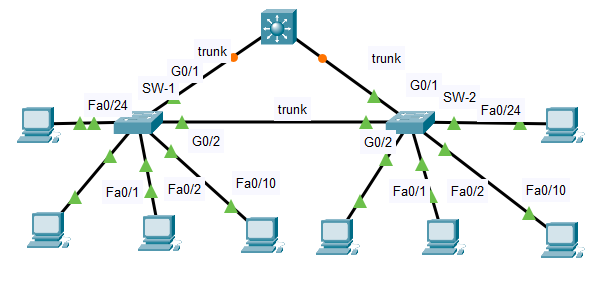
Packet Tracer - Switch Security Configuration

****

|  |  |
| --- | --- |
| **NAME** | **MOHAMAD SAIFUL NIZAM BIN ABD AZIZ** |
| **NO. MATRIC** | **A179830** |
| **INSTRUCTOR** | **TS. DR. WAN FARIZA BINTI FAUZI** |

Packet Tracer - Switch Security Configuration

# VLAN Table



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

Blank Line - no additional information

# 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

## Create a Secure Trunk.

* + - 1. Connect the G0/2 ports of the two access layer switches.
      2. Configure ports G0/1 and G0/2 as static trunks on both switches.
      3. Disable DTP negotiation on both sides of the link.
      4. Create VLAN 100 and give it the name Native on both switches.
      5. Configure all trunk ports on both switches to use VLAN 100 as the native VLAN.

## Secure Unused Switchports.

* + - 1. Shutdown all unused switch ports on SW-1.
      2. On SW-1, create a VLAN 999 and name it BlackHole. The configured name must match the requirement exactly.
      3. Move all unused switch ports to the BlackHole VLAN.

## Implement Port Security.

* + - 1. Activate port security on all the active access ports on switch SW-1.
      2. Configure the active ports to allow a maximum of 4 MAC addresses to be learned on the ports.
      3. For ports F0/1 on SW-1, statically configure the MAC address of the PC using port security.
      4. Configure each active access port so that it will automatically add the MAC addresses learned on the port to the running configuration.
      5. 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.

## Enable DHCP Snooping.

* + - 1. Enable dhcp snooping in the global configuration mode on SW-1 and SW-2.
      2. By default, all ports are untrusted. Explicitly configure the trunk ports as trusted on SW-1 and SW-2.
      3. Limit the DISCOVER messages to 6 on the remaining untrusted ports on SW-1 and SW-2.
      4. Enable dhcp snooping on VLAN 10, 20, 99 and 100 on SW-1 and SW-2.

## Configure PortFast, and BPDU Guard.

* + - 1. Enable PortFast on all the access ports that are in use on SW-1.
      2. Enable BPDU Guard on all the access ports that are in use on SW-1.
      3. Configure SW-2 so that all access ports will use PortFast by default.

**Reflection:**

List all the LAN attacks that can be mitigated for each part (Part 1-5).

Part 1: VLAN hopping and VLAN double-tagging.

Part 2: CDP Reconnaissance.

Part 3: MAC Address Spoofing.

Part 4: DHCP Starvation and DHCP Snooping.

Part 5: STP Attack.

List the commands used to verify the configuration of each part.

* show vlan brief
* show port-security