

Práctica de laboratorio: configuración básica de un switch

Topología

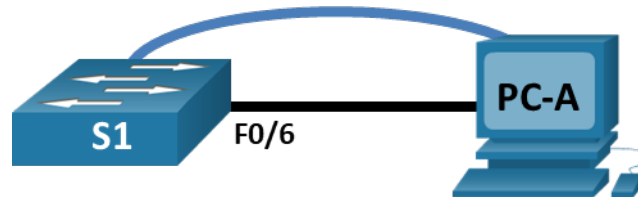


Tabla de asignación de direcciones

Dispositivo	Interfaz	IP Address / Prefix
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad: :2 /64
		fe80::2
PC-A	NIC	192.168.1.10 /24
		2001:db8:acad:3 /64
		fe80::3

Objetivos

Parte 1: Tender el cableado de red y verificar la configuración predeterminada del switch

Parte 2: Configurar parámetros básicos de los dispositivos de red

- Configurar los parámetros básicos del switch.
- Configurar la dirección IP de la computadora.

Parte 3: Verificar y probar la conectividad de red

- Mostrar la configuración del dispositivo.
- Probar la conectividad de extremo a extremo con ping.
- Probar las capacidades de administración remota con Telnet.

Parte 4: Administrar la tabla de direcciones MAC

- Registrar la dirección MAC del host.
- Determinar las direcciones MAC que el switch ha aprendido.
- Enumerar las opciones del comando **show mac address-table**.
- Configurar una dirección MAC estática.

Aspectos básicos/situación

Los switches Cisco se pueden configurar con una dirección IP especial conocida como interfaz virtual de switch (SVI). La SVI, o dirección de administración, se puede usar para el acceso remoto al switch a fin de ver o configurar los ajustes. Si la SVI de la VLAN 1 tiene asignada una dirección IP, de manera predeterminada todos los puertos en la VLAN 1 tienen acceso a la dirección IP de la SVI.

En esta práctica de laboratorio, armará una topología simple mediante cableado LAN Ethernet y accederá a un switch Cisco utilizando los métodos de acceso de consola y remoto. Examinará la configuración predeterminada del switch antes de configurar los parámetros básicos del switch. Estos ajustes básicos de switch incluyen nombre del dispositivo, descripción de la interfaz, contraseñas locales, mensaje del anuncio del día (MOTD), direcciones IP y dirección MAC estática. También demostrará el uso de una dirección IP de administración para la administración remota del switch. La topología consta de un switch y un host que solo usa puertos Ethernet y de consola.

Note: Los switches que se usan son Cisco Catalyst 2960 con Cisco IOS Release 15.0(2) (imagen lanbasek9). Se pueden utilizar otros switches y otras versiones de Cisco IOS. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio.

Nota: Asegúrese de que los interruptores se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor. Consulte el Apéndice A si desea conocer los procedimientos para inicializar y volver a cargar un switch.

La plantilla **default bias**, utilizada por Switch Database Manager (SDM), no proporciona capacidades de dirección IPv6. Verifique que el SDM utilice las plantillas **dual-ipv4-and-ipv6** o **lanbase-routing**. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

```
S1# show sdm prefer
```

Utilice los siguientes comandos para asignar la plantilla **dual-ipv4-and-ipv6** como plantilla predeterminada en SDM.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Recursos necesarios

- 1 Switch (Cisco 2960 con Cisco IOS Release 15.2 (2) imagen lanbasek9 o comparable)
- 1 PC (Windows con programa de emulación de terminal, como Tera Term)
- 1 cable de consola para configurar el dispositivo con Cisco IOS mediante el puerto de la consola
- 1 cable Ethernet como muestra la topología

Parte 1: Tender el cableado de red y verificar la configuración predeterminada del switch

En la parte 1, establecerá la topología de la red y verificará la configuración predeterminada del switch.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

- a. Conecte el cable de la consola como muestra la topología. En esta instancia, no conecte el cable Ethernet de la PC-A.

Nota: Si está utilizando Netlab, apague F0 / 6 en S1. Esto tiene el mismo efecto que no conectar PC-A a S1.

