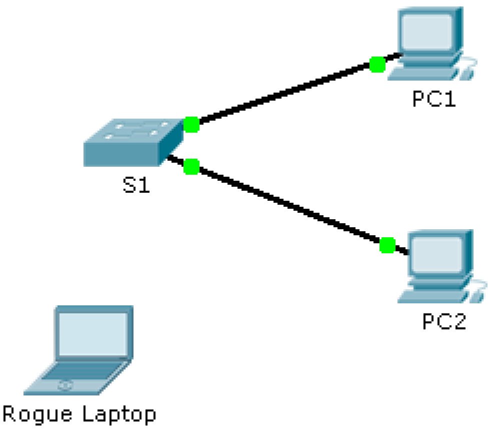
Week 8 Lab part 1 - Solution

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.

Read me first:

Part 1: Configure Port Security

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

```
S1(config)# enable
S1(config)# configure
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# switchport port-security
```

b. 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
```

c. 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
```

d. Set the violation so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.

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

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

```
S1(config-if-range)# exit
S1(config-if-range)# interface range fa0/3 - 24 , gi1/1 - 2
Comment: instead of gi1/1 - 2, it may be gi0/1 - 2
S1(config-if-range)# shutdown
```

Part 2: Verify Port Security

a. From **PC1**, ping **PC2**.

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

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

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

e. Disconnect **PC2** and connect **Rogue Laptop** to **PC2's** port. Verify that **Rogue Laptop** is unable to ping **PC1**.

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

```
S1# show port-security interface fa0/2
```

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

h. 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.