Práctica de laboratorio: Configuración de una dirección de administración del switch (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

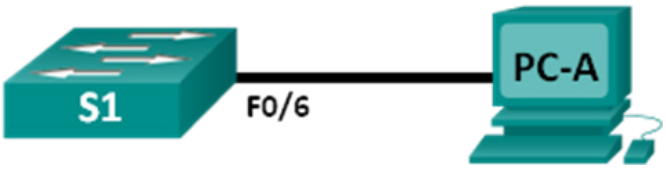


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	192.168.1.2	255.255.255.0	No aplicable
PC-A	NIC	192.168.1.10	255.255.255.0	No aplicable

Objetivos

Parte 1: Configurar un dispositivo de red básico

- Realizar el cableado de red tal como se muestra en la topología.
- Configurar los parámetros básicos del switch, incluidos el nombre de host, la dirección de administración y el acceso por Telnet.
- Configurar una dirección IP en la PC.

Parte 2: Verificar y probar la conectividad de red

- Mostrar la configuración del dispositivo.
- Probar la conectividad de extremo a extremo con ping.
- Probar la capacidad de administración remota con Telnet.
- Guardar el archivo de configuración en ejecución del switch.

Información básica/Situación

Los switches Cisco tienen una interfaz especial, conocida como “interfaz virtual del switch” (SVI). La SVI se puede configurar con una dirección IP, comúnmente conocida como la dirección de administración que se utiliza para el acceso remoto al switch para mostrar o configurar parámetros.

En esta práctica de laboratorio, armará una red simple mediante cableado LAN Ethernet y accederá a un switch Cisco utilizando los métodos de acceso de consola y remoto. Configurará los parámetros básicos del switch y el direccionamiento IP, y demostrará el uso de una dirección IP de administración para la administración remota del switch. La topología consta de un switch y un host, y utiliza puertos Ethernet y de consola únicamente.

Nota: los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados producidos pueden variar de lo que se muestra en las prácticas de laboratorio.

Nota: asegúrese de que el switch se haya borrado y no tenga una configuración de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Parte 1: Configurar un dispositivo de red básico

En la parte 1, configurará la red y los parámetros básicos, como nombres de host, direcciones IP de las interfaces y contraseñas.

Paso 1: Conectar la red

a. Realizar el cableado de red tal como se muestra en la topología.

b. Establezca una conexión de consola al switch desde la PC-A.

Paso 2: Configurar los parámetros básicos del switch

En este paso, configurará los parámetros básicos del switch, como el nombre de host, y configurará una dirección IP para la SVI. Asignar una dirección IP en el switch es solo el primer paso. Como administrador de red, debe especificar cómo se administrará el switch. Telnet y Shell seguro (SSH) son dos de los métodos de administración más comunes; sin embargo, Telnet es un protocolo muy inseguro. 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 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>`. Ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

b. Verifique que haya un archivo de configuración vacío con el comando **`show running-config`** del modo EXEC privilegiado. Si previamente se guardó un archivo de configuración, deberá eliminarlo. 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, solicite ayuda al instructor.

c. Ingrese al modo de configuración global y asigne un nombre de host al switch.

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

d. Configure el acceso por contraseña al switch.

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


e. Evite búsquedas no deseadas del Sistema de nombres de dominios (DNS).

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

f. Configure un mensaje del día (MOTD) de inicio de sesión.

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

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

```
S1(config)# exit
S1#
S1# exit
Unauthorized access is strictly prohibited.
S1>
```

¿Qué tecla de método abreviado se utilizan para pasar directamente del modo de configuración global al modo EXEC privilegiado?

_____

Ctrl+Z

h. Vuelva al modo EXEC privilegiado desde el modo EXEC del usuario.

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

Nota: la contraseña no se mostrará en la pantalla al ingresar.

i. Ingrese al modo de configuración global para configurar la dirección IP de la SVI para permitir la administración remota de switch.

```
S1# config t
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

j. Restrinja el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña.

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

k. Configure la línea de terminal virtual (VTY) para que el switch permita el acceso por Telnet. Si no configura una contraseña de VTY, no podrá acceder al switch mediante Telnet.

