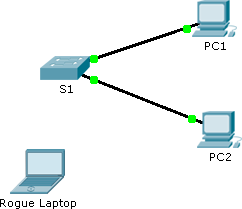


**Packet Tracer - Configuring Switch Port Security** (Instructor Version)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology



**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |
| PC2 | NIC | 10.10.10.11 | 255.255.255.0 |
| Rogue Laptop | NIC | 10.10.10.12 | 255.255.255.0 |

**Objective**

### Part 1: Configure Port Security Part 2: Verify Port Security

**Background**

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port’s ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

# Part 1: Configure Port Security

1. Access the command line for **S1** and enable port security on Fast Ethernet ports 0/1 and 0/2.

S1(config)# **interface range fa0/1 - 2**

S1(config-if-range)# **switchport port-security**

1. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

S1(config-if-range)# **switchport port-security maximum 1**

### Packet Tracer - Configuring Switch Port Security

1. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

S1(config-if-range)# **switchport port-security mac-address sticky**

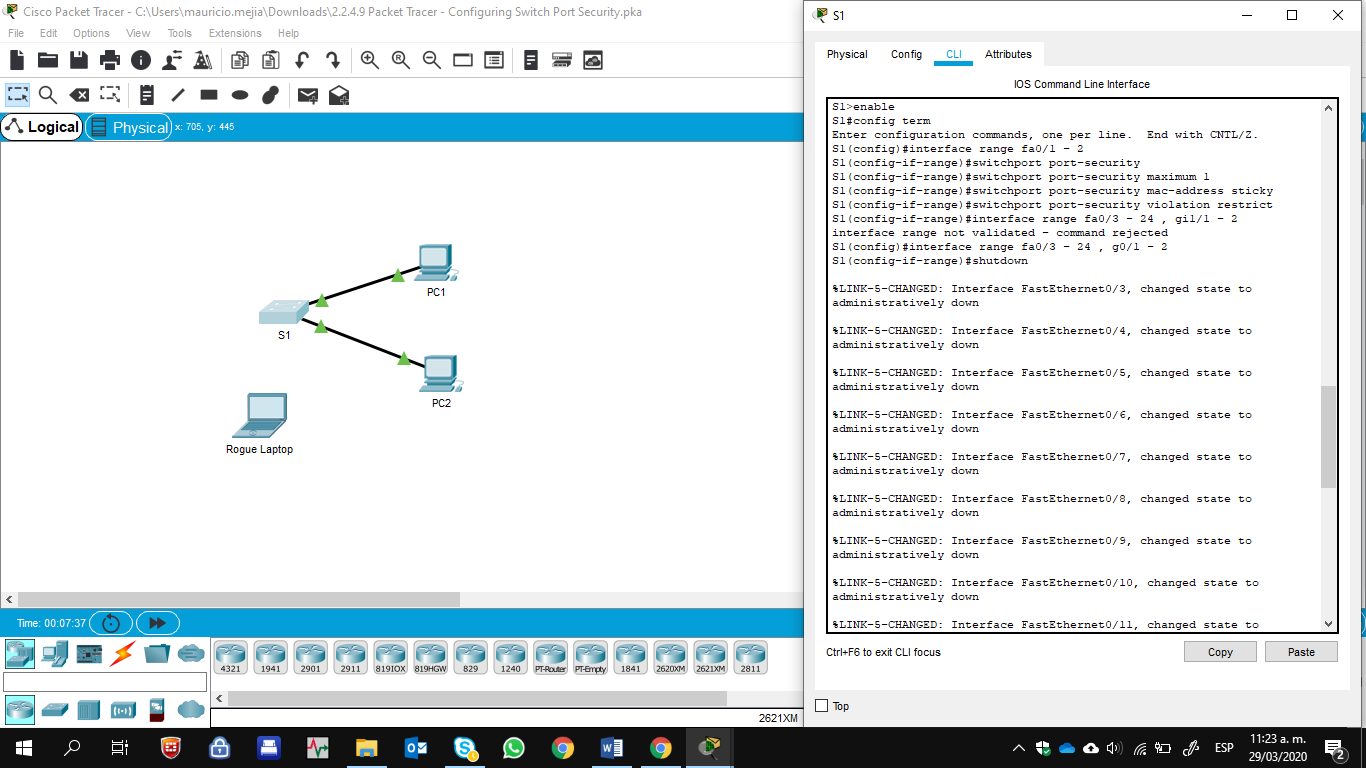
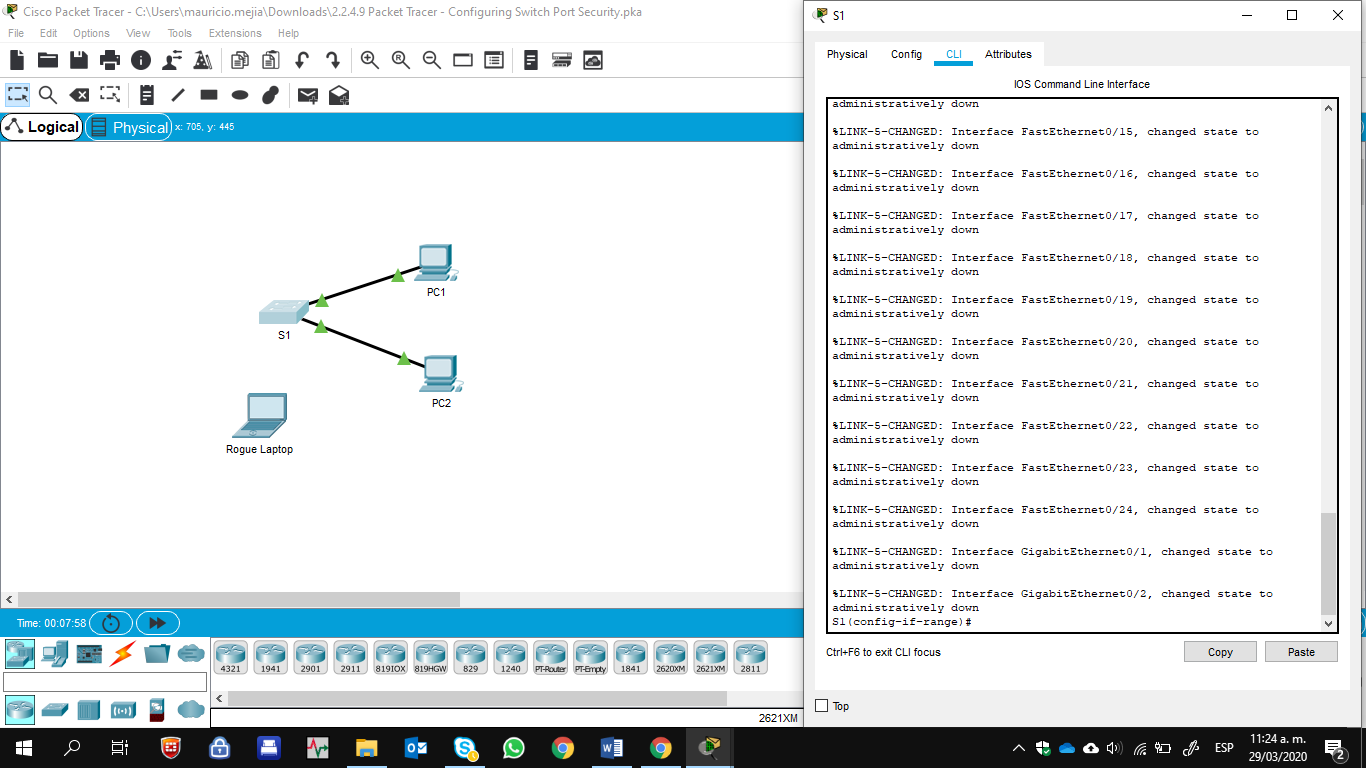
1. Set the violation so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but packets are dropped from an unknown source.

S1(config-if-range)# **switchport port-security violation restrict**

1. Disable all the remaining unused ports. Hint: Use the **range** keyword to apply this configuration to all the ports simultaneously.

