Packet Tracer - Switch Security Configuration (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

11.6.1 Packet Tracer – Switch Security Configuration Answer

VLAN Table

Switch	VLAN Number	VLAN Name	Port Membership	Network
SW-1	10	Admin	F0/1, F0/2	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	G0/1, G0/2	None
	999	BlackHole	All unused	None
SW-2	10	Admin	F0/1, F0/22	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	None	None
	999	BlackHole	All unused	None

Objectives

Part 1: Create a Secure Trunk

Part 2: Secure Unused Switchports

Part 3: Implement Port Security

Part 4: Enable DHCP Snooping

Part 5: Configure Rapid PVST PortFast and BPDU Guard

Background

You are enhancing security on two access switches in a partially configured network. You will implement the range of security measures that were covered in this module according to the requirements below. Note that routing has been configured on this network, so connectivity between hosts on different VLANs should function when completed.

Instructions

Step 1: Create a Secure Trunk.

a. Connect the G0/2 ports of the two access layer switches.

b. Configure ports G0/1 and G0/2 as static trunks on both switches.

c. Disable DTP negotiation on both sides of the link.

d. Create VLAN 100 and give it the name Native on both switches.

e. Configure all trunk ports on both switches to use VLAN 100 as the native VLAN.

Step 2: Secure Unused Switchports.

a. Shutdown all unused switch ports on SW-1.

b. On SW-1, create a VLAN 999 and name it BlackHole. The configured name must match the requirement exactly.

c. Move all unused switch ports to the BlackHole VLAN.

Step 3: Implement Port Security.

a. Activate port security on all the active access ports on switch SW-1.

b. Configure the active ports to allow a maximum of 4 MAC addresses to be learned on the ports.

c. For ports F0/1 on SW-1, statically configure the MAC address of the PC using port security.

d. Configure each active access port so that it will automatically add the MAC addresses learned on the port to the running configuration.

e. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum, generate a Syslog entry, but not disable the ports.

Step 4: Configure DHCP Snooping.

a. Configure the trunk ports on SW-1 as trusted ports.

b. Limit the untrusted ports on SW-1 to five DHCP packets per second.

c. On SW-2, enable DHCP snooping globally and for VLANs 10, 20 and 99.

Note: The DHCP snooping configuration may not score properly in Packet Tracer.

Step 5: Configure PortFast, and BPDU Guard.

a. Enable PortFast on all the access ports that are in use on SW-1.

b. Enable BPDU Guard on all the access ports that are in use on SW-1.

c. Configure SW-2 so that all access ports will use PortFast by default.

SW1 Configurations

```
enable
configure terminal
spanning-tree portfast default
interface FastEthernet0/1
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address 0010.11E8.3CBB
 spanning-tree portfast
```

```
 spanning-tree bpduguard enable
!
interface range FastEthernet0/2, FastEthernet0/10,FastEthernet0/24
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface range FastEthernet0/3 - 9, FastEthernet0/11 - 23
 switchport access vlan 999
 shutdown
!
interface range GigabitEthernet0/1 - 2
 switchport trunk native vlan 100
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
vlan 100
 name Native
vlan 999
 name BlackHole
```

SW-2 Configuration

```
enable
configure terminal
ip dhcp snooping
ip dhcp snooping vlan 10,20,99
spanning-tree portfast default
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/2
 switchport trunk native vlan 100
 switchport mode trunk
 switchport nonegotiate
```