BASTIONADO 3

SEGURIDAD DE PUERTOS DE CAPA 2

Objetivos

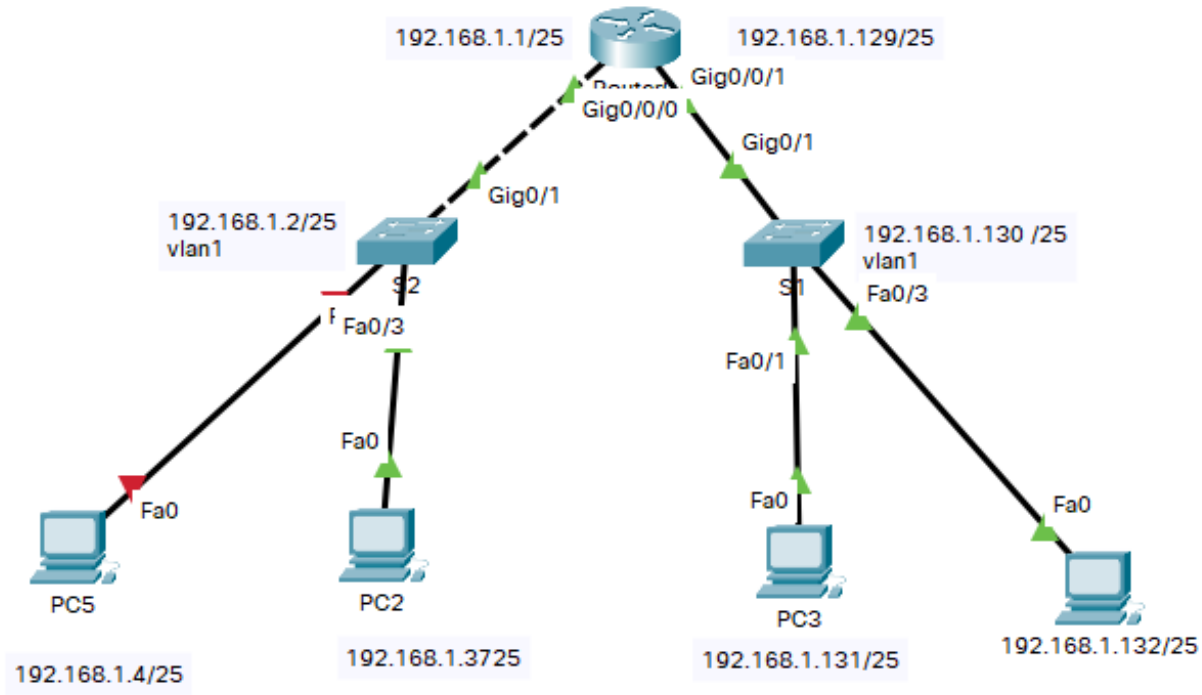
Seguir profundizando en el bastionado de redes. En esta ocasión, la seguridad que abordamos es la de los puertos de un switch.

Antecedentes/Escenario

La seguridad de puertos permite a los administradores especificar en forma estática las direcciones MAC permitidas en un puerto determinado, o permitir al switch aprender en forma dinámica un número limitado de direcciones MAC. Limitando a 1 el número de direcciones MAC permitidas en un puerto, la seguridad de puerto puede ser utilizada para controlar la falsificación de MAC y el desbordamiento de la tabla de direcciones MAC

Instrucciones

Inicio: Configure la siguiente instalación.



