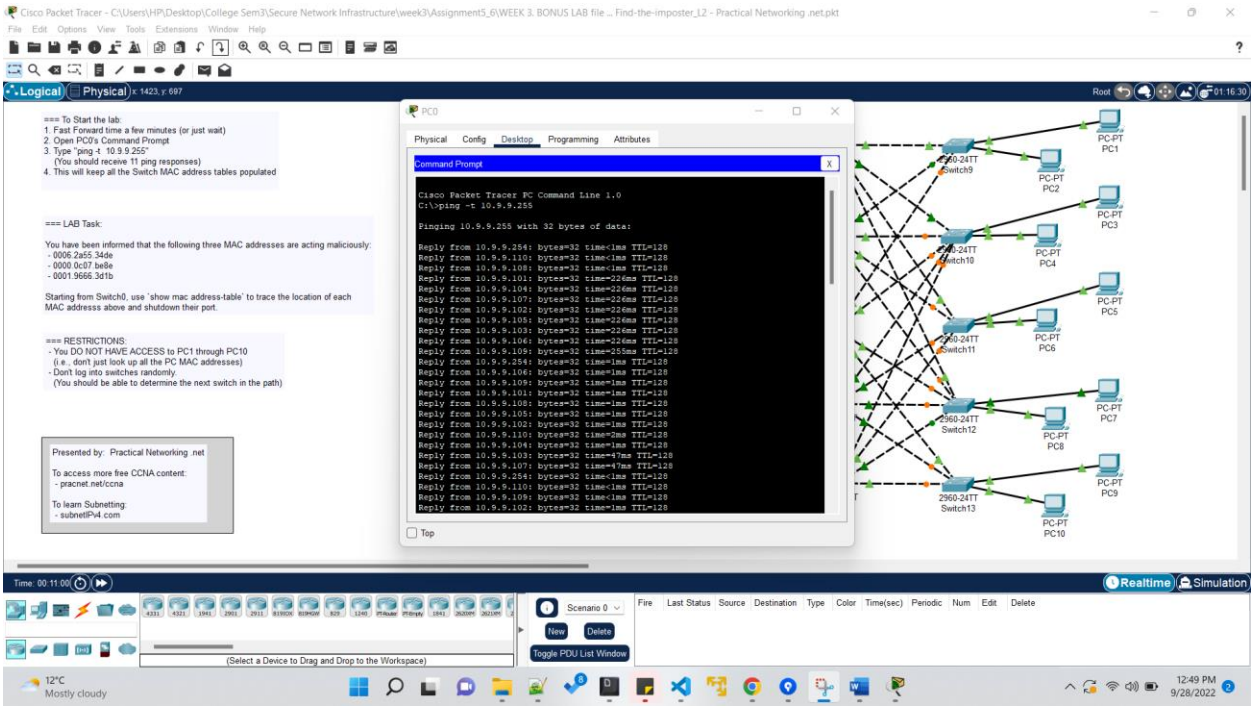
a. **show mac address-table -:** This command will the MAC address table in switch.
b. show cdp neighbors -: This command will the interfaces/port no. associated to which device with the Switch.

Issue Faced.

I faced one issue while doing this lab, issue was – I was not getting the Malicious MAC address in the Switch 9 and 10 as I stopped the ping command from PC0 in the background. But when I executed the PIN command in PC0, then I got all the MAC addresses and port no.s in the Switch 9 and 10.

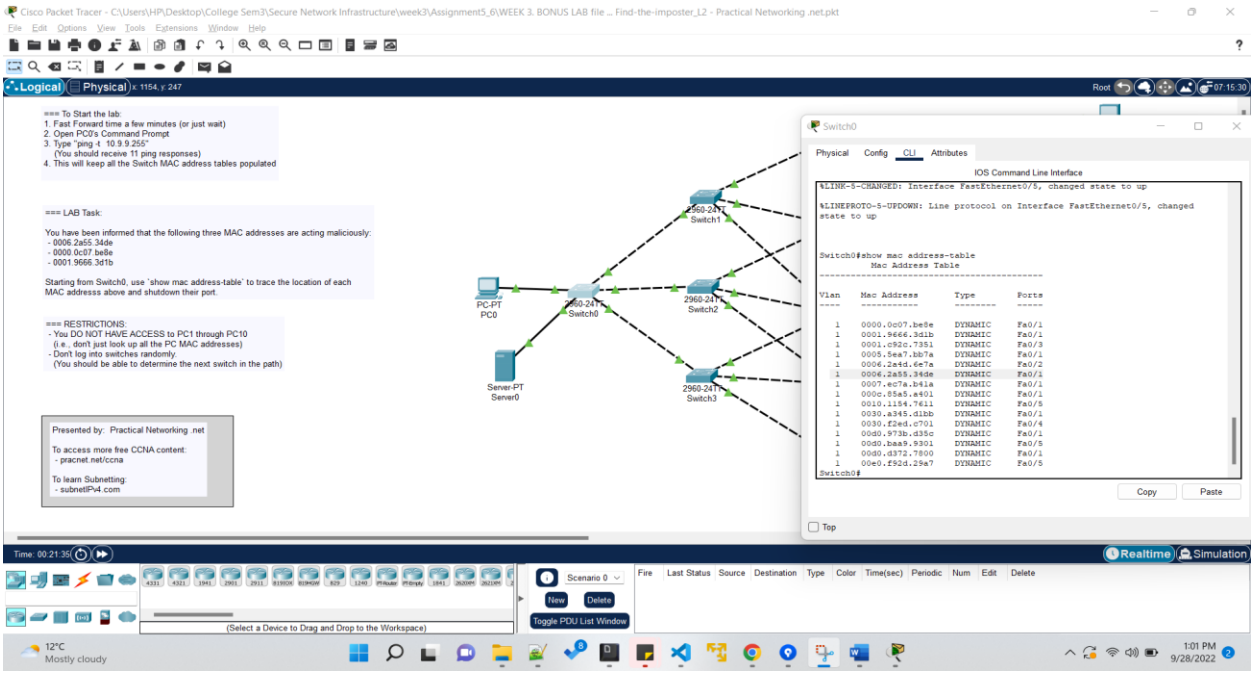
1. **Firstly perform, ping on PC1**

ping -t 10.9.9.255

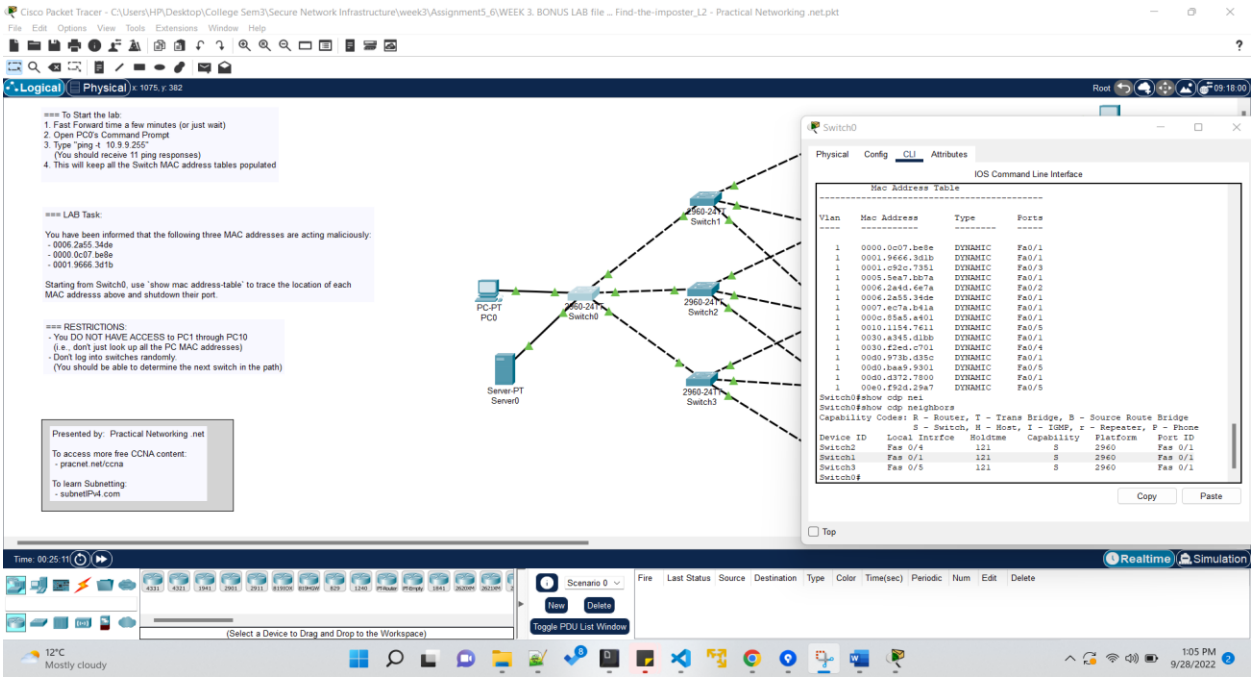


1. Now we will find this 0006.2a55.34de this MAC address.

Now Navigate to the Switch0 and run below two commands to find the Imposter.

