

Acceda a una CLI del switch Cisco Business serie 350 mediante SSH o Telnet

Objetivo

Los switches gestionados Cisco Small Business se pueden acceder y configurar de forma remota a través de la interfaz de línea de comandos (CLI). El acceso a la CLI permite ingresar comandos en una ventana basada en terminal. Si prefiere configurar el uso de comandos de terminal en su switch a través de la CLI en lugar de la utilidad basada en Web, esta sería una alternativa más fácil. Algunas tareas como la habilitación del modo de Capa 3 sólo se pueden realizar a través de la CLI.

Para acceder remotamente a la CLI de su switch, debe utilizar un cliente SSH o Telnet. También debe activar el servicio Telnet y SSH en su switch antes de poder acceder a él de forma remota.

Nota: Para obtener instrucciones sobre cómo configurar los parámetros de protocolo de control de transmisión (TCP) y protocolo de datagramas de usuario (UDP) en el switch, haga clic [aquí](#).

En este artículo se proporcionan instrucciones sobre cómo acceder a la CLI de su switch a través de SSH o Telnet mediante los siguientes clientes:

- PuTTY: cliente estándar de Telnet y SSH. Puede descargar un instalador [aquí](#) e instalarlo en su equipo con Windows.
- Terminal: aplicación preinstalada en cada equipo Mac OS X. También se conoce como shell o consola.

Importante: Antes de realizar una conexión SSH o Telnet al switch, debe establecer la dirección IP para el switch. Para obtener instrucciones, haga clic [aquí](#).

Dispositivos aplicables | Versión de software

- CBS250 ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))
- CBS350 ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))
- CBS350-2X ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))
- CBS350-4X ([Ficha técnica](#)) | 3.0.0.69 ([Descargar última](#))

Acceso a la CLI del switch a través de SSH

Las sesiones SSH se desconectan automáticamente después de que haya pasado el tiempo de inactividad configurado en el switch. El tiempo de espera de sesión inactivo predeterminado para SSH es de 10 minutos.

Para realizar una conexión SSH al switch, elija su plataforma:

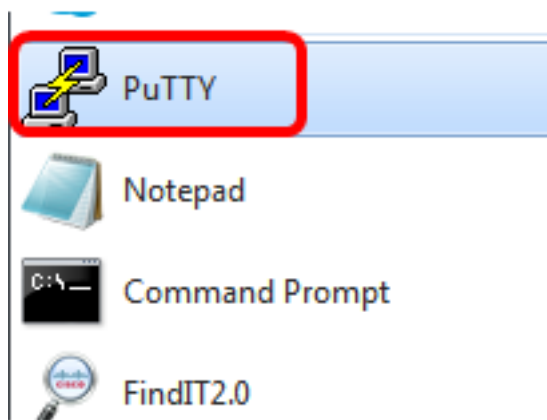
[Equipo de Windows con PuTTY](#)

[Ordenador Mac con Terminal](#)

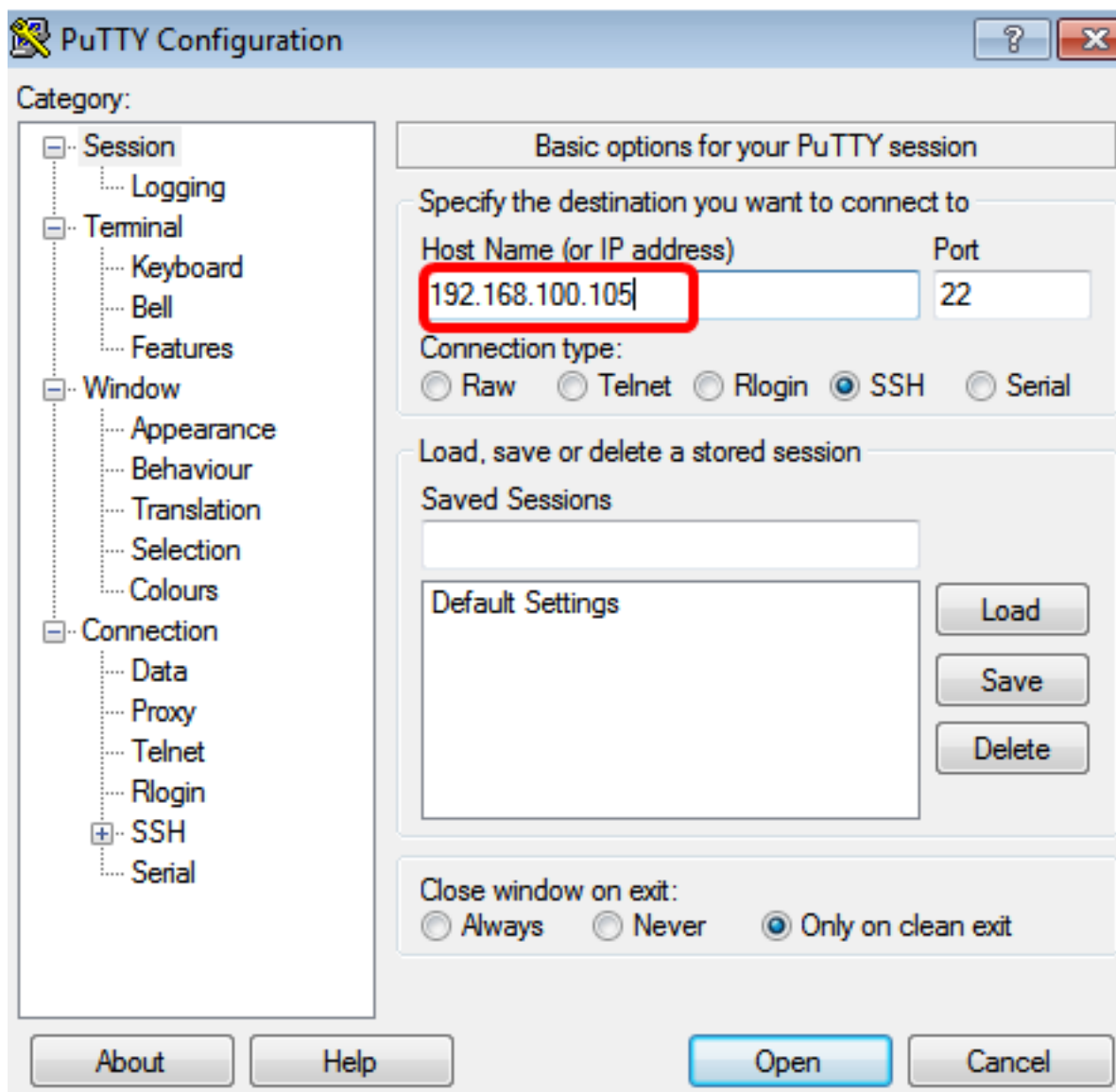
[Acceda a la CLI a través de SSH mediante PuTTY](#)

