

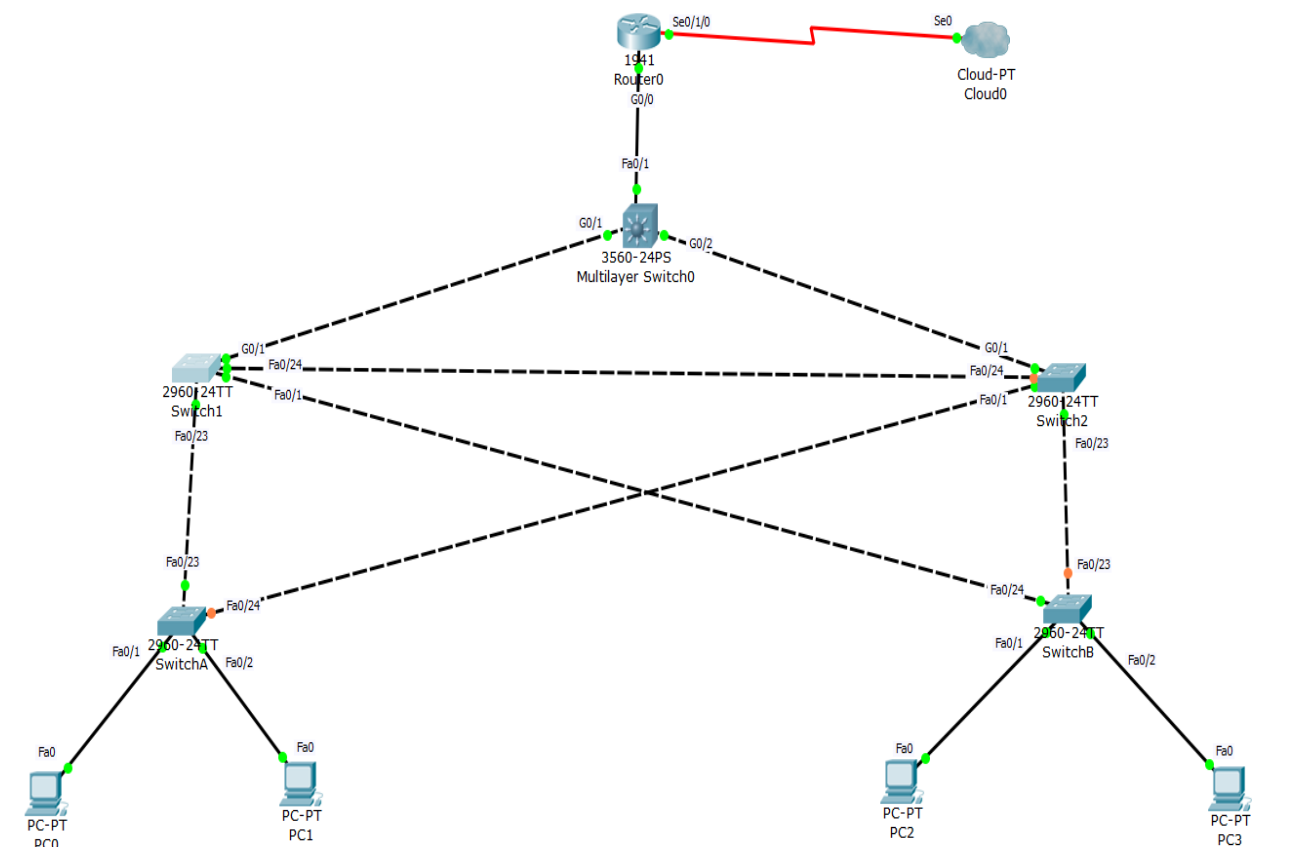
**Practical 8**

**Layer 2 Security** a) Assign the Central switch as the root bridge.  
b) Secure spanning-tree parameters to prevent STP manipulation attacks. c) Enable port security and disable unused ports.

