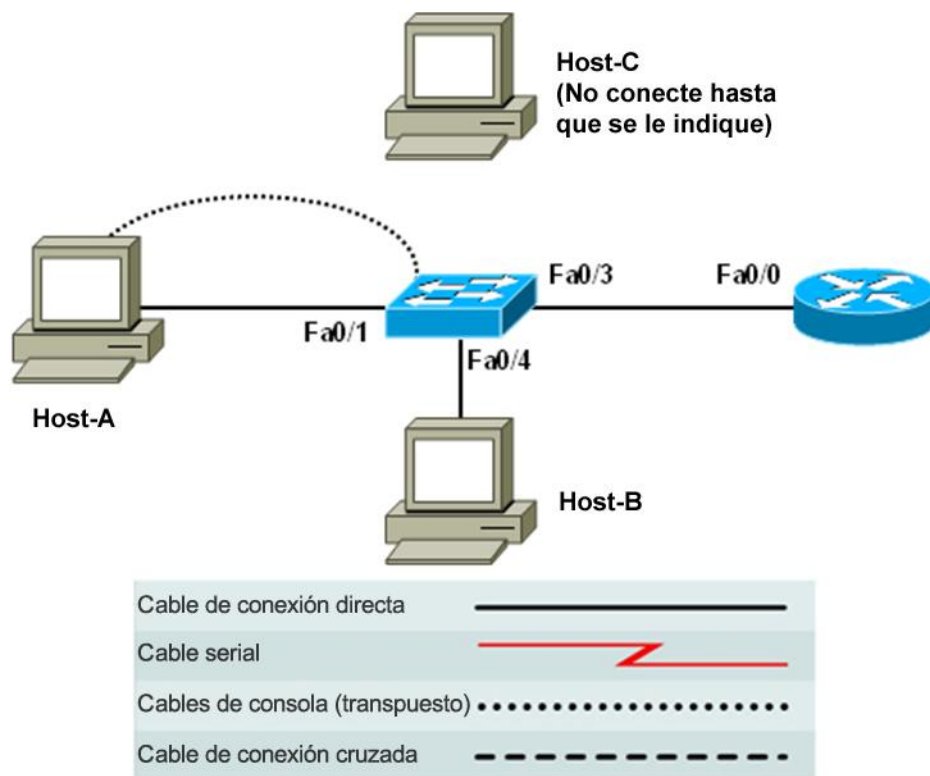


## Práctica de laboratorio 5.5.4 Configuración del switch Cisco 2960



Dispositivo	Nombre de Host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	Puerto del switch
S1	CustomerSwitch	VLAN 1	192.168.1.5	255.255.255.0	192.168.1.1	N/C
R1	CustomerRouter	Fa0/1	192.168.1.1	255.255.255.0	N/C	Fa0/5
H1	H1	NIC	192.168.1.2	255.255.255.0	192.168.1.1	Fa0/11
H2	H2	NIC	192.168.1.4	255.255.255.0	192.168.1.1	Fa0/18
H3	H3	NIC	192.168.1.6	255.255.255.0	192.168.1.1	Ninguno

### Objetivos

- Configurar los parámetros globales iniciales del switch.
- Configurar las PC hosts y conectarlas al switch.
- Configurar un router y conectarlo al switch.
- Configurar una dirección IP para la VLAN de administración de switches.
- Verificar la conectividad de la red.
- Configurar la seguridad básica de los puertos.
- Configurar los parámetros de velocidad y de dúplex de los puertos.

## Información básica / Preparación

En esta práctica de laboratorio, debe conectar varios hosts y un router al switch y probar la conectividad. También debe establecer las configuraciones de velocidad, de seguridad y de dúplex para un puerto del switch. Esta práctica de laboratorio describe la configuración básica del switch Cisco 2960 mediante los comandos de Cisco IOS. El switch Cisco Catalyst 2960 ya está configurado de fábrica y sólo es necesario asignarle información de seguridad básica antes de conectarlo a una red. Para usar Telnet o un producto de administración basado en IP con un switch Cisco, debe configurar una dirección IP de administración. Se debe configurar la VLAN 1 para que proporcione acceso IP a las funciones de administración. La información de esta práctica de laboratorio concierne también a otros switches; sin embargo, la sintaxis de los comandos puede variar.