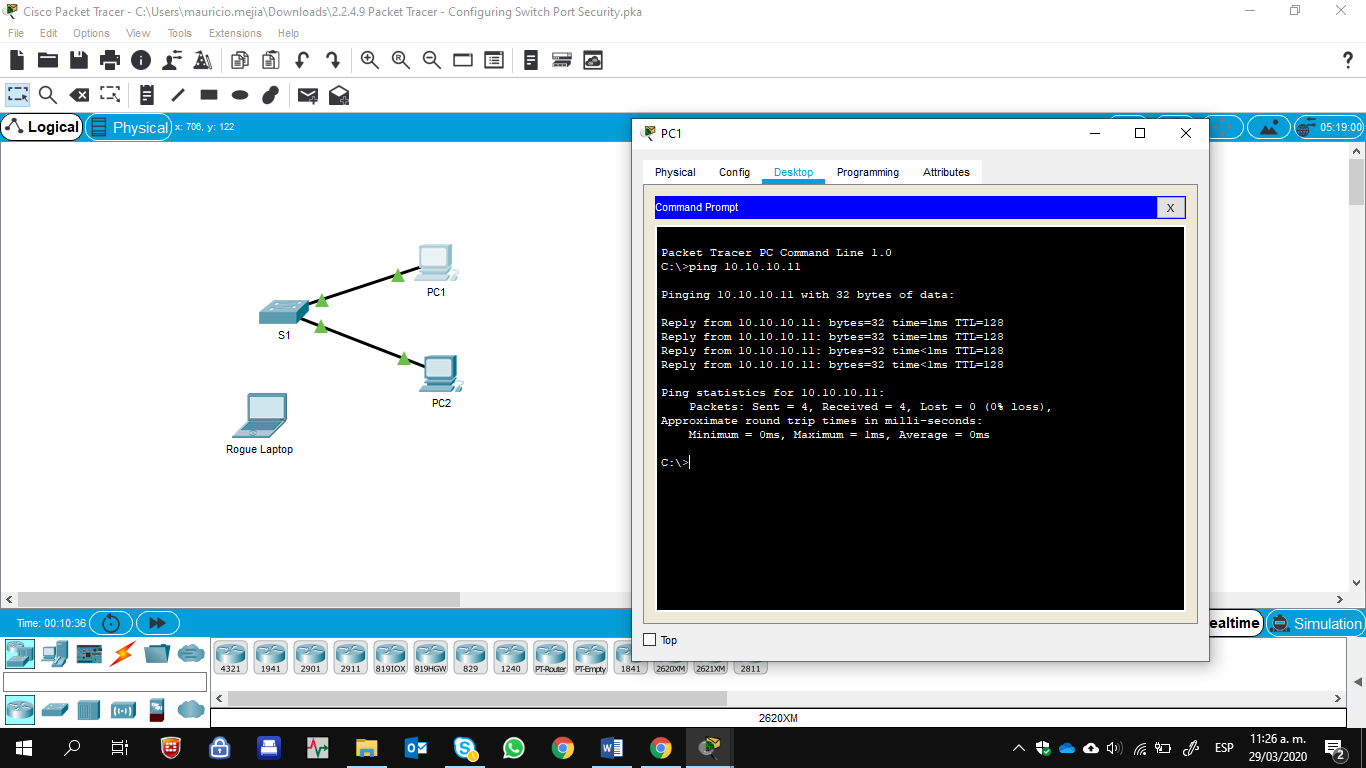
S1(config-if-range)# **interface range fa0/3 - 24 , gi1/1 - 2**

