

Práctica de laboratorio: configuración de los parámetros básicos de un switch

Topología

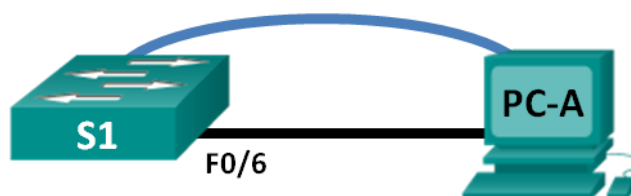


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objetivos

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

Parte 2: configurar los 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.
- Guardar el archivo de configuración en ejecución del switch.

Parte 4: administrar la tabla de direcciones MAC

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

Información básica/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 parámetros. Si se asigna una dirección IP a la SVI de la VLAN 1, de manera predeterminada, todos los puertos en la VLAN 1 tienen acceso a la dirección IP de administración de 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. Esta configuración básica del switch incluye el nombre del dispositivo, la descripción de interfaces, las contraseñas locales, el mensaje del día (MOTD), el direccionamiento IP, la configuración de una dirección MAC estática y la demostración del 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.

Nota: el switch que se utiliza es Cisco Catalyst 2960 con IOS de Cisco versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros switches y otras versiones del IOS de Cisco. 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 el switch se haya borrado y no tenga una configuración de inicio. Consulte el apéndice A para conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term, y capacidad para Telnet)
- Cable de consola para configurar el dispositivo con IOS de Cisco mediante el puerto de consola
- Cable Ethernet, como se muestra en 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. Realice el cableado de la conexión de consola tal como se muestra en la topología. En esta instancia, no conecte el cable Ethernet de la PC-A.

Nota: si utiliza Netlab, puede desactivar F0/6 en el S1, lo que tiene el mismo efecto que no conectar la PC-A al S1.

- b. Con Tera Term u otro programa de emulación de terminal, cree una conexión de consola de la PC-A al switch.

¿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. Si se parte de la suposición de que el switch no tenía ningún archivo de configuración almacenado en la memoria de acceso aleatorio no volátil (NVRAM), usted estará en la petición de entrada del modo EXEC del usuario en el switch, con la petición de entrada 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 el archivo de configuración esté limpio con el comando **show running-config** del modo EXEC privilegiado. Si se guardó un archivo de configuración anteriormente, se debe eliminar. Según cuál sea el modelo del switch y la versión del IOS, la configuración podría variar. Sin embargo, no debería haber contraseñas ni direcciones IP configuradas. Si su switch no tiene una configuración predeterminada, borre y recargue el switch.

Nota: en el apéndice A, se detallan los pasos para inicializar y volver a cargar los dispositivos.

- 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? _____

Examine el archivo de configuración de inicio en la NVRAM.

```
Switch# show startup-config
```

```
startup-config is not present
```

¿Por qué aparece este mensaje? _____

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

```
Switch# show interface vlan1
```

¿Hay alguna dirección IP asignada a la VLAN 1? _____ **No**

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

¿Está activa esta interfaz?

Los switches Cisco tienen el comando **no shutdown** configurado de manera predeterminada en la VLAN 1, pero la VLAN 1 no alcanzará el estado up/up hasta que se le asigne un puerto y este también esté activo. Si no hay ningún puerto en estado up en la VLAN 1, la interfaz VLAN 1 estará activa, pero el protocolo de línea estará inactivo. De manera predeterminada, todos los puertos se asignan inicialmente a la VLAN 1.

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

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

¿Qué resultado ve?

```
Vlan1 is up, line protocol is down
Internet protocol processing disabled
```

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

Nota: si utiliza Netlab, habilite la interfaz F0/6 en el S1.

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

¿Qué resultado ve?

```
Vlan1 is up, line protocol is up
Internet protocol processing disabled
```

- f. 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?

Las respuestas pueden variar. c2960-lanbasek9-mz.150-2-SE.bin

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

Las respuestas pueden variar. c2960-LANBASEK9-MZ

¿Cuál es la dirección MAC base de este switch? Las respuestas varían.