## Recursos necesarios

Se necesitan los siguientes recursos:

- Un switch Cisco 2960 o similar.
- Un router con interfaz Ethernet para conectarse al switch.
- Tres PC con Windows, cada una con un programa de emulación de terminal.
- Un cable conector de consola de RJ-45 a DB-9.
- Tres cables de conexión directa Ethernet.
- Acceso a la pantalla Command prompt (Símbolo del sistema) de la PC.
- Acceso a la configuración TCP/IP de red de la PC.

**Nota:** antes de continuar, siga las instrucciones en la sección “Borrar y recargar el switch” al final de esta práctica de laboratorio.

## Paso 1: Conectar el host con el switch y configurarlos

- a. Conecte el host H1 al puerto Fa0/11 del switch S1 con la interfaz Fast Ethernet y conecte el host H2 al puerto Fa0/18. Configure los hosts para que utilicen la misma subred IP para la dirección y la máscara que utiliza el switch, como se muestra en la tabla y en el diagrama de topología anterior.
- b. Todavía *no* conecte el host H3 al switch.

## Paso 2: Conectar el router con el switch y configurar el router

**Nota: si es necesario, consulte** la práctica de laboratorio 5.3.5, “Configuración de parámetros básicos del router con la CLI de Cisco IOS” para leer las instrucciones de configuración del nombre del host, las contraseñas y las direcciones de interfaces.

- a. Conecte el router al puerto Fa0/5 del switch.
- b. Configure el router con el nombre del host como **CustomerRouter**.
- c. Configure el acceso y la contraseña de consola, el acceso y la contraseña de VTY, y la contraseña secreta de enable.
- d. Configure la interfaz Fa0/1 del router como se muestra en la tabla de tipología.

### Paso 3: Configurar el switch

- a. Configure el switch con el nombre del host como CustomerSwitch.  

```
Switch>enable
Switch#config terminal
Switch(config)#hostname CustomerSwitch
```
- b. Establezca la contraseña del modo EXEC privilegiado como **cisco**.  

```
CustomerSwitch(config)#enable password cisco
```
- c. Establezca la contraseña secreta del modo EXEC privilegiado como **cisco123**.  

```
CustomerSwitch(config)#enable secret cisco123
```
- d. Establezca la contraseña de la consola como **cisco123**.  

```
CustomerSwitch(config)#line console 0
CustomerSwitch(config-line)#password cisco123
```
- e. Configure la línea de consola para que solicite una contraseña en el inicio de sesión.  

```
CustomerSwitch(config-line)#login
```
- f. Establezca la contraseña de VTY como **cisco123**.  

```
CustomerSwitch(config-line)#line vty 0 15
CustomerSwitch(config-line)#password cisco123
```
- g. Configure la VTY para que solicite una contraseña en el inicio de sesión.  

```
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#end
```

### Paso 4: Configurar la interfaz de administración en la VLAN 1

- a. Ingrese al modo de configuración global. Recuerde utilizar la contraseña nueva.  

```
CustomerSwitch>enable
CustomerSwitch#configure terminal
```
- b. Ingrese al modo de configuración de la interfaz para la VLAN 1:  

```
CustomerSwitch(config)#interface vlan 1
```
- c. Establezca la dirección IP, la máscara de subred y el gateway predeterminado para la interfaz de administración. La dirección IP debe ser válida para la red local donde se instala el switch.  

```
CustomerSwitch(config-if)#ip address 192.168.1.5 255.255.255.0
CustomerSwitch(config-if)#exit
CustomerSwitch(config)#ip default-gateway 192.168.1.1
CustomerSwitch(config)#end
```

### Paso 5: Verificar la configuración del switch

- a. Verifique que la dirección IP de la interfaz de administración en la VLAN 1 del switch y la dirección IP del host H1 se encuentren en la misma red local. Utilice el comando **show running-config** para verificar la configuración de la dirección IP del switch.  

```
CustomerSwitch#show running-configuration
Building configuration...

Current configuration : 1283 bytes
!
version 12,2
```

```
no service pad
hostname CustomerSwitch
!
enable secret 5 $1$XUe/$ch4WQ/SpcFCDd2iqd9bda/
enable password cisco
!
interface FastEthernet0/1
!
!
interface FastEthernet0/24
!
interface Vlan1
ip address 192.168.1.5 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
!
line con 0
password cisco123
login
line vty 0 4
password cisco123
login
line vty 5 15
password cisco123
login
!
end
```