Verifique la configuración de:

- ☐ Crear la configuración de red y asignar IPs a los equipos
- ☐ Asignar nombre a los equipos (S1, S2, R1, etc.…)
- ☐ Configurar acceso CLI con contraseña (line console 0)
- ☐ Configurar acceso seguro EXEC privilegiado (enable password XXXXX)
- ☐ Cifrado contraseña EXEC privilegiado (MD5) (enable secret XXXX)
- ☐ Cifrado de contraseñas general (service password-encryption)
- ☐ Configuración acceso líneas virtuales VTY (line vty 0 4)
- ☐ Banner (banner motd)
- ☐ Copia de la configuración actual (copy running-config startup-config)

Parte 1: Habilite el puerto seguro

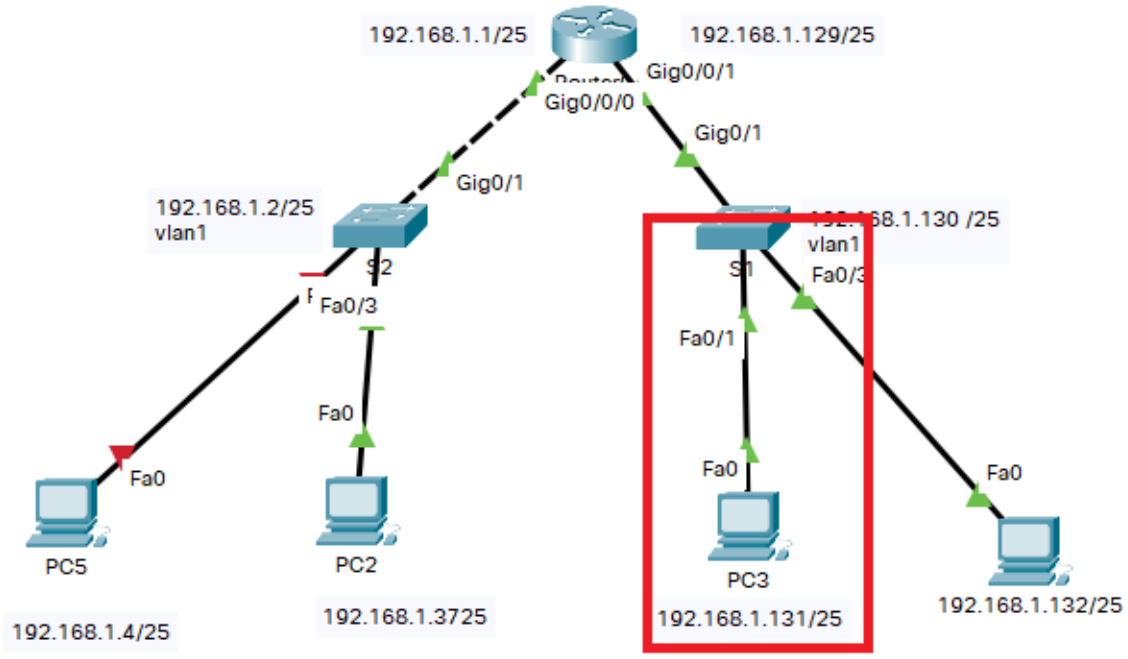
El proceso para habilitar el puerto seguro se inicia una vez que la interfaz se ha configurado como puerto de acceso:

```
S1>
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/1
S1(config-if)#switchport mode access
S1(config-if)#
```

Ahora habilite la seguridad del puerto con el comando switchport port-security

```
S1>
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-secu
S1(config-if)#switchport port-security
S1(config-if)#
```

Una vez configurado port-security se debe identificar un conjunto de direcciones MAC permitidas en ese puerto configuradas explícitamente o de forma dinámica y especificar un número máximo de direcciones MAC que serán permitidas.



En nuestra práctica vamos a configurar para que sólo PC3 acceda al puerto fa0/1

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix  :
   Physical Address.................: 00E0.F7A7.9DDC
   Link-local IPv6 Address.........: FE80::2E0:F7FF:FEA7:9DDC
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.131
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     192.168.1.129
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-95-6D-A2-79-00-E0-
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:
```

En la imagen podemos observer la dirección MAC de la tarjeta ethernet de PC3, por lo tanto procedemos a configurar S1 (fa0/1).

