Practical 8

- Packet Tracer - Layer 2 Security

Part 1 - Assign the central switch as the root bridge

Step 1: Determine the current root bridge.

Central# show spanning-tree

Step 2 - Assign central as the primary root bridge

Central(config)# spanning-tree vlan1 root primary

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

SW-1(config)# spanning-tree vlan1 root secondary

Step 4 - Verify the spanning-tree configuration

Central# show spanning-tree.

Part 2 - Secure spanning-tree parameters to prevent STP manipulation 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
SW-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 - Enable port security to prevent CAM table overflow attacks.

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
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

Step 2 - Verify Port Security

SW-A# show port-security interface F0/1

ping from C1 to C2
>ping 10.1.1.1

SW-A # show port-security interface F0/1

Step 3 - Disable unused ports

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.