Actividad colaborativa No 4

Diplomada de Profundización CISCO

Presentado por:

Yeison Javier Martinez Claros

Leidy Constanza Gutierrez Sanchez

Hawin Alexis Colmenares

Astrid Dayana Ordoñez

Brayan Leonardo García

Grupo: 203092_14

Tutor

Nilson Albeiro Ferreira

Univerisdad nacional abierta y a distacia UNAD

Cead Neiva

Introducción

El desarrollo de esta Cuarta actividad colaborativa es con el fin de fortalecer posteriormente el desarrollo de competencias en el área del saber específico orientadas a la Introducción a Enrutamiento Dinámico, OSPF de una sola área, Listas de control de acceso, DHCP, Traducción de direcciones IP para IPv4

Se realizara mediante el uso de las herramientas propuestas por el tutor del curso en el entorno de aprendizaje practico y de conocimiento en la plataforma, cada estudiante deberá realizar una serie de ejercicios con el fin de mejorar y aplicar conceptos y manejo de las redes, de igual forma el estudiante debe revisar el material sugerido para el abordaje de cada una de las temáticas.

En este trabajo colaborativo se desarrollara un trabajo grupal e individual donde el estudiante deberá revisar el material sugerido y desarrollar las actividades de forma óptima y eficaz dando resultado al compromiso acordado en el foro, con el fin de fortalecer posteriormente el desarrollo de competencias en el área del saber

Este trabajo colaborativo tiene como función desarrollar un potencial básico al estudiante de como configurar y administrar dispositivos de Networking mediante el estudio del modelo OSI, la arquitectura TCP/IP, y el uso de recursos y herramientas en función de los protocolos y servicios.

Se desarrollara una serie de tareas durante esta actividad con el fin de que cada uno de los integrantes del curso participen activamente creando así mismo un escenario de aprendizaje colaborativo en donde se plantearan inquietudes relacionadas con el desarrollo de las tareas propuestas, teniendo en cuenta que éstas pueden ser resueltas por algún estudiante.

Cada participación o aporte que se haga en el grupo se deberá publicar en el foro del entorno Colaborativo donde se establecerá un tema con el fin de que los estudiantes que pertenecen al grupo realicen una discusión académica en torno a cada una de las tareas

(Prácticas de laboratorio) adscritas a la Unidad 1, siguiendo tres fases secuenciales (pre-tarea, ciclo de tarea y pos-tarea), haciendo uso en toda intervención la Rúbrica TIGRE que ha sido realizado por el tutor del curso para discutir los resultados del Análisis individual de las tareas realizadas. Todos los estudiantes que forman parte del grupo deben subir sus aportes individuales al foro de trabajo colaborativo.

Cada una de las prácticas debe desarrollarse mediante el uso de la herramienta de Simulación PACKET TRACER y/o Laboratorio remoto (NETLAB) según sea requerido, las cuales se encuentran disponibles en el Entorno de Aprendizaje Práctico. En este escenario, el estudiante podrá hacer uso de cualquiera de las dos herramientas mencionadas con el fin de realizar los procesos de configuración de dispositivos de networking acorde con las indicaciones establecidas en cada una de las tareas (Prácticas de Laboratorio)

Al finalizar la actividad cada grupo deberá consolidar la información en documento Word con ciertos requerimiento dados por el tutor y todas las tareas deben ir acompañadas de su respectiva evidencia, ya sea como archivo de simulación o registro de su desarrollo en el laboratorio remoto para luego comprimirlas en archivo Zip y subirlo al entorno de evaluación y seguimiento para la respectiva revisión del tutor asignado del curso, cabe aclarar que dicha consolidación y construcción de este trabajo se realizara mediante la ayuda del tutor del curso asignado.

De igual forma cada estudiante deberá cumplir un rol o papel durante la actividad colaborativa para que dicho trabajo sea más organizado a la medida que se avance para la entrega del producto final

El estudiante que profundice en esta área del saber tendrá un amplio conocimiento donde lo podrá desarrollar en su vida profesional en el programa de Ingeniería de sistemas

Contenido

Práctica de laboratorio: configuración básica de RIPv2 y RIPng

Topología

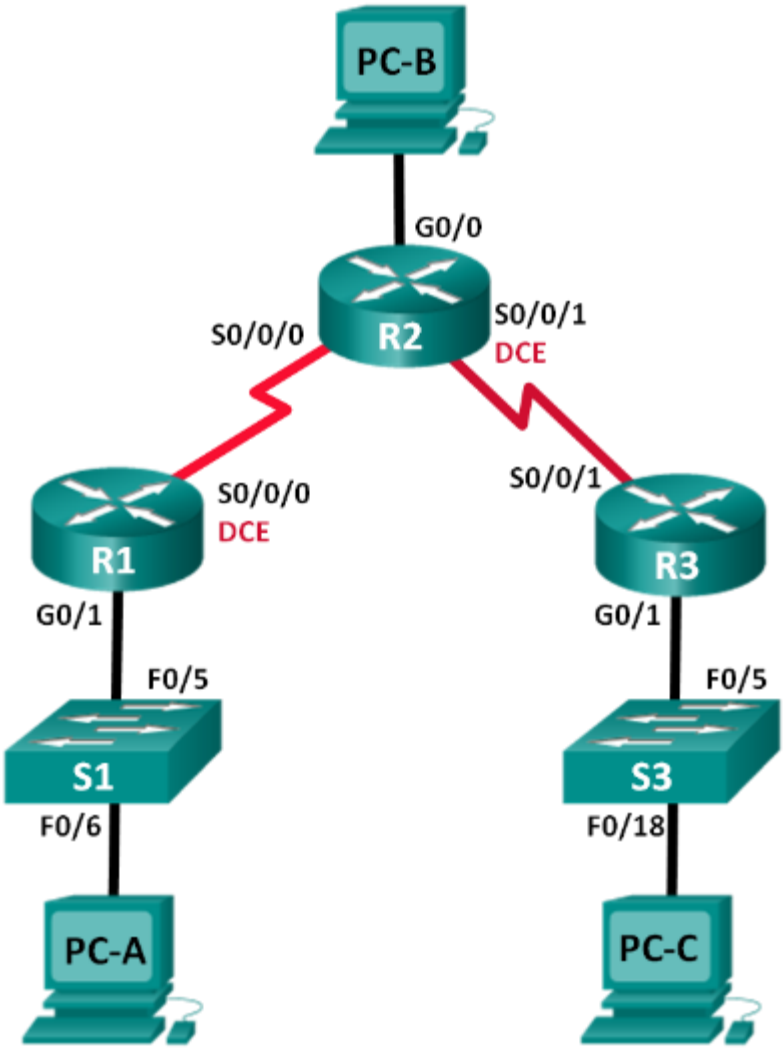


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	172.30.10.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar y verificar el routing RIPv2

- Configurar y verificar que se esté ejecutando RIPv2 en los routers.
- Configurar una interfaz pasiva.
- Examinar las tablas de routing.
- Desactivar la sumarización automática.
- Configurar una ruta predeterminada.
- Verificar la conectividad de extremo a extremo.

Parte 3: configurar IPv6 en los dispositivos

Parte 4: configurar y verificar el routing RIPng

- Configurar y verificar que se esté ejecutando RIPng en los routers.
- Examinar las tablas de routing.
- Configurar una ruta predeterminada.
- Verificar la conectividad de extremo a extremo.

Recursos necesarios

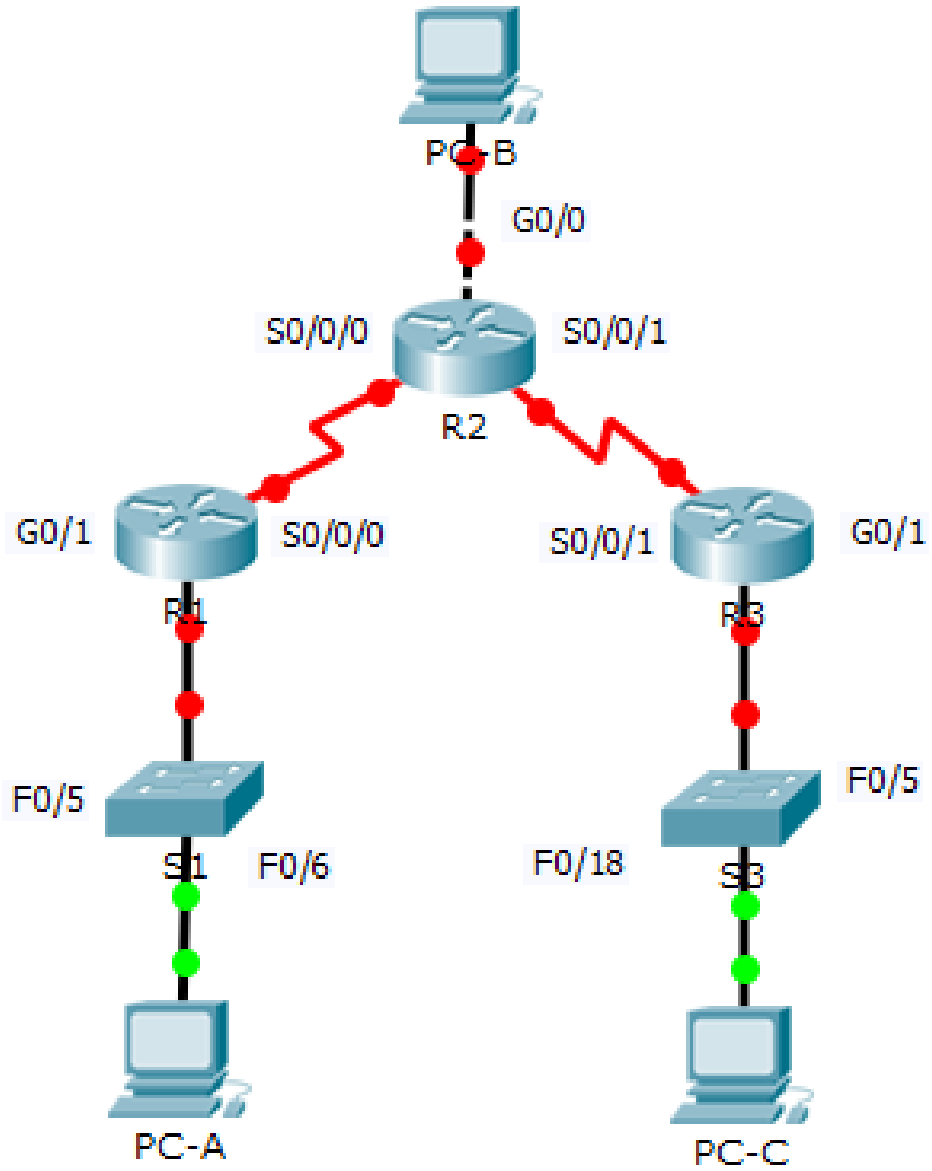
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

- 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: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos.

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



Paso 2. inicializar y volver a cargar el router y el switch.

Paso 3. configurar los parámetros básicos para cada router y switch.

a. Desactive la búsqueda del DNS.

b. Configure los nombres de los dispositivos como se muestra en la topología.

c. Configurar la encriptación de contraseñas.

d. Asigne **class** como la contraseña del modo EXEC privilegiado.

e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

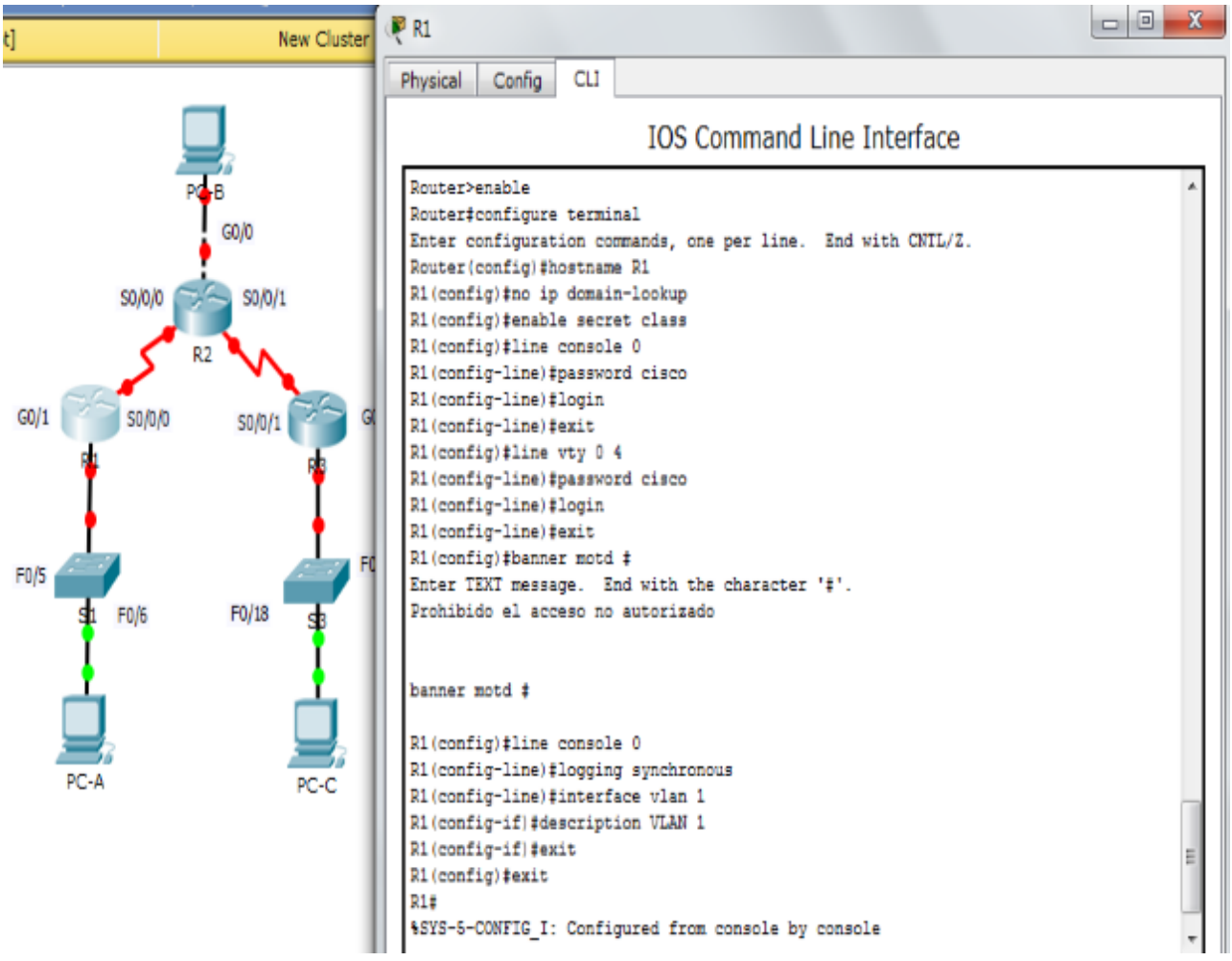
g. Configure **logging synchronous** para la línea de consola.

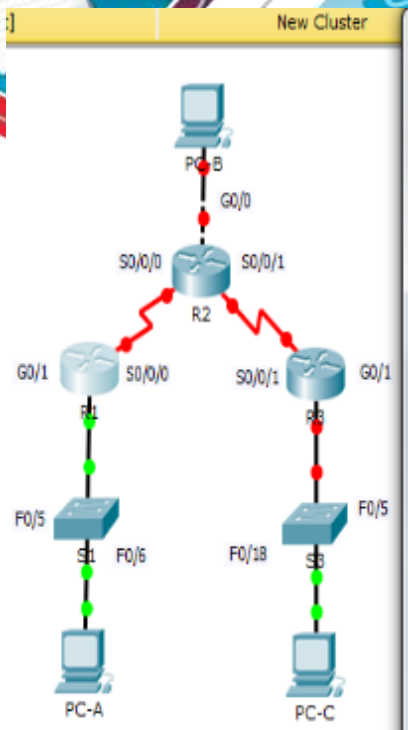
h. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.

i. Configure una descripción para cada interfaz con una dirección IP.

j. Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.

k. Copie la configuración en ejecución en la configuración de inicio.



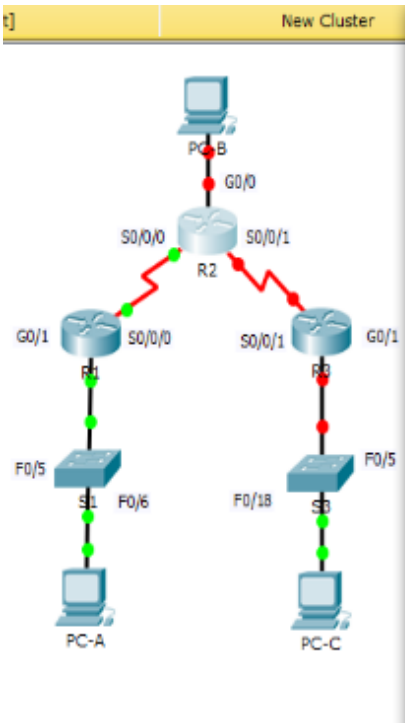


R1

Physical | Config | CLI

IOS Command Line Interface

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface G0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

R1(config-if)#exit
R1(config)#interface S0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 25000
Unknown clock rate
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

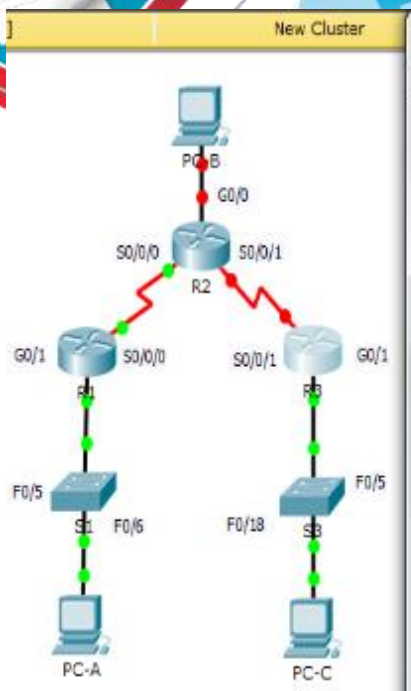


R2

Physical | Config | CLI

IOS Command Line Interface

```
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#bannerd motd #
                 ^
% Invalid input detected at '^' marker.

R2(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Prohibido el acceso no autorizado

line console 0
#

R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface S0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#
```

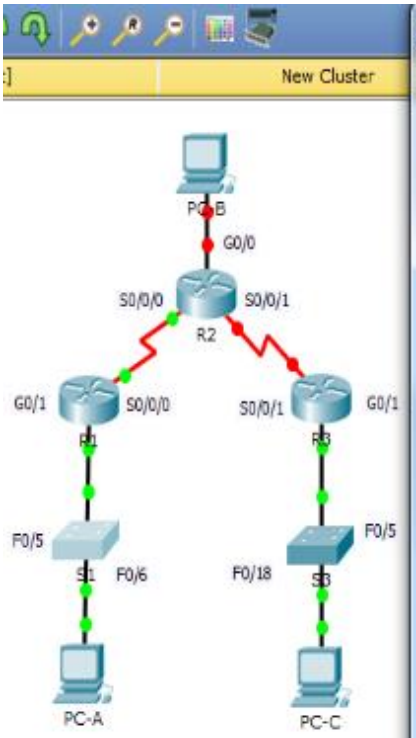


R3

Physical | Config | CLI

IOS Command Line Interface

```
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Prohibido el acceso a personal no autorizado
#

R3(config)#line console 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface S0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R3(config-if)#interface G0/1
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up
```

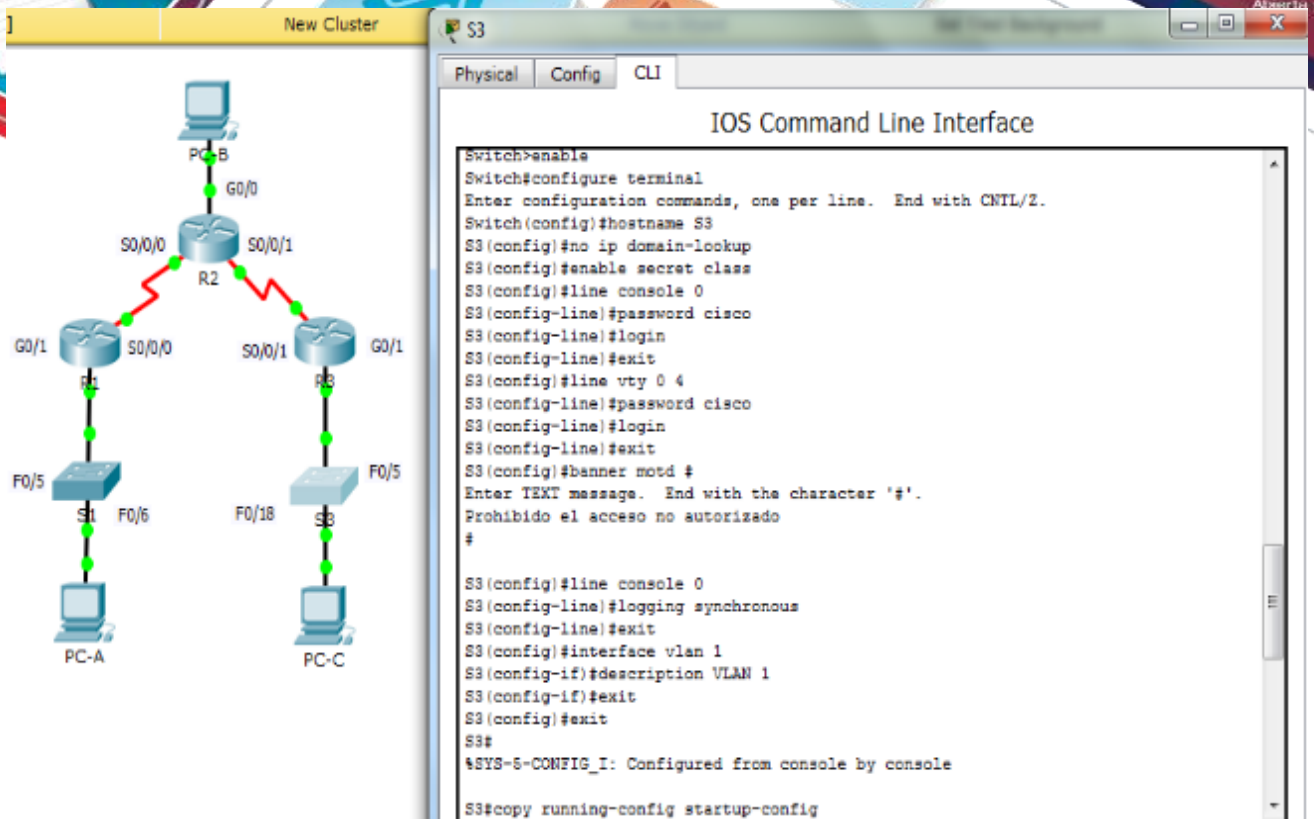


S1

Physical | Config | CLI

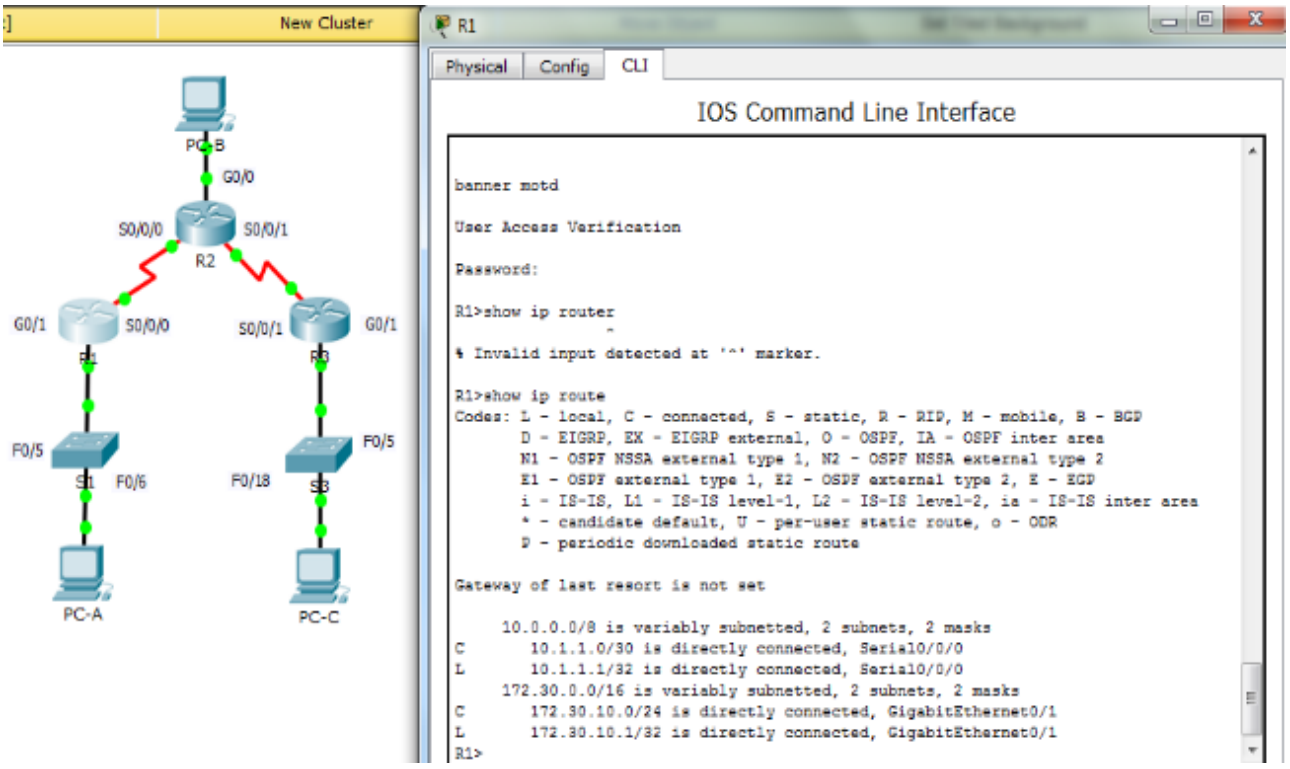
IOS Command Line Interface

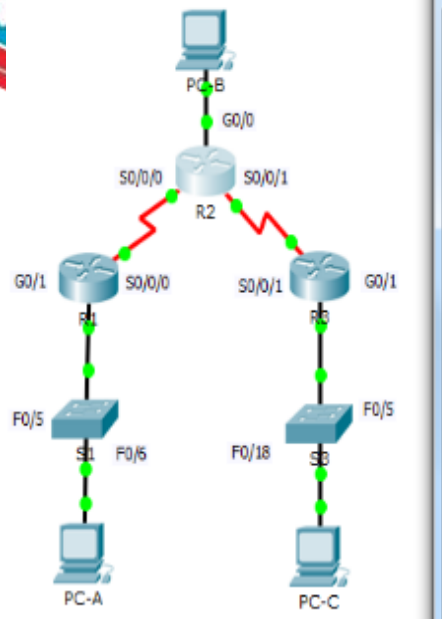
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#login
% Login disabled on line 1, until 'password' is set
% Login disabled on line 2, until 'password' is set
% Login disabled on line 3, until 'password' is set
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#line console 0
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Prohibido el acceso no autorizado
#

S1(config)#interface vlan 1
S1(config-if)#description VLAN 1
S1(config-if)#exit
```



Paso 4. configurar los equipos host.

Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.



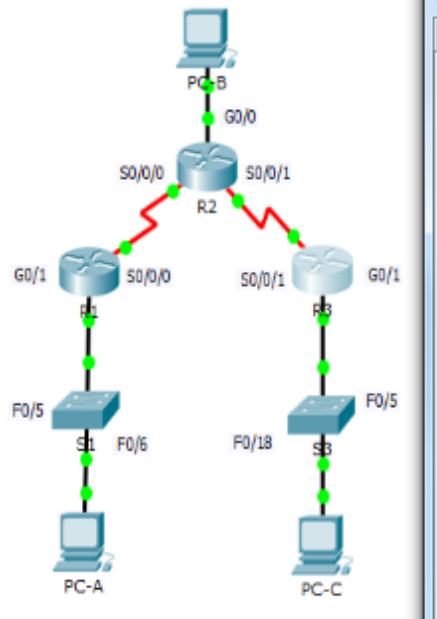


R2

Physical | Config | CLI

IOS Command Line Interface

```
R2#copy runnig-config startup-config
                   ^
% Invalid input detected at '^' marker.

R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
R2#
```



R3

Physical | Config | CLI

IOS Command Line Interface

```
Prohibido el acceso a personal no autorizado


User Access Verification

Password:

R3>ip show route
         ^
% Invalid input detected at '^' marker.

R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1
R3>
```

Probar la conectividad.

En este momento, las computadoras no pueden hacerse ping entre sí.

a. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.

b. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

Parte 2: configurar y verificar el routing RIPv2

En la parte 2, configurará el routing RIPv2 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente. Una vez que haya verificado RIPv2, deshabilitará el sumarización automática, configurará una ruta predeterminada y verificará la conectividad de extremo a extremo.

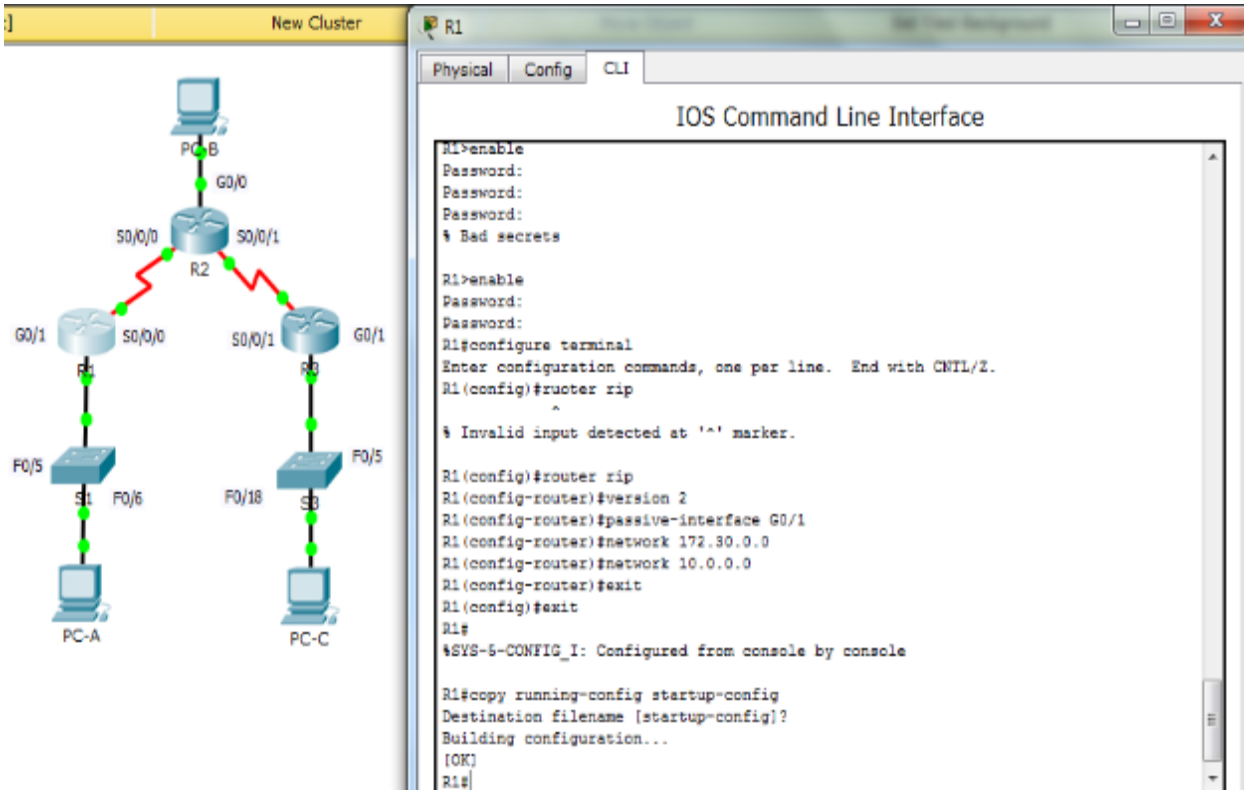
Configurar el enrutamiento RIPv2.

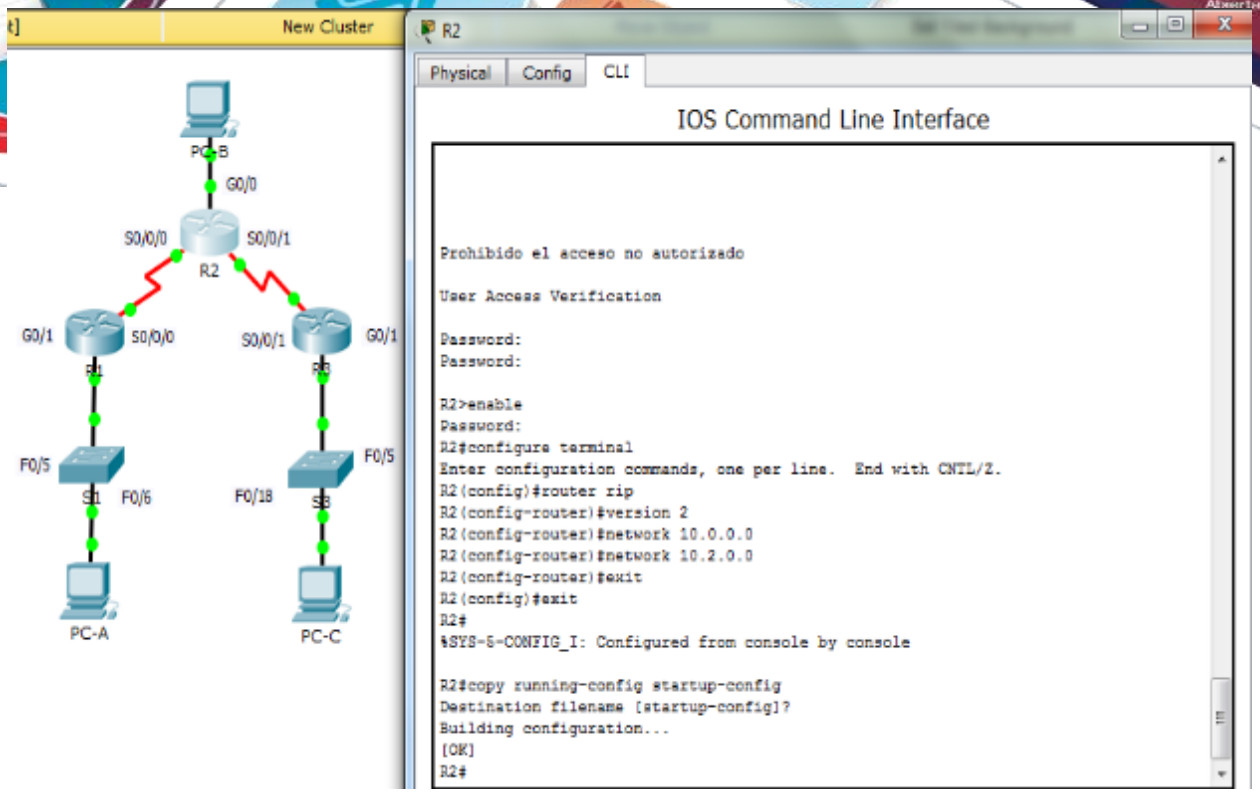
a. En el R1, configure RIPv2 como el protocolo de routing y anuncie las redes correspondientes.

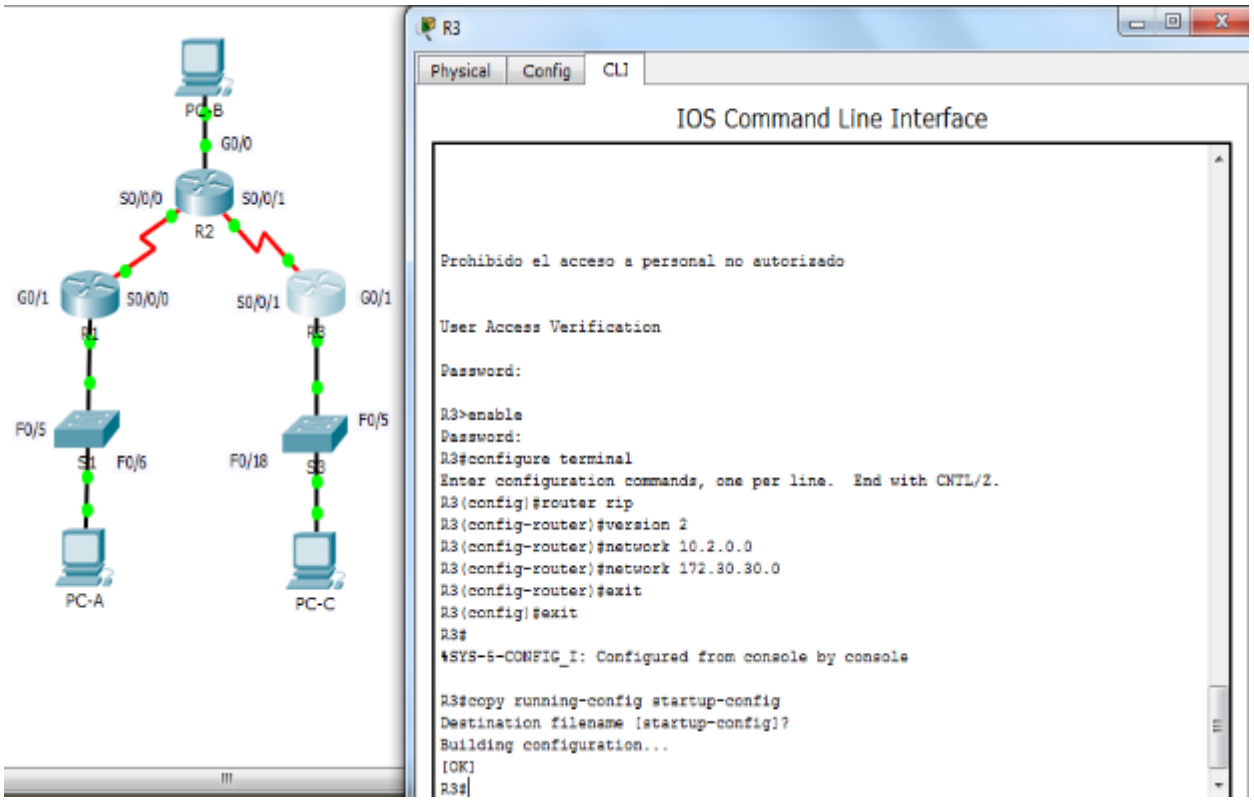
```
R1# config t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# passive-interface g0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```

b. Configure RIPv2 en el R3 y utilice la instrucción **network** para agregar las redes apropiadas y evitar actualizaciones de routing en la interfaz LAN.

c. Configure RIPv2 en el R2. No anuncie la red 209.165.201.0.




New Cluster
PC-B
G0/0
S0/0/0
S0/0/1
R2
G0/1
S0/0/0
S0/0/1
G0/1
F0/5
S1
F0/6
F0/18
S3
F0/5
PC-A
PC-C
R2
Physical
Config
CLI
IOS Command Line Interface
Prohibido el acceso no autorizado
User Access Verification
Password:
Password:
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#network 10.2.0.0
R2(config-router)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#


PC-B
G0/0
S0/0/0
S0/0/1
R2
G0/1
S0/0/0
S0/0/1
G0/1
F0/5
S1
F0/6
F0/18
S3
F0/5
PC-A
PC-C
R3
Physical
Config
CLI
IOS Command Line Interface
Prohibido el acceso a personal no autorizado
User Access Verification
Password:
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 10.2.0.0
R3(config-router)#network 172.30.30.0
R3(config-router)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#

Paso 5. examinar el estado actual de la red.

a. Se pueden verificar los dos enlaces seriales rápidamente mediante el comando **show ip interface brief** en R2.

```
R2# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         209.165.201.1   YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                10.1.1.2        YES manual up                    up
Serial0/0/1                10.2.2.2        YES manual up                    up
```

b. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? NO

¿Es posible hacer ping de la PC-A a la PC-C? SI

¿Es posible hacer ping de la PC-C a la PC-B? NO

¿Es posible hacer ping de la PC-C a la PC-A? SI

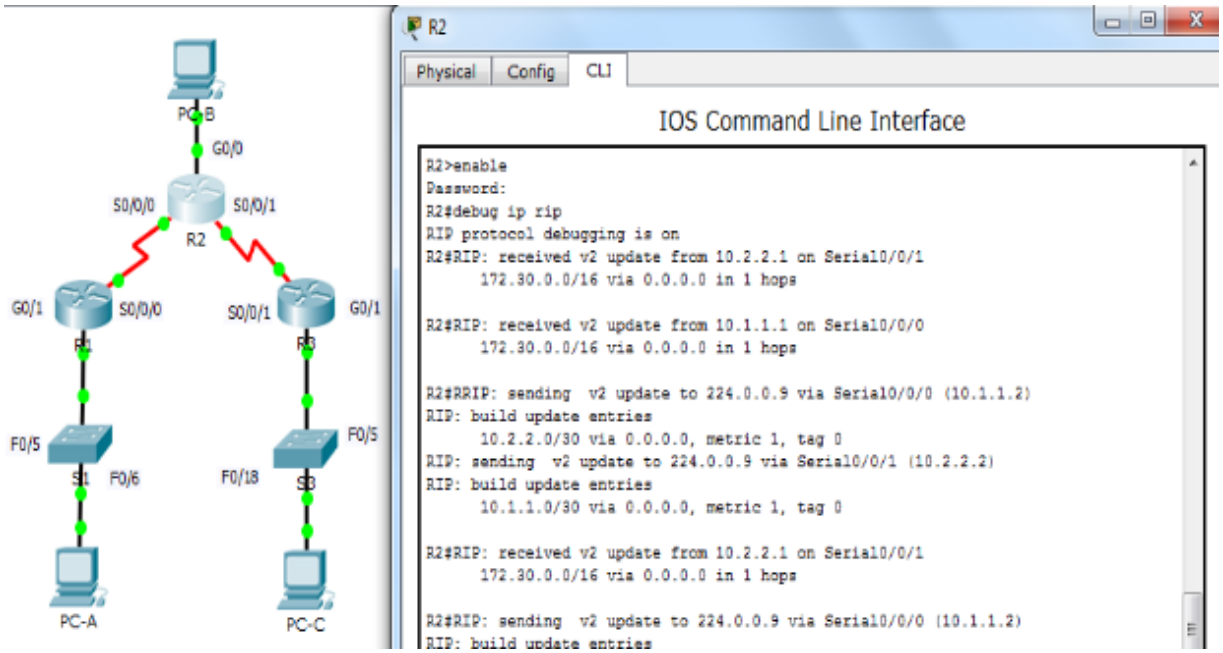
c. Verifique que RIPv2 se ejecute en los routers.

Puede usar los comandos **debug ip rip**, **show ip protocols** y **show run** para confirmar que RIPv2 esté en ejecución. A continuación, se muestra el resultado del comando **show ip protocols** para el R1.

```
R1# show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
    GigabitEthernet0/1
Routing Information Sources:
  Gateway         Distance      Last Update
  10.1.1.2              120
Distance: (default is 120)
```

Al emitir el comando **debug ip rip** en el R2, ¿qué información se proporciona que confirma que RIPv2 está en ejecución?

RIP protocol debugging este encendido



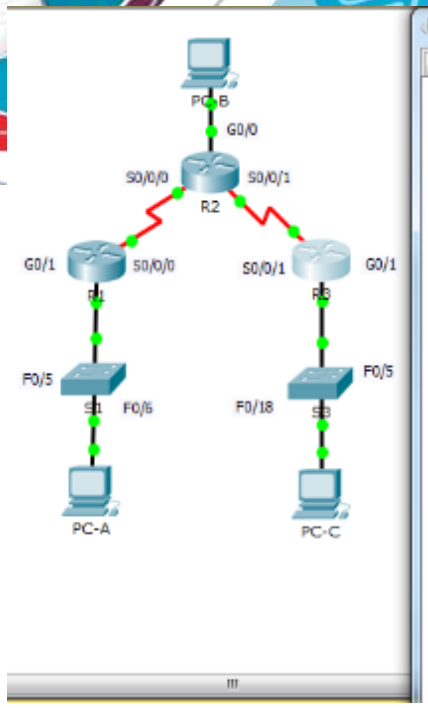
Cuando haya terminado de observar los resultados de la depuración, emita el comando **undebug all** en la petición de entrada del modo EXEC privilegiado.

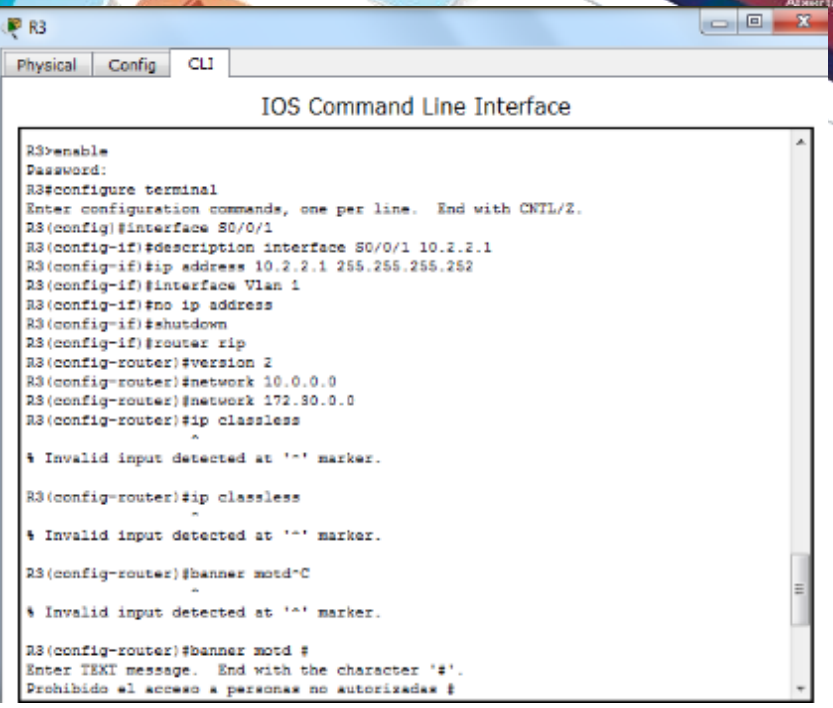
Al emitir el comando **show run** en el R3, ¿qué información se proporciona que confirma que RIPv2 está en ejecución?

Router RIP

Network 10.0.0.0

Network 172.30.0.0





d. Examinar el sumarización automática de las rutas.

Las LAN conectadas al R1 y el R3 se componen de redes no contiguas. El R2 muestra dos rutas de igual costo a la red 172.30.0.0/16 en la tabla de routing. El R2 solo muestra la dirección de red principal con clase 172.30.0.0 y no muestra ninguna de las subredes de esta red.

```
R2# show ip route
<Output Omitted>
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.2/32 is directly connected, Serial0/0/1
R     172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
                    [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/24 is directly connected, GigabitEthernet0/0
L        209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

El R1 solo muestra sus propias subredes para la red 172.30.0.0. El R1 no tiene ninguna ruta para las subredes 172.30.0.0 en el R3.

```
R1# show ip route
<Output Omitted>
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
R        10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
      172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.30.10.0/24 is directly connected, GigabitEthernet0/1
L        172.30.10.1/32 is directly connected, GigabitEthernet0/1
```

El R3 solo muestra sus propias subredes para la red 172.30.0.0. El R3 no tiene ninguna ruta para las subredes 172.30.0.0 en el R1.

```
R3# show ip route
<Output Omitted>
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
R        10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.30.30.0/24 is directly connected, GigabitEthernet0/1
L        172.30.30.1/32 is directly connected, GigabitEthernet0/1
```

Utilice el comando **debug ip rip** en el R2 para determinar las rutas recibidas en las actualizaciones RIP del R3 e indíquelas a continuación.

172.30.0.0

10.1.1.0

El R3 no está envía ninguna de las subredes 172.30.0.0, solo la ruta resumida 172.30.0.0/16, incluida la máscara de subred. Por lo tanto, las tablas de routing del R1 y el R2 no muestran las subredes 172.30.0.0 en el R3.

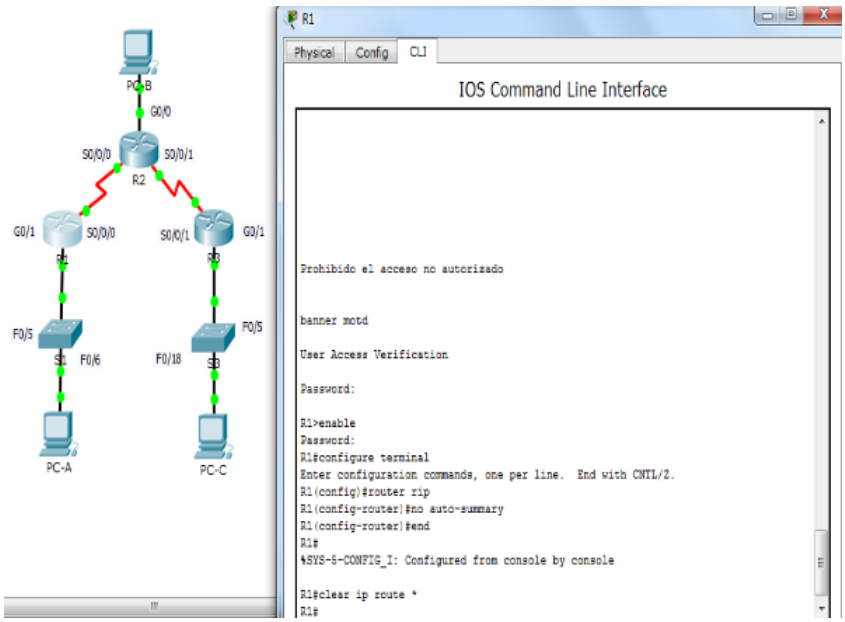
Paso 6. Desactivar la sumarización automática.

a. El comando **no auto-summary** se utiliza para desactivar la sumarización automática en RIPv2. Deshabilite la sumarización automática en todos los routers. Los routers ya no resumirán las rutas en los límites de las redes principales con clase. Aquí se muestra R1 como ejemplo.

```
R1(config)# router rip
R1(config-router)# no auto-summary
```

b. Emita el comando **clear ip route *** para borrar la tabla de routing.

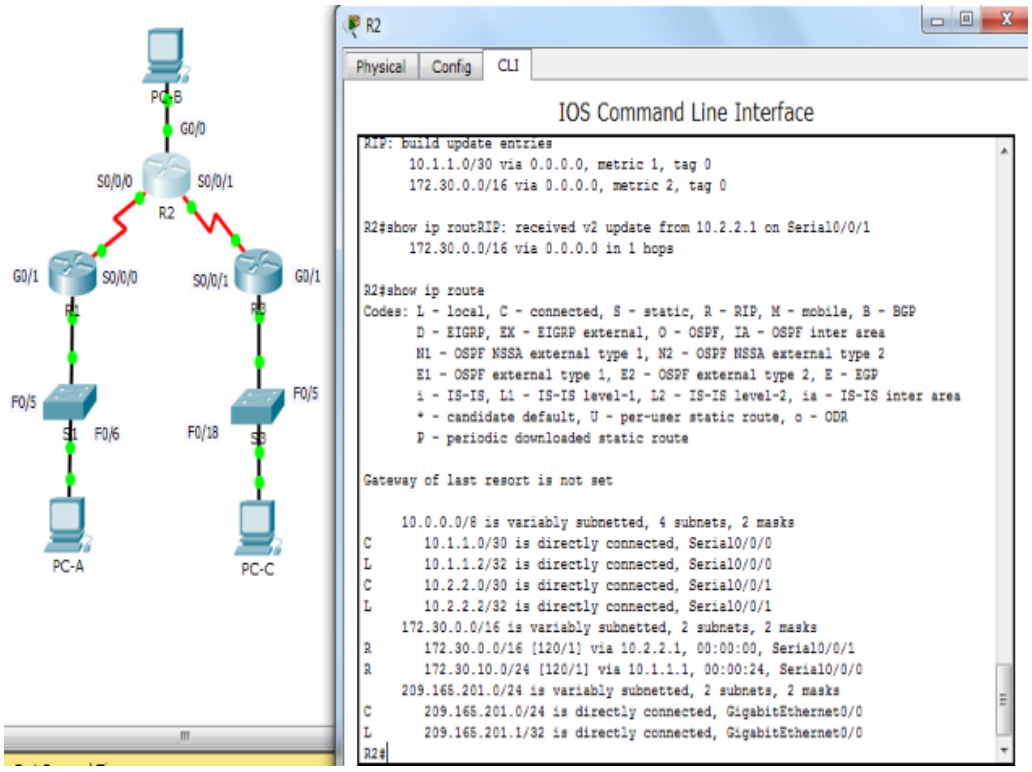
```
R1(config-router)# end
R1# clear ip route *
```



c. Examinar las tablas de enrutamiento Recuerde que la convergencia de las tablas de routing demora un tiempo después de borrarlas.

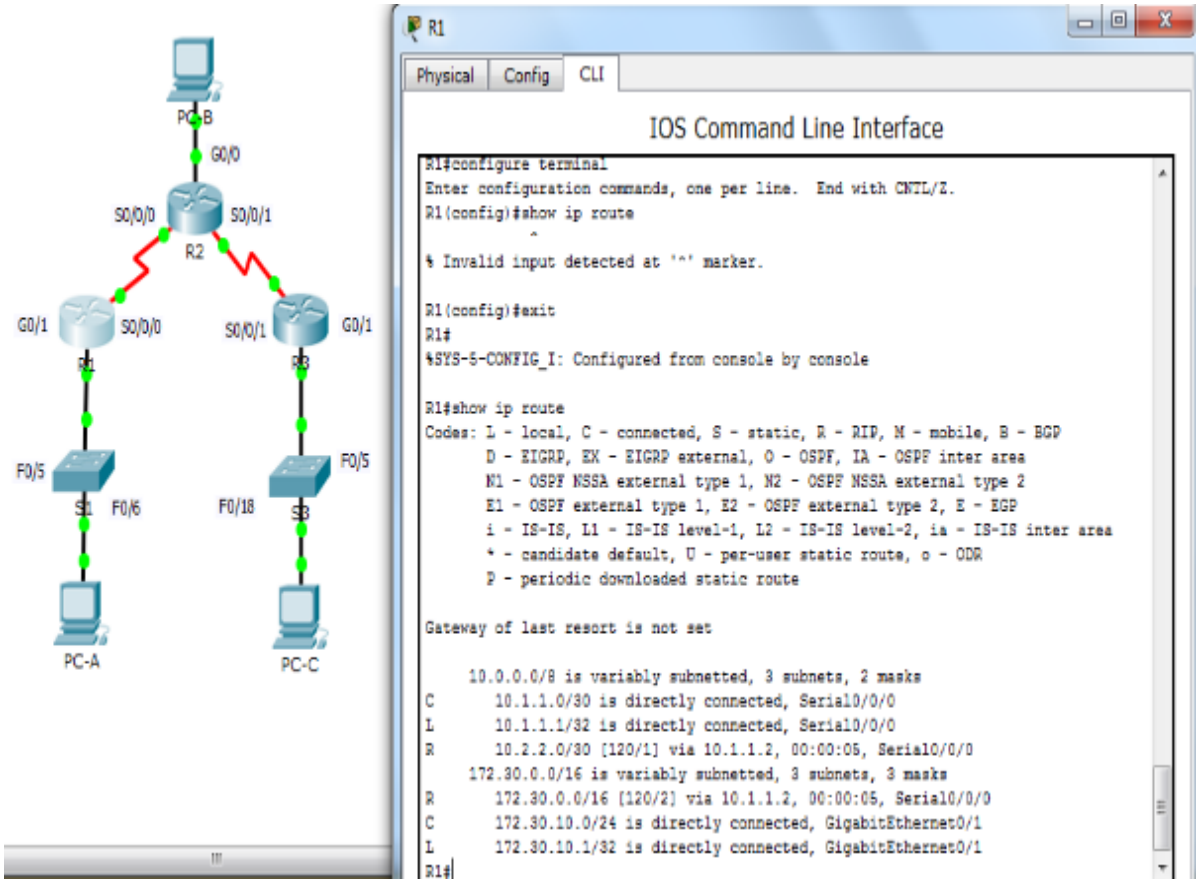
Las subredes LAN conectadas al R1 y el R3 ahora deberían aparecer en las tres tablas de routing.

```
R2# show ip route
<Output Omitted>
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.2/32 is directly connected, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R        172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:01, Serial0/0/1
                       [120/1] via 10.1.1.1, 00:01:15, Serial0/0/0
R        172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0
R        172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04, Serial0/0/1
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/24 is directly connected, GigabitEthernet0/0
L        209.165.201.1/32 is directly connected, GigabitEthernet0/0
```



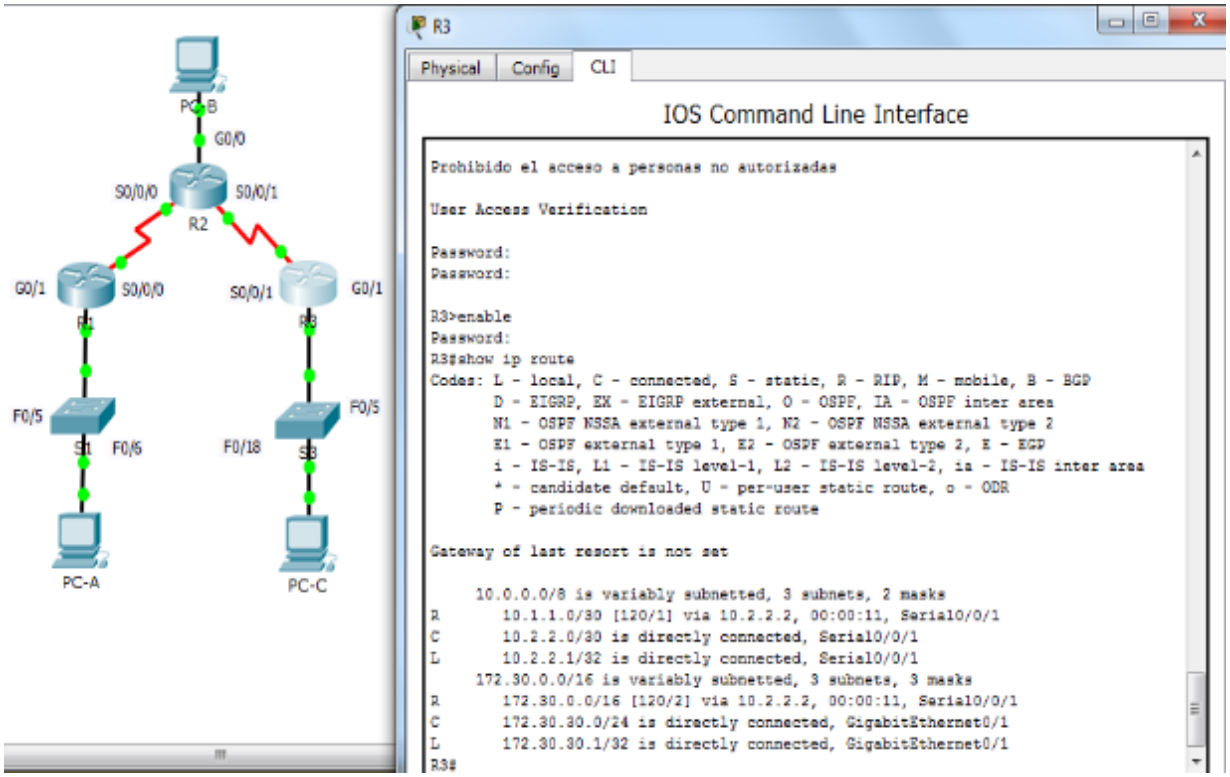

```
R1# show ip route
<Output Omitted>
```

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
R        10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0
      172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.30.10.0/24 is directly connected, GigabitEthernet0/1
L        172.30.10.1/32 is directly connected, GigabitEthernet0/1
R        172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0
```



R3# **show ip route**

```
<Output Omitted>
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
R        10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.30.30.0/24 is directly connected, GigabitEthernet0/1
L        172.30.30.1/32 is directly connected, GigabitEthernet0/1
R        172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1
```



d. Utilice el comando **debug ip rip** en el R2 para examinar las actualizaciones RIP.

R2# debug ip rip

Después de 60 segundos, emita el comando **no debug ip rip**.

¿Qué rutas que se reciben del R3 se encuentran en las actualizaciones RIP?

10.2.2.2

172.30.30.0

¿Se incluyen ahora las máscaras de las subredes en las actualizaciones de enrutamiento? Si se incluyen

Paso 7. Configure y redistribuya una ruta predeterminada para el acceso a Internet.

a. Desde el R2, cree una ruta estática a la red 0.0.0.0 0.0.0.0, con el comando **ip route**. Esto envía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet al establecer un gateway de último recurso en el router R2.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

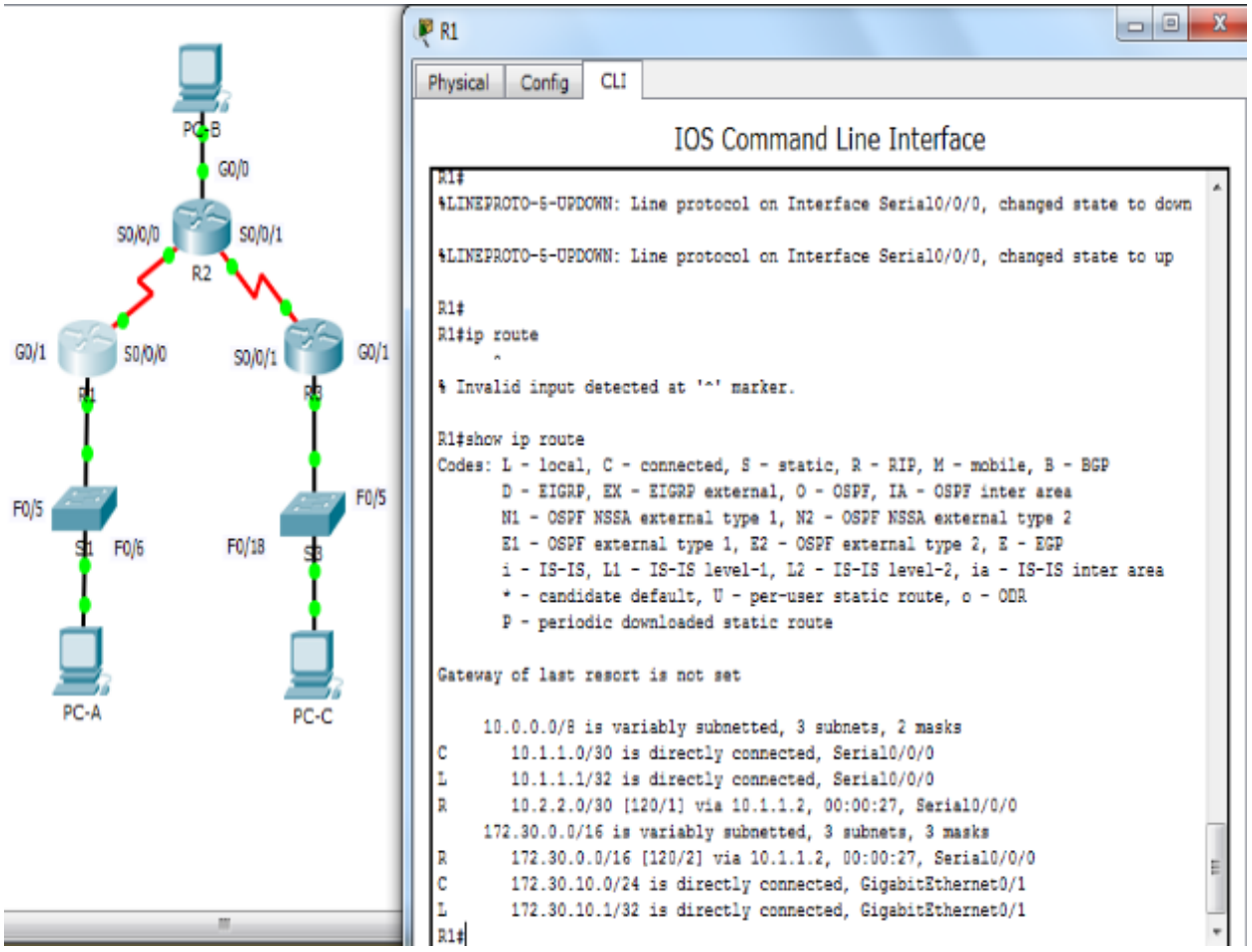
b. El R2 anunciará una ruta a los otros routers si se agrega el comando **default-information originate** a la configuración de RIP.

```
R2(config)# router rip
R2(config-router)# default-information originate
```

Paso 8. Verificar la configuración de enrutamiento.

c. Consulte la tabla de routing en el R1.

```
R1# show ip route
<Output Omitted>
Gateway of last resort is 10.1.1.2 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
R        10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
      172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.30.10.0/24 is directly connected, GigabitEthernet0/1
L        172.30.10.1/32 is directly connected, GigabitEthernet0/1
R        172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0
```

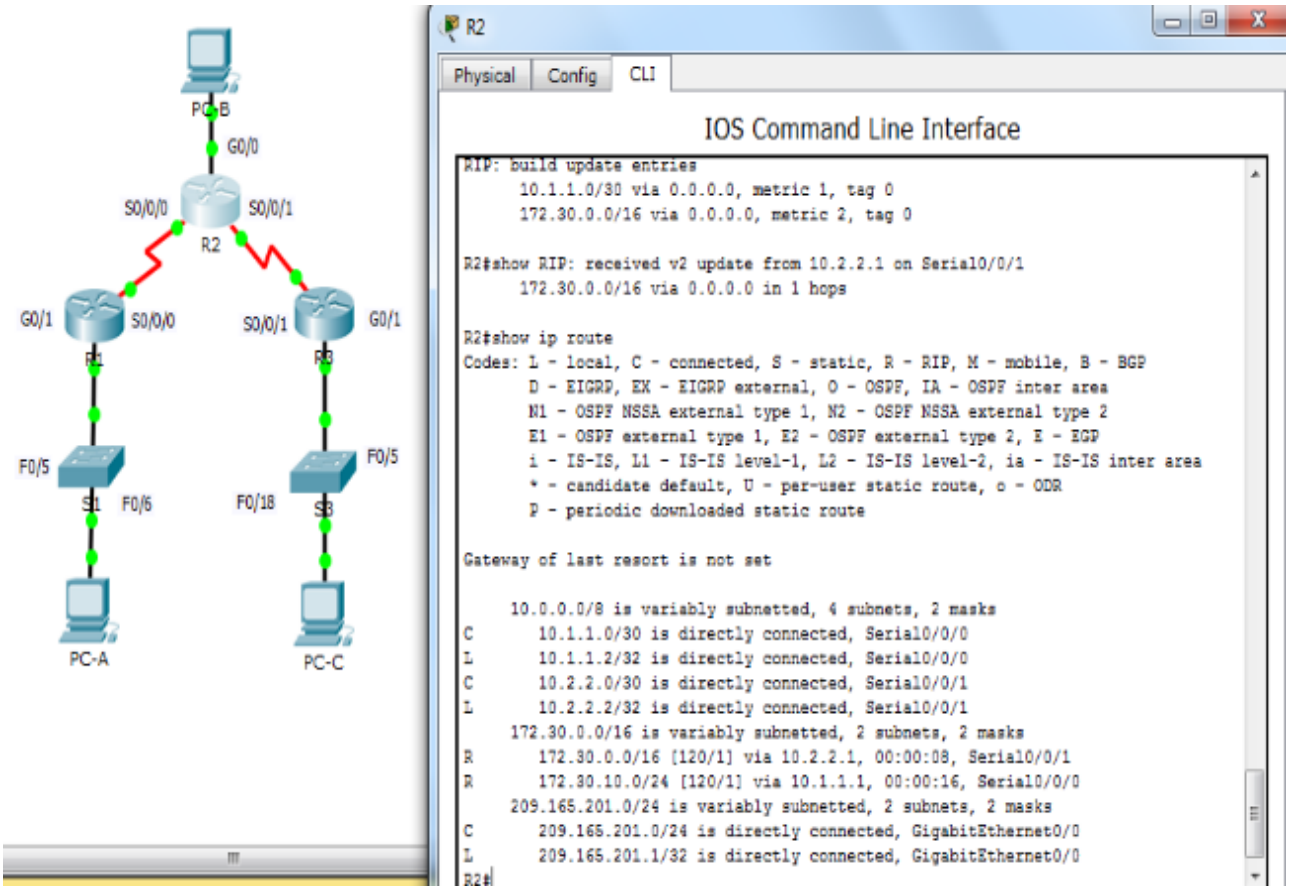


¿Cómo se puede saber, a partir de la tabla de routing, que la red dividida en subredes que comparten el R1 y el R3 tiene una ruta para el tráfico de Internet?

Porque la ruta estática predeterminada aparece publicada en los router R1 y R3

Por medio del RIP

d. Consulte la tabla de routing en el R2.



¿En qué forma se proporciona la ruta para el tráfico de Internet en la tabla de routing?

Publicando en los demás routers la ruta estática predeterminada

Paso 9. Verifique la conectividad.

a. Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 209.165.201.2.

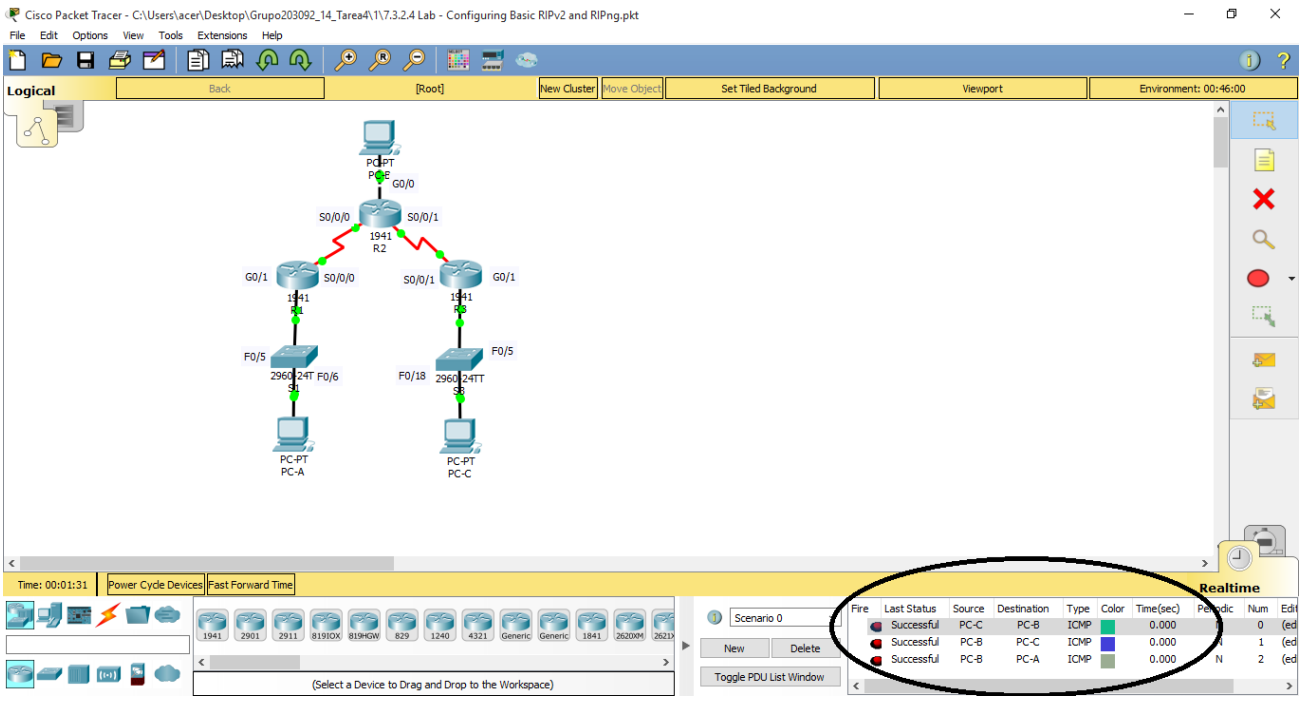
¿Tuvieron éxito los pings? Si

b. Verifique que los hosts dentro de la red dividida en subredes tengan posibilidad de conexión entre sí haciendo ping entre la PC-A y la PC-C.

¿Tuvieron éxito los pings? Si

Nota: quizá sea necesario deshabilitar el firewall de las computadoras.

Parte 3: configurar IPv6 en los dispositivos



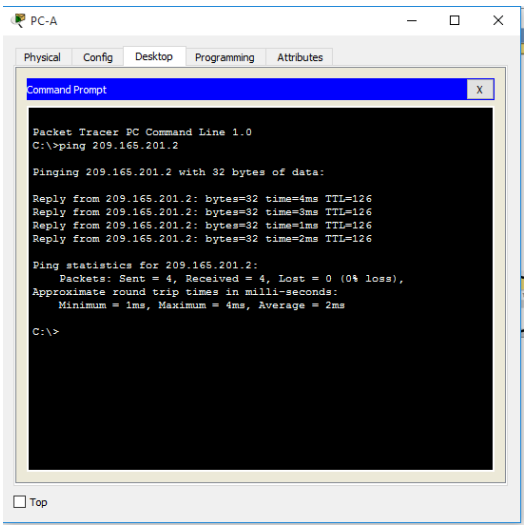
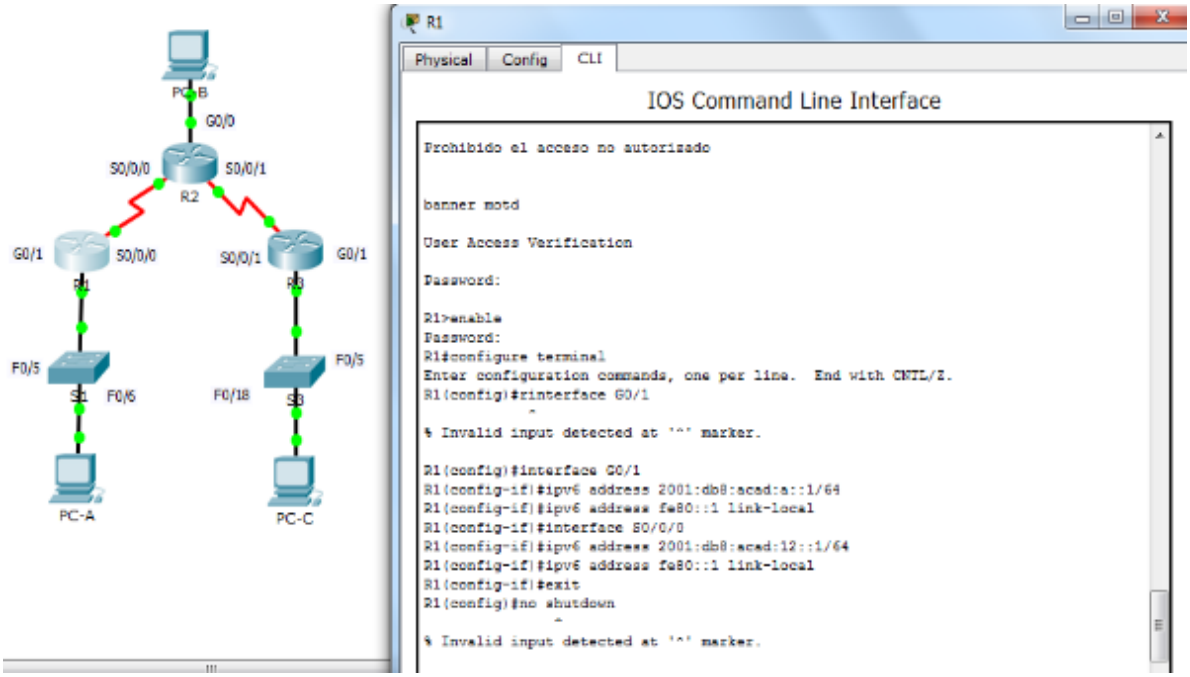
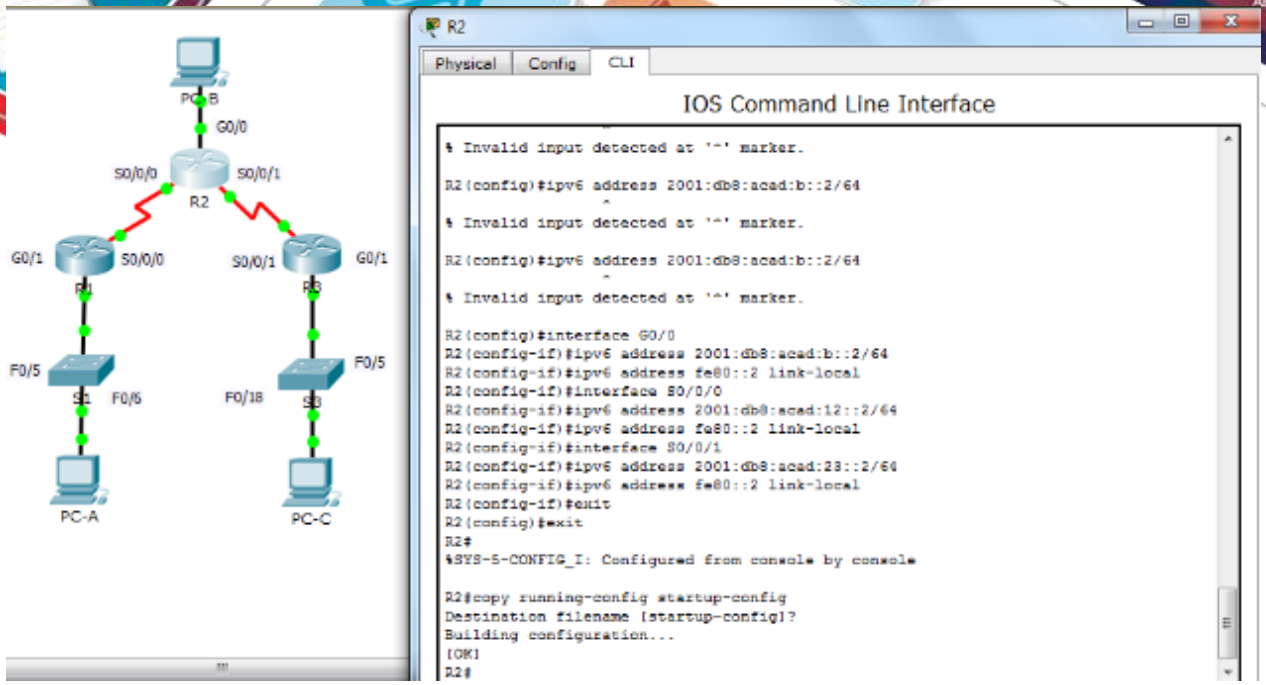
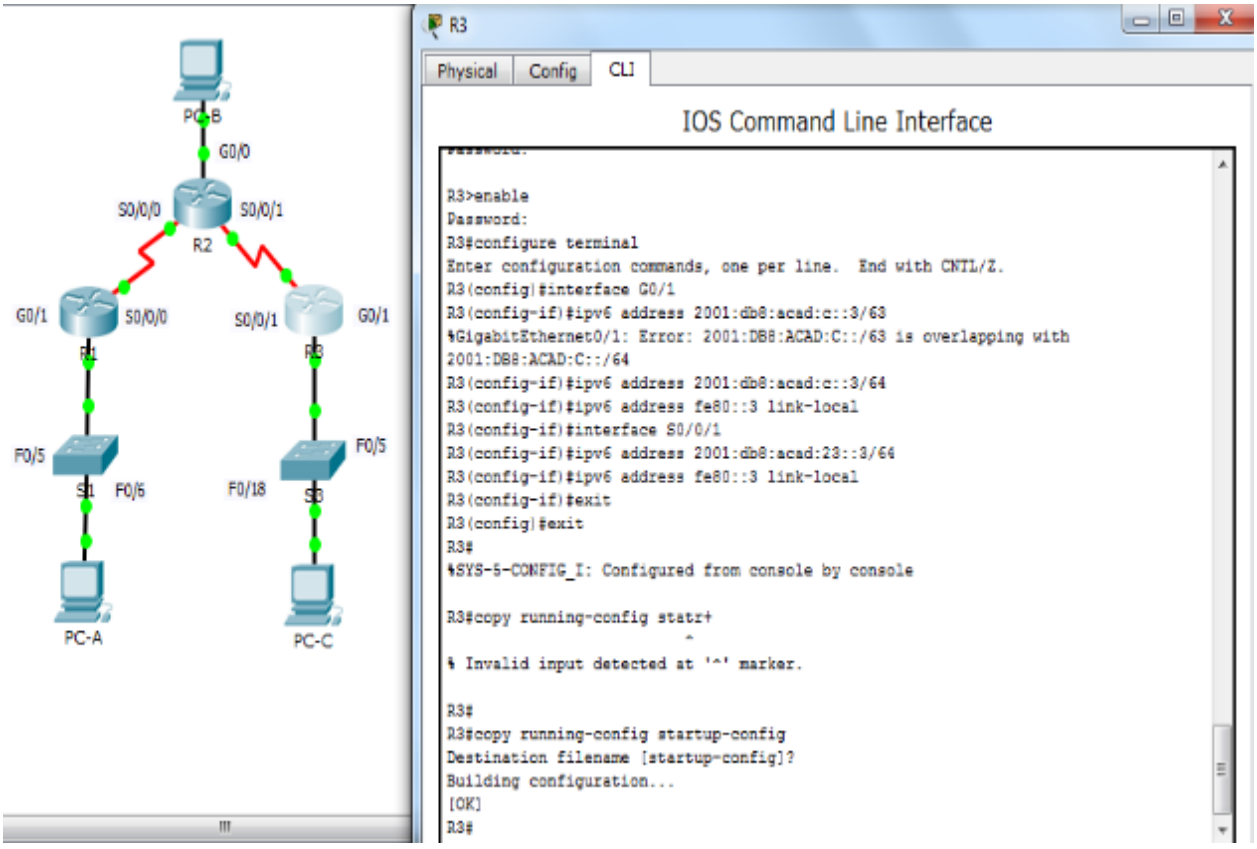


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6/longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1 link-local	No aplicable
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2 link-local	No aplicable
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	No aplicable
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

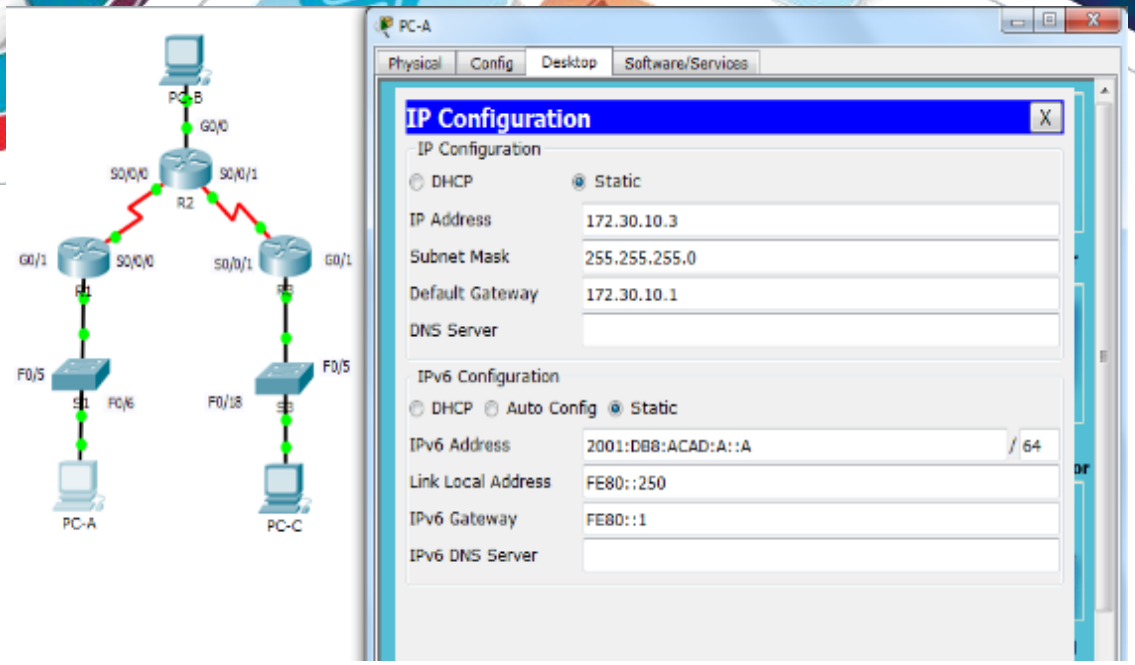


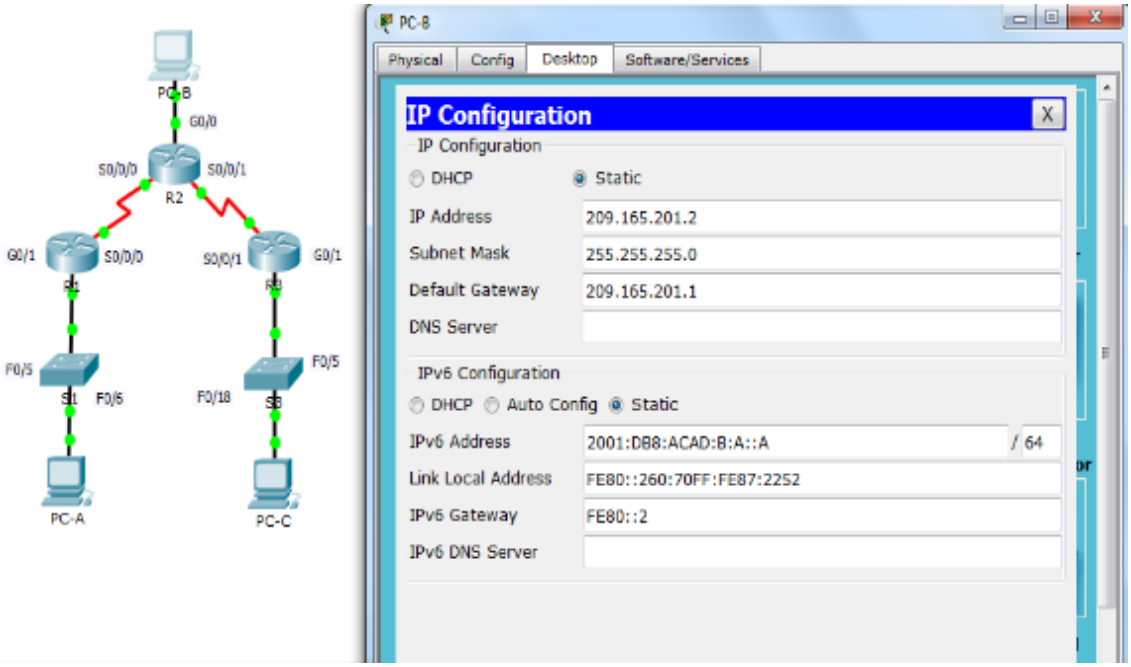


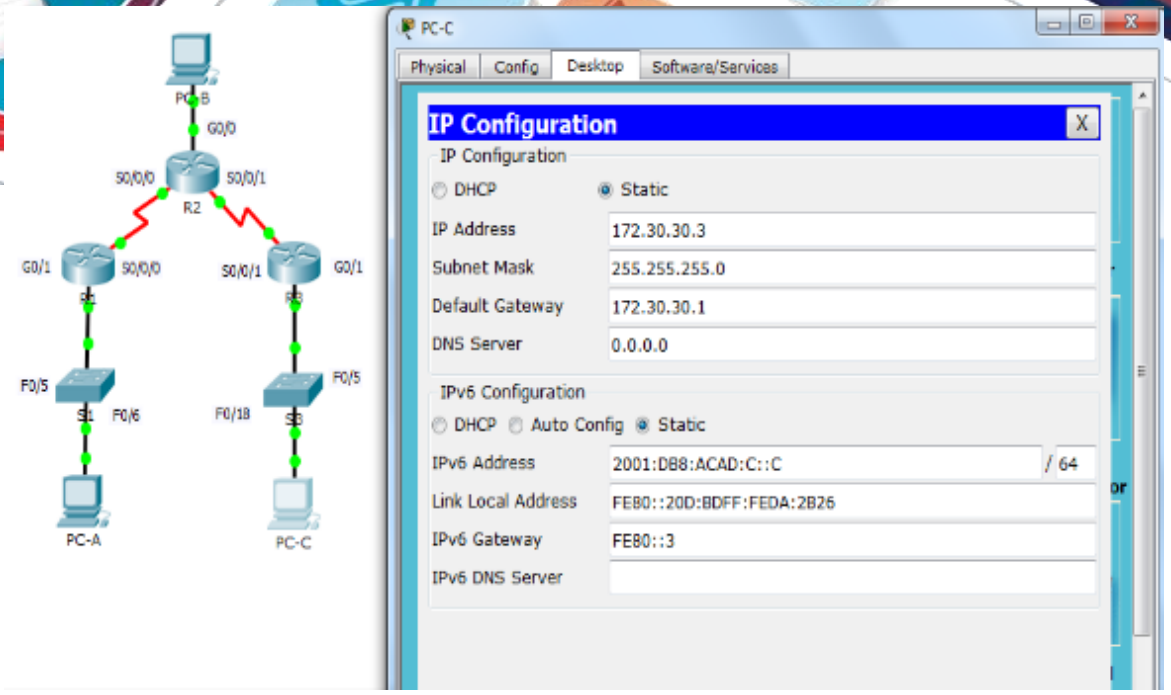


Paso 1. configurar los equipos host.

Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.


PC-B
G0/0
S0/0/0
S0/0/1
R2
G0/1
S0/0/0
S0/0/1
G0/1
F0/5
F0/6
F0/18
F0/5
PC-A
PC-C
PC-A
Physical
Config
Desktop
Software/Services
IP Configuration
IP Configuration
DHCP
Static
IP Address
172.30.10.3
Subnet Mask
255.255.255.0
Default Gateway
172.30.10.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:ACAD:A::A
/ 64
Link Local Address
FE80::250
IPv6 Gateway
FE80::1
IPv6 DNS Server


PC-B
G0/0
S0/0/0
S0/0/1
R2
G0/1
S0/0/0
S0/0/1
G0/1
F0/5
F0/6
F0/18
F0/5
PC-A
PC-C
PC-B
Physical
Config
Desktop
Software/Services
IP Configuration
IP Configuration
DHCP
Static
IP Address
209.165.201.2
Subnet Mask
255.255.255.0
Default Gateway
209.165.201.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:ACAD:B:A::A
/ 64
Link Local Address
FE80::260:70FF:FE87:2252
IPv6 Gateway
FE80::2
IPv6 DNS Server



Paso 2. configurar IPv6 en los routers.

Nota: la asignación de una dirección IPv6 además de una dirección IPv4 en una interfaz se conoce como "dual-stacking" (o apilamiento doble). Esto se debe a que las pilas de protocolos IPv4 e IPv6 están activas.

a. Para cada interfaz del router, asigne la dirección global y la dirección link local de la tabla de direccionamiento.

b. Habilite el routing IPv6 en cada router.

c. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.

Show ipv6 interface brief

d. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.

e. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

Parte 4: configurar y verificar el routing RIPng

En la parte 4, configurará el routing RIPng en todos los routers, verificará que las tablas de routing estén correctamente actualizadas, configurará y distribuirá una ruta predeterminada, y verificará la conectividad de extremo a extremo.

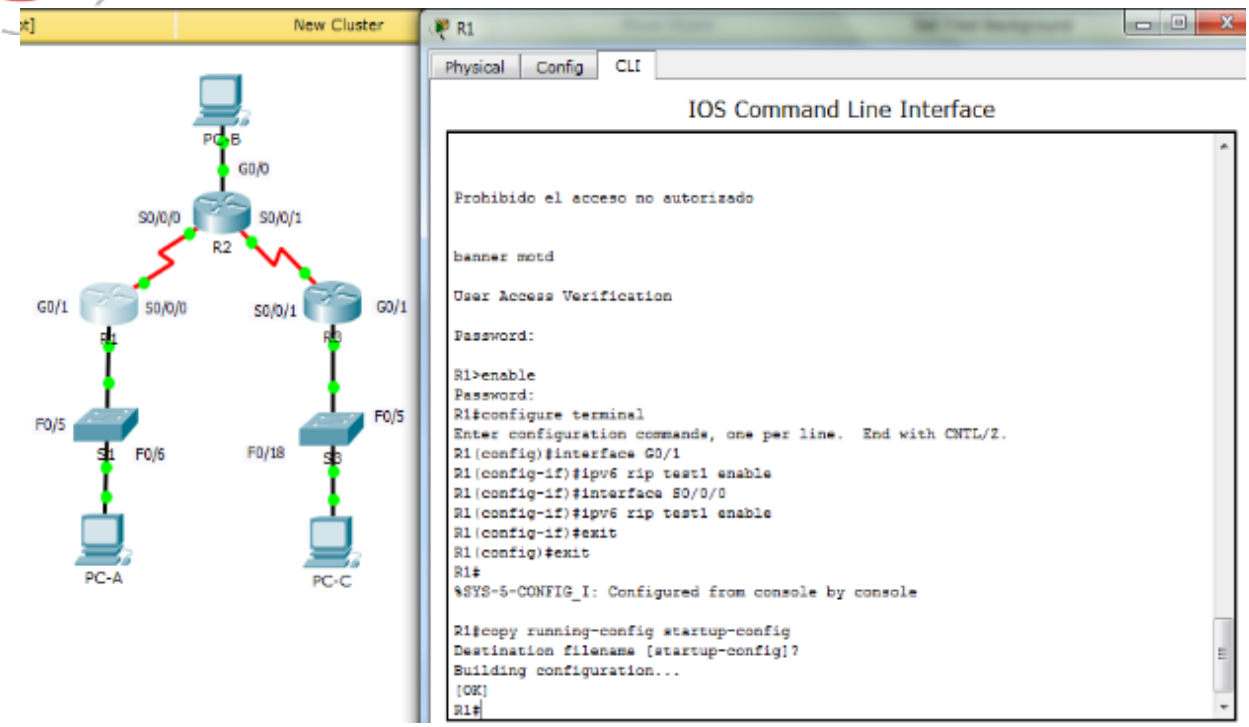
configurar el routing RIPng.

Con IPv6, es común tener varias direcciones IPv6 configuradas en una interfaz. La instrucción network se eliminó en RIPng. En cambio, el routing RIPng se habilita en el nivel de la interfaz y se identifica por un nombre de proceso pertinente en el nivel local, ya que se pueden crear varios procesos con RIPng.

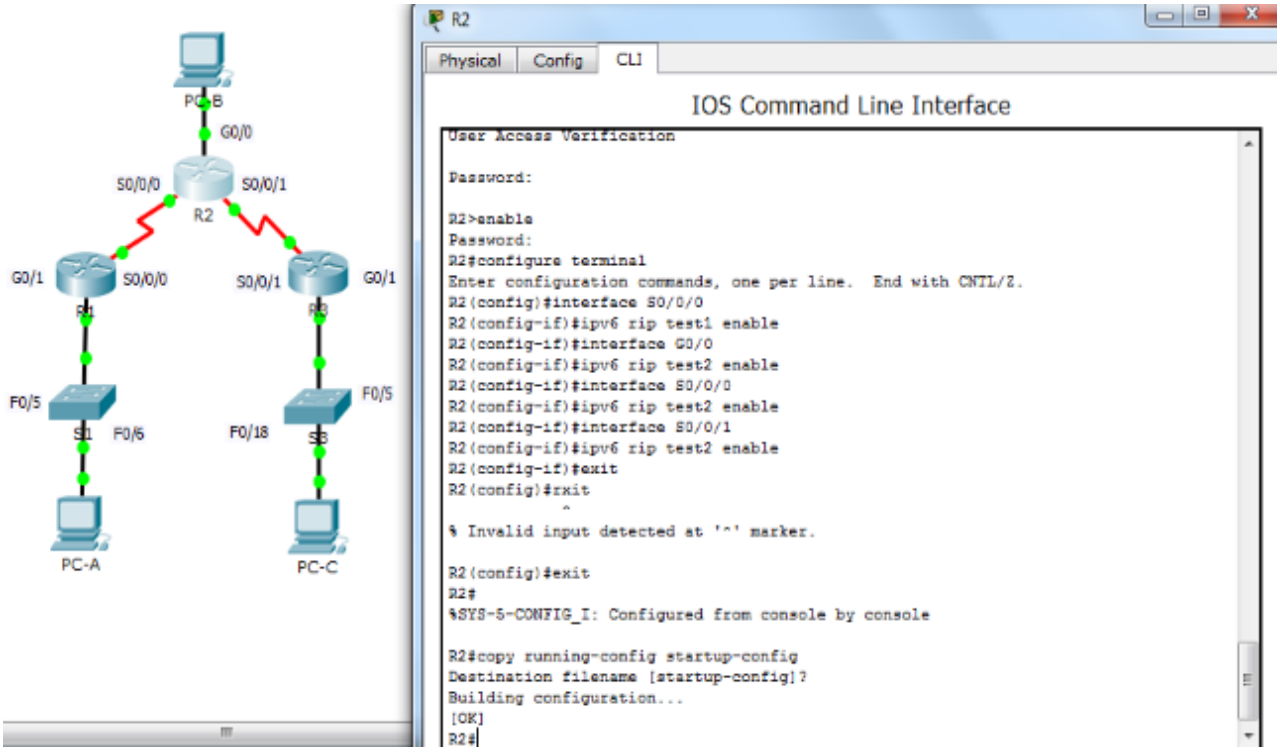
a. Emita el comando **ipv6 rip Test1 enable** para cada interfaz en el R1 que participará en el routing RIPng, donde **Test1** es el nombre de proceso pertinente en el nivel local.

```
R1(config)# interface g0/1
R1(config)# ipv6 rip Test1 enable
```

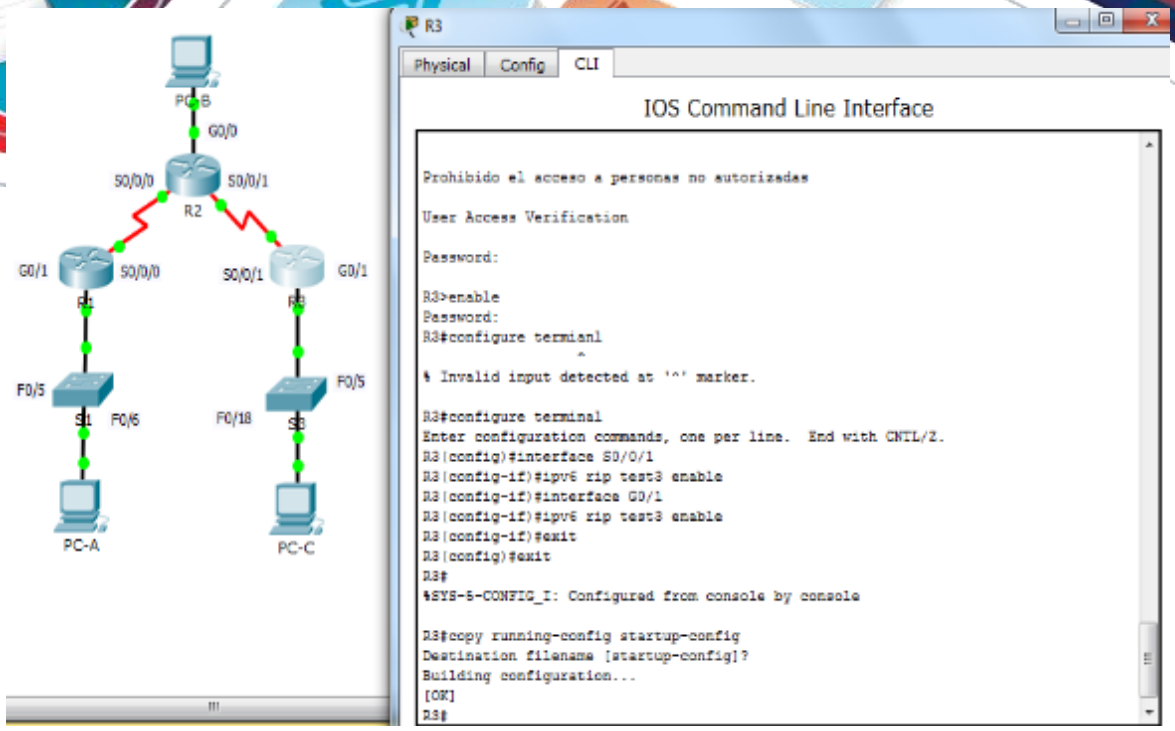
```
R1(config)# interface s0/0/0
R1(config)# ipv6 rip Test1 enable
```



b. Configure RIPng para las interfaces seriales en el R2, con **Test2** como el nombre de proceso. No lo configure para la interfaz G0/0



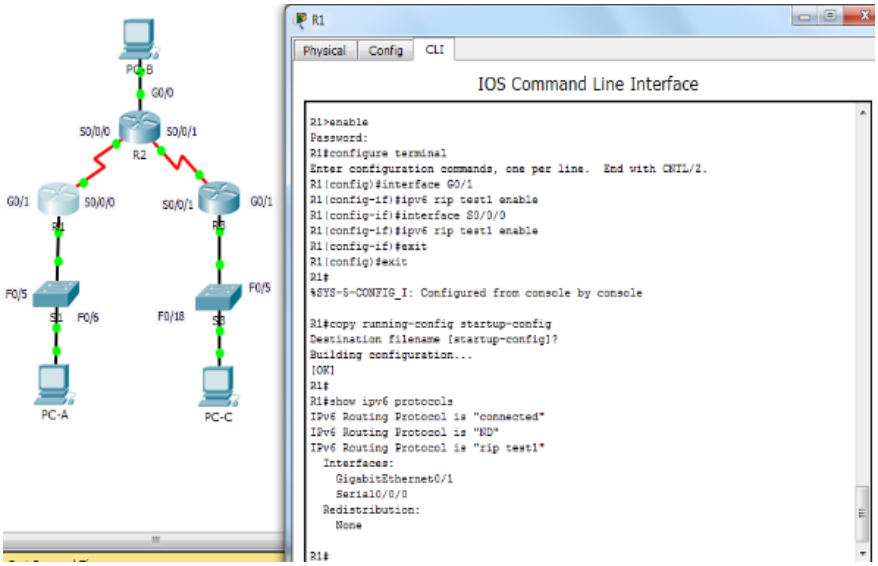
c. Configure RIPng para cada interfaz en el R3, con **Test3** como el nombre de proceso.



d. Verifique que RIPng se esté ejecutando en los routers.