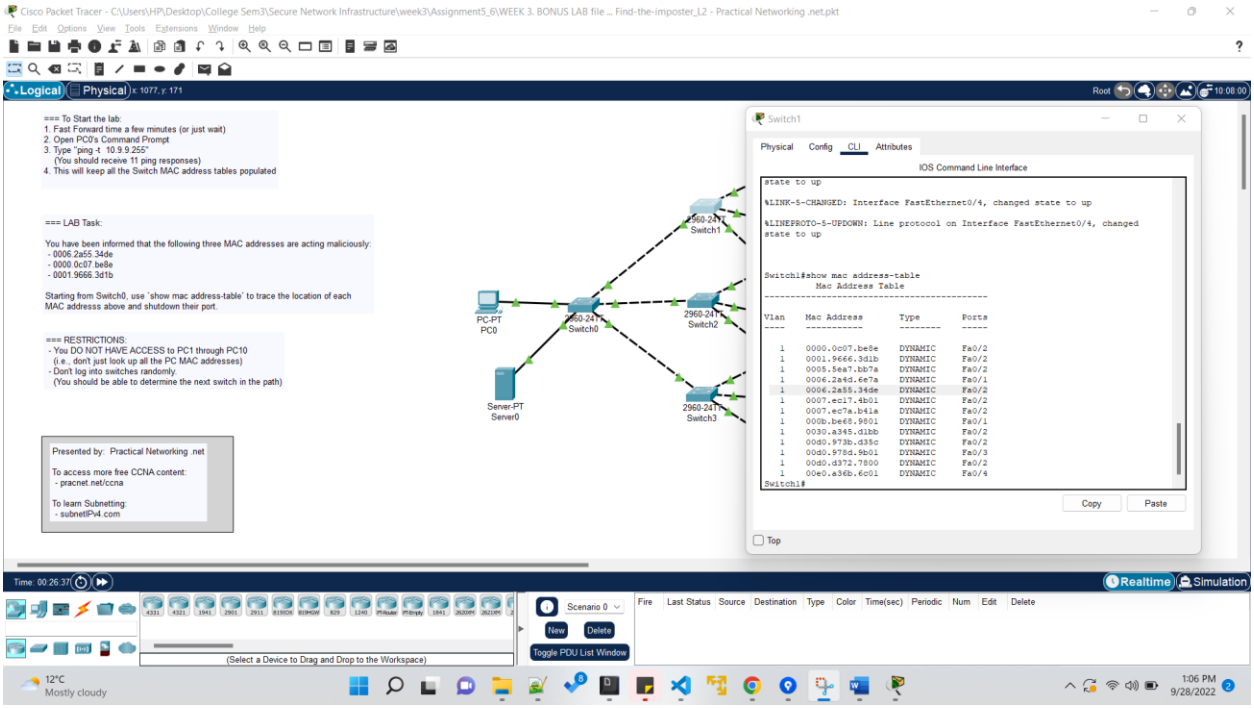


In the above step we found the MAC address and port number, but we are not sure which Switch we should check next. So, we will be running another command to find Switch with the F0/1 port.

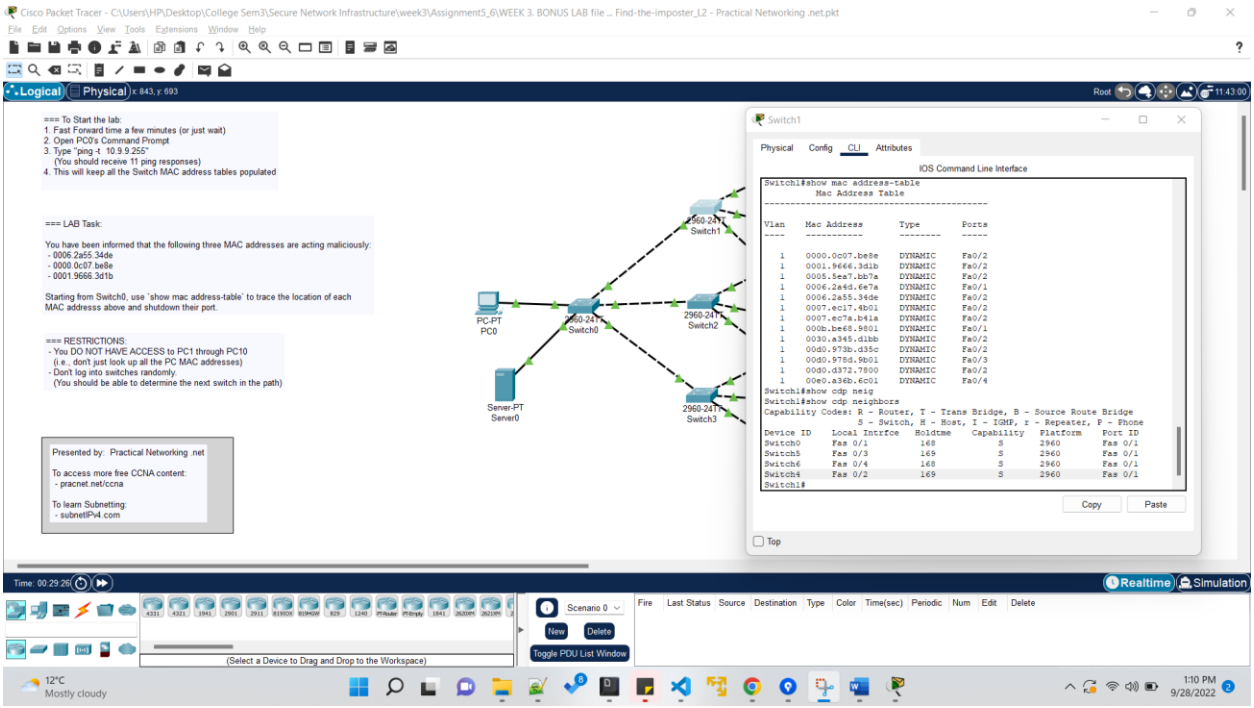


Now with above step we know that F0/1 is assigned to Switch1.

