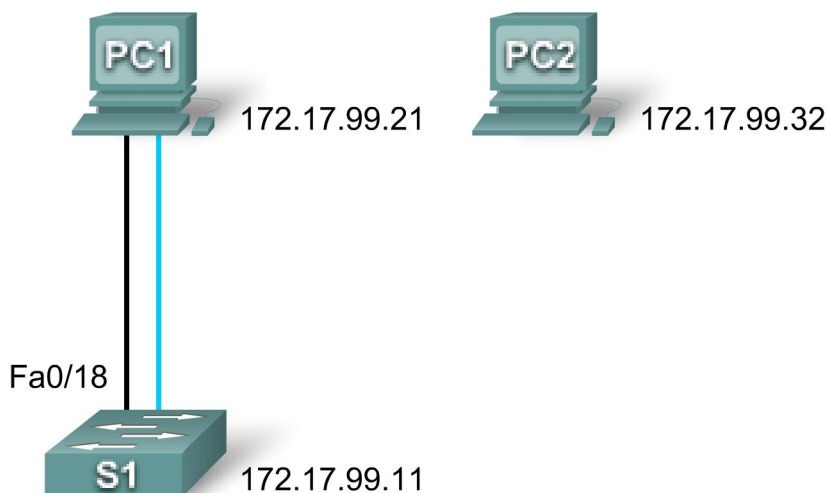


## Actividad del Packet Tracer 2.5.1: Configuración básica del switch

### Topología



**NOTA PARA EL USUARIO:** Esta actividad es una variación de la Práctica de laboratorio 2.5.1. Packet Tracer puede no admitir todas las tareas especificadas en la práctica de laboratorio. Esta actividad no debe considerarse equivalente a la realización del laboratorio práctico. Packet Tracer no sustituye la experiencia de las prácticas de laboratorio con equipos reales.

### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.1
PC2	NIC	172.17.99.22	255.255.255.0	172.17.99.1
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

### Objetivos de aprendizaje

- Borrar una configuración existente en un switch.
- Verificar la configuración predeterminada del switch.
- Crear una configuración básica de switch.
- Administrar la tabla de direcciones MAC.
- Configurar la seguridad de puertos.

## Introducción

En esta actividad, se examinará y configurará un switch LAN independiente. Pese a que el switch realiza funciones básicas en su estado predeterminado de manera no convencional, existe una cantidad de parámetros que un administrador de red debe modificar para garantizar una LAN segura y optimizada. En esta actividad se presentan los principios básicos de la configuración de switches.

### Tarea 1: Borrar una configuración existente de un switch

#### Paso 1: Ingrese al modo EXEC privilegiado escribiendo el comando **enable**.

Haga clic en S1 y luego en la ficha **CLI**. Ejecute el comando **enable** para entrar al modo EXEC privilegiado.

```
Switch>enable
Switch#
```

#### Paso 2: Elimine el archivo de información de la base de datos de la VLAN.

La información de la base de datos de la VLAN se almacena por separado de los archivos de configuración en `vlan.dat` de la memoria flash. Para quitar el archivo VLAN, ejecute el comando **delete flash:vlan.dat**.

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

#### Paso 3: Elimine el archivo de configuración de inicio del switch de la NVRAM.

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

#### Paso 4: Verifique que la información de la VLAN se haya eliminado.

Verifique con el comando **show vlan** que la configuración de la VLAN se haya eliminado.

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	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
10	VLAN10	active	
30	VLAN30	active	
1002	fddi-default	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

La información de la VLAN aún está en el switch. Siga el paso a continuación para borrarla.

### Paso 5: Vuelva a cargar el switch.

En el indicador del modo EXEC privilegiado, introduzca el comando **reload** para comenzar el proceso.

```
Switch#reload
```

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

```
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
```

<se omite el resultado>

```
Press RETURN to get started! [Enter]
```

```
Switch>
```

## Tarea 2: Verificar la configuración predeterminada de un switch

### Paso 1: Ingrese al modo privilegiado.

Puede acceder a todos los comandos del switch en modo privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado. El conjunto de comandos privilegiados incluye aquellos comandos del modo EXEC del usuario, así como el comando **configure** a través del cual se obtiene acceso a los modos de comando restantes.

```
Switch>enable
```

```
Switch#
```

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

### Paso 2: Examine la configuración actual del switch.

- a. Examine la configuración en ejecución actual mediante el comando **show running-config**.