Los comandos **show ipv6 protocols**, **show run**, **show ipv6 rip database** y **show ipv6 rip** *nombre de proceso* se pueden usar para confirmar que se esté ejecutando RIPng En el R1, emita el comando **show ipv6 protocols**.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test1"
  Interfaces:
    Serial0/0/0
    GigabitEthernet0/1
  Redistribution:
    None
```



¿En qué forma se indica RIPng en el resultado?

e. Emita el comando **show ipv6 rip Test1**.

```
R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 314
     Administrative distance is 120. Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 1, trigger updates 0
     Full Advertisement 0, Delayed Events 0
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
  Redistribution:
    None
```

¿Cuáles son las similitudes entre RIPv2 y RIPng?

El proceso de la propagación de rutas es igual en los dos es similar

f. Inspecciones la tabla de routing IPv6 en cada router. Escriba el comando apropiado que se usa para ver la tabla de routing en el espacio a continuación.

Show ipv6 route

En el R1, ¿cuántas rutas se descubrieron mediante RIPng? 2

En el R2, ¿cuántas rutas se descubrieron mediante RIPng? 3

En el R3, ¿cuántas rutas se descubrieron mediante RIPng? 2

g. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? Si es posible

¿Es posible hacer ping de la PC-A a la PC-C? Si es posible

¿Es posible hacer ping de la PC-C a la PC-B? Si es posible

¿Es posible hacer ping de la PC-C a la PC-A? Si es posible

¿Por qué algunos pings tuvieron éxito y otros no?

Porque no estaba activado el RIP

Paso 3. configurar y volver a distribuir una ruta predeterminada.

a. Desde el R2, cree una ruta estática predeterminada a la red:: 0/64 con el comando **ipv6 route** y la dirección IP de la interfaz de salida G0/0. Esto reenvía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet. Escriba el comando que utilizó en el espacio a continuación.

Ipv6 route 0.0.0.0.0.0.0.0::0/64

b. Las rutas estáticas se pueden incluir en las actualizaciones RIPng mediante el comando **ipv6 rip** *nombre de proceso* **default-information originate** en el modo de configuración de interfaz. Configure los enlaces seriales en el R2 para enviar la ruta predeterminada en actualizaciones RIPng.

```
R2(config)# int s0/0/0
R2(config-rtr)# ipv6 rip Test2 default-information originate
R2(config)# int s0/0/1


R2(config-rtr)# ipv6 rip Test2 default-information originate
```

Paso 4. Verificar la configuración de enrutamiento.

a. Consulte la tabla de routing IPv6 en el router R2.

```
R2# show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/64 [1/0]
     via 2001:DB8:ACAD:B::B
R   2001:DB8:ACAD:A::/64 [120/2]
     via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
     via ::, GigabitEthernet0/1
L   2001:DB8:ACAD:B::2/128 [0/0]
     via ::, GigabitEthernet0/1
R   2001:DB8:ACAD:C::/64 [120/2]
     via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
     via ::, Serial0/0/0
L   2001:DB8:ACAD:12::2/128 [0/0]
     via ::, Serial0/0/0
C   2001:DB8:ACAD:23::/64 [0/0]
     via ::, Serial0/0/1
L   2001:DB8:ACAD:23::2/128 [0/0]
     via ::, Serial0/0/1
L   FF00::/8 [0/0]
     via ::, Null0
```

¿Cómo se puede saber, a partir de la tabla de routing, que el R2 tiene una ruta para el tráfico de Internet?

Porque las rutas se publican en los demás routers estableciendo rutas estáticas

b. Consulte las tablas de routing del R1 y el R3.

¿Cómo se proporciona la ruta para el tráfico de Internet en sus tablas de enrutamiento?

El router que tiene el acceso a internet envía la ruta a los demás routers y se proporciona por medio de una ruta estática

Paso 5. Verifique la conectividad.

Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 2001:DB8:ACAD:B::B/64.

¿Tuvieron éxito los pings? No

Reflexión

1. ¿Por qué desactivaría la sumarización automática para RIPv2?

   Permite optimizar los recursos del router, manteniendo una red con mayor estabilidad y confiabilidad

   Porque en la versión 2 para la sumarizacion necesita clases completas para que detecte las redes}

   Para que identifique y actualice con las rutas directamente conectadas

2. En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3?

   Las rutas se inician con la letra R

   Con la ruta estática configurada con ip router

3. ¿En qué se diferencian la configuración de RIPv2 y la de RIPng?

   Ripng se habilita en una interfaz, no en la configuración del router

   En ripv2 admite actualizaciones RIPv1, Ripng no

   En Ripv2 podemos colocar etiquetas a las rutas

   Ripv2 codifica el siguiente salto en cada entrada de la ruta, mientras que con RIPng se requiere de una codificación especifica

   RIPv2 determina las redes sumarizadas en la interfaz

   RIPng puede configurar varias redes en cada interfaz con un proceso

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.

Práctica de laboratorio: configuración de OSPFv2 básico de área única

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	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	G0/0	192.168.2.1	255.255.255.0	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	G0/0	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-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar y verificar el routing OSPF

Parte 3: cambiar las asignaciones de ID del router

Parte 4: configurar interfaces OSPF pasivas

Parte 5: cambiar las métricas de OSPF

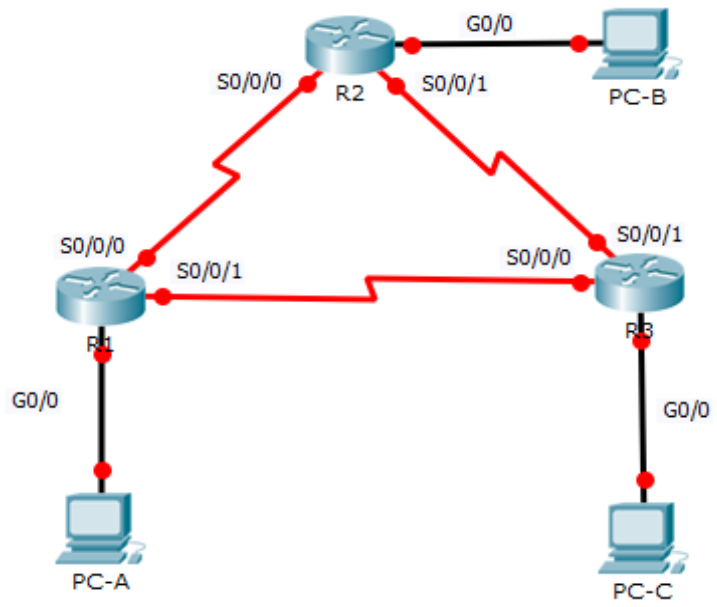
Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal 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

armar la red y configurar los parámetros básicos de los dispositivos

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

Step 2: realizar el cableado de red tal como se muestra en la topología.



Step 3: inicializar y volver a cargar los routers según sea necesario.

Step 4: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

c. Asigne **class** como la contraseña del modo EXEC privilegiado.

d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

e. Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.

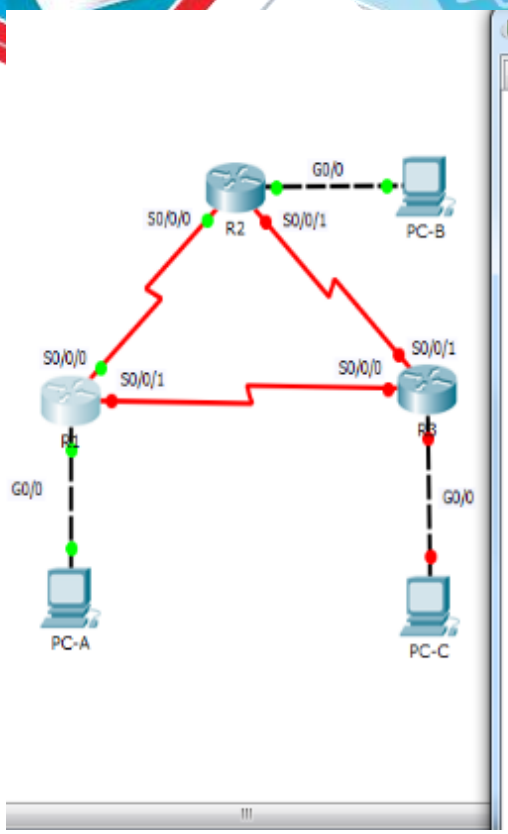
f. Configure **logging synchronous** para la línea de consola.

g. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.

h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.

i. Copie la configuración en ejecución en la configuración de inicio

Step 5: configurar los equipos host.

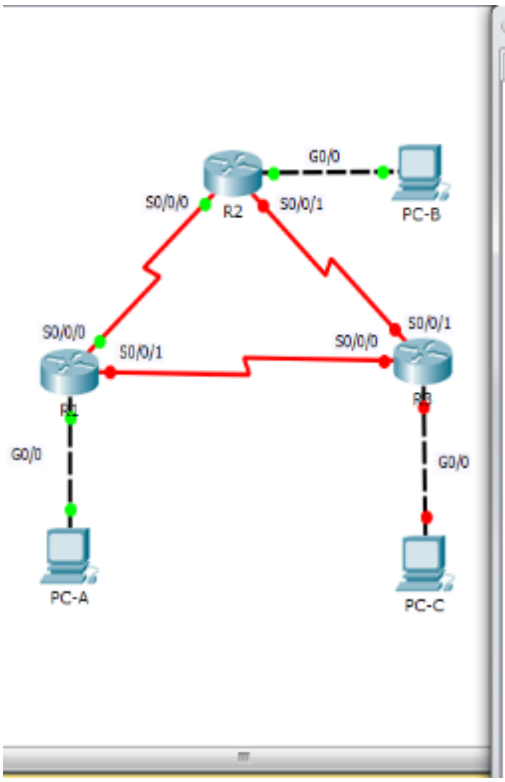


R1

Physical | Config | CLI

IOS Command Line Interface

```
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Prohibido el acceso no autorizado#

R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#interface G0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#interface S0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#clock rate 25000
Unknown clock rate
R1(config-if)#interface S0/0/1
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#interface S0/0/0
R1(config-if)#no shutdown
```

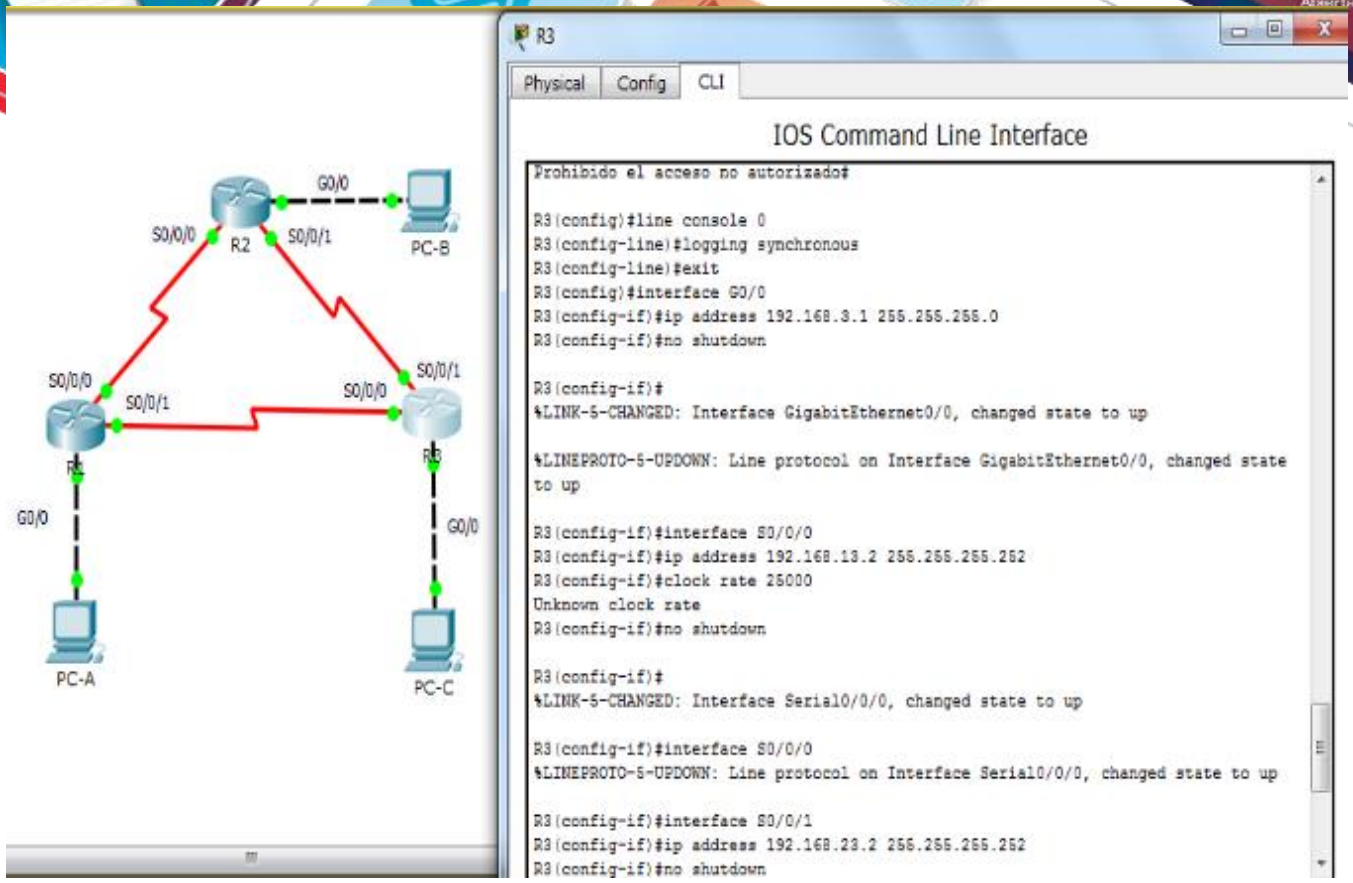


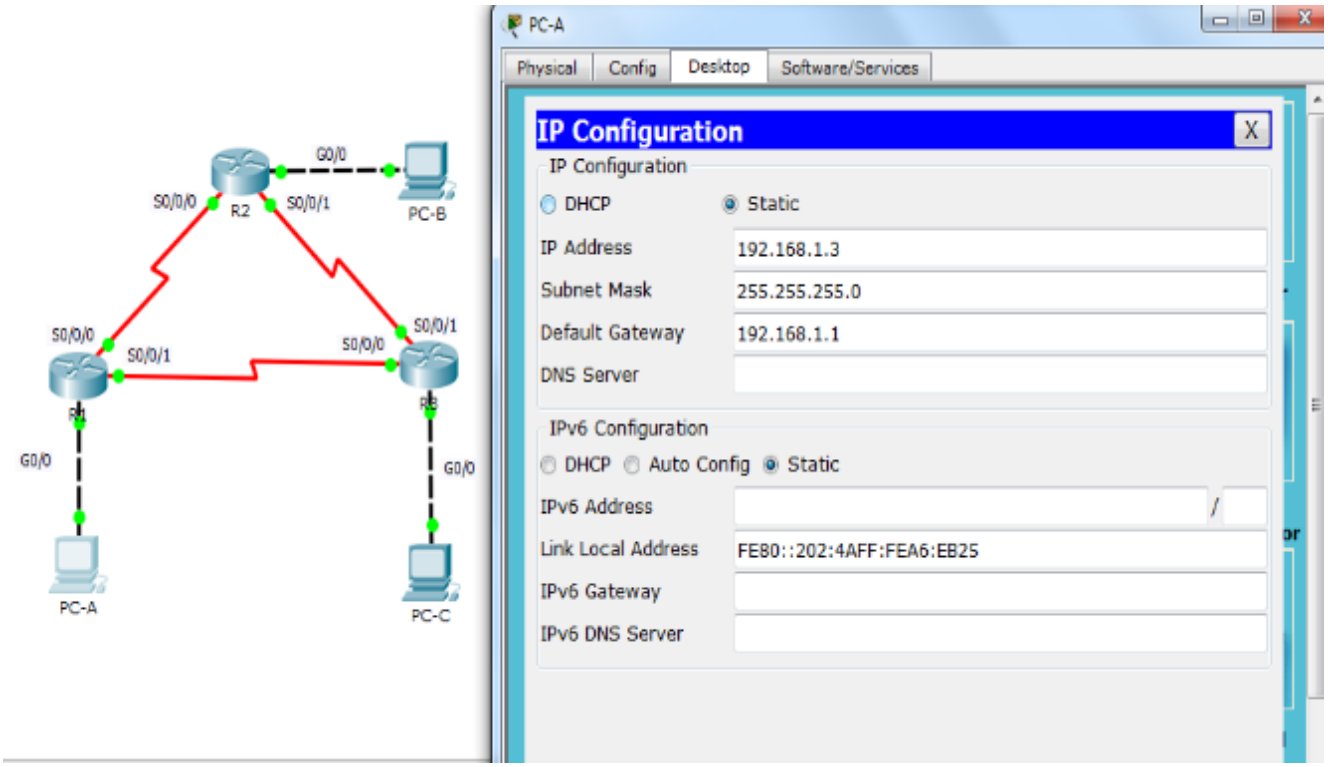
R2

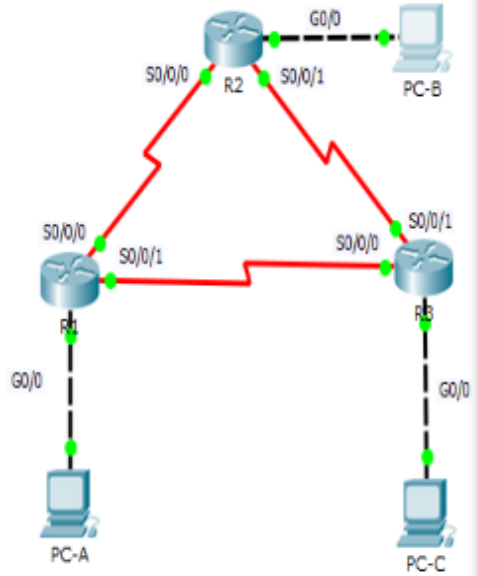
Physical | Config | CLI

IOS Command Line Interface

```
R2(config-line)#exit
R2(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Prohibido el acceso no autorizado#

R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface G0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R2(config-if)#interface S0/0/0
R2(config-if)#ip address 192.168.12.2 255.255.255.252
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#interface S0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#interface S0/0/1
R2(config-if)#ip address 192.168.22.1 255.255.255.252
R2(config-if)#clock rate 25000
Unknown clock rate
R2(config-if)#no shutdown
```


R3
Physical
Config
CLI
IOS Command Line Interface
Prohibido el acceso no autorizado!
R3(config)#line console 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface G0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R3(config-if)#interface S0/0/0
R3(config-if)#ip address 192.168.13.2 255.255.255.252
R3(config-if)#clock rate 25000
Unknown clock rate
R3(config-if)#no shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R3(config-if)#interface S0/0/0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R3(config-if)#interface S0/0/1
R3(config-if)#ip address 192.168.23.2 255.255.255.252
R3(config-if)#no shutdown
G0/0
S0/0/0
R2
S0/0/1
PC-B
S0/0/0
S0/0/1
S0/0/0
S0/0/1
G0/0
G0/0
PC-A
PC-C


PC-A
Physical
Config
Desktop
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::202:4AFF:FEA6:EB25
IPv6 Gateway
IPv6 DNS Server
G0/0
S0/0/0
R2
S0/0/1
PC-B
S0/0/0
S0/0/1
S0/0/0
S0/0/1
G0/0
G0/0
PC-A
PC-C



PC-B

Physical | Config | Desktop | Software/Services

IP Configuration

IP Configuration

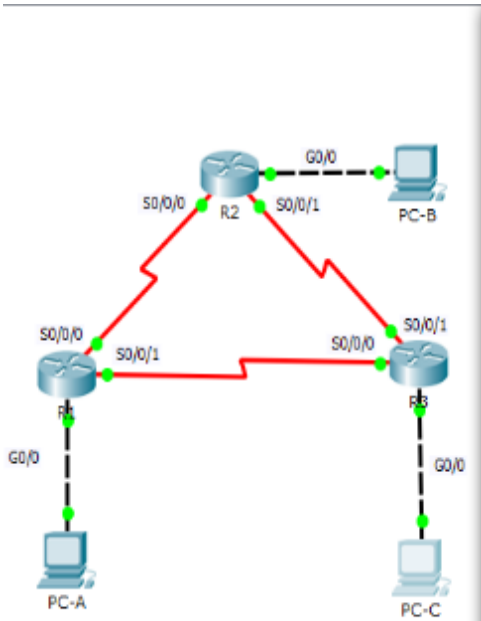
DHCP ○ Static ●

IP Address	192.168.2.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	

IPv6 Configuration

DHCP ○ Auto Config ○ Static ●

IPv6 Address	/
Link Local Address	FE80::260:5CFF:FE94:2D44
IPv6 Gateway	
IPv6 DNS Server	



PC-C

Physical | Config | Desktop | Software/Services

IP Configuration

IP Configuration

DHCP ○ Static ●

IP Address	192.168.3.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
DNS Server	

IPv6 Configuration

DHCP ○ Auto Config ○ Static ●

IPv6 Address	/
Link Local Address	FE80::20D:BDFF:FECA:850A
IPv6 Gateway	
IPv6 DNS Server	

Step 6: Probar la conectividad.

Los routers deben poder hacerse ping entre sí, y cada computadora debe poder hacer ping a su gateway predeterminado. Las computadoras no pueden hacer ping a otras computadoras hasta que no se haya configurado el routing OSPF. Verifique y resuelva los problemas, si es necesario.

Configurar y verificar el enrutamiento OSPF

En la parte 2, configurará el routing OSPFv2 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente. Después de verificar OSPF, configurará la autenticación de OSPF en los enlaces para mayor seguridad.

Configure el protocolo OSPF en R1.

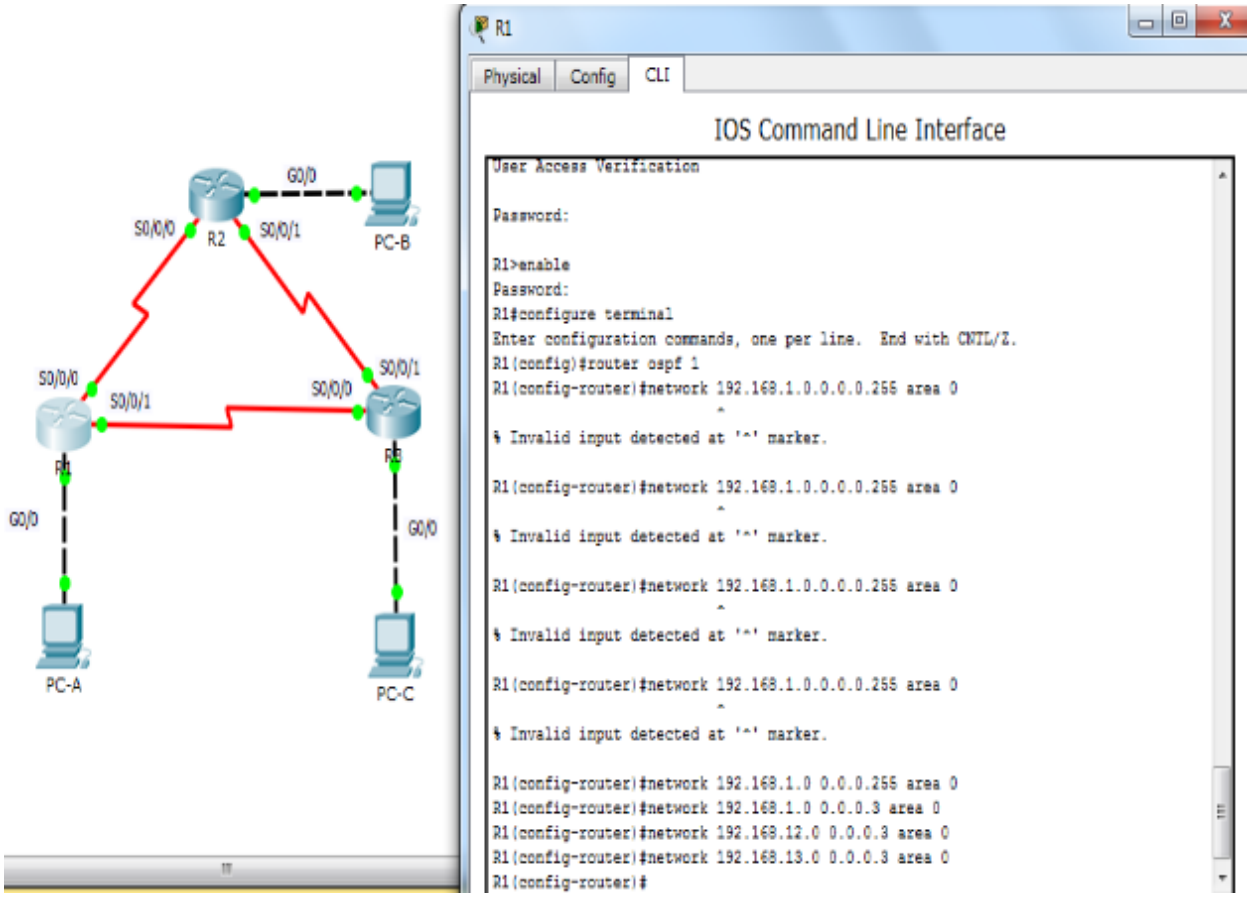
a. Use el comando **router ospf** en el modo de configuración global para habilitar OSPF en el R1.

```
R1(config)# router ospf 1
```

Nota: la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

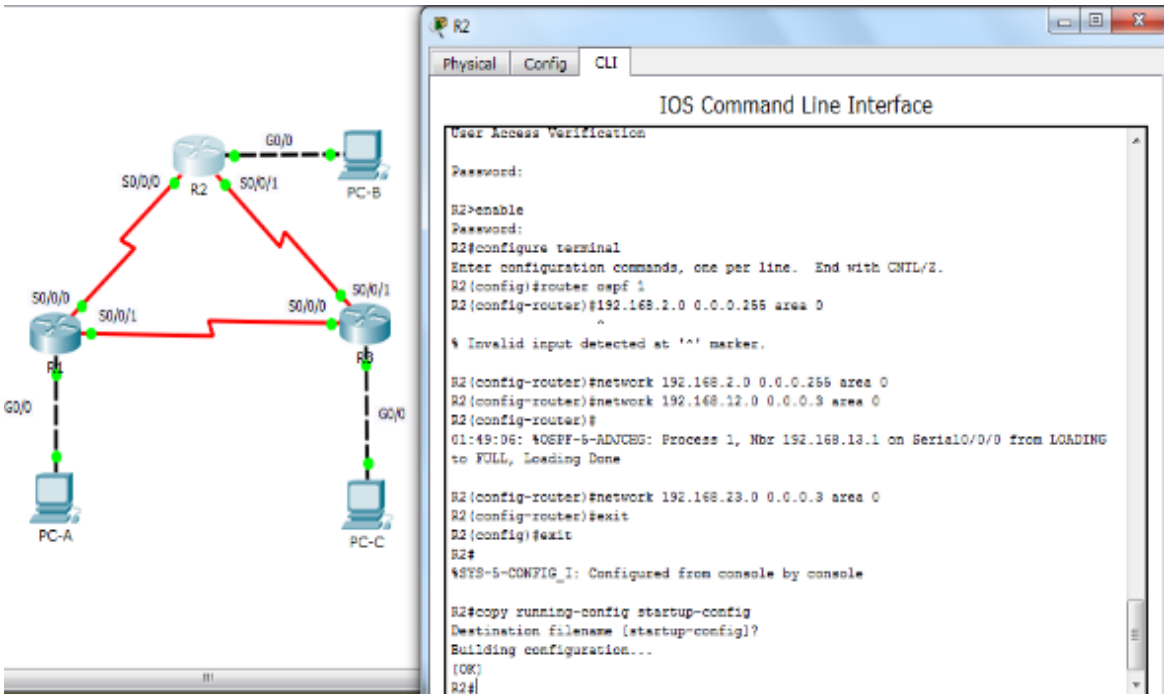
b. Configure las instrucciones **network** para las redes en el R1. Utilice la ID de área 0.

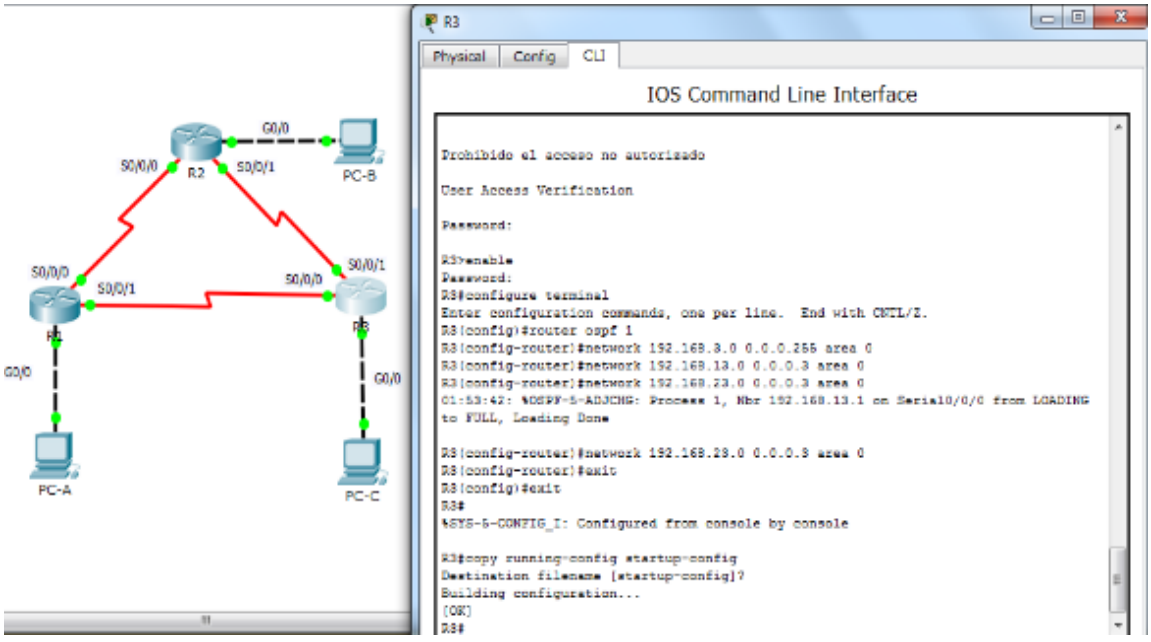
```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```



Step 7: Configure OSPF en el R2 y el R3.

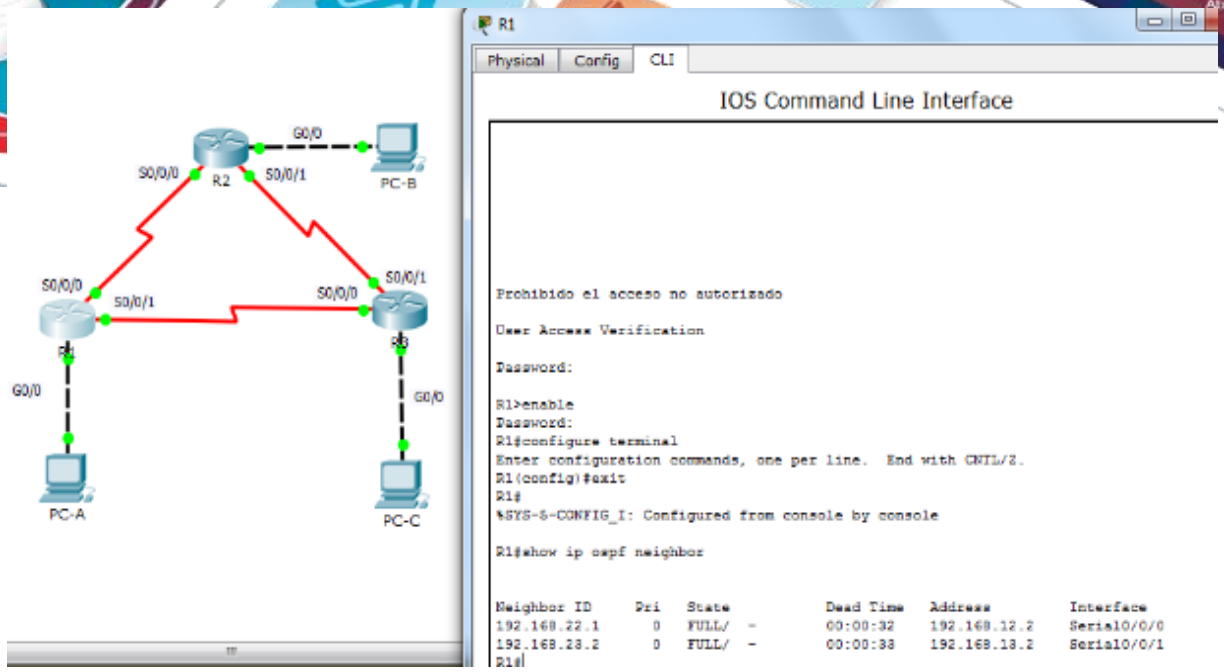
Use el comando **router ospf** y agregue las instrucciones **network** para las redes en el R2 y el R3. Cuando el routing OSPF está configurado en el R2 y el R3, se muestran mensajes de adyacencia de vecino en el R1.





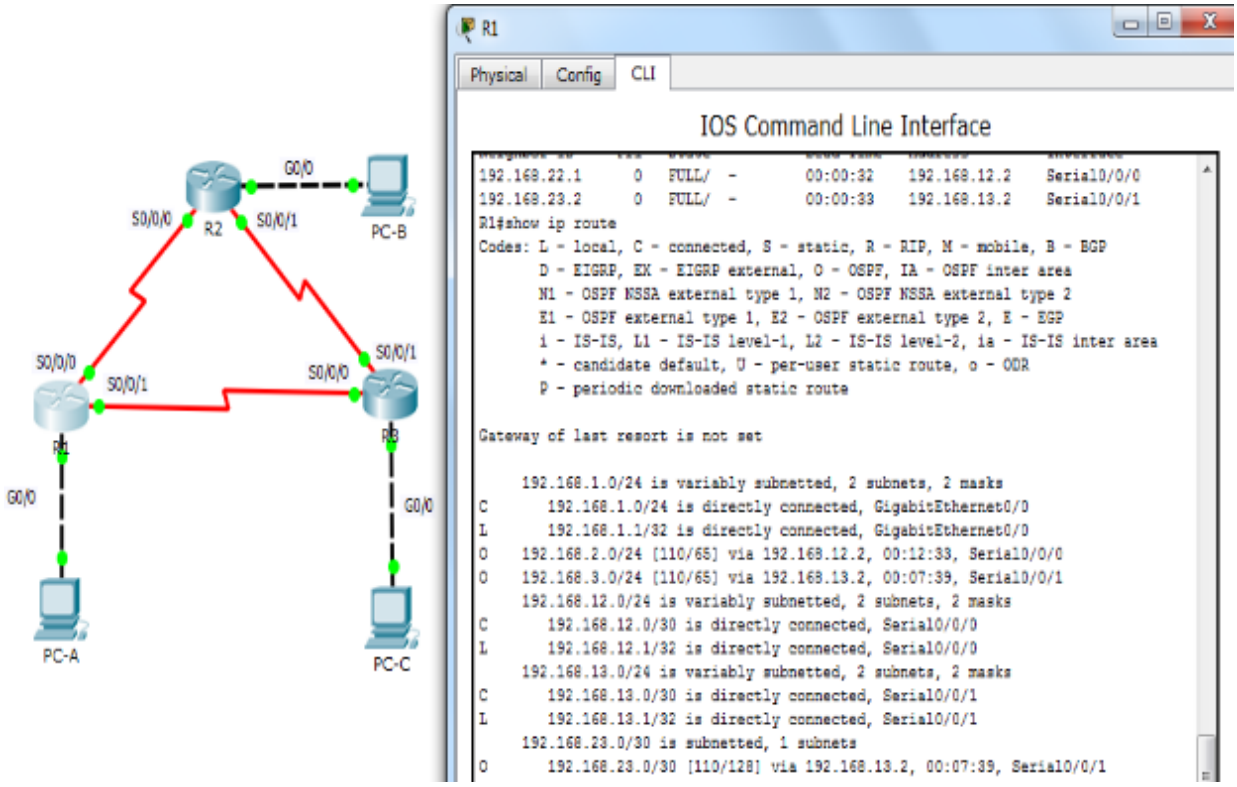
Step 8: verificar los vecinos OSPF y la información de routing.

a. Emita el comando **show ip ospf neighbor** para verificar que cada router indique a los demás routers en la red como vecinos.



b. Emita el comando **show ip route** para verificar que todas las redes aparezcan en la tabla de routing de todos los routers.

```
R1# show ip route
```



¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?

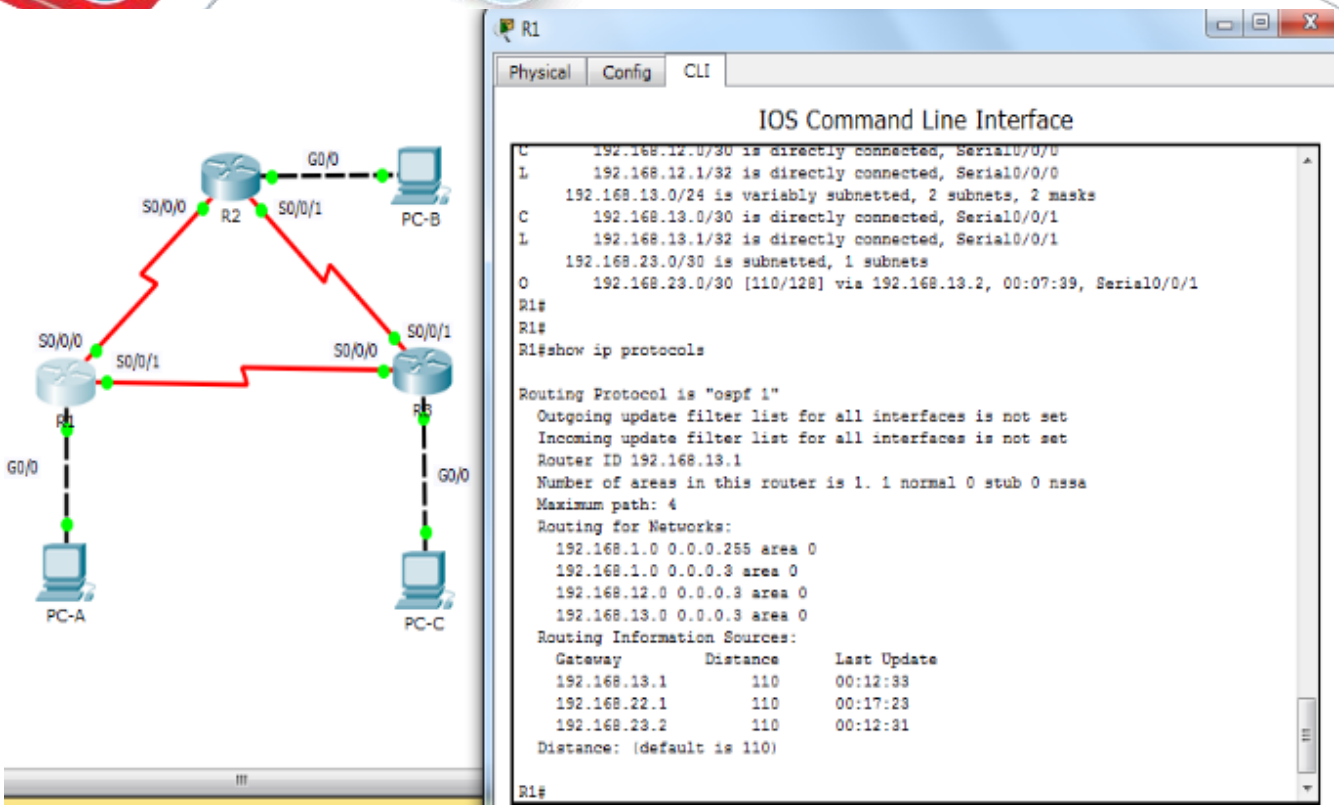
Show ip route ospf

Step 9: verificar la configuración del protocolo OSPF.

El comando **show ip protocols** es una manera rápida de verificar información fundamental de configuración de OSPF. Esta información incluye la ID del proceso OSPF, la ID del router, las redes que

anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.

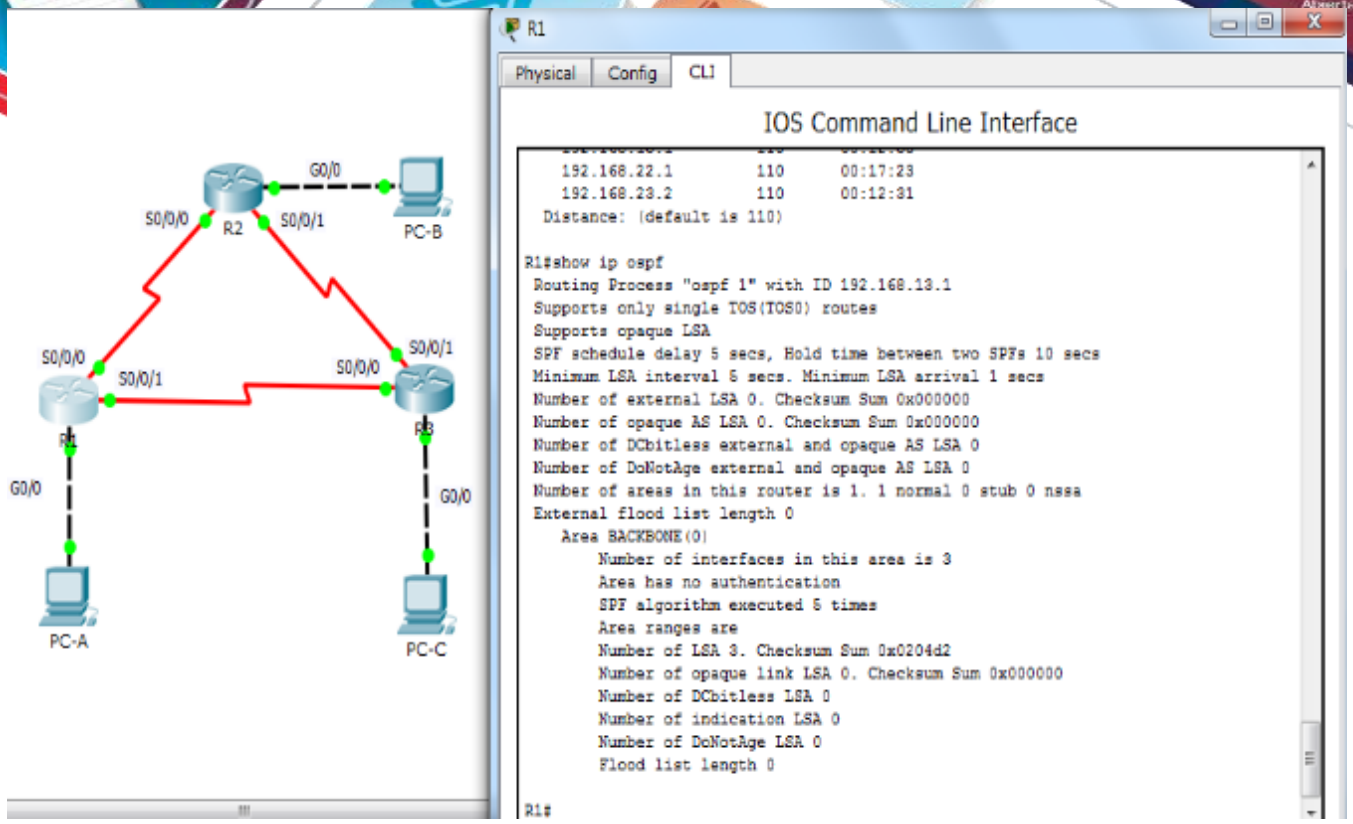
```
R1# show ip protocols
```



Step 10: verificar la información del proceso OSPF.

Use el comando **show ip ospf** para examinar la ID del proceso OSPF y la ID del router. Este comando muestra información de área OSPF y la última vez que se calculó el algoritmo SPF.

```
R1# show ip ospf
```

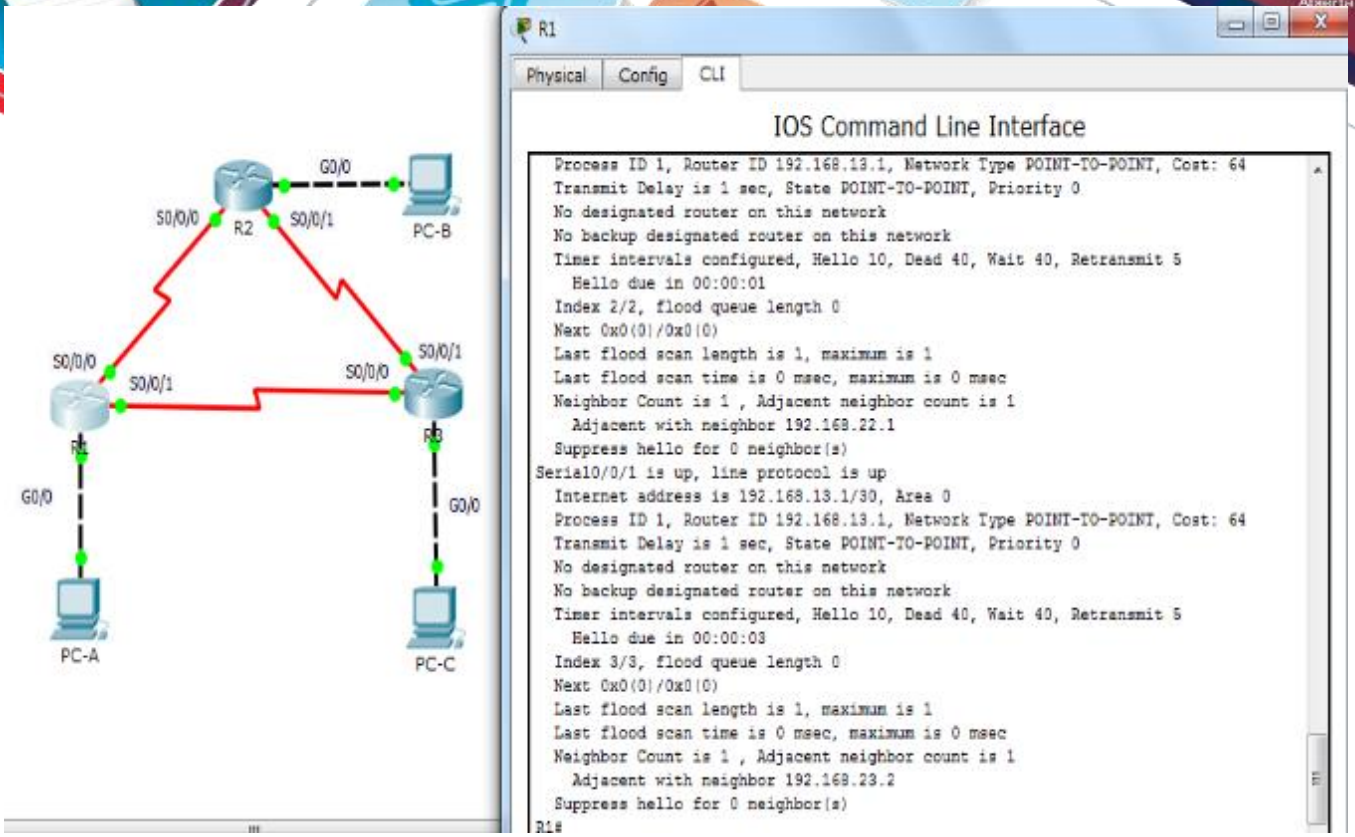


Step 11: verificar la configuración de la interfaz OSPF.

a. Emita el comando **show ip ospf interface brief** para ver un resumen de las interfaces con OSPF habilitado.

```
R1# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1      1     0               192.168.13.1/30    64    P2P   1/1
Se0/0/0      1     0               192.168.12.1/30    64    P2P   1/1
Gi0/0        1     0               192.168.1.1/24     1     DR    0/0
```

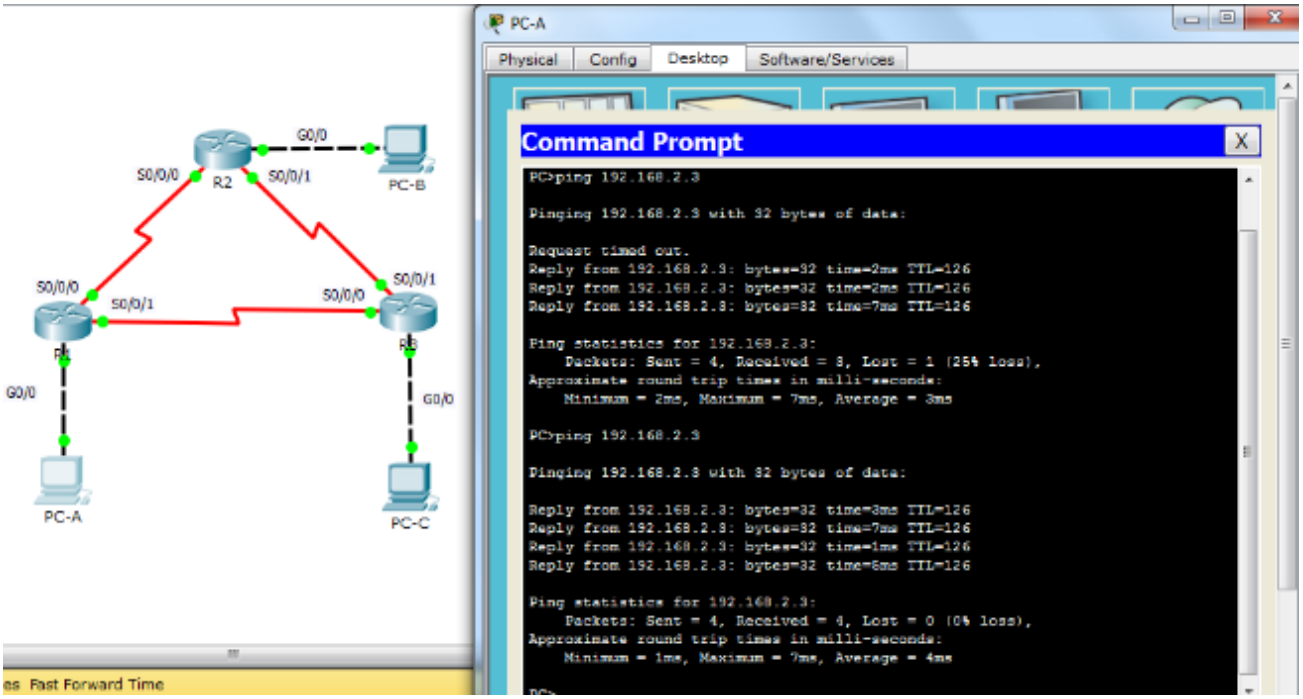
b. Para obtener una lista detallada de todas las interfaces con OSPF habilitado, emita el comando **show ip ospf interface**.



Step 12: Verificar la conectividad de extremo a extremo.

Se debería poder hacer ping entre todas las computadoras de la topología. Verifique y resuelva los problemas, si es necesario.

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.



cambiar las asignaciones de ID del router

El ID del router OSPF se utiliza para identificar de forma única el router en el dominio de enrutamiento OSPF. Los routers Cisco derivan la ID del router en una de estas tres formas y con la siguiente prioridad:

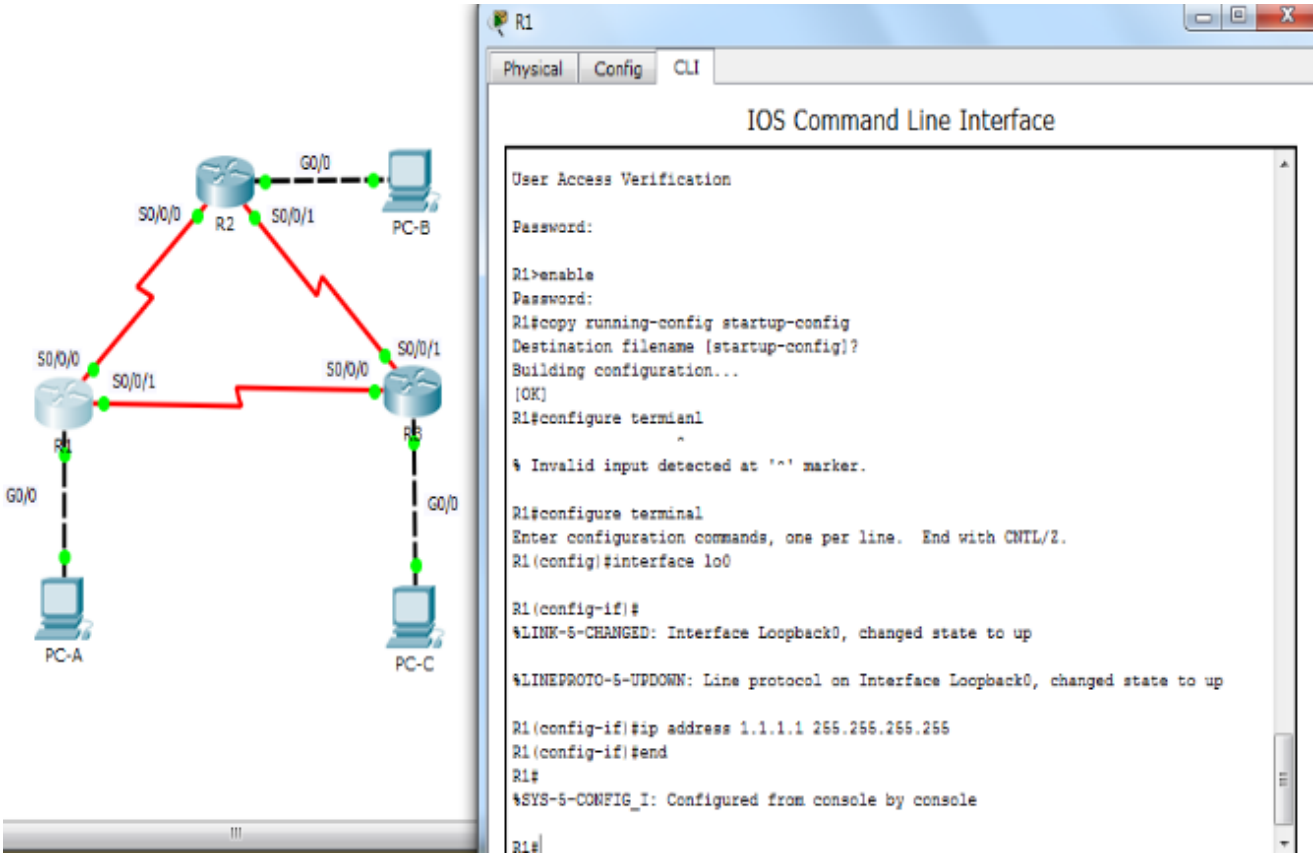
1) Dirección IP configurada con el comando de OSPF **router-id**, si la hubiera
2) Dirección IP más alta de cualquiera de las direcciones de loopback del router, si la hubiera
3) Dirección IP activa más alta de cualquiera de las interfaces físicas del router

Dado que no se ha configurado ningún ID o interfaz de loopback en los tres routers, el ID de router para cada ruta se determina según la dirección IP más alta de cualquier interfaz activa.

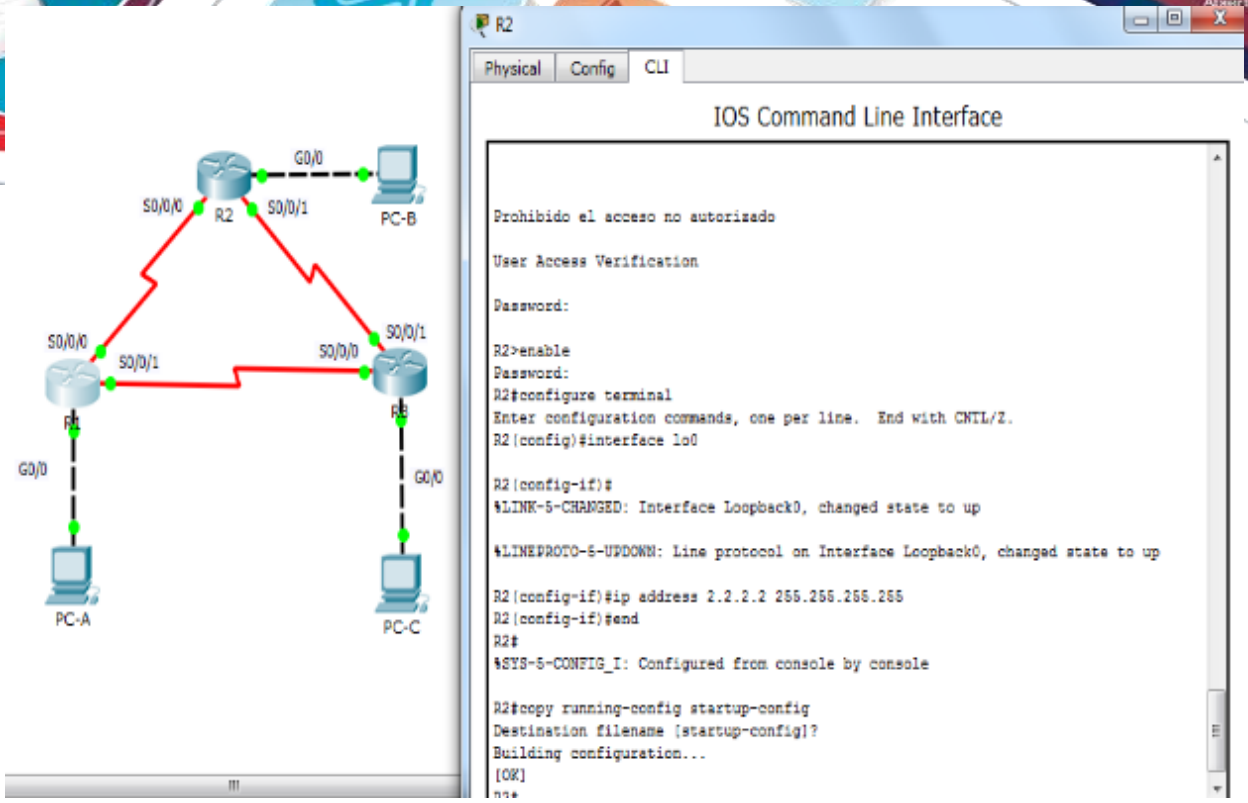
En la parte 3, cambiará la asignación de ID del router OSPF con direcciones de loopback. También usará el comando **router-id** para cambiar la ID del router.

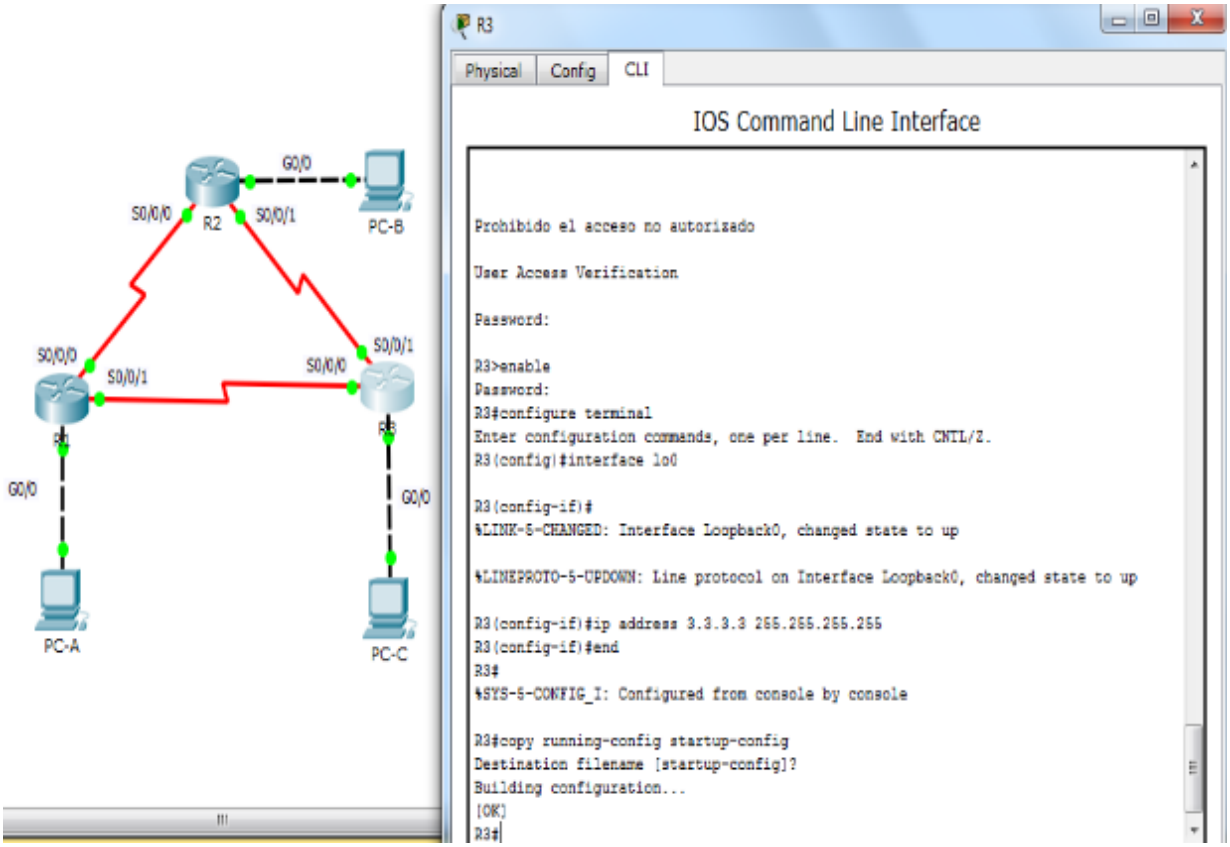
Step 1: Cambie las ID de router con direcciones de loopback.

a. Asigne una dirección IP al loopback 0 en el R1.



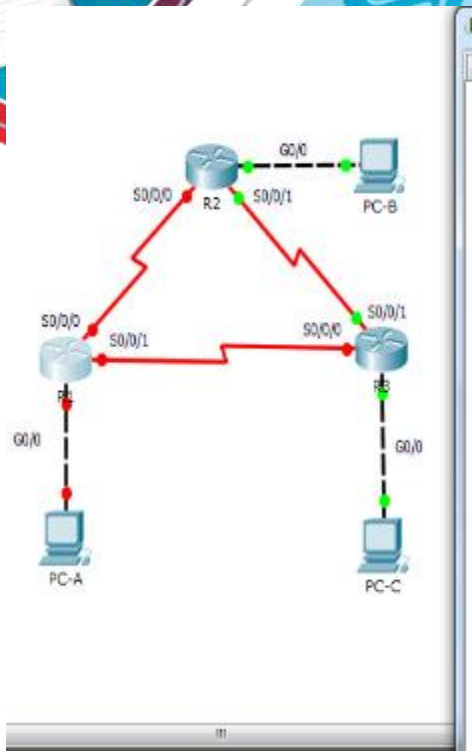
b. Asigne direcciones IP al loopback 0 en el R2 y el R3. Utilice la dirección IP 2.2.2.2/32 para el R2 y 3.3.3.3/32 para el R3.





c. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.

d. Debe volver a cargar los routers para restablecer la ID del router a la dirección de loopback. Emita el comando **reload** en los tres routers. Presione Enter para confirmar la recarga.

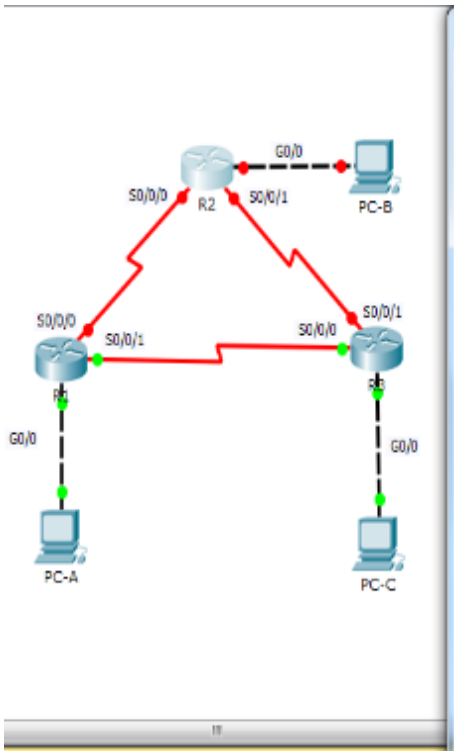


R1

Physical | Config | CLI

IOS Command Line Interface

```
Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#################################
```

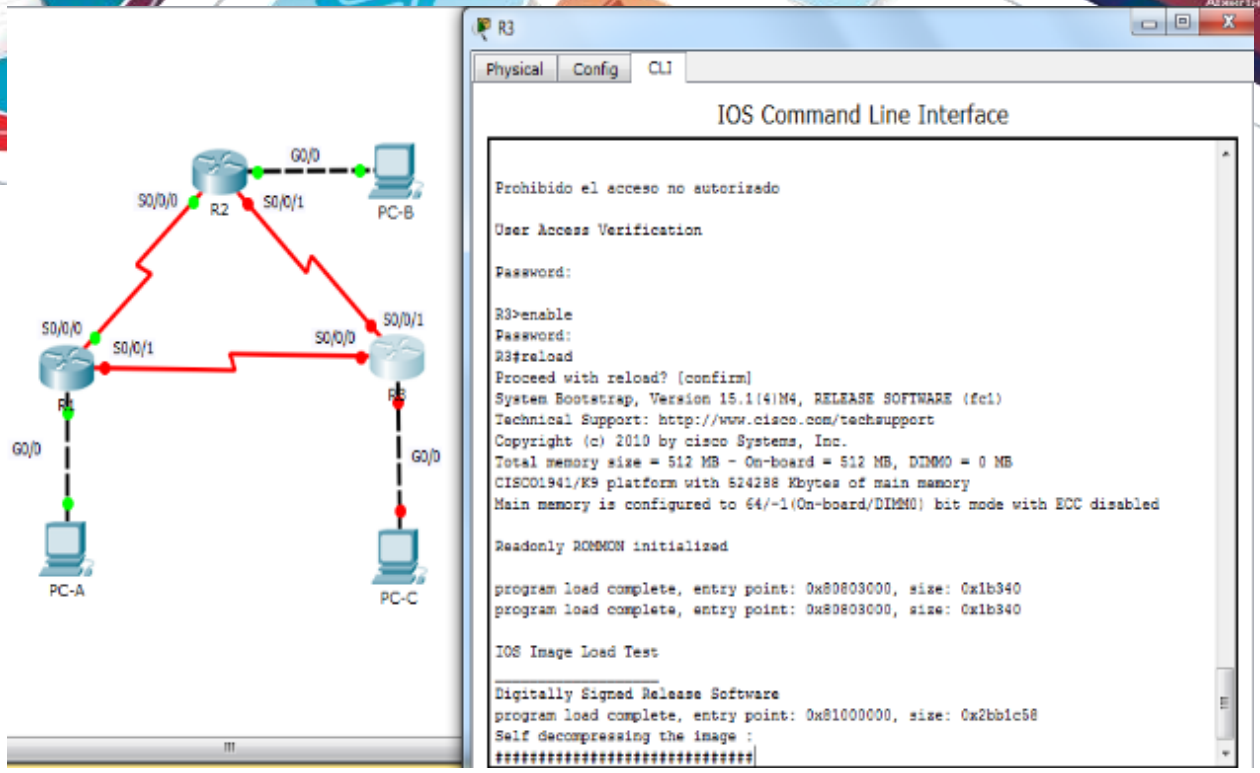


R2

Physical | Config | CLI

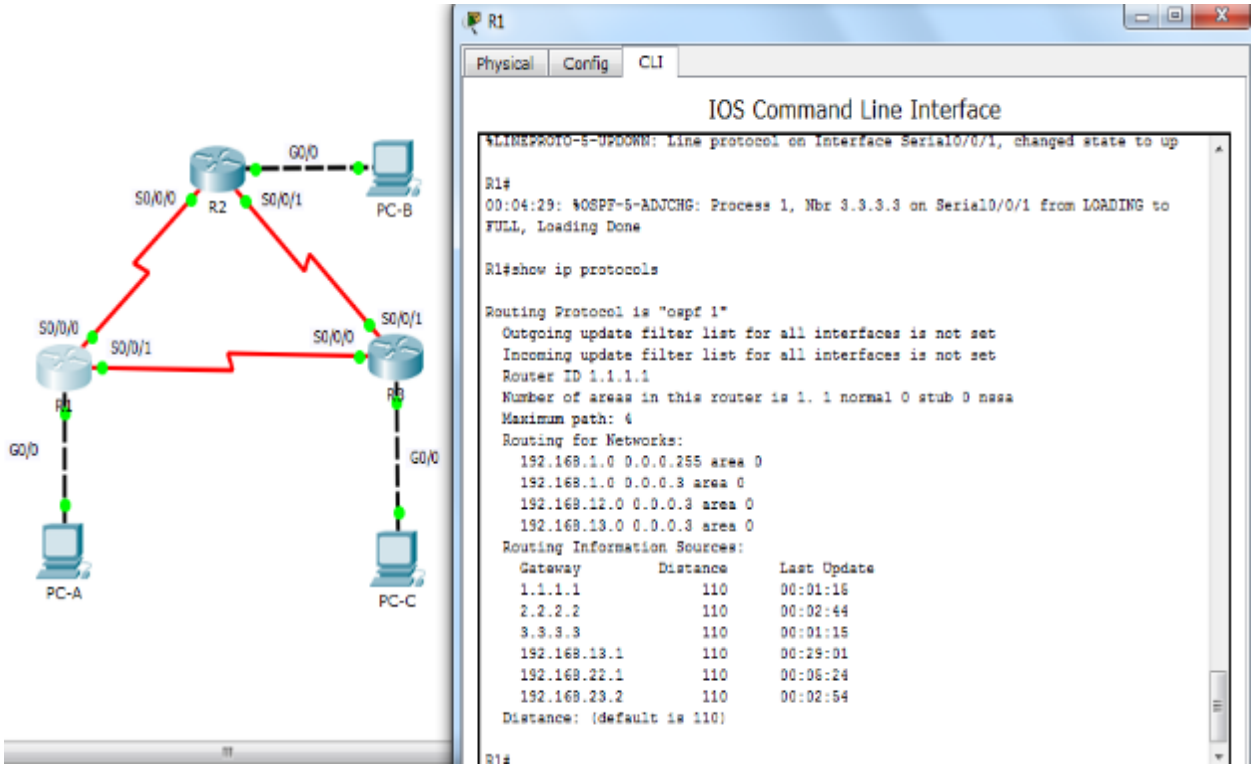
IOS Command Line Interface

```
Prohibido el acceso no autorizado

User Access Verification

Password:

R2>enable
Password:
R2#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#########################################
```



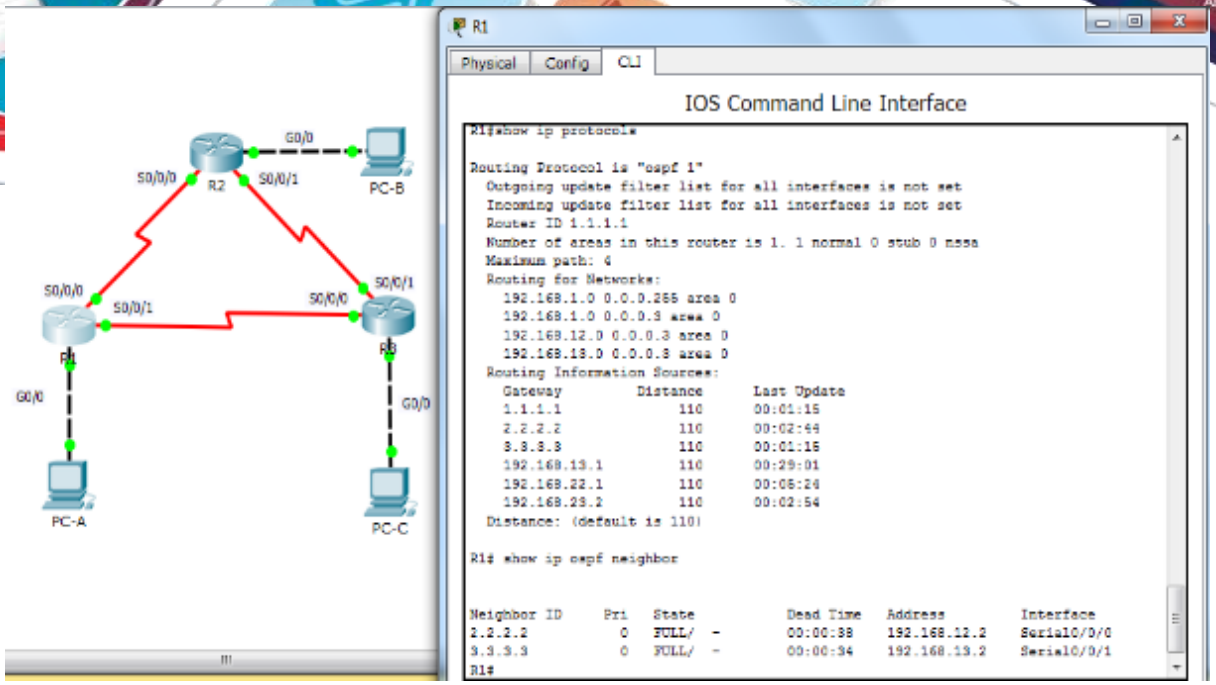
e. Una vez que se haya completado el proceso de recarga del router, emita el comando **show ip protocols** para ver la nueva ID del router.

```
R1# show ip protocols
```



f. Emita el comando **show ip ospf neighbor** para mostrar los cambios de ID de router de los routers vecinos.

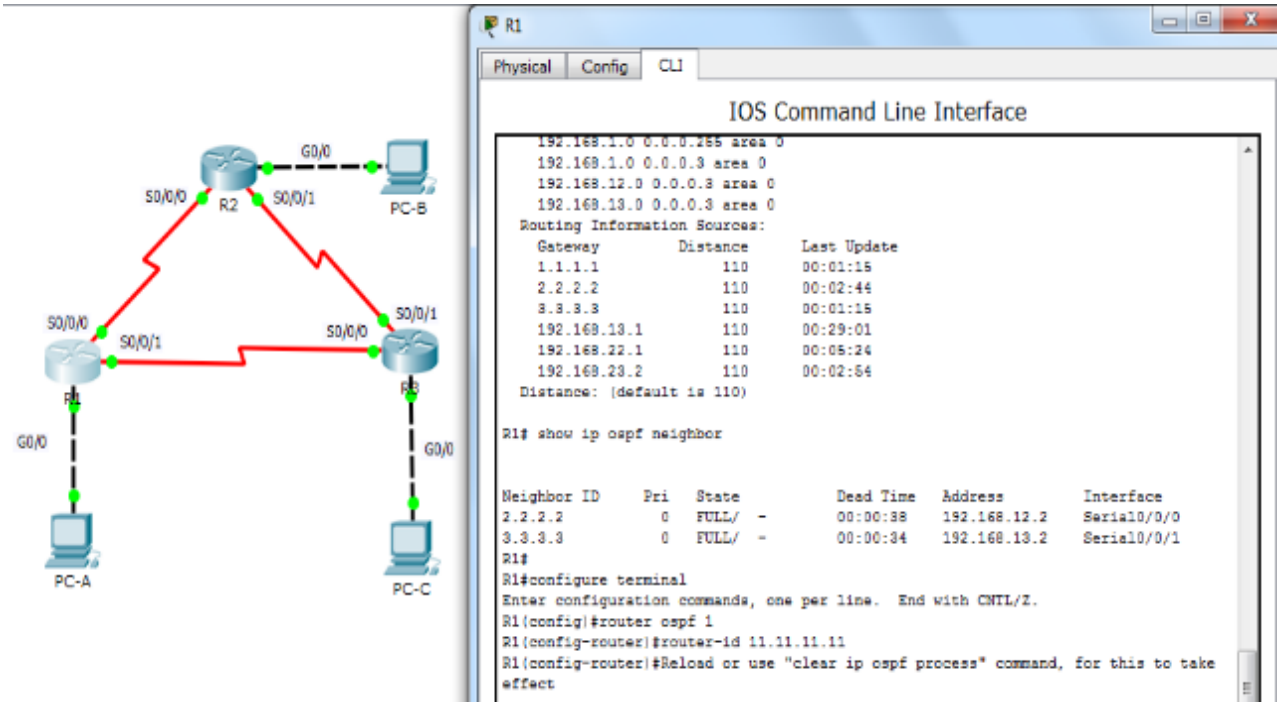
```
R1# show ip ospf neighbor
```



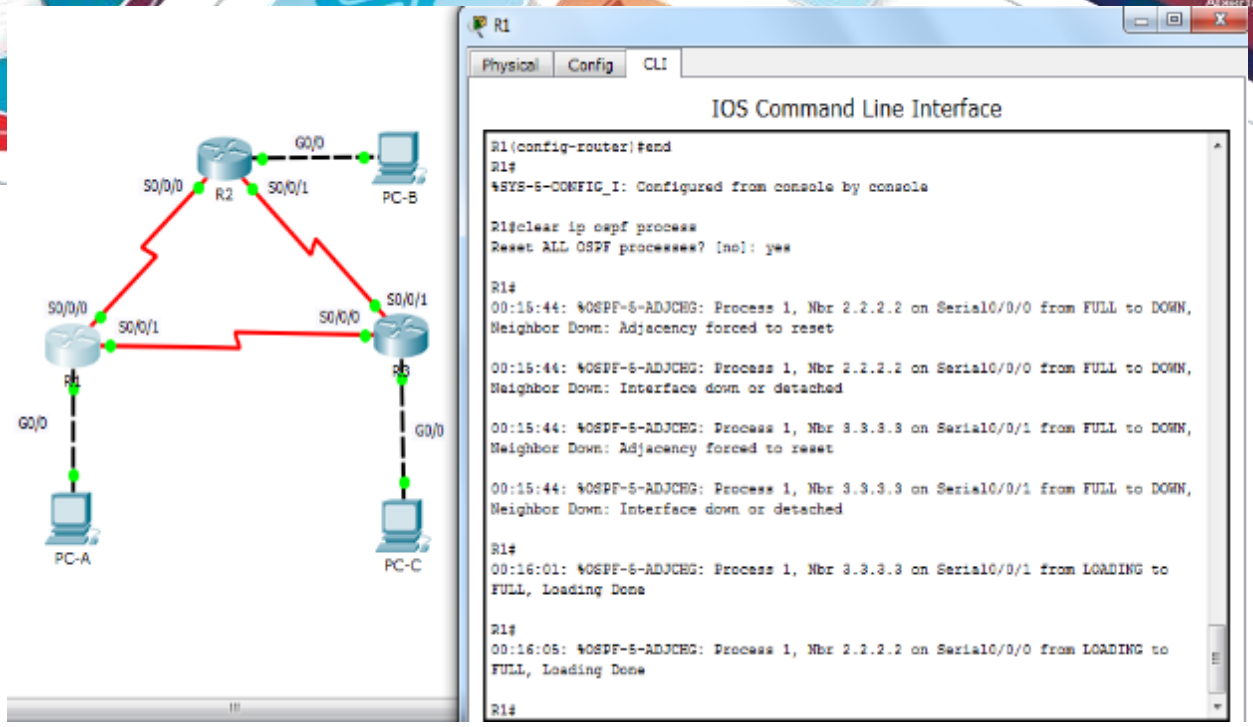
Step 2: cambiar la ID del router R1 con el comando router-id.

El método de preferencia para establecer la ID del router es mediante el comando **router-id**.

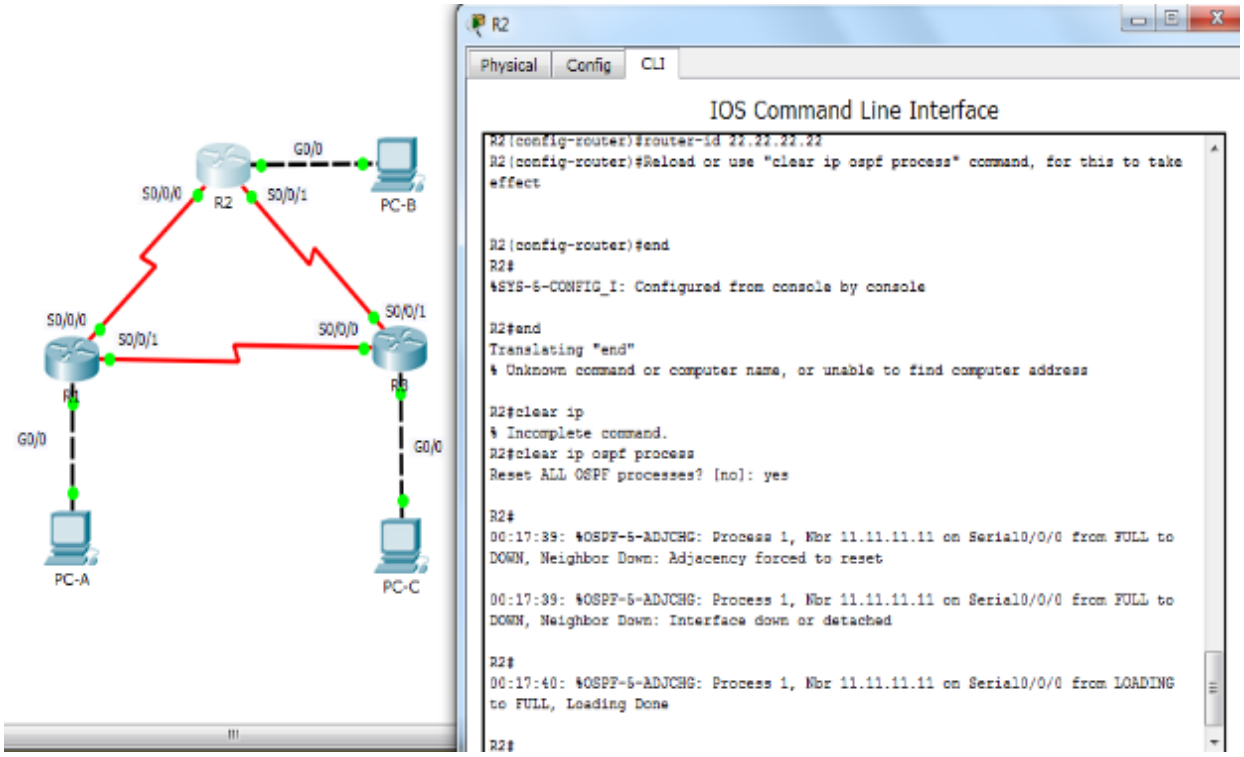
a. Emita el comando **router-id 11.11.11.11** en el R1 para reasignar la ID del router. Observe el mensaje informativo que aparece al emitir el comando **router-id**.

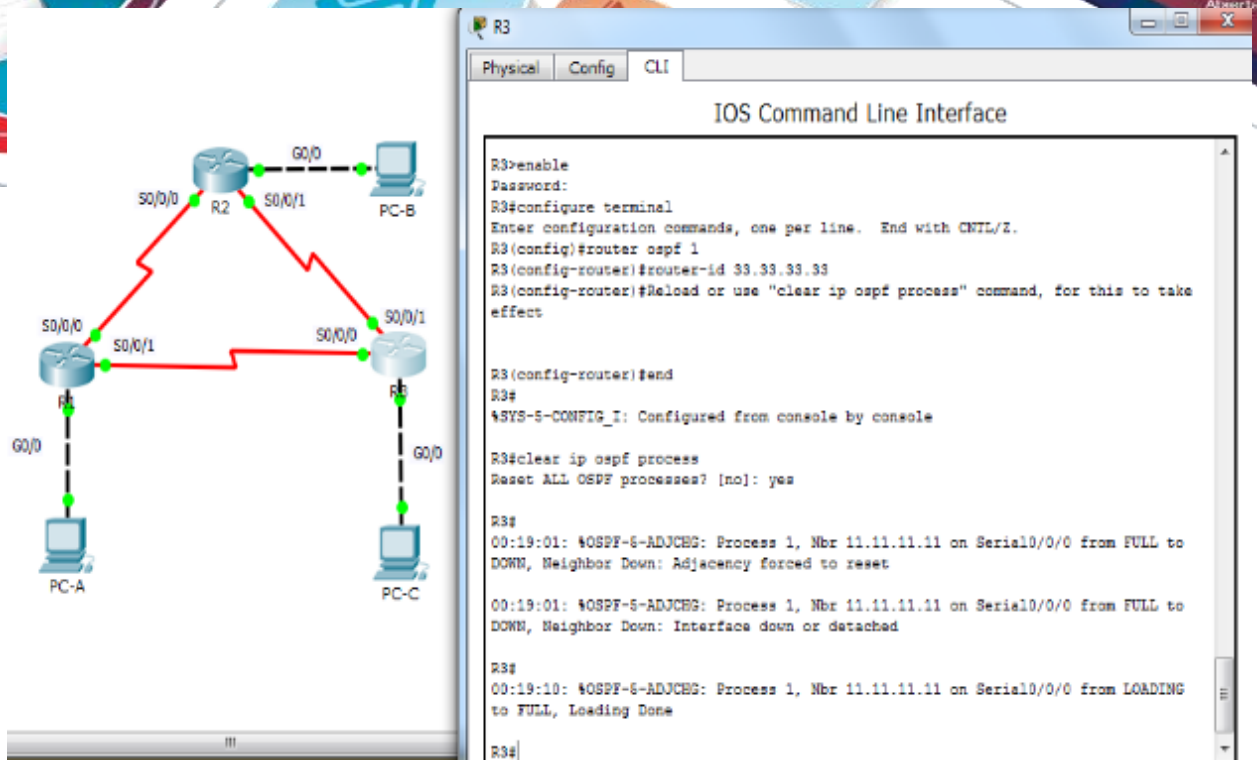


b. Recibirá un mensaje informativo en el que se le indique que debe volver a cargar el router o usar el comando **clear ip ospf process** para que se aplique el cambio. Emita el comando **clear ip ospf process** en los tres routers. Escriba **yes** (sí) como respuesta al mensaje de verificación de restablecimiento y presione Enter.



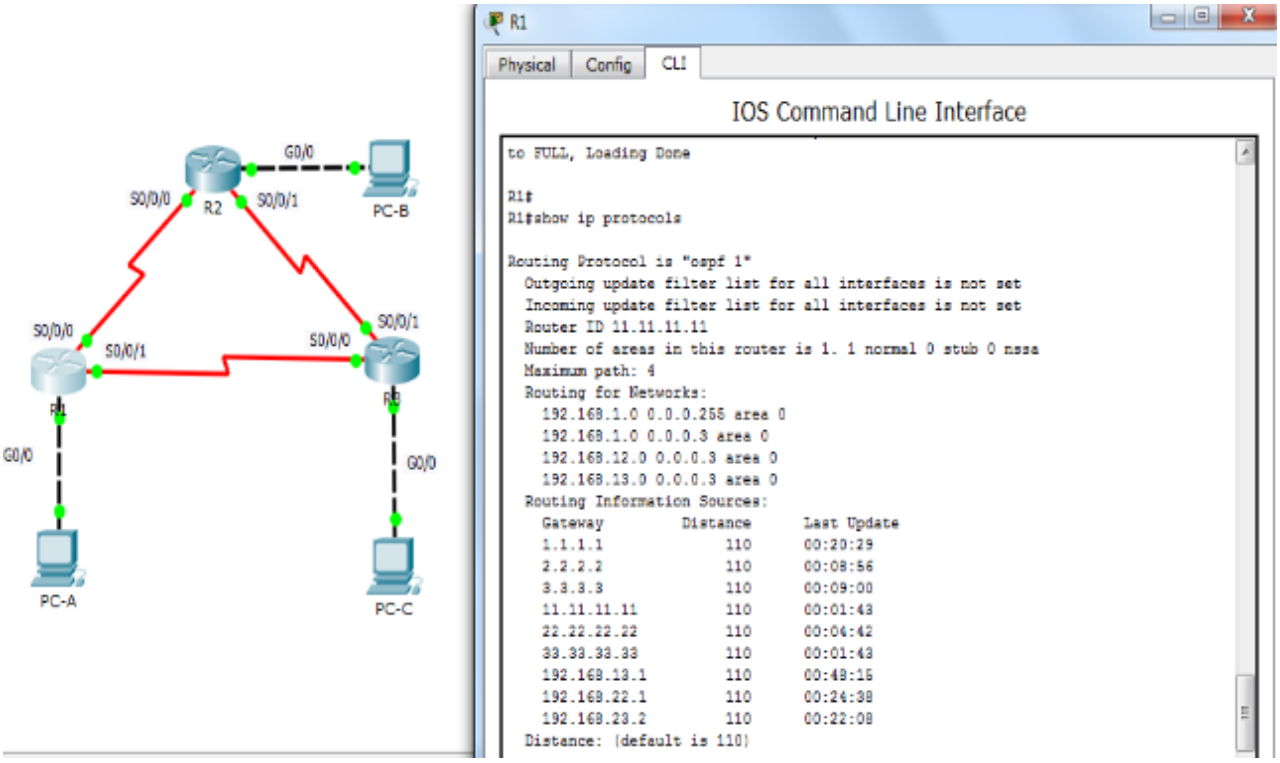
c. Establezca la ID del router R2 **22.22.22.22** y la ID del router R3 **33.33.33.33**. Luego, use el comando **clear ip ospf process** para restablecer el proceso de routing de OSPF.





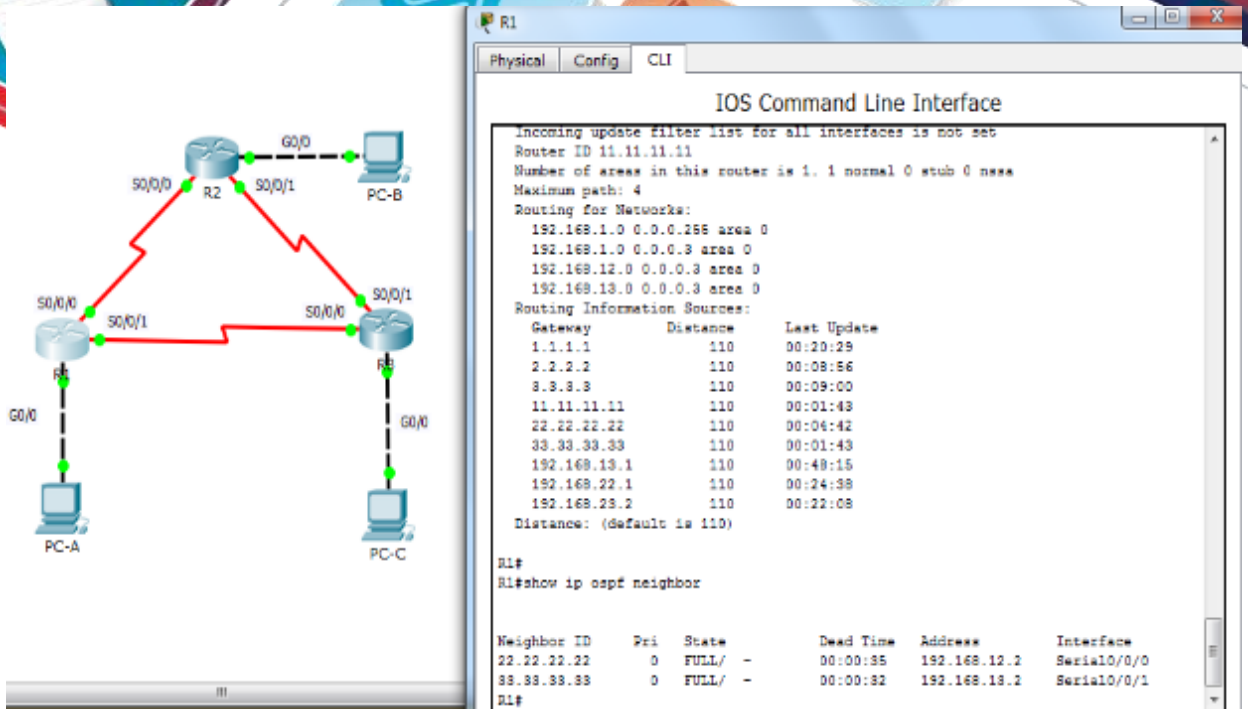
d. Emita el comando **show ip protocols** para verificar que la ID del router R1 haya cambiado.

```
R1# show ip protocols
```



e. Emita el comando **show ip ospf neighbor** en el R1 para verificar que se muestren las nuevas ID de los routers R2 y R3.

```
R1# show ip ospf neighbor
```



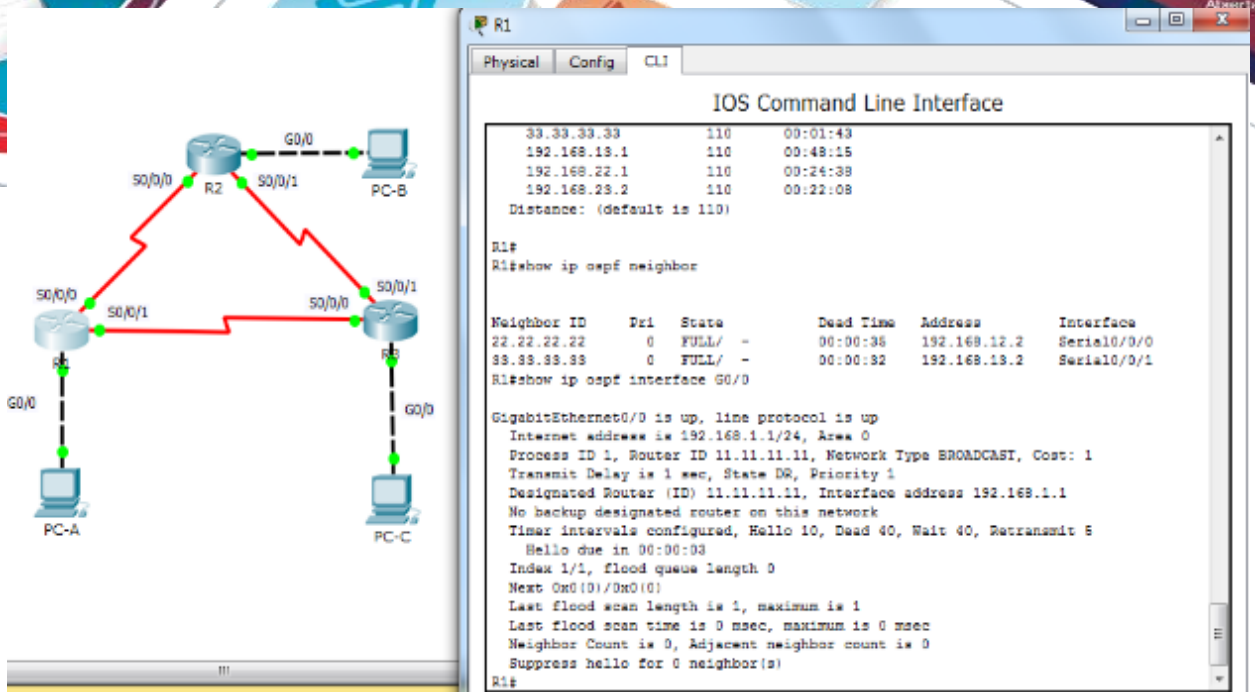
configurar las interfaces pasivas de OSPF

El comando **passive-interface** evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. En la parte 4, utilizará el comando **passive-interface** para configurar una única interfaz como pasiva. También configurará OSPF para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

Step 3: configurar una interfaz pasiva.

a. Emita el comando **show ip ospf interface g0/0** en el R1. Observe el temporizador que indica cuándo se espera el siguiente paquete de saludo. Los paquetes de saludo se envían cada 10 segundos y se utilizan entre los routers OSPF para verificar que sus vecinos estén activos.

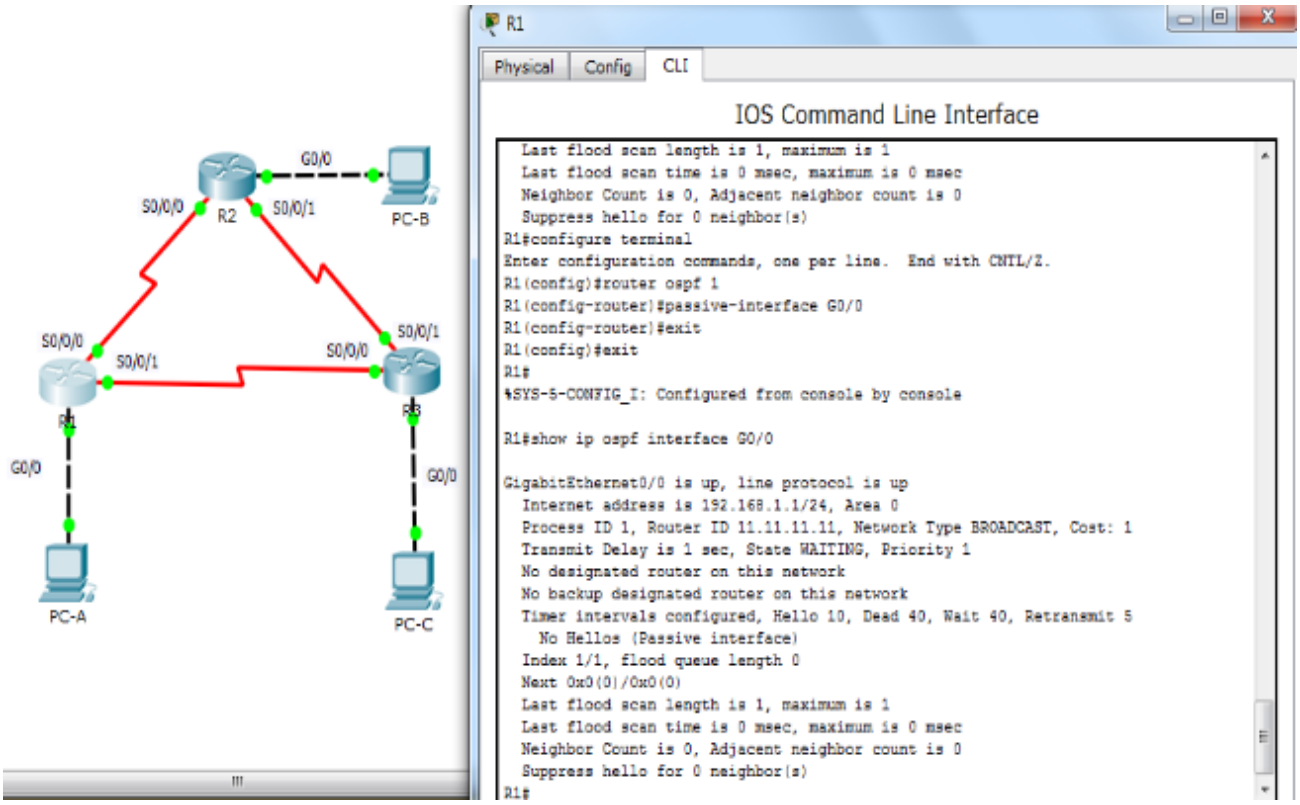
```
R1# show ip ospf interface g0/0
```



b. Emita el comando **passive-interface** para cambiar la interfaz G0/0 en el R1 a pasiva.

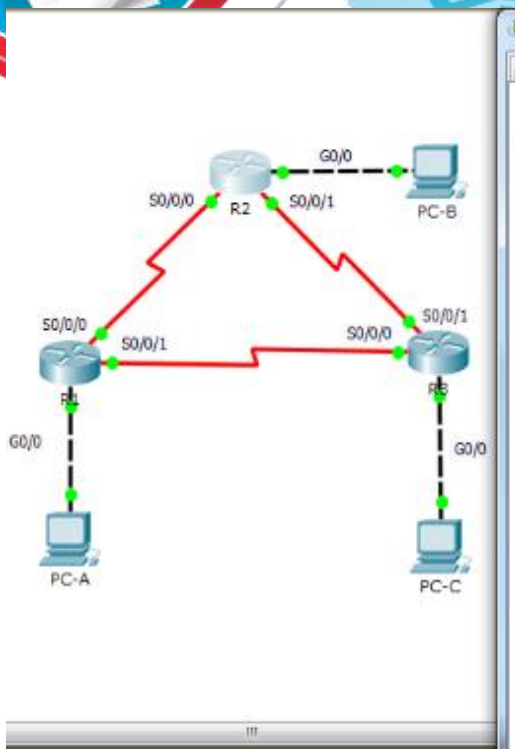
```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0
```

c. Vuelva a emitir el comando **show ip ospf interface g0/0** para verificar que la interfaz G0/0 ahora sea pasiva.



d. Emita el comando **show ip route** en el R2 y el R3 para verificar que todavía haya disponible una ruta a la red 192.168.1.0/24.