Las respuestas varían. 0C:D9:96:E2:3D:00.

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

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

¿La interfaz está activa o desactivada?

Debería estar activa, a menos que exista un problema de cableado.

¿Qué haría que una interfaz se active?

La conexión de un host u otro dispositivo

¿Cuál es la dirección MAC de la interfaz?

0CD9:96E2:3D06 (varía)

¿Cuál es la configuración de velocidad y de dúplex de la interfaz? _____ Full-duplex, 100 Mb/s

- h. Examine la configuración VLAN predeterminada del switch.

```
Switch# show vlan
```

¿Cuál es el nombre predeterminado de la VLAN 1? _____ default

¿Qué puertos hay en esta VLAN? _____

¿La VLAN 1 está activa? _____

¿Qué tipo de VLAN es la VLAN predeterminada? _____ enet (Ethernet)

- i. 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?

c2960-lanbasek9-mz.150-2.SE.bin (puede variar)

Parte 2. configurar los parámetros básicos de los dispositivos de red

En la parte 2, configurará los parámetros básicos para el switch y la computadora.

Paso 1. configurar los parámetros básicos del switch, incluidos el nombre de host, las contraseñas locales, el mensaje MOTD, la dirección de administración y el acceso por Telnet.

En este paso, configurará la computadora y los parámetros básicos del switch, como el nombre de host y la dirección IP para la SVI de administración del switch. La asignación de una dirección IP en el switch es solo el primer paso. Como administrador de red, debe especificar cómo se administra el switch. Telnet y SSH son los dos métodos de administración que más se usan. No obstante, Telnet no es un protocolo seguro. Toda la información que fluye entre los dos dispositivos se envía como texto no cifrado. Las contraseñas y otra información confidencial pueden ser fáciles de ver si se las captura mediante un programa detector de paquetes.

- a. Si se parte de la suposición de que el switch no tenía ningún archivo de configuración almacenado en la NVRAM, verifique que usted esté en el modo EXEC privilegiado. Introduzca el comando **enable** si la petición de entrada volvió a cambiar a Switch>.

```
Switch> enable
```

```
Switch#
```

- b. Ingrese al modo de configuración global.

```
Switch# configure terminal
```

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

```
Switch(config)#
```

La petición de entrada volvió a cambiar para reflejar el modo de configuración global.

- c. Asigne el nombre de host del switch.

```
Switch(config)# hostname S1
```

```
S1(config)#
```

- d. Configurar la encriptación de contraseñas.

```
S1(config)# service password-encryption
```

```
S1(config)#
```

- e. Asigne **class** como contraseña secreta para el acceso al modo EXEC privilegiado.

```
S1(config)# enable secret class
S1(config)#
```

- f. Evite las búsquedas de DNS no deseadas.

```
S1(config)# no ip domain-lookup
S1(config)#
```

- g. Configure un mensaje MOTD.

```
S1(config)# banner motd #
Enter Text message. End with the character '#'.
Unauthorized access is strictly prohibited. #
```

- h. Para verificar la configuración de acceso, alterne entre los modos.

```
S1(config)# exit
S1#
*Mar  1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console
S1# exit
S1 con0 is now available
```

Press RETURN to get started.

```
Unauthorized access is strictly prohibited.
S1>
```

¿Qué teclas de método abreviado se usan para ir directamente del modo de configuración global al modo EXEC privilegiado? _____ **Ctrl-Z**

- i. Vuelva al modo EXEC privilegiado desde el modo EXEC del usuario. Introduzca la contraseña **class** cuando se le solicite hacerlo.

```
S1> enable
Password:
S1#
```

Nota: cuando se introduce la contraseña, esta no se muestra.

- j. Ingrese al modo de configuración global para establecer 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.

```
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)# no shutdown
S1(config-if)# exit
S1(config)#
```

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.

- k. 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).

- l. Emita el comando **show vlan brief** para verificar que todos los puertos de usuario estén en la 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	

- m. Configure el gateway IP predeterminado para el 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. Sí responde a los pings de una red remota. 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. Suponiendo que la interfaz 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
S1(config)#
```

- n. También se debe restringir el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpen los comandos, use la opción **logging synchronous**.

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

- o. Configure las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet. Si no configura una contraseña de vty, no puede acceder al switch mediante telnet.