- b. Conéctese al switch desde PC-A a través de Tera Term u otro programa de emulación de terminales.

¿Por qué debe usar una conexión de consola para configurar inicialmente el switch? ¿Por qué no es posible conectarse al switch a través de Telnet o SSH?

Paso 2: Verificar la configuración predeterminada del switch.

En este paso, examinará la configuración predeterminada del switch, como la configuración actual del switch, la información de IOS, las propiedades de las interfaces, la información de la VLAN y la memoria flash.

Puede acceder a todos los comandos IOS del switch en el modo EXEC privilegiado. Se debe restringir el acceso al modo EXEC privilegiado con protección con contraseña para evitar el uso no autorizado, dado que proporciona acceso directo al modo de configuración global y a los comandos que se usan para configurar los parámetros de funcionamiento. Establecerá las contraseñas más adelante en esta práctica de laboratorio.

El conjunto de comandos del modo EXEC privilegiado incluye los comandos del modo EXEC del usuario y el comando **configure**, a través del cual se obtiene acceso a los modos de comando restantes. Use el comando **enable** para ingresar al modo EXEC privilegiado.

- a. Suponiendo que el switch no tenía almacenado un archivo de configuración en la memoria de acceso aleatorio no volátil (NVRAM), una conexión de consola mediante Tera Term u otro programa de emulación de terminales abrirá la línea de comandos del modo EXEC del usuario en el switch con el comienzo de línea Switch>. Use el comando **enable** para ingresar al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

Verifique que haya un archivo de configuración predeterminado limpio en el switch emitiendo el comando **show running-config** privileged EXEC mode command. Si se guardó un archivo de configuración anteriormente, se debe eliminar. Según cuál sea el modelo del switch y la versión de IOS, la configuración podría verse diferente. Sin embargo, no debería haber contraseñas ni direcciones IP configuradas. Si su switch no tiene una configuración predeterminada, borre y recargue el switch.

Nota: el Apéndice A detalla los pasos para inicializar y volver a cargar un interruptor..

- b. Examine el archivo de configuración activa actual.

```
Switch# show running-config
```

¿Cuántas interfaces FastEthernet tiene un switch 2960?

¿Cuántas interfaces Gigabit Ethernet tiene un switch 2960?

¿Cuál es el rango de valores que se muestra para las líneas vty?

- c. Examine el archivo de configuración de inicio en la NVRAM.

```
Switch# show startup-config
startup-config is not present
```

¿Por qué aparece este mensaje?

No se guardaron configuraciones para NVRAM.

- d. Examine las características de la SVI para la VLAN 1.

```
Switch# show interface vlan1
```

¿Hay alguna dirección IP asignada a VLAN 1?

¿Cuál es la dirección MAC de esta SVI? Las respuestas varían.

¿Está activa esta interfaz?

- e. Examine las propiedades IP de la VLAN 1 SVI.

```
Switch# show ip interface vlan1
```

¿Qué resultado ve?

- f. Conecte un cable Ethernet desde PC-A al puerto 6 del switch y examine las propiedades de IP de la SVI VLAN 1. Espere un momento para que el switch y la computadora negocien los parámetros de dúplex y velocidad.

Nota: Si está utilizando Netlab, habilite la interfaz F0 / 6 en S1.

```
Switch# show ip interface vlan1
```

¿Qué resultado ve?

- g. Examine la información de la versión del IOS de Cisco del switch.

```
Switch# show version
```

¿Cuál es la versión del IOS de Cisco que está ejecutando el switch?

¿Cuál es el nombre del archivo de imagen del sistema?

¿Cuál es la dirección MAC base de este switch?

- h. Examine las propiedades predeterminadas de la interfaz FastEthernet que usa la PC-A.

```
Switch# show interface f0/6
```

¿La interfaz está activa o inactiva?

¿Qué haría que una interfaz se active?

¿Cuál es la dirección MAC de la interfaz?

¿Cuál es la configuración de velocidad y de dúplex de la interfaz?

