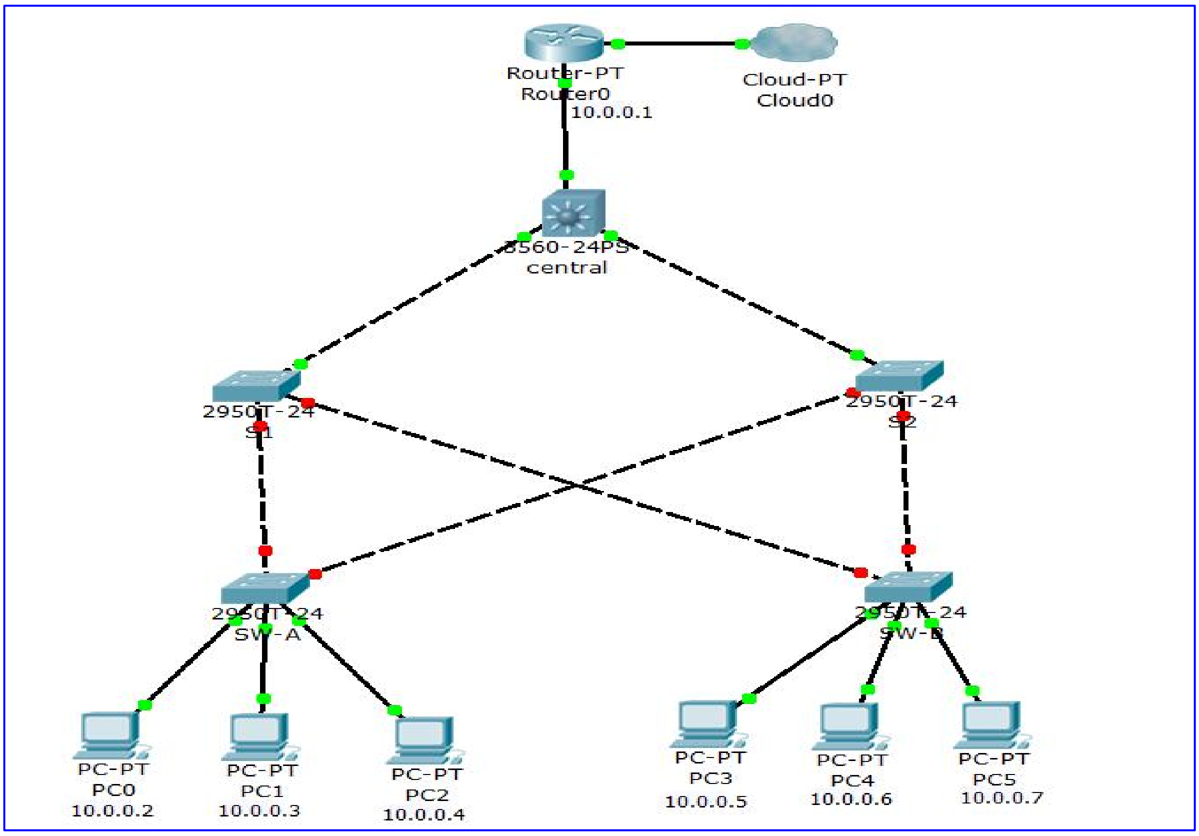
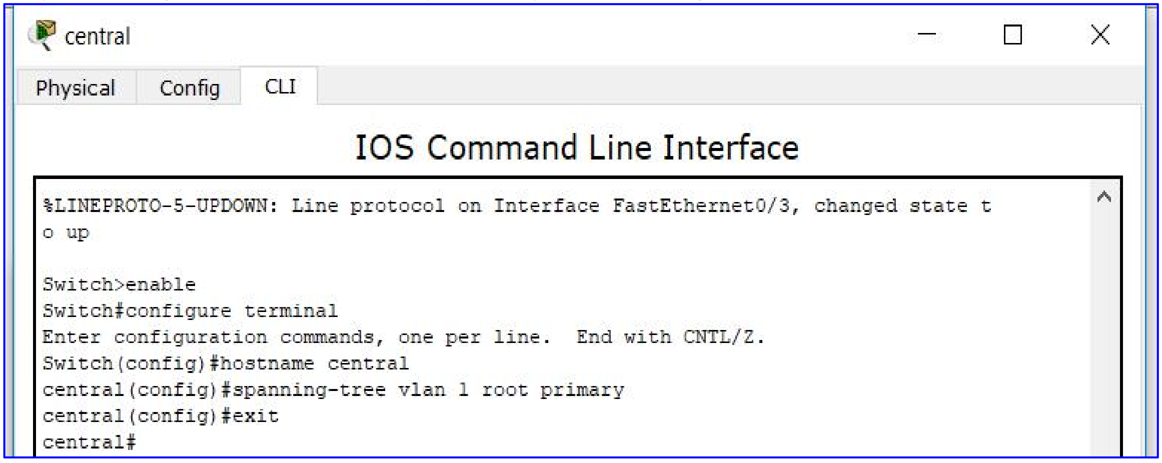
Practical NO.4