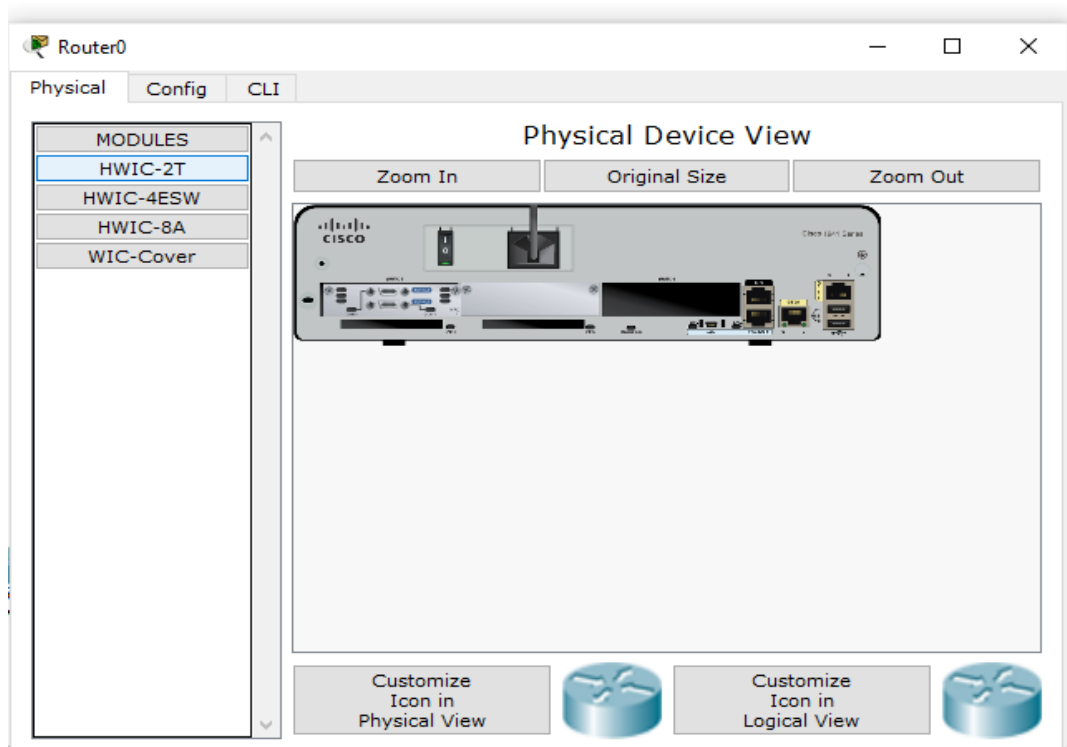
There have been a number of attacks on the network recently. For this reason, the network administrator has assigned us the task of configuring Layer 2 security.

For optimum performance and security, the administrator would like to ensure that the root bridge is the 3560 multi-layer switch. To prevent spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. To prevent against CAM (Content Addressable Memory) table overflow attacks, the network administrator has decided to configure port security to limit the number of MAC addresses each switch port can learn. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown.

