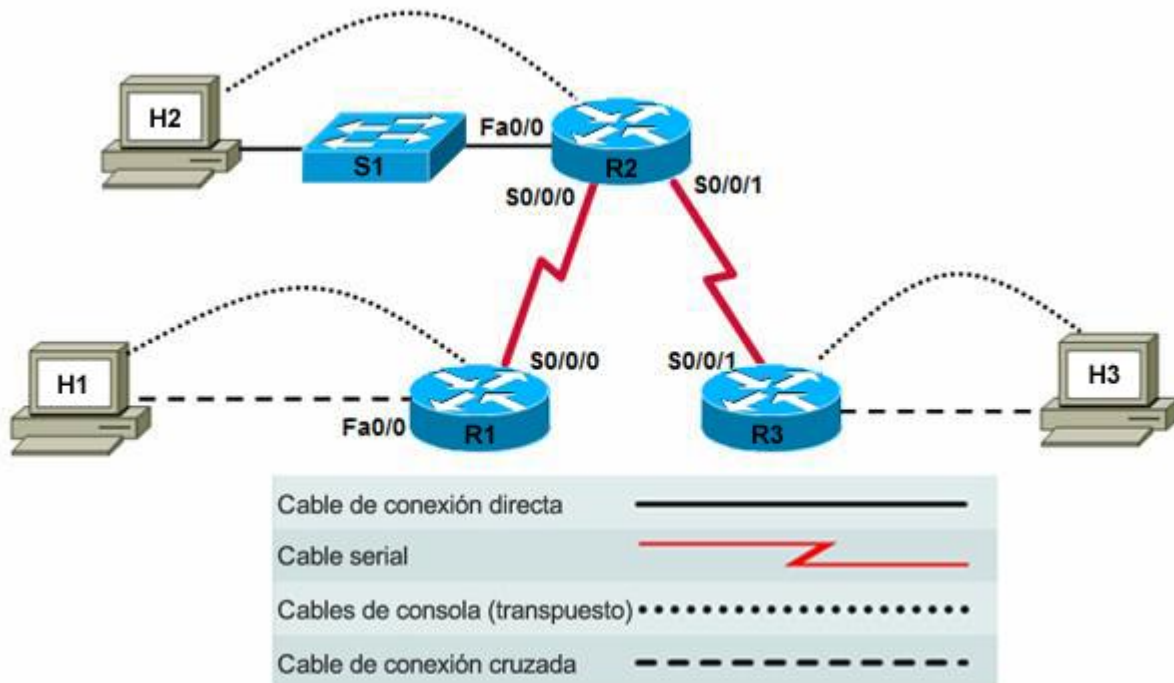


Práctica de laboratorio 9.5.3 Uso de Telnet y SSH para acceder a los dispositivos de red



Dispositivo	Nombre de Host	Interfaz	Dirección IP	Máscara de subred	Sentencias de red RIPv2
R1	R1	Serial 0/0/0 (DTE)	10.10.10.1	255.255.255.0	10.0.0.0
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0	192.168.1.0
R2	R2	Serial 0/0/0 (DCE)	10.10.10.2	255.255.255.0	10.0.0.0
		Serial 0/0/1 (DCE)	172.16.1.1	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.2.1	255.255.255.0	192.168.2.0
R3	R3	Serial 0/0/1 (DTE)	172.16.1.2	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.3.1	255.255.255.0	192.168.3.0
S1	S1	VLAN 1 – (Administración de redes)	192.168.2.99	255.255.255.0	N/C

Objetivos

- Establecimiento y administración de conexiones Telnet a un router remoto y switch.
- Verificar que la capa de aplicación entre el origen y el destino está funcionando adecuadamente.
- Recuperar información sobre routers remotos mediante el uso de comandos **show**.
- Configuración de un router para aceptar conexiones SSH utilizando la CLI del IOS de Cisco.
- Conexión de un router utilizando el cliente CLI de SSH a un router remoto ejecutando el servidor de SSH.

Información básica / Preparación

Telnet es una herramienta excelente para utilizarse en la resolución de problemas con funciones de capa superior. El uso de Telnet para acceder a los dispositivos de red permite a los técnicos ingresar comandos en cada dispositivo como si se hubieran conectado localmente. Además, la capacidad de acceder a dispositivos utilizando Telnet indica que existe conectividad de capa inferior entre los dispositivos. Telnet está ampliamente disponible en casi cualquier dispositivo de red.