- i. Examine la configuración VLAN configuración del switch.

```
Switch# show vlan
```

¿Cuál es el nombre predeterminado de la VLAN 1?

¿Qué puertos están en VLAN 1?

¿La VLAN 1 está activa?

¿Qué tipo de VLAN es la VLAN predeterminada?

- j. Examine la memoria flash.

Ejecute uno de los siguientes comandos para examinar el contenido del directorio flash.

```
Switch# show flash
```

```
Switch# dir flash:
```

Los archivos poseen una extensión, tal como .bin, al final del nombre del archivo. Los directorios no tienen una extensión de archivo.

¿Cuál es el nombre de archivo de la imagen de IOS de Cisco?

Parte 2: Configurar los parámetros básicos de los dispositivos de red

En la Parte 2, configurará los ajustes básicos para el switch y la PC.

Paso 1: Configurar los parámetros básicos del switch.

- a. Copie la siguiente configuración básica y péguela en S1 mientras se encuentre en el modo de configuración global.

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
```

- b. Establezca la dirección IP de la SVI del switch. Esto permite la administración remota del switch.

Antes de poder administrar el S1 en forma remota desde la PC-A, debe asignar una dirección IP al switch. El switch está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1. Sin embargo, la práctica recomendada para la configuración básica del switch es cambiar la VLAN de administración a otra VLAN distinta de la VLAN 1.

Con fines de administración, utilice la VLAN 99. La selección de la VLAN 99 es arbitraria y de ninguna manera implica que siempre deba usar la VLAN 99.

Primero, cree la nueva VLAN 99 en el switch. Luego, establezca la dirección IP del switch en 192.168.1.2 con la máscara de subred 255.255.255.0 en la interfaz virtual interna VLAN 99. La dirección IPv6 también se puede configurar en la interfaz SVI. Utilice las direcciones IPv6 que figuran en la tabla de direccionamiento.

```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1 (config-if) # ipv6 address 2001:db8:acad: :2/64
S1 (config-if) # ipv6 address fe80: :2 enlace local
S1(config-if)# no shutdown
S1(config-if)# exit
```

Observe que la interfaz VLAN 99 está en estado down, aunque haya introducido el comando **no shutdown**. Actualmente, la interfaz se encuentra en estado down debido a que no se asignaron puertos del switch a la VLAN 99.

- c. Asigne todos los puertos de usuario a VLAN 99.

```
S1(config)# interface range f0/1 - 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Para establecer la conectividad entre el host y el switch, los puertos que usa el host deben estar en la misma VLAN que el switch. Observe que, en el resultado de arriba, la interfaz VLAN 1 queda en estado down porque no se asignó ninguno de los puertos a la VLAN 1. Después de unos segundos, la VLAN 99 pasa al estado up porque ahora se le asigna al menos un puerto activo (F0/6 con la PC-A conectada).

- d. Emita el comando **show vlan brief** verificar que todos los puertos estén en VLAN 99.

```
S1# show vlan brief

VLAN Name Status Ports
----
1 default active
99 VLAN0099 active Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gi0/1, Gi0/2
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
```

- e. Configure el gateway predeterminado para S1. Si no se estableció ningún gateway predeterminado, no se puede administrar el switch desde una red remota que esté a más de un router de distancia. Aunque esta actividad no incluye un gateway IP externo, se debe tener en cuenta que finalmente conectará la LAN a un router para tener acceso externo. Si suponemos que la interfaz de LAN en el router es 192.168.1.1, establezca el gateway predeterminado para el switch.

```
S1(config)# ip default-gateway 192.168.1.1
```

- f. El acceso al puerto de la consola también debe restringirse con una contraseña. Utilice **cisco** como contraseña de inicio de sesión de la consola en esta actividad. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpan los comandos, use la opción **logging synchronous**.

```
S1(config)# line con 0
S1(config-line)# logging synchronous
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
```

- g. Configure las líneas de terminal virtual (vty) para el switch para permitir el acceso telnet. Si no configura una contraseña vty, no podrá hacer telnet al switch.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar 1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

¿Por qué se requiere el comando **login**?