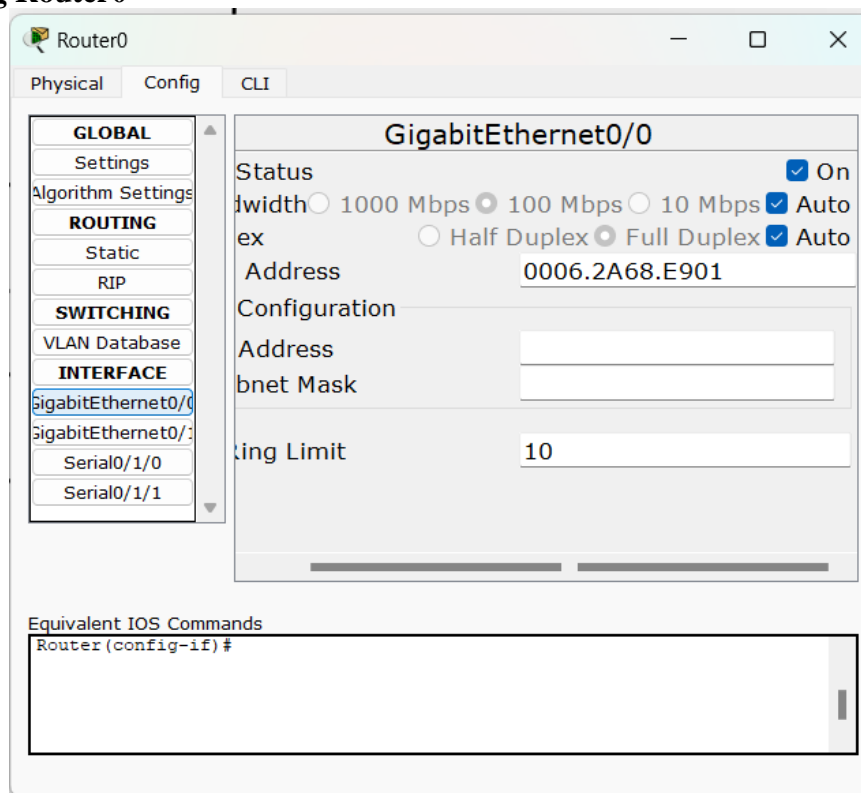
**Consider the following topology**

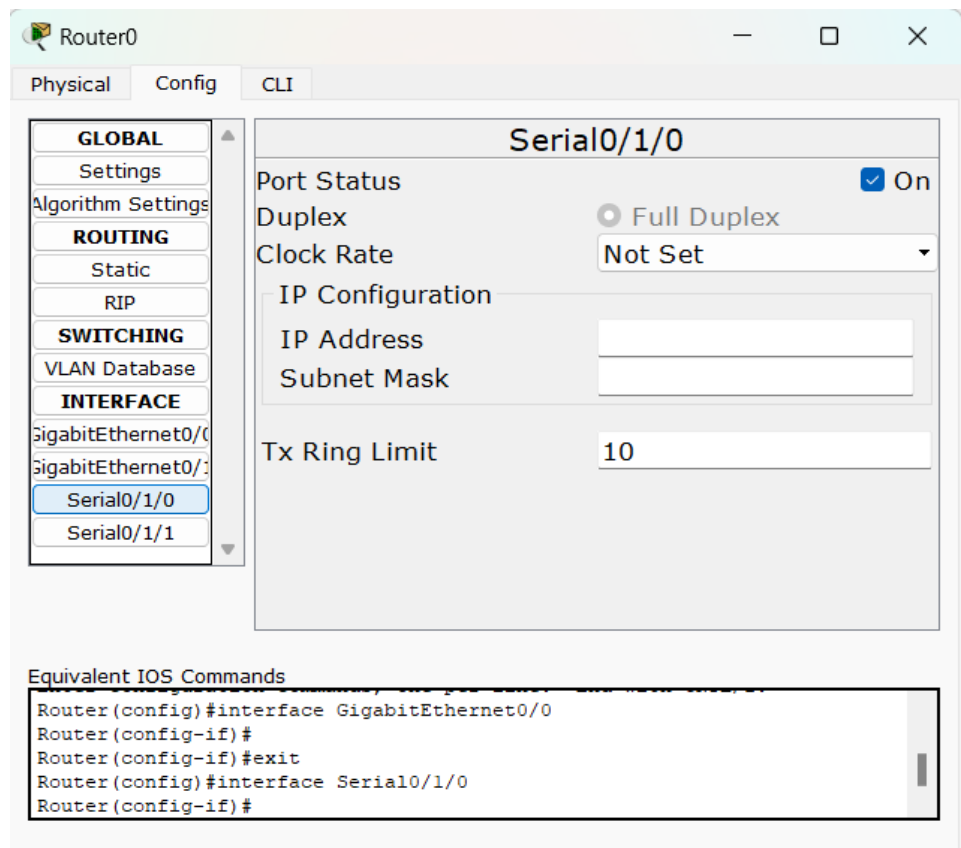
**Topology Configuration**

**Serial Interface must be added in the Router0 before configuring it**  
**The serial interface in Router0 is added as follows**