Telnet es un protocolo inseguro, lo que significa que todos los datos comunicados se pueden capturar y leer. El SSH es un método más seguro para tener acceso a dispositivos remotos. Las versiones más recientes del software IOS de Cisco contienen un servidor SSH y un cliente SSH. En algunos dispositivos, este servicio se activa en forma predeterminada. Otros dispositivos requieren la activación manual del servidor SSH. De manera similar, puede utilizarse un equipo remoto con un cliente SSH instalado para iniciar una sesión de CLI segura.

Esta práctica de laboratorio se enfoca en el uso de Telnet y SSH para acceder remotamente a los routers para recopilar información sobre éstos y verificar la conectividad de la capa superior. En esta práctica de laboratorio, usted hará telnet desde la estación de trabajo como cliente y desde un router a otro router remoto. Además, podrá configurar el acceso del SSH en un router y conectar mediante el uso de un cliente CLI del IOS de Cisco basado en el router.

Establezca una red similar a la del diagrama de topología. Se puede usar cualquier router que cumpla con los requisitos de interfaz que se ven en dicho diagrama, como los routers 800, 1600, 1700, 1800, 2500, 2600 o una combinación de estos. Consulte la tabla del resumen de la interfaz del router al final de esta práctica de laboratorio para determinar los identificadores de interfaz que se deben usar según el equipo disponible en el laboratorio. El resultado puede ser distinto del que aparece en esta práctica de laboratorio según el modelo del router.

Recursos requeridos

Se necesitan los siguientes recursos:

- Un router con dos interfaces seriales y una interfaz Fast Ethernet (1841 u otro)
- Dos routers con una interfaz serial y una interfaz Fast Ethernet (1841 u otro)
- Un switch 2960 (o similar) para la LAN de R2.
- Tres computadoras con Windows XP (los hosts H2 y H3 se utilizan principalmente para la configuración de los routers R2 y R3)
- Cables Ethernet de Categoría 5 de conexión directa y cruzados, según se requieran
- Dos cables seriales nulos
- Cable de consola para configurar los routers
- Acceso a la petición de entrada de comandos del host H1
- Acceso a la configuración TCP/IP de red del host H1

En los hosts H1, H2 y H3, inicie una sesión HyperTerminal a cada router.

Nota: Asegúrese de que se hayan borrado las configuraciones de inicio de los routers y switches. Las instrucciones para borrar se proporcionan en el Manual del laboratorio, que se encuentra en la sección Tools del sitio Web Academy Connection. Consulte al instructor si no sabe cómo hacerlo.

Parte 1. Trabajo con Telnet para verificar las configuraciones y la conectividad del dispositivo

Tarea 1: Construcción de la red y verificación de la conectividad de la capa de red

Paso 1: Configurar la información básica en cada router y el switch.

- Construya y configure la red de acuerdo con el diagrama de topología y la tabla de configuración del dispositivo. **Si fuera necesario, consulte** la Práctica de laboratorio 5.3.5, “Configuración de parámetros básicos del router con la CLI del IOS de Cisco,” para ver las instrucciones para configurar el nombre del host, las contraseñas y las direcciones de interfaces.
- Configure RIPv2 en cada router y publique las redes mostradas en la tabla de configuración del dispositivo. Si fuera necesario, consulte la Práctica de laboratorio 6.1.5, “Configuración y verificación de RIP”, para obtener instrucciones para configurar el protocolo de enrutamiento RIP.
- Configure los parámetros básicos en el switch S1 para incluir el nombre del host, las contraseñas y la dirección IP de la VLAN 1. Si fuera necesario, consulte la Práctica de laboratorio 5.5.4, “Configuración del switch Cisco 2960”.

Paso 2: Configurar los hosts.

Configure los hosts H1, H2 y H3 con una dirección IP, máscara de subred y gateway predeterminado compatibles con la dirección IP de la interfaz del gateway predeterminado del router para la LAN a la que están conectados.

Paso 3: Verificar la conectividad de la capa de red de extremo a extremo.

- En H1, abra una ventana del indicador de comandos, seleccione **Inicio > Ejecutar** y teclee **cmd**. También puede seleccionar **Inicio > Todos los programas > Accesorios > Indicador de comandos**.
- Utilice el comando **ping** para probar la conectividad de extremo a extremo. Haga ping desde H1 en la LAN de R1 al H3 en la LAN de R3 (por ejemplo, 192.168.3.2).

```
C:\>ping 192.168.3.2
```
- Si H3 no está conectado al R3, haga ping a la dirección IP 172.16.1.2 de la interfaz serial 0/0/1 de R3.

```
C:\>ping 172.16.1.2
```
- Si los pings se realizan con éxito a R3, ¿qué indica eso sobre la conectividad de la capa OSI entre H1 y R3?

Nota: Si los pings no tuvieron éxito, resuelva los problemas de configuraciones y conexiones del router y del host.

Tarea 2: Establecer una sesión Telnet desde un equipo host

Paso 1: Hacer Telnet desde H1 al router remoto R2.

El software IOS del router Cisco tiene integrado el software cliente y servidor de Telnet. La mayoría de los sistemas operativos informáticos tienen un cliente Telnet. Muchos sistemas operativos de servidor también tienen un servidor Telnet, aunque por lo general los sistemas operativos de escritorio de Microsoft Windows no lo tienen.

En muchos casos, no tendrá acceso directo a un router a través de la consola para que pueda hacer Telnet a otros routers. Por lo general, hace telnet a un router desde una computadora host. Desde ahí, puede hacer Telnet a otros routers que se pueden acceder a través de la red.

- a. Desde la petición de entrada de comandos en H1, haga telnet a la interfaz Fast Ethernet 0/0 en el router R2.

```
C:\>telnet 192.168.2.1
```

- b. Ingrese la contraseña **cisco** para acceder al router.
 - c. ¿Qué petición de entrada mostró el router? _____
 - d. Ejecute el comando **show version**.
 - e. ¿Cuál es la versión del software IOS de Cisco para el router remoto R2? _____ .
 - f. ¿Cuántas y qué tipo de interfaces tiene el router remoto R2? _____
 - g. Si el Telnet de H1 a R2 tiene éxito, ¿qué indica eso sobre la conectividad de la capa OSI entre los dispositivos?
-

Paso 2: Finalizar la sesión Telnet desde H1 al router remoto R2.

Salga de la sesión Telnet desde el host H1 al R2 tecleando **exit**.

Tarea 3: Realizar operaciones Telnet básicas entre los routers

Paso 1: Hacer Telnet desde R1 al router remoto R2.

Nota: Telnet utiliza las líneas vty en el router remoto para conectarse. Si las líneas vty no están configuradas para iniciar sesión o no se ha establecido una contraseña, no podrá conectarse al router remoto utilizando Telnet.

- a. Haga Telnet a la dirección IP 10.10.10.2 de la interfaz serial 0/0/0 de R2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
Password:
```

- b. Utilice la contraseña **cisco** para ingresar al router.
- c. ¿Qué petición de entrada mostró el router? _____

Paso 2: Observar las interfaces en el router remoto R2.

- a. Ejecute el comando **show ip interface brief** en la petición de entrada del router remoto.

```
R2>show ip interface brief
```

- b. Enumere las interfaces que se encuentren activas en el router remoto R2.
-

Paso 3: Visualizar la tabla de enrutamiento en el router remoto.

Ejecute el comando **show ip route** en la petición de entrada del router. ¿Qué rutas aprendió R2 de RIP?

```
R2>show ip route
```

Paso 4: Mostrar los vecinos CDP para R2.

- Utilice el Protocolo de descubrimiento de Cisco (CDP, Cisco Discovery Protocol) para ver información acerca de dispositivos Cisco directamente conectados a R2. Ingrese el comando **show cdp neighbors** en el indicador del router.
- Enumere todas las ID de los dispositivos que están conectados al router remoto. ¿Cuál es la plataforma para cada dispositivo?

```
R2>show cdp neighbors
```

Paso 5: Suspender la sesión Telnet actual en R2.

- Presione **Ctrl-Shift-6** y luego presione la tecla **x**. Esta acción sólo suspende la sesión y regresa al router anterior. No se desconecta de este router.
- ¿Qué petición de entrada mostró el router? _____

Paso 6: Reanudar la sesión Telnet a R2.

- Presione la tecla **Enter** en la petición de entrada del router. ¿Con qué responde el router?

Al presionar la tecla **Enter** se reanuda la sesión Telnet que se suspendió anteriormente.

- ¿Qué petición de entrada mostró el router? _____

Paso 7: Cerrar la sesión Telnet a R2.

- Finalice la sesión Telnet tecleando **exit**.
- ¿Con qué responde el router? _____
- ¿Qué petición de entrada mostró el router? _____

Nota: Cuando se suspende la sesión Telnet, puede desconectarse de esa sesión mediante el uso del comando **disconnect** y el número de sesión.

Tarea 4: Realizar operaciones de Telnet entre múltiples routers

Paso 1: Hacer Telnet desde R1 al router remoto R2.

- Desde R1, haga Telnet a la dirección IP 10.10.10.2 de la interfaz serial 0/0/0 de R2.
- Utilice la contraseña **cisco** para ingresar al router.

Paso 2: Establecer una sesión Telnet adicional desde R2 a R3.

- Desde R2, haga Telnet a la dirección IP 172.16.1.2 de la interfaz serial 0/0/1 de R3.
- Utilice la contraseña **cisco** para acceder al router.
- ¿Qué petición de entrada mostró el router? _____

Paso 3: Suspender la sesión Telnet a R3.

- Presione **Ctrl-Shift-6** y luego presione la tecla **x**.
- ¿Qué petición de entrada mostró el router? _____

Paso 4: Visualizar las sesiones Telnet activas.

Ingrese el comando **show sessions** en el indicador de comandos de R1. ¿Cuántas sesiones se están llevando a cabo? _____

Nota: La sesión predeterminada se indica por un asterisco (*). Esta es la sesión que se reanuda cuando presiona **Enter**.

```
R2>show sessions
```

Paso 5: Reanudar la sesión Telnet a R2.

- a. Presione **Enter** en el indicador del router. ¿Con qué responde el router?

b. ¿Qué petición de entrada mostró el router? _____

c. ¿Por qué el indicador dice R3? _____

Paso 6: Desconectar las sesiones desde R1 a R2 y R3

- a. Ingrese el comando **exit** en el indicador R3 y luego presione **Enter** para cerrar la conexión a R3.

```
R3>exit  
[Connection to 172.16.1.2 closed by foreign host]  
R2>
```

- b. Suspenda la sesión R2 desde R1 (sesión 1 en R1) presionando **Ctrl-Shift-6**, seguido por la **tecla x**. **Utilice el comando disconnect para finalizar la conexión a R2.**

```
R1>disconnect 1  
Closing connection to 10.10.10.2 [confirm]
```

Tarea 4: Remover de la contraseña de vty de R3

Paso 1: Hacer Telnet desde R1 al router remoto R3.

- a. Hacer Telnet a la dirección IP de la interfaz serial 0/0/1 172.16.1.2.

```
R1>telnet 172.16.1.2  
Trying 172.16.1.2 ... Open  
User Access Verification  
Password:
```

- b. Utilice la contraseña **cisco** para ingresar al router.
- c. ¿Qué petición de entrada mostró el router? _____

Paso 2: Desde el modo EXEC privilegiado en R3, retirar la contraseña de vty.

- a. Ejecute el comando **enable** en el indicador de comandos R3> e ingrese la contraseña **class**.
- b. ¿Qué petición de entrada mostró el router? _____
- c. Retire la contraseña para las líneas vty en R3.

```
R3>enable  
R3#config t  
R3(config)#line vty 0 4  
R3(config-line)#no password  
R3(config-line)#end  
R3#
```

- d. Salga de la sesión Telnet en R3 y regrese a R1.

```
R3#exit
[Connection to 172.16.1.2 closed by foreign host]
R1#
```

Paso 3: Hacer Telnet desde R1 al router remoto R3 nuevamente.

- a. Hacer Telnet a la dirección IP de la interfaz serial 0/0/1 172.16.1.2.

```
R1>telnet 172.16.1.2
```

- b. ¿Puede hacer telnet a R3? _____

- c. ¿Qué mensaje recibió? ¿Por qué?

Paso 4: Conectarse a R3 mediante la consola y restablecer la contraseña de vty.

- a. Ejecute el comando **enable** en el indicador de comandos R3> e ingrese la contraseña **class**.
- b. Restablezca la contraseña para las líneas vty en R3.

```
R3>enable
R3#config t
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#end
R3#
```

Parte 2. Trabajo con SSH para verificar las configuraciones y la conectividad del dispositivo

El Shell Seguro, o SSH, es una versión de encriptación RSA de Telnet. Toda la información, inclusive las ID de usuario, las contraseñas y los datos que pasan entre un cliente SSH y el servidor SSH se encriptan. Dado que SSH es protocolo de la capa de aplicación, una conexión SSH demuestra que todas las capas OSI están funcionando, inclusive la encriptación en la capa de presentación.

Tarea 1: Configurar SSH en el router R2

Paso 1: Hacer Telnet desde R1 al router remoto R2.

- a. Haga Telnet a la dirección IP 10.10.10.2 de la interfaz serial 0/0/0 de R2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
Password:
```

- b. Utilice la contraseña **cisco** para ingresar al router.

- c. ¿Qué petición de entrada mostró el router? _____

Paso 2: Configurar el servidor SSH en R2.

- a. Cree un nombre de dominio y una ID de usuario y contraseña de Telnet o SSH para conexiones vty remotas.

Nota: Al crear una ID de usuario y contraseña y especificar el inicio de sesión local para las líneas vty, cualquier intento para hacer telnet o SSH a este router requiere la entrada del nombre de usuario y la contraseña creados.

Dado que el usuario administrativo tiene un nivel privilegiado de 15 (el más alto) y el nivel privilegiado de 15 está configurado para las líneas vty, el indicador del router va directamente al modo EXEC privilegiado (enable) al conectar a R2 utilizando Telnet o SSH.

El uso de una ID de usuario y contraseña especiales para asegurar el acceso vty de Telnet y SSH al router no afecta la contraseña de la consola (línea con 0) o la contraseña secreta de enable.

```
Router#config terminal
R2(config)#ip domain-name customer.com
R2(config)#username admin privilege 15 password 0 cisco123
R2(config)#exit
```

- b. Configure las líneas de terminal vty para aceptar conexiones remotas de clientes Telnet y SSH y valide la ID de usuario mediante la base de datos de nombres de usuario del router local.

```
R2(config)#line vty 0 4
R2(config-line)#privilege level 15
R2(config-line)#login local
R2(config-line)#transport input telnet ssh
R2(config-line)#exit
```

Nota: Si Telnet no se especifica en el comando **transport input** anterior, sólo se permitirán las conexiones remotas de SSH a este router.

- c. Genere el par de claves de encriptación RSA para que el router lo utilice para autenticación y encriptación de los datos SSH que se están transmitiendo. Ingrese **768** para la cantidad de bits del módulo. De manera predeterminada, es 512.

```
R2(config)#crypto key generate rsa
El nombre para las claves será: R2.customer.com
Elija el tamaño del módulo de la clave en el rango de 360 a 2048 para
sus Claves de propósito general. Elegir un módulo de clave mayor a 512
puede llevarse algunos minutos.
```

```
How many bits in the modulus [512] 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
*Mar 20 13:17:50.123: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
R2(config)#exit
```

- d. Verifique que SSH esté habilitado y la versión utilizada con el comando **show ip ssh**.

```
R2#show ip ssh
```

- e. Complete la siguiente información según el resultado del comando **show ip ssh**.

```
Versión SSH habilitada _____
Expiración de autenticación _____
Reintentos de autenticación _____
```

- f. Ejecute el comando **show running-config**. ¿Qué indicación existe de que el servidor SSH ha sido configurado en R2? _____

- g. Guarde la configuración en ejecución en la configuración de inicio.

```
R2#copy running-config startup-config
```


- h. Salga de la sesión Telnet en R2 y regrese a R1.

```
R2#exit
[Connection to 10.10.10.2 closed by foreign host]
R1#
```

Tarea 2: Iniciar sesión en R2 utilizando el cliente SSH de la CLI de R1

Nota: Usted también puede iniciar sesión en un router o switch habilitado por SSH utilizando una computadora con un cliente GUI, como por ejemplo PuTTY. Este procedimiento se describe en la Práctica de laboratorio 8.3.4, “Configuración de un router remoto mediante SSH”.

Paso 1: Utilizar la característica de ayuda de la CLIE del IOS de Cisco con el comando ssh.

Desde la sesión terminal de R1, utilice la característica de ayuda del IOS de Cisco para mostrar las opciones de inicio de sesión para el cliente SSH de R1.

```
R1#ssh ?
-c      Seleccionar el algoritmo de encriptación
-l      Iniciar sesión utilizando este nombre de usuario
-m      Seleccionar el algoritmo HMAC
-o      Especificar las opciones
-p      Conectar a este puerto
-v      Especificar la versión del protocolo SSH
WORD    Dirección IP o nombre del host de un sistema remoto

R1#ssh -l admin ?
-c      Seleccionar el algoritmo de encriptación
-m      Seleccionar el algoritmo HMAC
-o      Especificar las opciones
-p      Conectar a este puerto
-v      Especificar la versión del protocolo SSH
WORD    Dirección IP o nombre del host de un sistema remoto
```

Paso 2: Iniciar sesión en R2 utilizando SSH.

En este paso, usted iniciará sesión en el servidor SSH de R2 desde el cliente SSH de la CLI de R1. Establece una sesión remota segura con R2 desde la cual puede ejecutar los comandos show y configuration.

- a. Inicie sesión en R2 especificando el nombre de usuario **admin** y la contraseña **cisco123**, los cuales se configuraron anteriormente y la dirección IP en la interfaz S0/0/0 de R2.

```
R1#ssh -l admin 10.10.10.2

Password:
Unauthorized Use Prohibited
R2#
```

- b. ¿Por qué obtuvo el indicador del router en modo EXEC privilegiado (enable)?

- c. En R2, ejecute el comando **show ssh**, para ver las conexiones SSH al router.

```
R2#show ssh
Conexión Versión Modo Encriptación Hmac Estado Nombre de
usuario
0          1.99      IN   aes128-cbc hmac-sha1 Session started admin
0          1.99      OUT  aes128-cbc hmac-sha1 Session started admin
%No SSHv1 server connections running.
```

- d. Salga de la sesión SSH en R2 y regrese a R1.

```
R2#exit  
[Connection to 10.10.10.2 closed by foreign host]  
R1>
```

Nota: **Ctrl-Shift-6** seguido por la tecla **x** y los comandos utilizados anteriormente con Telnet, son los mismos para SSH.

Tarea 3: Reflexión

- a. **Conectividad HTTP** – Usted también puede verificar la conectividad de la capa de aplicación utilizando la interfaz HTTP para un router o switch. Si el comando **ip http server** está presente en el dispositivo que ejecuta config, puede abrir un explorador en una computadora que tenga conectividad de red a la dirección IP del router o switch (o nombre, si DNS está habilitado) y acceder a la aplicación de administración de GUI de HTTP en el dispositivo. Esto puede ser una interfaz HTTP básica para los routers que no sean SDM o puede ser SDM y SDM Express para routers habilitados para SDM. Dado que HTTP es un protocolo de la capa de aplicación, una conexión HTTP exitosa demuestra que todas las capas OSI están funcionando.
- b. Compare las ventajas y desventajas de Telnet y SSH.

- c. Si puede hacer ping a la interfaz del router pero no puede conectarse a ésta utilizando Telnet o SSH, ¿cuál podría ser el problema y qué capas del modelo OSI son afectadas?

Resumen de la interfaz del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
Nota: Observe las interfaces para saber exactamente cómo está configurado el router. La interfaz identifica el tipo de router y la cantidad de interfaces que tiene el router. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. Lo que se ha presentado son los identificadores de las posibles combinaciones de interfaces en el dispositivo. Esta tabla de interfaces no incluye ningún otro tipo de interfaz aunque puede existir otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo de esto. La información entre paréntesis es la abreviatura legal que se puede utilizar en los comandos IOS de Cisco para representar la interfaz.				