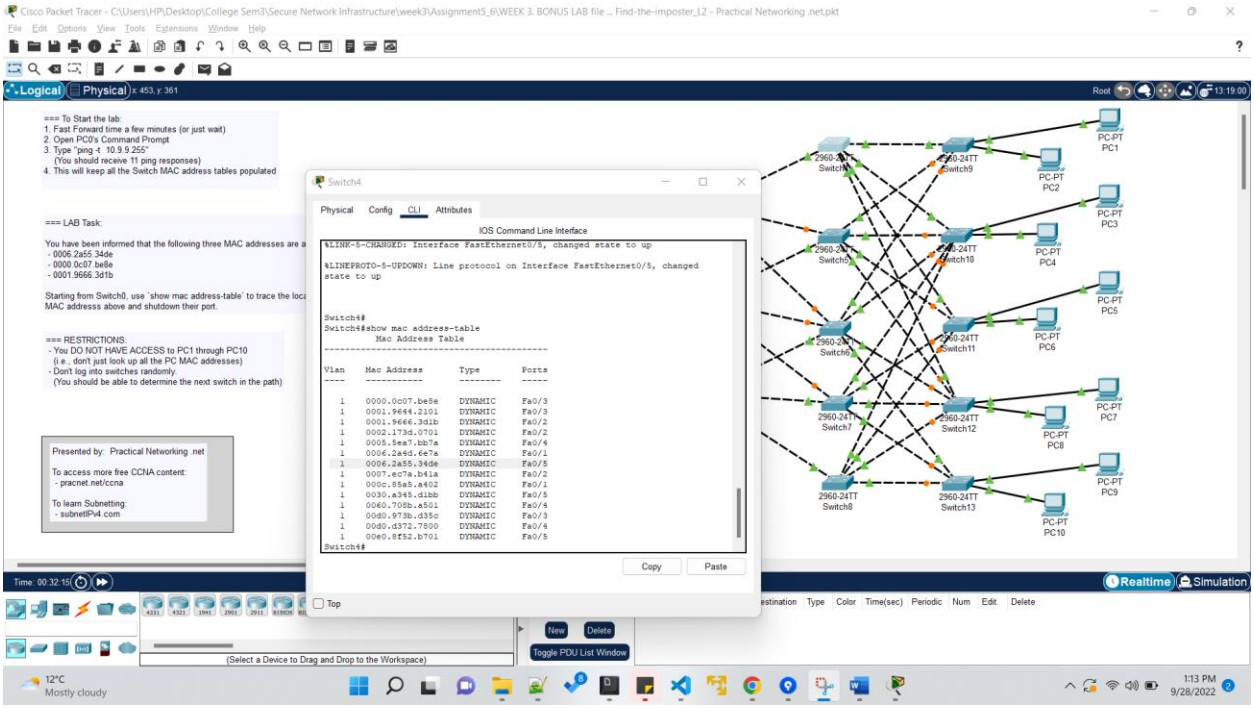
So, we will open the Switch1 and perform same Commands to find the Next Switch.



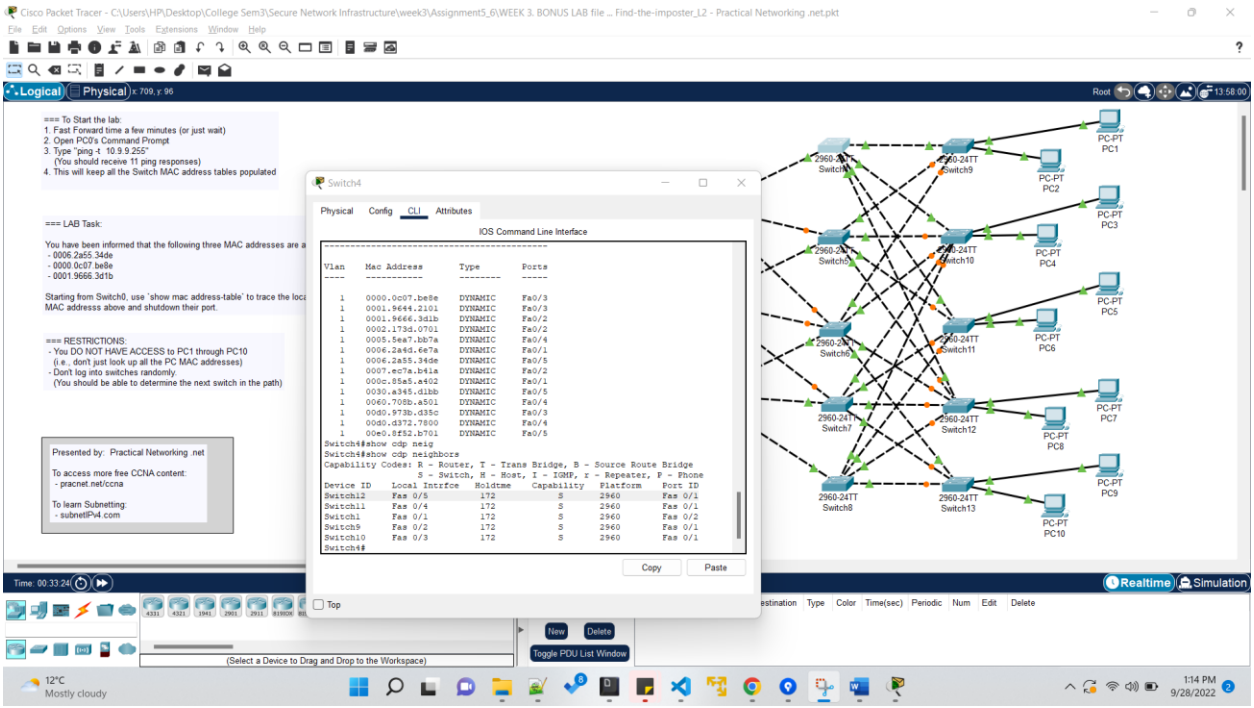
Now we know that port no. for the MAC address is Fa0/2, now we need to find the next switch with Fa0/2 port.



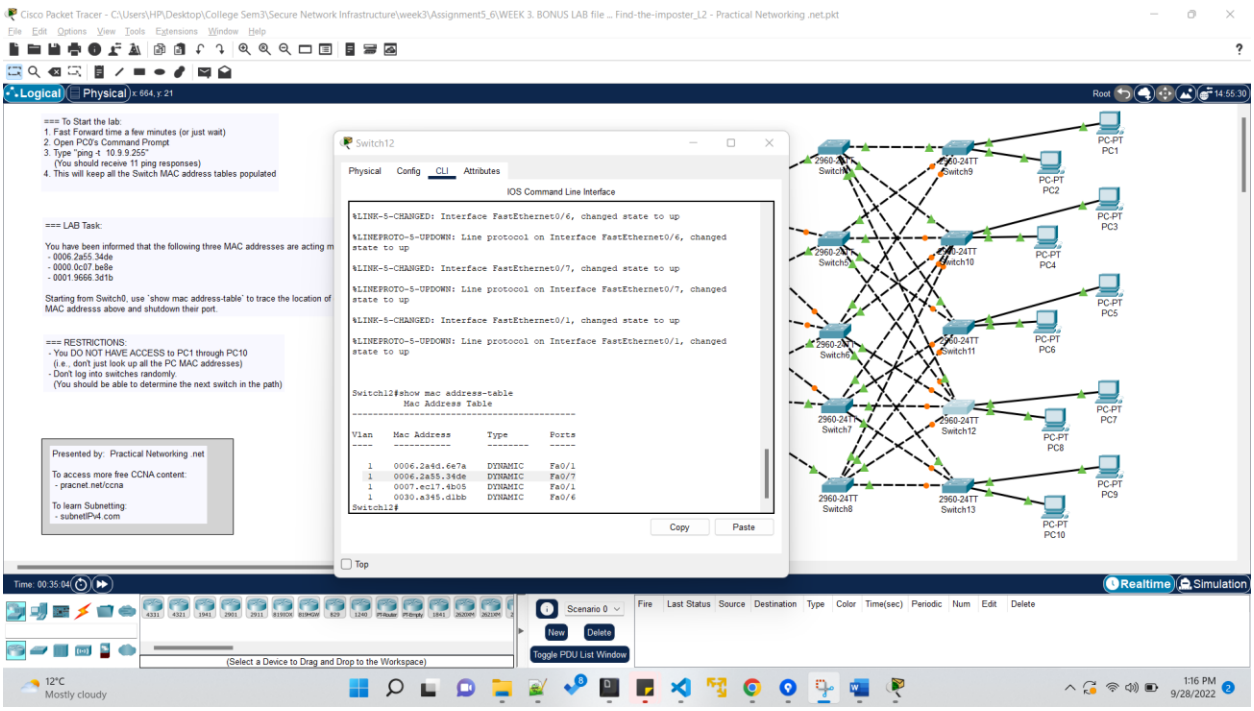
Now we found that Fa0/2 is at Switch4. Now we will open the Switch4 and check the next PC who is holding the imposter MAC address. With same commands.