R2# **show ip route**

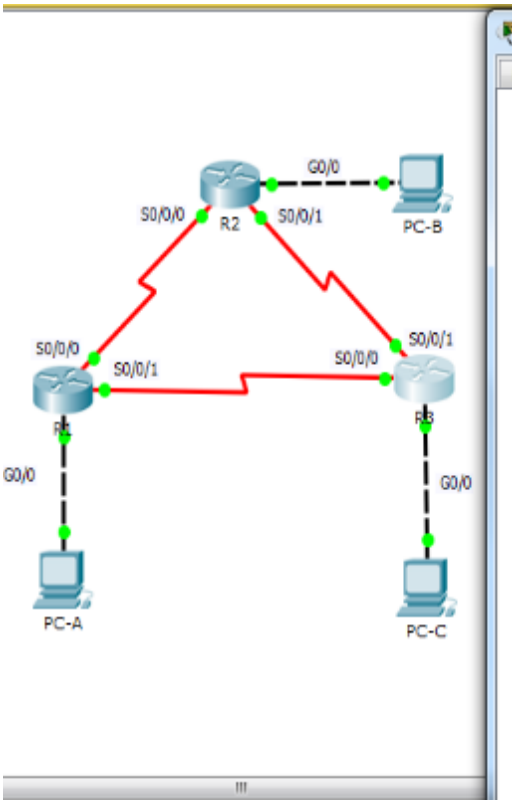


R2

Physical | Config | CLI

IOS Command Line Interface

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:00:37, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/129] via 192.168.12.1, 00:00:27, Serial0/0/0
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
     192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0/30 [110/128] via 192.168.12.1, 00:00:37, Serial0/0/0
     192.168.22.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.22.0/30 is directly connected, Serial0/0/1
L       192.168.22.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/192] via 192.168.12.1, 00:00:27, Serial0/0/0
R2#
```



R3

Physical | Config | CLI

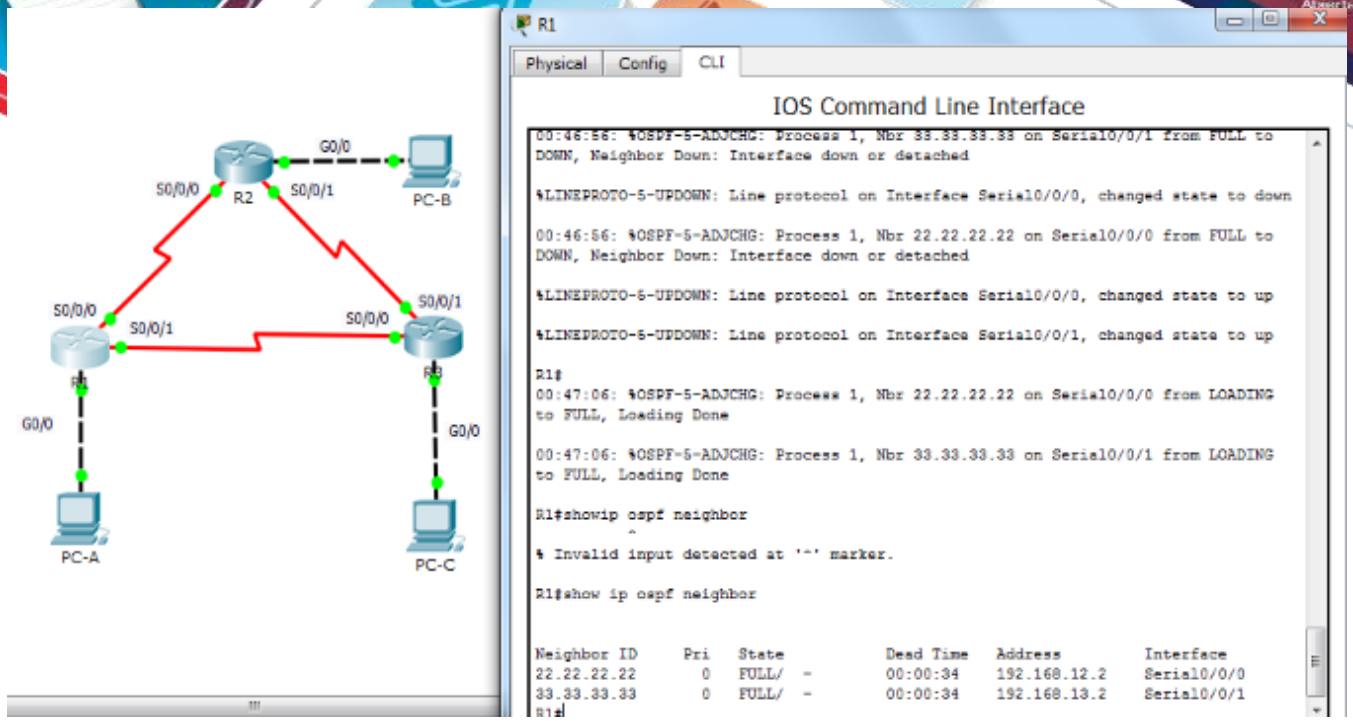
IOS Command Line Interface

```
R3>enable
Password:
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:03:58, Serial0/0/0
O    192.168.2.0/24 [110/129] via 192.168.13.1, 00:03:58, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:03:58, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
R3#
```

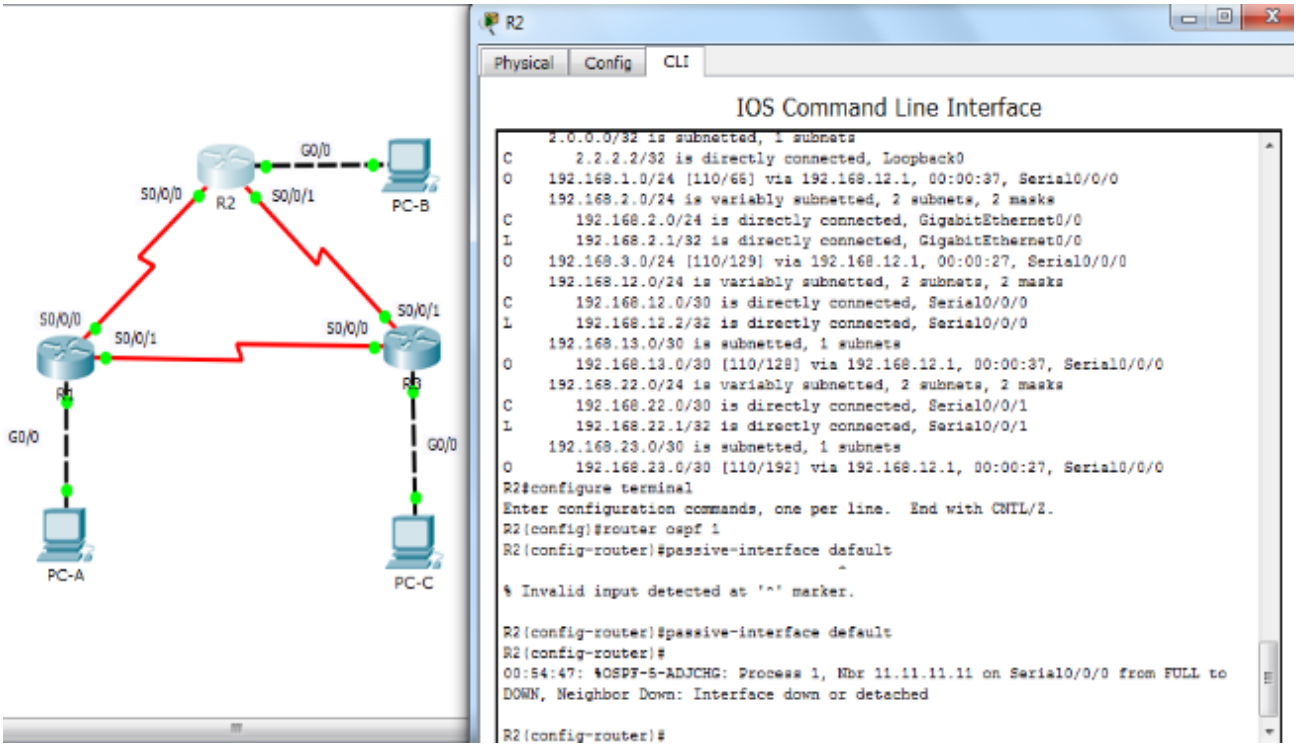
Step 4: establecer la interfaz pasiva como la interfaz predeterminada en un router.

a. Emita el comando **show ip ospf neighbor** en el R1 para verificar que el R2 aparezca como un vecino OSPF.

R1# **show ip ospf neighbor**

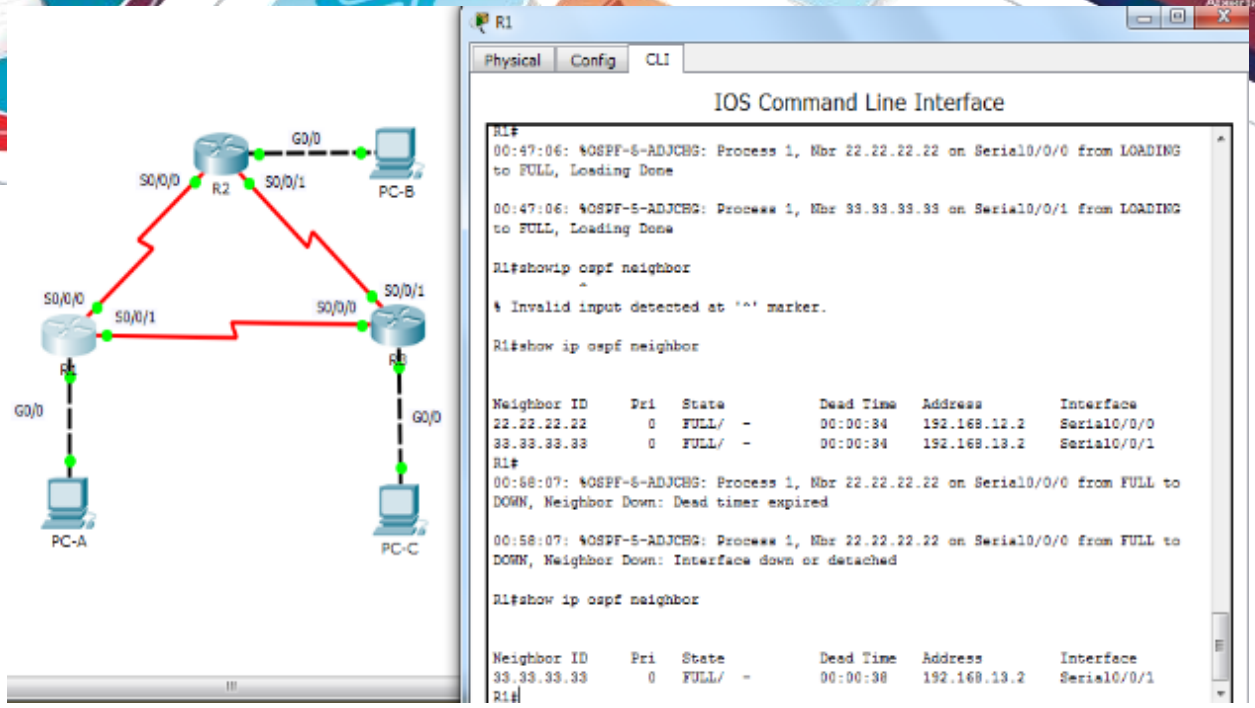


b. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPF como pasivas de manera predeterminada.



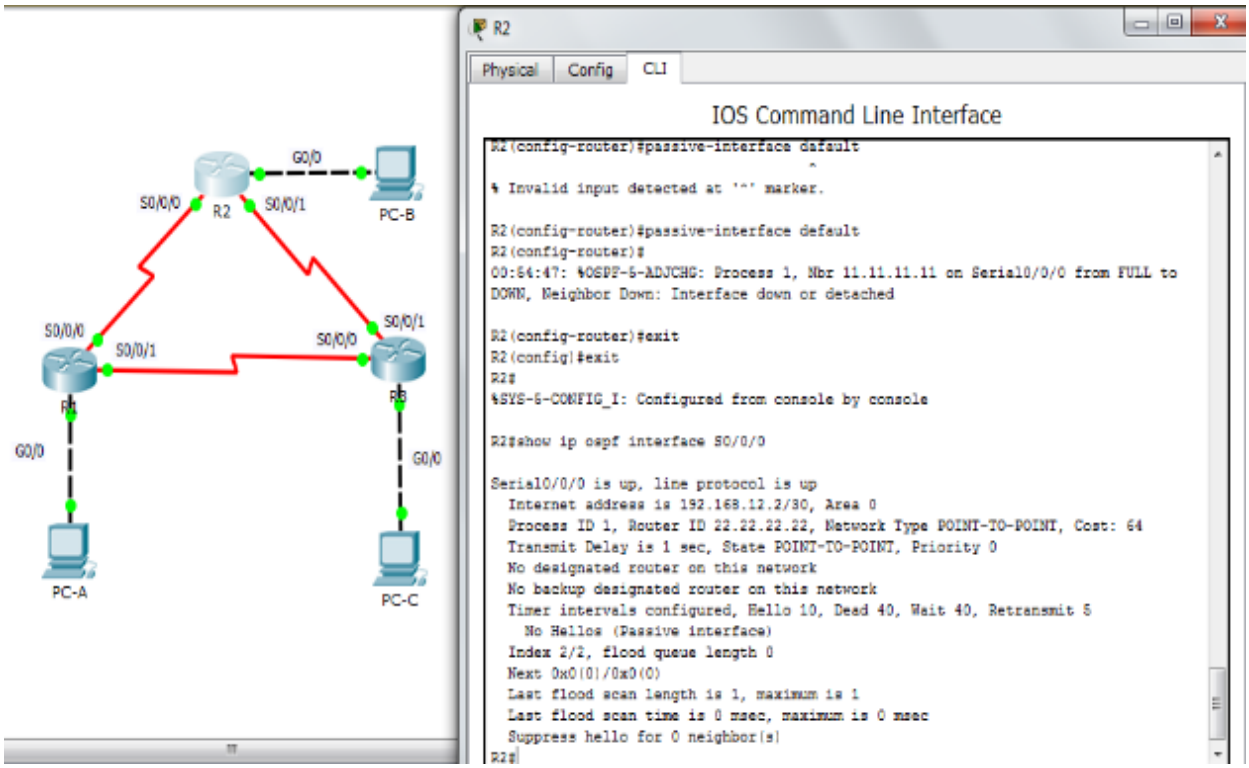
c. Vuelva a emitir el comando **show ip ospf neighbor** en el R1. Una vez que el temporizador de tiempo muerto haya caducado, el R2 ya no se mostrará como un vecino OSPF.

```
R1# show ip ospf neighbor
```

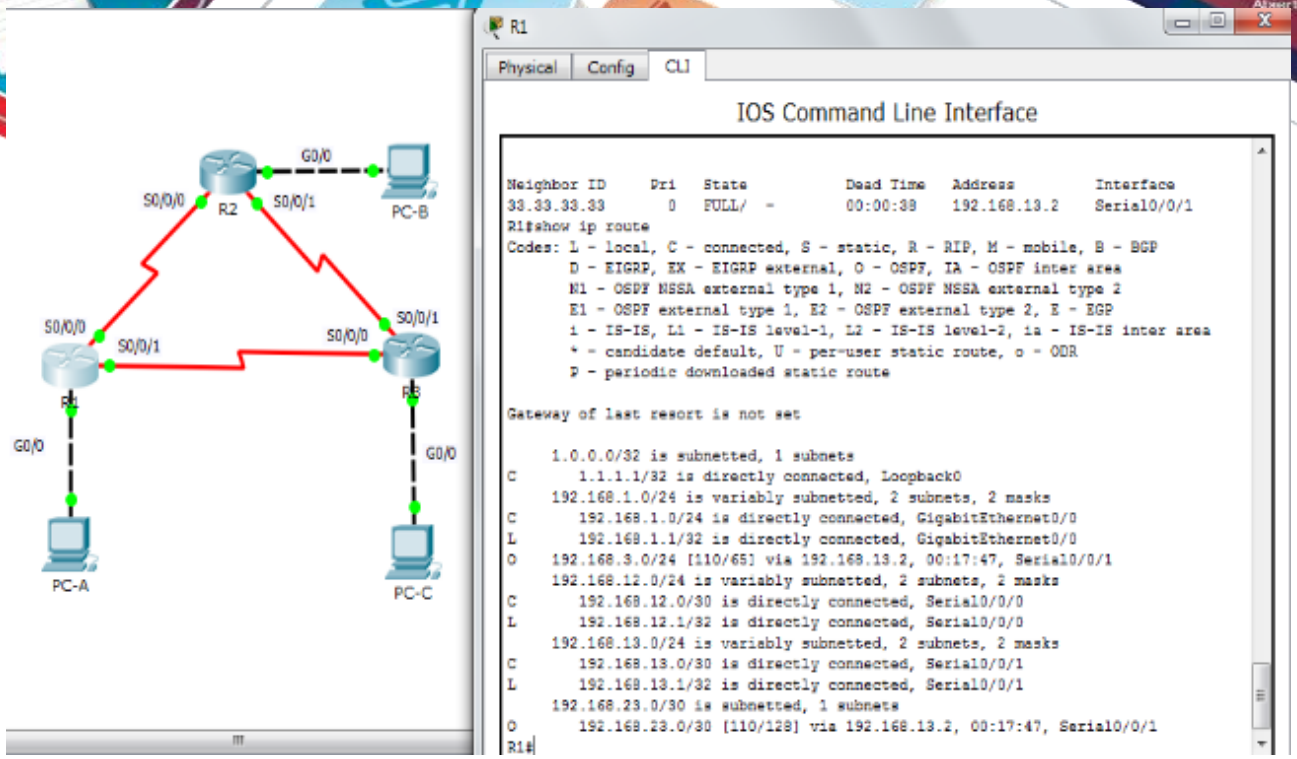


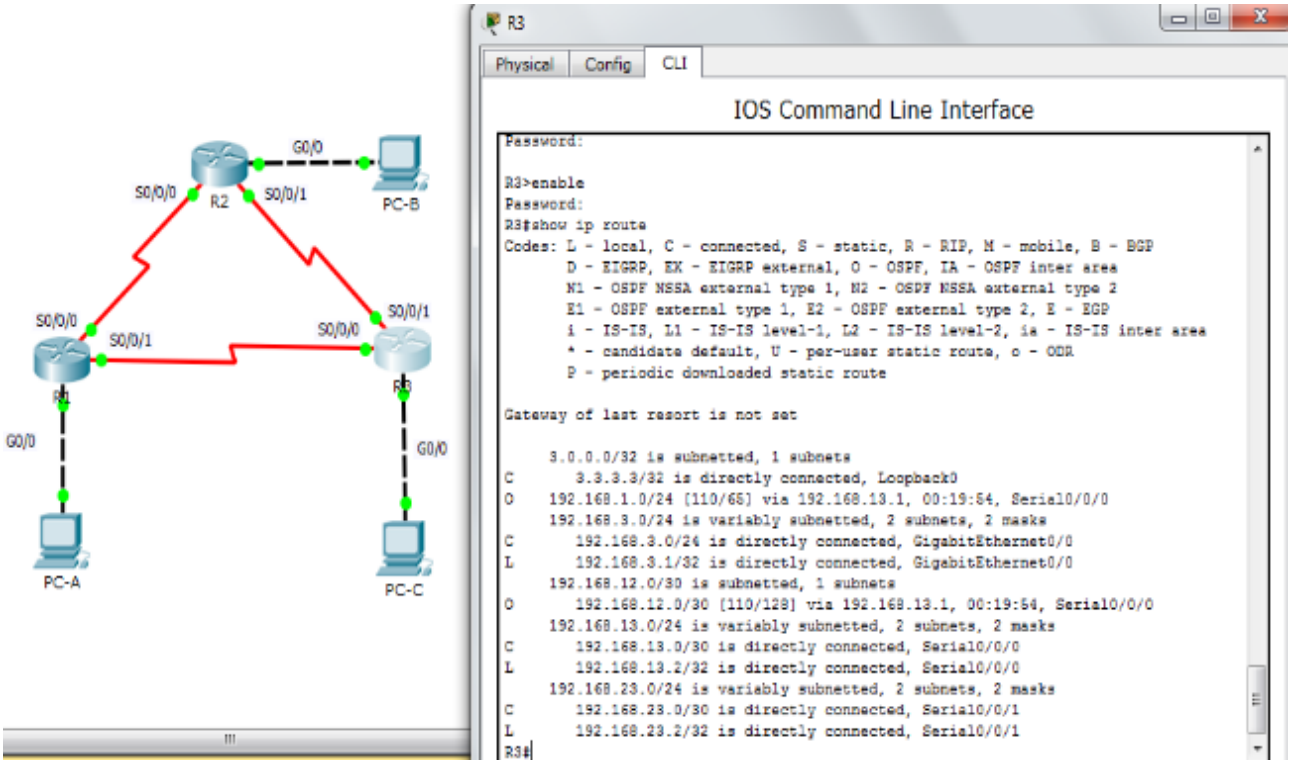
d. Emita el comando **show ip ospf interface S0/0/0** en el R2 para ver el estado de OSPF de la interfaz S0/0/0.

```
R2# show ip ospf interface s0/0/0
```

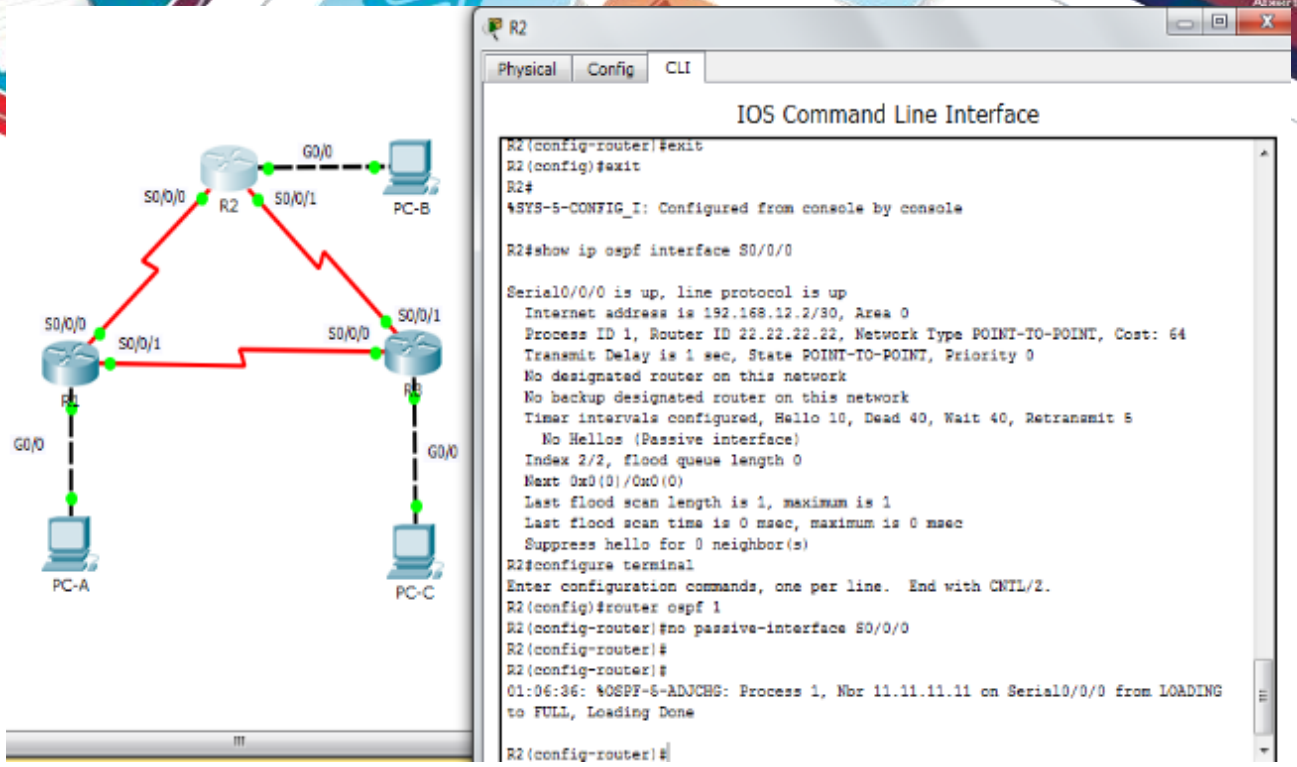


e. Si todas las interfaces en el R2 son pasivas, no se anuncia ninguna información de routing. En este caso, el R1 y el R3 ya no deberían tener una ruta a la red 192.168.2.0/24. Esto se puede verificar mediante el comando **show ip route**.





f. En el R2, emita el comando **no passive-interface** para que el router envíe y reciba actualizaciones de routing OSPF. Después de introducir este comando, verá un mensaje informativo que explica que se estableció una adyacencia de vecino con el R1.



g. Vuelva a emitir los comandos **show ip route** y **show ipv6 ospf neighbor** en el R1 y el R3, y busque una ruta a la red 192.168.2.0/24.

¿Qué interfaz usa el R3 para enrutarse a la red 192.168?2.0/24? 192.168.2.0/24[110/129]

192.168.13.1, 00:01:19, serial 0/0/0

192.168.3.0/24

¿Cuál es la métrica de costo acumulado para la red 192.168?2.0/24 en el R3? Costo acumulado 129

¿El R2 aparece como vecino OSPF en el R1? Si

¿El R2 aparece como vecino OSPF en el R3? No

¿Qué indica esta información? Que en el router 1 se indico que la interface S0/0/0 conectada al R1 no es una interfaz pasiva, por ello aparece como vecino el R2 en el R1 y no en el R3

h. Cambie la interfaz S0/0/1 en el R2 para permitir que anuncie las rutas OSPF. Registre los comandos utilizados a continuación.

R2# configure terminal

R2(config)#router ospf 1

R2(config-router)#no passive-interface S0/0/0

i. Vuelva a emitir el comando **show ip route** en el R3.

¿Qué interfaz usa el R3 para enrutarse a la red 192.168?2.0/24? 192.168.3.0/24 is directly connected, GigabitEthernet 0/0

¿Cuál es la métrica de costo acumulado para la red 192.168?2.0/24 en el R3 y cómo se calcula?
192.168.2.0/24[110/65] via 192.168.23.1, 00:00:31, serial 0/0/1

Costo Acumulado: 65 se calcula sumando el costo de la interfaz que conecta el router 3 con el R1 y de la interfaz que conecta el R3 con el R2

¿El R2 aparece como vecino OSPF del R3? Si

cambiar las métricas de OSPF

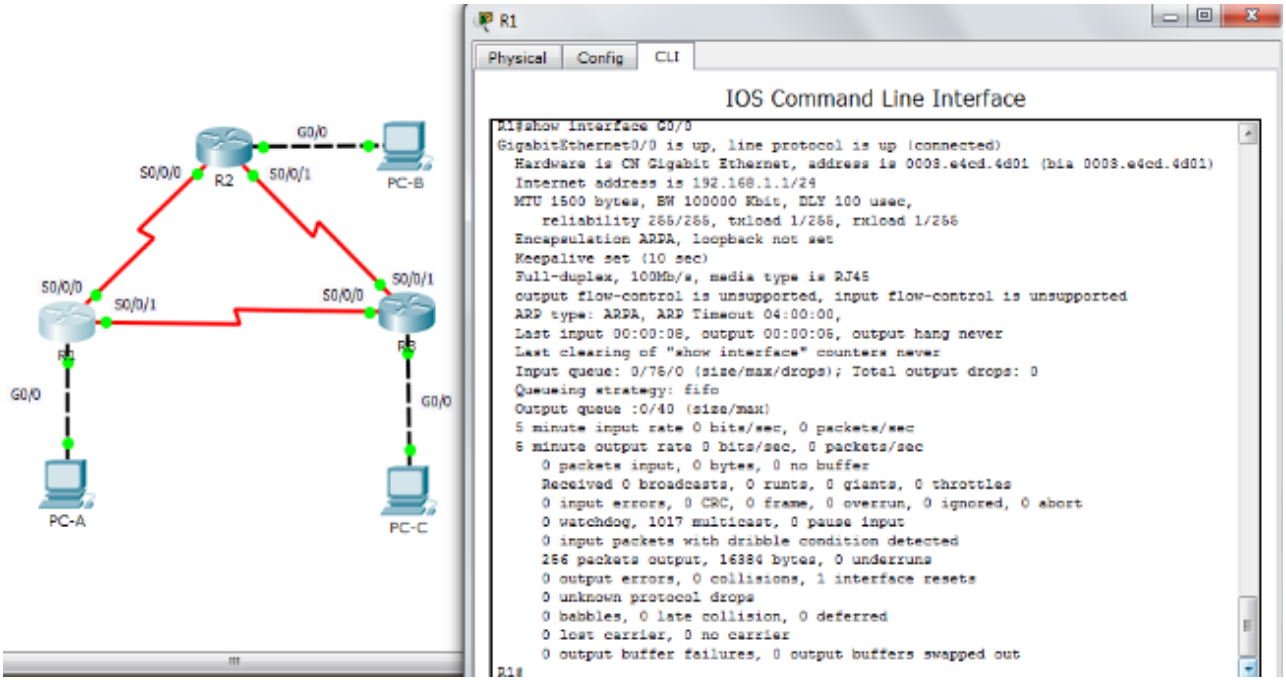
En la parte 3, cambiará las métricas de OSPF con los comandos **auto-cost reference-bandwidth**, **bandwidth** e **ip ospf cost**.

Nota: en la parte 1, se deberían haber configurado todas las interfaces DCE con una frecuencia de reloj de 128000.

Step 5: cambiar el ancho de banda de referencia en los routers.

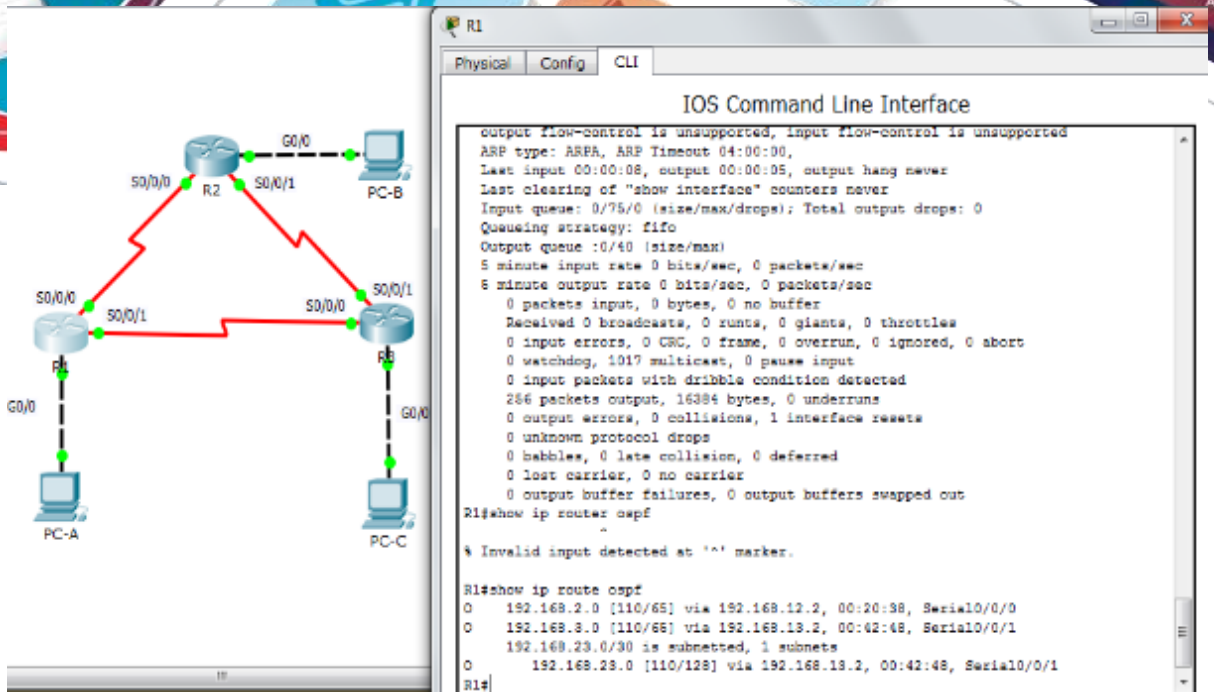
El ancho de banda de referencia predeterminado para OSPF es 100 Mb/s (velocidad Fast Ethernet). Sin embargo, la mayoría de los dispositivos de infraestructura moderna tienen enlaces con una velocidad superior a 100 Mb/s. Debido a que la métrica de costo de OSPF debe ser un número entero, todos los enlaces con velocidades de transmisión de 100 Mb/s o más tienen un costo de 1. Esto da como resultado interfaces Fast Ethernet, Gigabit Ethernet y 10G Ethernet con el mismo costo. Por eso, se debe cambiar el ancho de banda de referencia a un valor más alto para admitir redes con enlaces más rápidos que 100 Mb/s.

a. Emita el comando **show interface** en el R1 para ver la configuración del ancho de banda predeterminado para la interfaz G0/0.



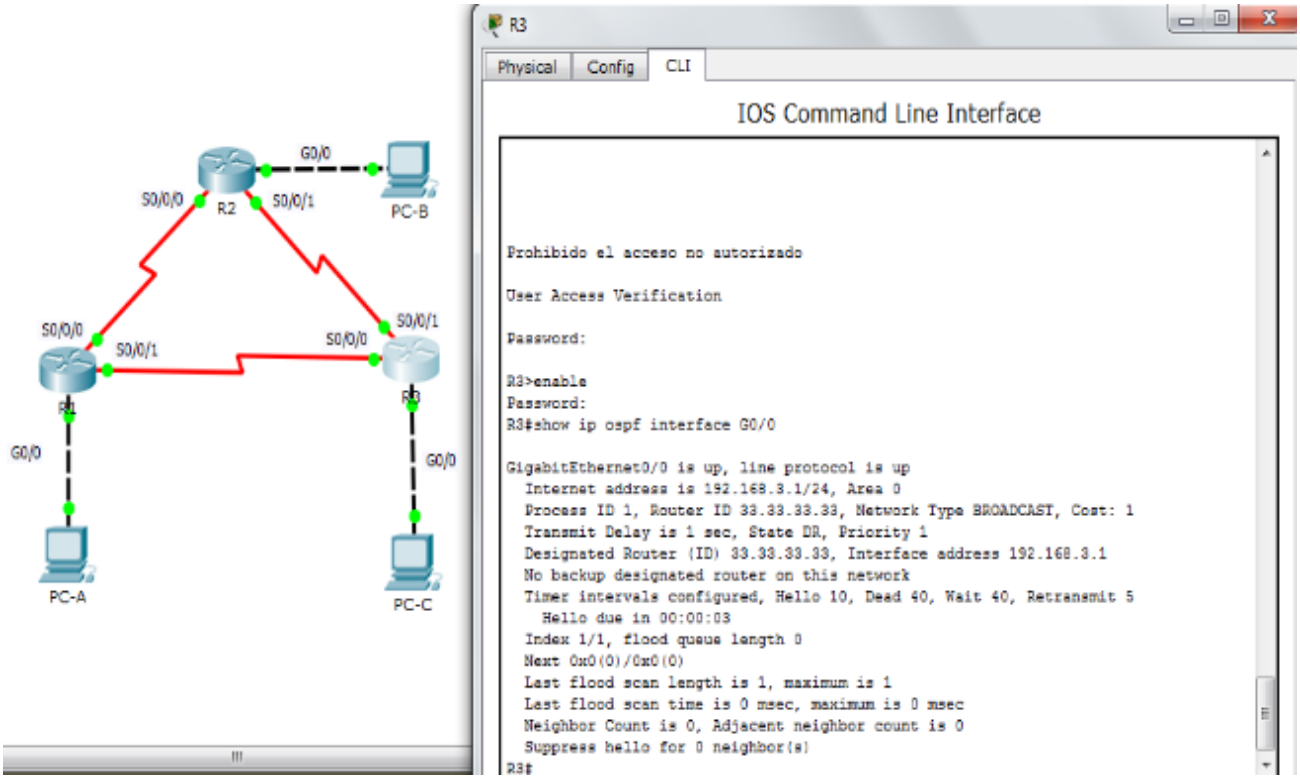
Nota: si la interfaz del equipo host solo admite velocidad Fast Ethernet, la configuración de ancho de banda de G0/0 puede diferir de la que se muestra arriba. Si la interfaz del equipo host no admite velocidad de gigabit, es probable que el ancho de banda se muestre como 100 000 Kbit/s.

b. Emita el comando **show ip route ospf** en el R1 para determinar la ruta a la red 192.168.3.0/24.

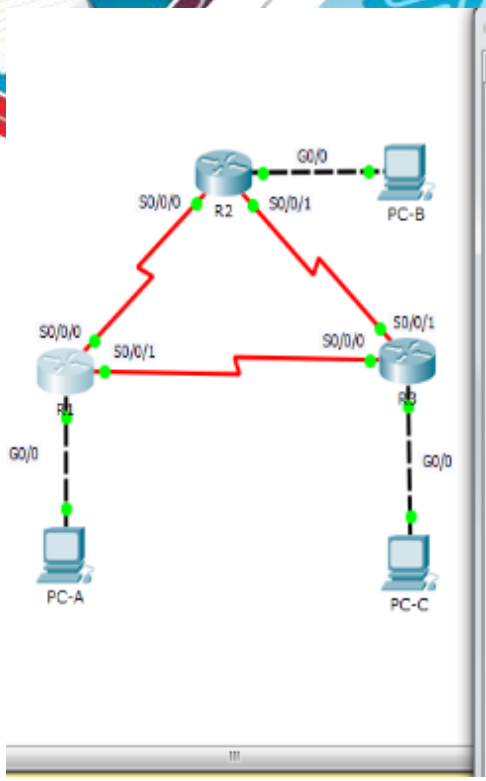


Nota: el costo acumulado del R1 a la red 192.168.3.0/24 es 65.

c. Emita el comando **show ip ospf interface** en el R3 para determinar el costo de routing para G0/0.



d. Emita el comando **show ip ospf interface s0/0/1** en el R1 para ver el costo de routing para S0/0/1.



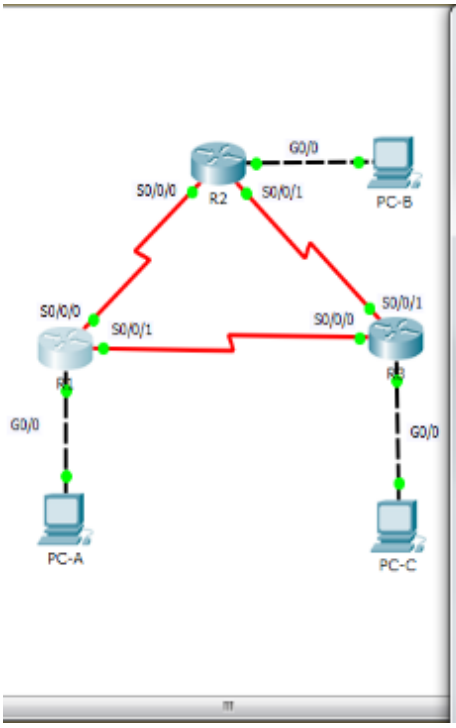
R1

Physical | Config | CLI

IOS Command Line Interface

```
% Invalid input detected at '^' marker.

R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 00:20:38, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:42:48, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 00:42:48, Serial0/0/1
R1#
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#show ip ospf interface S0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 22.22.22.22
  Suppress hello for 0 neighbor(s)
R1#
```

e. Emita el comando **auto-cost reference-bandwidth 10000** en el R1 para cambiar la configuración de ancho de banda de referencia predeterminado. Con esta configuración, las interfaces de 10 Gb/s tendrán un costo de 1, las interfaces de 1 Gb/s tendrán un costo de 10, y las interfaces de 100 Mb/s tendrán un costo de 100.

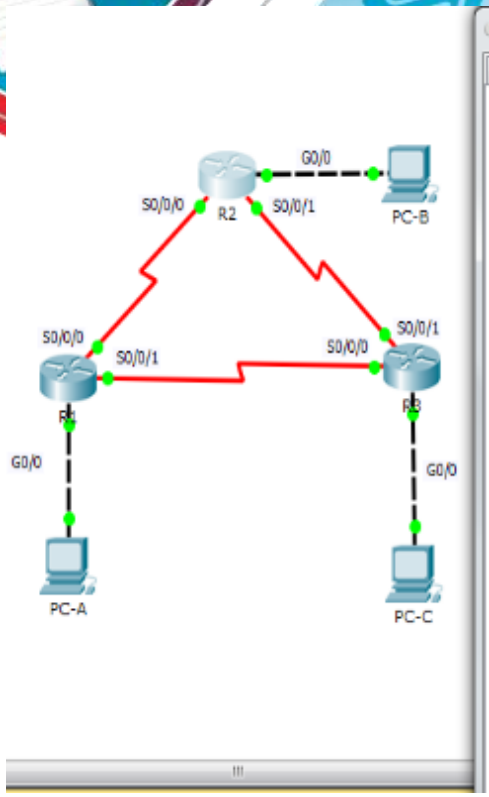


R1

Physical | Config | CLI

IOS Command Line Interface

```
O       192.168.23.0 [110/128] via 192.168.13.2, 00:42:48, Serial0/0/1
R1#
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#show ip ospf interface S0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 22.22.22.22
  Suppress hello for 0 neighbor(s)
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#
```

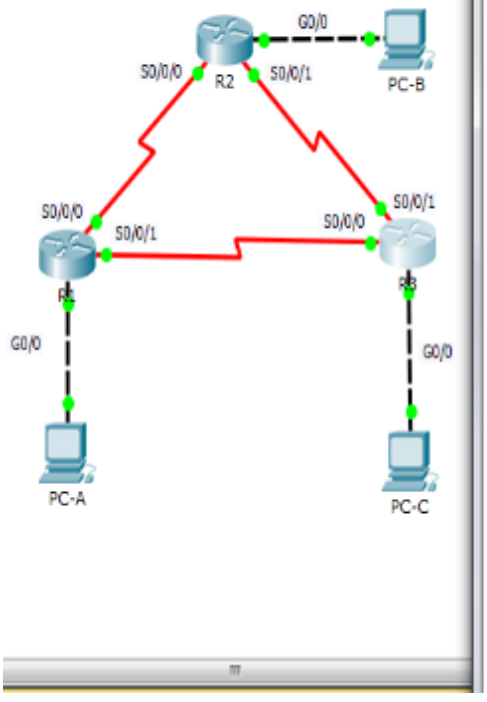


R2

Physical | Config | CLI

IOS Command Line Interface

```
Press RETURN to get started.



Prohibido el acceso no autorizado

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R2(config-router)#
```



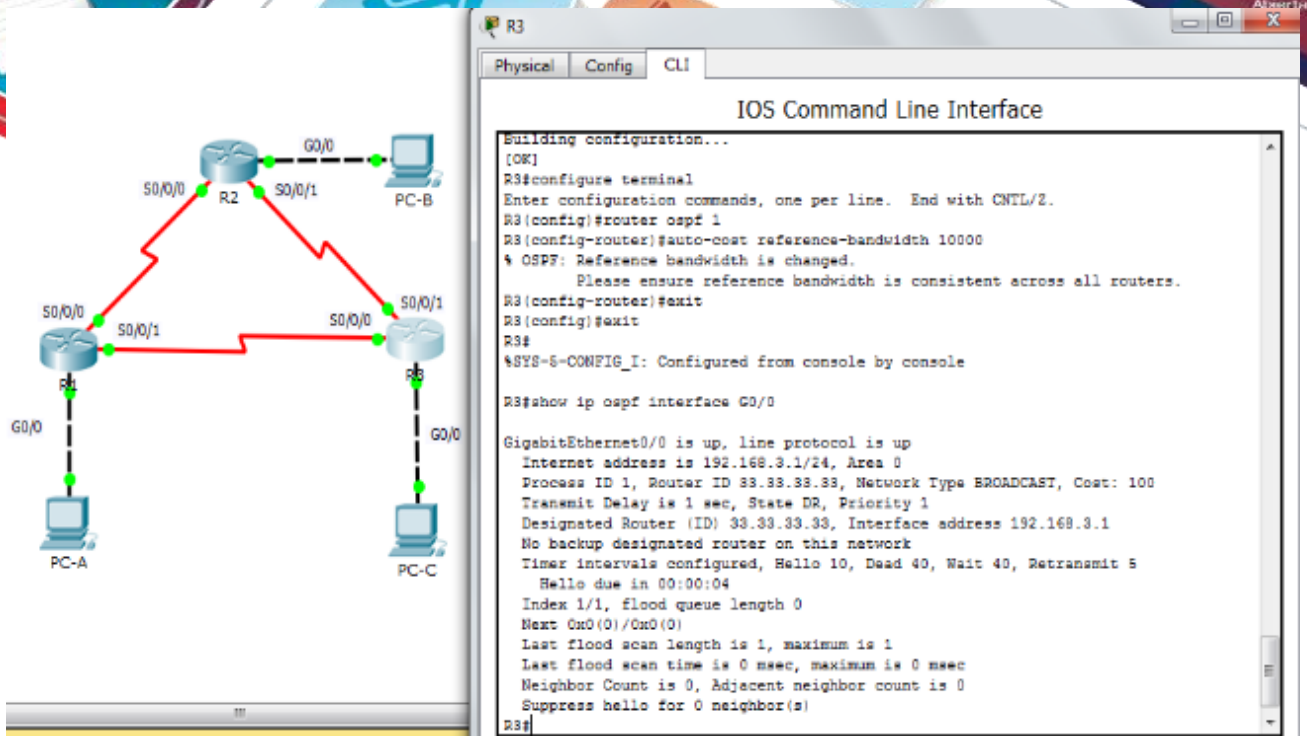
R3

Physical | Config | CLI

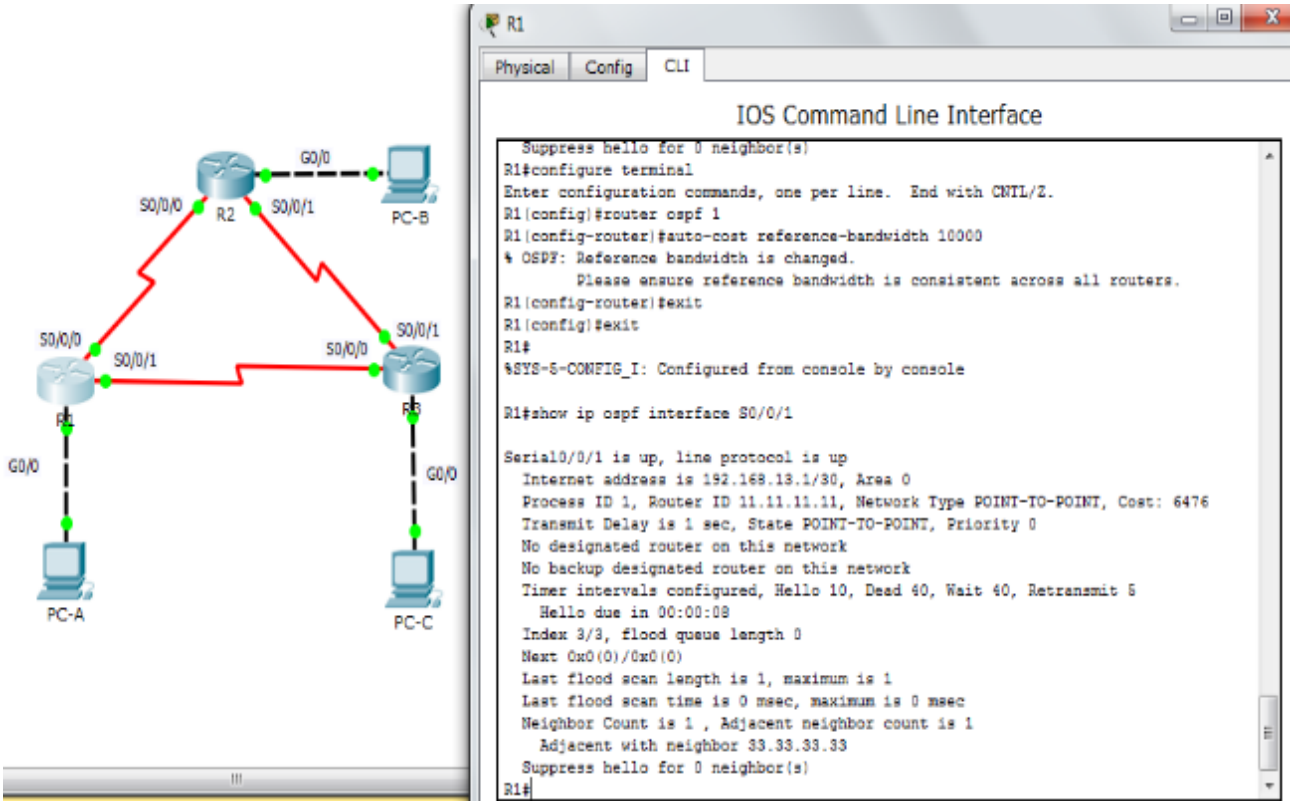
IOS Command Line Interface

```
R3>enable
Password:
R3#show ip ospf interface G0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R3(config-router)#
```

g. Vuelva a emitir el comando **show ip ospf interface** para ver el nuevo costo de G0/0 en el R3 y de S0/0/1 en el R1.

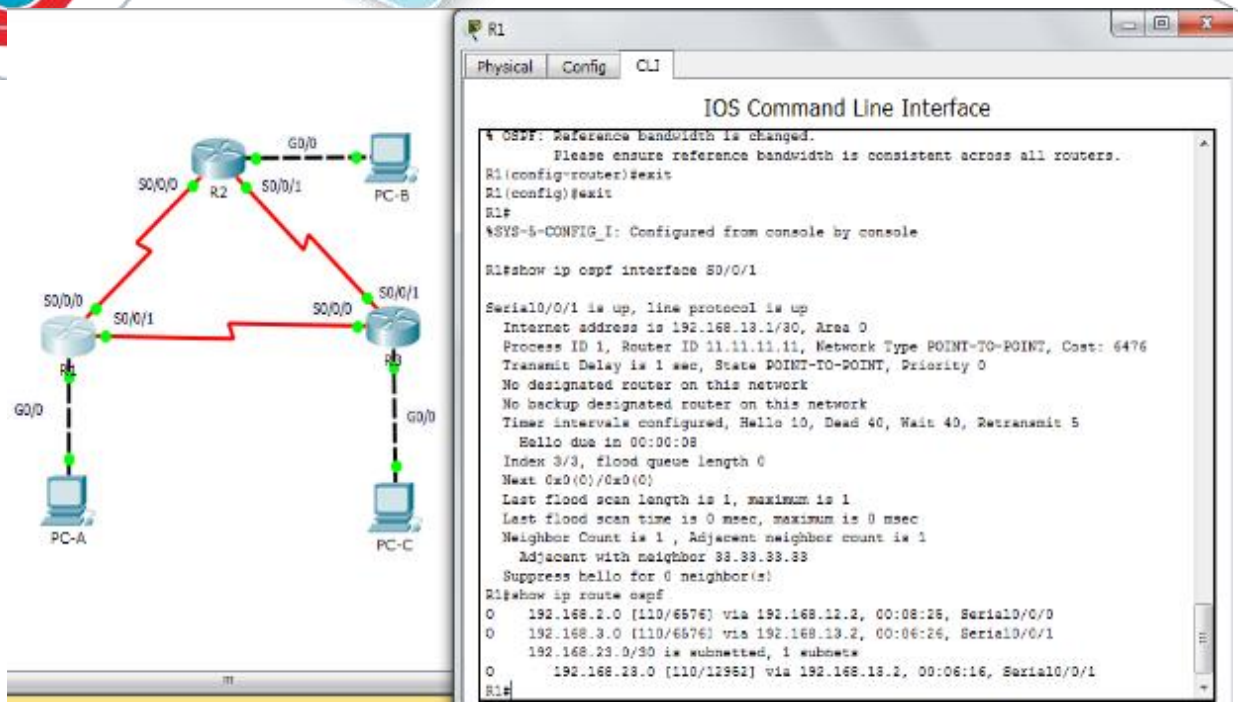


Nota: si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo será diferente del que se muestra en el resultado. Por ejemplo, el costo será de 100 para la velocidad Fast Ethernet (100 Mb/s).

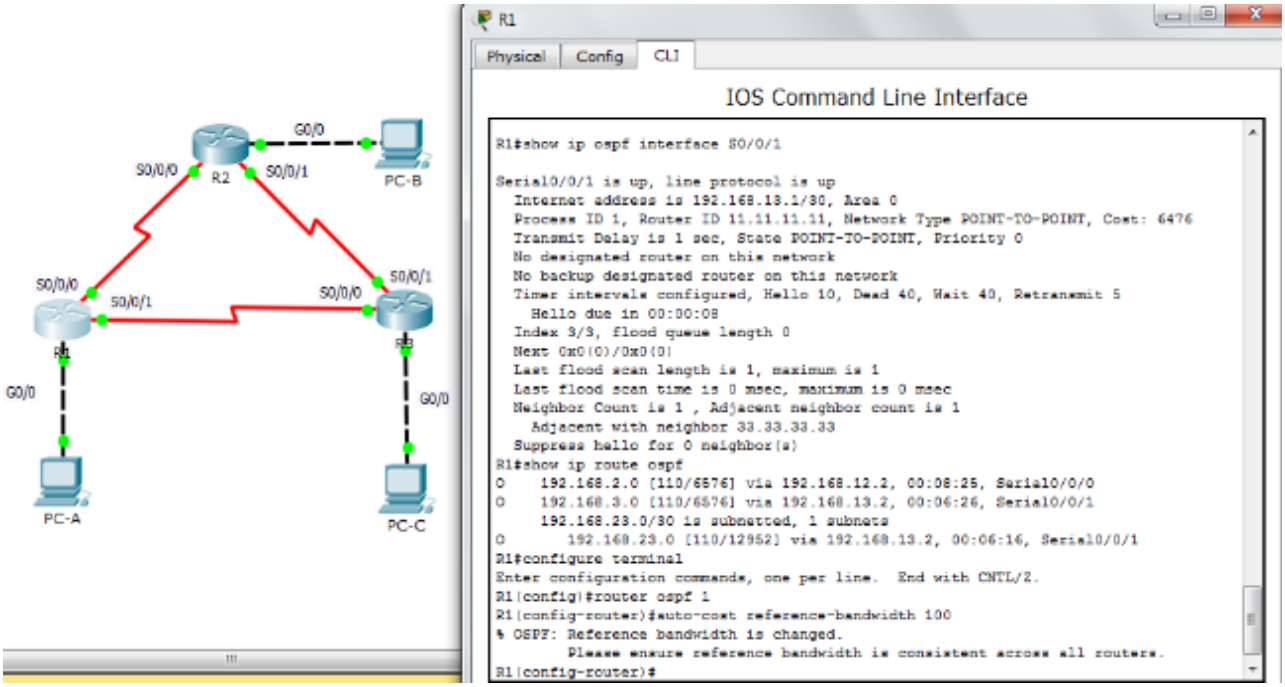


h. Vuelva a emitir el comando **show ip route ospf** para ver el nuevo costo acumulado de la ruta 192.168.3.0/24 (10 + 6476 = 6486).

Nota: si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo total será diferente del que se muestra en el resultado. Por ejemplo, el costo acumulado será 6576 si G0/0 está funcionando con velocidad Fast Ethernet (100 Mb/s).



h. Para restablecer el ancho de banda de referencia al valor predeterminado, emita el comando **auto-cost reference-bandwidth 100** en los tres routers.



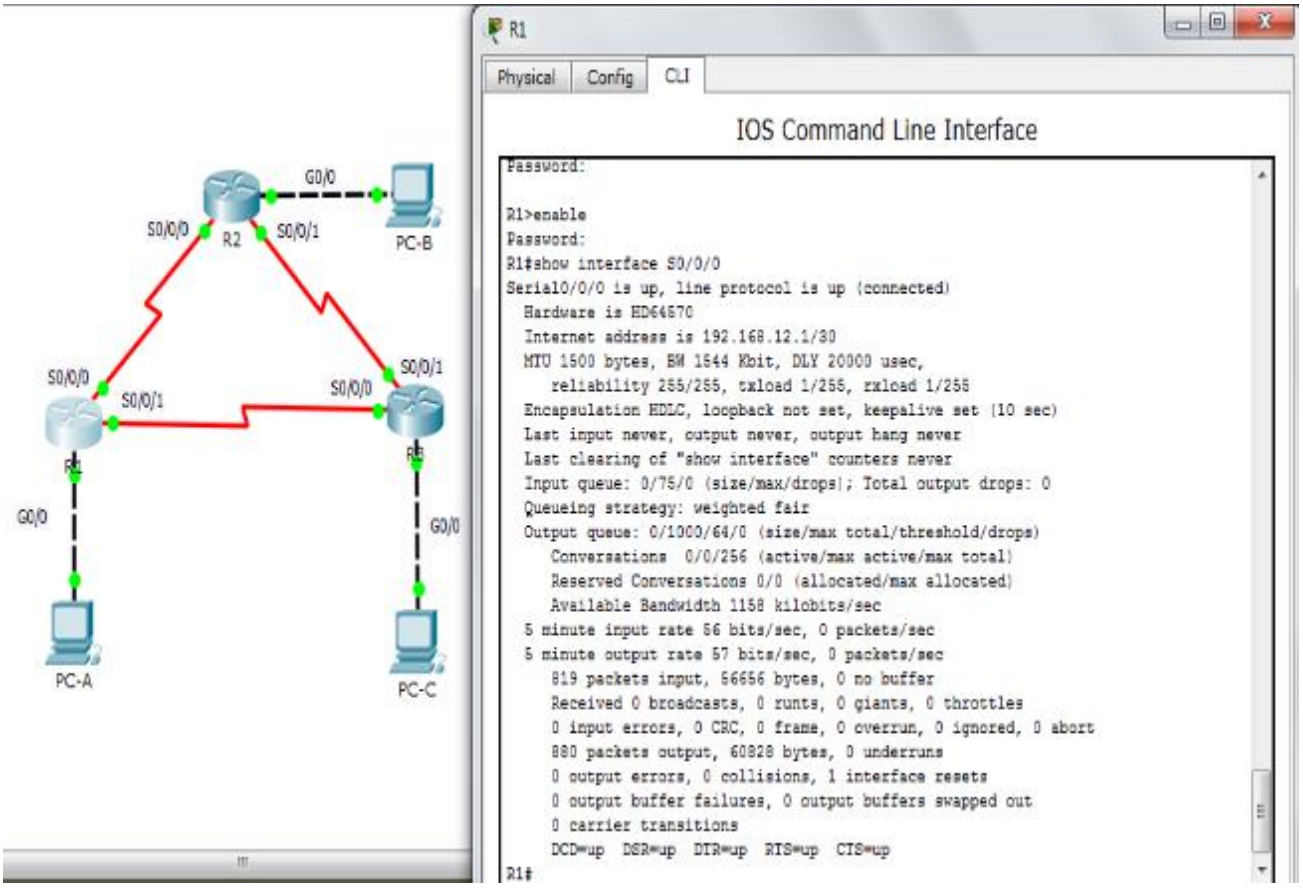
¿Por qué querría cambiar el ancho de banda de referencia OSPF predeterminado? La formula usada para calcular la métrica es: costo= 100.000.000/el ancho de la banda de interfaz en bps. Es recomendable cambiar este valor, ya que el resultado del costo no admite números negativos y los redondeara al numero entero mas cercano es decir a 1.

Step 6: cambiar el ancho de banda de una interfaz.

En la mayoría de los enlaces seriales, la métrica del ancho de banda será 1544 Kbits de manera predeterminada (la de un T1). Si esta no es la velocidad real del enlace serial, se deberá cambiar la configuración del ancho de banda para que coincida con la velocidad real, a fin de permitir que el costo de la ruta se calcule correctamente en OSPF. Use el comando **bandwidth** para ajusta la configuración del ancho de banda de una interfaz.

Nota: un concepto erróneo habitual es suponer que con el comando **bandwidth** se cambia el ancho de banda físico, o la velocidad, del enlace. El comando modifica la métrica de ancho de banda que utiliza OSPF para calcular los costos de routing, pero no modifica el ancho de banda real (la velocidad) del enlace.

a. Emita el comando **show interface s0/0/0** en el R1 para ver la configuración actual del ancho de banda de S0/0/0. Aunque la velocidad de enlace/frecuencia de reloj en esta interfaz estaba configurada en 128 Kb/s, el ancho de banda todavía aparece como 1544 Kb/s.



b. Emita el comando **show ip route ospf** en el R1 para ver el costo acumulado de la ruta a la red 192.168.23.0/24 con S0/0/0. Observe que hay dos rutas con el mismo costo (128) a la red 192.168.23.0/24, una a través de S0/0/0 y otra a través de S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1
                      [110/128] via 192.168.12.2, 00:00:42, Serial0/0/0
```

c. Emita el comando **bandwidth 128** para establecer el ancho de banda en S0/0/0 en 128 Kb/s.

```
R1(config)# interface s0/0/0
R1(config-if)# bandwidth 128
```

d. Vuelva a emitir el comando **show ip route ospf**. En la tabla de routing, ya no se muestra la ruta a la red 192.168.23.0/24 a través de la interfaz S0/0/0. Esto es porque la mejor ruta, la que tiene el costo más bajo, ahora es a través de S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1
```

e. Emita el comando **show ip ospf interface brief**. El costo de S0/0/0 cambió de 64 a 781, que es una representación precisa del costo de la velocidad del enlace.

```
R1# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1      1     0               192.168.13.1/30    64    P2P   1/1
Se0/0/0      1     0               192.168.12.1/30    781   P2P   1/1
Gi0/0        1     0               192.168.1.1/24     1     DR    0/0
```

f. Cambie el ancho de banda de la interfaz S0/0/1 a la misma configuración que S0/0/0 en el R1.

g. Vuelva a emitir el comando **show ip route ospf** para ver el costo acumulado de ambas rutas a la red 192.168.23.0/24. Observe que otra vez hay dos rutas con el mismo costo (845) a la red 192.168.23.0/24: una a través de S0/0/0 y otra a través de S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1
                      [110/845] via 192.168.12.2, 00:00:09, Serial0/0/0
```

Explique la forma en que se calcularon los costos del R1 a las redes 192.168.3.0/24 y 192.168.23.0/30.

192.168.3.0 [110 /782] via 192.168.13.2, 00:00:00 serial 0/0/1

192.168.23.0 [110/ /845] via 192.168.12.2, 00:00:00 serial 0/0/0

h. Emita el comando **show ip route ospf** en el R3. El costo acumulado de 192.168.1.0/24 todavía se muestra como 65. A diferencia del comando **clock rate**, el comando **bandwidth** se tiene que aplicar en ambos extremos de un enlace serial.

```
R3# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
      192.168.12.0/30 is subnetted, 1 subnets
O        192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1
                      [110/128] via 192.168.13.1, 00:30:58, Serial0/0/0
```

i. Emita el comando **bandwidth 128** en todas las interfaces seriales restantes de la topología.

¿Cuál es el nuevo costo acumulado a la red 192.168?23.0/24 en el R1? ¿Por qué?

R1#show ip route ospf

192.168.2.0[110/782] via 192.168.12.2, 00:30:50, serial 0/0/0

192.168.3.0 [110/782] via 192.168.13.2, 00:30:50, Serial 0/0/1

192.168.23.0/30 is subnetteed, 1 subnets

R1# costo acumulado: 1562 ya que el costo acumulado es la suma de las interfaces que se conocen al router el resultado 1562

Step 7: cambiar el costo de la ruta.

De manera predeterminada, OSPF utiliza la configuración de ancho de banda para calcular el costo de un enlace. Sin embargo, puede reemplazar este cálculo si configura manualmente el costo de un enlace mediante el comando **ip ospf cost**. Al igual que el comando **bandwidth**, el comando **ip ospf cost** solo afecta el lado del enlace en el que se aplicó.

a. Emita el comando **show ip route ospf** en el R1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
O     192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
                      [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0
```

b. Aplique el comando **ip ospf cost 1565** a la interfaz S0/0/1 en el R1. Un costo de 1565 es mayor que el costo acumulado de la ruta a través del R2, que es 1562.

```
R1(config)# int s0/0/1
R1(config-if)# ip ospf cost 1565
```

c. Vuelva a emitir el comando **show ip route ospf** en el R1 para mostrar el efecto que produjo este cambio en la tabla de routing. Todas las rutas OSPF para el R1 ahora se enrutan a través del R2.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
O     192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0
```

Nota: la manipulación de costos de enlace mediante el comando **ip ospf cost** es el método de preferencia y el más fácil para cambiar los costos de las rutas OSPF. Además de cambiar el costo basado en el ancho de banda, un administrador de red puede tener otros motivos para cambiar el costo de una ruta, como la preferencia por un proveedor de servicios específico o el costo monetario real de un enlace o de una ruta.

Explique la razón por la que la ruta a la red 192.168.3.0/24 en el R1 ahora atraviesa el R2.

OSPF analiza la mejor ruta y con el menor costo pasando por el R2 se logra un menor costo

Reflexión

1. ¿Por qué es importante controlar la asignación de ID de router al utilizar el protocolo OSPF?

   Los routers usan el ID para identificarse dentro del dominio OSPF

   Es importante el ID del router OSPF por que se utiliza para identificar de forma única el router en el dominio de enrutamiento OSPF

2. ¿Por qué el proceso de elección de DR/BDR no es una preocupación en esta práctica de laboratorio?

   Al asignar un ID a cada router atraves de este se determina el DR y el BDR, dependiendo del ID mas elevado para el DR y el menos para el DBR

   R1, R2 y R3 estan conectados a través de enlaces punto a punto. Por lo tanto, no ocurre la elección de DR/BDR. La selección y los procesos de DR/BDR

3. ¿Por qué querría configurar una interfaz OSPF como pasiva?

   Para evitar que se envíen mensajes de routing por determinada interfaz

   Se requiere para incluir una interfaz en el ospf pero sin transmitir paquetes hechos por la misma interfaz

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.

Ejercicio No 3 - 8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3

Práctica de laboratorio: configuración de OSPFv3 básico de área única

Topología

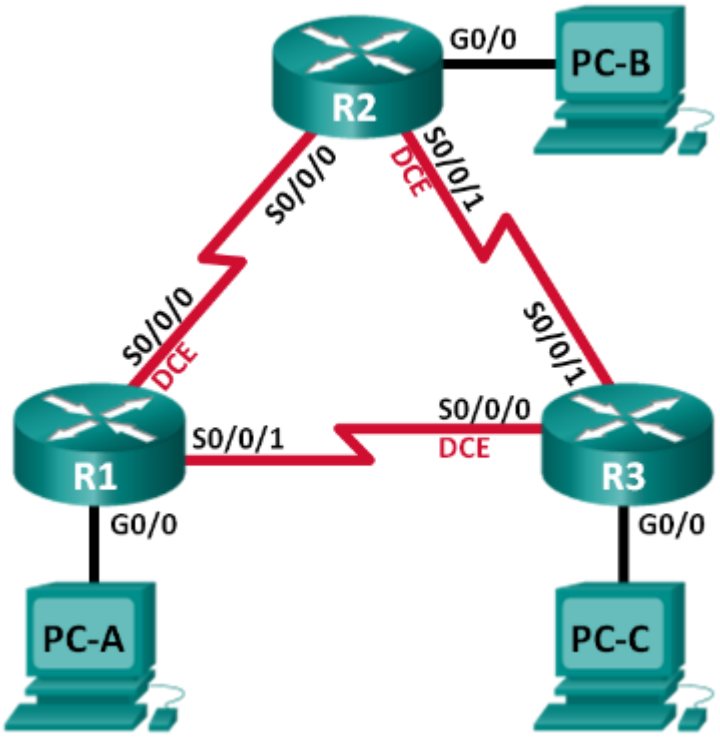


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Gateway predeterminado
R1	G0/0	2001:DB8:ACAD:A::1/64 FE80::1 link-local	No aplicable
	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:13::1/64 FE80::1 link-local	No aplicable
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	No aplicable
	S0/0/1 (DCE)	2001:DB8:ACAD:23::2/64 FE80::2 link-local	No aplicable
R3	G0/0	2001:DB8:ACAD:C::3/64 FE80::3 link-local	No aplicable
	S0/0/0 (DCE)	2001:DB8:ACAD:13::3/64 FE80::3 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	No aplicable
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

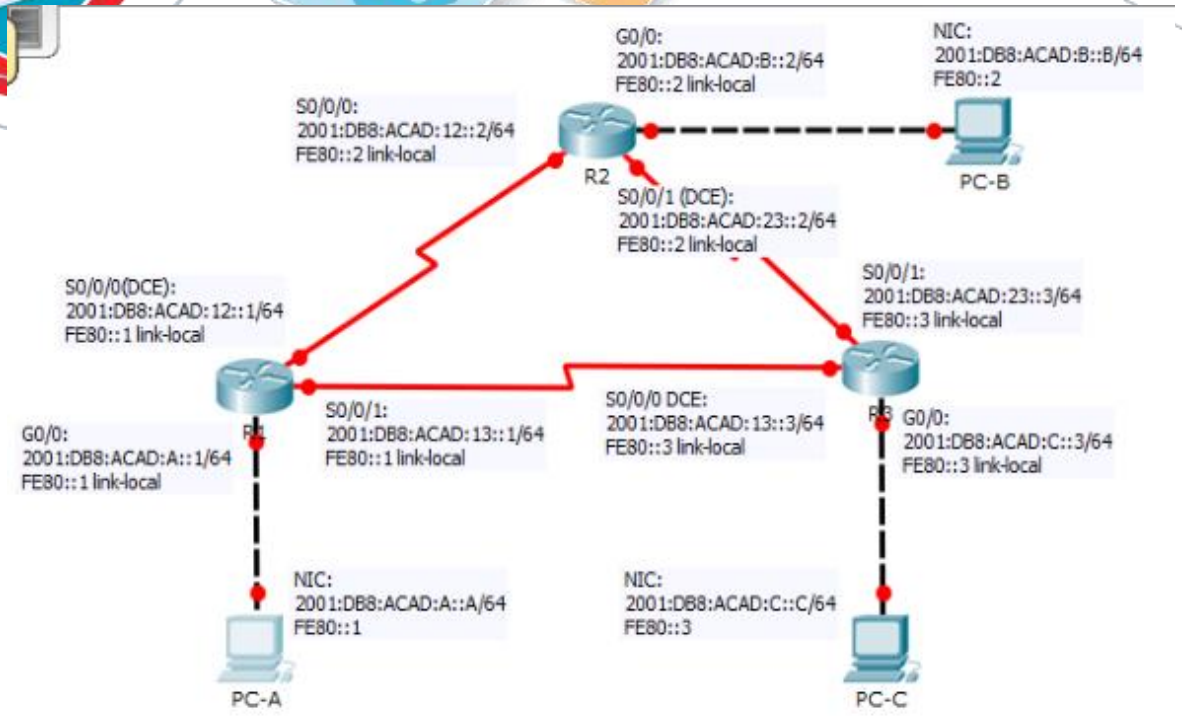
Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal 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

armar la red y configurar los parámetros básicos de los dispositivos

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

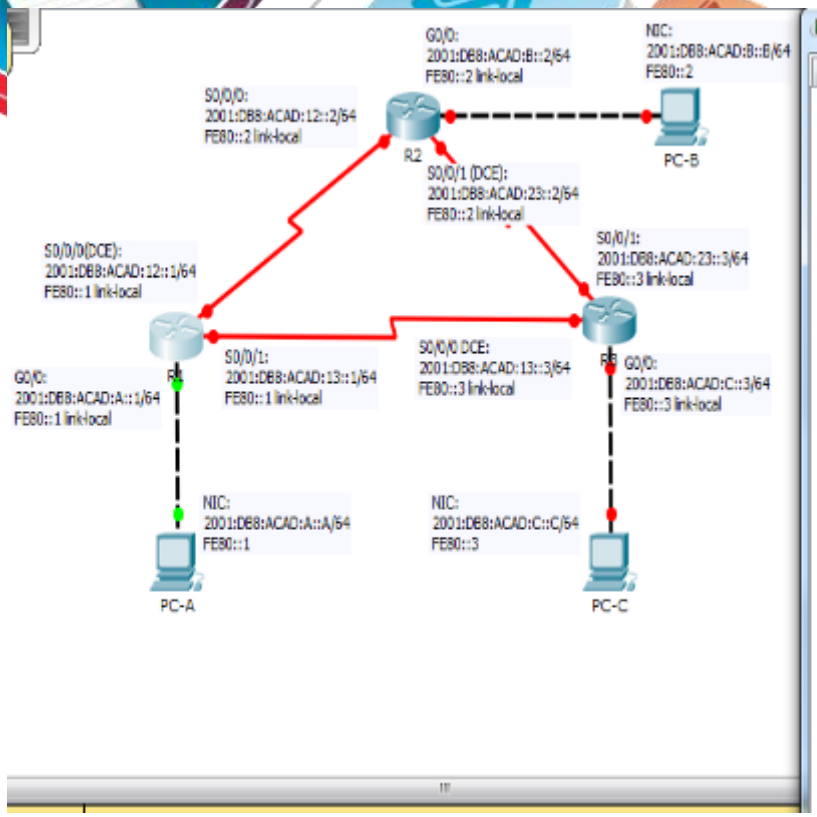
Step 8: realizar el cableado de red tal como se muestra en la topología.

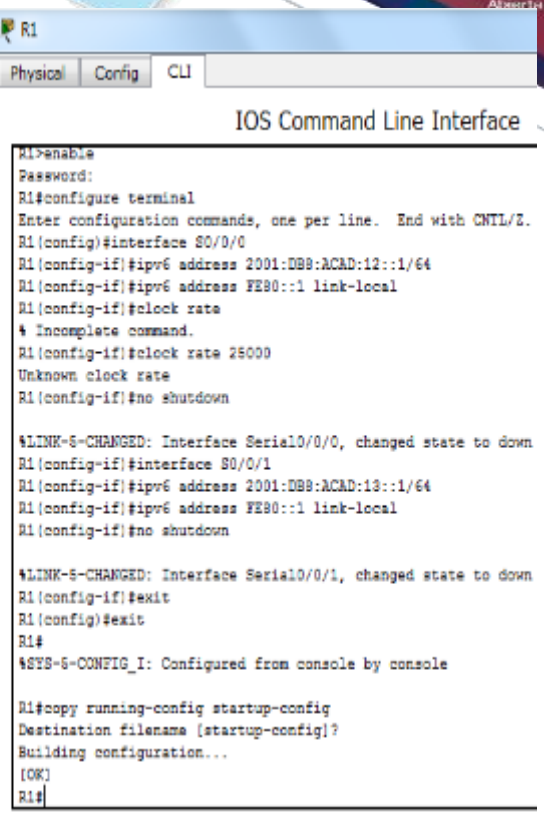


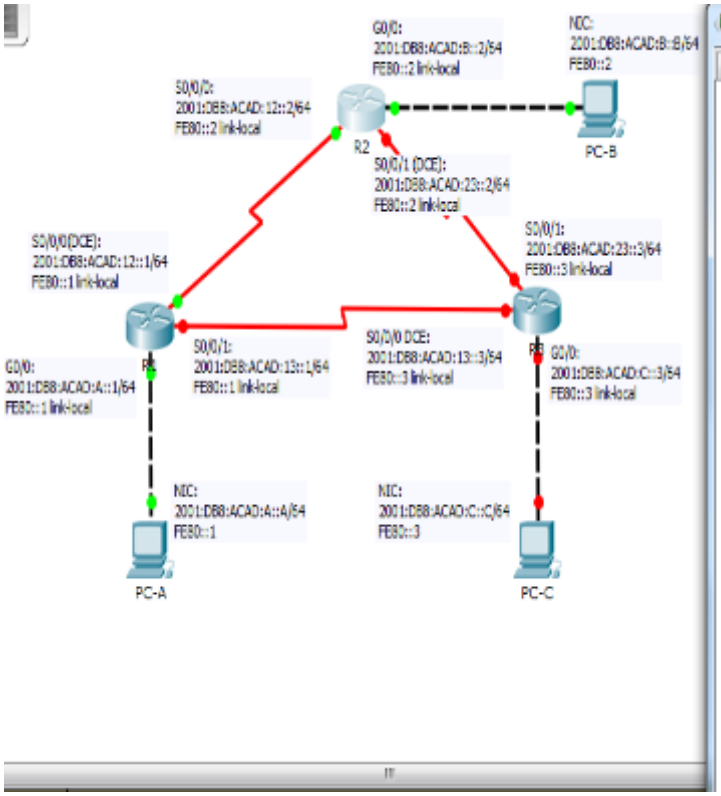
Step 9: inicializar y volver a cargar los routers según sea necesario.

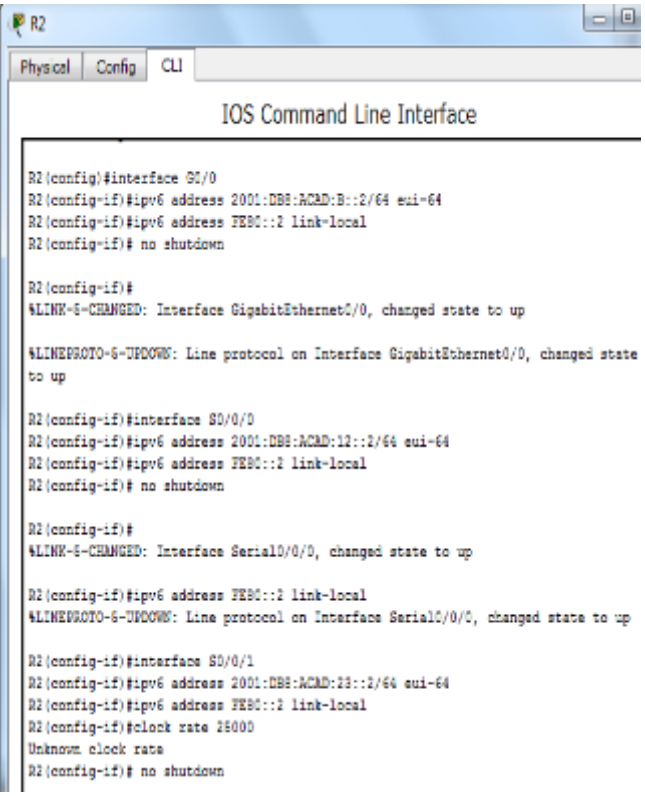
Step 10: configurar los parámetros básicos para cada router.

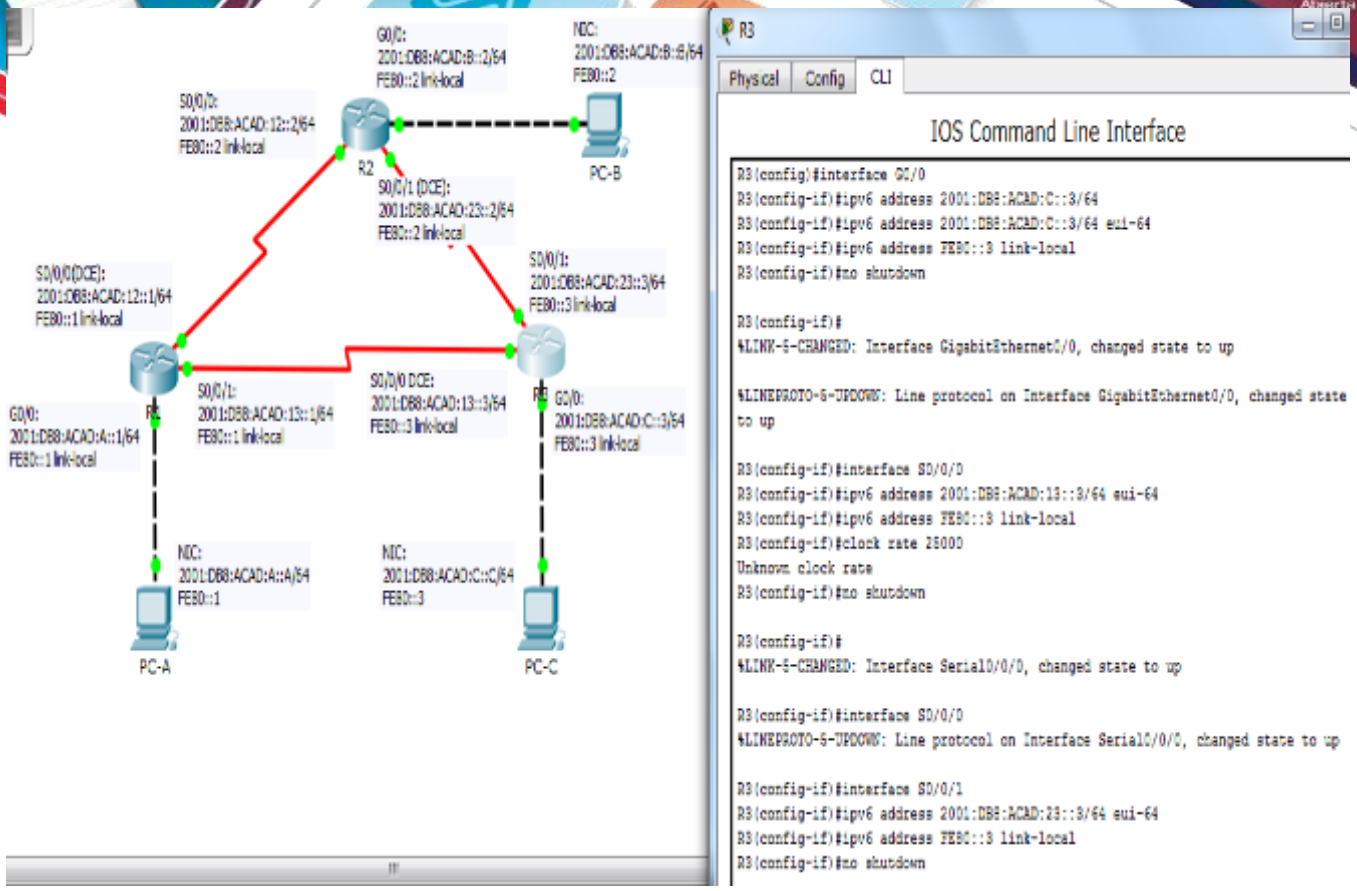
a. Desactive la búsqueda del DNS.
b. Configure el nombre del dispositivo como se muestra en la topología.
c. Asigne **class** como la contraseña del modo EXEC privilegiado.
d. Asigne **cisco** como la contraseña de vty.
e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
f. Configure **logging synchronous** para la línea de consola.
g. Cifre las contraseñas de texto no cifrado.
h. Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.
i. Habilite el routing de unidifusión IPv6 en cada router.
j. Copie la configuración en ejecución en la configuración de inicio


G0/0:
2001:DB8:ACAD:B::2/64
FE80::2 link-local
NIC:
2001:DB8:ACAD:B::B/64
FE80::2
S0/0/0:
2001:DB8:ACAD:12::2/64
FE80::2 link-local
R2
PC-B
S0/0/1 (DCE):
2001:DB8:ACAD:23::2/64
FE80::2 link-local
S0/0/0(DCE):
2001:DB8:ACAD:12::1/64
FE80::1 link-local
S0/0/1:
2001:DB8:ACAD:23::3/64
FE80::3 link-local
S0/0/1:
2001:DB8:ACAD:13::1/64
FE80::1 link-local
S0/0/0 DCE:
2001:DB8:ACAD:13::3/64
FE80::3 link-local
G0/0:
2001:DB8:ACAD:A::1/64
FE80::1 link-local
G0/0:
2001:DB8:ACAD:C::3/64
FE80::3 link-local
NIC:
2001:DB8:ACAD:A::A/64
FE80::1
NIC:
2001:DB8:ACAD:C::C/64
FE80::3
PC-A
PC-C

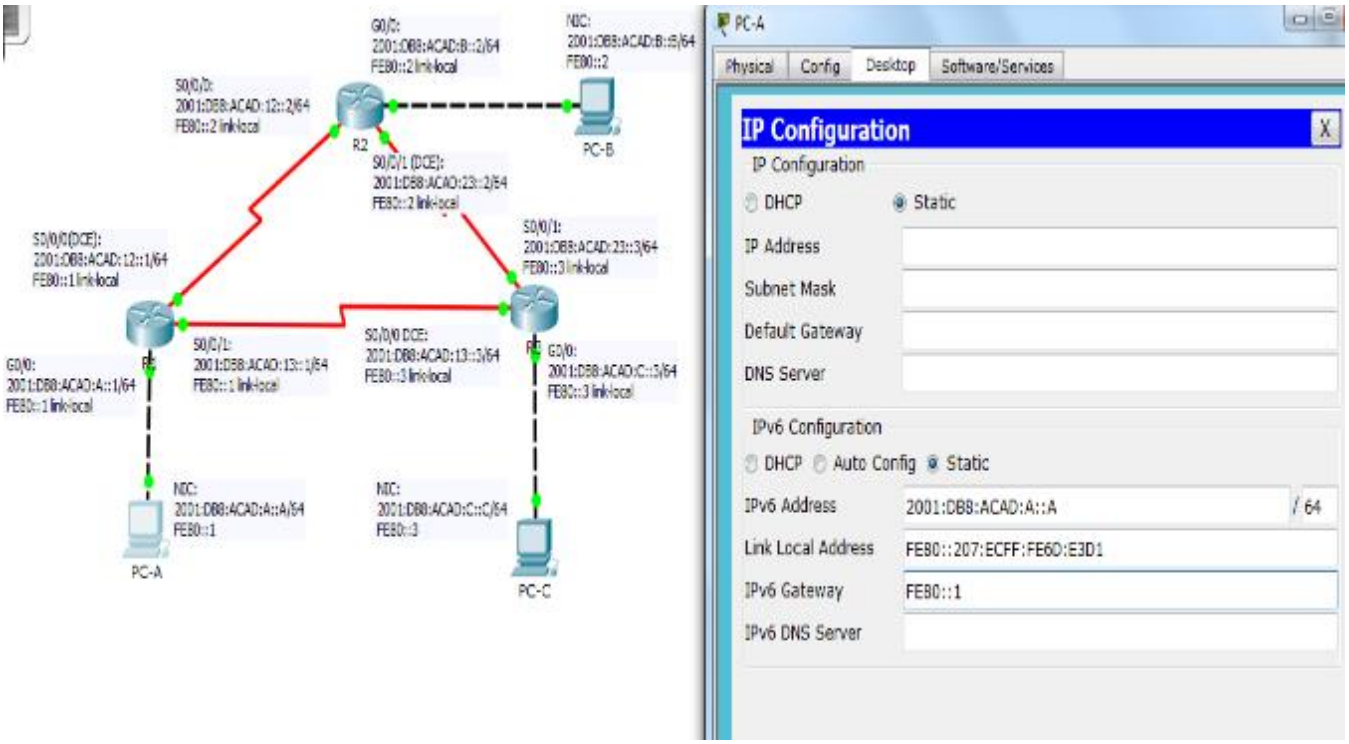

R1
Physical
Config
CLI
IOS Command Line Interface
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface S0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#clock rate
% Incomplete command.
R1(config-if)#clock rate 25000
Unknown clock rate
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#interface S0/0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:13::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

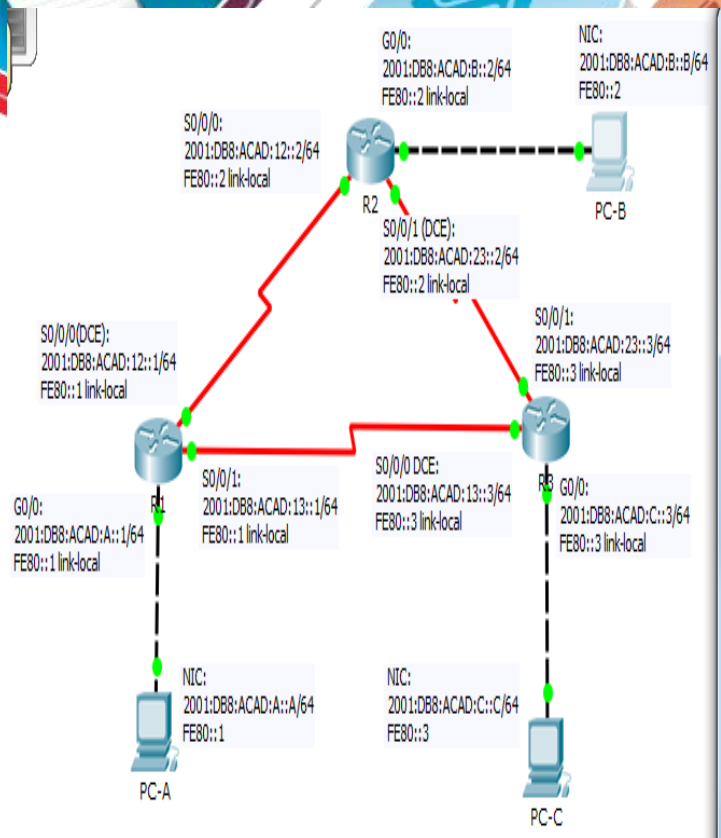

G0/0:
2001:DB8:ACAD:B::2/64
FE80::2 link-local
NIC:
2001:DB8:ACAD:B::B/64
FE80::2
S0/0/0:
2001:DB8:ACAD:12::2/64
FE80::2 link-local
R2
PC-B
S0/0/1 (DCE):
2001:DB8:ACAD:23::2/64
FE80::2 link-local
S0/0/0(DCE):
2001:DB8:ACAD:12::1/64
FE80::1 link-local
S0/0/1:
2001:DB8:ACAD:23::3/64
FE80::3 link-local
S0/0/1:
2001:DB8:ACAD:13::1/64
FE80::1 link-local
S0/0/0 DCE:
2001:DB8:ACAD:13::3/64
FE80::3 link-local
G0/0:
2001:DB8:ACAD:A::1/64
FE80::1 link-local
G0/0:
2001:DB8:ACAD:C::3/64
FE80::3 link-local
NIC:
2001:DB8:ACAD:A::A/64
FE80::1
NIC:
2001:DB8:ACAD:C::C/64
FE80::3
PC-A
PC-C

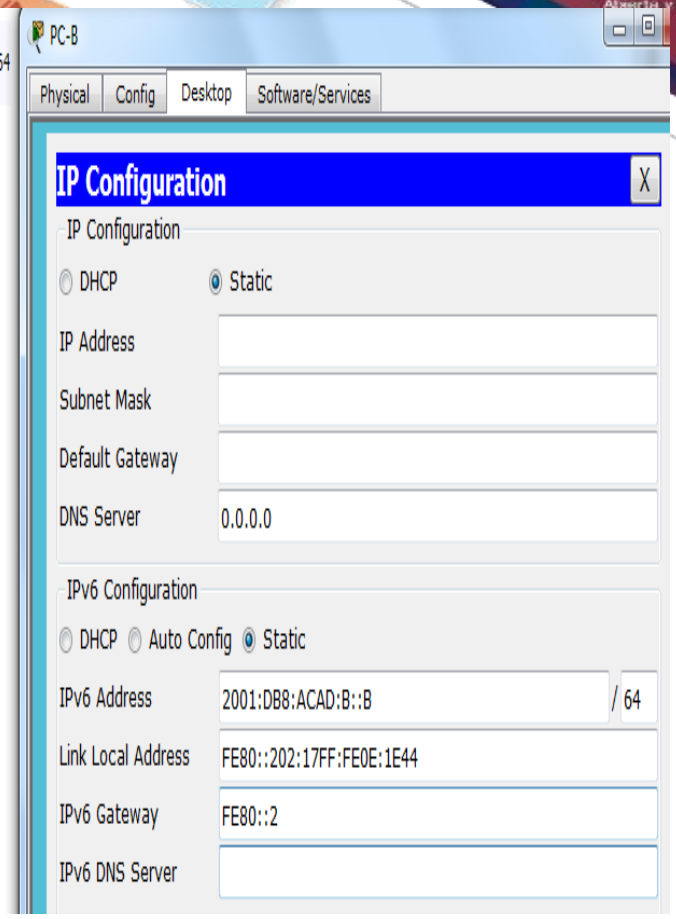

R2
Physical
Config
CLI
IOS Command Line Interface
R2(config)#interface G0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64 eui-64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)# no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#interface S0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64 eui-64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)# no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#ipv6 address FE80::2 link-local
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config-if)#interface S0/0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64 eui-64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#clock rate 25000
Unknown clock rate
R2(config-if)# no shutdown

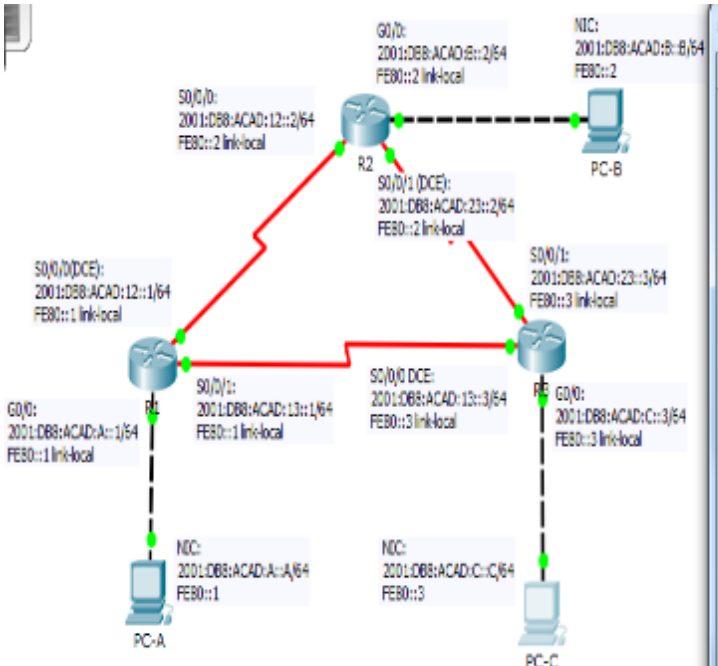


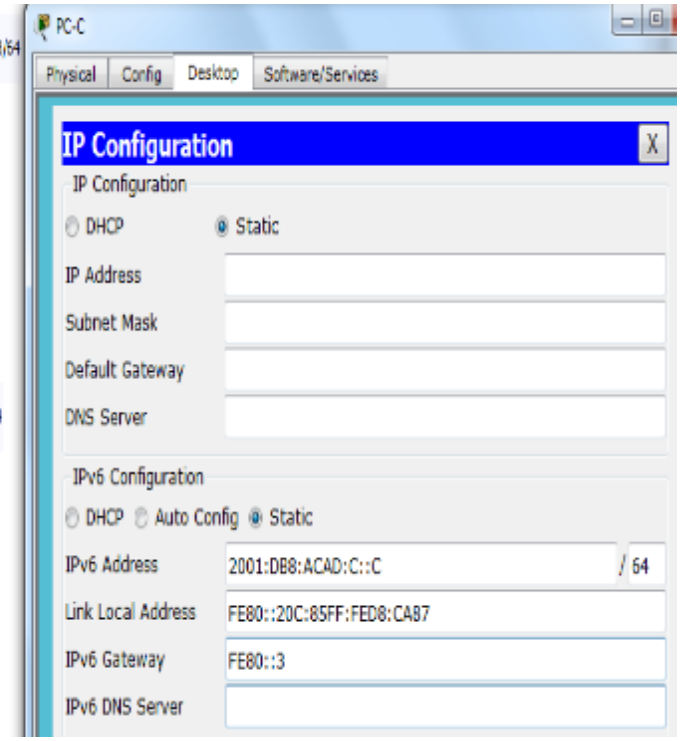
Step 11: configurar los equipos host.




G0/0:
2001:DB8:ACAD:B::2/64
FE80::2 link-local
NIC:
2001:DB8:ACAD:B::B/64
FE80::2
S0/0/0:
2001:DB8:ACAD:12::2/64
FE80::2 link-local
R2
PC-B
S0/0/1 (DCE):
2001:DB8:ACAD:23::2/64
FE80::2 link-local
S0/0/0(DCE):
2001:DB8:ACAD:12::1/64
FE80::1 link-local
S0/0/1:
2001:DB8:ACAD:23::3/64
FE80::3 link-local
S0/0/1:
2001:DB8:ACAD:13::1/64
FE80::1 link-local
S0/0/0 DCE:
2001:DB8:ACAD:13::3/64
FE80::3 link-local
G0/0:
2001:DB8:ACAD:A::1/64
FE80::1 link-local
G0/0:
2001:DB8:ACAD:C::3/64
FE80::3 link-local
NIC:
2001:DB8:ACAD:A::A/64
FE80::1
NIC:
2001:DB8:ACAD:C::C/64
FE80::3
PC-A
PC-C

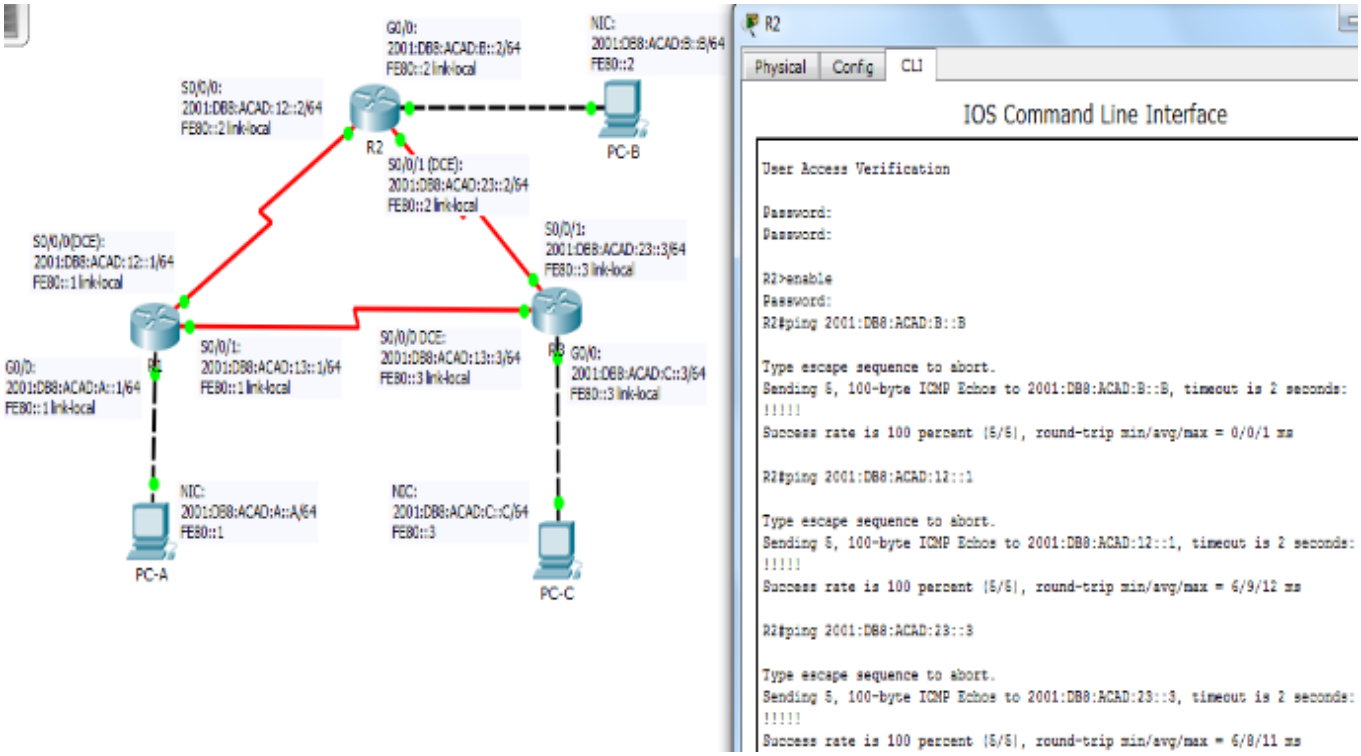

PC-B
Physical
Config
Desktop
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
Subnet Mask
Default Gateway
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:ACAD:B::B
/ 64
Link Local Address
FE80::202:17FF:FE0E:1E44
IPv6 Gateway
FE80::2
IPv6 DNS Server


G0/0:
2001:DB8:ACAD:B::2/64
FE80::2 link-local
NIC:
2001:DB8:ACAD:B::B/64
FE80::2
S0/0/0:
2001:DB8:ACAD:12::2/64
FE80::2 link-local
R2
PC-B
S0/0/1 (DCE):
2001:DB8:ACAD:23::2/64
FE80::2 link-local
S0/0/0(DCE):
2001:DB8:ACAD:12::1/64
FE80::1 link-local
S0/0/1:
2001:DB8:ACAD:23::3/64
FE80::3 link-local
S0/0/1:
2001:DB8:ACAD:13::1/64
FE80::1 link-local
S0/0/0 DCE:
2001:DB8:ACAD:13::3/64
FE80::3 link-local
G0/0:
2001:DB8:ACAD:A::1/64
FE80::1 link-local
G0/0:
2001:DB8:ACAD:C::3/64
FE80::3 link-local
NIC:
2001:DB8:ACAD:A::A/64
FE80::1
NIC:
2001:DB8:ACAD:C::C/64
FE80::3
PC-A
PC-C


PC-C
Physical
Config
Desktop
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
Subnet Mask
Default Gateway
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:ACAD:C::C
/ 64
Link Local Address
FE80::20C:85FF:FED8:CA87
IPv6 Gateway
FE80::3
IPv6 DNS Server

Step 12: Probar la conectividad.

Los routers deben poder hacerse ping entre sí, y cada computadora debe poder hacer ping a su gateway predeterminado. Las computadoras no pueden hacer ping a otras computadoras hasta que no se haya configurado el routing OSPFv3. Verifique y resuelva los problemas, si es necesario.



configurar el routing OSPFv3

En la parte 2, configurará el routing OSPFv3 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente.

Step 13: asignar ID a los routers.

