1.4 – ENSA - PacketKnows – Configuring Switch Port Security

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**

NOTE

- **Power all the devices first by clicking the triangle button on the upper navbar.**
- **Right click the device then click the web console first to configure on the device**
- **Always type "save" when configuring IP addresses of PC's**

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

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

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

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

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.

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

Part 2: Verify Port Security

a. Remove the link/cable for e0/1 of PC2, then connect the Rouge PC in e0/1.
b. Trying pining PC1 using Rouge PC

Note: The Rouge PC should not able to ping PC1