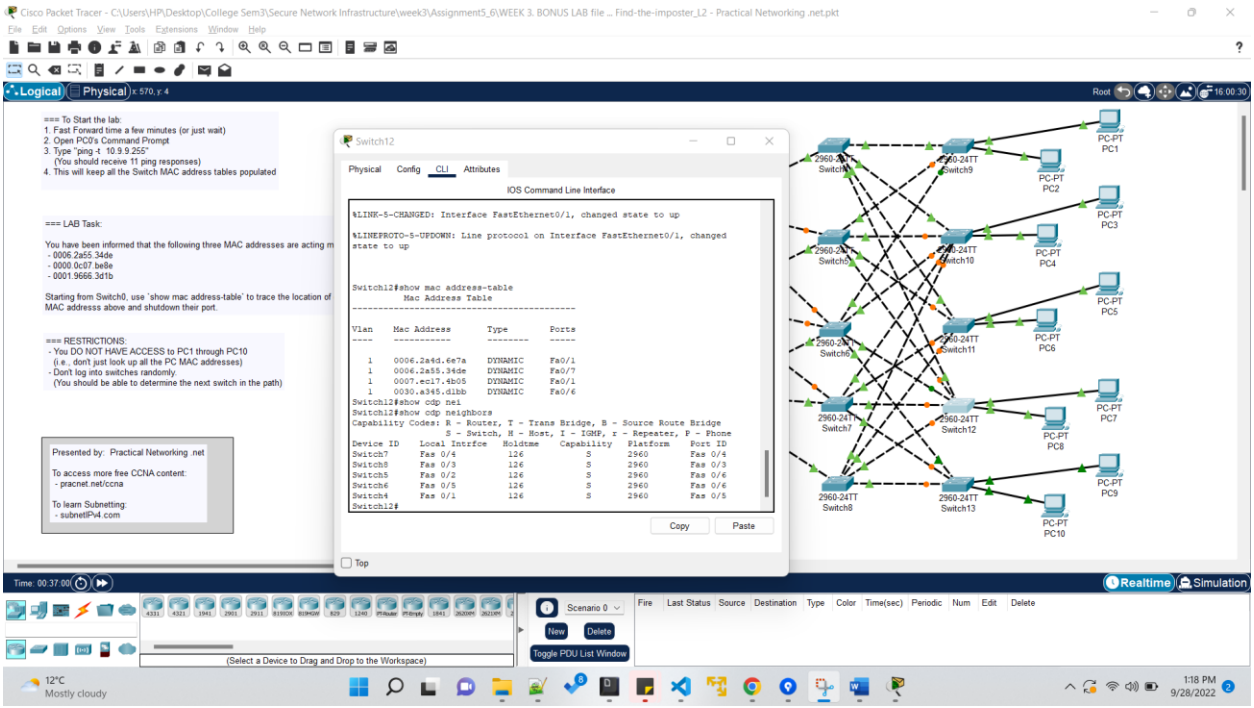
Now we found the Malicious MAC address is using port no. Fa0/5, now we need to find the next switch which is using this port.



Now we found the Switch12 is using Fa0/5 port, SO now we will open the Switch5 and run commands to find the MAC address table.



Now we know the port Fa0/7 s using the malicious MAC address SO now we need to find the which PC is using that port.



With **#show cdp neighbors**, we are not able to find the Fa0/7 port using cisco discovery protocol command. So we will try to shutdown the interface and see in the packet tracer if any connection is broken.

To shut down the interface. We will move to the configuration mode and then navigate to the Fa0/7 port and shut it down.

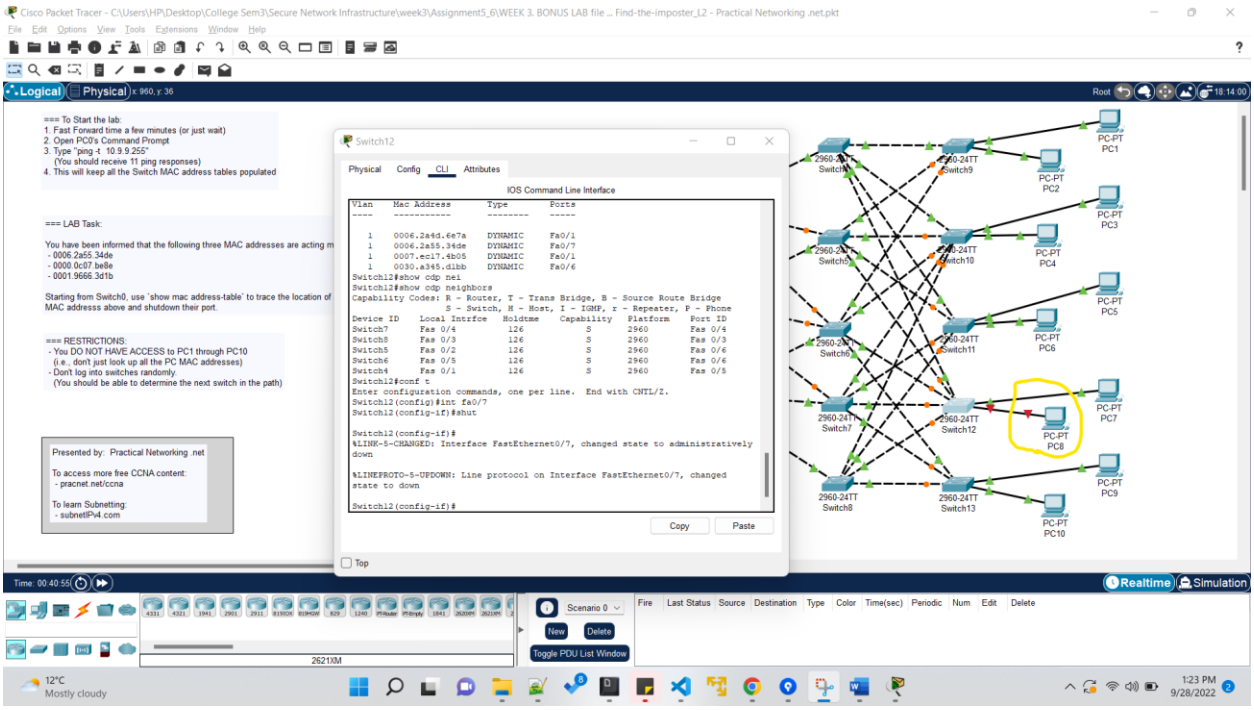
We used below commands

Switch12#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
Switch12(config)#**int fa0/7**
Switch12(config-if)#**shut**

