

DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACION DE
SOLUCIONESINTEGRADAS (LAN/WAN)

PARTICIPANTES

KIARA TAYSE ESCOBAR OLMEDO

TUTOR

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONALABIERTA Y A DISTANCIA
FACULTAD BASICA DE INGENIERIA Y TECNOLOGIA
INGENIERIA DE SISTEMAS

AÑO 2017

INTRODUCCION

Cuando hablamos de compartir información y de realizar la comunicación entre distintos sistemas tecnológicos, el enrutamiento dinámico es uno de los primeros conceptos que nos vienen a la cabeza. Bajo este proceso una serie de máquinas que se encuentren dentro de una misma red tendrán capacidad para llevar a cabo una comunicación entre ellas de forma permanente. Su comunicación se ocupará de que las tablas de enrutamiento estén siempre en una actualización adecuada, se controlará el estado vinculado a los enlaces y además se podrán comprobar cuáles son las rutas más convenientes en base al estado del análisis de la red. Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

Las redes de datos que usamos en nuestras vidas cotidianas para aprender, jugar y trabajar varían desde pequeñas redes locales hasta grandes internetworks globales. En su casa, posiblemente tenga un router y dos o más computadoras. En el trabajo, su organización probablemente tenga varios routers y switches que atienden a las necesidades de comunicación de datos de cientos o hasta miles de PC.

Los protocolos de enrutamiento dinámico generalmente se usan en redes de mayor tamaño para facilitar la sobrecarga administrativa y operativa que implica el uso de rutas estáticas únicamente. Normalmente, una red usa una combinación de un protocolo de enrutamiento dinámico y rutas estáticas. En la mayoría de las redes, se usa un único protocolo de enrutamiento dinámico; sin embargo, hay casos en que las distintas partes de la red pueden usar diferentes protocolos de enrutamiento.

Un profesional de redes debe estar capacitado para tomar decisiones fundadas respecto de cuándo usar un protocolo de enrutamiento dinámico y qué protocolo de enrutamiento es la mejor opción para un entorno en particular.

OBJETIVOS

- ... Identificar y solucionar problemas propios de enrutamiento mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces
- ... Describir la función de los protocolos de enrutamiento dinámico y ubicar estos protocolos en el contexto del diseño de redes actual.
- ... Identificar los distintos elementos de la tabla de enrutamiento.
- ... Describir cómo los protocolos de enrutamiento usan las métricas e identificar los tipos de métricas que usan los protocolos de enrutamiento dinámico.

DESARROLLO DE LAS TAREAS PROPUESTAS

Práctica de laboratorio 7.3.2.4: configuración básica de RIPv2 y RIPvng-

Topología

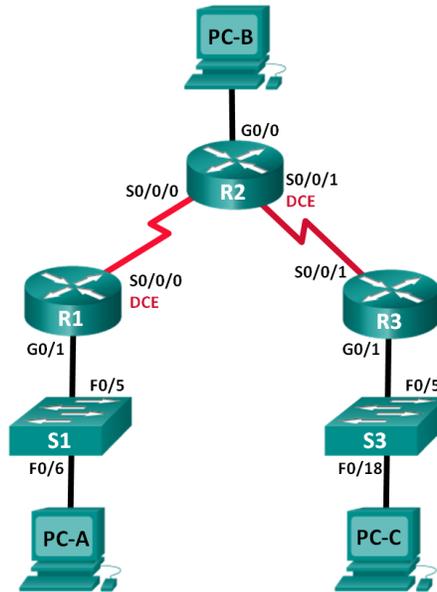


Tabla de direccionamiento

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.

Información básica/situación

RIP versión 2 (RIPv2) se utiliza para enrutar direcciones IPv4 en redes pequeñas. RIPv2 es un protocolo de routing vector distancia sin clase, según la definición de RFC 1723. Debido a que RIPv2 es un protocolo de routing sin clase, las máscaras de subred se incluyen en las actualizaciones de routing. De manera predeterminada, RIPv2 resume automáticamente las redes en los límites de redes principales. Cuando se deshabilita la sumarización automática, RIPv2 ya no resume las redes a su dirección con clase en routers fronterizos.

RIP de última generación (RIPng) es un protocolo de routing vector distancia para enrutar direcciones IPv6, según la definición de RFC 2080. RIPng se basa en RIPv2 y tiene la misma distancia administrativa y limitación de 15 saltos.

En esta práctica de laboratorio, configurará la topología de la red con routing RIPv2, deshabilitará la sumarización automática, propagará una ruta predeterminada y usará comandos de CLI para ver y verificar la información de routing RIP. Luego, configurará la topología de la red con direcciones IPv6, configurará RIPng, propagará una ruta predeterminada y usará comandos de CLI para ver y verificar la información de routing RIPng.

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

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

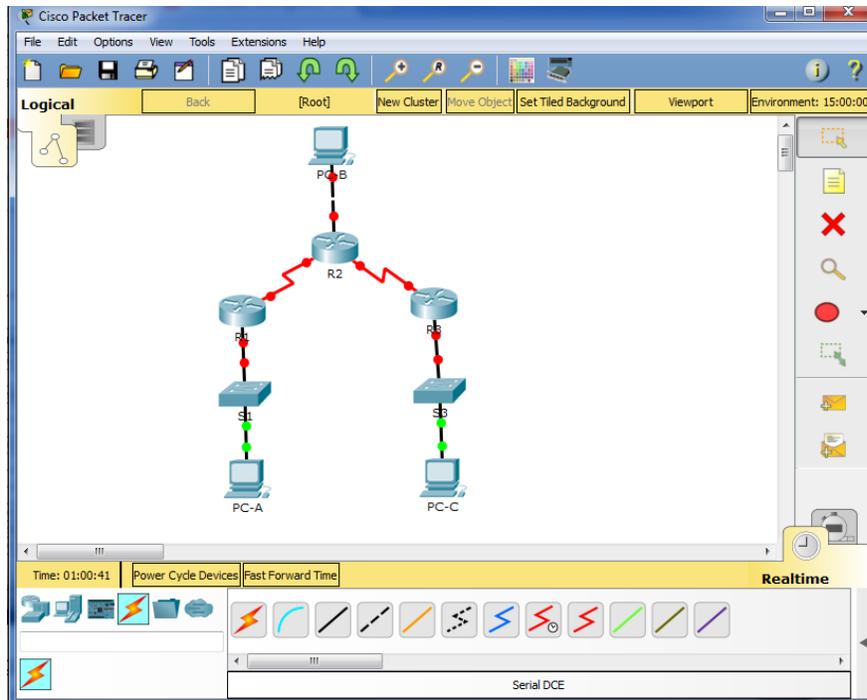
Recursos necesarios

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

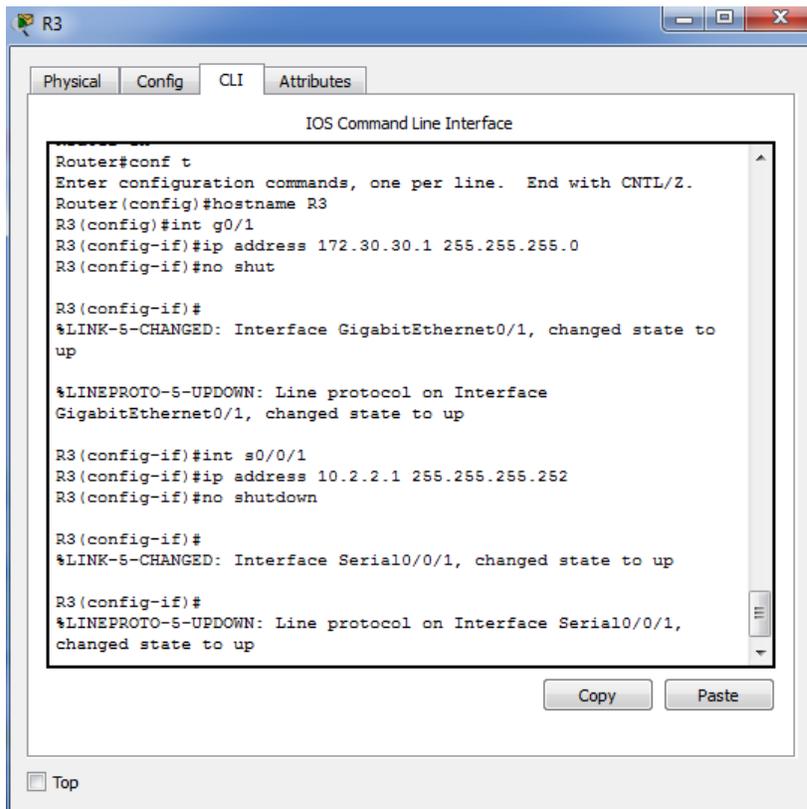
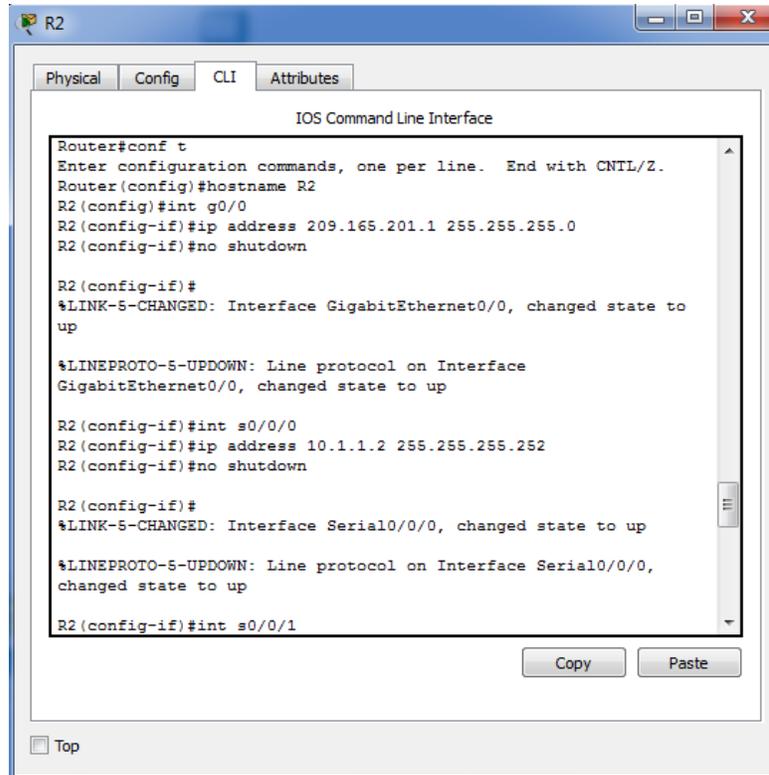
```
R1
Physical Config CLI Attributes
IOS Command Line Interface
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#no shutdown

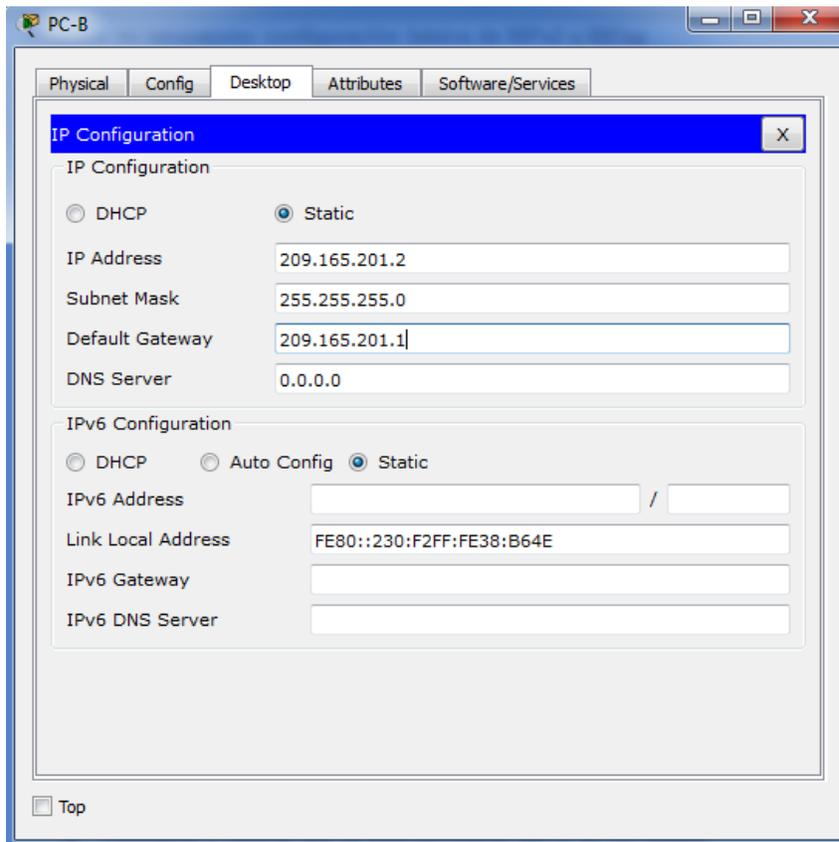
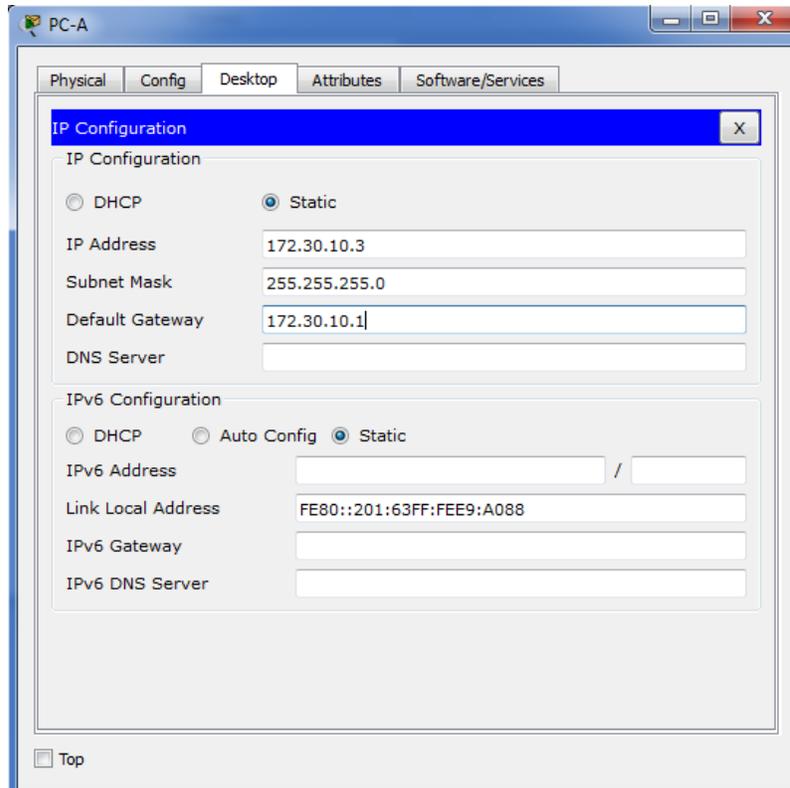
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

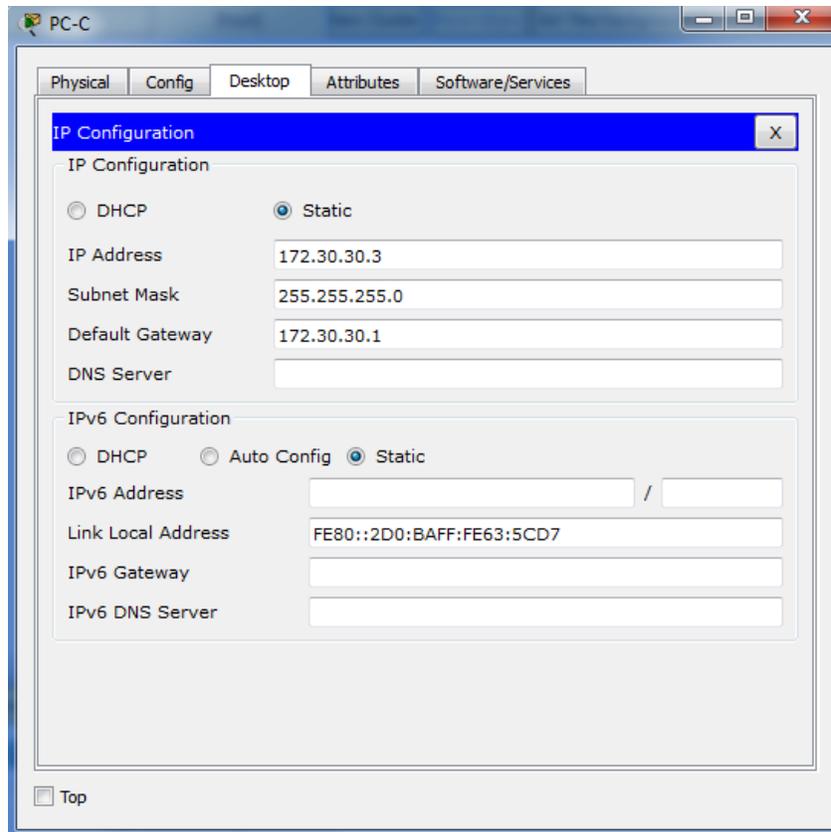
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R1(config-if)#int s0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Copy Paste
Top
```







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

- Desactive la búsqueda del DNS.
- Configure los nombres de los dispositivos como se muestra en la topología.
- Configure la encriptación de contraseñas.
- Asigne **class** como la contraseña del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- Configure **logging synchronous** para la línea de consola.
- Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- Configure una descripción para cada interfaz con una dirección IP.
- Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.
- Copie la configuración en ejecución en la configuración de inicio.

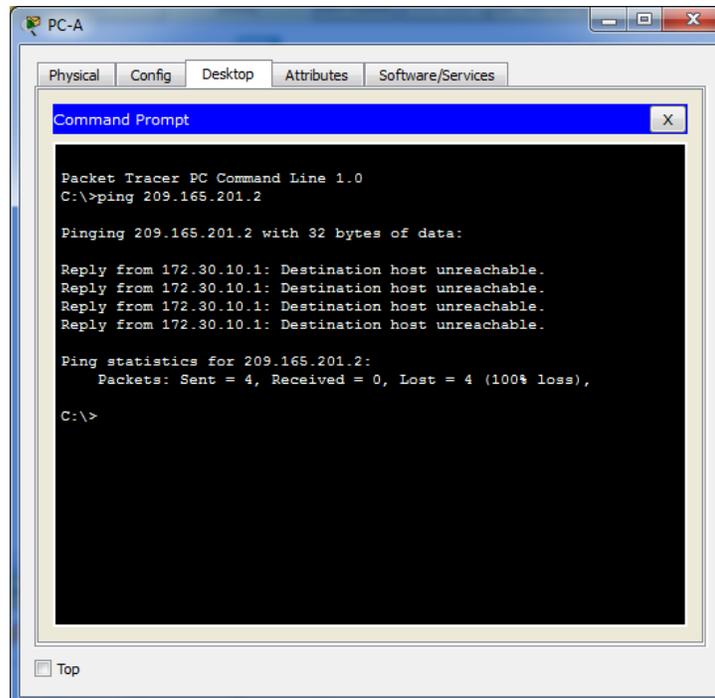
Paso 4. configurar los equipos host.

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

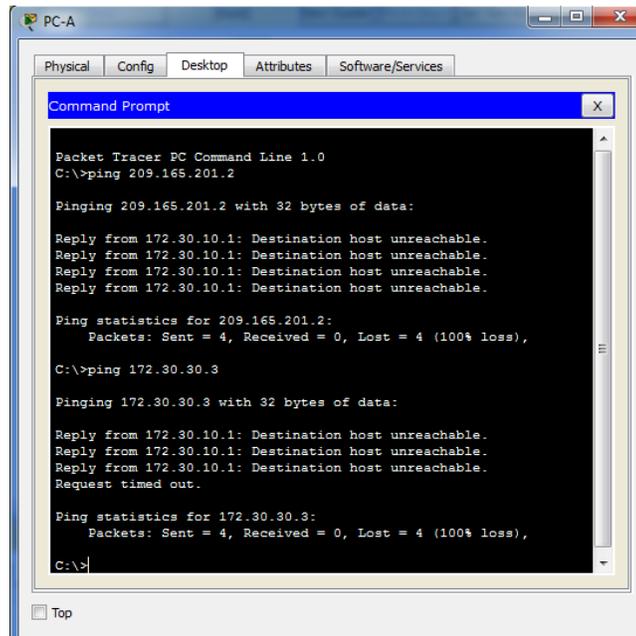
Paso 5. Probar la conectividad.

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

- **Ping entre PC-A y PCB, no puede hacerse**



- Ping entre PC-A y PC-C, no puede hacerse



- Ping entre PC-C y PC-A y PC-B

```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Request timed out.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

- Ping entre PC-B y PC-A y PC-C

```
PC-B
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 209.165.201.1: Destination host unreachable.
Reply from 209.165.201.1: Destination host unreachable.
Request timed out.
Reply from 209.165.201.1: Destination host unreachable.

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 209.165.201.1: Destination host unreachable.

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

- a. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.
 - Ping de PC-A a router 1

```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Request timed out.

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.30.10.1
Pinging 172.30.10.1 with 32 bytes of data:
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

- Ping de PC-B a router 2

```
PC-B
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 209.165.201.1: Destination host unreachable.

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 209.165.201.1
Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

- Ping de PC-C a router 3

```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.30.30.1
Pinging 172.30.30.1 with 32 bytes of data:
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

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

- Entre R1 y R2

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

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

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

R1>enable
R1#ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

R1#
```

- Entre R2 y R3

```
IOS Command Line Interface

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

%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

R2>enable
R2#ping 172.30.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

R2#
```

Parte 2: configurar y verificar el routing RIPv2

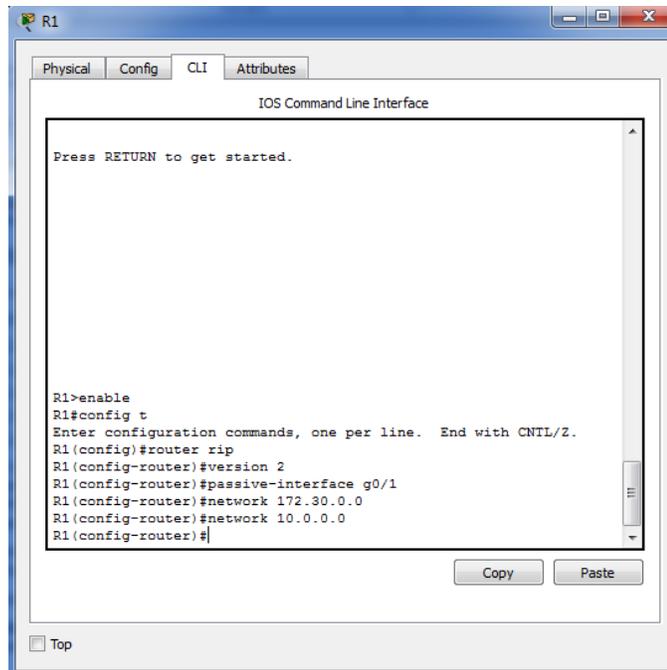
En la parte 2, configurará el routing RIPv2 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente. Una vez que haya verificado RIPv2, deshabilitará el sumarización automática, configurará una ruta predeterminada y verificará la conectividad de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

Paso 1. 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
```

El comando **passive-interface** evita que las actualizaciones de routing se envíen a través de la interfaz especificada. Este proceso evita tráfico de routing innecesario en la LAN. Sin embargo, la red a la que pertenece la interfaz especificada aún se anuncia en las actualizaciones de routing enviadas por otras interfaces.



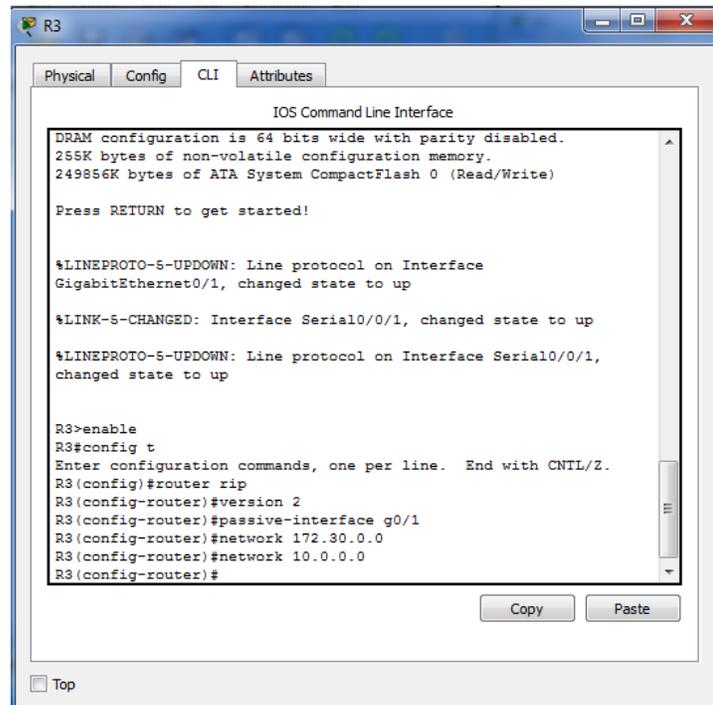
The screenshot shows the CLI window for router R1. The window title is 'R1' and it has tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The main area is titled 'IOS Command Line Interface' and contains the following text:

```
Press RETURN to get started.

R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
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
R1(config-router)#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons and a 'Top' button.

- 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.



The screenshot shows the CLI window for router R3. The window title is 'R3' and it has tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The main area is titled 'IOS Command Line Interface' and contains the following text:

```
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

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

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

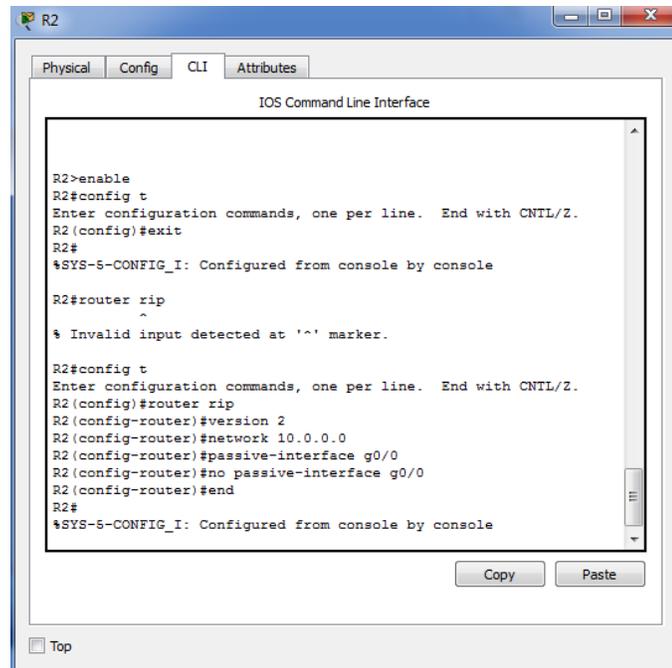
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

R3>enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#passive-interface g0/1
R3(config-router)#network 172.30.0.0
R3(config-router)#network 10.0.0.0
R3(config-router)#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons and a 'Top' button.

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

Nota: no es necesario establecer la interfaz G0/0 como pasiva en el R2, porque la red asociada a esta interfaz no se está anunciando.

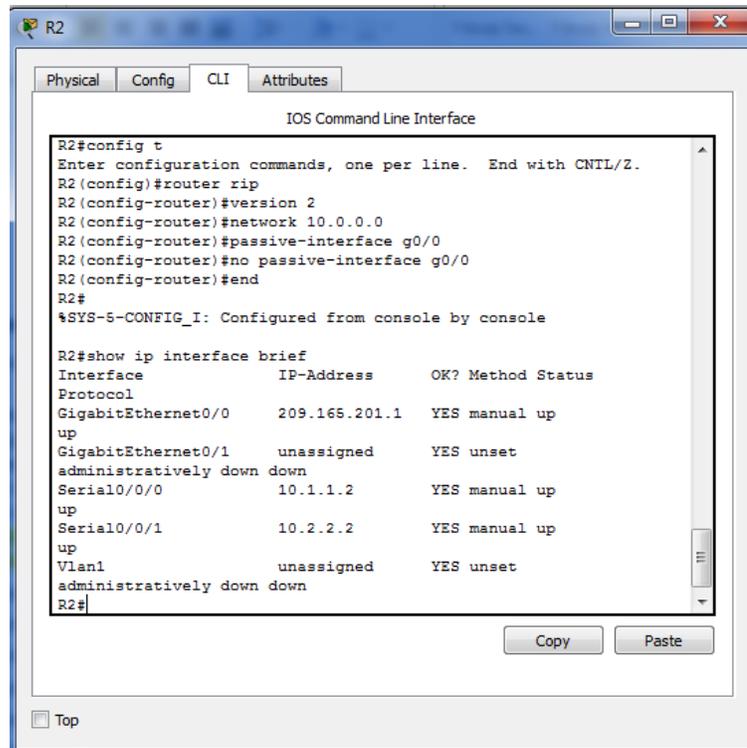


Paso 2. examinar el estado actual de la red.

- 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



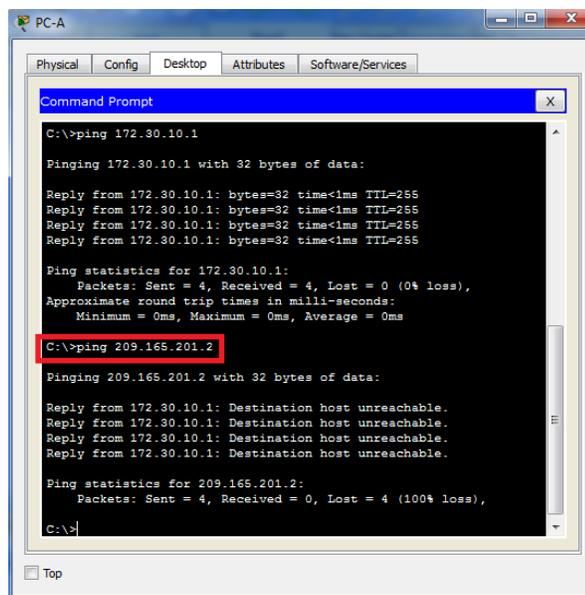
b. Verifique la conectividad entre las computadoras.

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

R/.No

¿Por qué?

R/. De R2 no hay una ruta que llegue a PC-B o no está anunciando la ruta a PC-B, esta red no está participando en RIP

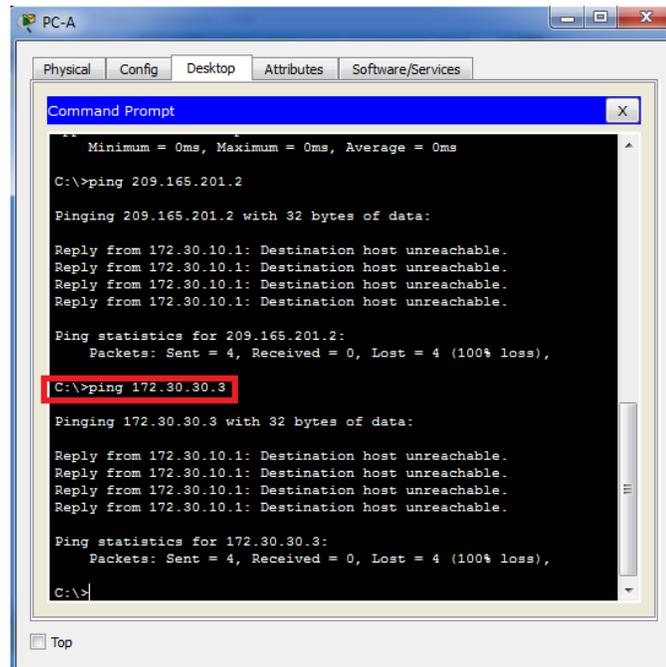


¿Es posible hacer ping de la PC-A a la PC-C?

R/.No

¿Por qué?

R/.R1 y R3 no tienen rutas hacia la subred específica en el router remoto.



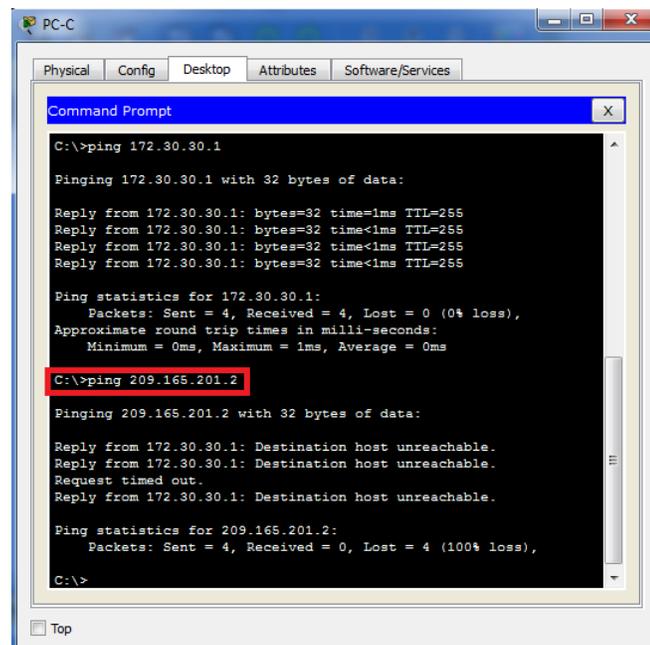
```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

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

R/.No

¿Por qué?

R/.No hay una ruta que llegue a PC-B o no está anunciando la ruta a PC-B, esta red no está participando en RIP



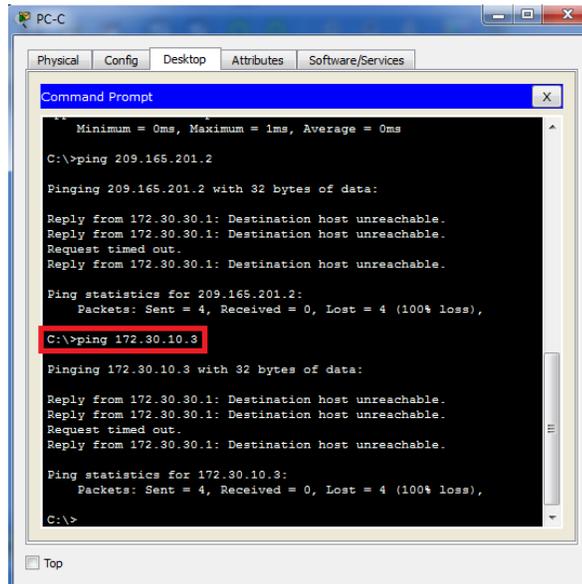
```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.1
Pinging 172.30.30.1 with 32 bytes of data:
Reply from 172.30.30.1: bytes=32 time=1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Request timed out.
Reply from 172.30.30.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

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

R/.No

¿Por qué?

R/.R1 y R3 no tienen rutas hacia la subred específica en el router remoto.



```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Request timed out.
Reply from 172.30.30.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.30.10.3
Pinging 172.30.10.3 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Request timed out.
Reply from 172.30.30.1: Destination host unreachable.
Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

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)
```

```
R1>enable
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 1 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
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           00:00:17
Distance: (default is 120)
R1#
```

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

R/.Nos envía versión 2 por la dirección multicast 224.0.0.9 via serial 0/0/0 y via serial 0/0/1

```
R2>en
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.0.0/16 via 0.0.0.0 in 1 hops
```

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

```
R2
Physical Config CLI Attributes
IOS Command Line Interface
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
R2#undebbug all
All possible debugging has been turned off
R2#
```

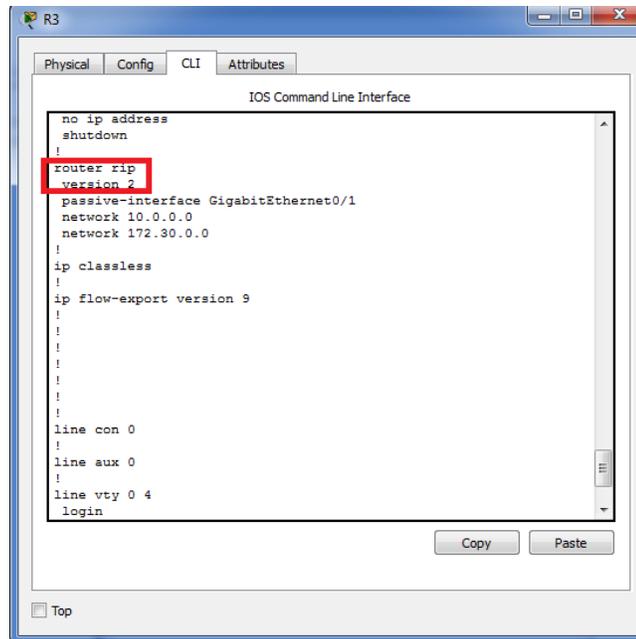
Al emitir el comando **show run** en el R3, ¿qué información se proporciona que confirma que RIPv2 está en ejecución?

R/. Router rip

Versión 2

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3>enable
R3#show run
Building configuration...

Current configuration : 849 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
```



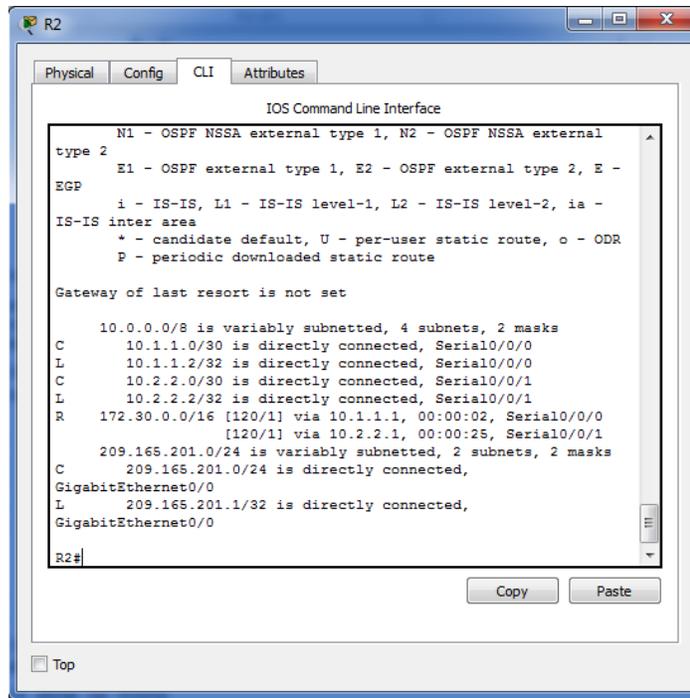
- d. Examinar el sumarización automática de las rutas.

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
```

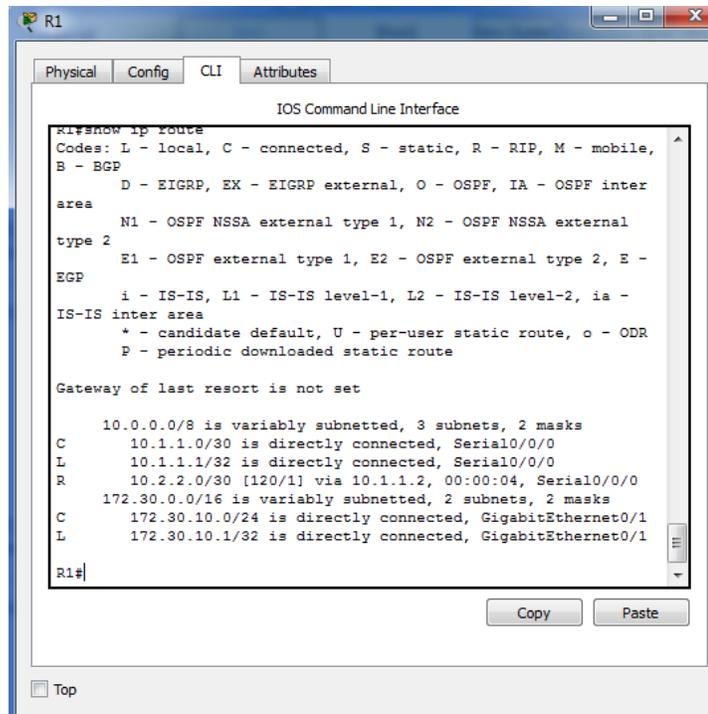


El R1 solo muestra sus propias subredes para la red 172.30.0.0. El R1 no tiene ninguna ruta para las subredes 172.30.0.0 en el R3.

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
```

```
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, 3 subnets, 2 masks
R   10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:22, Serial0/0/1
C   10.2.2.0/30 is directly connected, Serial0/0/1
L   10.2.2.1/32 is directly connected, Serial0/0/1
L   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#
```

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

R/. 172.30.0.0/16 via 0.0.0.0 in 1 hops

```
R2>enableRIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops

R2>enableRIP: sending v2 update to 224.0.0.9 via Serial0/0/0
(10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0

R2#debug ip rip RIP: received v2 update from 10.1.1.1 on
Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops

RIP protocol debugging is on
R2#
```

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 3. Desactivar la sumarización automática.

- 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
```

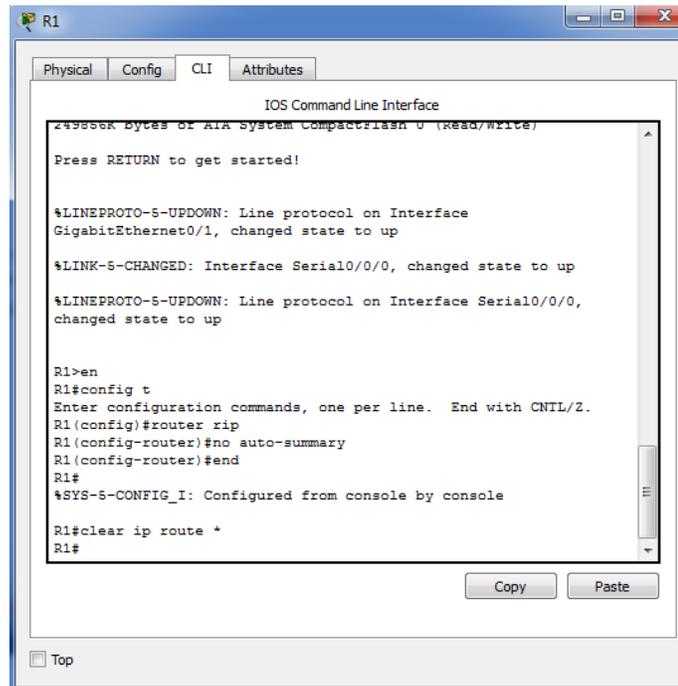
```
R1(config-router)# no auto-summary
```

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

```
R1(config-router)# end
```

```
R1# clear ip route *
```

Para R1 tendremos:



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
249886K bytes of ATA System CompactFlash 0 (read/write)
Press RETURN to get started!

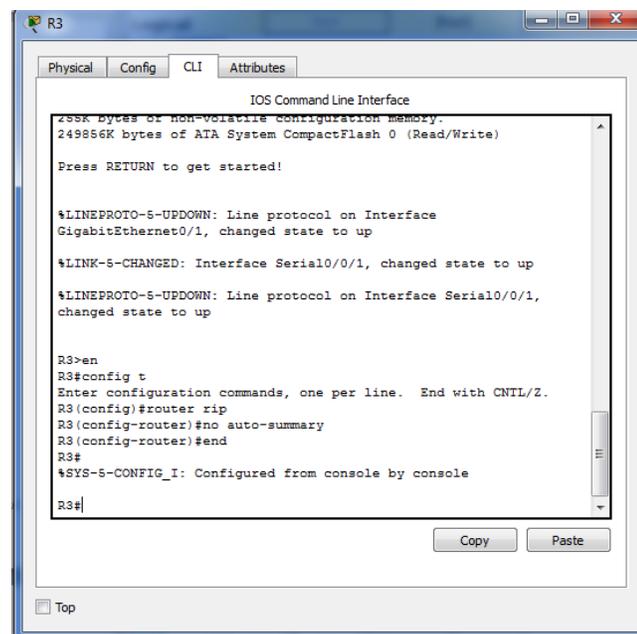
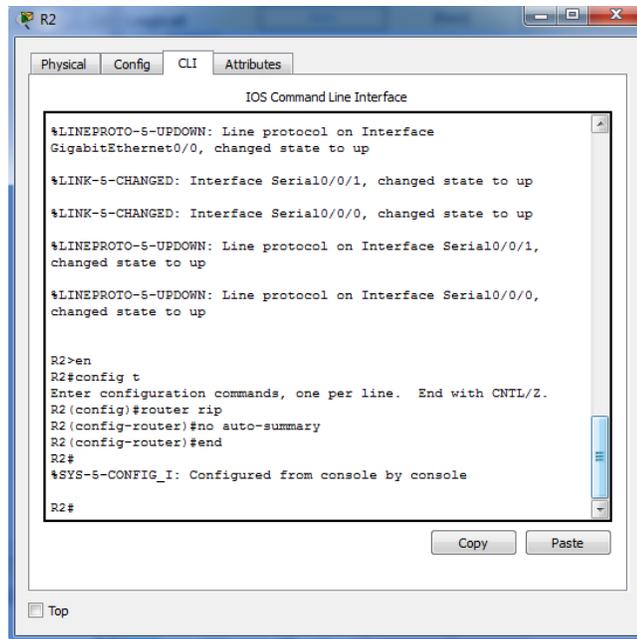
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#no auto-summary
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#clear ip route *
R1#
```



- 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

```

R2
Physical Config CLI Attributes

%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

R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

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
R   172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R   172.30.0.0/16 is possibly down, routing via 10.2.2.1, Serial0/0/1
R   172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:08, Serial0/0/0
R   172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
C   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

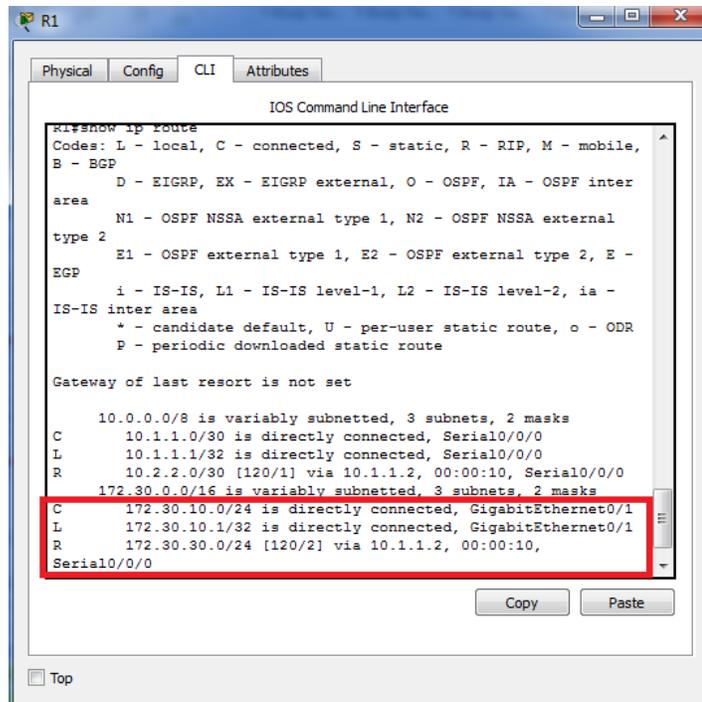
```

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
```

```
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, 3 subnets, 2 masks
R    10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:04, Serial0/0/1
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    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R    172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:04,
Serial0/0/1
C    172.30.30.0/24 is directly connected, GigabitEthernet0/1
L    172.30.30.1/32 is directly connected, GigabitEthernet0/1
```

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?

R/.172.30.30.0/24 via 0.0.0.0, metric 2, tag 0

¿Se incluyen ahora las máscaras de las subredes en las actualizaciones de enrutamiento? R/.SI

```
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.30.0/24 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.30.0/24 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
```

```
R2#undebug all
^
% Invalid input detected at '^' marker.

