Práctica de laboratorio: configuración y verificación de ACL de IPv6

Topología

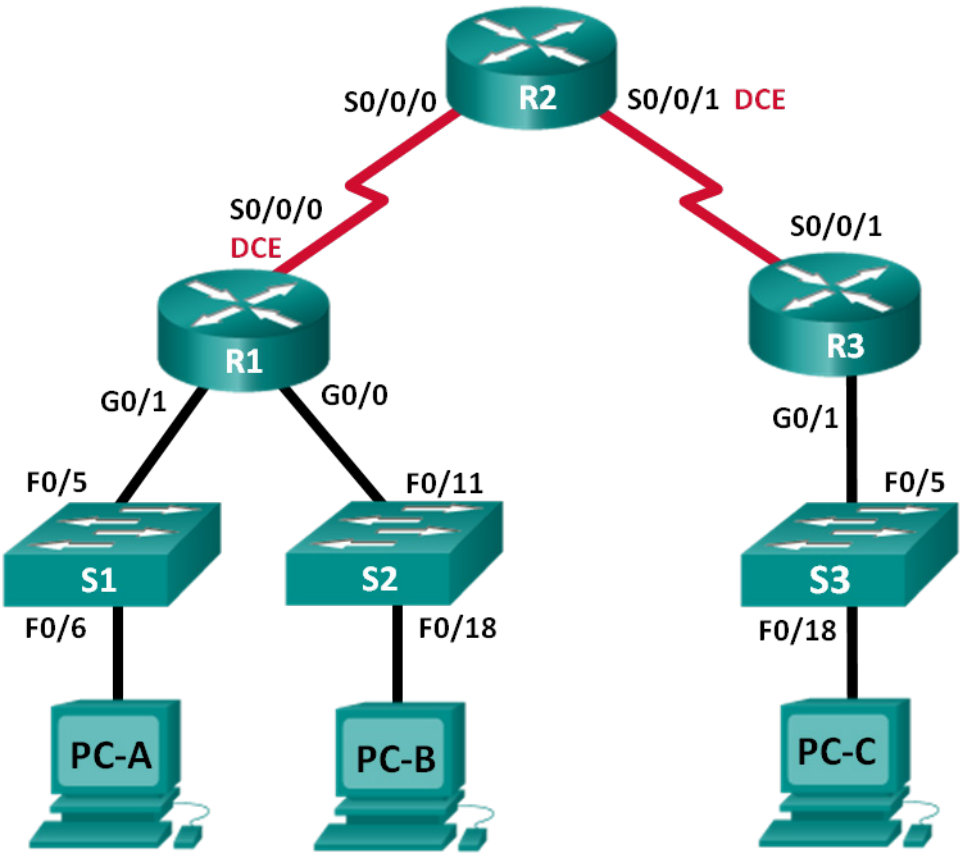


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Gateway predeterminado
R1	G0/0	2001:DB8:ACAD:B::1/64	N/A
	G0/1	2001:DB8:ACAD:A::1/64	N/A
	S0/0/0 (DCE)	2001:DB8:AAAA:1::1/64	N/A
R2	S0/0/0	2001:DB8:AAAA:1::2/64	N/A
	S0/0/1 (DCE)	2001:DB8:AAAA:2::2/64	N/A
R3	G0/1	2001:DB8:CAFE:C::1/64	N/A
	S0/0/1	2001:DB8:AAAA:2::1/64	N/A
S1	VLAN1	2001:DB8:ACAD:A::A/64	N/A
S2	VLAN1	2001:DB8:ACAD:B::A/64	N/A
S3	VLAN1	2001:DB8:CAFE:C::A/64	N/A
PC-A	NIC	2001:DB8:ACAD:A::3/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::3/64	FE80::1
PC-C	NIC	2001:DB8:CAFE:C::3/64	FE80::1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Parte 2: configurar los dispositivos y verificar la conectividad

Parte 3: configurar y verificar las ACL de IPv6

Parte 4: editar las ACL de IPv6

Información básica/situación

Puede filtrar el tráfico IPv6 mediante la creación de listas de control de acceso (ACL) de IPv6 y su aplicación a las interfaces, en forma similar al modo en que se crean ACL de IPv4 con nombre. Los tipos de ACL de IPv6 son extendida y con nombre. Las ACL estándar y numeradas ya no se utilizan con IPv6. Para aplicar una ACL de IPv6 a una interfaz vty, use el nuevo comando **ipv6 traffic-filter**. El comando **ipv6 access-class** todavía se usa para aplicar una ACL de IPv6 a las interfaces.

En esta práctica de laboratorio, aplicará reglas de filtrado IPv6 y luego verificará que restrinjan el acceso según lo esperado. También editará una ACL de IPv6 y borrará los contadores de coincidencias.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red y borrará cualquier configuración, en caso de ser necesario.

Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar los routers y los switches.

Parte 2: Configurar dispositivos y verificar la conectividad

En la parte 2, configurará los parámetros básicos en los routers, los switches y las computadoras. Consulte la topología y la tabla de direccionamiento incluidos al comienzo de esta práctica de laboratorio para conocer los nombres de los dispositivos y obtener información de direcciones.

Paso 1: configurar direcciones IPv6 en todas las computadoras.

Configure las direcciones IPv6 de unidifusión global según la tabla de direccionamiento. Utilice la dirección link-local **FE80::1** para el gateway predeterminado en todas las computadoras.

Paso 2: configurar los switches.

a. Desactive la búsqueda del DNS.
b. Asigne el nombre de host.
c. Asigne **ccna-lab.com** como nombre de dominio.
d. Cifre las contraseñas de texto no cifrado.
e. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
f. Cree una base de datos de usuarios local con el nombre de usuario **admin** y la contraseña **classadm**.
g. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
h. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
i. Habilite el inicio de sesión en las líneas VTY con la base de datos local.
j. Genere una clave criptográfica rsa para ssh con un tamaño de módulo de 1024 bits.
k. Cambie las líneas VTY de transport input a «all» solo para SSH y Telnet.
l. Asigne una dirección IPv6 a la VLAN 1 según la tabla de direccionamiento.
m. Desactive administrativamente todas las interfaces inactivas.

Paso 3: configurar los parámetros básicos en todos los routers.

a. Desactive la búsqueda del DNS.

b. Asigne el nombre de host.

c. Asigne **ccna-lab.com** como nombre de dominio.

d. Cifre las contraseñas de texto no cifrado.

e. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.

f. Cree una base de datos de usuarios local con el nombre de usuario **admin** y la contraseña **classadm**.

g. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

h. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

i. Habilite el inicio de sesión en las líneas VTY con la base de datos local.

j. Genere una clave criptográfica rsa para ssh con un tamaño de módulo de 1024 bits.

k. Cambie las líneas VTY de transport input a «all» solo para SSH y Telnet.

Paso 4: configurar los parámetros de IPv6 en el R1.

a. Configure la dirección IPv6 de unidifusión en las interfaces G0/0, G0/1 y S0/0/0.

b. Configure la dirección IPv6 link-local en las interfaces G0/0, G0/1 y S0/0/0. Utilice **FE80::1** como la dirección link-local en las tres interfaces.

c. Establezca la frecuencia de reloj en S0/0/0 en 128000.

d. Habilite las interfaces.

e. Habilite el routing de unidifusión IPv6.

f. Configure una ruta predeterminada IPv6 para que use la interfaz S0/0/0.

```
R1(config)# ipv6 route ::/0 s0/0/0
```

Paso 5: configurar los parámetros de IPv6 en el R2.

a. Configure la dirección IPv6 de unidifusión en las interfaces S0/0/0 y S0/0/1.

b. Configure la dirección IPv6 link-local en las interfaces S0/0/0 y S0/0/1. Utilice **FE80::2** como la dirección link-local en ambas interfaces.

c. Establezca la frecuencia de reloj en S0/0/1 en 128000.

d. Habilite las interfaces.

e. Habilite el routing de unidifusión IPv6.

f. Configure rutas estáticas IPv6 para la administración del tráfico de las subredes LAN del R1 y el R3.

```
R2(config)# ipv6 route 2001:db8:acad::/48 s0/0/0
R2(config)# ipv6 route 2001:db8:cafe:c::/64 s0/0/1
```

Paso 6: configurar los parámetros de IPv6 en el R3.

a. Configure la dirección IPv6 de unidifusión en las interfaces G0/1 y S0/0/1.

b. Configure la dirección IPv6 link-local en las interfaces G0/1 y S0/0/1. Utilice **FE80::1** como la dirección link-local en ambas interfaces.

c. Habilite las interfaces.

d. Habilite el routing de unidifusión IPv6.

e. Configure una ruta predeterminada IPv6 para que use la interfaz S0/0/1.

```
R3(config)# ipv6 route ::/0 s0/0/1
```

Paso 7: Verifique la conectividad.

a. Se debería poder hacer ping entre todas las computadoras de la topología.

b. Acceda al R1 mediante Telnet desde todas las computadoras en la topología.

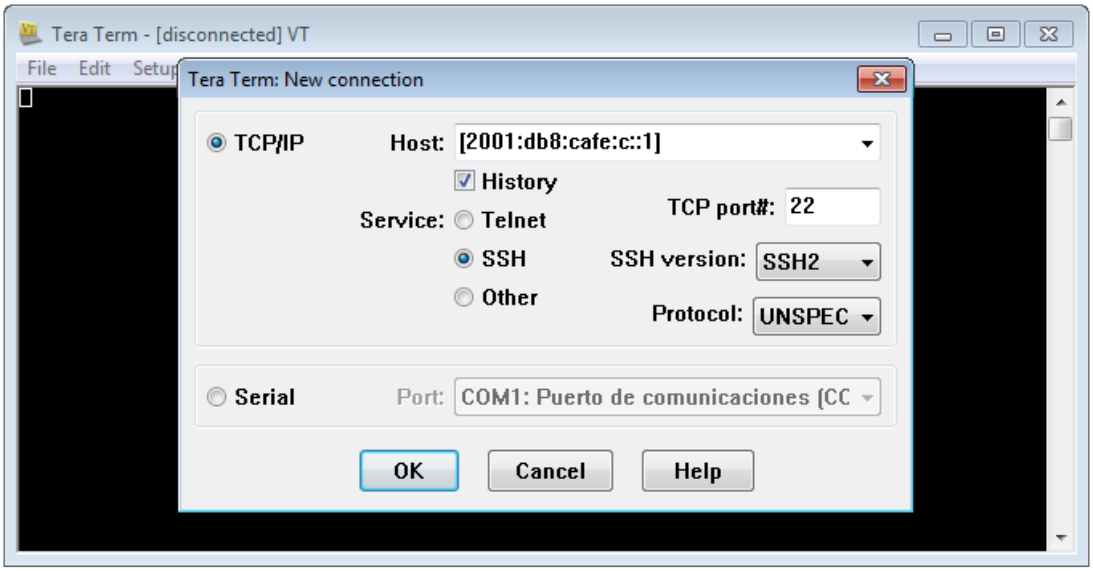
c. Acceda al R1 mediante SSH desde todas las computadoras en la topología.

d. Acceda al S1 mediante Telnet desde todas las computadoras en la topología.

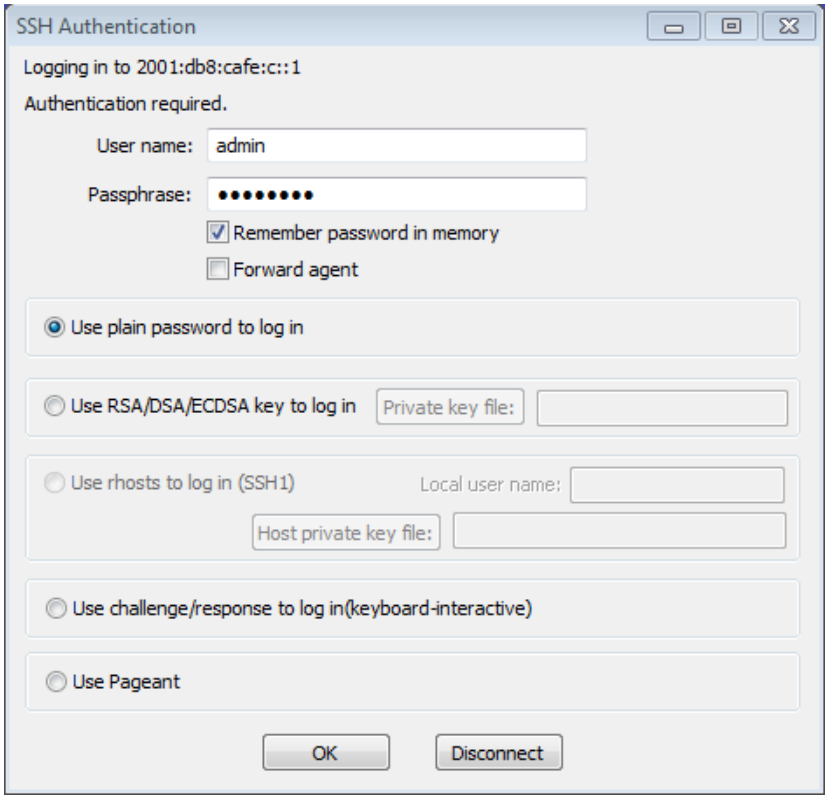
e. Acceda al S1 mediante SSH desde todas las computadoras en la topología.

f. Solucione los problemas de conectividad ahora, porque las ACL que cree en la parte 3 de esta práctica de laboratorio restringirán el acceso a ciertas áreas de la red.

Nota: Tera Term requiere que la dirección IPv6 de destino esté entre corchetes. Introduzca la dirección IPv6 como se muestra, haga clic en **OK** (Aceptar) y, luego, haga clic en **Continue** (Continuar) para aceptar la advertencia de seguridad y conectarse al router.



Introduzca las credenciales de usuario configuradas (nombre de usuario **admin** y contraseña **classadm**) y seleccione **Use plain password to log in** (Usar contraseña no cifrada para iniciar sesión) en el cuadro de diálogo SSH Authentication (Autenticación de SSH). Haga clic en **Aceptar** para continuar.



Parte 3: configurar y verificar las ACL de IPv6

Paso 1: configurar y verificar las restricciones de VTY en el R1.

a. Cree una ACL para permitir que solo los hosts de la red 2001:db8:acad:a::/64 accedan al R1 mediante telnet. Todos los hosts deben poder acceder al R1 mediante ssh.

```
R1(config)# ipv6 access-list RESTRICT-VTY
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any
R1(config-ipv6-acl)# permit tcp any any eq 22
```

b. Aplique la ACL RESTRICT-VTY a las líneas VTY del R1.

```
R1(config-ipv6-acl)# line vty 0 4
R1(config-line)# ipv6 access-class RESTRICT-VTY in
R1(config-line)# end
R1#
```

c. Visualice la nueva ACL.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any sequence 10
    permit tcp any any eq 22 sequence 20
```


d. Verifique que la ACL RESTRICT-VTY solo permita tráfico de Telnet de la red 2001:db8:acad:a::/64.

¿De qué forma la ACL RESTRICT-VTY permite únicamente el acceso de hosts de la red 2001:db8:acad:a::/64 al R1 mediante telnet?

¿Qué hace la segunda instrucción permit en la ACL RESTRICT-VTY?

Paso 2: restringir el acceso por Telnet a la red 2001:db8:acad:a::/64.

a. Cree una ACL denominada RESTRICTED-LAN que bloquee el acceso por Telnet a la red 2001:db8:acad:a::/64.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# remark Block Telnet from outside
R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet
R1(config-ipv6-acl)# permit ipv6 any any
```

b. Aplique la ACL RESTRICTED-LAN a la interfaz G0/1 para todo el tráfico saliente.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

c. Desde la PC-B y la PC-C, acceda al S1 mediante Telnet para verificar que se haya restringido Telnet. Desde la PC-B, acceda al S1 mediante SSH para verificar que todavía se pueda llegar al dispositivo mediante SSH. Resuelva cualquier problema, si es necesario.