1. ¿Cuántas interfaces Fast Ethernet tiene el switch? \_\_\_\_\_
2. ¿Cuántas interfaces Gigabit Ethernet tiene el switch? \_\_\_\_\_
3. ¿Cuál es el rango de valores que se muestra para las líneas vty?  
\_\_\_\_\_

- b. Examine el contenido actual de la NVRAM ejecutando el comando **show startup-config**.

1. ¿Por qué el switch emite esta respuesta?  
\_\_\_\_\_

- c. Analice las características de la interfaz virtual VLAN1 ejecutando el comando **show interface vlan1**.

1. ¿Hay una dirección IP establecida en el switch? \_\_\_\_\_
2. ¿Cuál es la dirección MAC de esta interfaz virtual del switch? \_\_\_\_\_
3. ¿Está activa esta interfaz? \_\_\_\_\_

- d. Ahora consulte las propiedades IP de la interfaz mediante **show ip interface vlan1**.

1. ¿Qué resultado ve?  
\_\_\_\_\_

### Paso 3: Muestre la información IOS de Cisco.

- a. Visualice la información de IOS de Cisco mediante el comando **show version**.

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

\_\_\_\_\_

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

\_\_\_\_\_

3. ¿Cuál es la dirección MAC base de este switch?

\_\_\_\_\_

### Paso 4: Examine las interfaces Fast Ethernet.

- a. Examine las propiedades predeterminadas de la interfaz Fast Ethernet que utiliza PC1 mediante el comando **show interface fastethernet 0/18**.

```
Switch#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
```

<se omite el resultado>

1. ¿La interfaz está activa o desactivada? \_\_\_\_\_
2. ¿Qué haría que una interfaz se active? \_\_\_\_\_
3. ¿Cuál es la dirección MAC de la interfaz? \_\_\_\_\_
4. ¿Cuál es la configuración de velocidad y de dúplex de la interfaz? \_\_\_\_\_

### Paso 5: Examine la información de la VLAN.

- a. Examine la configuración predeterminada de la VLAN del switch mediante el comando **show vlan**.

1. ¿Cuál es el nombre de la VLAN 1? \_\_\_\_\_
2. ¿Qué puertos hay en esta VLAN? \_\_\_\_\_
3. ¿La VLAN 1 está activa? \_\_\_\_\_
4. ¿Qué tipo de VLAN es la VLAN predeterminada? \_\_\_\_\_

### Paso 6: Examine la memoria flash.

- a. Hay dos comandos para analizar la memoria flash: **dir flash:** o **show flash**. Ejecute uno de los dos comandos para examinar el contenido del directorio flash.

1. ¿Qué archivos o directorios se encuentran?

\_\_\_\_\_

### Paso 7: Examine y guarde el archivo de configuración de inicio.

Anteriormente en el paso 2, se observó que el archivo de configuración de inicio no existía. Realice un cambio en la configuración del switch y luego guárdelo. Escriba los siguientes comandos:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
```

Para guardar el contenido del archivo de configuración en ejecución en la RAM no volátil (NVRAM), ejecute el comando **copy running-config startup-config**.

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

Ahora consulte el contenido de la NVRAM. La configuración actual se ha escrito en la NVRAM.

## Tarea 3: Crear una configuración básica de switch

### Paso 1: Asigne un nombre al switch.

Ingrese el modo de configuración global. El modo de configuración le permite administrar el switch. Ingrese los comandos de configuración, uno en cada línea. Observe que el indicador de la línea de comandos cambia para reflejar el indicador actual y el nombre del switch. En el último paso de la tarea anterior, usted configuró el nombre de host. A continuación encontrará un resumen de los comandos utilizados.

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

### Paso 2: Configure las contraseñas de acceso.

Entre al modo de **configuración de línea** para la consola. Establezca **cisco** como contraseña para iniciar sesión. También configure las líneas vty 0 a 15 con la contraseña **cisco**.

```
S1#configure terminal
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

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

### Paso 3: Configure las contraseñas del modo de comando.

Establezca la contraseña secreta de enable como class.

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

#### Paso 4: Configure la dirección de la capa 3 del switch.

Configure la dirección IP del switch en 172.17.99.11 con una máscara de subred de 255.255.255.0 en la interfaz virtual interna VLAN 99. La VLAN se debe crear primero en el switch antes de que se pueda asignar la dirección.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

#### Paso 5: Asigne puertos a la VLAN del switch.

Asigne Fastethernet 0/1, 0/8 y 0/18 a puertos a la VLAN 99.