- b. Guarde la configuración.

```
CustomerSwitch#copy running-config startup-config
```

### Paso 6: Verificar la conectividad mediante Telnet y el comando ping

- Para verificar que el switch y el router estén configurados correctamente, haga ping en la dirección IP de la interfaz Fa0/1 del router (gateway predeterminado) desde la CLI del switch.
- ¿Los pings funcionan correctamente? \_\_\_\_\_ .
- Para verificar que los hosts y el switch estén configurados correctamente, haga ping a la dirección IP del switch desde el host H1.
- ¿Los pings funcionan correctamente? \_\_\_\_\_ .
- Si el ping no funciona correctamente, verifique nuevamente las conexiones y las configuraciones. Verifique que todos los cables sean correctos y que las conexiones estén colocadas correctamente. Verifique las configuraciones del router, del switch y del host.
- Abra el intérprete de comandos en el host H1 e inicie una sesión en Telnet con la dirección IP asignada a la VLAN 1 de administración del switch.
- Escriba la contraseña de VTY configurada en el Paso 3. ¿Cuál es el resultado? \_\_\_\_\_

En el intérprete de comandos del switch, ejecute el comando **show version**.

```
CustomerSwitch>show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(0.0.16)FX, CISCO
DEVELOPMENT TEST VERSION
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Compiled Tue 17-May-05 01:43 by yenanh

ROM: Bootstrap program is C2960 boot loader  
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M), Version 12.2 [lqian-flo\_pilsner 100]

Switch uptime is 3 days, 20 hours, 8 minutes  
System returned to ROM by power-on  
System image file is "flash:c2960-lanbase-mz.122-0.0.16.FX.bin"

cisco WS-C2960-24TC-L (PowerPC405) processor with 61440K/4088K bytes of memory.

Processor board ID FHH0916001J

Last reset from power-on

Target IOS Version 12.2(25)FX

1 Virtual Ethernet interface

24 FastEthernet interfaces

2 Gigabit Ethernet interfaces

The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address : 00:0B:FC:FF:E8:80

Motherboard assembly number : 73-9832-02

Motherboard serial number : FHH0916001J

Motherboard revision number : 01

System serial number : FHH0916001J

Hardware Board Revision Number : 0x01

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
* 1	26	WS-C2960-24TC-L	12.2(0.0.16)FX	C2960-
LANBASE-M				

Configuration register is 0xF

- h. ¿Cuál es la versión de Cisco IOS de este switch? \_\_\_\_\_ .
- i. Escriba **quit** en el intérprete de comandos del switch para finalizar la sesión en Telnet.

## Paso 7: Determinar qué direcciones MAC adquirió el switch

- a. En la pantalla Command prompt (Símbolo del sistema) de Windows, obtenga las direcciones de Capa 2 de la tarjeta de interfaz de red de la PC para cada host, mediante el comando **ipconfig /all**.

Host H1: \_\_\_\_\_ .

Host H2: \_\_\_\_\_ .

Host H3: \_\_\_\_\_ .

- b. Determine cuáles son las direcciones MAC que obtuvo el switch por medio del comando **show mac-address-table** en el intérprete de comandos del modo EXEC privilegiado.

CustomerSwitch#**show mac-address-table**

Mac Address Table

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
All	000b.be7f.ed40	STATIC	CPU
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU

```

All      0100.0cdd.dddd      STATIC      CPU
 1      000b.db04.a5cd      DYNAMIC      Fa0/5
 1      000c.3076.8380      DYNAMIC      Fa0/11
 1      000d.1496.36ad      DYNAMIC      Fa0/18
Total Mac Addresses for this criterion: 7

```

- c. ¿Cuántas direcciones dinámicas figuran? \_\_\_\_\_ .
- d. ¿Las direcciones MAC concuerdan con las direcciones MAC del host? \_\_\_\_\_ .
- e. Revise las opciones del comando **mac-address-table** mediante la herramienta de ayuda ?.

