**Configure Switch/Router (** Execute command on all switches and routers**) SW/R1 config**

**Configure secret**

enable secret enpa55

**Configure console password**

line console 0

password conpa55

login

exit

**Configure SSH login**

ip domain-name ccnasecurity.com

username admin secret adminpa55

line vty 0 4

login local

crypto key generate rsa

1024

**Configure Root Bridge**

**Determine the current root bridge.**

Central# show spanning-tree

(to determine the current root bridge)

**Assign Central as the primary root bridge**

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

**Assign SW-1 as a secondary root bridge**

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

**Verify the spanning-tree configuration.**

Central# show spanning-tree

( You can see the This bridge is the root) **output**

**Protect Against STP Attacks**

**Enable PortFast on all access ports**

SW-A , SW-B(config)#

interface range f0/1 – 4

spanning-tree portfast

**Enable BPDU guard on all access ports**

SW-A , SW-B(config)#

interface range f0/1 – 4

spanning-tree bpduguard enable

**Enable root guard**

SW-1 , SW-2(config)#

interface range f0/23 – 24

spanning-tree guard root

**Configure Port Security and Disable Unused Ports**

**Configure basic port security on all ports connected to host devices**

SW-A , SW-B(config)#

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

**Verify port security**

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

( Here you see port security:Enabled, violation Mode : Shutdown, Mac addresses :2)

* 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

**Disable unused ports**

SW-A , SW-B(config)#

interface range f0/5 – 22

shutdown