```
S1(config)# line vty 0 4
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
```

Paso 3: Configurar una dirección IP en la PC-A

a. Asigne la dirección IP y la máscara de subred a la PC, como se muestra en la Addressing Table de la página 1. A continuación, se describe el procedimiento para asignar una dirección IP em una PC con Windows 7:

1) Haga clic en el ícono **Inicio de Windows** > **Panel de control**.
2) Haga clic en **Ver por:** > **Categoría**.
3) Seleccione **Ver el estado y las tareas de red** > **Cambiar configuración del adaptador**.
4) Haga clic con el botón secundario en **Conexión de área local** y seleccione **Propiedades**.
5) Seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** y haga clic en **Propiedades** > **Aceptar**.
6) Haga clic en el botón de opción **Usar la siguiente dirección IP** e introduzca manualmente la dirección IP y la máscara de subred.

Parte 2: Verificar y probar la conectividad de red

Ahora 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 dispositivo S1

a. Regrese a la conexión de consola utilizando Tera Term en la PC-A para mostrar y verificar la configuración del switch por medio de la emisión del comando **show run**. A continuación, se muestra una configuración de muestra. Los parámetros que configuró están resaltados en amarillo. Las demás son opciones de configuración predeterminadas del IOS.

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

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no 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
!
interface FastEthernet0/2

<resultado omitido>

interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

b. Verifique el estado de su interfaz de administración SVI. La interfaz VLAN 1 debería tener estado up/up (activo/activo) y tener una dirección IP asignada. Observe que el puerto de switch F0/6 también está activado, porque la PC-A está conectada a él. Dado que todos los puertos de switch están inicialmente en VLAN 1 de manera predeterminada, puede comunicarse con el switch mediante la dirección IP que configuró para VLAN 1.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.2     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
```

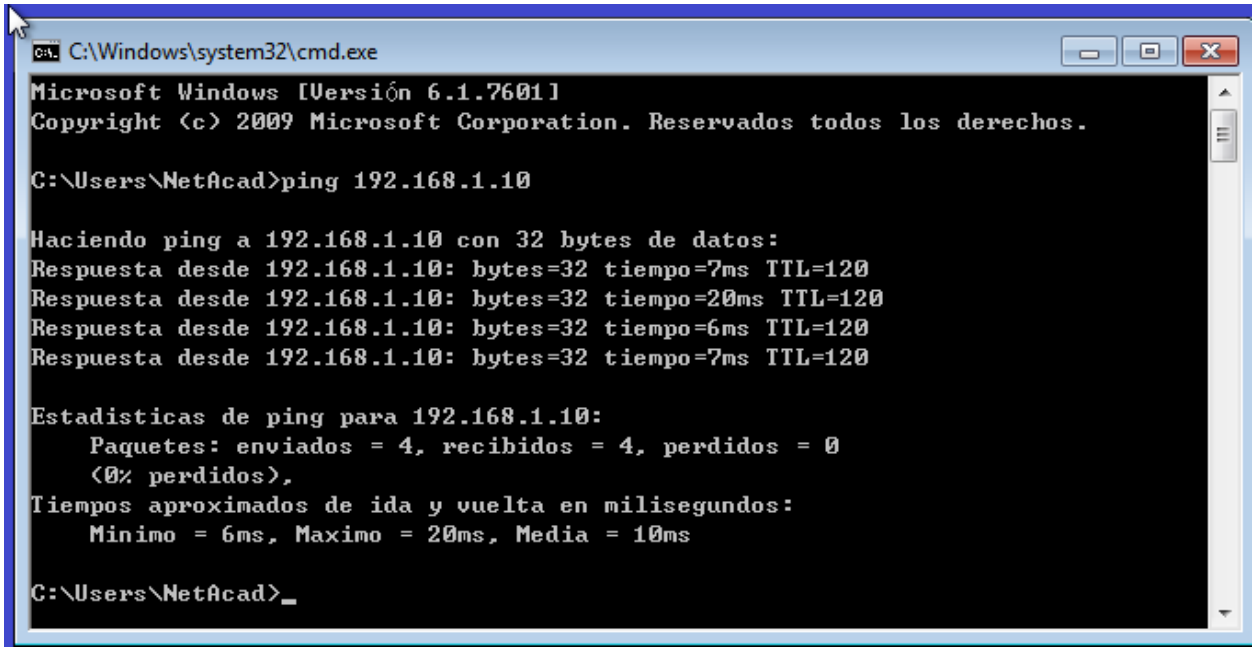
Paso 2: Probar la conectividad de extremo a extremo