### Configuring Router0



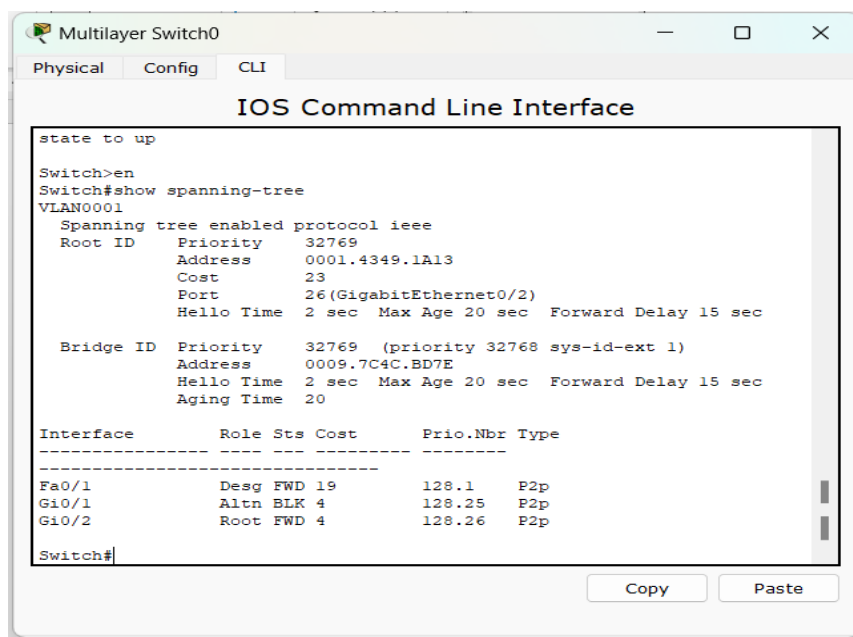


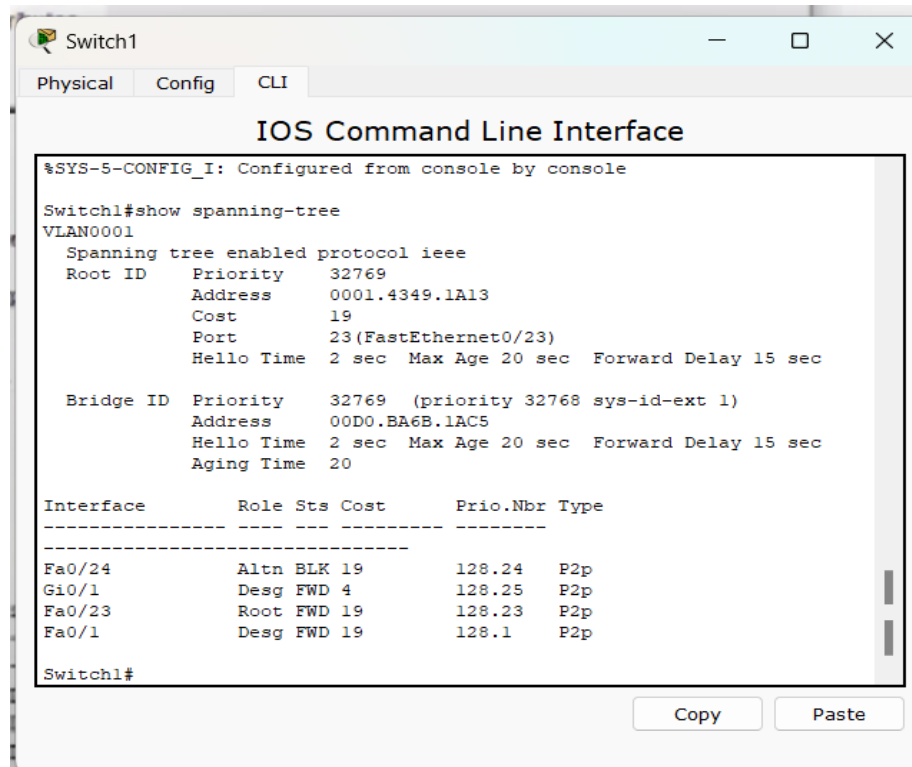
## Part 1: Configure Root Bridge

### Step 1: Determine the current root bridge.

From **Multilayer Switch0**, issue the **show spanning-tree** command to determine the current root bridge, to see the ports in use, and to see their status.

```
switch>en
switch# show spanning-tree
```





**Step 2: Assign Multilayer Switch0 as the primary root bridge.** Using the **spanning-tree vlan 1 root primary** command, and assign **Multilayer switch0** as the root bridge.