Switch12(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

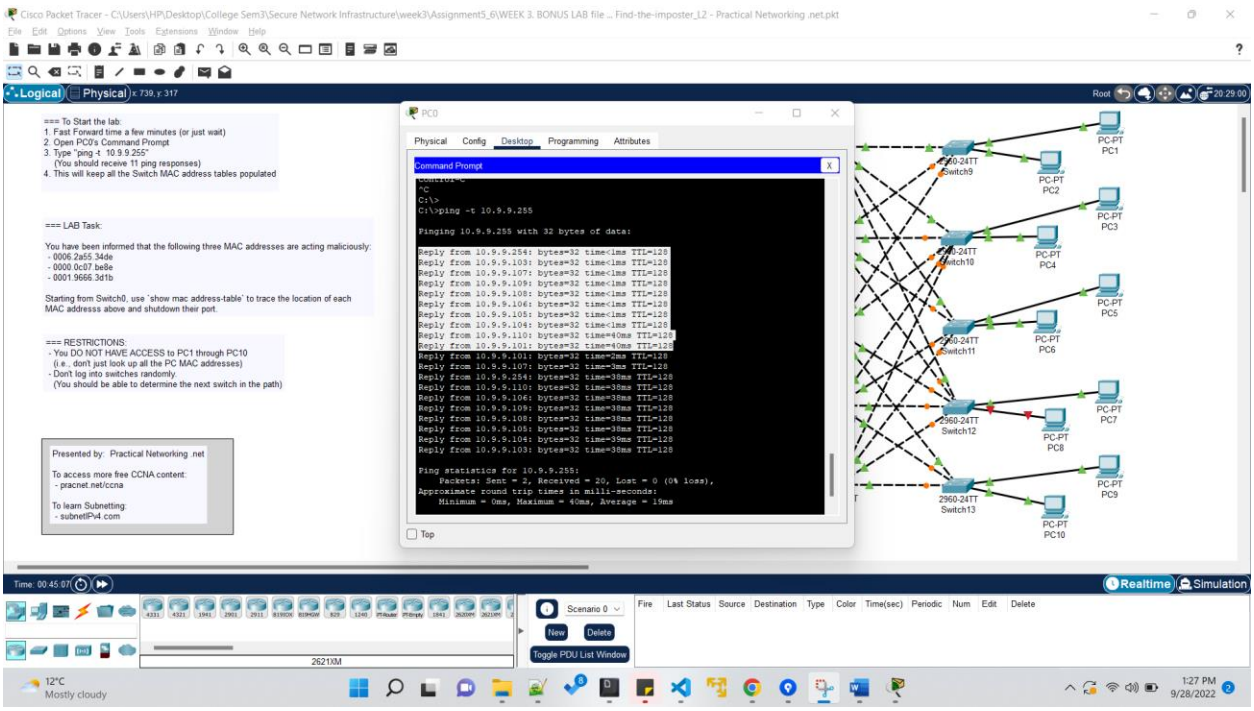
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down

Switch12(config-if)#



Now we will check with the PING command whether 1 PC is shutdown or not.

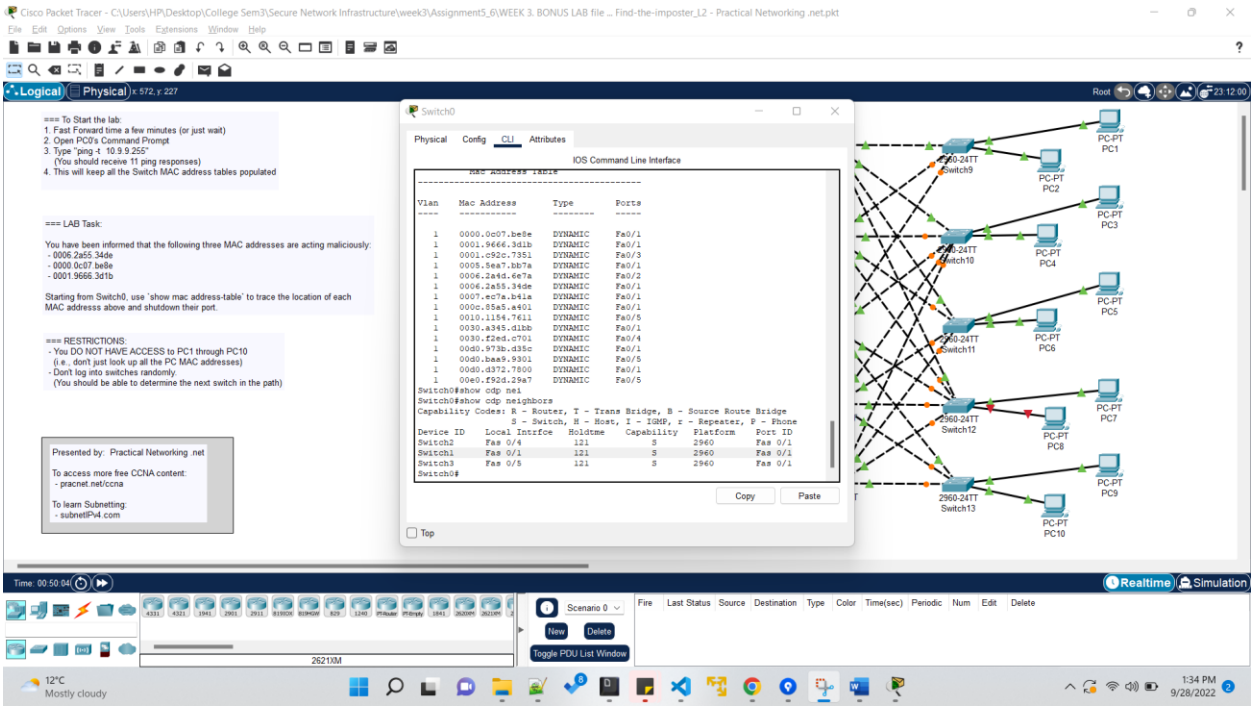
So here also it is showing only response from 10 Ips.



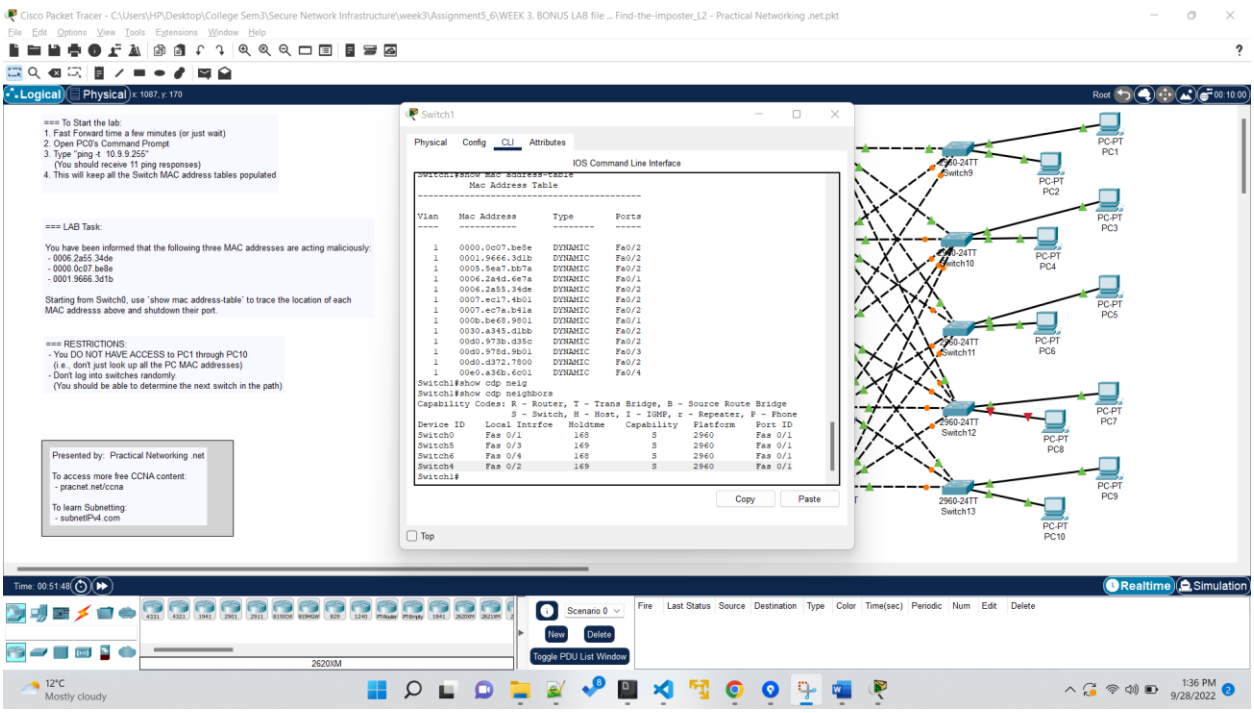
So with above steps we found that, PC8 was using the 0006.2a55.34de malicious MAC Address. Now we will try to find other two Malicious MAC addresses.