Abra una ventana del símbolo del sistema (cmd.exe) en la PC-A: haga clic en el ícono **Inicio de Windows** e introduzca **cmd** en el campo **Buscar programas y archivos**. Verifique la dirección IP de la PC-A mediante el comando **ipconfig /all**. Este comando muestra el nombre de host de la PC y la información de la dirección IPv4. Haga ping a la propia dirección de la PC-A y a la dirección de administración del S1.

a. Haga ping a la dirección de la propia PC-A primero.

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

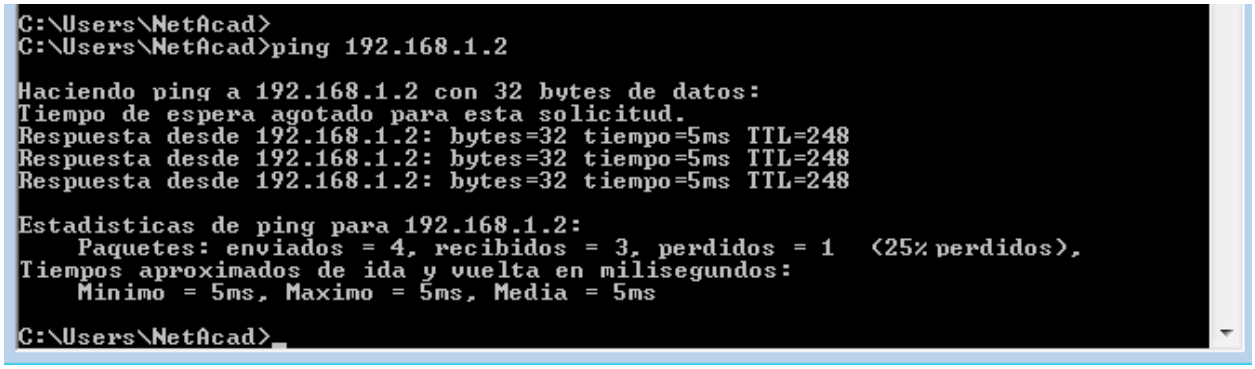
El resultado debe ser similar a la siguiente pantalla:



b. Haga ping a la dirección de administración de SVI del S1.

```
C:\Users\NetAcad> ping 192.168.1.2
```

El resultado debe ser similar a la siguiente pantalla. Si los resultados del ping no son correctos, resuelva los problemas de configuración de los parámetros básicos del dispositivo. Si es necesario, revise el cableado físico y el direccionamiento IP.



Paso 3: Probar y verificar la administración remota del S1

Ahora utilizará Telnet para acceder al switch S1 en forma remota mediante la dirección de administración de SVI. 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 PC de administración podría estar ubicada en la planta baja. Telnet no es un protocolo seguro. Sin embargo, en esta práctica de laboratorio lo usará para probar el acceso remoto. Toda la información enviada por Telnet, incluidos los comandos y las contraseñas, se envían durante la sesión como texto no cifrado. En las prácticas de laboratorio posteriores, utilizará Shell seguro (SSH) para acceder a los dispositivos de red en forma remota.

