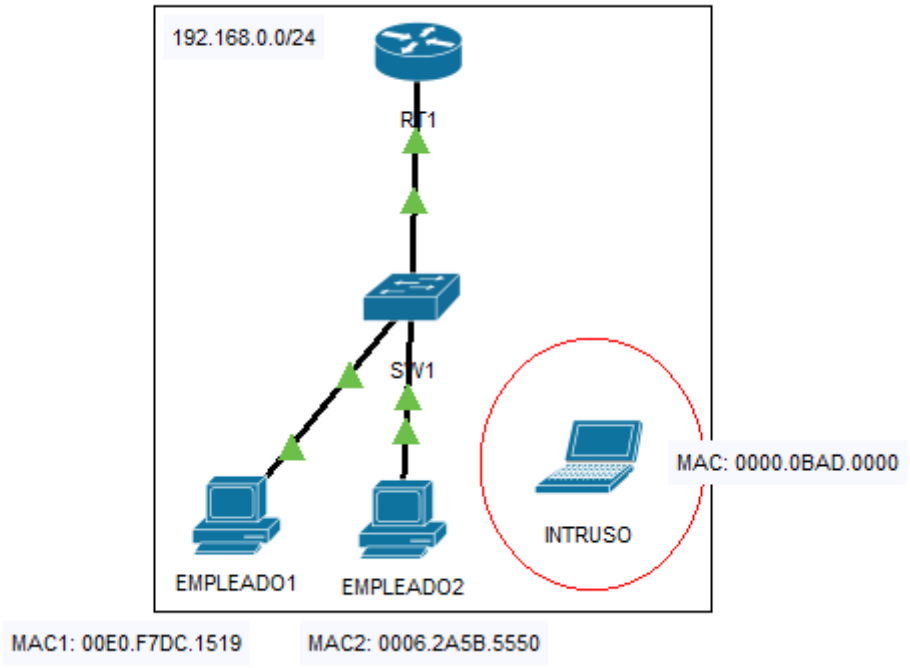
Configuración de Port Security.

"Topología de red Implementada"



Descripción: *En la siguiente imagen se muestran empleados conectados al SW1 de la VLAN 10, donde hay un intruso que ocupara el puesto del empleado 2 cuando este se vaya o se levante para realizar un ataque o espiar la red.*

¿Qué es Port Security?:

Port Security, en el contexto de redes informáticas, se refiere a una característica de seguridad que se utiliza en switches para controlar el acceso a los puertos Ethernet. Su objetivo principal es prevenir el acceso no autorizado a la red al restringir qué direcciones MAC pueden enviar o recibir tráfico a través de un puerto específico del switch. Esto ayuda a proteger la red contra ataques como el "spoofing" de direcciones MAC y evita que dispositivos no autorizados se conecten a la red.

Configuración de Port Security.

```
RT1>enable

RT1#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

RT1(config)#
```

#Crear una Sub-interfaz para que los PCs de las VLAN 10 puedan comunicarse#

```
RT1(config)#interface g0/0/0.10

RT1(config-subif)#

RT1(config-subif)#encapsulation dot1Q 10

RT1(config-subif)#ip address 192.168.0.1 255.255.255.0

RT1(config-subif)#no shutdown

RT1(config-subif)#description ENLACE HACIA RED LAN

RT1(config-subif)#exit

RT1(config)#
```

#POOL DHCP para direccionamiento IP dinámico#

```
RT1(config)#ip dhcp pool TRABAJADORES

RT1(dhcp-config)#network 192.168.0.0 255.255.255.0

RT1(dhcp-config)#default-router 192.168.0.1

RT1(dhcp-config)#dns-server 8.8.8.8

RT1(dhcp-config)#exit

RT1(config)#
```