Layer 2 Security

Structure:

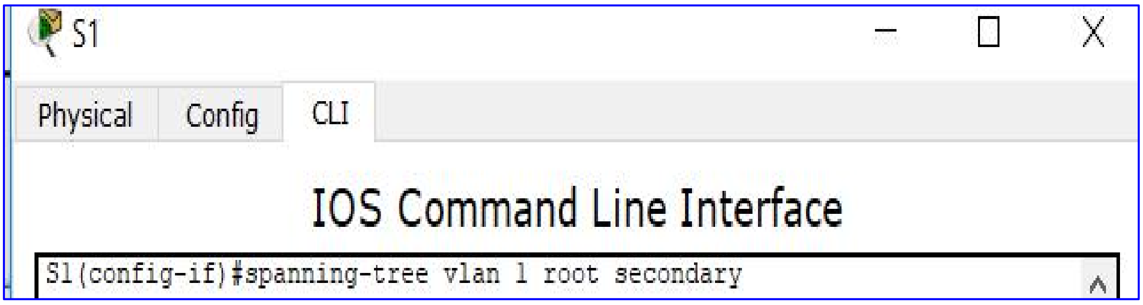


Step1: Assign central as the primary root bridge



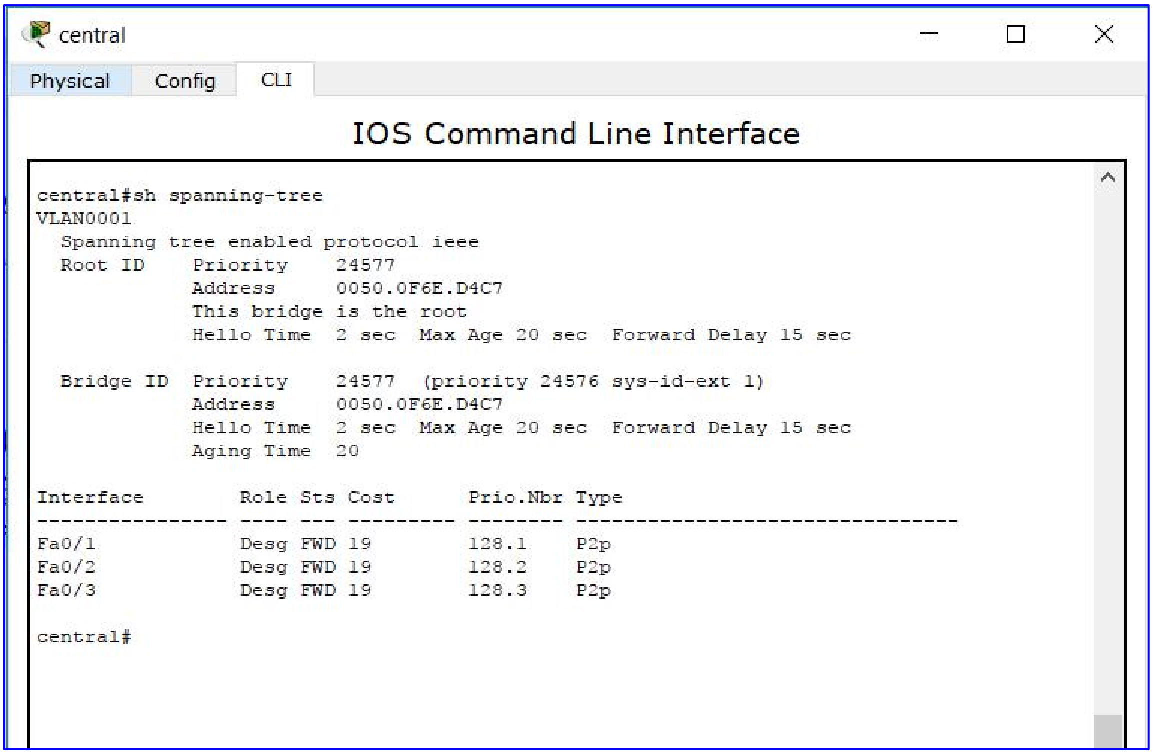
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state t
o up

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname central
central(config)#spanning-tree vlan 1 root primary
central(config)#exit
central#
```

Step 2: Assign Switch-S1 as the secondary root bridge



```
S1(config-if)#spanning-tree vlan 1 root secondary
```

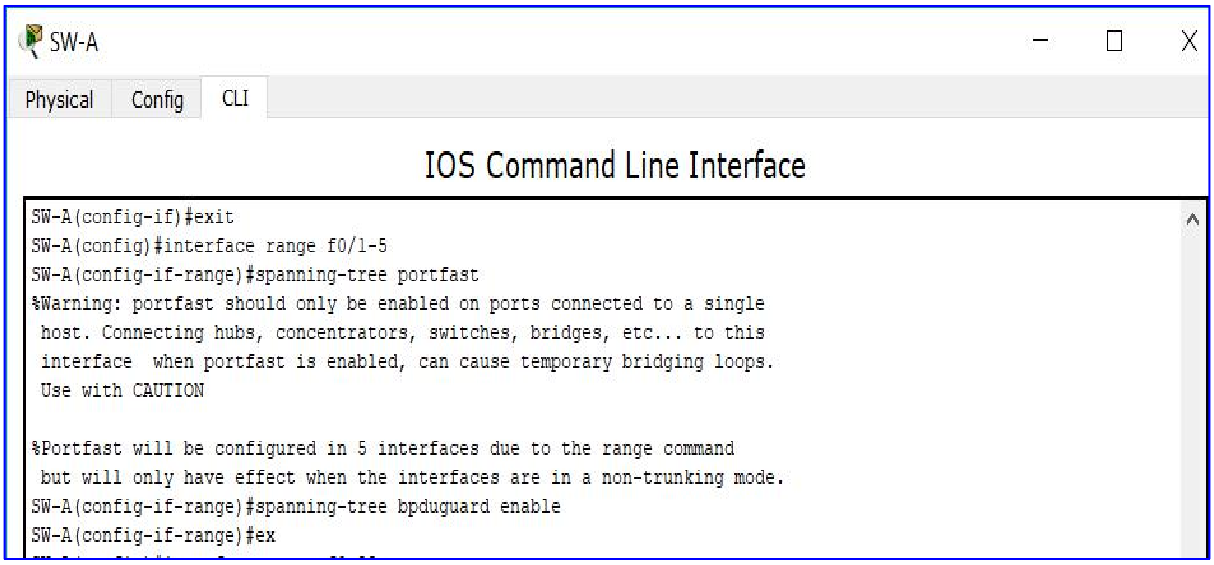
Step3: Verify the spanning-tree configuration



```
central#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0050.0F6E.D4C7
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     0050.0F6E.D4C7
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p

central#
```

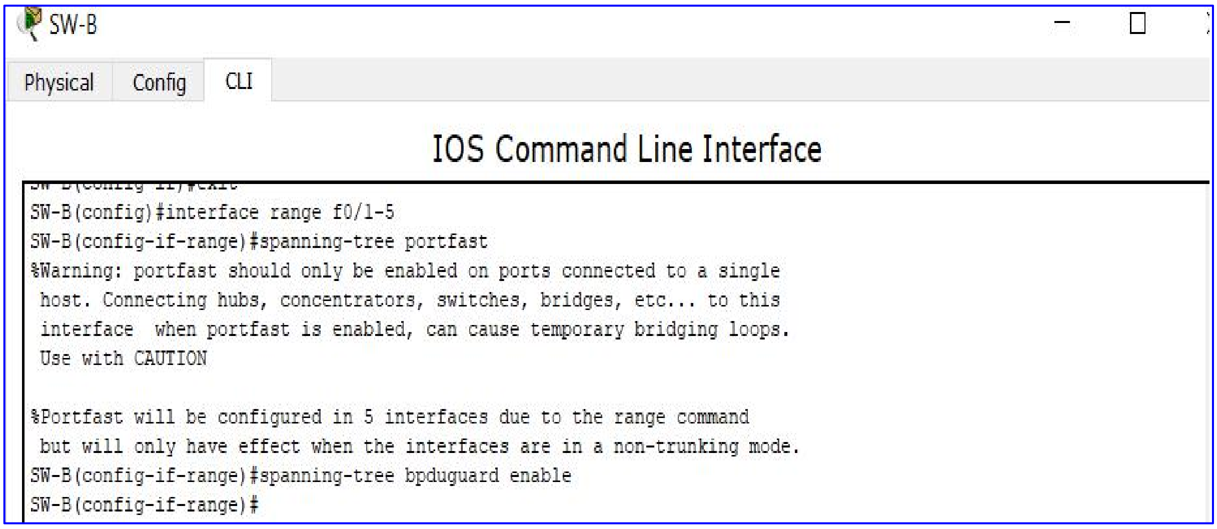
Step 4: Enable Portfast on all access port And Enable BPDU guard on all access port

Switch SW-A:



```
SW-A(config-if)#exit
SW-A(config)#interface range f0/1-5
SW-A(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 5 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
SW-A(config-if-range)#spanning-tree bpduguard enable
SW-A(config-if-range)#ex
```

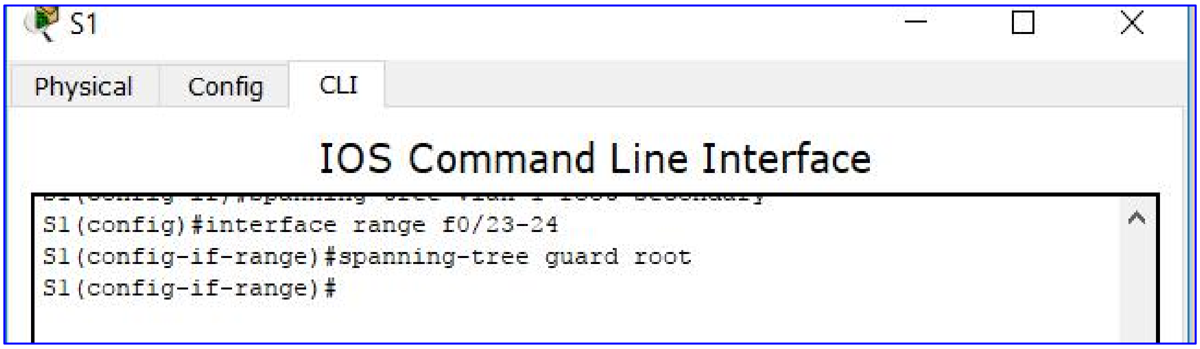
Switch SW-B:



```
SW-B(config-if)#exit
SW-B(config)#interface range f0/1-5
SW-B(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 5 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
SW-B(config-if-range)#spanning-tree bpduguard enable
SW-B(config-if-range)#
```

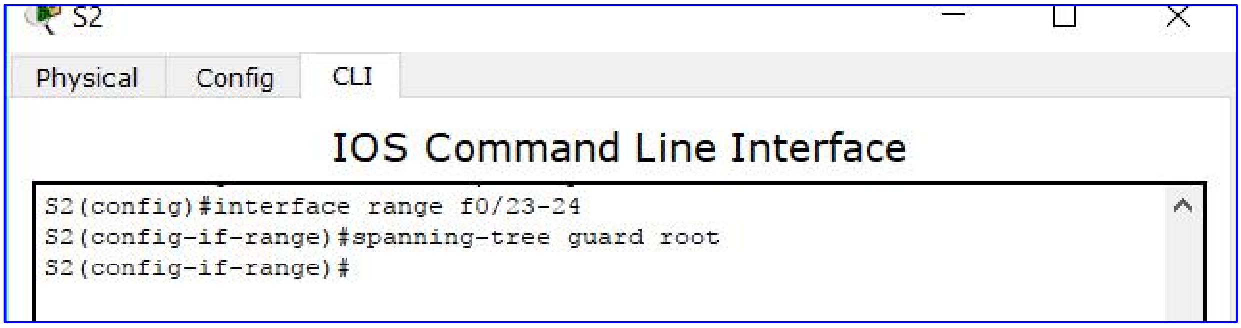
Step 5: Enable root guard

Switch:S1



```
S1(config-if)#spanning-tree vlan 1-1000 secondary
S1(config)#interface range f0/23-24
S1(config-if-range)#spanning-tree guard root
S1(config-if-range)#
```

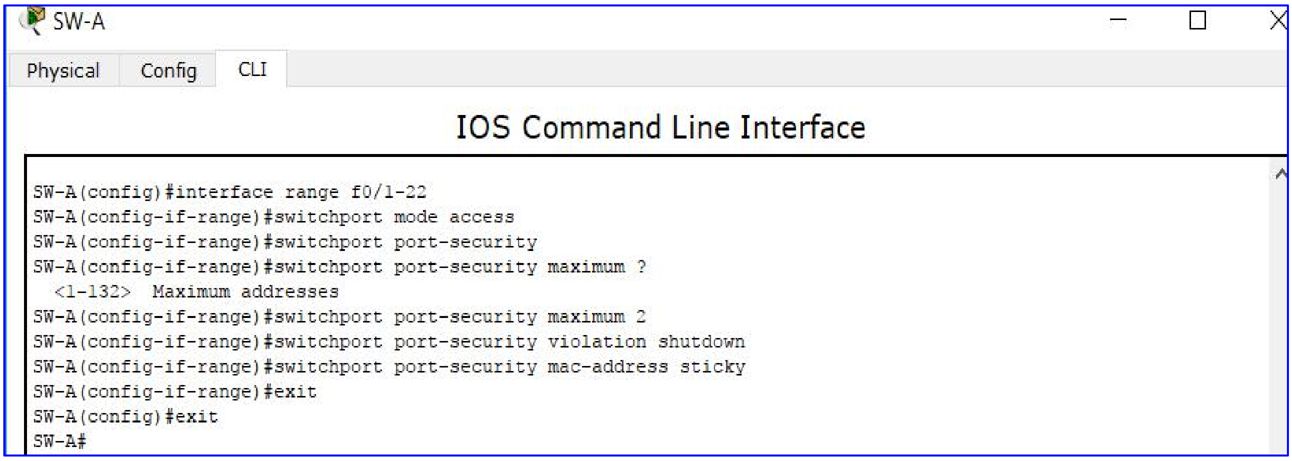
Switch:S2



```
S2(config)#interface range f0/23-24
S2(config-if-range)#spanning-tree guard root
S2(config-if-range)#
```

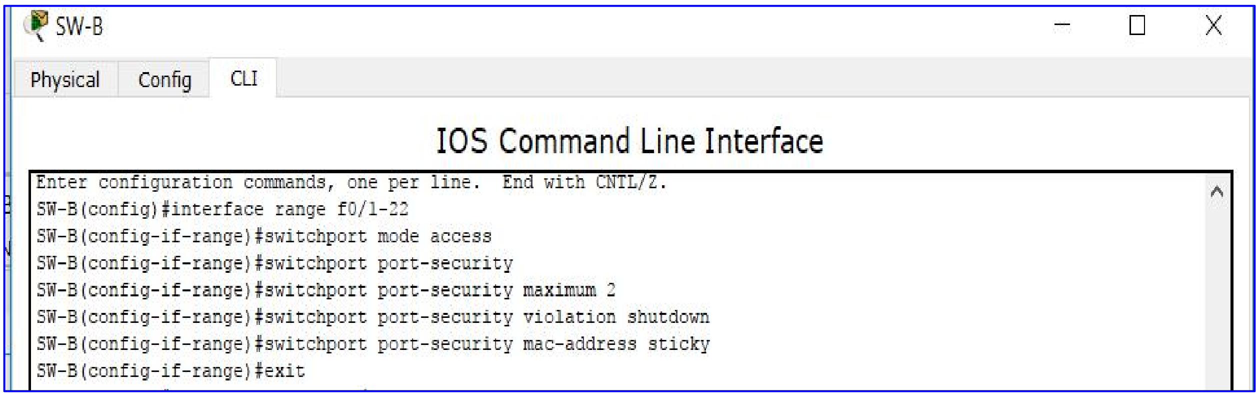
Step 6: Configure port security and disable unused port

SW-A:



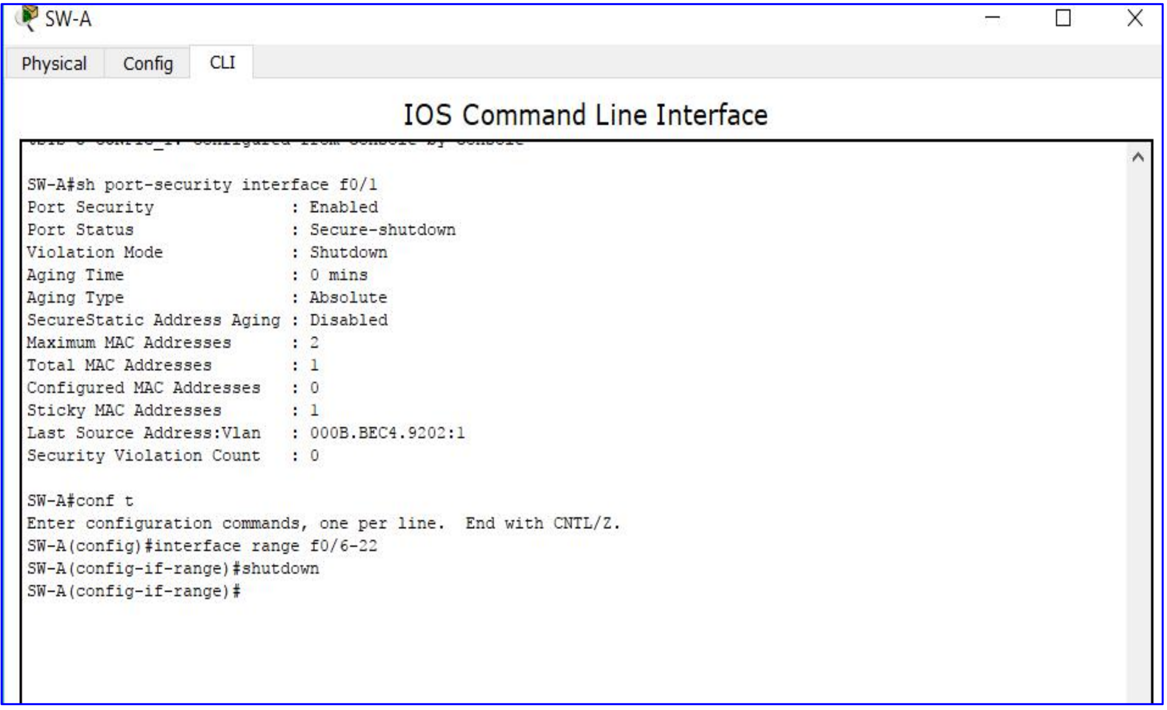
```
SW-A(config)#interface range f0/1-22
SW-A(config-if-range)#switchport mode access
SW-A(config-if-range)#switchport port-security
SW-A(config-if-range)#switchport port-security maximum ?
  <1-132>  Maximum addresses
SW-A(config-if-range)#switchport port-security maximum 2
SW-A(config-if-range)#switchport port-security violation shutdown
SW-A(config-if-range)#switchport port-security mac-address sticky
SW-A(config-if-range)#exit
SW-A(config)#exit
SW-A#
```

SW-B:



```
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)#interface range f0/1-22
SW-B(config-if-range)#switchport mode access
SW-B(config-if-range)#switchport port-security
SW-B(config-if-range)#switchport port-security maximum 2
SW-B(config-if-range)#switchport port-security violation shutdown
SW-B(config-if-range)#switchport port-security mac-address sticky
SW-B(config-if-range)#exit
```

Step 7: Verify port security:

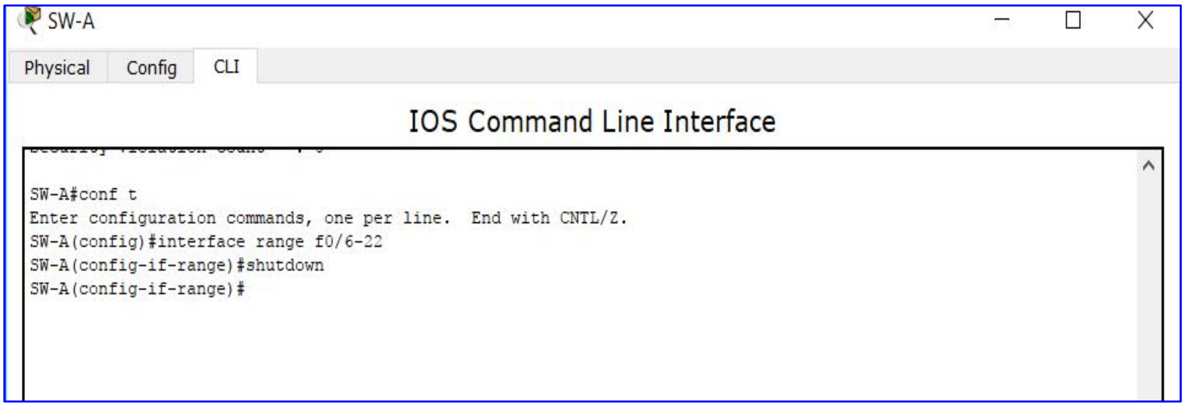


```
%SYS-5-CONFIG_I: Configured from console by console

SW-A#sh port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 000B.BEC4.9202:1
Security Violation Count   : 0

SW-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)#interface range f0/6-22
SW-A(config-if-range)#shutdown
SW-A(config-if-range)#
```

c

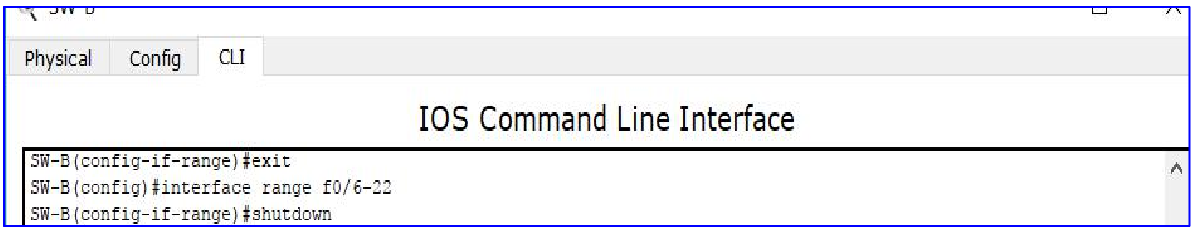
Step 8: Disable unused ports

Switch SW-A:



```
Security Violation Count   : 0

SW-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)#interface range f0/6-22
SW-A(config-if-range)#shutdown
SW-A(config-if-range)#
```

Switch SW-B:



```
SW-B(config-if-range)#exit
SW-B(config)#interface range f0/6-22
SW-B(config-if-range)#shutdown
```