Nota: Las imágenes pueden variar según la versión del sistema operativo Windows que esté utilizando. En este ejemplo, se utiliza Windows 7 Ultimate y la versión PuTTY es 0.63.

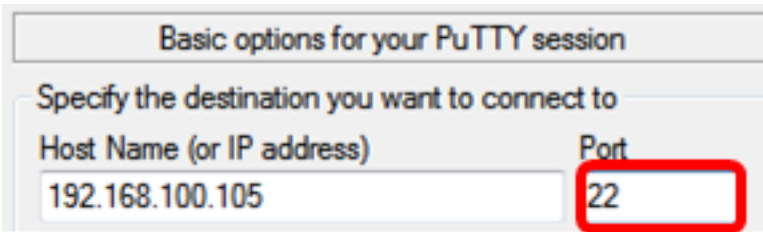
Paso 1. Inicie el cliente PuTTY en el equipo.



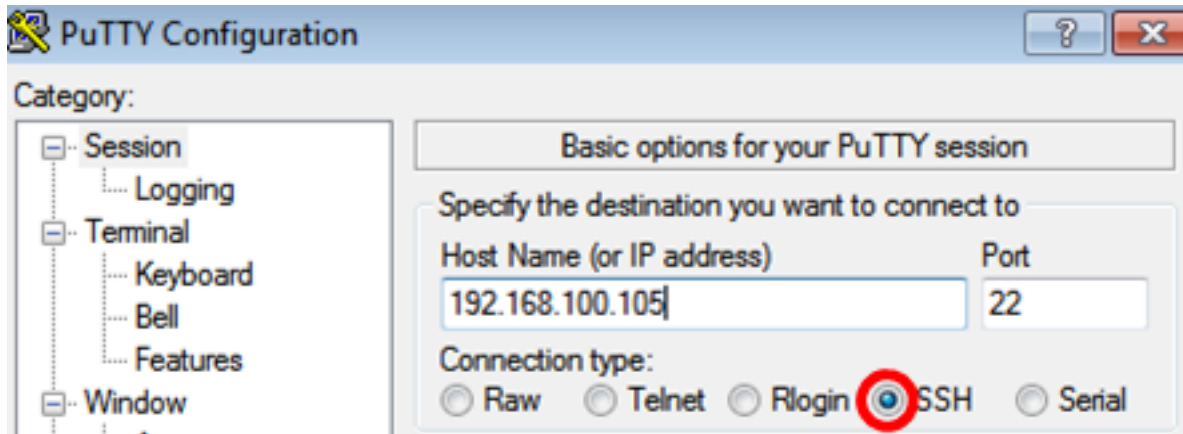
Paso 2. Introduzca el nombre de host o la dirección IP del switch al que desea acceder de forma remota en el campo *Host Name (o IP address)*.



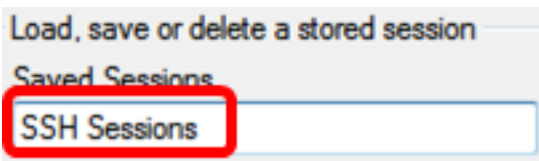
Paso 3. Ingrese **22** como el número de puerto que se utilizará para la sesión SSH en el campo *Port*.



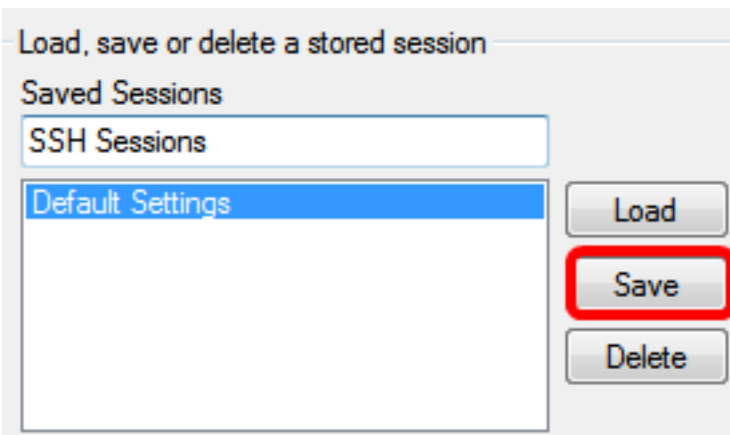
Paso 4. En el área Tipo de conexión, haga clic en el botón de opción **SSH** para elegir SSH como método de conexión con el switch.