Paso 2: Configurar una dirección IP en la PC-A.

Asigne a la computadora la dirección IP y la máscara de subred que se muestran en la tabla de direccionamiento. Aquí se describe una versión abreviada del procedimiento. No se requiere una puerta de enlace predeterminada para esta topología; sin embargo, puede ingresar **192.168.1.1** and **fe80::1** para simular un enrutador conectado a S1.

- 1) Navega hasta el **Panel de control**.
- 2) En la vista Categoría, seleccione **Ver el estado y las tareas de la red**.
- 3) Haga clic en **Cambiar la configuración del** adaptador en el panel izquierdo.
- 4) Haga clic con el botón derecho en una interfaz **Ethernet** y elija **Propiedades**.
- 5) Elija **el Protocolo de Internet versión 4 (TCP / IPv4)** y haga clic en **Propiedades**.
- 6) Haga clic en el botón de opción **Usar la siguiente dirección IP** e ingrese la dirección IP y la máscara de subred y haga clic en **Aceptar**.
- 7) Seleccione **Protocolo de Internet versión 6 (TCP / IPv6)** y haga clic en **Propiedades**.
- 8) Haga clic en el botón de opción **Usar la siguiente dirección IPv6** e ingrese la dirección IPv6 y el prefijo y haga clic en **Aceptar** para continuar
- 9) Haga clic en **Aceptar** para salir de la ventana Propiedades.

Parte 3: Verificar y probar la conectividad de red

En la parte 3, verificará y registrará la configuración del switch, probará la conectividad de extremo a extremo entre la PC-A y el S1, y probará la capacidad de administración remota del switch.

Paso 1: Mostrar la configuración del switch

Use la conexión de la consola en PC-A para mostrar y verificar la configuración del switch. El comando **show run** muestra la configuración en ejecución completa, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas.

- Se muestra una configuración de ejemplo. Los parámetros que configuró están resaltados en amarillo. Las demás son opciones de configuración predeterminadas del IOS.

```
S1# show run
Building configuration...

Current configuration : 2206 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$mtvc$6nc.1vkr3p6bj7yge.jng0
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
interface FastEthernet0/24
switchport access vlan 99
!
interface GigabitEthernet0/1
switchport access vlan 99
!
interface GigabitEthernet0/2
switchport access vlan 99
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan99
ip address 192.168.1.2 255.255.255.0
ipv6 address FE80::2 link-local
```



```
IPv6 address 2001:DB8:ACAD: :2/64
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
password 7 00071A150754
logging synchronous
login
line vty 0 4
password 7 121A0C041104
login
line vty 5 15
password 7 121A0C041104
login
!
end
```

- b. Verifique la configuración de la VLAN 99 de administración.

```
S1# show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is EtherSVI, address is 0cd9.96e2.3d41 (bia 0cd9.96e2.3d41)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 0:00:06, output 0:08:45, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    175 packets input, 22989 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es el ancho de banda en esta interfaz?

¿Cuál es el estado de la VLAN 99?

¿Cuál es el estado del protocolo de línea?

Paso 2: Probar la conectividad de extremo a extremo con ping

- Desde la línea de comandos en PC-A, emita el comando ping a la dirección de PC-A primero.

```
C:\> ping 192.168.1.10
```

- En el símbolo del sistema de la PC-A, haga ping a la dirección de administración de SVI del S1.

```
C:\> ping 192.168.1.2
```

Debido a que la PC-A debe resolver la dirección MAC del S1 mediante ARP, es posible que se agote el tiempo de espera del primer paquete. Si los resultados del ping siguen siendo incorrectos, resuelva los problemas de configuración de los parámetros básicos del dispositivo. Verifique el cableado físico y las direcciones lógicas.

Paso 3: Probar y verificar la administración remota del S1

Ahora utilizará Telnet para acceder al switch en forma remota. En esta práctica de laboratorio, la PC-A y el S1 se encuentran uno junto al otro. En una red de producción, el switch podría estar en un armario de cableado en el piso superior, mientras que la computadora de administración podría estar ubicada en la planta baja. En este paso, utilizará Telnet para acceder al switch S1 en forma remota mediante la dirección de administración de SVI. Telnet no es un protocolo seguro; sin embargo, lo usará para probar el acceso remoto. Con Telnet, toda la información, incluidos los comandos y las contraseñas, se envía durante la sesión como texto no cifrado. En las prácticas de laboratorio posteriores, usará SSH para acceder a los dispositivos de red en forma remota.

- Abra Tera Term u otro programa de emulación de terminal con capacidad Telnet.
- Seleccione el servidor Telnet y proporcione la dirección de administración SVI para utilizar a S1. La contraseña es **cisco**.
- Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Acceda al modo EXEC con privilegios con el comando **enable** y suministre la contraseña secreta **class**.
- Guarde la configuración.

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
```

