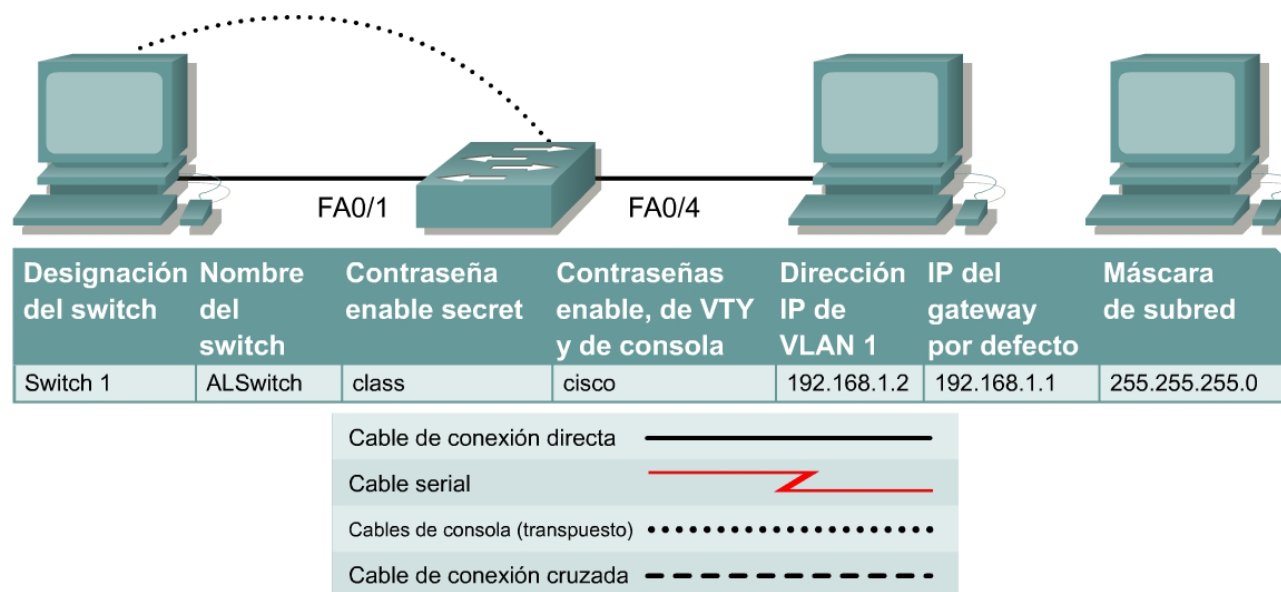


## Práctica de laboratorio 6.2.5 Configuración de la seguridad de puerto



### Objetivo

- Crear y verificar una configuración de switch básica.
- Configurar la seguridad de puerto en los puertos FastEthernet individuales.

### Información básica / Preparación

Cree una red con un cableado similar al del diagrama. El resultado de la configuración que se utiliza en esta práctica de laboratorio se obtiene con un switch serie 2950. El uso de cualquier otro switch puede producir resultados distintos. Realice los siguientes pasos en cada switch a menos que se le indique específicamente lo contrario. También se proporcionan instrucciones para los switch Serie 1900, que inicialmente muestra un Menú de interfaz de usuario. Seleccione la opción “Línea de comandos” del menú para realizar los pasos para esta práctica de laboratorio.

Inicie una sesión de HyperTerminal.

**Nota:** Vaya a las instrucciones de borrar y recargar al final de esta práctica de laboratorio. Realice ese procedimiento en todos los switch que se utilizarán en esta práctica antes de continuar.

### Paso 1 Configurar el switch

Configure el nombre de host, las contraseñas de acceso y modo de comando, así como también los parámetros de administración de la LAN. Estos valores se muestran en la tabla. Si se producen problemas al realizar esta configuración, consulte la Práctica de Laboratorio Configuración básica del switch.

### Paso 2 Configurar los hosts conectados al switch

- Configure los hosts para que utilicen la misma subred IP para la dirección, máscara y gateway por defecto que el switch.

- b. Hace falta un tercer host para esta práctica de laboratorio. Se debe configurar con la dirección 192.168.1.7. La máscara de subred es 255.255.255.0 y el gateway por defecto es 192.168.1.1.

**Nota:** No conecte aún este PC al switch.

### Paso 3 Verificar la conectividad

- a. Para verificar que los hosts y el switch estén configurados correctamente, haga ping a la dirección IP del switch desde los hosts.
- b. ¿Fueron exitosos los pings? \_\_\_\_\_
- c. Si la respuesta es no, realice el diagnóstico de fallas en la configuración de los hosts y del switch.