S1(config-if-range)# **shutdown**

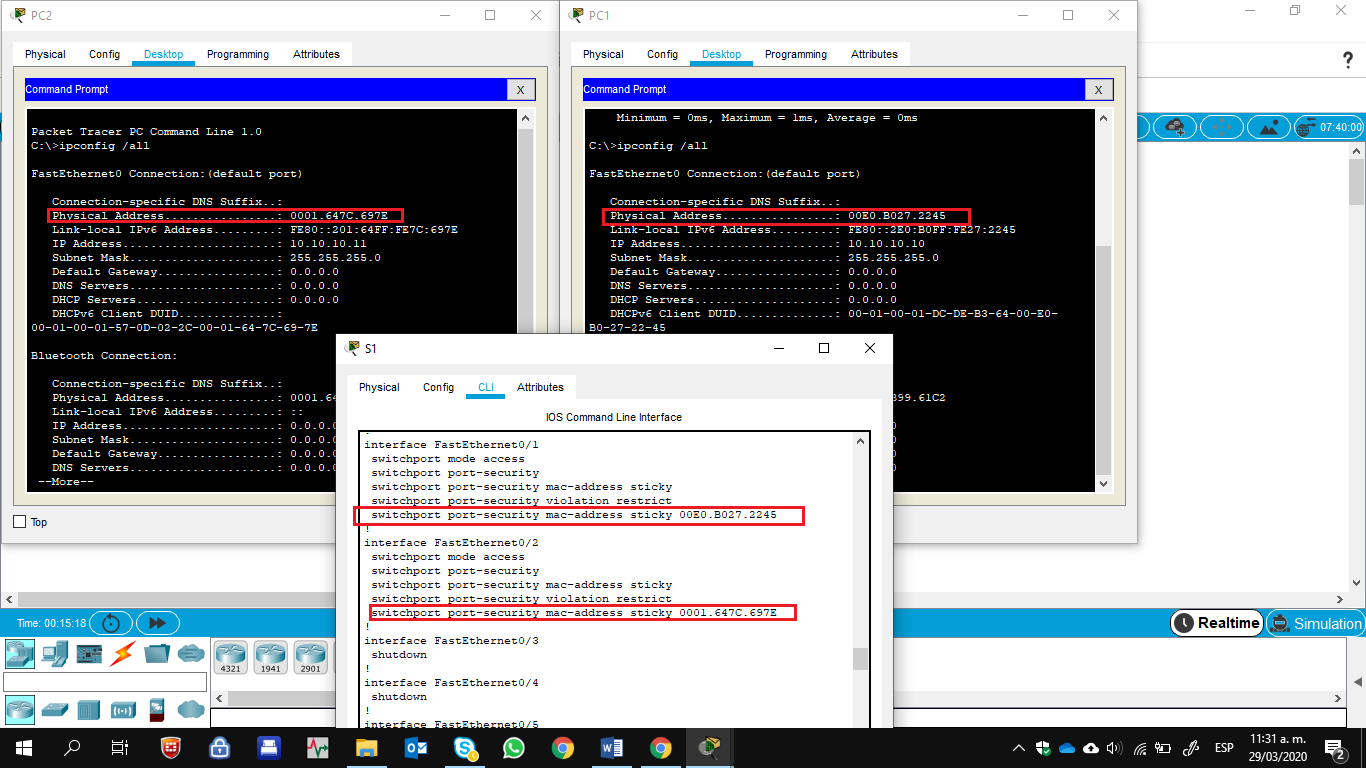
 

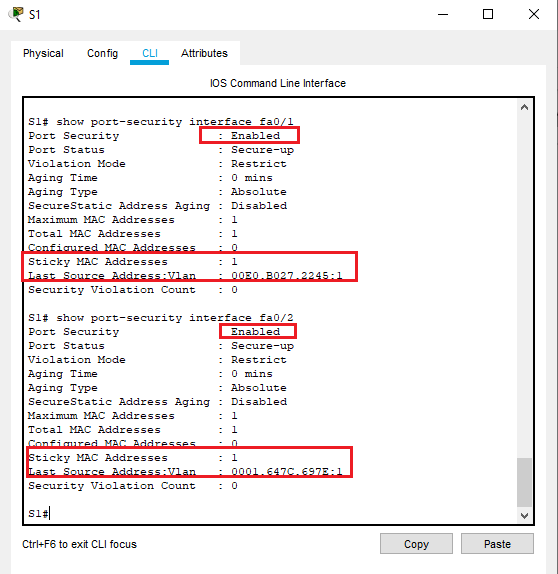
# Part 2: Verify Port Security

1. From **PC1**, ping **PC2**.

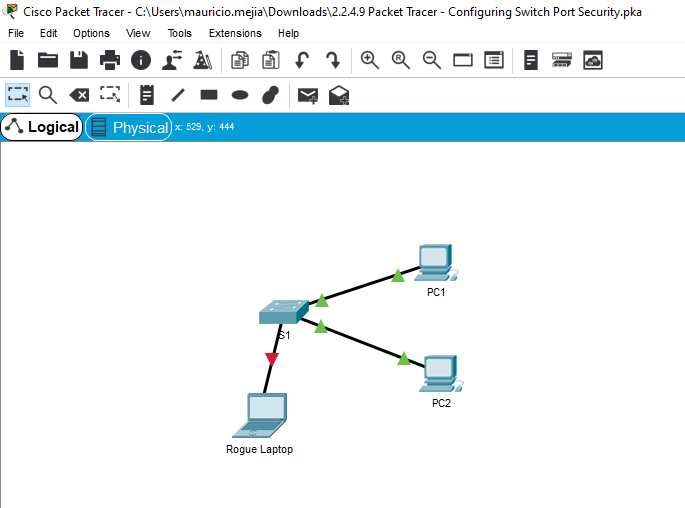


1. Verify port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration

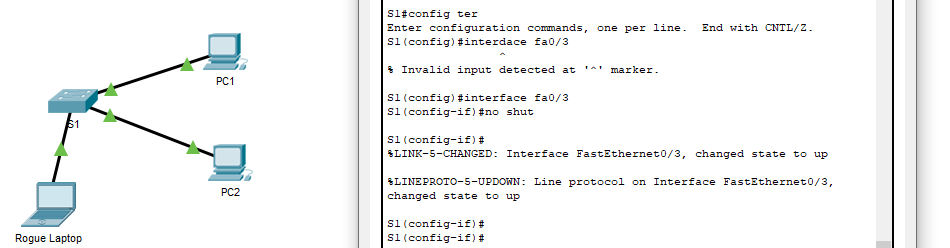


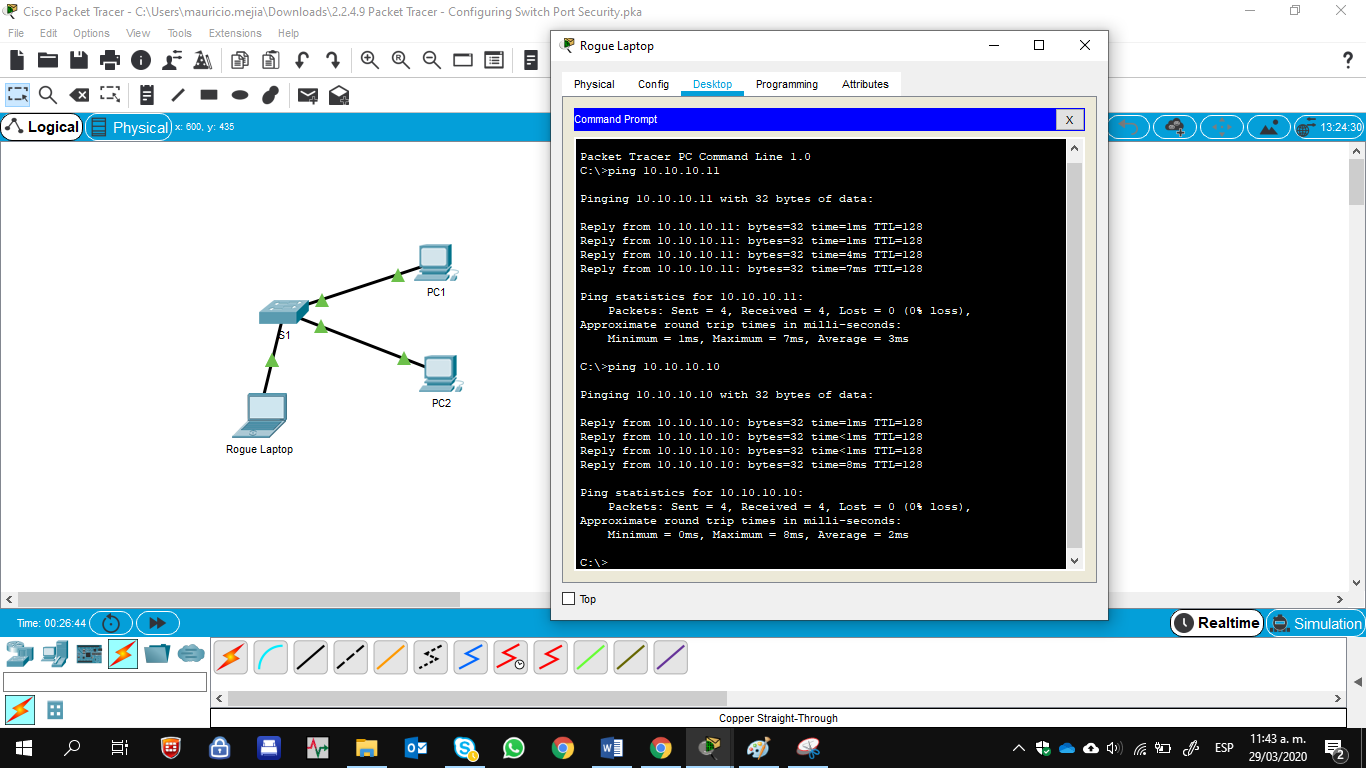


