

Práctica de laboratorio: Resolución de problemas de PPP básico con autenticación

Topología

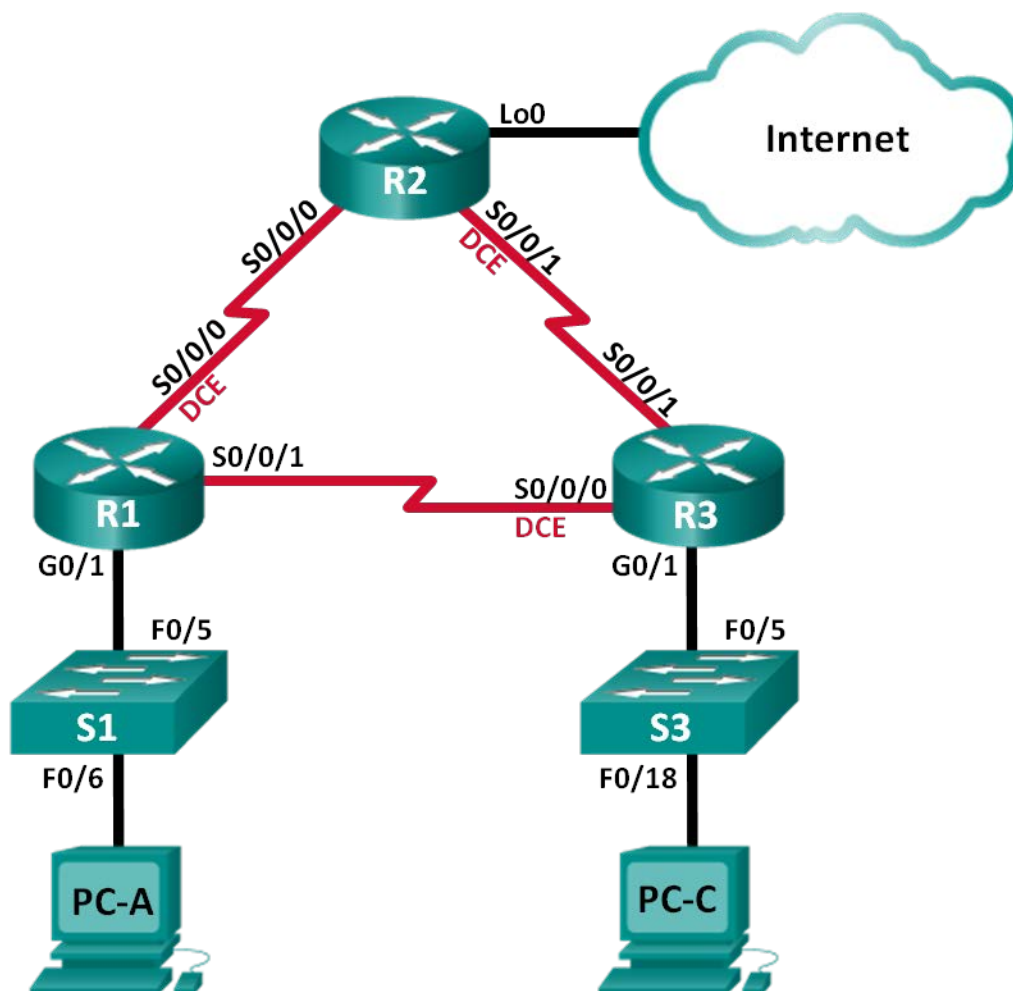


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	Lo0	209.165.200.225	255.255.255.252	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objetivos

Parte 1: Armar la red y cargar las configuraciones de los dispositivos

Parte 2: Resolver problemas de la capa de enlace de datos

Parte 3: Resolver problemas de la capa de red

Información básica/situación

Un ingeniero de redes inexperto configuró los routers de la compañía. Varios errores en la configuración han resultado en problemas de conectividad. El gerente le solicitó que resuelva los problemas, corrija los errores de configuración y documente su trabajo. Según los conocimientos de PPP y los métodos de prueba estándar, busque y corrija los errores. Asegúrese de que todos los enlaces seriales usen la autenticación CHAP de PPP y que se pueda llegar a todas las redes.

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 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 esta 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)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 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: Armar la red y cargar las configuraciones de los dispositivos

En la parte 1, establecerá la topología de la red, configurará los parámetros básicos en los equipos host y cargará las configuraciones en los routers.

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

Paso 2: Configurar los equipos host.

Paso 3: Cargar las configuraciones de los routers.

Cargue las siguientes configuraciones en el router apropiado. Todos los routers tienen las mismas contraseñas. La contraseña del modo EXEC privilegiado es **class**. La contraseña para el acceso a la consola y a VTY es **cisco**. Todas las interfaces seriales deben configurarse con la encapsulación PPP y autenticarse con CHAP con la contraseña **chap123**.