### Paso 4 Anotar las direcciones MAC del host

- a. Determine y anote las direcciones de capa 2 de las tarjetas de interfaz de red del PC.  
En Windows 98, verifique con **Inicio > Ejecutar > winipcfg**. Haga clic en **More info** (más información).
- b. PC1 \_\_\_\_\_
- c. PC2 \_\_\_\_\_

### Paso 5 Determinar las direcciones MAC que el switch ha aprendido

- a. Determine cuáles son las direcciones MAC que el switch ha aprendido por medio del comando **show mac-address-table** en el indicador del modo exec privilegiado, como se indica a continuación:  
  

```
ALSwitch#show mac-address-table
```
- b. ¿Cuántas direcciones dinámicas hay? \_\_\_\_\_
- c. ¿Cuántas direcciones MAC hay en total? \_\_\_\_\_
- d. ¿Las direcciones MAC concuerdan con las direcciones MAC del host?  
\_\_\_\_\_

### Paso 6 Determinar las opciones show MAC table

- a. Introduzca el siguiente comando para determinar las opciones disponibles para el comando **mac-address-table** use la opción **?** como se indica a continuación:  
  

```
ALSwitch(config)#mac-address-table ?
```

### Paso 7 Configurar una dirección MAC estática

Configure una dirección MAC estática en la interfaz FastEthernet 0/4 como se indica a continuación:

**Nota:** Use la dirección que se ha registrado para PC4 en el Paso 4. La dirección MAC 00e0.2917.1884 se usa en la sentencia del ejemplo solamente.

```
ALSwitch(config)#mac-address-table static 00e0.2917.1884 interface  
fastethernet 0/4 vlan 1
```

2900:

```
ALSwitch(config)#mac-address-table static 00e0.2917.1884 fastethernet 0/4 vlan 1
```

1900:

```
ALSwitch(config)#mac-address-table permanent 00e0.2917.1884 ethernet 0/4
```

## Paso 8 Verificar los resultados

- a. Introduzca lo siguiente para verificar las entradas de la tabla de direcciones MAC.

```
ALSwitch#show mac-address-table
```

- b. ¿Cuántas direcciones MAC hay en total ahora? \_\_\_\_\_

## Paso 9 Anotar las opciones de seguridad de puerto

- a. Determine cuáles son las opciones para configurar la seguridad de puerto en la interfaz FastEthernet 0/4.

1900:

```
ALSwitch(config)#interface ethernet 0/4
ALSwitch(config-if)#port secure ?
max-mac-count    Maximum number of addresses allowed on the port
<cr>
```

2950:

```
ALSwitch(config-if)#switchport port-security ?
aging            Port-security aging commands
mac-address      Secure mac address
maximum          Max secure addrs
violation        Security Violation Mode
<cr>
```

- b. Para permitir que el puerto de switch FastEthernet 0/4 acepte sólo un dispositivo, introduzca **port security** como se indica a continuación:

```
ALSwitch(config-if)#switchport mode access
ALSwitch(config-if)#switchport port-security
ALSwitch(config-if)#switchport port-security mac-address sticky
```

1900:

```
ALSwitch(config-if)#port secure
```

## Paso 10 Verificar los resultados

- a. Introduzca el siguiente comando para verificar las entradas de la tabla mac-address table.

```
ALSwitch#show mac-address-table
```

- b. ¿Cómo se enumeran los tipos de direcciones de las dos direcciones MAC?

\_\_\_\_\_

- c. Muestre los valores de seguridad de puerto.

```
ALSwitch#show port-security
```

1900:

```
ALSwitch#show mac-address-table security
```

### Paso 11 Mostrar el archivo de configuración activa

- a. ¿Hay sentencias que reflejan directamente la implementación de seguridad en el listado de la configuración activa?
- 

- b. ¿Qué significan esas sentencias?
- 

### Paso 12 Limitar la cantidad de hosts por puerto

- a. En la interfaz FastEthernet 0/4, configure en 1 el número máximo de MAC para la seguridad de puerto, como se indica a continuación:

1900:

```
ALSwitch(config)#interface Ethernet 0/4
ALSwitch(config-if)#port secure max-mac-count 1
```

2950:

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

- b. Desconecte el PC que está conectado a FastEthernet 0/4. Conéctelo al puerto del PC al que se le ha asignado la dirección IP 192.168.1.7. Este PC aún no se ha conectado al switch. Es posible que sea necesario hacer ping a la dirección 192.168.1.2 del switch para generar tráfico.
- c. Anote cualquier observación.
- 

### Paso 13 Configurar el puerto para que se desconecte si se produce una violación de seguridad

- a. Se ha decidido que, en caso de que se produzca una violación de seguridad, la interfaz se debe desactivar. Introduzca el siguiente comando para hacer que la acción de seguridad sea la desactivación:

```
ALSwitch(config-if)#switchport port-security violation shutdown
```

2900XL:

```
ALSwitch(config-if)#port security action shutdown
```

1900:

La acción por defecto ante una violación de dirección es "suspender".

- b. ¿Qué otras opciones de acción hay disponibles para la seguridad de puerto?
- 

- c. Si es necesario, haga ping a la dirección de switch 192.168.1.2 desde el PC 192.168.1.7. Ahora el PC está conectado a la interfaz FastEthernet 0/4. Esto garantiza que hay tráfico desde el PC hacia el switch.

- d. Anote cualquier observación.

---

---

### Paso 14 Mostrar la información de configuración del puerto 0/4

- a. Para ver la información de configuración del puerto FastEthernet 0/4 solamente, escriba **show interface fastethernet 0/4**, como se indica a continuación, en el indicador del modo EXEC privilegiado:

```
ALSwitch#show interface fastethernet 0/4
```

```
1900:
```

```
ALSwitch#show interface ethernet 0/4
```

- b. ¿Cuál es el estado de esta interfaz?

FastEthernet0/4 es \_\_\_\_\_, protocolo de línea es \_\_\_\_\_

```
1900:
```

```
ALSwitch#show interface ethernet 0/4
```

- c. ¿Cuál es el estado de esta interfaz?

Ethernet 0/4 es \_\_\_\_\_, protocolo de línea es \_\_\_\_\_

### Paso 15 Reactivar el puerto

- a. Si se produce una violación de seguridad y el puerto se desconecta, use el comando **no shutdown** para reactivarlo.
- b. Practique la reactivación de este puerto algunas veces cambiando el puerto de host 0/4 original por el nuevo puerto de host. Vuelva a conectar el host original, escriba el comando **no shutdown** en la interfaz y haga ping on la ventana de símbolo del sistema. El **ping** debe repetirse varias veces o se puede usar el comando **ping 192.168.1.2 -n 200**. Esto establecerá la cantidad de paquetes de ping en 200 en lugar de 4. Luego, cambie los hosts e intente de nuevo.

### Paso 16 Salir del switch

Escriba **exit** para salir de la pantalla de bienvenida del switch:

```
Switch#exit
```

Al completar estos pasos, termine la sesión escribiendo **exit** y apague todos los dispositivos. Entonces, quite y guarde los cables y el adaptador.

## Borrar y recargar el switch

En la mayoría de las prácticas de laboratorio del CCNA 3 y CCNA 4, es necesario comenzar con un switch que no está configurado. El uso de un switch que cuente con una configuración existente puede provocar resultados impredecibles. Estas instrucciones permiten preparar el switch antes de realizar la práctica de laboratorio de modo que las opciones de configuración anteriores no interfieran con el mismo. El siguiente procedimiento se utiliza para borrar las configuraciones anteriores y comenzar con un switch sin configurar. Se proporcionan instrucciones para los switch de las Series 2900, 2950 y 1900.

### Switch de las series 2900 y 2950

1. Entre al modo EXEC privilegiado escribiendo **enable**.

Si se le pide una contraseña, introduzca **class** (si no funciona, consulte al instructor).

```
Switch>enable
```

2. Elimine el archivo de información de la base de datos de la VLAN.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]? [Enter]  
Delete flash:vlan.dat? [confirm] [Intro]
```

Si no hay ningún archivo VLAN, aparece el siguiente mensaje:

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Elimine el archivo de configuración inicial de la NVRAM del switch.

```
Switch#erase startup-config
```

Como respuesta, aparecerá la siguiente petición de entrada:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Presione **Intro** para confirmar.

La respuesta deberá ser:

```
Erase of nvram: complete
```

4. Verifique que se haya eliminado la información de la VLAN.

Verifique que la configuración de la VLAN se haya eliminado en el Paso 2 mediante el comando **show vlan**. Si la información de configuración de VLAN anterior (que no sea la VLAN 1 de administración por defecto) aún permanece, será necesario apagar y encender el switch (reiniciar el hardware) en lugar de ejecutar el comando **reload**. Para apagar y encender el switch, retire el cable de alimentación de la parte posterior del switch o desenchúfelo. Luego, conéctelo nuevamente.

Si la información de la VLAN se ha eliminado con éxito en el Paso 2, vaya al Paso 5 y reinicie el switch por medio del comando **reload**.

5. Reinicie el software (por medio del comando **reload**)

**Nota:** No es necesario realizar este paso si el switch se ha reiniciado apagándolo y encendiéndolo.

- a. En el modo EXEC privilegiado, introduzca el comando **reload**.

```
Switch#reload
```

Como respuesta, aparecerá la siguiente petición de entrada:

```
System configuration has been modified. Save? [yes/no] :
```

- b. Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:

```
Proceed with reload? [confirm] [Intro]
```

La primera línea de la respuesta será:

```
Reload requested by console.
```

La siguiente petición de entrada aparecerá después de que el switch se recargue:

```
Would you like to enter the initial configuration dialog? [yes/no] :
```

- c. Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:

```
Press RETURN to get started! [Intro]
```

### Switch serie 1900

1. Elimine la información de protocolo de agregación de enlaces virtual de la VLAN (VTP).

```
#delete vtp
```

```
This command resets the switch with VTP parameters set to factory defaults.
```

```
All other parameters will be unchanged.
```

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Introduzca **y** y presione **Intro**.

2. Elimine la configuración inicial de la NVRAM del switch.

```
#delete nvram
```

Este comando reinicia el switch con los valores preconfigurados de fábrica. Todos los parámetros del sistema se establecen en los valores preconfigurados de fábrica. Se eliminan todas las direcciones estáticas y dinámicas.

Reset system with factory defaults, [**Y**]es or [**N**]o?

Introduzca **y** y presione **Intro**.