#Crear la VLAN y poner las interfaces en modo troncal y acceso#

SW1>enable

SW1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW1(config)#

SW1(config)#**vlan 10**

SW1(config-vlan)#**name TRABAJADORES**

SW1(config-vlan)#**exit**

SW1(config)#

SW1(config)#**interface range f0/1-10**

SW1(config-if-range)#**description TRABAJADORES**

SW1(config-if-range)#**switchport mode access**

SW1(config-if-range)#**switchport access vlan 10**

SW1(config-if-range)#exit

SW1(config)#

SW1(config)#**interface g0/1**

SW1(config-if)#**switchport mode trunk**

SW1(config-if)#**description ENLACE HACIA RT1**

SW1(config-if)#exit

SW1(config)#

#Apagar interfaces que no se usaran#

SW1(config)#**interface range f0/10-24**

```
SW1(config-if-range)#shutdown


%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down

SW1(config-if-range)#exit

SW1(config)#interface g0/2

SW1(config-if)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
```

#Seguridad de puertos#

```
SW1(config)#interface range f0/1-10

SW1(config-if-range)#switchport port-security

SW1(config-if-range)#switchport port-security mac-address ?

  H.H.H   48 bit mac address

  sticky  Configure dynamic secure addresses as sticky

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

SW1(config-if-range)#switchport port-security max 1

SW1(config-if-range)#switchport port-security violation ?

  protect   Security violation protect mode

  restrict  Security violation restrict mode

  shutdown  Security violation shutdown mode

SW1(config-if-range)#switchport port-security violation shutdown

SW1(config-if-range)#exit
```

#Verificar si detecto las MAC de sus trabajadores#

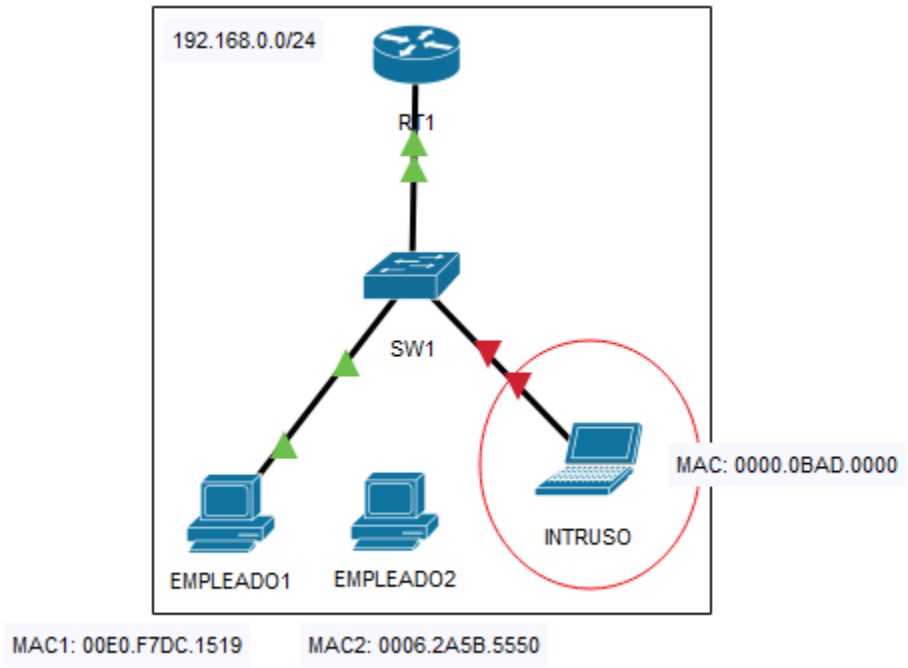
```
SW1#show port-security address
```

```
               Secure Mac Address Table

-----------------------------------------------------------------------
--------

Vlan    Mac
Address       Type                            Ports   Remaining Age

                                                                    (m
ins)

----    -----------       ----                          -----   -----
--------

  10    00E0.F7DC.1519    SecureSticky                  Fa0/1
-

  10    0006.2A5B.5550    SecureSticky                  Fa0/2
-

-----------------------------------------------------------------------
--------

Total Addresses in System (excluding one mac per port)     : 0

Max Addresses limit in System (excluding one mac per port) : 1024
```