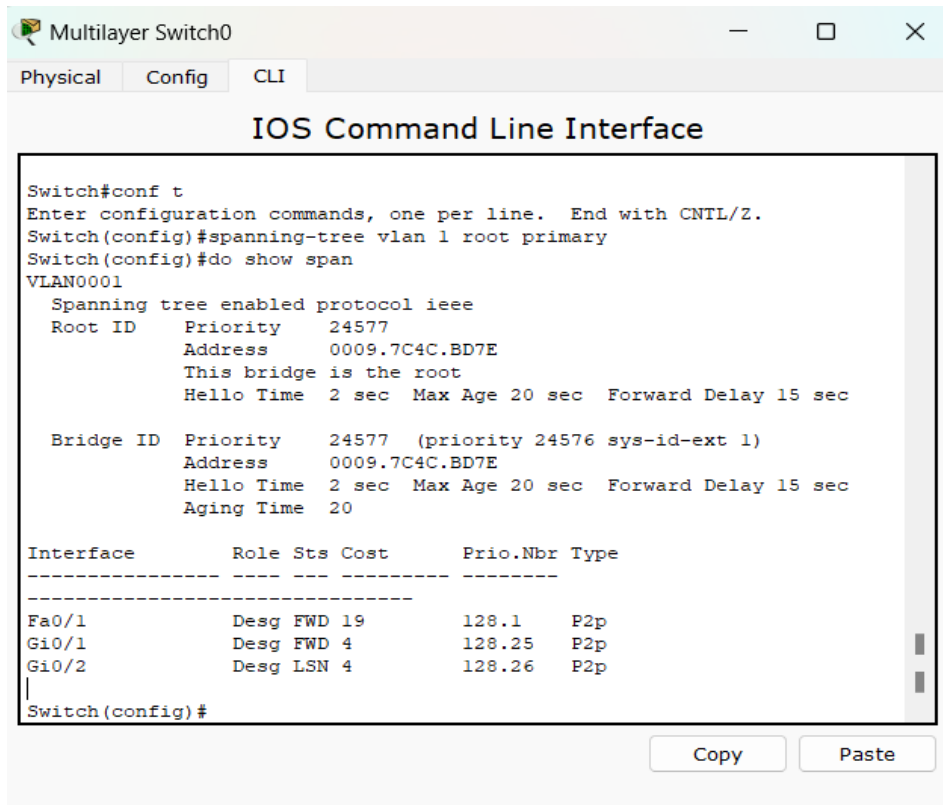
```
switch#conf t
switch(config)#spanning-tree vlan 1 root primary
switch(config)#do show span
```

**Step 3: Assign Switch1 as a secondary root bridge.** Assign SW-1 as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command.

```
switch#conf t
switch(config)#spanning-tree vlan 1 root secondary
```

**Step 4: Verify the spanning-tree configuration.** Issue the **show spanning-tree** command to verify that Multi-layer Switch0 is the root bridge.

```
switch# show spanning-tree
```



## Part 2: Protect Against STP Attacks

Secure the STP parameters to prevent STP manipulation attacks.

### Step 1: Enable PortFast on all access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the SwitchA and SwitchB, use the spanning-tree portfast command.

```
SwitchA>en
SwitchA#conf t
SwitchA(config)#int range f0/1-2
SwitchA(config-if-range)#spanning-tree portfast
```

```
SwitchB>en
SwitchB#conf t
SwitchB(config)#int range f0/1-2
SwitchB(config-if-range)#spanning-tree portfast
```

**Step 2: Enable BPDU guard on all access ports.**

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU guard on SwitchA and SwitchB access ports.

```
SwitchA(config)#int range f0/1-2
SwitchA(config-if-range)#spanning-tree bpduguard enable

SwitchB(config)#int range f0/1-2
SwitchB(config-if-range)#spanning-tree bpduguard enable
```

**Step 3: Enable root guard.**

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the show spanning-tree command to determine the location of the root port on each switch.

