P8(Packet Tracer - Layer 2 VLAN Security)

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).

Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.

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.

S**tep 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and**

SW-2.

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for

trunking, including all trunk security mechanisms. 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

The network administrator wants to access all switch and routing devices using a management PC. For

security purposes, the administrator wants to ensure that all managed devices are on a separate VLAN.

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

a. Enable VLAN 20 on SW-A.

SW-A(config)# vlan 20

SW-A(config-vlan)# exit

b. 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

Step 3: Connect and configure the management PC.

Connect the management PC to SW-A port F0/1 and ensure that it is assigned an available IP address within

the 192.168.20.0/24 network.

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.

The management PC should be able to ping SW-A, SW-B, SW-1, SW-2, and Central.

Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

a. 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

b. 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.

Be sure to configure the default gateway on the management PC to allow for connectivity.

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.

a. 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

b. 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

PC> ssh -l SSHadmin 192.168.20.100

Step 5: Check results

!!! Script for SW-1

conf t

interface f0/23

switchport mode trunk

switchport trunk native vlan 15

switchport nonegotiate

no shutdown

vlan 20

exit

interface vlan 20

ip address 192.168.20.3 255.255.255.0

!!! Script for SW-2

conf t

interface f0/23

switchport mode trunk

switchport trunk native vlan 15

switchport nonegotiate

no shutdown

vlan 20

exit

interface vlan 20

ip address 192.168.20.4 255.255.255.0

!!! Script for SW-A

conf t

vlan 20

exit

interface vlan 20

ip address 192.168.20.1 255.255.255.0

interface f0/1

switchport access vlan 20

no shutdown

The ping should have failed because for a device within a different VLAN to successfully ping a

!!! Script for SW-B

conf t

vlan 20

exit

interface vlan 20

ip address 192.168.20.2 255.255.255.0

!!! Script for Central

conf t

vlan 20

exit

interface vlan 20

ip address 192.168.20.5 255.255.255.0

!!! Script for R1

conf t

interface GigabitEthernet0/0.1

ip access-group 101 in

interface GigabitEthernet0/0.2

ip access-group 101 in

interface g0/0.3

encapsulation dot1q 20

ip address 192.168.20.100 255.255.255.0

access-list 101 deny ip any 192.168.20.0 0.0.0.255

access-list 101 permit ip any any

access-list 102 permit ip host 192.168.20.50 any

line vty 0 4

access-class 102 in