Tabla de Direccionamiento IP

Nombre	Departamento	VLAN	IP	Red/Mask	Gateway	Interfaz	MAC
RT1	N/A	N/A	192.168.0.1	192.168.0.0/24	N/A	G0/0/0.10	N/A
SW1	TRABAJADORES	10	N/A	192.168.0.0/24	N/A	G0/0	N/A
SW1	TRABAJADORES	10	N/A	192.168.0.0/24	N/A	F0/1-10	N/A
EMPLEADO1	TRABAJADORES	10	DHCP	192.168.0.0/24	192.168.0.1	Fa0	00E0.F7DC.1519
EMPLEADO2	TRABAJADORES	10	DHCP	192.168.0.0/24	192.168.0.1	Fa0	0006.2A5B.5550
INTRUSO	N/A	N/A	DHCP	192.168.0.0/24	192.168.0.1	Fa0	0000.0BAD.0000

El EMPLEADO2 se fue a colación y rápidamente el INTRUSO aprovecha la situación para conectarse y tener acceso a la red. Vemos que no le funciono. Ya que se produjo una violación y se apagó automáticamente el puerto.



#Se observa la violación del puerto F0/2#

SW1#**show port-security**

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

Fa0/1 1 1 0 Shutdown

Fa0/2 1 1 1 Shutdown

SW1#**show port-security interface f0/2**

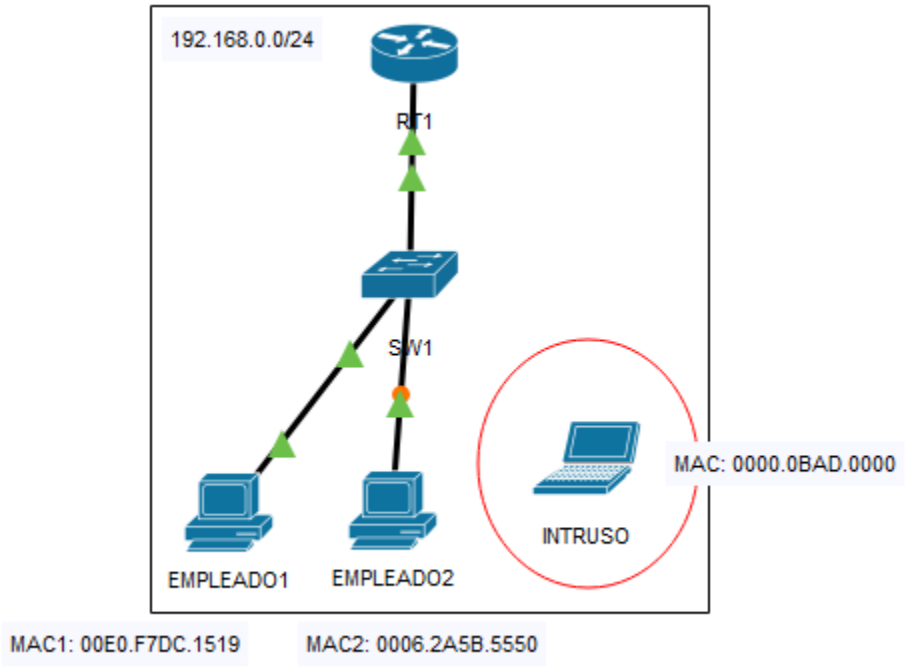
Port Security : Enabled

```
Port Status : Secure-shutdown

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 0000.0BAD.0000:10

Security Violation Count : 1
```

Ahora, el EMPLEADO2 vuelve a su lugar, conecta el cable y aún no tiene conexión a internet, Nosotros como administradores debemos levantar manualmente la interfaz F0/2 del EMPLEADO2 ya que no se levantará del SW1 hasta indicárselo.

```
SW1(config)#interface f0/2

SW1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down

SW1(config-if)#no shutdown

SW1(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
```

```
SW1(config-if)#
```



Descarga aquí la topología (Port-Security.pkt)