```
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?
```

Sin el comando **login**, el switch no solicitará que se introduzca una contraseña.

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. Para esta topología, no se requiere ningún gateway predeterminado; sin embargo, puede introducir **192.168.1.1** para simular un router conectado al S1.

- 1) Haga clic en el ícono **Inicio** de Windows > **Panel de control**.
- 2) Haga clic en **Ver por:** y elija **Íconos pequeños**.
- 3) Seleccione **Centro de redes y recursos compartidos** > **Cambiar configuración del adaptador**.
- 4) Seleccione **Conexión de área local**, haga clic con el botón secundario y elija **Propiedades**.
- 5) Seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** > **Propiedades**.
- 6) Haga clic en el botón de opción **Usar la siguiente dirección IP** e introduzca la dirección IP y la máscara de subred.

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.

Desde la conexión de consola en la PC-A, muestre y verifique 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.

- a. Aquí se muestra un ejemplo de configuración. 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 15.0
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 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
interface FastEthernet0/24
switchport access vlan 99
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan99
ip address 192.168.1.2 255.255.255.0
no ip route-cache
!
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 104D000A0618  
logging synchronous  
login  
line vty 0 4  
password 7 14141B180F0B  
login  
line vty 5 15  
password 7 14141B180F0B  
login  
!  
end
```

S1#

- 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 00:00:06, output 00:08:45, 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? _____ 1 000 000 Kb/s (1 Gb/seg)

¿Cuál es el estado de la VLAN 99? _____ up

¿Cuál es el estado del protocolo de línea? _____ up

Paso 2. probar la conectividad de extremo a extremo con ping.

- a. En el símbolo del sistema de la PC-A, haga ping a la dirección de la propia PC-A primero.

```
C:\Users\User1> ping 192.168.1.10
```

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

```
C:\Users\User1> 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. Revise el cableado físico y el direccionamiento lógico, si es necesario.

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.

Nota para el instructor: si en su institución no se permite el uso de Telnet en el símbolo del sistema de Windows, es posible usar Tera Term u otro programa de emulación de terminal con capacidad para Telnet.

Nota: si utiliza Windows 7, es posible que el administrador deba habilitar el protocolo Telnet. Para instalar el cliente de Telnet, abra una ventana cmd y escriba **pkgmgr /iu:"TelnetClient"**. A continuación, se muestra un ejemplo.

```
C:\Users\User1> pkgmgr /iu:"TelnetClient"
```

- a. Con la ventana cmd abierta en la PC-A, emita un comando de Telnet para conectarse al S1 a través de la dirección de administración de SVI. La contraseña es **cisco**.

```
C:\Users\User1> telnet 192.168.1.2
```

- b. Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Acceda al modo EXEC privilegiado.
- c. Escriba **exit** para finalizar la sesión de Telnet.

Paso 4. guardar el archivo de configuración en ejecución del switch.

Guarde la configuración.

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

Parte 4. Administrar la tabla de direcciones MAC

En la parte 4, determinará la dirección MAC que detectó el switch, configurará una dirección MAC estática en una interfaz del switch y, a continuación, eliminará la dirección MAC estática de esa interfaz.

Paso 1. registrar la dirección MAC del host.

En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** para determinar y registrar las direcciones (físicas) de capa 2 de la NIC de la computadora.

PC-A: 00-50-56-BE-6C-89 (las respuestas variarán)

Paso 2. Determine 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? _____ 1 (puede variar)

¿Cuántas direcciones MAC hay en total? _____ 24 (puede variar)

¿La dirección MAC dinámica coincide con la dirección MAC de la PC-A? _____ **Si**

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**?

_____ 12 (puede variar)

- 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? _____ 1 (puede variar)

- c. Vea la entrada de la dirección MAC para la PC-A. El formato de dirección MAC para el comando es xxxx.xxxx.xxxx.

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

Paso 4. Configure una dirección MAC estática.

- a. limpie la tabla de direcciones MAC.

Para eliminar las direcciones MAC existentes, use el comando **clear mac address-table** del modo EXEC privilegiado.

