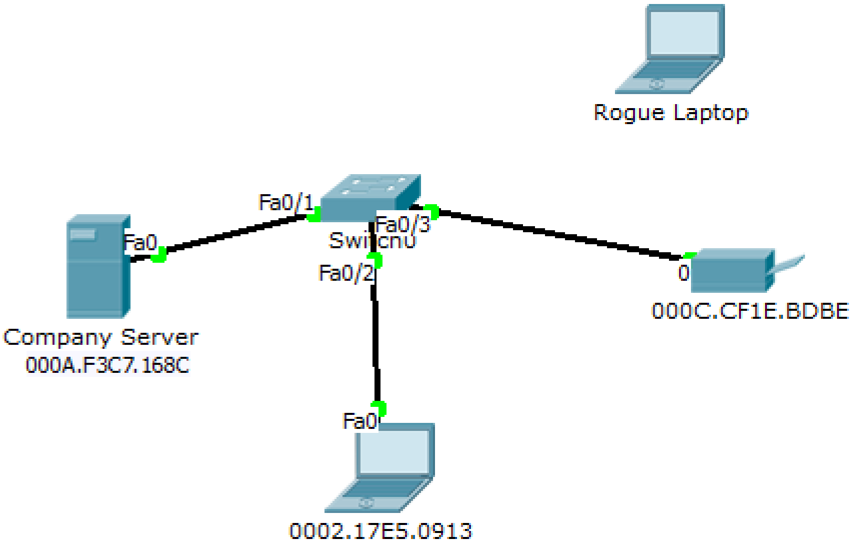
Lab 2.2.1.1: Switch Security Implementation

Topology



Objective

1. Verify the Layer 2 configuration of a switch port connected to an end station.
2. Use Packet Tracer to configure the first three ports of a switch a permanent MAC address (one MAC address per port) and security shutdown feature.
3. Validate security implementation and explain the process to another student or the class.

Scenario

You are the network administrator for Alpha-Beta Co.., Inc. The Corporate headquarters for your business has mandated that on all switches in all offices, security must be implemented. The memorandum delivered to you this morning states:

Dear Network Administrators:

Please be reminded of the following tasks today Monday Nov. 16, 20xx:

a. *The first three ports of all configurable switches located in all offices must be secured with specific MAC addresses — one address will be reserved for the Printer, one address will be reserved for the laptop in the office, and one address will be reserved for the office server.*
b. *Disable the remaining ports so that users can't access them.*
c. *If a port's security is breached, shut it down the port until the reason for the violation can be verified and certified.*

Please implement these policy no later than the date stated in this memorandum. For questions, call the Central Office Corporate Headquarters..

Thank you.

The Network Management Team"

- Create a Packet Tracer basing on the topology to test this new security policy. Once you have created your file, test it to ensure if it is operational or validated.
- Save your work on a file name **Lab 2311-Swtich Security Implementation**.

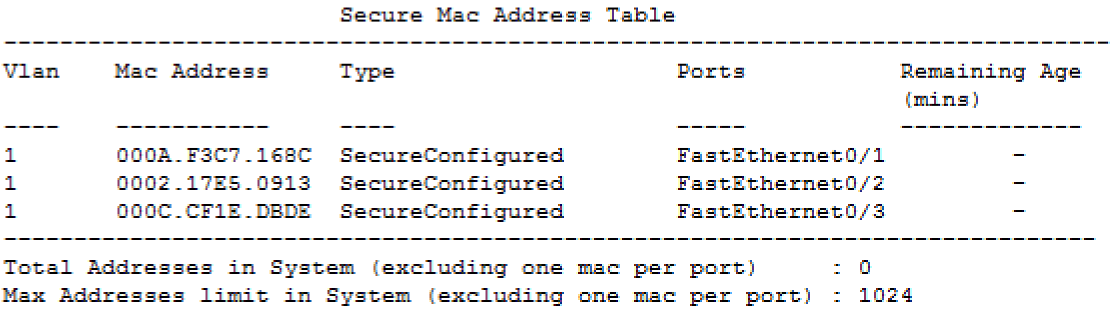
Part 1: Configure Port Security to Fa0/1, Fa0/2, and Fa0/3. Given the prompt and initial command in securing the port, finish the procedure in securing the intended ports.

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)# int fa0/2
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#int fa0/3
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#exit
Switch(config-if)#int rang fa0/4-24, gi1/1, gi1/2
Switch(config-if)#shutdown
Switch#copy run start
```

Part 2: Verify the port security status for Fa0/1, Fa0/2, and Fa0/3. :

a. After configuring port security for the Printer, Server and Laptop, make sure that all devices are reporting to the switch on their correct ports. Verify by displaying the secure MAC Address Table

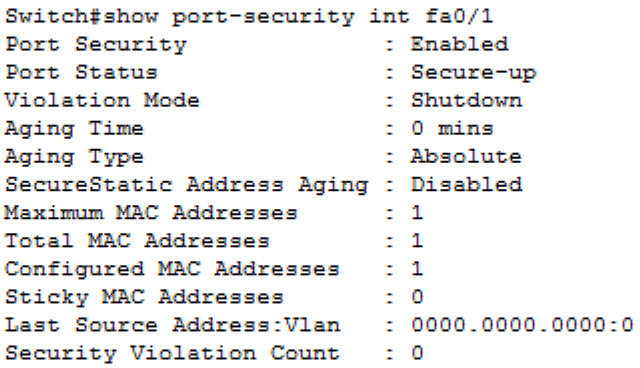
Switch# ____



```
                        Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                     Ports          Remaining Age
                                                                   (mins)
----    -----------       ----                     -----          -------------
1       000A.F3C7.168C    SecureConfigured         FastEthernet0/1        -
1       0002.17E5.0913    SecureConfigured         FastEthernet0/2        -
1       000C.CF1E.DBDE    SecureConfigured         FastEthernet0/3        -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

b. Verify the by displaying the secure MAC Address Table

```
Switch# show port-security int fa0/1
```



```
Switch#show port-security int fa0/1
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

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

d. Remove the laptop and connect the **Rogue Laptop** to the port.

e. Verify the connection by pinging **company server**, notice that the link lights turned red.

f. Show the port security violations for the connected port of the **Rogue Laptop**.

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

g. Remove the **Printer** and Reconnect a **new Printer**. Notice that the port link is still red. Troubleshoot and enable the port where the **printer** and **laptop** is connected.

h. Test the connection again by pinging the devices.

Reflection

1. Why would one port on a switch be secured on a switch using these scenario parameters (and not all the ports on the same switch)?

____

____

2. Why would a network administrator use a network simulator to create, configure, and validate a security plan, instead of using the small- to medium-sized business' actual, physical equipment?

____

____