L2 - GSBWiFi: Single Device Restriction via MAC-Based Access Explanation

A student in a dormitory reported being able to connect to the Wi-Fi with only one device. When attempting to connect a second device (e.g., a laptop) using the same username and password, access was denied. Although both devices could authenticate successfully in the login portal, only the first device could actually use the network.

Access Attempt:

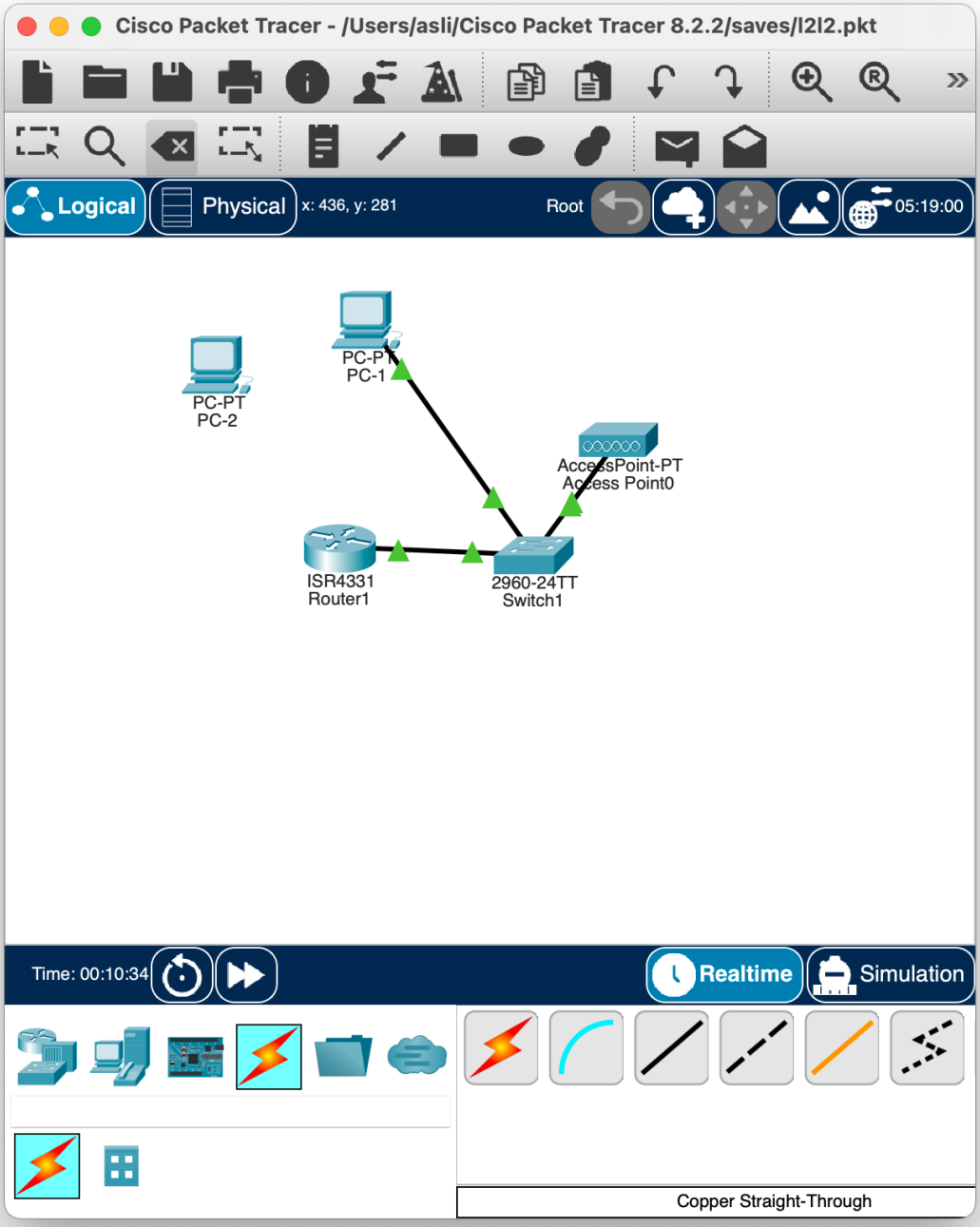
Device 1 connects → success
Device 2 connects using same credentials → blocked
Ping fails from second device even though IP and DNS may appear configured

On inspecting the switch CLI configuration, it was observed that Port Security was active with sticky MAC learning:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#copy running-config startup-config
                ^
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
show port-security interface FastEthernet0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00D0.FFC4.6B38:1
Security Violation Count   : 0

Switch#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

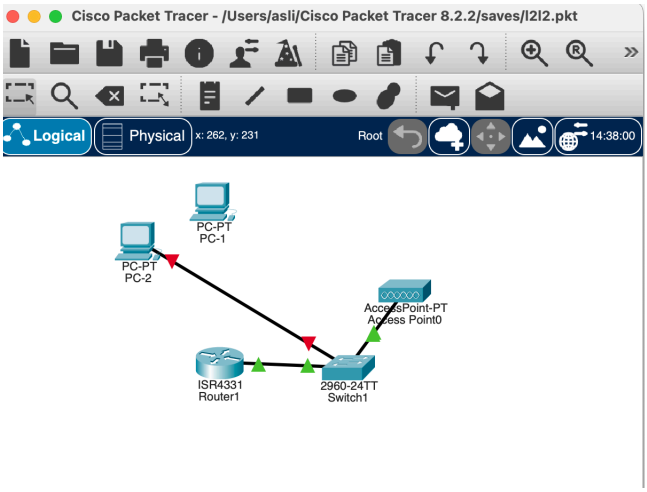
```
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00D0.FFC4.6B38:1
Security Violation Count   : 0

Switch#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch#show port-security interface FastEthernet0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0004.9A63.E76C:1
Security Violation Count   : 0

Switch#
```



Troubleshooting Steps:
Verified that PC1 (device 1) had a MAC like 00D0.FFC4.6B39.
PC2 (device 2) had a different MAC like 0004.9A63.E76C.
When PC1 was removed and PC2 plugged into the same port, the switch shut down the port due to the MAC mismatch.
Running show port-security interface FastEthernet0/1 revealed the violation and learned MAC.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time=12ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

To trigger the Switch's Port Security feature to activate, I sent ping.
The Switch learns the MAC address only with data traffic coming from that port.
Just plugging in the cable is not enough.
Sending an active packet like a ping causes the switch to "see" a new MAC address coming from that port.



This issue is strictly within the OSI Layer 2 – Data Link Layer.
MAC filtering and sticky MAC address learning are L2 functions, as they operate using MAC addresses and affect frame-level transmission between directly connected nodes.
Even if two devices have valid IP settings and proper physical connections, communication fails if the switch restricts MAC-level access.