```

CustomerSwitch(config)#mac-address-table ?
address          address keyword
aging-time       aging-time keyword
count           count keyword
dynamic          dynamic entry type
interface        interface keyword
multicast        multicast info for selected wildcard
notification     MAC notification parameters and history table
static           static entry type
vlan             VLAN keyword
|               Output modifiers
<cr>

```

- f. Configure una dirección MAC estática en la interfaz Fast Ethernet 0/18. Utilice la dirección que registró para H1 en el Paso 7. La dirección MAC XXXX.YYYY.ZZZZ se usa solamente en este ejemplo.

```

CustomerSwitch(config)#mac-address-table static XXXX.YYYY.ZZZZ interface
fastethernet 0/18 vlan 1

```

- g. Verifique las entradas de la tabla de direcciones MAC.

```

CustomerSwitch#show mac-address-table
      Mac Address Table
-----

```

Vlan	Mac Address	Type	Ports
All	000b.be7f.ed40	STATIC	CPU
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0100.0cdd.dddd	STATIC	CPU
1	000b.db04.a5cd	DYNAMIC	Fa0/5
1	000c.3076.8380	DYNAMIC	Fa0/11
1	000d.1496.36ad	STATIC	Fa0/18

- h. ¿Cuántas direcciones MAC hay en este momento? \_\_\_\_\_ .
- i. ¿Qué tipo de direcciones son? \_\_\_\_\_

## Paso 8: Configurar la seguridad básica de los puertos

- a. Determine las opciones para configurar la seguridad de los puertos en la interfaz Fast Ethernet 0/4.

```

CustomerSwitch#configure terminal
CustomerSwitch(config)#interface fastEthernet 0/18
CustomerSwitch(config-if)#switchport port-security ?
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addrs

```

```
violation Security Violation Mode
```

- b. Para permitir que la interfaz FastEthernet 0/4 del puerto del switch acepte sólo un dispositivo, configure la seguridad de puerto.

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

- c. Verifique los parámetros de la seguridad de puerto.

```
CustomerSwitch#show port-security
Secure Port    MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)         (Count)          (Count)
-----
Fa0/18         1              0              0              Shutdown
-----
```

- d. ¿Qué acción de seguridad realiza el puerto Fa0/18 si existe una violación a la seguridad?

\_\_\_\_\_ .

- e. ¿Cuál es el número máximo de direcciones seguras? \_\_\_\_\_ .

- f. Visualice la configuración en ejecución.

**Nota:** algunos resultados se omiten en la siguiente visualización.

```
CustomerSwitch#show running-config
Building configuration...
Current configuration : 1452 bytes
version 12,2
hostname CustomerSwitch
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/18
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
!
interface FastEthernet0/5
!

mac-address-table static 000b.db04.a5cd vlan 1 interface
FastEthernet0/18
!
end
```

- g. ¿Existen extractos que reflejen directamente la implementación de seguridad en la lista de la configuración en ejecución?

\_\_\_\_\_

### Paso 9: Conectar otra PC al puerto seguro del switch

- Si no cuenta con otra PC disponible (H3) o no puede desconectar la PC, siga con el Paso 9 (opcional).
- Desconecte el host H2 de la interfaz Fast Ethernet 0/18 y conecte el host H3 al puerto. El host H3 aún no se conectó al switch. Desde H3, haga ping en la dirección 192.168.1.5 del switch para generar algo de tráfico.
- Registre cualquier observación en la PC y en la sesión de la terminal del switch.

---

```
01:11:12: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting
Fa0/18 in err-disable state
01:11:12: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, cause
d by MAC address 000c.3076.8380 on port FastEthernet0/18.
01:11:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, chang
ed state to down
01:11:14: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

- Observe sólo la información de configuración del puerto 0/18 de la interfaz Fast Ethernet.

```
CustomerSwitch#show interface fastethernet 0/18
```

- ¿Cuál es el estado de esta interfaz?

La interfaz Fast Ethernet 0/18 está \_\_\_\_\_ y el protocolo de la línea está \_\_\_\_\_.

### Paso 9 alternativo (opcional):

Si no cuenta con una tercera PC (host H3), está trabajando con una configuración remota de la práctica de laboratorio y no puede desconectar H2 de manera física, puede utilizar el siguiente procedimiento para cambiar la dirección MAC de H2. Este procedimiento funciona para una amplia variedad de NIC.

- Seleccione la opción **Start > Settings > Control Panel** (Inicio > Configuración > Panel de control) y haga doble clic en **Network Connections** (Conexiones de Red).
- Haga clic derecho en la NIC para la que desea cambiar la dirección MAC. Luego, seleccione **Properties** (Propiedades).
- En la ficha **General**, haga clic en el botón **Configure** (Configurar).
- En la ficha **Advanced** (Opciones avanzadas), en la sección **Property** (Propiedades), haga clic en **Network Address or Locally Administered Address** (Dirección de red o dirección administrada localmente).
- En la parte derecha, en **Values** (Valores), escriba la nueva dirección MAC. Utilice la dirección MAC original, pero cambie sólo el último valor. Por ejemplo, si la dirección MAC original es 000C29C1510A, cámbiela a 000C29C1510B.
- Escriba **c:\>ipconfig /all** para verificar los cambios.
- Desde H2, haga ping en la dirección 192.168.1.5 de la VLAN 1 del switch.

```
c:\>ping 192.168.1.5
```



- h. Registre cualquier observación en la PC y en la sesión de la terminal del switch.

```
01:11:12: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting
Fa0/18 in err-disable state
01:11:12: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, cause
d by MAC address 000c.3076.8380 on port FastEthernet0/18.
01:11:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, chang
ed state to down
01:11:14: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

- i. Observe sólo la información de configuración del puerto 0/18 de la interfaz Fast Ethernet.

```
CustomerSwitch#show interface fastethernet 0/18
```

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

La interfaz Fast Ethernet 0/18 está \_\_\_\_\_ y el protocolo de la línea está \_\_\_\_\_

### Paso 10: Reactivar el puerto

- a. Limpie la entrada de la dirección sin modificación para el puerto Fa0/18 con el comando **clear port-security**.

```
S1#clear port-security sticky interface fa0/18 access
```

- b. Para cambiar el estado de la interfaz de error disable a administratively up, ejecute el comando **shutdown** y luego el comando **no shutdown**.

```
S1(config)#interface fa0/18
S1(config-if)#shutdown
S1(config-if)#no shutdown
```

- c. Escriba el host original o restablezca la dirección MAC a su valor original. Haga ping desde la pantalla del intérprete de comandos. Puede hacer ping varias veces o utilizar el comando **ping 192.168.1.5 -n 100**, que establece la cantidad de paquetes de ping en 100, en lugar de 4.

### Paso 11: Configurar las opciones de duplex y de velocidad para los puertos

- a. Cambie los parámetros predeterminados de los puertos a **auto-duplex** y **auto-speed**. Si una computadora con una NIC de 100 Mbps está conectada al puerto, automáticamente cambia al modo full-duplex de 100 Mbps. Si un hub está conectado al puerto del switch, generalmente cambia al modo half-duplex con 10 Mbps.
- b. Ejecute el comando **show interfaces** para ver los parámetros de los puertos Fa0/5, Fa0/11 y Fa0/18. Este comando genera una gran cantidad de resultados. Presione la barra espaciadora hasta que pueda ver toda la información de estos puertos. ¿Cuáles son los parámetros de duplex y de velocidad para estos puertos?

Port Fa0/5 \_\_\_\_\_ .

Port Fa0/11 \_\_\_\_\_ .

Port Fa0/18 \_\_\_\_\_ .

- c. A veces es necesario establecer la velocidad y el duplex de un puerto para asegurarse de que funcione de una manera determinada. Puede establecer la velocidad y el duplex con los comandos **duplex** y **speed** mientras se encuentra en el modo de configuración de la interfaz. Para que el puerto 5 de FastEthernet funcione en half duplex y con 10 Mbps, ejecute los siguientes comandos:

```
CustomerSwitch>enable
CustomerSwitch#Config Terminal
CustomerSwitch(config-if)#interface fastEthernet 0/10
```

```
CustomerSwitch(config-if)#speed 10  
CustomerSwitch(config-if)#duplex half  
CustomerSwitch(config-if)#end  
CustomerSwitch#
```

- d. Ejecute el comando **show interfaces** nuevamente. ¿Cuál es el parámetro actual de duplex y de velocidad para Fa0/5? \_\_\_\_\_ .

### Paso 12: Salir del switch

- a. Escriba **exit** para salir del switch y volver a la pantalla de bienvenida.

```
Switch#exit
```

- b. Una vez que completó todos los pasos, apague todos los dispositivos. Retire y guarde los cables y el adaptador.

### Paso 13: Reflexión

- a. ¿Qué contraseña debe escribir para pasar del modo de usuario al modo EXEC privilegiado en el switch Cisco? ¿Por qué?

\_\_\_\_\_  
\_\_\_\_\_

- b. ¿Qué símbolo se utiliza para mostrar que se ha logrado hacer ping en el software Cisco IOS?

\_\_\_\_\_

- c. ¿Cuál es el beneficio de utilizar la seguridad del puerto?

\_\_\_\_\_  
\_\_\_\_\_

- d. ¿Qué otras medidas de seguridad relacionadas con el puerto se pueden implementar para mejorar la seguridad del switch aún más?

\_\_\_\_\_  
\_\_\_\_\_

## Borrar y recargar el switch

En la mayoría de las prácticas de laboratorio de CCNA Discovery, es necesario comenzar con un switch que no esté configurado. El uso de un switch con una configuración existente puede provocar resultados inesperados. Las siguientes instrucciones permiten preparar el switch antes de realizar la práctica de laboratorio, para que no interfieran las opciones de configuración previas. Se suministran instrucciones para los switches de las Series 2900 y 2950.

- a. Escriba el comando **enable** para ingresar al modo EXEC privilegiado. Si se le solicita una contraseña, escriba **class** (si no funciona, consulte con el instructor).

```
Switch>enable
```

- b. Elimine el archivo de información de la base de datos de la VLAN.

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

Si no hay ningún archivo de VLAN, se puede ver el siguiente mensaje:

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

- c. Elimine el archivo de configuración de inicio del switch de la NVRAM.

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

La respuesta a la línea de comandos es:

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

Presione **Enter** (Intro) para confirmar.

La respuesta debe ser:

```
Erase of nvram: complete
```

- d. Utilizando el comando **show vlan**, verifique que la información de la VLAN se haya eliminado en el Paso b. Si se eliminó la información de la VLAN, vaya al Paso e y reinicie el switch por medio del comando **reload**.

Si la información de la configuración anterior de la VLAN (aparte de la administración predeterminada de la VLAN 1) sigue presente, debe reiniciar el switch (reiniciar el hardware) en lugar de ejecutar el comando **reload**. Para reiniciar el switch, retire el cable de alimentación de la parte posterior del switch o desenchúfelo y luego vuelva a enchufarlo.

- e. Reinicie el software con el comando **reload** en el modo EXEC privilegiado.

**Nota:** no es necesario ejecutar este paso si el switch se ha reiniciado con el método de reinicio.

- 1) En el modo EXEC privilegiado, ejecute el comando **reload**:

```
Switch(config)#reload
```

La respuesta a la línea de comandos es:

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

Escriba **n** y luego presione **Enter** (Intro).

La respuesta a la línea de comandos es:

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

La primera línea de la respuesta es:

```
Reload requested by console.
```

Una vez que se recarga el switch, aparece el siguiente mensaje:

```
Would you like to enter the initial configuration dialog? [yes/no]:  
Escriba n y luego presione Enter (Intro).  
La respuesta a la línea de comandos es:  
Press RETURN to get started! [Enter]
```

## Borrar y recargar el router

- a. Escriba el comando **enable** para ingresar al modo EXEC privilegiado.

```
Router>enable
```

- b. En el modo EXEC privilegiado, escriba el comando **erase startup-config**.

```
Router#erase startup-config
```

La respuesta a la línea de comandos es:

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

- c. Presione **Enter** (Intro) para confirmar.

La respuesta es:

```
Erase of nvram: complete
```

- d. En el modo EXEC privilegiado, escriba el comando **reload**.

```
Router(config)#reload
```

La respuesta a la línea de comandos es:

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

- e. Escriba **n** y luego presione **Enter** (Intro).

La respuesta a la línea de comandos es:

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

- f. Presione **Enter** (Intro) para confirmar.

La primera línea de la respuesta es:

```
Reload requested by console.
```

Después de que el router se recarga, aparece la siguiente pregunta:

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

- g. Escriba **n** y luego presione **Enter** (Intro).

La respuesta a la línea de comandos es:

```
Press RETURN to get started!
```

- h. Presione **Enter** (Intro).

El router está listo para iniciar la práctica de laboratorio asignada.