Practical 9: Layer 2 VLAN Security

All devices have been preconfigured with:

o Enable secret password: ciscoenpa55

o Console password: ciscoconpa55   
o SSH username and password: SSHadmin / ciscosshpa55

Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10). Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

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 F0/23 on SW-1 to port F0/23 on SW-2

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

On both SW-1 and SW-2, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.

SW-1(config)# interface f0/23

SW-1(config-if)# switchport mode trunk

SW-1(config-if)# switchport trunk native vlan 15

SW-1(config-if)# switchport nonegotiate

SW-1(config-if)# no shutdown

SW-2(config)# interface f0/23

SW-2(config-if)# switchport mode trunk

SW-2(config-if)# switchport trunk native vlan 15

SW-2(config-if)# switchport nonegotiate

SW-2(config-if)# no shutdown

Part 3: Enable VLAN 20 as a Management VLAN

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

1. Enable VLAN 20 on SW-A.

SW-A(config)# vlan 20

SW-A(config-vlan)# exit

1. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.
2. SW-A(config)# interface vlan 20
3. 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.

1. Create the management VLAN on all switches: SW-B, SW-1, SW-2, and Central.

SW-B(config)# vlan 20

SW-B(config-vlan)# exit

SW-1(config)# vlan 20

SW-1(config-vlan)# exit

SW-2(config)# vlan 20

SW-2(config-vlan)# exit

Central(config)# vlan 20

Central(config-vlan)# exit

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

SW-B(config)# interface vlan 20

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

SW-1(config)# interface vlan 20

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

SW-2(config)# interface vlan 20

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

Central(config)# interface vlan 20

Central(config-if)# ip address 192.168.20.5 255.255.255.0

Step 3: Connect and configure the management PC.

Step 4: On SW-A, ensure the management PC is part of VLAN 20. Interface F0/1 must be part of VLAN 20.

SW-A(config)# interface f0/1

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

SW-A(config-if)# no shutdown

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

Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

1. Create subinterface g0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.

R1(config)# interface g0/0.3

R1(config-subif)# encapsulation dot1q 20

1. Assign an IP address within the 192.168.20.0/24 network. R1(config)# interface g0/0.3

R1(config-subif)# ip address 192.168.20.100 255.255.255.0

Step 2: Verify connectivity between the management PC and R1. B

Step 3: Enable security. While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

1. Create an ACL that allows only the Management PC to access the router. Example: (may vary from student configuration)

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

1. Apply the ACL to the proper interface(s). Example: (may vary from student configuration)

R1(config)# interface g0/0.1

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

R1(config-subif)# interface g0/0.2

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

R1(config-subif)# line vty 0 4

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

Step 4: Verify security.

1. Verify only the Management PC can access the router.

Use SSH to access R1 with username SSHadmin and password ciscosshpa55.

PC> ssh -l SSHadmin 192.168.20.100

1. From the management PC, ping SW-A, SW-B, and R1. Were the pings successful?

The pings should have been successful

1. From D1, ping the management PC. Were the pings successful?

The ping should have failed.