On Switch1, enable root guard on ports F0/23 and F0/24. On Switch2, enable root guard on ports F0/23 and F0/24.

```
Switch1>en
Switch1#conf t
Switch1(config)#int range f0/23-24
Switch1(config-if-range)#spanning-tree guard root

Switch2>en
Switch2#conf t
Switch2(config)#int range f0/23-24
Switch2(config-if-range)#spanning-tree guard root
```

**Part 3: Configure Port Security and Disable Unused Ports****Step 1: Configure basic port security on all ports connected to host devices.**

This procedure should be performed on all access ports on SwitchA and SwitchB. Set the maximum number of learned MAC addresses to 2, allow the MAC address to be learned dynamically, and set the violation to **shutdown**. Note: A switch port must be configured as an access port to enable port security.

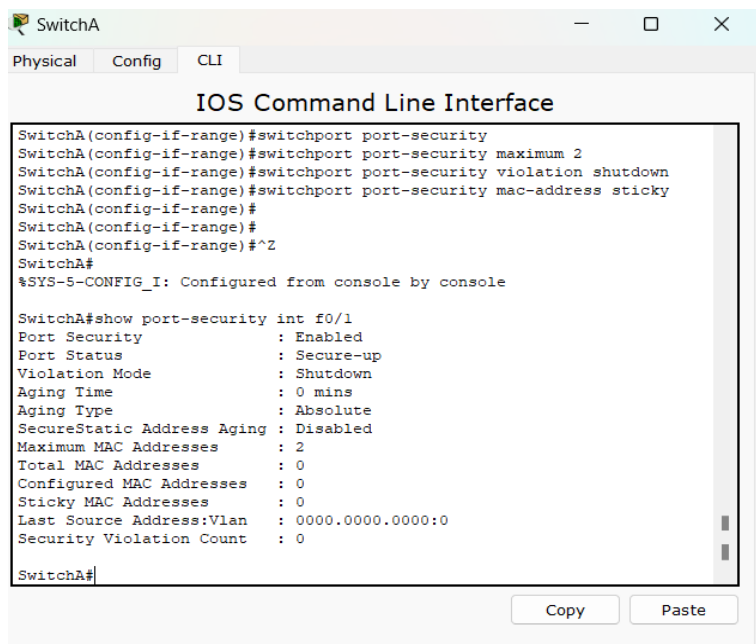
```
SwitchA>en
SwitchA#conf t
SwitchA(config)#int range f0/1-2
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport port-security
SwitchA(config-if-range)#switchport port-security maximum 2
SwitchA(config-if-range)#switchport port-security violation shutdown
SwitchA(config-if-range)#switchport port-security mac-address sticky
```

```
SwitchB>en
SwitchB#conf t
SwitchB(config)#int range f0/1-2
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport port-security
SwitchB(config-if-range)#switchport port-security maximum 2
SwitchB(config-if-range)#switchport port-security violation shutdown
SwitchB(config-if-range)#switchport port-security mac-address sticky
```

### Step 2: Verify port security.

On SwitchA, issue the command `show port-security int f0/1` to verify that port security has been configured.

```
SwitchA#show port-security int f0/1
```



The screenshot shows a terminal window titled "SwitchA" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal shows the following commands and output:

```
SwitchA(config-if-range)#switchport port-security
SwitchA(config-if-range)#switchport port-security maximum 2
SwitchA(config-if-range)#switchport port-security violation shutdown
SwitchA(config-if-range)#switchport port-security mac-address sticky
SwitchA(config-if-range)#
SwitchA(config-if-range)#
SwitchA(config-if-range)#^Z
SwitchA#
%SYS-5-CONFIG_I: Configured from console by console

SwitchA#show port-security int f0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 2
Total MAC Addresses    : 0
Configured MAC Addresses : 0
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

SwitchA#
```

At the bottom of the terminal window, there are "Copy" and "Paste" buttons.

```
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 2
Total MAC Addresses    : 0
Configured MAC Addresses : 0
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

**Step 3: Disable unused ports.**

Disable all ports that are currently unused.

```
SwitchA(config)#int range f0/3-22  
SwitchA(config-if-range)#shutdown
```

```
SwitchB(config)#int range f0/3-22  
SwitchB(config-if-range)#shutdown
```

Hence the Port security has been enabled.

\*\*\*\*\*