

Packet Tracer - Configuración básica del conmutador - Modo físico

Topología

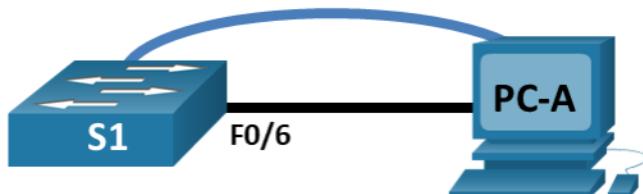


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP / Prefijo
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
PC-A	NIC	192.168.1.10 /24
		2001:db8:acad:1::10 /64

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

Parte 3: Verificar y probar la conectividad de red

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 conmutador 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 usará una dirección IP de administración para la administración remota del conmutador. La topología consta de un conmutador y un dispositivo que solo usa puertos Ethernet y de consola. Verificará la conectividad de red y administrará una tabla de direcciones MAC utilizando dos dispositivos finales.

Instrucciones

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. Desde el estante, haga clic y arrastre el interruptor **S1** y colóquelo en el lado izquierdo de la tabla.
- b. Desde el estante, haga clic y arrastre el dispositivo **PC-A** y colóquelo en el lado derecho de la mesa. Encienda el PC-A.
- c. Conecte un cable de consola desde el dispositivo **PC-A** al conmutador **S1**, como se muestra en la topología. No conecte el cable de red a dispositivo PC-A en este momento.
- d. En la pestaña **Escritorio** de PC-A, utilice **Terminal** para conectarse al conmutador.

¿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?

Para poder realizar la configuracion inicial ya que Telnet o SSH no estan abilitados

Por que el switch aun no tiene una configuracion para poder acceder por 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 conmutador 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 actividad.

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 conmutador no tenía almacenado un archivo de configuración en la memoria de acceso aleatorio no volátil (NVRAM), una conexión de consola mediante **Terminal** abrirá la línea de comandos del modo EXEC del usuario en el conmutador con el comienzo de línea **conmutador>**. Use el comando **enable** para ingresar al modo EXEC privilegiado.
Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.
- b. Verifique que haya un archivo de configuración predeterminado limpio en el conmutador emitiendo el comando **show running-config** privileged EXEC mode command. Examine el archivo de configuración activa actual.

¿Cuántas interfaces GigabitEthernet tiene el conmutador?

28

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

0 - 4

- 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?

Porque el switch es nuevo

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

```
Switch# show interface vlan1
```

¿Hay alguna dirección IP asignada a VLAN 1?

No

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

0060.2fde.172d

¿Está activa esta interfaz?

No

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

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

¿Qué resultado ve?

- f. Conecte un cable Ethernet de **PC-A** a GigabitEthernet1/0/6 en el conmutador. Aguarde un momento para que el switch y la computadora negocien los parámetros de dúplex y velocidad. Examine las propiedades IP de la VLAN 1 SVI.

¿Qué resultado ve?

%LINK-5-CHANGED: Interface GigabitEthernet1/0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up

- g. Ingrese al modo de configuración global y active la interfaz SVI VLAN 1.

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

¿Qué resultado ve?

- i. 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?

16.3.2

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

CAT3K_CAA-UNIVERSALK9

¿Cuál es la dirección MAC base de este conmutador?

00:60:2F:DE:17:2D

- j. Examine las propiedades predeterminadas de la interfaz GigabitEthernet1/0/6 que usa la PC-A.

```
conmutador# show interface gig1/0/6
```

¿La interfaz está activa o inactiva?

Activa

¿Qué haría que una interfaz se desactive?

Aplicando el comando no shut down

¿Cuál es la dirección MAC de la interfaz?

000c.8589.1806

¿Cuál es la configuración de velocidad y de dúplex de la interfaz? 100MB/s, full duplex

- k. Examine la configuración VLAN configuración del switch.

conmutador# **show vlan**

¿Cuál es el nombre de la VLAN 1?

Default

¿Qué puertos están en VLAN 1?

Los 28 Gig1/01 - Gig1/0/24 y Gig1/1/1-Gig1/1/4

¿La VLAN 1 está activa?

Si

¿Qué tipo de VLAN es la VLAN predeterminada?

Ethernet

- l. Examine la memoria flash.

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

conmutador# **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?

cat3k_caa-universalk9.16.03.02.SPA.bin

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 conmutador. 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 conmutador en 192.168.1.2 con la máscara de subred 255.255.255.0 en la interfaz virtual interna VLAN 99. Una dirección IPv6 también se puede configurar en la interfaz SVI. Utilice las direcciones IPv6 que figuran en la **tabla de direccionamiento**.