OSPFv3 sigue utilizando una dirección de 32 bits para la ID del router. Debido a que no hay direcciones IPv4 configuradas en los routers, asigne manualmente la ID del router mediante el comando **router-id**.

a. Emita el comando **ipv6 router ospf** para iniciar un proceso OSPFv3 en el router.

```
R1(config)# ipv6 router ospf 1
```

Nota: la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

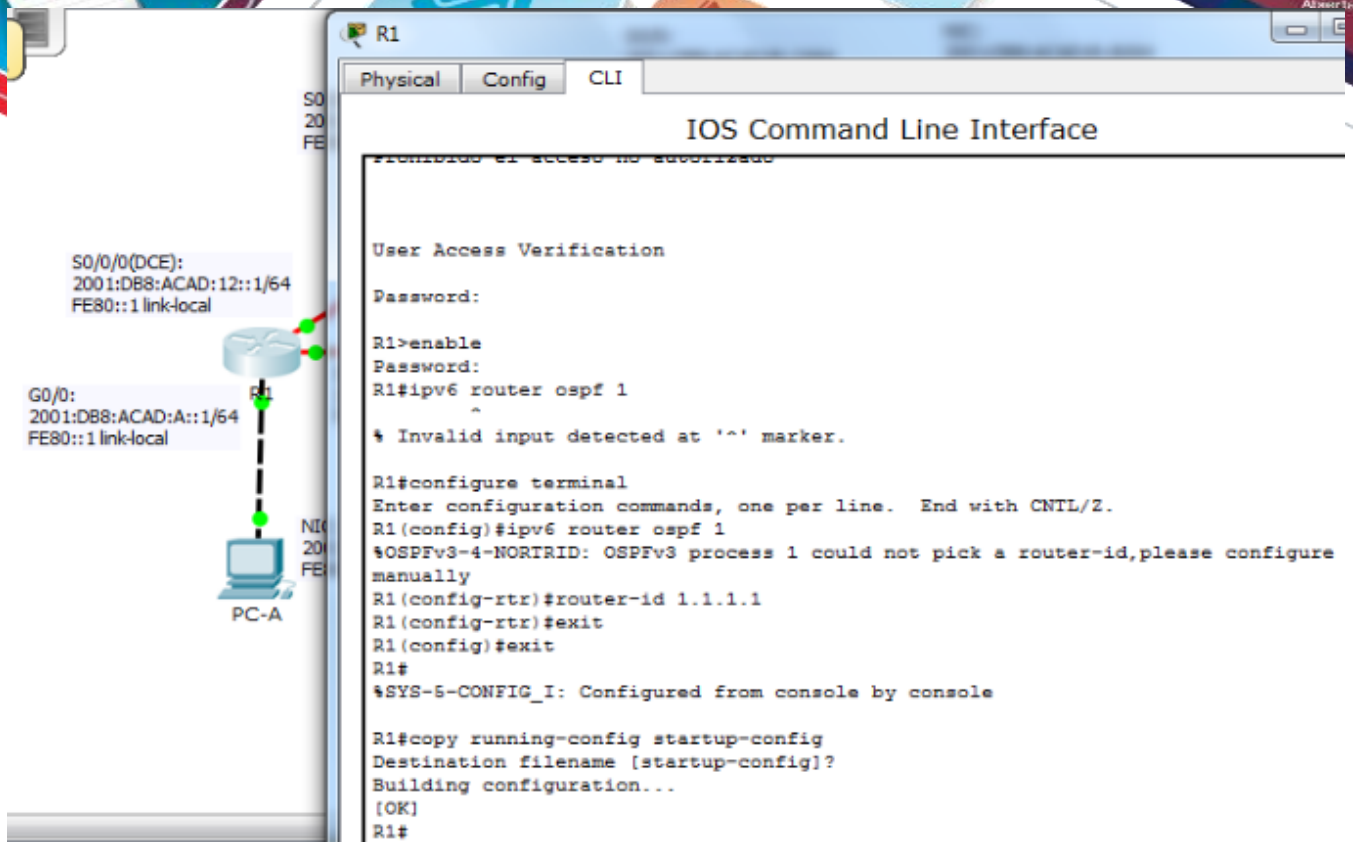
b. Asigne la ID de router OSPFv3 **1.1.1.1** al R1.

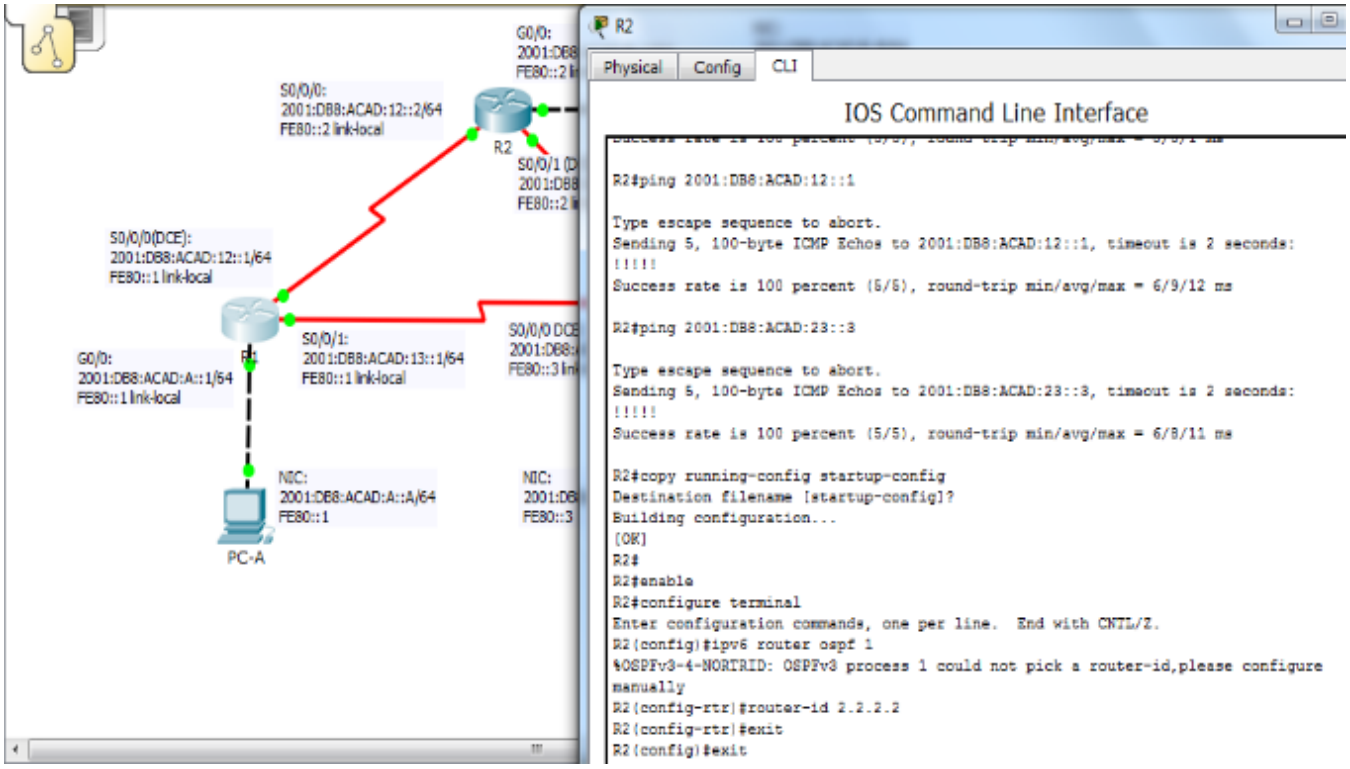
```
R1(config-rtr)# router-id 1.1.1.1
```

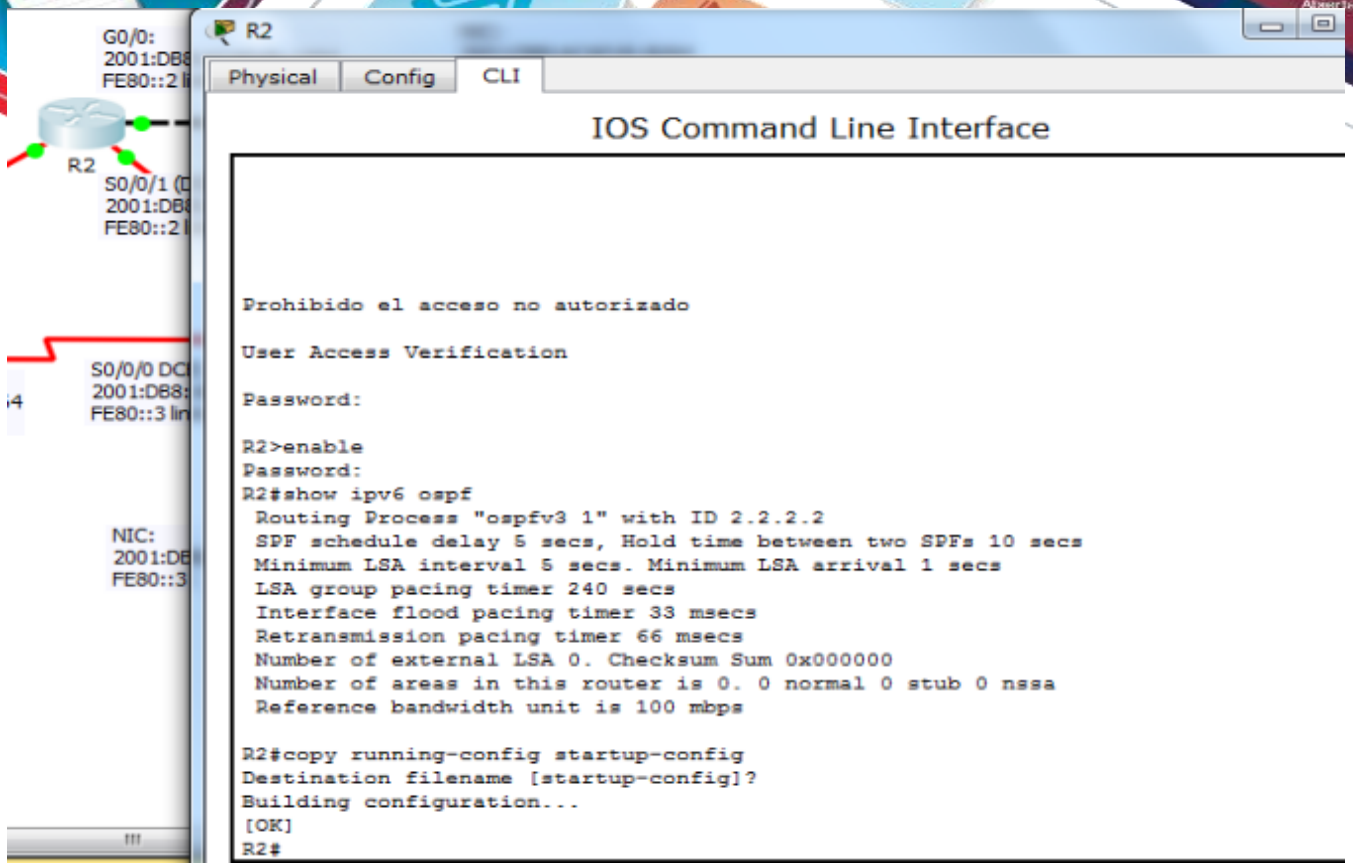
c. Inicie el proceso de routing de OSPFv3 y asigne la ID de router **2.2.2.2** al R2 y la ID de router **3.3.3.3** al R3.

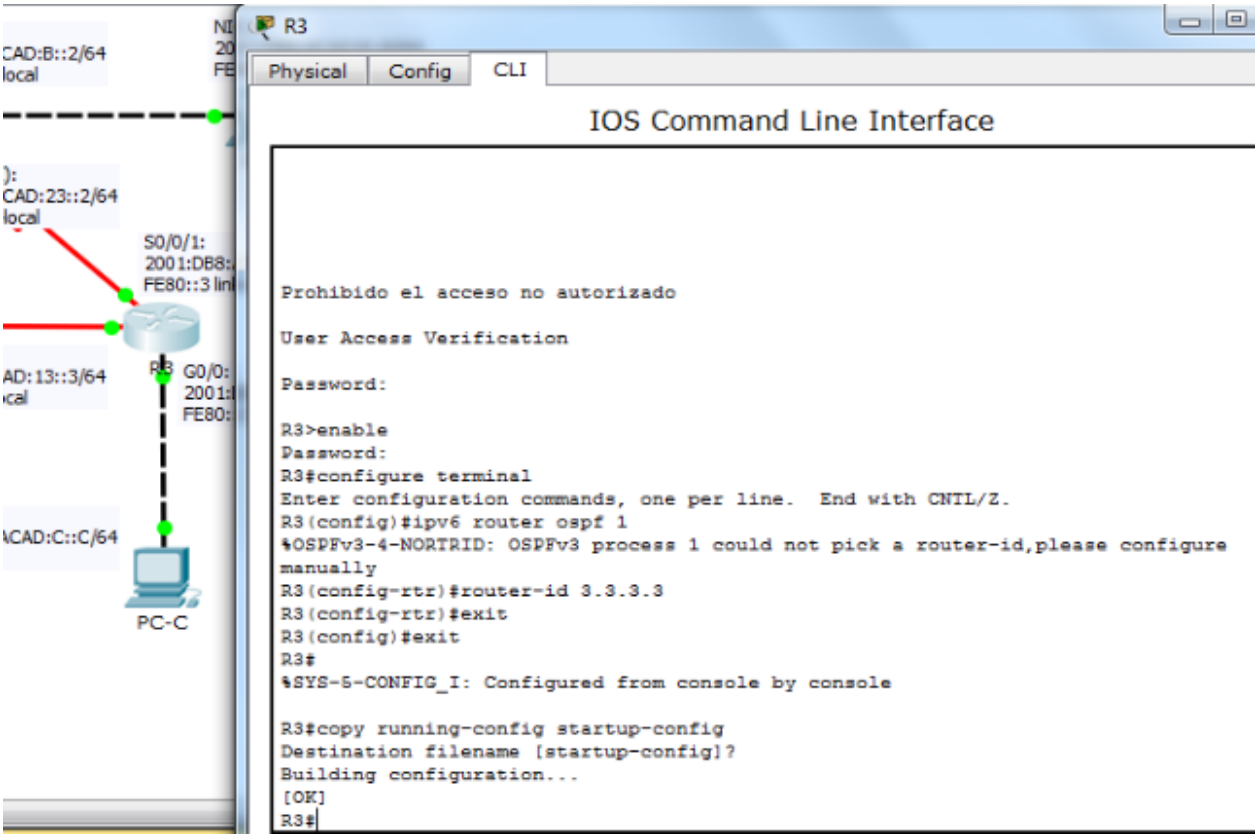
d. Emita el comando **show ipv6 ospf** para verificar las ID de router de todos los routers.

```
R2# show ipv6 ospf
 Routing Process "ospfv3 1" with ID 2.2.2.2
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 <Output Omitted>
```


R1
Physical
Config
CLI
IOS Command Line Interface
S0/0/0(DCE):
2001:DB8:ACAD:12::1/64
FE80::1 link-local
G0/0:
2001:DB8:ACAD:A::1/64
FE80::1 link-local
PC-A
User Access Verification
Password:
R1>enable
Password:
R1#ipv6 router ospf 1
% Invalid input detected at '^' marker.
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#


R2
Physical
Config
CLI
IOS Command Line Interface
S0/0/0:
2001:DB8:ACAD:12::2/64
FE80::2 link-local
S0/0/0(DCE):
2001:DB8:ACAD:12::1/64
FE80::1 link-local
S0/0/1:
2001:DB8:ACAD:13::1/64
FE80::1 link-local
G0/0:
2001:DB8:ACAD:A::1/64
FE80::1 link-local
NIC:
2001:DB8:ACAD:A::A/64
FE80::1
PC-A
R2#ping 2001:DB8:ACAD:12::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/12 ms
R2#ping 2001:DB8:ACAD:23::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/8/11 ms
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
R2#enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#exit
R2(config)#exit

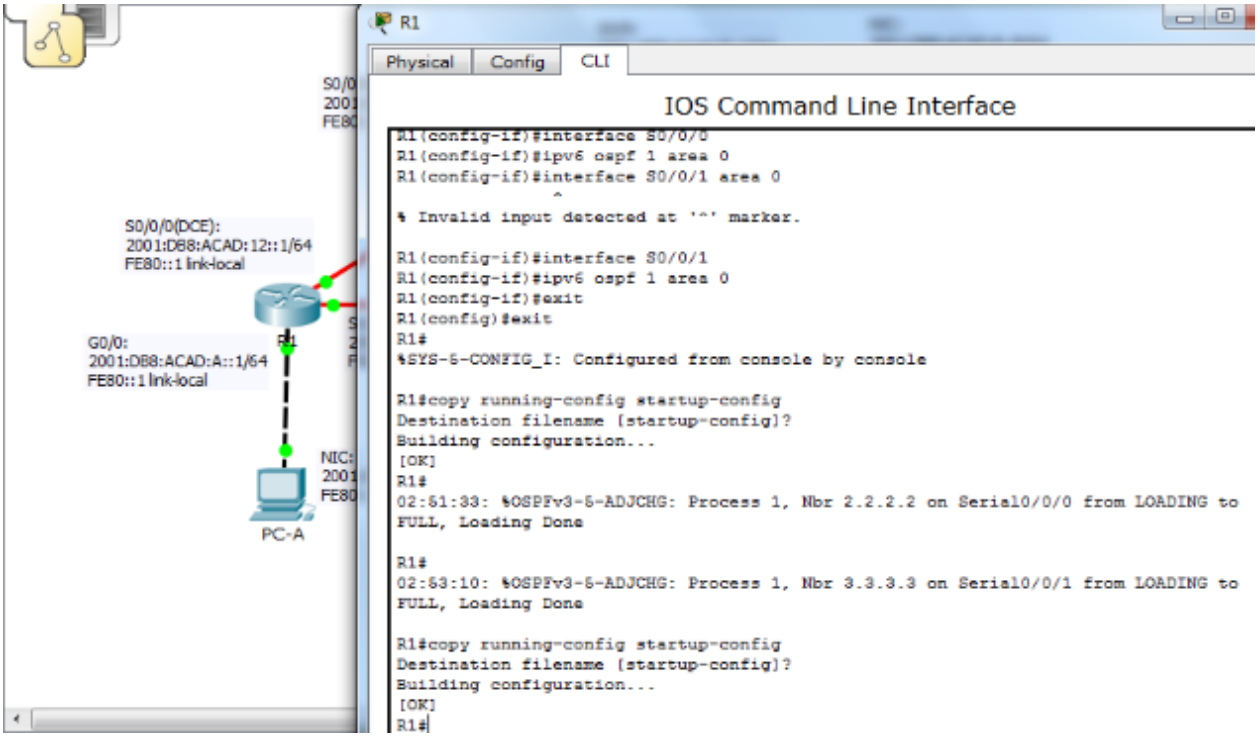

R2
Physical
Config
CLI
IOS Command Line Interface
Prohibido el acceso no autorizado
User Access Verification
Password:
R2>enable
Password:
R2#show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

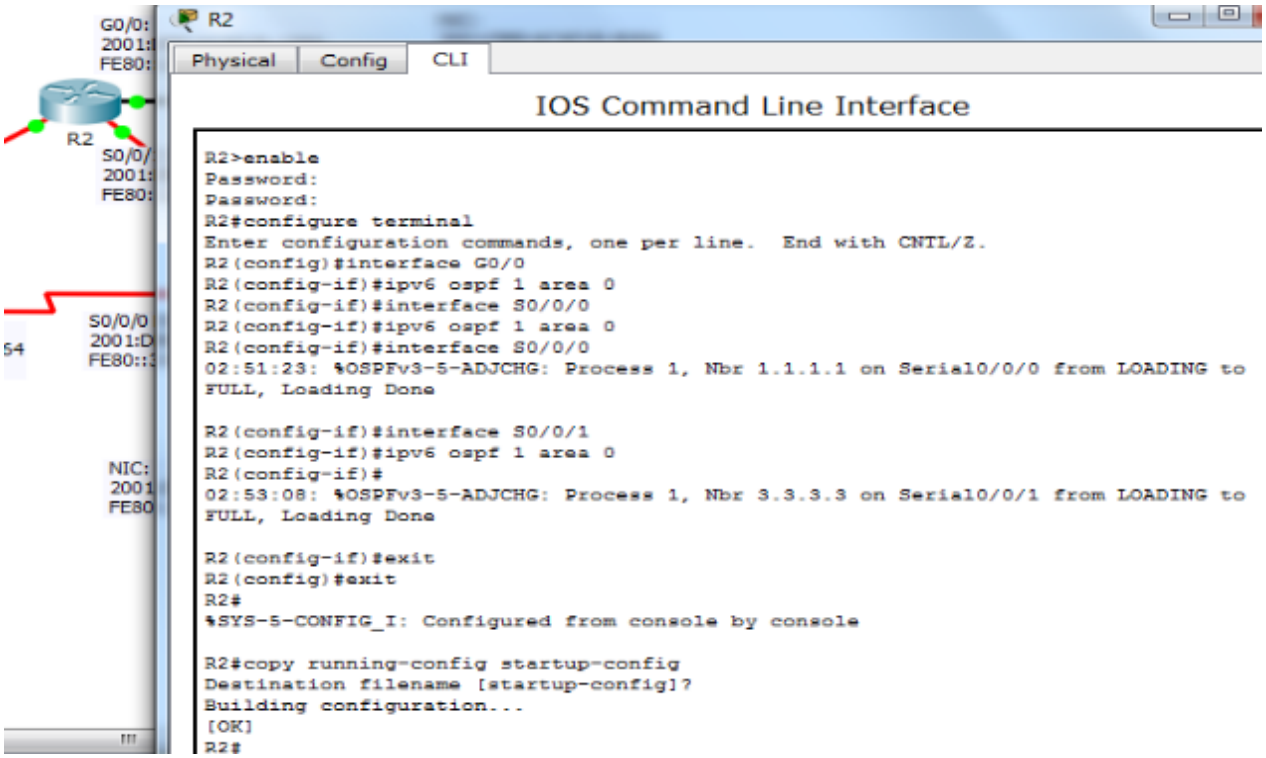

R3
Physical
Config
CLI
IOS Command Line Interface
PC-C
Prohibido el acceso no autorizado
User Access Verification
Password:
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure
manually
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#

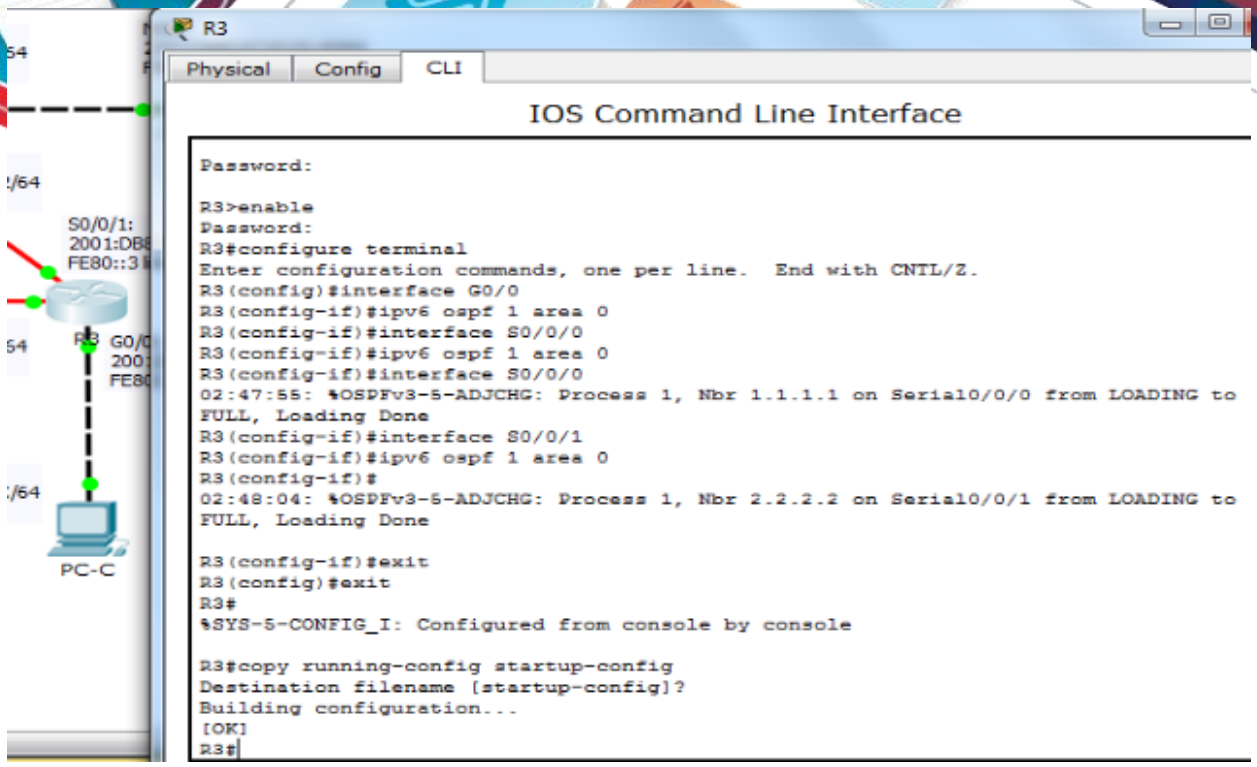
Step 14: configurar OSPFv6 en el R1.

Con IPv6, es común tener varias direcciones IPv6 configuradas en una interfaz. La instrucción network se eliminó en OSPFv3. En cambio, el routing OSPFv3 se habilita en el nivel de la interfaz.

a. Emita el comando **ipv6 ospf 1 area 0** para cada interfaz en el R1 que participará en el routing OSPFv3.

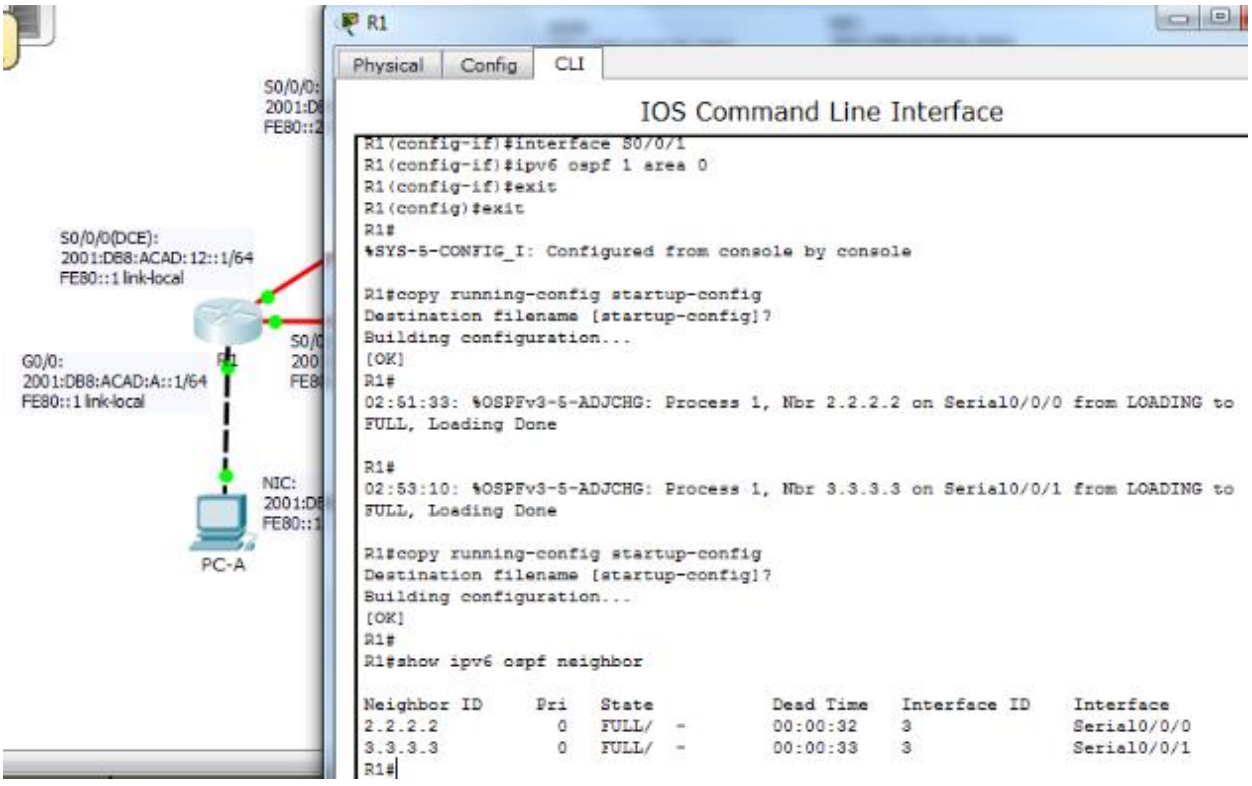






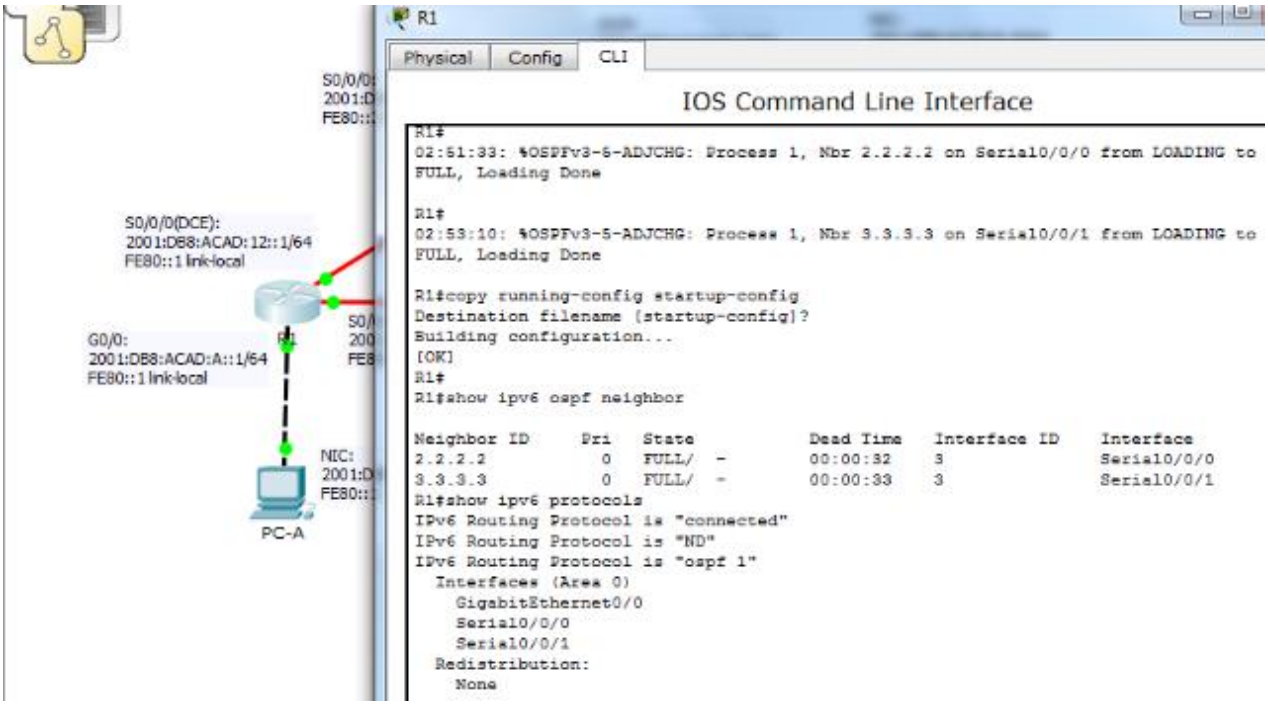
Step 15: verificar vecinos de OSPFv3.

Emita el comando **show ipv6 ospf neighbor** para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.



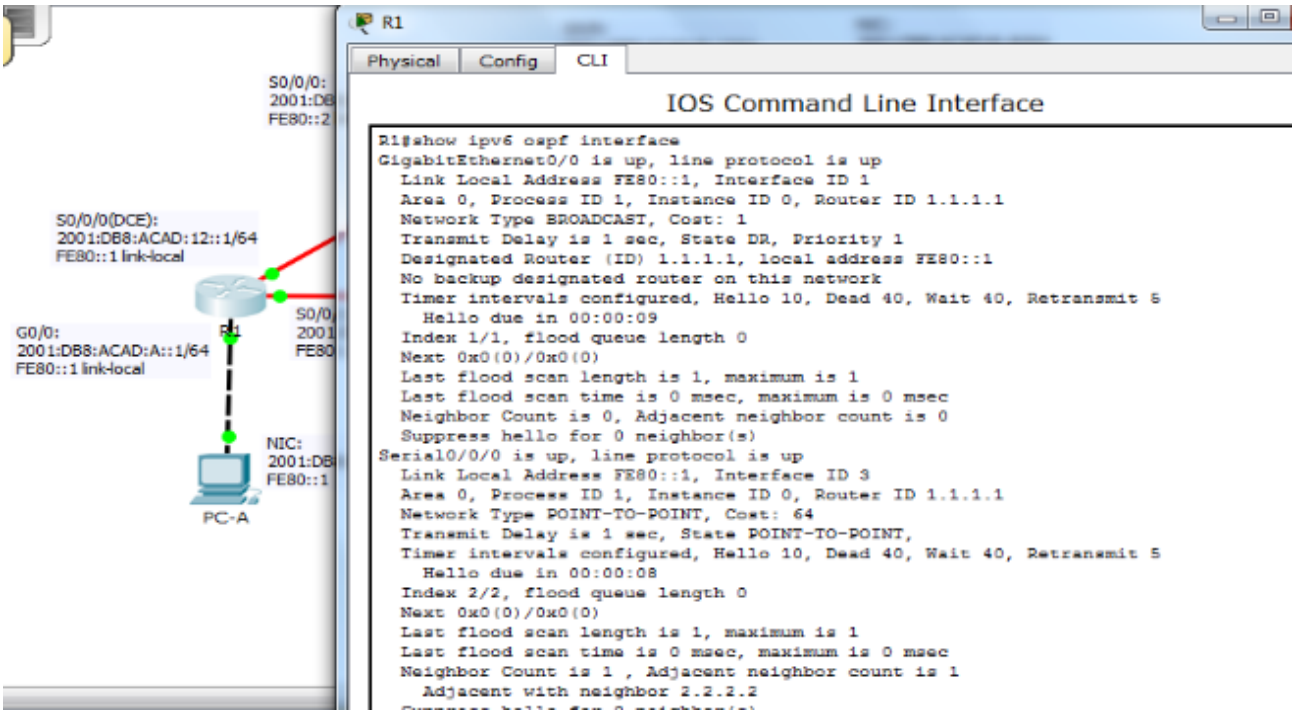
Step 16: verificar la configuración del protocolo OSPFv3.

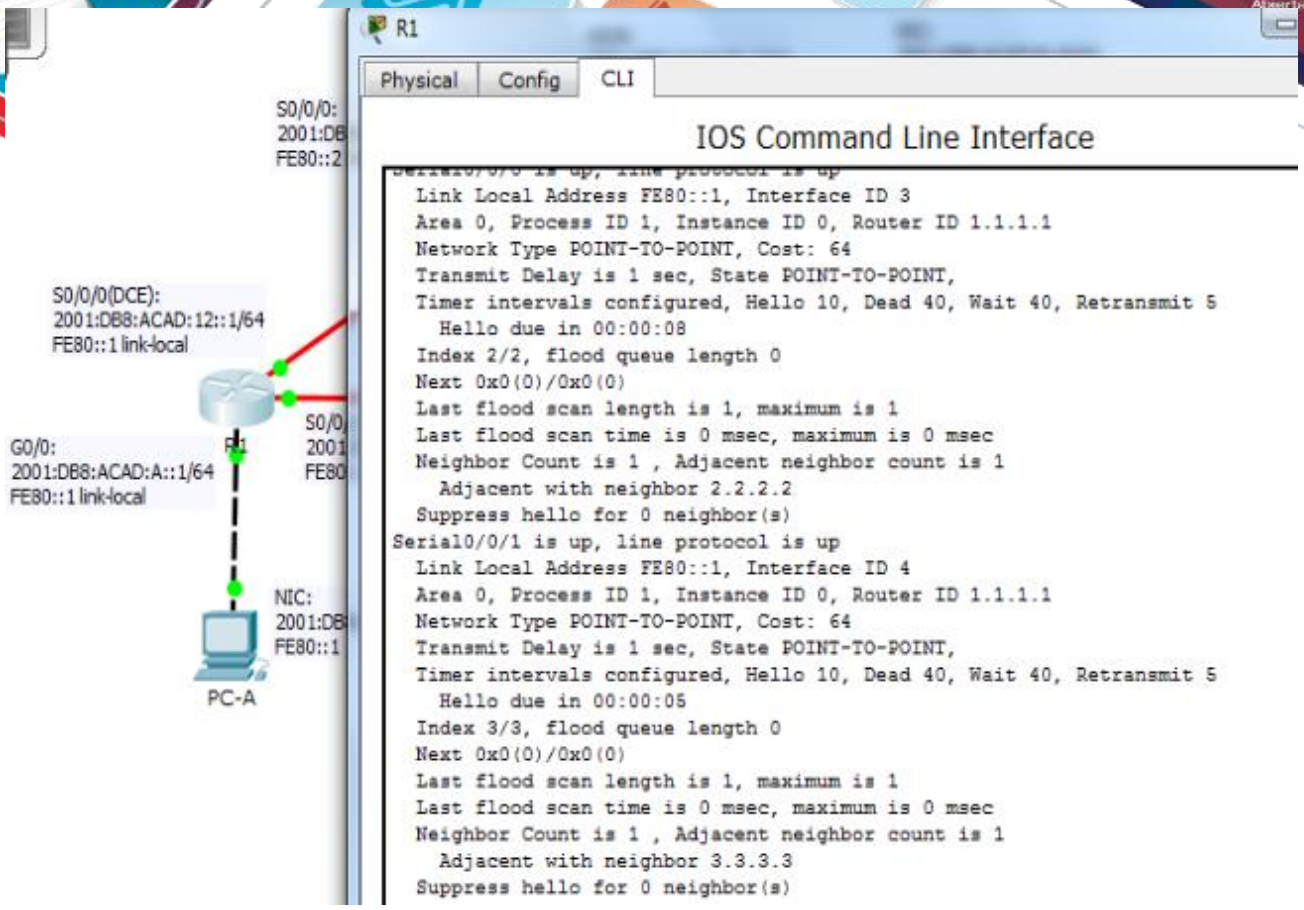
El comando **show ipv6 protocols** es una manera rápida de verificar información fundamental de configuración de OSPFv3, incluidas la ID del proceso OSPF, la ID del router y las interfaces habilitadas para OSPFv3.



Step 17: verificar las interfaces OSPFv3.

a. Emita el comando **show ipv6 ospf interface** para mostrar una lista detallada de cada interfaz habilitada para OSPF.



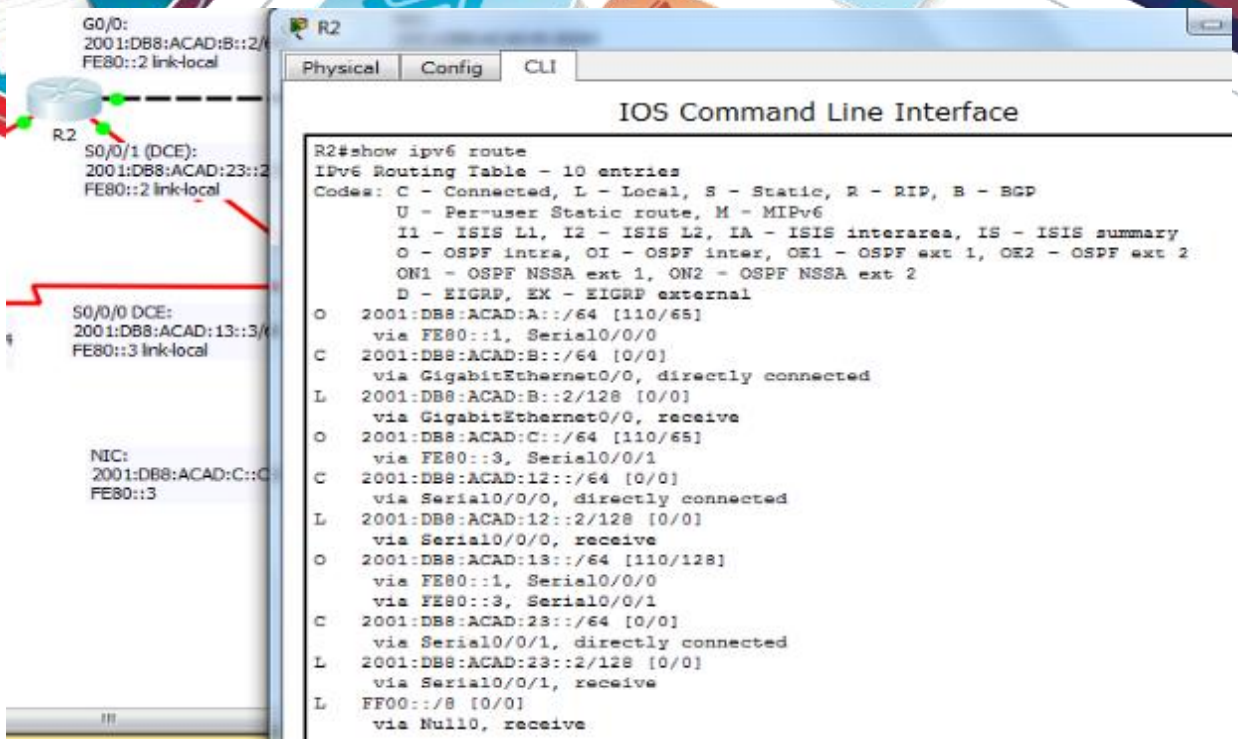


b. Para mostrar un resumen de las interfaces con OSPFv3 habilitado, emita el comando **show ipv6 ospf interface brief**.

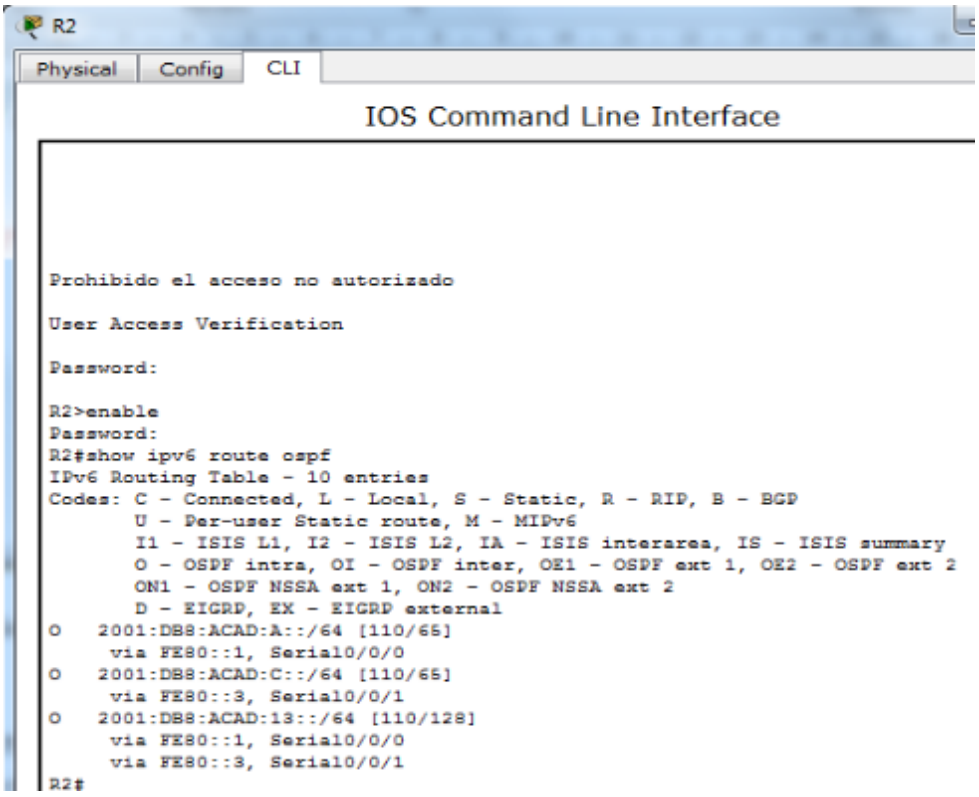
```
R1# show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Se0/0/1      1     0               7          64    P2P   1/1
Se0/0/0      1     0               6          64    P2P   1/1
Gi0/0        1     0               3          1     DR    0/0
```

Step 18: verificar la tabla de routing IPv6.

Emita el comando **show ipv6 route** para verificar que todas las redes aparezcan en la tabla de routing.



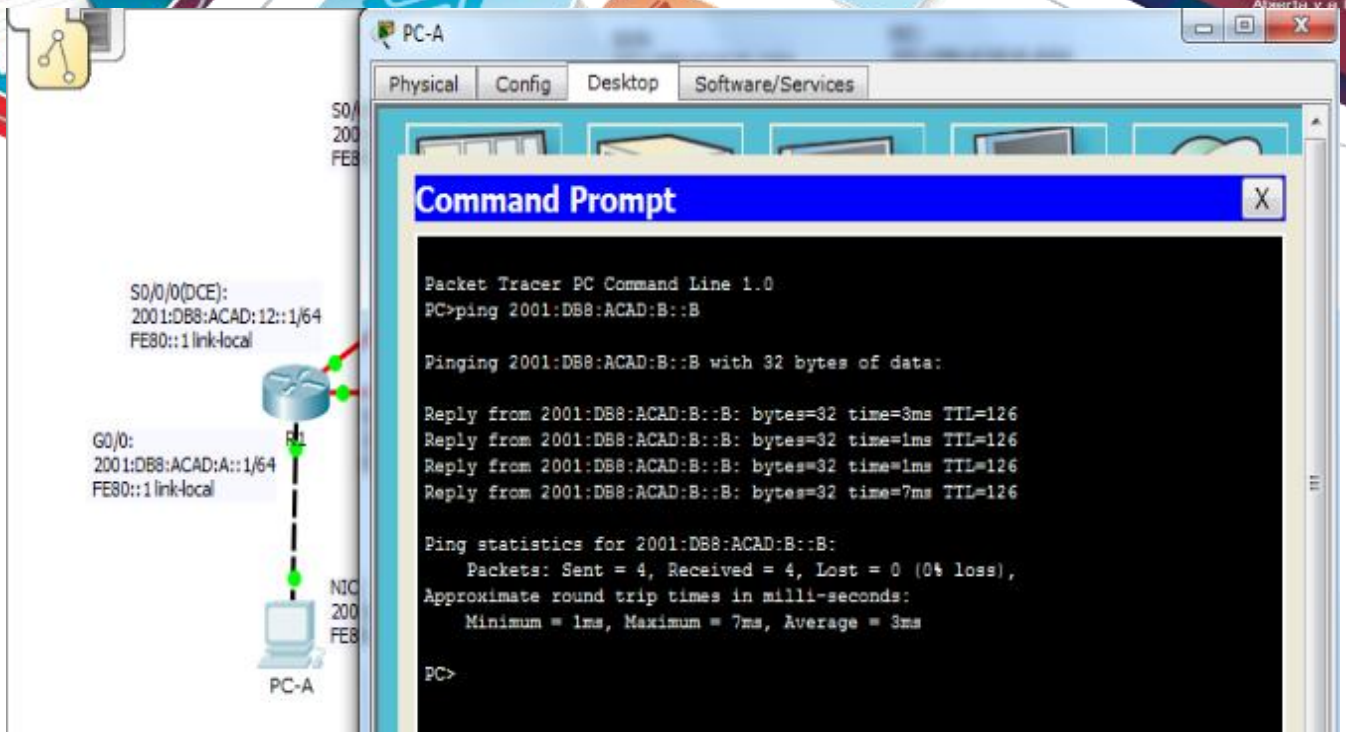
¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing? Show ipv6 route ospf

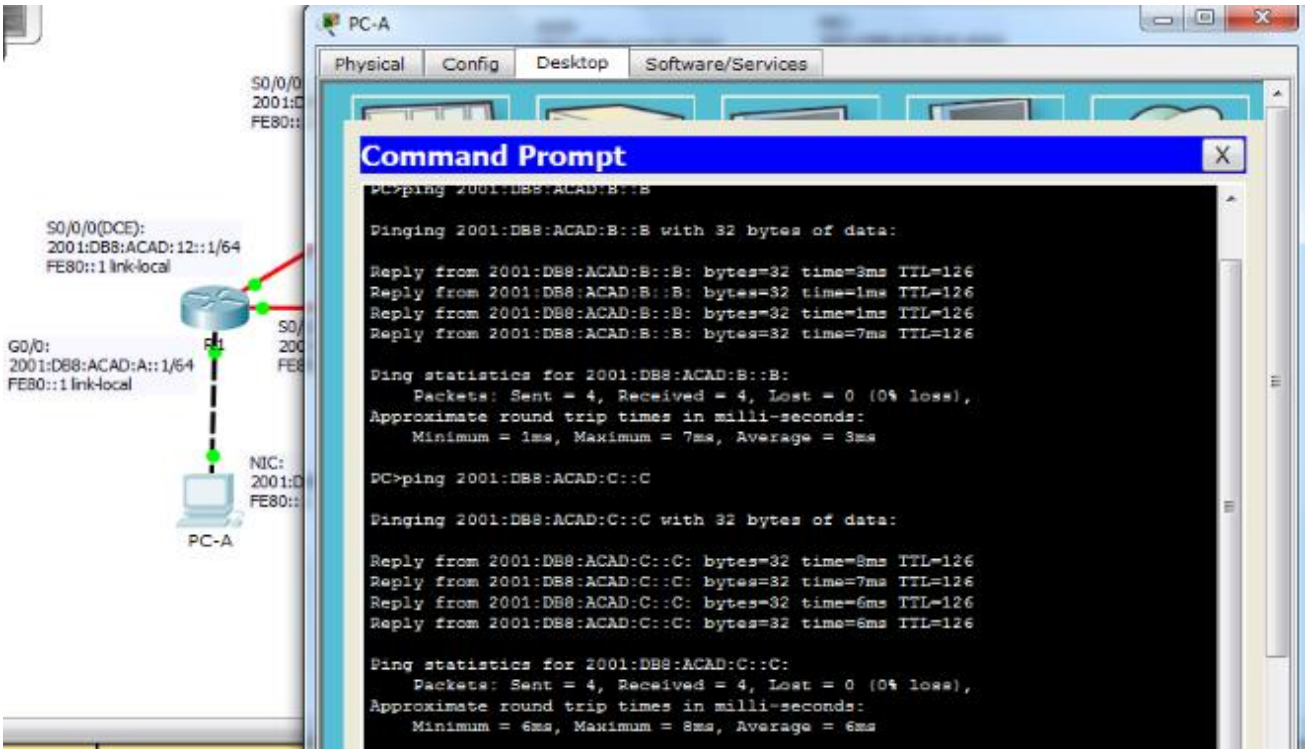


Step 19: Verificar la conectividad de extremo a extremo.

Se debería poder hacer ping entre todas las computadoras de la topología. Verifique y resuelva los problemas, si es necesario.

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

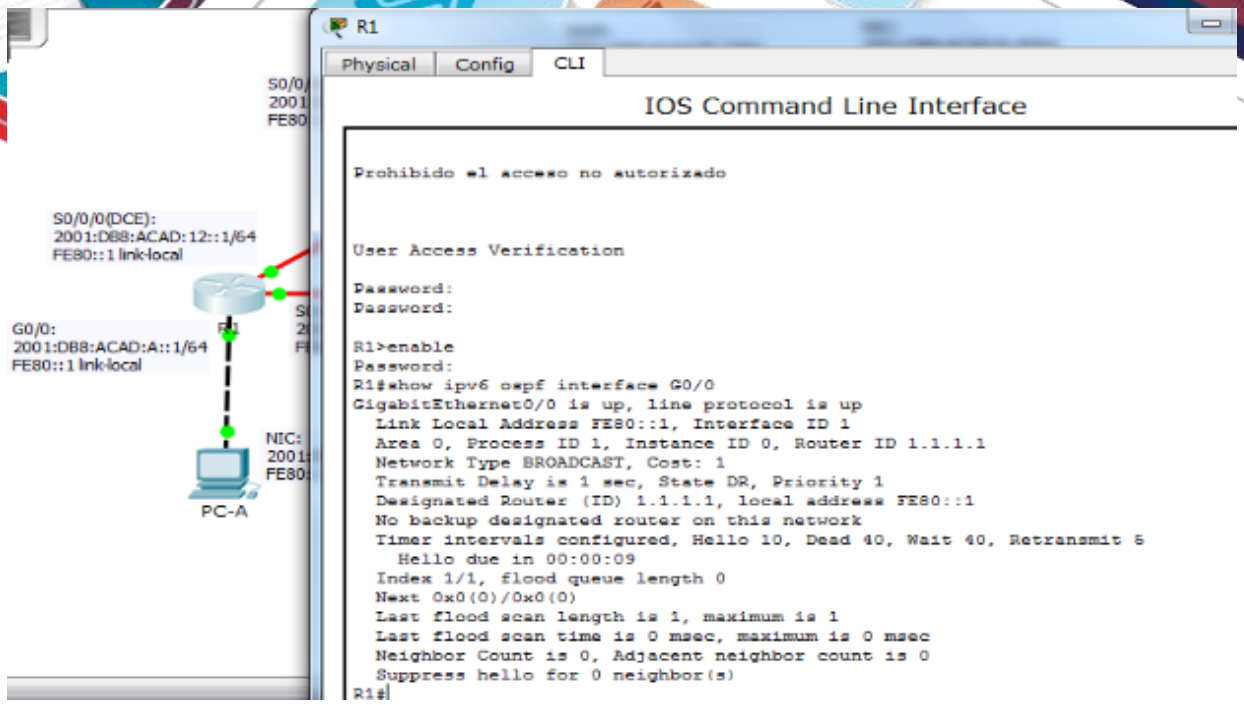




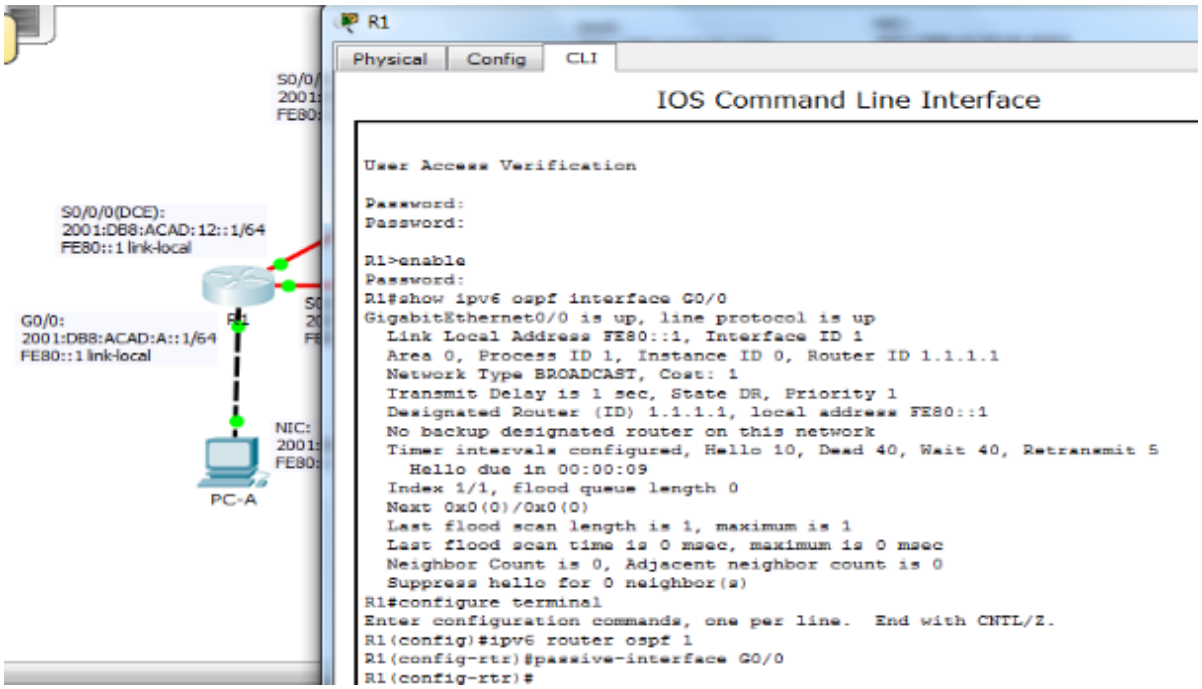
configurar las interfaces pasivas de OSPFv3

Step 20: configurar una interfaz pasiva.

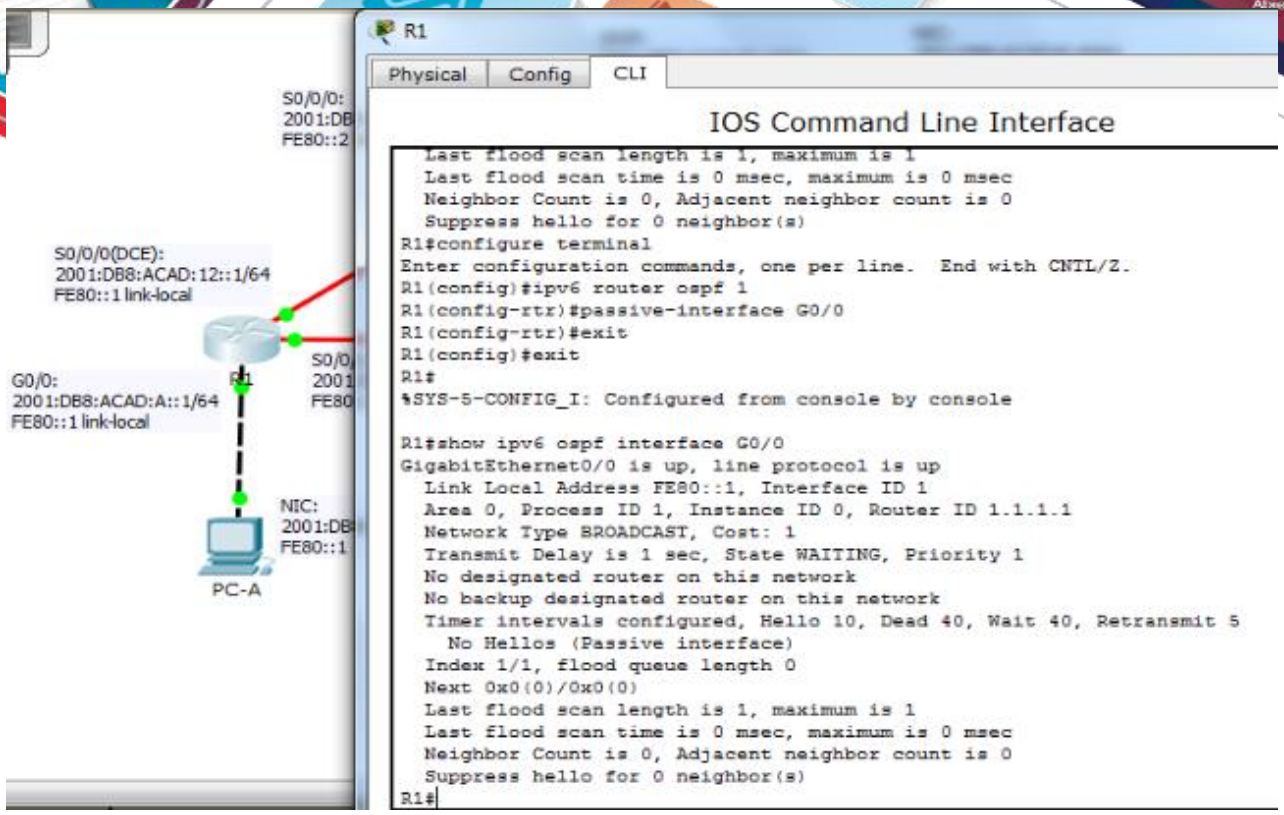
a. Emita el comando **show ipv6 ospf interface g0/0** en el R1. Observe el temporizador que indica cuándo se espera el siguiente paquete de saludo. Los paquetes de saludo se envían cada 10 segundos y se utilizan entre los routers OSPF para verificar que sus vecinos estén activos.



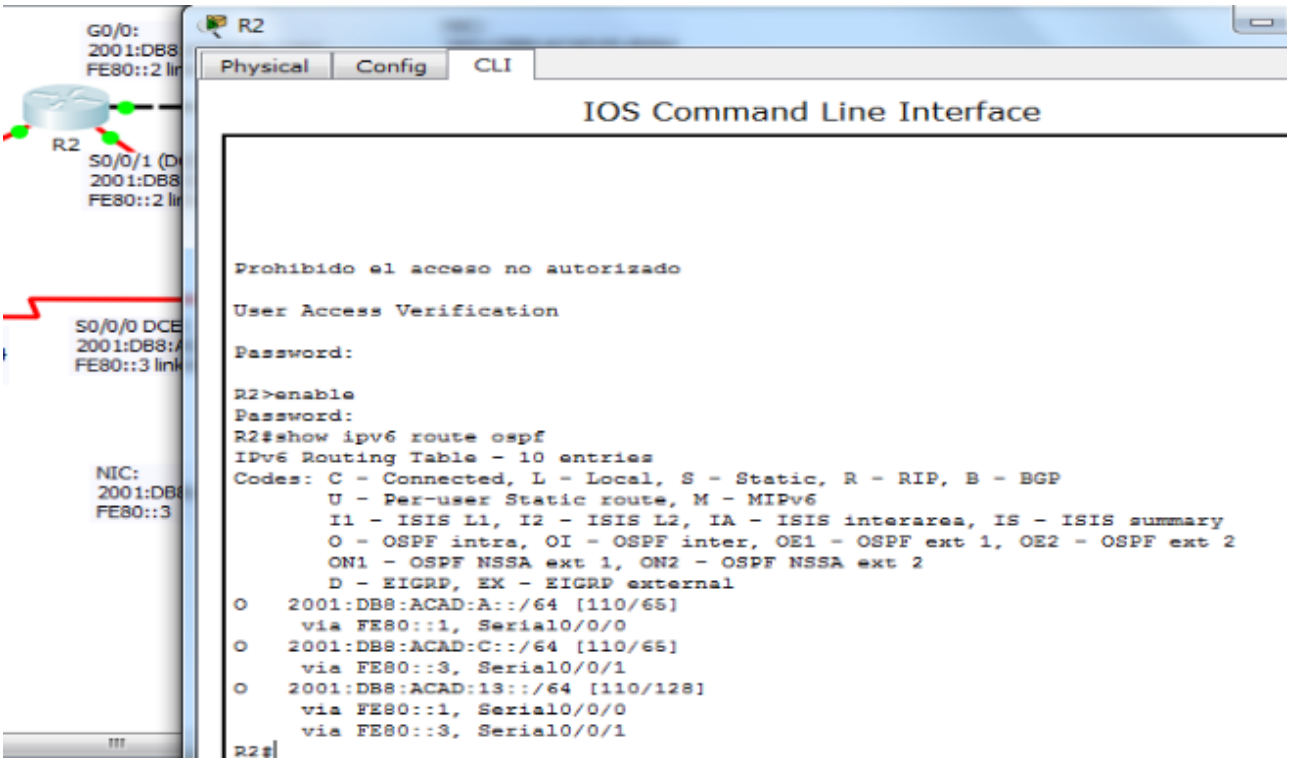
b. Emita el comando **passive-interface** para cambiar la interfaz G0/0 en el R1 a pasiva.

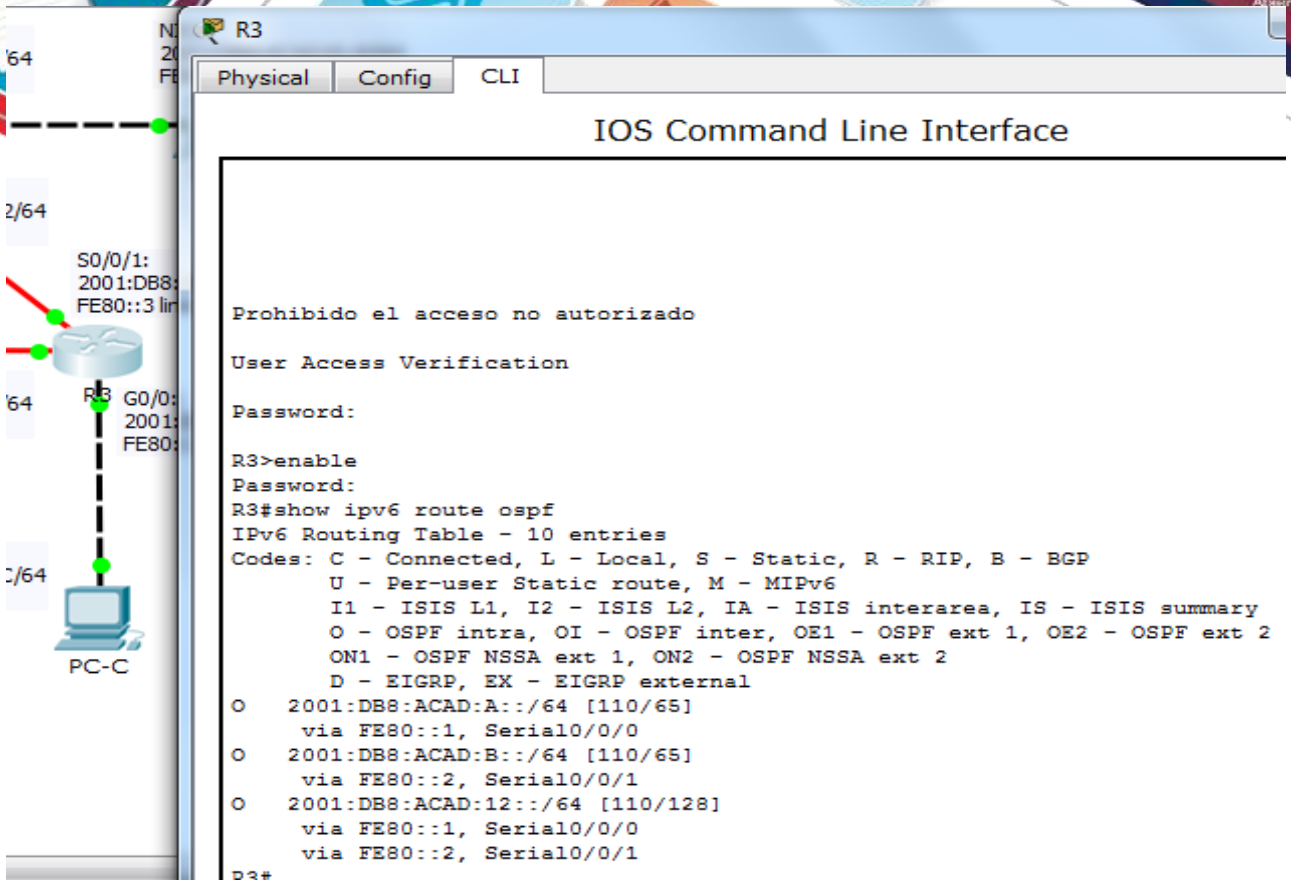


c. Vuelva a emitir el comando **show ipv6 ospf interface g0/0** para verificar que la interfaz G0/0 ahora sea pasiva.



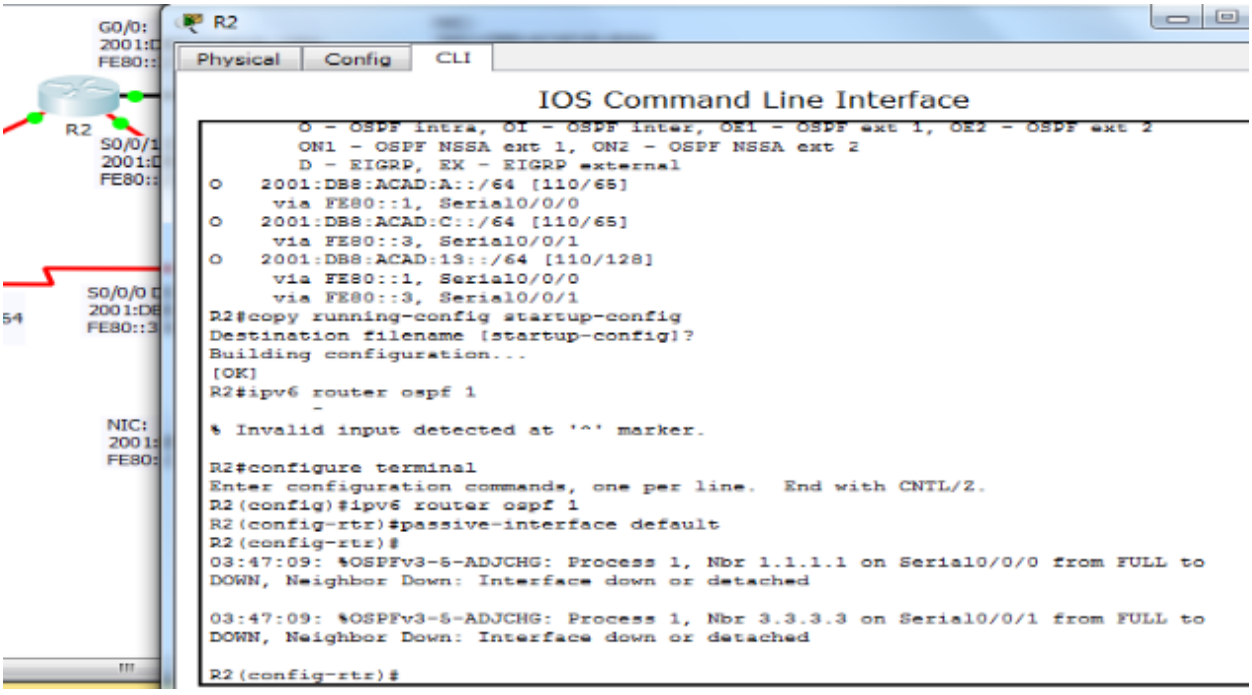
d. Emita el comando **show ipv6 route ospf** en el R2 y el R3 para verificar que todavía haya disponible una ruta a la red 2001:DB8:ACAD:A::/64.



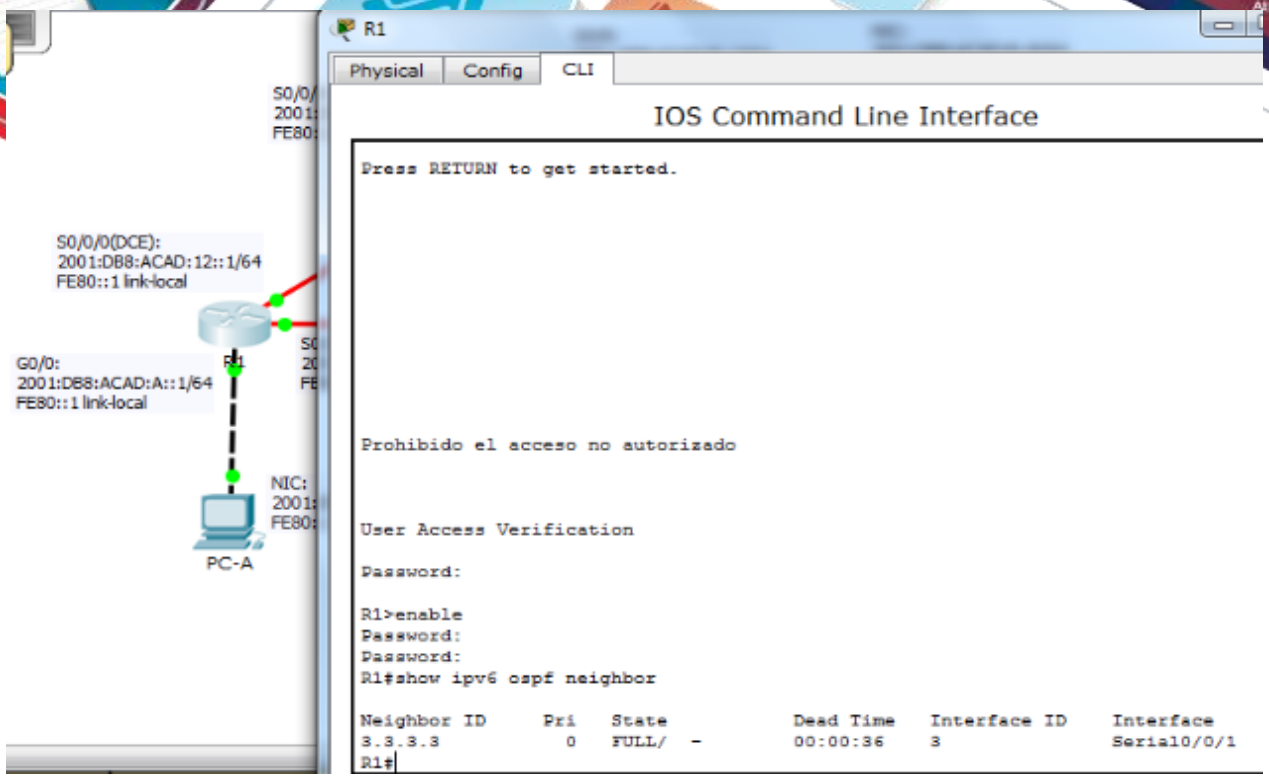


Step 21: establecer la interfaz pasiva como la interfaz predeterminada en el router.

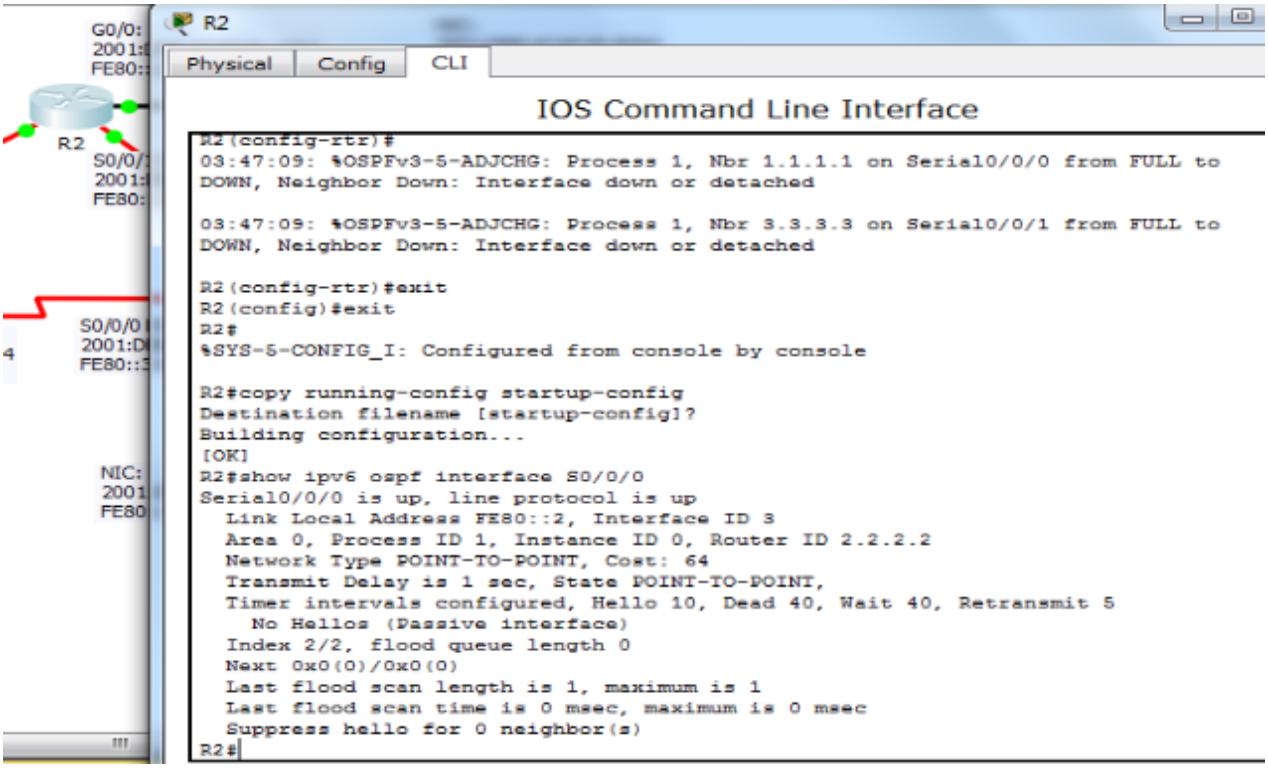
a. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPFv3 como pasivas de manera predeterminada.



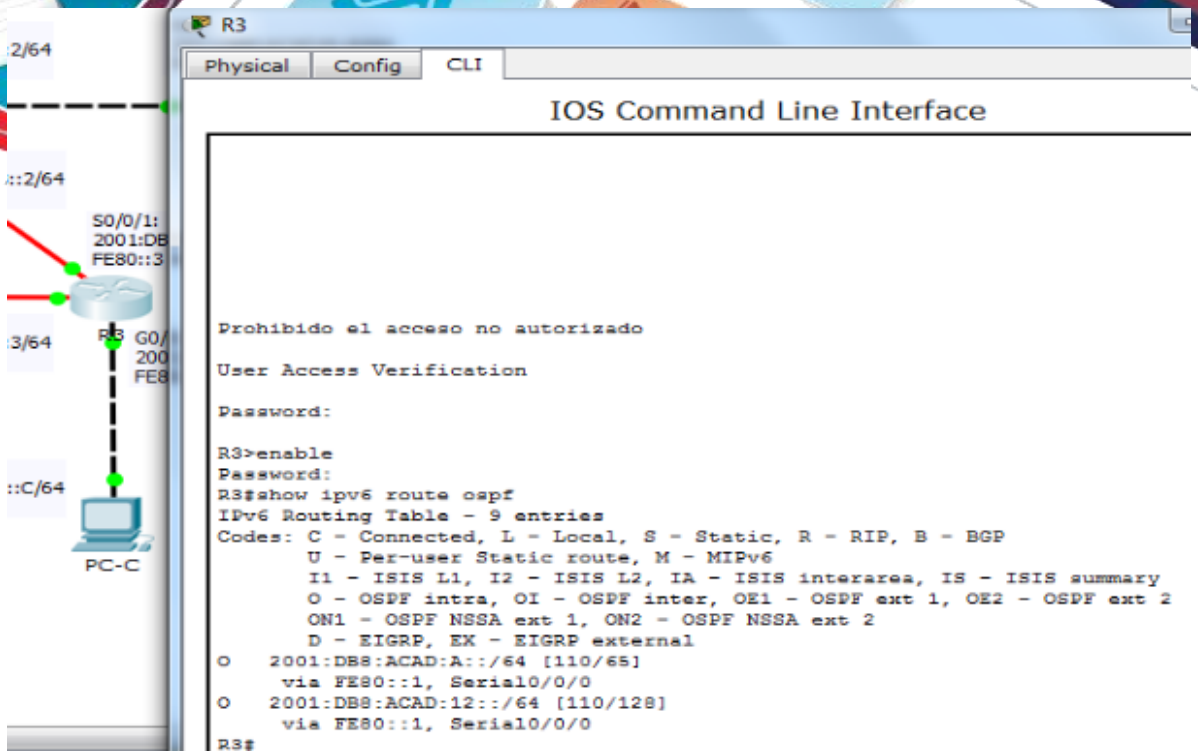
b. Emita el comando **show ipv6 ospf neighbor** en el R1. Una vez que el temporizador de tiempo muerto caduca, el R2 ya no se muestra como un vecino OSPF.



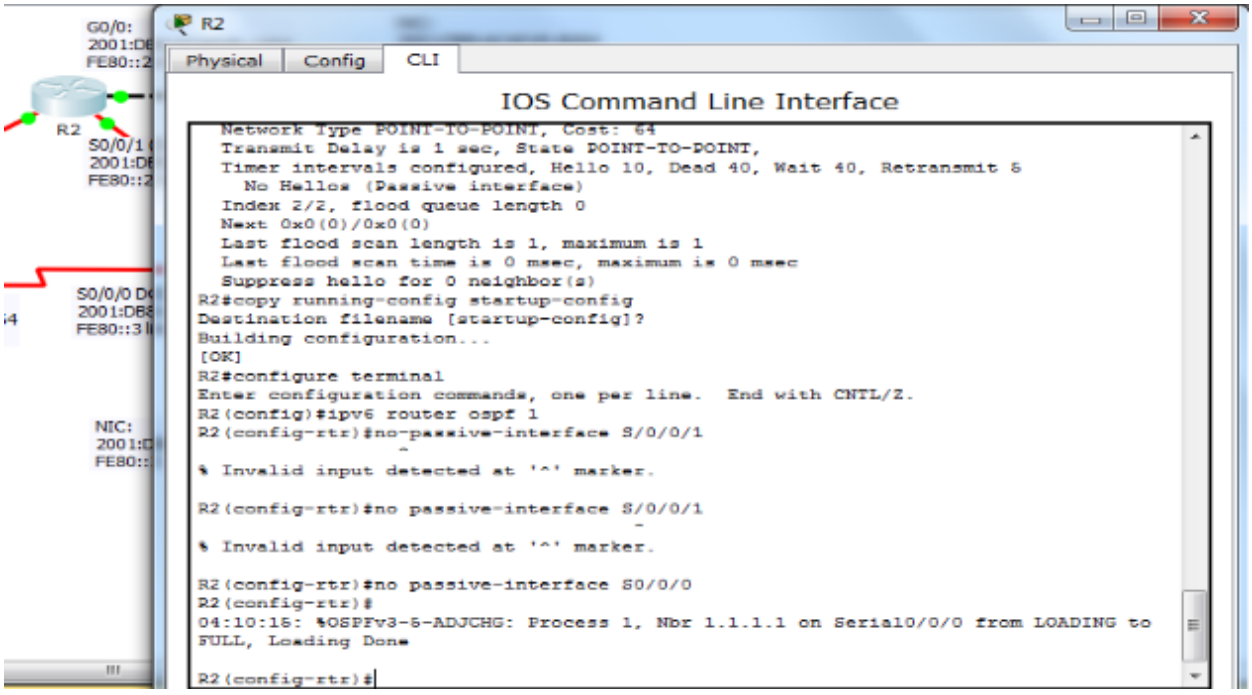
c. En el R2, emita el comando **show ipv6 ospf interface s0/0/0** para ver el estado OSPF de la interfaz S0/0/0.



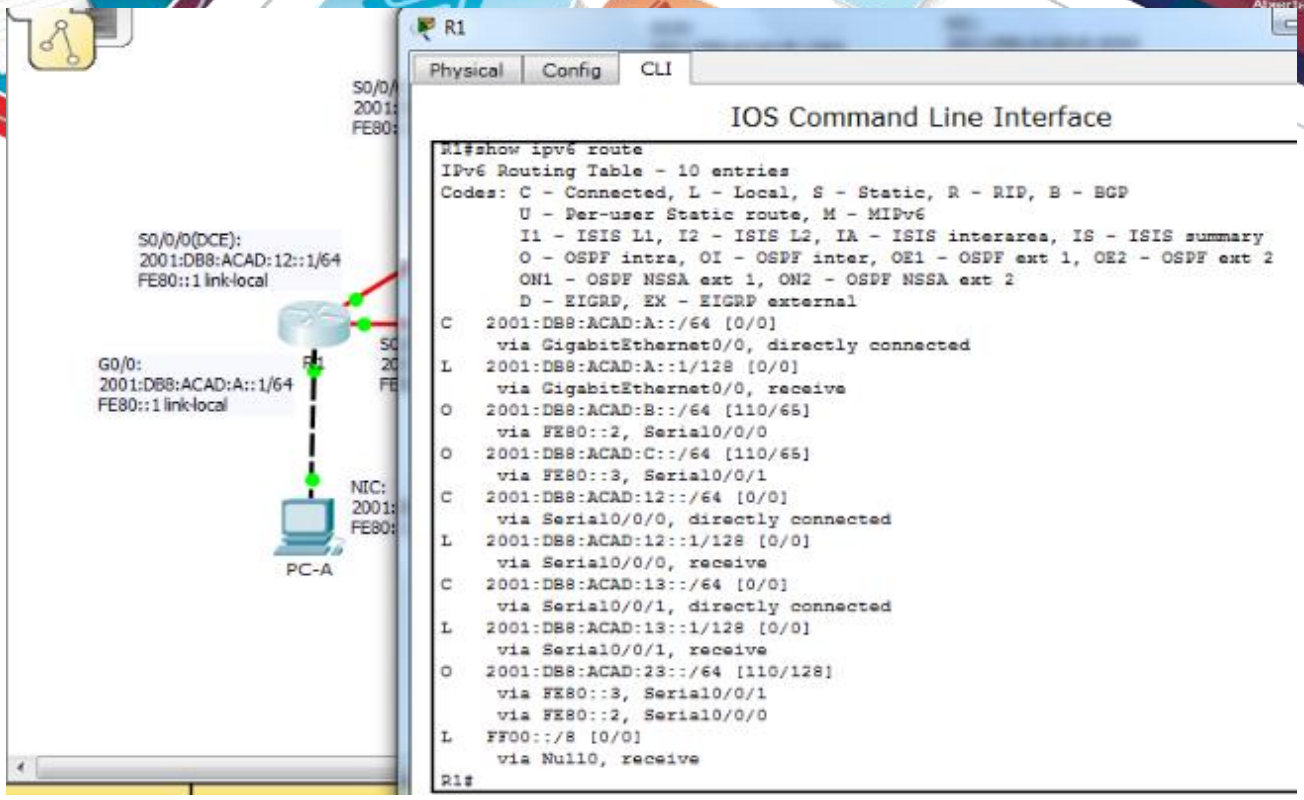
d. Si todas las interfaces OSPFv3 en el R2 son pasivas, no se anuncia ninguna información de routing. Si este es el caso, el R1 y el R3 ya no deberían tener una ruta a la red 2001:DB8:ACAD:B::/64. Esto se puede verificar mediante el comando **show ipv6 route**.

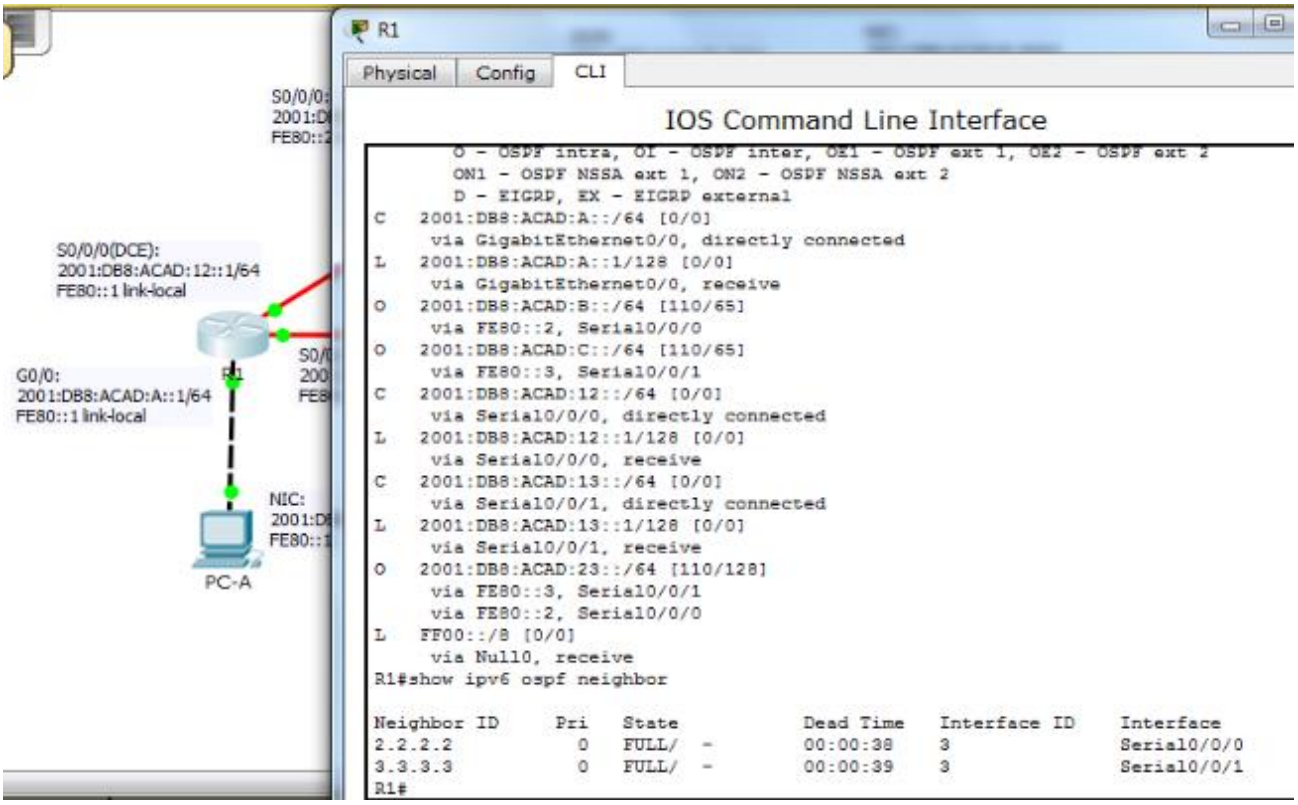


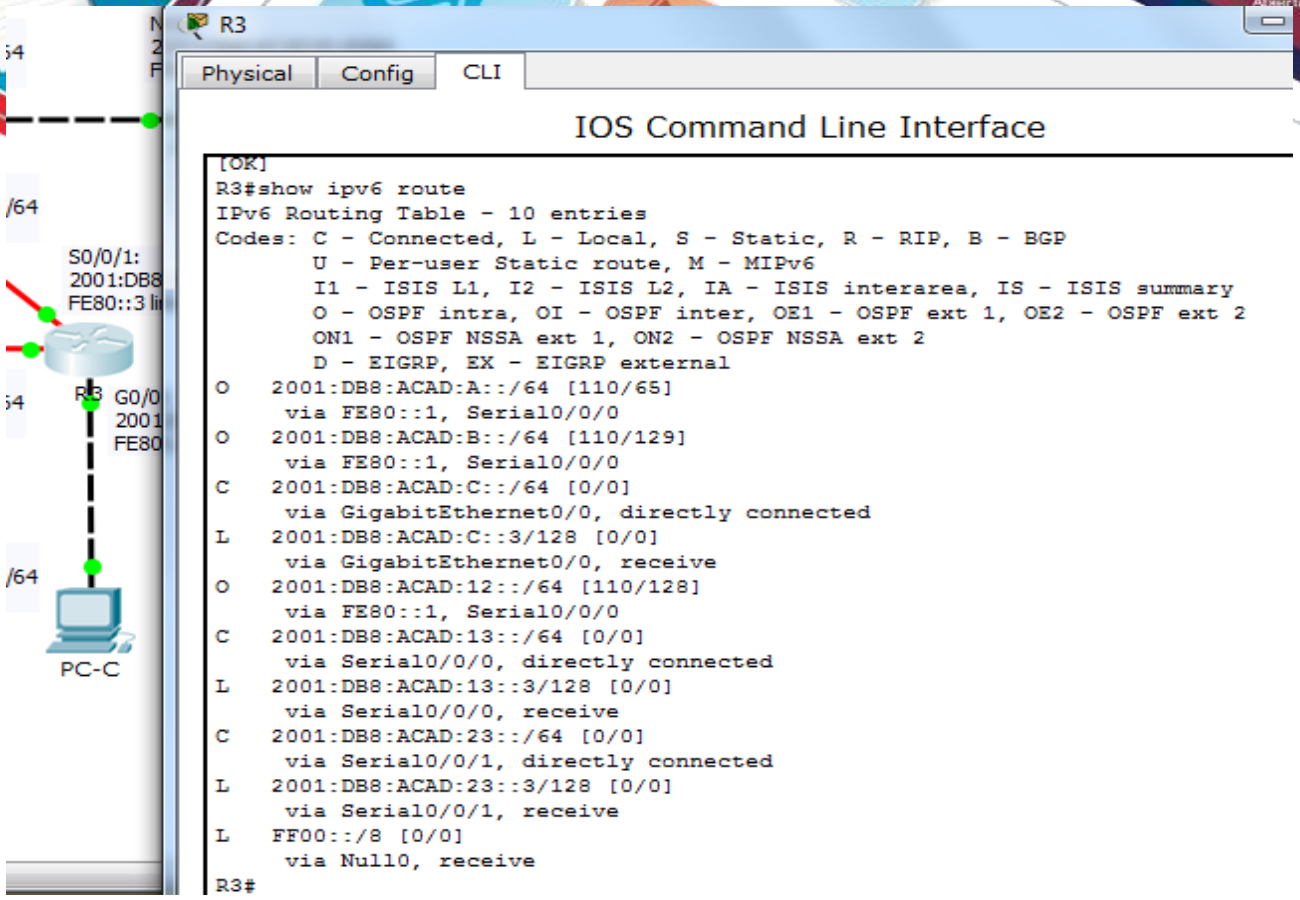
e. Ejecute el comando **no passive-interface** para cambiar S0/0/1 en el R2 a fin de que envíe y reciba actualizaciones de routing OSPFv3. Después de introducir este comando, aparece un mensaje informativo que explica que se estableció una adyacencia de vecino con el R3.

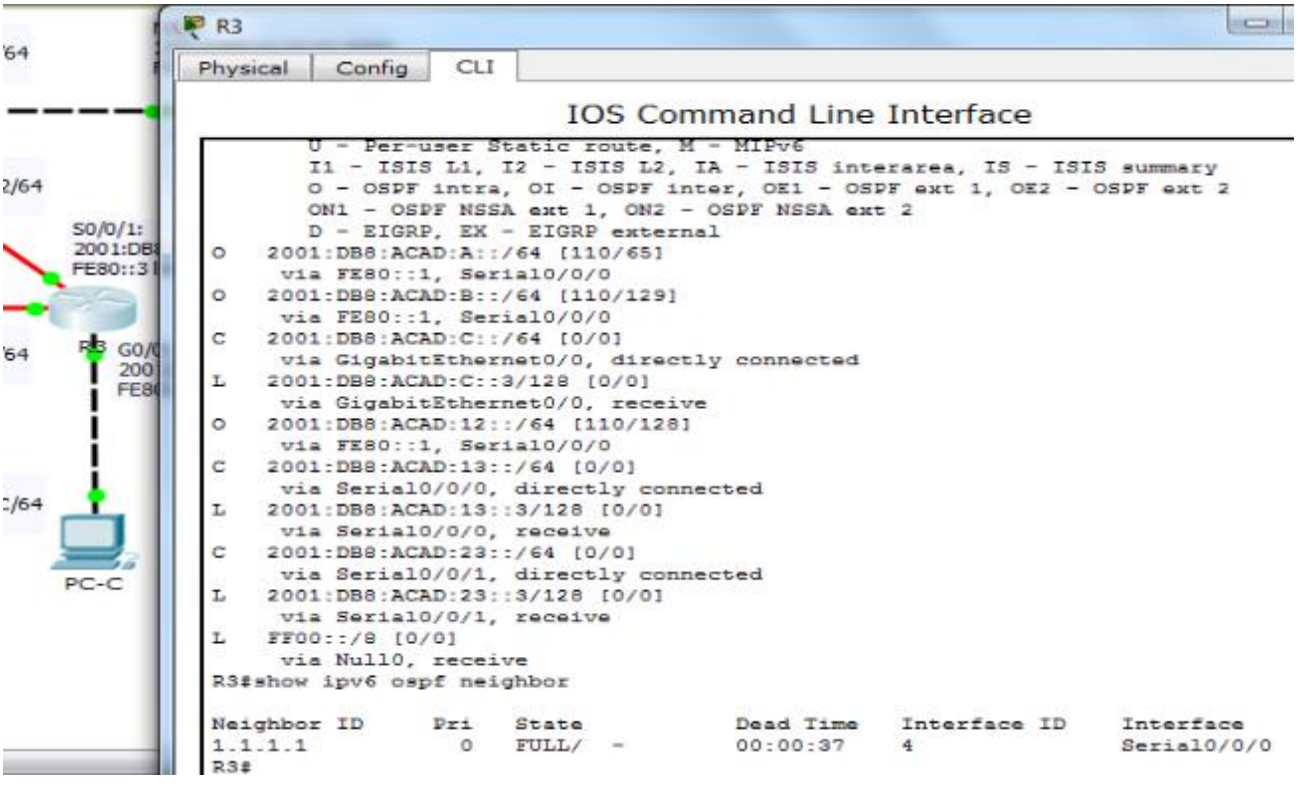


f. Vuelva a emitir los comandos **show ipv6 route** y **show ipv6 ospf neighbor** en el R1 y el R3, y busque una ruta a la red 2001:DB8:ACAD:B::/64.


R1
Physical
Config
CLI
IOS Command Line Interface
S0/0/0(DCE):
2001:DB8:ACAD:12::1/64
FE80::1 link-local
G0/0:
2001:DB8:ACAD:A::1/64
FE80::1 link-local
NIC:
PC-A
R1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:B::/64 [110/65]
via FE80::2, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65]
via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
via Serial0/0/0, receive
C 2001:DB8:ACAD:13::/64 [0/0]
via Serial0/0/1, directly connected
L 2001:DB8:ACAD:13::1/128 [0/0]
via Serial0/0/1, receive
O 2001:DB8:ACAD:23::/64 [110/128]
via FE80::3, Serial0/0/1
via FE80::2, Serial0/0/0
L FF00::/8 [0/0]
via Null0, receive
R1#


R1
Physical
Config
CLI
IOS Command Line Interface
S0/0/0(DCE):
2001:DB8:ACAD:12::1/64
FE80::1 link-local
G0/0:
2001:DB8:ACAD:A::1/64
FE80::1 link-local
NIC:
PC-A
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:B::/64 [110/65]
via FE80::2, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65]
via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
via Serial0/0/0, receive
C 2001:DB8:ACAD:13::/64 [0/0]
via Serial0/0/1, directly connected
L 2001:DB8:ACAD:13::1/128 [0/0]
via Serial0/0/1, receive
O 2001:DB8:ACAD:23::/64 [110/128]
via FE80::3, Serial0/0/1
via FE80::2, Serial0/0/0
L FF00::/8 [0/0]
via Null0, receive
R1#show ipv6 ospf neighbor
Neighbor ID Pri State Dead Time Interface ID Interface
2.2.2.2 0 FULL/ - 00:00:38 3 Serial0/0/0
3.3.3.3 0 FULL/ - 00:00:39 3 Serial0/0/1
R1#





¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64?

2001:DB8:ACAD:B::/64 [110/65]

Via FE80::2, Serial 0/0/0

¿Cuál es la métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1?

2001:DB8:ACAD:B::/64 [110/65]

¿El R2 aparece como vecino OSPFv3 en el R1?

No aparece

¿El R2 aparece como vecino OSPFv3 en el R3?

Si aparece

¿Qué indica esta información?

En la configuración realizada al router dos la interfaz conectada al router uno se configuro como interfaz pasiva

g. En el R2, emita el comando **no passive-interface S0/0/0** para permitir que se anuncien las actualizaciones de routing OSPFv3 en esa interfaz.

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#
02:37:34: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING t
o FULL, Loading Done

R2(config-rtr)#
```

h. Verifique que el R1 y el R2 ahora sean vecinos OSPFv3.

```
R1#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:38    3               Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:32    3               Serial0/0/1
R1#
```

Reflexión

1. Si la configuración OSPFv6 del R1 tiene la ID de proceso 1 y la configuración OSPFv3 del R2 tiene la ID de proceso 2, ¿se puede intercambiar información de routing entre ambos routers? ¿Por qué?

Sí, siempre y cuando el ID del proceso sea el mismo al crear el proceso de routing y al asignado a la interfaz

2. ¿Cuál podría haber sido la razón para eliminar el comando **network** en OSPFv3?
   - OSPFv3 se configura directamente en cada interfaz, usando el comando
   - **Ipv6 ospf id-proceso área id-área**
   - Esto se hace porque en IPV6 podemos asignar varias direcciones a la misma interfaz, entonces solo con agregar la interfaz estamos agregando todas las subredes.

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.				

Ejercicio No 4 - 10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router

Práctica de laboratorio: configuración de DHCPv4 básico en un router

Topología

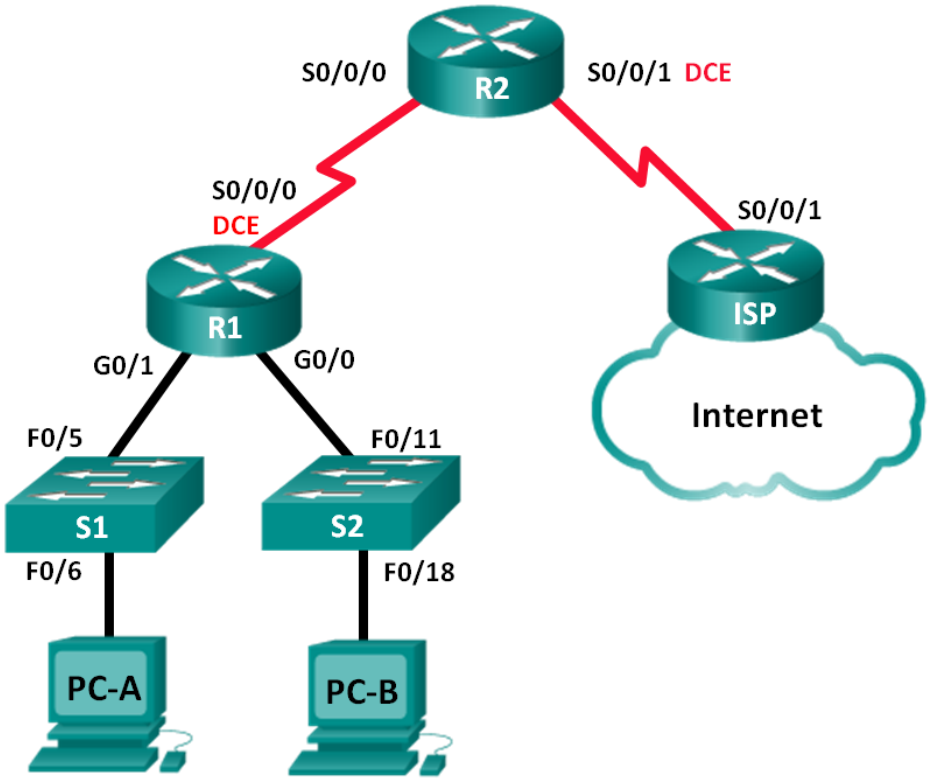


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.224	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.224	N/A
PC-A	NIC	DHCP	DHCP	DHCP

PC-B	NIC	DHCP	DHCP	DHCP

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

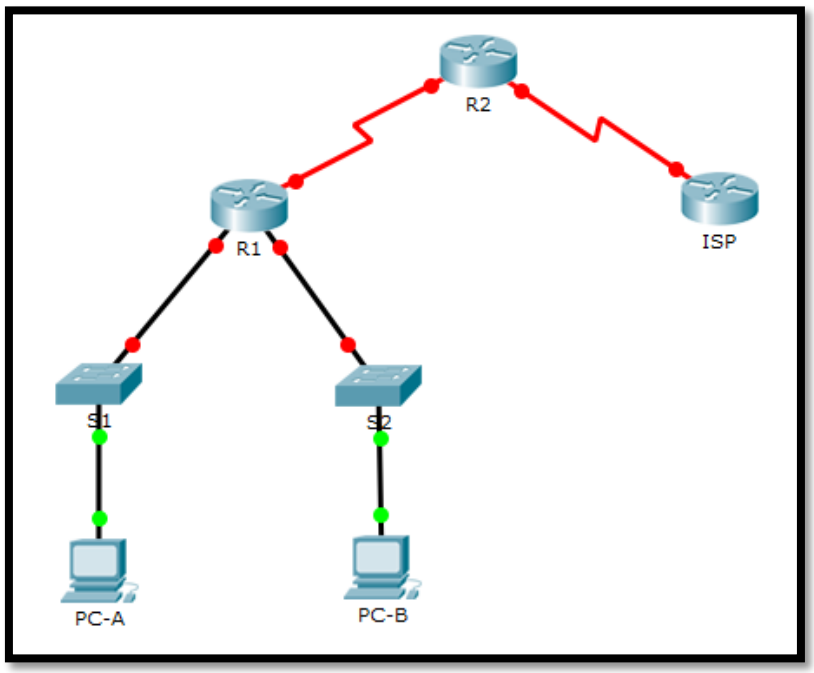
Cables Ethernet y seriales, como se muestra en la topología

Parte 1 armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los routers y switches con los parámetros básicos, como las contraseñas y las direcciones IP. Además, configurará los parámetros de IP de las computadoras en la topología.

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.



Paso 3 configurar los parámetros básicos para cada router.

a) Desactive la búsqueda DNS.
b) Configure el nombre del dispositivo como se muestra en la topología.
c) Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

d) Asigne **cisco** como la contraseña de consola y la contraseña de vty.

e) Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.

f) Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.

g) Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.

