Packet Tracer - Implement STP Security

# Objectives

* Assign the Central switch as the root bridge.
* Secure spanning-tree parameters to prevent STP manipulation 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.

All switch devices have been preconfigured with the following:

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

# Instructions

## Configure Root Bridge

### 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.

#### Question:

Which switch is the current root bridge?

Type your answers here.

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

Draw your topology diagram here.

### Assign Central as the primary root bridge.

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

### 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.

### 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

#### Questions:

Which switch is the current root bridge?

Type your answers here.

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

Draw your topology diagram here.

## Protect Against STP Attacks

Secure the STP parameters to prevent STP manipulation attacks.

### 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.

### 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.

**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 defaultcommand in global configuration mode. For grading purposes in this activity, please use the spanning-tree bpduguard enable command.

### 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.

end of document