

## Practical 7: Packet Tracer - Layer 2 Security Topology

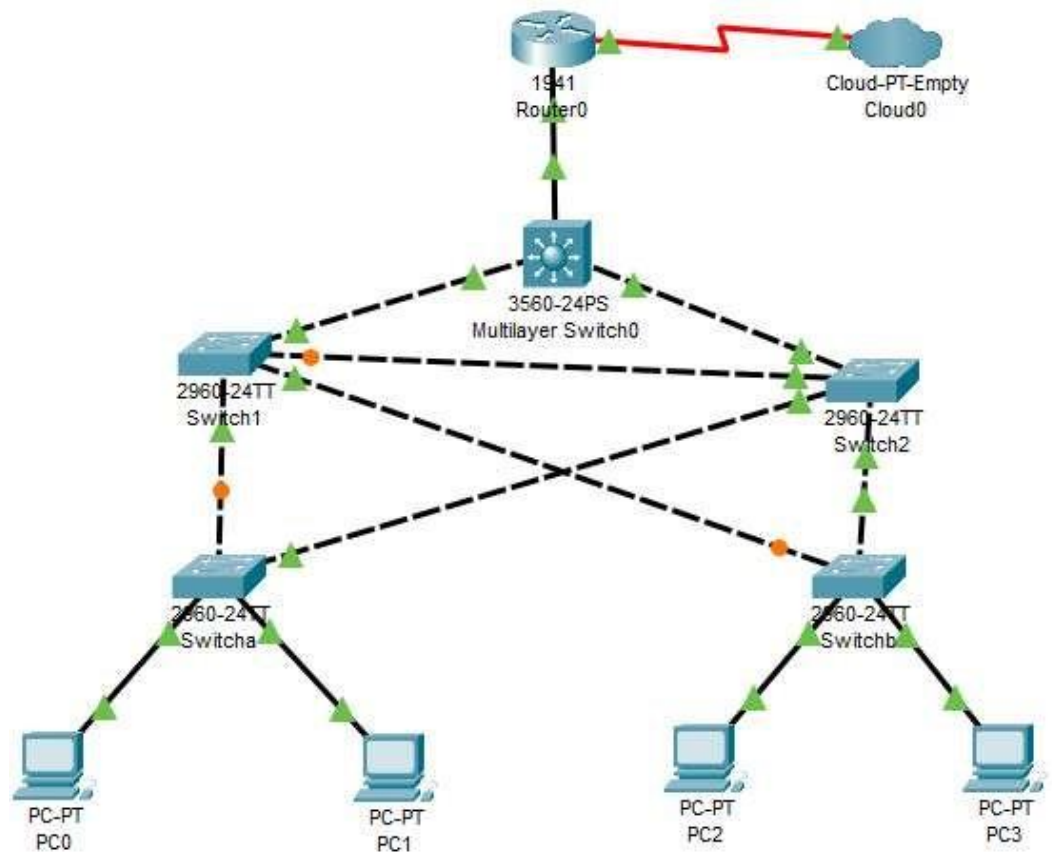
### Objectives

- 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.**

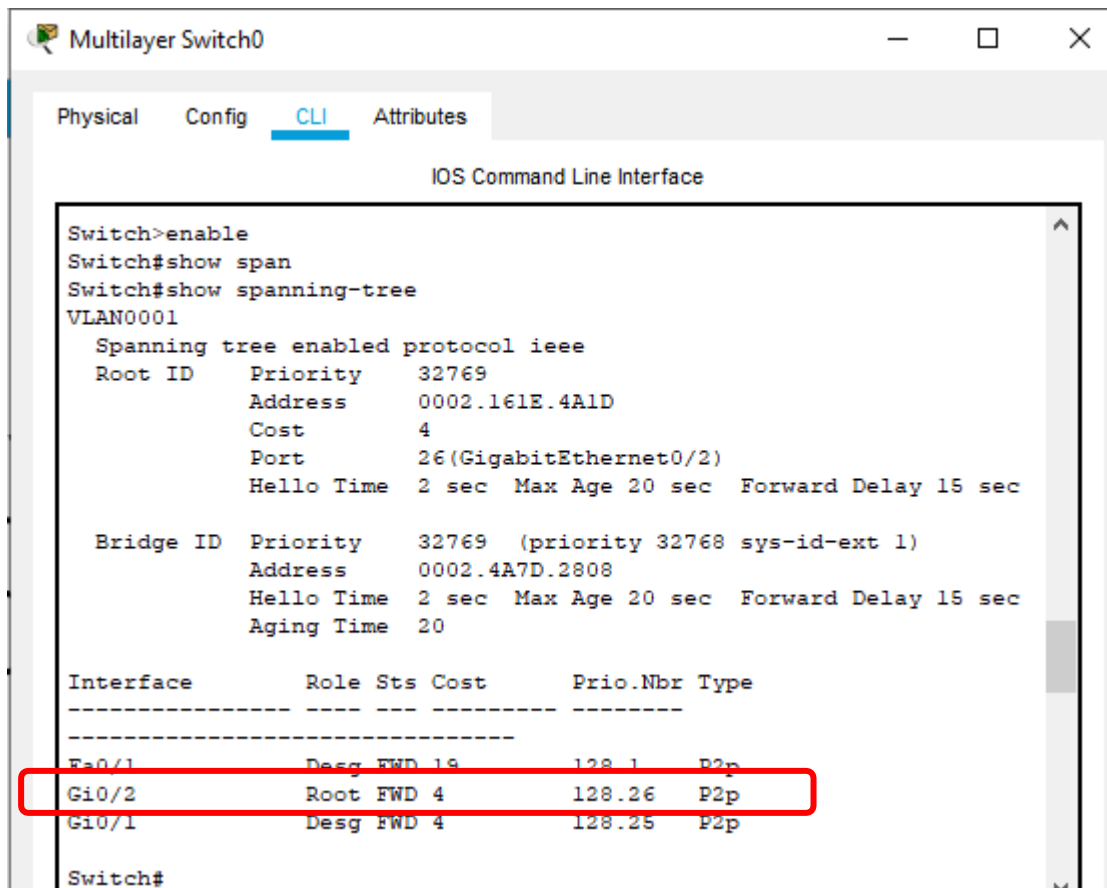
Device	Interface	Switch Port
PC 0	FastEthernet0	Switcha F0/1
PC 1	FastEthernet0	Switcha F0/2
PC 2	FastEthernet0	Switchb F0/1
PC 3	FastEthernet0	Switchb F0/2
Switch a	F0/23	Switch1 F0/23
	F0/24	Switch2 F0/1
Switch b	F0/23	Switch2 F0/23
	F0/24	Switch1 F0/1
Switch 1	F0/24	Switch2 F0/24
	GE 0/1	Multilayer 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
```



```
Multilayer Switch0
Physical Config CLI Attributes
IOS Command Line Interface

Switch>enable
Switch#show span
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0002.161E.4A1D
             Cost        4
             Port        26(GigabitEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0002.4A7D.2808
             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
Gi0/2          Root FWD 4       128.26  P2p
Gi0/1          Desg FWD 4       128.25  P2p