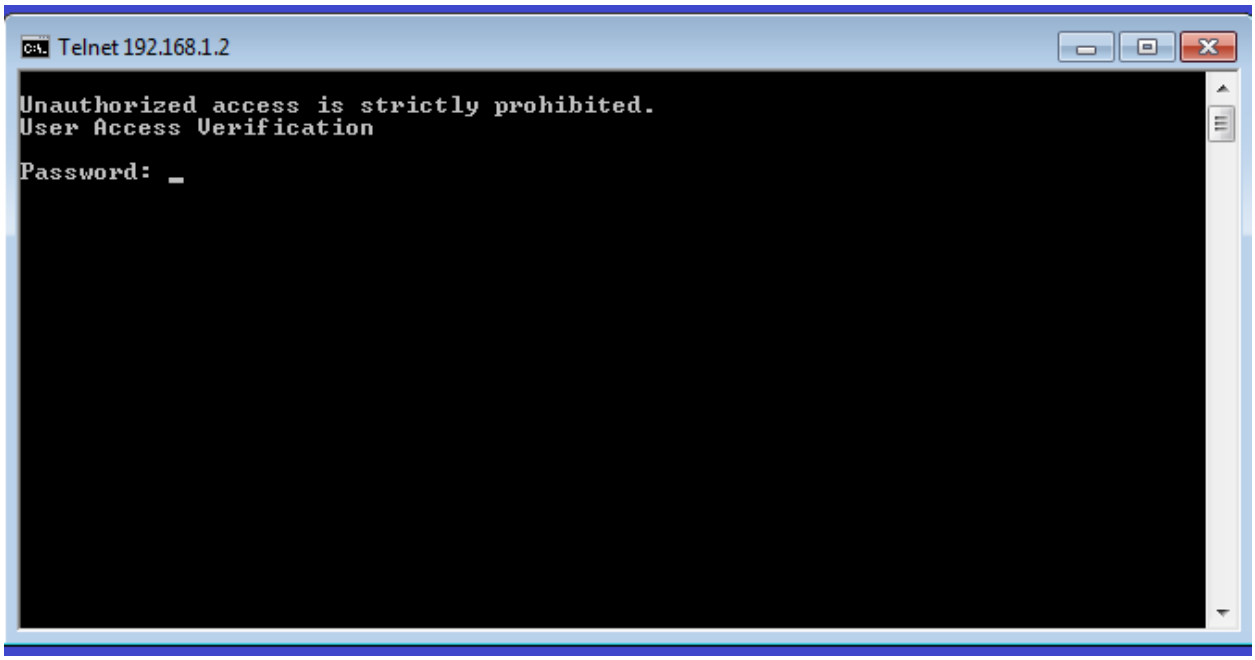
Nota: Windows 7 no admite Telnet en forma nativa. El administrador debe habilitar este protocolo. Para instalar el cliente Telnet, abra una ventana del símbolo del sistema y escriba **pkgmgr /iu:"TelnetClient"**.

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


a. Con la ventana del símbolo del sistema 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\NetAcad> telnet 192.168.1.2
```

El resultado debe ser similar a la siguiente pantalla:



b. Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Escriba **enable** en la petición de entrada. Introduzca la contraseña **class** para ingresar al modo EXEC privilegiado y para emitir un comando **show run**.

Paso 4: Guardar el archivo de configuración

a. Desde la sesión de Telnet, emita el comando **copy run start** en la petición de entrada.

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

b. Salga de la sesión de Telnet escribiendo **quit**. Volverá al símbolo del sistema de Windows 7.

Reflexión

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

_____

Todavía no se configuró ningún parámetro de direccionamiento IP. Cuando un switch se pone en servicio por primera vez, no tiene conectividad de red configurada.

Configuraciones de dispositivos

Switch S1 (completo)

```
S1#show run
Building configuration...
!
Current configuration : 1508 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no 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
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
```



```
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password cisco
 login
line vty 0 4
```



```
 password class
 login
line vty 5 15
 login
!
end
```