2. Now we will find this 0000.0c07.be8e MAC address.

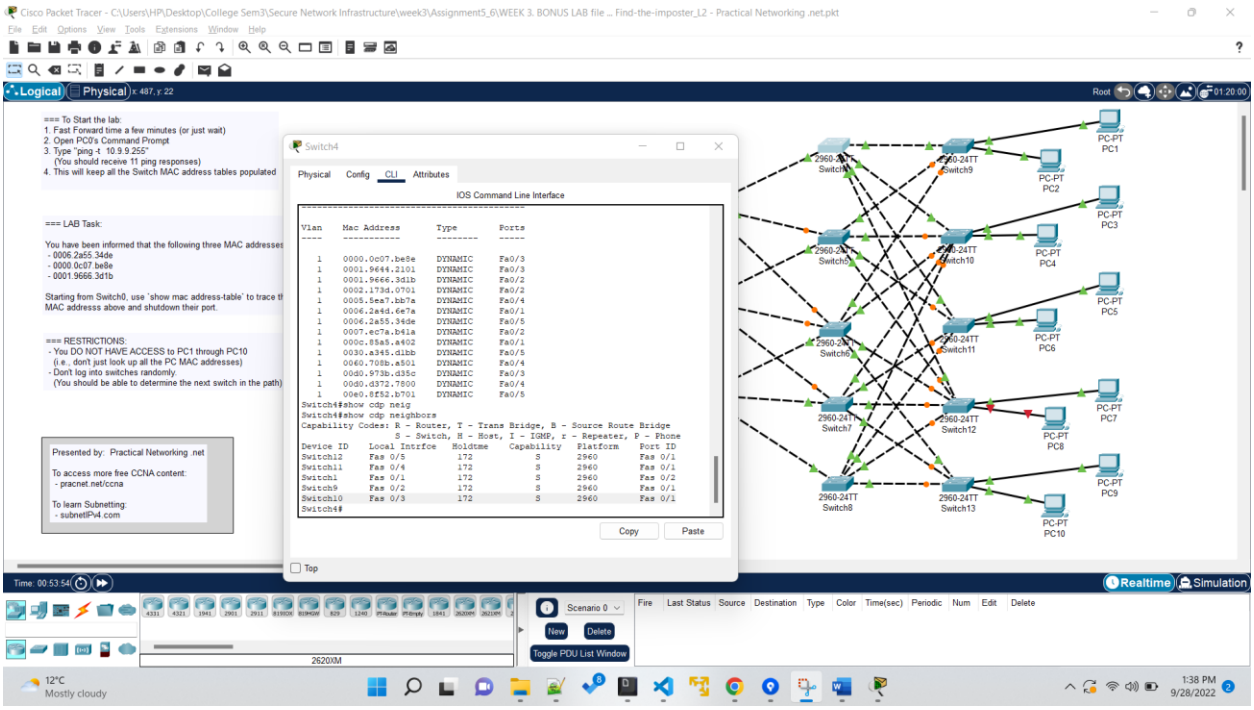
Open the Switch0 and repeat the same steps again.



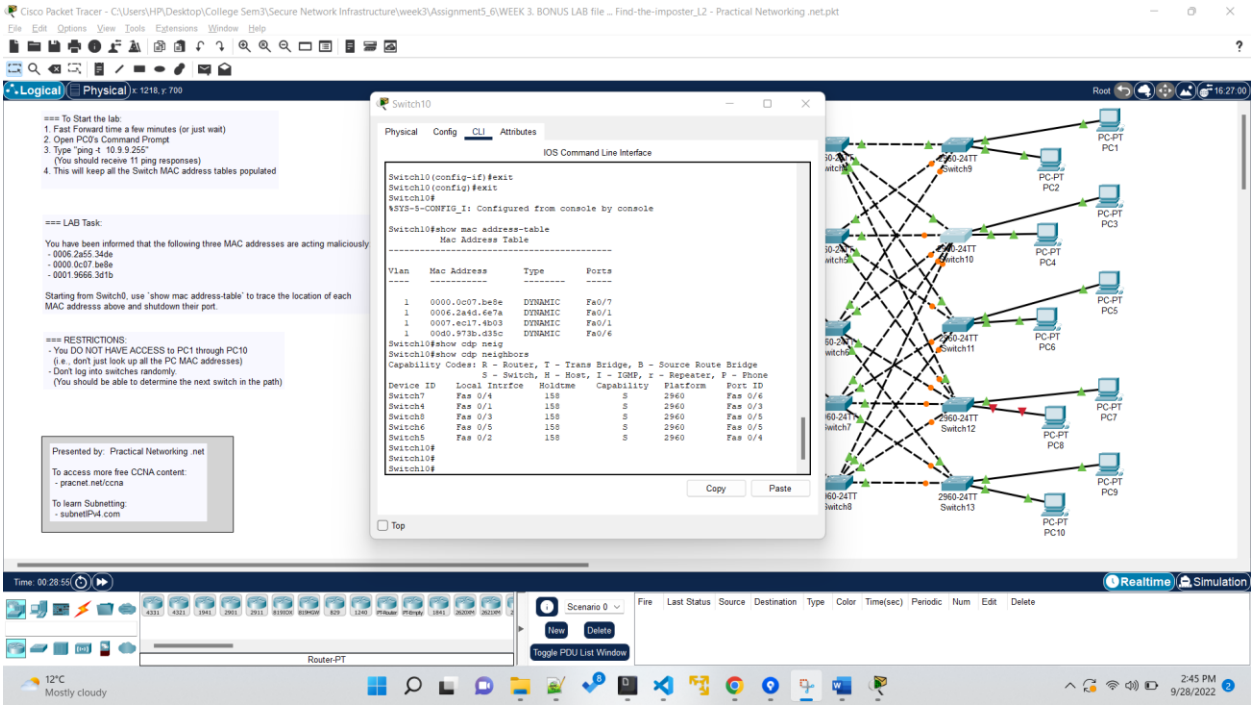
With above step in Switch0, we found that port F0/1 is holding the MAC address and F0/1 port is assigned to the Switch1.



With above step in Switch1, we found that port F0/2 is holding the MAC address and F0/2 port is assigned to the Switch4.

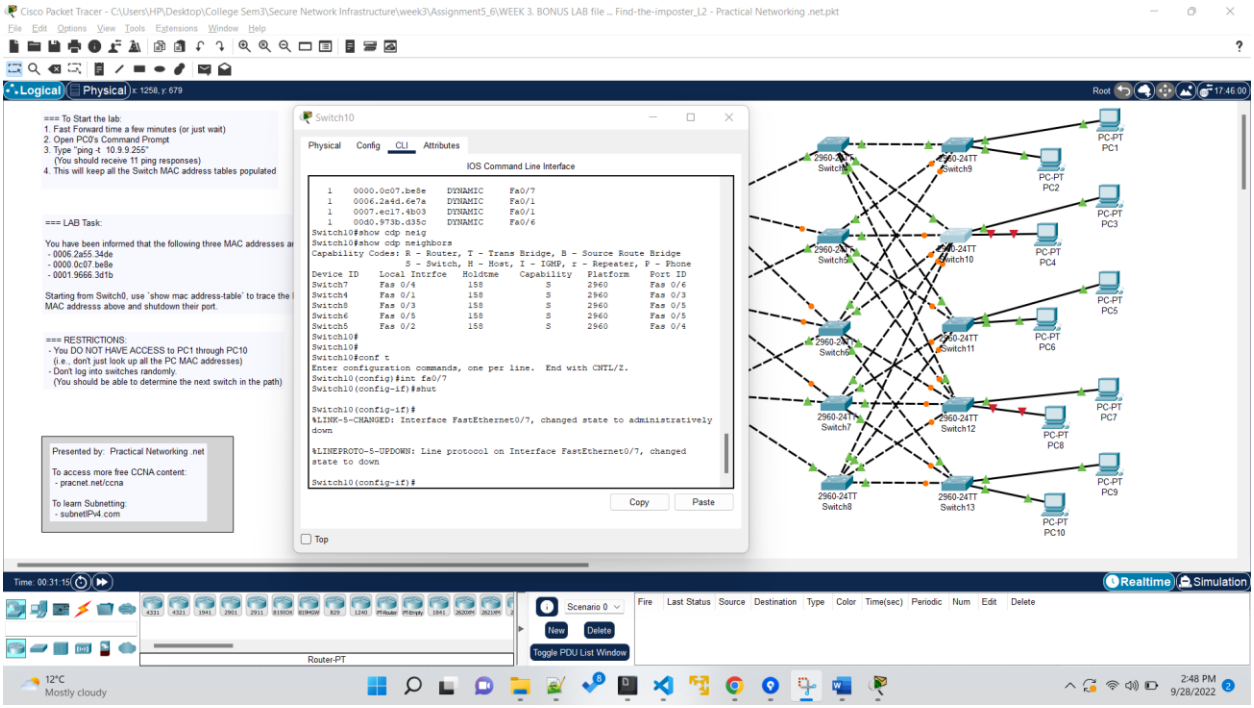


With above step in Switch4, we found that port F0/3 is holding the MAC address and F0/3 port is assigned to the Switch10.