- Escriba **exit** para finalizar la sesión de Telnet.

Parte 4: Administrar la tabla de direcciones MAC

En la Parte 4 determinará las direcciones MAC que el switch ha aprendido, configurará una dirección MAC estática en una interfaz del switch y luego retirará la dirección MAC estática de la interfaz.

Paso 1: Registrar la dirección MAC del host

Abra una línea de comandos en PC-A y emita el comando **ipconfig /all** para determinar y registrar las direcciones Capa 2 (físicas) del NIC.

Paso 2: Determinar las direcciones MAC que el switch ha aprendido

Muestre las direcciones MAC con el comando **show mac address-table**.

```
S1# show mac address-table
```

¿Cuántas direcciones dinámicas hay?

¿Cuántas direcciones MAC hay en total?

¿Coincide la dirección MAC dinámica con la dirección MAC de PC-A?

Paso 3: Enumerar las opciones del comando **show mac address-table**

- a. Muestre las opciones de la tabla de direcciones MAC.

```
S1# show mac address-table ?
```

¿Cuántas opciones se encuentran disponibles para el comando **show mac address-table**?

- b. Emita el comando **show mac address-table dynamic** para mostrar solo las direcciones MAC que se detectaron dinámicamente.

```
S1# show mac address-table dynamic
```

¿Cuántas direcciones dinámicas hay?

- c. Observe la entrada de dirección MAC de PC-A. El formato de dirección MAC del comando es **xxxx.xxxx.xxxx**.

```
S1# show mac address-table address <PC-A MAC here>
```

Paso 4: Configurar una dirección MAC estática

- a. Limpie la tabla de direcciones MAC.

Para quitar las direcciones MAC existentes, use el comando **clear mac address-table dynamic** en el modo EXEC con privilegios.

```
S1# clear mac address-table dynamic
```

- b. Verifique que la tabla de direcciones MAC se haya eliminado.

```
S1# show mac address-table
```

¿Cuántas direcciones MAC estáticas hay?

¿Cuántas direcciones dinámicas hay?

- c. Examine nuevamente la tabla de direcciones MAC

Es muy probable que una aplicación en ejecución en la computadora ya haya enviado una trama por la NIC hacia el S1. Observe la tabla de direcciones MAC de nuevo en el modo EXEC con privilegios para ver si S1 ha vuelto a aprender la dirección MAC de PC-A.

```
S1# show mac address-table
```

¿Cuántas direcciones dinámicas hay?

¿Por qué cambió esto desde la última visualización?

Si el S1 aún no volvió a detectar la dirección MAC de la PC-A, haga ping a la dirección IP de la VLAN 99 del switch desde la PC-A y, a continuación, repita el comando **show mac address-table**.

- d. Configure una dirección MAC estática.

Para especificar a qué puertos se puede conectar un host, una opción es crear una asignación estática de la dirección MAC del host a un puerto.

Configure una dirección MAC estática en F0/6 con la dirección que se registró para la PC-A en la parte 4, paso 1. La dirección MAC 0050.56BE.6C89 se usa solo como ejemplo. Debe utilizar la dirección MAC de PC-A, que es diferente de la que se da aquí como ejemplo.

```
S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

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

```
S1# show mac address-table
```

¿Cuántas direcciones MAC hay en total?

¿Cuántas direcciones estáticas hay?

- f. Elimine la entrada de MAC estática. Ingrese al modo de configuración global y elimine el comando escribiendo **no** delante de la cadena de comandos.

Nota: La dirección MAC 0050.56BE.6C89 se usa solo en el ejemplo. Utilice la dirección MAC para PC-A.

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

- g. Verifique que la dirección MAC estática se haya borrado.

