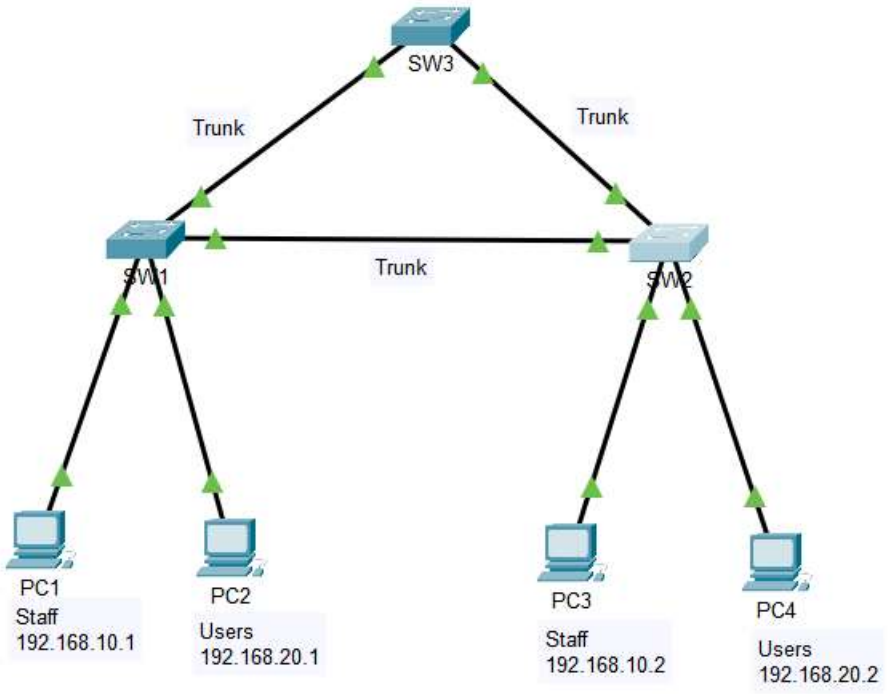
Redes de Computadores - RECOMP

Layer two Security Configuration

Lab Topology:

The lab network topology is illustrated below:



Device	VLAN ID	VLAN Name	Network
SW1	10	Staff	192.168.10.0/24
	20	Users	192.168.20.0/24
	100	Native	None
	999	BlackHole	None
SW2	10	Staff	192.168.10.0/24
	20	Users	192.168.20.0/24
	100	Native	None
	999	BlackHole	None
SW3	10	Staff	192.168.10.0/24
	20	Users	192.168.20.0/24
	100	Native	None
	999	BlackHole	None

Table 1 – VLANs table

Objectives

Part 1: Initial Configuration

Part 2: Create a Secure Trunk

Part 3: Secure Unused Switchports

Part 4: Implement Port Security

Part 5: Configure PortFast, and BPDU Guard.

Background

Enhancing security on two access switches in the network, implement the set of security measures according to the requirements below.

Instructions

Step 1: Initial Configuration

a) Assign each switch a hostname according to the topology diagram.
b) Configure the PC's IP addresses accordingly with Table 1.
c) Create the VLAN 10 and 20, in all the switches.

```
SW1(config)#vlan 10
SW1(config-vlan)#name Staff
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Users
```

d) Configure the interfaces as access ports and assign the VLANs created, in both switches (SW1 e SW2).

```
SW1(config)#interface FastEthernet0/1
SW1(config-if)#switchport access vlan 10
SW1(config)#interface FastEthernet0/2
SW1(config-if)#switchport access vlan 20
```

Step 2: Create a Secure Trunk.

a) Configure all switches as **static trunks**.

```
SW1(config)#interface range GigabitEthernet0/1-2
SW1(config-if)#switchport mode trunk
```

b) Disable DTP negotiation on all sides of the trunk links.

```
SW1(config)#interface GigabitEthernet0/2
SW1(config-if)#switchport nonegotiate
```

c) Create VLAN 100 and give it the name Native on all switches.

```
SW1(config)#vlan 100
SW1(config-vlan)#name Native
```

d) Configure all trunk ports on all switches to use VLAN 100 as the native VLAN.

```
SW1(config)#interface range GigabitEthernet0/1-2
SW1(config-if-range)#switchport trunk native vlan 100
```

Step 3: Secure Unused Switch ports.

a) Shutdown all unused ports on the switches.

```
SW1(config)#interface range fa0/3-24
SW1(config-if-range)#shutdown
```

b) On all switches, create a VLAN 999 and name it BlackHole.

```
SW3(config)#vlan 999
SW3(config-vlan)#name BlackHole
```

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

```
SW1(config)#interface range fa0/3-24
SW1(config-if-range)#switchport access vlan 999
```

Step 4: Implement Port Security.

a) Activate port security on all the active access ports on all the switches.

```
SW1(config)#interface FastEthernet0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
```

b) Configure the active ports to allow a maximum of 2 MAC addresses to be learned on the ports.

```
SW1(config-if)#switchport port-security maximum 1
```

c) For SW1, statically configure the MAC address of the PC1 using port security.

```
SW1(config-if)#switchport port-security mac-address sticky
000A.F331.42CE
```

Note: Check the MAC address of your PC1 matches the given MAC.

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

```
SW1(config-if)#switchport port-security mac-address sticky
```

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

```
SW1(config-if)#switchport port-security violation restrict
```

Step 5: Configure PortFast, and BPDU Guard.

a) Configure STP to work with Rapid STP in all the switches.

```
SW1(config)#spanning-tree mode rapid-pvst
```

b) Enable PortFast on all the access ports that are in use on SW1.

```
SW1(config)#interface range fastEthernet 0/1-2
SW1(config-if-range)#spanning-tree portfast
```

c) Configure SW2 so that all access ports will use PortFast by default.

```
SW2(config)#spanning-tree portfast default
```

d) Enable BPDU Guard on all the access ports that are in use on SW1.

```
SW1(config)#interface range fastEthernet 0/1-2
SW1(config-if-range)#spanning-tree bpduguard enable
```

e) Configuring SW1 as the Primary and SW2 as the Secondary Root Bridges for VLAN 10 and 20.

```
SW1(config)# spanning-tree vlan 10 root primary
SW1(config)# spanning-tree vlan 20 root primary


SW2(config)#spanning-tree vlan 10 root secondary
SW2(config)#spanning-tree vlan 20 root secondary
```

Can verify the success of the command using:

```
SW1#show spanning-tree vlan 10-20
```