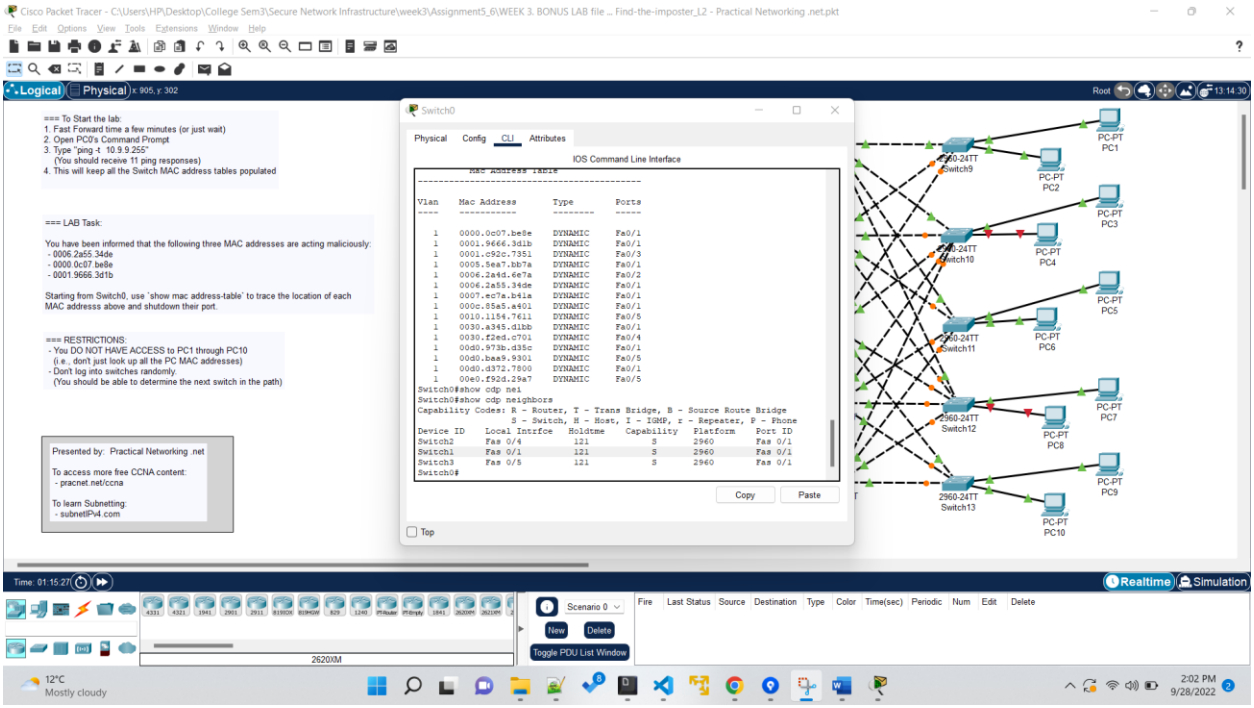
Its fa0/7 interface which have this malicious MAC address.

Now shutdown this port and check which PC is disconnected.