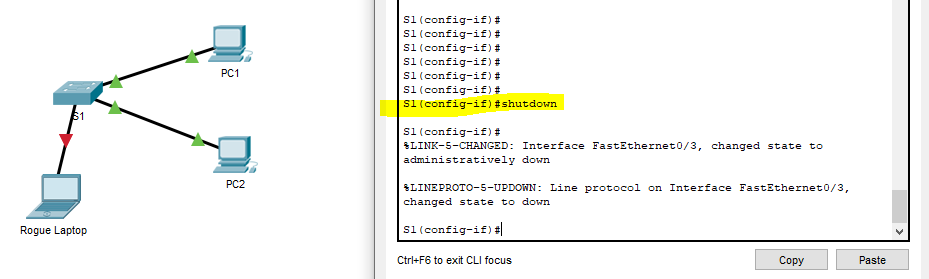
1. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.



1. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**

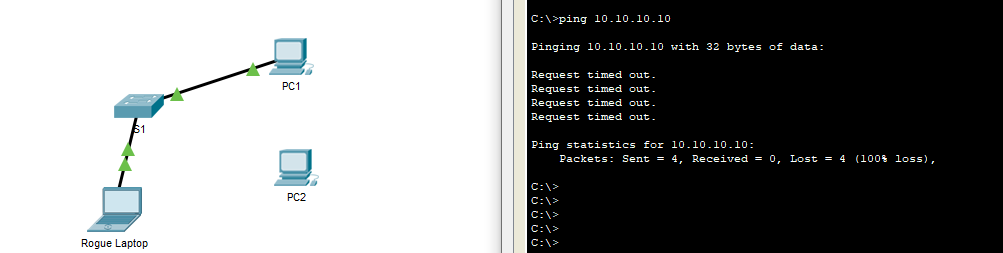






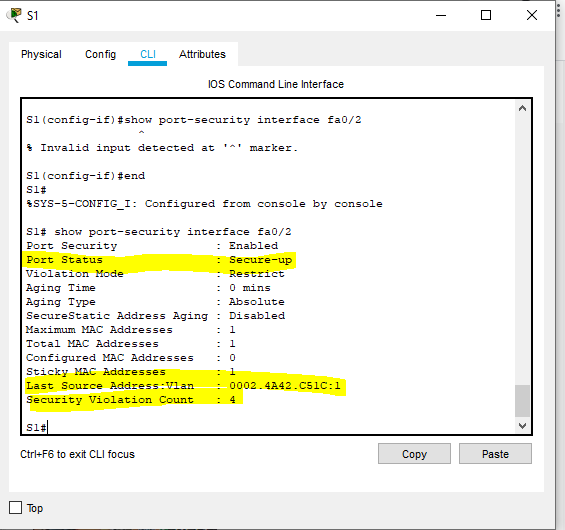
1. Disconnect **PC2** and connect **Rogue Laptop** to **PC2’s** port. Verify that **Rogue Laptop** is unable to ping

**PC1**.

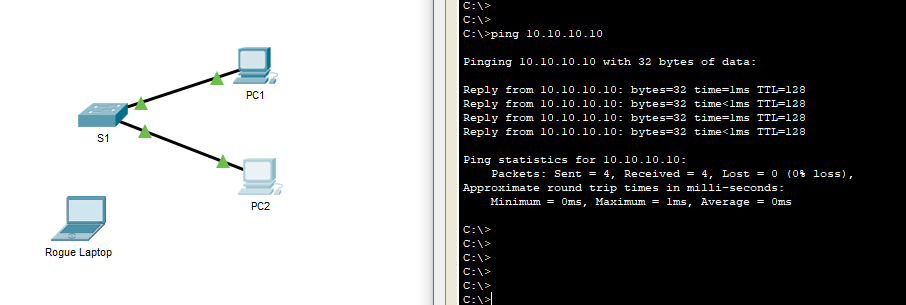


1. Display the port security violations for the port **Rogue Laptop** is connected to.

S1# show port-security interface fa0/2



1. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.



1. Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not? The port security that was enabled on the port only allowed the device, whose MAC was learned first, access to the port while preventing all other devices access.