Observe que la interfaz VLAN 99 está en estado down (abajo), 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.

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. Después de unos segundos, la VLAN 99 pasa al estado up porque ahora se le asigna al menos un puerto activo (Fa0/6 con la **PC-A** conectada).

- d. Emita el comando **show vlan brief** verificar que todos los puertos estén en VLAN 99.
- e. Configure la puerta de enlace predeterminada 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.
- 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
```

- g. Configure las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet. Si no configura una contraseña vty, no podrá usar Telnet para acceder al conmutador.

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

Para que entren en funcionamiento

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 para que funcione; sin embargo, usted debe ingresar **192.168.1.1** y **fe80::1** para simular un enrutador conectado a **S1**.

- a. Navegue a la pestaña **Escritorio** (Desktop).
- b. Haga clic en **IP Configuration** (Configuración de IP).
- c. Compruebe que el botón Configuración de IP **estática** esté seleccionado.
- d. Introduzca la dirección IPv4 (IP Address), Subnet Mask (Máscara de subred), y Default Gateway (puerta de enlace predeterminado).
- e. Compruebe que el botón Configuración de IPv6 **estática** esté seleccionado.
- f. Introduzca la dirección IPv6, el prefijo y la puerta de enlace predeterminada
- g. Haga clic en **X** para cerrar la ventana **IP Configuration**.

Parte 3: Verificar y probar la conectividad de red

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

Paso 1: Mostrar la configuración del switch

Use la conexión de la consola en **PC-A** para mostrar y verificar la configuración del conmutador. 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. 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 : 2424 bytes
!
version 16.3.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil!
no ip cef
no ipv6 cef
!
!
no ip domain-lookup
!
<output omitted>
!
interface GigabitEthernet1/0/6
switchport access vlan 99
!
<output omitted>
!
interface GigabitEthernet1/0/24
switchport access vlan 99
!
<output omitted>
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan99
  mac-address 00e0.f795.d201
  ip address 192.168.1.2 255.255.255.0
  ipv6 address FE80::2 link-local
  ipv6 address 2001:DB8:ACAD:1::2/64
!
ip default-gateway 192.168.1.1
ip classless
```

```
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
password 7 0822455D0A16
logging synchronous
login
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
password 7 0822455D0A16
login
!
end
```

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

S1# show interface vlan 99

¿Cuál es el ancho de banda en esta interfaz?

BW 100000 Kbit

¿Cuál es el estado de la VLAN 99?

Activa Up

¿Cuál es el estado del protocolo de línea?

line protocol is up

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

Compruebe que PC-A puede hacer ping a la dirección IPv4 e IPv6 para S1.

```
C:\> ping 192.168.1.2
C:\ > ping 2001:db8:acad: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 actividad, 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 conmutador **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 como texto no cifrado. En las siguientes actividades, usará SSH para acceder a los dispositivos de red en forma remota.

- Abra la pestaña **Escritorio** en **PC-A**.
- Desplácese hacia abajo en la lista de aplicaciones y haga clic en **Telnet/SSH Client**.
- Establezca el **tipo de conexión** como **Telnet**.

- d. Introduzca la dirección de administración de SVI para conectarse a S1 y haga clic en **Conectar**.
- e. 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**.
- f. Guarde la configuración.
- g. Escriba **exit** para finalizar la sesión de Telnet. Haga clic en **No** en la ventana emergente.

Paso 4: Implemente el conmutador S1 en la red de producción.

Ahora instalará el conmutador **S1** en la red de producción y desconectará el cable de la consola. Telnet se utilizará para acceder de forma remota al conmutador y completar cualquier configuración y verificación adicionales. En las siguientes actividades, usará SSH para acceder a los dispositivos de red en forma remota.

- a. Mueva el conmutador **S1** al **rack**.
- b. Haga clic con el botón derecho en el conmutador **S1** y seleccione **Inspeccionar parte posterior** (Inspect Rear).
- c. Haga clic y arrastre el **cable de la consola** hasta la **tablero de cables**.

Preguntas de reflexión

1. ¿Por qué debería configurar la contraseña de vty del switch?

La líneas VTY permiten el acceso remoto si no se configura una contraseña, cualquiera podría entrar

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

La VLAN 1 es la predeterminada, cambiarla reduce los riesgos de seguridad.

3. ¿Cómo puede evitar que las contraseñas se envíen en texto sin cifrado?

Usando SSH en lugar de telnet