d. Use el comando **show ipv6 access-list** para ver la ACL RESTRICTED-LAN.

```
R1# show ipv6 access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet (6 matches) sequence 20
    permit ipv6 any any (45 matches) sequence 30
```

Observe que cada instrucción identifica el número de aciertos o coincidencias que se produjeron desde la aplicación de la ACL a la interfaz.

e. Use el comando **clear ipv6 access-list** para restablecer los contadores de coincidencias de la ACL RESTRICTED-LAN.

```
R1# clear ipv6 access-list RESTRICTED-LAN
```

f. Vuelva a mostrar la ACL con el comando **show access-lists** para confirmar que se hayan borrado los contadores.

```
R1# show access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any sequence 30
```


Parte 4: editar las ACL de IPv6

En la parte 4, editará la ACL RESTRICTED-LAN que creó en la parte 3. Antes de editar la ACL, se recomienda eliminarla de la interfaz a la que esté aplicada. Una vez que haya terminado de editarla, vuelva a aplicar la ACL a la interfaz.

Nota: muchos administradores de red hacen una copia de la ACL y editan la copia. Después de terminar la edición, el administrador debe eliminar la ACL antigua y aplicar la ACL editada a la interfaz. Este método mantiene la ACL implementada hasta que esté listo para aplicar la copia editada.

Paso 1: eliminar la ACL de la interfaz.

```
R1(config)# int g0/1
R1(config-if)# no ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Paso 2: Use el comando show access-lists para ver la ACL.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (36 matches) sequence 30
```

Paso 3: Introduzca una nueva instrucción de ACL con número de secuencia.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host 2001:db8:acad:a::a
eq 23 sequence 15
```

¿Qué hace esta nueva instrucción permit?

Paso 4: insertar una nueva instrucción de ACL al final de la ACL.

```
R1(config-ipv6-acl)# permit tcp any host 2001:db8:acad:a::3 eq www
```

Nota: esta instrucción permit solo se usa para mostrar cómo agregar una instrucción al final de una ACL. Nunca habrá coincidencias con esta línea de la ACL, dado que la instrucción permit anterior coincide con todo.

Paso 5: Use el comando do show access-lists para ver el cambio en la ACL.

```
R1(config-ipv6-acl)# do show access-list
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
    permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (124 matches) sequence 30
    permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```


Nota: el comando **do** se puede usar para ejecutar cualquier comando de EXEC privilegiado en el modo de configuración global o un submodo de este.

Paso 6: eliminar una instrucción de ACL.

Utilice el comando **no** para eliminar la instrucción permit que acaba de agregar.

```
R1(config-ipv6-acl)# no permit tcp any host 2001:DB8:ACAD:A::3 eq www
```

Paso 7: usar el comando do show access-lists RESTRICTED-LAN para ver la ACL.

```
R1(config-ipv6-acl)# do show access-list RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (214 matches) sequence 30
```

Paso 8: volver a aplicar la ACL RESTRICTED-LAN a la interfaz G0/1.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Paso 9: probar los cambios en la ACL.

Desde la PC-B, acceda al S1 mediante Telnet. Resuelva cualquier problema, si es necesario.

Reflexión

1. ¿Cuál es la causa de que el conteo de coincidencias en la instrucción **permit ipv6 any any** en RESTRICTED-LAN siga aumentando?

2. ¿Qué comando utilizaría para restablecer los contadores de la ACL en las líneas VTY?

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.