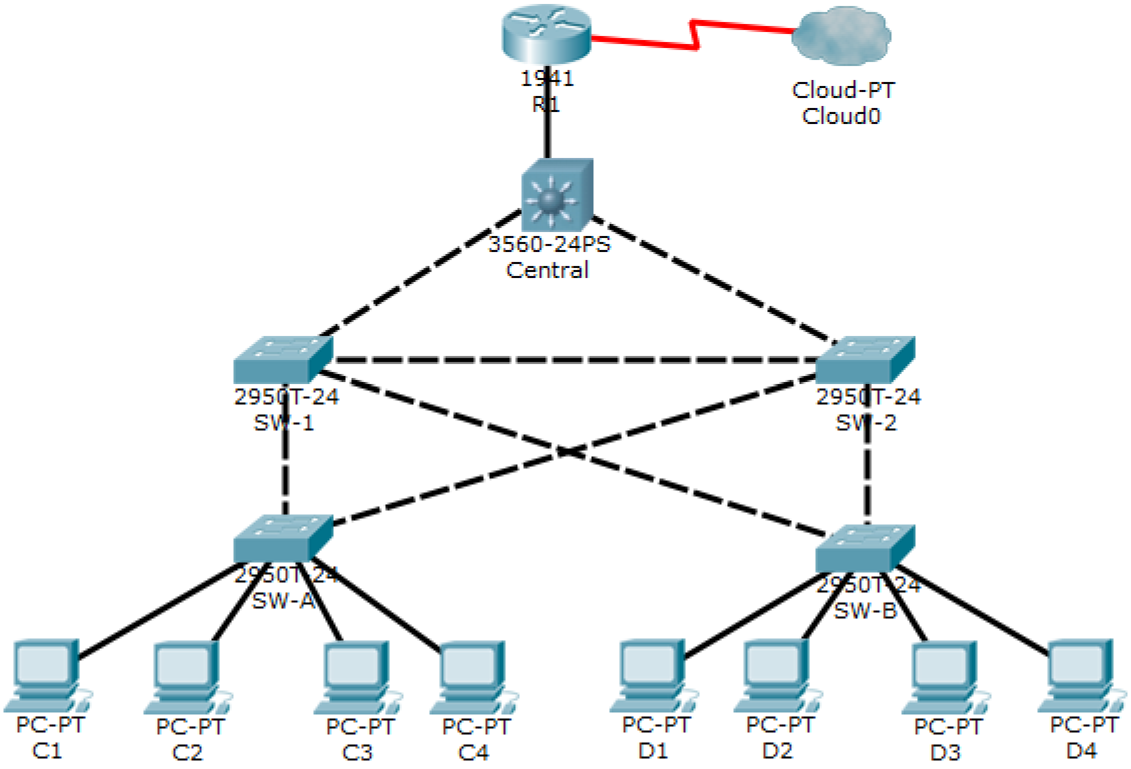
Packet Tracer - Layer 2 Security (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

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.

All switch devices have been preconfigured with the following:

- Enable password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- SSH username and password: **SSHadmin** / **ciscosshpa55**

Part 1: Configure Root Bridge

Step 1: Determine the current root bridge.

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

Which switch is the current root bridge?

____

Current root is SW-1.

Based on the current root bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

Step 2: Assign Central as the primary root bridge.

Using the **spanning-tree vlan 1 root primary** command, and assign **Central** as the root bridge.

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

Step 3: Assign SW-1 as a secondary root bridge.

Assign **SW-1** as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command.

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

Step 4: Verify the spanning-tree configuration.

Issue the **show spanning-tree** command to verify that **Central** is the root bridge.

```
Central# show spanning-tree
VLAN0001
   Spanning tree enabled protocol ieee
   Root ID  Priority      24577
            Address       00D0.D31C.634C
            This bridge is the root
            Hello Time  2 sec  Max Age  20 sec   Forward Delay  15 sec
```

Which switch is the current root bridge?

____

Current root is Central

Based on the new root-bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

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 **SW-A** and **SW-B**, use the **spanning-tree portfast** command.

```
SW-A(config)# interface range f0/1 - 4
SW-A(config-if-range)# spanning-tree portfast

SW-B(config)# interface range f0/1 - 4
```

```
SW-B(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 **SW-A** and **SW-B** access ports.

```
SW-A(config)# interface range f0/1 - 4
SW-A(config-if-range)# spanning-tree bpduguard enable

SW-B(config)# interface range f0/1 - 4
SW-B(config-if-range)# spanning-tree bpduguard enable
```

Note: Spanning-tree BPDU guard can be enabled on each individual port using the **spanning-tree bpduguard enable** command in interface configuration mode or the **spanning-tree portfast bpduguard default** command in global configuration mode. For grading purposes in this activity, please use the **spanning-tree bpduguard enable** command.

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 **SW-1**, enable root guard on ports F0/23 and F0/24. On **SW-2**, enable root guard on ports F0/23 and F0/24.

```
SW-1(config)# interface range f0/23 - 24
SW-1(config-if-range)# spanning-tree guard root

SW-2(config)# interface range f0/23 - 24
SW-2(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 **SW-A** and **SW-B**. 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.

```
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 2
SW-A(config-if-range)# switchport port-security violation shutdown
SW-A(config-if-range)# switchport port-security mac-address sticky

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
```

Why is port security not enabled on ports that are connected to other switch devices?

____

____

____

____

____

Ports connected to other switch devices have a multitude of MAC addresses learned for that single port. Limiting the number of MAC addresses that can be learned on these ports can significantly impact network functionality.

Step 2: Verify port security.

a. On **SW-A**, issue the command **show port-security interface f0/1** to verify that port security has been configured.

```
SW-A# show port-security interface 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
```

b. Ping from **C1** to **C2** and issue the command **show port-security interface f0/1** again to verify that the switch has learned the MAC address for **C1**.

Step 3: Disable unused ports.

Disable all ports that are currently unused.

```
SW-A(config)# interface range f0/5 - 22
SW-A(config-if-range)# shutdown

SW-B(config)# interface range f0/5 - 22
SW-B(config-if-range)# shutdown
```

Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to view feedback and verification of which of the required components have been completed.

!!!Script for Central

```
conf t
```

```
spanning-tree vlan 1 root primary
end
```

!!!Script for SW-1

```
conf t
spanning-tree vlan 1 root secondary
interface range f0/23 - 24
 spanning-tree guard root
end
```

!!!Script for SW-2

```
conf t
interface range f0/23 - 24
 spanning-tree guard root
end
```

!!!Script for SW-A

```
conf t
interface range f0/1 - 4
 spanning-tree portfast
 spanning-tree bpduguard enable
interface range f0/1 - 22
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
interface range f0/5 - 22
 shutdown
end
```

!!!Script for SW-B

```
conf t
interface range f0/1 - 4
 spanning-tree portfast
 spanning-tree bpduguard enable
interface range f0/1 - 22
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
interface range f0/5 - 22
 shutdown
end
```