Switch#
```

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.

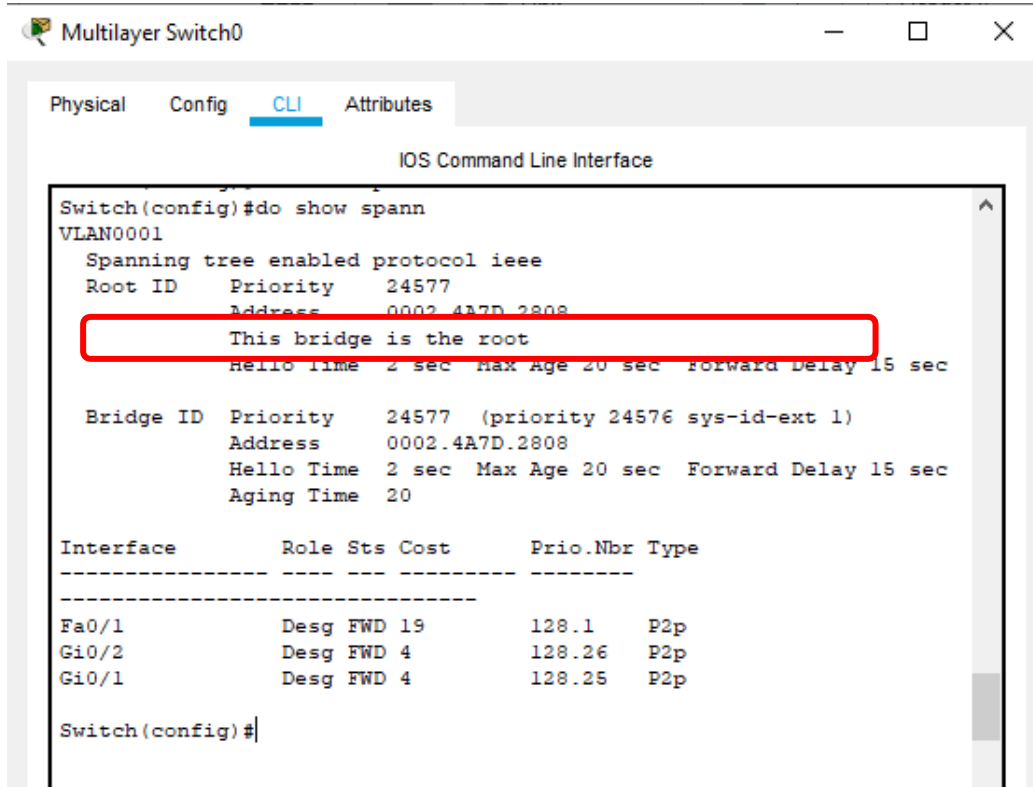
Now we need to make Multilayer Switch0 as the Root Bridge. Type the following commands in the CLI mode of Multilayer Switch0.

```
Switch#
```

```
Switch#configure terminal
```

```
Switch(config)#spanning-tree vlan 1 root primary
```

```
Switch(config)#do show spann
```



```
Switch(config)#do show spann
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    24577
           Address    0002.4A7D.2808
           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    0002.4A7D.2808
           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
Gi0/2          Desg FWD 4       128.26   P2p
Gi0/1          Desg FWD 4       128.25   P2p

Switch(config)#
```

**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
```

```
Switch2(config)#do show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0002.4A7D.2808
             Cost        4
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28673 (priority 28672 sys-id-ext 1)
             Address     0002.161E.4A1D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/24         Desg FWD 19        128.24  P2p
Gi0/1          Root FWD 4         128.25  P2p
Fa0/23         Desg FWD 19        128.23  P2p
Fa0/1          Desg FWD 19        128.1   P2p
```

**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 terminal
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 terminal
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 unused 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
```

The screenshot shows a window titled 'Switcha' with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the 'IOS Command Line Interface'. The output of the command 'Switcha#show port-security' is shown as a table:

Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security Action
	(Count)	(Count)	(Count)	
Fa0/1	2	0	0	Shutdown
Fa0/2	2	0	0	Shutdown

Below the table, the output of 'Switcha#show port-security int' is shown. The command 'Switcha#show port-security interface f0/1' is highlighted with a red box, and its output is displayed below it:

```
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
```

At the bottom of the window, there is a status bar with 'Ctrl+F6 to exit CLI focus' and buttons for 'Copy' and 'Paste'.



**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 unused ports are disabled.**