```
Router(config)#hostname R1
R1(config)#interface g0/0
R1(config-if)#ip address 192.168.0.1 255.255.2550
                                      ^
% Invalid input detected at '^' marker.

R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

R1(config-if)#int g0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
```

```
R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.2.253 255.255.255.252
R1(config-if)#no shutdown
```

```
R1(config-if)#clock rate 128000
R1(config-if)#exit
R1(config)#no ip domain-lookup
R1(config)#enable password class
R1(config)#enable secret password class
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exit
```

```
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#enable secret password class
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#int s0/0/0
R2(config-if)#ip address 192.168.2.254 255.255.255.252
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#int s0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

R2(config-if)#int s0/0/1
R2(config-if)#clock rate 128000
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#
```

```
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#enable secret password class
ISP(config)#line vty 0 4 password cisco
                           ^
% Invalid input detected at '^' marker.

ISP(config)#line vt4 0 4
                 ^
% Invalid input detected at '^' marker.

ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#int s0/0/1
ISP(config-if)#ip address 209.165.200.225 255.255.255.244
Bad mask 0xFFFFFFF4 for address 209.165.200.225
ISP(config-if)#ip address 209.165.200.225 255.255.255.224
ISP(config-if)#no shut

ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
```

h) Configure EIGRP for R1.

R1(config)# **router eigrp 1**

R1(config-router)# **network 192.168.0.0 0.0.0.255**

R1(config-router)# **network 192.168.1.0 0.0.0.255**

R1(config-router)# **network 192.168.2.252 0.0.0.3**

R1(config-router)# **no auto-summary**

```
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 192.168.2.252 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#exit
```

i) Configure EIGRP y una ruta predeterminada al ISP en el R2.

R2(config)# **router eigrp 1**

R2(config-router)# **network 192.168.2.252 0.0.0.3**

R2(config-router)# **redistribute static**

R2(config-router)# **exit**

R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.200.225**

```
R2(config)#router eigrp 1
R2(config-router)#network 192.168.2.252 0.0.0.3
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253
(Serial0/0/0) is up: new adjacency

R2(config-router)#redistribute static
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

j) Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.

ISP(config)# **ip route 192.168.0.0 255.255.252.0 209.165.200.226**

```
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#exit
```

k) Copie la configuración en ejecución en la configuración de inicio

```
R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R2#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
ISP#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

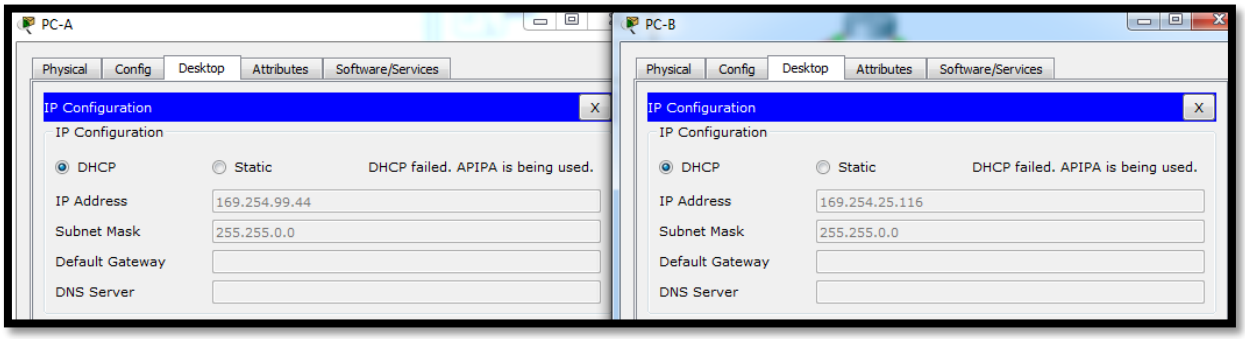
Paso 4 verificar la conectividad de red entre los routers.

Si algún ping entre los routers falla, corrija los errores antes de continuar con el siguiente paso. Use los comandos **show ip route** y **show ip interface brief** para detectar posibles problemas.

```
R1#ping 192.168.2.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms

R1#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
3/6/13 ms
```

```
R2#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9
ms
```

Paso 5 verificar que los equipos host estén configurados para DHCP.



Parte 2 configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

Para asignar automáticamente la información de dirección en la red, configure el R2 como servidor de DHCPv4 y el R1 como agente de retransmisión DHCP.

Paso 1 configurar los parámetros del servidor de DHCPv4 en el router R2.

En el R2, configure un conjunto de direcciones DHCP para cada LAN del R1. Utilice el nombre de conjunto **R1G0** para G0/0 LAN y **R1G1** para G0/1 LAN. Asimismo, configure las direcciones que se excluirán de los

conjuntos de direcciones. La práctica recomendada indica que primero se deben configurar las direcciones excluidas, a fin de garantizar que no se arrienden accidentalmente a otros dispositivos.

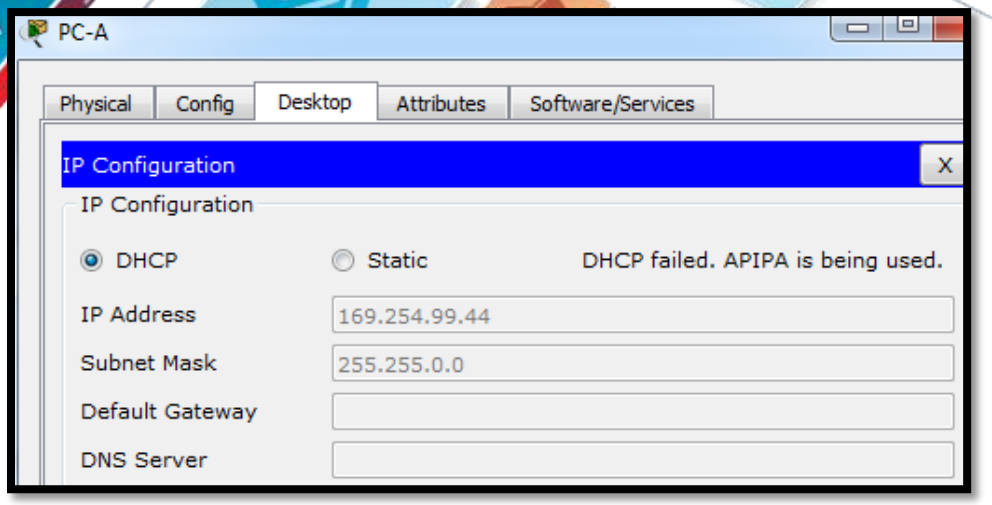
Excluya las primeras nueve direcciones en cada LAN del R1; empiece por .1. El resto de las direcciones deben estar disponibles en el conjunto de direcciones DHCP. Asegúrese de que cada conjunto de direcciones DHCP incluya un gateway predeterminado, el dominio **ccna-lab.com**, un servidor DNS (209.165.200.225) y un tiempo de arrendamiento de dos días.

En las líneas a continuación, escriba los comandos necesarios para configurar los servicios DHCP en el router R2, incluso las direcciones DHCP excluidas y los conjuntos de direcciones DHCP.

Nota: los comandos requeridos para la parte 2 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar DHCP en el R1 y el R2 sin consultar el apéndice.

```
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default router 192.168.1.1
                           ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
                    ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#lease 2
                  ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#exit
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
                    ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#lease 2
                  ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#exit
```

En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando **ipconfig /all**. ¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué?



No, porque el router configurado con los parámetros DHCP está en otra red.

Paso 2 configurar el R1 como agente de retransmisión DHCP.

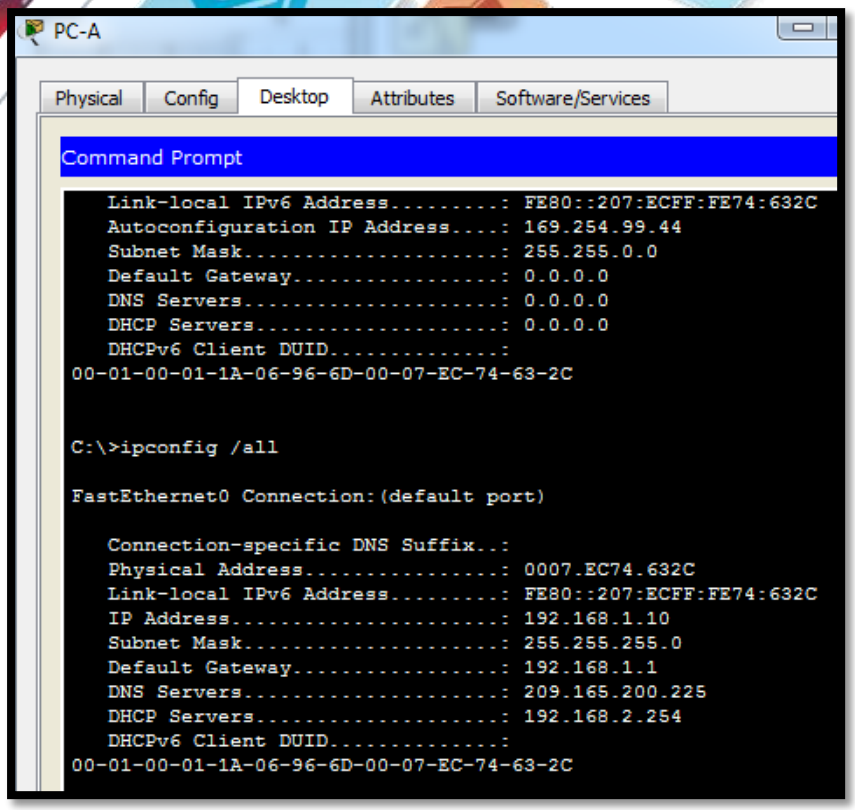
Configure las direcciones IP de ayuda en el R1 para que reenvíen todas las solicitudes de DHCP al servidor de DHCP en el R2.

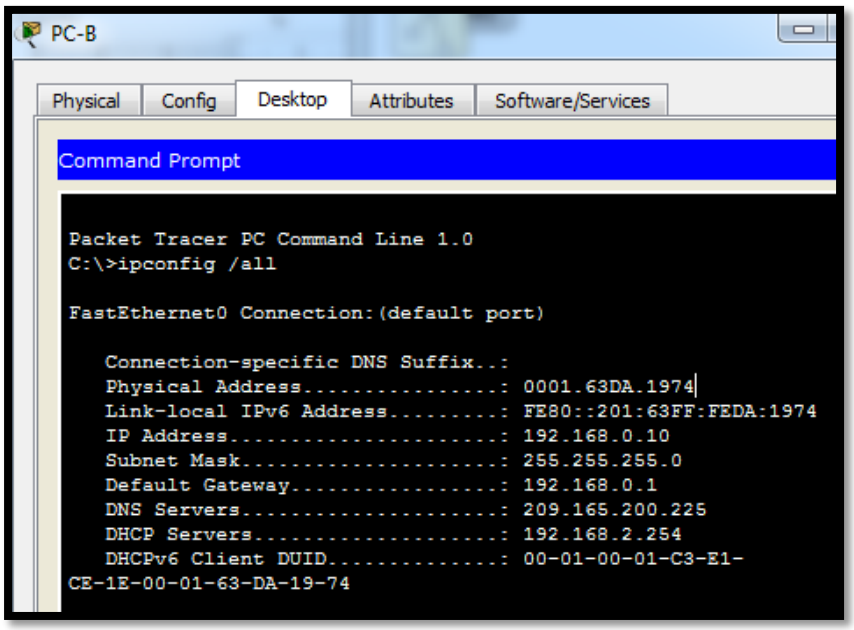
En las líneas a continuación, escriba los comandos necesarios para configurar el R1 como agente de retransmisión DHCP para las LAN del R1.

```
R1(config)#interface g0/0
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
R1(config)#interface g0/1
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
```

Paso 3 registrar la configuración IP para la PC-A y la PC-B.

En la PC-A y la PC-B, emita el comando ipconfig /all para verificar que las computadoras recibieron la información de la dirección IP del servidor de DHCP en el R2. Registre la dirección IP y la dirección MAC de cada computadora.





Según el pool de DHCP que se configuró en el R2, ¿cuáles son las primeras direcciones IP disponibles que la PC-A y la PC-B pueden arrendar?

192.168.1.10 y 192.168.0.10

Paso 4 verificar los servicios DHCP y los arrendamientos de direcciones en el R2.

a. En el R2, introduzca el comando **show ip dhcp binding** para ver los arrendamientos de direcciones DHCP. Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado?

Las direcciones físicas de los dispositivos a los cuales se les tiene asignada una dirección dinámica, junto con el tiempo de arrendamiento de dichas direcciones y el tipo de asignación.

```
R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration
Type
                 Hardware address
192.168.1.10     0007.EC74.632C           --
Automatic
192.168.0.10     0001.63DA.1974           --
Automatic
```

b. En el R2, introduzca el comando **show ip dhcp server statistics** para ver la actividad de mensajes y las estadísticas del pool de DHCP.

¿Cuántos tipos de mensajes DHCP se indican en el resultado?

Comando no soportado por packet tracer.

```
R2#show ip dhcp server statistics
                  ^
% Invalid input detected at '^' marker.
```

c. En el R2, introduzca el comando show ip dhcp pool para ver la configuración del pool de DHCP.

En el resultado del comando show ip dhcp pool, ¿a qué hace referencia el índice actual (Current index)?

A las direcciones de las puertas de enlace de cada interfaz conectada al router R1

```
Pool R1G1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.254     1    / 2     / 254

Pool R1G0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.0.1          192.168.0.1      - 192.168.0.254     1    / 2     / 254
```

d. En el R2, introduzca el comando show run | section dhcp para ver la configuración DHCP en la configuración en ejecución.

```
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 209.165.200.225
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 209.165.200.225
```

e. En el R1, introduzca el comando **show run interface** para las interfaces G0/0 y G0/1 para ver la configuración de retransmisión DHCP en la configuración en ejecución.

```
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.2.254
```

```
R1#show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.2.254
```

Reflexión

¿Cuál cree que es el beneficio de usar agentes de retransmisión DHCP en lugar de varios routers que funcionen como servidores de DHCP?

Centralizar equipos para que sirvan como servidores DHCP minimiza la carga y el uso de hardware para este menester en la red actual, además de que se deben ejecutar menos comandos para configurar dichos servicios DHCP; la administración es más sencilla que no estando centralizado el servicio.

Ejercicio No 5 - 10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch

Práctica de laboratorio: configuración de DHCPv4 básico en un switch

Topología

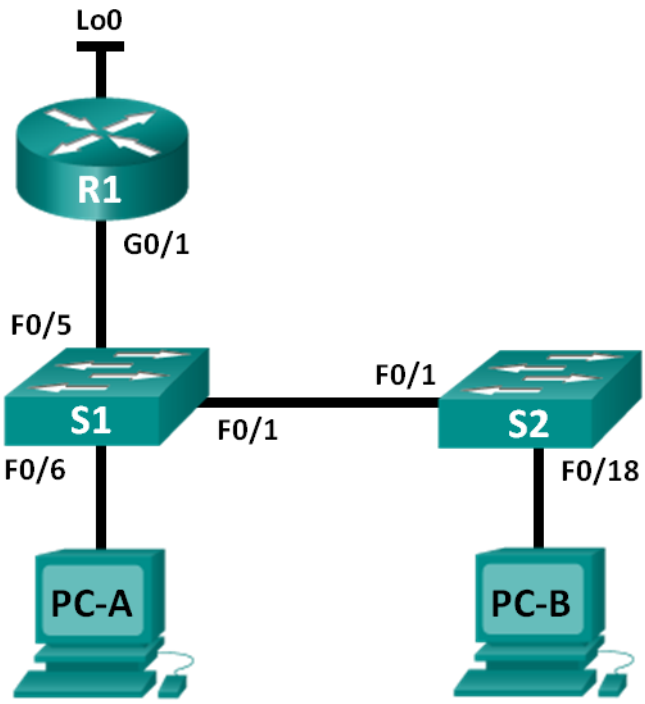


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.225	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: cambiar la preferencia de SDM

- Establecer la preferencia de SDM en lanbase-routing en el S1.

Parte 3: configurar DHCPv4

- Configurar DHCPv4 para la VLAN 1.
- Verificar la conectividad y DHCPv4.

Parte 4: configurar DHCP para varias VLAN

- Asignar puertos a la VLAN 2.
- Configurar DHCPv4 para la VLAN 2.
- Verificar la conectividad y DHCPv4.

Parte 5: habilitar el routing IP

- Habilite el routing IP en el switch.
- Crear rutas estáticas.

Información básica/situación

Un switch Cisco 2960 puede funcionar como un servidor de DHCPv4. El servidor de DHCPv4 de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones identificados que están asociados a VLAN específicas e interfaces virtuales de switch (SVI). El switch Cisco 2960 también puede funcionar como un dispositivo de capa 3 y hacer routing entre VLAN y una cantidad limitada de rutas estáticas. En esta práctica de laboratorio, configurará DHCPv4 para VLAN únicas y múltiples en un switch Cisco 2960, habilitará el routing en el switch para permitir la comunicación entre las VLAN y agregará rutas estáticas para permitir la comunicación entre todos los hosts.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

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 esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

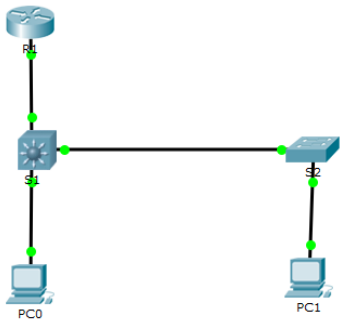
Nota: asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 1 router (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, como se muestra en la topología

armar la red y configurar los parámetros básicos de los dispositivos

Paso 22: realizar el cableado de red tal como se muestra en la topología.



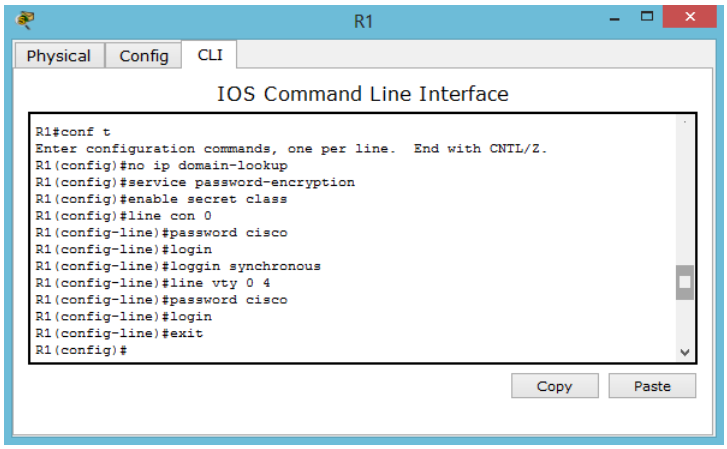
Paso 23: inicializar y volver a cargar los routers y switches.

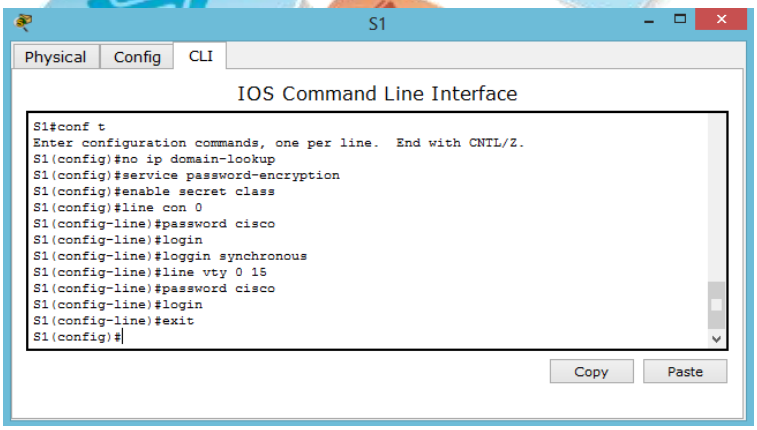
Paso 24: configurar los parámetros básicos en los dispositivos.

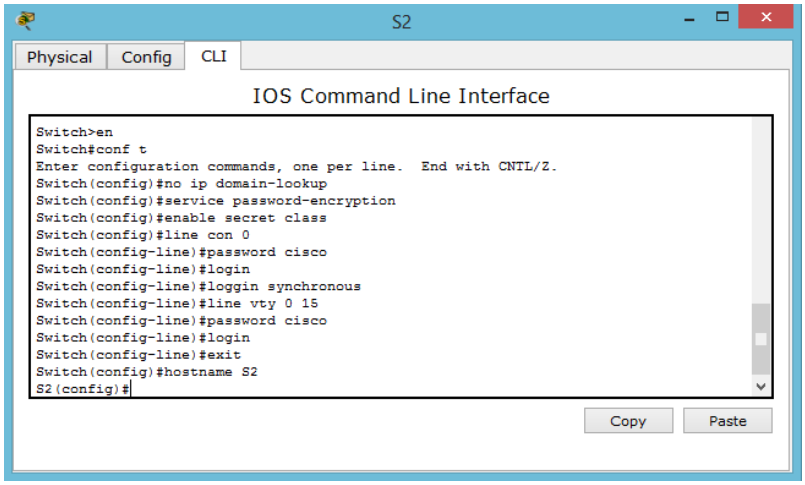
a. Asigne los nombres de dispositivos como se muestra en la topología.

b. Desactive la búsqueda del DNS.

c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.



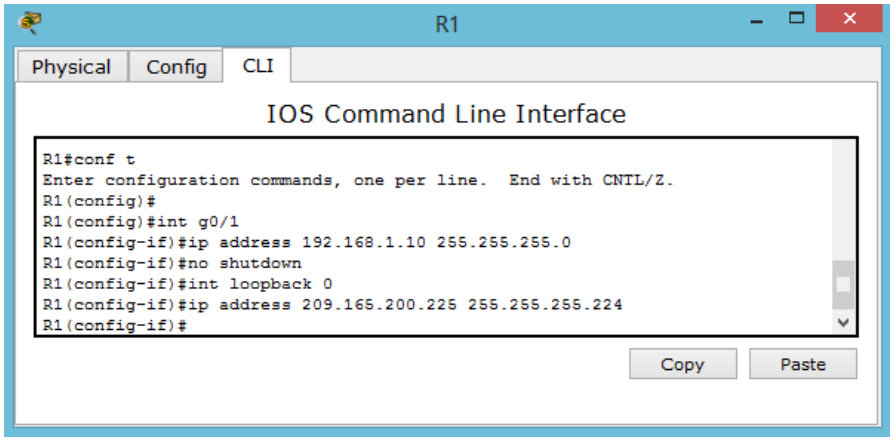


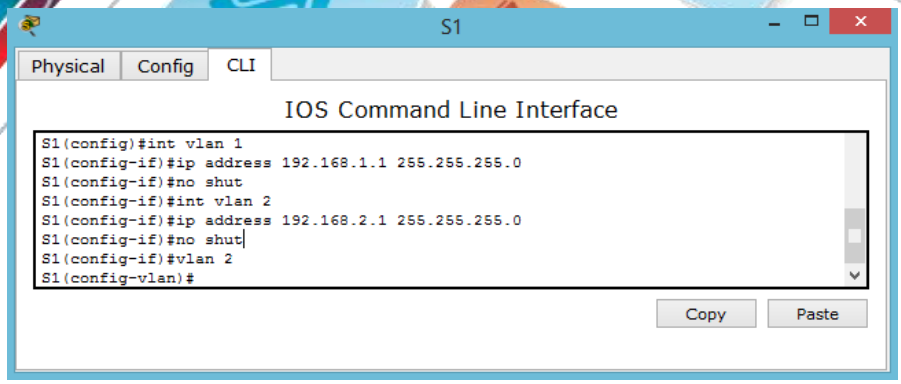


d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

e. Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.

f. Guarde la configuración en ejecución en el archivo de configuración de inicio.





cambiar la preferencia de SDM

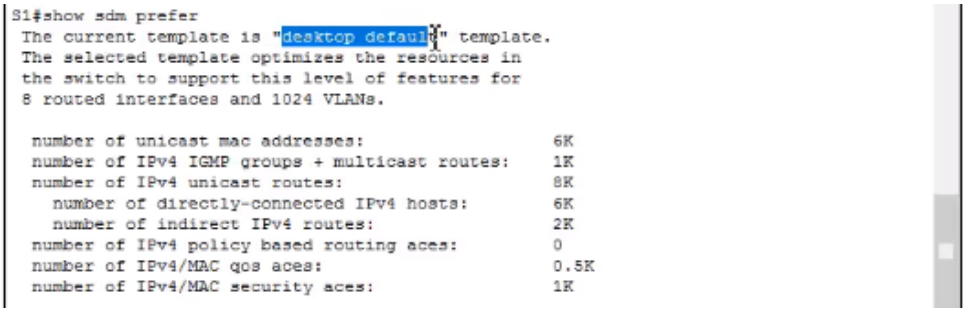
Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch Cisco 2960. Las plantillas pueden habilitarse para admitir funciones específicas según el modo en que se utilice el switch en la red. En esta práctica de laboratorio, la plantilla lanbase-routing está habilitada para permitir que el switch realice el routing entre VLAN y admita el routing estático.

Paso 25: mostrar la preferencia de SDM en el S1.

En el S1, emita el comando **show sdm prefer** en modo EXEC privilegiado. Si no se cambió la plantilla predeterminada de fábrica, debería seguir siendo **default**. La plantilla **default** no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será **dual-ipv4-and-ipv6 default**.

```
S1# show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                  8K
  number of IPv4 IGMP groups:                       0.25K
  number of IPv4/MAC qos aces:                      0.125k
  number of IPv4/MAC security aces:                 0.375k
```

¿Cuál es la plantilla actual? “defaul”



a. Establezca la preferencia de SDM en **lanbase-routing**. (Si lanbase-routing es la plantilla actual, continúe con la parte 3). En el modo de configuración global, emita el comando **sdm prefer lanbase-routing**.

```
S1(config)# sdm prefer lanbase-routing
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

¿Qué plantilla estará disponible después de la recarga? Routing

b. Se debe volver a cargar el switch para que la plantilla esté habilitada.

```
S1# reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

Nota: la nueva plantilla se utilizará después del reinicio, incluso si no se guardó la configuración en ejecución. Para guardar la configuración en ejecución, responda **yes** (sí) para guardar la configuración modificada del sistema.

Paso 26: verificar que la plantilla lanbase-routing esté cargada.

Emita el comando **show sdm prefer** para verificar si la plantilla lanbase-routing se cargó en el S1.

```
S1# show sdm prefer
 The current template is "lanbase-routing" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                  4K
  number of IPv4 IGMP groups + multicast routes:    0.25K
  number of IPv4 unicast routes:                    0.75K
    number of directly-connected IPv4 hosts:        0.75K
    number of indirect IPv4 routes:                 16
  number of IPv6 multicast groups:                  0.375k
  number of directly-connected IPv6 addresses:      0.75K
    number of indirect IPv6 unicast routes:         16
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.125k
  number of IPv4/MAC security aces:                 0.375k
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0.375k
  number of IPv6 security aces:                     127
```

```
S1#show sdm prefer
The current template is "routing" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

 number of unicast mac addresses:                  3K
 number of IPv4 IGMP groups + multicast routes:    1K
 number of IPv4 unicast routes:                    11K
 number of directly-connected IPv6 addresses:      3K
 number of indirect IPv6 unicast routes:           8K
 number of IPv4 policy based routing aces:         0.5K
 number of IPv4/MAC qos aces:                      0.5K
 number of IPv4/MAC security aces:                 1K
```

configurar DHCPv4

En la parte 3, configurará DHCPv4 para la VLAN 1, revisará las configuraciones IP en los equipos host para validar la funcionalidad de DHCP y verificará la conectividad de todos los dispositivos en la VLAN 1.

Paso 27: configurar DHCP para la VLAN 1.

a. Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.

ip dhcp excluded-address 192.168.1.1 192.168.1.10

Cree un pool de DHCP con el nombre **DHCP1**. En el espacio proporcionado, escriba el comando que utilizó.

ip dhcp pool DHCP1

b. Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

network 192.168.1.0 255.255.255.0

c. Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.

default-router 192.168.1.1

d. Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.

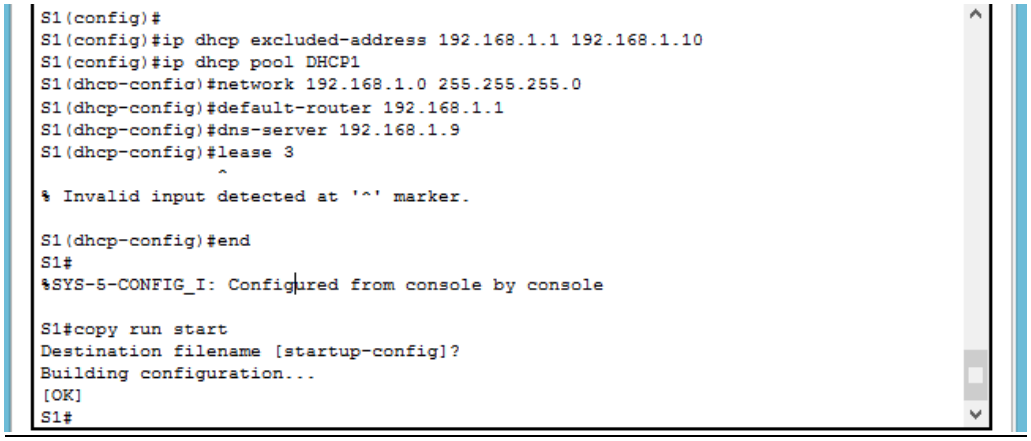
dns-server 192.168.1.9

e. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

lease 3

f. Guarde la configuración en ejecución en el archivo de configuración de inicio.

copy run start



Paso 28: verificar la conectividad y DHCP.

a. En la PC-A y la PC-B, abra el símbolo del sistema y emita el comando **ipconfig**. Si la información de IP no está presente, o si está incompleta, emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.1.11

Máscara de subred: 255.255.255.0

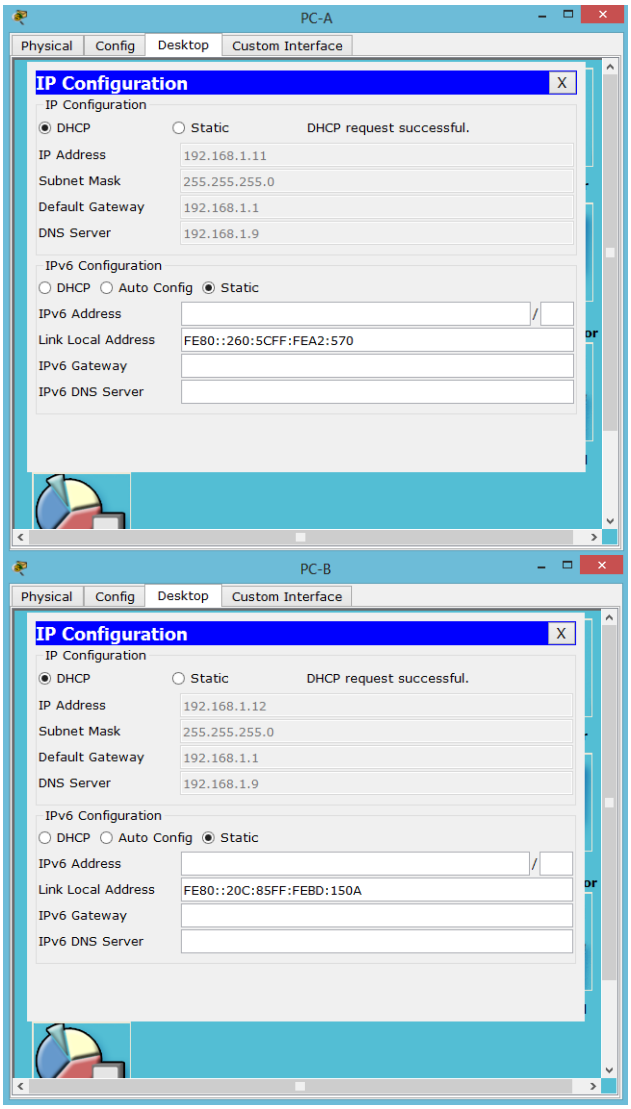
Gateway predeterminado: 192.168.1.1

Para la PC-B, incluya lo siguiente:

Dirección IP: 192.168.1.12

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1



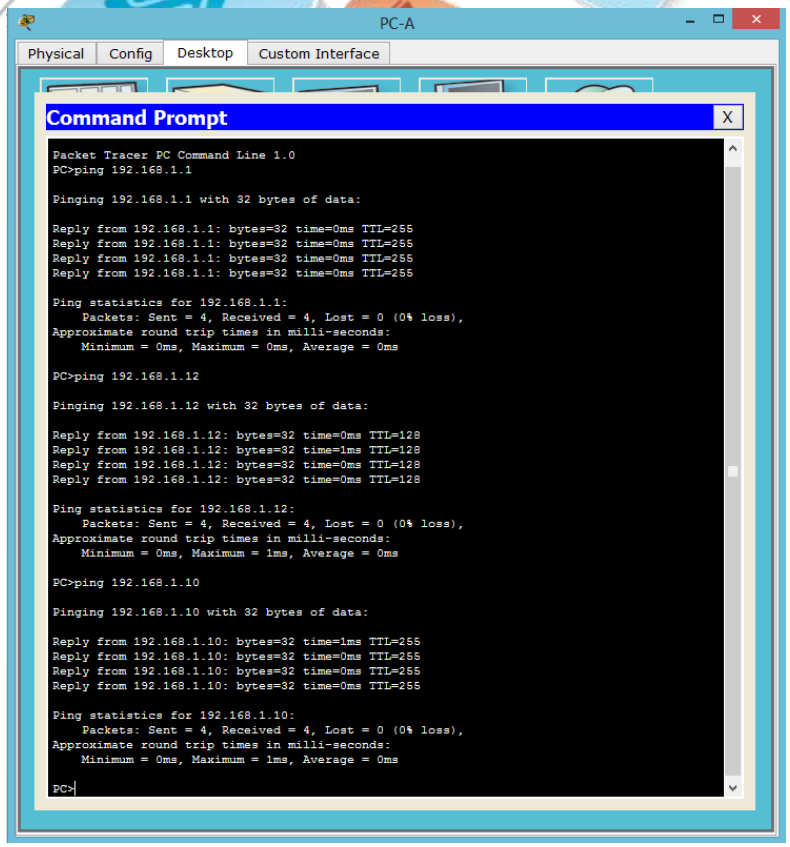
b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? SI

¿Es posible hacer ping de la PC-A a la PC-B? SI

¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1? SI

Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.



configurar DHCPv4 para varias VLAN

En la parte 4, asignará la PC-A un puerto que accede a la VLAN 2, configurará DHCPv4 para la VLAN 2, renovará la configuración IP de la PC-A para validar DHCPv4 y verificará la conectividad dentro de la VLAN.

Paso 29: asignar un puerto a la VLAN 2.

Coloque el puerto F0/6 en la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

S1(config)#int f0/6

S1(config-if)#switchpor mode access

S1(config-if)#switchpor access vlan 2

S1(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

Paso 30: configurar DHCPv4 para la VLAN 2.

a. Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.

   ip dhcp excluded-address 192.168.2.1 192.168.2.10

b. Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó.

   ip dhcp pool DHCP2

c. Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

   network 192.168.2.0 255.255.255.0

d. Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.

default-router 192.168.2.1

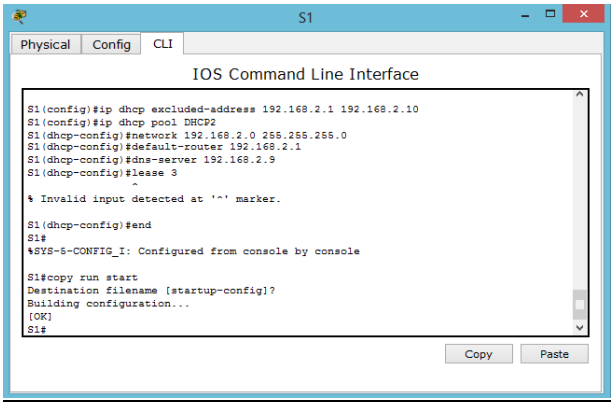
e. Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.

dns-server 192.168.2.9

f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

lease 3

g. Guarde la configuración en ejecución en el archivo de configuración de inicio.



Paso 31: verificar la conectividad y DHCPv4.

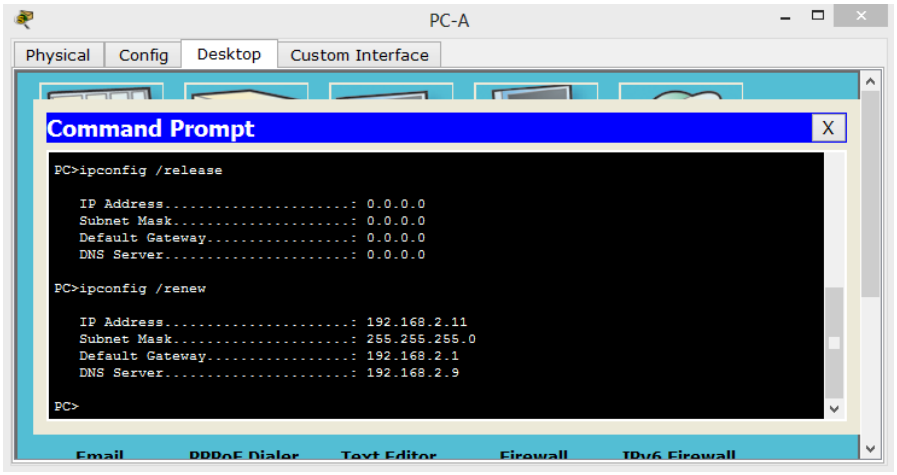
a. En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.2.11

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.2.1



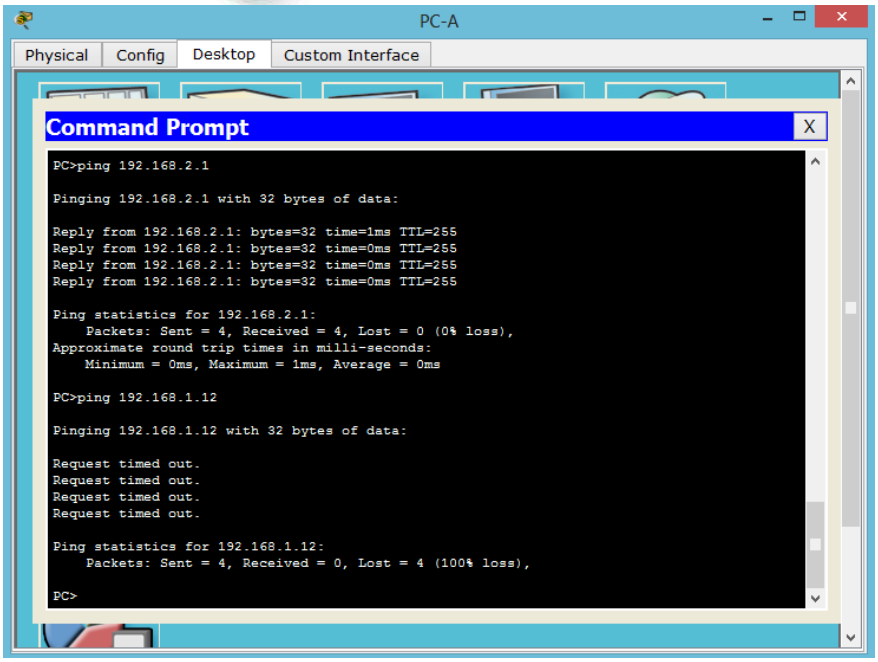
b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado de la VLAN 2 y a la PC-B.

¿Es posible hacer ping de la PC-A al gateway predeterminado? SI

¿Es posible hacer ping de la PC-A a la PC-B? NO

¿Los pings eran correctos? ¿Por qué?

Da ping a la puerta de enlace porque se encuentra en la misma red, en el caso de la PC-B no da ping por estar en una red diferente



c. Emita el comando **show ip route** en el S1.

¿Qué resultado arrojó este comando?

No ha sido configurada la puerta de enlace y no muestra la puerta de routeo.

```
S1#show ip route
Default gateway is not set

Host               Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
S1#
```

habilitar el routing IP

En la parte 5, habilitará el routing IP en el switch, que permitirá la comunicación entre VLAN. Para que todas las redes se comuniquen, se deben implementar rutas estáticas en el S1 y el R1.

habilitar el routing IP en el S1.

d. En el modo de configuración global, utilice el comando **ip routing** para habilitar el routing en el S1.

```
S1(config)# ip routing
```

e. Verificar la conectividad entre las VLAN.

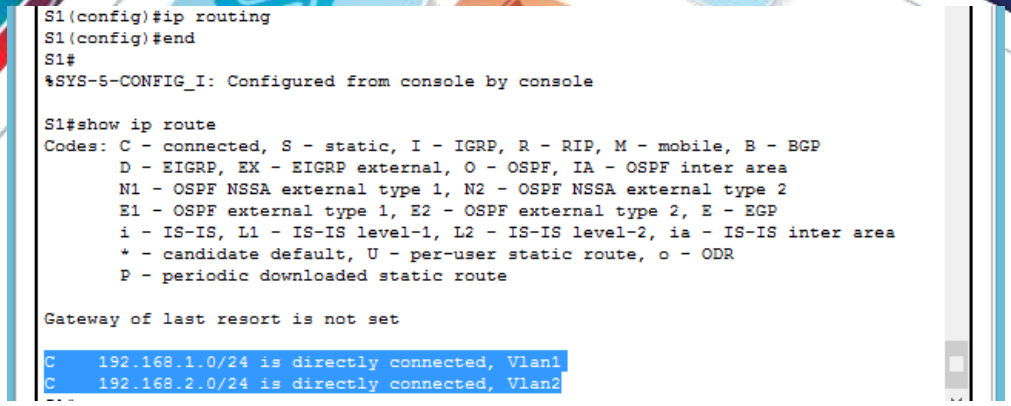
¿Es posible hacer ping de la PC-A a la PC-B? SI

¿Qué función realiza el switch?

El switch está ruteando entre VLANs

f. Vea la información de la tabla de routing para el S1.

¿Qué información de la ruta está incluida en el resultado de este comando?



```
S1(config)#ip routing
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Vlan1
C    192.168.2.0/24 is directly connected, Vlan2
```

g. Vea la información de la tabla de routing para el R1.

¿Qué información de la ruta está incluida en el resultado de este comando?

Las redes VLAN 1 y VLAN 2

h. ¿Es posible hacer ping de la PC-A al R1? NO

¿Es posible hacer ping de la PC-A a la interfaz Lo0? NO

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Deben agregarse routers a la tabla de routeo.

Paso 32: asignar rutas estáticas.

Habilitar el routing IP permite que el switch enrute entre VLAN asignadas en el switch. Para que todas las VLAN se comuniquen con el router, es necesario agregar rutas estáticas a la tabla de routing del switch y del router.

a. En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.

ip route 0.0.0.0 0.0.0.0 192.168.1.10

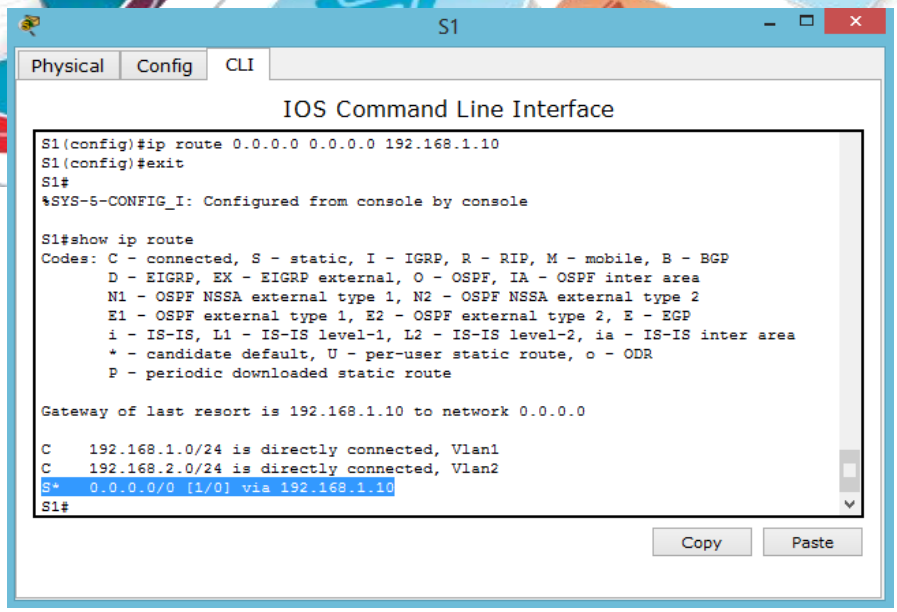
b. En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

ip route 192.168.2.0 255.255.255.0 g0/1

c. Vea la información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?

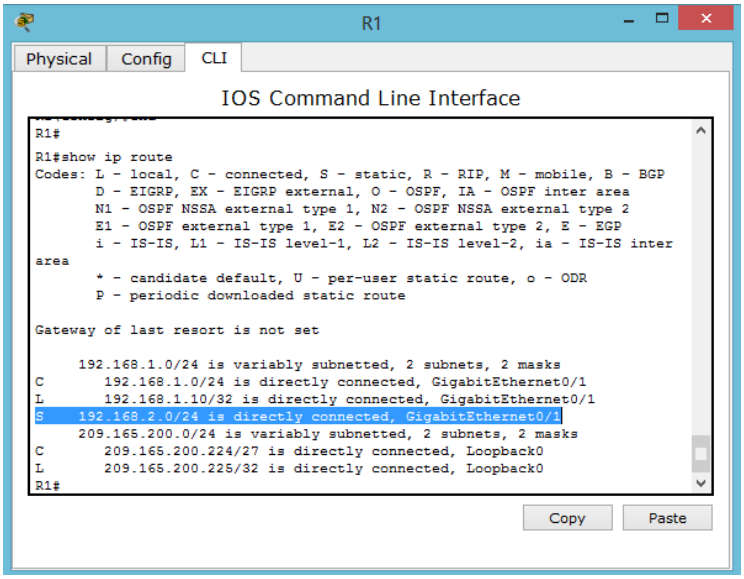
La ruta por defecto representada es: **S* 0.0.0.0/0 [1/0] via 192.168.1.10**



d. Vea la información de la tabla de routing para el R1.

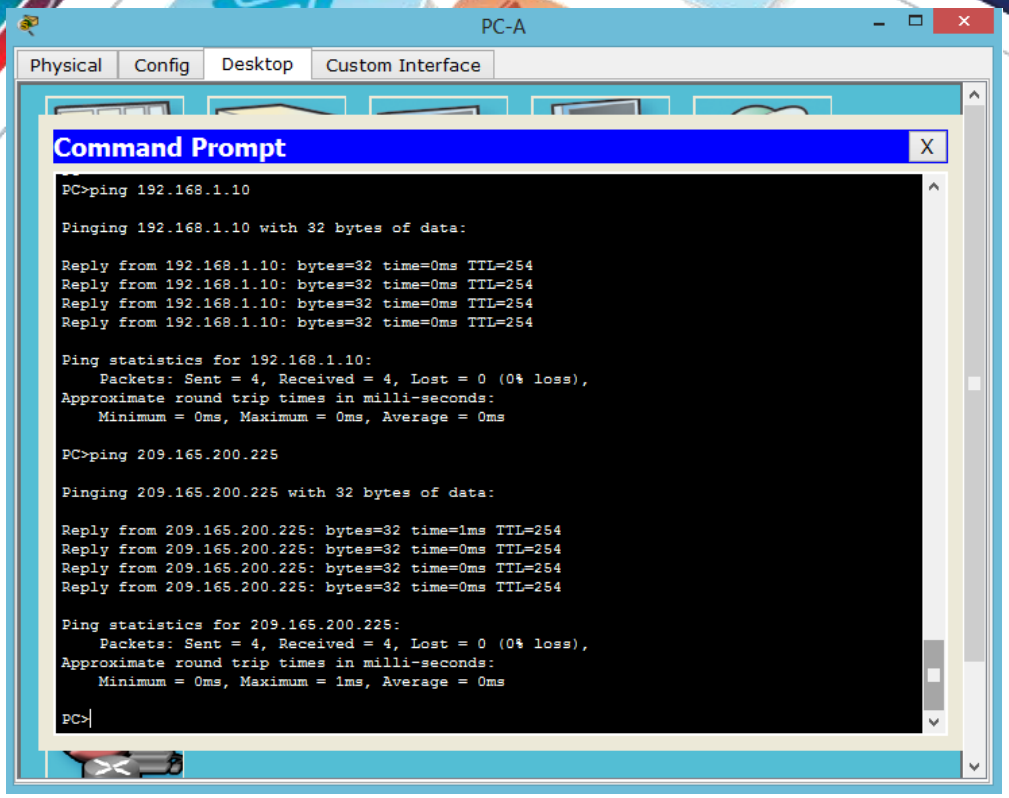
¿Cómo está representada la ruta estática?

S 192.168.2.0/24 is directly connected, GigabitEthernet0/1



e. ¿Es posible hacer ping de la PC-A al R1? SI

¿Es posible hacer ping de la PC-A a la interfaz Lo0? SI


PC-A
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Ping statistics for 209.165.200.225:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>

Reflexión

1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

   Porque hay una ventana de tiempo, donde las direcciones excluidas podrían ser directamente incluidas en un host.

2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

   El switch asignará las configuraciones IP basándose en la asignación de VLAN en el puerto en el que los host están conectados

3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?

   El switch puede tener las funciones como el del servidor DHCP y como ruteo estático y entre VLANs

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.

Apéndice A: comandos de configuración

Configurar DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

Configurar DHCPv4 para varias VLAN

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)# ip dhcp pool DHCP2
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.2.1
S1(dhcp-config)# dns-server 192.168.2.9
S1(dhcp-config)# lease 3
```

Habilitar routing IP

```
S1(config)# ip routing
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```

Ejercicio No 6 - 10.2.3.5 Lab- Configuring Stateless and Stateful DHCPv6

Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado

Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1	64	No aplicable
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Solo mediante configuración automática de dirección sin estado (SLAAC)
- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
- Mediante DHCPv6 con estado

Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

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 esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

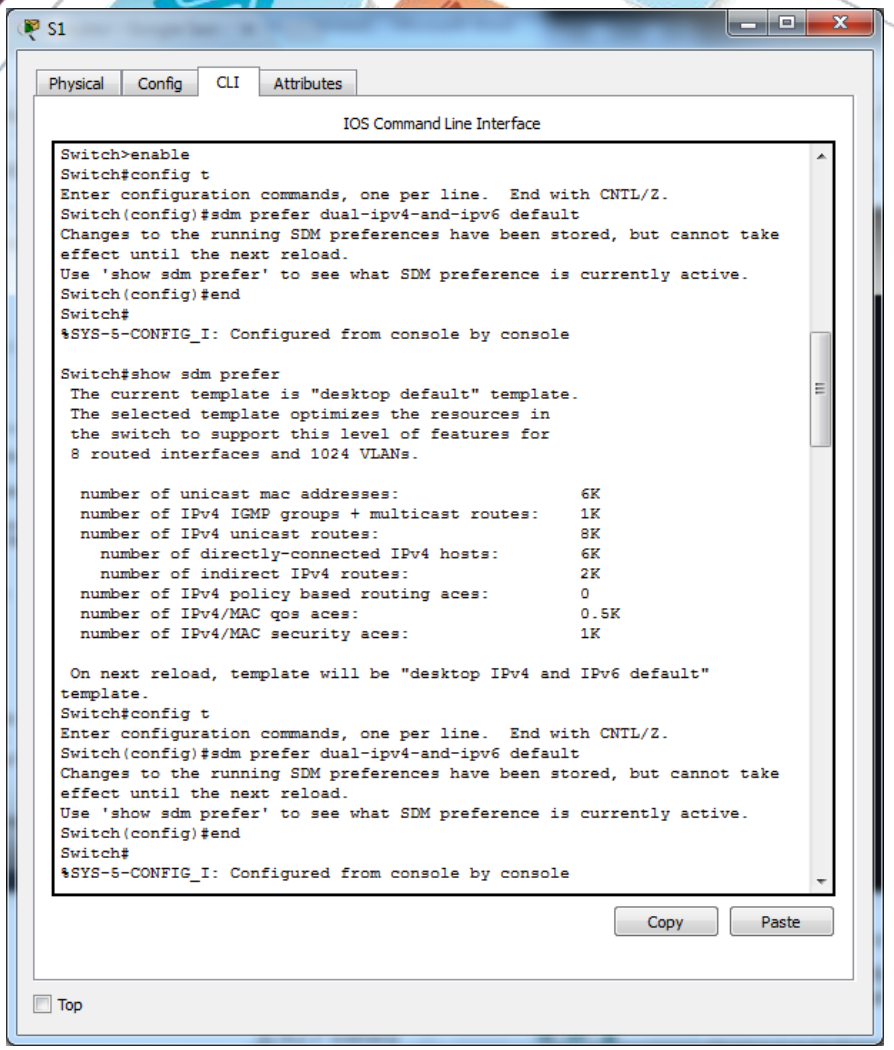
Nota: asegúrese de que el router y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota: la plantilla **default bias** que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla **dual-ipv4-and-ipv6** o la plantilla **lanbase-routing** en SDM. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

```
S1# show sdm prefer
```

Siga estos pasos para asignar la plantilla **dual-ipv4-and-ipv6** como la plantilla de SDM predeterminada:

```
S1# config t
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```



Ejecutamos el comando **show sdm prefer** seguido de la configuración mostrada.

Recursos necesarios

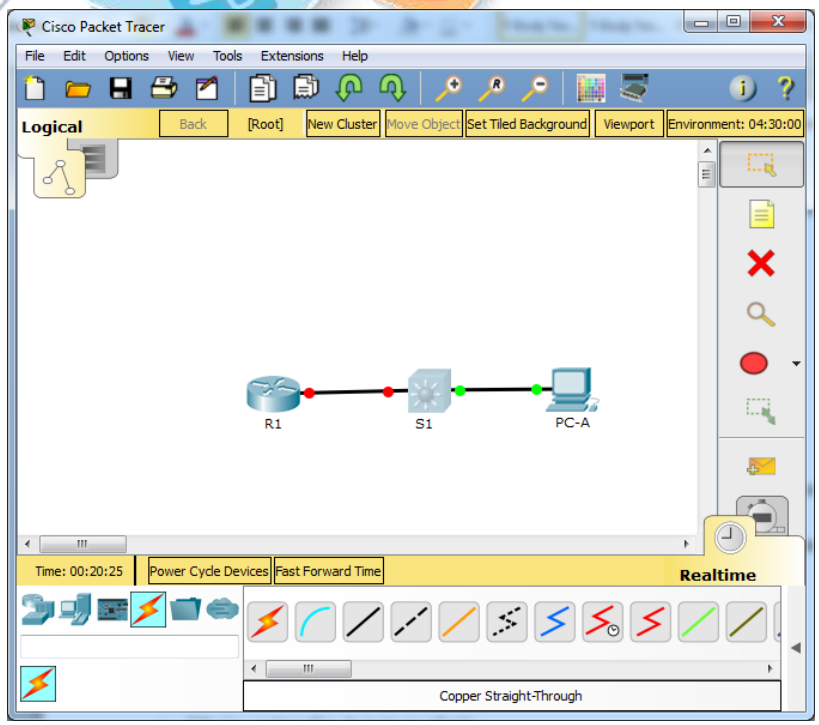
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Nota: los servicios de cliente DHCPv6 están deshabilitados en Windows XP. Se recomienda usar un host con Windows 7 para esta práctica de laboratorio.

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos de configuración, como los nombres de dispositivos, las contraseñas y las direcciones IP de interfaz.

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

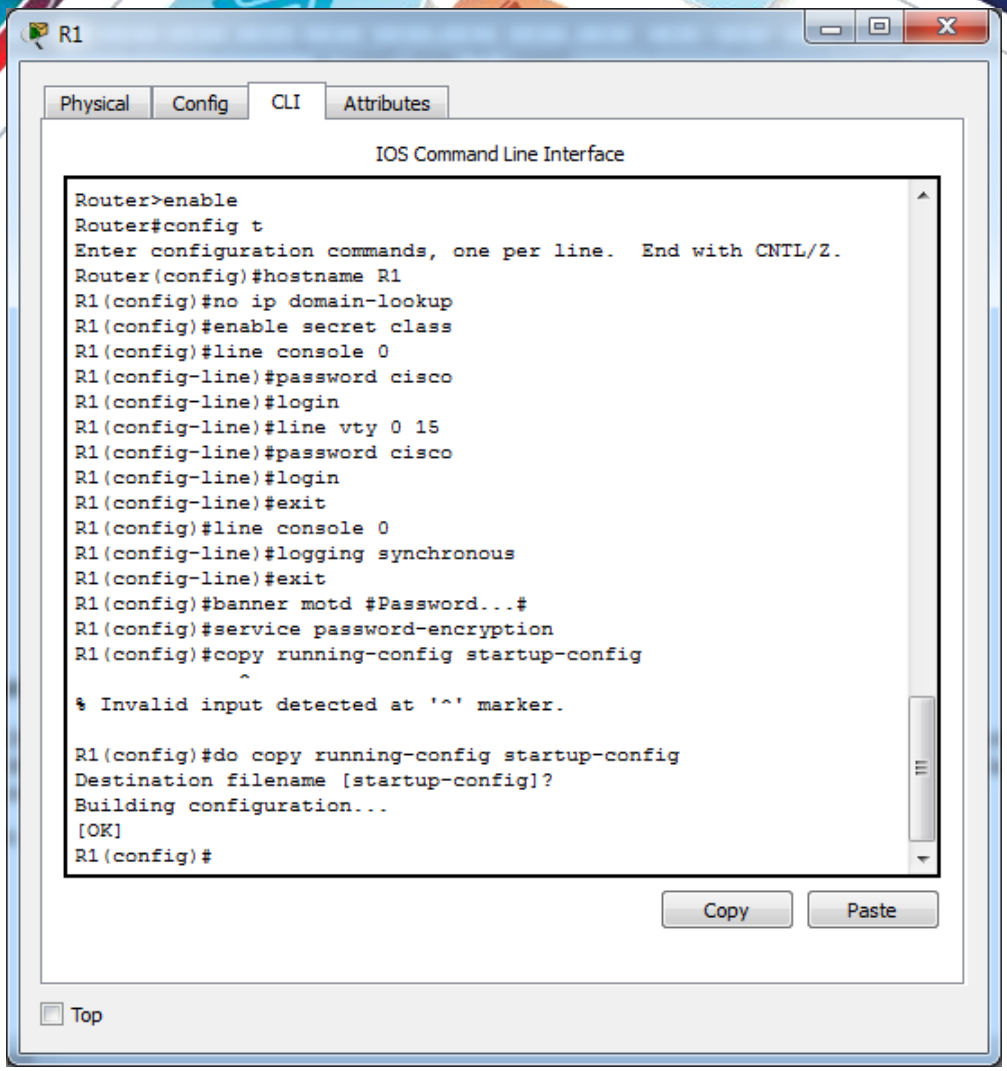


Realizamos la topología junto con el cableado.

Step 2: inicializar y volver a cargar el router y el switch según sea necesario.

Step 3: Configurar R1

a. Desactive la búsqueda del DNS.
b. Configure el nombre del dispositivo.
c. Cifre las contraseñas de texto no cifrado.
d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
g. Establezca el inicio de sesión de consola en modo sincrónico.
h. Guardar la configuración en ejecución en la configuración de inicio.



Configuramos el router R1 con todas las especificaciones dadas.

Step 4: configurar el S1.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo.

c. Cifre las contraseñas de texto no cifrado.

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

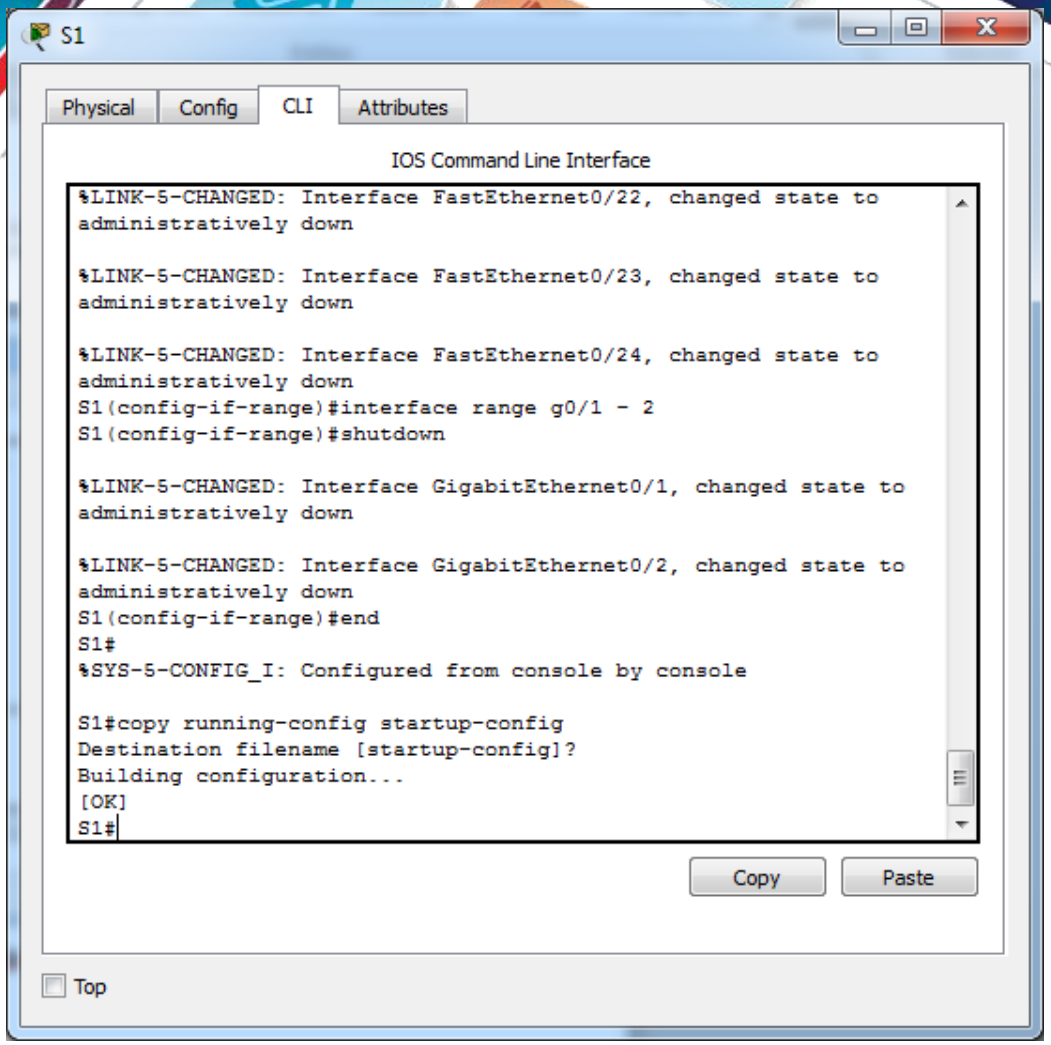
e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

g. Establezca el inicio de sesión de consola en modo sincrónico.

h. Desactive administrativamente todas las interfaces inactivas.

i. Guarde la configuración en ejecución en la configuración de inicio.

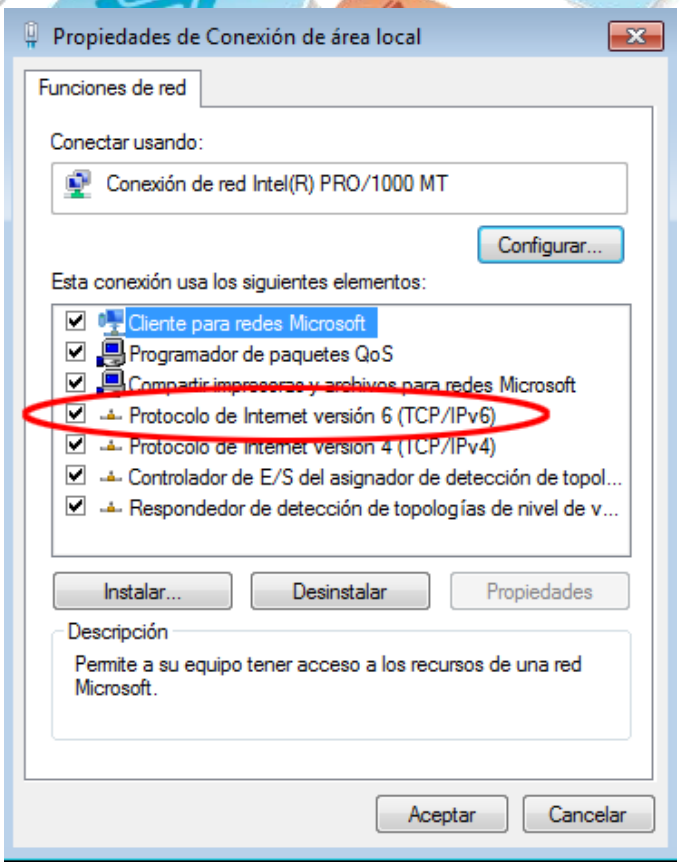


Configuramos el switch S1 con todas las especificaciones dadas.

Parte 3: configurar la red para SLAAC

Step 5: preparar la PC-A.

a. Verifique que se haya habilitado el protocolo IPv6 en la ventana Propiedades de conexión de área local. Si la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) no está marcada, haga clic para activarla.

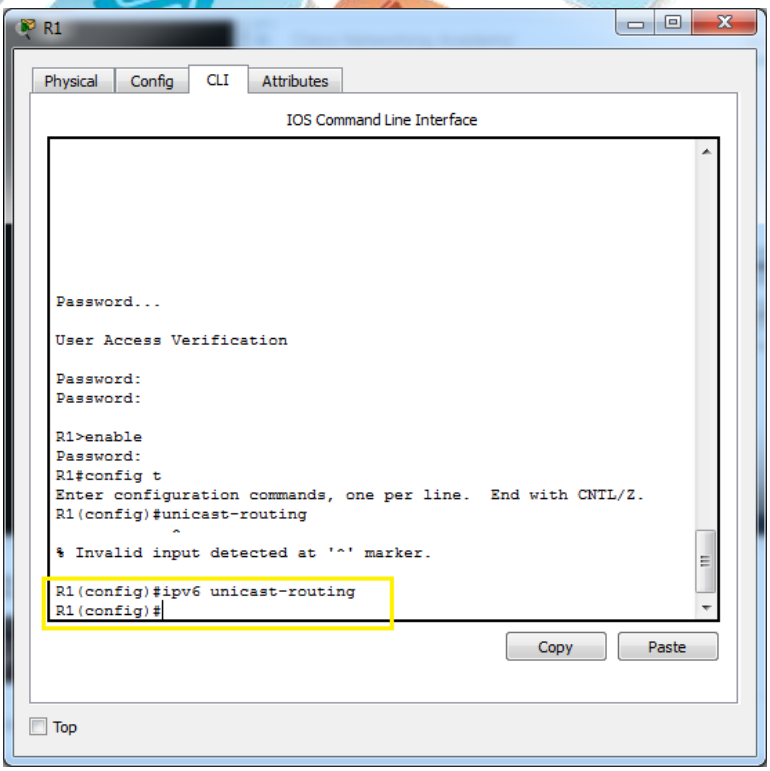


b. Inicie una captura del tráfico en la NIC con Wireshark.

c. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes. La entrada de filtro que se usa con Wireshark es **ipv6.dst==ff02::1**, como se muestra aquí.

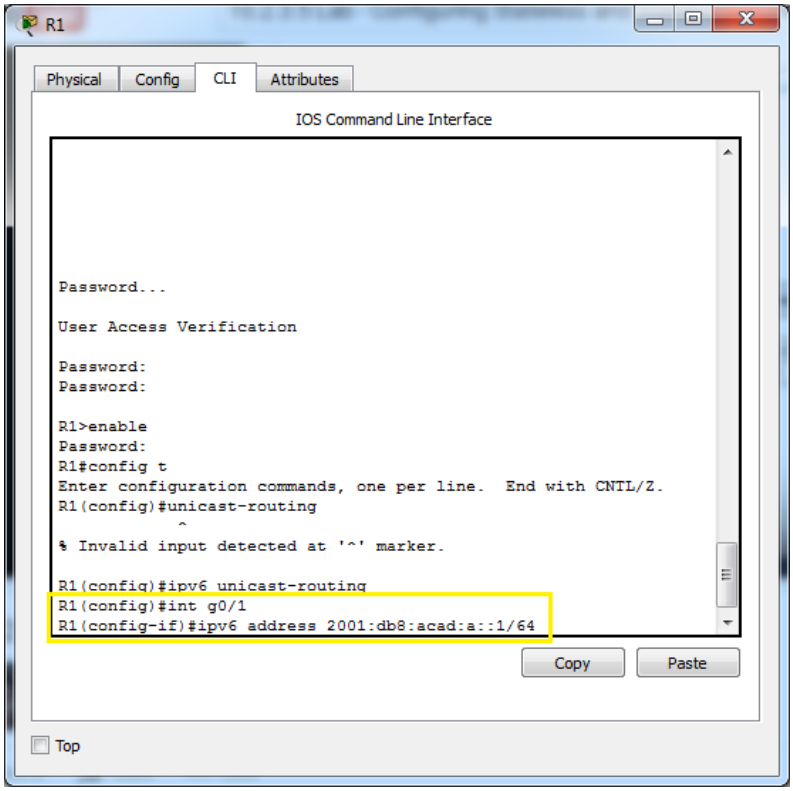
Step 6: Configurar R1

a. Habilite el routing de unidifusión IPv6.



Configuramos la unificación del IPv6 al R1

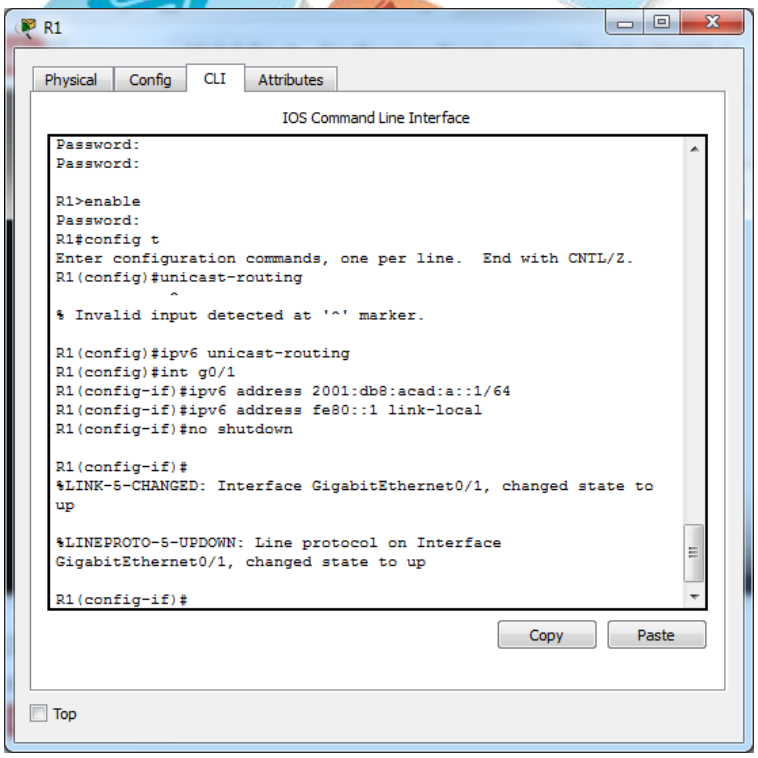
b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.



Configuramos la dirección IPv6 al R1

c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.

d. Active la interfaz G0/1.

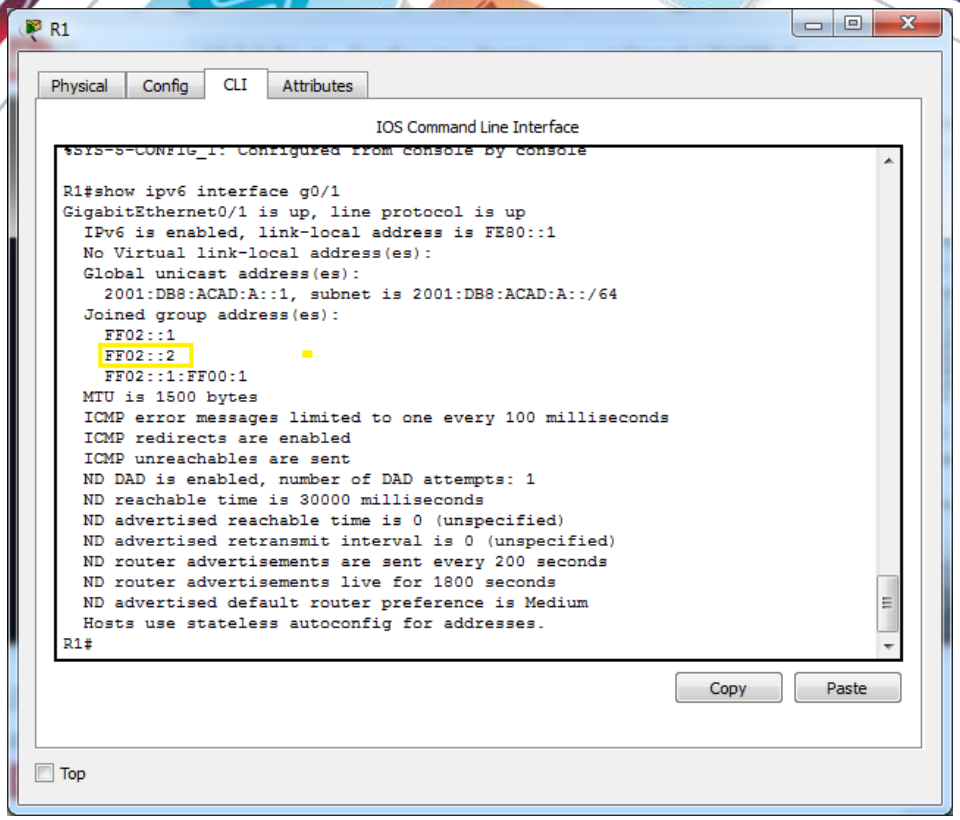


Configuramos la link-local y activamos el puerto.

Step 7: verificar que el R1 forme parte del grupo de multidifusión de todos los routers.

Use el comando **show ipv6 interface g0/1** para verificar que G0/1 forme parte del grupo de multidifusión de todos los routers (FF02::2). Los mensajes RA no se envían por G0/1 sin esa asignación de grupo.

R1# **show ipv6 interface g0/1**
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.

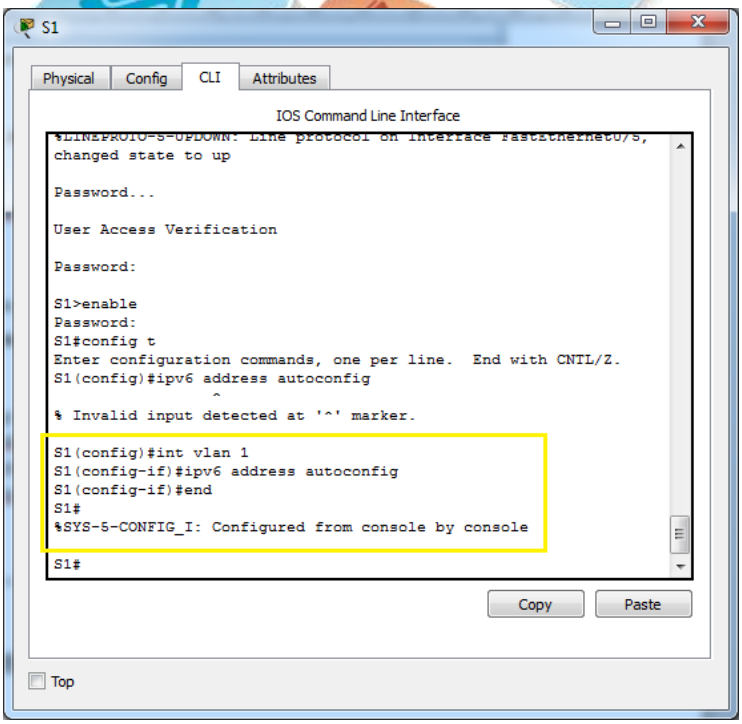


Verificamos que el puerto G0/1 forma parte de la multidifusión

Step 8: configurar el S1.

Use el comando **ipv6 address autoconfig** en la VLAN 1 para obtener una dirección IPv6 a través de SLAAC.

S1(config)# **interface vlan 1**
S1(config-if)# **ipv6 address autoconfig**
S1(config-if)# **end**

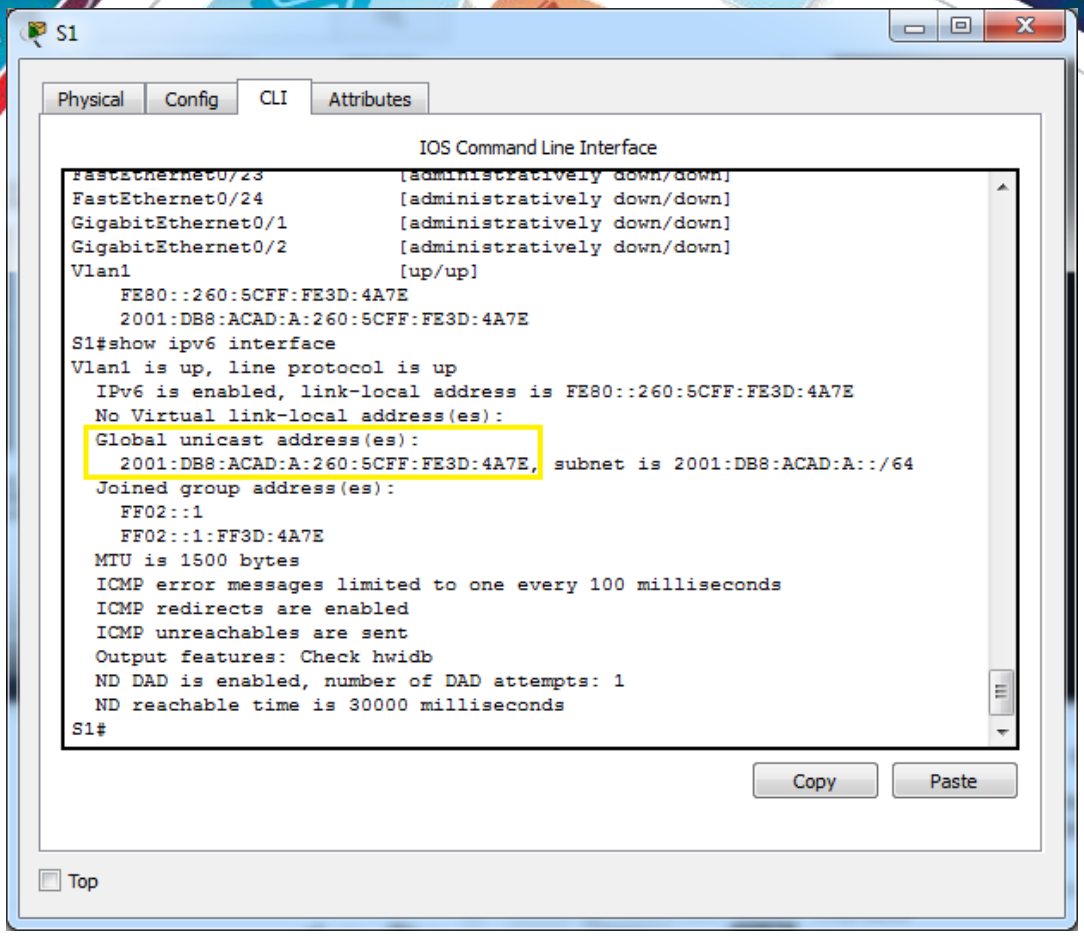


Obtenemos la SLAAC del S1

Step 9: verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

Use el comando **show ipv6 interface** para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

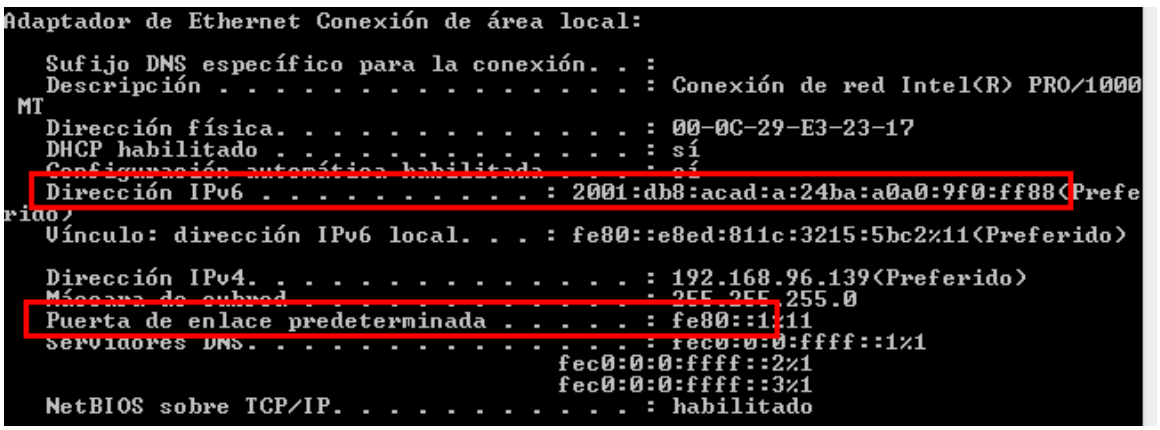
S1# **show ipv6 interface**
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
No Virtual link-local address(es):
Stateless address autoconfig enabled
Global unicast address(es):
2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]
valid lifetime 2591988 preferred lifetime 604788
Joined group address(es):
FF02::1
FF02::1:FFE8:8A40
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
Output features: Check hwidb
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
Default router is FE80::1 on Vlan1

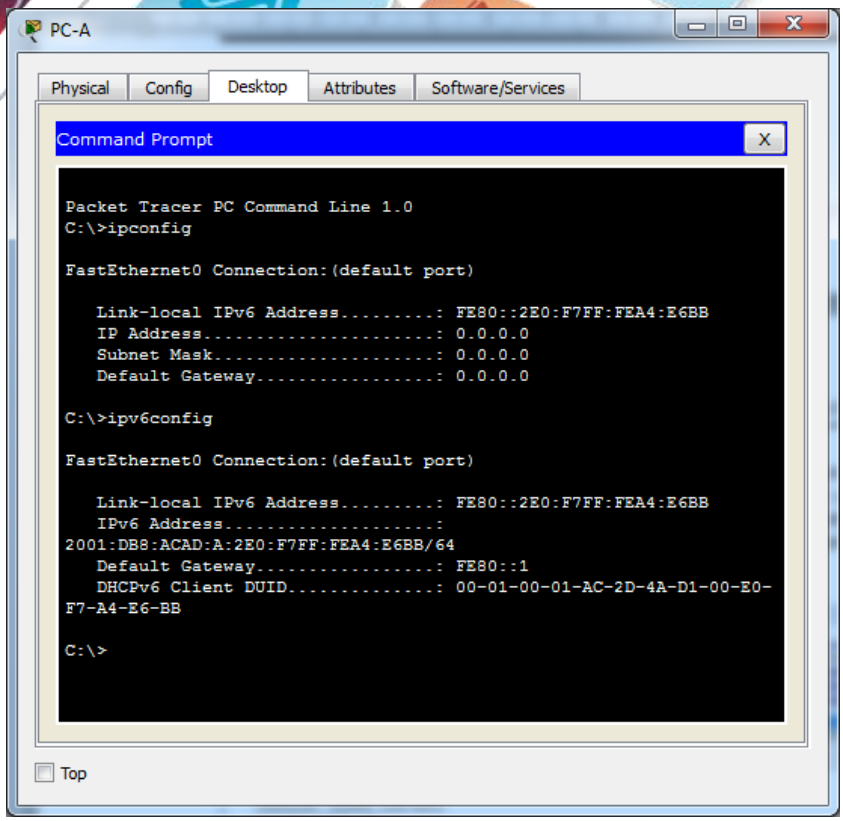


Verificamos la SLAAC proporcionada.

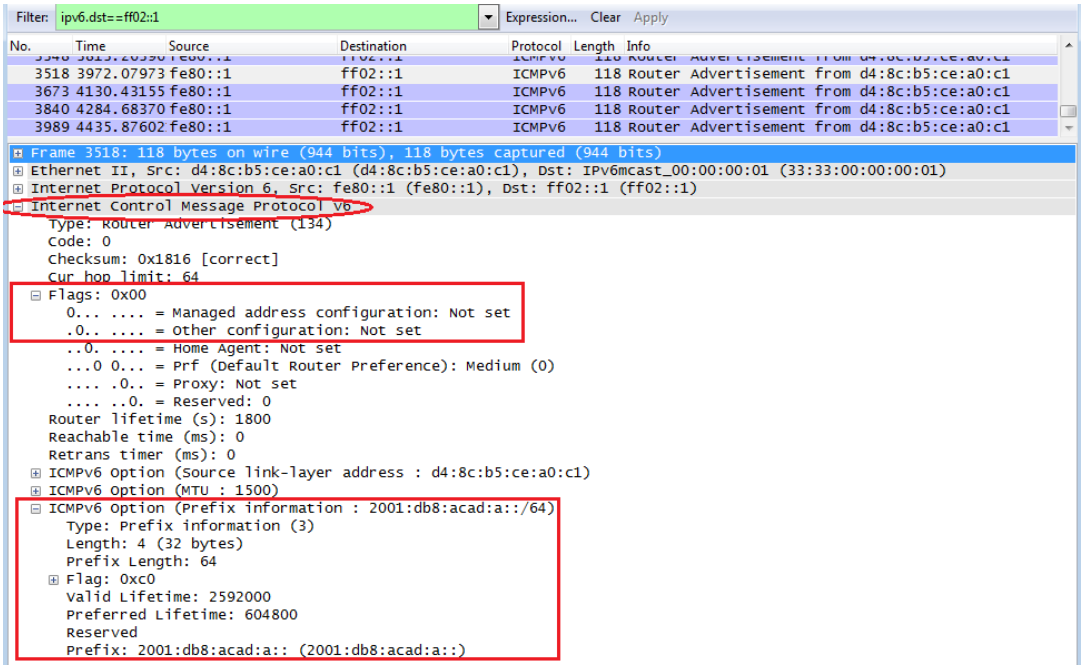
Step 10: Verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

a. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all**. Verifique que la PC-A muestre una dirección IPv6 con el prefijo 2001:db8:acad:a::/64. El gateway predeterminado debe tener la dirección FE80::1.





b. En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.



Parte 3: configurar la red para DHCPv6 sin estado

Step 11: configurar un servidor de DHCP IPv6 en el R1.

a. Cree un pool de DHCP IPv6.

R1(config)# **ipv6 dhcp pool IPV6POOL-A**

b. Asigne un nombre de dominio al pool.

R1(config-dhcpv6)# **domain-name ccna-statelessDHCPv6.com**

c. Asigne una dirección de servidor DNS.

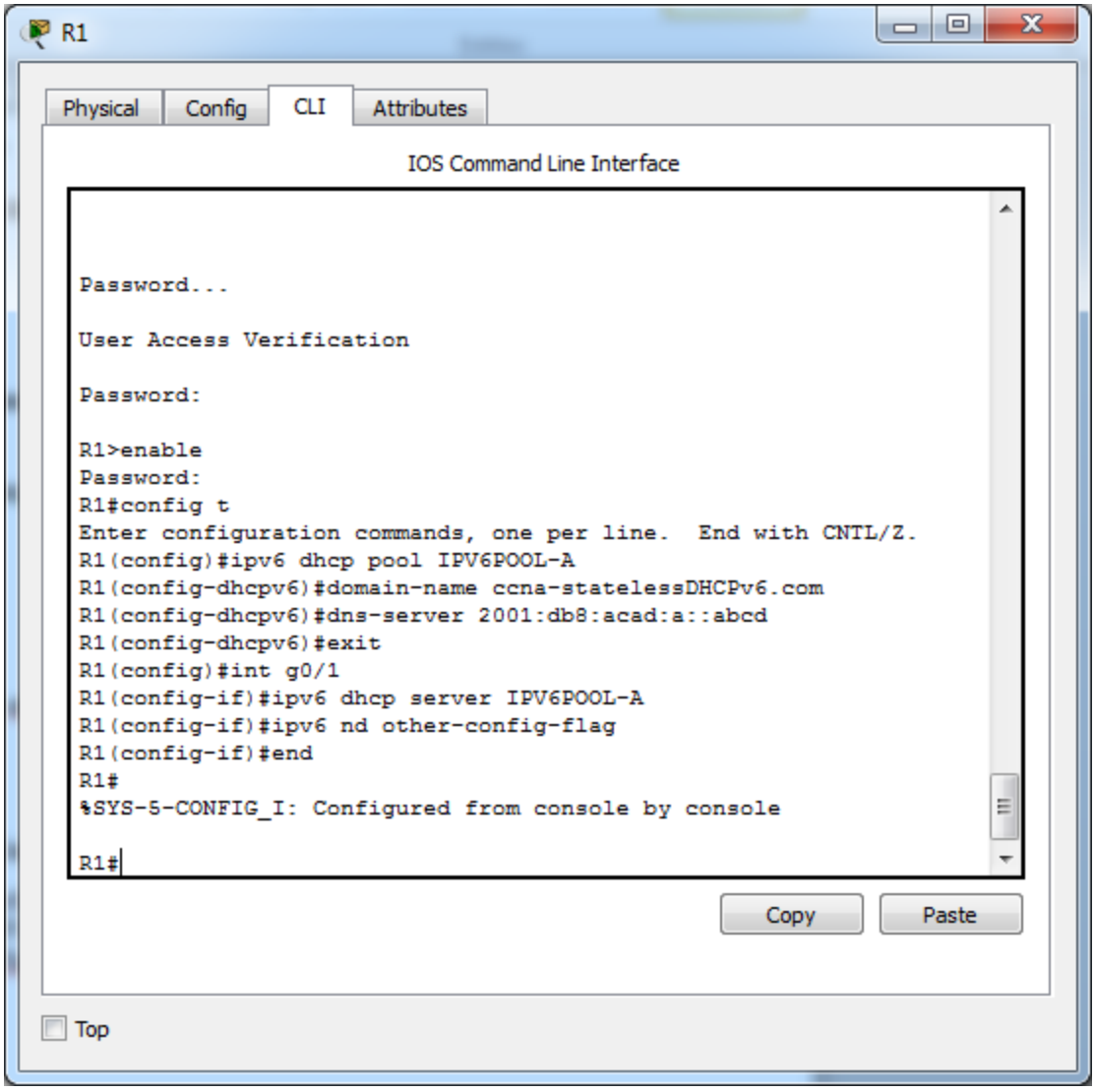
R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**
R1(config-dhcpv6)# **exit**

d. Asigne el pool de DHCPv6 a la interfaz.

R1(config)# **interface g0/1**
R1(config-if)# **ipv6 dhcp server IPV6POOL-A**

e. Establezca la detección de redes (ND) DHCPv6 **other-config-flag**.