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#interface fa0/8
S1(config-if)#switchport access vlan 99
S1(config-if)#interface fa0/18
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

#### Paso 6: Establezca el gateway predeterminado del switch.

S1 es un switch de Capa 2, por lo tanto toma decisiones de envío en base al encabezado de la Capa 2. Si se conectan múltiples redes a un switch, es necesario que especifique cómo el switch envía las tramas de internetwork, ya que la ruta se debe determinar en la capa tres. Esto se lleva a cabo al especificar una dirección de gateway predeterminado dirigida a un router o al switch de la capa 3. 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 172.17.99.1, establezca el gateway predeterminado para el switch.

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

#### Paso 7: Verifique la configuración de administración de las LAN.

Verifique la configuración de interfaz de la VLAN 99 mediante el comando **show interface vlan 99**.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.47ac.1eb8 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 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 21:40:21, output never, 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
<Se omite el resultado>
```

¿Cuál es el ancho de banda en esta interfaz? \_\_\_\_\_

¿Cuál es la estrategia para formar las colas? \_\_\_\_\_

### Paso 8: Configure la dirección IP y el gateway predeterminado para PC1.

Establezca la dirección IP de la PC1 en 172.17.99.21 con una máscara de subred 255.255.255.0. Configure un gateway predeterminado de 172.17.99.11. Haga clic en PC1 y en su ficha **Desktop**, luego, en IP Configuration para introducir los parámetros de direccionamiento.

### Paso 9: Verifique la conectividad.

Para verificar que los hosts y los switches estén configurados correctamente, haga ping en el switch desde PC1.

Si el ping no tuviera éxito, realice la resolución de problemas en la configuración del switch y del host. Observe que pueden ser necesarios varios intentos para que los pings tengan éxito.

### Paso 10: Configure la velocidad del puerto y la configuración de dúplex para una interfaz Fast Ethernet.

Realice la configuración de velocidad y dúplex en Fast Ethernet 0/18. Utilice el comando **end** para regresar al modo EXEC privilegiado al finalizar.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
```

El valor predeterminado en la interfaz Ethernet del switch es de detección automática, por lo tanto negocia automáticamente las configuraciones óptimas. Usted debe establecer el modo dúplex y la velocidad manualmente sólo si un puerto debe funcionar a una cierta velocidad y en modo dúplex. Configurar puertos en forma manual puede conducir a una falta de concordancia en el dúplex, lo cual puede disminuir el rendimiento en forma significativa.

Observe cómo el enlace entre PC1 y S1 se desactivó. Quite los comandos **speed 100** y **duplex full**. Ahora verifique la configuración de la interfaz Fast Ethernet mediante el comando **show interface fa0/18**.

```
S1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
<Se omite el resultado>
```

### Paso 11: Guarde la configuración.

Ha completado la configuración básica del switch. Ahora haga una copia de seguridad del archivo de configuración en ejecución a NVRAM para garantizar que los cambios que se han realizado no se pierdan si el sistema se reinicia o se apaga.

```
S1#copy running-config startup-config

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

### Paso 12: Examine el archivo de configuración de inicio.

Para ver la configuración que se guarda en la NVRAM, ejecute el comando **show startup-config** en el modo EXEC privilegiado (modo enable).

¿Todos los cambios realizados están grabados en el archivo?

## Tarea 4: Administrar la tabla de direcciones MAC

### Paso 1: Anote las direcciones MAC de los hosts.

Determine y anote las direcciones de la capa 2 (física) de las tarjetas de interfaz de red de la PC utilizando los siguientes pasos:

- Haga clic en el equipo PC.
- Seleccione la ficha **Desktop**.
- Haga clic en **Command Prompt**.
- Escriba el comando **ipconfig /all**.

### Paso 2: Determine las direcciones MAC que el switch ha adquirido.

Muestre las direcciones MAC utilizando el comando **show mac-address-table** en modo EXEC privilegiado. Si no hay direcciones MAC; haga ping desde PC1 a S1, y luego verifique nuevamente.

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

### Paso 3: Borre la tabla de direcciones MAC.

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

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

### Paso 4: Verifique los resultados.

Verifique que la tabla de direcciones MAC esté en blanco.

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

### Paso 5: Examine de nuevo la tabla MAC.

Observe la tabla de direcciones MAC nuevamente en el modo EXEC privilegiado. La tabla no se ha modificado, haga ping a S1 desde PC1 y verifique nuevamente.

### Paso 6: Configure una dirección MAC estática.

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

Configure una dirección MAC estática en la interfaz Fast Ethernet 0/18 con la dirección guardada para PC1 en el Paso 1 de esta tarea, 0002.16E8.C285.