```
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?

al menos 20 (es posible que se hayan creado otras entradas estáticas de forma manual).

Nota para el instructor: las primeras 20 direcciones estáticas en la tabla de direcciones MAC están incorporadas.

¿Cuántas direcciones dinámicas hay?

0 (es posible que haya 1, según la rapidez con la que el switch vuelve a adquirir las direcciones)

- 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 nuevamente la tabla de direcciones MAC en el modo EXEC privilegiado para ver si el S1 volvió a detectar la dirección MAC para la PC-A.

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

¿Cuántas direcciones dinámicas hay? _____ **1**

¿Por qué cambió esto desde la última visualización?

El switch volvió a adquirir dinámicamente la dirección MAC de la computadora.

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 usar la dirección MAC de su PC-A, que es distinta de la del 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? _____ **21 (varía)**

¿Cuántas direcciones estáticas hay?

Hay 22 direcciones estáticas. La cantidad total de direcciones MAC y de direcciones estáticas debe ser la misma, debido a que no hay otros dispositivos conectados actualmente al S1

- 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. Use la dirección MAC de su 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? _____ **20 (varía)**

Reflexión

1. ¿Por qué debe configurar las líneas vty para el switch?
-

Si no configura una contraseña de vty, no podrá acceder al switch mediante telnet.

2. ¿Para qué se debe cambiar la VLAN 1 predeterminada a un número de VLAN diferente?
-

Para mejorar la seguridad.

3. ¿Cómo puede evitar que las contraseñas se envíen como texto no cifrado?

Con la emisión del comando **service password-encryption**.

4. ¿Para qué se debe configurar una dirección MAC estática en una interfaz de puerto?

Para especificar los puertos a los que se puede conectar un host.

Apéndice A: inicialización y recarga de un router y un switch

Paso 1. inicializar y volver a cargar el router.

- a. Acceda al router mediante el puerto de consola y habilite el modo EXEC privilegiado.

```
Router> enable
Router#
```

- b. Introduzca el comando **erase startup-config** para eliminar la configuración de inicio de la NVRAM.

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

- c. Emita el comando **reload** para eliminar una configuración antigua de la memoria. Cuando reciba el mensaje Proceed with reload?, presione Enter. (Si presiona cualquier otra tecla, se cancela la recarga).

```
Router# reload
Proceed with reload? [confirm]
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Nota: es posible que reciba una petición de entrada para guardar la configuración en ejecución antes de volver a cargar el router. Responda escribiendo **no** y presione Enter.

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

- d. Una vez que se vuelve a cargar el router, se le solicita introducir el diálogo de configuración inicial. Escriba **no** y presione Enter.

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

- e. Aparece otra petición de entrada para finalizar la instalación automática. Responda escribiendo **yes** (sí) y presione Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Paso 2. inicializar y volver a cargar el switch.

- 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 00:06:33 +00:00 config.text
 4 -rwx     13336   Mar 1 1993 00:06:33 +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 total (20886528 bytes free)
```

```
Switch#
```

- 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.
- e. Se le solicita que confirme la eliminación de este archivo. Presione Intro para confirmar.

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

```
Switch#
```

- f. 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 Intro para confirmar.

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

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

```
[OK]
```

```
Erase of nvram: complete
```

```
Switch#
```

- g. Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Luego, recibirá una petición de entrada para confirmar la recarga del switch. Presione Enter para continuar.

```
Switch# reload
```

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

Nota: es posible que reciba 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
```

- h. 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 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
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  
!  
interface GigabitEthernet0/2
```

```
!  
interface Vlan1  
  no ip address  
!  
interface Vlan99  
  ip address 192.168.1.2 255.255.255.0  
!  
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 0822455D0A16  
  logging synchronous  
  login  
line vty 0 4  
  password 7 01100F175804  
  login  
line vty 5 15  
  password 7 01100F175804  
  login  
!  
end
```