Q. 7) Configuring Layer 2 Security

Topology:

1. Configure Root Bridge
2. In central switch’s CLI:

Enter:

en

show spanning-tree

We have to assign central switch as root bridge (Currently switch 1 is root bridge), for which we will enter following command:

en

conf t

spanning-tree vlan 1 root primary

do show spann

1. In switch1’s CLI:

Make this switch as secondary switch:

en

conf t

spanning-tree vlan 1 root secondary

do show spann

B) Protect Against STP attack

1. Enable PortFast and bpdu on all access ports for both switches.

Enter these commands on both switches. (A and B)

en

conf t

int range f0/1-4

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

1. Enable root guard.

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

F0/24.

Enter: (For both switches) (1 and 2)

do show spann

We have Used the show spanning-tree command to determine the location of the

root port on each switch. As root guard can be enabled on all ports on a switch that are not root ports.

1. Now Enter: (For both switches) (1 and 2)

conf t

int range f0/23-24

spanning-tree guard root

C) Configure Port Security and disable unused ports.

1. Enter on both switches: (A and B)

en

conf t

int 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

1. Verify port security.

Enter: (for both switches) (A and B)

Show port-security interface f0/1

Ping 10.1.1.11 from C1 and then again enter show port-security interface f0/1 to show that the switch has learned the MAC address for C1.

1. Disable unused ports.

Enter: for both switches (A and B)

int range f0/5-22

shutdown