R1(config-if)# **ipv6 nd other-config-flag**
R1(config-if)# **end**

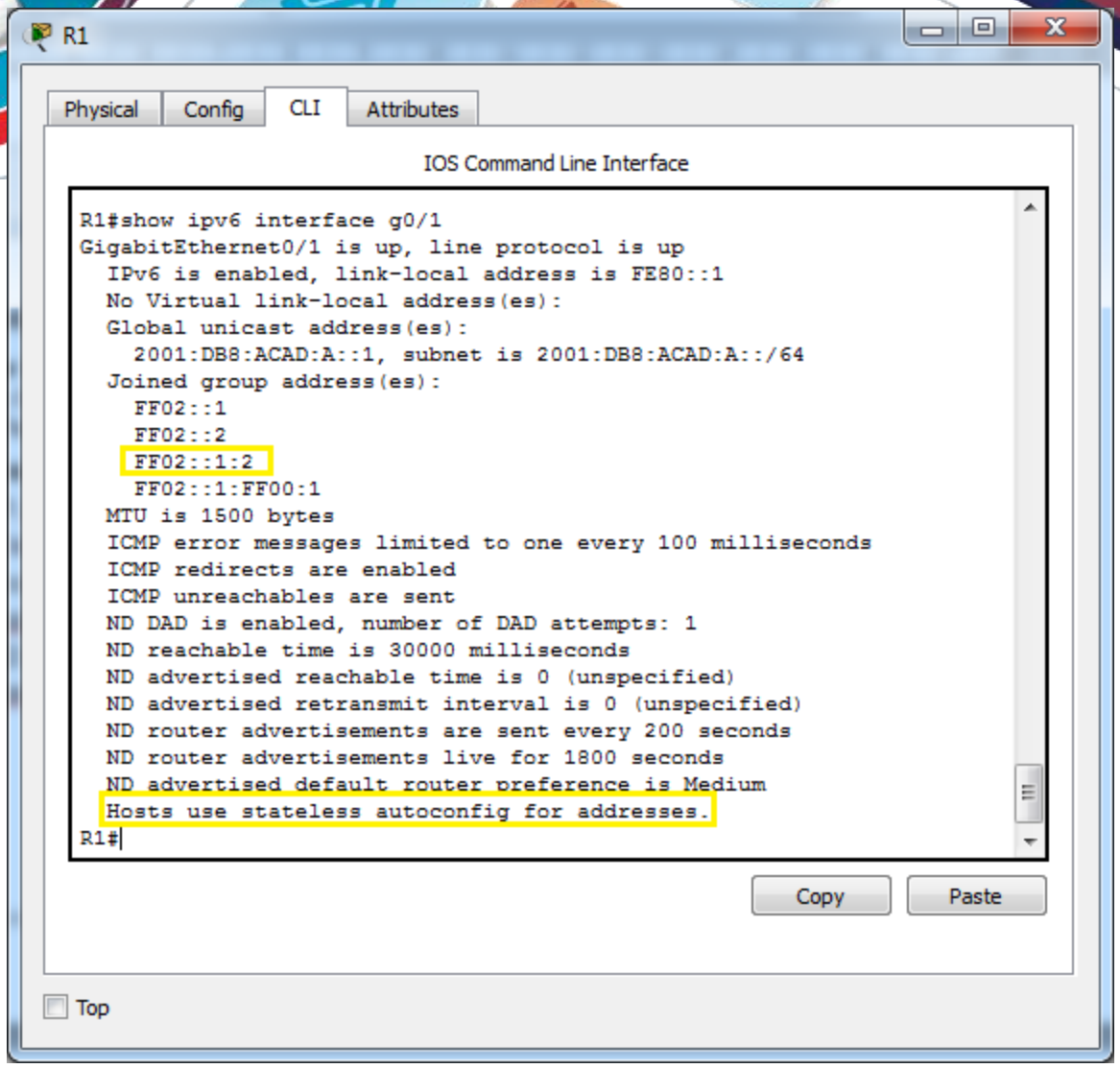


Configuramos el servidor DHCPv6 sin estado

Step 12: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

Use el comando **show ipv6 interface g0/1** para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando **show** verifica que se haya establecido other-config-flag.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:2
    FF02::1:FF00:1
    FF05::1:3
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
  Hosts use DHCP to obtain other configuration.
```

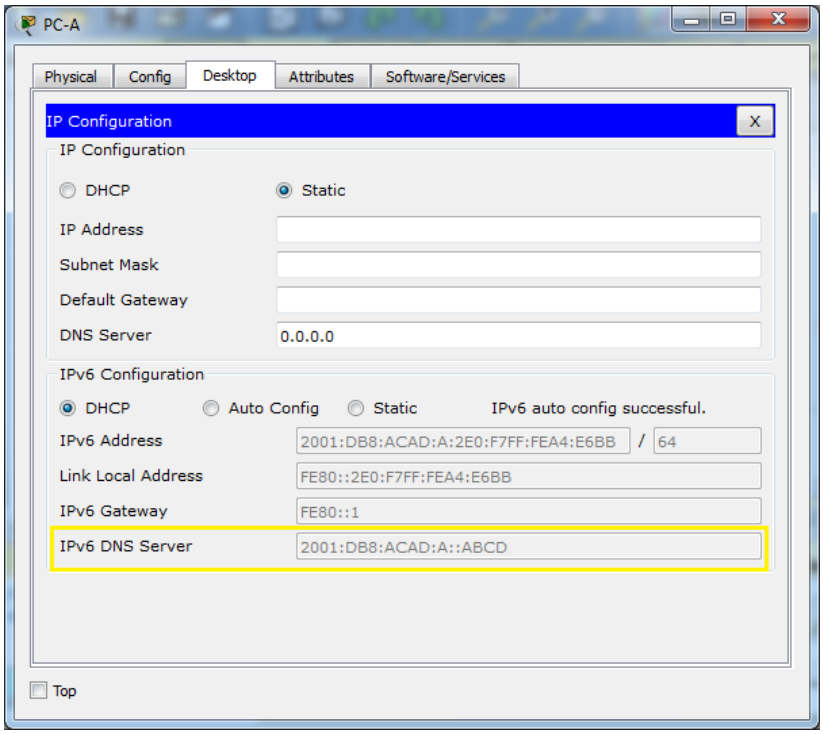


Verificamos la configuración de DHCPv6 en la interfaz G0/1 del R1

Step 13: ver los cambios realizados en la red en la PC-A.

Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente mediante SLAAC.

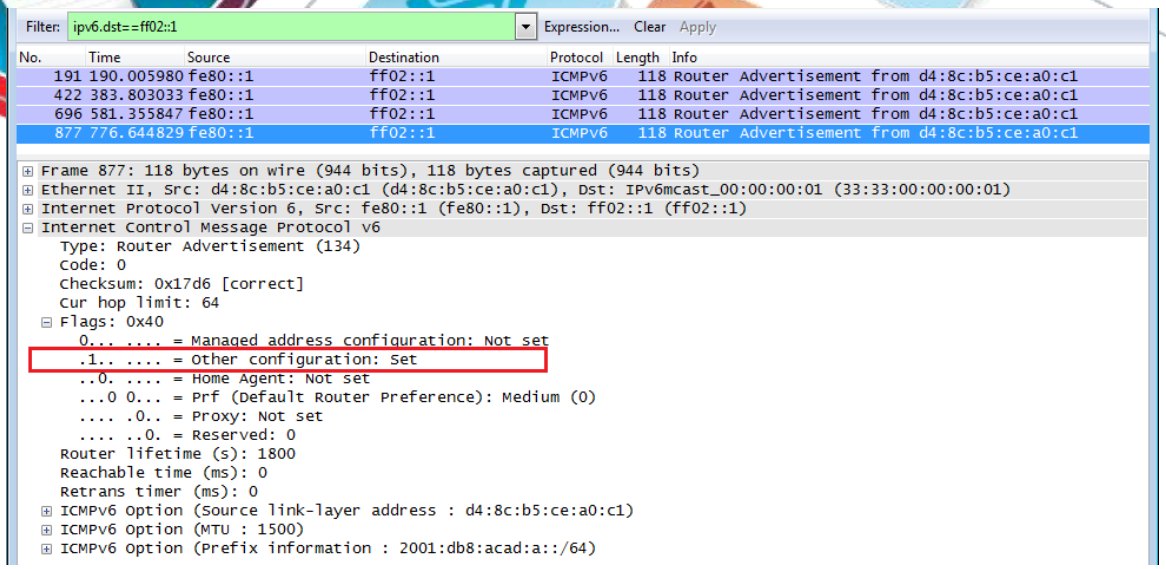
```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : ccna-statelessDHCPv6.com
   Descripción . . . . . . . . . . . . . . . : Conexión de red Intel(R) PRO/1000
 MT
   Dirección física. . . . . . . . . . . . . : 00-0C-29-E3-23-17
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 192.168.96.139(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::1%11
   IAID DHCPv6 . . . . . . . . . . . . . . . : 234884137
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-
E3-23-17
   Servidores DNS. . . . . . . . . . . . . . : 2001:db8:acad:a::abcd
   NetBIOS sobre TCP/IP. . . . . . . . . . . : Habilitado

Adaptador de túnel isatap.localdomain:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . : ccna-statelessDHCPv6.com
   Descripción . . . . . . . . . . . . . . . : Adaptador ISATAP de Microsoft
   Dirección física. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí
```



En la PC-A se asignó automáticamente la IPv6 DNS Server

Step 14: ver los mensajes RA en Wireshark.

Desplácese hasta el último mensaje RA que se muestra en Wireshark y expándalo para ver la configuración de indicadores ICMPv6. Observe que el indicador Other configuration (Otra configuración) está establecido en 1.



Step 15: verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.

Use los comandos **show ipv6 dhcp binding** y **show ipv6 dhcp pool** para verificar que la PC-A no haya obtenido una dirección IPv6 del pool de DHCPv6.

R1# **show ipv6 dhcp binding**

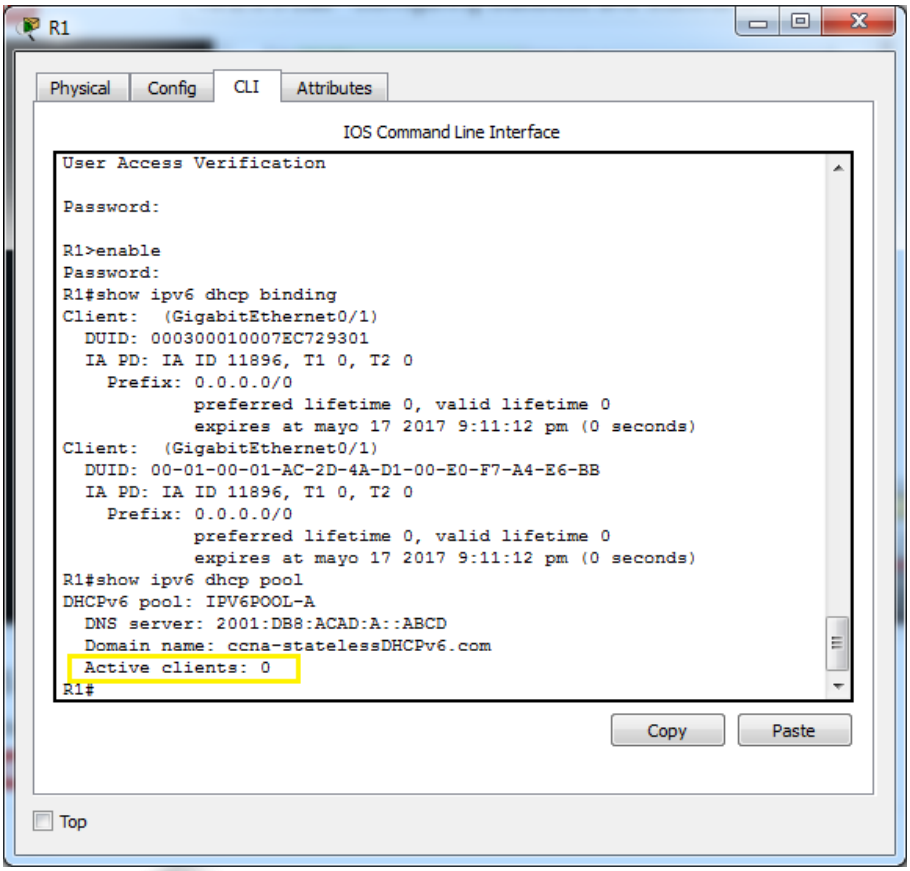
R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-statelessDHCPv6.com

Active clients: 0



Verificamos que la dirección IPv6 de la PC-A del POOL

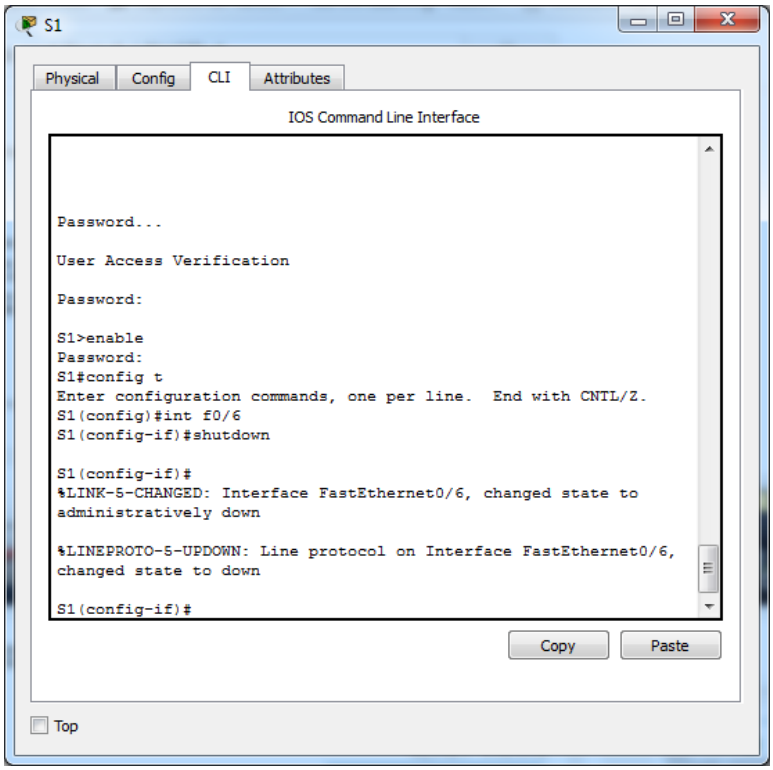
Step 16: restablecer la configuración de red IPv6 de la PC-A.

a. Desactive la interfaz F0/6 del S1.

Nota: la desactivación de la interfaz F0/6 evita que la PC-A reciba una nueva dirección IPv6 antes de que usted vuelva a configurar el R1 para DHCPv6 con estado en la parte 4.

S1(config)# **interface f0/6**

S1(config-if)# **shutdown**



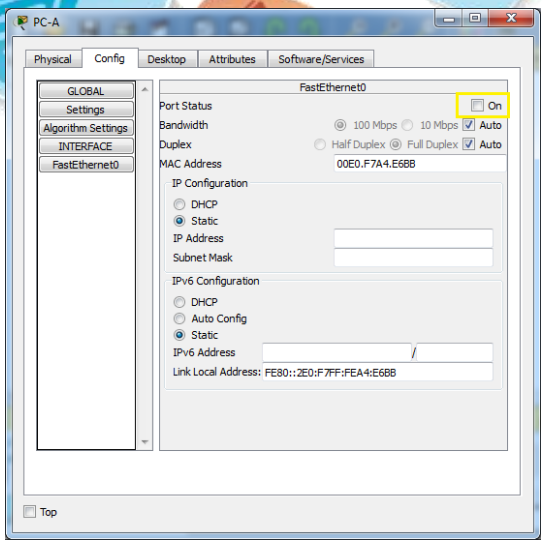
Desactivamos el puerto F0/6 del Switch S1

b. Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.

c. Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.

1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.

2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.



Parte 4: configurar la red para DHCPv6 con estado

Step 17: preparar la PC-A.

a. Inicie una captura del tráfico en la NIC con Wireshark.

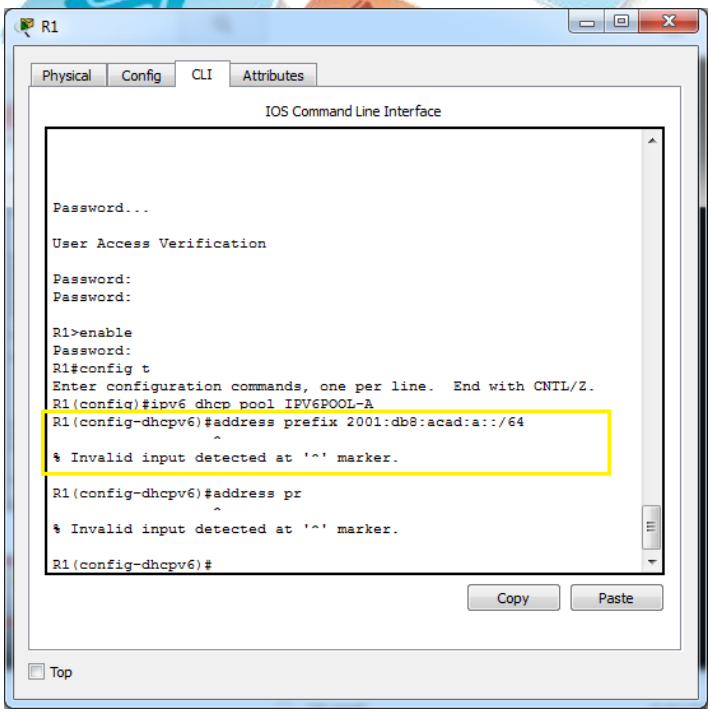
b. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes.

Step 18: cambiar el pool de DHCPv6 en el R1.

a. Agregue el prefijo de red al pool.

R1(config)# **ipv6 dhcp pool IPV6POOL-A**

R1(config-dhcpv6)# **address prefix 2001:db8:acad:a::/64**

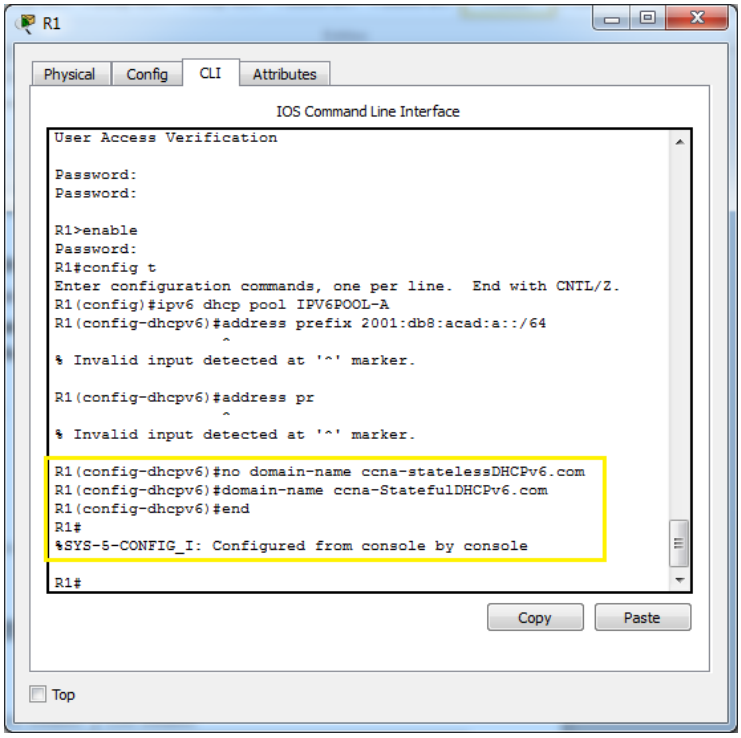


Packet Tracer No soporta el comando **address prefix 2001:db8:acad:a::/64**

b. Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.

Nota: debe eliminar el antiguo nombre de dominio. El comando **domain-name** no lo reemplaza.

R1(config-dhcpv6)# **no domain-name ccna-statelessDHCPv6.com**
R1(config-dhcpv6)# **domain-name ccna-StatefulDHCPv6.com**
R1(config-dhcpv6)# **end**



Cambiamos el nombre del dominio

c. Verifique la configuración del pool de DHCPv6.

R1# **show ipv6 dhcp pool**

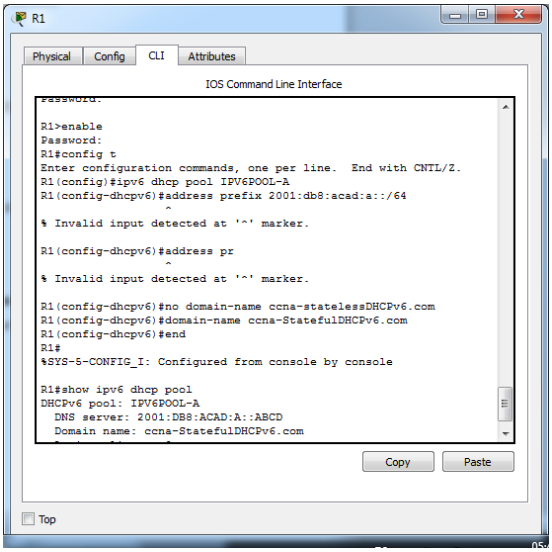
DHCPv6 pool: IPV6POOL-A

Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (0 in use, 0 conflicts)

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-StatefulDHCPv6.com

Active clients: 0

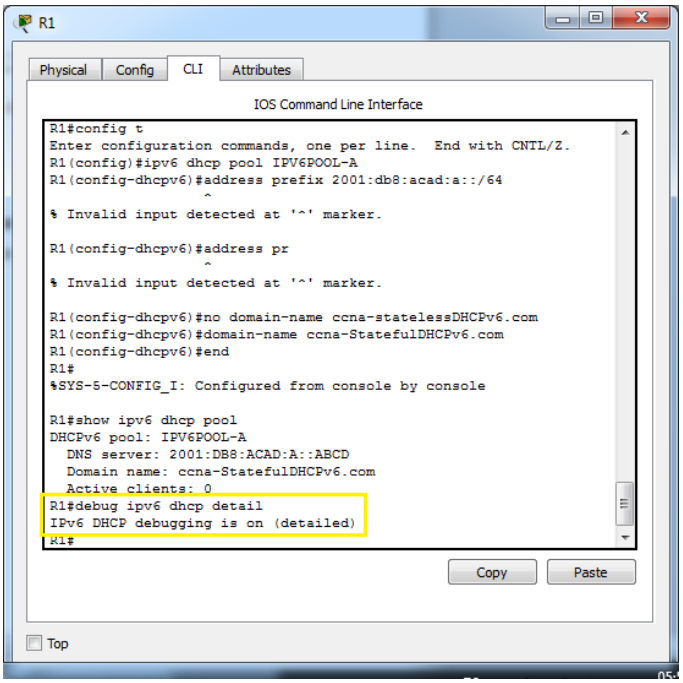


Ejecutamos el comando **show ipv6 dhcp pool**

d. Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

R1# **debug ipv6 dhcp detail**

IPv6 DHCP debugging is on (detailed)

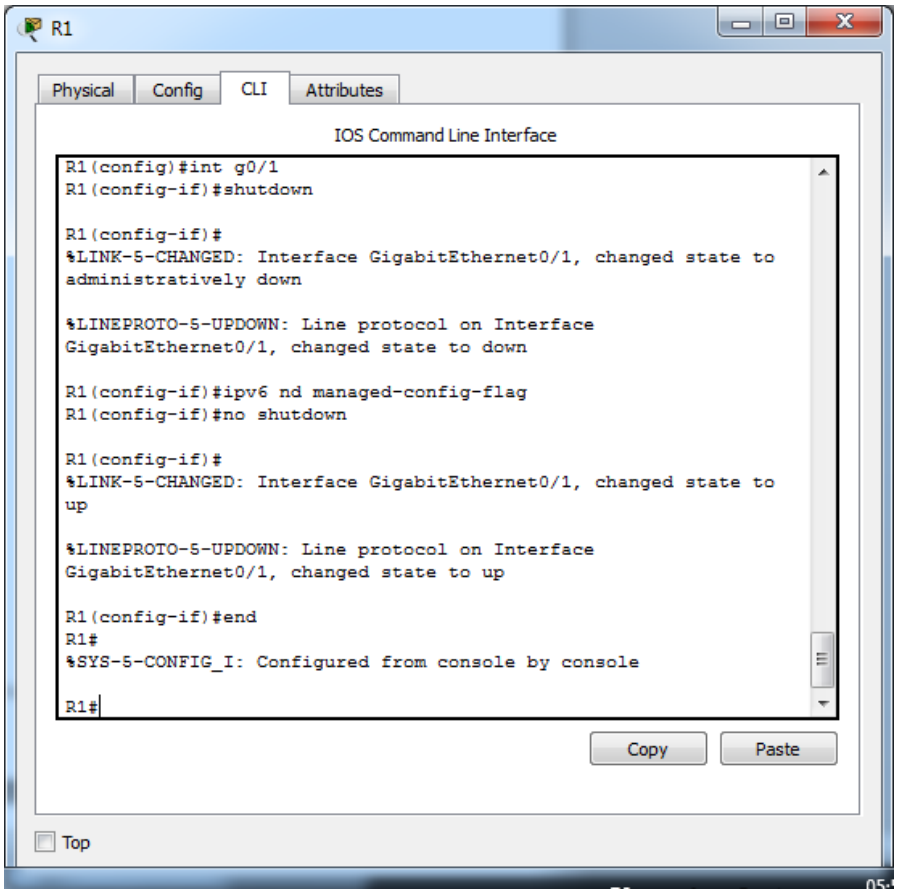


Ejecutamos el comando **debug ipv6 dhcp detail**

Step 19: establecer el indicador en G0/1 para DHCPv6 con estado.

Nota: la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.

R1(config)# **interface g0/1**
R1(config-if)# **shutdown**
R1(config-if)# **ipv6 nd managed-config-flag**
R1(config-if)# **no shutdown**
R1(config-if)# **end**

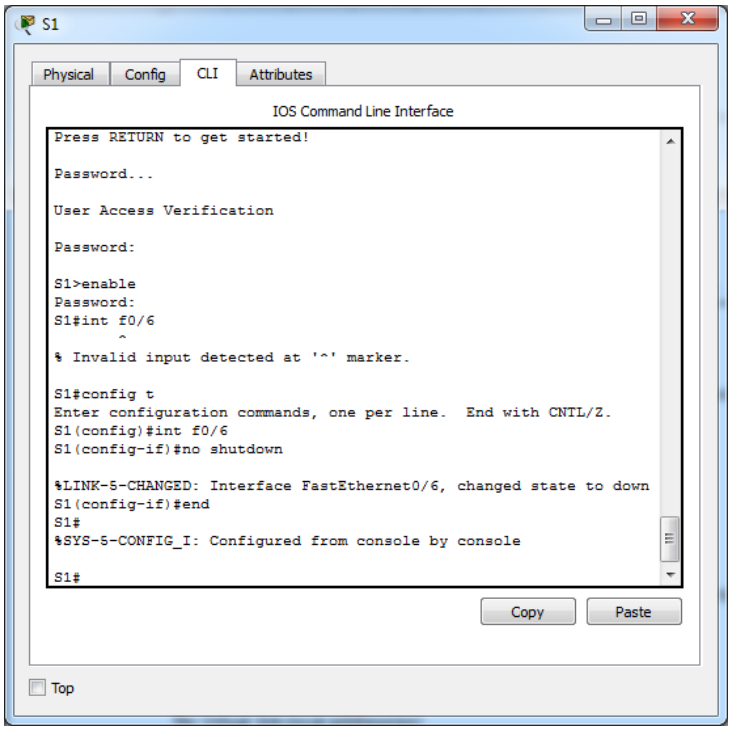


Configuramos el puerto G0/1

Step 20: habilitar la interfaz F0/6 en el S1.

Ahora que configuró el R1 para DHCPv6 con estado, puede volver a conectar la PC-A a la red activando la interfaz F0/6 en el S1.

S1(config)# **interface f0/6**
S1(config-if)# **no shutdown**
S1(config-if)# **end**



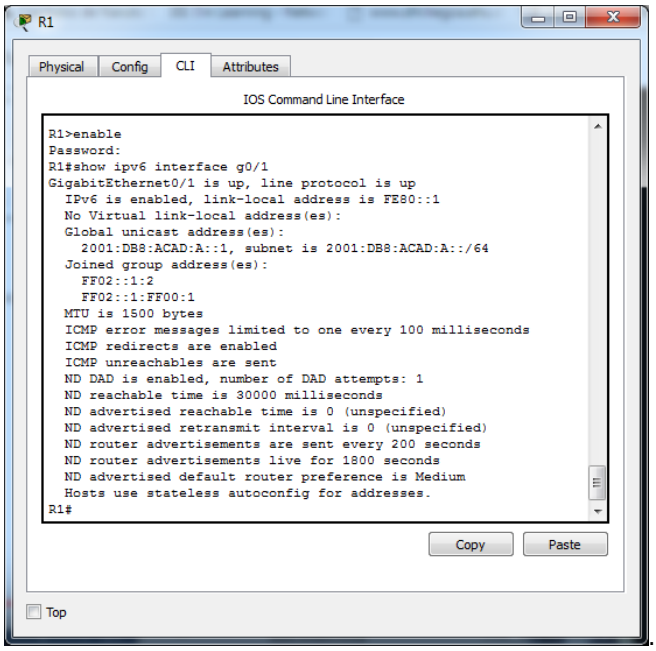
Encendemos el puerto F0/6 en el Switch S1

Step 21: verificar la configuración de DHCPv6 con estado en el R1.

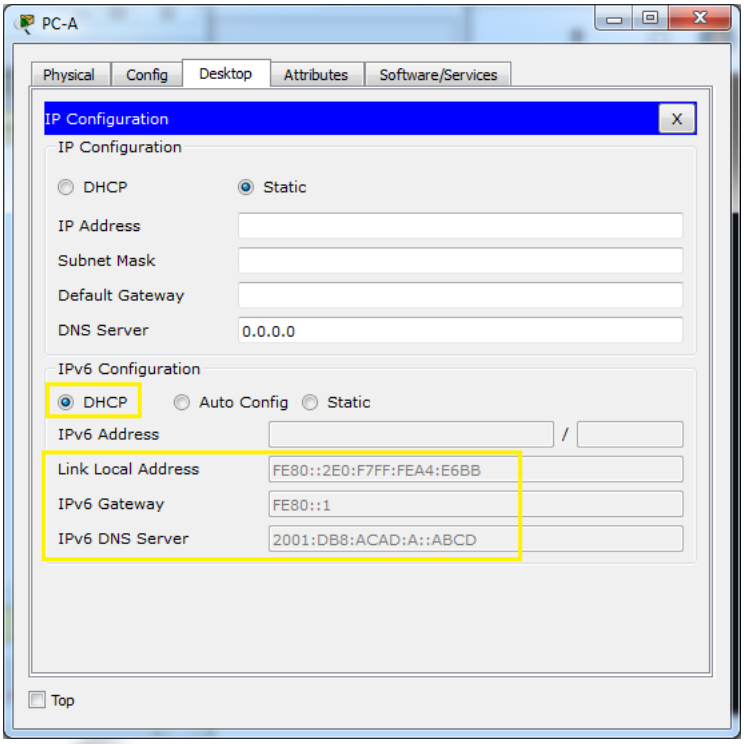
a. Emita el comando **show ipv6 interface g0/1** para verificar que la interfaz esté en el modo DHCPv6 con estado.

R1# **show ipv6 interface g0/1**
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:2
FF02::1:FF00:1
FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.



b. En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.



La PC-A obtiene la IPv6 de la puerta de enlace y la IPv6 del DNS server.

La PC-A no posee un dirección IPv6 porque el comando **address prefix 2001:db8:acad:a::/64** no lo permite ejecutar Packet Tracer

c. Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

R1# **show ipv6 dhcp pool**

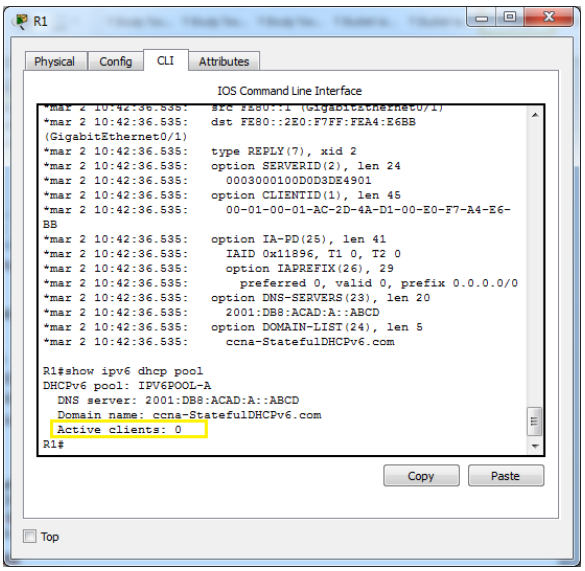
DHCPv6 pool: IPV6POOL-A

Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (1 in use, 0 conflicts)

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-StatefulDHCPv6.com

Active clients: 1



d. Emita el comando **show ipv6 dhcp binding** para verificar que la PC-A haya recibido su dirección IPv6 de unidifusión del pool de DHCP. Compare la dirección de cliente con la dirección IPv6 link-local en la PC-A mediante el comando **ipconfig /all**. Compare la dirección proporcionada por el comando **show** con la dirección IPv6 que se indica con el comando **ipconfig /all** en la PC-A.

R1# **show ipv6 dhcp binding**

Client: FE80::D428:7DE2:997C:B05A

DUID: 0001000117F6723D000C298D5444

Username : unassigned

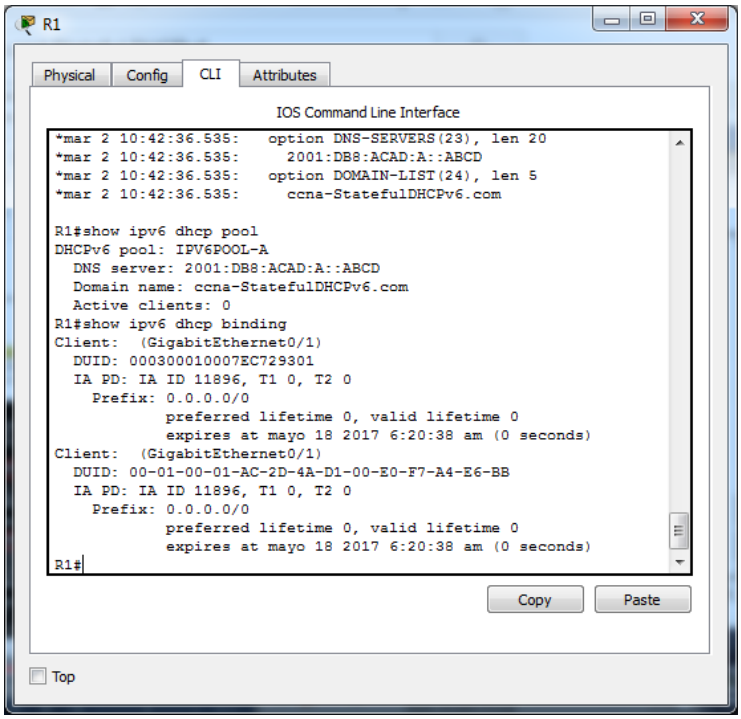
IA NA: IA ID 0x0E000C29, T1 43200, T2 69120

Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE

preferred lifetime 86400, valid lifetime 172800

expires at Mar 07 2013 04:09 PM (171595 seconds)

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : ccna-StatefulDHCPv6.com
   Descripción . . . . . . . . . . . . . . . : Conexión de red Intel(R) PRO/1000
 MT
   Dirección física. . . . . . . . . . . . . : 00-0C-29-E3-23-17
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce(Pref
erido)
   Concesión obtenida. . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:07:59
   La concesión expira . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:38:03
   Dirección IPv6 . . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a:11(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 192.168.96.139(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::1%11
   IAID DHCPv6 . . . . . . . . . . . . . . . : 234884137
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-
E3-23-17
   Servidores DNS. . . . . . . . . . . . . . : 2001:db8:acad:a::abcd
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```



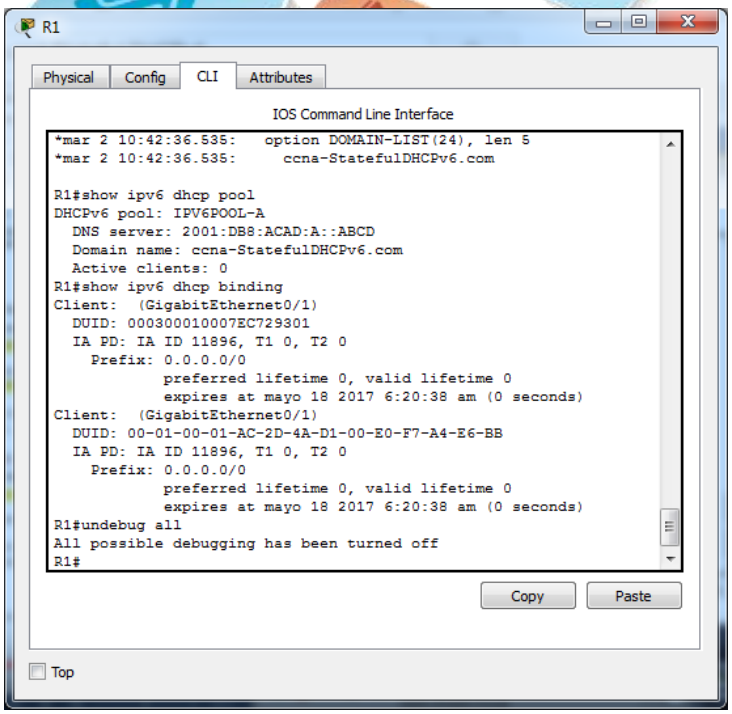
Ejecutamos el comando **show ipv6 dhcp binding**

e. Emita el comando **undebug all** en el R1 para detener la depuración de DHCPv6.

Nota: escribir **u all** es la forma más abreviada de este comando y sirve para saber si quiere evitar que los mensajes de depuración se desplacen hacia abajo constantemente en la pantalla de la sesión de terminal. Si hay varias depuraciones en proceso, el comando **undebug all** las detiene todas.

R1# **u all**

Se ha desactivado toda depuración posible



Ejecutamos el comando **undebug all**

f. Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.

1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents

*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

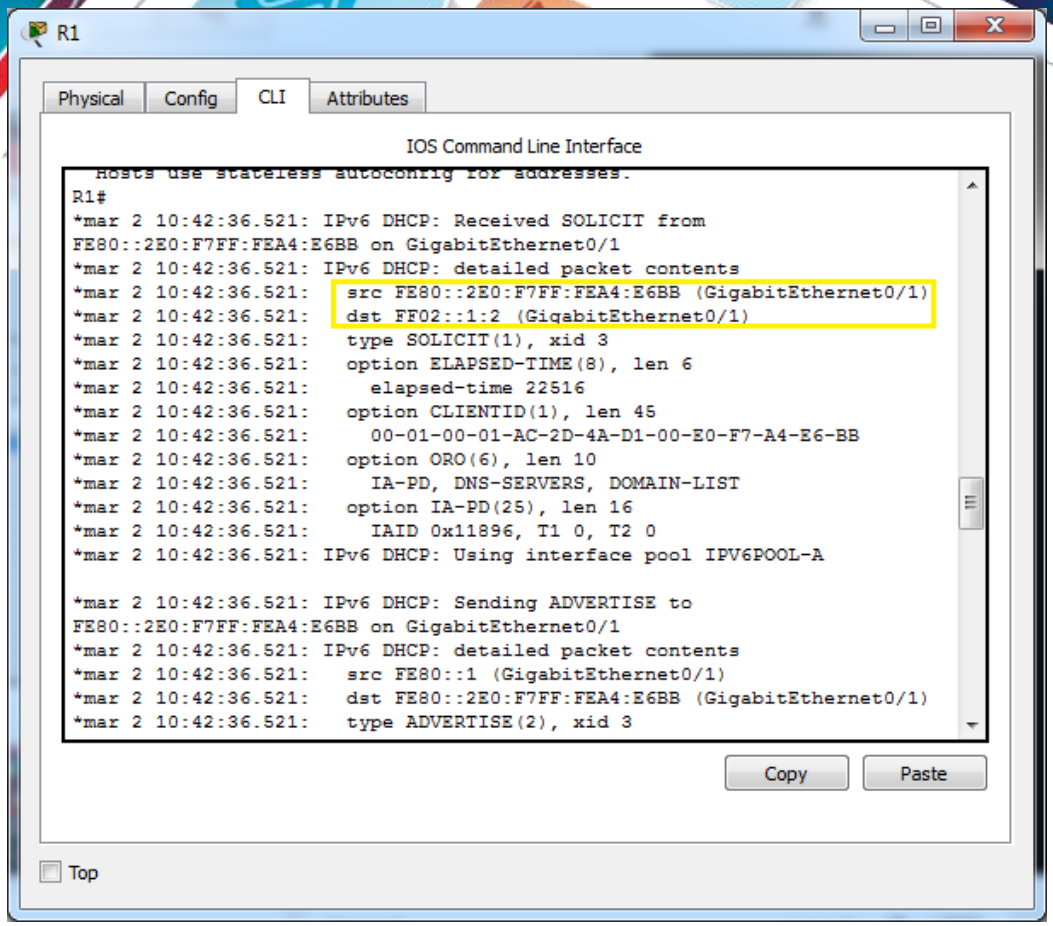
*Mar 5 16:42:39.775: dst FF02::1:2

*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238

*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2

*Mar 5 16:42:39.775: elapsed-time 6300

*Mar 5 16:42:39.775: option CLIENTID(1), len 14



Examinamos la solicitud de PC-A

2) Examine el mensaje de respuesta enviado a la PC-A con la información de red DHCP.

*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents

*Mar 5 16:42:39.779: src FE80::1

*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

*Mar 5 16:42:39.779: type REPLY(7), xid 1039238

*Mar 5 16:42:39.779: option SERVERID(2), len 10

*Mar 5 16:42:39.779: 00030001FC994775C3E0

*Mar 5 16:42:39.779: option CLIENTID(1), len 14

*Mar 5 16:42:39.779: 00010001

R1#17F6723D000C298D5444

*Mar 5 16:42:39.779: option IA-NA(3), len 40

*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120

*Mar 5 16:42:39.779: option IAADDR(5), len 24

*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE

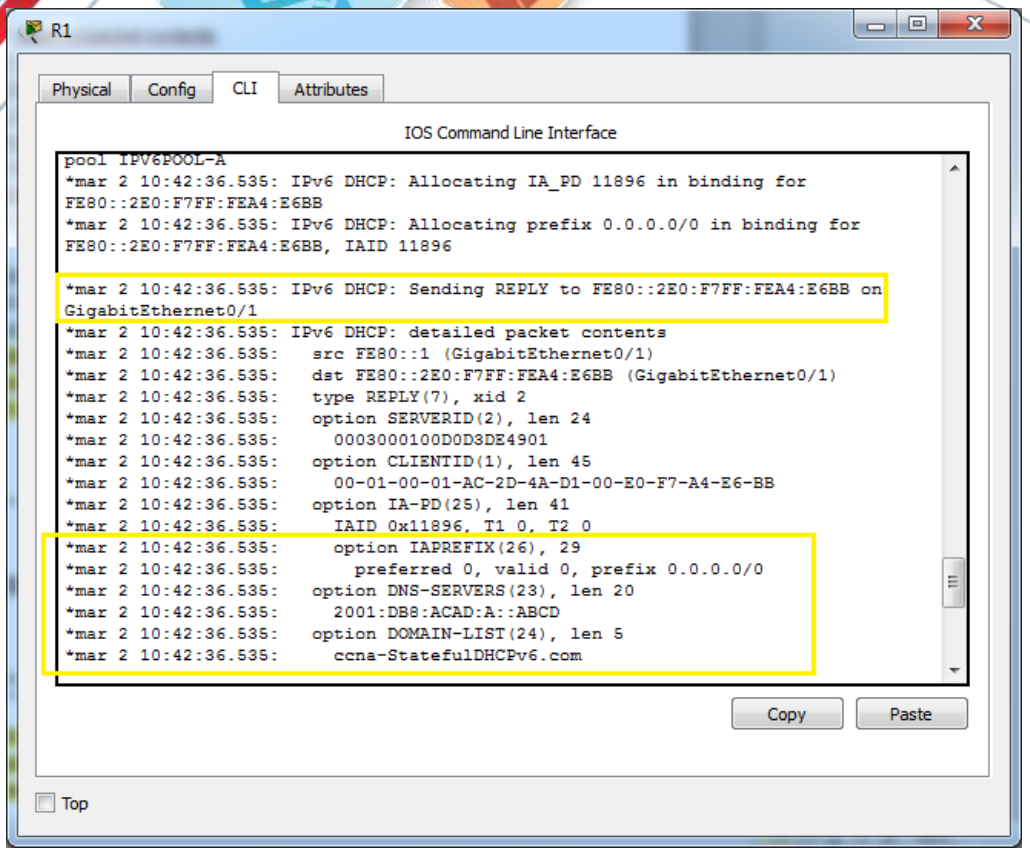
*Mar 5 16:42:39.779: preferred 86400, valid 172800

*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16

*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD

*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26

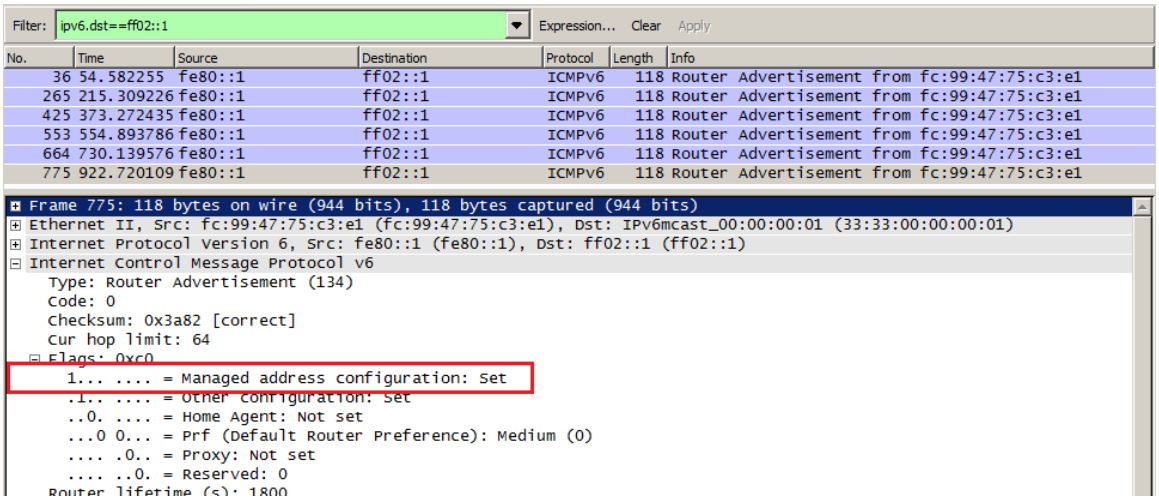
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com



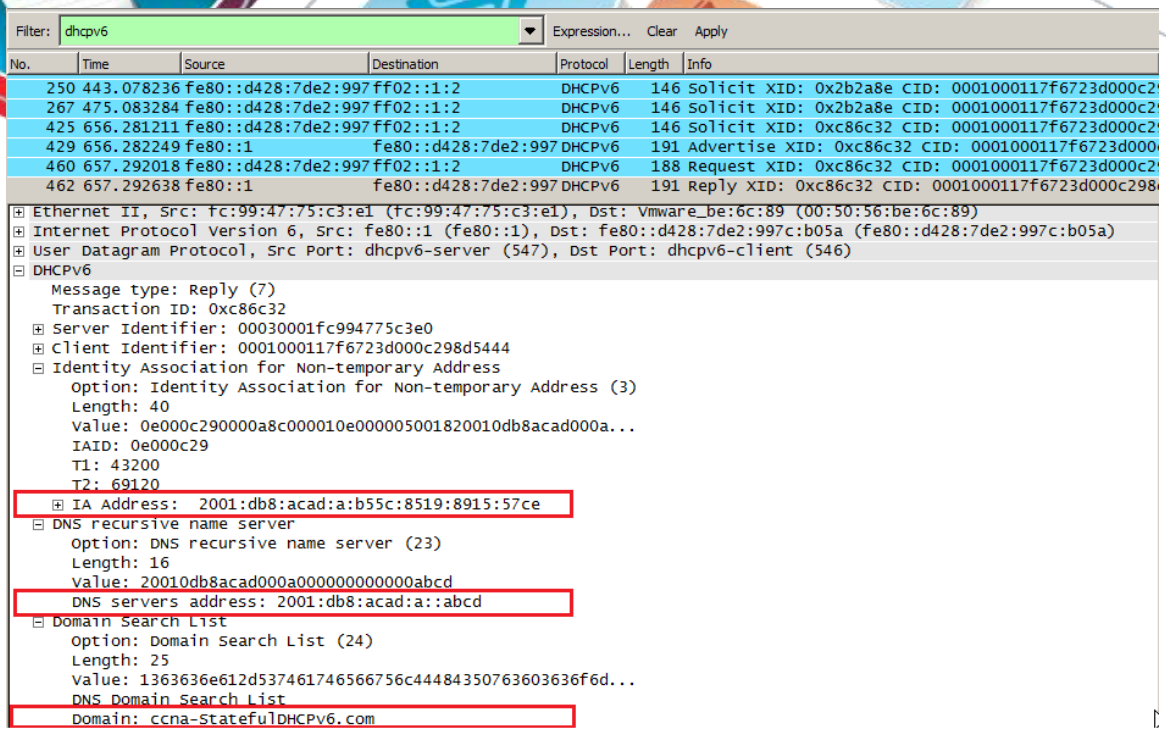
Step 22: verificar DHCPv6 con estado en la PC-A.

a. Detenga la captura de Wireshark en la PC-A.

b. Expanda el mensaje RA más reciente que se indica en Wireshark. Verifique que se haya establecido el indicador **Managed address configuration** (Configuración de dirección administrada).



c. Cambie el filtro en Wireshark para ver solo los paquetes **DHCPv6** escribiendo **dhcpv6** y, a continuación, haga clic en **Apply** (Aplicar). Resalte la última respuesta DHCPv6 de la lista y expanda la información de DHCPv6. Examine la información de red DHCPv6 incluida en este paquete.



Reflexión

1. ¿Qué método de direccionamiento IPv6 utiliza más recursos de memoria en el router configurado como servidor de DHCPv6: DHCPv6 sin estado o DHCPv6 con estado? ¿Por qué?

   DHCPv6 con estado utiliza más recursos de memoria. Las respuestas varían, pero DHCPv6 con estado requiere que el router almacene la información de estado dinámico de los clientes DHCPv6. Los clientes DHCPv6 sin estado no utilizan el servidor de DHCP para obtener información de dirección, de modo que no es necesario almacenarla.

2. ¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado?

   Cisco recomienda DHCPv6 sin estado para implementar redes IPv6 sin Cisco Network Registrar (CNR).

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.

IdT y DHCP

Objetivo

Configure DHCP para IPv4 o IPv6 en un router Cisco 1941.

Situación

En este capítulo, se presenta el concepto del uso del proceso de DHCP en la red de una pequeña a mediana empresa; sin embargo, el protocolo DHCP también tiene otros usos.

Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.
- Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones DHCP del servidor de DHCP.
- Muestre los resultados que validen que cada terminal garantiza una dirección IP del servidor. Utilice un programa de captura de pantalla para guardar la información del resultado o emplee el comando de la tecla **ImprPant**.
- Presente sus conclusiones a un compañero de clase o a la clase.

Recursos necesarios

Software de Packet Tracer

Reflexión

1. ¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica? ¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?

   El router 1941 ofrece una amplia gama de servicios de seguridad en comparación con otros ISR más pequeño, lo cual lo convierte en la opción más confiable si de seguridad y prestaciones se trata. Pero al igual, también se podría implementar un ISR más pequeño como servidor DHCP, solo que tendría un menor rendimiento y sería más vulnerable a los ataques de piratas informáticos.

2. ¿Cómo cree que las pequeñas y medianas empresas pueden usar la asignación de direcciones IP de DHCP en el mundo de las redes IPv6 e IdT? Mediante la técnica de la lluvia de ideas, piense y registre cinco respuestas posibles.

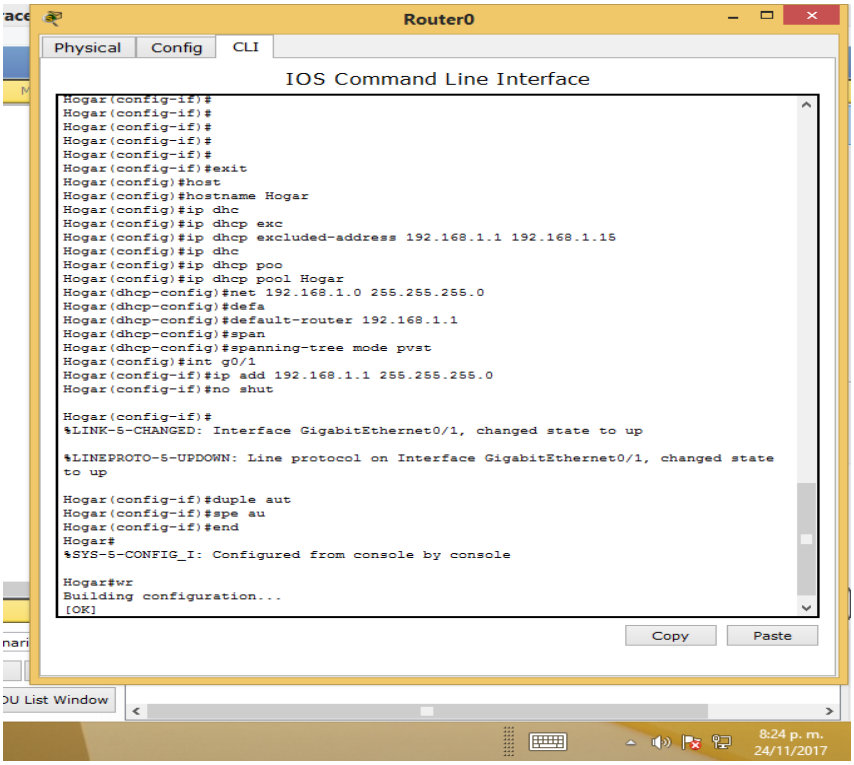
   1. Mediante el direccionamiento IP DHCP se podría controlar el proceso de secado del cuero en una fábrica de botas.

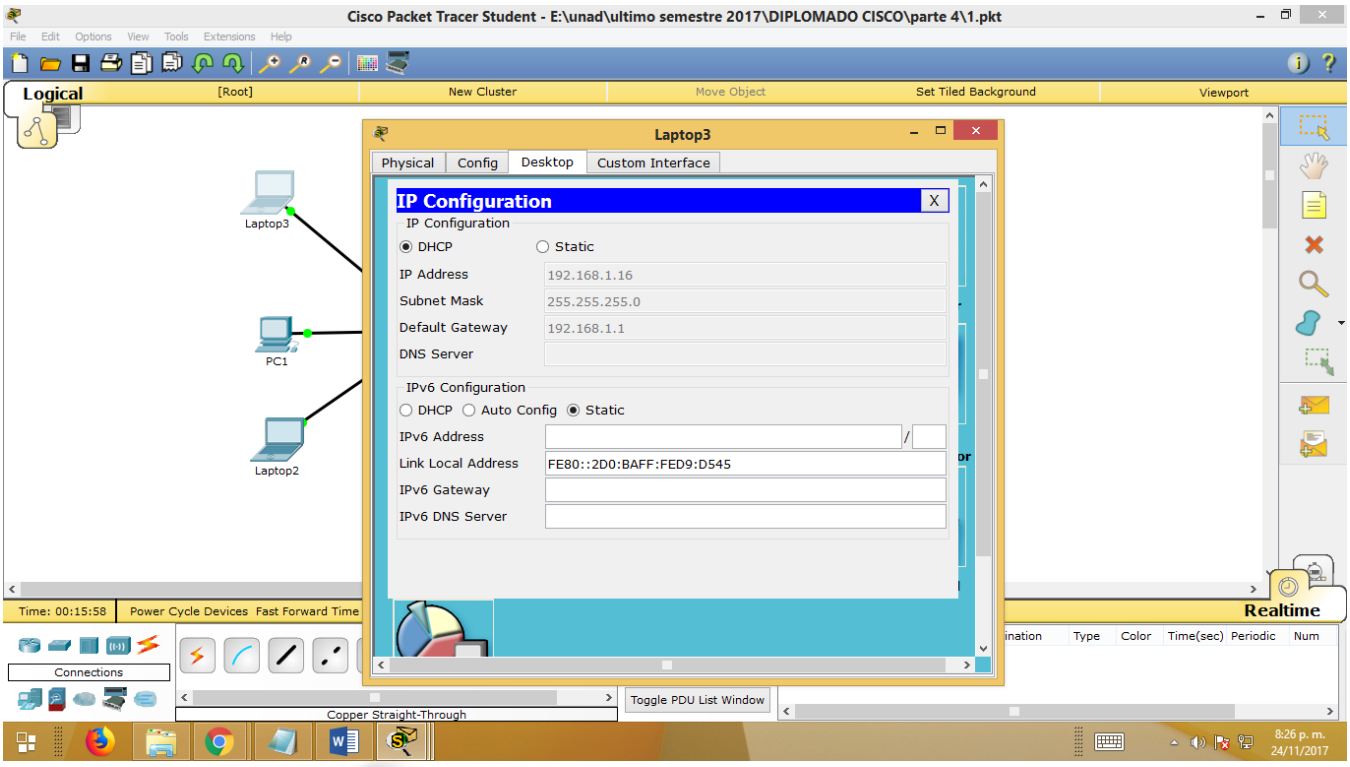
   2. Una empresa de vigilancia, mediante el uso de direccionamiento IP de DHCP en sus propios servidores, podría controlar el sistema de CCTV.

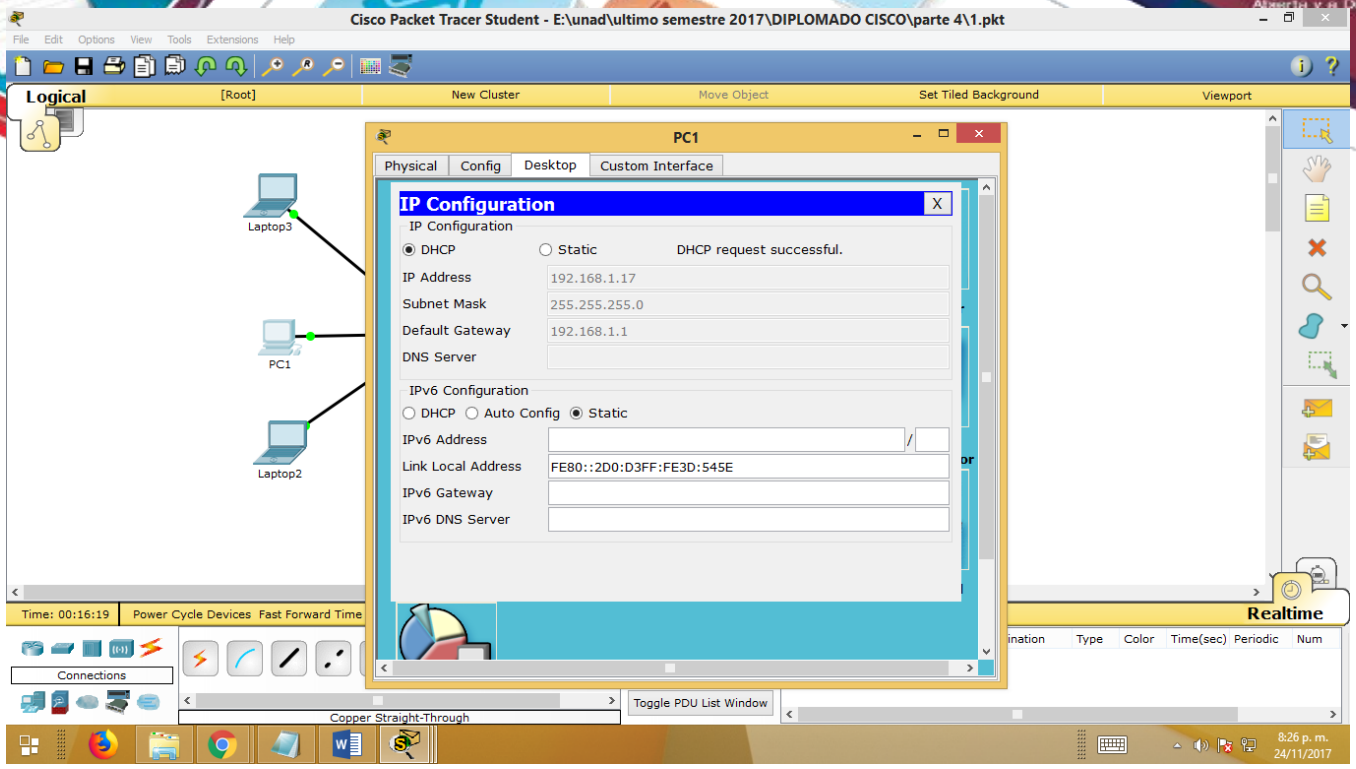
   3. Se podrían controlar algunos electrodomésticos, por ejemplo, un horno microondas, dentro de un hogar automatizado (domótica); mediante la ubicación del servidor DNS y la dirección DHCP del servidor.

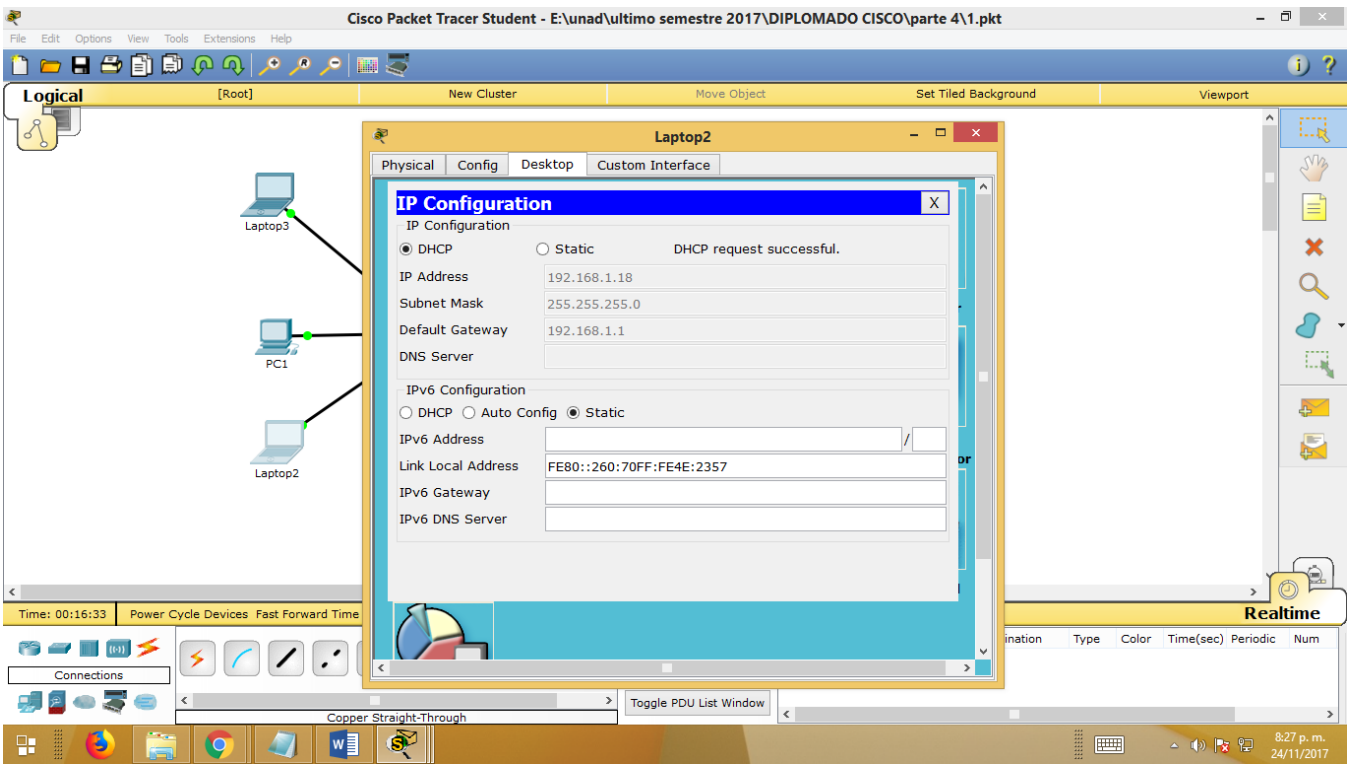
4. Se podrían identificar averías o errores de los dispositivos de red mediante la asignación de direcciones IP de un servidor DHCP en una empresa de archivo y saber si necesitan o no mantenimiento.

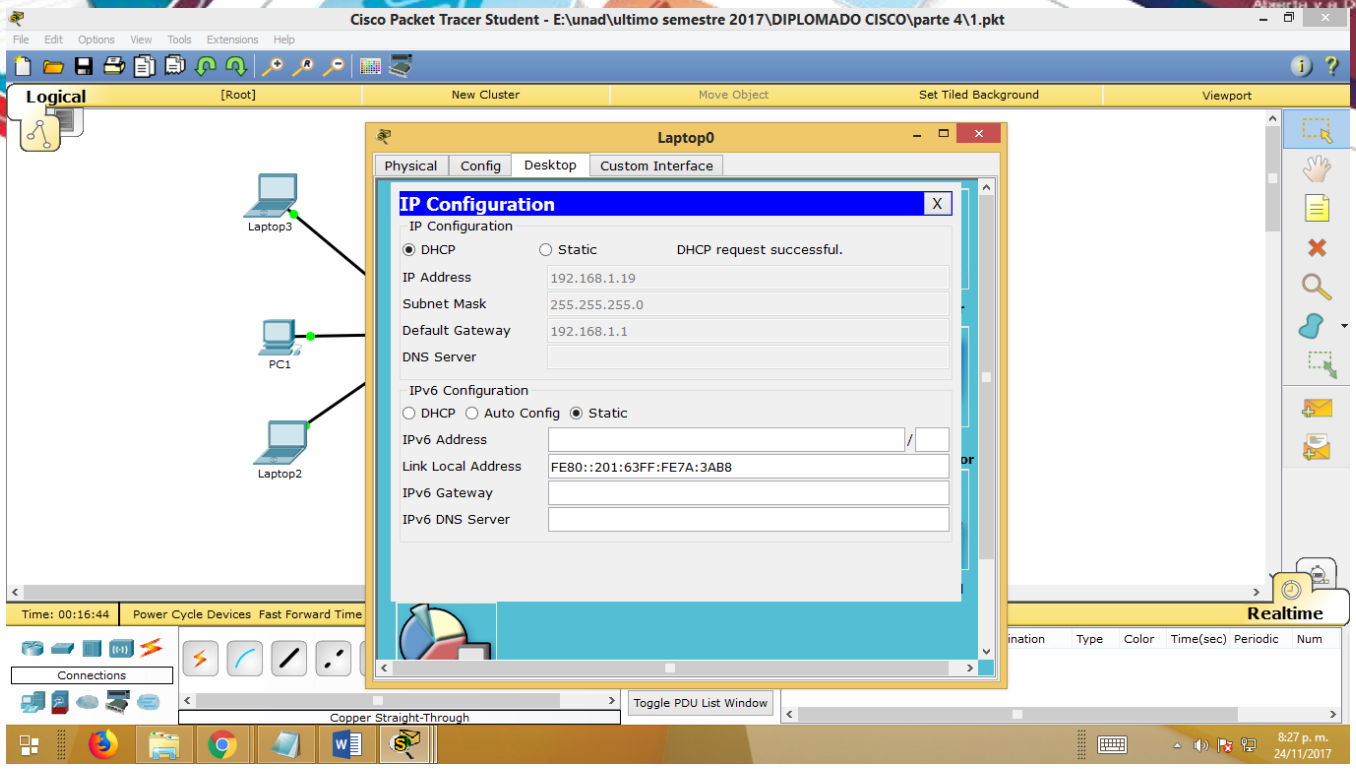
5. Se puede controlar y monitorear el estado y funcionamiento de un PLC mediante el direccionamiento IP de un servidor propio DHCP de una fábrica de refrescos.

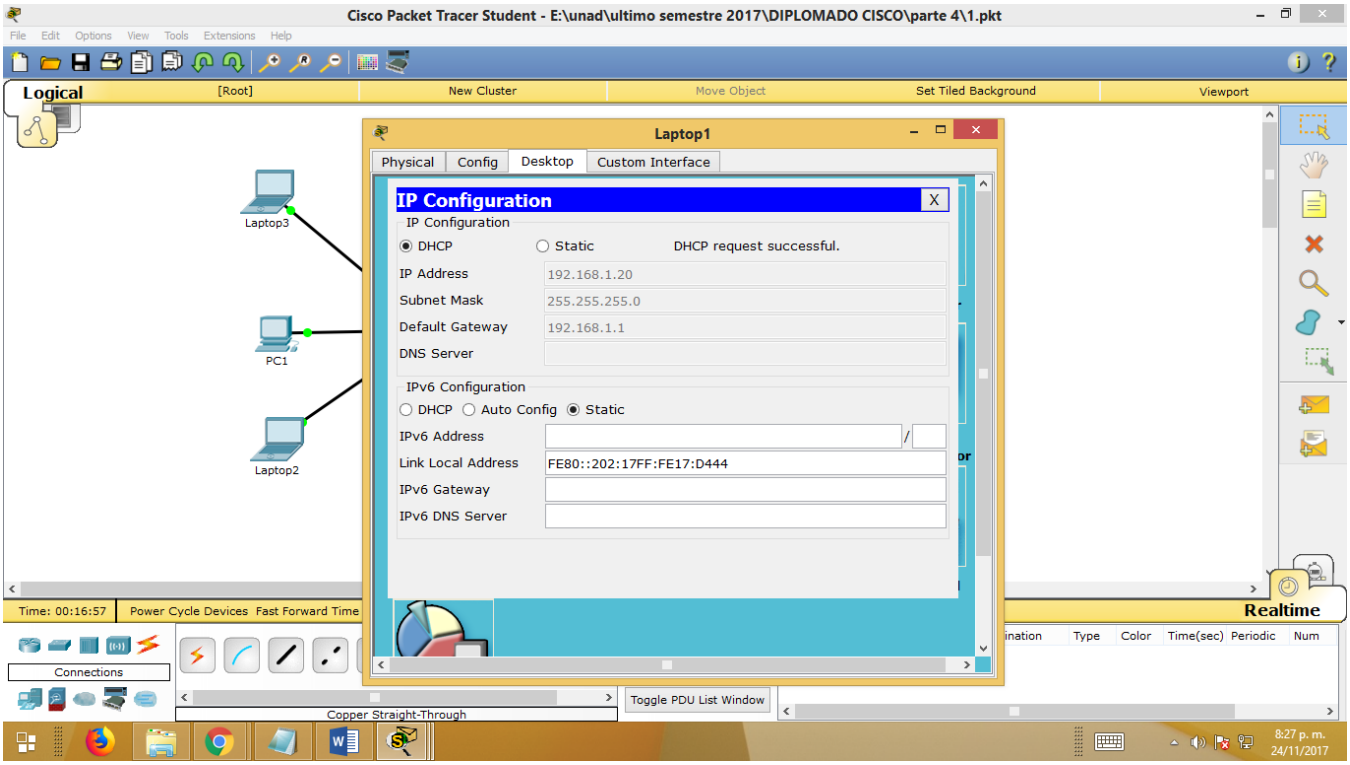





Cisco Packet Tracer Student - E:\unad\ultimo semestre 2017\DIPLOMADO CISCO\parte 4\1.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address 192.168.1.17
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::2D0:D3FF:FE3D:545E
IPv6 Gateway
IPv6 DNS Server
Laptop3
PC1
Laptop2
Time: 00:16:19
Power Cycle Devices Fast Forward Time
Realtime
Connections
Copper Straight-Through
Toggle PDU List Window
8:26 p. m.
24/11/2017


Cisco Packet Tracer Student - E:\unad\ultimo semestre 2017\DIPLOMADO CISCO\parte 4\1.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Laptop2
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address 192.168.1.18
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::260:70FF:FE4E:2357
IPv6 Gateway
IPv6 DNS Server
Laptop3
PC1
Laptop2
Time: 00:16:33
Power Cycle Devices Fast Forward Time
Realtime
Connections
Copper Straight-Through
Toggle PDU List Window
8:27 p. m.
24/11/2017


Cisco Packet Tracer Student - E:\unad\ultimo semestre 2017\DIPLOMADO CISCO\parte 4\1.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Laptop0
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address 192.168.1.19
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::201:63FF:FE7A:3AB8
IPv6 Gateway
IPv6 DNS Server
Laptop3
PC1
Laptop2
Time: 00:16:44
Power Cycle Devices Fast Forward Time
Realtime
Connections
Copper Straight-Through
Toggle PDU List Window
8:27 p. m.
24/11/2017


Cisco Packet Tracer Student - E:\unad\ultimo semestre 2017\DIPLOMADO CISCO\parte 4\1.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Laptop1
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address 192.168.1.20
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::202:17FF:FE17:D444
IPv6 Gateway
IPv6 DNS Server
Laptop3
PC1
Laptop2
Time: 00:16:57
Power Cycle Devices Fast Forward Time
Realtime
Connections
Copper Straight-Through
Toggle PDU List Window
8:27 p. m.
24/11/2017

Ejercicio No 8 - 11.2.2.6 Lab - Configuring Dynamic and Static NAT

Práctica de laboratorio: configuración de NAT dinámica y estática

Topología

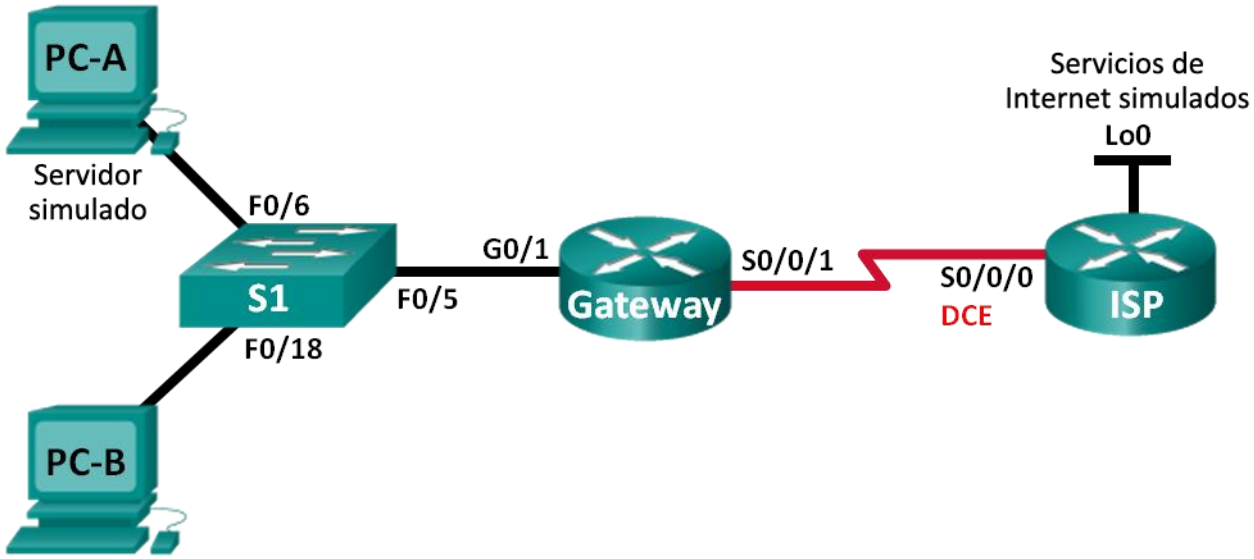


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (servidor simulado)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

En esta práctica de laboratorio, un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/27. Esto proporciona 30 direcciones IP públicas a la empresa. Las direcciones 209.165.200.225 a 209.165.200.241 son para la asignación estática, y las direcciones 209.165.200.242 a 209.165.200.254 son para la asignación dinámica. Del ISP al router de gateway se usa una ruta estática, y del gateway al router ISP se usa una ruta predeterminada. La conexión del ISP a Internet se simula mediante una dirección de loopback en el router ISP.

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 esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 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

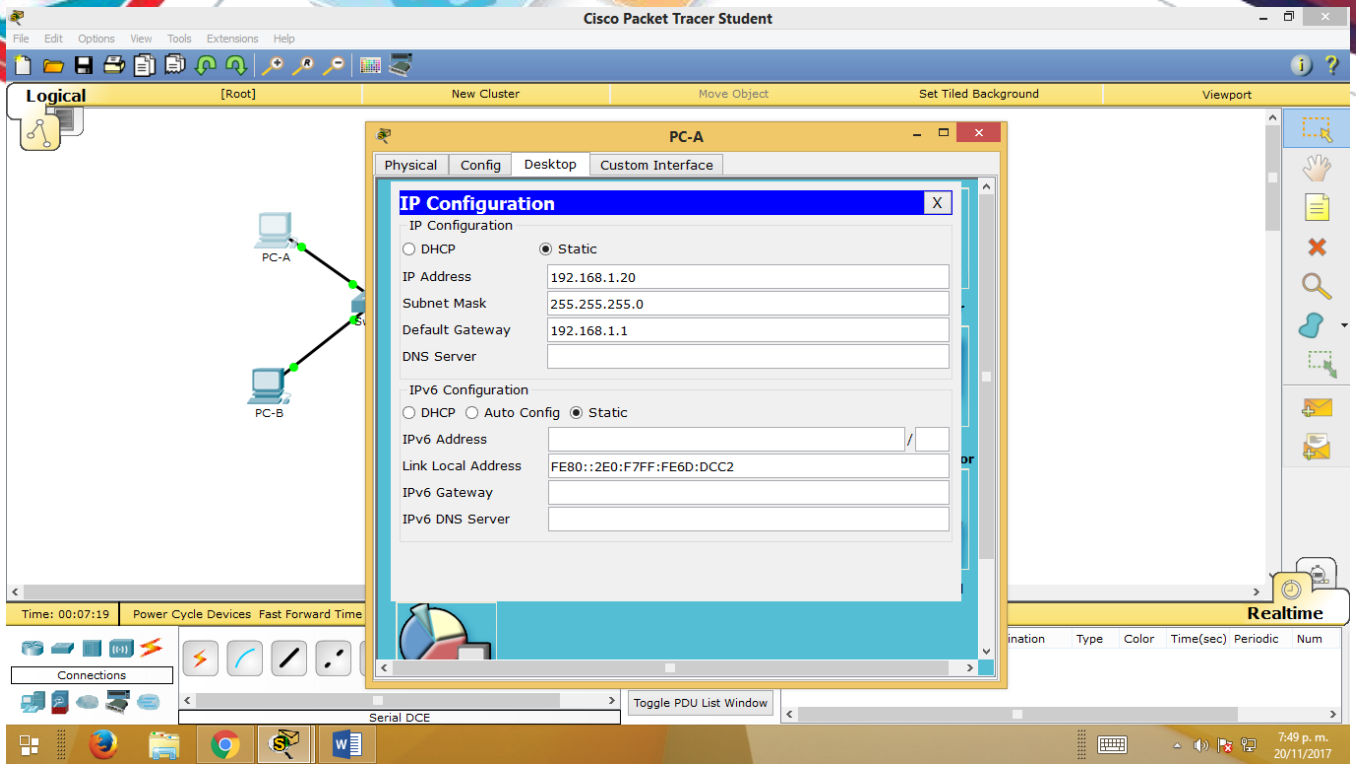
armar la red y verificar la conectividad

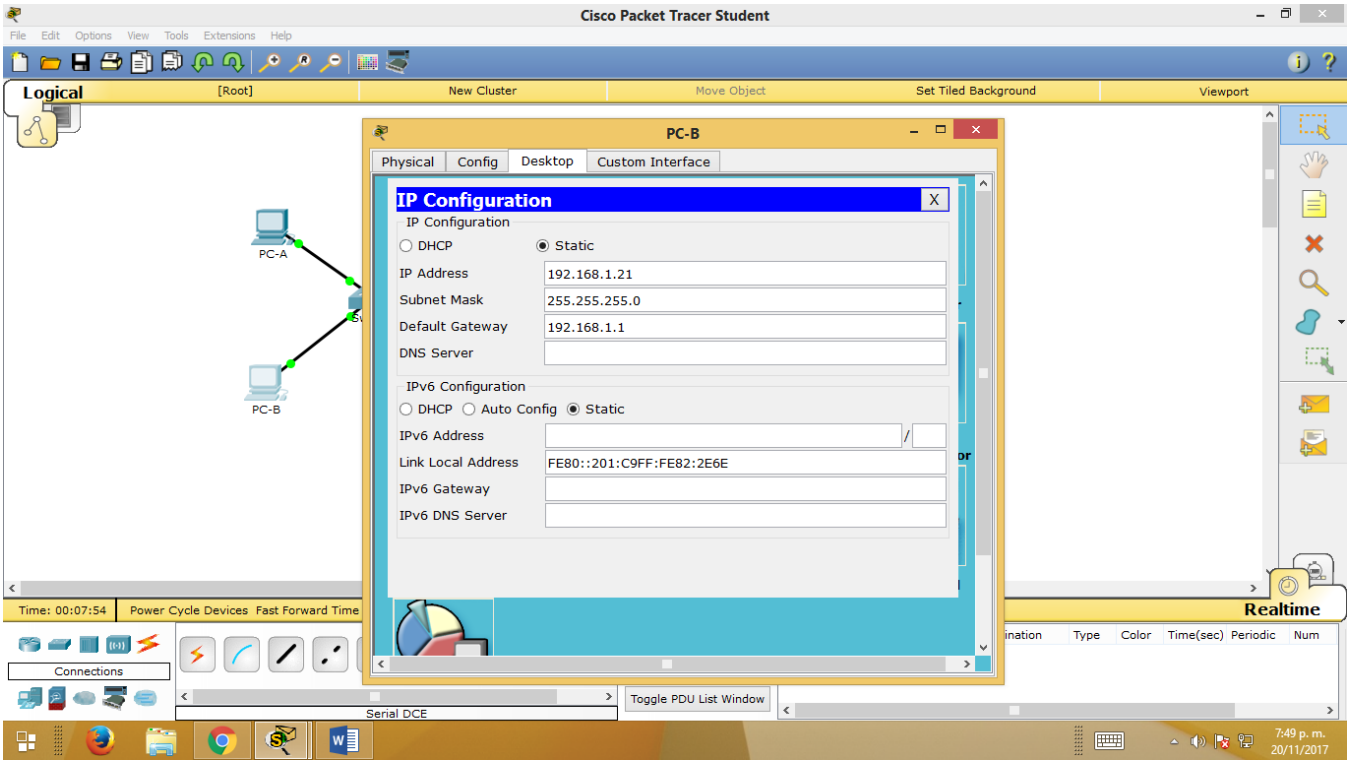
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

Step 23: realizar el cableado de red tal como se muestra en la topología.

Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

Step 24: configurar los equipos host.





Step 25: inicializar y volver a cargar los routers y los switches según sea necesario.

Step 26: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

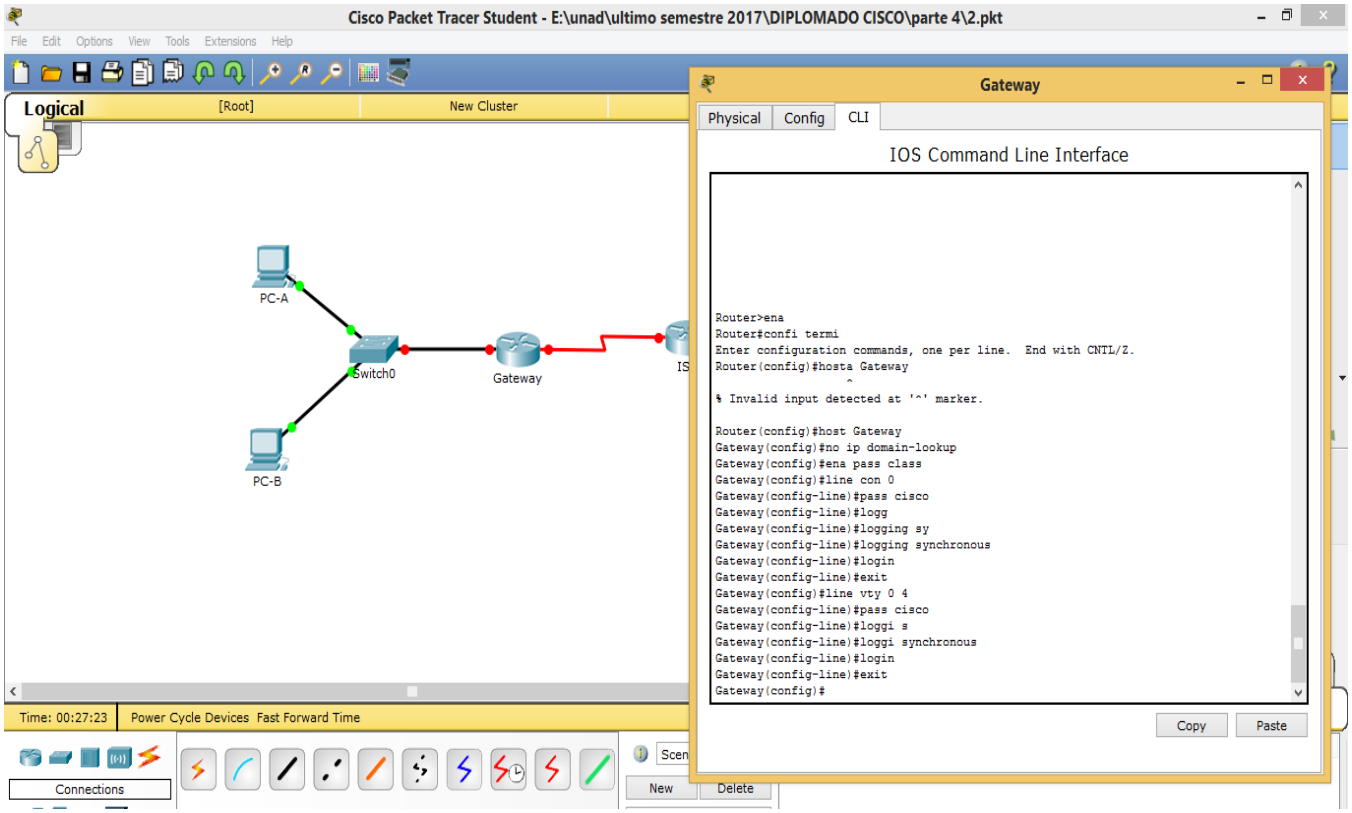
c. Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.

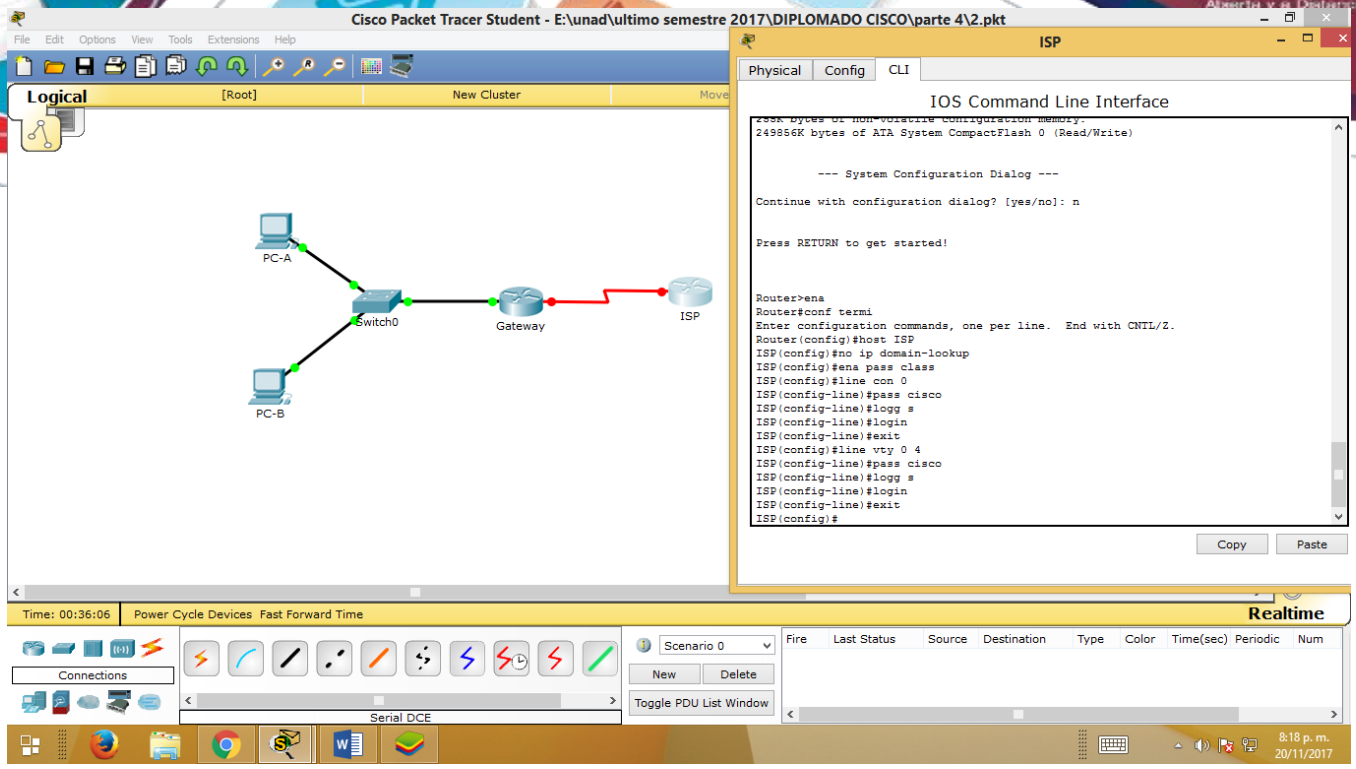
d. Configure el nombre del dispositivo como se muestra en la topología.

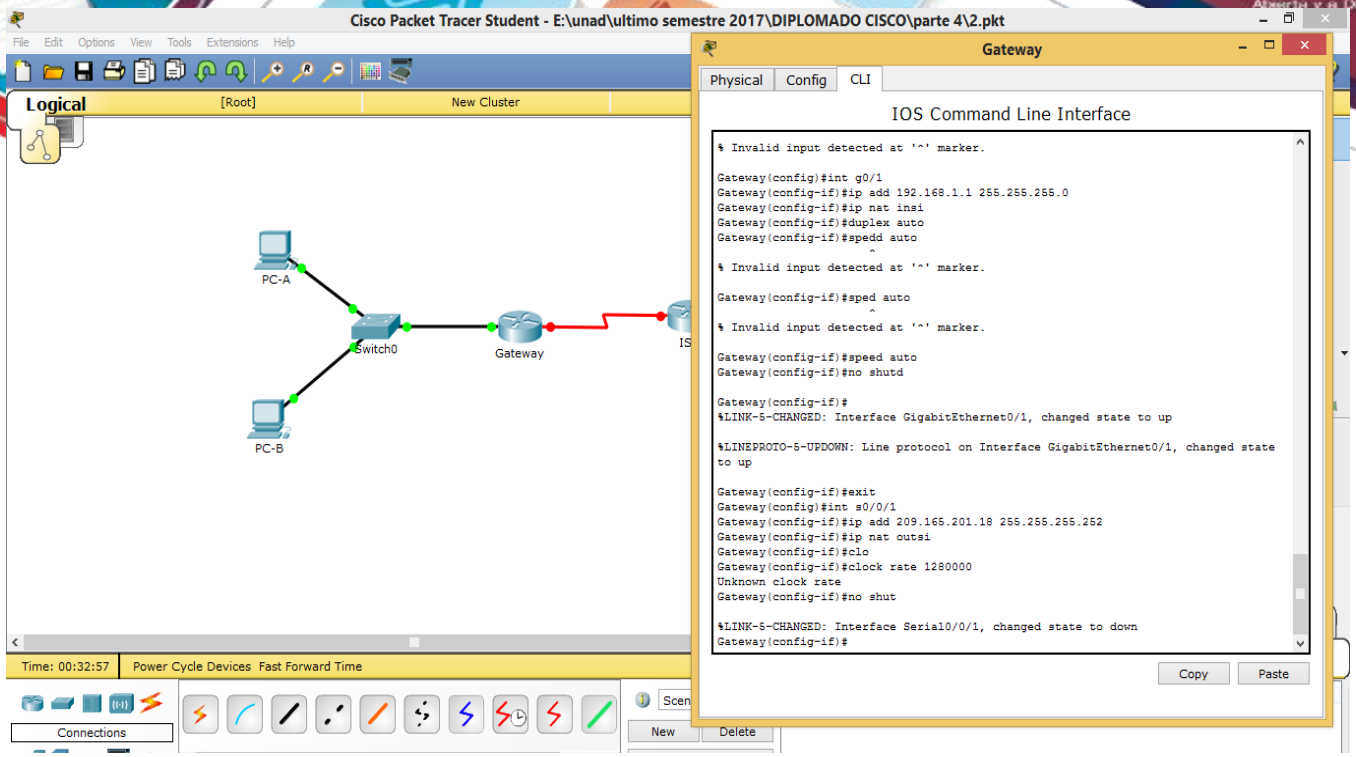
e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

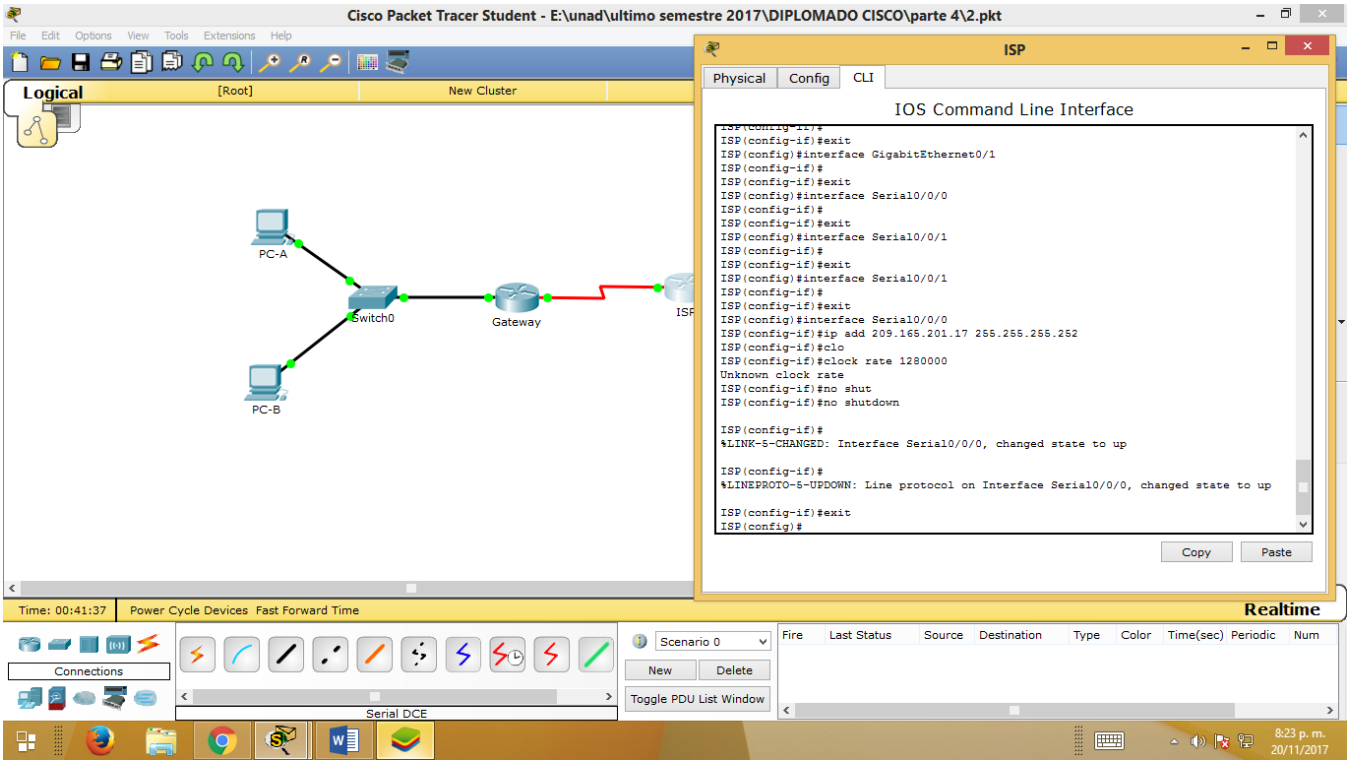
f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.




Cisco Packet Tracer Student - E:\unad\ultimo semestre 2017\DIPLOMADO CISCO\parte 4\2.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
PC-A
Switch0
Gateway
ISP
PC-B
ISP
Physical
Config
CLI
IOS Command Line Interface
249856K bytes of ATA System CompactFlash 0 (Read/Write)
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>ena
Router#conf termi
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host ISP
ISP(config)#no ip domain-lookup
ISP(config)#ena pass class
ISP(config)#line con 0
ISP(config-line)#pass cisco
ISP(config-line)#logg s
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#pass cisco
ISP(config-line)#logg s
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#
Copy
Paste
Time: 00:36:06
Power Cycle Devices Fast Forward Time
Realtime
Connections
Serial DCE
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
8:18 p. m.
20/11/2017


Cisco Packet Tracer Student - E:\unad\ultimo semestre 2017\DIPLOMADO CISCO\parte 4\2.pkt
Gateway
Physical
Config
CLI
IOS Command Line Interface
% Invalid input detected at '^' marker.
Gateway(config)#int g0/1
Gateway(config-if)#ip add 192.168.1.1 255.255.255.0
Gateway(config-if)#ip nat insi
Gateway(config-if)#duplex auto
Gateway(config-if)#spedd auto
% Invalid input detected at '^' marker.
Gateway(config-if)#sped auto
% Invalid input detected at '^' marker.
Gateway(config-if)#speed auto
Gateway(config-if)#no shutd
Gateway(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Gateway(config-if)#exit
Gateway(config)#int s0/0/1
Gateway(config-if)#ip add 209.165.201.18 255.255.255.252
Gateway(config-if)#ip nat outsi
Gateway(config-if)#clo
Gateway(config-if)#clock rate 1280000
Unknown clock rate
Gateway(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Gateway(config-if)#
Copy
Paste
Logical
[Root]
New Cluster
PC-A
Switch0
Gateway
PC-B
Time: 00:32:57
Power Cycle Devices
Fast Forward Time
Connections
New
Delete


Cisco Packet Tracer Student - E:\unad\ultimo semestre 2017\DIPLOMADO CISCO\parte 4\2.pkt
ISP
Physical
Config
CLI
IOS Command Line Interface
ISP(config-if)#exit
ISP(config)#interface GigabitEthernet0/1
ISP(config-if)#
ISP(config-if)#exit
ISP(config)#interface Serial0/0/0
ISP(config-if)#
ISP(config-if)#exit
ISP(config)#interface Serial0/0/1
ISP(config-if)#
ISP(config-if)#exit
ISP(config)#interface Serial0/0/1
ISP(config-if)#
ISP(config-if)#exit
ISP(config)#interface Serial0/0/0
ISP(config-if)#ip add 209.165.201.17 255.255.255.252
ISP(config-if)#clo
ISP(config-if)#clock rate 1280000
Unknown clock rate
ISP(config-if)#no shut
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
ISP(config-if)#exit
ISP(config)#
Copy
Paste
Logical
[Root]
New Cluster
PC-A
Switch0
Gateway
PC-B
Time: 00:41:37
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Scenario 0
New
Delete
Toggle PDU List Window
Serial DCE
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
8:23 p. m.
20/11/2017

Step 27: crear un servidor web simulado en el ISP.

a. Cree un usuario local denominado **webuser** con la contraseña cifrada **webpass**.

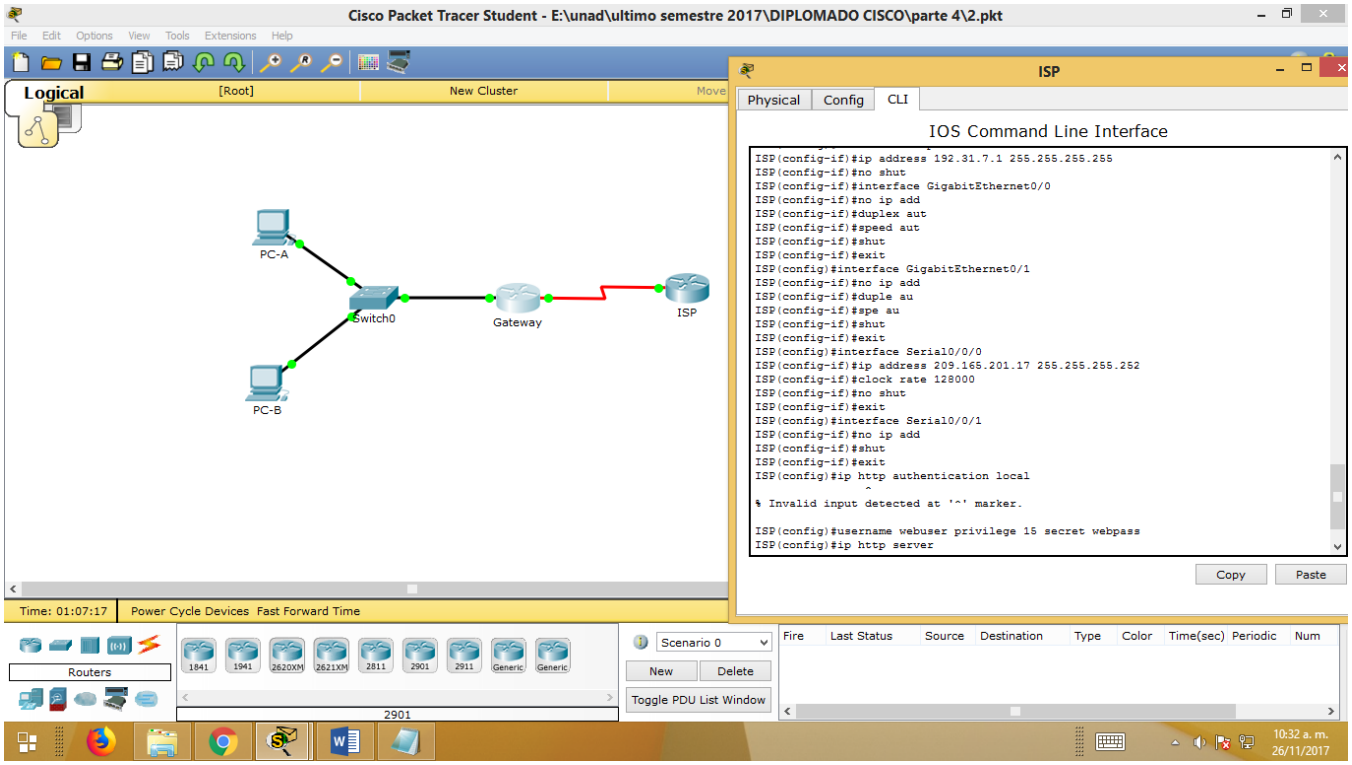
```
ISP(config)# username webuser privilege 15 secret webpass
```

b. Habilite el servicio del servidor HTTP en el ISP.

```
ISP(config)# ip http server
```

c. Configure el servicio HTTP para utilizar la base de datos local.

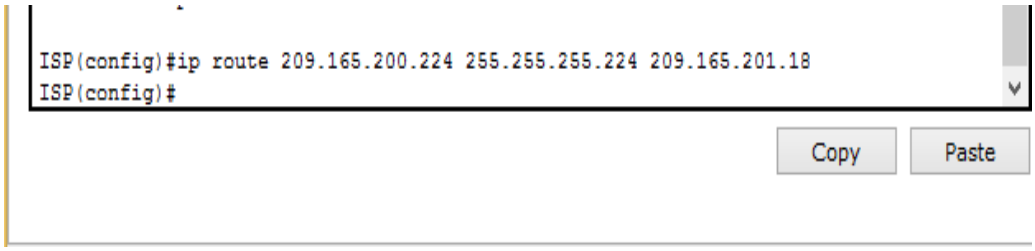
```
ISP(config)# ip http authentication local
```



Step 28: configurar el routing estático.

a. Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```



b. Cree una ruta predeterminada del router Gateway al router ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

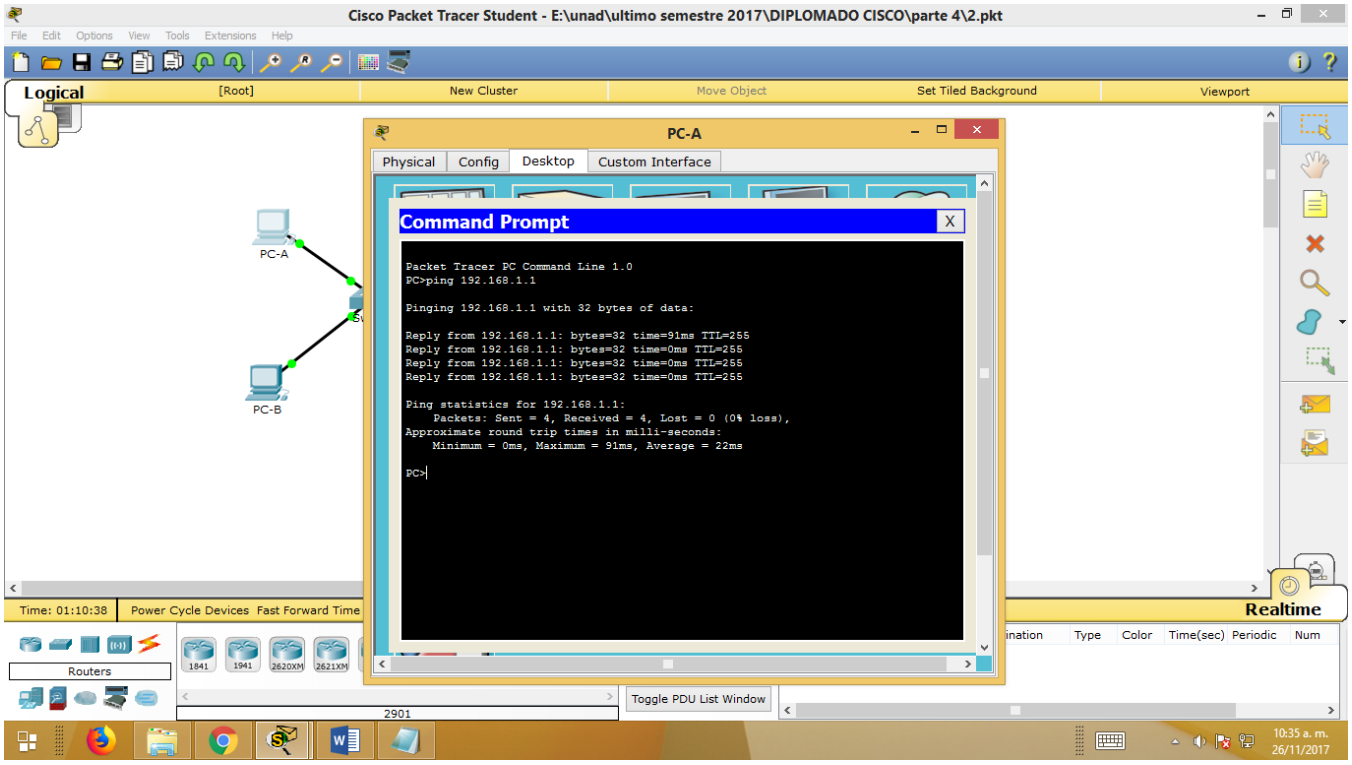
```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

Copy Paste

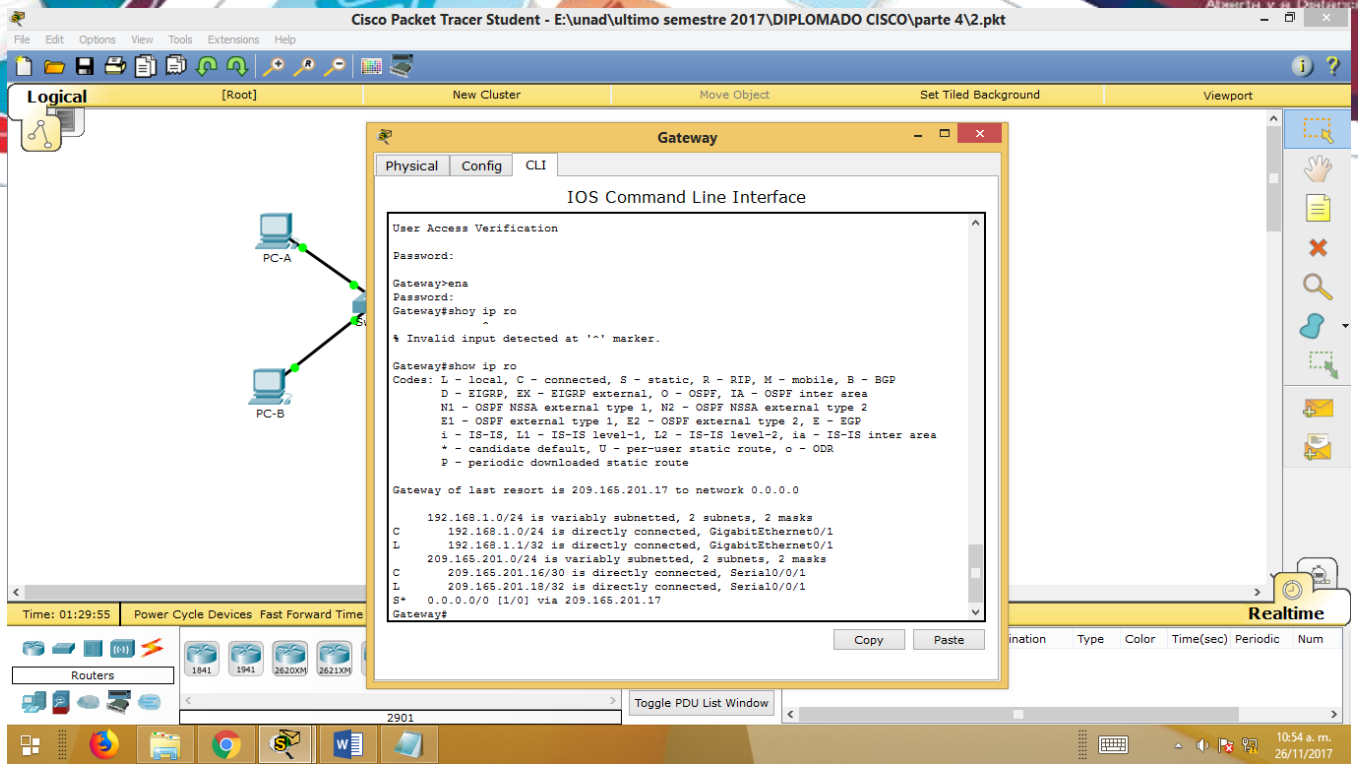
Step 29: Guardar la configuración en ejecución en la configuración de inicio.