```
S1>
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-secu
S1(config-if)#switchport port-security
S1(config-if)#sw
S1(config-if)#switchport po
S1(config-if)#switchport port-security ma
S1(config-if)#switchport port-security mac-address
S1(config-if #switchport port-security mac-address 00E0.F7A7.9DDC
S1(config-if)#sw
S1(config-if)#switchport po
S1(config-if)#switchport port-security ma
S1(config-if)#switchport port-security max
S1(config-if)#switchport port-security maximum 1
S1(config-if)#
```

Se ha configurado para que sólo acceda esa MAC (00E0.F7A7.9DDC y solo sea 1)

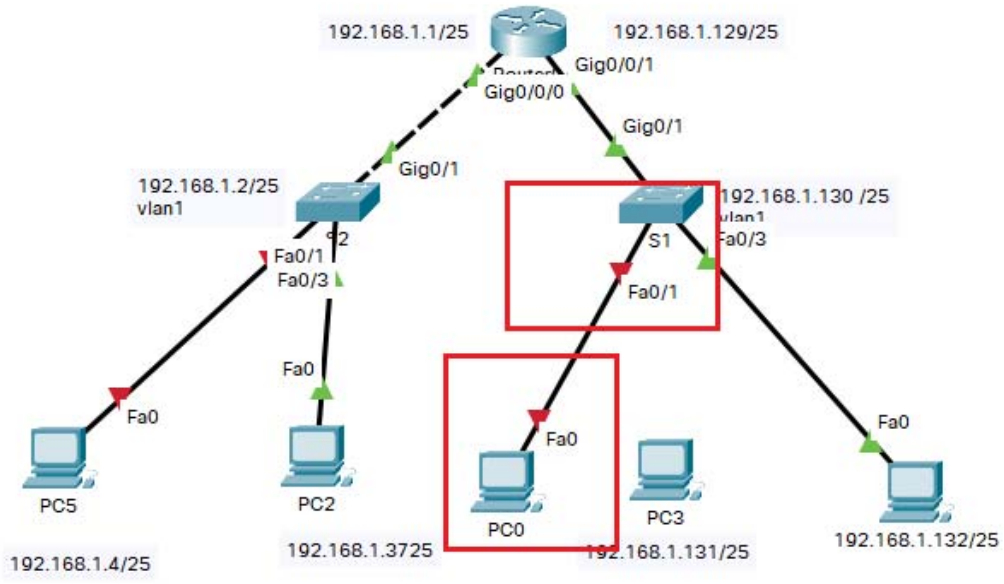
Podríamos configurar el commando ***switchport port-security mac-address sticky*** para que fuse agregando dinámicamente las direcciones MAC que se fuesen conectando al puerto hasta el máximo indicado-configurado.

Ahora nos toca definer como va a reaccionar el puerto habilitado si ocurre un intento de violación, para eso, se utiliza el siguiente commando:

S1(config-if)#switchport port-security violation shutdown

Cuando supera el número máximo de direcciones MAC permitidas o se detecta una dirección MAC desconocida, se interpretará como una violación. El Puerto del switch toma la opción shutdown, dejándolo inoperable y tendrá que ser habilitado manualmente desde el modo interfaz con los commandos de interfaz shutdown y no shutdown.

Tan solo queda ahora conectar otro PC distinto de PC3 y probar si deshabilita o no el Puerto configurado.



En la imagen puede verse que el puerto fa0/1 se ha deshabilitado automáticamente.

Si ejecuto el comando S1#show run , puedo ver la configuración del Puerto fa0/1.

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address 00E0.F7A7.9DDC
!
interface FastEthernet0/2
!
interface FastEthernet0/3
```

Ahora es tu turno y tienes que habilitar la configuración de puertos dinámica y restringida a 1 PC en ambos switches. Prueba a conectar un PC diferente y verifica que los puertos se desconectan y dejan de dar servicio.

[1]

[1] Todos los comandos port-security pueden eliminarse anteponiendo un no al propio comando.