R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.30.0/24 via 0.0.0.0 in 1 hops

R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/1
(10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
172.30.30.0/24 via 0.0.0.0, metric 2, tag 0

undebug all
All possible debugging has been turned off
R2#no debug ip rip
RIP protocol debugging is off
R2#
```

Paso 4. Configure y redistribuya una ruta predeterminada para el acceso a Internet.

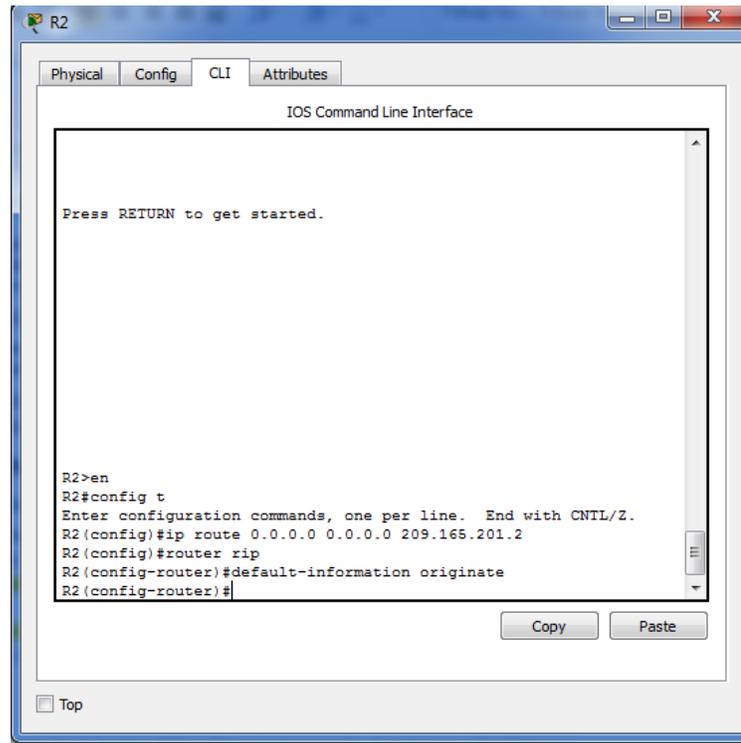
- Desde el R2, cree una ruta estática a la red 0.0.0.0 0.0.0.0, con el comando **ip route**. Esto envía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet al establecer un gateway de último recurso en el router R2.

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

- 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 5. 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

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
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 10.1.1.2 to network 0.0.0.0
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, 00:00:01, 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, 00:00:01,
Serial0/0/0
R* 0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:01, Serial0/0/0
R1#
Copy Paste
Top
```

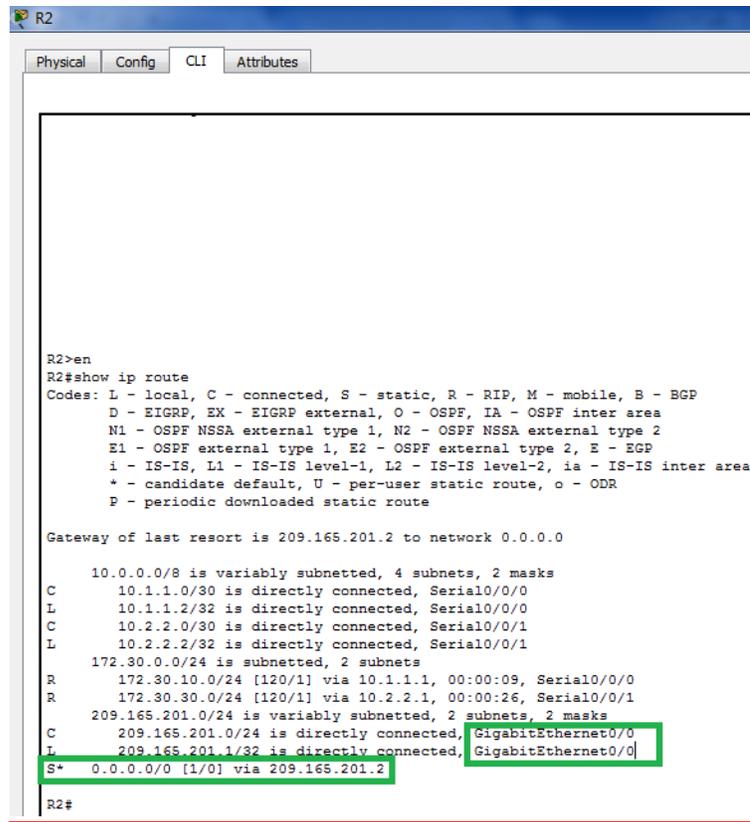
¿Cómo se puede saber, a partir de la tabla de routing, que la red dividida en subredes que comparten el R1 y el R3 tiene una ruta para el tráfico de Internet?

R/. Hay un Gateway de último alcance, es decir, una puerta de enlace y la ruta predeterminada o por defecto aparece o nos muestra en la tabla de ruteo que esta prendida a través de 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?

R/.R2 tiene una ruta estática por defecto a través de 0.0.0.0/0 [1/0] via 209.165.201.2 la cual es directamente conectada a G0/0



```
R2>en
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 209.165.201.2 to network 0.0.0.0

 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
 L   172.30.0.0/24 is subnetted, 2 subnets
 R   172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
 R   172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:26, Serial0/0/1
 C   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
 S*  0.0.0.0/0 [1/0] via 209.165.201.2
R2#
```

Paso 6. 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?

R/.SI

```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Request timed out.
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 7ms

C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=2ms TTL=126
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 5ms

C:\>
```

```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=12ms TTL=126
Reply from 209.165.201.2: bytes=32 time=11ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>
```

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?

R/.Si

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

```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Reply from 209.165.201.2: bytes=32 time=2ms TTL=126
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 5ms

C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=20ms TTL=125
Reply from 172.30.30.3: bytes=32 time=12ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 20ms, Average = 14ms

C:\>
```

```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=12ms TTL=126
Reply from 209.165.201.2: bytes=32 time=11ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.10.3: bytes=32 time=14ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Reply from 172.30.10.3: bytes=32 time=22ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms TTL=125

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 22ms, Average = 15ms

C:\>
```

Parte 3: configurar IPv6 en los dispositivos

En la parte 3, configurará todas las interfaces con direcciones IPv6 y verificará la conectividad.

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

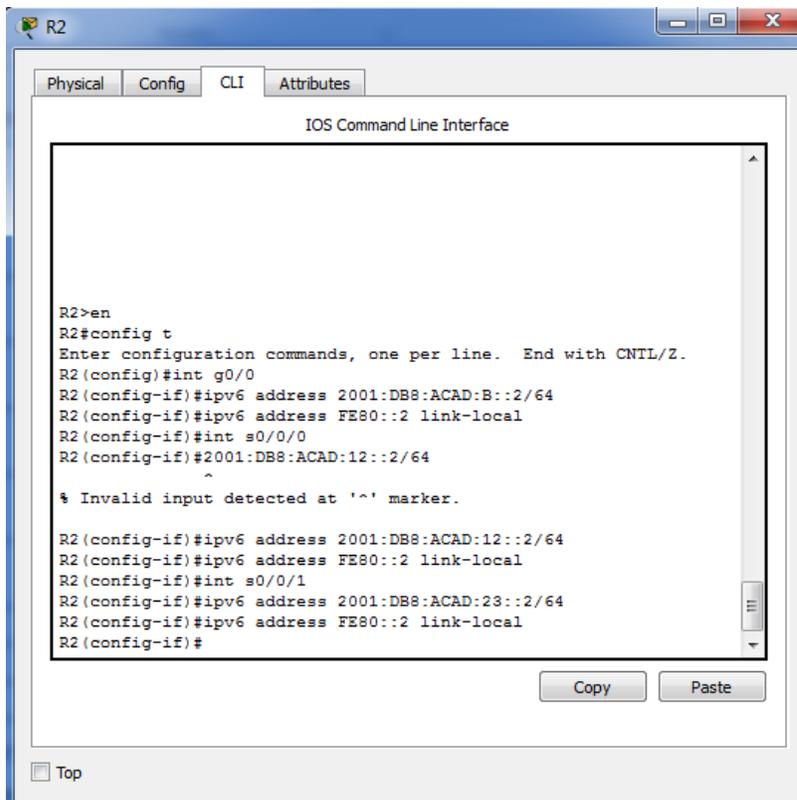
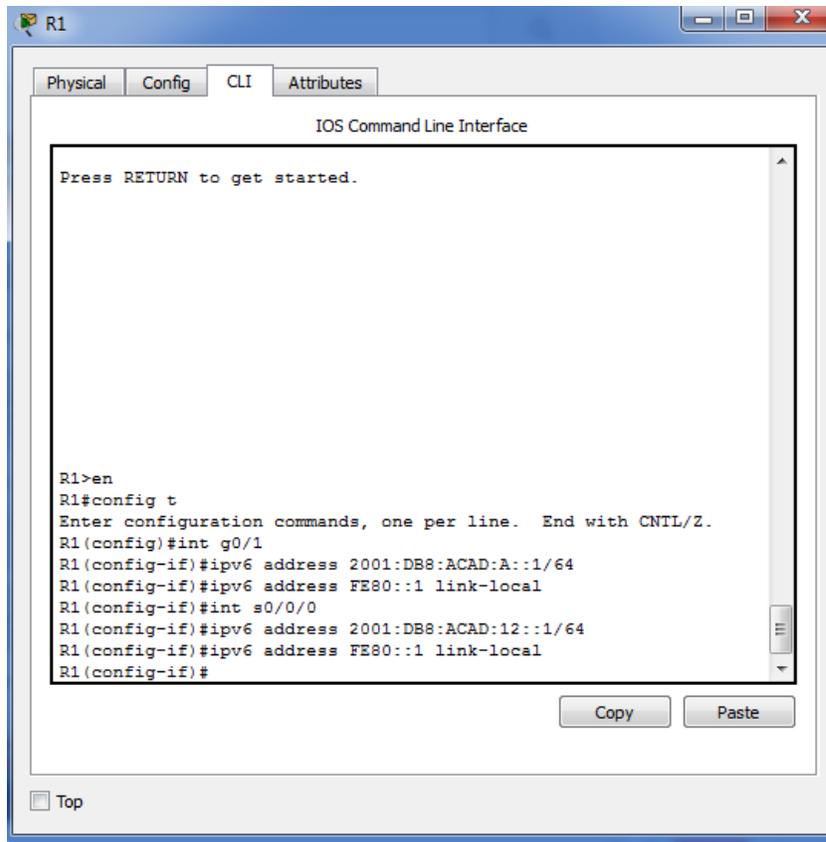
Paso 1. configurar los equipos host.

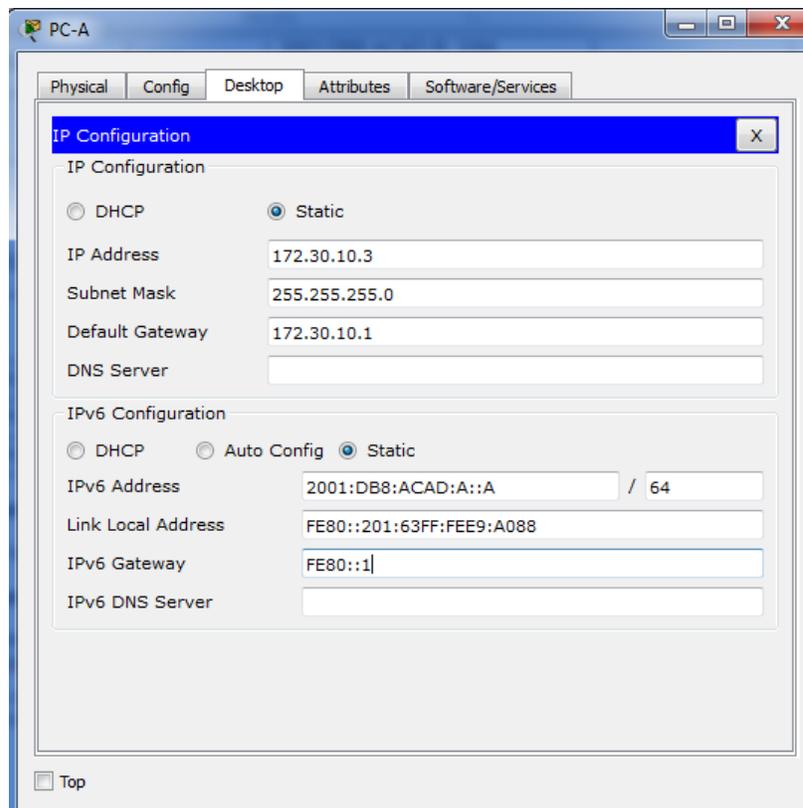
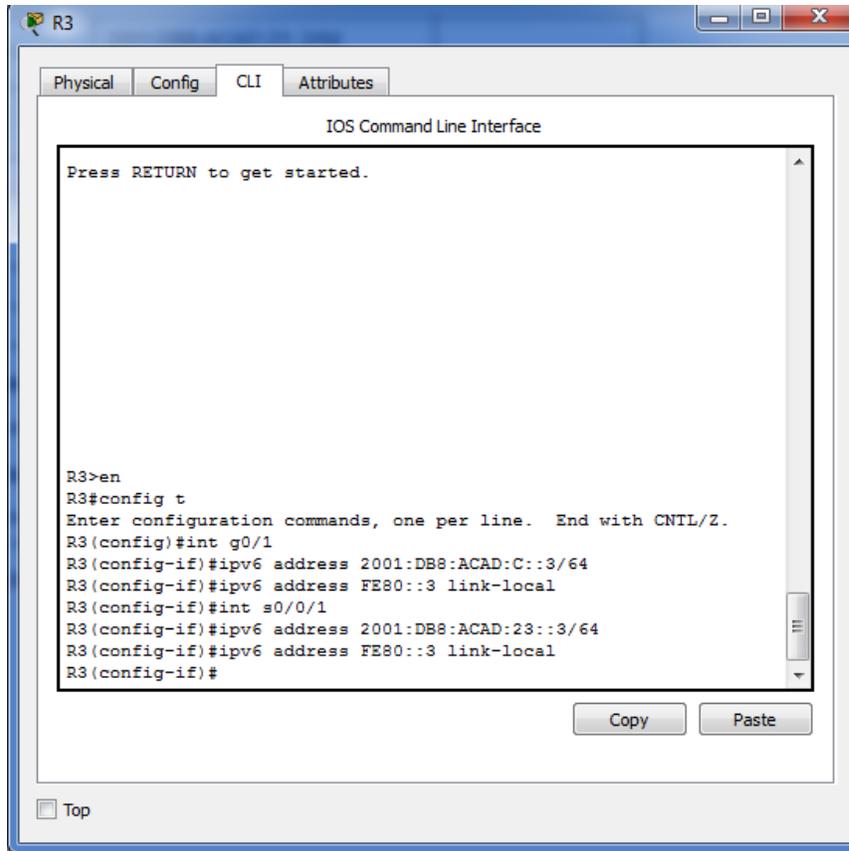
Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

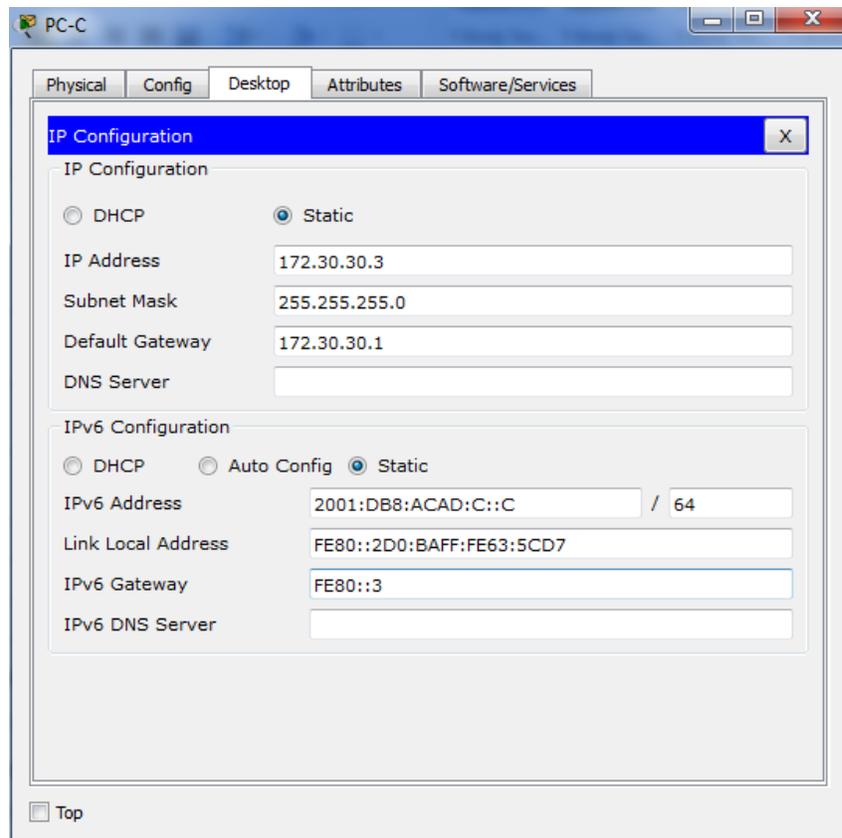
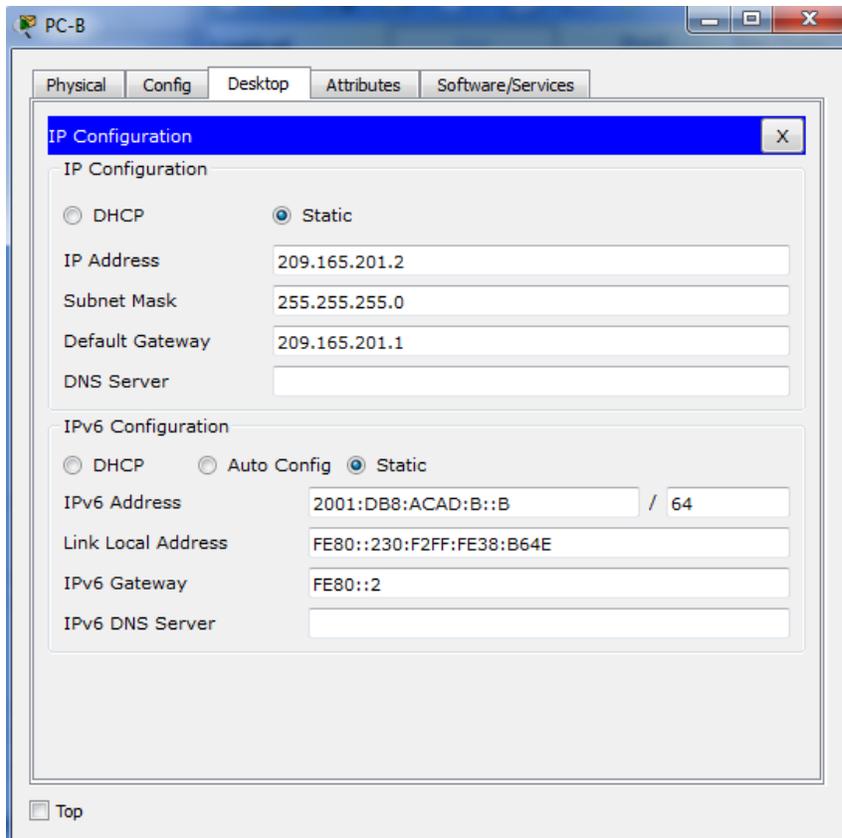
Paso 2. configurar IPv6 en los routers.

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.

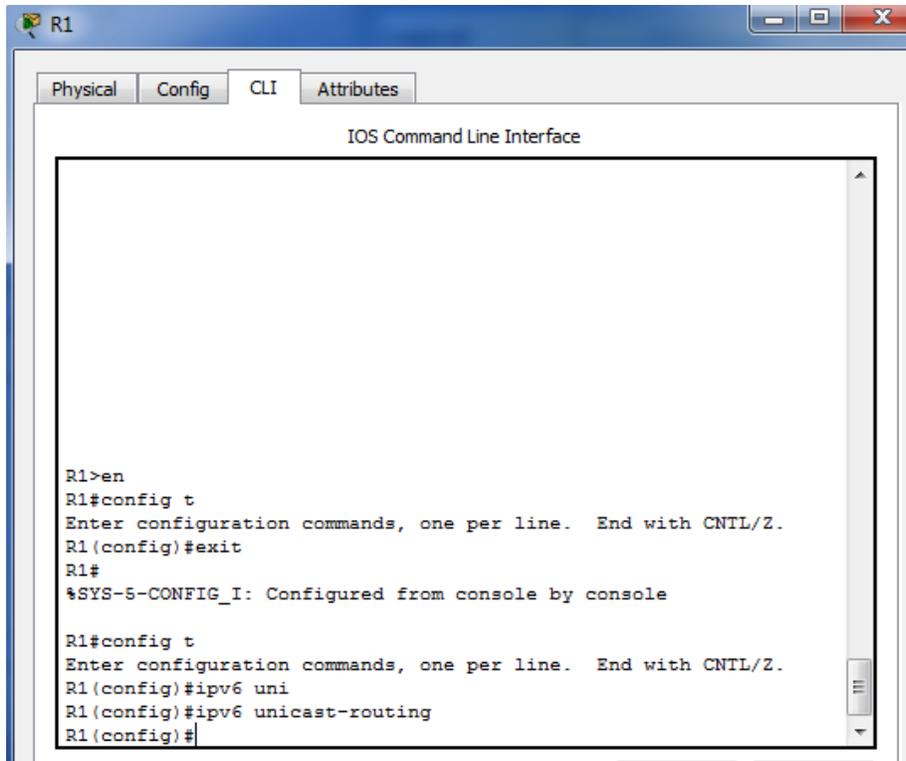
- a. Para cada interfaz del router, asigne la dirección global y la dirección link local de la tabla de direccionamiento.







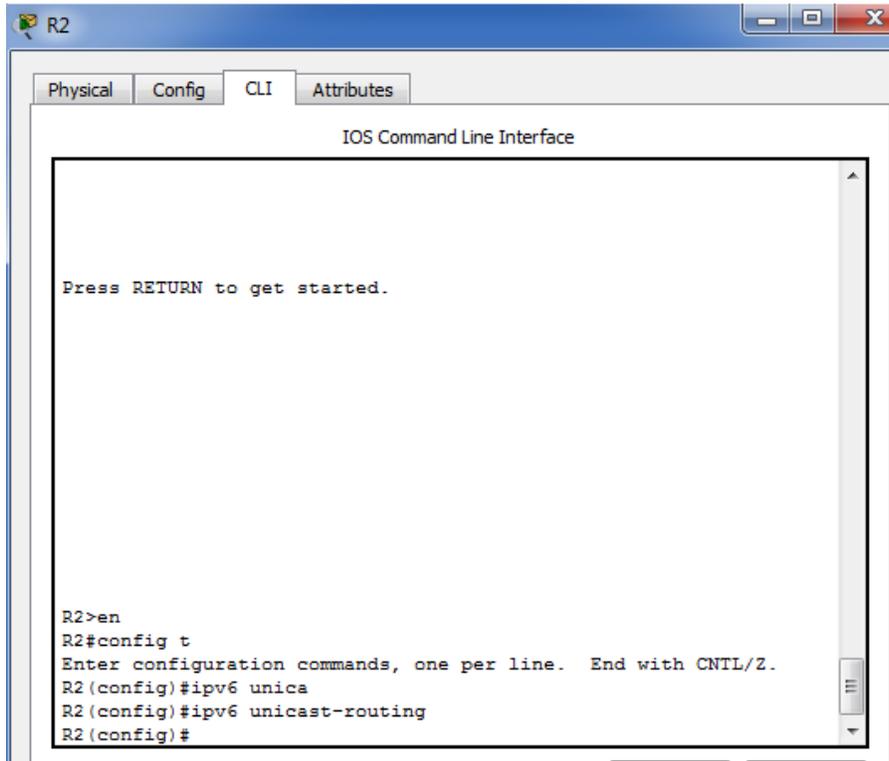
b. Habilite el routing IPv6 en cada router.



The screenshot shows a window titled 'R1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following sequence of commands and responses:

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

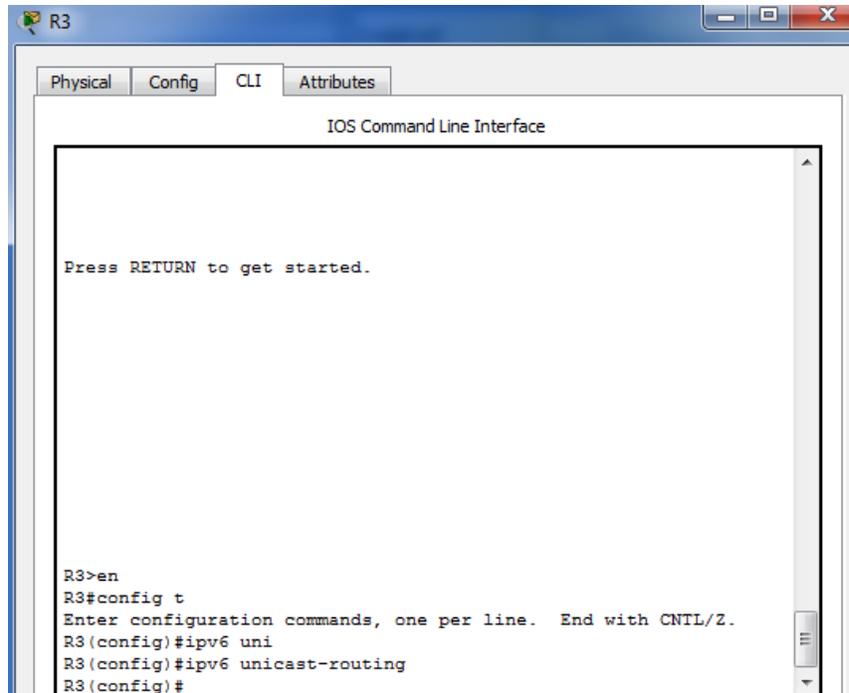
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 uni
R1(config)#ipv6 unicast-routing
R1(config)#
```



The screenshot shows a window titled 'R2' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following sequence of commands and responses:

```
Press RETURN to get started.

R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#
```

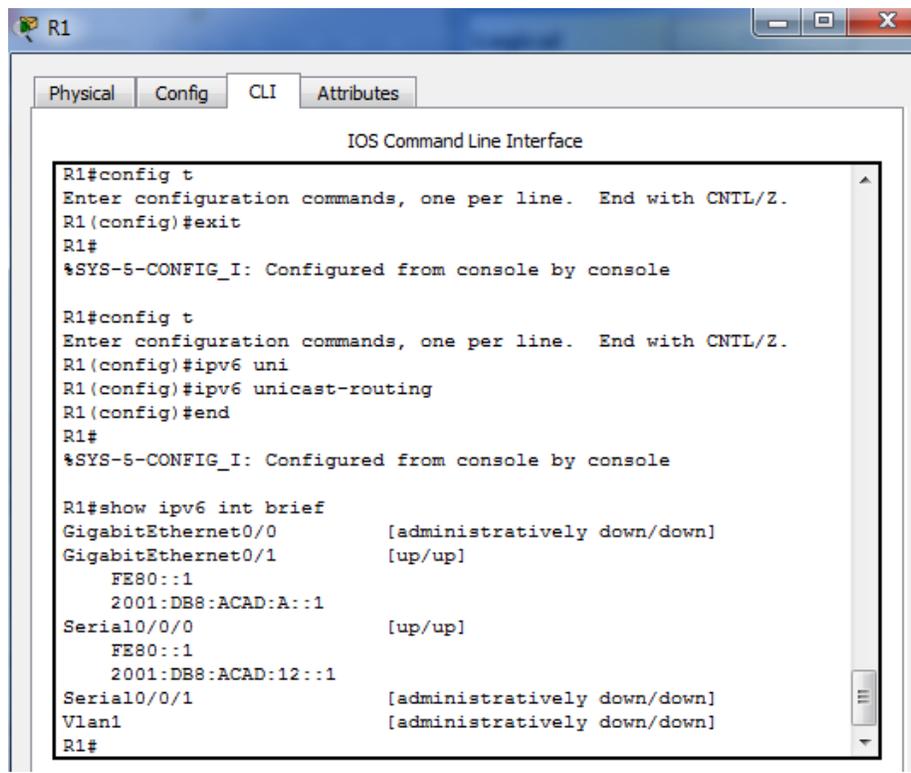


The screenshot shows the CLI window for router R3. The 'CLI' tab is selected. The text in the window reads: 'Press RETURN to get started.' followed by a series of commands: 'R3>en', 'R3#config t', 'R3(config)#ipv6 uni', 'R3(config)#ipv6 unicast-routing', and 'R3(config)#'.

```
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 uni
R3(config)#ipv6 unicast-routing
R3(config)#
```

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.

R/.Show ipv6 interface brief



The screenshot shows the CLI window for router R1. The 'CLI' tab is selected. The text in the window shows the configuration process: 'R1#config t', 'R1(config)#exit', 'R1# %SYS-5-CONFIG_I: Configured from console by console', 'R1#config t', 'R1(config)#ipv6 uni', 'R1(config)#ipv6 unicast-routing', 'R1(config)#end', 'R1# %SYS-5-CONFIG_I: Configured from console by console', and finally the verification command 'R1#show ipv6 int brief' with its output.

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

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 uni
R1(config)#ipv6 unicast-routing
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 int brief
GigabitEthernet0/0      [administratively down/down]
GigabitEthernet0/1      [up/up]
    FE80::1
    2001:DB8:ACAD:A::1
Serial10/0/0            [up/up]
    FE80::1
    2001:DB8:ACAD:12::1
Serial10/0/1            [administratively down/down]
Vlan1                   [administratively down/down]
R1#
```

```
R2
Physical Config CLI Attributes
IOS Command Line Interface

R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ipv6 int brief
GigabitEthernet0/0      [up/up]
    FE80::2
    2001:DB8:ACAD:B::2
GigabitEthernet0/1      [administratively down/down]
Serial0/0/0             [up/up]
    FE80::2
    2001:DB8:ACAD:12::2
Serial0/0/1             [up/up]
    FE80::2
    2001:DB8:ACAD:23::2
Vlan1                   [administratively down/down]
R2#
```

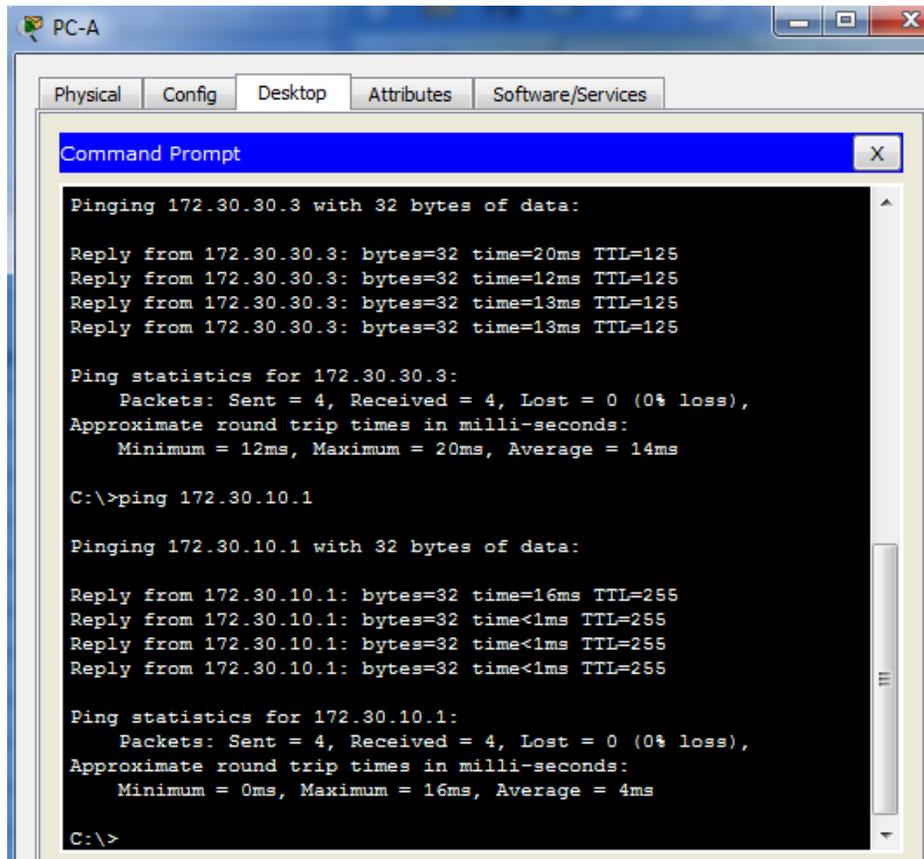
```
R3
Physical Config CLI Attributes
IOS Command Line Interface

R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ipv6 int brief
GigabitEthernet0/0      [administratively down/down]
GigabitEthernet0/1      [up/up]
    FE80::3
    2001:DB8:ACAD:C::3
Serial0/0/0             [administratively down/down]
Serial0/0/1             [up/up]
    FE80::3
    2001:DB8:ACAD:23::3
Vlan1                   [administratively down/down]
R3#
```

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

- Ping de PC-A a R1



The screenshot shows a Windows Command Prompt window titled "PC-A". The window has tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The Command Prompt displays the following text:

```
Command Prompt
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.30.3: bytes=32 time=20ms TTL=125
Reply from 172.30.30.3: bytes=32 time=12ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 20ms, Average = 14ms

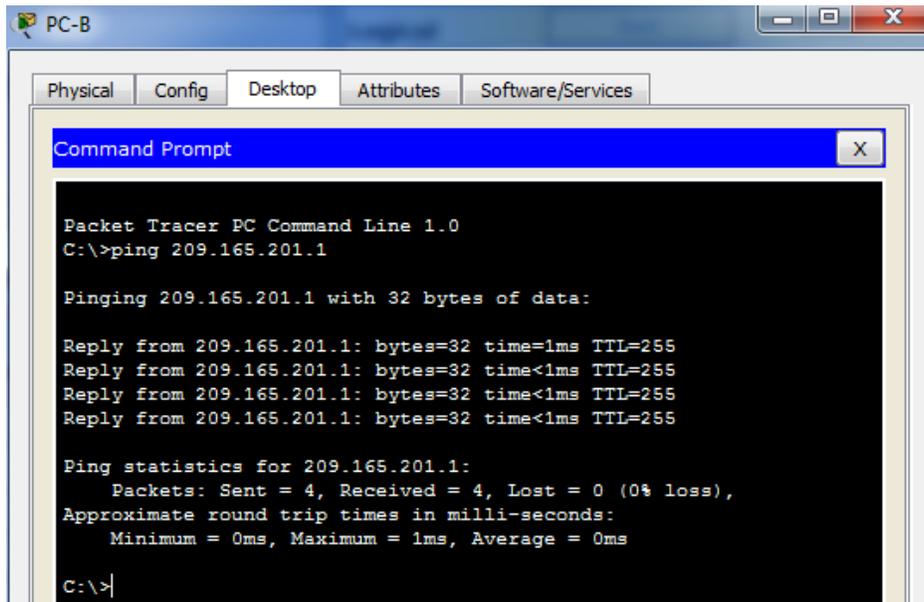
C:\>ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:
Reply from 172.30.10.1: bytes=32 time=16ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 4ms

C:\>
```

- Ping de PC-B a R2



The screenshot shows a Packet Tracer PC Command Line window titled "PC-B". The window has tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

- Ping de PC-C a R3

```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 172.30.10.3 with 32 bytes of data:
Reply from 172.30.10.3: bytes=32 time=14ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Reply from 172.30.10.3: bytes=32 time=22ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 22ms, Average = 15ms
C:\>ping 172.30.30.1
Pinging 172.30.30.1 with 32 bytes of data:
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

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

- **Ping entre R1 y R2**

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

R1>en
R1#ping 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms

R1#
```

- **Ping entre R2 y R3**

```
R2
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

R2>en
R2#ping 172.30.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms
R2#
```

- Ping entre R3 y R1

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

R3>en
R3#ping 172.30.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.10.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
2/5/20 ms
R3#
```

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.

Paso 1. 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.

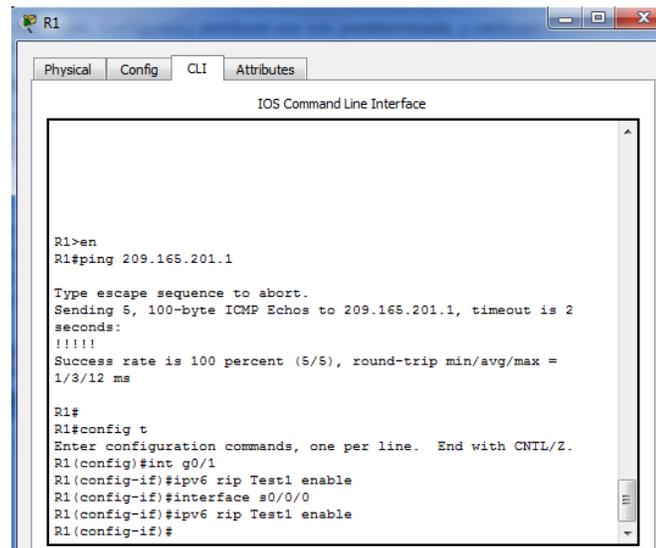
- a. Emita el comando **ipv6 rip Test1 enable** para cada interfaz en el R1 que participará en el routing RIPng, donde **Test1** es el nombre de proceso pertinente en el nivel local.

```
R1(config)# interface g0/1
```

```
R1(config)# ipv6 rip Test1 enable
```

```
R1(config)# interface s0/0/0
```

```
R1(config)# ipv6 rip Test1 enable
```



The screenshot shows the CLI of router R1. It displays the output of a ping command to 209.165.201.1, which is successful. Below that, it shows the configuration of interfaces g0/1 and s0/0/0 with the command 'ipv6 rip Test1 enable' applied to both.

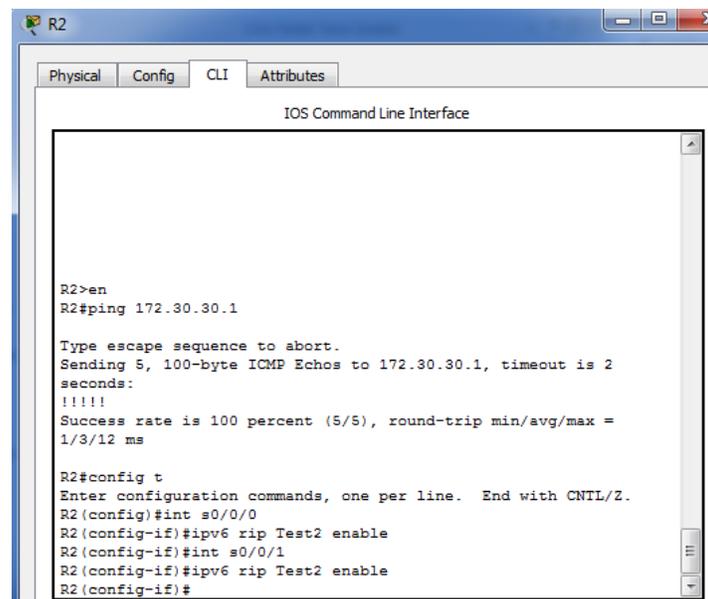
```
R1
Physical Config CLI Attributes
IOS Command Line Interface

R1>en
R1#ping 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms

R1#
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#
```

- 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



The screenshot shows the CLI of router R2. It displays the output of a ping command to 172.30.30.1, which is successful. Below that, it shows the configuration of interfaces s0/0/0 and s0/0/1 with the command 'ipv6 rip Test2 enable' applied to both. The G0/0 interface is not configured.

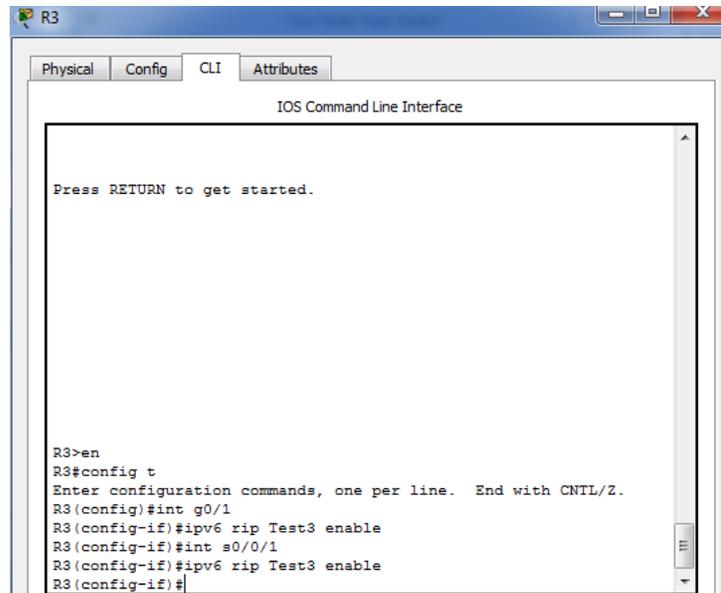
```
R2
Physical Config CLI Attributes
IOS Command Line Interface

R2>en
R2#ping 172.30.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#
```

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

A screenshot of the R3 router's CLI interface. The window title is 'R3'. The tabs are 'Physical', 'Config', 'CLI', and 'Attributes'. The main area is titled 'IOS Command Line Interface'. The text inside shows the following commands and their outputs:

```
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#
```

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"

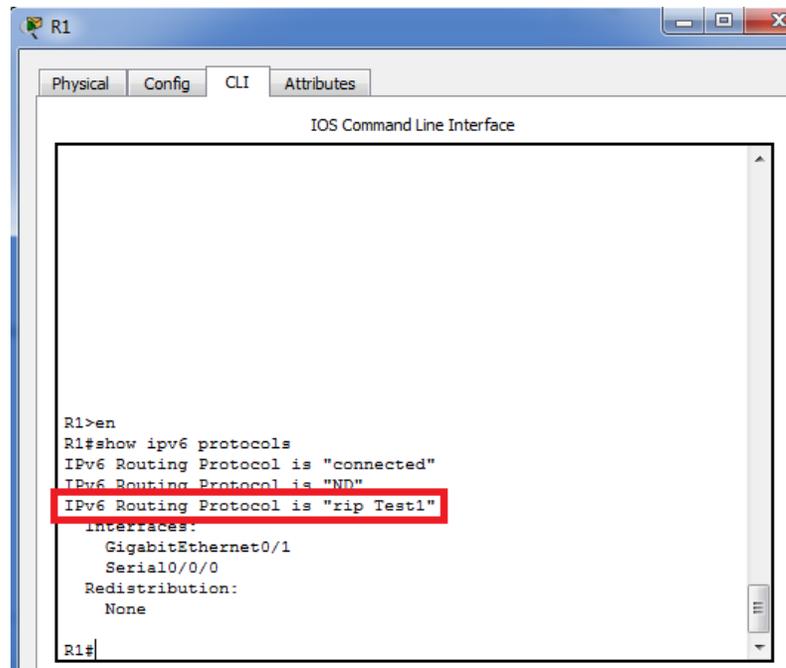
Interfaces:

Serial0/0/0

GigabitEthernet0/1

Redistribution:

None

A screenshot of the R1 router's CLI interface. The window title is 'R1'. The tabs are 'Physical', 'Config', 'CLI', and 'Attributes'. The main area is titled 'IOS Command Line Interface'. The text inside shows the following commands and their outputs:

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

The line 'IPv6 Routing Protocol is "rip Test1"' is highlighted with a red box.

¿En qué forma se indica RIPng en el resultado?

R/.RIPng esta listado por el nombre del proceso

- 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

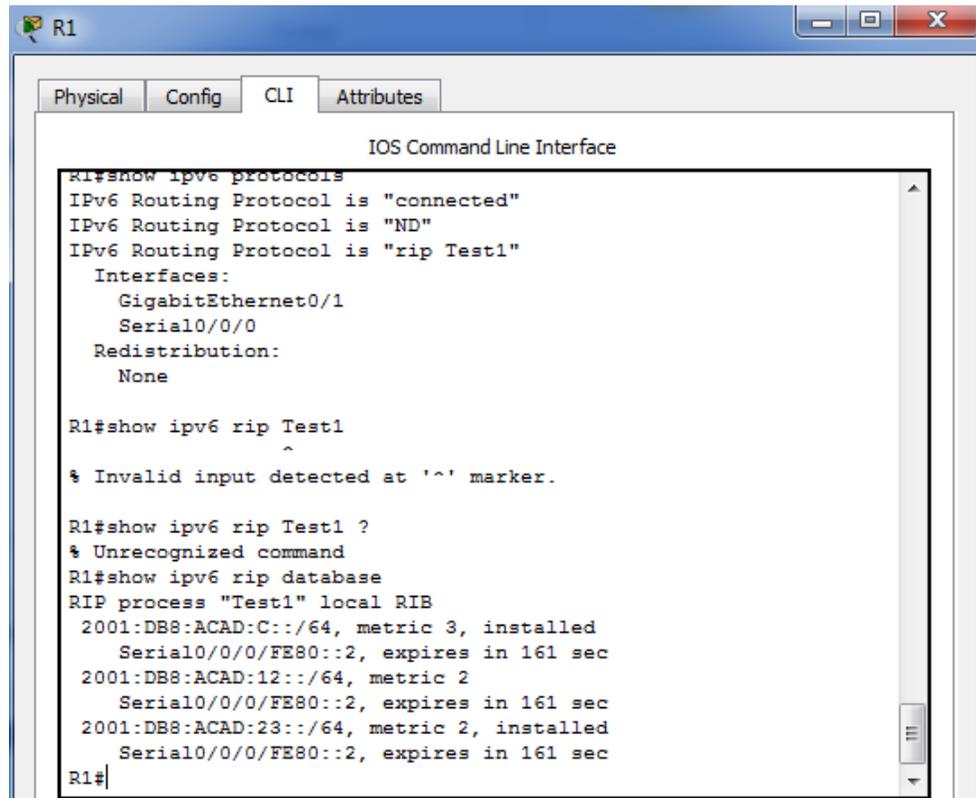
Interfaces:

GigabitEthernet0/1

Serial0/0/0

Redistribution:

None



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

R1#show ipv6 rip Test1
^
% Invalid input detected at '^' marker.

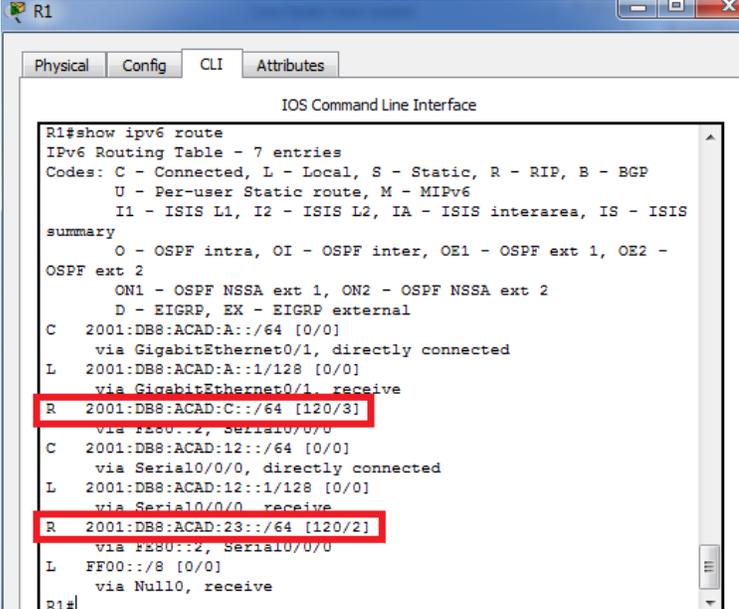
R1#show ipv6 rip Test1 ?
% Unrecognized command
R1#show ipv6 rip database
RIP process "Test1" local RIB
  2001:DB8:ACAD:C::/64, metric 3, installed
    Serial0/0/0/FE80::2, expires in 161 sec
  2001:DB8:ACAD:12::/64, metric 2
    Serial0/0/0/FE80::2, expires in 161 sec
  2001:DB8:ACAD:23::/64, metric 2, installed
    Serial0/0/0/FE80::2, expires in 161 sec
R1#
```

¿Cuáles son las similitudes entre RIPv2 y RIPng?

R/.RIPv2 y RIPng tienen la distancia administrativa de 120 y usan el conteo de saltos como la métrica y envían actualizaciones cada 30 segundos

- 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.

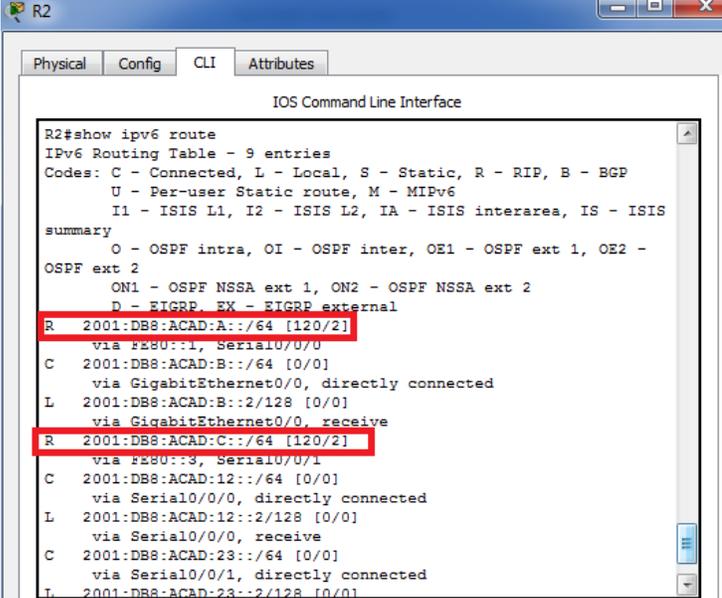
R/.Show ipv6 route



```
R1#show ipv6 route
IPv6 Routing Table - 7 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 GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
  via GigabitEthernet0/1, receive
R 2001:DB8:ACAD:C::/64 [120/3]
  via FE80::2, Serial0/0/0
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
R 2001:DB8:ACAD:23::/64 [120/2]
  via FE80::2, Serial0/0/0
L FE00::/8 [0/0]
  via Null0, receive
R1#
```

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

R/.Dos



```
R2#show ipv6 route
IPv6 Routing Table - 9 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
R 2001:DB8:ACAD:A::/64 [120/2]
  via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:B::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:B::2/128 [0/0]
  via GigabitEthernet0/0, receive
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, directly connected
L 2001:DB8:ACAD:12::2/128 [0/0]
  via Serial0/0/0, receive
C 2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::2/128 [0/0]
```

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

R/.Dos

```
R3#show ipv6 route
IPv6 Routing Table - 7 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
R 2001:DB8:ACAD:A::/64 [120/3]
  via FE80::2, Serial0/0/1
C 2001:DB8:ACAD:C::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:C::3/128 [0/0]
  via GigabitEthernet0/1, receive
R 2001:DB8:ACAD:12::/64 [120/2]
  via FE80::2, Serial0/0/1
C 2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::3/128 [0/0]
  via Serial0/0/1, receive
L FF00::/8 [0/0]
  via Null0, receive
R3#
```

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

R/.Dos

Verifique la conectividad entre las computadoras.

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

R/.No

```
PC-A
Command Prompt
C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=11ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125
Reply from 172.30.30.3: bytes=32 time=12ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:\>ping 2001:DB8:ACAD:B::B

Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Request timed out.

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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

R/.Si

```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 2001:DB8:ACAD:B::B

Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Request timed out.

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 2001:DB8:ACAD:C::C

Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=25ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 25ms, Average = 15ms

C:\>
```

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

R./No

```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Reply from 172.30.10.3: bytes=32 time=13ms TTL=125
Reply from 172.30.10.3: bytes=32 time=13ms TTL=125
Reply from 172.30.10.3: bytes=32 time=13ms TTL=125

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 13ms, Average = 12ms

C:\>ping 2001:DB8:ACAD:B::B

Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

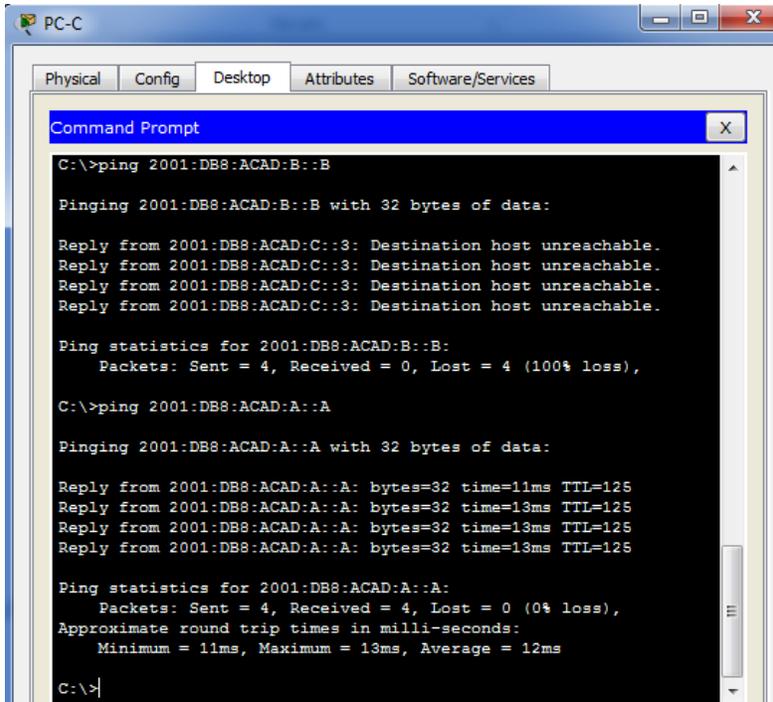
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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

R./Si



```
C:\>ping 2001:DB8:ACAD:B::B

Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 2001:DB8:ACAD:A::A

Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::A: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125

Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:\>
```

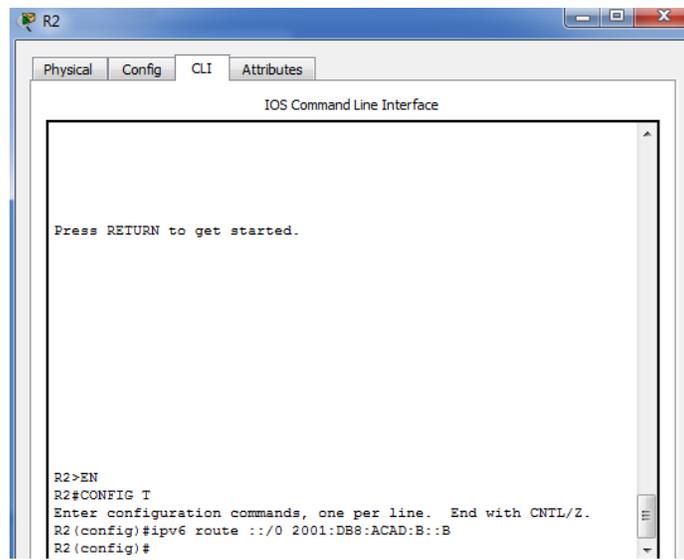
¿Por qué algunos pings tuvieron éxito y otros no?

R/.No hay una ruta que se notifique para PC-B para la red 2001:DB8:ACAD:B::/64 NETWORK

Paso 2. configurar y volver a distribuir una ruta predeterminada.

- 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.

R/.`ipv6 route ::/0 2001:DB8:ACAD:B::B`



```
R2
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

R2>EN
R2#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#
```

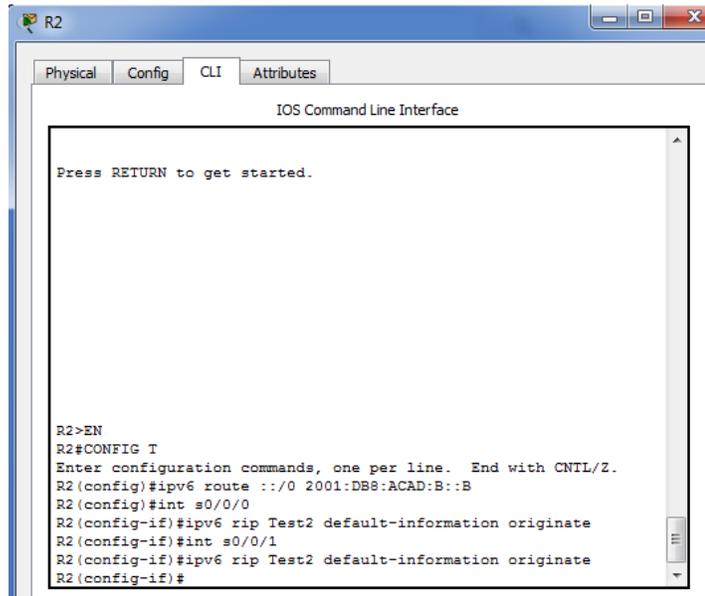
- b. Las rutas estáticas se pueden incluir en las actualizaciones RIPng mediante el comando **ipv6 rip nombre de proceso default-information originate** en el modo de configuración de interfaz. Configure los enlaces seriales en el R2 para enviar la ruta predeterminada en actualizaciones RIPng.

```
R2(config)# int s0/0/0
```

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

```
R2(config)# int s0/0/1
```

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



```
R2
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

R2>EN
R2#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#
```

Paso 3. 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
```

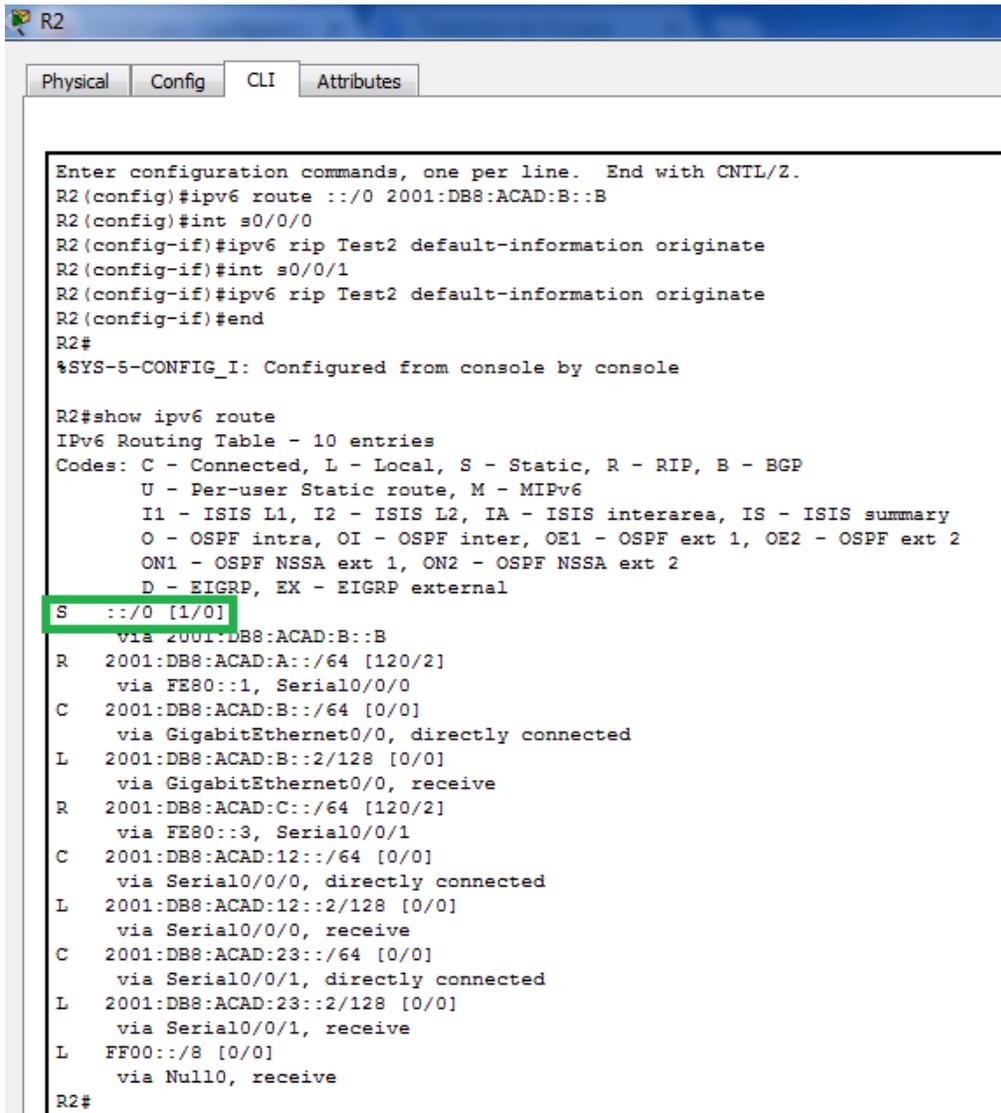
```
C 2001:DB8:ACAD:12::/64 [0/0]
```

```
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
```



```
R2
Physical Config CLI Attributes
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

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  ::/0 [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 GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:B::2/128 [0/0]
  via GigabitEthernet0/0, receive
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, directly connected
L  2001:DB8:ACAD:12::2/128 [0/0]
  via Serial0/0/0, receive
C  2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L  2001:DB8:ACAD:23::2/128 [0/0]
  via Serial0/0/1, receive
L  FF00::/8 [0/0]
  via Null0, receive
R2#
```

¿Cómo se puede saber, a partir de la tabla de routing, que el R2 tiene una ruta para el tráfico de Internet?
R/. Tiene una ruta estática por defecto que se muestra en R la señalada en verde arriba

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

```

R1#show ipv6 route
IPv6 Routing Table - 8 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
R  ::/0 [120/2]
  via FE80::2, Serial0/0/0
C  2001:DB8:ACAD:A::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:A::1/128 [0/0]
  via GigabitEthernet0/1, receive
R  2001:DB8:ACAD:C::/64 [120/3]
  via FE80::2, Serial0/0/0
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
R  2001:DB8:ACAD:23::/64 [120/2]
  via FE80::2, Serial0/0/0
L  FF00::/8 [0/0]

```

```

R3>en
R3#show ipv6 route
IPv6 Routing Table - 8 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
R  ::/0 [120/2]
  via FE80::2, Serial0/0/1
R  2001:DB8:ACAD:A::/64 [120/3]
  via FE80::2, Serial0/0/1
C  2001:DB8:ACAD:C::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:C::3/128 [0/0]
  via GigabitEthernet0/1, receive
R  2001:DB8:ACAD:12::/64 [120/2]
  via FE80::2, Serial0/0/1
C  2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L  2001:DB8:ACAD:23::3/128 [0/0]

```

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

R/.La tabla de ruteo se muestra distribuida gracias a RIPng con una métrica de 2

Paso 4. 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.

```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=25ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125
Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 25ms, Average = 15ms
C:\>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 9ms
C:\>
```

```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 12ms
C:\>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=15ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 15ms, Average = 9ms
C:\>
```

¿Tuvieron éxito los pings?

R/. SI

Reflexión

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

Sería bueno para que todos los routers no sumaricen las rutas hacia la clase mayor y así pueda haber continuidad entre redes discontinuas

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

Aprendieron de las actualizaciones de RIP recibidas desde el router 2 donde fue configurada la ruta por defecto en este caso R2

3. ¿En qué se diferencian la configuración de RIPv2 y la de RIPv6?

RIPv2 se configura como notificando las redes y RIPv6 se configura en las interfaces

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.

https://www.youtube.com/watch?v=_0VD7mIHceY

Práctica de laboratorio 8.2.4.5: Configuración de OSPFv2 Básico de área única

Topología

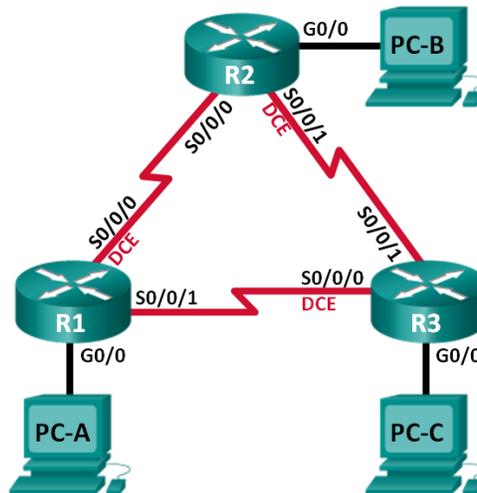


Tabla de direccionamiento

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

Información básica/situación

El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace para las redes IP. Se definió OSPFv2 para redes IPv4, y OSPFv3 para redes IPv6. OSPF detecta cambios en la topología, como fallas de enlace, y converge en una nueva estructura de routing sin bucles muy rápidamente. Computa cada ruta con el algoritmo de Dijkstra, un algoritmo SPF (Shortest Path First).

En esta práctica de laboratorio, configurará la topología de la red con routing OSPFv2, cambiará las asignaciones de ID de router, configurará interfaces pasivas, ajustará las métricas de OSPF y utilizará varios comandos de CLI para ver y verificar la información de routing OSPF.

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 universal9). Pueden utilizarse otros routers 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.

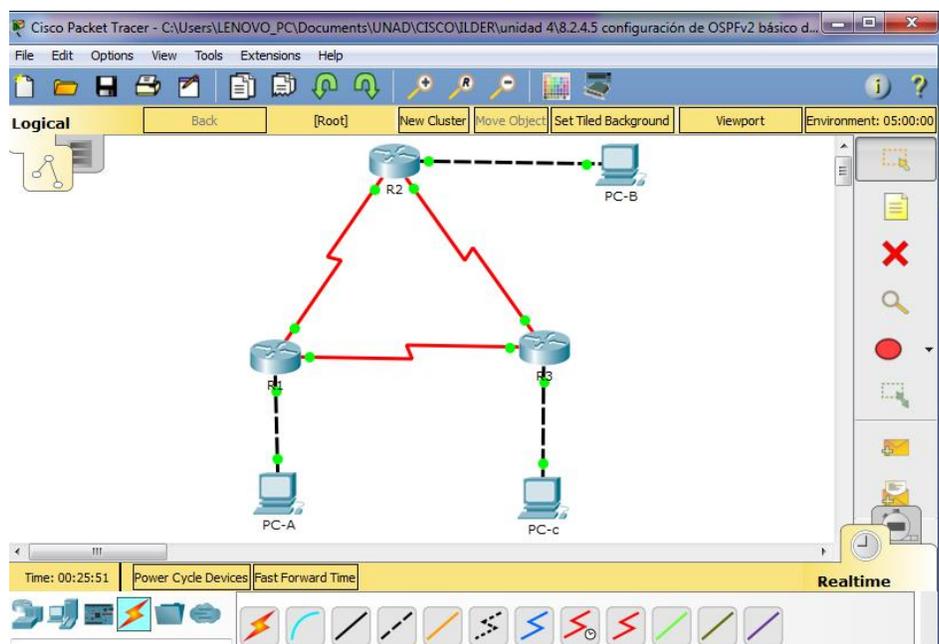
Nota: asegúrese de que los routers se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

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

Part 2: 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.

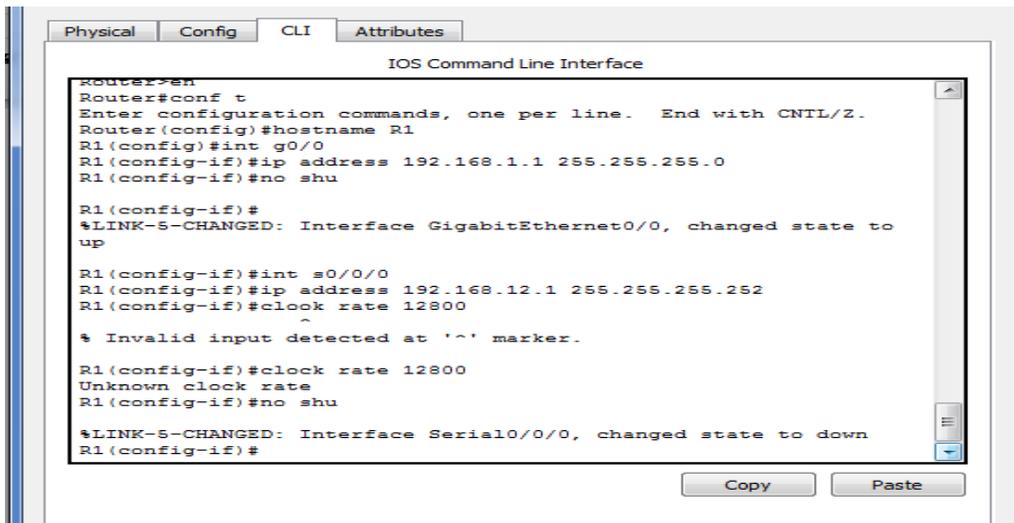


Step 1: realizar el cableado de red tal como se muestra en la topología.

Step 2: inicializar y volver a cargar los routers según sea necesario.

Step 3: 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**.



```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shu

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

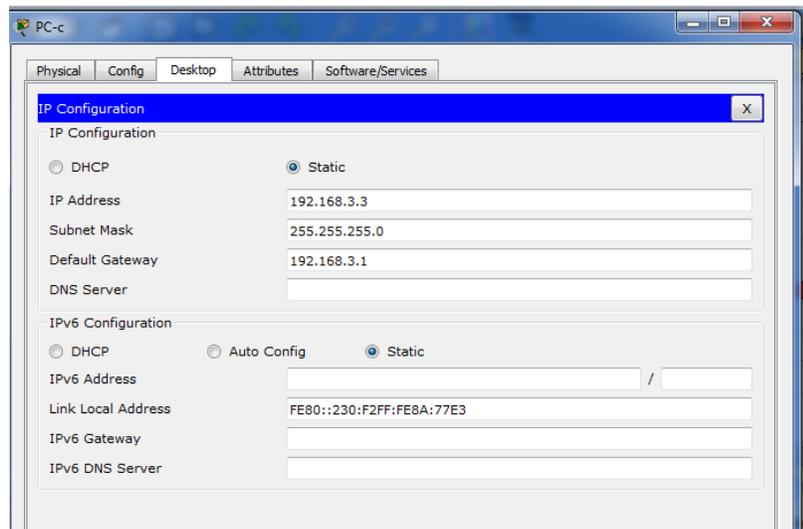
R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#clock rate 12800
^
% Invalid input detected at '^' marker.

R1(config-if)#clock rate 12800
Unknown clock rate
R1(config-if)#no shu

%LINK-S-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
```

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

Step 4: configurar los equipos host.



Step 5: 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.

Part 3: 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.

Step 1: Configure el protocolo OSPF en R1.

- 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.

- 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
```

```

Physical  Config  CLI  Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

%LINK-5-CHANGED: Interface Serial0/0/1, 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
GigabitEthernet0/0, changed state to up

R1>show ip ospf neighbor

R1>en
R1#show ip ospf neighbor

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
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 2: 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.

```

R1#
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
R1#
00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to
FULL, Loading Done
R1#

```

Step 3: verificar los vecinos OSPF y la información de routing.

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

```

R1# show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address         Interface
192.168.23.2     0    FULL/ -         00:00:33   192.168.13.2   Serial0/0/1
192.168.23.1     0    FULL/ -         00:00:30   192.168.12.2   Serial0/0/0

```

- 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

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

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0

```

```

L      192.168.1.1/32 is directly connected, GigabitEthernet0/0
O      192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O      192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
      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      192.168.12.1/32 is directly connected, Serial0/0/0
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.13.0/30 is directly connected, Serial0/0/1
L      192.168.13.1/32 is directly connected, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
      [110/128] via 192.168.13.2, 00:31:38, Serial0/0/1

```

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

show ip route

Step 4: 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
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.23.2    110          00:19:16
    192.168.23.1    110          00:20:03
  Distance: (default is 110)

```

Step 5: 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
Routing Process "ospf 1" with ID 192.168.13.1
  Start time: 00:20:23.260, Time elapsed: 00:25:08.296
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Supports area transit capability

```

```

Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps

```

Area BACKBONE (0)

```

Number of interfaces in this area is 3
Area has no authentication
SPF algorithm last executed 00:22:53.756 ago
SPF algorithm executed 7 times
Area ranges are
Number of LSA 3. Checksum Sum 0x019A61
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```

Step 6: verificar la configuración de la interfaz OSPF.

- 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	

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

```
R1# show ip ospf interface
```

```

Serial0/0/1 is up, line protocol is up
Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64

```

```

Topology-MTID    Cost    Disabled    Shutdown    Topology Name
      0         64         no         no         Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, 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 192.168.23.2
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID    Cost    Disabled    Shutdown    Topology Name
      0         64         no         no         Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:03
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
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 192.168.23.1
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
Topology-MTID    Cost    Disabled    Shutdown    Topology Name
      0         1         no         no         Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0

```

```
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
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)
```

Step 7: 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.

Part 4: 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

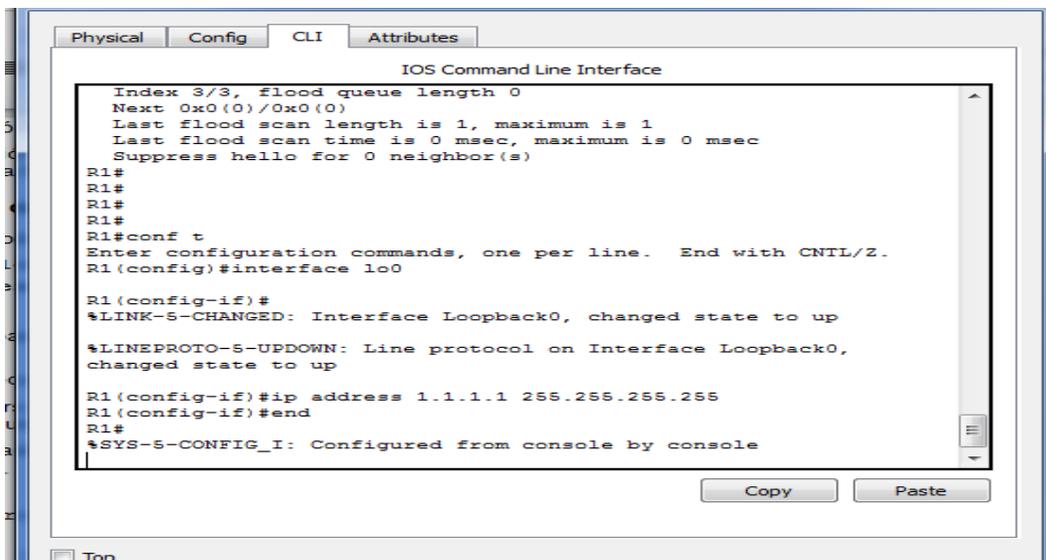
Dado que no se ha configurado ningún ID o interfaz de loopback en los tres routers, el ID de router para cada ruta se determina según la dirección IP más alta de cualquier interfaz activa.

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.

```
R1(config)# interface lo0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```



- 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.
- 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
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3          110          00:01:00
    2.2.2.2          110          00:01:14
  Distance: (default is 110)
```

- 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

Neighbor ID    Pri   State           Dead Time   Address        Interface
3.3.3.3        0     FULL/ -         00:00:35   192.168.13.2  Serial0/0/1
2.2.2.2        0     FULL/ -         00:00:32   192.168.12.2  Serial0/0/0
R1#
```

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**.

```
R1(config)# router ospf 1
R1(config-router)# router-id 11.11.11.11
Reload or use "clear ip ospf process" command, for this to take effect
R1(config)# end
```

- 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
*** IP Routing is NSF aware ***
```

```

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    33.33.33.33      110          00:00:19
    22.22.22.22      110          00:00:31
    3.3.3.3          110          00:00:41
    2.2.2.2          110          00:00:41
  Distance: (default is 110)

```

- 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
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:36	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

Part 5: 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 1: 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
```

```

GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1         no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

```

```
oob-resync timeout 40
Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
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)
```

- 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.

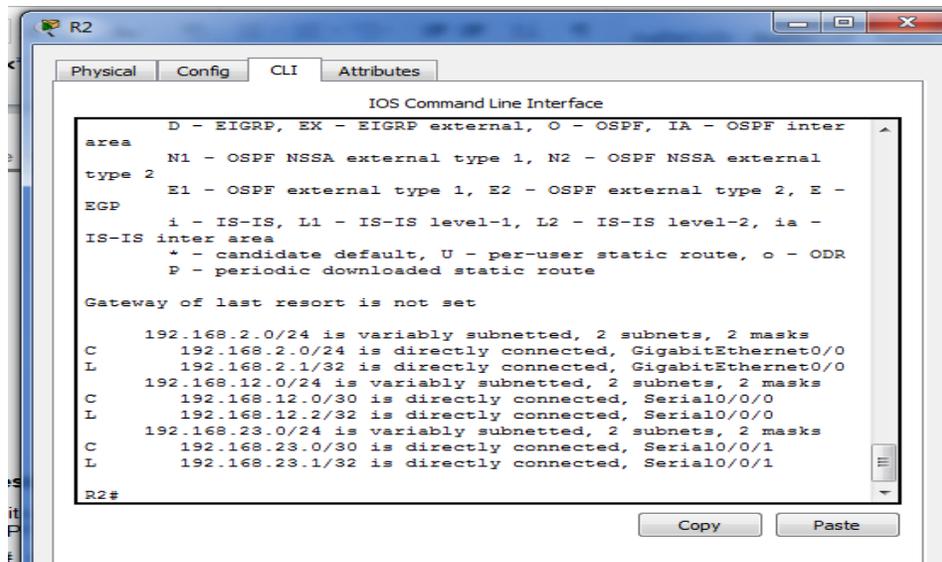
```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                 1         no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  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)
```

- 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
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

```
2.0.0.0/32 is subnetted, 1 subnets
C    2.2.2.2 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, 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 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
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 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
      [110/128] via 192.168.12.1, 00:58:32, 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    192.168.23.1/32 is directly connected, Serial0/0/1
```



Step 2: establecer la interfaz pasiva como la interfaz predeterminada en un router.

- 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
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

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

```
R2(config)# router ospf 1
```

```
R2(config-router)# passive-interface default
```

```
R2(config-router)#
```

```
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

- 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
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:34	192.168.13.2	Serial0/0/1

- 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
```

```
Serial0/0/0 is up, line protocol is up
```

```
Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
```

```
Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64
```

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

```
Transmit Delay is 1 sec, State POINT_TO_POINT
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
oob-resync timeout 40
```

```
No Hellos (Passive interface)
```

```
Supports Link-local Signaling (LLS)
```

```
Cisco NSF helper support enabled
```

```
IETF NSF helper support enabled
```

```
Index 2/2, flood queue length 0
```

```
Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 0, maximum is 0
```

```
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)
```

- 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.

```
R2(config)# router ospf 1
```

```
R2(config-router)# no passive-interface s0/0/0
```

```
R2(config-router)#
```

```
*Apr  3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING to FULL, Loading Done
```

- 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?

R/. Está usando el serial0/0/0

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3?

R/. Costo 129.

¿El R2 aparece como vecino OSPF en el R1?

R/. Si

¿El R2 aparece como vecino OSPF en el R3?

R/. No

¿Qué indica esta información?

El tráfico es el R2. Desde R3 puede ser ruteado, pero a través del router 1. La S0/0/1 en R2 aun está configurada como un serial pasivo de tal forma que la información de OSPF no está notificando a través de la interfaz S0/0/1. El costo 129 es el costo acumulado que resulta del tráfico hasta llegar a la red 2 a través de dos enlaces seriales, donde cada enlace serial tiene un costo de 64.

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

R/. R2(config-router) #no passive-interface s0/0/1

- 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?

R/. Está usando Serial0/0/1

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3 y cómo se calcula?

R/. El costo acumulado es 65. Costo Acumulado $65=64+1$

¿El R2 aparece como vecino OSPF del R3?

R/. Si

Part 6: 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 1: 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.

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

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:17:31, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
  279 packets output, 89865 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    1 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

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.

```
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, 00:00:57, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
```

```
O      192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
[110/128] via 192.168.12.2, 00:01:08, Serial0/0/0
```

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.

```
R3# show ip ospf interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
        0          1         no           no           Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  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)
```

- 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# show ip ospf interface s0/0/1
```

```
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
        0          64         no           no           Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, 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 192.168.23.2
  Suppress hello for 0 neighbor(s)
```

La suma de los costos de estas dos interfaces es el costo acumulado de la ruta a la red 192.168.3.0/24 en el R3 (1 + 64 = 65), como puede observarse en el resultado del comando **show ip route**.

- 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(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.
```

- f. Emita el comando **auto-cost reference-bandwidth 10000** en los routers R2 y R3.

- 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.

```
R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
                0         10         no         no         Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  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)
```

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).

```
R1# show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 6476
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
                0         6476         no         no         Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
```

```

Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, 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 192.168.23.2
Suppress hello for 0 neighbor(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).

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 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
O       192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
       192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
       [110/12952] via 192.168.12.2, 00:05:17, Serial0/0/

```

Nota: cambiar el ancho de banda de referencia en los routers de 100 a 10 000 cambió los costos acumulados de todas las rutas en un factor de 100, pero el costo de cada enlace y ruta de interfaz ahora se refleja con mayor precisión.

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

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

R1(config-router)# **auto-cost reference-bandwidth 100**

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

¿Por qué querría cambiar el ancho de banda de referencia OSPF predeterminado?

Los equipos actuales, soportan velocidades en enlaces que son mayores a 100Mb/s, para obtener un costo y un cálculo más exacto para estos enlaces más rápidos, un costo de referencia de ancho de banda más alto será necesario

Step 2: 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.

```
R1# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
<Output Omitted>
```

- 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.

Para llegar a la red 3, el costo es de 782, así: Luego, $782=781+1$

- 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?

El nuevo costo acumulado es 1562. En la imagen inferior se muestra el por qué tiene ese costo.

```
R1#show ip route ospf
O   192.168.2.0 [110/782] via 192.168.12.2, 00:27:01, Serial0/0/0
O   192.168.3.0 [110/782] via 192.168.13.2, 00:27:01, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O     192.168.23.0 [110/1562] via 192.168.12.2, 00:01:11, Serial0/0/0
    [110/1562] via 192.168.13.2, 00:01:11, Serial0/0/1
R1#
```

Luego, $1562=781+781$

Step 3: 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.

Porque el costo es menor que por la otra serial, ya que en 1, el costo es de 1563 mientras que por la otra, el costo es de 1565

Reflexión

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

El ID del router controla el router designado (DR) y el router designado alterno (BDR) en el proceso de selección del DR y BDR en una red de multiacceso. Si el ID del router está asociado con una interfaz esquivada, ésta puede ser cambiada. Y si la interfaz se cae, puede ocasionar cambios en el ID del router. Por esta razón se debe usar una dirección loopback que no se desactiva o usar el comando `router-id`

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

Porque la elección del DR/BDR sólo se hace en una red multiacceso, como puede ser Ethernet o Frame Relay. No nos preocupa porque los enlaces seriales de este laboratorio son punto-punto.

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

Cuando se configura una interfaz LAN como pasiva se elimina las notificaciones e información de ruteo innecesaria en esa interface, liberando ancho de banda. El router aún va a notificar esa red a sus vecinos dentro de OSPF.

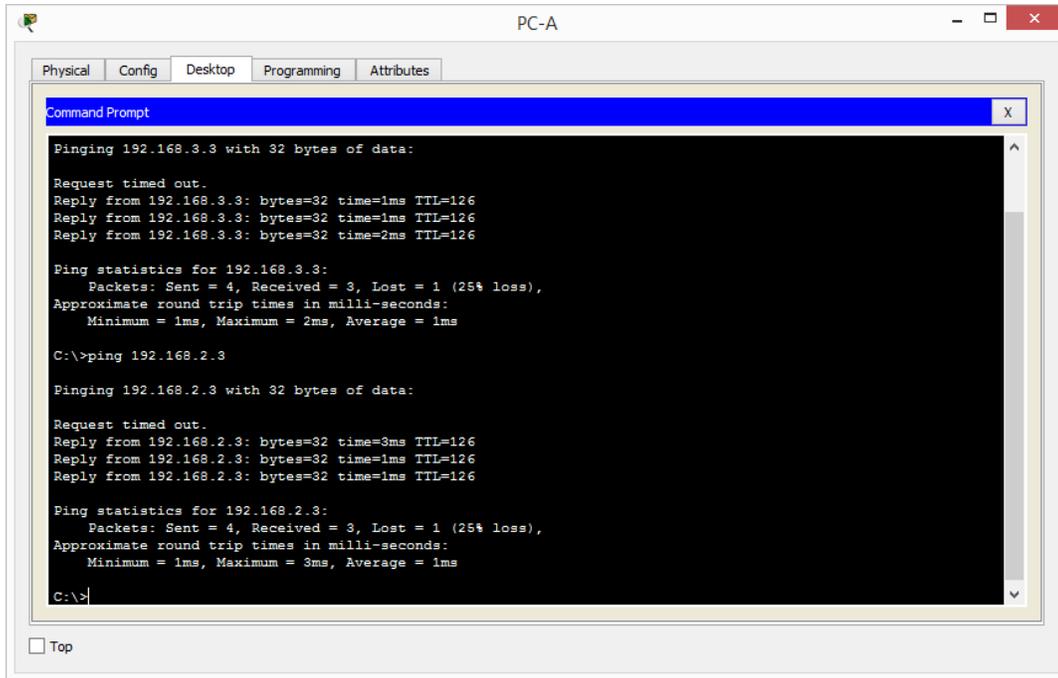


Tabla de resumen de interfaces del router

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.

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

Información básica/situación

El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace para las redes IP. Se definió OSPFv2 para redes IPv4, y OSPFv3 para redes IPv6.

En esta práctica de laboratorio, configurará la topología de la red con routing OSPFv3, asignará ID de router, configurará interfaces pasivas y utilizará varios comandos de CLI para ver y verificar la información de routing OSPFv3.

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). Pueden utilizarse otros routers 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 se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

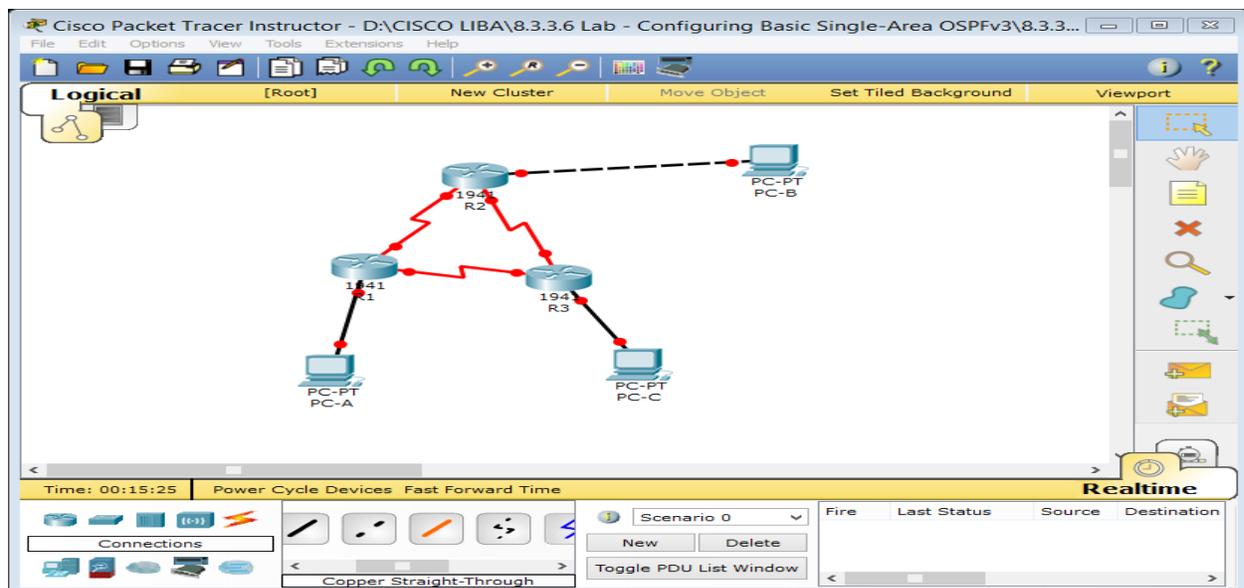
Recursos necesarios

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

Part 7: 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 1: realizar el cableado de red tal como se muestra en la topología.

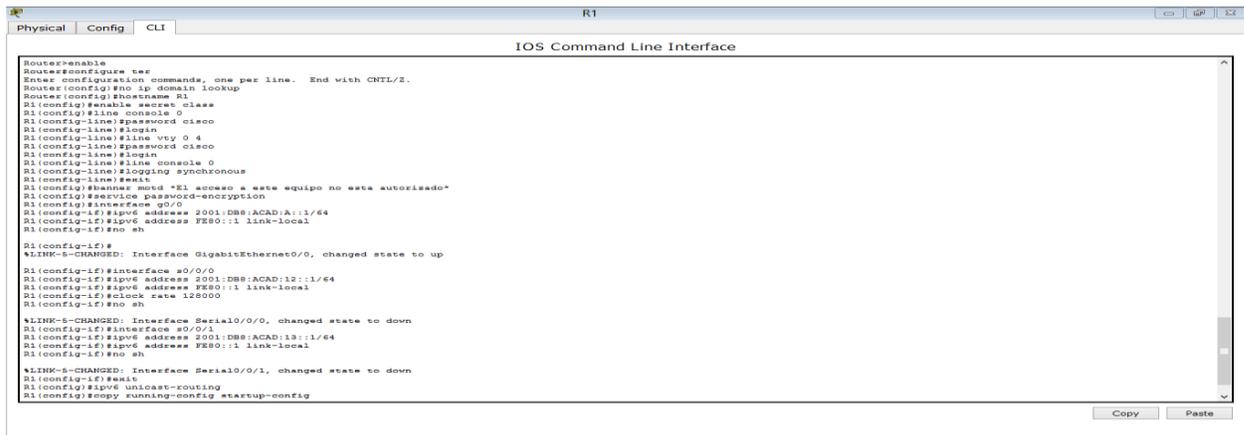


Step 2: inicializar y volver a cargar los routers según sea necesario.

Step 3: configurar los parámetros básicos para cada router.

- Desactive la búsqueda del DNS.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **class** como la contraseña del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de vty.
- Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- Configure **logging synchronous** para la línea de consola.
- 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



```

Router>enable
Router#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#banner motd *El acceso a este equipo no esta autorizado*
R1(config)#service password-encryption
R1(config)#interface g0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no sh
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
R1(config-if)#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 128000
R1(config-if)#no sh
%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 sh
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#exit
R1(config)#service password-encryption
R1(config)#copy running-config startup-config

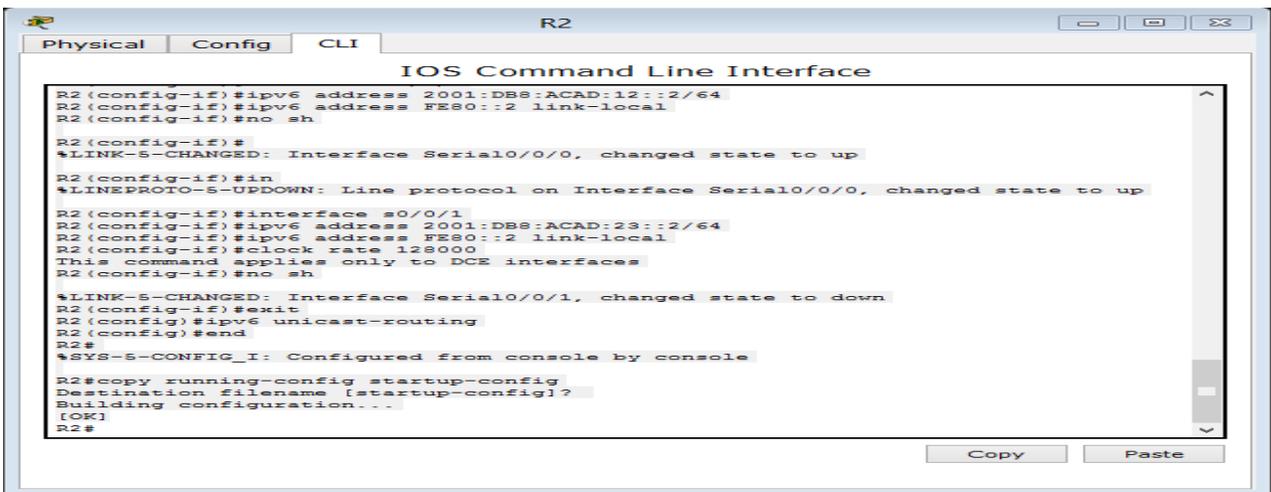
```

```

R1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

[OK]

```



```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#enable secret class
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#logging synchronous
Router(config-line)#login
Router(config-line)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#banner motd *Prohibido el acceso no autorizado a este dispositivo*
Router(config)#hostname R2
R2(config)#service password-encryption
R2(config)#interface g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no sh
R2(config-if)#
%LINK-5-CHANGED: 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
R2(config-if)#ipv6 address FE80::2 link-local

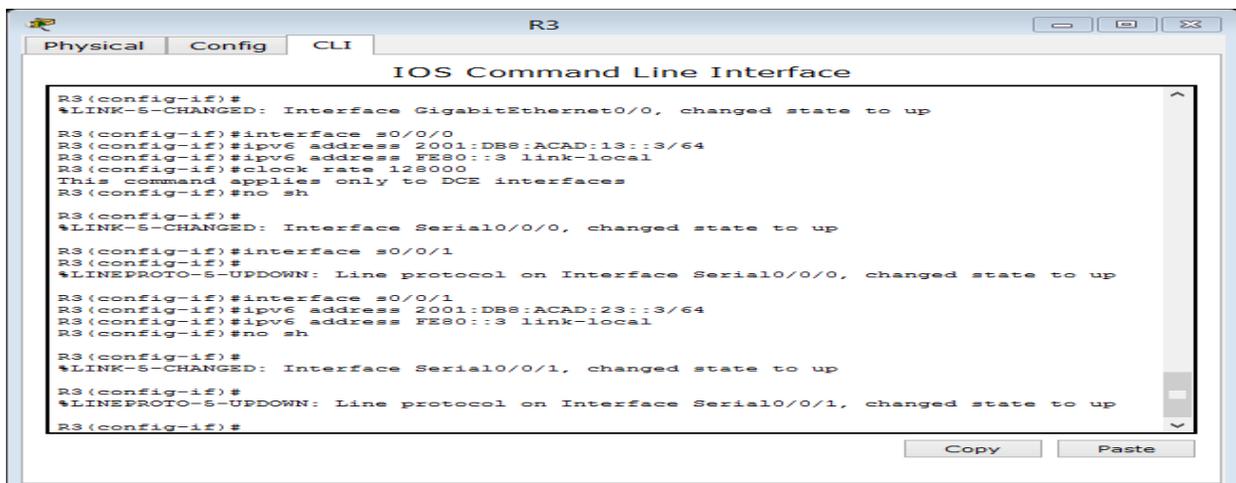
```

```

R2(config-if)#no sh
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#in
%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
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

[OK]

```



```

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line console 0
R3(config-line)#logging synchronous
R3(config-line)#end
R3#

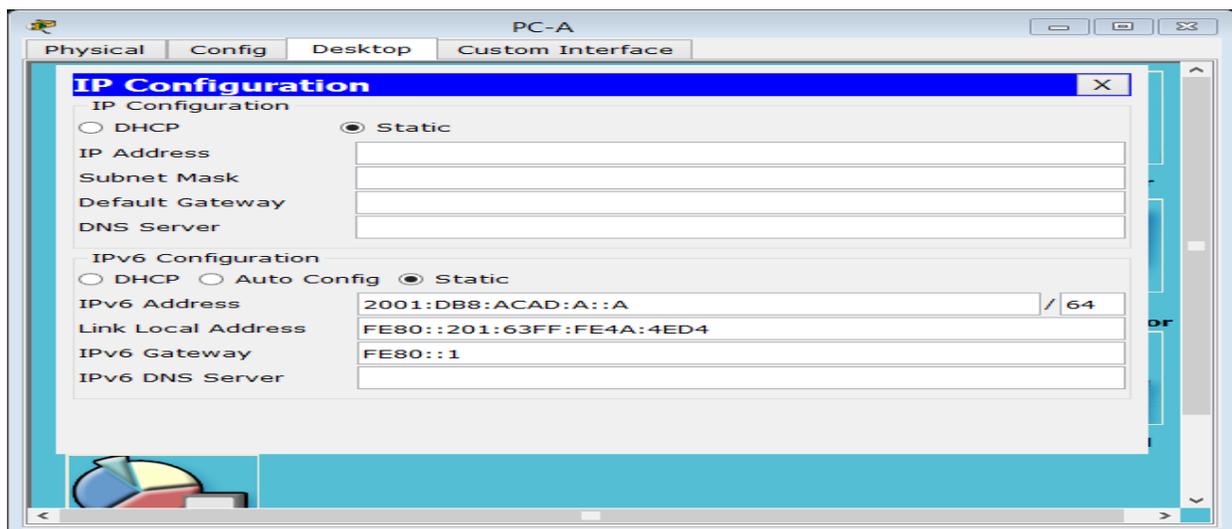
```

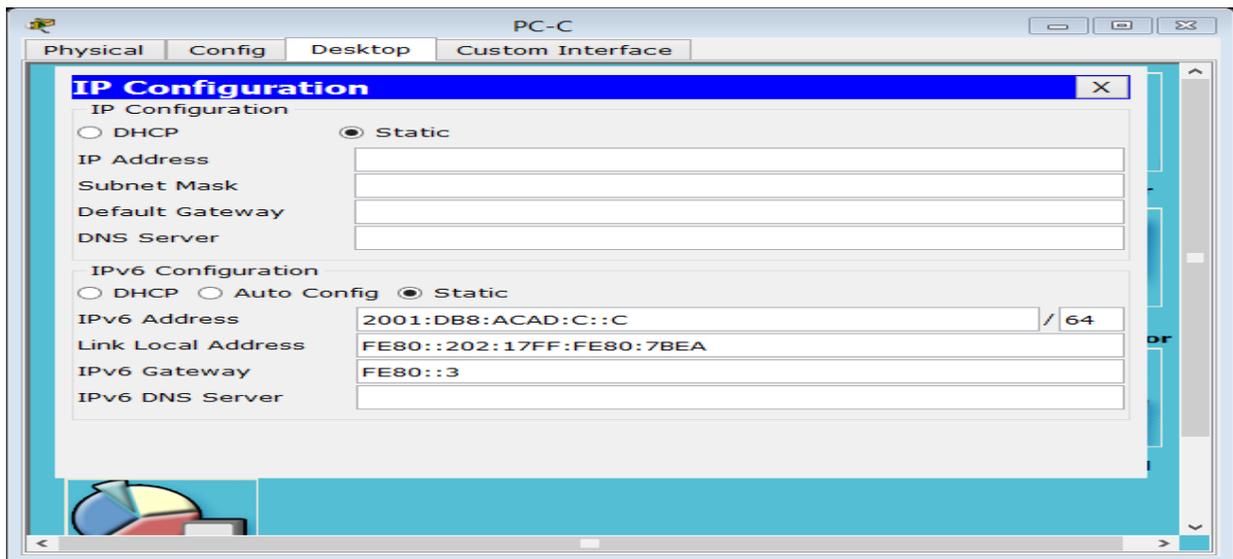
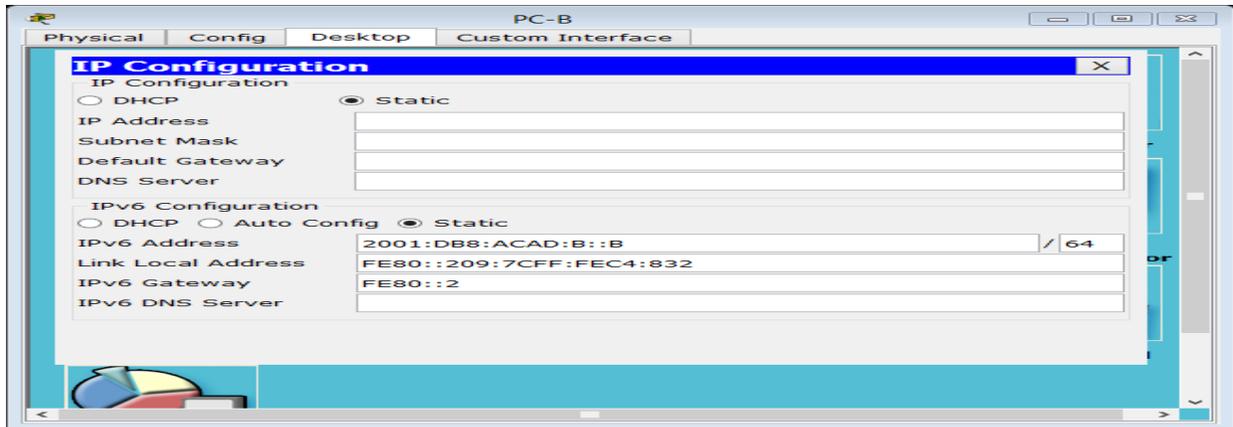
```

%SYS-5-CONFIG_I: Configured from console by console
R3#configure te
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#banner motd *Esta prohibido el acceso no autorizado a este equipo*
R3(config)#service password-encryption
R3(config)#interface g0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no sh
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:13::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#clock rate 128000
This command applies only to DCE interfaces
R3(config-if)#no sh
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R3(config-if)#interface s0/0/1
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no sh
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
R3(config-if)#

```

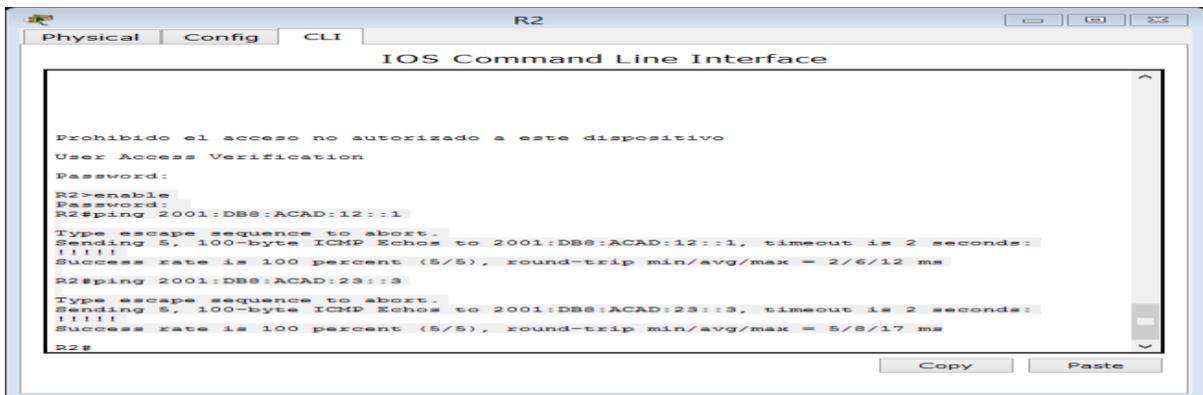
Step 4: configurar los equipos host.





Step 5: 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.



```
R2>enable
Password:
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 = 2/6/12 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 = 5/5/17 ms
R2#
```

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/12 ms

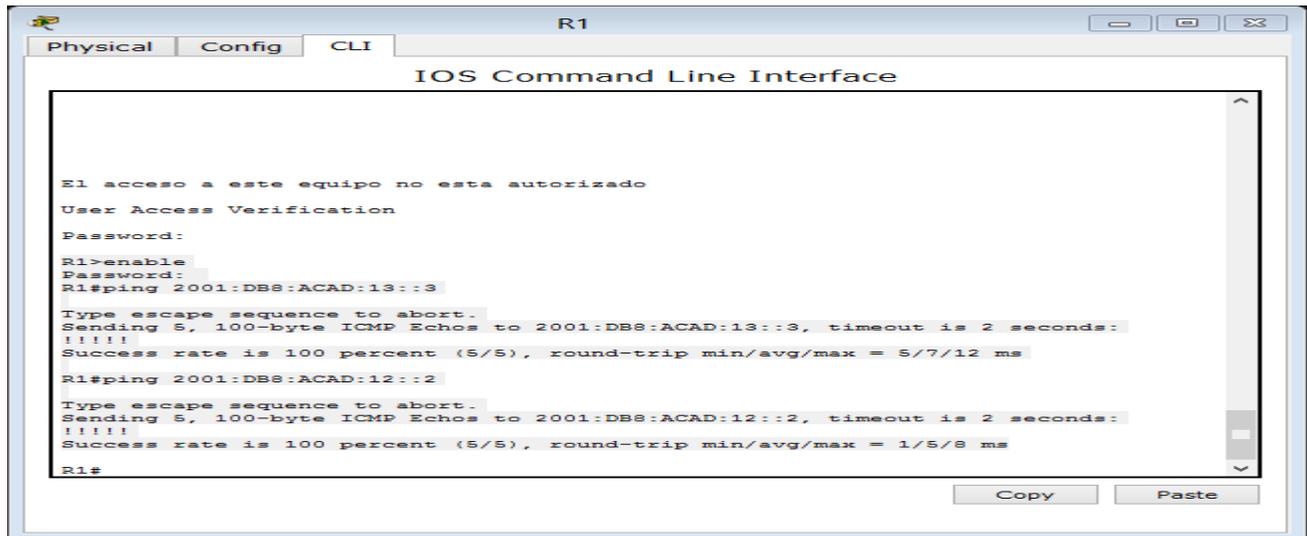
R2#ping 2001:DB8:ACAD:23::3

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 = 5/8/17 ms



```
Physical Config CLI
IOS Command Line Interface

El acceso a este equipo no esta autorizado
User Access Verification
Password:
R1>enable
Password:
R1#ping 2001:DB8:ACAD:13::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/12 ms
R1#ping 2001:DB8:ACAD:12::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/8 ms
R1#
```

R1>enable

Password:

R1#ping 2001:DB8:ACAD:13::3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::3, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/12 ms

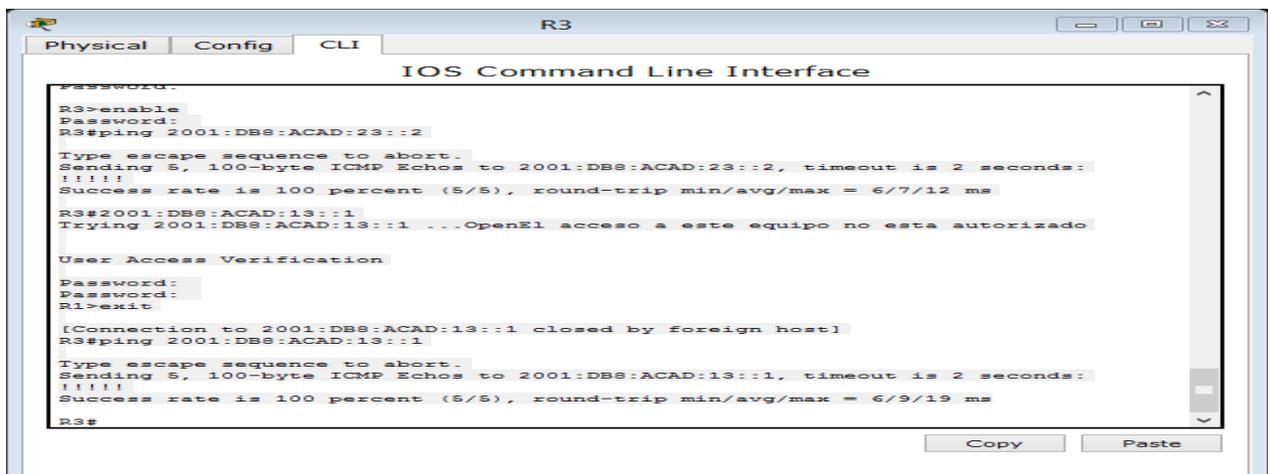
R1#ping 2001:DB8:ACAD:12::2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/8 ms

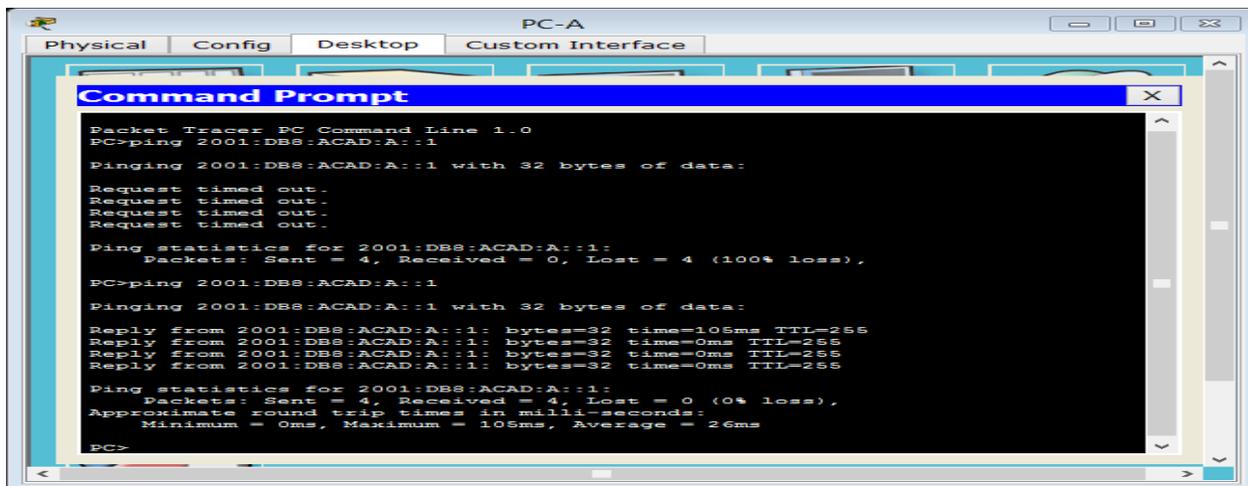


```
Physical Config CLI
IOS Command Line Interface

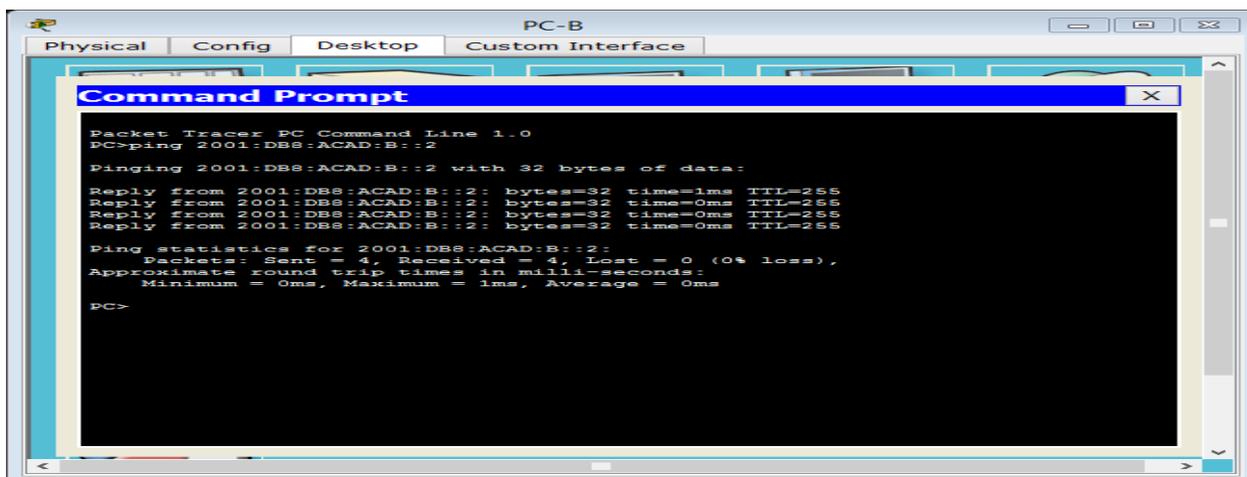
Password:
R3>enable
Password:
R3#ping 2001:DB8:ACAD:23::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/12 ms
R3#2001:DB8:ACAD:13::1
Trying 2001:DB8:ACAD:13::1 ...OpenEl acceso a este equipo no esta autorizado
User Access Verification
Password:
Password:
R1>exit

[Connection to 2001:DB8:ACAD:13::1 closed by foreign host]
R3#ping 2001:DB8:ACAD:13::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/19 ms
R3#
```

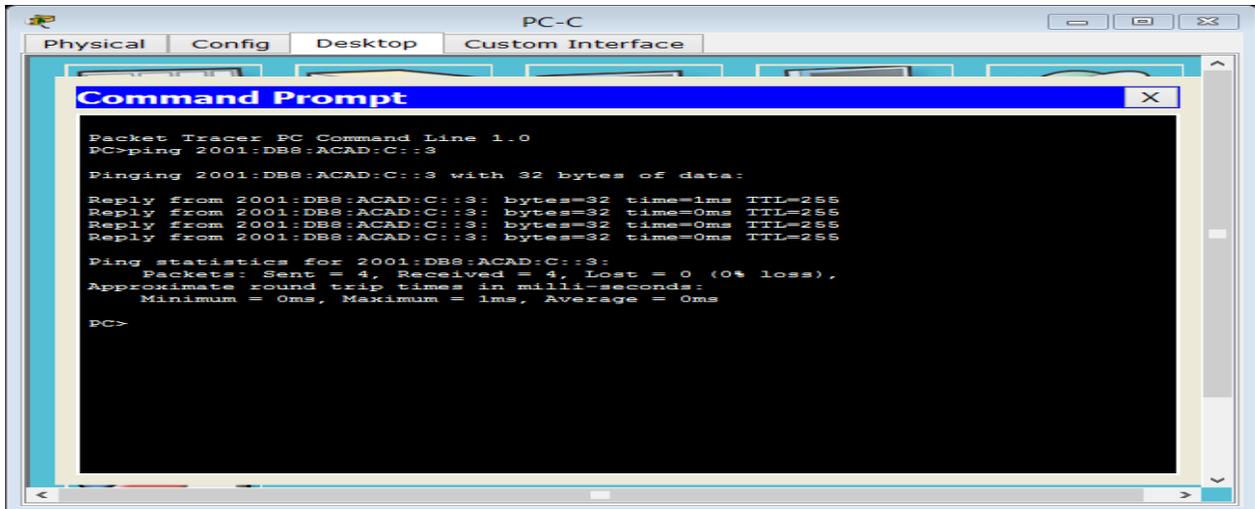
```
R3>enable
Password:
R3#ping 2001:DB8:ACAD:23::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/12 ms
R3#ping 2001:DB8:ACAD:13::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/19 ms
```



```
PC>ping 2001:DB8:ACAD:A::1
```



```
PC>ping 2001:DB8:ACAD:B::2
```



PC>ping 2001:DB8:ACAD:C::3

Part 8: 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 1: 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**.

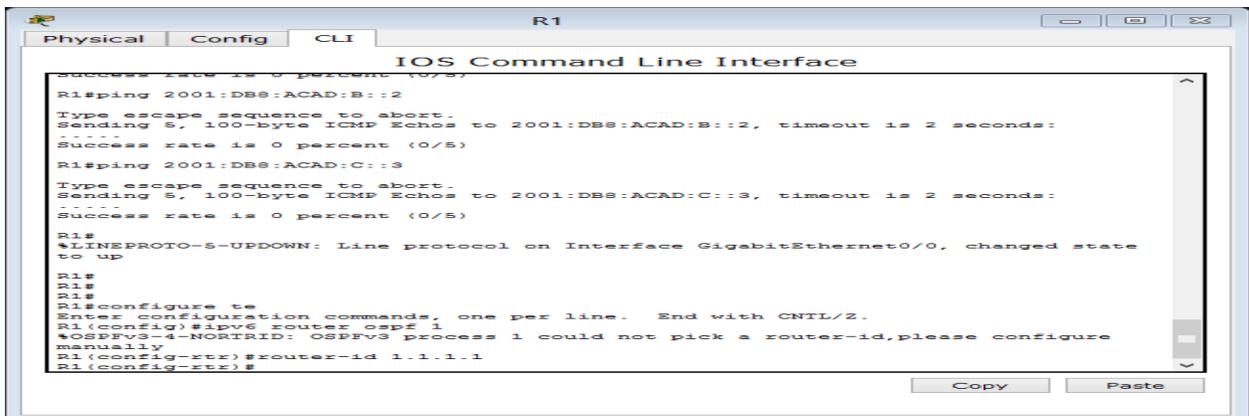
- Emita el comando **ipv6 router ospf** para iniciar un proceso OSPFv3 en el router.

```
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.

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

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



- 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.

```

R2
IOS Command Line Interface

Press RETURN to get started.

Prohibido el acceso no autorizado a este dispositivo
User Access Verification
Password:
R2>enable
Password:
R2#configure ter
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-rttr)#router-id 2.2.2.2
R2(config-rttr)#
  
```

```

R3
IOS Command Line Interface

Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/19 ms
R3#2001:DB8:ACAD:13::1
Trying 2001:DB8:ACAD:13::1 ...OpenEl acceso a este equipo no esta autorizado

User Access Verification
Password:
R1>exit

[Connection to 2001:DB8:ACAD:13::1 closed by foreign host]
R3#ping 2001:DB8:ACAD:13::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/19 ms

R3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 1
* IPv6 routing not enabled
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 1
*OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R3(config-rttr)#router-id 3.3.3.3
R3(config-rttr)#
  
```

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>

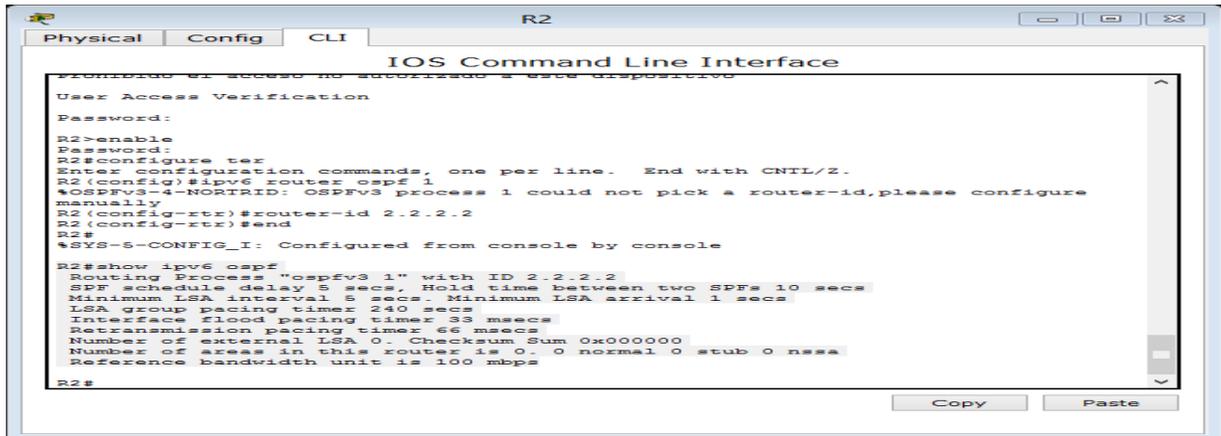
```

R1
IOS Command Line Interface

El acceso a este equipo no esta autorizado
User Access Verification
Password:
Password:
R1>enable
Password:
R1#show ipv6 ospf
Routing Process "ospfv3 1" with ID 1.1.1.1
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 msec
Retransmission pacing timer 66 msec
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
R1#
  
```

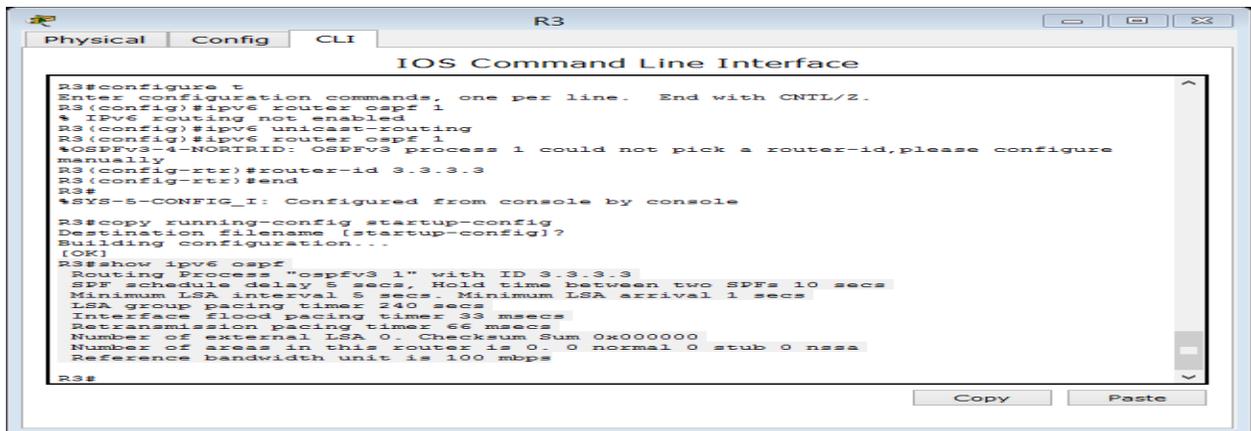
R1#show ipv6 ospf
 Routing Process "ospfv3 1" with ID 1.1.1.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
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
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
R2>enable
Password:
R2#configure ter
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-rtx)#router-id 2.2.2.2
R2(config-rtx)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
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 msec
Retransmission pacing timer 66 msec
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#
```

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 msec
Retransmission pacing timer 66 msec
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



```
R3
Physical Config CLI
IOS Command Line Interface
R3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 1
% IPv6 routing not enabled
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R3(config-rtx)#router-id 3.3.3.3
R3(config-rtx)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
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 msec
Retransmission pacing timer 66 msec
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
R3#
```

R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
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 msec
Retransmission pacing timer 66 msec

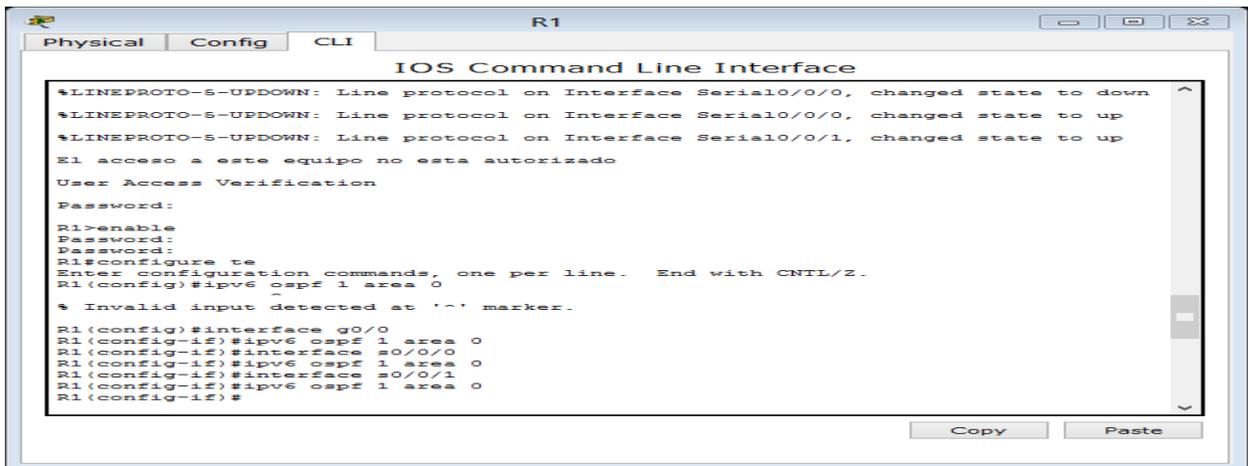
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps

Step 2: 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.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# interface s0/0/1
R1(config-if)# ipv6 ospf 1 area 0
```



```
R1(config)#interface g0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 ospf 1 area 0
```

R1(config-if)#**Nota:** la ID del proceso debe coincidir con la ID del proceso que usó en el paso 1a.

- b. Asigne las interfaces en el R2 y el R3 al área 0 de OSPFv3. Al agregar las interfaces al área 0, debería ver mensajes de adyacencia de vecino.

```
R2
Physical Config CLI
IOS Command Line Interface
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
R2 (config)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2 (config)#interface g0/0
R2 (config-if)#ipv6 ospf 1 area 0
R2 (config-if)#interface s0/0/0
R2 (config-if)#ipv6 ospf 1 area 0
R2 (config-if)#interface s0/0/1
R2 (config-if)#ipv6 ospf 1 area 0
22:02:48: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R2 (config-if)#ipv6 ospf 1 area 0
R2 (config-if)#
```

```
R2(config)#interface g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
22:02:48: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

```
R3
Physical Config CLI
IOS Command Line Interface
Esta prohibido el acceso no autorizado a este equipo
User Access Verification
Password:
R3>enable
Password:
R3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R3 (config)#ipv6 ospf 1 area 0
-
* Invalid input detected at '' marker.
R3 (config)#interface g0/0
R3 (config-if)#ipv6 ospf 1 area 0
R3 (config-if)#interface s0/0/0
R3 (config-if)#ipv6 ospf 1 area 0
R3 (config-if)#
23:04:53: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R3 (config-if)#interface s0/0/1
R3 (config-if)#ipv6 ospf 1 area 0
R3 (config-if)#
23:05:11: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
R3 (config-if)#
```

```
R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
23:04:53: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
23:05:11: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
R1#
```

```
*Mar 19 22:14:43.251: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
```

```
R1#
```

```
*Mar 19 22:14:46.763: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
```

```
22:42:15: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
```

```
23:05:04: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
```

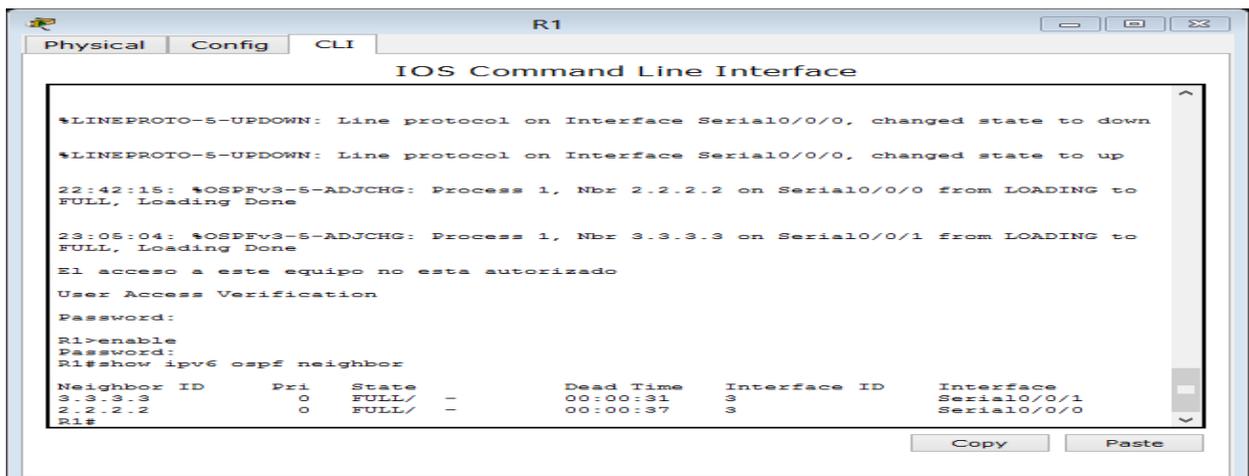
Step 3: verificar vecinos de OSPFv3.

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.

```
R1# show ipv6 ospf neighbor
```

```
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:39	6	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:36	6	Serial0/0/0



```
R1
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
22:42:15: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
23:05:04: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
El acceso a este equipo no está autorizado
User Access Verification
Password:
R1>enable
Password:
R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
3.3.3.3          0    FULL/ -         00:00:31   3            Serial0/0/1
2.2.2.2          0    FULL/ -         00:00:37   3            Serial0/0/0
R1#
```

```
R1#show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:31	3	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:37	3	Serial0/0/0

```

R2
Physical Config CLI
IOS Command Line Interface

22:25:55: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to
FULL, Loading Done
Prohibido el acceso no autorizado a este dispositivo
User Access Verification
Password:
R2>enable
Password:
R2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#end
R2#
*SYS-5-CONFIG_I: Configured from console by console
R2#show ipv6 ospf neighbor
* Invalid input detected at '^' marker.
R2#show ipv6 ospf neighbor
Neighbor ID      Pri  State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:00:35   3             Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:32   4             Serial0/0/1
R2#

```

```

R2#show ipv6 ospf neighbor
Neighbor ID Pri State Dead Time Interface ID Interface
1.1.1.1 0 FULL/ - 00:00:35 3 Serial0/0/0
3.3.3.3 0 FULL/ - 00:00:32 4 Serial0/0/1

```

```

R3
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

Esta prohibido el acceso no autorizado a este equipo
User Access Verification
Password:
R3>enable
Password:
R3#show ipv6 ospf neighbor
Neighbor ID      Pri  State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:00:31   4             Serial0/0/0
2.2.2.2          0    FULL/ -         00:00:39   4             Serial0/0/1
R3#

```

```

R3#show ipv6 ospf neighbor
Neighbor ID Pri State Dead Time Interface ID Interface
1.1.1.1 0 FULL/ - 00:00:31 4 Serial0/0/0
2.2.2.2 0 FULL/ - 00:00:39 4 Serial0/0/1

```

Step 4: 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.

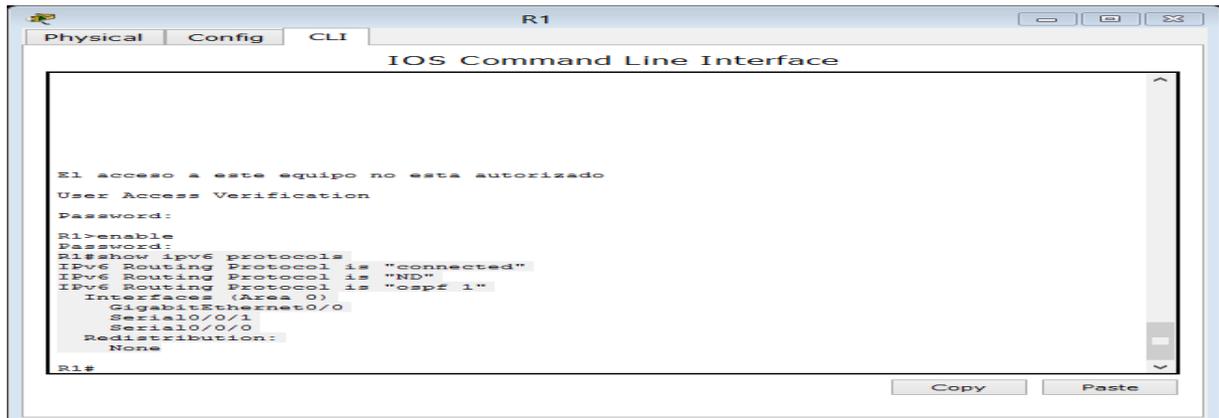
```

R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
Router ID 1.1.1.1
Number of areas: 1 normal, 0 stub, 0 nssa
Interfaces (Area 0):
Serial0/0/1
Serial0/0/0
GigabitEthernet0/0

```

Redistribution:

None



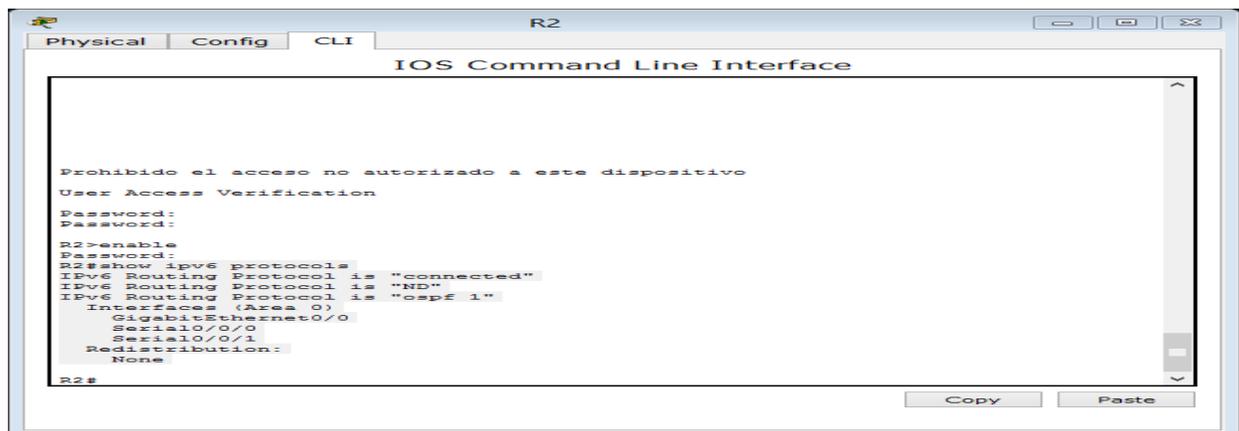
```
Physical Config CLI
IOS Command Line Interface

El acceso a este equipo no esta autorizado
User Access Verification
Password:
R1>enable
Password:
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/1
    Serial0/0/0
  Redistribution:
    None
R1#
```

R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
Interfaces (Area 0)
GigabitEthernet0/0
Serial0/0/1
Serial0/0/0

Redistribution:

None



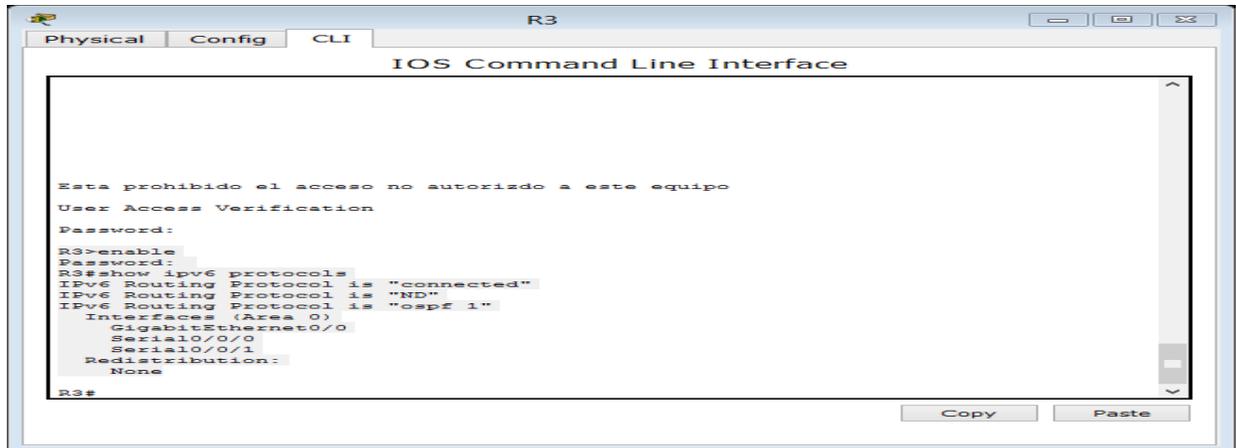
```
Physical Config CLI
IOS Command Line Interface

Prohibido el acceso no autorizado a este dispositivo
User Access Verification
Password:
R2>enable
Password:
R2#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
R2#
```

R2#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
Interfaces (Area 0)
GigabitEthernet0/0
Serial0/0/0
Serial0/0/1

Redistribution:

None



```

R3>enable
Password:
R3#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
Interfaces (Area 0)
GigabitEthernet0/0
Serial0/0/0
Serial0/0/1
Redistribution:
None

```

Step 5: verificar las interfaces OSPFv3.

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

```
R1# show ipv6 ospf interface
```

```

Serial0/0/1 is up, line protocol is up
Link Local Address FE80::1, Interface ID 7
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Graceful restart helper support enabled
Index 1/3/3, flood queue length 0
Next 0x0(0)/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 3.3.3.3
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 6
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT

```

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:00

Graceful restart helper support enabled

Index 1/2/2, flood queue length 0

Next 0x0(0)/0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 2

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 2.2.2.2

Suppress hello for 0 neighbor(s)

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3

Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 1.1.1.1, local address FE80::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

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

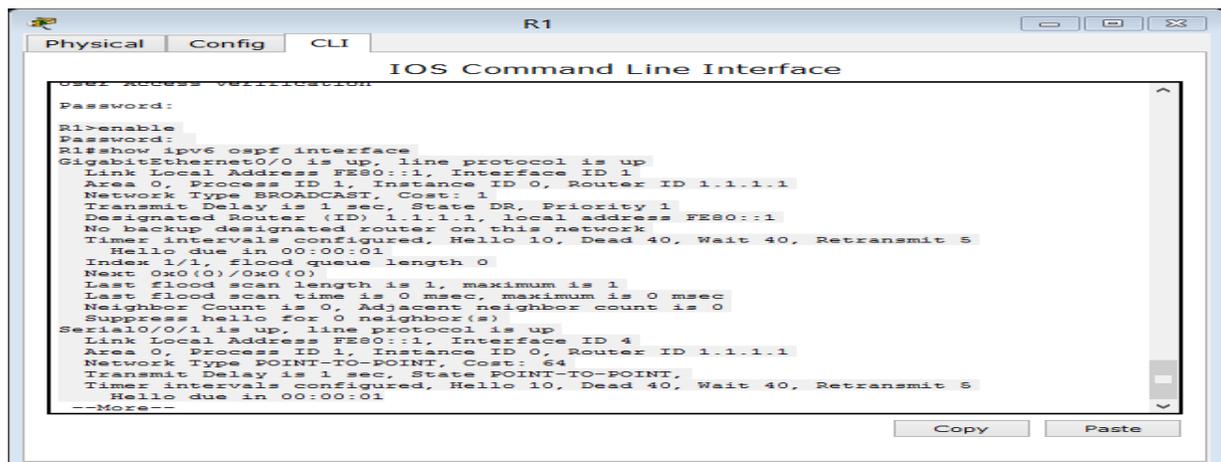
Next 0x0(0)/0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

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)



```
R1
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
R1>enable
Password:
R1#show ipv6 ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  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)
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 4
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
--More--
Copy Paste
```

R1>enable

Password:

R1#show ipv6 ospf interface

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 1

Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 1.1.1.1, local address FE80::1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
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)

Serial0/0/1 is up, line protocol is up

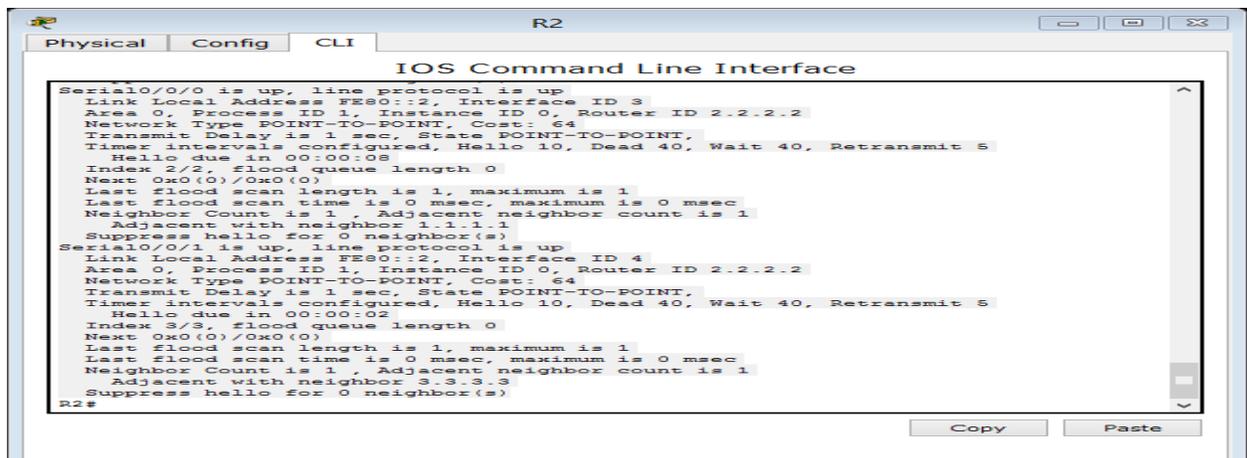
Link Local Address FE80::1, Interface ID 4
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Index 2/2, flood queue length 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 3.3.3.3

Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Index 3/3, 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 2.2.2.2

Suppress hello for 0 neighbor(s)



R2#show ipv6 ospf interface

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::2, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 2.2.2.2, local address FE80::2
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
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)
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
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 1.1.1.1
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
Link Local Address FE80::2, Interface ID 4
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 3/3, 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 3.3.3.3
Suppress hello for 0 neighbor(s)

```
User Access Verification
Password:
R3>enable
Password:
R3#show ipv6 ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, local address FE80::3
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:02
  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)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:07
```

R3#show ipv6 ospf interface

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::3, Interface ID 1

Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 3.3.3.3, local address FE80::3

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:02

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)

Serial0/0/0 is up, line protocol is up

Link Local Address FE80::3, Interface ID 3

Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3

Network Type POINT-TO-POINT, Cost: 64

Transmit Delay is 1 sec, State POINT-TO-POINT,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:07

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 1.1.1.1

Suppress hello for 0 neighbor(s)

Serial0/0/1 is up, line protocol is up

Link Local Address FE80::3, Interface ID 4

Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3

Network Type POINT-TO-POINT, Cost: 64

Transmit Delay is 1 sec, State POINT-TO-POINT,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

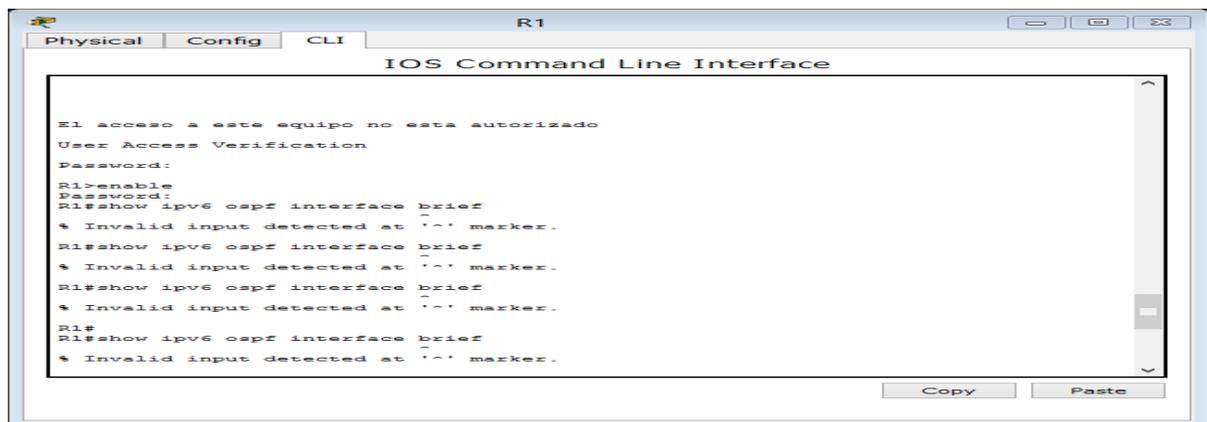
Hello due in 00:00:08

Index 3/3, 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 2.2.2.2
 Suppress hello for 0 neighbor(s)

- 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	



Packet tracer no soporta este comando.

Step 6: verificar la tabla de routing IPv6.

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

R2# **show ipv6 route**

IPv6 Routing Table - default - 10 entries
 Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
 B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
 IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
 ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
 O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

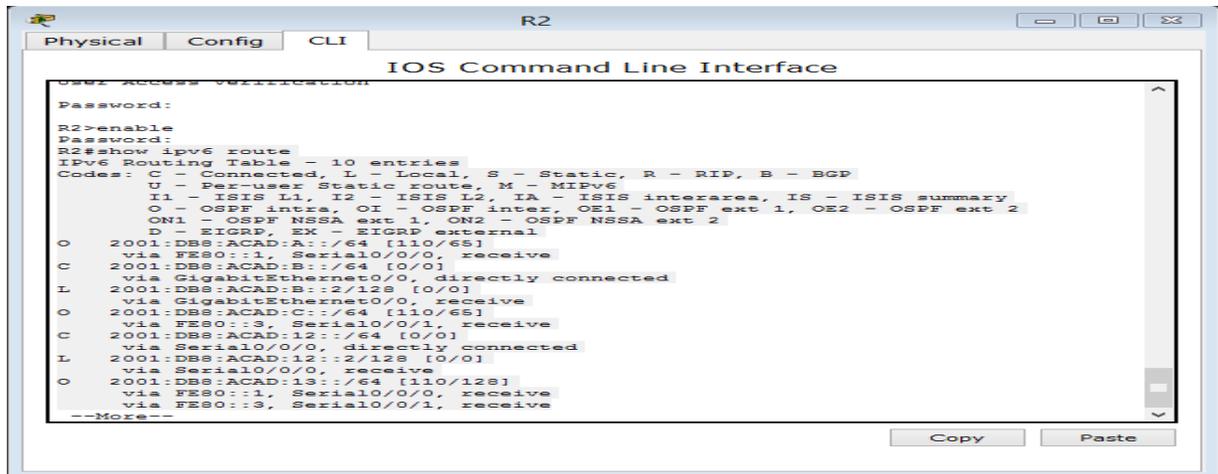
O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0

C 2001:DB8:ACAD:B::/64 [0/0]
 via GigabitEthernet0/0, directly connected

L 2001:DB8:ACAD:B::2/128 [0/0]
 via GigabitEthernet0/0, receive

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::2/128 [0/0]
 via Serial0/0/0, receive
O 2001:DB8:ACAD:13::/64 [110/128]
 via FE80::3, Serial0/0/1
 via FE80::1, Serial0/0/0
 C 2001:DB8:ACAD:23::/64 [0/0]
 via Serial0/0/1, directly connected
 L 2001:DB8:ACAD:23::2/128 [0/0]
 via Serial0/0/1, receive
 L FF00::/8 [0/0]
 via Null0, receive



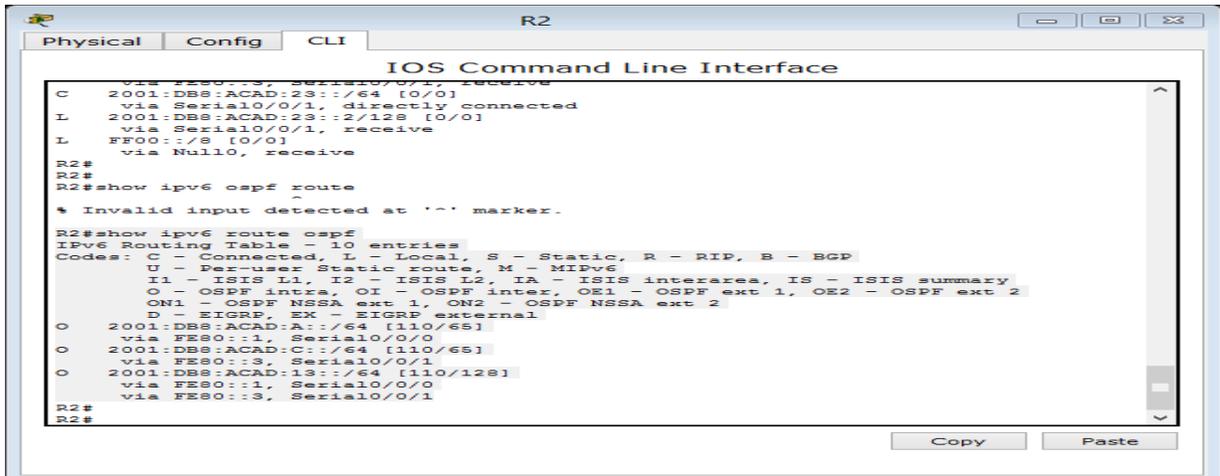
R2#show ipv6 route
 IPv6 Routing Table - 10 entries
 Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external

O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0, receive
 C 2001:DB8:ACAD:B::/64 [0/0]
 via GigabitEthernet0/0, directly connected
 L 2001:DB8:ACAD:B::2/128 [0/0]
 via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:C::/64 [110/65]
 via FE80::3, Serial0/0/1, receive
 C 2001:DB8:ACAD:12::/64 [0/0]
 via Serial0/0/0, directly connected
 L 2001:DB8:ACAD:12::2/128 [0/0]
 via Serial0/0/0, receive
O 2001:DB8:ACAD:13::/64 [110/128]

via FE80::1, Serial0/0/0, receive
via FE80::3, Serial0/0/1, receive

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



```
Physical Config CLI R2
IOS Command Line Interface
C 2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::2/128 [0/0]
  via Serial0/0/1, receive
L FF00::/8 [0/0]
  via Null0, receive
R2#
R2#
R2#show ipv6 ospf route
% Invalid input detected at '^' marker.
R2#show ipv6 route ospf
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
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:13::/64 [110/128]
  via FE80::1, Serial0/0/0
R2#
R2#
```

R2#show ipv6 route ospf

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

O 2001:DB8:ACAD:A::/64 [110/65]

via FE80::1, Serial0/0/0

O 2001:DB8:ACAD:C::/64 [110/65]

via FE80::3, Serial0/0/1

O 2001:DB8:ACAD:13::/64 [110/128]

via FE80::1, Serial0/0/0

via FE80::3, Serial0/0/1

Step 7: 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.

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>ping 2001:DB8:ACAD:C::C
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=8ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 2ms
PC>
```

```
PC>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Ping statistics for 2001:DB8:ACAD:B::B:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
PC>ping 2001:DB8:ACAD:C::C
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=8ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Ping statistics for 2001:DB8:ACAD:C::C:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 8ms, Average = 2ms
```

```
PC-B
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 2001:DB8:ACAD:A::A
Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=5ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 4ms
PC>ping 2001:DB8:ACAD:C::C
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=9ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 9ms, Average = 4ms
PC>
```

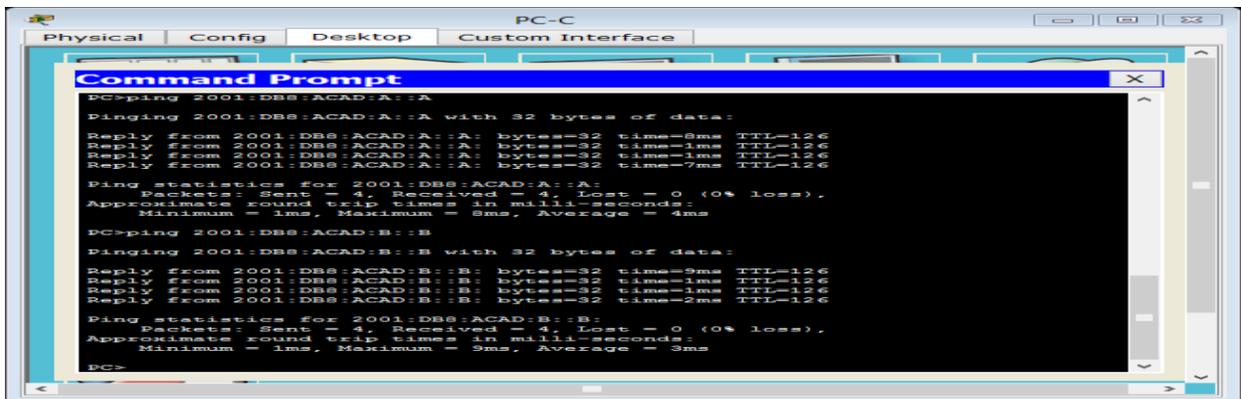
```
PC>ping 2001:DB8:ACAD:A::A
Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=5ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
```

Ping statistics for 2001:DB8:ACAD:A::A:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 11ms, Average = 4ms

PC>ping 2001:DB8:ACAD:C::C

Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=9ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=8ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Ping statistics for 2001:DB8:ACAD:C::C:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 9ms, Average = 4ms



```
PC-C
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 2001:DB8:ACAD:A::A
Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=9ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=7ms TTL=126
Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 9ms, Average = 4ms
PC>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=9ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 9ms, Average = 3ms
PC>
```

PC>ping 2001:DB8:ACAD:A::A

Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=8ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=7ms TTL=126
Ping statistics for 2001:DB8:ACAD:A::A:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 8ms, Average = 4ms

PC>ping 2001:DB8:ACAD:B::B

Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=9ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Ping statistics for 2001:DB8:ACAD:B::B:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 9ms, Average = 3ms

Part 9: configurar las interfaces pasivas de OSPFv3

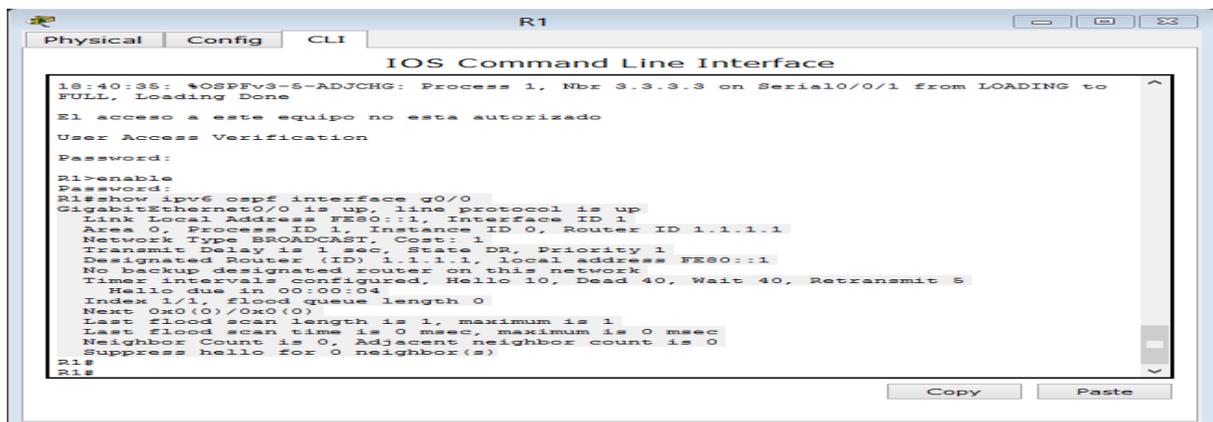
El comando **passive-interface** evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. En la parte 3, utilizará el comando **passive-interface** para configurar una única interfaz como pasiva. También configurará OSPFv3 para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

Step 1: configurar una interfaz pasiva.

- 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.

R1# **show ipv6 ospf interface g0/0**

```
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
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)
```



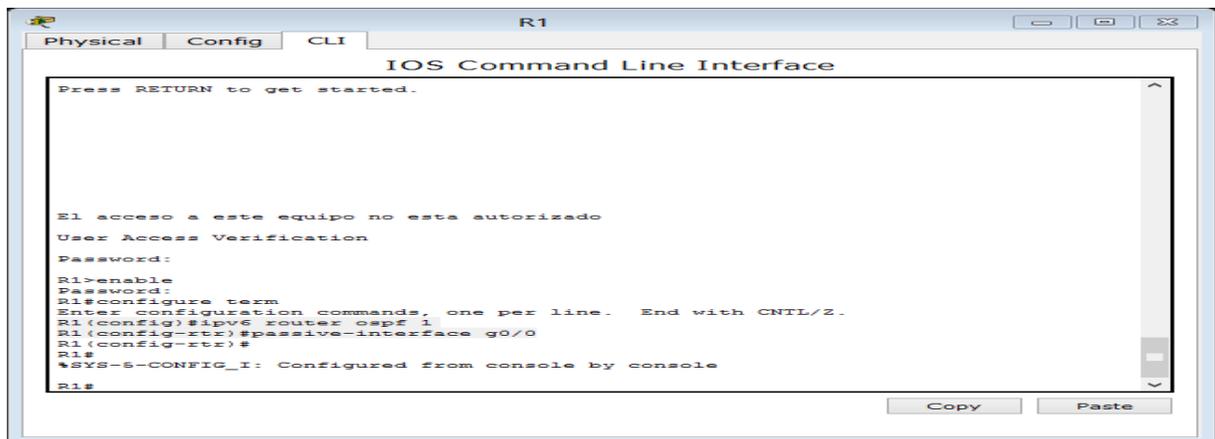
```
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
```

No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
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)

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

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

```
R1(config-rtr)# passive-interface g0/0
```



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

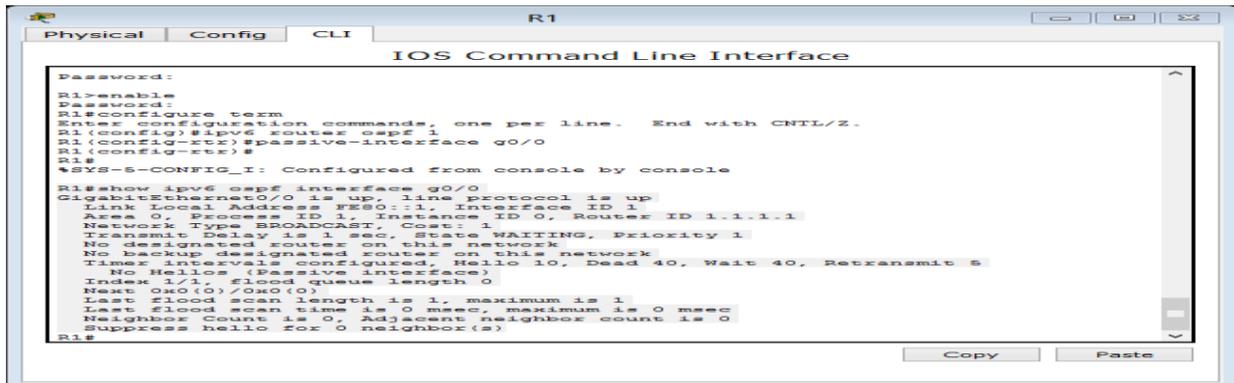
```
R1(config-rtr)#passive-interface g0/0
```

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

```
R1# show ipv6 ospf interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up  
Link Local Address FE80::1, Interface ID 3  
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1  
Network Type BROADCAST, Cost: 1  
Transmit Delay is 1 sec, State WAITING, Priority 1  
No designated router on this network  
No backup designated router on this network  
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
No Hellos (Passive interface)  
Wait time before Designated router selection 00:00:34  
Graceful restart helper support enabled  
Index 1/1/1, flood queue length 0  
Next 0x0(0)/0x0(0)/0x0(0)  
Last flood scan length is 0, maximum is 0  
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)



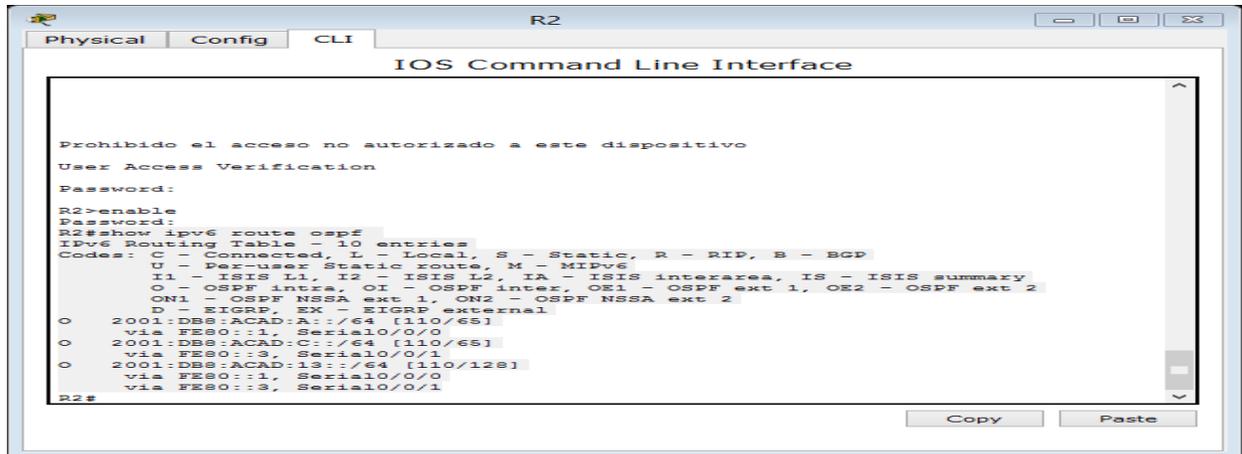
```
R1
Physical Config CLI
IOS Command Line Interface
Password:
R1>enable
R1#configure term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtt)#passive-interface g0/0
R1(config-rtt)#
R1#
*SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 1/1, flood queue length 0
Next OMO(0)/OMO(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)
R1#
```

```
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
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)
```

- 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.

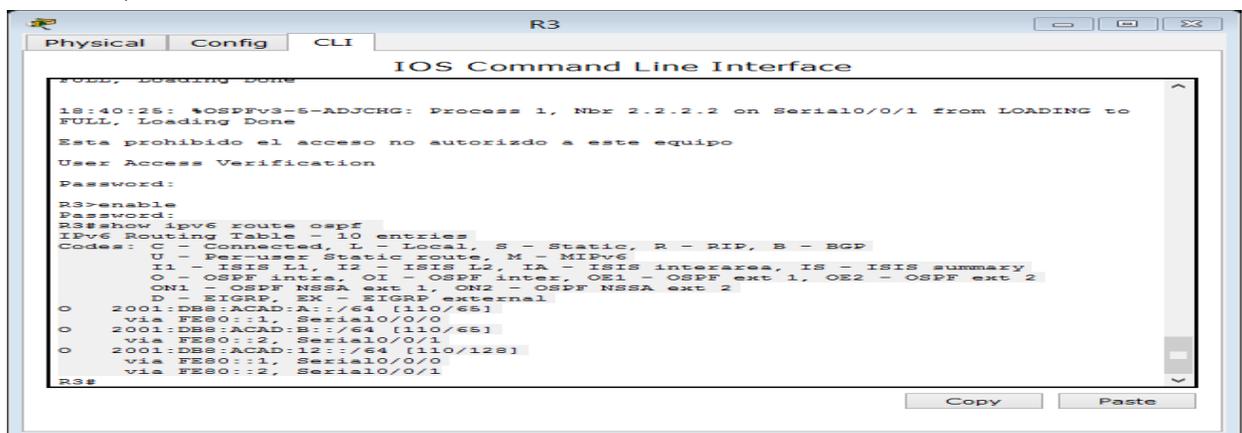
R2# **show ipv6 route ospf**

```
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:13::/64 [110/128]
  via FE80::3, Serial0/0/1
  via FE80::1, Serial0/0/0
```



R2#show ipv6 route ospf
 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
 O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0
 O 2001:DB8:ACAD:C::/64 [110/65]
 via FE80::3, Serial0/0/1
 O 2001:DB8:ACAD:13::/64 [110/128]
 via FE80::1, Serial0/0/0
 via FE80::3, Serial0/0/1



R3#show ipv6 route ospf
 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

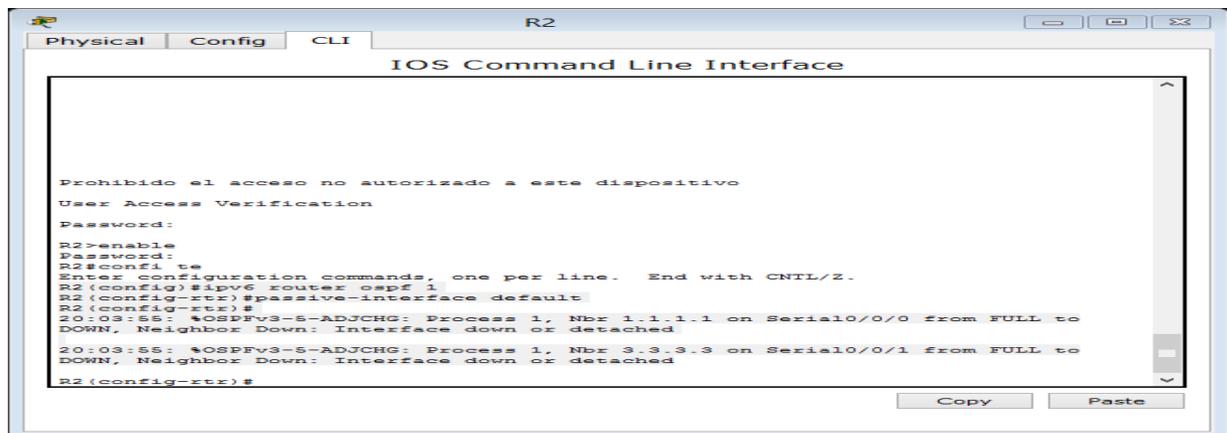
```
O 2001:DB8:ACAD:A::/64 [110/65]
via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:B::/64 [110/65]
via FE80::2, Serial0/0/1
O 2001:DB8:ACAD:12::/64 [110/128]
via FE80::1, Serial0/0/0
via FE80::2, Serial0/0/1
```

Step 2: 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.

```
R2(config)# ipv6 router ospf 1
```

```
R2(config-rtr)# passive-interface default
```



```
R2(config)#ipv6 router ospf 1
```

```
R2(config-rtr)#passive-interface default
```

```
R2(config-rtr)#
```

```
20:03:55: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
20:03:55: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

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

```
R1# show ipv6 ospf neighbor
```

```
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:37	6	Serial0/0/1

```

R1
Physical Config CLI
IOS Command Line Interface

20:44:01: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Dead timer expired
20:44:01: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached
El acceso a este equipo no esta autorizado
User Access Verification
Password:
R1>enable
Password:
R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time      Interface ID   Interface
3.3.3.3         0    FULL/-         00:00:31      3             Serial0/0/1
R1#
Copy Paste

```

R1#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface

3.3.3.3 0 FULL/ - 00:00:31 3 Serial0/0/1

- 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.

R2# **show ipv6 ospf interface s0/0/0**

```

Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2, Interface ID 6
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Graceful restart helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 3
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)

```

R2
Physical Config CLI
IOS Command Line Interface

Prohibido el acceso no autorizado a este dispositivo
User Access Verification

Password:
Password:

R2>enable
Password:
R2#comando show ipv6 ospf interface s0/0/0
* Invalid input detected at '^' marker.

R2#show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
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
Suppress hello for 0 neighbor(s)
R2#
Copy Paste

```

```

R2#show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
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
Suppress hello for 0 neighbor(s)

```

- 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**.

```

R1
Physical Config CLI
IOS Command Line Interface

Password:
R1>enable
Translating "enable"
* Unknown command or computer name, or unable to find computer address

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 [110/129]
  via FE80::3, Serial0/0/1, receive
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1, receive
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]
--More--
Copy Paste

```

```

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 [110/129]

via FE80::3, Serial0/0/1, receive

O 2001:DB8:ACAD:C::/64 [110/65]

via FE80::3, Serial0/0/1, receive

C 2001:DB8:ACAD:12::/64 [0/0]

via Serial0/0/0, directly connected

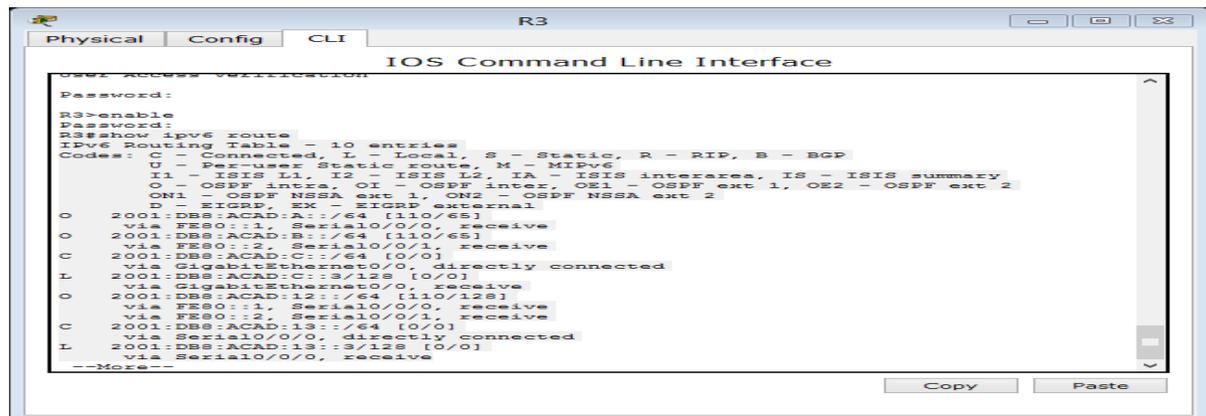
L 2001:DB8:ACAD:12::1/128 [0/0]

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]



```
Physical  Config  CLI
IOS Command Line Interface
Password:
R3>enable
Password:
R3#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
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0, receive
O 2001:DB8:ACAD:B::/64 [110/65]
  via FE80::2, Serial0/0/1, receive
C 2001:DB8:ACAD:C::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:C::3/128 [0/0]
  via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:12::/64 [110/128]
  via FE80::1, Serial0/0/0, receive
  via FE80::2, Serial0/0/1, receive
C 2001:DB8:ACAD:13::/64 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:ACAD:13::3/128 [0/0]
  via Serial0/0/0, receive
--More--
Copy Paste
```

R3#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

O 2001:DB8:ACAD:A::/64 [110/65]

via FE80::1, Serial0/0/0, receive

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

via FE80::2, Serial0/0/1, receive

C 2001:DB8:ACAD:C::/64 [0/0]

via GigabitEthernet0/0, directly connected

L 2001:DB8:ACAD:C::3/128 [0/0]

via GigabitEthernet0/0, receive

O 2001:DB8:ACAD:12::/64 [110/128]

via FE80::1, Serial0/0/0, receive

via FE80::2, Serial0/0/1, receive

C 2001:DB8:ACAD:13::/64 [0/0]

via Serial0/0/0, directly connected

L 2001:DB8:ACAD:13::3/128 [0/0]

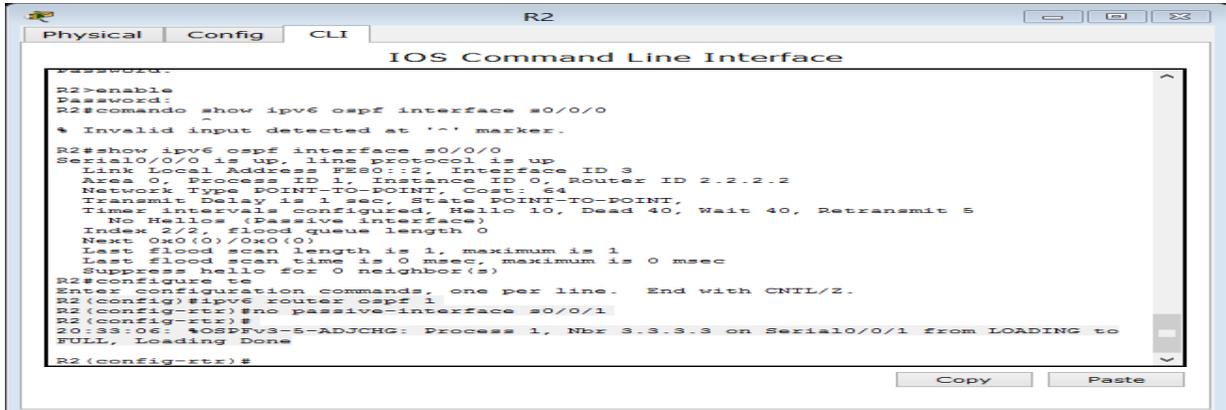
via Serial0/0/0, receive

- 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.

R2(config)# ipv6 router ospf 1

R2(config-rtr)# no passive-interface s0/0/1

*Apr 8 19:21:57.939: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done



```
IOS Command Line Interface
R2>enable
Password:
R2#command show ipv6 ospf interface s0/0/0
% Invalid input detected at '^' marker.
R2#show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
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
Suppress hello for 0 neighbor(s)
R2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
20:33:06: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to
FULL, Loading Done
R2(config-rtr)#
```

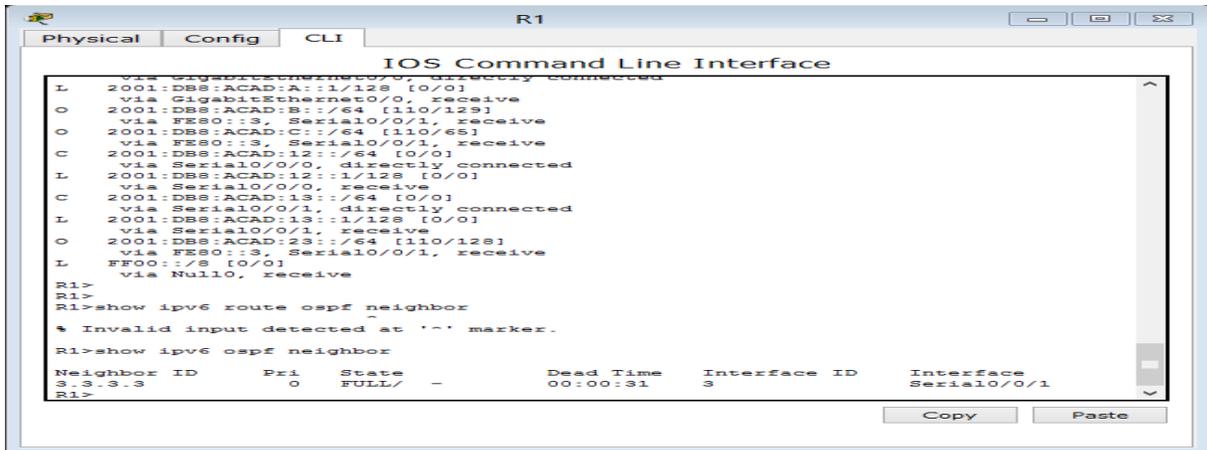
R2(config)#ipv6 router ospf 1

R2(config-rtr)#no passive-interface s0/0/1

R2(config-rtr)#

20:33:06: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done

- 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.



```
IOS Command Line Interface
R1>show ipv6 route ospf neighbor
% Invalid input detected at '^' marker.
R1>show ipv6 ospf neighbor
Neighbor ID Pri State Dead Time Interface ID Interface
3.3.3.3 0 FULL/ - 00:00:31 3 Serial0/0/1
R1>
```

R1>show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface

3.3.3.3 0 FULL/ - 00:00:31 3 Serial0/0/1

```

R1>show ipv6 route ospf neighbor
% Invalid input detected at '^' marker.
R1>show ipv6 ospf neighbor
Neighbor ID      Pri  State           Dead Time   Interface ID  Interface
3.3.3.3          0    FULL/ -         00:00:31    3             Serial0/0/1
R1>enable
Translating "enable"
% Unknown command or computer name, or unable to find computer address
R1>enable
Password:
R1#show ipv6 route ospf
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
O 2001:DB8:ACAD:B::/64 [110/129]
  via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:23::/64 [110/128]
  via FE80::3, Serial0/0/1
R1#

```

R1#show ipv6 route ospf
 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
 O 2001:DB8:ACAD:B::/64 [110/129]
 via FE80::3, Serial0/0/1
 O 2001:DB8:ACAD:C::/64 [110/65]
 via FE80::3, Serial0/0/1
 O 2001:DB8:ACAD:23::/64 [110/128]
 via FE80::3, Serial0/0/1

```

R3>enable
Password:
R3#show ipv6 route ospf neighbor
% Invalid input detected at '^' marker.
R3#show ipv6 ospf neighbor
Neighbor ID      Pri  State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:00:32    4             Serial0/0/0
2.2.2.2          0    FULL/ -         00:00:32    4             Serial0/0/1
R3#

```

R3#show ipv6 route ospf neighbor
 % Invalid input detected at '^' marker.
 R3#show ipv6 ospf neighbor
 Neighbor ID Pri State Dead Time Interface ID Interface
 1.1.1.1 0 FULL/ - 00:00:32 4 Serial0/0/0
 2.2.2.2 0 FULL/ - 00:00:32 4 Serial0/0/1

```

R3#show ipv6 route ospf neighbor
* Invalid input detected at '^' marker.
R3#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:00:32   4             Serial0/0/0
2.2.2.2          0    FULL/ -         00:00:32   4             Serial0/0/1
R3#show ipv6 ospf route
* Invalid input detected at '^' marker.
R3#show ipv6 route ospf
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
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:B::/64 [110/65]
  via FE80::2, Serial0/0/1
O 2001:DB8:ACAD:12::/64 [110/128]
  via FE80::1, Serial0/0/0
  via FE80::2, Serial0/0/1
R3#

```

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

O 2001:DB8:ACAD:A::/64 [110/65]

via FE80::1, Serial0/0/0

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

via FE80::2, Serial0/0/1

O 2001:DB8:ACAD:12::/64 [110/128]

via FE80::1, Serial0/0/0

via FE80::2, Serial0/0/1

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64? Serial0/0/1

¿Cuál es la métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1? 129

¿El R2 aparece como vecino OSPFv3 en el R1? No solo muestra R3

¿El R2 aparece como vecino OSPFv3 en el R3? SI 3.3.3.3

¿Qué indica esta información?

Todo el tráfico desde la red uno será ruteado a través de R3 la interface serial 0/0/0 está configurada como pasivo de tal manera que OSPFv3 no envía información de ruteo notificándose a través de esta interfaz.

El costo acumulado 129 resulta del tráfico que pasa por R3 hacia la ruta 2001:DB8:ACAD:B::/ Este tráfico debe pasar por dos interfaces seriales T1 de 1544 Mb/s de un costo de 64 cada uno más el link de la interface de R2 G0/0 con un costo de 1

- 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>enable
Password:
R2#no passive-interface S0/0/0
^
% Invalid input detected at '^' marker.
R2#configure te
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#no passive-interface S0/0/0
^
% Invalid input detected at '^' marker.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface S0/0/1
R2(config-rtr)#no passive-interface S0/0/0
R2(config-rtr)#
21:33:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:00:37   3             Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:37   4             Serial0/0/1
R2#

```

```

R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface S0/0/1
R2(config-rtr)#no passive-interface S0/0/0
R2(config-rtr)#

```

21:33:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

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

```

R2>enable
Password:
R2#no passive-interface S0/0/0
^
% Invalid input detected at '^' marker.
R2#configure te
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#no passive-interface S0/0/0
^
% Invalid input detected at '^' marker.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface S0/0/1
R2(config-rtr)#no passive-interface S0/0/0
R2(config-rtr)#
21:33:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:00:37   3             Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:37   4             Serial0/0/1
R2#

```

```

R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface S0/0/1
R2(config-rtr)#no passive-interface S0/0/0
R2(config-rtr)#

```

21:33:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

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?

Si porque el ID del proceso OSPFv3 es usado únicamente de manera local en el router no necesita coincidir con el ID del proceso usado en los otros routers en el área OSPFv3.

2. ¿Cuál podría haber sido la razón para eliminar el comando **network** en OSPFv3?

Al remover la entrada network ayuda a prevenir errores en las direcciones de tipo IPV6, también una interfaz IPV6 puede tener multiples direcciones IPV6 asignadas a ella, para la asignación de de la interface a una área OSPFv6 todas las redes multicast en la interfaz serán asignadas automáticamente al área OSPFv6 y tendrán una ruta creada en la tabla de ruteo ipv6.

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.

Practica de laboratorio 10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router

Topología

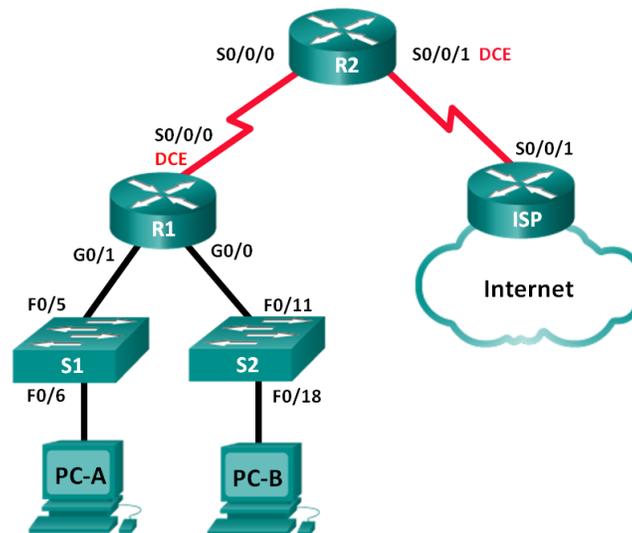


Tabla de direccionamiento

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

Objetivos

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

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

Información básica/situación

El protocolo de configuración dinámica de host (DHCP) es un protocolo de red que permite a los administradores de red administrar y automatizar la asignación de direcciones IP. Sin DHCP, el administrador debe asignar y configurar manualmente las direcciones IP, los servidores DNS preferidos y los gateways predeterminados. A medida que aumenta el tamaño de la red, esto se convierte en un problema administrativo cuando los dispositivos se trasladan de una red interna a otra.

En esta situación, la empresa creció en tamaño, y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su tarea es configurar el router R2 para asignar direcciones IPv4 en dos subredes diferentes conectadas al router R1.

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

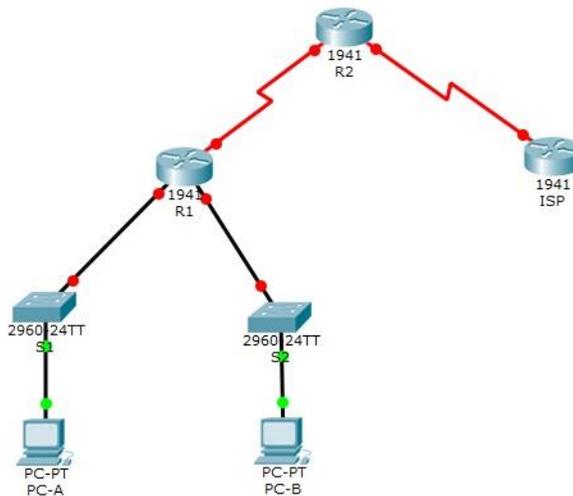
Recursos necesarios

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

Part 10: 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.

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

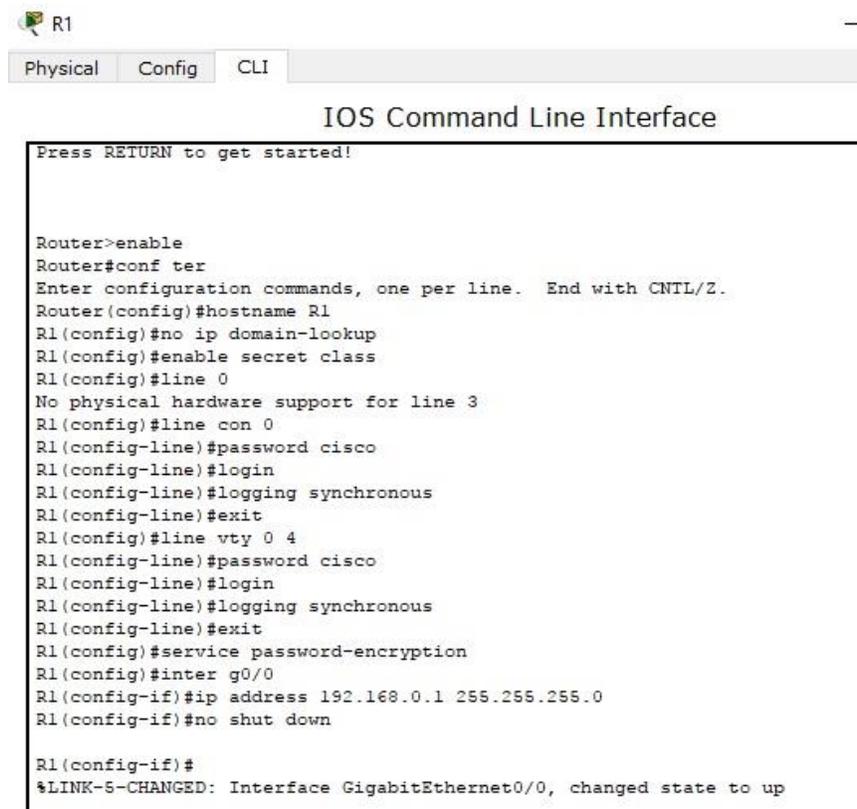


Step 2: inicializar y volver a cargar los routers y los switches.

Step 3: configurar los parámetros básicos para cada router.

- Desactive la búsqueda DNS.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.
- Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.
- Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.

Configuración Router 1.



```
Router R1
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started!

Router>enable
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line 0
No physical hardware support for line 3
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#inter g0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut down

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

Configuración Router 2.

```

R2
Physical Config CLI
IOS Command Line Interface

Router>enable
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host name R2
      ^
% Invalid input detected at '^' marker.

Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#loggin synchronous
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#loggin synchronous
R2(config-line)#exi
R2(config)#service password-encryption
R2(config)#inter g0/0
R2(config-if)#inter s0/0/0
R2(config-if)#ip address 192.168.2.254
R2(config-if)#ip address 192.168.2.254 255.255.255.252
R2(config-if)#no shut down

```

Configuración Router ISP.

```

ISP
Physical Config CLI
IOS Command Line Interface

Router>ena
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#enable secret class
ISP(config)#line con 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#loggin synchronous
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#loggin synchronous
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#int s0/0/1
ISP(config-if)#ip address 209.165.200.225 255.255.255.224
ISP(config-if)#no shut down

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

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

ISP(config-if)#

```

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>enabl
Password:
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
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)#

```

- 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)#
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>ena
Password:
ISP#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#

```

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

Step 4: verificar la conectividad de red entre los routers.

Ping ISP- R1

```

ISP#ping 192.168.2.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/7/16 ms

```

Ping ISP-R2

```

ISP#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 = 1/8/19 ms

```

Ping R1-ISP

```
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 = 2/6/14 ms
```

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.

Step 5: verificar que los equipos host estén configurados para DHCP.

Part 11: 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.

Step 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 (packet tracer no permite configurarlo).

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 Configuration (DHCP)

```
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
```

```
R2(config)#ip dhcp pool R1G0
```

```
R2(dhcp-config)#network 192.168.0.1
```

```
% Incomplete command.
```

```
R2(dhcp-config)#network 192.168.0.1 255.255.255.0
```

```
R2(dhcp-config)#default-router 192.168.0.1
```

```
R2(dhcp-config)#domain ccna-lab.com
```

```
^
```

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

```
R2(dhcp-config)#dns-server 209.165.200.225
```

```
R2(dhcp-config)#lease 2
```

```
^
```

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

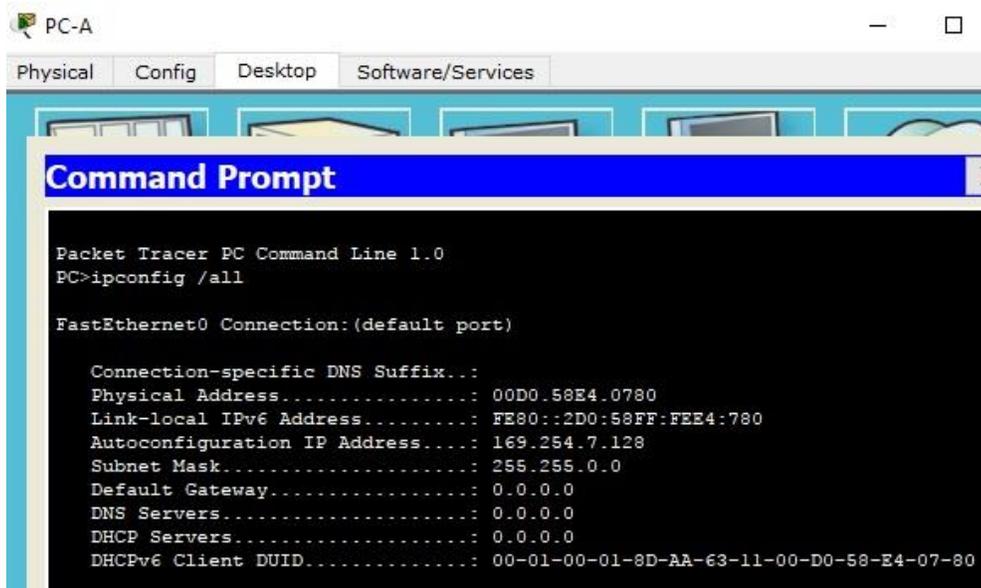
```
R2(dhcp-config)#lease 2
```

```
^
```

```
% Invalid input detected at '^' marker.
R2(dhcp-config)#exit
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
R2(dhcp-config)#domain-name ccna-lab.com
^
% Invalid input detected at '^' marker.
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#lease 2
```

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?

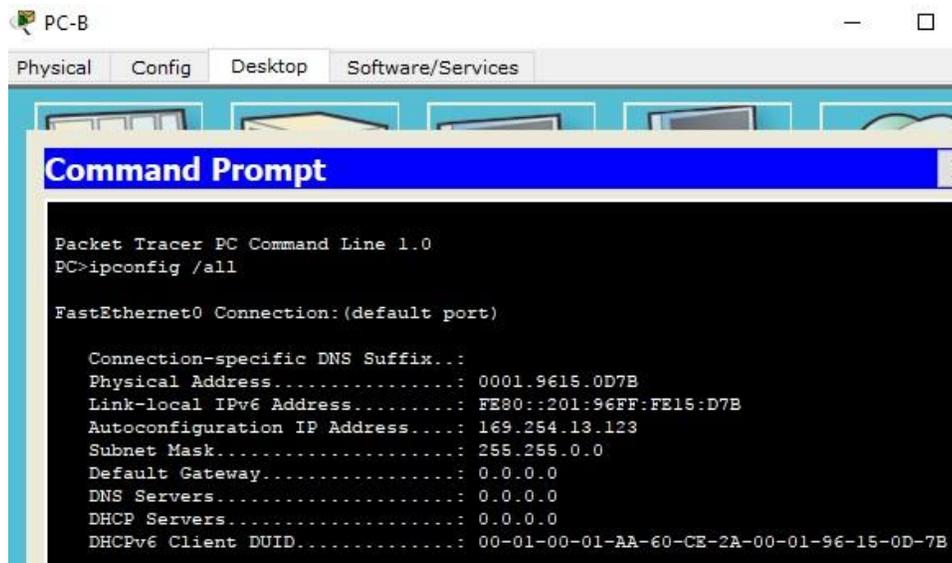
R// Los equipos host no recibieron una dirección IP del servidor DHCP en R2 hasta que R1 se configuró como un agente de retransmisión para DHCP.



```
Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix... :
Physical Address.....: 00D0.58E4.0780
Link-local IPv6 Address.....: FE80::2D0:58FF:FEE4:780
Autoconfiguration IP Address....: 169.254.7.128
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-8D-AA-63-11-00-D0-58-E4-07-80
```



Step 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.

```
R2>ena
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/0
R2(config-if)#ip helper-address 192.168.2.254
R2(config-if)#exit
R2(config)#int g0/1
R2(config-if)#ip helper-address 192.168.2.254
R2(config-if)#exit
R2(config)#
```

Step 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.

IP PC-A

```

PC>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 00D0.58E4.0780
    Link-local IPv6 Address.....: FE80::2D0:58FF:FEE4:780
    IP Address.....: 192.168.1.10
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 192.168.1.1
    DNS Servers.....: 209.165.200.225
    DHCP Servers.....: 192.168.2.254
    DHCPv6 Client DUID.....: 00-01-00-01-8D-AA-63-11-00-D0-58-E4-07-80

```

IP PC-B

```

PC>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0001.9615.0D7B
    Link-local IPv6 Address.....: FE80::201:96FF:FE15:D7B
    IP Address.....: 192.168.0.10
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 192.168.0.1
    DNS Servers.....: 209.165.200.225
    DHCP Servers.....: 192.168.2.254
    DHCPv6 Client DUID.....: 00-01-00-01-AA-60-CE-2A-00-01-96-15-0D-7B
Complete...

```

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?

R// PC-A: 192.168.1.10

PC-B: 192.168.0.10

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

- En el R2, introduzca el comando **show ip dhcp binding** para ver los arrendamientos de direcciones DHCP.

```

R2>enable
R2#show ip dhcp binding

```

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.0.10	0001.9615.0D7B	--	Automatic
192.168.1.10	00D0.58E4.0780	--	Automatic

Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado?

R// Las direcciones de hardware del cliente identifican las computadoras específicas que se han unido a la red.

- 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?

R// 10 tipos.

- 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)?
R// La siguiente dirección disponible para ser arrendada.
- d. En el R2, introduzca el comando **show run | section dhcp** para ver la configuración DHCP en la configuración en ejecución.

```

hostname R2
!
!
!
!
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 R1G0
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 209.165.200.225
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
!
!|
!
no ip cef
no ipv6 cef
!

```

- e. En el R2, 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.

```

interface GigabitEthernet0/0
no ip address
ip helper-address 192.168.2.254
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
ip helper-address 192.168.2.254
duplex auto
speed auto
shutdown

```

Reflexión

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

R// Tener un servidor DHCP de enrutador independiente para cada subred agregaría más complejidad, disminuiría la administración centralizada para la red, y también requeriría que cada enrutador trabaje más arduamente administrando su propio DHCP mientras enruta el tráfico. Un servidor DHCP (RT / PC) dedicado es más fácil de administrar y está más centralizado.

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 de DHCP

Router R1

R1(config)# interface g0/0

```
R1(config-if)# ip helper-address 192.168.2.254
```

```
R1(config-if)# exit
```

```
R1(config-if)# interface g0/1
```

```
R1(config-if)# ip helper-address 192.168.2.254
```

Router R2

```
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
```

```
R2(dhcp-config)# dns-server 209.165.200.225
```

```
R2(dhcp-config)# domain-name ccna-lab.com
```

```
R2(dhcp-config)# lease 2
```

```
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
```

```
R2(dhcp-config)# lease 2
```

Práctica de laboratorio 10.1.2.5: configuración de DHCPv4 básico en un switch

Topología

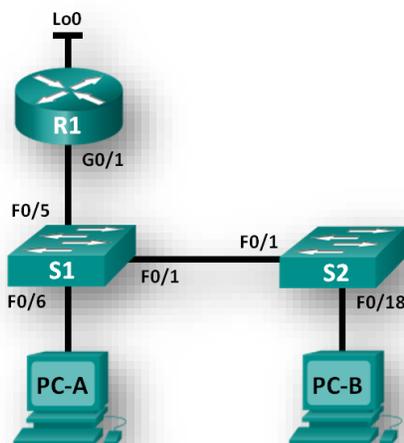


Tabla de direccionamiento

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 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.

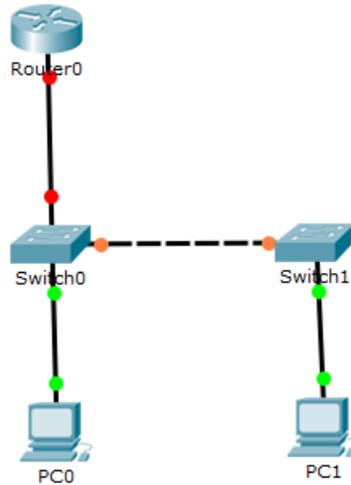
Nota: asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

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

Parte 12: ARMAR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

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



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

Paso 3: Configurar los parámetros básicos en los dispositivos.

- Asigne los nombres de dispositivos como se muestra en la topología.
- Desactive la búsqueda del DNS.
- Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/1
Router(config-if)#ip address 192.168.1.10 255.255.255.0
Router(config-if)#no shut

Router(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

Router(config-if)#int lo 0

Router(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ip address 209.165.200.225 255.255.255.224
Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shut
Router(config-if)#
Router(config-if)#
```

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

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#int vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shut

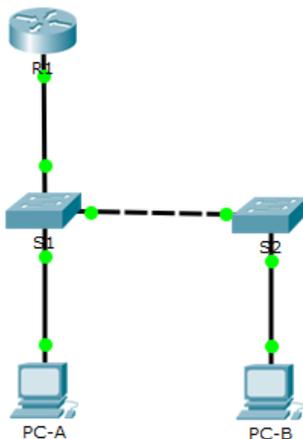
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#int vlan 2
S1(config-if)#ip address 192.168.2.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#
S1(config-if)#
S1(config-if)#|

```

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



Parte 13: 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 1: 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?

R/. Las respuestas variarán, "predeterminado" o "ipv4 dual e ipv6 predeterminado" o "enrutamiento base LAN"

Paso 2: Cambiar la preferencia de SDM en el S1.

- 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?

R/-Enrutamiento base LAN.

- 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]
```

```
S1#reload
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 3: 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

Parte 14: 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 1: 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.

R/.S1 (config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10

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

R/.S1 (config)#ip dhcp pool DHCP1

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

R/. S1 (dhcp-config)#network 192.168.1.0 255.255.255.0

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

R/. (dhcp-config)#default-router 192.168.1.1

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

R/. S1 (dhcp-config)#dns-server 192.168.1.9

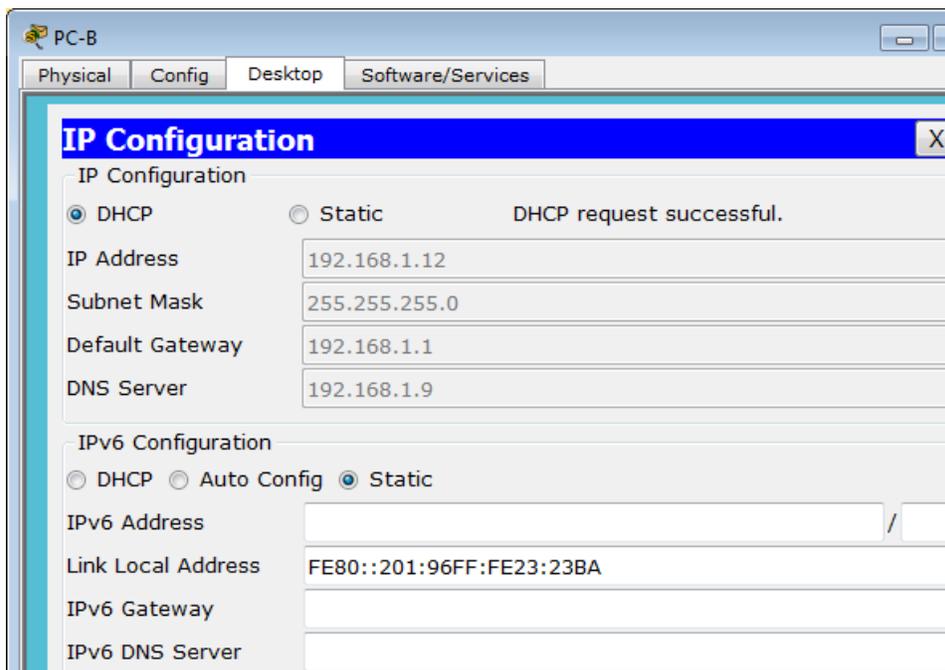
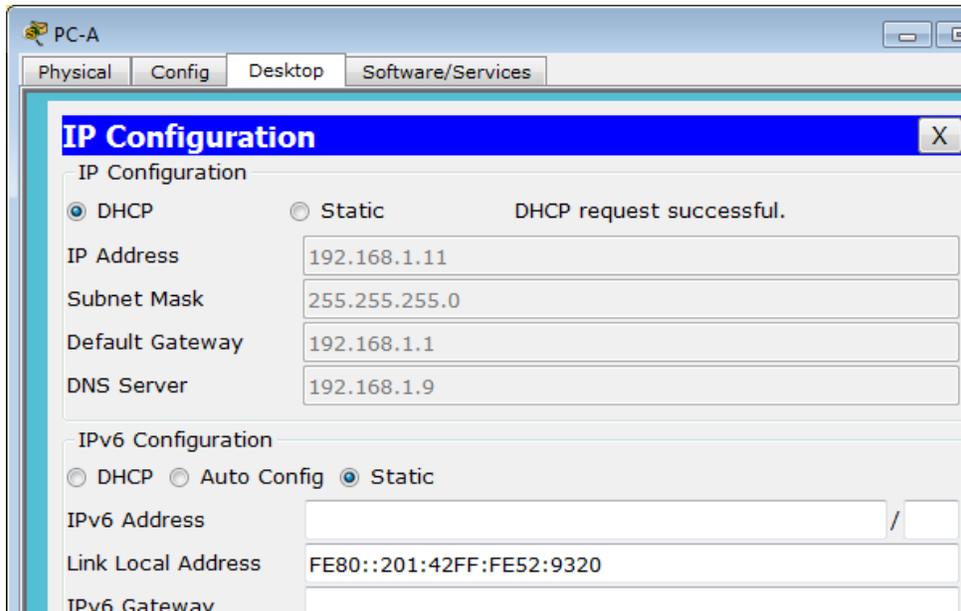
- f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

R/. S1 (dhcp-config)#lease 3

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

Paso 2: Verificar la conectividad y DHCP.

- 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.

Parte 15: 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 1: 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 fa0/6

S1 (config)# switchport mode access

S1 (config)# switchport access vlan 2

Paso 2: 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.

R/. S1(config) # 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.

R/. S1(config) # 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.

R/. S1(dhcp-config) # 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.

R/. S1(dhcp-config) # 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.

S1(dhcp-config) # dns-server 192.168.2.9

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

R/. S1(dhcp-config) # lease 3

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

Paso 3: 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?

Debido a que la puerta de enlace predeterminada está en la misma red que la PC-A, PC-A puede hacer ping a la puerta de enlace predeterminada. PC-B está en una red diferente; Por lo tanto, el ping de PC-A no tiene éxito

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

¿Qué resultado arrojó este comando?

No se ha establecido ninguna puerta de enlace predeterminada y no hay ninguna tabla de enrutamiento en el conmutador

Parte 16: 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.

Paso 1: Habilitar el routing IP en el S1.

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

S1(config)# **ip routing**

b. 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 enrutando entre VLANs

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

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

El conmutador muestra una tabla de enrutamiento que muestra las VLAN como redes conectadas directamente 192.168.1.0/24 y 192.168.2.0/24.

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

```
Router#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

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.10/32 is directly connected, GigabitEthernet0/1
       209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.0/24 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
```

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

La salida del enrutador muestra redes conectadas directamente de 192.168.1.0 y 209.165.200.224 pero no tiene ninguna entrada para la red 192.168.2.0

e. ¿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?

Para que se produzca la comunicación entre todas las redes, se deben agrgar rutas a las tablas de enrutamiento.

Paso 2: 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.

S1 (config) # ip route 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.

Router(config)#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?

Gateway de último recurso es 192.168.1.10 a la red o.o.o.o dos redes directamente conectadas y una red estática.

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

¿Cómo está representada la ruta estática?

S 192.168.2.0/24 está conectado directamente, GigabitEthernet0 / 1

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

R/. Satisfactorio

- f.** ¿Es posible hacer ping de la PC-A a la interfaz Lo0?

R/. Satisfactorio

Reflexión

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

Las direcciones estáticas fueron excluidas punto de crear pool el DHCPv4 una ventana de tiempo existes cuando se excluye la direcciones y podría ser dado dinámicamente hacia el hosts.

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

Los switch fue asignada la configuración IP basándose en la asigna miento de VLAN y el asigna miento en el puerto de Vlan en puerto asignado en el puerto donde está conectado el host.

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

Este switch 2960 puede tener funciones del servidor DHCP y puede establecer estáticas y entre VLAN

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
```

PRACTICA DE LABORATORIO 10.2.3.5 LAB - CONFIGURING STATELESS AND STATEFUL DHCPV6

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

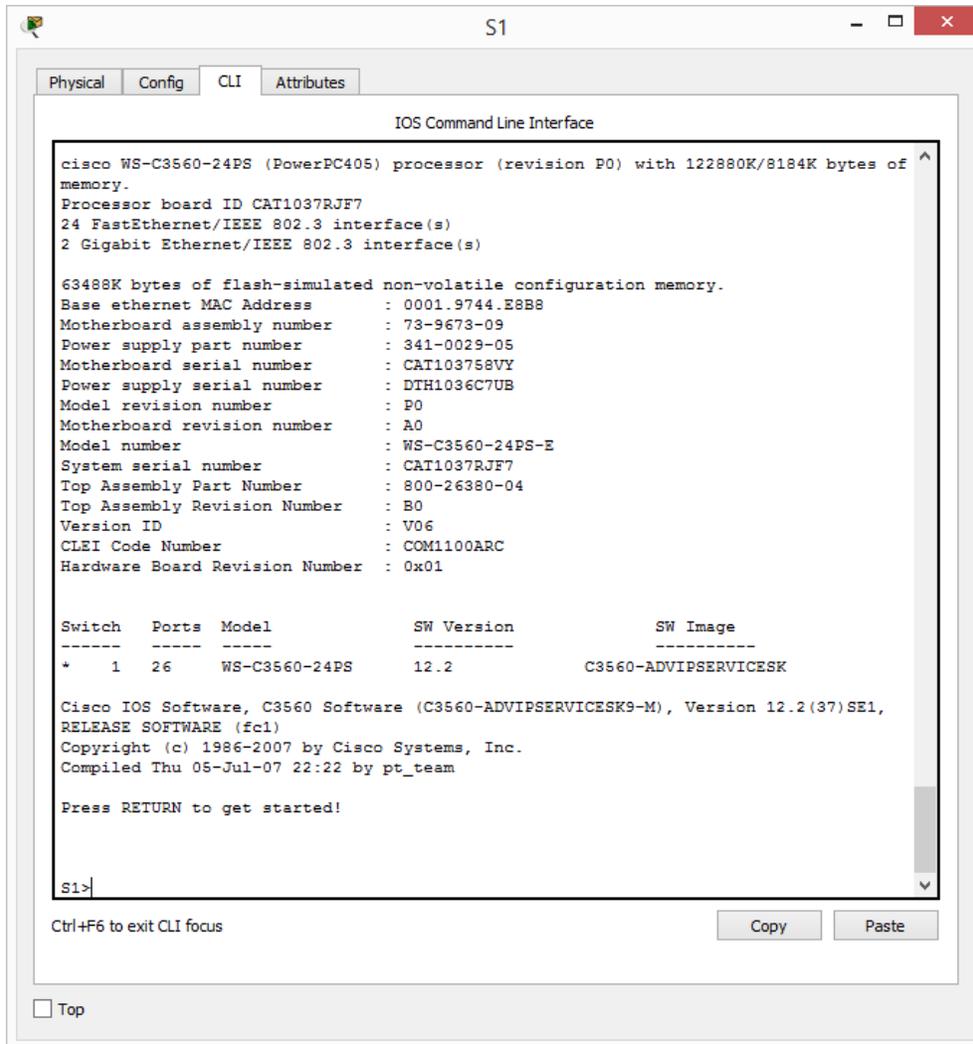
Switch>ENABLE
Switch#show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          6K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:           8K
  number of directly-connected IPv4 hosts: 6K
  number of indirect IPv4 routes:        2K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:             0.5K
number of IPv4/MAC security aces:       1K

Switch#
```

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
```



Recursos necesarios

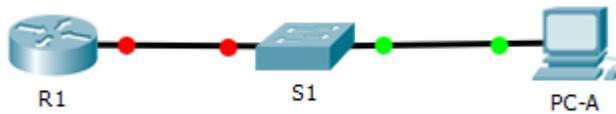
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para 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.

Part 17: 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.

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



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.

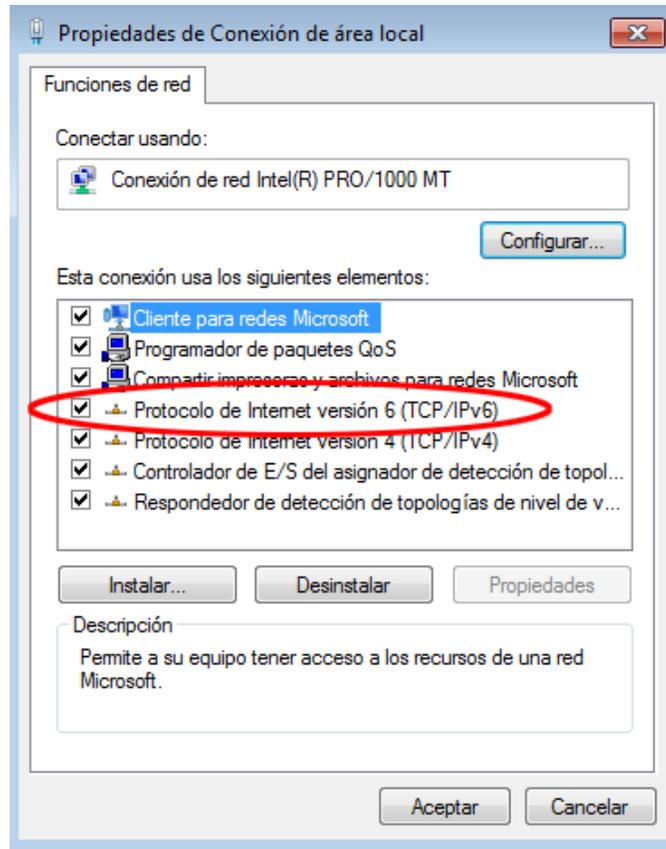
Step 4: configurar el S1.

- 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.

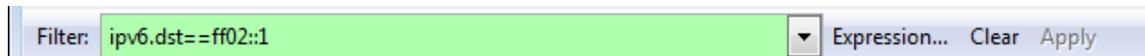
Part 18: configurar la red para SLAAC

Step 1: 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.

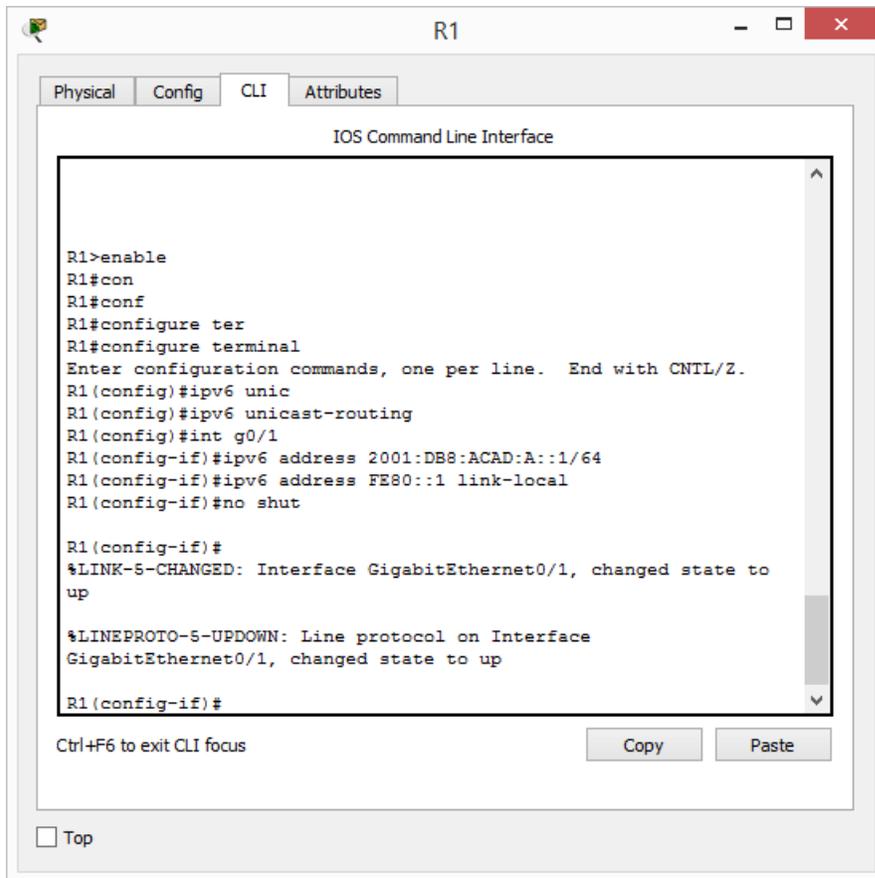


- b. Inicie una captura del tráfico en la NIC con Wireshark.
- c. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes. La entrada de filtro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



Step 2: Configurar R1

- a. Habilite el routing de unidifusión IPv6.
- b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.
- c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.
- d. Active la interfaz G0/1.

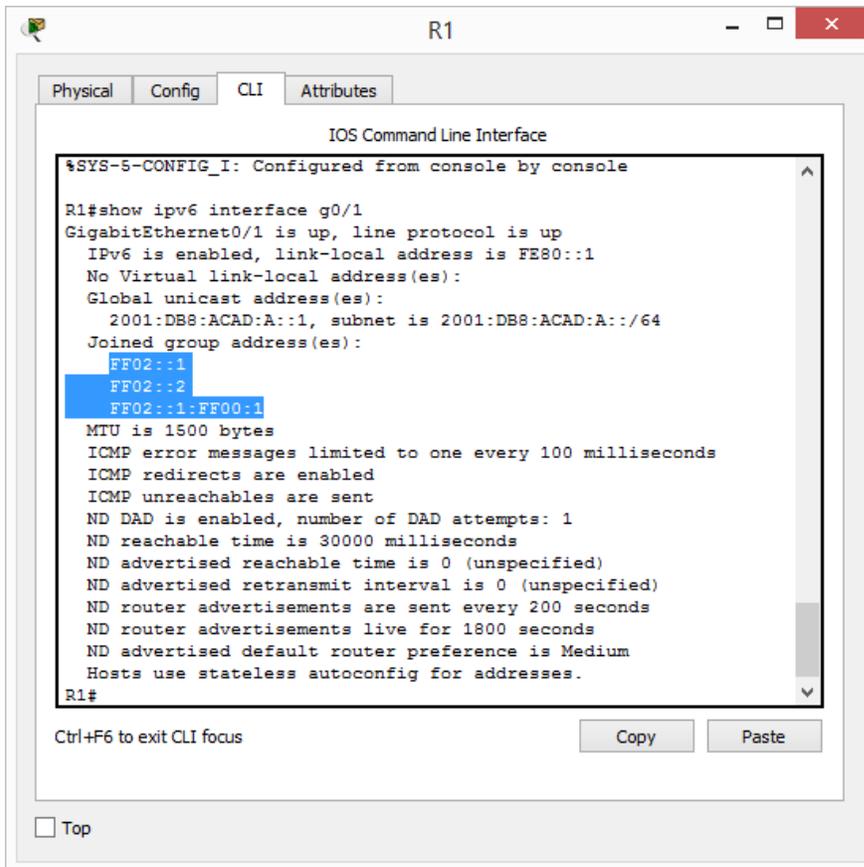


Step 3: verificar que el R1 forme parte del grupo de multidifusión de todos los routers.

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 unreachable 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.



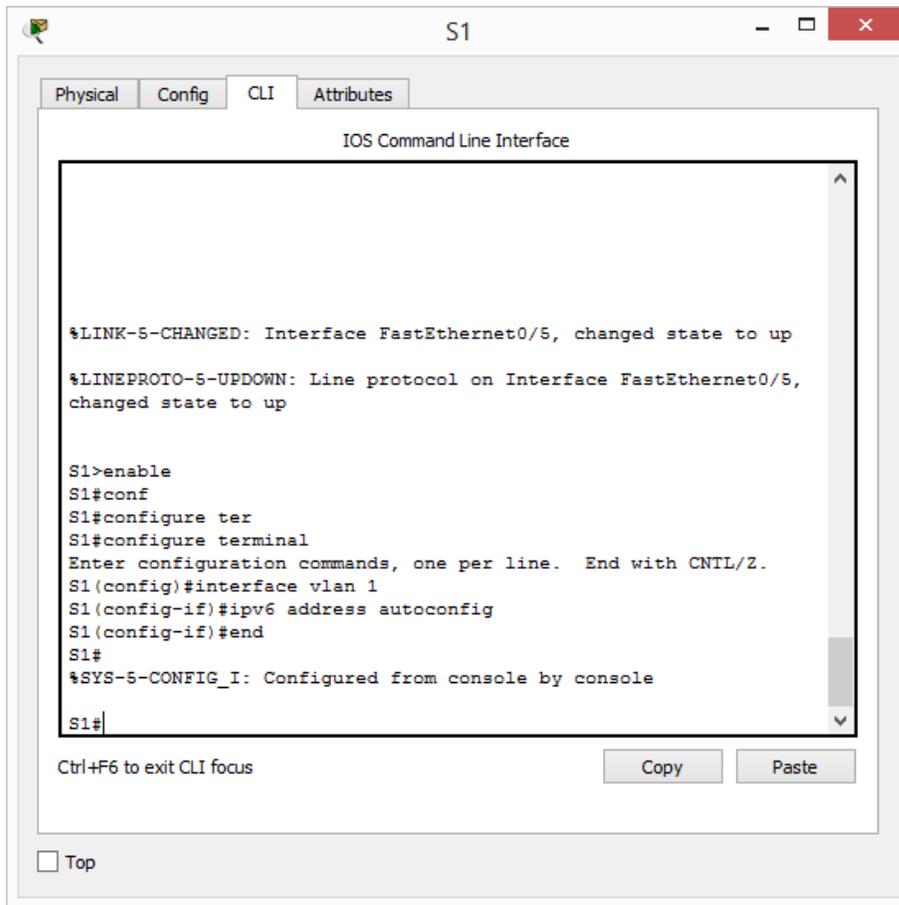
```
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console

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 unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
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.
R1#
```

Step 4: configurar el S1.

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

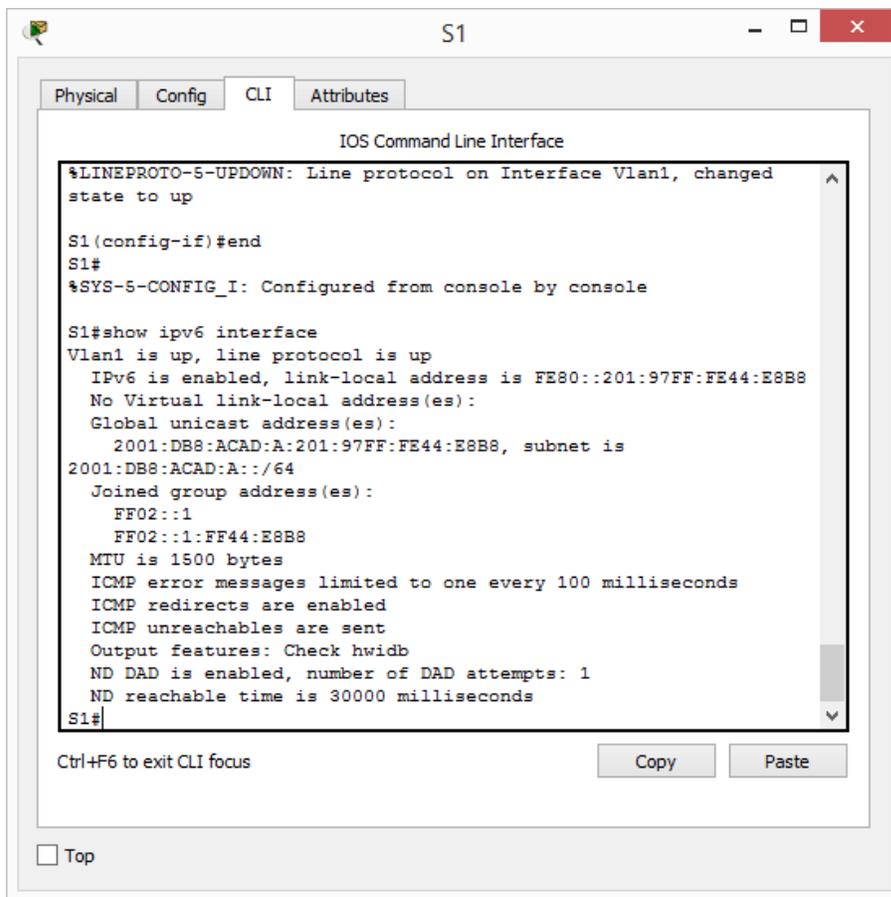
```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
S1(config-if)# end
```



Step 5: verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

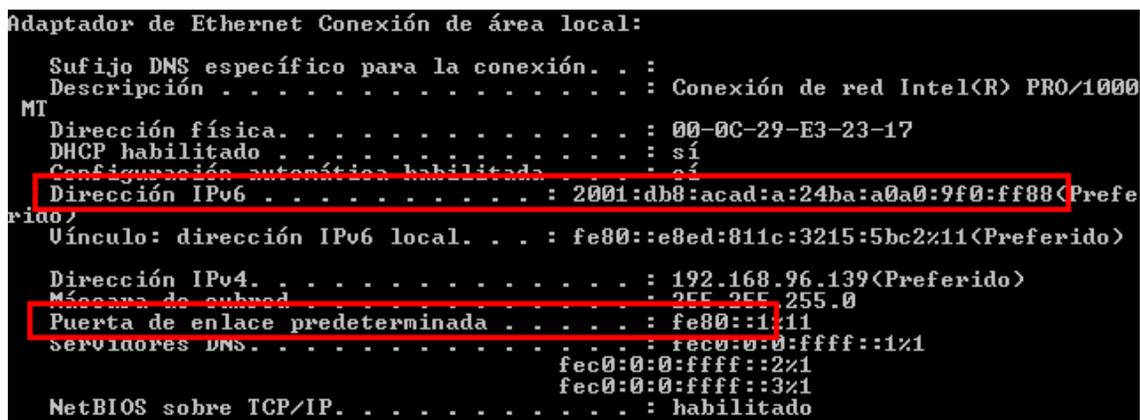
Use el comando **show ipv6 interface** para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

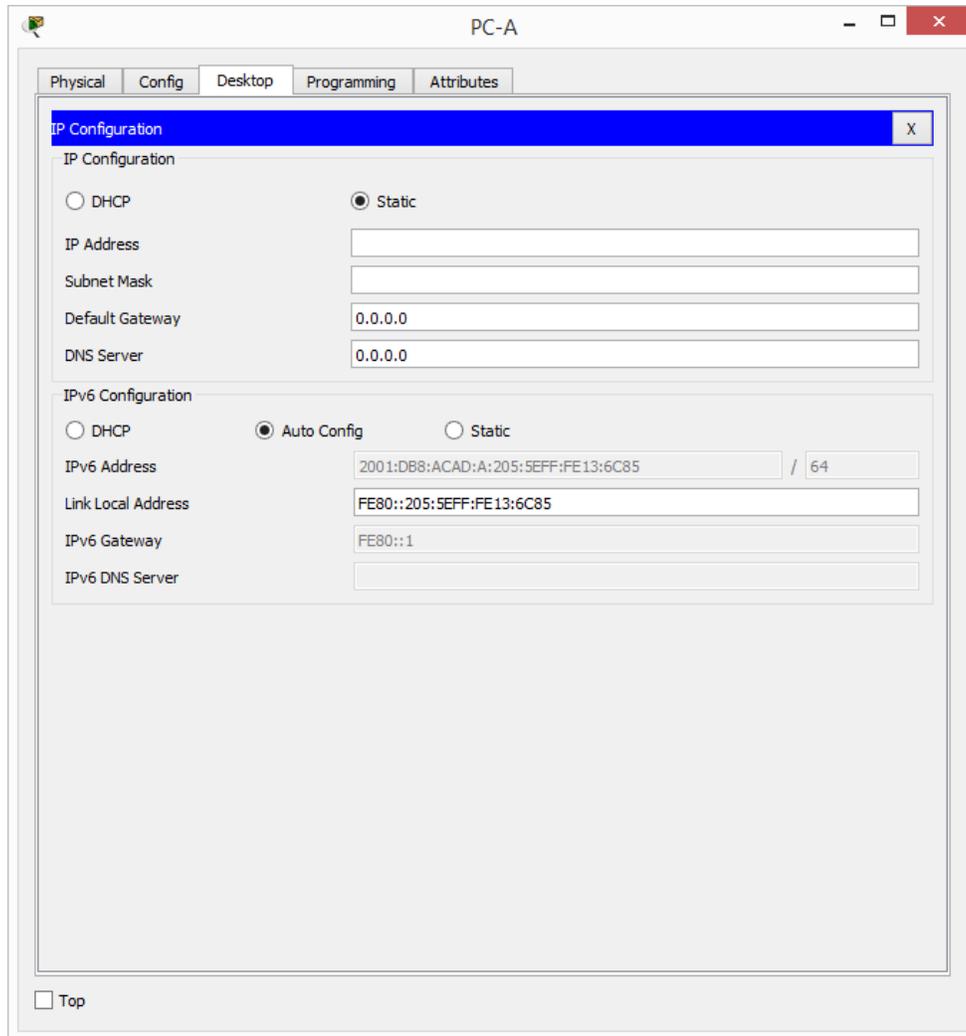
```
S1# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
No Virtual link-local address(es):
Stateless address autoconfig enabled
Global unicast address(es):
  2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]
    valid lifetime 2591988 preferred lifetime 604788
Joined group address(es):
  FF02::1
  FF02::1:FE8:8A40
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable 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
```



Step 6: 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.

Filter: `ipv6.dst==ff02::1` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
3348	3912.20390	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3518	3972.07973	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3673	4130.43155	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3840	4284.68370	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3989	4435.87602	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1

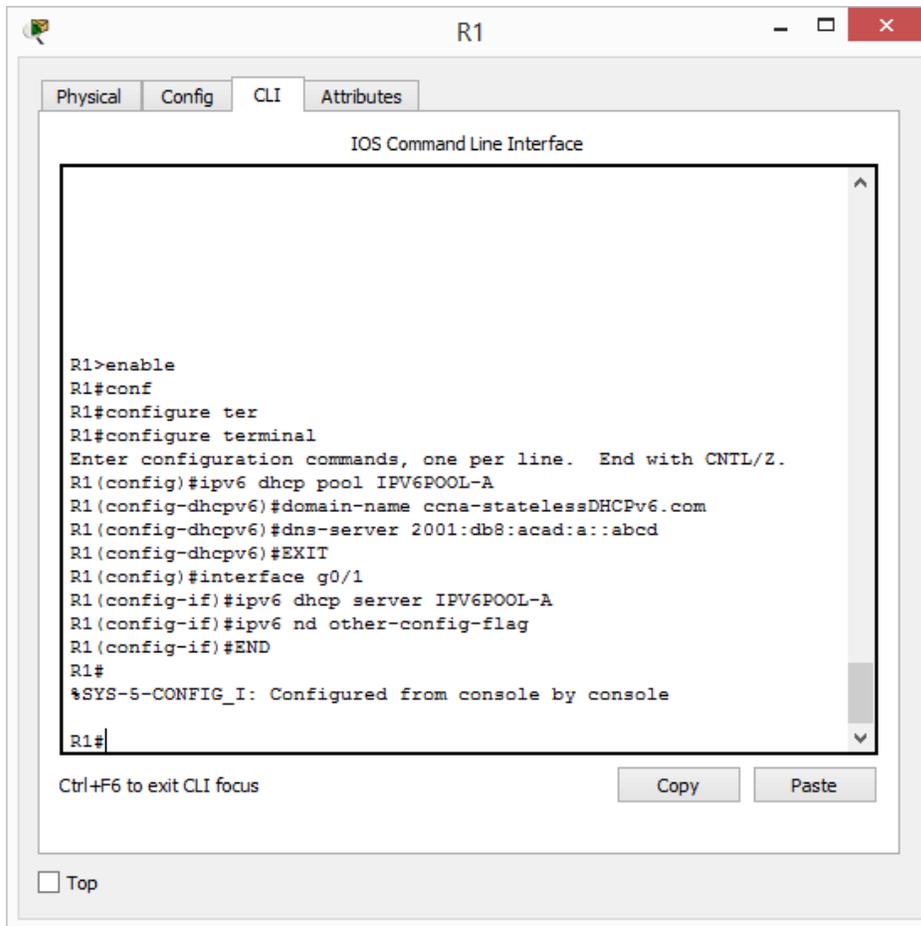
Frame 3518: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x1816 [correct]
 - Cur hop limit: 64
 - Flags: 0x00
 - 0... .. = Managed address configuration: Not set
 - .0... .. = Other configuration: Not set
 - ..0... .. = Home Agent: Not set
 - ...0 0... = Prf (Default Router Preference): Medium (0)
 -0.. = Proxy: Not set
 -0. = Reserved: 0
 - Router lifetime (s): 1800
 - Reachable time (ms): 0
 - Retrans timer (ms): 0
 - ICMPv6 option (Source link-layer address : d4:8c:b5:ce:a0:c1)
 - ICMPv6 Option (MTU : 1500)
 - ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)
 - Type: Prefix information (3)
 - Length: 4 (32 bytes)
 - Prefix Length: 64
 - Flag: 0xc0
 - Valid Lifetime: 2592000
 - Preferred Lifetime: 604800
 - Reserved
 - Prefix: 2001:db8:acad:a:: (2001:db8:acad:a::)

Part 19: configurar la red para DHCPv6 sin estado

Step 1: configurar un servidor de DHCP IPv6 en el R1.

- Cree un pool de DHCP IPv6.
R1(config)# **ipv6 dhcp pool IPV6POOL-A**
- Asigne un nombre de dominio al pool.
R1(config-dhcpv6)# **domain-name ccna-statelessDHCPv6.com**
- Asigne una dirección de servidor DNS.
R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**
R1(config-dhcpv6)# **exit**
- Asigne el pool de DHCPv6 a la interfaz.
R1(config)# **interface g0/1**
R1(config-if)# **ipv6 dhcp server IPV6POOL-A**
- Establezca la detección de redes (ND) DHCPv6 **other-config-flag**.
R1(config-if)# **ipv6 nd other-config-flag**
R1(config-if)# **end**



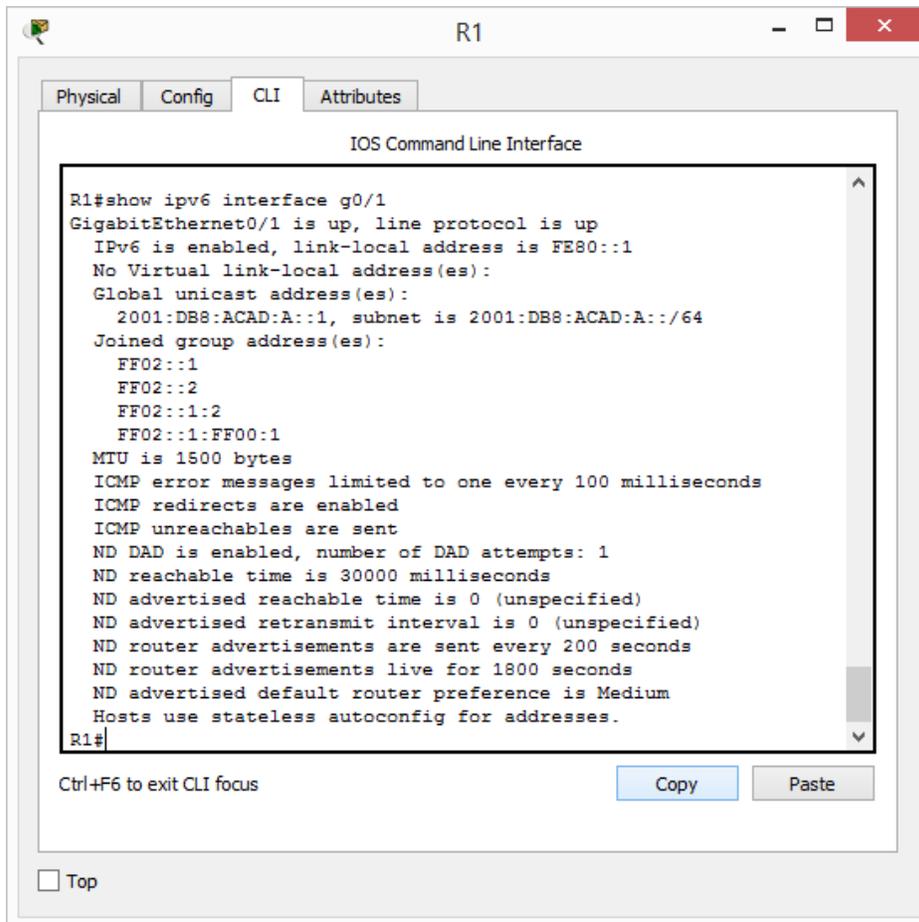
Step 2: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

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 unreachable 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.
```



Step 3: 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
MI
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(Preferido)
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-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí

```

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address: 2001:DB8:ACAD:A:205:5EFF:FE13:6C85 / 64

Link Local Address: FE80::205:5EFF:FE13:6C85

IPv6 Gateway: FE80::1

IPv6 DNS Server: 2001:DB8:ACAD:A::ABCD

Step 4: 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.

Filter: `ipv6.dst==ff02::1`

No.	Time	Source	Destination	Protocol	Length	Info
191	190.005980	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
422	383.803033	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
696	581.355847	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
877	776.644829	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1

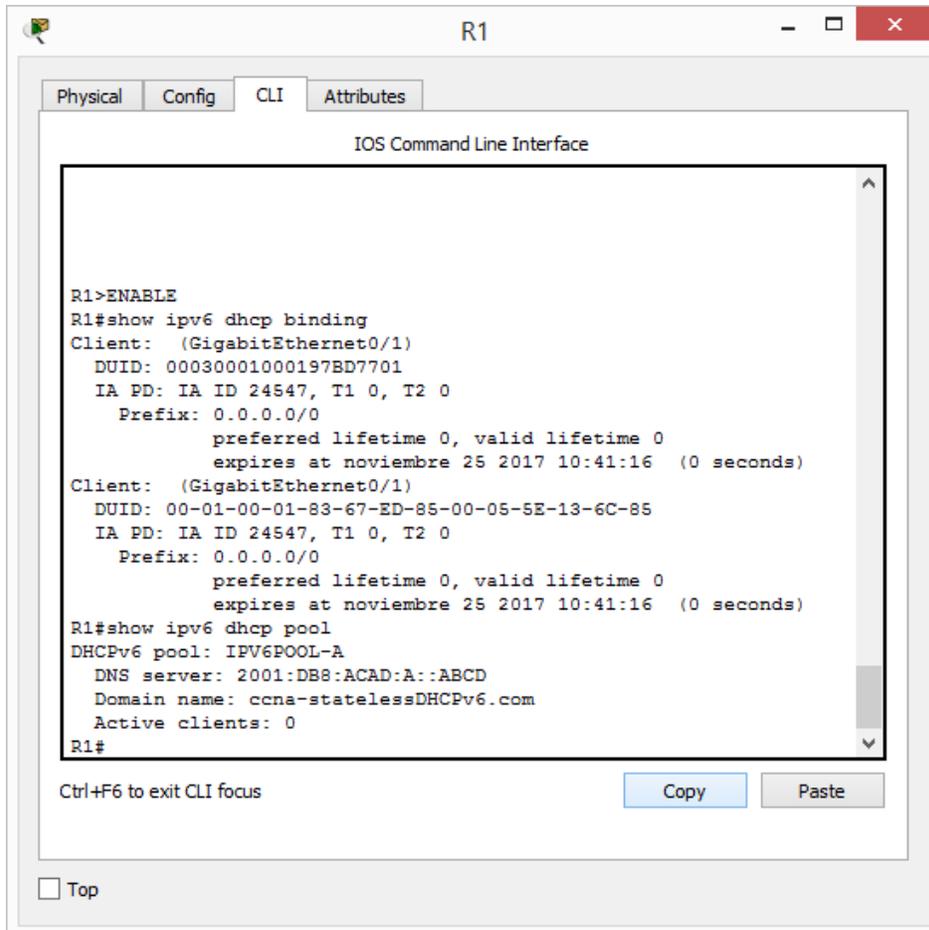
Frame 877: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x17d6 [correct]
 - Cur hop limit: 64
 - Flags: 0x40
 - 0... .. = Managed address configuration: Not set
 - .1... .. = Other configuration: Set**
 - ..0... .. = Home Agent: NOT set
 - ...0... = Prf (Default Router Preference): Medium (0)
 -0.. = Proxy: Not set
 -0.. = Reserved: 0
 - Router lifetime (s): 1800
 - Reachable time (ms): 0
 - Retrans timer (ms): 0
 - ICMPv6 option (Source link-layer address : d4:8c:b5:ce:a0:c1)
 - ICMPv6 option (MTU : 1500)
 - ICMPv6 option (Prefix information : 2001:db8:acad:a::/64)

Step 5: 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
```

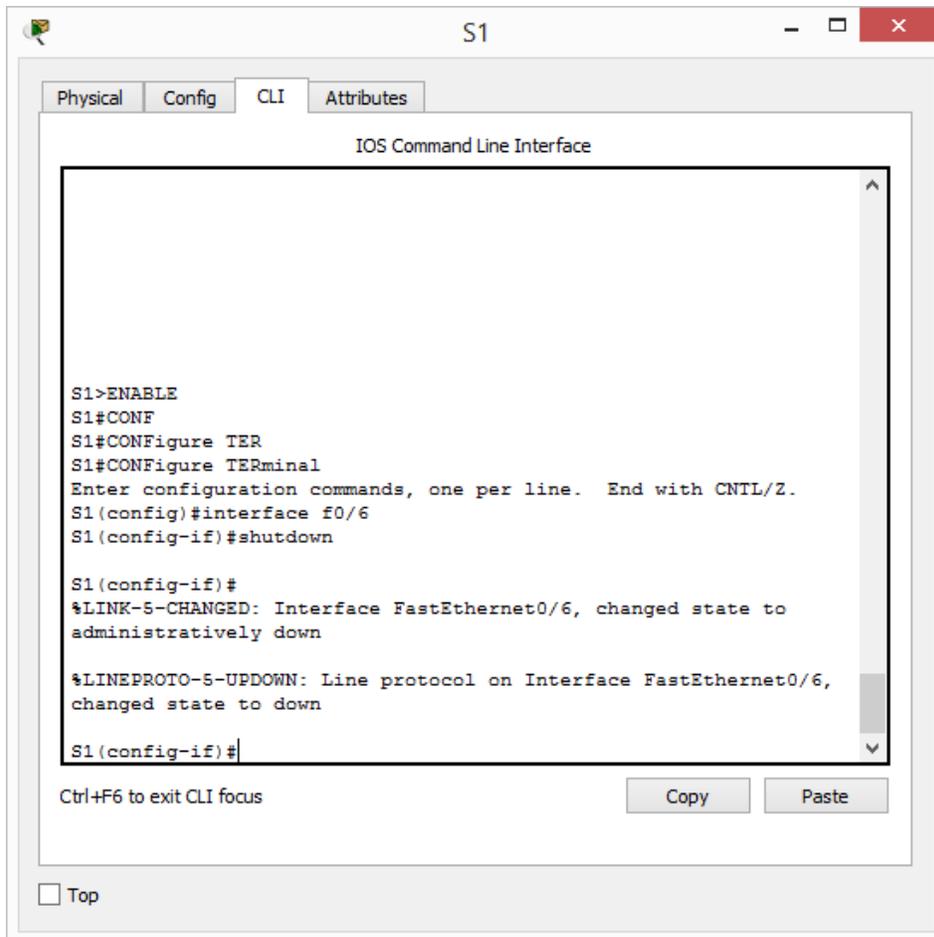


Step 6: restablecer la configuración de red IPv6 de la PC-A.

- 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
```

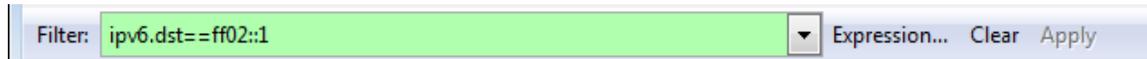


- b. Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.
- c. Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.
 - 1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 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.

Part 20: configurar la red para DHCPv6 con estado

Step 1: preparar la PC-A.

- Inicie una captura del tráfico en la NIC con Wireshark.
- 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 2: cambiar el pool de DHCPv6 en el R1.

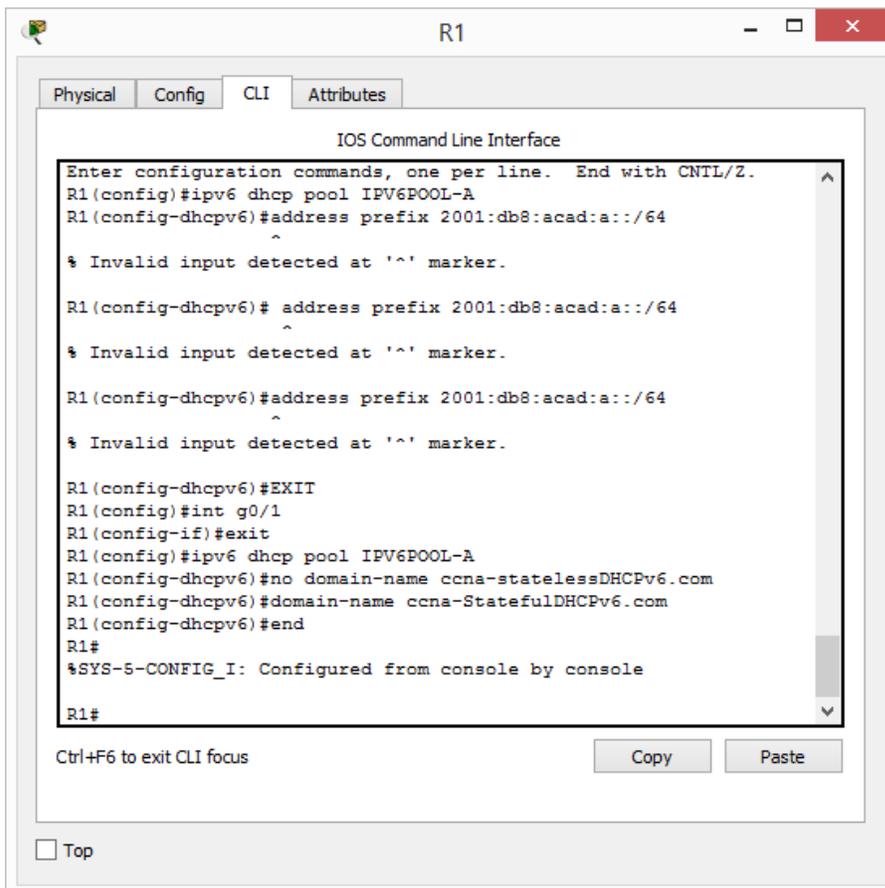
- Agregue el prefijo de red al pool.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```

- 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
```



- 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
```

```
R1
```

Physical Config CLI Attributes

IOS Command Line Interface

```
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.

R1(config-dhcpv6)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.

R1(config-dhcpv6)#EXIT
R1(config)#int g0/1
R1(config-if)#exit
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
R1#
```

Ctrl+F6 to exit CLI focus

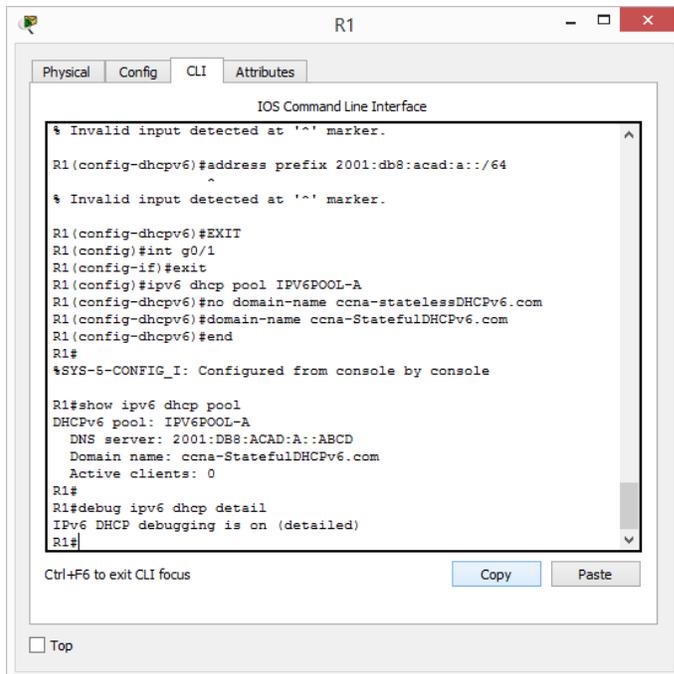
Copy Paste

Top

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)
```

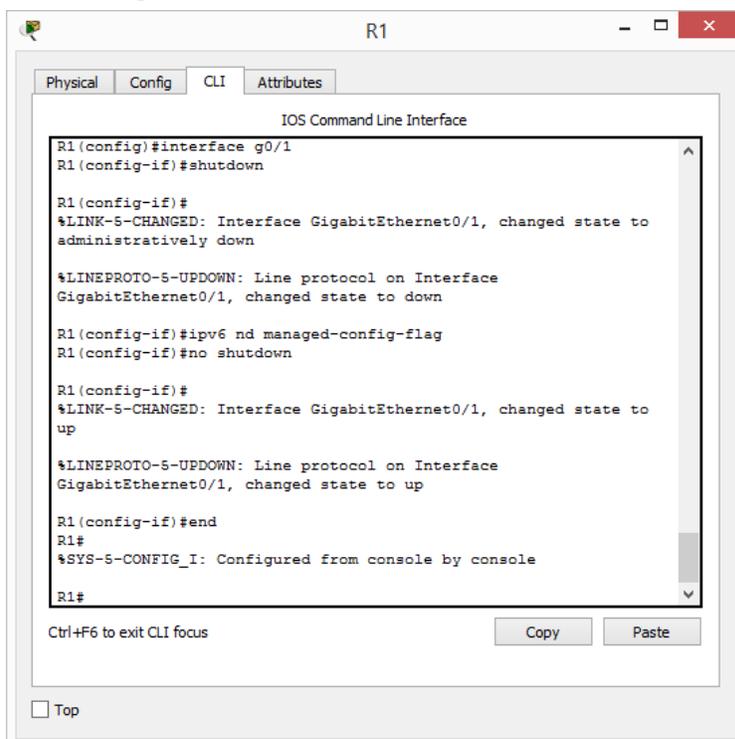


```
R1
IOS Command Line Interface
% Invalid input detected at '^' marker.
R1(config-dhcpv6)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.
R1(config-dhcpv6)#EXIT
R1(config)#int g0/1
R1(config-if)#exit
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
R1#
R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R1#
```

Step 3: 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
```



```
R1
IOS Command Line Interface
R1(config)#interface g0/1
R1(config-if)#shutdown

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

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

R1(config-if)#ipv6 nd managed-config-flag
R1(config-if)#no shutdown

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

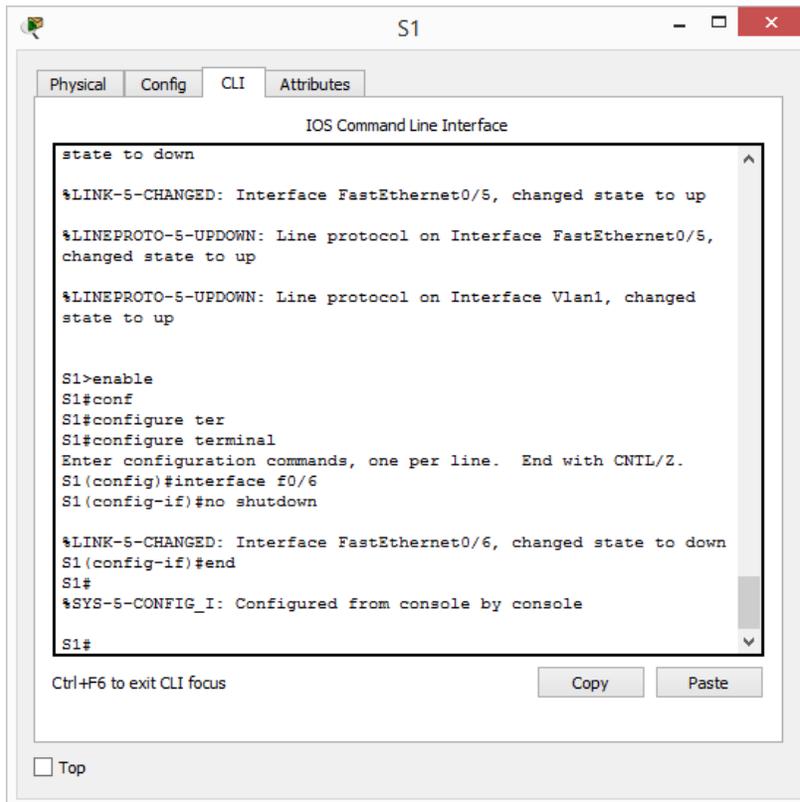
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

Step 4: 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
```



Step 5: verificar la configuración de DHCPv6 con estado en el R1.

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

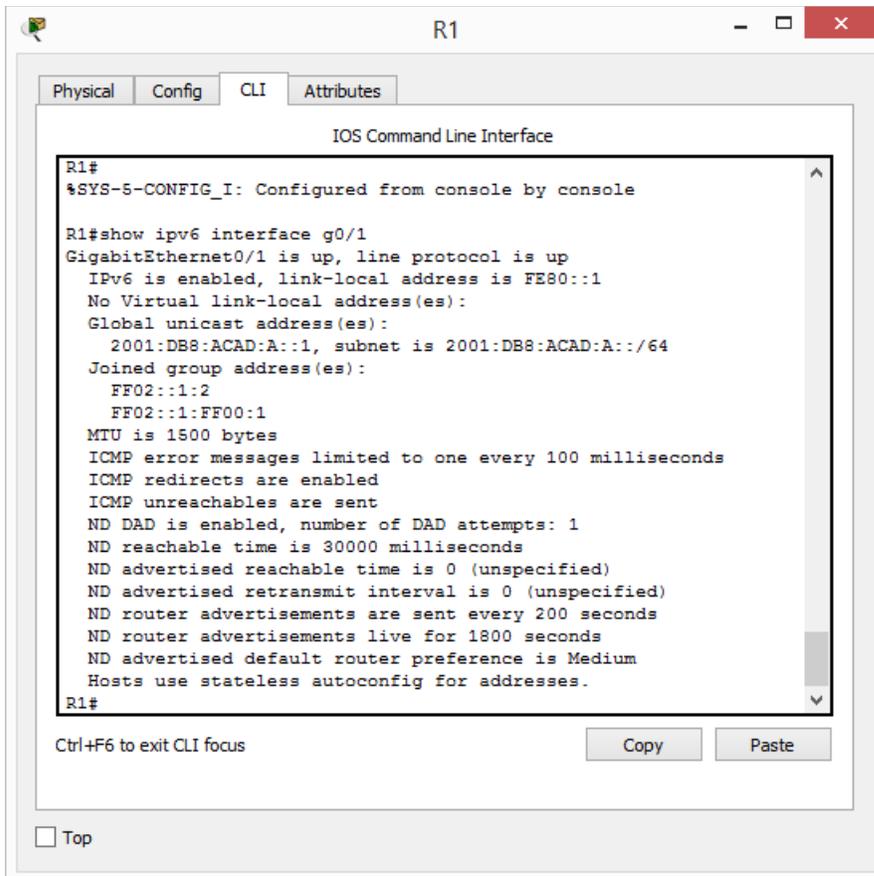
```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  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 unreachable 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)
```

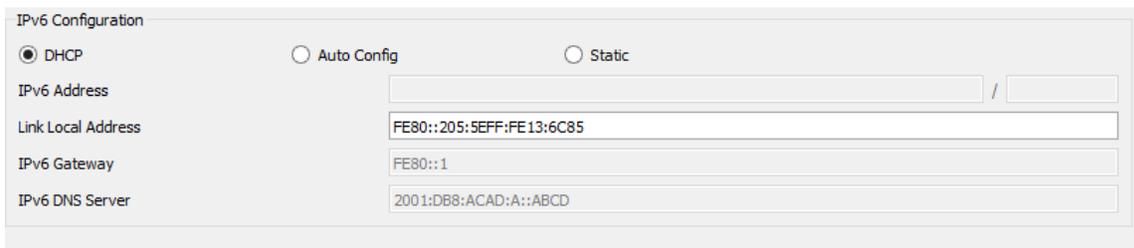
```
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
```

Hosts use DHCP to obtain routable addresses.

Hosts use DHCP to obtain other configuration.



- 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.



- 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<Preferido>
  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<Preferido>
  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
```

- 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
```

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
*mar. 1 03:46:15.230: 2001:DB8:ACAD:A::ABCD
*mar. 1 03:46:15.230: option DOMAIN-LIST(24), len 5
*mar. 1 03:46:15.230: ccna-StatefulDHCPv6.com

R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 0
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00030001000197BD7701
IA PD: IA ID 24547, T1 0, T2 0
Prefix: 0.0.0.0/0
preferred lifetime 0, valid lifetime 0
expires at noviembre 25 2017 11:17:40 (0 seconds)
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85
IA PD: IA ID 24547, T1 0, T2 0
Prefix: 0.0.0.0/0
preferred lifetime 0, valid lifetime 0
expires at noviembre 25 2017 11:17:40 (0 seconds)
R1#undebug all
All possible debugging has been turned off
R1#
Ctrl+F6 to exit CLI focus
Copy Paste
 Top

```

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

```

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

*mar. 1 03:45:54.470: IPv6 DHCP: Received SOLICIT from FE80::205:5EFF:FE13:6C85 on GigabitEthernet0/1

*mar. 1 03:45:54.470: IPv6 DHCP: detailed packet contents

*mar. 1 03:45:54.470: src FE80::205:5EFF:FE13:6C85 (GigabitEthernet0/1)

*mar. 1 03:45:54.470: dst FF02::1:2 (GigabitEthernet0/1)

*mar. 1 03:45:54.470: type SOLICIT(1), xid 3

*mar. 1 03:45:54.470: option ELAPSED-TIME(8), len 6

*mar. 1 03:45:54.470: elapsed-time 43995

*mar. 1 03:45:54.470: option CLIENTID(1), len 45

*mar. 1 03:45:54.470: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85

*mar. 1 03:45:54.470: option ORO(6), len 10

*mar. 1 03:45:54.470: IA-PD, DNS-SERVERS, DOMAIN-LIST

*mar. 1 03:45:54.470: option IA-PD(25), len 16

*mar. 1 03:45:54.470: IAID 0x24547, T1 0, T2 0

*mar. 1 03:45:54.470: IPv6 DHCP: Using interface pool IPV6POOL-A

*mar. 1 03:45:54.470: IPv6 DHCP: Sending ADVERTISE to FE80::205:5EFF:FE13:6C85 on GigabitEthernet0/1

*mar. 1 03:45:54.470: IPv6 DHCP: detailed packet contents

*mar. 1 03:45:54.470: src FE80::1 (GigabitEthernet0/1)

*mar. 1 03:45:54.470: dst FE80::205:5EFF:FE13:6C85 (GigabitEthernet0/1)

*mar. 1 03:45:54.470: type ADVERTISE(2), xid 3

*mar. 1 03:45:54.470: option SERVERID(2), len 24

*mar. 1 03:45:54.470: 000300010030A312AA01

*mar. 1 03:45:54.470: option CLIENTID(1), len 45

*mar. 1 03:45:54.470: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85

*mar. 1 03:45:54.470: option IA-PD(25), len 45

*mar. 1 03:45:54.470: IAID 0x24547, T1 0, T2 0

*mar. 1 03:45:54.470: option IAPREFIX(26), 29

*mar. 1 03:45:54.470: preferred 0, valid 0, prefix 0.0.0.0/0

*mar. 1 03:45:54.481: IPv6 DHCP: Received REQUEST from FE80::205:5EFF:FE13:6C85 on GigabitEthernet0/1

*mar. 1 03:45:54.481: IPv6 DHCP: detailed packet contents

*mar. 1 03:45:54.481: src FE80::205:5EFF:FE13:6C85 (GigabitEthernet0/1)

*mar. 1 03:45:54.481: dst FE80::1 (GigabitEthernet0/1)

*mar. 1 03:45:54.481: type REQUEST(3), xid 2

*mar. 1 03:45:54.481: option ELAPSED-TIME(8), len 6

*mar. 1 03:45:54.481: elapsed-time 0

*mar. 1 03:45:54.481: option SERVERID(2), len 24

*mar. 1 03:45:54.481: 000300010030A312AA01

*mar. 1 03:45:54.481: option CLIENTID(1), len 45

*mar. 1 03:45:54.481: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85
*mar. 1 03:45:54.481: option ORO(6), len 10
*mar. 1 03:45:54.481: IA-PD, DNS-SERVERS, DOMAIN-LIST
*mar. 1 03:45:54.481: option IA-PD(25), len 45
*mar. 1 03:45:54.481: IAID 0x24547, T1 0, T2 0
*mar. 1 03:45:54.481: option IAPREFIX(26), 29
*mar. 1 03:45:54.481: preferred 0, valid 0, prefix 0.0.0.0/0
*mar. 1 03:45:54.481: IPv6 DHCP: Using interface pool IPV6POOL-A
*mar. 1 03:45:54.481: IPv6 DHCP: Creating binding for FE80::205:5EFF:FE13:6C85 in pool
IPV6POOL-A
*mar. 1 03:45:54.481: IPv6 DHCP: Allocating IA_PD 24547 in binding for FE80::205:5EFF:FE13:6C85
*mar. 1 03:45:54.481: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for
FE80::205:5EFF:FE13:6C85, IAID 24547

*mar. 1 03:45:54.481: IPv6 DHCP: Sending REPLY to FE80::205:5EFF:FE13:6C85 on
GigabitEthernet0/1
*mar. 1 03:45:54.481: IPv6 DHCP: detailed packet contents
*mar. 1 03:45:54.481: src FE80::1 (GigabitEthernet0/1)
*mar. 1 03:45:54.481: dst FE80::205:5EFF:FE13:6C85 (GigabitEthernet0/1)
*mar. 1 03:45:54.481: type REPLY(7), xid 2
*mar. 1 03:45:54.481: option SERVERID(2), len 24
*mar. 1 03:45:54.481: 000300010030A312AA01
*mar. 1 03:45:54.481: option CLIENTID(1), len 45
*mar. 1 03:45:54.481: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85
*mar. 1 03:45:54.481: option IA-PD(25), len 41
*mar. 1 03:45:54.481: IAID 0x24547, T1 0, T2 0
*mar. 1 03:45:54.481: option IAPREFIX(26), 29
*mar. 1 03:45:54.481: preferred 0, valid 0, prefix 0.0.0.0/0
*mar. 1 03:45:54.481: option DNS-SERVERS(23), len 20
*mar. 1 03:45:54.481: 2001:DB8:ACAD:A::ABCD

*mar. 1 03:45:54.481: option DOMAIN-LIST(24), len 5
*mar. 1 03:45:54.481: ccna-StatefulDHCPv6.com

*mar. 1 03:46:15.230: IPv6 DHCP: Received SOLICIT from FE80::205:5EFF:FE13:6C85 on
GigabitEthernet0/1
*mar. 1 03:46:15.230: IPv6 DHCP: detailed packet contents
*mar. 1 03:46:15.230: src FE80::205:5EFF:FE13:6C85 (GigabitEthernet0/1)
*mar. 1 03:46:15.230: dst FF02::1:2 (GigabitEthernet0/1)
*mar. 1 03:46:15.230: type SOLICIT(1), xid 4
*mar. 1 03:46:15.230: option ELAPSED-TIME(8), len 6
*mar. 1 03:46:15.230: elapsed-time 0
*mar. 1 03:46:15.230: option CLIENTID(1), len 45
*mar. 1 03:46:15.230: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85
*mar. 1 03:46:15.230: option ORO(6), len 10
*mar. 1 03:46:15.230: IA-PD, DNS-SERVERS, DOMAIN-LIST
*mar. 1 03:46:15.230: option IA-PD(25), len 16
*mar. 1 03:46:15.230: IAID 0x24547, T1 0, T2 0

*mar. 1 03:46:15.230: IPv6 DHCP: Using interface pool IPV6POOL-A

*mar. 1 03:46:15.230: IPv6 DHCP: Sending ADVERTISE to FE80::205:5EFF:FE13:6C85 on GigabitEthernet0/1

*mar. 1 03:46:15.230: IPv6 DHCP: detailed packet contents

*mar. 1 03:46:15.230: src FE80::1 (GigabitEthernet0/1)

*mar. 1 03:46:15.230: dst FE80::205:5EFF:FE13:6C85 (GigabitEthernet0/1)

*mar. 1 03:46:15.230: type ADVERTISE(2), xid 4

*mar. 1 03:46:15.230: option SERVERID(2), len 24

*mar. 1 03:46:15.230: 000300010030A312AA01

*mar. 1 03:46:15.230: option CLIENTID(1), len 45

*mar. 1 03:46:15.230: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85

*mar. 1 03:46:15.230: option IA-PD(25), len 45

*mar. 1 03:46:15.230: IAID 0x24547, T1 0, T2 0

*mar. 1 03:46:15.230: option IAPREFIX(26), 29

*mar. 1 03:46:15.230: preferred 0, valid 0, prefix 0.0.0.0/0

*mar. 1 03:46:15.230: IPv6 DHCP: Received REQUEST from FE80::205:5EFF:FE13:6C85 on GigabitEthernet0/1

*mar. 1 03:46:15.230: IPv6 DHCP: detailed packet contents

*mar. 1 03:46:15.230: src FE80::205:5EFF:FE13:6C85 (GigabitEthernet0/1)

*mar. 1 03:46:15.230: dst FE80::1 (GigabitEthernet0/1)

*mar. 1 03:46:15.230: type REQUEST(3), xid 3

*mar. 1 03:46:15.230: option ELAPSED-TIME(8), len 6

*mar. 1 03:46:15.230: elapsed-time 0

*mar. 1 03:46:15.230: option SERVERID(2), len 24

*mar. 1 03:46:15.230: 000300010030A312AA01

*mar. 1 03:46:15.230: option CLIENTID(1), len 45

*mar. 1 03:46:15.230: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85

*mar. 1 03:46:15.230: option ORO(6), len 10

*mar. 1 03:46:15.230: IA-PD, DNS-SERVERS, DOMAIN-LIST

*mar. 1 03:46:15.230: option IA-PD(25), len 45

*mar. 1 03:46:15.230: IAID 0x24547, T1 0, T2 0

*mar. 1 03:46:15.230: option IAPREFIX(26), 29

*mar. 1 03:46:15.230: preferred 0, valid 0, prefix 0.0.0.0/0

*mar. 1 03:46:15.230: IPv6 DHCP: Using interface pool IPV6POOL-A

*mar. 1 03:46:15.230: IPv6 DHCP: Creating binding for FE80::205:5EFF:FE13:6C85 in pool IPV6POOL-A

*mar. 1 03:46:15.230: IPv6 DHCP: Allocating IA_PD 24547 in binding for FE80::205:5EFF:FE13:6C85

*mar. 1 03:46:15.230: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for FE80::205:5EFF:FE13:6C85, IAID 24547

*mar. 1 03:46:15.230: IPv6 DHCP: Sending REPLY to FE80::205:5EFF:FE13:6C85 on GigabitEthernet0/1

*mar. 1 03:46:15.230: IPv6 DHCP: detailed packet contents

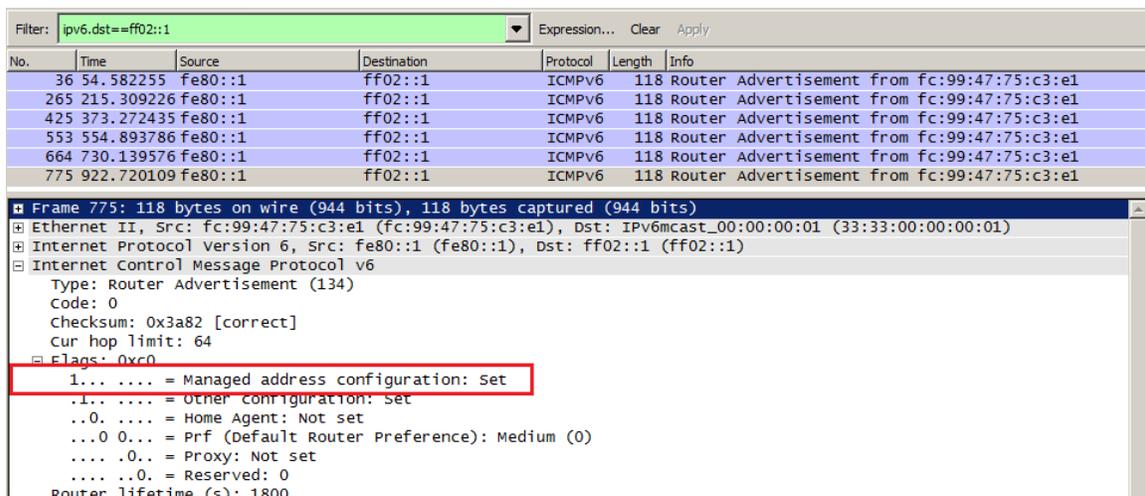
*mar. 1 03:46:15.230: src FE80::1 (GigabitEthernet0/1)

*mar. 1 03:46:15.230: dst FE80::205:5EFF:FE13:6C85 (GigabitEthernet0/1)

- *mar. 1 03:46:15.230: type REPLY(7), xid 3
- *mar. 1 03:46:15.230: option SERVERID(2), len 24
- *mar. 1 03:46:15.230: 000300010030A312AA01
- *mar. 1 03:46:15.230: option CLIENTID(1), len 45
- *mar. 1 03:46:15.230: 00-01-00-01-83-67-ED-85-00-05-5E-13-6C-85
- *mar. 1 03:46:15.230: option IA-PD(25), len 41
- *mar. 1 03:46:15.230: IAID 0x24547, T1 0, T2 0
- *mar. 1 03:46:15.230: option IAPREFIX(26), 29
- *mar. 1 03:46:15.230: preferred 0, valid 0, prefix 0.0.0.0/0
- *mar. 1 03:46:15.230: option DNS-SERVERS(23), len 20
- *mar. 1 03:46:15.230: 2001:DB8:ACAD:A::ABCD
- *mar. 1 03:46:15.230: option DOMAIN-LIST(24), len 5
- *mar. 1 03:46:15.230: ccna-StatefulDHCPv6.com

Step 6: 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.

No.	Time	Source	Destination	Protocol	Length	Info
250	443.078236	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
267	475.083284	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
425	656.281211	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0xc86c32 CID: 0001000117f6723d000c2
429	656.282249	fe80::1	fe80::d428:7de2:997ff02::1:2	DHCPv6	191	Advertise XID: 0xc86c32 CID: 0001000117f6723d000c2
460	657.292018	fe80::d428:7de2:997ff02::1:2		DHCPv6	188	Request XID: 0xc86c32 CID: 0001000117f6723d000c2
462	657.292638	fe80::1	fe80::d428:7de2:997ff02::1:2	DHCPv6	191	Reply XID: 0xc86c32 CID: 0001000117f6723d000c298

<input checked="" type="checkbox"/> Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: Vmware_be:6c:89 (00:50:56:be:6c:89)						
<input checked="" type="checkbox"/> Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)						
<input checked="" type="checkbox"/> User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)						
<input checked="" type="checkbox"/> DHCPv6						
Message type: Reply (7)						
Transaction ID: 0xc86c32						
<input checked="" type="checkbox"/> Server Identifier: 00030001fc994775c3e0						
<input checked="" type="checkbox"/> Client Identifier: 0001000117f6723d000c298d5444						
<input checked="" type="checkbox"/> Identity Association for Non-temporary Address						
Option: Identity Association for Non-temporary Address (3)						
Length: 40						
Value: 0e000c290000a8c000010e000005001820010db8acad000a...						
IAID: 0e000c29						
T1: 43200						
T2: 69120						
<input checked="" type="checkbox"/> IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce						
<input checked="" type="checkbox"/> DNS recursive name server						
Option: DNS recursive name server (23)						
Length: 16						
Value: 20010db8acad000a000000000000abcd						
<input checked="" type="checkbox"/> DNS servers address: 2001:db8:acad:a:abcd						
<input checked="" type="checkbox"/> Domain Search List						
Option: Domain Search List (24)						
Length: 25						
Value: 1363636e612d537461746566756c44484350763603636f6d...						
<input checked="" type="checkbox"/> DNS Domain Search List						
<input checked="" type="checkbox"/> Domain: ccna-StatefulDHCPv6.com						

Reflexión

- ¿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?

R/. _dhcp con estado requiere que el router guarde dinámicamente el estado de los clientes dhcpv6 y sin estado los clientes no usan el servidor dhcp para obtener las direcciones por eso no se guardan ¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado?

R/. Con estado

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?*

R. Desde mi punto de vista pienso que están utilizando el router Cisco 1941, porque este permite guardar la configuración de la red, es fácil de configurar, y tiene un buen manejo doméstico.

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. La pueden utilizar de manera que puedan expandir las conexiones disponibles, debido a que las direcciones Ipv4 estará siendo próximamente limitada y se tendrá que utilizar nuevos protocolos de conexión.

2. También la pueden utilizar porque permiten la confiabilidad de la información de su red, ganando seguridad en cada uno de los dispositivos que se usan en las empresas.

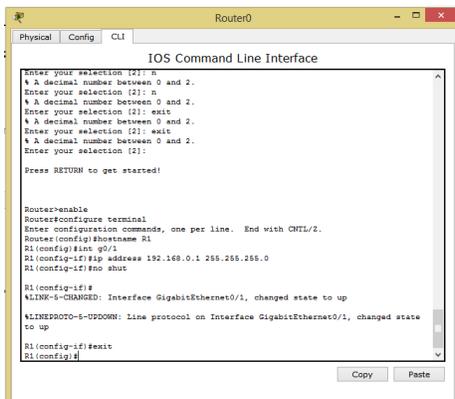
3. Permite la identificación posibles problemas que tengamos en la red de la empresa, un ejemplo claro puede ser, cuando: una tarjeta de red que está enviando paquetes continuamente y está provocando una saturación de la red local.

4. A la hora de conectarnos de forma remota en la red local a distintos dispositivos, pongamos el caso de una impresora, un disco duro de red, etc. donde mapear estos dispositivos en los equipos informáticos será mucho más sencillo si su dirección IP se mantiene invariable siempre.

5. De igual forma permite a las empresas que los routers hagan reservar determinadas direcciones para equipos concretos.

Configuración de práctica.

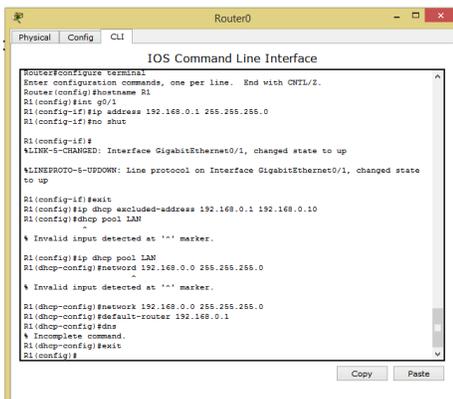
1. configuración de cambio de nombre del Router – R1
2. Configuración de la IPv4 o IPv6
3. Configuración de la puerta de enlace



```
Router0
Physical Config CLI
IOS Command Line Interface
Enter your selection [2]: n
  * A decimal number between 0 and 2.
Enter your selection [2]: n
  * A decimal number between 0 and 2.
Enter your selection [2]: exit
  * A decimal number between 0 and 2.
Enter your selection [2]: exit
  * A decimal number between 0 and 2.
Enter your selection [2]:
Press RETURN to get started!

Router>enable
Router>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/1
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut

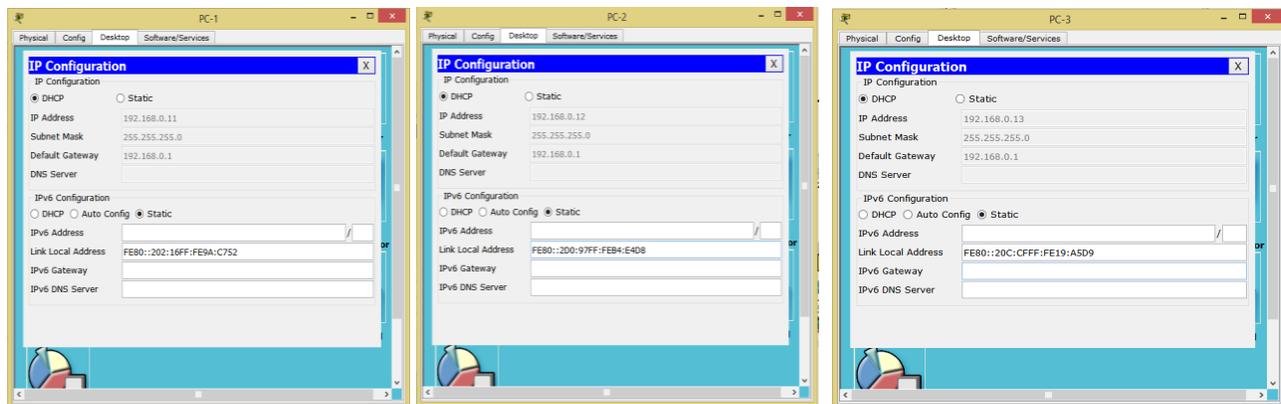
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)#exit
R1(config)#
```



```
Router0
Physical Config CLI
IOS Command Line Interface
Router>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/1
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut

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)#ip dhcp excluded-address 192.168.0.1 192.168.0.10
R1(config)#dhcp pool LAN
  * Invalid input detected at *** marker.
R1(config)#ip dhcp pool LAN
R1(dhcp-config)#network 192.168.0.0 255.255.255.0
  * Invalid input detected at *** marker.
R1(dhcp-config)#network 192.168.0.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.0.1
  * Incomplete command.
R1(dhcp-config)#exit
R1(config)#
```

4. Configuración de direcciones Ipv6 y DHCP



CONCLUSIONES

Puedo concluir de acuerdo a lo practicado e investigado que las configuraciones Ipv4 llegará un momento donde no tendran espacio (o numeros disponibles) para la configuracion de la demanda de equipos (o usuarios) conectados a la red, es por esto que se busca la alternativa de las direcciones Ipv6 se busca poder tener miles, millones de dispositivos, sensores y todo tipo de objetos conectado a la red, los cuales funcionaran de manera eficiente y eficaz. También puedo decir que con la IPv6 se busca gestionar todo tipo de redes, haciendo de estas un nuevo conjunto de redes que permitiran la optimizacion y racionalizacion de su uso, y po consecuente tener un uso adecuado de los recursos que nos ofrece la red (ahorro de energía); de igual forma se busca que los usuarios tengan mas seguridad a la hora de utilizar los formatos online, lo que nos indica que el usuario puede estar tranquilo cuando utilice estos servicios que le ofrece la red.

Por otra parte esta configuración nos permite ahorrar el tiempo facilitándonos la administración de las direcciones IP, puesto que él nos configurara automáticamente las direcciones IP necesarias, es decir, que elimina la intervención humana en las maquinas clientes. Las direcciones son controladas por el servidor, lo cual logra su facilitación al momento de dar seguimiento y supervisar. También beneficia en evitar los conflictos de direcciones que se producen al configurar un equipo nuevo en la red con una dirección IP ya asignada (que no se repita números de configuración IP).

PRACTICA DE LABORATORIO 11.2.2.6 LAB - CONFIGURING DYNAMIC AND STATIC NAT

Topología

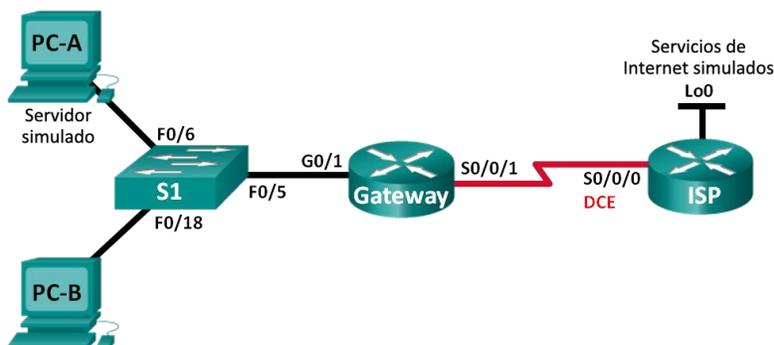


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	2.255.255.0	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
	G0/0	192.31.7.1	255.255.255.0	N/A
Servidor ISP	NIC	192.31.7.2	255.255.255.0	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 universal9). 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

Part 21: armar la red y verificar la conectividad

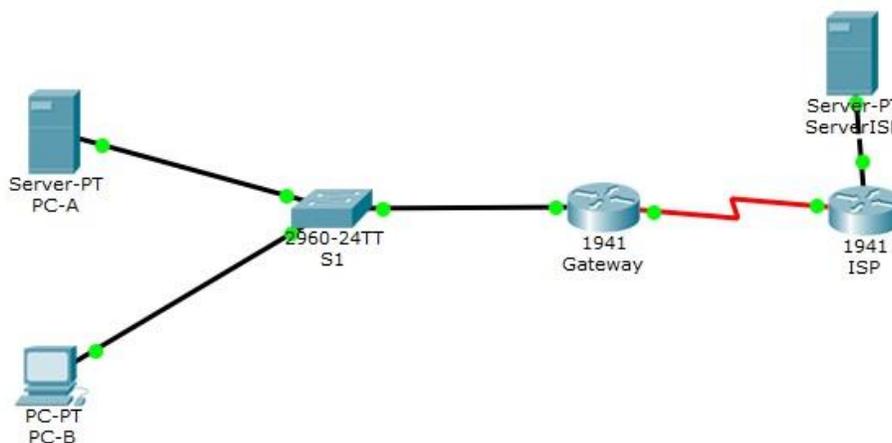
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

Step 1: 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.

R//

Se aclara que en la topología inicial hay como servidor simulado una pc, por ello se coloca directamente un servidor en la topología final. De igual forma en la Lo0 es un servidor simulado, por ello se coloca un servidor, debido a que en packet tracer no se puede habilitar el servidor web desde el router.



Step 2: configurar los equipos host.

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

Step 4: configurar los parámetros básicos para cada router.

- Desactive la búsqueda del DNS.
- Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

Step 5: crear un servidor web simulado en el ISP.

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

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

R// esto no se puede realizAr en packet tracer en el ISP.

- Habilite el servicio del servidor HTTP en el ISP.

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

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

```
ISP(config)# ip http authentication local
```

Step 6: configurar el routing estático.

- 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
```

```
ISP#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

- Cree una ruta predeterminada del router Gateway al router ISP.

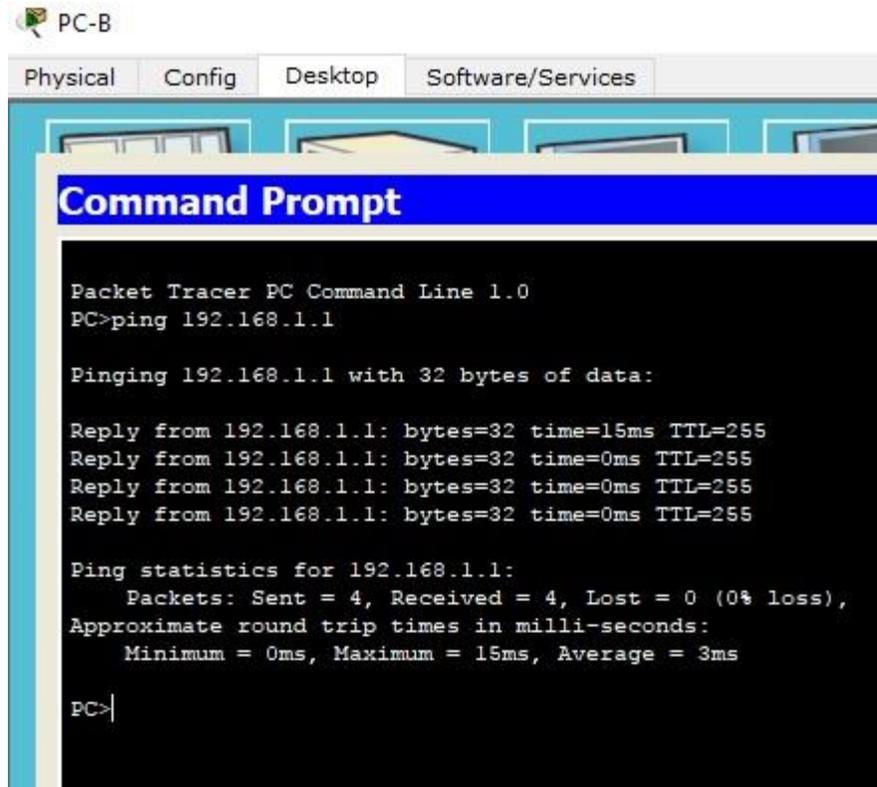
```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

```
Gateway>enable
Gateway#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Step 7: Guardar la configuración en ejecución en la configuración de inicio.

Step 8: Verificar la conectividad de la red

- 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.

Tabla de routing Gateway.

```

Gateway#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 209.165.201.17 to network 0.0.0.0

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/1
L       209.165.201.18/32 is directly connected, Serial0/0/1
S*    0.0.0.0/0 [1/0] via 209.165.201.17

```

Tabla de routing ISP.

```

ISP>enabl
ISP#show ip rout
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

    192.31.7.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.31.7.0/24 is directly connected, GigabitEthernet0/0
L       192.31.7.1/32 is directly connected, GigabitEthernet0/0
    209.165.200.0/27 is subnetted, 1 subnets
S       209.165.200.224/27 [1/0] via 209.165.201.18
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/0
L       209.165.201.17/32 is directly connected, Serial0/0/0

```

Part 22: 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 1: 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
```

```

Gateway>ena
Gateway#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#ip nat inside source static 192.168.1.20 209.165.200.225
Gateway(config)#

```

Step 2: 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

```

```

Gateway(config)#interface g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface s0/0/1
Gateway(config-if)#ip nat outside
Gateway(config-if)#

```

Step 3: 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     ---               ---
```

```
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?

R// el router, que a su vez es asignada por El proveedor de Internet.

¿Quién asigna la dirección local interna?

R//El administrador de red.

- 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.

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
SERVER>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 192.31.7.2: bytes=32 time=2ms TTL=126
Reply from 192.31.7.2: bytes=32 time=1ms TTL=126
Reply from 192.31.7.2: bytes=32 time=1ms TTL=126
Reply from 192.31.7.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 3ms
```

```
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     ---               ---
```

```

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   192.31.7.2:1     192.31.7.2:1
icmp 209.165.200.225:2 192.168.1.20:2   192.31.7.2:2     192.31.7.2:2
icmp 209.165.200.225:3 192.168.1.20:3   192.31.7.2:3     192.31.7.2:3
icmp 209.165.200.225:4 192.168.1.20:4   192.31.7.2:4     192.31.7.2:4
icmp 209.165.200.225:5 192.168.1.20:5   192.31.7.1:5     192.31.7.1:5
icmp 209.165.200.225:6 192.168.1.20:6   192.31.7.1:6     192.31.7.1:6
icmp 209.165.200.225:7 192.168.1.20:7   192.31.7.1:7     192.31.7.1:7
icmp 209.165.200.225:8 192.168.1.20:8   192.31.7.1:8     192.31.7.1:8
--- 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? R// el número de puertos varia.

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     ---               ---

```

R// en este punto se hace directamente es mirar desde la PC-A una página que tiene el Servidor ISP.

Configuración del mensaje en el servidor ISP.

ServerISP

Physical Config Services Desktop Software/Services

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

File Name: index.html

```

<html>
<center><font size='+2' color='blue'>Cisco Packet
Tracer</font></center>
<hr>Bienvenido al Servidor ISP. Opening doors to new
opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>

```

Visualización del mensaje en PC-A



Tabla

```

Gateway>ena
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225     192.168.1.20      ---                ---
tcp 209.165.200.225:1025 192.168.1.20:1025 192.31.7.2:80     192.31.7.2:80
tcp 209.165.200.225:1026 192.168.1.20:1026 192.31.7.2:80     192.31.7.2:80
tcp 209.165.200.225:1027 192.168.1.20:1027 192.31.7.2:80     192.31.7.2:80

```

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?

R// para el ejemplo de la guía como es por Telnet el puerto será el 23. Sin embargo para este caso se utilizó el WEB

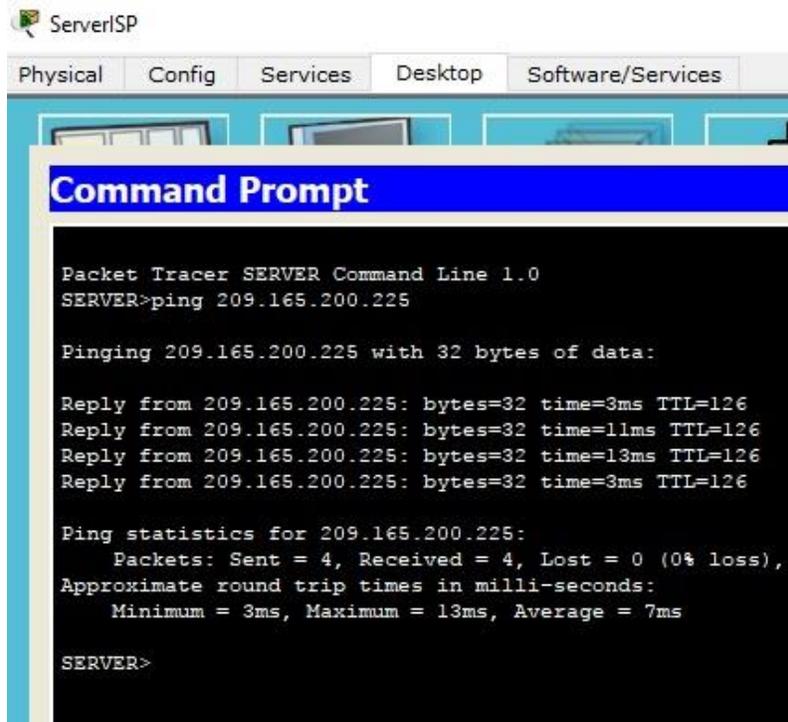
¿Cuáles son los números de puerto que se usaron?

Global/local interno: R// para el ejemplo de la guía es el puerto:1034. Sin embargo para la práctica es el :1025(varia)

Global/local externo: R// para el ejemplo de la guía es el puerto :23. Sin embargo para la práctica es el :80

- 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.

Ping servidor ISP a PC-A



Ping Router ISP a PC-A

```

ISP#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 = 1/1/1 ms

```

- 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 statistics
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
```

```
Gateway#show ip nat statistics
Total translations: 5 (1 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 44 Misses: 21
Expired translations: 17
Dynamic mappings:
Gateway#
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Part 23: 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 1: 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
```

```
Gateway#show ip nat translation
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.200.225     192.168.1.20     ---                ---
~ . . . !
```

Step 2: 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 3: 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 4: 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
```

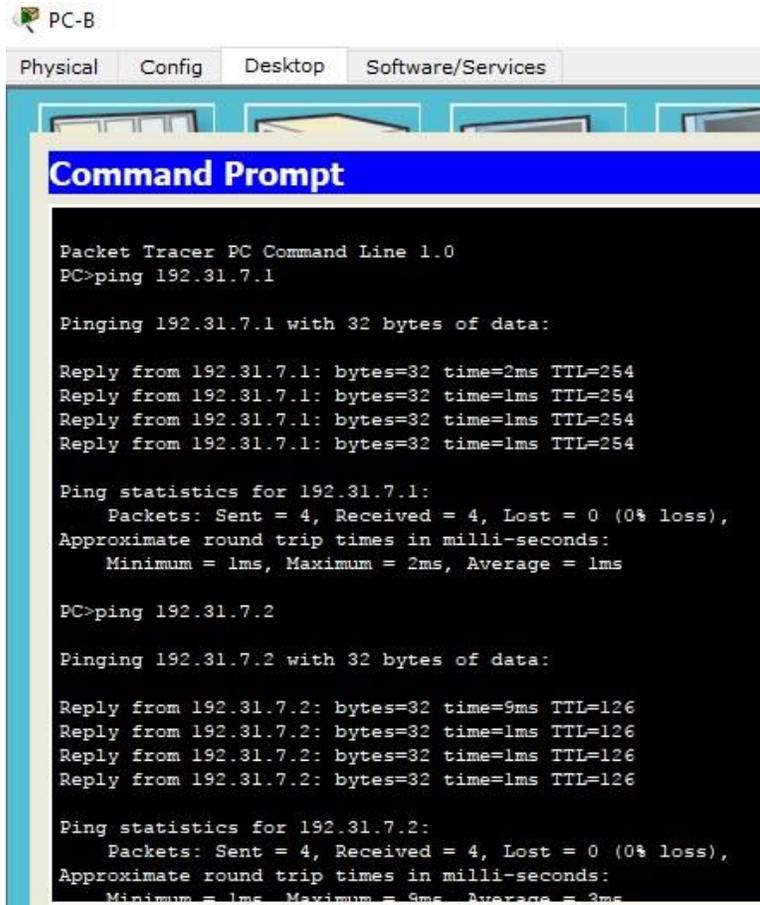
Step 5: definir la NAT desde la lista de origen interna hasta el conjunto externo.

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 6: probar la configuración.

- 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.



```
PC-B
Physical Config Desktop Software/Services

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 192.31.7.2: bytes=32 time=9ms TTL=126
Reply from 192.31.7.2: bytes=32 time=1ms TTL=126
Reply from 192.31.7.2: bytes=32 time=1ms TTL=126
Reply from 192.31.7.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 3ms
```

```
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	---	---

```
Gateway#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.242:10	192.168.1.21:10	192.31.7.2:10	192.31.7.2:10
icmp	209.165.200.242:11	192.168.1.21:11	192.31.7.2:11	192.31.7.2:11
icmp	209.165.200.242:12	192.168.1.21:12	192.31.7.2:12	192.31.7.2:12
icmp	209.165.200.242:9	192.168.1.21:9	192.31.7.2:9	192.31.7.2:9
---	209.165.200.225	192.168.1.20	---	---

¿Cuál es la traducción de la dirección host local interna de la PC-B?

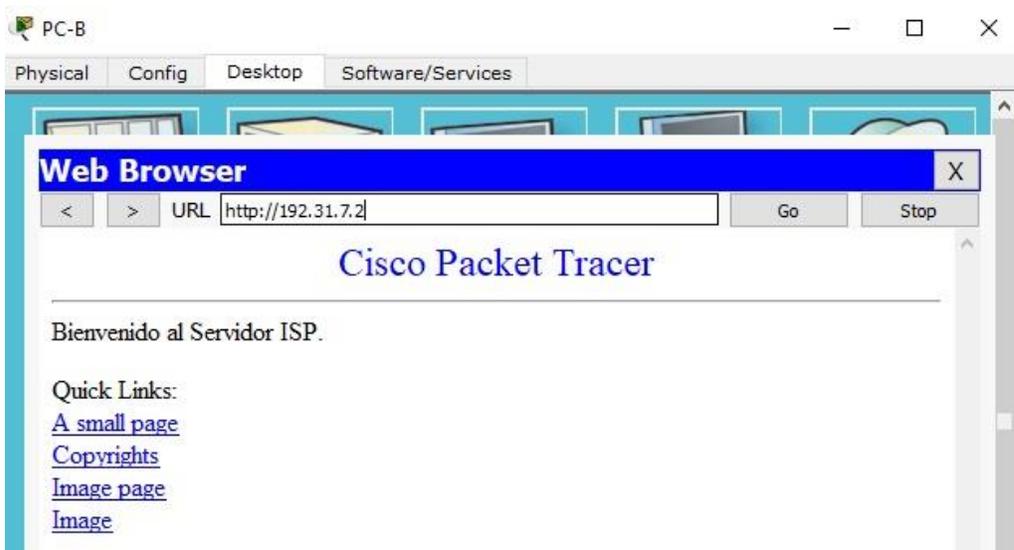
192.168.1.21 = 209.165.200.242

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?

R// 10,11,12 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     ---               ---
Gateway>enab
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.200.225    192.168.1.20     ---               ---
tcp 209.165.200.242:1025 192.168.1.21:1025 192.31.7.2:80    192.31.7.2:80
```

¿Qué protocolo se usó en esta traducción?

R/. tcp

¿Qué números de puerto se usaron?

R/.Interno: 1025

Externo: 80

¿Qué número de puerto bien conocido y qué servicio se usaron?

R/.80, 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
```

```
Gateway#show ip nat statistics
```

```
Total translations: 2 (1 static, 1 dynamic, 1 extended)
```

```
Outside Interfaces: Serial0/0/1
```

```
Inside Interfaces: GigabitEthernet0/1
```

```
Hits: 63 Misses: 34
```

```
Expired translations: 29
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
access-list 1 pool public_access refCount 1
```

```
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
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Step 7: 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.

```
Gateway#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 63 Misses: 34
Expired translations: 29
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
 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
Gateway#
```

- c. Haga ping al ISP (192.31.7.1) desde ambos hosts.

```
PC>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 192.31.7.2: bytes=32 time=7ms TTL=126
Reply from 192.31.7.2: bytes=32 time=11ms TTL=126
Reply from 192.31.7.2: bytes=32 time=10ms TTL=126
Reply from 192.31.7.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 11ms, Average = 9ms
```

```
SERVER>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 192.31.7.2: bytes=32 time=1ms TTL=126
Reply from 192.31.7.2: bytes=32 time=10ms TTL=126
Reply from 192.31.7.2: bytes=32 time=11ms TTL=126
Reply from 192.31.7.2: bytes=32 time=24ms TTL=126

Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 24ms, Average = 11ms
```

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

- 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	---	---

Gateway#show ip nat statistics

```

Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 75 Misses: 46
Expired translations: 41
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
  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

```

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?

R// 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?

R// 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

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.

PRACTICA DE LABORATORIO 11.2.3.7 LAB - CONFIGURING NAT POOL OVERLOAD AND PAT

Topología

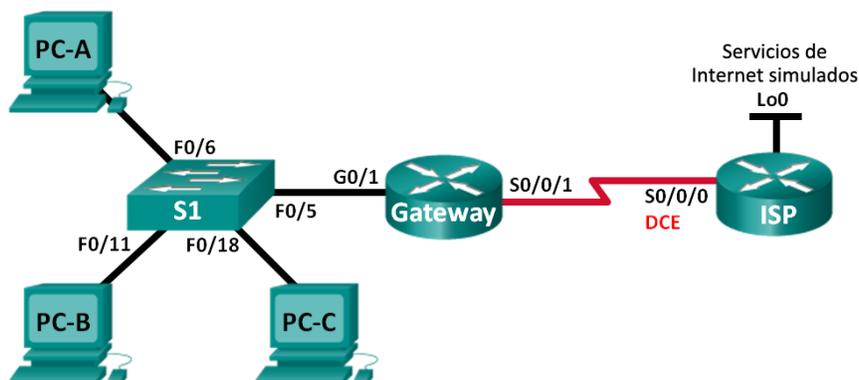


Tabla de direccionamiento

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.

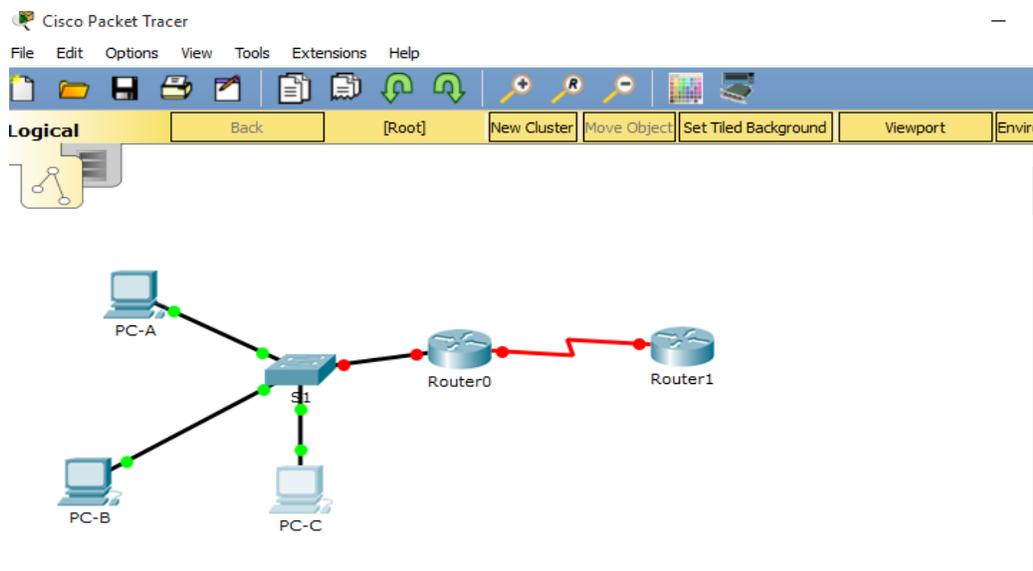
Recursos necesarios

- 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

Part 24: armar la red y verificar la conectividad

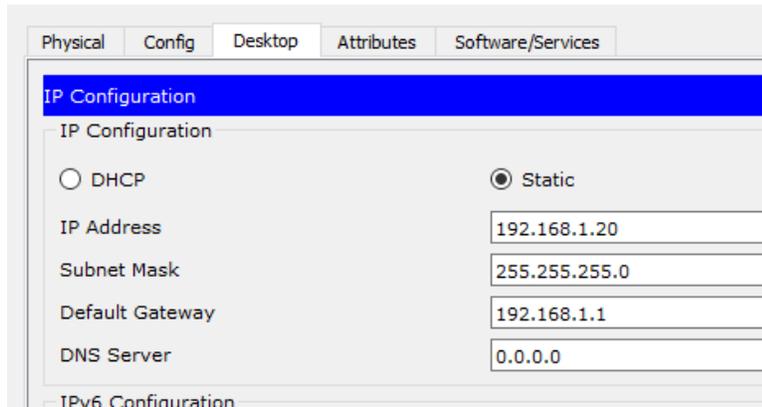
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

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



Step 2: configurar los equipos host.

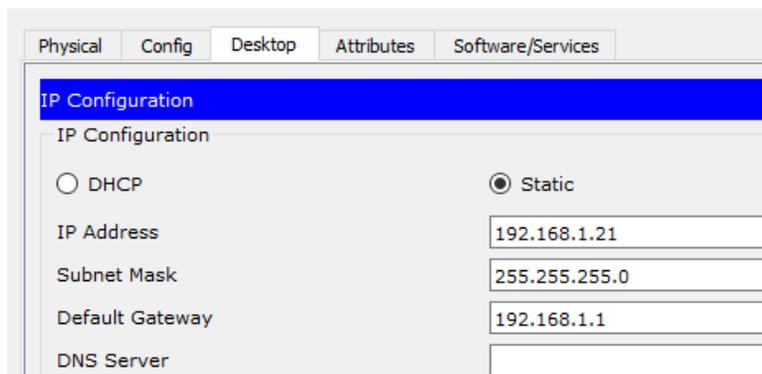
PC-A



The screenshot shows the IP Configuration window for PC-A. The 'Config' tab is selected. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IP Address	192.168.1.20
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

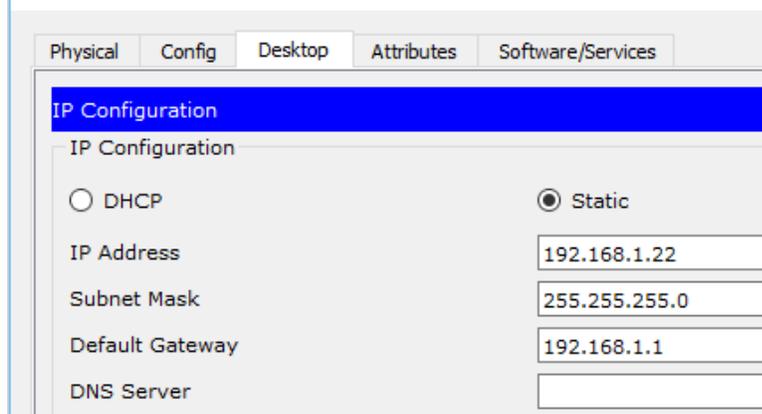
PC-B



The screenshot shows the IP Configuration window for PC-B. The 'Config' tab is selected. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IP Address	192.168.1.21
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	

PC-C



The screenshot shows the IP Configuration window for PC-C. The 'Config' tab is selected. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IP Address	192.168.1.22
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	

Step 3: inicializar y volver a cargar los routers y los switches.

Step 4: configurar los parámetros básicos para cada router.

```
Press RETURN to get started!

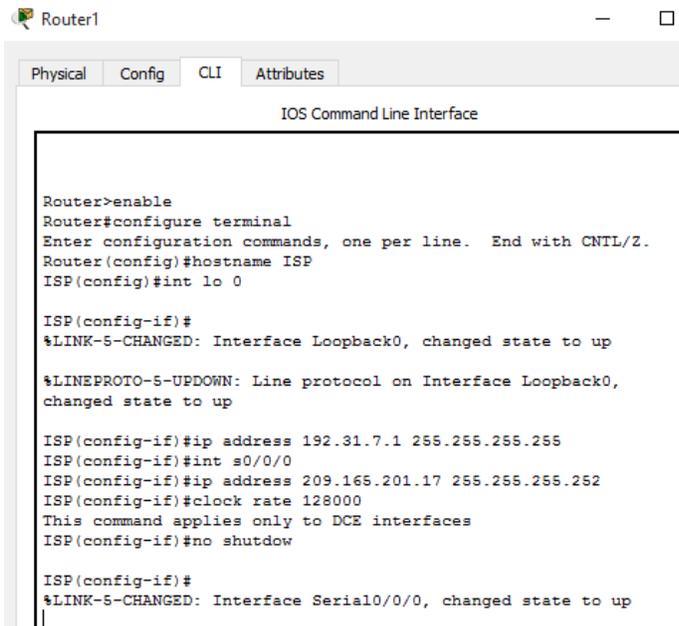
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname gateway
gateway(config)#int g0/1
gateway(config-if)#ip address 192.168.1.1 255.255.255.0
gateway(config-if)#no shutdown

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)#int s0/0/1
gateway(config-if)#ip address 209.165.201.18 255.255.255.252
gateway(config-if)#no shutdown

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



The screenshot shows a Cisco IOS CLI window titled "Router1" with tabs for Physical, Config, CLI, and Attributes. The CLI window displays the following configuration commands and their outputs:

```
Router1>enable
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#hostname ISP
ISP1(config)#int lo 0

ISP1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up

ISP1(config-if)#ip address 192.31.7.1 255.255.255.255
ISP1(config-if)#int s0/0/0
ISP1(config-if)#ip address 209.165.201.17 255.255.255.252
ISP1(config-if)#clock rate 128000
This command applies only to DCE interfaces
ISP1(config-if)#no shutdow

ISP1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

- Desactive la búsqueda del DNS.
- Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

Step 5: 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
```

```
ISP(config-if)#exit
ISP(config)#ip route 209.165.200.224 255.255.255.248
209.165.201.18
ISP(config)#
```

- b. Cree una ruta predeterminada del router Gateway al router ISP.

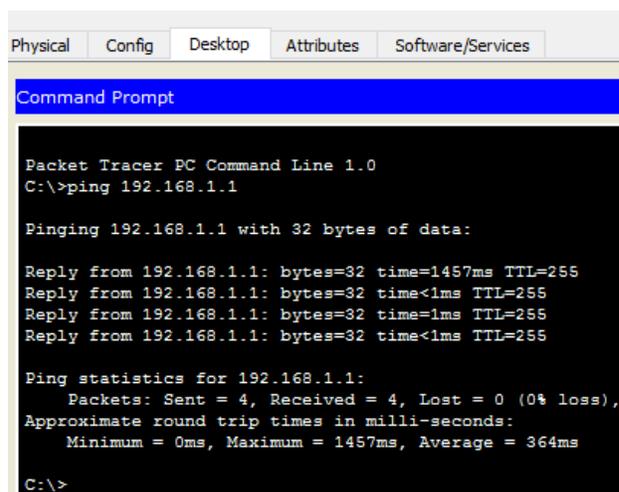
```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

```
gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
gateway(config)#
```

Step 6: 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.

PC-A



```
Physical Config Desktop Attributes Software/Services
Command Prompt

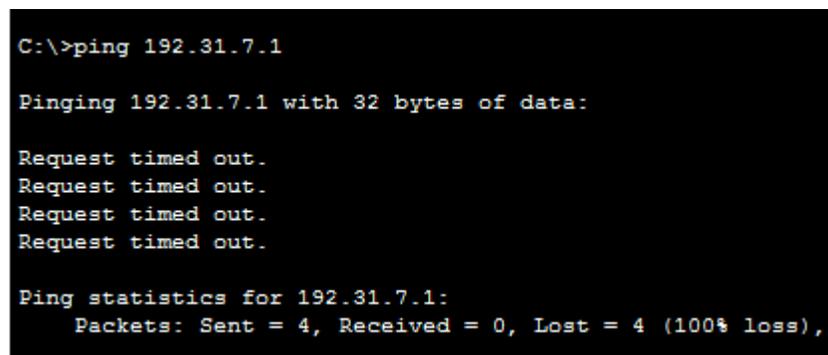
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1457ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1457ms, Average = 364ms

C:\>
```



```
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.

Part 25: 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 1: 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 2: 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 3: 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 4: 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 5: 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.

```
C:\>ping 192.31.7.1  
  
Pinging 192.31.7.1 with 32 bytes of data:  
  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 192.31.7.1:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>ping 192.31.7.1  
  
Pinging 192.31.7.1 with 32 bytes of data:  
  
Reply from 192.31.7.1: bytes=32 time=62ms TTL=254  
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254  
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254  
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254  
  
Ping statistics for 192.31.7.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 62ms, Average = 16ms
```

PC-B

```
Physical  Config  Desktop  Attributes  Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

PC-C

```
Physical  Config  Desktop  Attributes  Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Step 6:

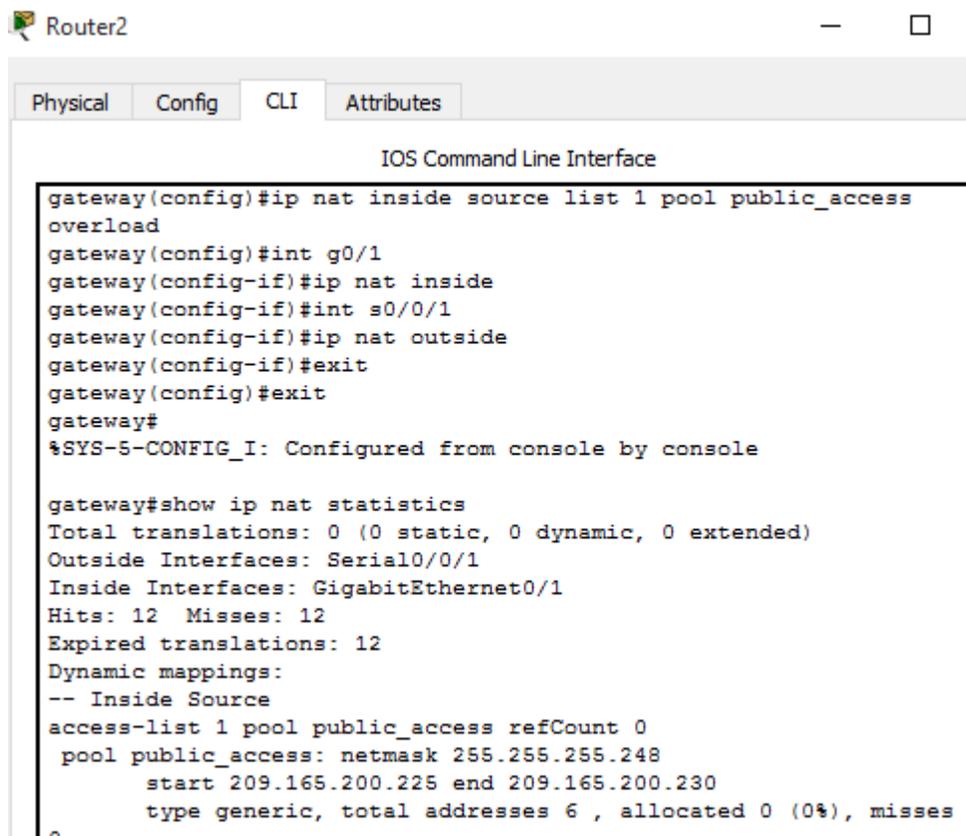
- a. Muestre las estadísticas de NAT en el router Gateway.

```
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
```



The screenshot shows a terminal window titled "Router2" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The user has entered several commands to configure NAT and view statistics. The output shows the configuration of an access-list and a NAT pool, followed by the execution of "show ip nat statistics" which displays the current state of NAT translations and mappings.

```
gateway(config)#ip nat inside source list 1 pool public_access
overload
gateway(config)#int g0/1
gateway(config-if)#ip nat inside
gateway(config-if)#int s0/0/1
gateway(config-if)#ip nat outside
gateway(config-if)#exit
gateway(config)#exit
gateway#
%SYS-5-CONFIG_I: Configured from console by console

gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12 Misses: 12
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
  pool public_access: netmask 255.255.255.248
    start 209.165.200.225 end 209.165.200.230
    type generic, total addresses 6 , allocated 0 (0%), misses
```

b. 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? _____12_____

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

```
ISP>ping 192.168.1.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2
seconds:
```

Porque Gracias a la configuración nat ISP solo va a reconocer la ip de Gateway y no lo permite reconocer las direcciones de los host internos.

Part 26: 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 1: borrar las NAT y las estadísticas en el router Gateway.

Step 2: verificar la configuración para NAT.

- Verifique que se hayan borrado las estadísticas.

```
gateway#show ip nat translations
gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
   start 209.165.200.225 end 209.165.200.230
   type generic, total addresses 6 , allocated 0 (0%), misses
0
gateway#
```

- Verifique que las interfaces externa e interna estén configuradas para NAT.
- Verifique que la ACL aún esté configurada para NAT.

```
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
   start 209.165.200.225 end 209.165.200.230
```

¿Qué comando usó para confirmar los resultados de los pasos a al c?

Step 3: 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 4: 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

gateway>enable
gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)#no ip nat pool public_access 209.165.200.225
209.165.200.230 netmask 255.255.255.248
%Pool public_access in use, cannot destroy
gateway(config)#no ip nat inside source list 1 pool public_access
overload
gateway(config)#no ip nat pool public_access 209.165.200.225
209.165.200.230 netmask 255.255.255.248
gateway(config)#
```

Step 5: asociar la lista de origen a la interfaz externa.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload

gateway(config)#ip nat inside source list 1 interface serial
0/0/1 overload
gateway(config)#show ip nat statistics
^
% Invalid input detected at '^' marker.

gateway(config)#exit
gateway#
%SYS-5-CONFIG_I: Configured from console by console

gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 0 Misses: 4
Expired translations: 0
Dynamic mappings:
gateway#
```

Step 6: probar la configuración PAT.

- Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.
- 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
```

```
gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 0 Misses: 4
Expired translations: 0
Dynamic mappings:
gateway#
```

```
gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12 Misses: 16
Expired translations: 12
Dynamic mappings:
gateway#
```

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
192.31.7.1:1024				
icmp	209.165.201.18:1025	192.168.1.21:2	192.31.7.1:2	
192.31.7.1:1025				
icmp	209.165.201.18:1026	192.168.1.21:3	192.31.7.1:3	
192.31.7.1:1026				
icmp	209.165.201.18:1027	192.168.1.21:4	192.31.7.1:4	
192.31.7.1:1027				
icmp	209.165.201.18:1028	192.168.1.22:1	192.31.7.1:1	
192.31.7.1:1028				
icmp	209.165.201.18:1029	192.168.1.22:2	192.31.7.1:2	
192.31.7.1:1029				
icmp	209.165.201.18:1030	192.168.1.22:3	192.31.7.1:3	
192.31.7.1:1030				
icmp	209.165.201.18:1031	192.168.1.22:4	192.31.7.1:4	
192.31.7.1:1031				
icmp	209.165.201.18:1	192.168.1.20:1	192.31.7.1:1	
192.31.7.1:1				
icmp	209.165.201.18:2	192.168.1.20:2	192.31.7.1:2	
192.31.7.1:2				
icmp	209.165.201.18:3	192.168.1.20:3	192.31.7.1:3	
192.31.7.1:3				
icmp	209.165.201.18:4	192.168.1.20:4	192.31.7.1:4	
192.31.7.1:4				

```
gateway#
```

Reflexión

¿Qué ventajas tiene la PAT?

R/. Se ahorran las direcciones Ip públicas utilizando una interface con una sola ip pública por medio de diferentes puertos para los paquetes además de proveer seguridad.

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.

PRACTICA DE LABORATORIO 9.2.1.10: PACKET TRACER CONFIGURING STANDARD ACLS

Topología

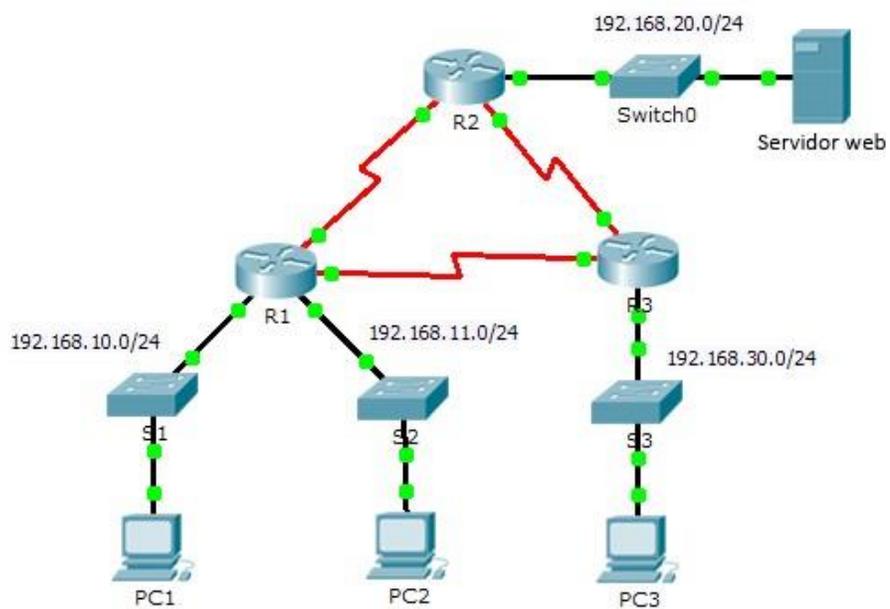


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
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

Objetivos

Parte 1: planificar una implementación de ACL

Parte 2: configurar, aplicar y verificar una ACL estándar

Información básica/situación

Las listas de control de acceso (ACL) estándar son scripts de configuración del router que controlan si un router permite o deniega paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, incluidas las direcciones IP y el routing del protocolo de routing de gateway interior mejorado (EIGRP).

Parte 1: planificar una implementación de ACL

Paso 1: investigar la configuración actual de red.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tenga conectividad completa. Elija una computadora y haga ping a otros dispositivos en la red para verificar que la red tenga plena conectividad. Debería poder hacer ping correctamente a todos los dispositivos

Paso 2: evaluar dos políticas de red y planificar las implementaciones de ACL.

a. En el **R2** están implementadas las siguientes políticas de red:

- La red 192.168.11.0/24 no tiene permiso para acceder al **servidor web** en la red 192.168.20.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.11.0/24 al **servidor web** en 192.168.20.254 sin interferir con otro tráfico, se debe crear una ACL en el **R2**. La lista de acceso se debe colocar en la interfaz de salida hacia el **servidor web**. Se debe crear una segunda regla en el **R2** para permitir el resto del tráfico.

b. En el **R3** están implementadas las siguientes políticas de red:

- La red 192.168.10.0/24 no tiene permiso para comunicarse con la red 192.168.30.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.10.0/24 a la red 192.168.30.0/24 sin interferir con otro tráfico, se debe crear una lista de acceso en el **R3**. La ACL se debe colocar en la interfaz de salida hacia la **PC3**.

Se debe crear una segunda regla en el **R3** para permitir el resto del tráfico.

Parte 2: configurar, aplicar y verificar una ACL estándar

Paso 1: configurar y aplicar una ACL estándar numerada en el R2.

a. Cree una ACL con el número 1 en el **R2** con una instrucción que deniegue el acceso a la red 192.168.20.0/24 desde la red 192.168.11.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

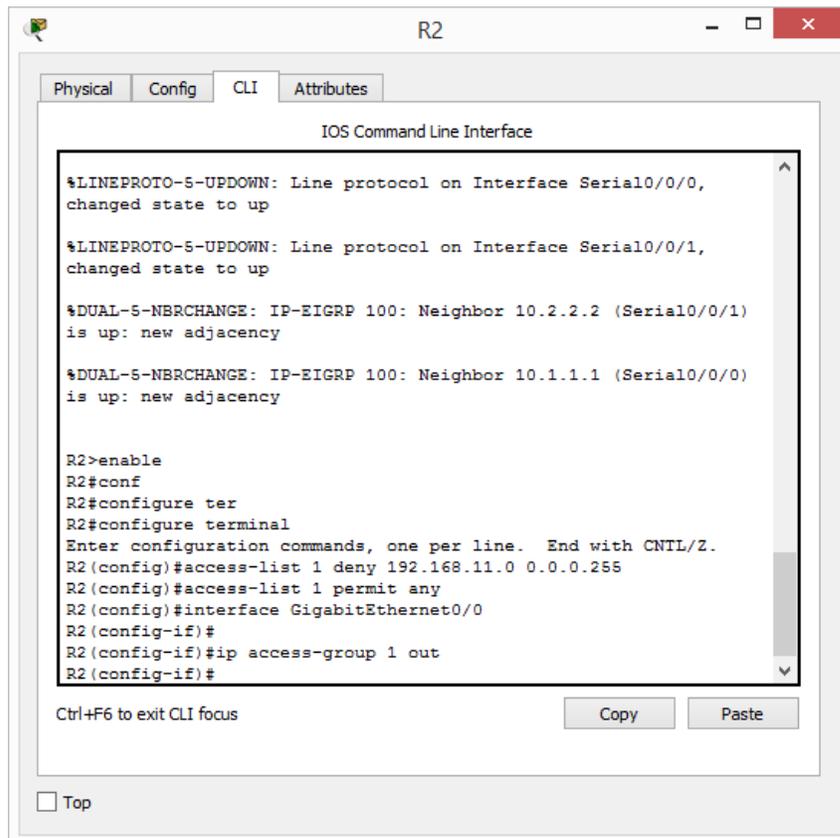
b. De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con una regla. Para permitir el resto del tráfico, configure la siguiente instrucción:

```
R2(config)# access-list 1 permit any
```

- c. Para que la ACL realmente filtre el tráfico, se debe aplicar a alguna operación del router. Para aplicar la ACL, colóquela en la interfaz Gigabit Ethernet 0/0 para el tráfico saliente.

```
R2 (config) # interface  
GigabitEthernet0/0
```

```
R2 (config-if) # ip access-group 1  
out
```



Paso 2: configurar y aplicar una ACL estándar numerada en el R3.

- a. Cree una ACL con el número 1 en el R3 con una instrucción que deniegue el acceso a la red 192.168.30.0/24 desde la red de la PC1 (192.168.10.0/24).

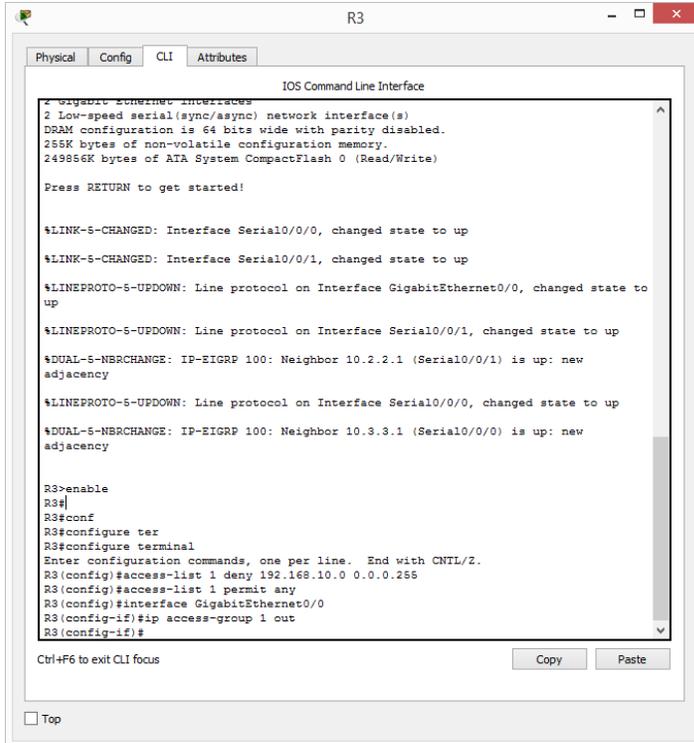
```
R3 (config) # access-list 1 deny 192.168.10.0 0.0.0.255
```

- b. De manera predeterminada, las ACL deniegan todo el tráfico que no coincide con una regla. Para permitir el resto del tráfico, cree una segunda regla para la ACL 1.

```
R3 (config) # access-list 1 permit  
any
```

- c. Para aplicar la ACL, colóquela en la interfaz Gigabit Ethernet 0/0 para el tráfico saliente.

```
R3 (config) # interface  
GigabitEthernet0/0  
  
R3 (config-if) # ip access-group 1  
out
```



Paso 3: verificar la configuración y la funcionalidad de la ACL.

a. En el **R2** y el **R3**, introduzca el comando **show access-list** para verificar las configuraciones de la ACL.

Introduzca el comando **show run** o **show ip interface gigabitethernet 0/0** para verificar la colocación de las ACL.

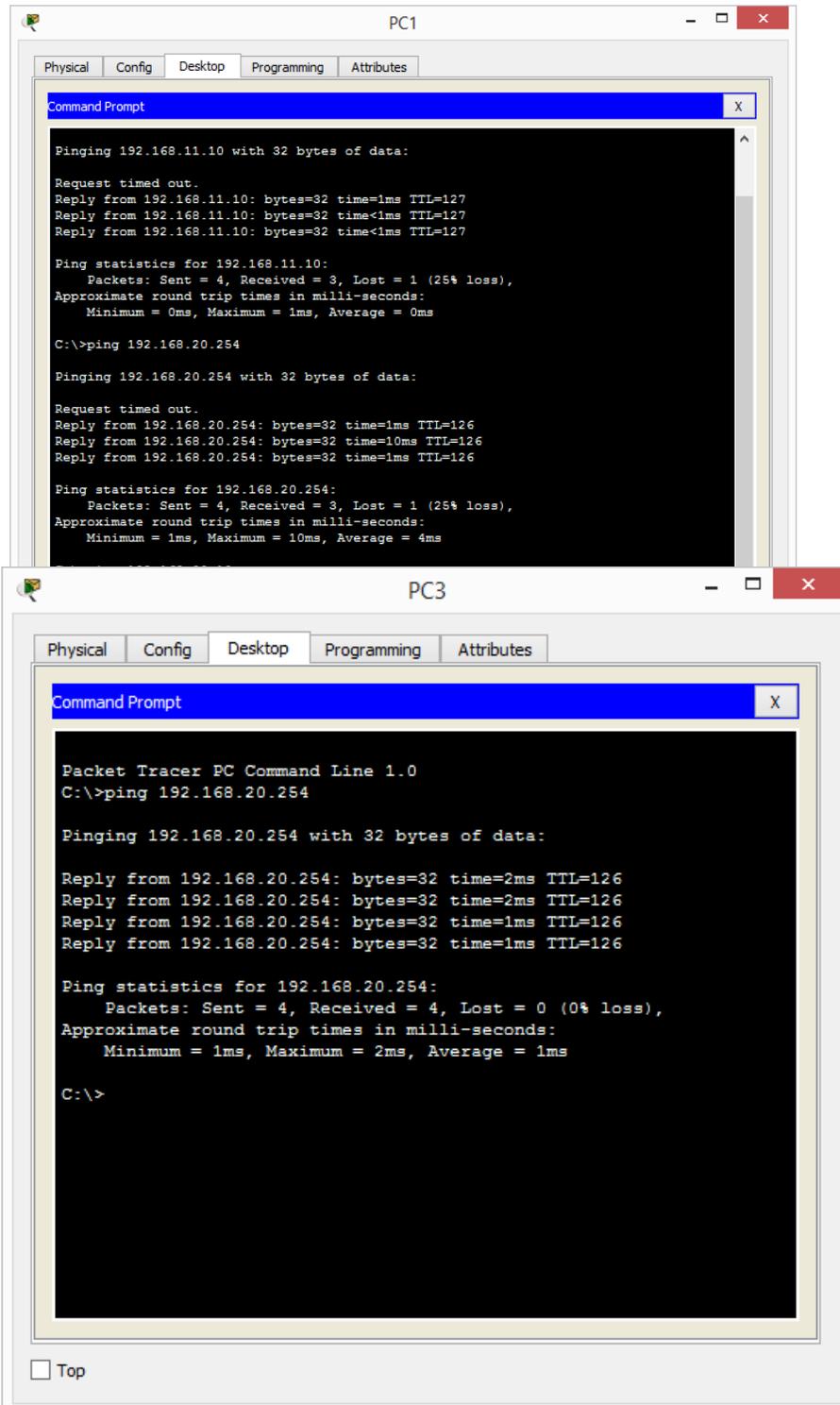
```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config)#show access-list
% Invalid input detected at '^' marker.
R3(config)#exit
R3#
#SYS-5-CONFIG_I: Configured from console by console
enable
R3#show access-list
Standard IP access list 1
 10 deny 192.168.10.0 0.0.0.255
 20 permit any
R3#show ip interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
 Internet address is 192.168.30.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is 1
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
--More--
Ctrl+F6 to exit CLI focus
Copy Paste
 Top
```

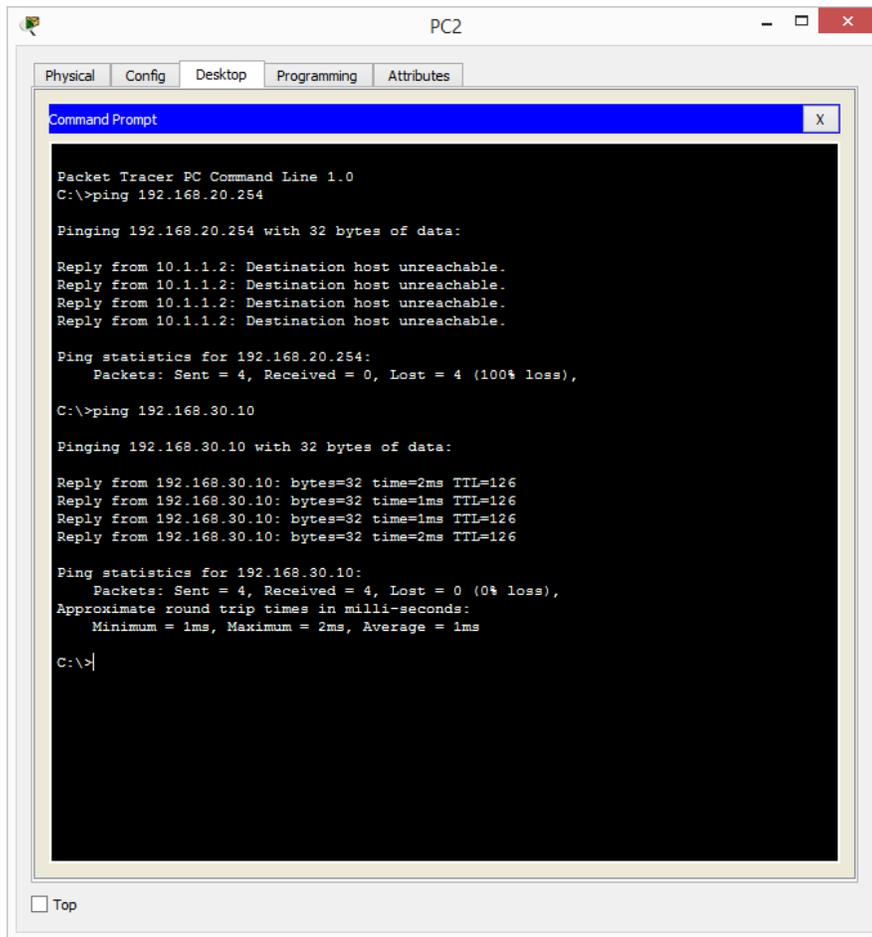
```
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2#show access-list
Standard IP access list 1
 10 deny 192.168.11.0 0.0.0.255
 20 permit any
R2#show ip interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
 Internet address is 192.168.20.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is 1
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
 IP output packet accounting is disabled
 IP access violation accounting is disabled
 TCP/IP header compression is disabled
 RTP/IP header compression is disabled
 Probe proxy name replies are disabled
 Policy routing is disabled
 Network address translation is disabled
 BGP Policy Mapping is disabled
--More--
Ctrl+F6 to exit CLI focus
Copy Paste
 Top
```

b. Una vez colocadas las dos ACL, el tráfico de la red se restringe según las políticas detalladas en la parte 1. Utilice las siguientes pruebas para verificar las implementaciones de ACL:

- Un ping de 192.168.10.10 a 192.168.11.10 se realiza correctamente.

- Un ping de 192.168.10.10 a 192.168.20.254 se realiza correctamente.
- Un ping de 192.168.11.10 a 192.168.20.254 falla.
- Un ping de 192.168.10.10 a 192.168.30.10 falla.
- Un ping de 192.168.11.10 a 192.168.30.10 se realiza correctamente.
- Un ping de 192.168.30.10 a 192.168.20.254 se realiza correctamente.





- **Configuration de router 2 y router 3**

Router 2 Configuration

```
R2>en
R2#conf t
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#int g0/0

R2(config-if)#ip access-group 1 out
```

Router 3 Configuration

```
R3>en
R3#conf t
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#int g0/0

R3(config-if)#ip access-group 1 out
```

PRACTICA DE LABORATORIO 9.2.1.11:PACKET TRACER - CONFIGURING NAMED STANDARD ACLS

Topología

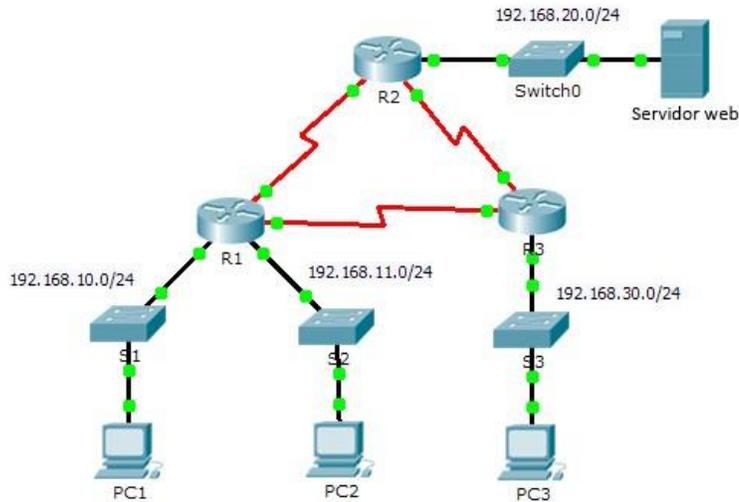


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
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

Objetivos

Parte 1: planificar una implementación de ACL

Parte 2: configurar, aplicar y verificar una ACL estándar

Información básica/situación

Las listas de control de acceso (ACL) estándar son scripts de configuración del router que controlan si un router permite o deniega paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, incluidas las direcciones IP y el routing del protocolo de routing de gateway interior mejorado (EIGRP).

Parte 1: planificar una implementación de ACL

Paso 1: investigar la configuración actual de red.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tenga conectividad completa. Elija una computadora y haga ping a otros dispositivos en la red para verificar que la red tenga plena conectividad. Debería poder hacer ping correctamente a todos los dispositivos.

Paso 2: evaluar dos políticas de red y planificar las implementaciones de ACL.

a. En el **R2** están implementadas las siguientes políticas de red:

- La red 192.168.11.0/24 no tiene permiso para acceder al **servidor web** en la red 192.168.20.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.11.0/24 al **servidor web** en 192.168.20.254 sin interferir con otro tráfico, se debe crear una ACL en el **R2**. La lista de acceso se debe colocar en la interfaz de salida hacia el **servidor web**. Se debe crear una segunda regla en el **R2** para permitir el resto del tráfico.

b. En el **R3** están implementadas las siguientes políticas de red:

- La red 192.168.10.0/24 no tiene permiso para comunicarse con la red 192.168.30.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.10.0/24 a la red 192.168.30.0/24 sin interferir con otro tráfico, se debe crear una lista de acceso en el **R3**. La ACL se debe colocar en la interfaz de salida hacia la **PC3**.

Se debe crear una segunda regla en el **R3** para permitir el resto del tráfico.

Parte 2: configurar, aplicar y verificar una ACL estándar

Paso 1: configurar y aplicar una ACL estándar numerada en el R2.

a. Cree una ACL con el número 1 en el **R2** con una instrucción que deniegue el acceso a la red

192.168.20.0/24 desde la red 192.168.11.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0  
0.0.0.255
```

- b. De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con una regla.

Para permitir el resto del tráfico, configure la siguiente instrucción:

```
R2(config)# access-list 1 permit any
```

- c. Para que la ACL realmente filtre el tráfico, se debe aplicar a alguna operación del router. Para aplicar la

ACL, colóquela en la interfaz Gigabit Ethernet 0/0 para el tráfico saliente.

```
R2(config)# interface GigabitEthernet0/0
```

```
R2(config-if)# ip access-group 1 out
```

Paso 2: configurar y aplicar una ACL estándar numerada en el R3.

- a. Cree una ACL con el número 1 en el **R3** con una instrucción que deniegue el acceso a la red 192.168.30.0/24 desde la red de la **PC1** (192.168.10.0/24).

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

- b. De manera predeterminada, las ACL deniegan todo el tráfico que no coincide con una regla. Para permitir el resto del tráfico, cree una segunda regla para la ACL 1.

```
R3(config)# access-list 1 permit any
```

- c. Para aplicar la ACL, colóquela en la interfaz Gigabit Ethernet 0/0 para el tráfico saliente.

```
R3(config)# interface GigabitEthernet0/0
```

```
R3(config-if)# ip access-group 1 out
```

Paso 3: verificar la configuración y la funcionalidad de la ACL.

- a. En el **R2** y el **R3**, introduzca el comando **show access-list** para verificar las configuraciones de la ACL.

Introduzca el comando **show run** o **show ip interface gigabitethernet 0/0** para verificar la colocación de las ACL.

- b. Una vez colocadas las dos ACL, el tráfico de la red se restringe según las políticas detalladas en la parte 1. Utilice las siguientes pruebas para verificar las implementaciones de ACL:

- Un ping de 192.168.10.10 a 192.168.11.10 se realiza correctamente.
- Un ping de 192.168.10.10 a 192.168.20.254 se realiza correctamente.
- Un ping de 192.168.11.10 a 192.168.20.254 falla.
- Un ping de 192.168.10.10 a 192.168.30.10 falla.
- Un ping de 192.168.11.10 a 192.168.30.10 se realiza correctamente.
- Un ping de 192.168.30.10 a 192.168.20.254 se realiza correctamente.

Configuration de router 2 y router 3

Router 2 Configuration

```
R2>en
R2#conf t
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#int g0/0
R2(config-if)#ip access-group 1 out
```

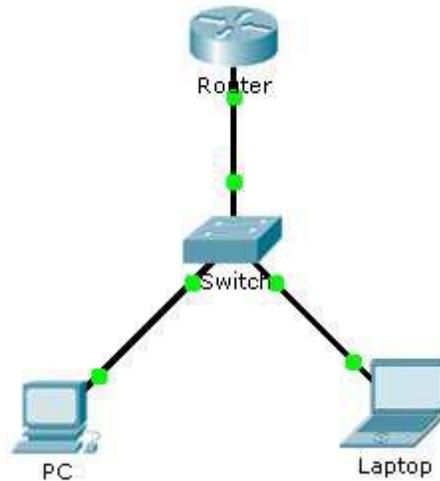
Router 3 Configuration

```
R3>en
R3#conf t
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#int g0/0

R3(config-if)#ip access-group 1 out
```

Practica De Laboratorio 9.2.3.3: CONFIGURING AN ACL ON VTY LINES

Topología



Addressing Table

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

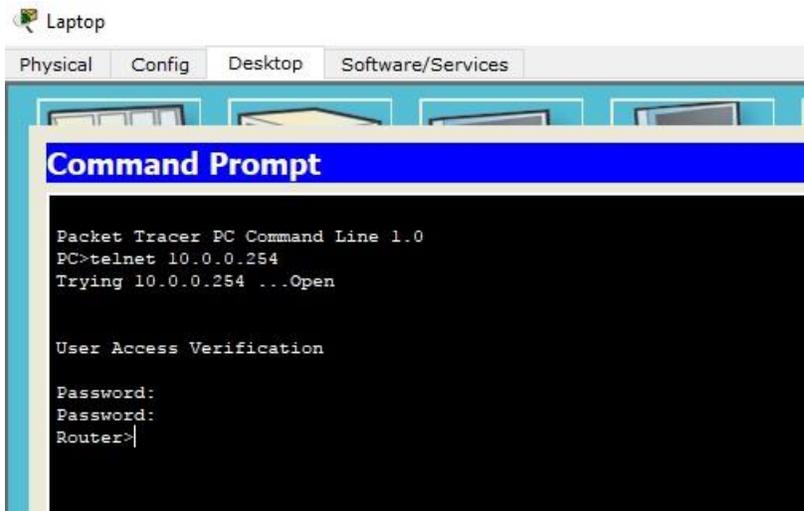
Step 1: Verify Telnet access before the ACL is configured.

Both computers should be able to Telnet to the Router. The password is **cisco**.

```
Packet Tracer PC Command Line 1.0
PC>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification
Password:
Password:
```

The screenshot shows a Packet Tracer PC Command Line window. The title bar reads "Command Prompt". The window content shows the following text: "Packet Tracer PC Command Line 1.0", "PC>telnet 10.0.0.254", "Trying 10.0.0.254 ...Open", "User Access Verification", "Password:", and "Password:". The window is set against a dark background with white text.

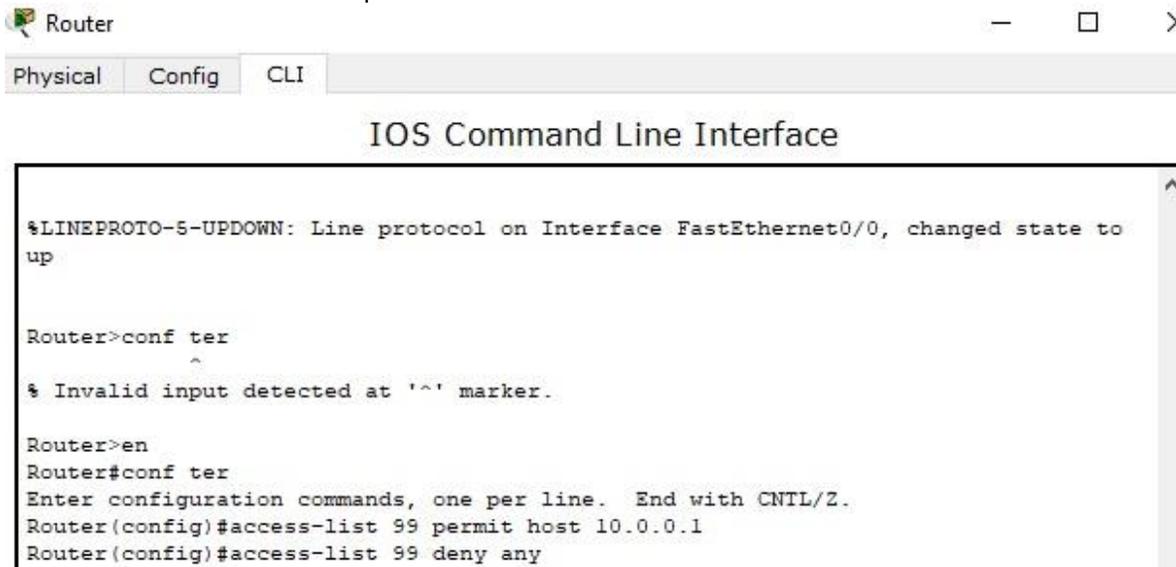


Step 2: Configure a numbered standard ACL.

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
```

```
Router(config)#line vty 0 15
Router(config-line)#access-list 99 d
      ^
% Invalid input detected at '^' marker.

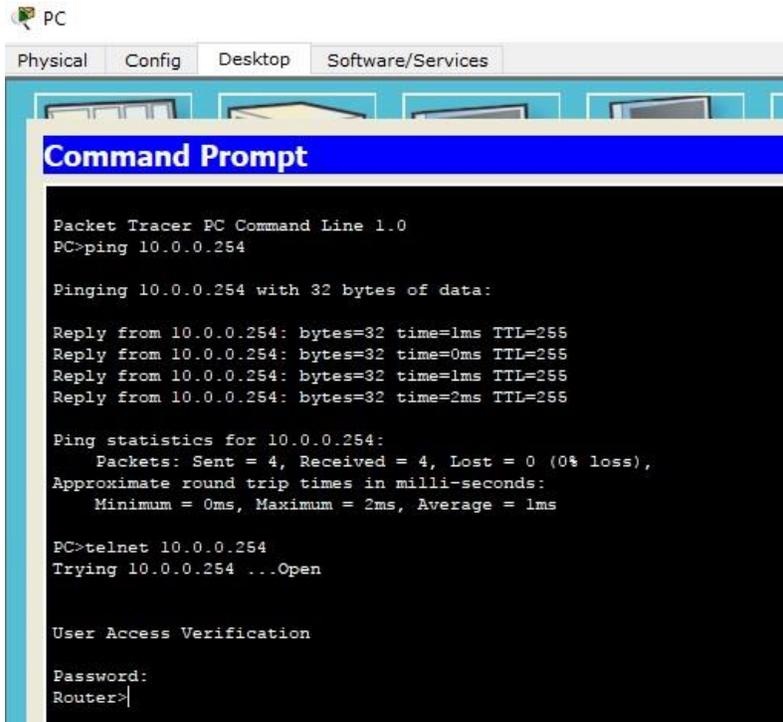
Router(config-line)#access-class 99 in
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show acc
Standard IP access list 99
    10 permit host 10.0.0.1
    20 deny any
Router#
```

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.



The screenshot shows a Packet Tracer PC Command Prompt window. The window title is "PC" and it has tabs for "Physical", "Config", "Desktop", and "Software/Services". The main content area is titled "Command Prompt" and displays the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=1ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=1ms TTL=255
Reply from 10.0.0.254: bytes=32 time=2ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

PC>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router#>
```

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=0ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
PC>
```

PRACTICA DE LABORATORIO 9.5.2.6: PACKET TRACER - CONFIGURING IPV6 ACLS

Tabla de direcciones

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objetivos

Parte 1: Configure, aplique y verifique una ACL IPv6

Parte 2: Configurar, aplicar y verificar una segunda ACL de IPv6

Parte 1: Configure, aplique y verifique una ACL IPv6

Los registros indican que una computadora en la red 2001: DB8: 1: 11 :: 0/64 está actualizando repetidamente su página web causando un ataque de denegación de servicio (DoS) contra Server3. Hasta que el cliente pueda ser identificado y limpiado, debe bloquear el acceso HTTP y HTTPS a esa red con una lista de acceso.

Paso 1: Configure Una Acl Que Bloqueará El Acceso Http Y Https.

Configure an ACL named BLOCK_HTTP on R1 with the following statements.

a. Bloquear el tráfico HTTP y HTTPS de llegar a 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
```

```
R1>
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#
```

b. Permitir que todo el tráfico IPv6 pase

```
R1(config-ipv6-acl)#deny tcp any host
R1(config-ipv6-acl)#permit ip any any
R1(config-ipv6-acl)#
```

Paso 2: Aplique la ACL a la interfaz correcta.

Aplique la ACL en la interfaz más cercana al origen del tráfico que se va a bloquear.

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

```
R1(config)#int g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

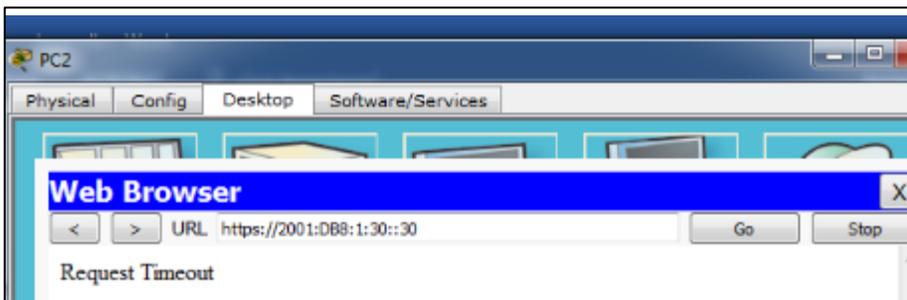
Paso 3: Verificar la implementación de ACL

Verifique que la ACL esté funcionando según lo previsto realizando las siguientes pruebas:

- Open the web browser of PC1 to [http:// 2001:DB8:1:30::30](http://2001:DB8:1:30::30) or <https://2001:DB8:1:30::30>. The website should appear.



- //Open the web browser of PC2 to [http:// 2001:DB8:1:30::30](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.

```

PC>PING 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=126

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

PC>

```

Parte 2: Configurar, aplicar y verificar una segunda ACL de IPv6

Los registros ahora indican que su servidor está recibiendo pings de muchas direcciones IPv6 diferentes en un ataque de denegación de servicio distribuido (DDoS). Debe filtrar peticiones de ping ICMP a su servidor

Step 1: Create an access list to block ICMP.

Configure una ACL denominada BLOCK_ICMP en R3 con las siguientes sentencias:

```

R3>
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP

```

Block all ICMP traffic from any hosts to any destination.

```

R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any

```

Allow all other IPv6 traffic to pass.

```

R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#

```

Paso 2: Aplique la ACL a la interfaz correcta.

En este caso, el tráfico ICMP puede provenir de cualquier fuente. Para asegurarse de que el tráfico ICMP se bloquea independientemente de su origen o de los cambios que se produzcan en la topología de red, aplique la ACL más cercana al destino.

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g0/0
R3(config-if)#ipv6 traffic-filterer BLOCK_ICMP out
^
% Invalid input detected at '^' marker.
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

Paso 3: Verifique que funcione la lista de acceso adecuado.

Ping de PC2 a 2001: DB8: 1: 30 :: 30. El ping debe fallar. segundo.

```
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Ping de PC1 a 2001: DB8: 1: 30 :: 30. El ping debe fallar.

```
PC>PING 2001:db8:1:30::30

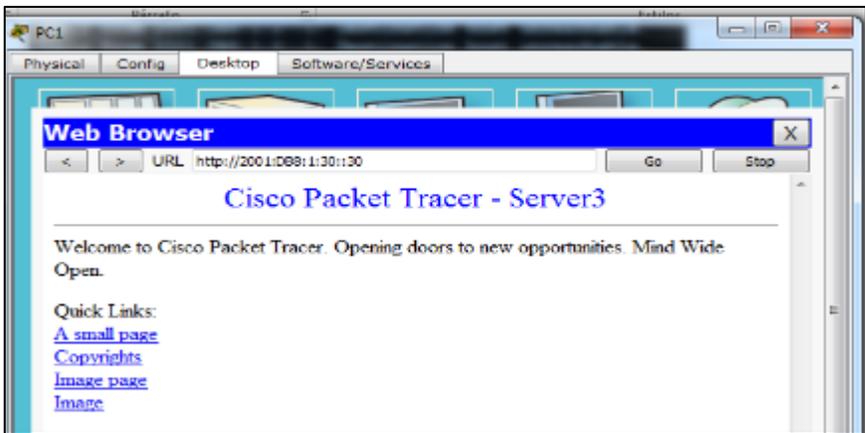
Pinging 2001:db8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Abra el explorador Web de PC1 a <http://2001:DB8:1:30::30> o <https://2001:DB8:1:30::30>. El sitio web debe mostrar



CONCLUSIONES

- Otros de los objetivos de este tipo de enrutamiento incluyen que los routers puedan llevar a cabo procesos para compartir información dinámicamente, realizar el descubrimiento de redes remotas y optimizar el rendimiento para utilizar siempre la mejor ruta. Para profundizar en la aplicación del enrutamiento dinámico es conveniente conocer los tres tipos que existen: vector de distancia, estado de enlace y sistema híbrido.
- Una red escalable requiere un diseño de red jerárquico. Switches, agregados de enlaces, redundancia lan y la inalámbricas son tecnologías que proporcionan o mejoran el acceso de usuarios a los recursos de red.
- Una Lista de Control de Acceso o ACL (del inglés, Access Control List) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido
- Para que OSPF sea más eficaz y escalable, este protocolo admite el routing jerárquico mediante áreas. Un área OSPF es un grupo de routers que comparten la misma información de estado de enlace en sus LSDB.

BIBLIOGRAFÍA

(First, 2011)

First, O. S. (5 de agosto de 2011). *Características de OSPF*. Recuperado el 20 de noviembre de 2017, de Características de OSPF:

<http://ecovi.uagro.mx/ccna2/course/module8/8.1.1.5/8.1.1.5.html>