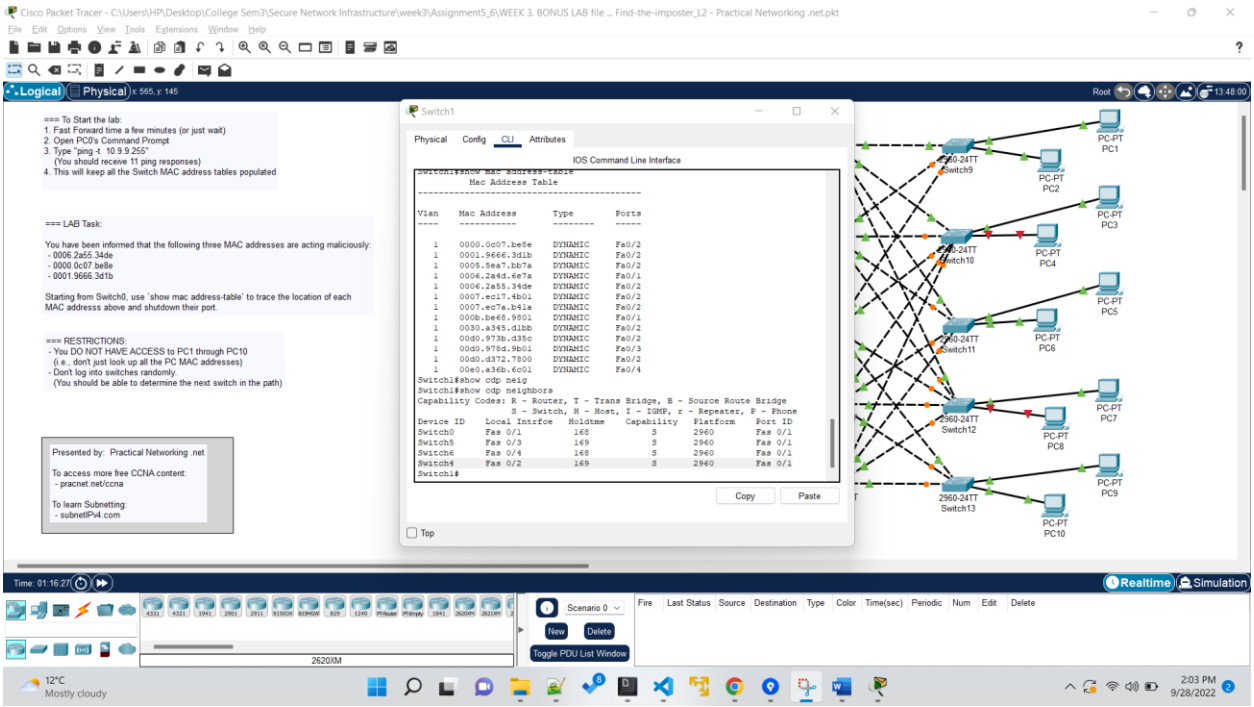


3. Now we will find this 0001.9666.3d1b this MAC address.

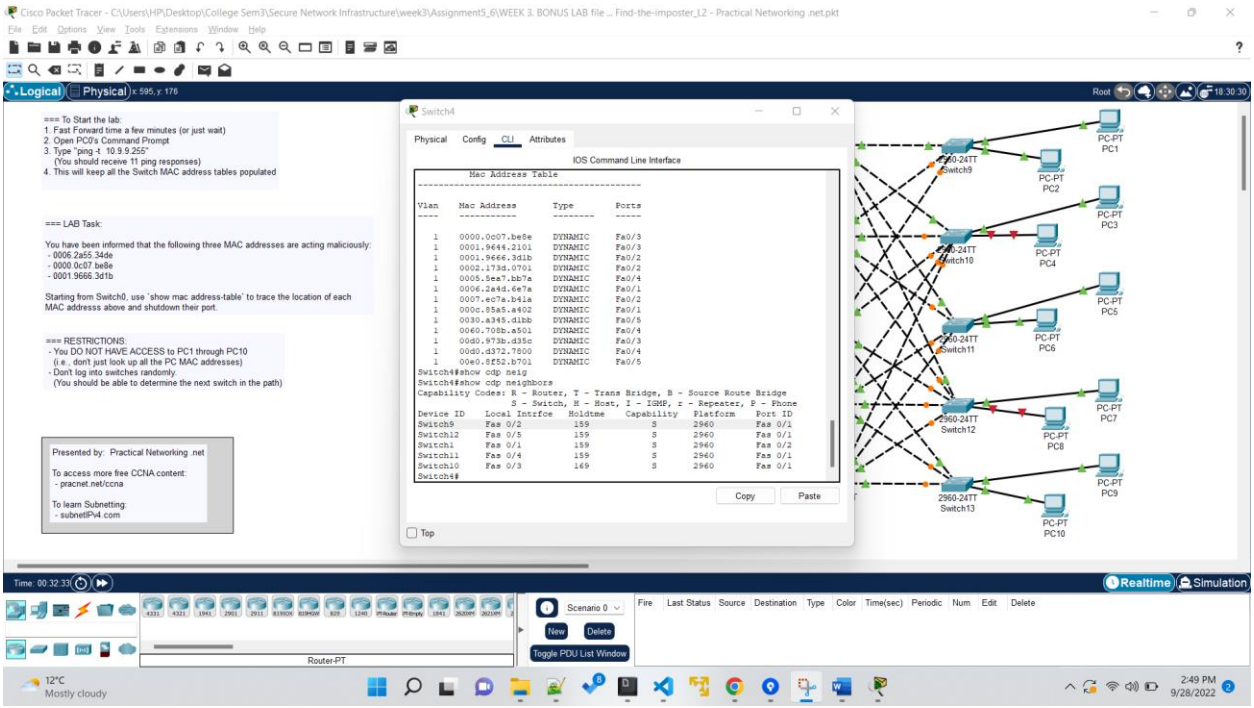
Open the Switch0 and repeat the same steps again.



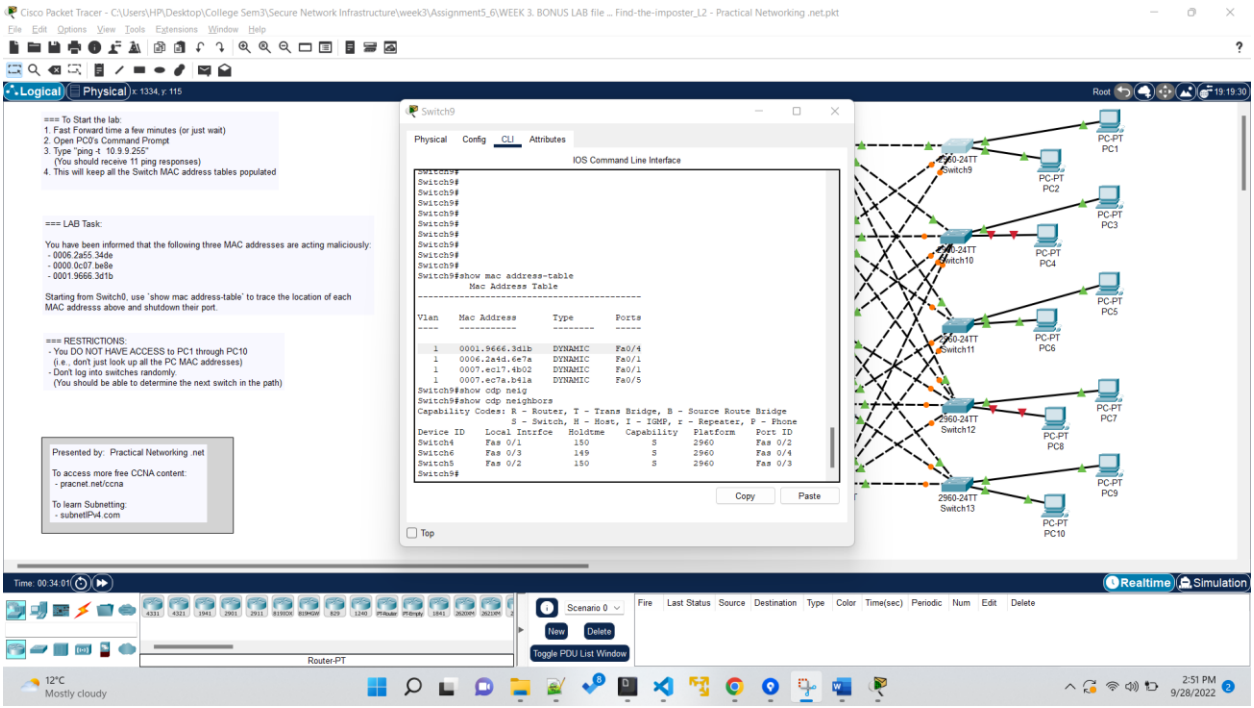
With above step in Switch0, we found that port F0/1 is holding the MAC address and F0/1 port is assigned to the Switch1.



With above step in Switch1, we found that port F0/2 is holding the MAC address and F0/2 port is assigned to the Switch4.

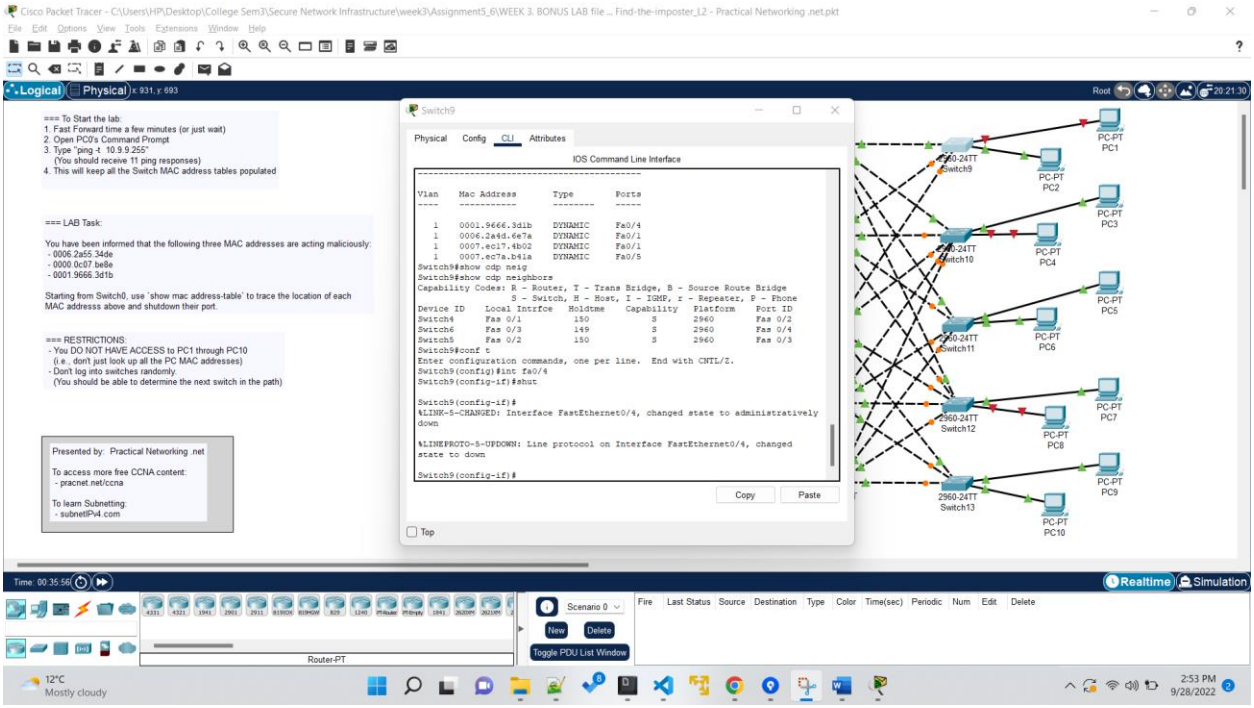


With above step in Switch4, we found that port F0/2 is holding the MAC address and F0/2 port is assigned to the Switch9.



Its fa0/7 interface which have this malicious MAC address.

Now shutdown this port and check which PC is disconnected.



TO verify the malicious MAC addresses, we will check the MAC address of the disconnected PCs for the validation.