Paso 5. (Opcional) Para guardar la sesión, introduzca el nombre de la sesión en el campo *Sesiones guardadas*.



Paso 6. Haga clic en **Guardar** para guardar la sesión.

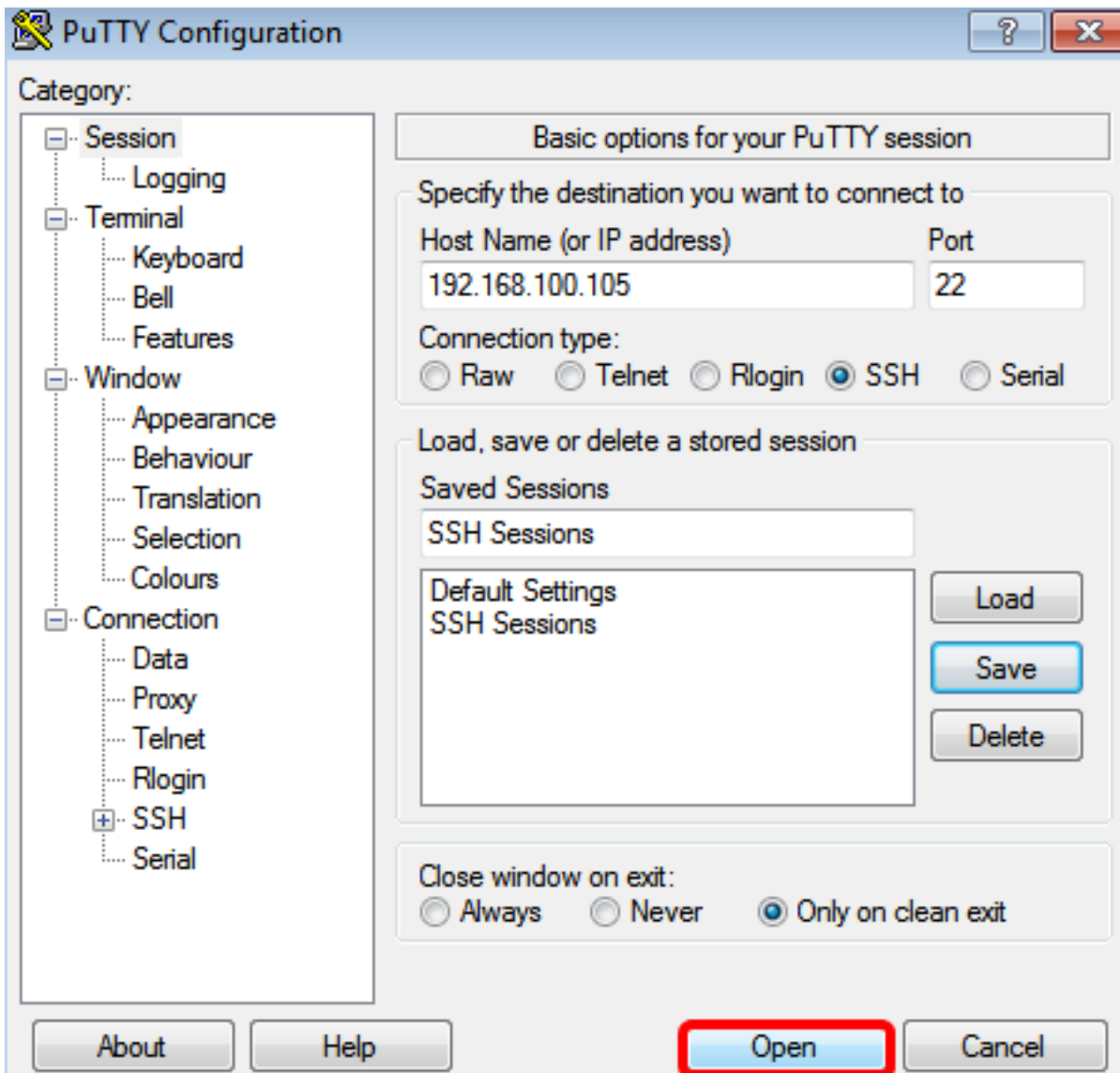


Paso 7. (Opcional) En la ventana Cerrar del área de salida, haga clic en el botón de opción para elegir el comportamiento de la ventana SSH al salir.



Nota: En este ejemplo, sólo se elige al salir limpio.

Paso 8. Haga clic en **Abrir** para iniciar la sesión.



Paso 9. Si es la primera vez que utiliza SSH para conectarse al switch, puede recibir una advertencia de brechas de seguridad. Esta advertencia le permite saber que es posible que se conecte a otro ordenador que pretende ser el switch. Una vez que se haya asegurado de haber introducido la dirección IP correcta en el campo Host Name (Nombre de host) en el paso 4, haga clic en **Yes** para actualizar la clave Rivest Shamir Adleman 2 (RSA2) para incluir el nuevo switch.

PuTTY Security Alert



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:

ssh-rsa 1024 6f:7d:af:33:11:8c:b1:8b:15:3f:b1:ed:45:b9:46:63

If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, hit No.

If you do not trust this host, hit Cancel to abandon the connection.

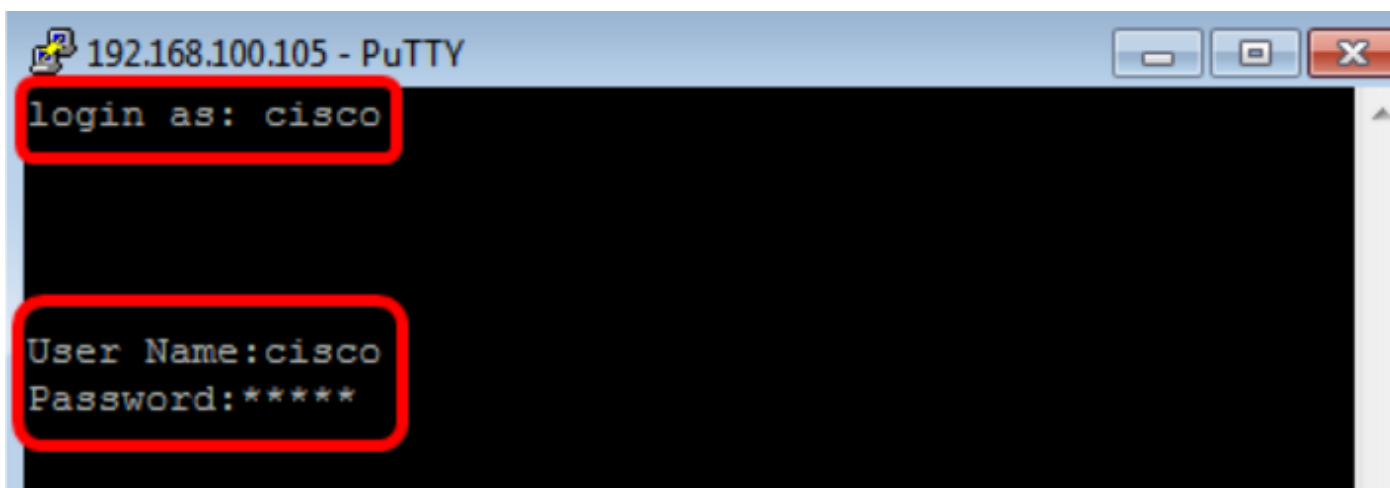
Yes

No

Cancel

Help

Paso 10. Ingrese el nombre de usuario y la contraseña del switch en los campos *login as*, *User Name* y *Password* en consecuencia.



Ahora debería haber accedido con éxito de forma remota a la CLI de su switch a través de SSH mediante PuTTY.

[Acceso a la CLI a través de SSH mediante Terminal](#)

Nota: Las imágenes pueden variar según la versión del sistema operativo del ordenador Mac que esté utilizando. En este ejemplo, se utiliza macOS Sierra y la versión de Terminal es 2.7.1.

Paso 1. Vaya a **Aplicaciones > Utilidades** y luego inicie la aplicación **Terminal.app**.



Paso 2. Ingrese el comando `ssh` y luego la dirección IP para acceder a la CLI del switch.

```
Cisco: ~Cisco$ ssh [ip-address]
```

```
Cisco — ssh 192.168.100.105 — 81x24
```

```
Last login: Thu Jun 15 11:10:09 on ttys001
Cisco:~ Cisco$ ssh 192.168.100.105
The authenticity of host '192.168.100.105 (192.168.100.105)' can't be established.
RSA key fingerprint is SHA256:Uhbwk5NQ7f/10IJnH/PaX3/UuYSy8B6zawW5c7jkm1Y.
Are you sure you want to continue connecting (yes/no)?
```

Nota: En este ejemplo, 192.168.100.105.

Paso 3. Cuando el mensaje le indique si desea continuar conectando, introduzca **Sí**.

```
Cisco — ssh 192.168.100.105 — 83x24
```

```
Last login: Thu Jun 15 11:10:09 on ttys001
Cisco:~ Cisco$ ssh 192.168.100.105
The authenticity of host '192.168.100.105 (192.168.100.105)' can't be established.
RSA key fingerprint is SHA256:Uhbwk5NQ7f/10IJnH/PaX3/UuYSy8B6zawW5c7jkm1Y.
Are you sure you want to continue connecting (yes/no) yes
```

Paso 4. Ingrese el nombre de usuario y la contraseña del switch en los campos *User Name* y *Password* en consecuencia.

```
Cisco — ssh 192.168.100.105 — 83x24
```

```
Last login: Thu Jun 15 11:10:09 on ttys001
Cisco:~ Cisco$ ssh 192.168.100.105
The authenticity of host '192.168.100.105 (192.168.100.105)' can't be established.
RSA key fingerprint is SHA256:Uhbwk5NQ7f/10IJnH/PaX3/UuYSy8B6zawW5c7jkm1Y.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.100.105' (RSA) to the list of known hosts.

User Name:cisco
Password:*****
```

Ahora debería haber accedido con éxito remotamente a la CLI de su switch a través de SSH mediante el Terminal.

Acceda a la CLI del switch a través de Telnet

Las sesiones Telnet se desconectan automáticamente después de que haya pasado el tiempo de inactividad configurado en el switch. El tiempo de espera de sesión inactivo predeterminado para Telnet es de 10 minutos.

Para realizar una conexión Telnet al switch, elija su plataforma:

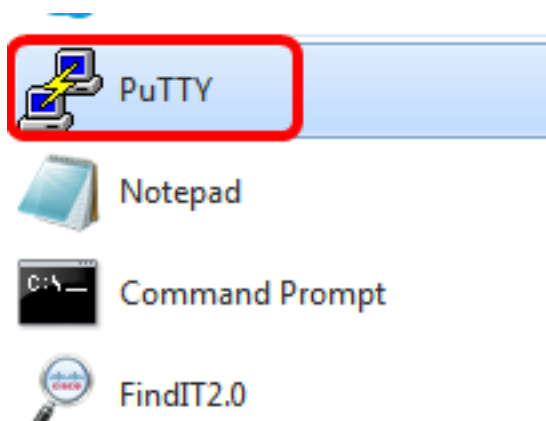
[Equipo de Windows con PuTTY](#)

[Ordenador Mac con Terminal](#)

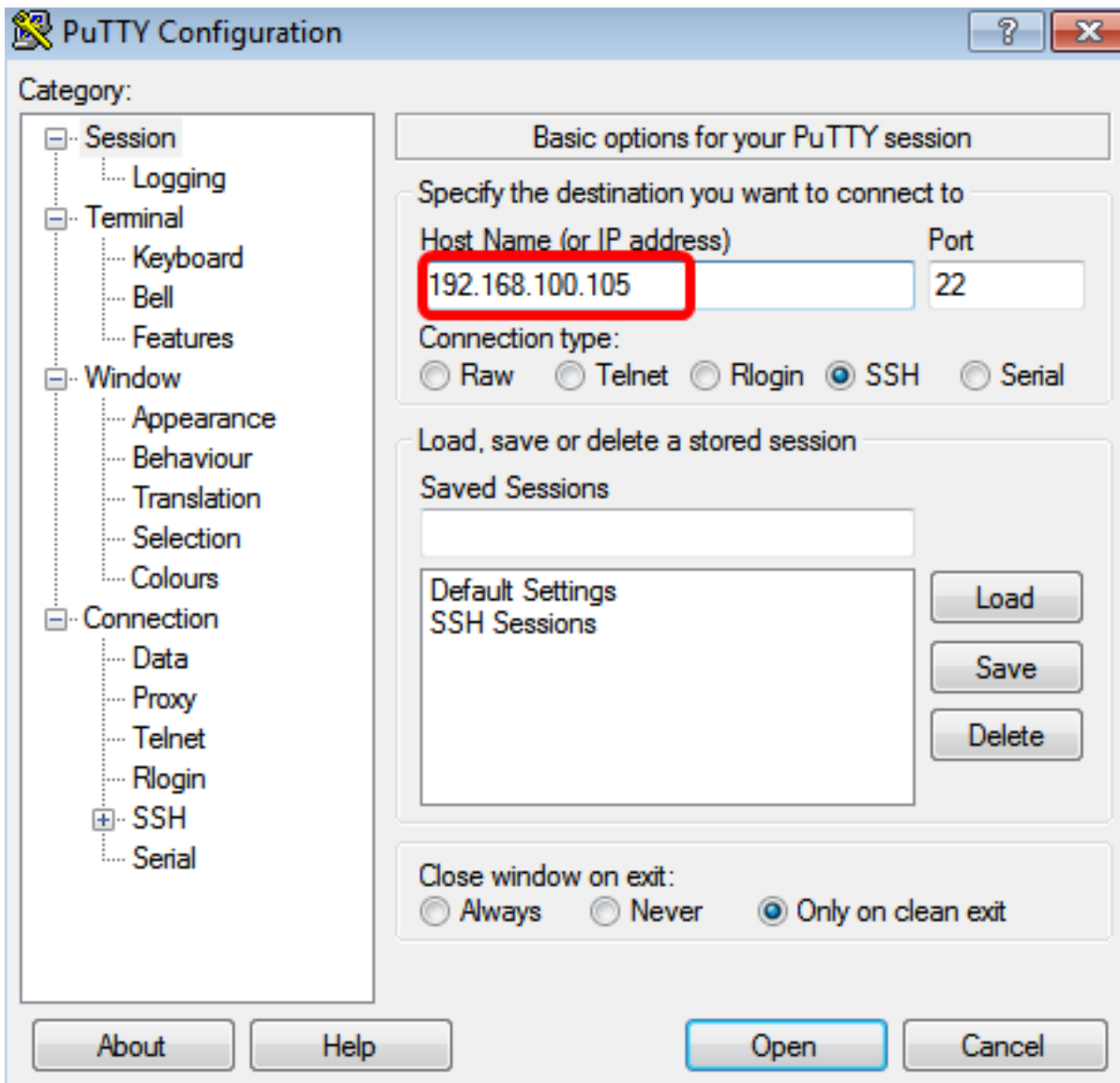
Acceda a la CLI a través de Telnet mediante PuTTY

Nota: Las imágenes pueden variar según la versión del sistema operativo Windows que esté utilizando. En este ejemplo, se utiliza Windows 7 Ultimate y la versión PuTTY es 0.63.

Paso 1. Inicie el cliente PuTTY en el equipo.

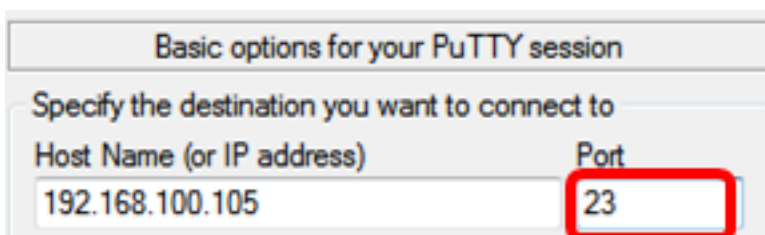


Paso 2. Introduzca el nombre de host o la dirección IP del switch al que desea acceder de forma remota en el campo *Host Name (o IP address)*.

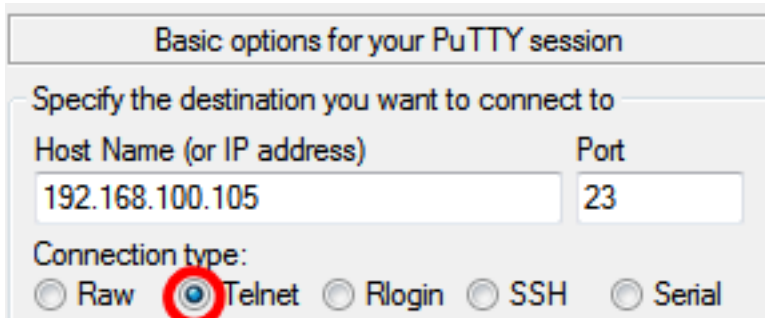


Nota: En este ejemplo, se utiliza 192.168.100.105.

Paso 3. Ingrese **23** como el número de puerto que se utilizará para la sesión Telnet en el campo Port (Puerto).

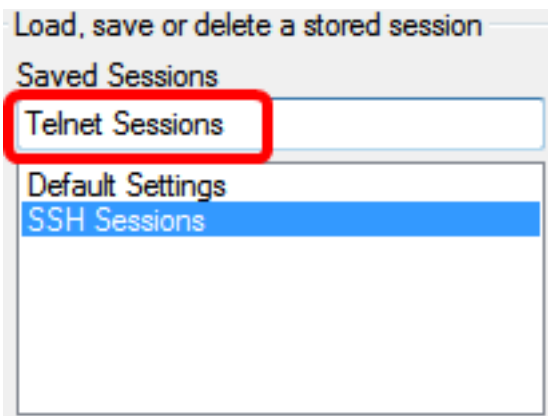


Paso 4. En el área Tipo de conexión, haga clic en el botón de opción **Telnet** para elegir Telnet como método de conexión con el switch.



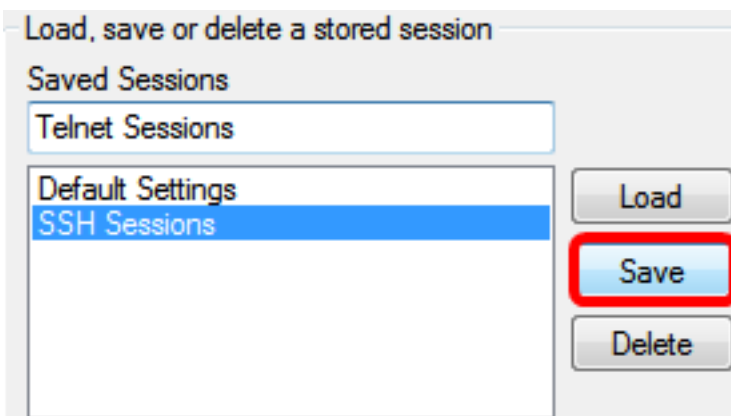
Paso 5. (Opcional) Para guardar la sesión, introduzca el nombre de la sesión en el campo

Sesiones guardadas.

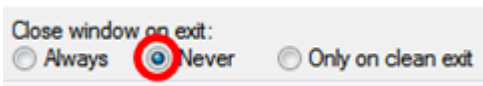


Nota: En este ejemplo, se utilizan sesiones Telnet.

Paso 6. Haga clic en **Guardar** para guardar la sesión.

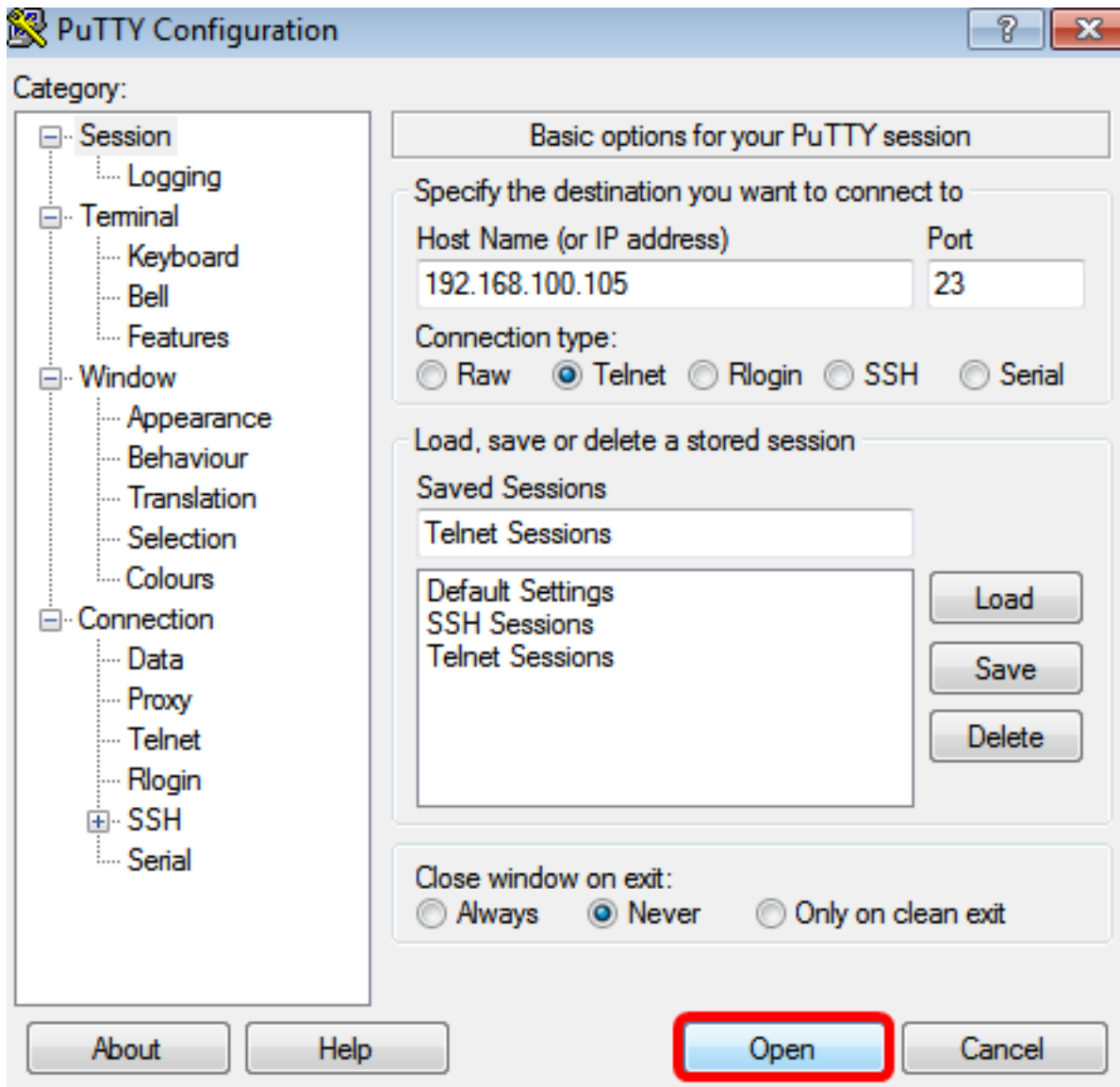


Paso 7. Opcional) En la ventana Cerrar del área de salida, haga clic en el botón de opción para elegir el comportamiento de la ventana SSH al salir.

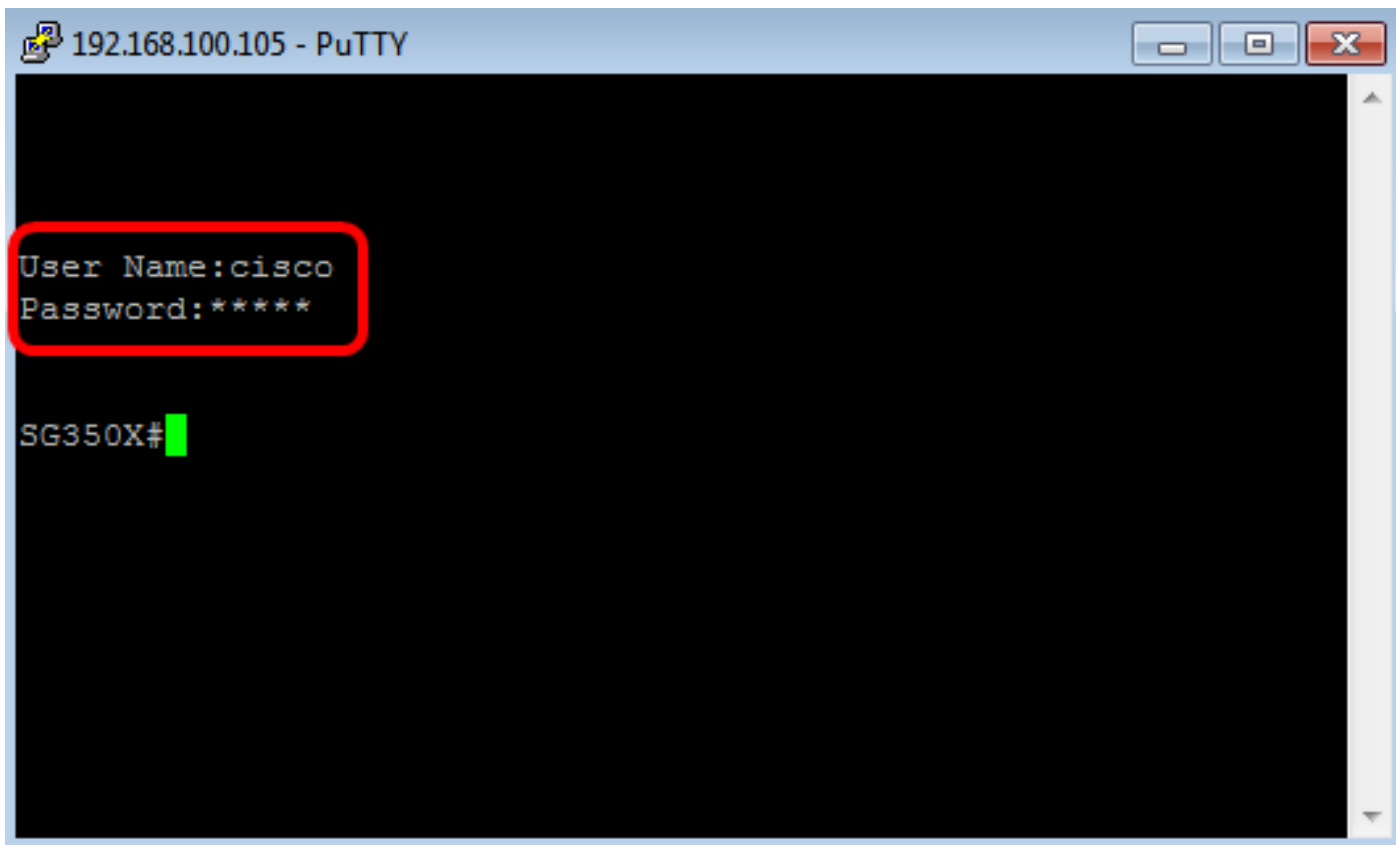


Nota: En este ejemplo, Nunca se elige.

Paso 8. Haga clic en **Abrir** para iniciar la sesión.



Paso 9. Ingrese el nombre de usuario y la contraseña del switch en los campos login como, *User Name* y *Password* según corresponda.



Ahora debería haber accedido con éxito de forma remota a la CLI de su switch a través de Telnet mediante PuTTY.

[Acceda a la CLI a través de Telnet mediante Terminal](#)

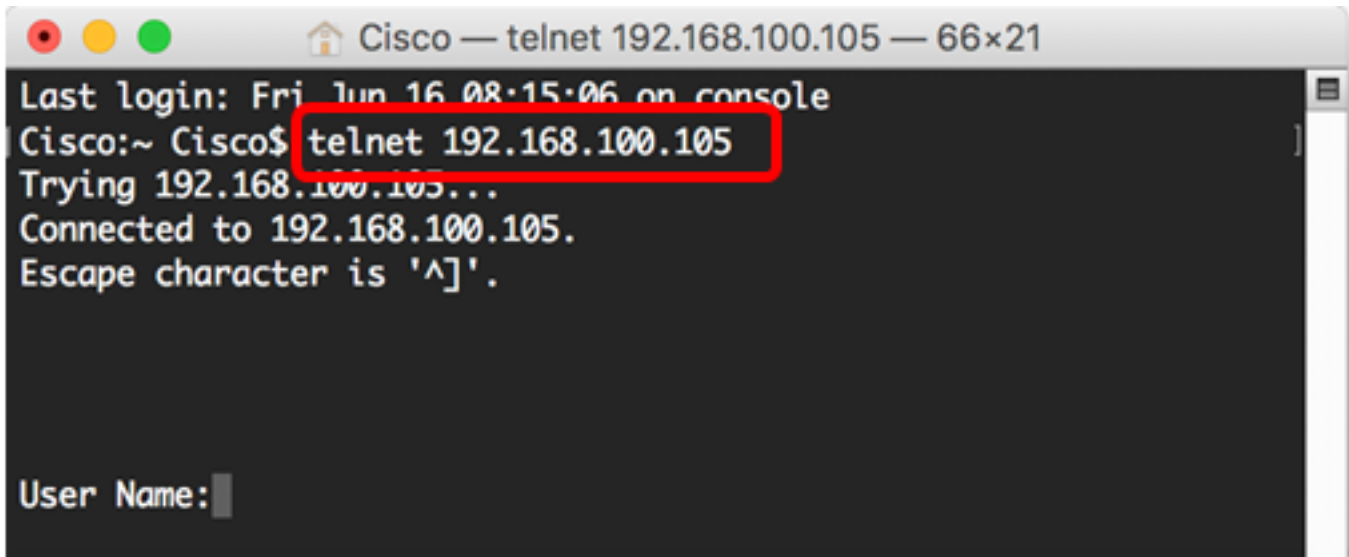
Nota: Las imágenes pueden variar según la versión del sistema operativo del ordenador Mac que esté utilizando. En este ejemplo, se utiliza macOS Sierra y la versión de Terminal es 2.7.1.

Paso 1. Vaya a **Aplicaciones > Utilidades** y luego inicie la aplicación **Terminal.app**.



Paso 2. Ingrese el comando **telnet** y luego la dirección IP para acceder a la CLI del switch.

```
Cisco: ~Cisco$ telnet [ip-address]
```

A terminal window titled "Cisco — telnet 192.168.100.105 — 66x21". The output shows: "Last login: Fri Jun 16 08:15:06 on console", "Cisco:~ Cisco\$ telnet 192.168.100.105" (highlighted with a red box), "Trying 192.168.100.105...", "Connected to 192.168.100.105.", "Escape character is '^]'.", and "User Name: " with a cursor.

```
 Cisco — telnet 192.168.100.105 — 66x21
Last login: Fri Jun 16 08:15:06 on console
Cisco:~ Cisco$ telnet 192.168.100.105
Trying 192.168.100.105...
Connected to 192.168.100.105.
Escape character is '^]'.

User Name: 
```

Paso 3. Ingrese el nombre de usuario y la contraseña del switch en los campos *User Name* y *Password* en consecuencia.

A terminal window showing the continuation of the telnet session. The output shows: "Last login: Fri Jun 16 08:15:06 on console", "Cisco:~ Cisco\$ telnet 192.168.100.105", "Trying 192.168.100.105...", "Connected to 192.168.100.105.", "Escape character is '^]'.", and "User Name:cisco", "Password:*****" (highlighted with a red box).

```
 Last login: Fri Jun 16 08:15:06 on console
Cisco:~ Cisco$ telnet 192.168.100.105
Trying 192.168.100.105...
Connected to 192.168.100.105.
Escape character is '^]'.

User Name:cisco
Password:*****
```

Ahora debería haber accedido con éxito de forma remota a la CLI de su switch a través de Telnet mediante la Terminal.