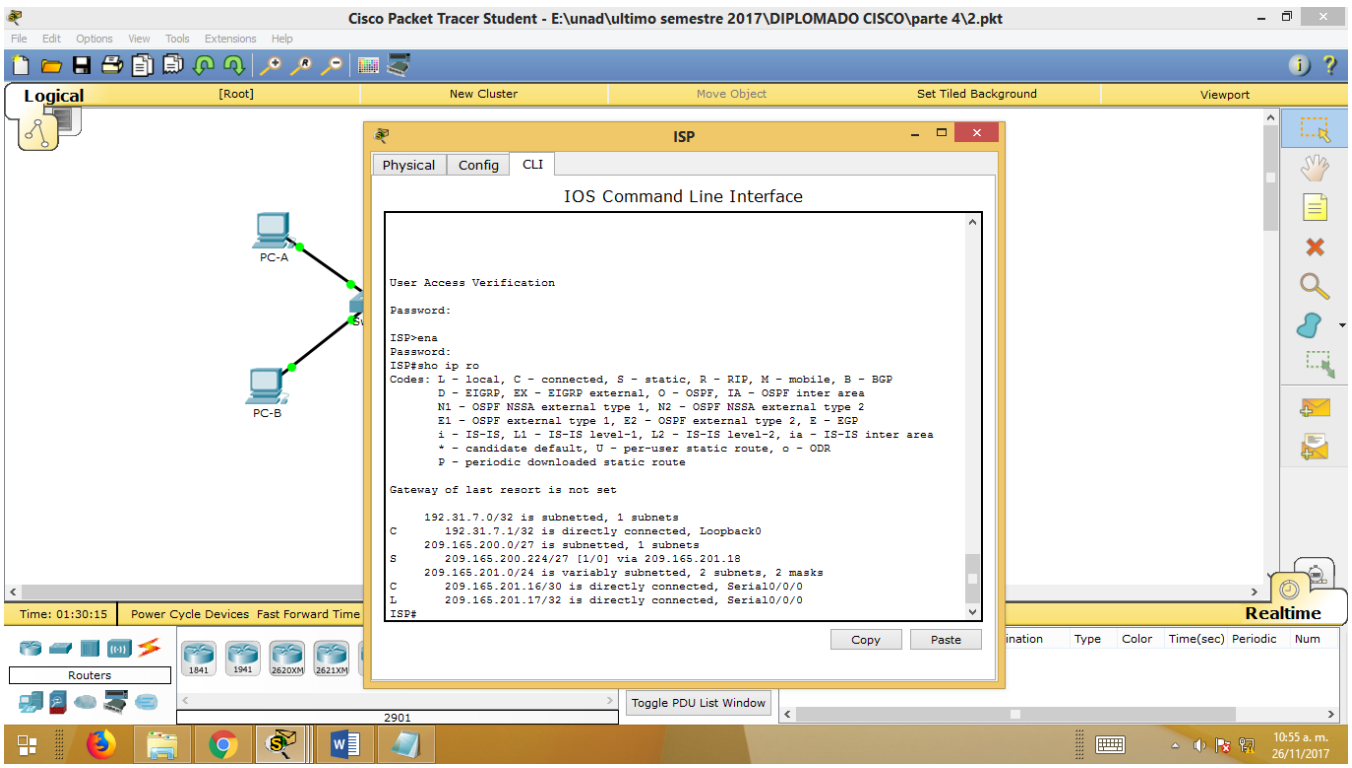
Step 30: Verificar la conectividad de la red

a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.



b. Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.





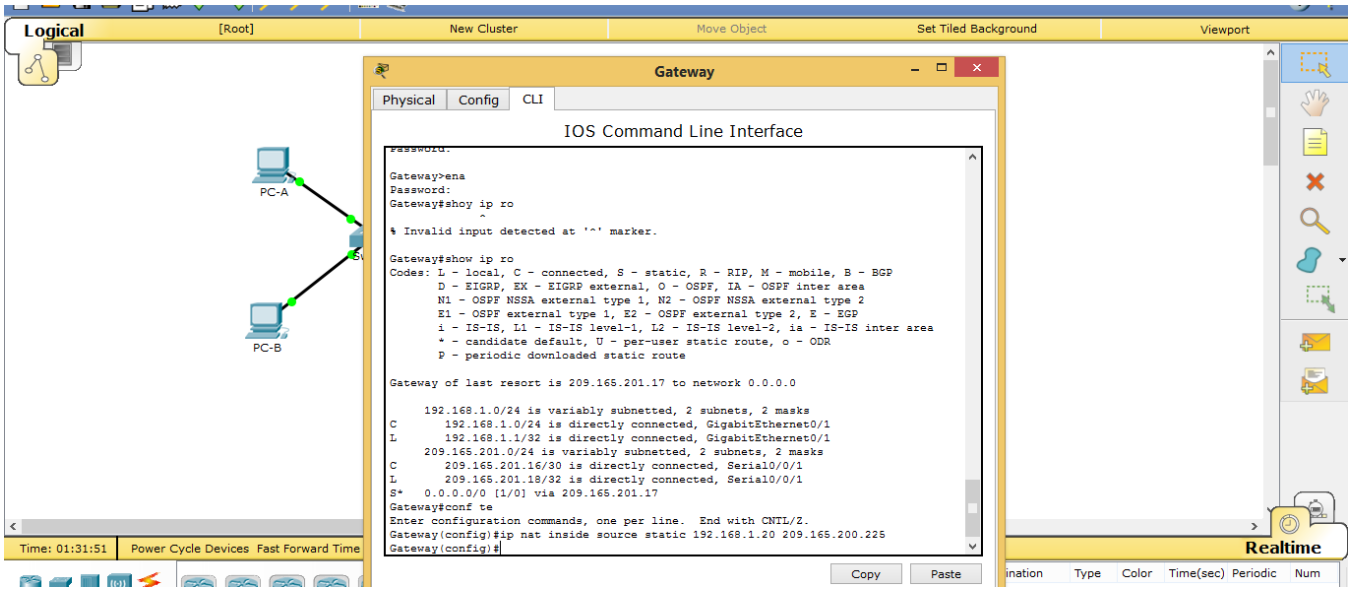
configurar y verificar la NAT estática.

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

Step 31: configurar una asignación estática.

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

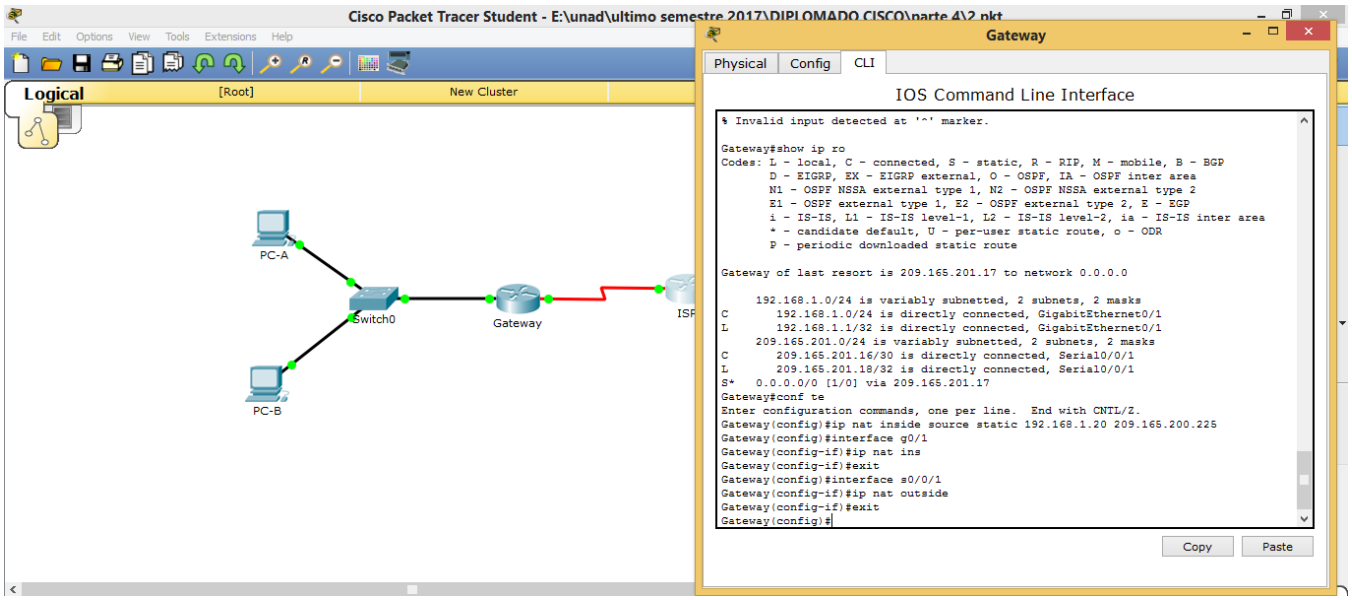
```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```



Step 32: Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```



Step 33: probar la configuración.

a. Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
```

¿Cuál es la traducción de la dirección host local interna?

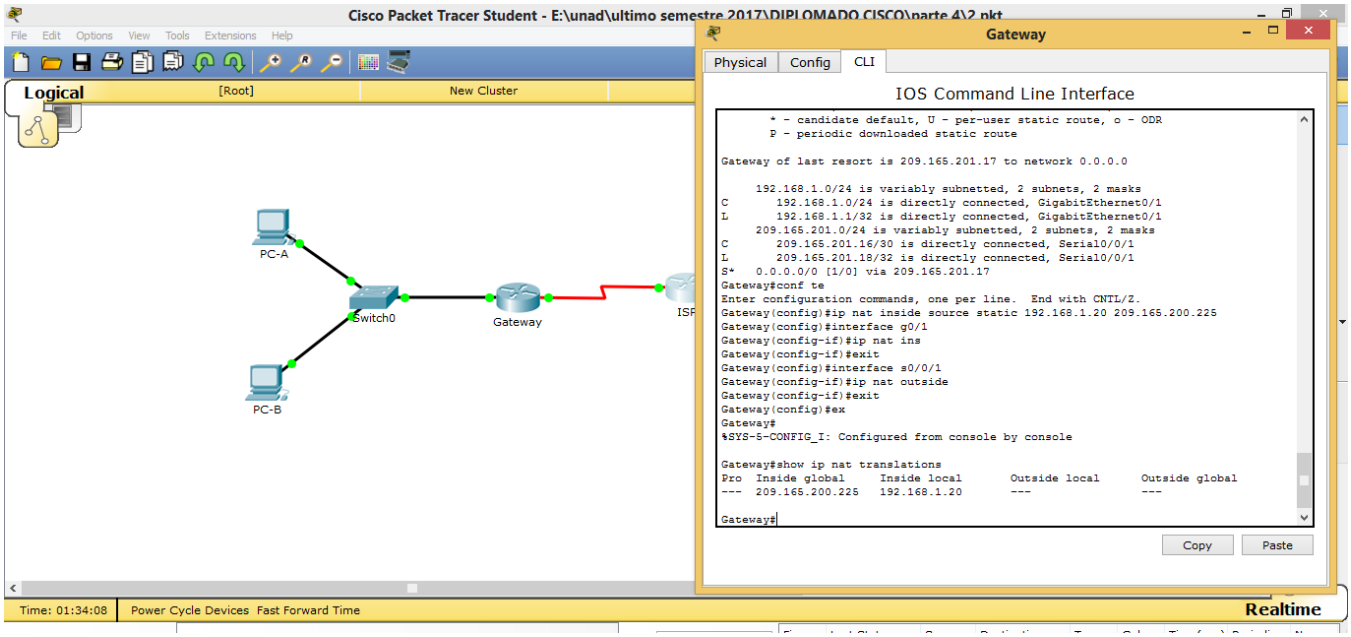
192.168.1.20 = _ 209.165.200.225 _____

¿Quién asigna la dirección global interna?

El router del pool de la NAT. _____

¿Quién asigna la dirección local interna?

El administrador de la estación de trabajo. _____

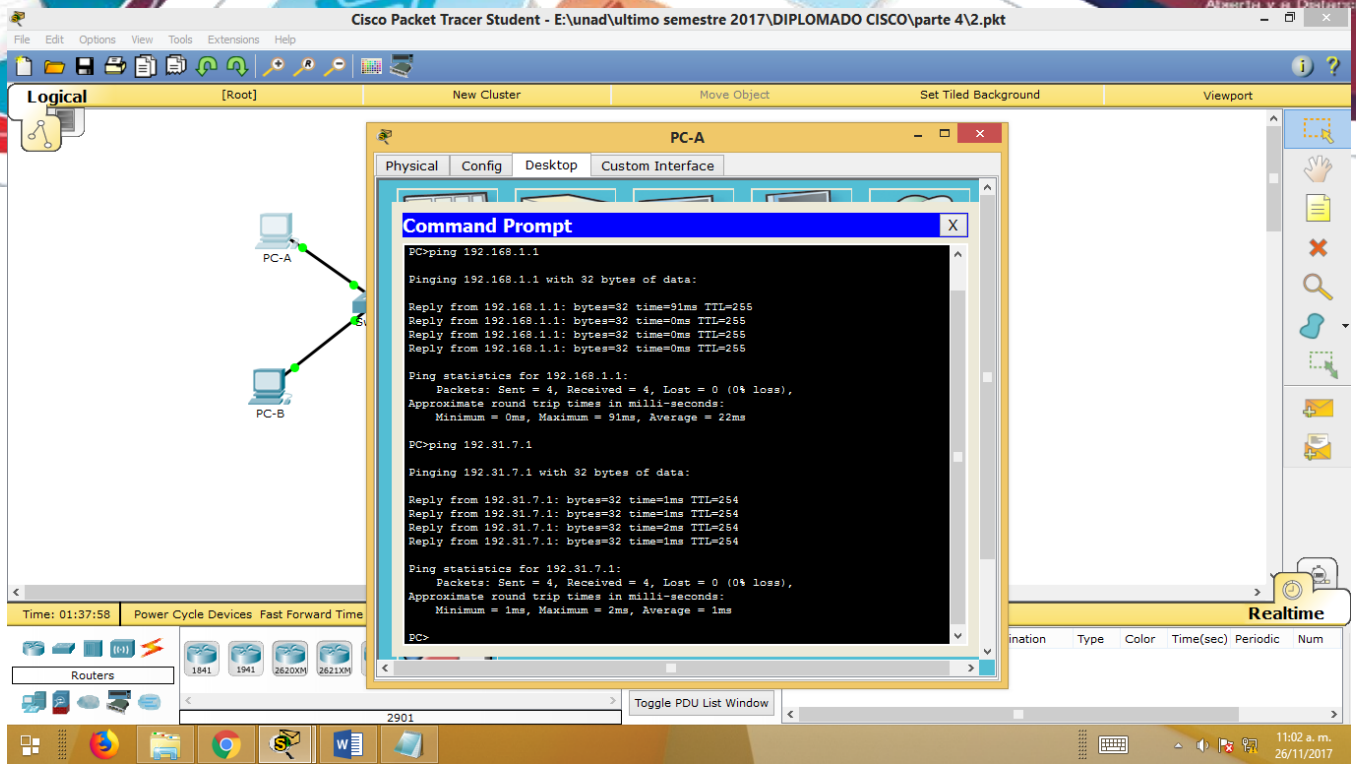


b. En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.225    192.168.1.20       ---                ---
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? 1, las respuestas varían.



Nota: puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:1	192.168.1.20:1	192.31.7.1:1	192.31.7.1:1
tcp	209.165.200.225:1034	192.168.1.20:1034	192.31.7.1:23	192.31.7.1:23
---	209.165.200.225	192.168.1.20	---	---

Nota: es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

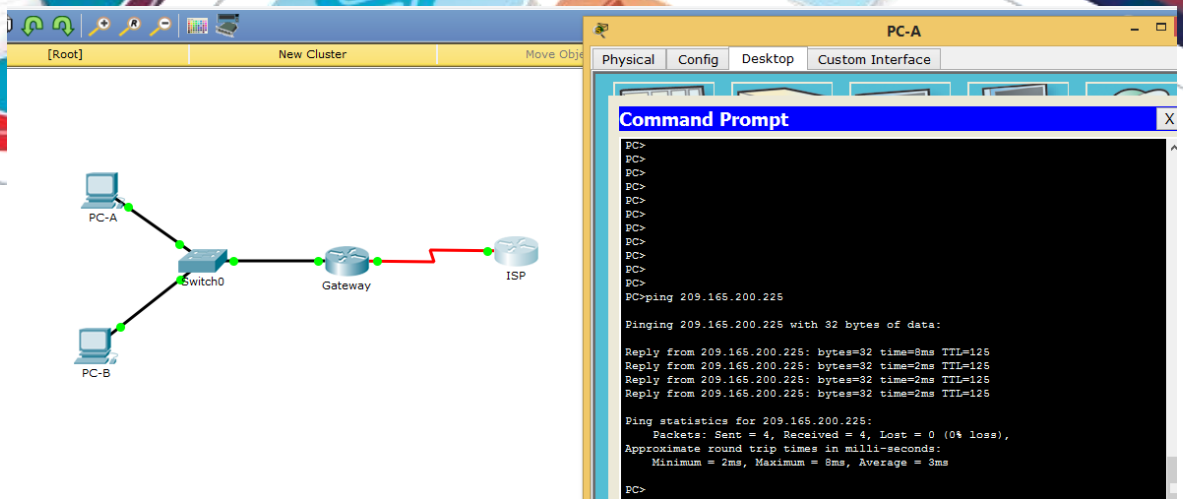
¿Qué protocolo se usó para esta traducción? _ tcp _____

¿Cuáles son los números de puerto que se usaron?

Global/local interno: _____ 1034, las respuestas varían. _____

Global/local externo: _____23_____

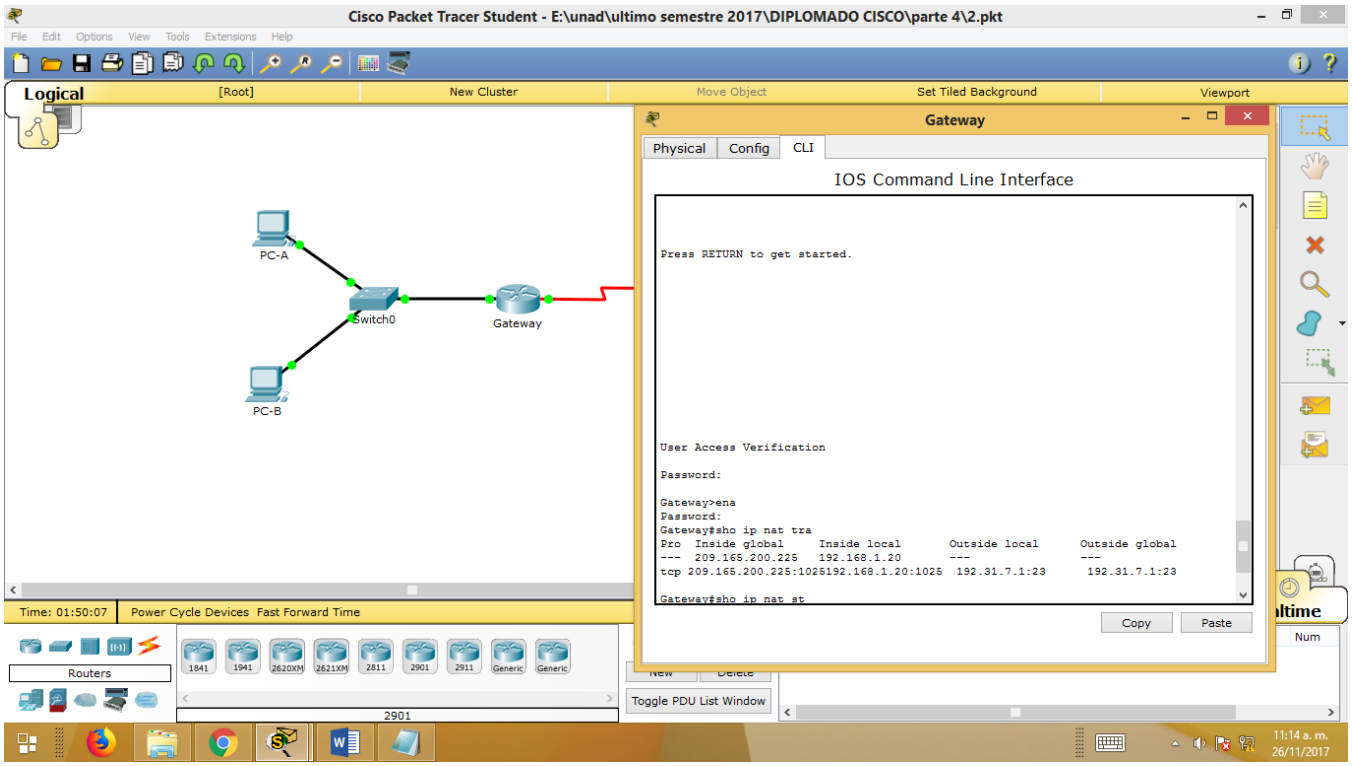
d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.



e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

```
Gateway# show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:12
--- 209.165.200.225     192.168.1.20       ---                ---
```

Observe que la dirección local externa y la dirección global externa son iguales. Esta dirección es la dirección de origen de red remota del ISP. Para que el ping del ISP se realice correctamente, la dirección global interna de NAT estática 209.165.200.225 se tradujo a la dirección local interna de la PC-A (192.168.1.20).

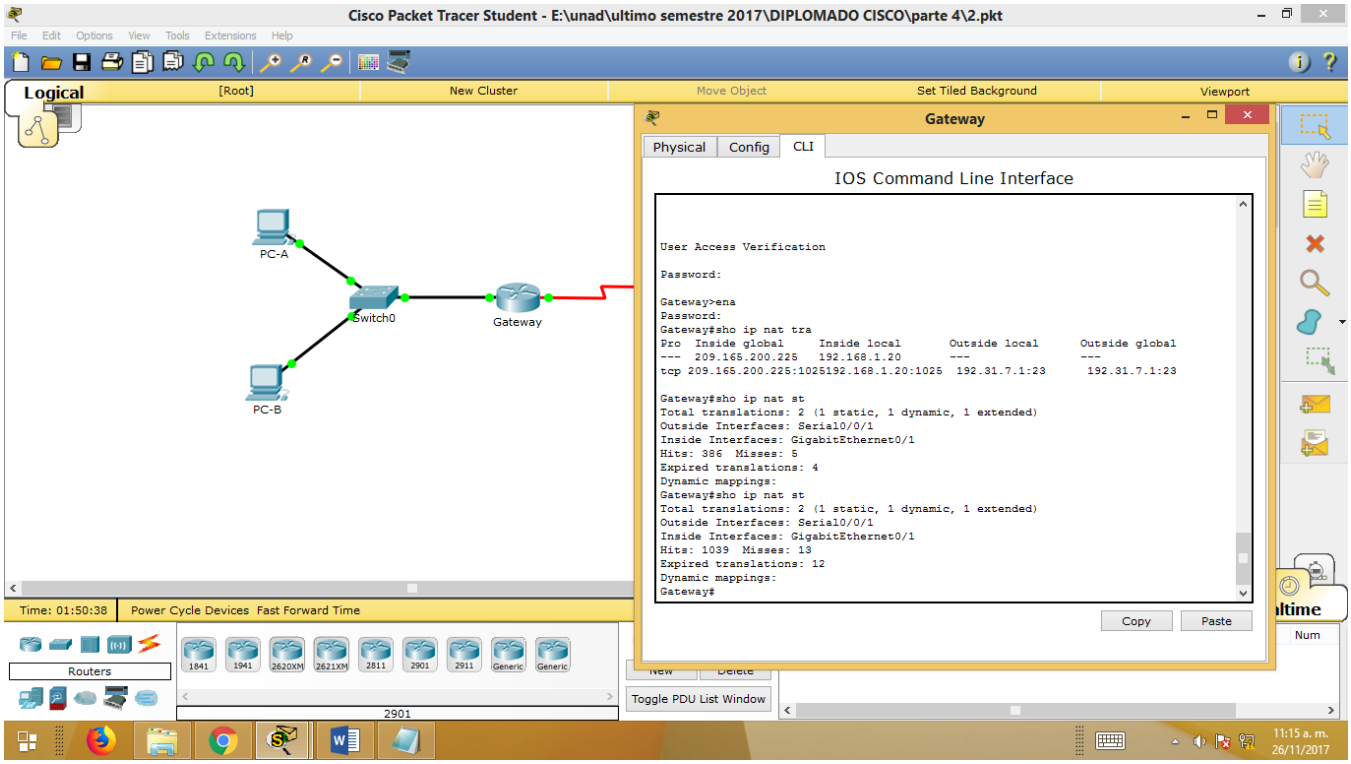


f. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

```
Gateway# show ip nat statics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
```

```
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.



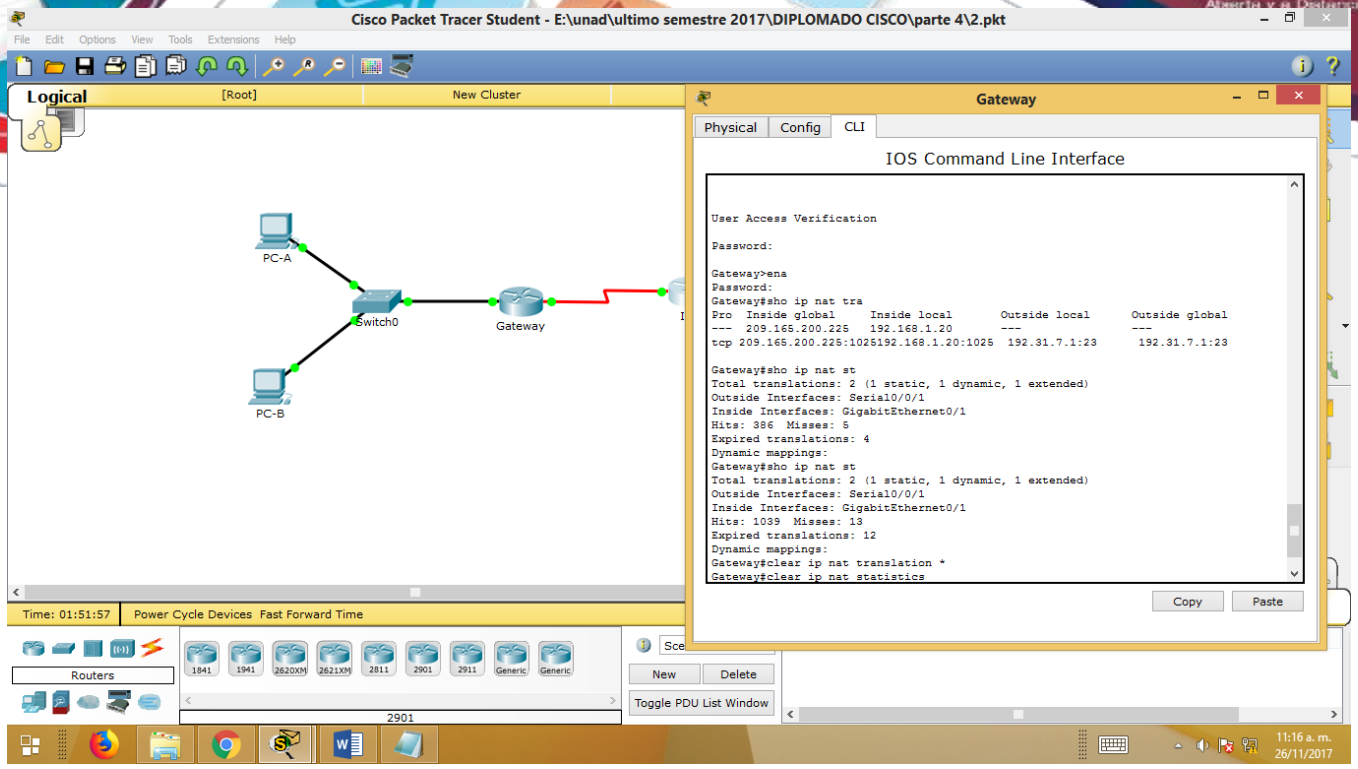
configurar y verificar la NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

Step 34: borrar las NAT.

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

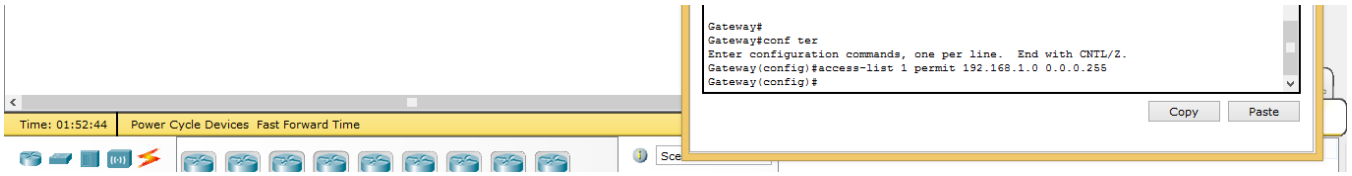
```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```



Step 35: definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.

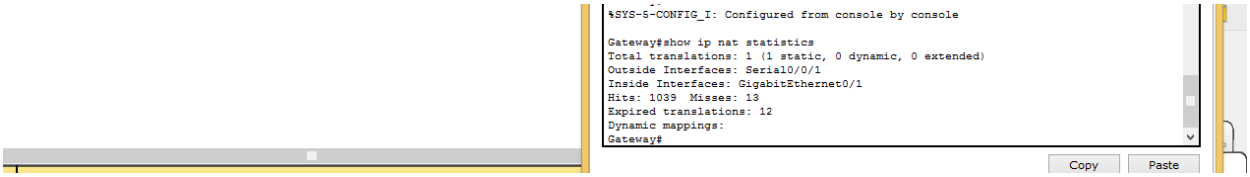
La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```



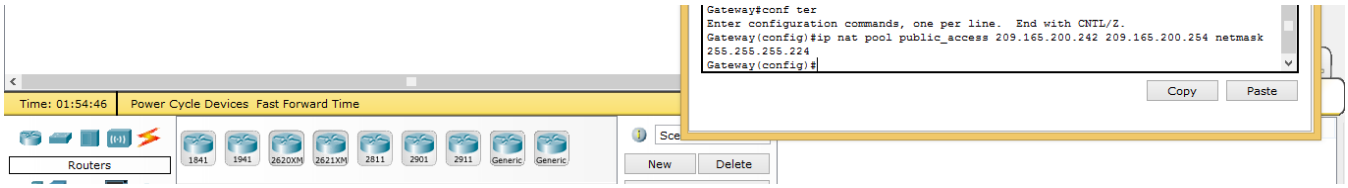
Step 36: verificar que la configuración de interfaces NAT siga siendo válida.

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.



Step 37: definir el conjunto de direcciones IP públicas utilizables.

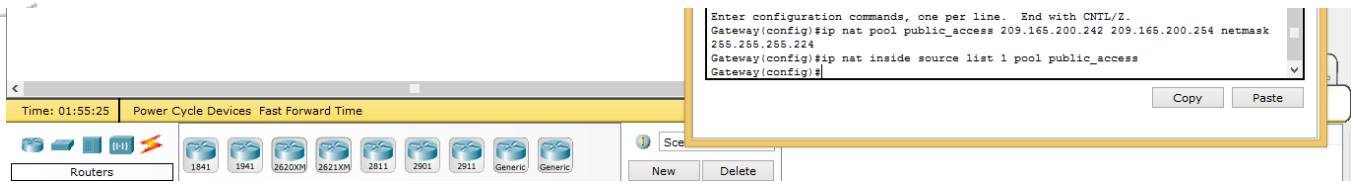
```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```



Step 38: definir la NAT desde la lista de origen interna hasta el conjunto externo.

Nota: recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```



Step 39: probar la configuración.

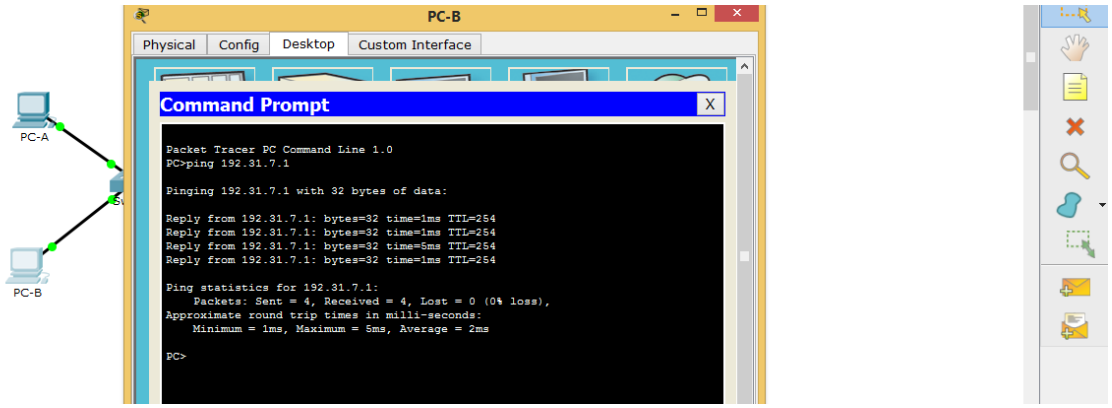
a. En la PC-B, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242    192.168.1.21       ---                ---
```

¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = _ 209.165.200.242 _____

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.



¿Qué número de puerto se usó en este intercambio ICMP? 1, las respuestas varían. _

b. En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.

c. Muestre la tabla de NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80      192.31.7.1:80
```

```
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80     192.31.7.1:80
--- 209.165.200.242    192.168.1.22       ---                ---
```

¿Qué protocolo se usó en esta traducción? __ tcp _____

¿Qué números de puerto se usaron?

Interno: _ 1038 a 1052. Las respuestas varían _____

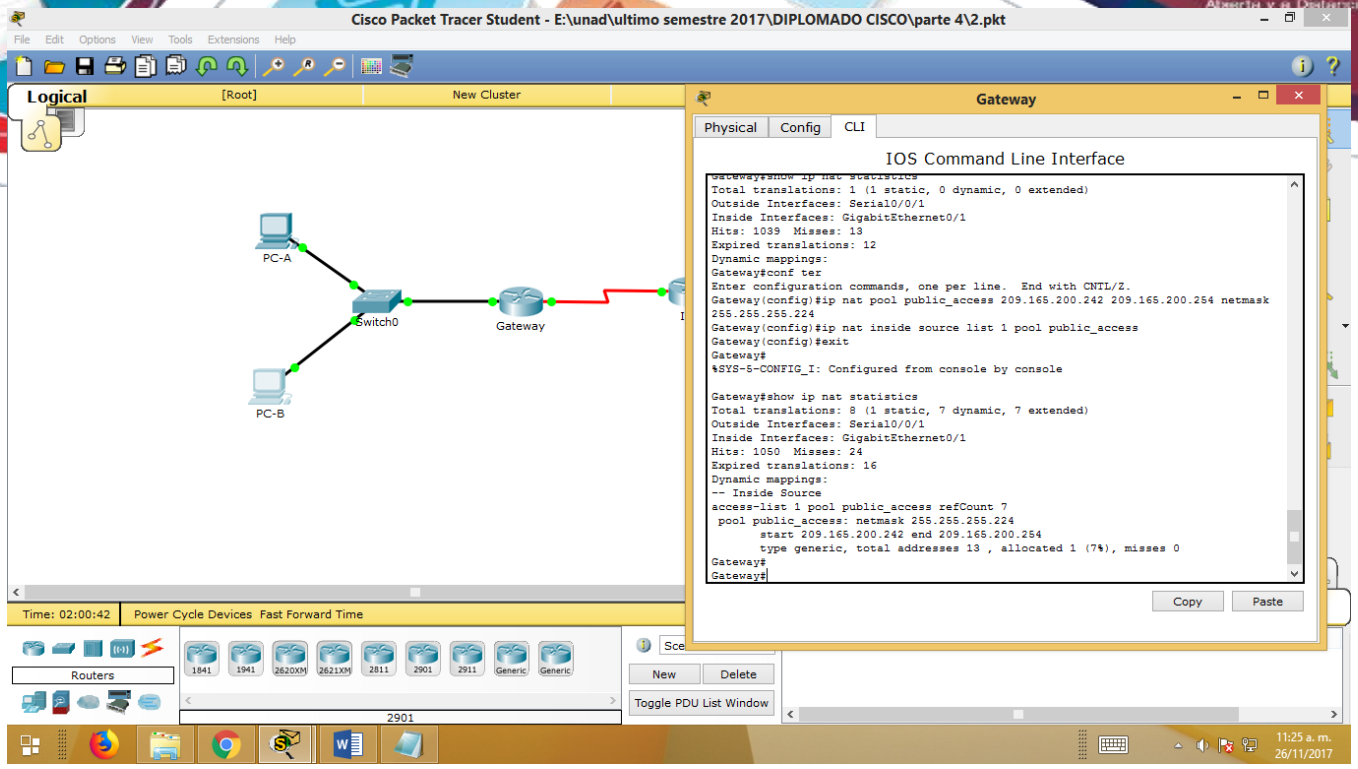
Externo: _ 80 _____

¿Qué número de puerto bien conocido y qué servicio se usaron? __ puerto 80, www o http ___

d. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.



Step 40: eliminar la entrada de NAT estática.

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

```
Gateway(config)# no ip nat inside source static 192.168.1.20
209.165.200.225


Static entry in use, do you want to delete child entries? [no]: yes
```

b. Borre las NAT y las estadísticas.

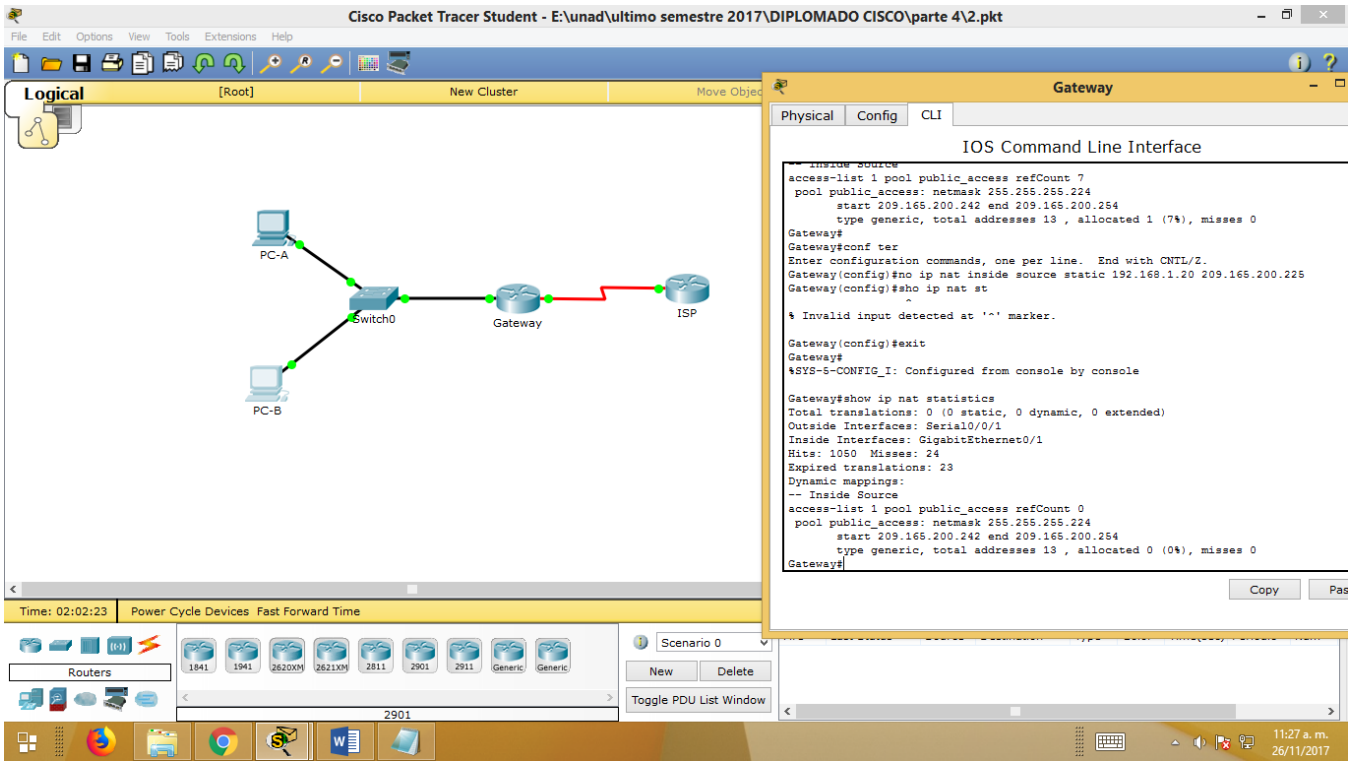
c. Haga ping al ISP (192.31.7.1) desde ambos hosts.

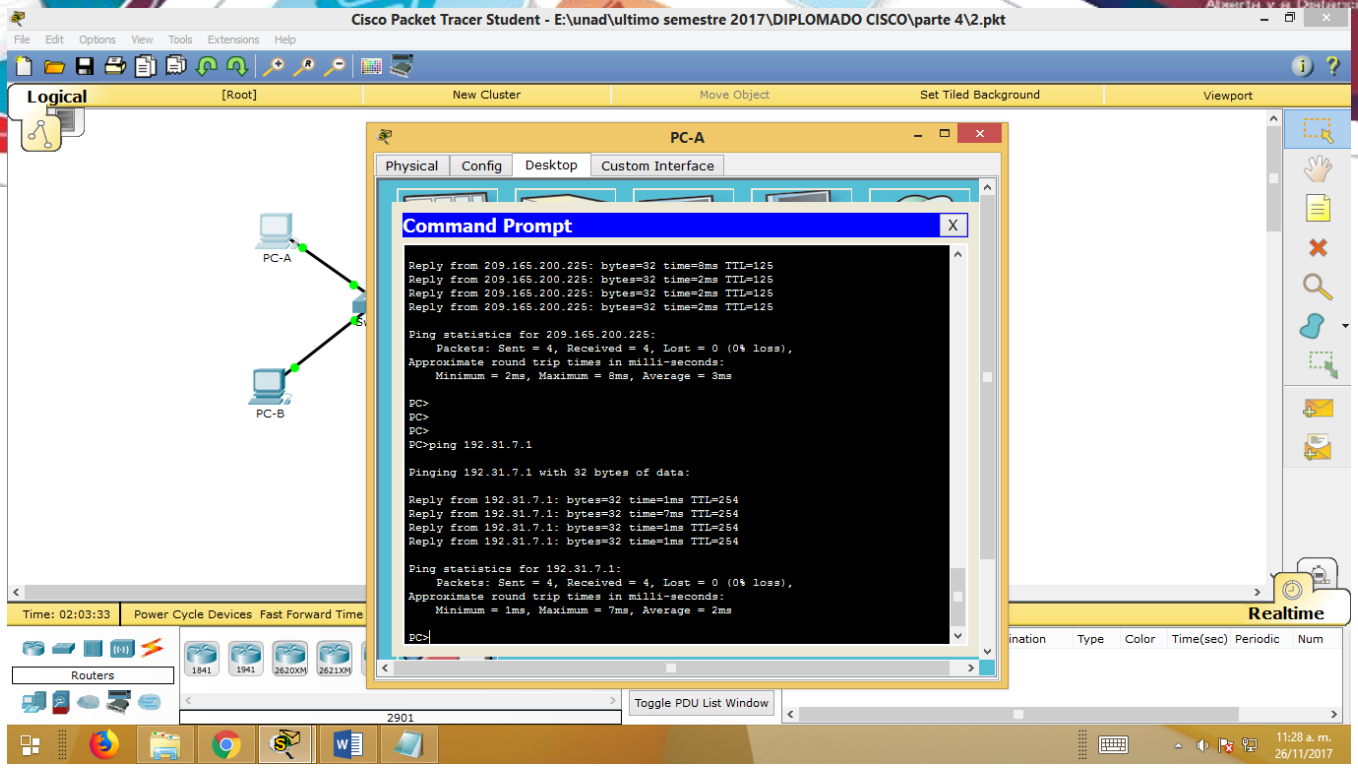
d. Muestre la tabla y las estadísticas de NAT.

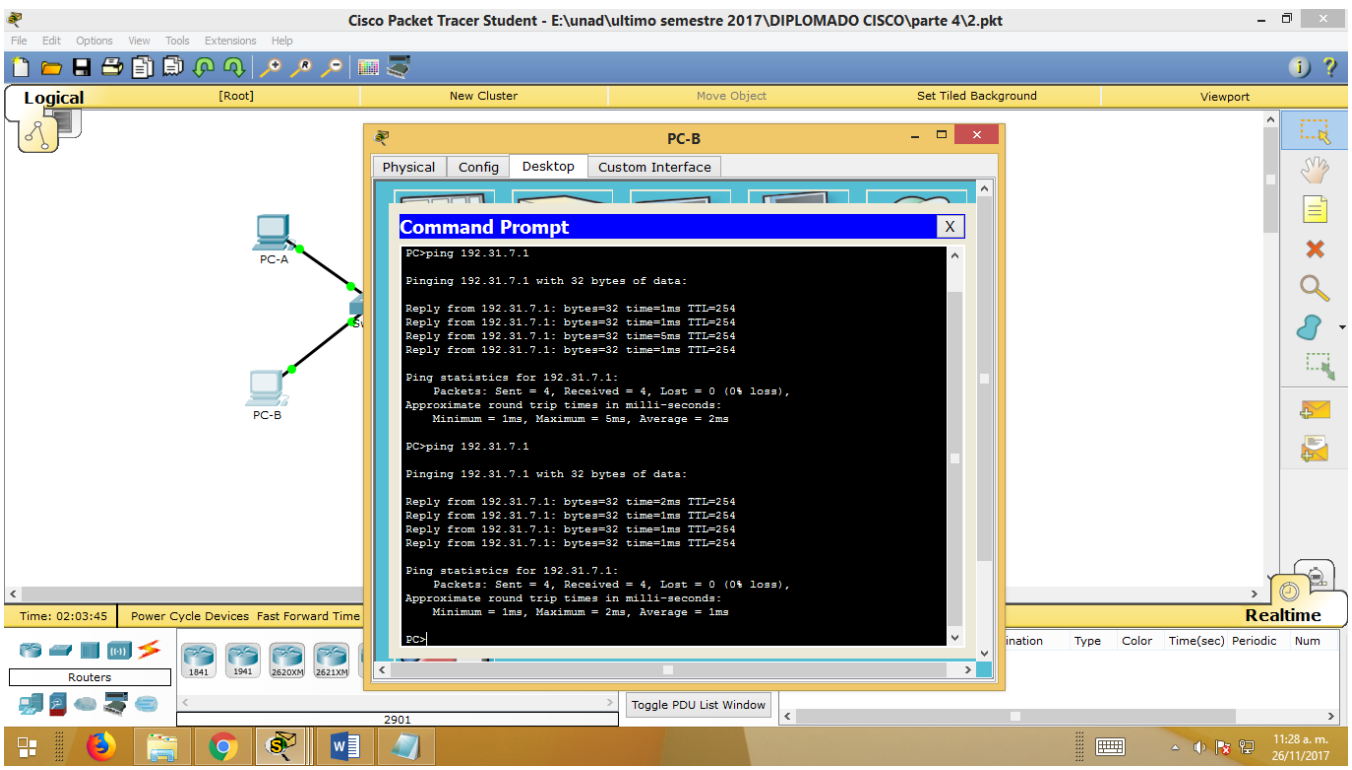
```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16  Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243    192.168.1.20       ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.242    192.168.1.21       ---                ---
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.







Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

Las respuestas varían, pero deberían incluir: siempre que no haya suficientes direcciones IP públicas y para evitar el costo de adquisición de direcciones públicas de un ISP. NAT también puede proporcionar una medida de seguridad al ocultar las direcciones internas de las redes externas.

2. ¿Cuáles son las limitaciones de NAT?

   NAT necesita la información de IP o de números de puerto en el encabezado IP y el encabezado TCP de los paquetes para la traducción. Esta es una lista parcial de los protocolos que no se pueden utilizar con NAT: SNMP, LDAP, Kerberos versión. 5.

la 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.				

Ejercicio No 9 - 11.2.3.7 Lab - Configuring NAT Pool Overload and PAT

Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT

Topología

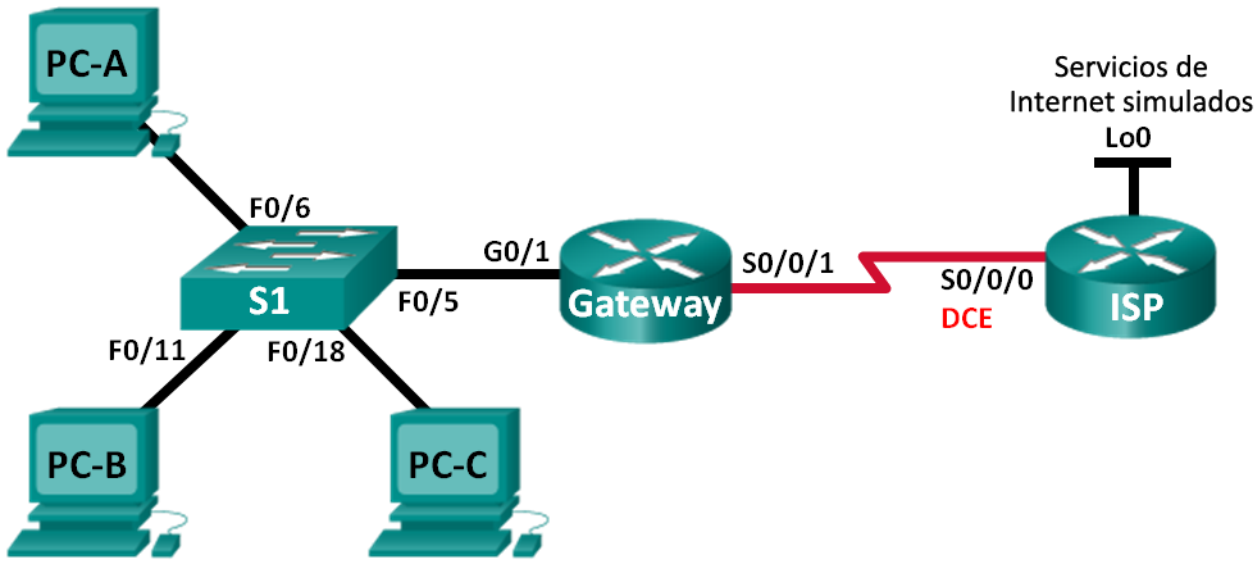


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar un conjunto de NAT con sobrecarga

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

En la parte 2, el ISP asignó una única dirección IP, 209.165.201.18, a su empresa para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Usará la traducción de la dirección del puerto (PAT) para convertir varias direcciones internas en la única dirección pública utilizable. Se probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

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 esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 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

armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

Step 41: realizar el cableado de red tal como se muestra en la topología.

Step 42: configurar los equipos host.

Step 43: inicializar y volver a cargar los routers y los switches.

Step 44: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

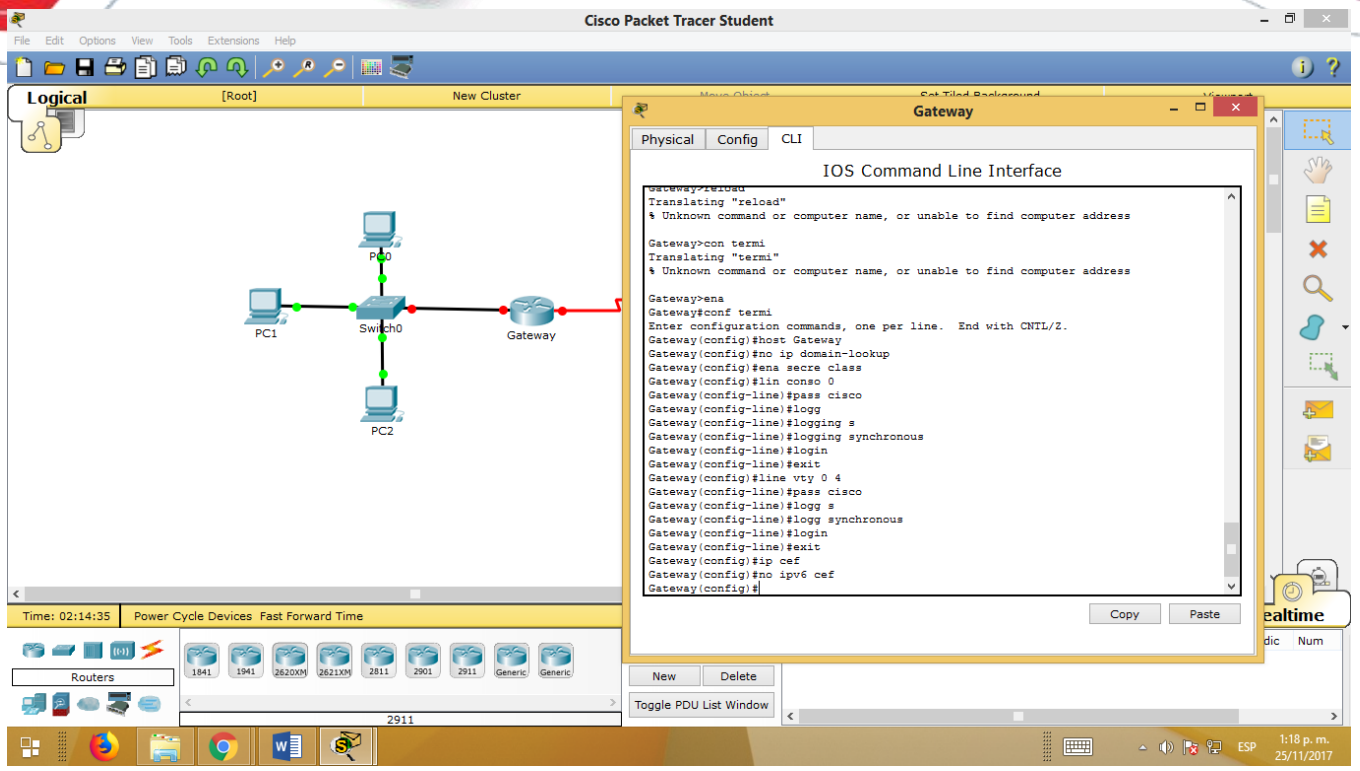
c. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

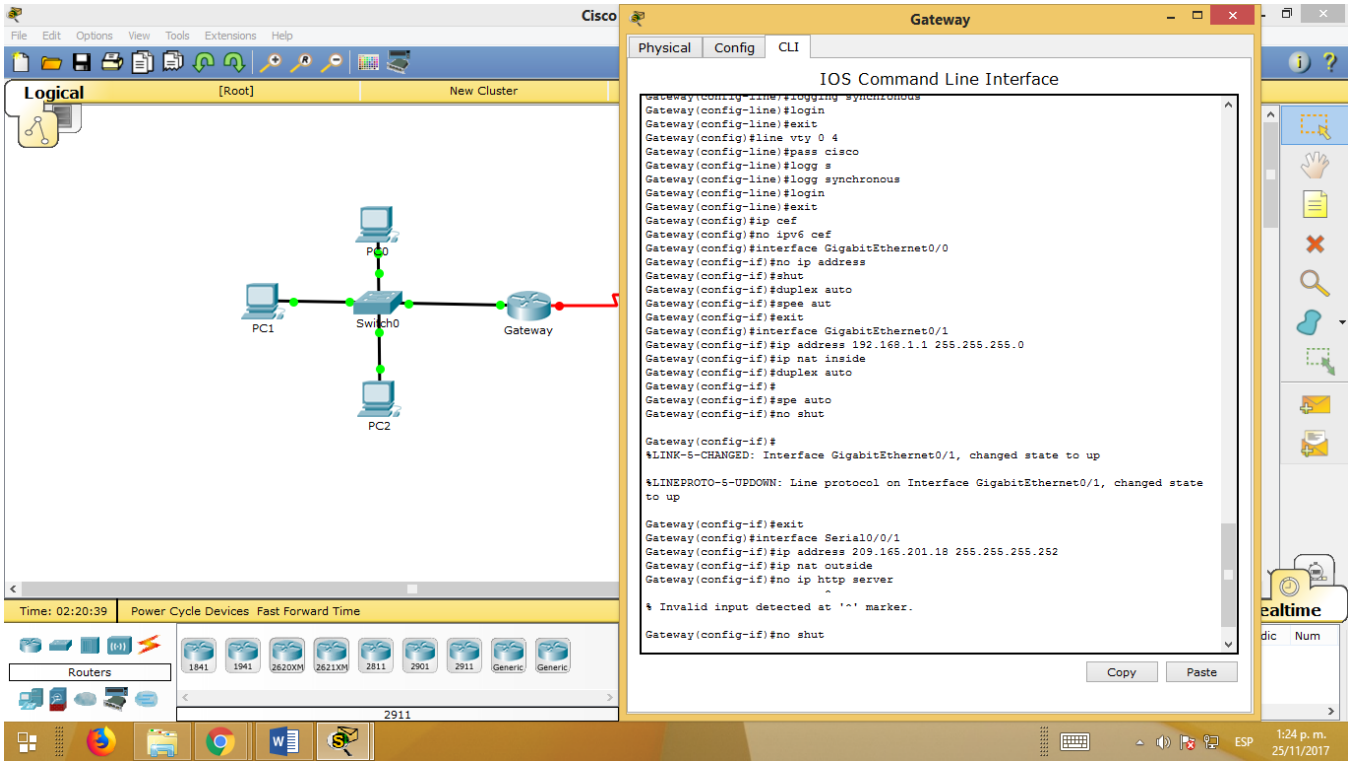
d. Configure el nombre del dispositivo como se muestra en la topología.

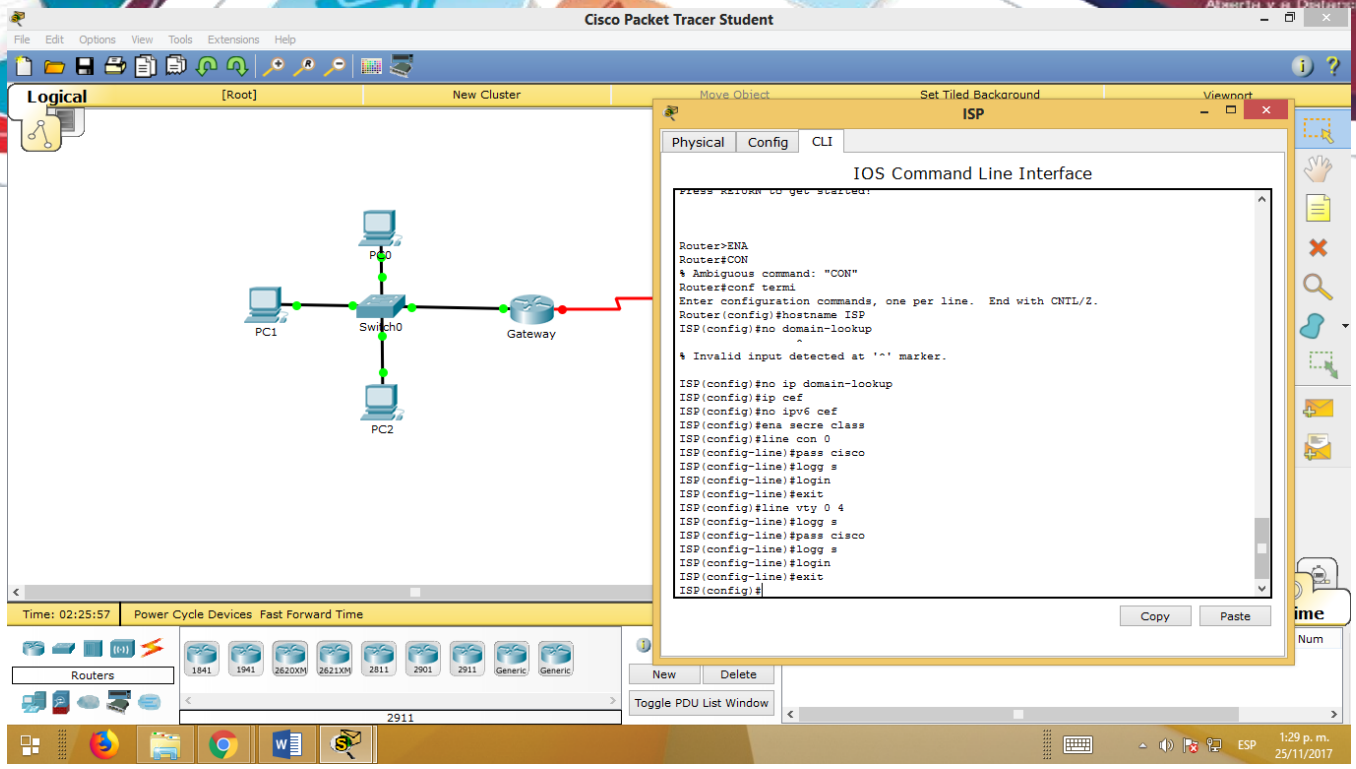
e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

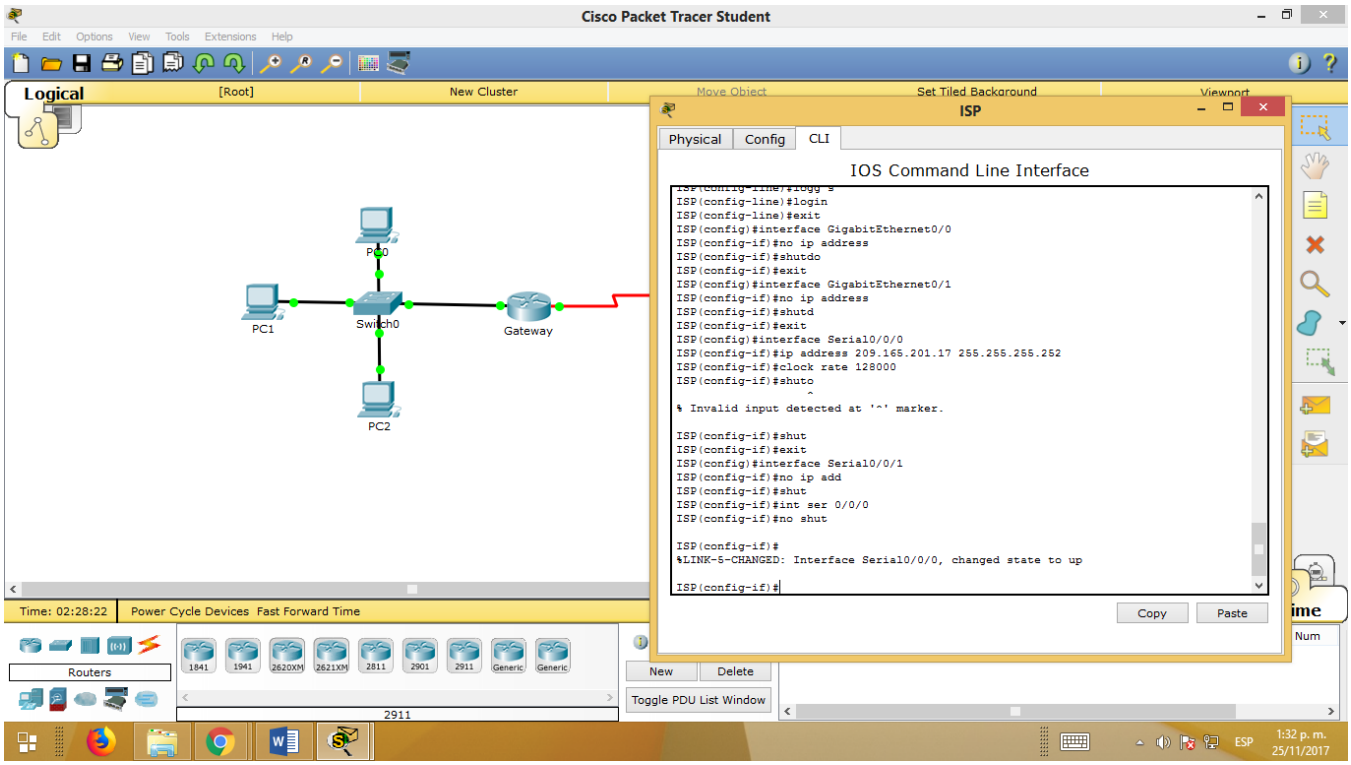
f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.






Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC0
PC1
Switch0
Gateway
PC2
ISP
Physical
Config
CLI
IOS Command Line Interface
Router>ENA
Router#CON
% Ambiguous command: "CON"
Router#conf termi
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#no domain-lookup
% Invalid input detected at '^' marker.
ISP(config)#no ip domain-lookup
ISP(config)#ip cef
ISP(config)#no ipv6 cef
ISP(config)#ena secre class
ISP(config)#line con 0
ISP(config-line)#pass cisco
ISP(config-line)#logg s
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#logg s
ISP(config-line)#pass cisco
ISP(config-line)#logg s
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#
Copy
Paste
Time: 02:25:57
Power Cycle Devices Fast Forward Time
Routers
2911
New
Delete
Toggle PDU List Window
Num
ESP
1:29 p. m.
25/11/2017


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC0
PC1
Switch0
Gateway
PC2
ISP
Physical
Config
CLI
IOS Command Line Interface
ISP(config-line)#logg s
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#interface GigabitEthernet0/0
ISP(config-if)#no ip address
ISP(config-if)#shutdo
ISP(config-if)#exit
ISP(config)#interface GigabitEthernet0/1
ISP(config-if)#no ip address
ISP(config-if)#shutd
ISP(config-if)#exit
ISP(config)#interface Serial0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#shuto
% Invalid input detected at '^' marker.
ISP(config-if)#shut
ISP(config-if)#exit
ISP(config)#interface Serial0/0/1
ISP(config-if)#no ip add
ISP(config-if)#shut
ISP(config-if)#int ser 0/0/0
ISP(config-if)#no shut
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
ISP(config-if)#
Copy
Paste
Time: 02:28:22
Power Cycle Devices Fast Forward Time
Routers
2911
New
Delete
Toggle PDU List Window
Num
ESP
1:32 p. m.
25/11/2017

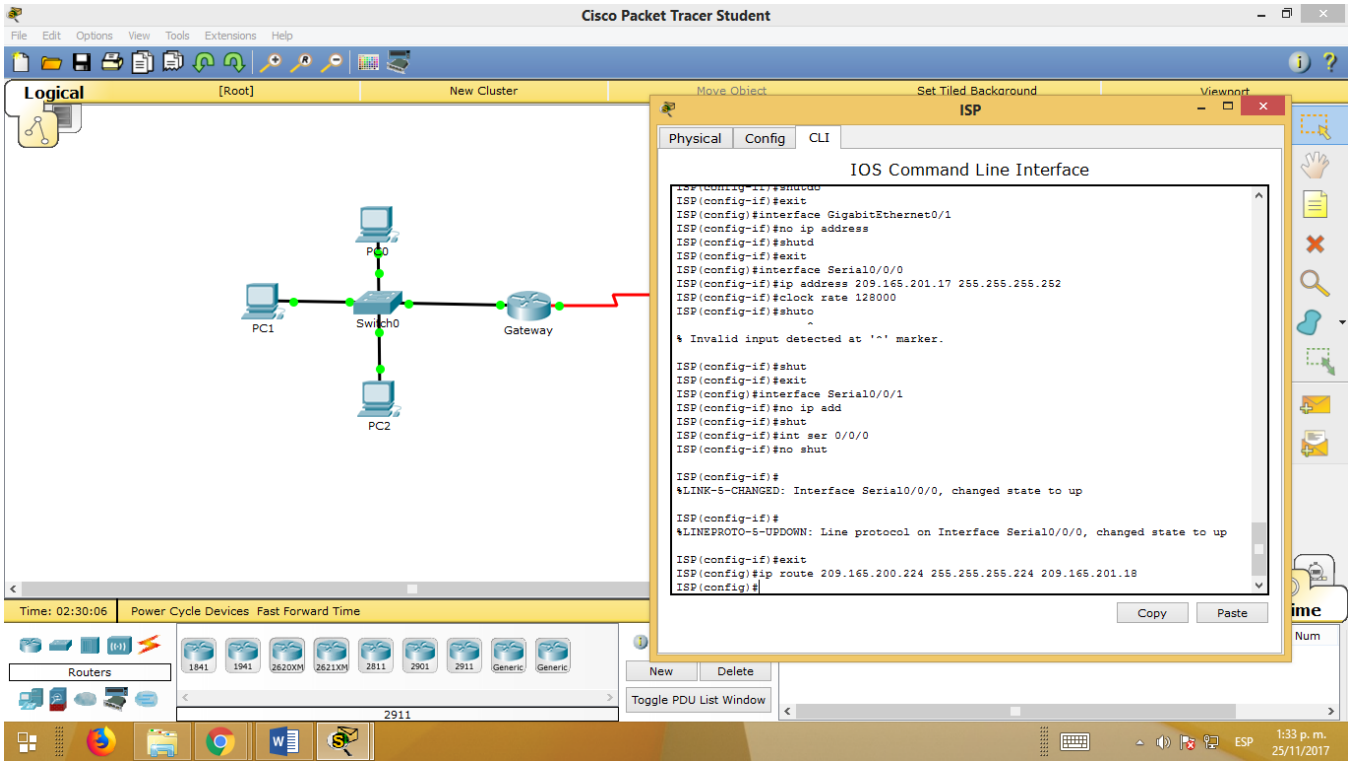
Step 45: configurar el routing estático.

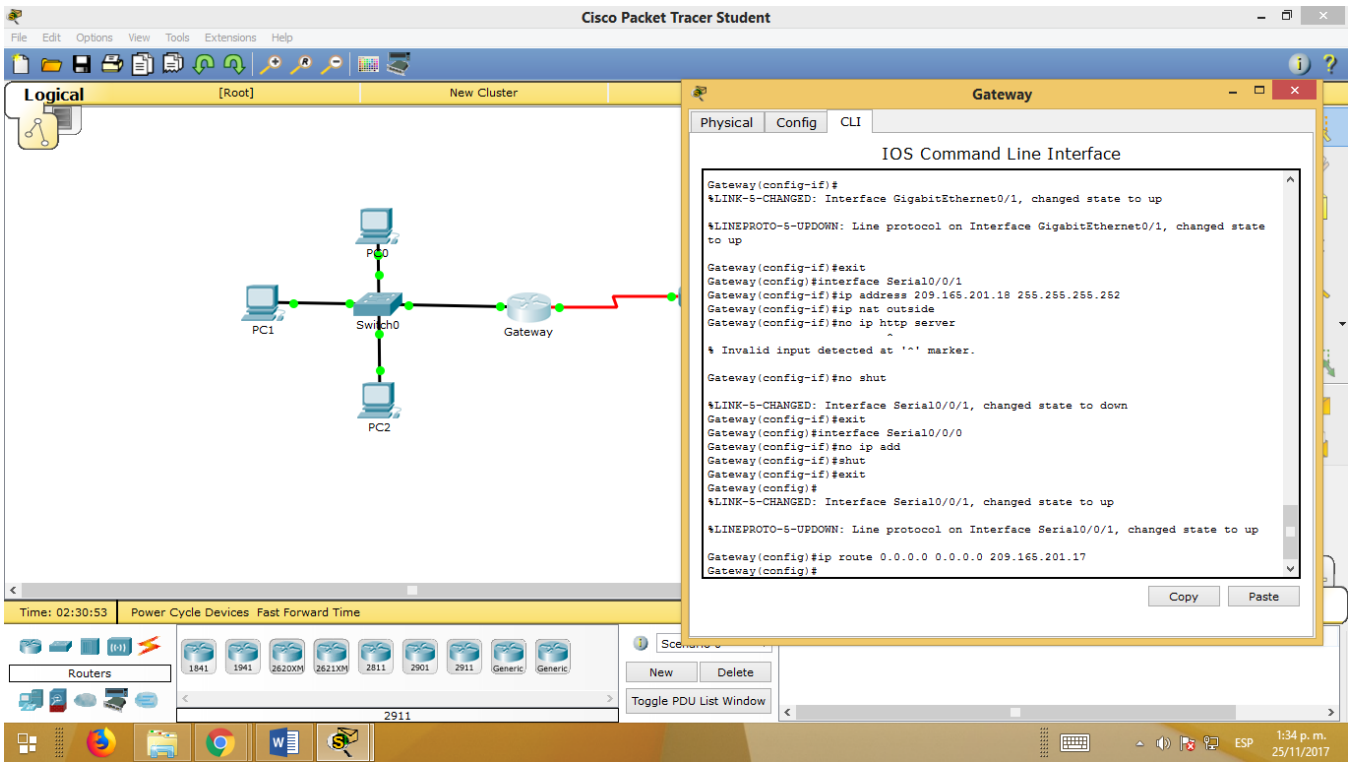
a. Cree una ruta estática desde el router ISP hasta el router Gateway.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

b. Cree una ruta predeterminada del router Gateway al router ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

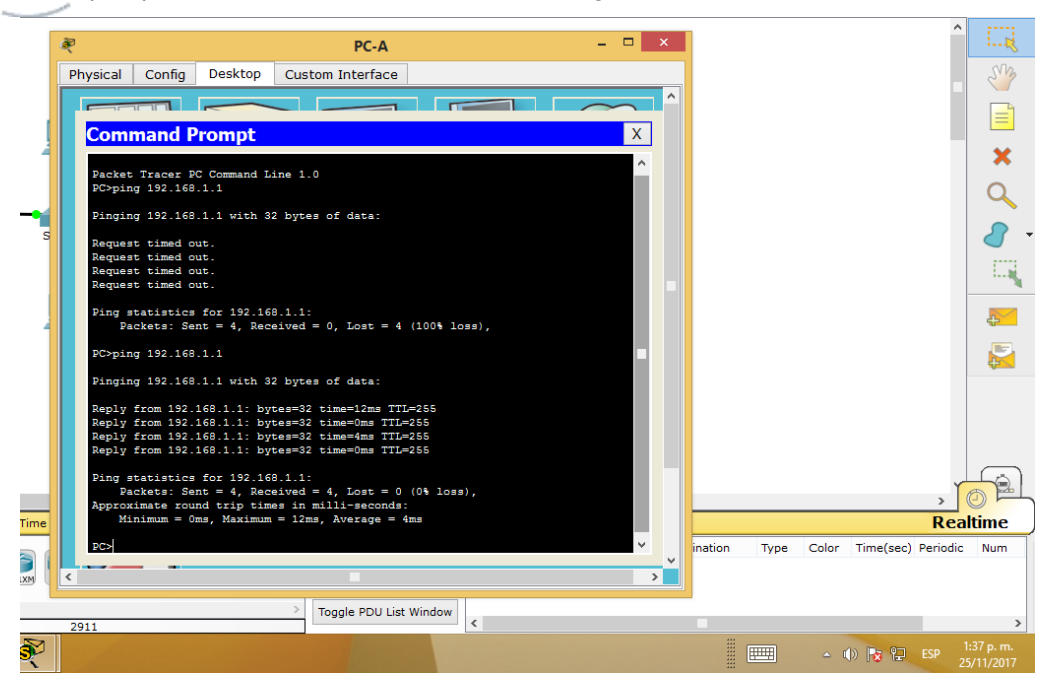




Step 46: Verificar la conectividad de la red

a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.



configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

Step 47: definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 48: definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.225
209.165.200.230 netmask 255.255.255.248
```

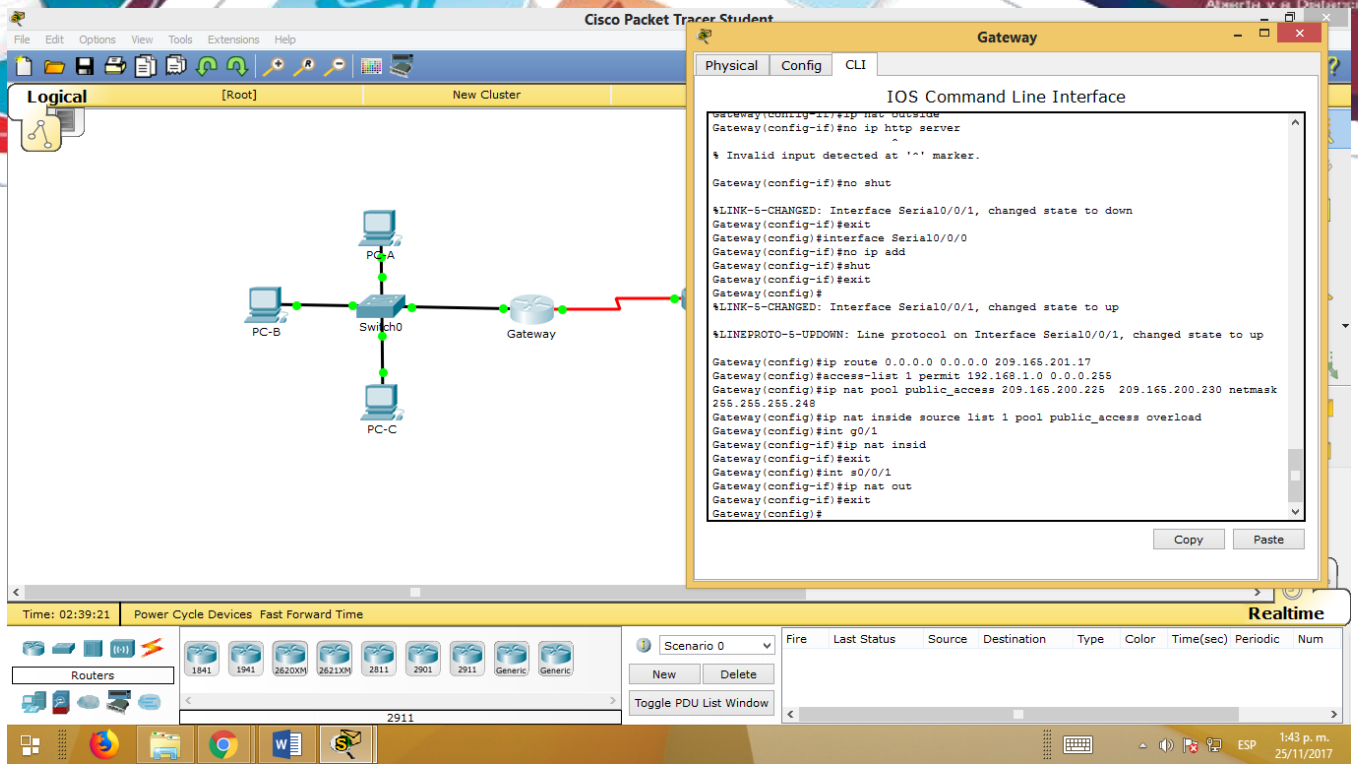
Step 49: definir la NAT desde la lista de origen interna hasta el conjunto externo.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

Step 50: Especifique las interfaces.

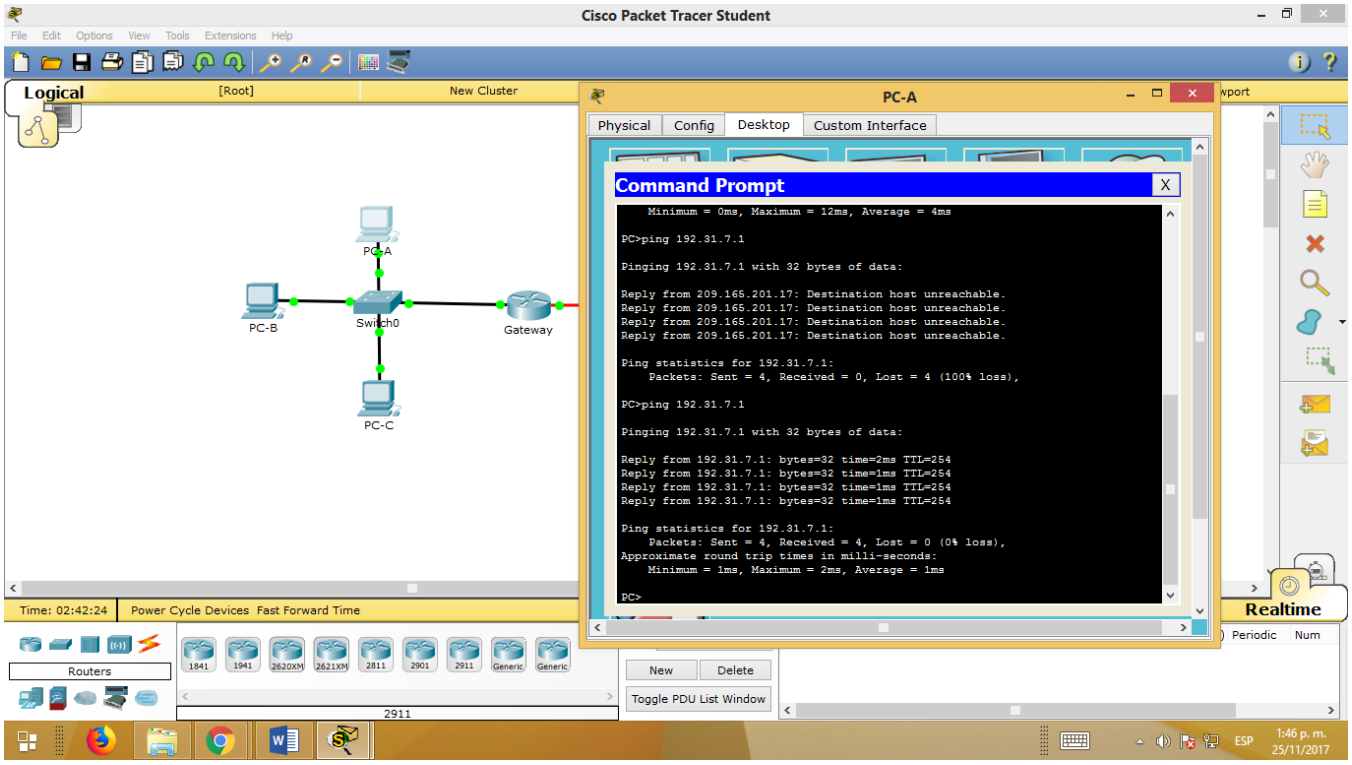
Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```



Step 51: verificar la configuración del conjunto de NAT con sobrecarga.

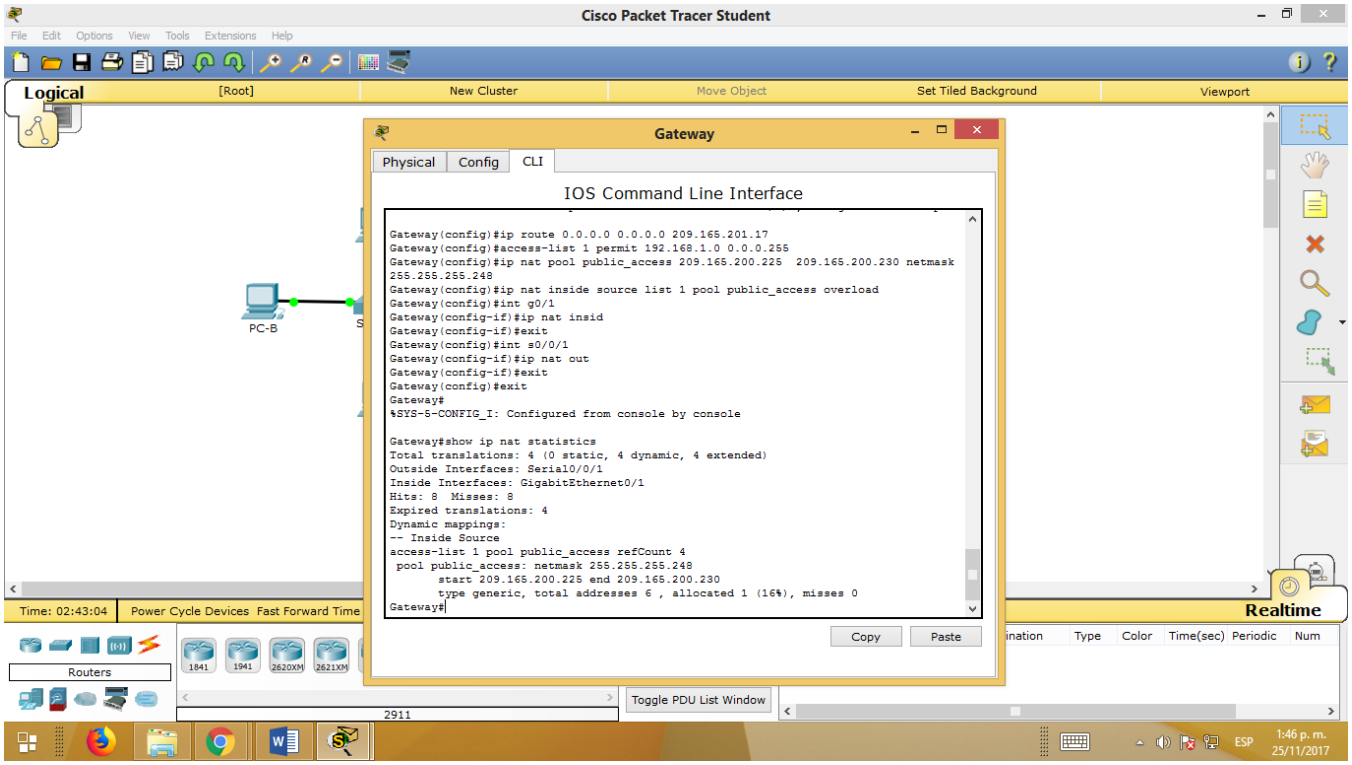
a. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.



b. Muestre las estadísticas de NAT en el router Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
```

```
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
 pool public_access: netmask 255.255.255.248
        start 209.165.200.225 end 209.165.200.230
        type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```



c. Muestre las NAT en el router Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:0 192.168.1.20:1     192.31.7.1:1       192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1     192.31.7.1:1       192.31.7.1:2
```

Nota: es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior?
____3_____

¿Cuántas direcciones IP globales internas se indican? ___1_____

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas?
___3_____

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

El ping fallaría debido a que el router conoce la ubicación de la dirección global interna en la tabla de routing, pero la dirección local interna no se anuncia.

configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Step 52: borrar las NAT y las estadísticas en el router Gateway.

Step 53: verificar la configuración para NAT.

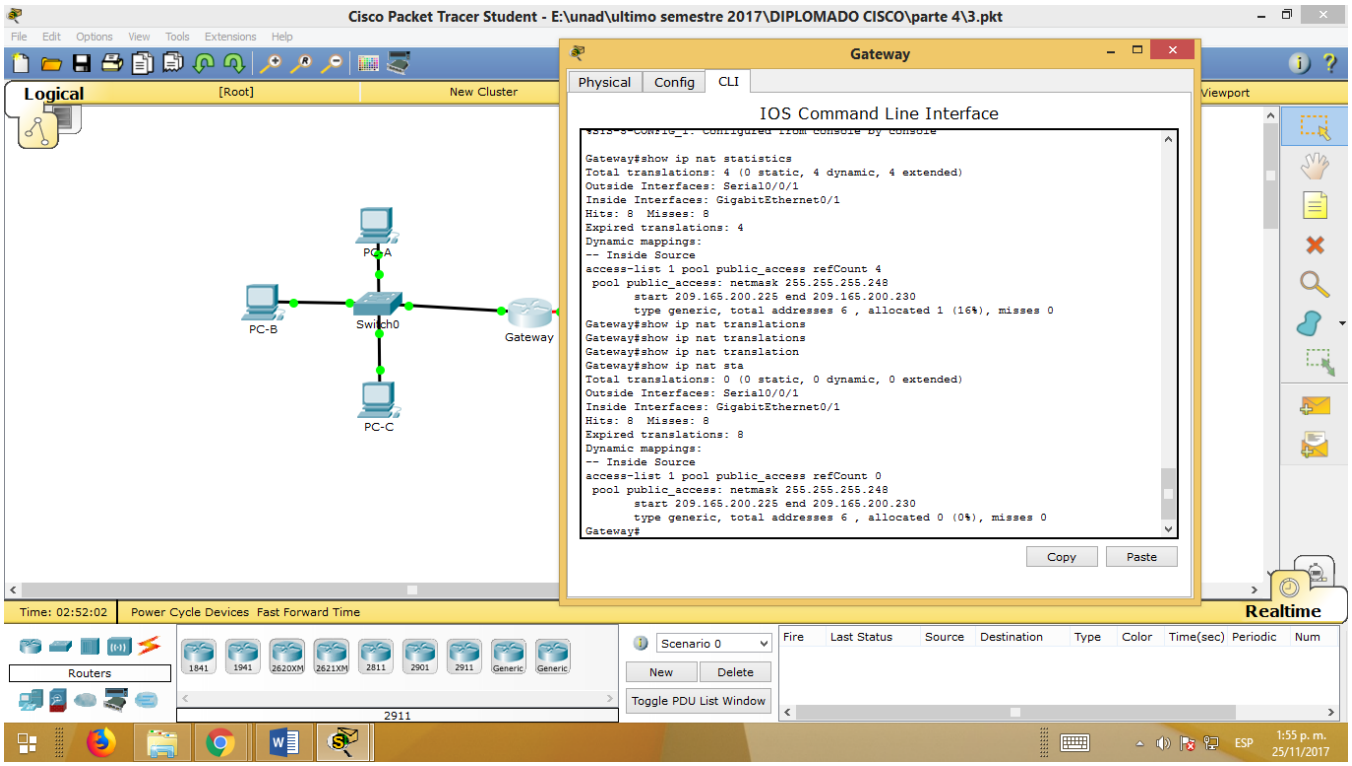
a. Verifique que se hayan borrado las estadísticas.

b. Verifique que las interfaces externa e interna estén configuradas para NAT.

c. Verifique que la ACL aún esté configurada para NAT.

¿Qué comando usó para confirmar los resultados de los pasos a al c?

Gateway# show ip nat statistics



Step 54: eliminar el conjunto de direcciones IP públicas utilizables.

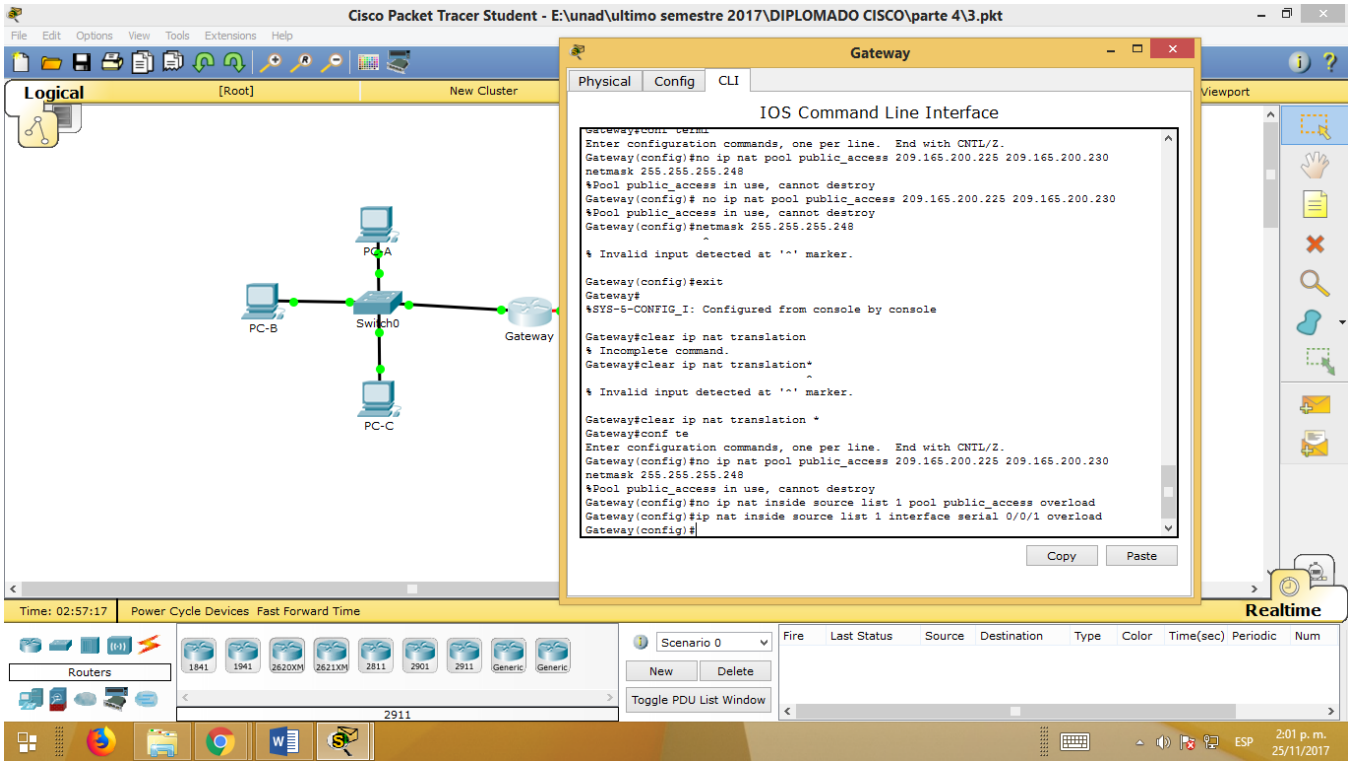
```
Gateway(config)# no ip nat pool public_access 209.165.200.225
209.165.200.230 netmask 255.255.255.248
```

Step 55: eliminar la traducción NAT de la lista de origen interna al conjunto externo.

```
Gateway(config)# no ip nat inside source list 1 pool public_access
overload
```

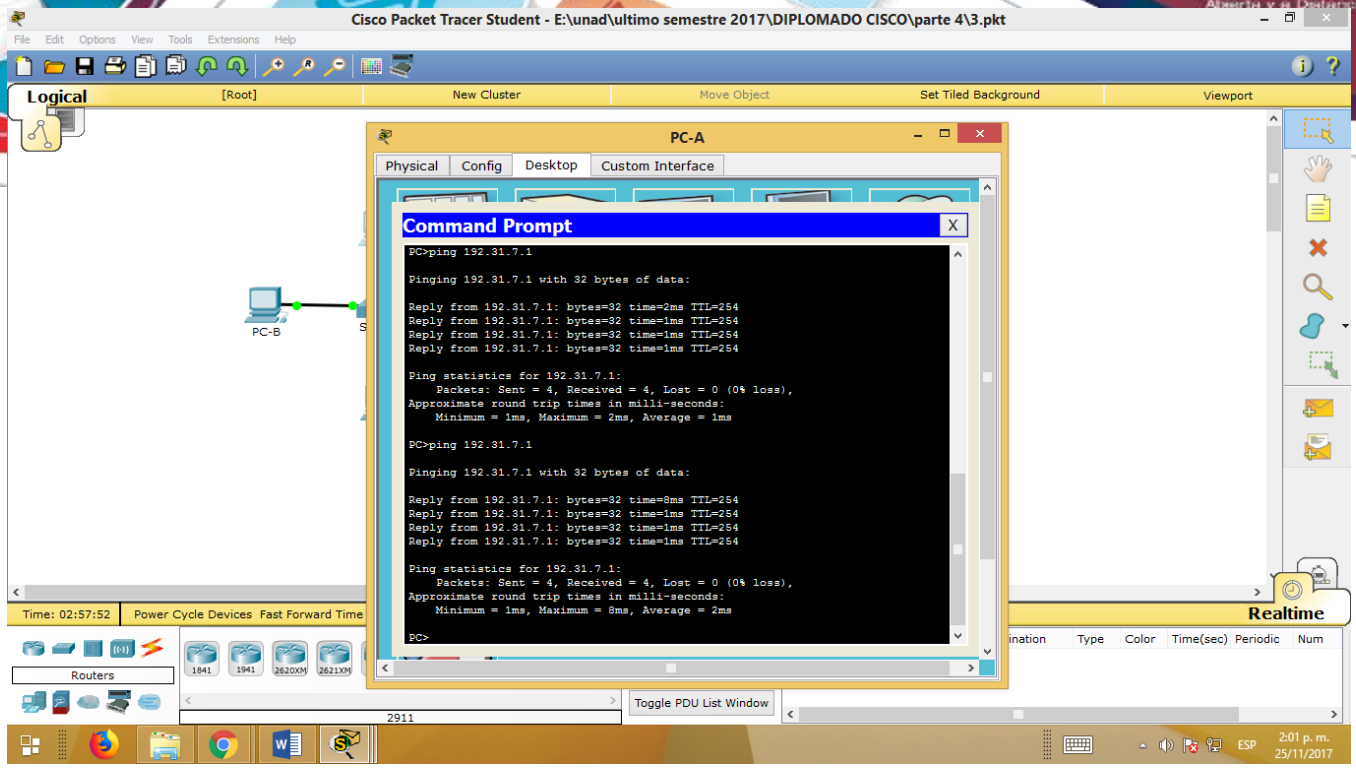
Step 56: asociar la lista de origen a la interfaz externa.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1
overload
```



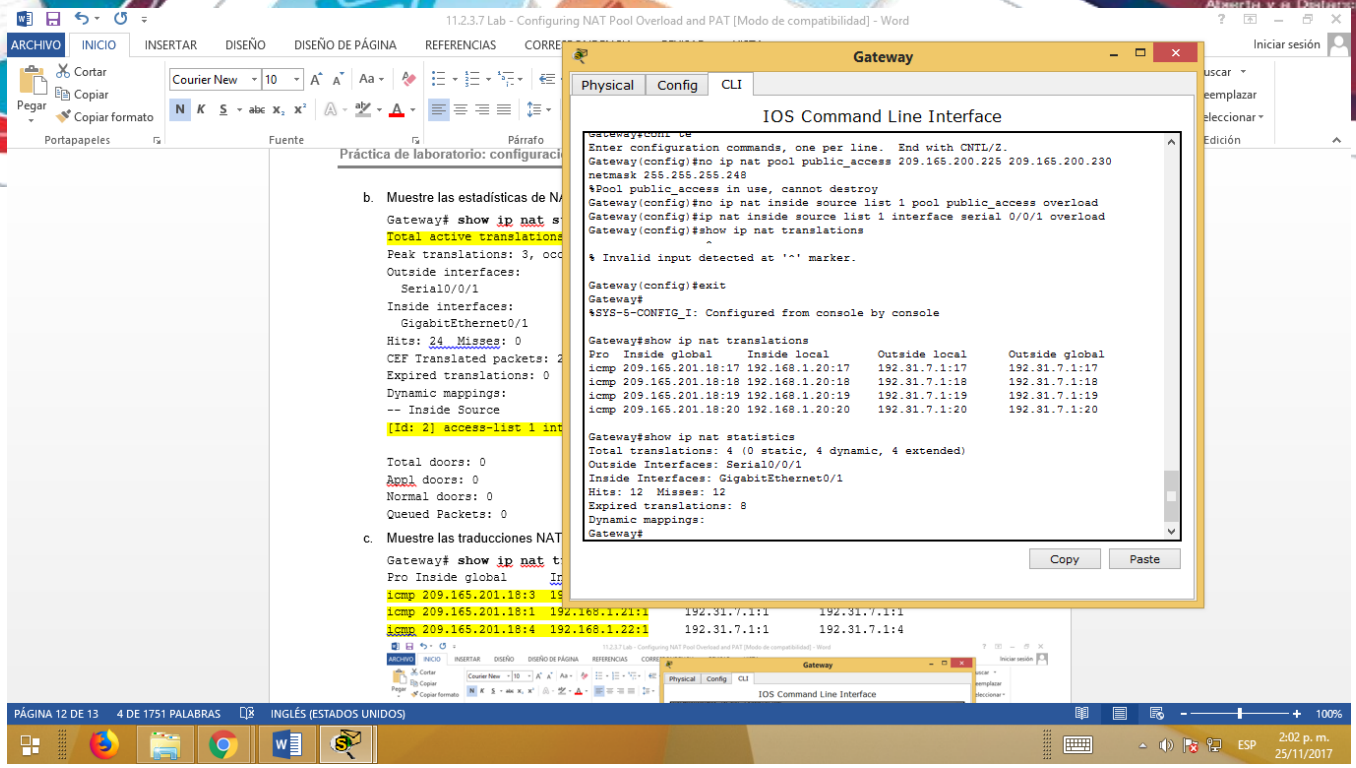
Step 57: probar la configuración PAT.

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.



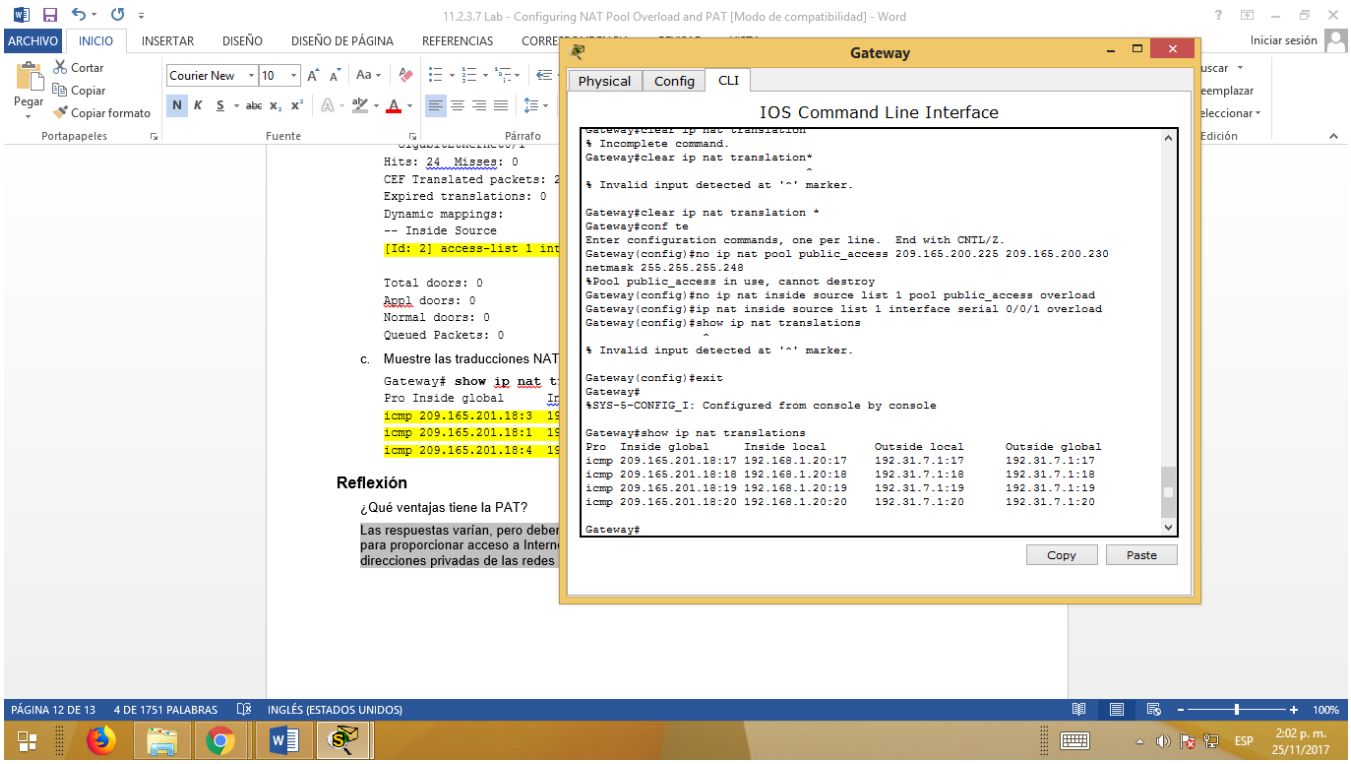
b. Muestre las estadísticas de NAT en el router Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```



c. Muestre las traducciones NAT en el Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.201.18:3  192.168.1.20:1     192.31.7.1:1       192.31.7.1:3
icmp 209.165.201.18:1  192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.201.18:4  192.168.1.22:1     192.31.7.1:1       192.31.7.1:4
```



Reflexión

¿Qué ventajas tiene la PAT?

