**Layer 2 VLAN Security**

**Part 1: Configure Switch/Router**

**Step 1: Configure secret**

Execute command on all switches/router

SW/R1(config)# enable secret enpa55

**Step 2: Configure console password**

Execute command on all switches/router

SW/R1(config)#

line console 0

password conpa55

login

**Step 3: Configure SSH login**

Execute command on all switches/router

SW/R1(config)#

ip domain-name ccnasecurity.com

username admin secret adminpa55

line vty 0 4

login local

crypto key generate rsa

How many bits in the modulus [512]: 1024

**Part 2: Create a Redundant Link between SW-1 and SW-2**

**Step 1: Connect SW-1 and SW-2.**

Using a crossover cable, connect port Fa0/23 on SW-1 to port Fa0/23 on SW-2.

**Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.** (Execute command on SW- 1 and SW-2)

SW1/2(config)#

int fa0/23

switchport mode trunk

switchport trunk native vlan 15

switchport nonegotiate

no shutdown

**Part 3: Enable VLAN 20 as a Management VLAN**

**Step 1: Enable a management VLAN (VLAN 20) on SW-A.**

SW-A(config)# vlan 20

SW-A(config-vlan)# exit

SW-A(config)# int vlan 20

SW-A(config-if)# ip address 192.168.20.1 255.255.255.0

**Step 2: Enable the same management VLAN on all other switches**

(Execute command on SW-B, SW-1, SW-2, and Central)

SW(config)# vlan 20

SW(config-vlan)# exit

***Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.***

SW-B(config)# int vlan 20

SW-B(config-if)# ip address 192.168.20.2 255.255.255.0

SW-1(config)#int vlan 20

SW-1(config-if)#ip address 192.168.20.3 255.255.255.0

SW-2(config)#int vlan 20

SW-2(config-if)#ip address 192.168.20.4 255.255.255.0

Central(config)# int vlan 20

Central(config-if)# ip address 192.168.20.5 255.255.255.0

**Step 3: Connect and configure the management PC.**

***Connect the management PC using copper straight-through to SW-A port***

***Fa0/1 and ensure that it is assigned an available IP address 192.168.20.50***

**Step 4: On SW-A, ensure the management PC is part of VLAN 20.**

SW-A(config)# int fa0/1

SW-A(config)# switchport mode access

SW-A(config-if)# switchport access vlan 20

**Step 5: Verify connectivity of the management PC to all switches.**

C1> ping 192.168.20.1 (SW-A)

(Successful)

C1> ping 192.168.20.2 (SW-B)

(Successful)

C1> ping 192.168.20.3 (SW-1)

(Successful)

C1> ping 192.168.20.4 (SW-2)

(Successful)

C1> ping 192.168.20.5 (Central)

(Successful)

**Part 4: Enable the Management PC to Access Router R1**

**Step 1: Enable a new subinterface on router R1.**

R1(config)# int gig0/0.3

R1(config-subif)# encapsulation dot1q 20

R1(config-subif)# ip address 192.168.20.100 255.255.255.0

**Step 2: Set default gateway in management PC.**

C1 – 192.168.20.100

**Step 3: Verify connectivity between the management PC and R1.**

C1> ping 192.168.20.100

(Successful)

**Step 4: Enable security.**

R1(config)# access-list 101 deny ip any 192.168.20.0 0.0.0.255

R1(config)# access-list 101 permit ip any any

R1(config)# access-list 102 permit ip host 192.168.20.50 any

**Step 5: Apply ACL on correct interfaces**

R1(config)# int gig0/0.1

R1(config-subif)# ip access-group 101 in

R1(config-subif)# int gig0/0.2

R1(config-subif)# ip access-group 101 in

R1(config-subif)# line vty 0 4

R1(config-line)# access-class 102 in

**Step 6: Verify connectivity between the management PC and SW-A, SW-B and R1**

C1> ping 192.168.20.1 (SW-A)

(Successful)

C1> ping 192.168.20.2 (SW-B)

(Successful)

C1> ping 192.168.20.100 (R1)

(Successful)

**Step 7: Verify connectivity between the D1 and management PC.**

D1>ping 192.168.20.50

(Unsuccessful – Destination host unreachable)