Practical 8: Packet Tracer - Layer 2 Security

All switch devices have been preconfigured with the following:

Enable password: ciscoenpa55

Console password: ciscoconpa55

SSH username and password: SSHadmin / ciscosshpa55

**Write the commands for the above**

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.

Step 2: Assign Central as the primary root bridge.

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

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

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

Step 4: Verify the spanning-tree configuration.

show spanningtree

Part 2: Protect Against STP Attacks

Step 1: Enable PortFast on all access ports.

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.

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 S

W-B(config-if-range)# spanning-tree bpduguard enable

Step 3: Enable root guard.

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.

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 SWA(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

Step 2: Verify port security.

On SW-A, issue the command

SW-A# show port-security interface f0/1

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