Las respuestas varían, pero deben incluir que PAT minimiza la cantidad de direcciones públicas necesarias para proporcionar acceso a Internet y que los servicios de PAT, como los de NAT, sirven para "ocultar" las direcciones privadas de las redes externas.

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)

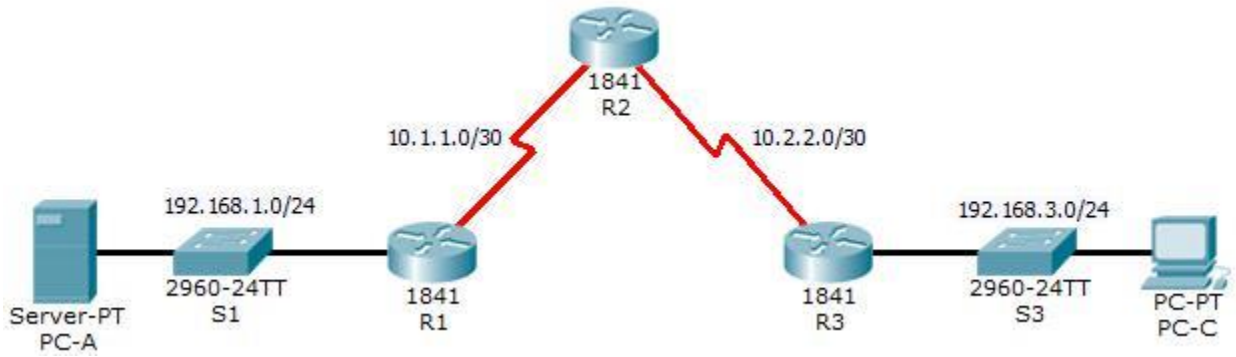
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores 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.

Ejercicio No 10 - 4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks_Instructor

Packet Tracer - Configure IP ACLs to Mitigate Attacks (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A

	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Objectives

ϕ. Verify connectivity among devices before firewall configuration.

γ. Use ACLs to ensure remote access to the routers is available only from management station PC-C.

η. Configure ACLs on R1 and R3 to mitigate attacks.

ι. Verify ACL functionality.

Background / Scenario

Access to routers R1, R2, and R3 should only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, a server providing DNS, SMTP, FTP, and HTTPS services.

Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and/or destination IP address. In this activity, you create ACLs on edge routers R1 and R3 to achieve this goal. You then verify ACL functionality from internal and external hosts.

The routers have been pre-configured with the following:

g. Enable password: **ciscoenpa55**

a. Password for console:
ciscoconpa55 ○ Username for VTY
lines: **SSHadmin**

○ Password for VTY lines:
ciscosshpa55 ○ IP addressing

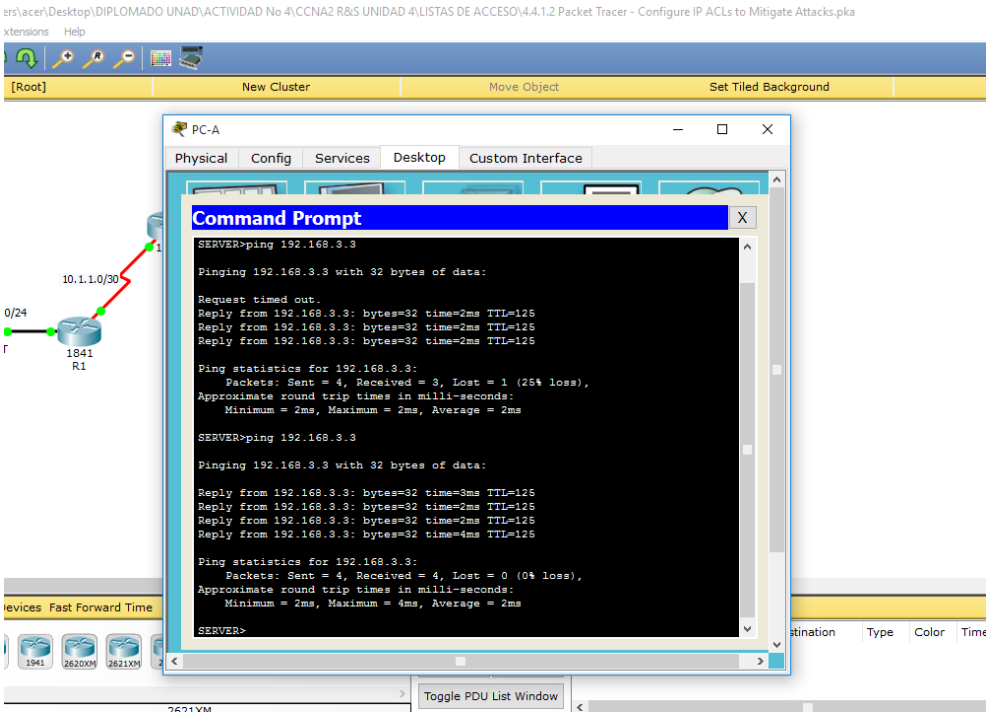
- Static routing

Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

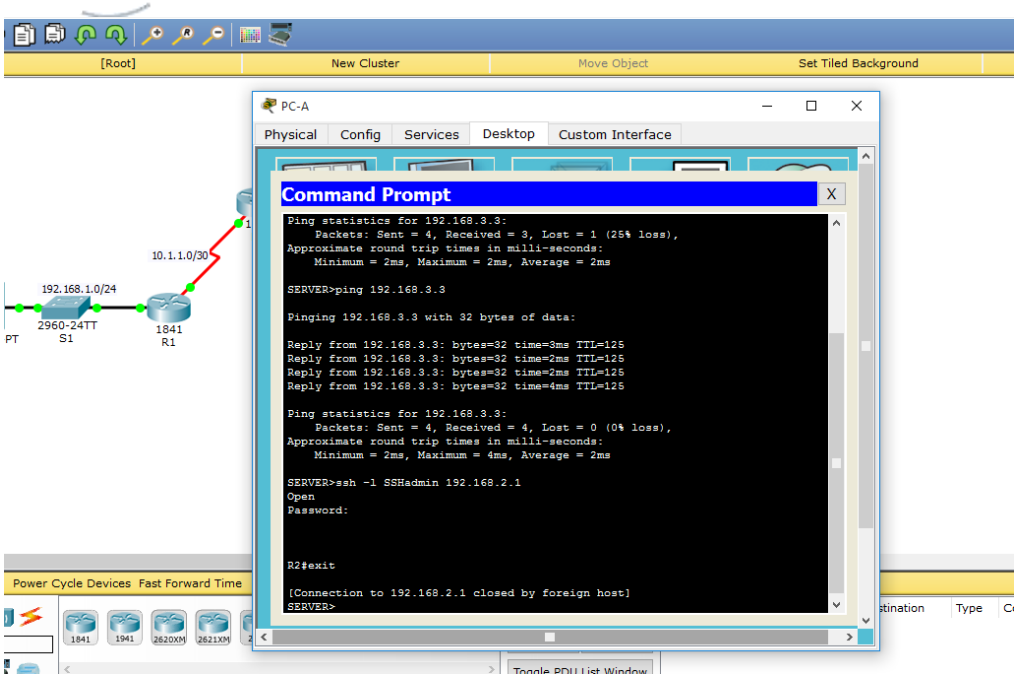
Step 1: From PC-A, verify connectivity to PC-C and R2.

a. From the command prompt, ping **PC-C** (192.168.3.3).



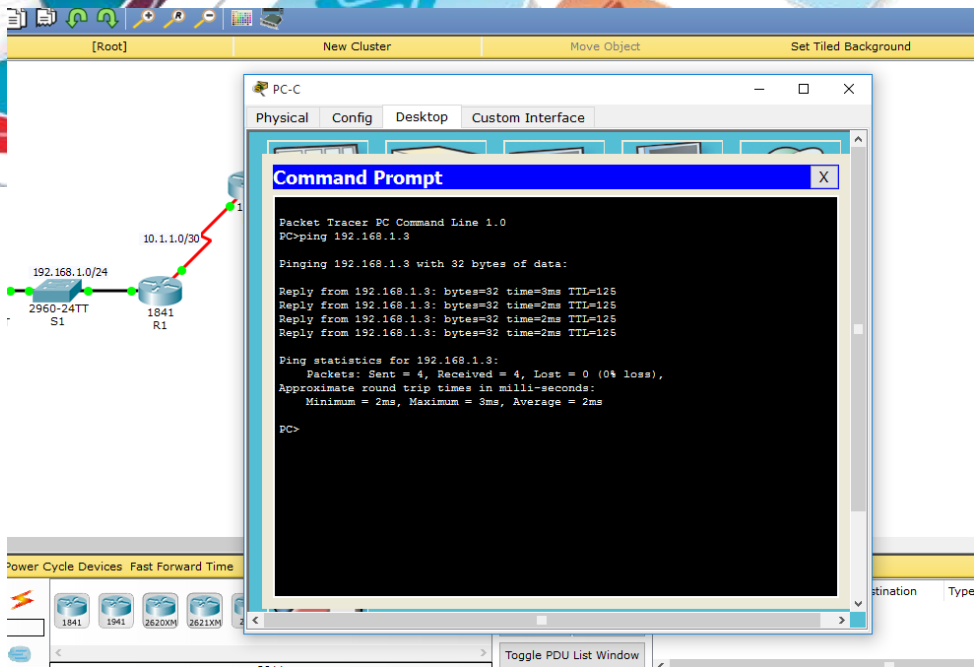
b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. When finished, exit the SSH session.

```
PC> ssh -l SSHadmin 192.168.2.1
```



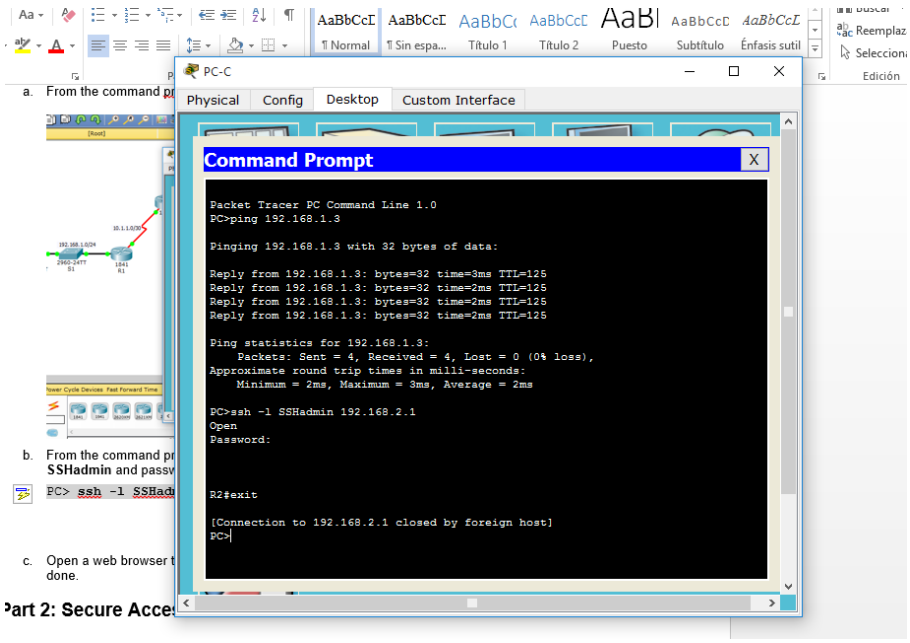
Step 2: From PC-C, verify connectivity to PC-A and R2.

a. From the command prompt, ping **PC-A** (192.168.1.3).

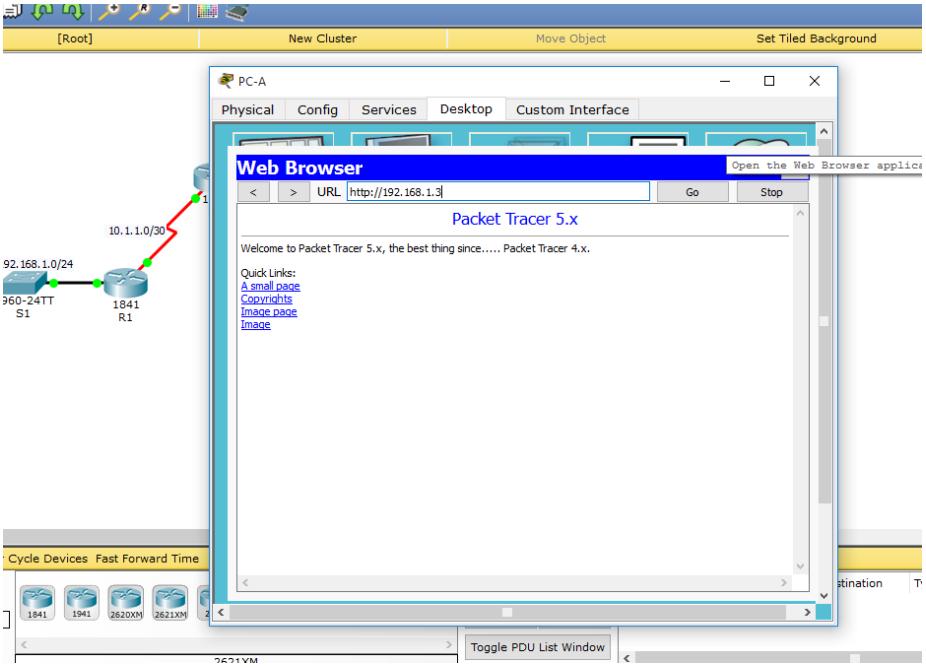


b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. Close the SSH session when finished.

```
PC> ssh -l SSHadmin 192.168.2.1
```



c. Open a web browser to the **PC-A** server (192.168.1.3) to display the web page. Close the browser when done.



Part 2: Secure Access to Routers

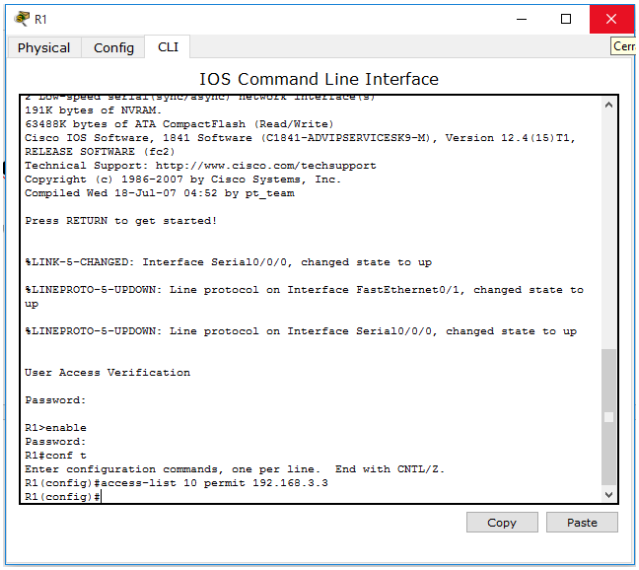
Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.

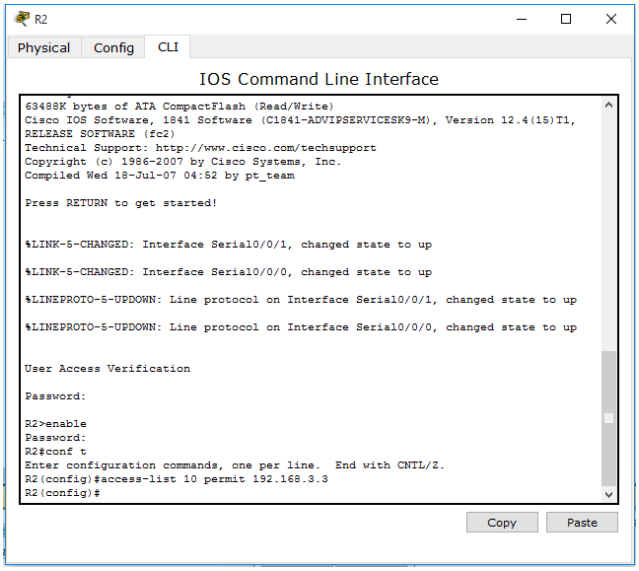
Use the **access-list** command to create a numbered IP ACL on **R1**, **R2**, and **R3**.

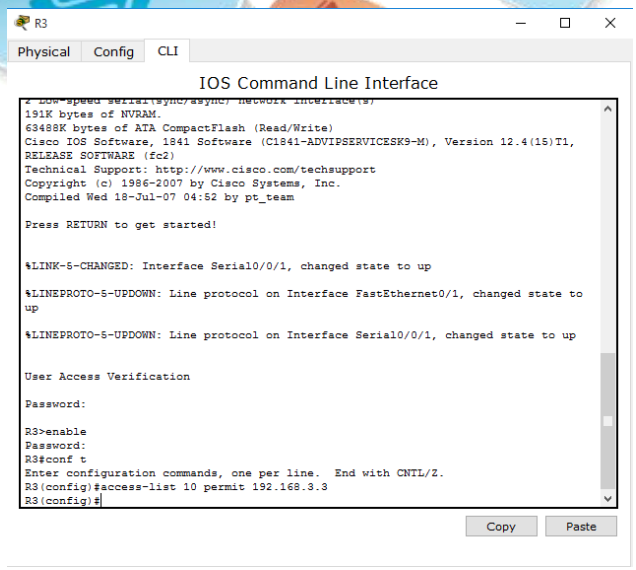
```
R1(config)# access-list 10 permit 192.168.3.3 0.0.0.0
```

```
R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0
```

```
R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0
```


R1
Physical
Config
CLI
IOS Command Line Interface
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
User Access Verification
Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3
R1(config)#
Copy
Paste


R2
Physical
Config
CLI
IOS Command Line Interface
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
User Access Verification
Password:
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3
R2(config)#
Copy
Paste



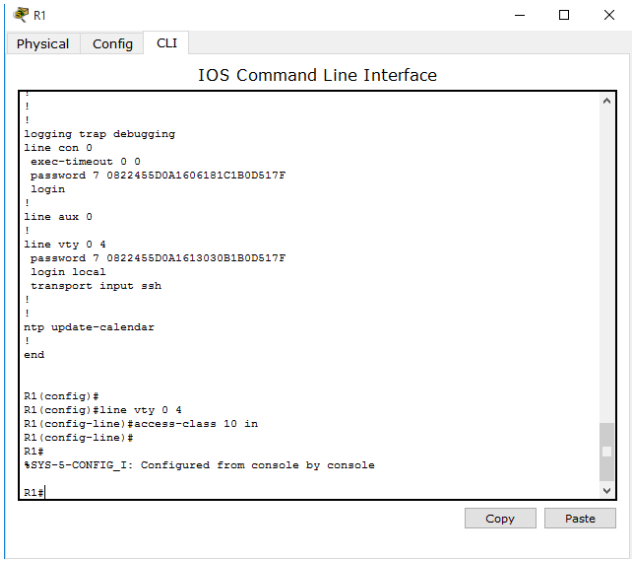
Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

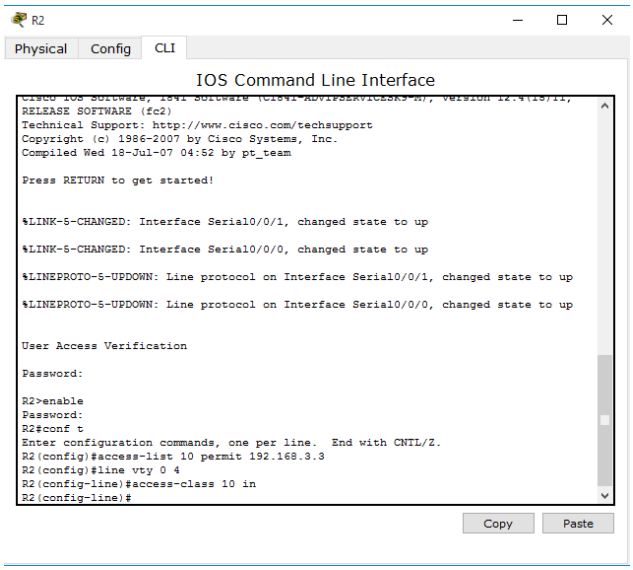
Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

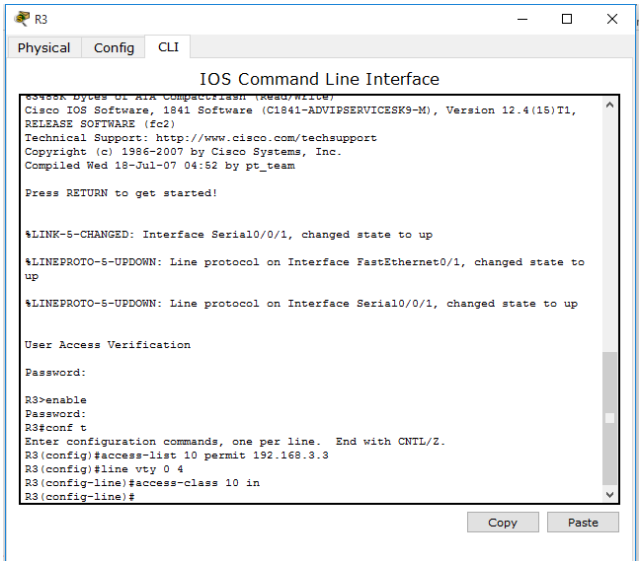
```
R1(config-line)# access-class 10 in
```

```
R2(config-line)# access-class 10 in
```

```
R3(config-line)# access-class 10 in
```



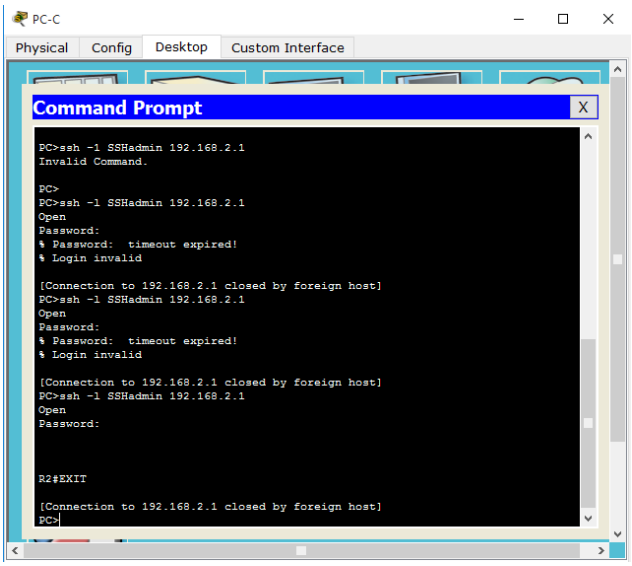

R2
Physical
Config
CLI
IOS Command Line Interface
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
User Access Verification
Password:
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#
Copy
Paste


R3
Physical
Config
CLI
IOS Command Line Interface
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
User Access Verification
Password:
R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#
Copy
Paste

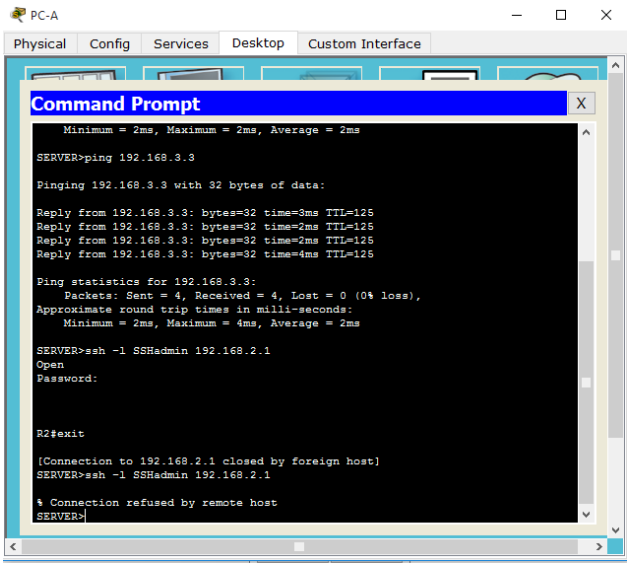
Step 3: Verify exclusive access from management station PC-C.

a. Establish a SSH session to 192.168.2.1 from **PC-C** (should be successful).

```
PC> ssh -l SSHadmin 192.168.2.1
```



b. Establish a SSH session to 192.168.2.1 from **PC-A** (should fail).

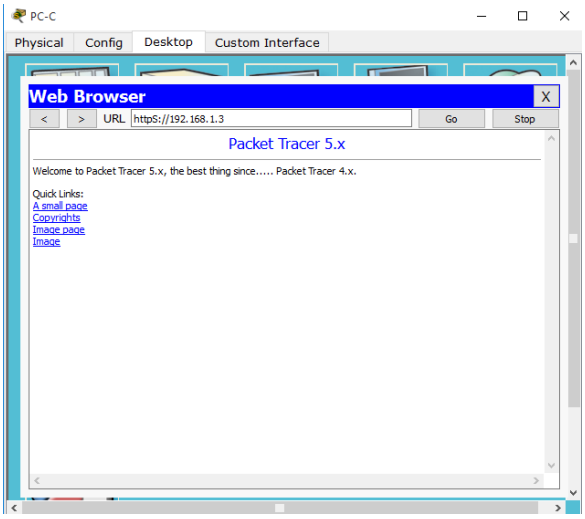


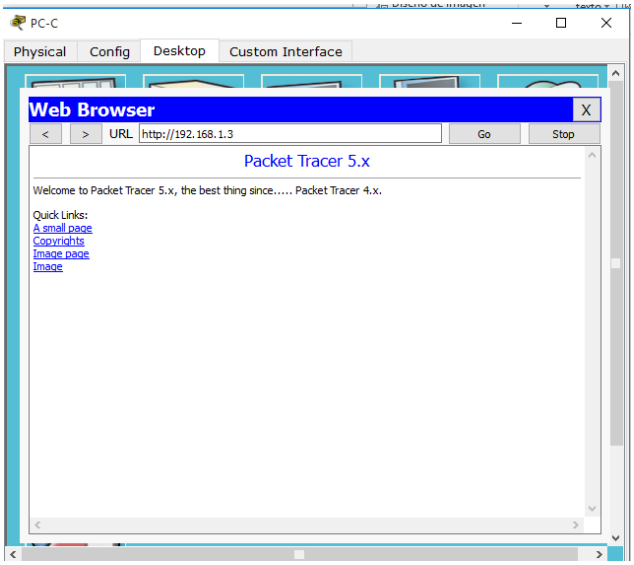
Part 3: Create a Numbered IP ACL 120 on R1

Permit any outside host to access DNS, SMTP, and FTP services on server **PC-A**, deny any outside host access to HTTPS services on **PC-A**, and permit **PC-C** to access **R1** via SSH.

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server **PC-A**.

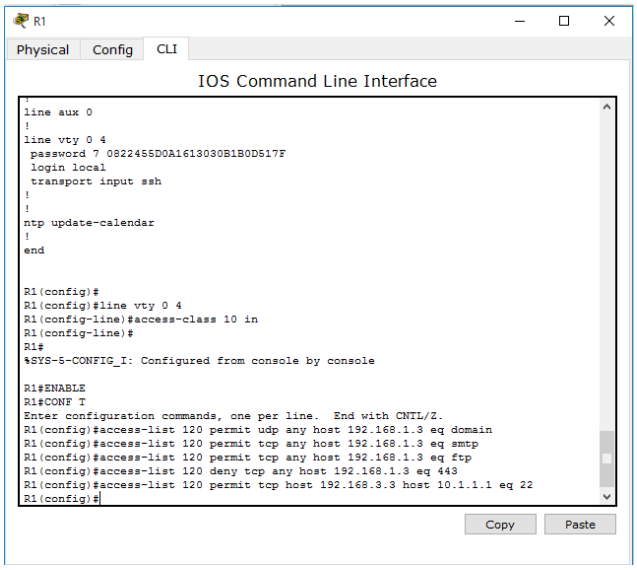




Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

```
R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp

R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443

R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq
22
```

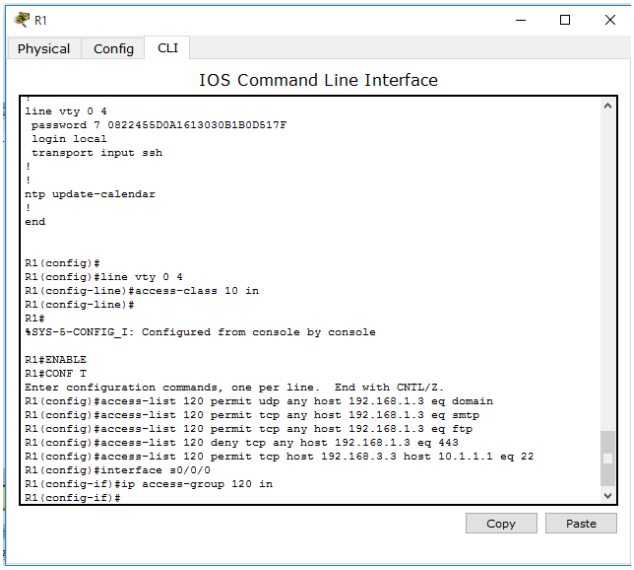


Step 3: Apply the ACL to interface S0/0/0.

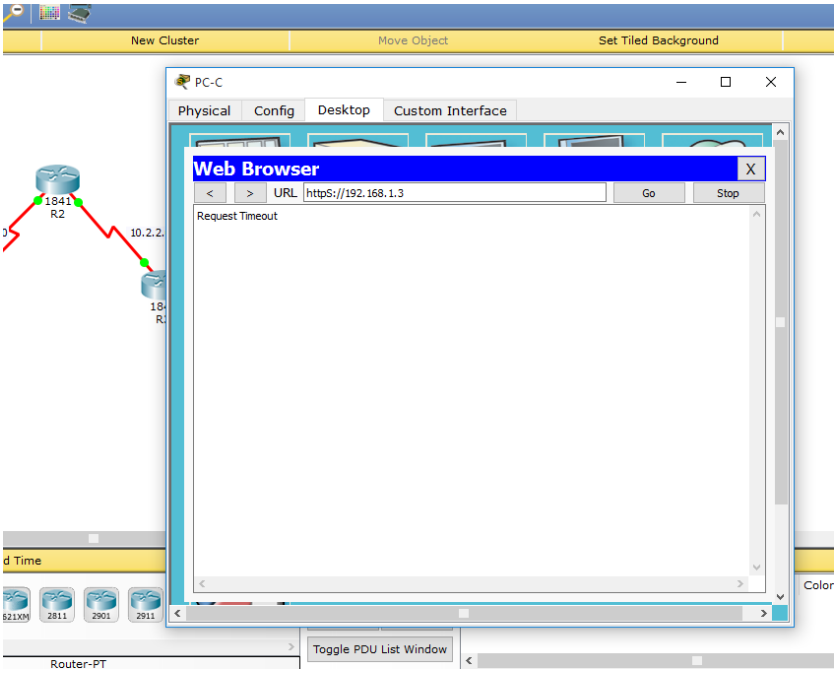
Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0.

```
R1(config)# interface s0/0/0
```

```
R1(config-if)# ip access-group 120 in
```



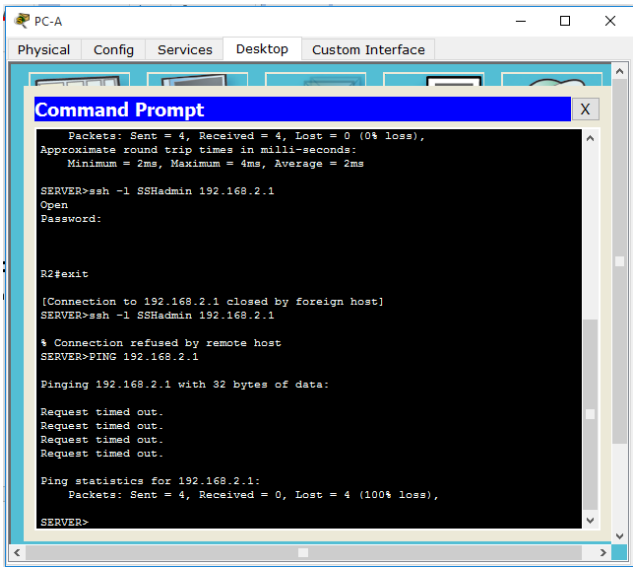
Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.



Part 4: Modify An Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to **R1**); deny all other incoming ICMP packets.

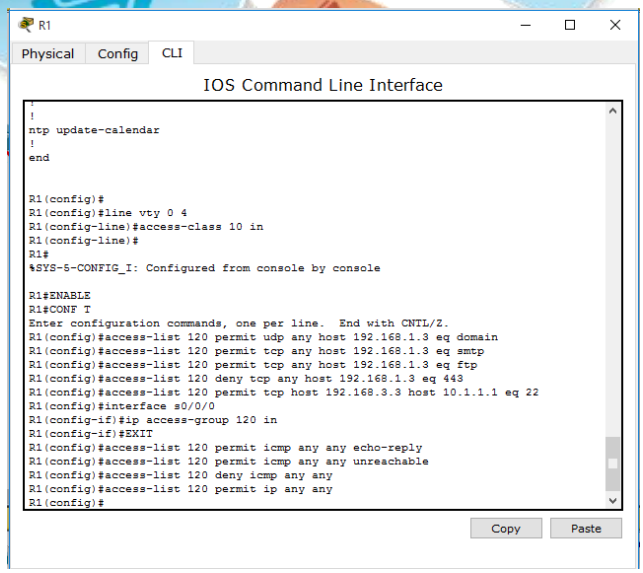
Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.



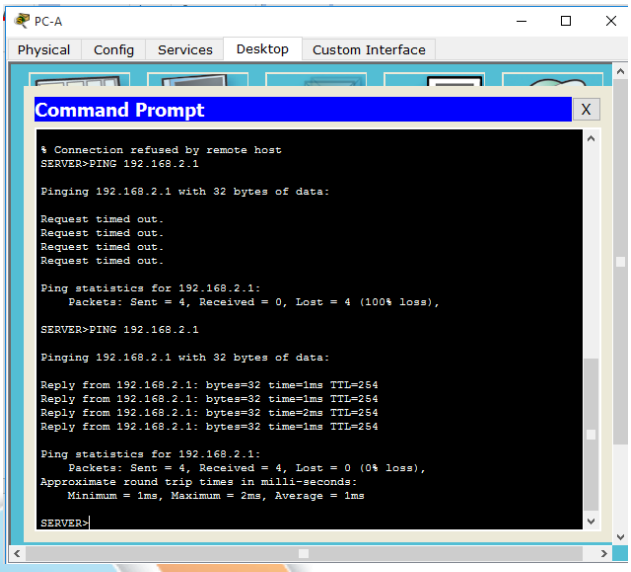
Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

```
R1(config)# access-list 120 permit icmp any any echo-reply

R1(config)# access-list 120 permit icmp any any unreachable

R1(config)# access-list 120 deny icmp any any

R1(config)# access-list 120 permit ip any any
```



Step 3: Verify that PC-A can successfully ping the loopback interface on R2.



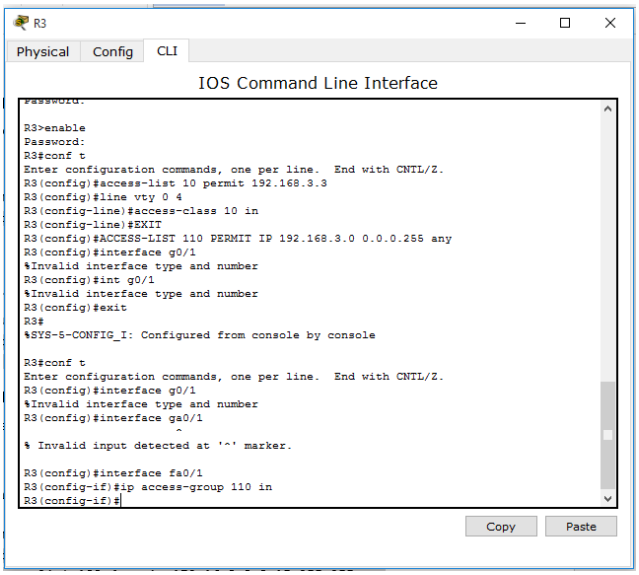
Part 5: Create a Numbered IP ACL 110 on R3

Deny all outbound packets with source address outside the range of internal IP addresses on **R3**.

Step 1: Configure ACL 110 to permit only traffic from the inside network.

Use the **access-list** command to create a numbered IP ACL.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any
```

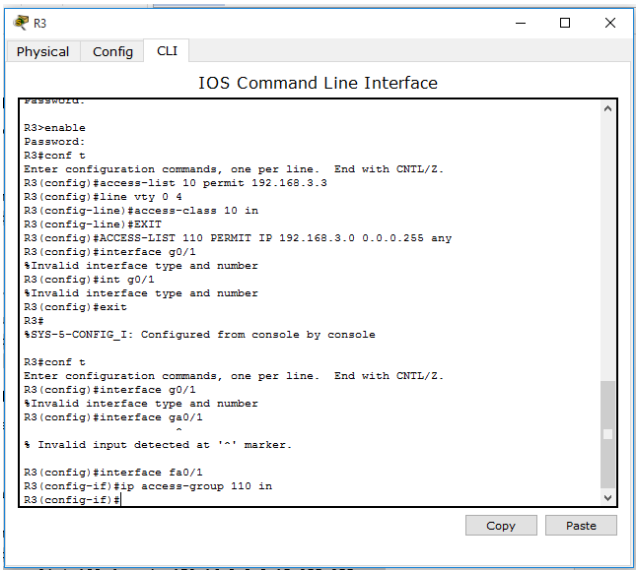


Step 2: Apply the ACL to interface F0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface F0/1.

```
R3(config)# interface fa0/1
```

```
R3(config-if)# ip access-group 110 in
```



Part 6: Create a Numbered IP ACL 100 on R3

On **R3**, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

Step 1: Configure ACL 100 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).

Use the **access-list** command to create a numbered IP ACL.

```
R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any
```

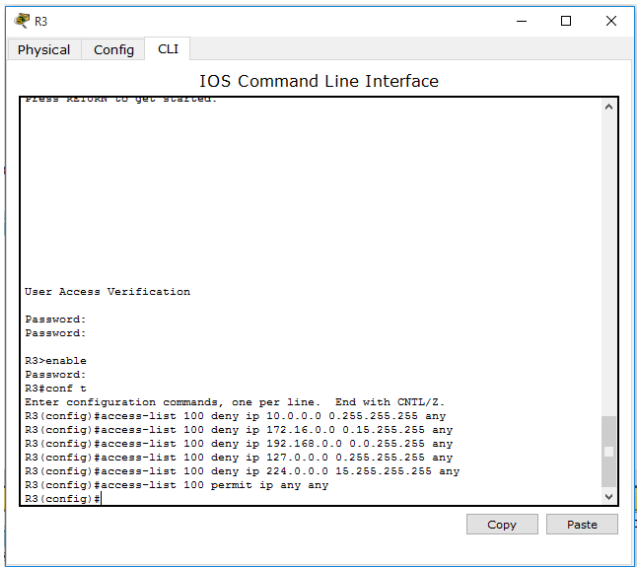
```
R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any
```

```
R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any
```

```
R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
```

```
R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
```

```
R3(config)# access-list 100 permit ip any any
```

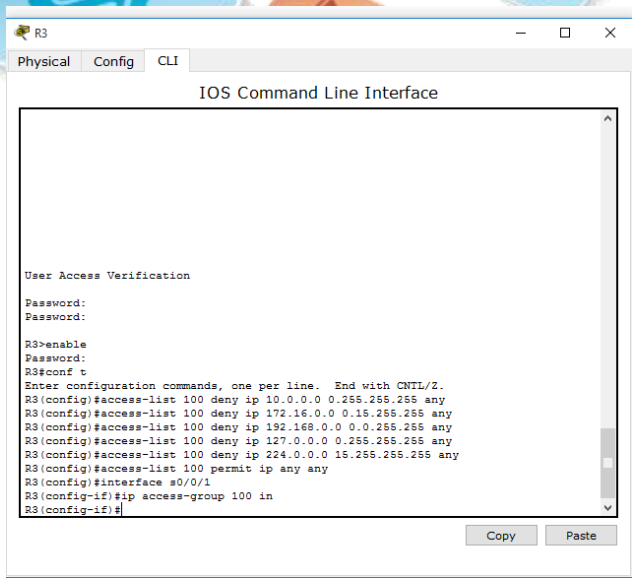


Step 2: Apply the ACL to interface Serial 0/0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.

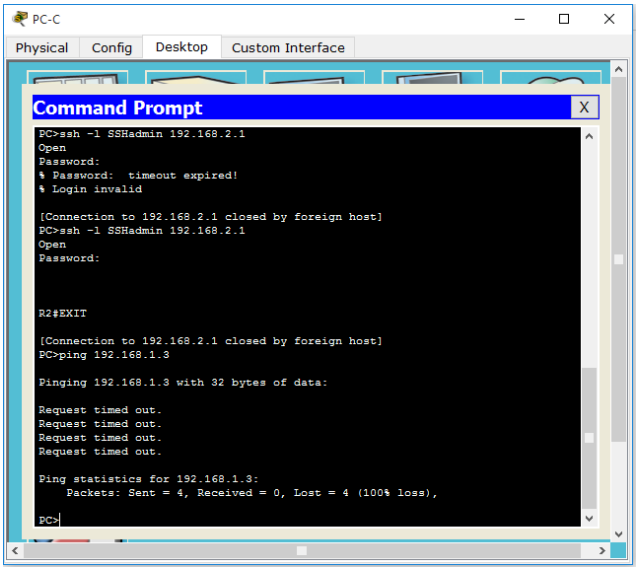
```
R3(config)# interface s0/0/1
```

```
R3(config-if)# ip access-group 100 in
```



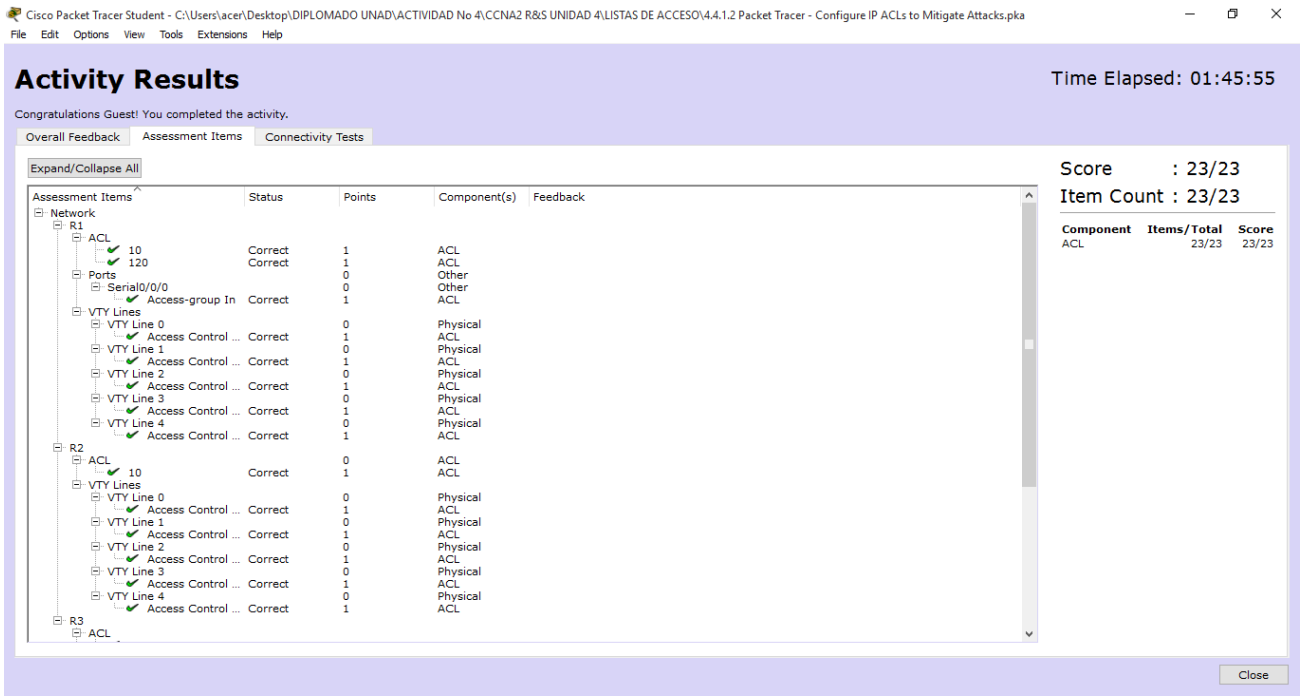
Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

From the **PC-C** command prompt, ping the **PC-A** server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.



Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed



!!!Script for R1

```
access-list 10 permit 192.168.3.3 0.0.0.0

line vty 0 4

 access-class 10 in

access-list 120 permit udp any host 192.168.1.3 eq domain

access-list 120 permit tcp any host 192.168.1.3 eq smtp

access-list 120 permit tcp any host 192.168.1.3 eq ftp

access-list 120 deny tcp any host 192.168.1.3 eq 443
```

```
access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1
eq 22 interface s0/0/0

 ip access-group 120 in

access-list 120 permit icmp any any echo-reply

access-list 120 permit icmp any any unreachable

access-list 120 deny icmp any any

access-list 120 permit ip any any
```

!!!Script for R2

```
access-list 10 permit 192.168.3.3 0.0.0.0

line vty 0 4

 access-class 10 in
```

!!!Script for R3

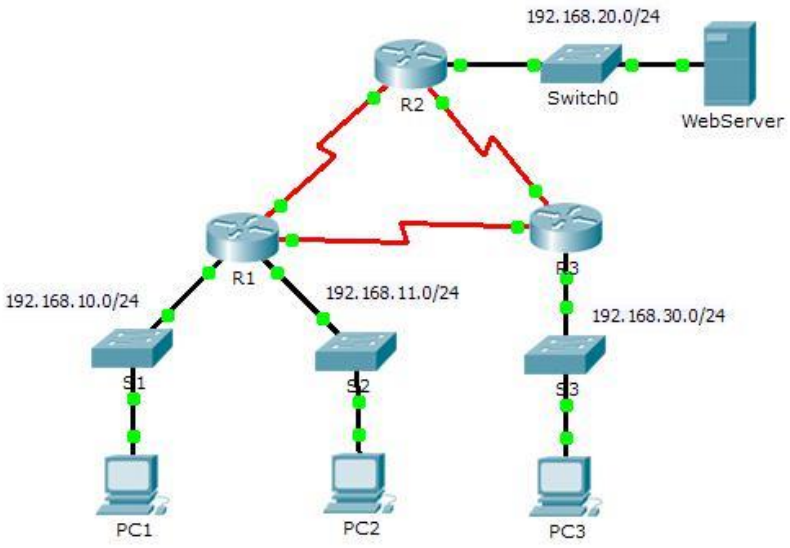
```
access-list 10 permit 192.168.3.3 0.0.0.0

line vty 0 4

 access-class 10 in


access-list 100 deny ip 10.0.0.0 0.255.255.255 any

access-list 100 deny ip 172.16.0.0 0.15.255.255 any

access-list 100 deny ip 192.168.0.0 0.0.255.255 any

access-list 100 deny ip 127.0.0.0 0.255.255.255 any
```

```
access-list 100 deny ip 224.0.0.0 15.255.255.255 any

access-list 100 permit ip any any

interface s0/0/1

 ip access-group 100 in

access-list 110 permit ip 192.168.3.0 0.0.0.255 any

interface fa0/1

 ip access-group 110 in
```

Packet Tracer - Configuring Standard ACLs (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objectives

Part 1: Plan an ACL Implementation

Background / Scenario

Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring

standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

Part 1:Plan an ACL Implementation

Step 1: Investigate the current network configuration.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.

Step 2: Evaluate two network policies and plan ACL implementations.

f. The following network policies are implemented on **R2**:

The 192.168.11.0/24 network is not allowed access to the **WebServer** on the 192.168.20.0/24 network.

All other access is permitted.

To restrict access from the 192.168.11.0/24 network to the **WebServer** at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

h. The following network policies are implemented on **R3**:

The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.

All other access is permitted.

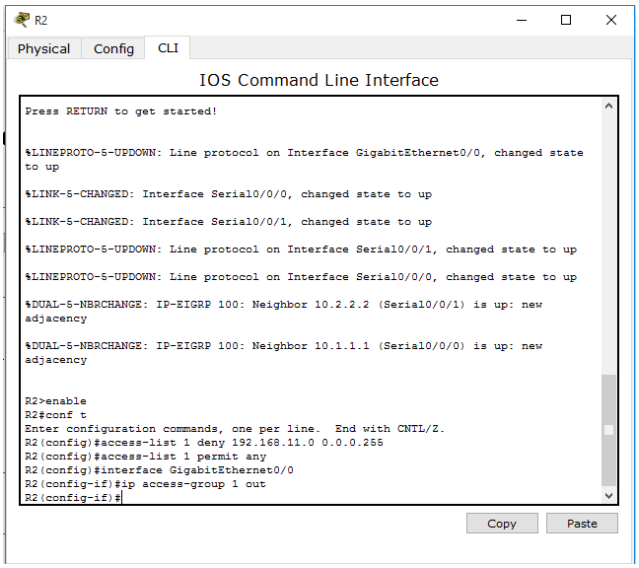
To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

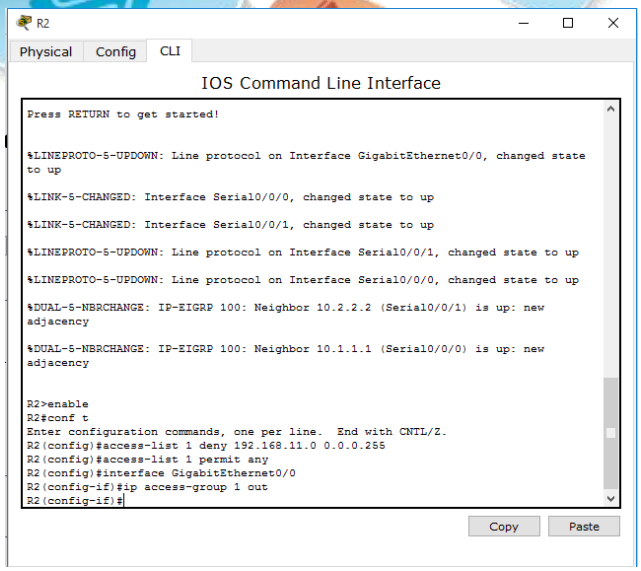
a. Create an ACL using the number 1 on **R2** with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```



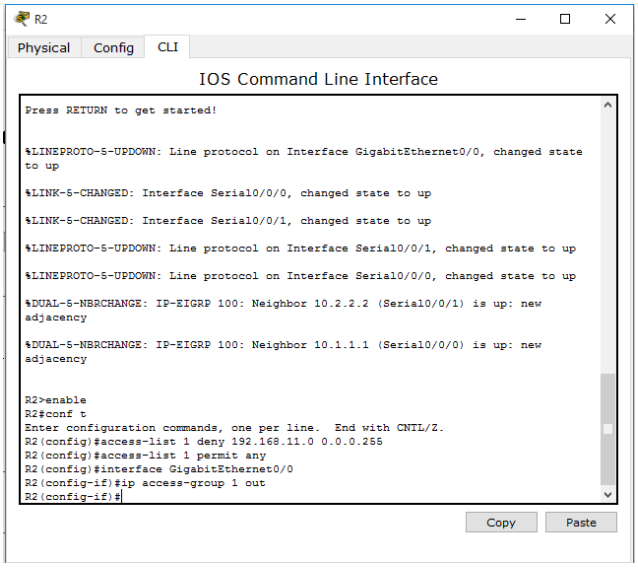
b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:

```
R2(config)# access-list 1 permit any
```



c. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

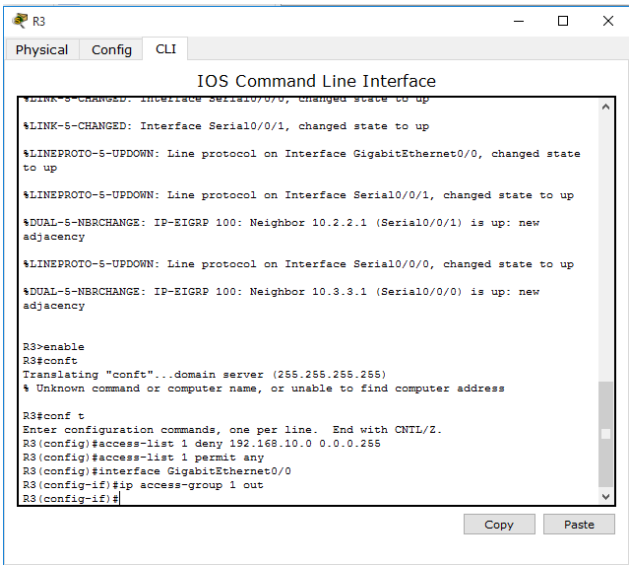
```
R2(config)# interface
GigabitEthernet0/0 R2(config-if)# ip
access-group 1 out
```



Step 2: Configure and apply a numbered standard ACL on R3.

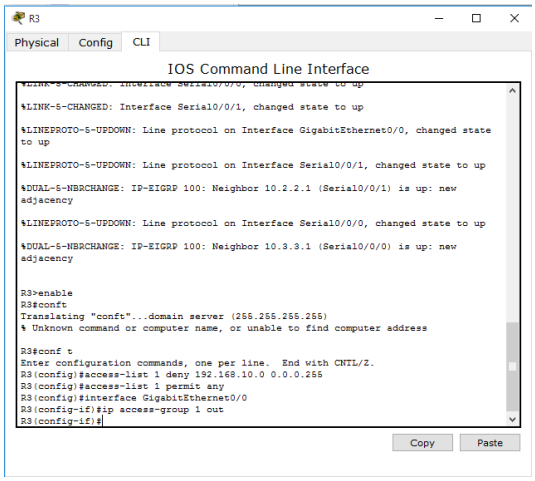
a. Create an ACL using the number 1 on **R3** with a statement that denies access to the 192.168.30.0/24 network from the **PC1** (192.168.10.0/24) network.

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```



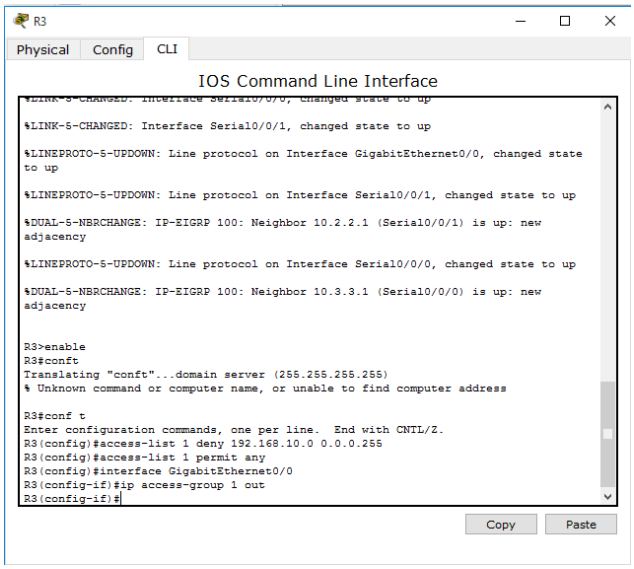
b. By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, create a second rule for ACL 1.

```
R3(config)# access-list 1 permit any
```



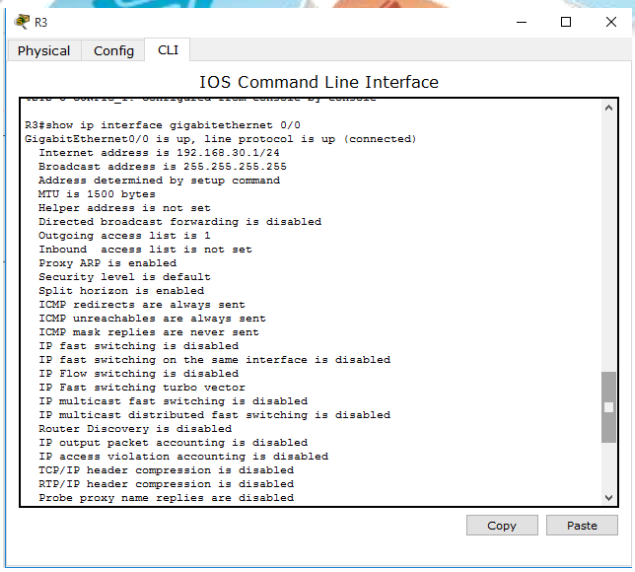
c. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

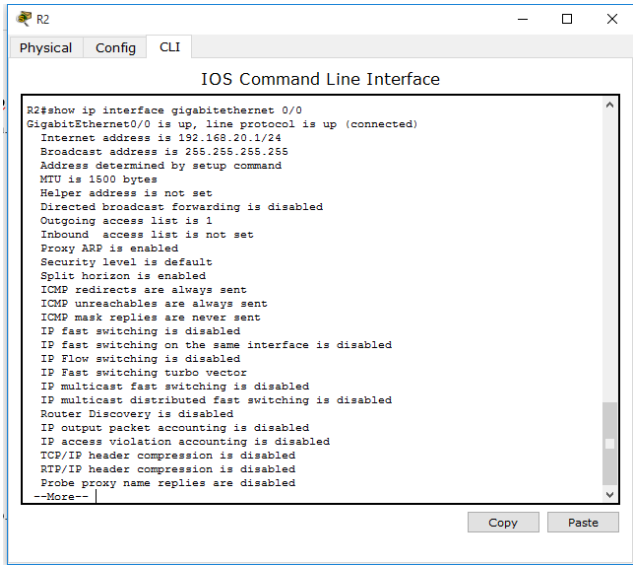
```
R3(config)# interface
GigabitEthernet0/0 R3(config-if)# ip
access-group 1 out
```



Step 3: Verify ACL configuration and functionality.

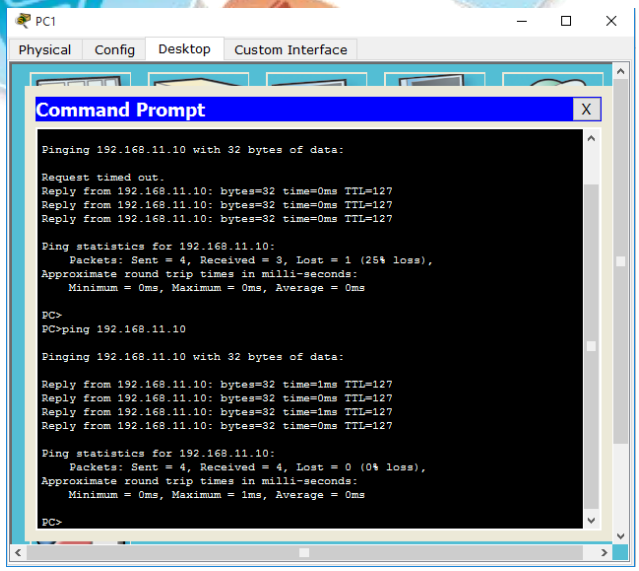
a. On **R2** and **R3**, enter the **show access-list** command to verify the ACL configurations. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.



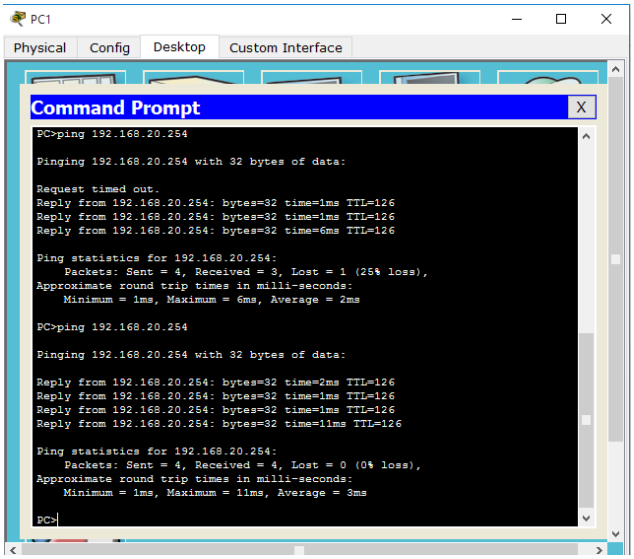


a. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:

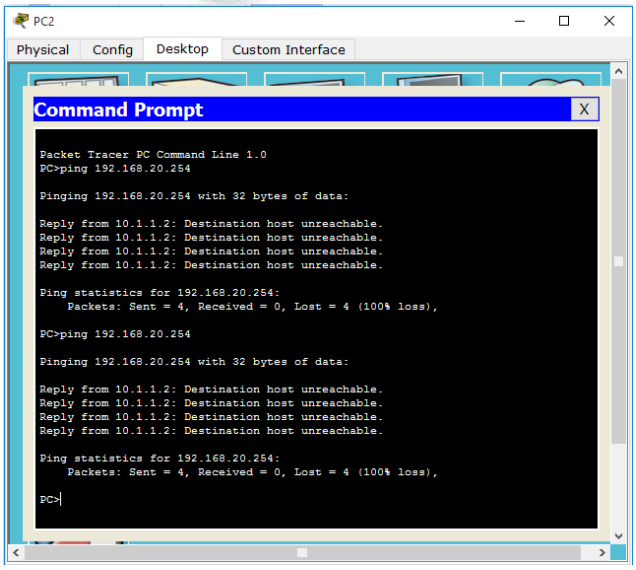
A ping from 192.168.10.10 to 192.168.11.10 succeeds.



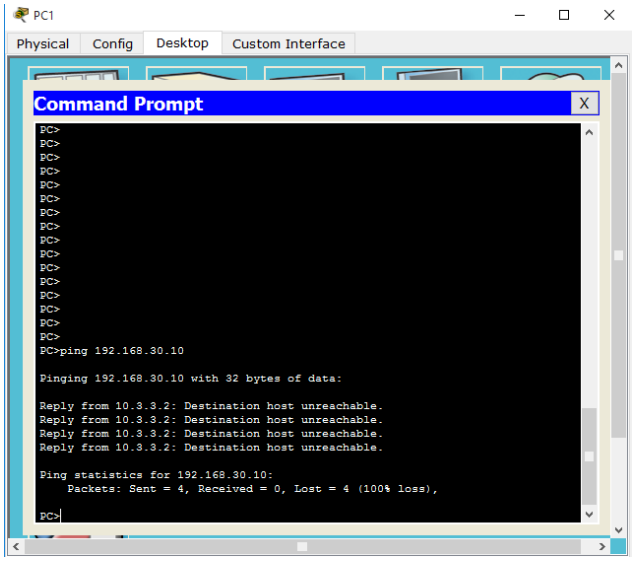
A ping from 192.168.10.10 to 192.168.20.254 succeeds.



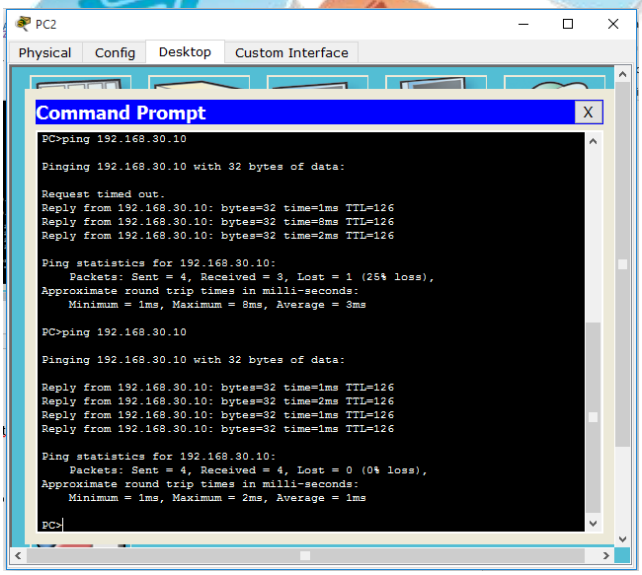
A ping from 192.168.11.10 to 192.168.20.254 fails.



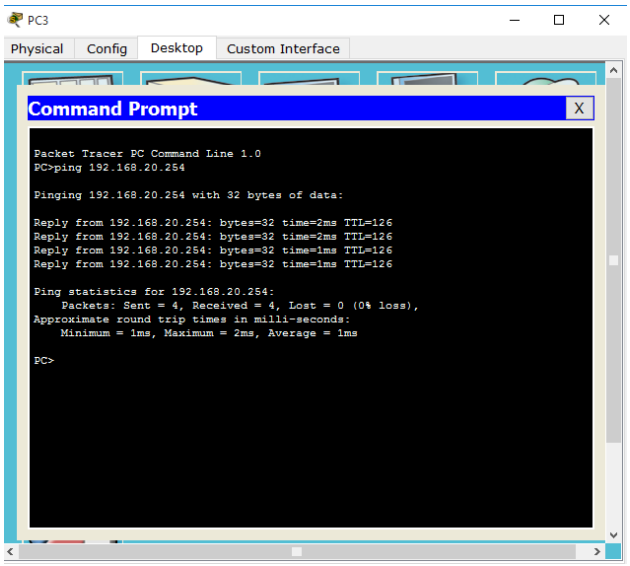
α. A ping from 192.168.10.10 to 192.168.30.10 fails.



α. A ping from 192.168.11.10 to 192.168.30.10 succeeds.



α. A ping from 192.168.30.10 to 192.168.20.254 succeeds.

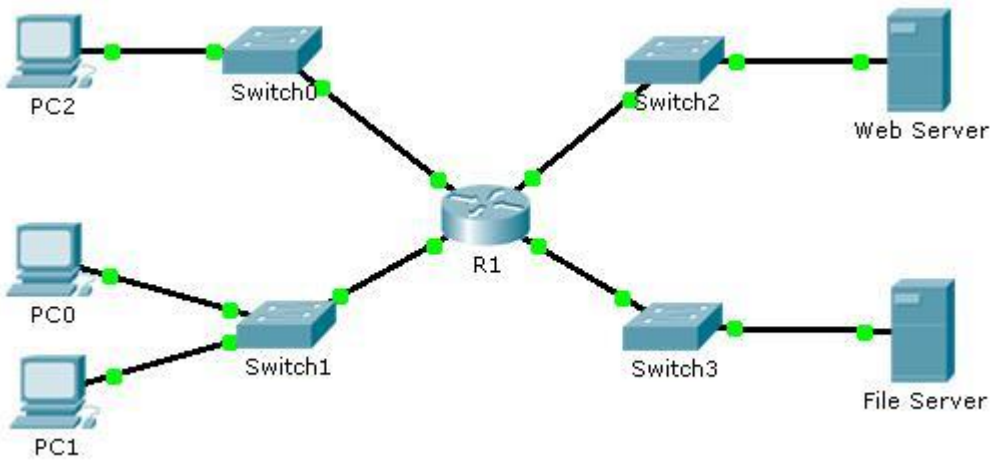


Ejercicio No 12 - 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs Instructions IG

Packet Tracer - Configuring Named Standard ACLs (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objectives

Part 1: Configure and Apply a Named Standard ACL

Part 2: Verify the ACL Implementation

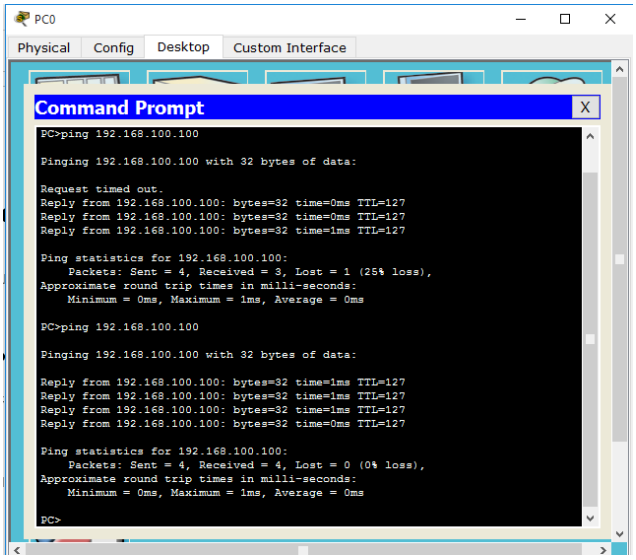
Background / Scenario

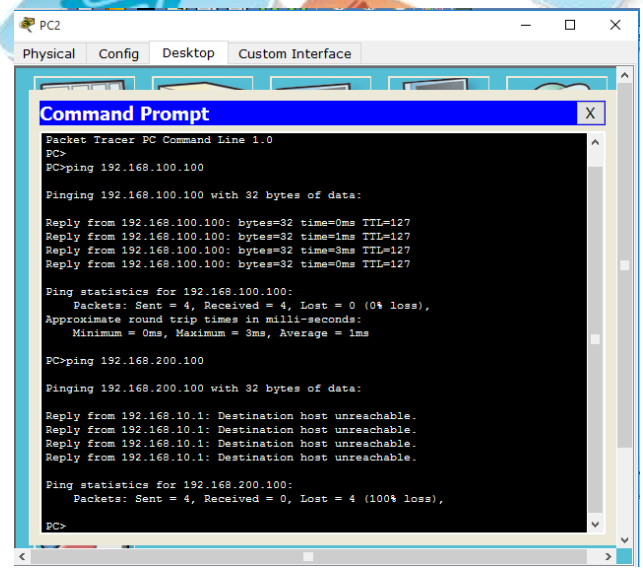
The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied access.

Part 1: Configure and Apply a Named Standard ACL

Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the **Web Server** and **File Server**.

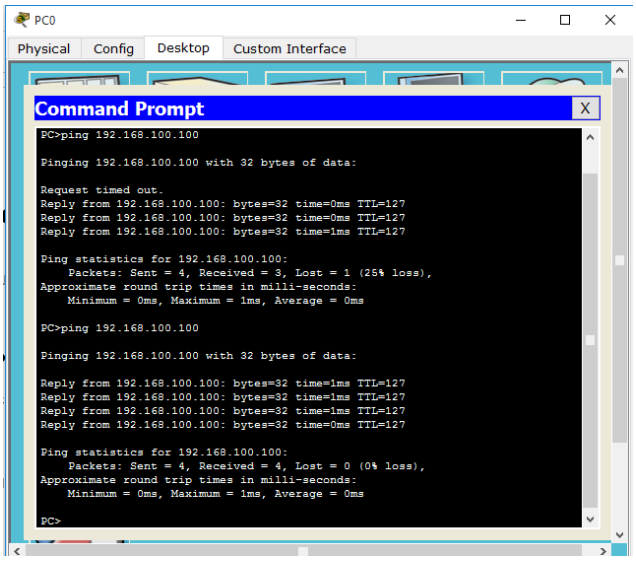


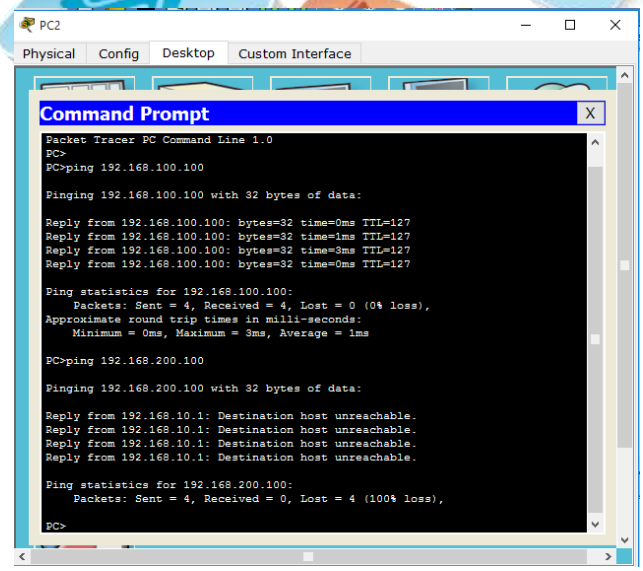


Part 1: Configure and Apply a Named Standard ACL

Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the **Web Server** and **File Server**.



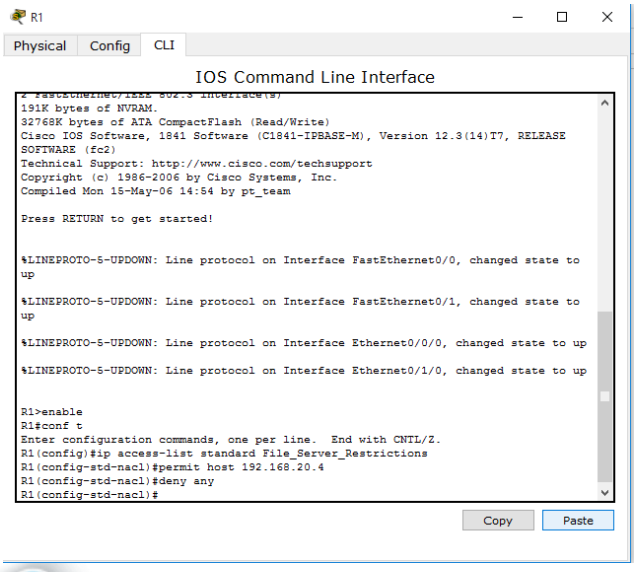


Step 2: Configure a named standard ACL.

Configure the following named ACL on **R1**.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# deny any
```

Note: For scoring purposes, the ACL name is case-sensitive.

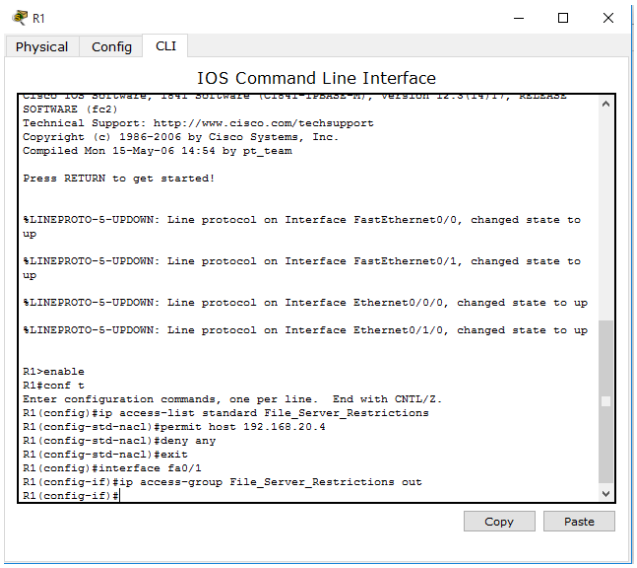


Step 3: Apply the named ACL.

a. Apply the ACL outbound on the interface Fast Ethernet 0/1.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

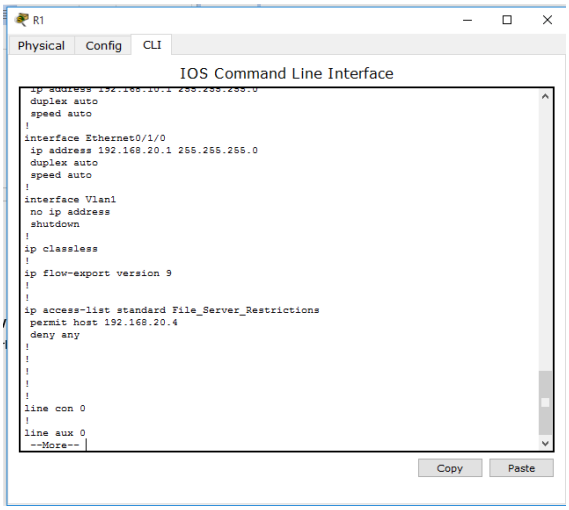
b. Save the configuration.



Part 2: Verify the ACL Implementation

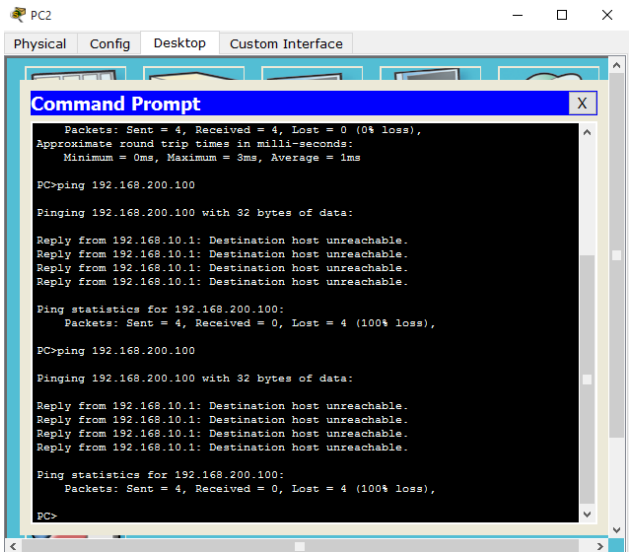
Step 1: Verify the ACL configuration and application to the interface.

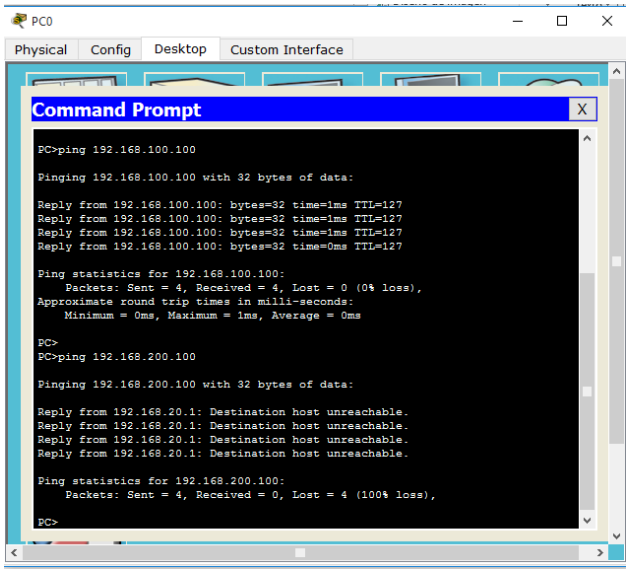
Use the **show access-lists** command to verify the ACL configuration. Use the Use the **interface fastethernet 0/1** command to verify that the ACL is applied correctly **show run** or **show ip** to the interface.

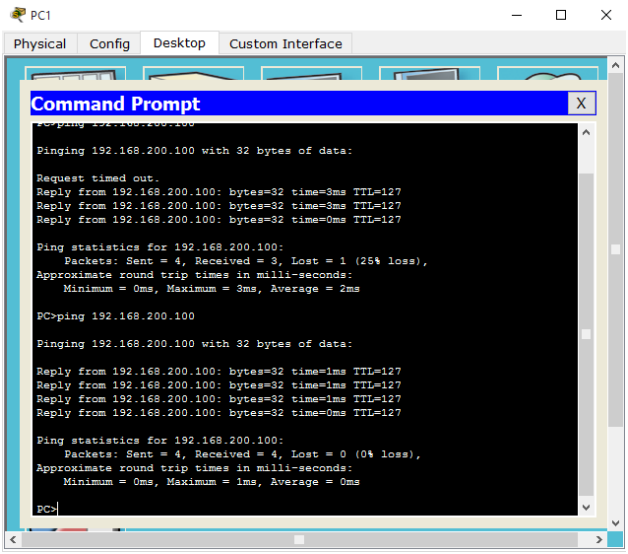


Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the **Web Server**, but only **PC1** should be able to ping the **File Server**

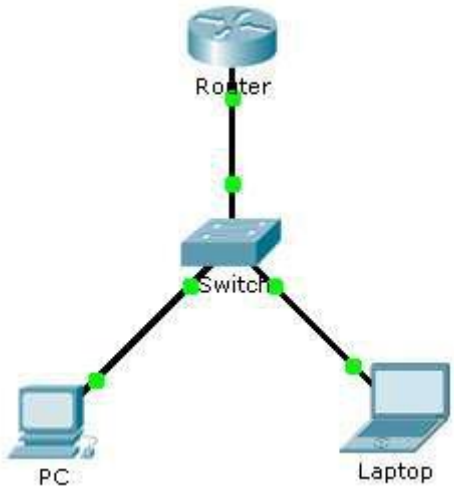



PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>


PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Pinging 192.168.200.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.200.100: bytes=32 time=3ms TTL=127
Reply from 192.168.200.100: bytes=32 time=3ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 2ms
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>

Ejercicio No 13 - 9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines Instructions IG

Packet Tracer - Configuring an ACL on VTY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	F0/0	10.0.0.254	255.0.0.0	N/A

PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Laptop	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Objectives

Part 1: Configure and Apply an ACL to VTY Lines

Part 2: Verify the ACL Implementation

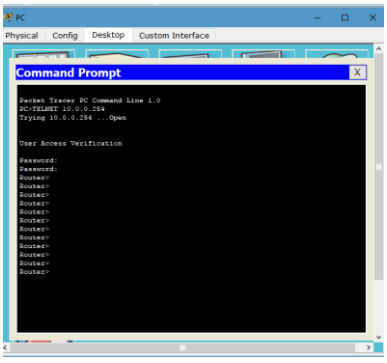
Background

As network administrator, you must have remote access to your router. This access should not be available to other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows **PC** access to the Telnet lines, but denies all other source IP addresses.

Part 1: Configure and Apply an ACL to VTY Lines

Step 1: Verify Telnet access before the ACL is configured.

Both computers should be able to Telnet to the **Router**. The password is **cisco**.

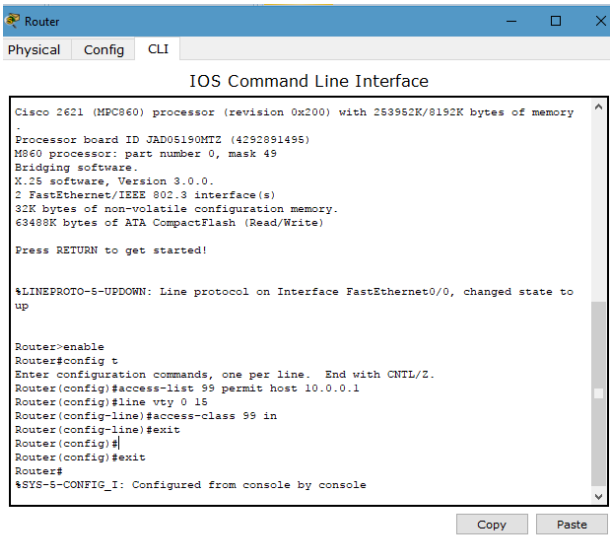


Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on **Router**.

```
Router(config)# access-list 99 permit host 10.0.0.1
```

Because we do not want to permit access from any other computers, the implicit deny property of the access list satisfies our requirements.

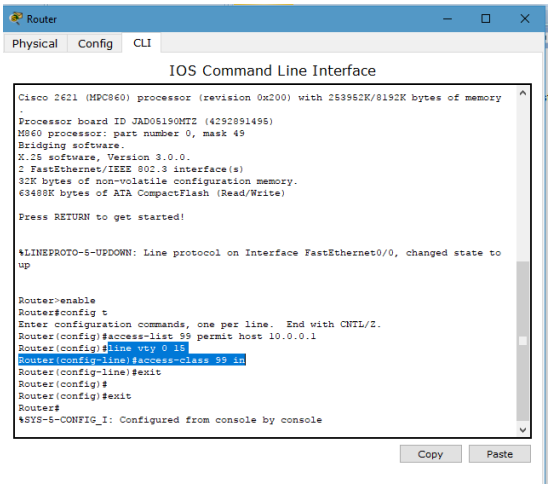


Step 3: Place a named standard ACL on the router.

Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration mode for lines 0 – 4 and use the **access-class** command to apply the ACL to all the VTY lines:

```
Router(config)# line vty 0 15
```

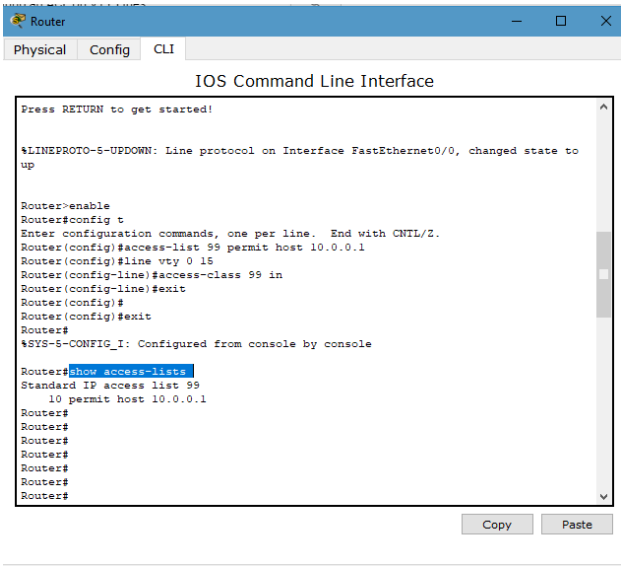
```
Router(config-line)# access-class 99 in
```



Part 2: Verify the ACL Implementation

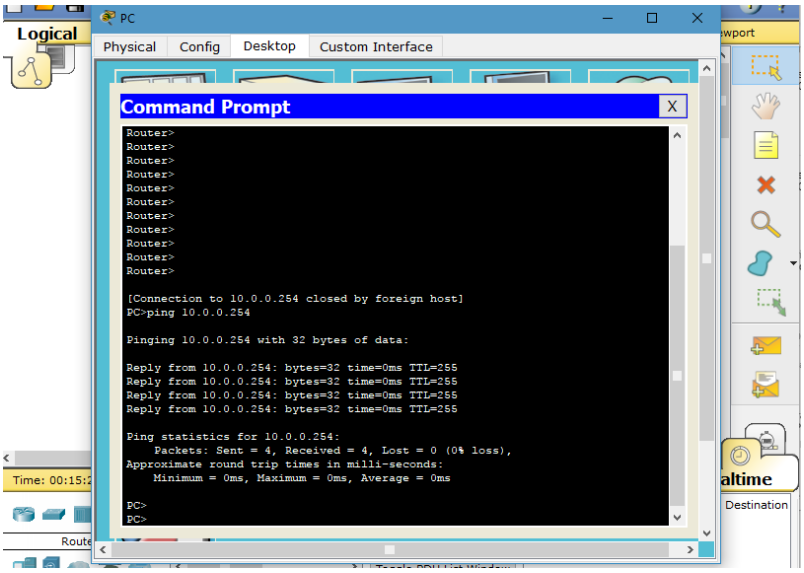
Step 1: Verify the ACL configuration and application to the VTY lines.

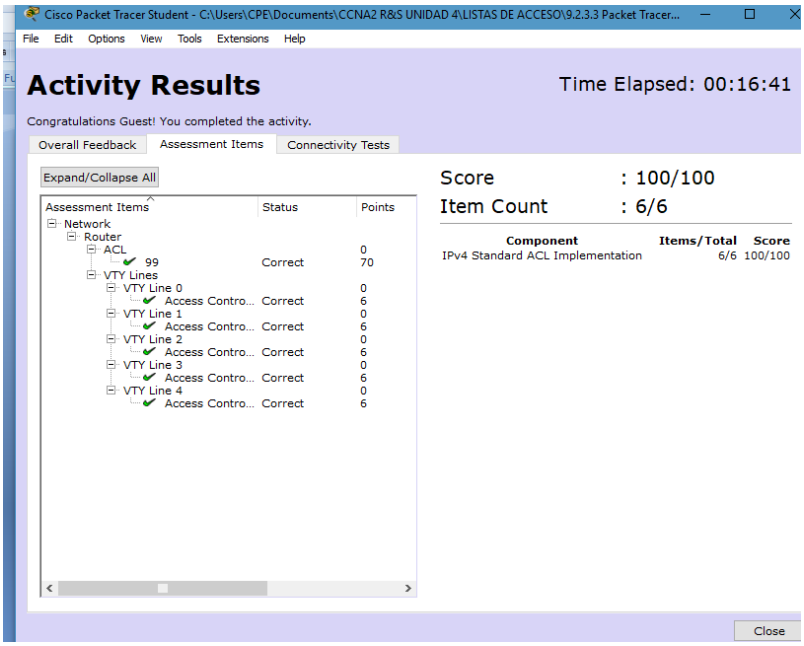
Use the **show access-lists** to verify the ACL configuration. Use the **show run** command to verify the ACL is applied to the VTY lines.



Step 2: Verify that the ACL is working properly.

Both computers should be able to ping the **Router**, but only **PC** should be able to Telnet to it

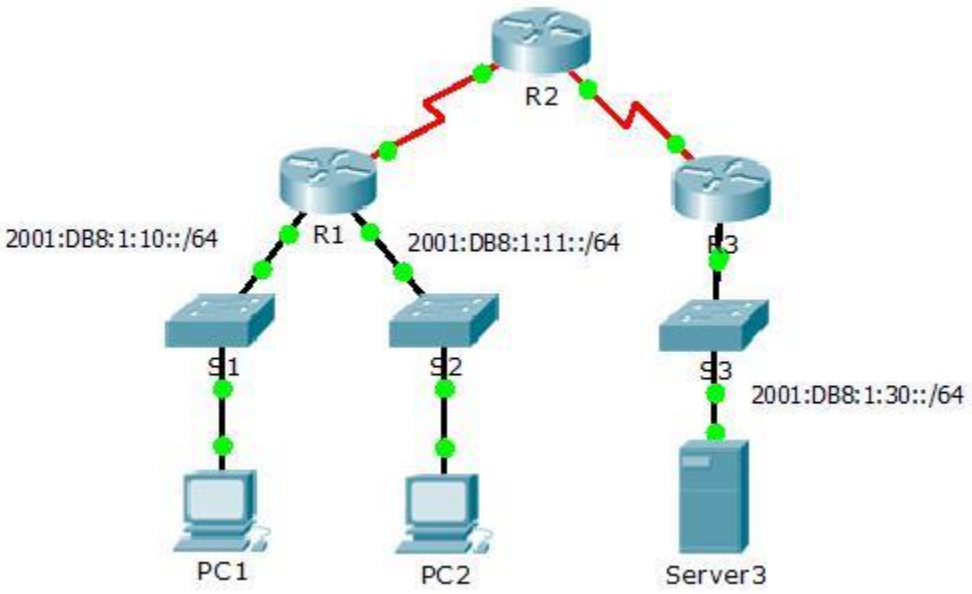




Ejercicio No 14 - 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs Instructions IG

Packet Tracer - Configuring IPv6 ACLs

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectives

Part 1: Configure, Apply, and Verify an IPv6 ACL

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Part 1: Configure, Apply, and Verify an IPv6 ACL

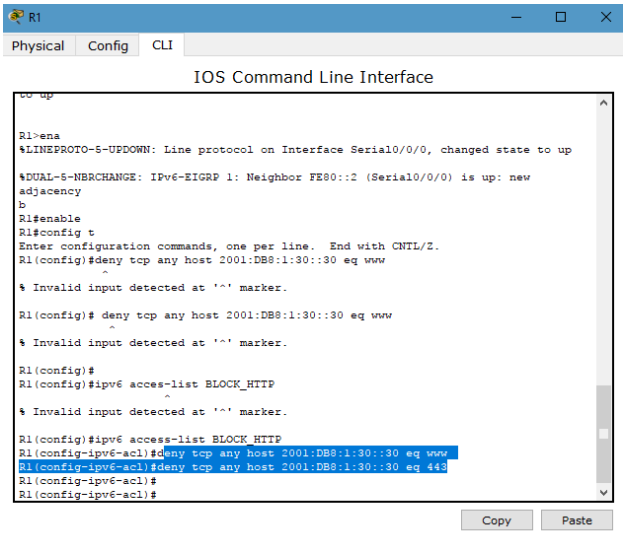
Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

Step 1: Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named **BLOCK_HTTP** on **R1** with the following statements.

a. Block HTTP and HTTPS traffic from reaching **Server3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```



a. Allow all other IPv6 traffic to pass.

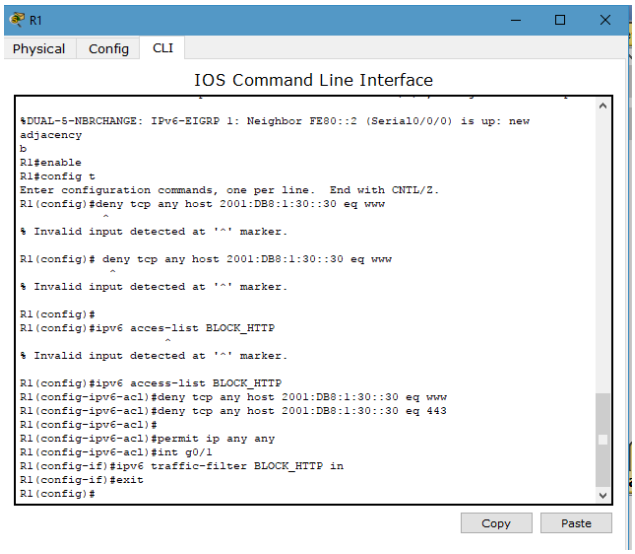
```
R1(config)# permit ipv6 any any
```

Step 2: Apply the ACL to the correct interface.

Apply the ACL on the interface closest the source of the traffic to be blocked.

```
R1(config)# interface GigabitEthernet0/1
```

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```



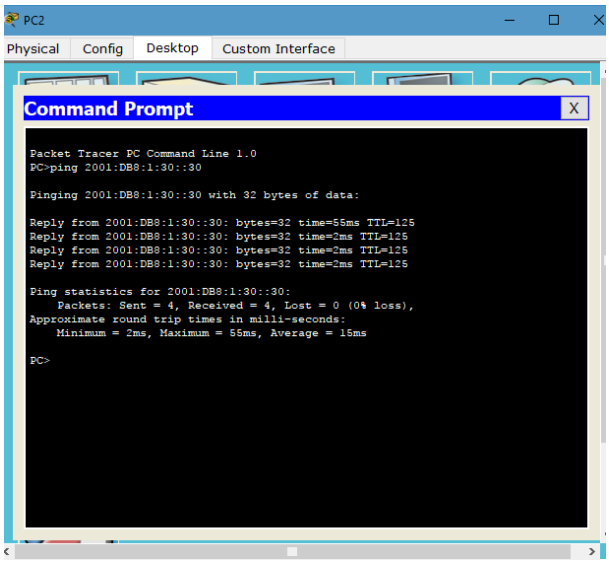
Step 3: Verify the ACL implementation.

Verify the ACL is operating as intended by conducting the following tests:

α. Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.

β. Open the **web browser** of **PC2** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked

Ping from **PC2** to 2001:DB8:1:30::30. The ping should be successful



Part 2: Configure, Apply, and Verify a Second IPv6 ACL

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

Step 1: Create an access list to block ICMP.

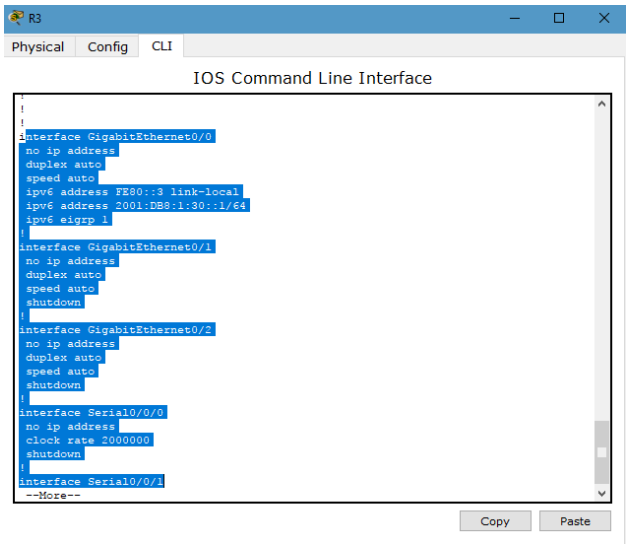
Configure an ACL named **BLOCK_ICMP** on **R3** with the following statements:

j. Block all ICMP traffic from any hosts to any destination.

```
R3(config)# deny icmp any any
```

k. Allow all other IPv6 traffic to pass.

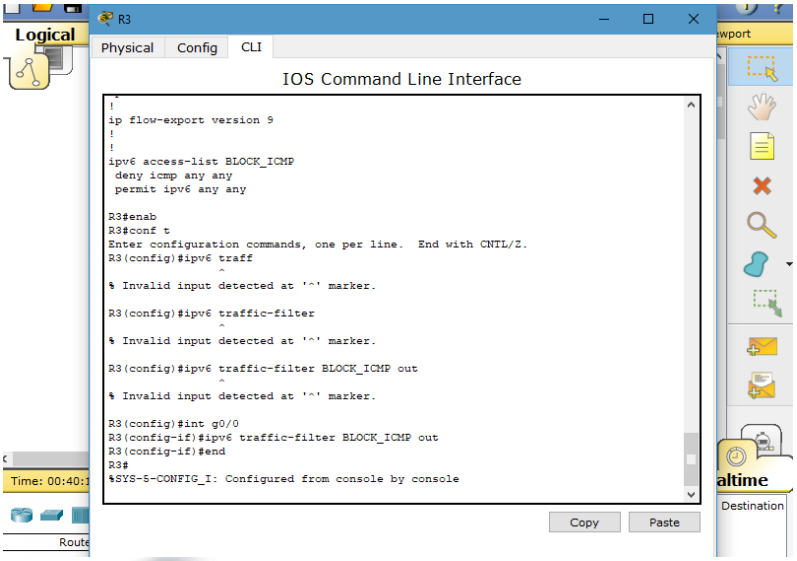
```
R3(config)# permit ipv6 any any
```



Step 2: Apply the ACL to the correct interface.

In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked regardless of its source or changes that occur to the network topology, apply the ACL closest to the destination.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ipv6 traffic-filter BLOCK_ICMP
out
```

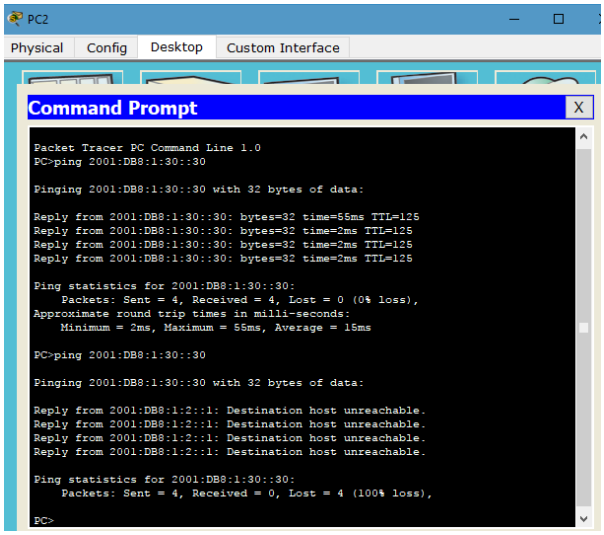


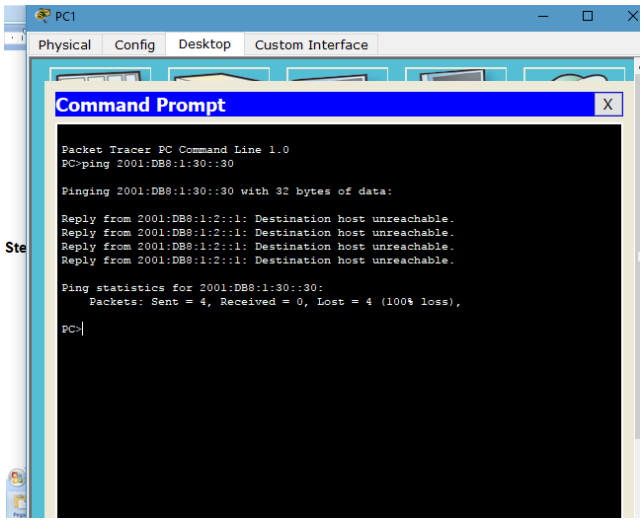
Step 3: Verify that the proper access list functions.

g. Ping from **PC2** to 2001:DB8:1:30::30. The ping should fail.

h. Ping from **PC1** to 2001:DB8:1:30::30. The ping should fail.

Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should display





Conclusión

La presente actividad nos permitió comprender, entender y analizar los entorno de aprendizaje del Diplomado de Profundización CISCO cuyo fin es de fortalecer y desarrollar competencias en el área del saber específico orientadas al uso de protocolos de enrutamiento avanzado, y de igual forma esta actividad es de tipo colaborativo donde el aprendizaje está basado en tareas orientadas a la Introducción a Enrutamiento Dinámico, OSPF de una sola área, Listas de control de acceso, DHCP, Traducción de direcciones IP para IPv4 y el uso de recursos y herramientas en función de los protocolos y servicios., de este modo la persona que profundiza en este tema podrá tener un amplio conocimiento donde serán valiosos en el desarrollo de su vida personal y profesional

Referencias bibliográficas

Temática: Enrutamiento Dinámico
CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

Temática: OSPF de una sola área
CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

Temática: Listas de control de acceso
CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

Temática: DHCP
CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Temática: Traducción de direcciones IP para IPv4
CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

OVA Unidad 4 - Video - Principios de Enrutamiento

Este Objeto Virtual de Aprendizaje, titulado Video - Principios de Enrutamiento, tiene como objetivo, orientar al estudiante sobre la configuración básica de Switches y Routers.

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de:

https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm