Practical 7: Packet Tracer - Layer 2 Security Topology

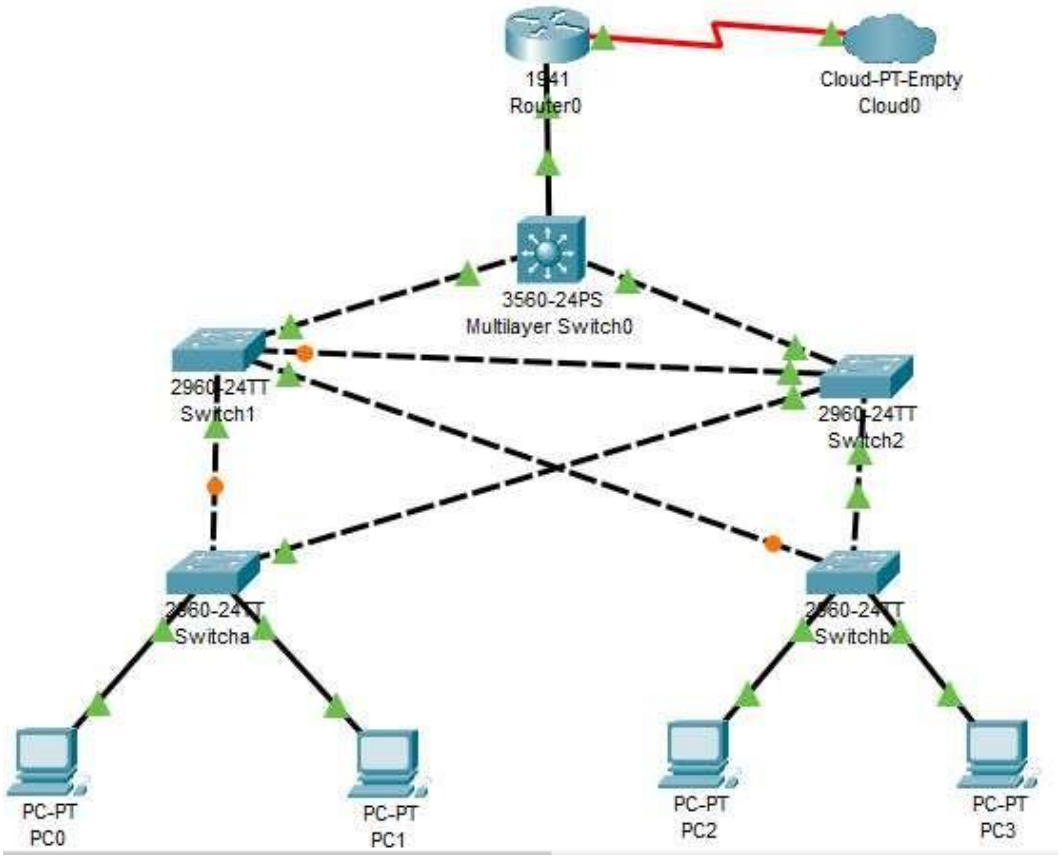
Objectives

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable port security to prevent CAM table overflow attacks.

Background / Scenario

There have been a number of attacks on the network recently. For this reason, the network administrator has assigned you 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 Central switch. To prevent spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. To prevent against CAM 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.

Let us consider the following topology to present this case:



Let us consider the following interface table to connect the network devices:

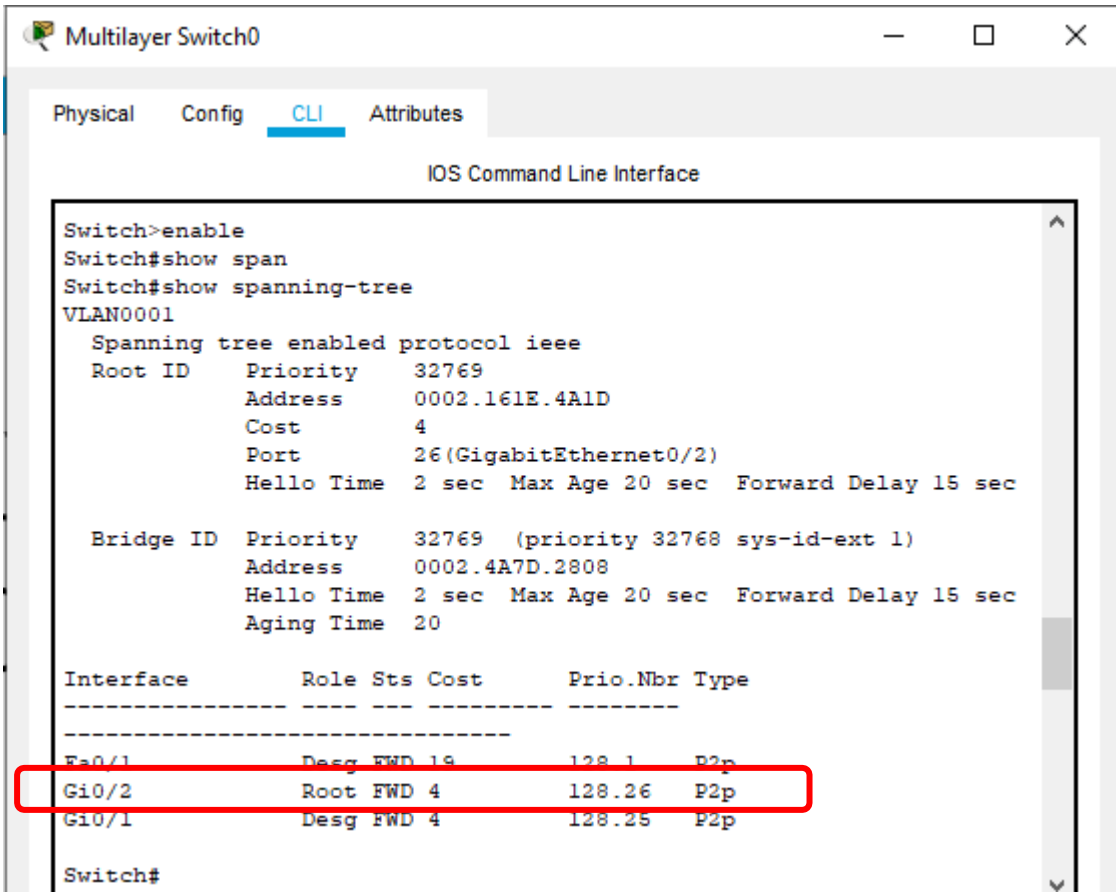
Note: Add one Serial Port in Router 0 and in Empty Cloud 0.

Device	Interface	Switch Port
PC 0	FastEthernet0	Switcha F0/1
PC 1	FastEthernet0	Switcha F0/2
PC 2	FastEthernet0	Switchb F0/1
PC 3	FastEthernet0	Switchb F0/2
Switch a	F0/23	Switch1 F0/23
	F0/24	Switch2 F0/1
Switch b	F0/23	Switch2 F0/23
	F0/24	Switch1 F0/1
Switch 1	F0/24	Switch2 F0/24
	GE 0/1	Multilayer Switch0 GE 0/1
Switch 2	GE 0/1	Multilayer Switch0 GE 0/2
Router 0	GE 0/1	Multilayer Switch0 F0/1
	S0/1/0	Cloud0 S4

Part 1: Configure Root Bridge

Type the following command in CLI mode of Multilayer Switch0, to check which is the Root bridge

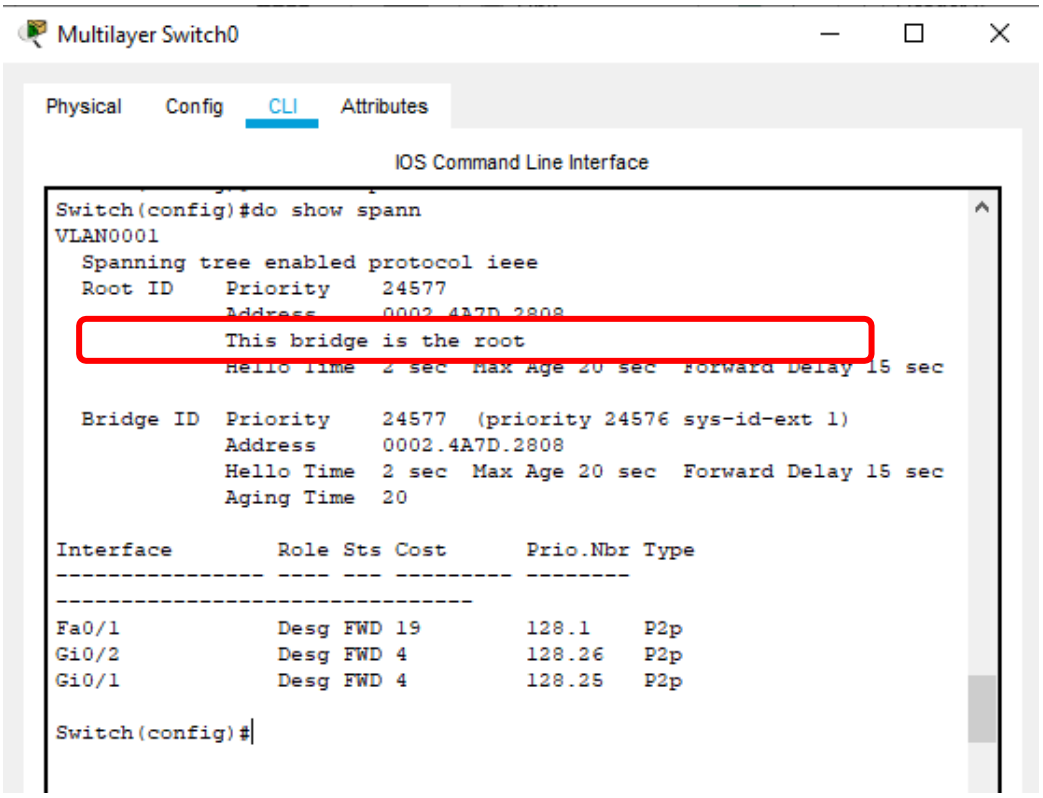
Switch>enable
Switch#show spanning-tree



The output shows that the bridge connected to GigabitEthernet 0/2 is the Root Bridge, i.e., Switch 2 is the Root Bridge in the above topology.

Now we need to make Multilayer Switch0 as the Root Bridge. Type the following commands in the CLI mode of Multilayer Switch0.

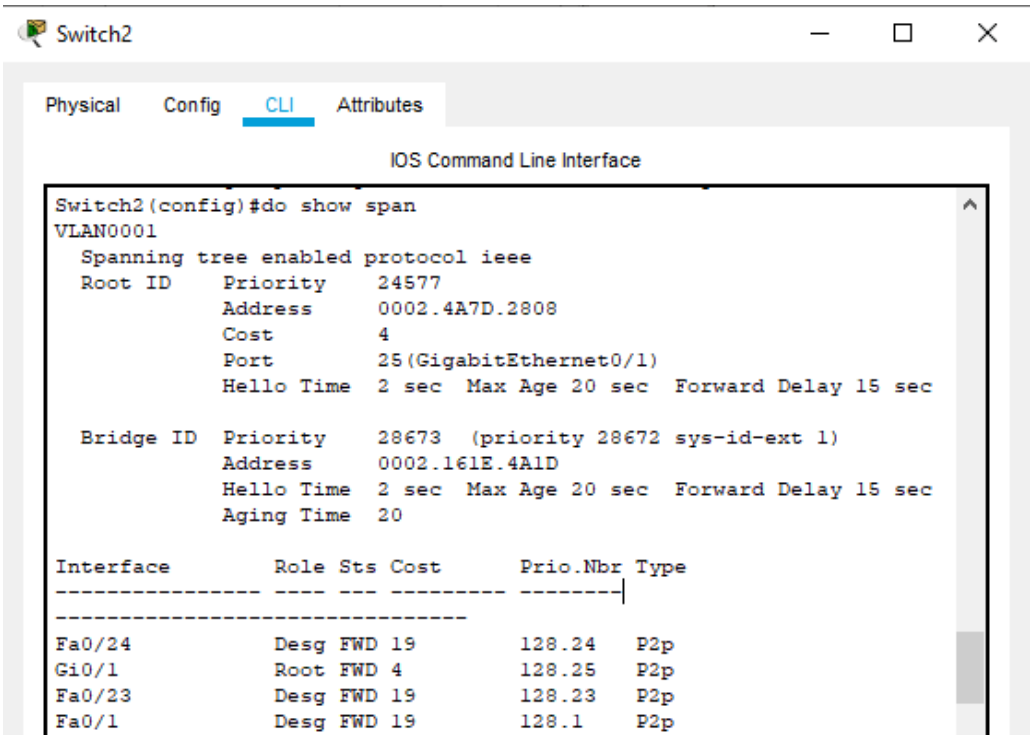
Switch#
Switch#configure terminal
Switch(config)#spanning-tree vlan 1 root primary
Switch(config)#do show spann



Now, we have made the Multilayer Switch0 as the Root Bridge.

But we also need to remove the Switch2 from Root Bridge. For that open the CLI mode of Switch2 and type the following code.

Switch2#configure terminal
Switch2(config)#spanning-tree vlan 1 root secondary
Switch2(config)#do show span



Thus, we have successfully made the central (Multilayer Switch0) as the Root Bridge.

Part 2: Protect Against STP Attacks
Open CLI mode of Switch a and type the following command

```
Switcha>enable
Switcha#configure termial
Switcha(config)#interface range fastEthernet 0/1-2
Switcha(config-if-range)#switchport mode access
Switcha(config-if-range)#spanning-tree portfast
Switcha(config-if-range)#spanning-tree bpduguard enable
```

Now minimize the Switch a window and open the Switch b CLI mode and type the same command

```
Switchb>enable
Switchb#configure termial
Switchb(config)#interface range fastEthernet 0/1-2
Switchb(config-if-range)#switchport mode access
Switchb(config-if-range)#spanning-tree portfast
Switchb(config-if-range)#spanning-tree bpduguard enable
```

Now minimize the Switch b window and open the Switch 1 CLI mode and type the following command

```
Switch1>enable
Switch1#configure terminal
Switch1(config)#interface range fastEthernet 0/23-24
Switch1(config-if-range)#spanning-tree guard root
```

Now minimize the Switch 1 window and open the Switch 2 CLI mode and type the same command

```
Switch2>enable
Switch2#configure terminal
Switch2(config)#interface range fastEthernet 0/23-24
Switch2(config-if-range)#spanning-tree guard root
```

Thus, we have Protected all the switch against STP Attacks.

Part 3: Configure Port Security and Disable unsed ports

Open CLI mode of Switch a and type the following command

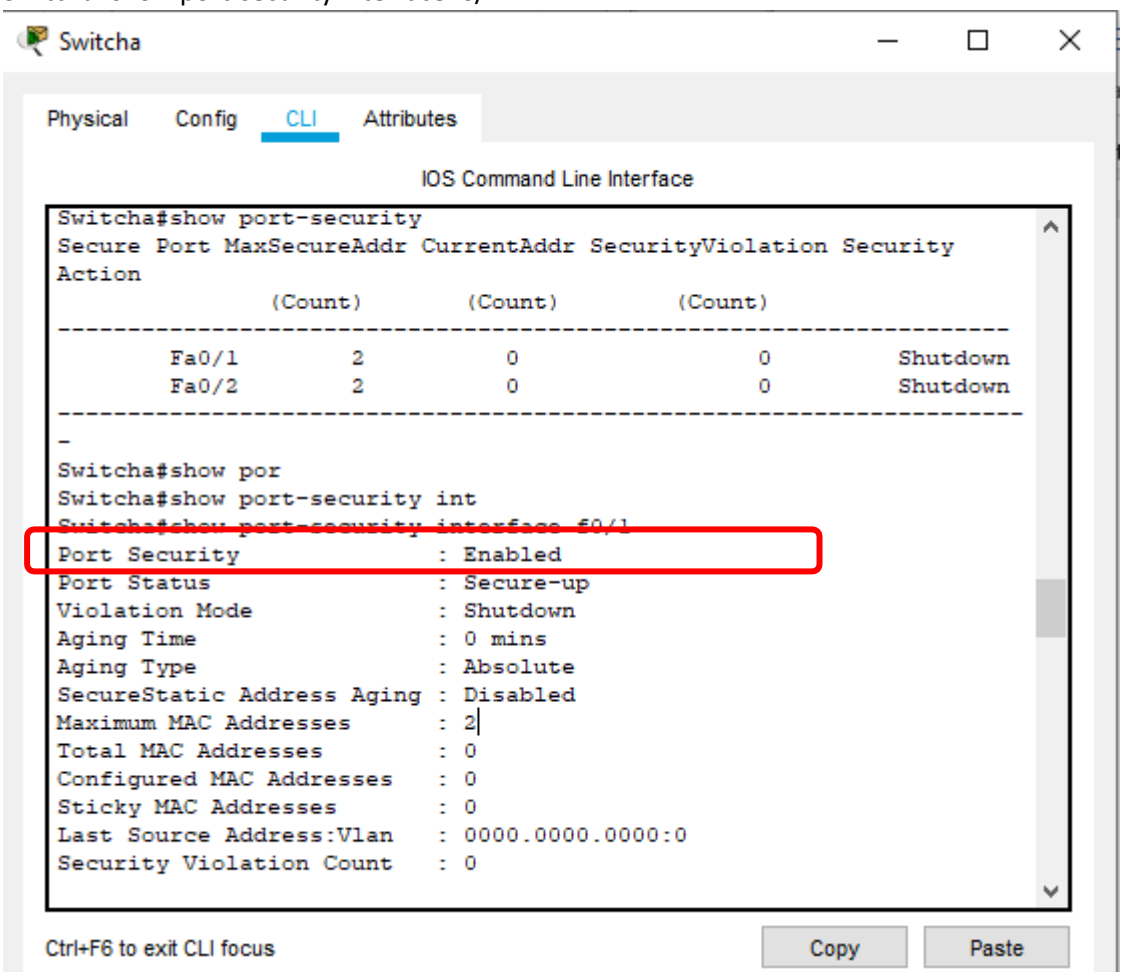
Switcha(config-if-range)#switchport port-security
Switcha(config-if-range)#switchport port-security maximum 2
Switcha(config-if-range)#switchport port-security mac-address sticky
Switcha(config-if-range)#switchport port-security violation shutdown

Now minimize the Switch a window and open the Switch b CLI mode and type the same command

Switchb(config-if-range)#switchport port-security
Switchb(config-if-range)#switchport port-security maximum 2
Switchb(config-if-range)#switchport port-security mac-address sticky
Switchb(config-if-range)#switchport port-security violation shutdown

Now let us check if the security is enabled or not. Open CLI mode of Switch a and type the following

Switcha(config-if-range)# CTRL Z
Switcha#show port-security interface f0/1



Let us now disable all the unused ports in switch a and switch b.

Open the CLI mode of Switch a and type the following command

```
Switcha#enable
Switcha#configure terminal
Switcha(config)#interface range fastEthernet 0/3-22
Switcha(config-if-range)#shutdown
```

Open the CLI mode of Switch b and type the following command

```
Switchb#enable
Switchb#configure terminal
Switchb(config)#interface range fastEthernet 0/3-22
Switchb(config-if-range)#shutdown
```

Thus, Port Security is enabled and all the unsed ports are disabled.