```
S1# show mac address-table
```

¿Cuántas direcciones MAC estáticas hay en total?

Apéndice A: inicializar y volver a cargar un interruptor

- a. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

- b. Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

```
Switch# show flash
Directory of flash:/
```

```
2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text
3 -rwx 1632 Mar 1 1993 0:06:33 +00:00 config.text
4 -rwx 13336 Mar 1 1993 0:06:33 +00:00 multiple-fs
5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin
6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat
```

32514048 bytes totales (20886528 bytes libres)

- c. Si se encontró el archivo **vlan.dat** en la memoria flash, elimínalo.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

- d. Se le solicitará que verifique el nombre de archivo. Si introdujo el nombre correctamente, presione Enter; de lo contrario, puede cambiar el nombre de archivo.

Recibirá un pedido de confirmación para eliminar este archivo. Presione Enter para confirmar.

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

- e. Utilice el comando **erase startup-config** para eliminar el archivo de configuración de inicio de la NVRAM. Se le solicita que elimine el archivo de configuración. Presione Enter para confirmar.

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

- f. Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Luego recibirá un pedido de confirmación de la recarga del switch. Presione Enter para continuar.

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

Nota: Puede recibir un mensaje para guardar la configuración en ejecución antes de volver a cargar el switch. Responda escribiendo **no** y presione Enter.

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

- g. Una vez que se vuelve a cargar el switch, debe ver una petición de entrada del diálogo de configuración inicial. Responda escribiendo **no** en la petición de entrada y presione Enter.

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

Configuraciones de dispositivos

Switch S1

```
S1#sh run
Building configuration...
Current configuration : 2359 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$mtvc$6nc.1vkr3p6bj7yge.jng0
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!interface FastEthernet0/1
  switchport access vlan 99
!
interface FastEthernet0/2
  switchport access vlan 99
!
interface FastEthernet0/3
  switchport access vlan 99
!
interface FastEthernet0/4
  switchport access vlan 99
!
interface FastEthernet0/5
  switchport access vlan 99
!
interface FastEthernet0/6
  switchport access vlan 99
!
interface FastEthernet0/7
  switchport access vlan 99
!
interface FastEthernet0/8
  switchport access vlan 99
!
interface FastEthernet0/9
  switchport access vlan 99
!
interface FastEthernet0/10
  switchport access vlan 99
```

```
!  
interface FastEthernet0/11  
  switchport access vlan 99  
!  
interface FastEthernet0/12  
  switchport access vlan 99  
!  
interface FastEthernet0/13  
  switchport access vlan 99  
!  
interface FastEthernet0/14  
  switchport access vlan 99  
!  
interface FastEthernet0/15  
  switchport access vlan 99  
!  
interface FastEthernet0/16  
  switchport access vlan 99  
!  
interface FastEthernet0/17  
  switchport access vlan 99  
!  
interface FastEthernet0/18  
  switchport access vlan 99  
!  
interface FastEthernet0/19  
  switchport access vlan 99  
!  
interface FastEthernet0/20  
  switchport access vlan 99  
!  
interface FastEthernet0/21  
  switchport access vlan 99  
!  
interface FastEthernet0/22  
  switchport access vlan 99  
!  
interface FastEthernet0/23  
  switchport access vlan 99  
!  
interface FastEthernet0/24  
  switchport access vlan 99  
!  
interface GigabitEthernet0/1  
  switchport access vlan 99  
!  
interface GigabitEthernet0/2  
  switchport access vlan 99  
!  
interface Vlan1
```

```
no ip address
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD::2/64
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7 00071A150754
 logging synchronous
 login
line vty 0 4
 password 7 121A0C041104
 login
line vty 5 15
 password 7 121A0C041104
 login
!
end
```