Configuración del router R1:

```
hostname R1
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
interface g0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface s0/0/0
 ip address 192.168.12.1 255.255.255.252
 clock rate 128000
 encapsulation ppp
 ppp authentication chap
interface s0/0/1
 ip address 192.168.31.1 255.255.255.252
 encapsulation ppp
 ppp authentication pap
exit
router ospf 1
 router-id 1.1.1.1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.13.0 0.0.0.3 area 0
 passive-interface g0/1
exit
line con 0
 password cisco
```

```
logging synchronous
login
line vty 0 4
password cisco
login
```

Configuración del router R2:

```
hostname R2
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R1 password chap123
username r3 password chap123
interface lo0
 ip address 209.165.200.225 255.255.255.252
interface s0/0/0
 ip address 192.168.12.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
interface s0/0/1
 ip address 192.168.23.1 255.255.255.252
 clock rate 128000
no shutdown
exit
router ospf 1
 router-id 2.2.2.2
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 default-information originate
exit
ip route 0.0.0.0 0.0.0.0 loopback0
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

Configuración del router R3:

```
hostname R3
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
```

```
username R3 password chap123
interface g0/1
  ip address 192.168.3.1 255.255.255.0
  no shutdown
interface s0/0/0
  ip address 192.168.13.2 255.255.255.252
  clock rate 128000
  encapsulation ppp
  ppp authentication chap
  no shutdown
interface s0/0/1
  ip address 192.168.23.2 255.255.255.252
  encapsulation ppp
  ppp authentication chap
  no shutdown
exit
router ospf 1
  router-id 3.3.3.3
  network 192.168.13.0 0.0.0.3 area 0
  network 192.168.23.0 0.0.0.3 area 0
  passive-interface g0/1
line con 0
  password cisco
  logging synchronous
  login
line vty 0 4
  password cisco
  login
```

Paso 4: Guardar la configuración en ejecución.

Parte 2: Resolver problemas de la capa de enlace de datos

En la parte 2, utilizará comandos **show** para resolver problemas de la capa de enlace de datos. Asegúrese de verificar las configuraciones, como la frecuencia de reloj, la encapsulación, CHAP, los nombres de usuario y las contraseñas.

Paso 1: Examinar la configuración del R1.

- a. Utilice el comando **show interfaces** para determinar si se estableció PPP en ambos enlaces seriales.

Sobre la base de los resultados de **show interfaces** para S0/0/0 y S0/0/1, ¿cuáles son los posibles problemas con los enlaces PPP?

- b. Utilice el comando **debug ppp authentication** para ver el resultado en tiempo real de la autenticación PPP durante la resolución de problemas.

```
R1# debug ppp authentication
PPP authentication debugging is on
```

- c. Utilice el comando **show run interface s0/0/0** para examinar la configuración en S0/0/0.

Resuelva todos los problemas que detecte para S0/0/0. Registre los comandos utilizados para corregir la configuración.

Después de corregir el problema, ¿qué información proporciona el resultado de debug?

- d. Utilice el comando **show run interface s0/0/1** para examinar la configuración en S0/0/1.

Resuelva todos los problemas que detecte para S0/0/1. Registre los comandos utilizados para corregir la configuración.

Después de corregir el problema, ¿qué información proporciona el resultado de debug?

- e. Utilice el comando **no debug ppp authentication** o **undebg all** para desactivar el resultado de la depuración de PPP.

- f. Utilice el comando **show running-config | include username** para verificar la configuración correcta del nombre de usuario y la contraseña.

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

Paso 2: Examinar la configuración del R2.

- a. Utilice el comando **show interfaces** para determinar si se estableció PPP en ambos enlaces seriales.

¿Se establecieron todos los enlaces? _____

Si la respuesta es negativa, ¿cuáles son los enlaces que se deben examinar? ¿Cuáles son los problemas posibles?

- b. Utilice el comando **show run interface** para examinar los enlaces que no se establecieron.
- Resuelva todos los problemas que detecte para las interfaces. Registre los comandos utilizados para corregir la configuración.

- c. Utilice el comando **show running-config | include username** para verificar la configuración correcta del nombre de usuario y la contraseña.

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

- d. Utilice el comando **show ppp interface serial** para la interfaz serial cuyos problemas debe resolver.

¿Se estableció el enlace? _____

Paso 3: Examinar la configuración del R3.

- a. Utilice el comando **show interfaces** para determinar si se estableció PPP en ambos enlaces seriales.

¿Se establecieron todos los enlaces? _____

Si la respuesta es negativa, ¿cuáles son los enlaces que se deben examinar? ¿Cuáles son los problemas posibles?

- b. Utilice el comando **show run interface** para examinar cualquier enlace serial que no se haya establecido.

Resuelva todos los problemas que detecte en las interfaces. Registre los comandos utilizados para corregir la configuración.

- c. Utilice el comando **show running-config | include username** para verificar la configuración correcta del nombre de usuario y la contraseña.

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

- d. Utilice el comando **show interface** para verificar que se hayan establecido los enlaces seriales.

e. ¿Se establecieron todos los enlaces PPP? _____

f. ¿Se puede hacer ping de la PC-A a Lo0? _____

g. ¿Puede PC-A hacer ping a PC-C? _____

Nota: puede ser necesario deshabilitar el firewall de las computadoras para que los pings entre estas se realicen correctamente.

Parte 3: Resolver problemas de la capa de red

En la parte 3, verificará que se haya establecido la conectividad de capa 3 en todas las interfaces mediante el análisis de la configuración IPv4 y OSPF.

Paso 1: Verifique que las interfaces que se indican en la tabla de direccionamiento estén activas y configuradas con la información de dirección IP correcta.

Emita el comando **show ip interface brief** en todos los routers para verificar que las interfaces estén en estado up/up (activo/activo).

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

Paso 2: Verificar el routing OSPF.

Emita el comando **show ip protocols** para verificar que OSPF se esté ejecutando y que todas las redes se anuncien.

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

¿Puede PC-A hacer ping a PC-C? _____

Si no hay conectividad entre todos los hosts, continúe con la resolución de cualquier problema restante.

Nota: puede ser necesario deshabilitar el firewall de las computadoras para que los pings entre estas se realicen correctamente.

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)
<p>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.</p>				