```
S1(config)#mac-address-table static 0002.16E8.C285 vlan 99 interface  
fastethernet 0/18  
S1(config)#end
```

### Paso 7: Verifique los resultados.

Verifique las entradas de la tabla de direcciones MAC.

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



### Paso 8: Elimine la entrada MAC estática.

Entre al modo de configuración y quite la MAC estática colocando un **no** al principio de la cadena de comandos.

```
S1(config)#no mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
S1(config)#end
```

### Paso 9: Verifique los resultados.

Verifique que la dirección MAC estática se haya borrado mediante el comando **show mac-address-table static**.

## Tarea 5: Configurar la seguridad del puerto

### Paso 1: Configure un segundo host.

Para esta tarea es necesario un segundo host. Establezca la dirección IP de PC2 en 172.17.99.22, con una máscara de subred de 255.255.255.0 y un gateway predeterminado de 172.17.99.11. No conecte aún esta PC al switch.

### Paso 2: Verifique la conectividad.

Verifique que la PC1 y el switch aún están correctamente configurados haciendo ping a la dirección IP de la VLAN 99 del switch desde el host. Si los pings no tuvieran éxito, realice la resolución de problemas en la configuración del switch y del host.

### Paso 3: Determine las direcciones MAC que el switch ha adquirido.

Muestre las direcciones MAC aprendidas utilizando el comando **show mac-address-table** en modo EXEC privilegiado.

### Paso 4: Enumere las opciones de seguridad de los puertos.

Explore las opciones para configurar la seguridad de los puertos en la interfaz Fast Ethernet 0/18.

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
    mac-address      Secure mac address
    maximum          Max secure addresses
    violation         Security violation mode
    <cr>
```

### Paso 5: Configure la seguridad de los puertos en un puerto de acceso.

Configure el puerto Fast Ethernet 0/18 del switch para que acepte sólo dos dispositivos, para que adquiera las direcciones MAC de esos dispositivos en forma dinámica y para que desactive el puerto en caso de violación.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#exit
```

### Paso 6: Verifique los resultados.

Muestre la configuración de seguridad del puerto mediante el comando **show port-security interface fa0/18**.

¿Cuántas direcciones seguras están permitidas en Fast Ethernet 0/18?

¿Qué medida de seguridad debe tomarse para este puerto?

### Paso 7: Examine el archivo de configuración en ejecución.

S1#**show running-config**

¿Hay afirmaciones enumeradas que reflejan directamente la implementación de seguridad de la configuración en ejecución?

### Paso 8: Modifique las configuraciones de seguridad de los puertos en un puerto.

En la interfaz Fast Ethernet 0/18, cambie a 1 el conteo máximo de direcciones MAC de seguridad de los puertos.

```
S1(config-if)#switchport port-security maximum 1
```

### Paso 9: Verifique los resultados.

Muestre la configuración de seguridad del puerto mediante el comando **show port-security interface fa0/18**.

¿Las configuraciones de seguridad de los puertos reflejan las modificaciones del Paso 8?

Haga ping en la dirección VLAN99 del switch desde la PC1 para verificar la conectividad y actualizar la tabla de direcciones MAC.

### Paso 10: Introduzca un host malicioso.

Desconecte el equipo PC conectado a Fast Ethernet 0/18 desde el switch. Conecte PC2, que tiene asignada la dirección IP 172.17.99.22, al puerto Fast Ethernet 0/18. Haga ping a la dirección 172.17.99.11 de la VLAN 99 desde el nuevo host.

¿Que sucedió cuando intentó hacer ping en S1?

Nota: La convergencia puede tardar hasta un minuto. Alterne entre los modos de **simulación** y **tiempo real** para acelerar la convergencia.

### Paso 11: Reactive el puerto.

Siempre y cuando el host no autorizado ni permitido esté conectado a Fast Ethernet 0/18, no pasará ningún tráfico entre el host y el switch. Vuelva a conectar PC1 a Fast Ethernet 0/18 e introduzca los siguientes comandos en el switch para reactivar el puerto.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#no shutdown
S1(config-if)#end
```

### Paso 12: Verifique la conectividad.

Después de la convergencia, PC1 debe estar en condiciones de hacer ping nuevamente en S1.

### Paso 13: Verifique los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.