Universidad Nacional Abierta y a Distancia – UNAD
Vicerrectoría Académica y de Investigación - VIACI
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA.
Programa de Ingeniería Electrónica
203092 DIPLOMADO DE PROFUNDIZACIÓN CISCO

PASO 7 – ACTIVIDAD COLABORATIVA 4

PRESENTADO POR:

LINA MARYOLY QUIÑONES

DANILO ERNESTO POSSO

RONALD EDUARDO MURILLO

NESTOR LEONEL AQUITE

JHON JAIRO PONTON - CÓDIGO 16891891

GRUPO 203092_24

TUTOR

JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLÓGIA E INGENIERÍA - ECBTI

NOVIEMBRE DE 2017

INTRODUCCIÓN

En el presente archivo se puede observar el desarrollo de los laboratorios correspondientes al curso de profundización en cisco módulo CCNA2. En el cual se comprenden los dispositivos que se pueden usar en la creación y diseño de redes LAN. Así como también las configuraciones básicas y de seguridad que se deben tener presentes en los routers.

Se trabajo siguiendo las instrucciones asignadas en cada actividad de laboratorio y posteriormente se realizó el procedimiento, dejando las evidencias correspondientes, con la ayuda del software Packet Tracer, el cual permitio analizar mejor la información y aplicar los conocimientos adquiridos.

Con la participación de los estudiantes del grupo colaborativo, pretendemos obtener varios resultados y opiniones a los diferentes temas tratados, aportando los conocimientos adquiridos para aprender nuevos conceptos, con el fin de apropiarnos de todos los contenidos y así posteriormente poder aplicarlos para la solución adecuada a las necesidades presentadas en el campo de las redes y comunicaciones.

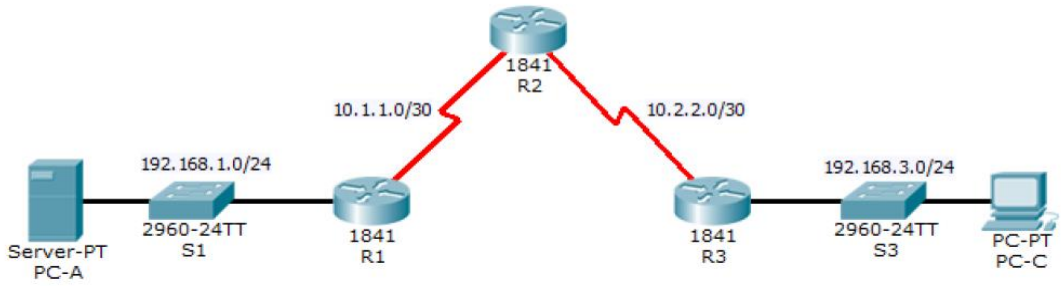
OBJETIVOS

- Conocer los conceptos del Routing dinamico
- Conocer que son y para que sirven las listas de control de acceso
- Conocer cómo funciona el traductor de direcciones NAT para IPv4
- Profundizar en los conceptos de DHCP

DESARROLLO DE ACTIVIDADES

4.4.1.2 Packet Tracer: Configure IP ACLs to Mitigate Attacks

Topology



Addressing Table

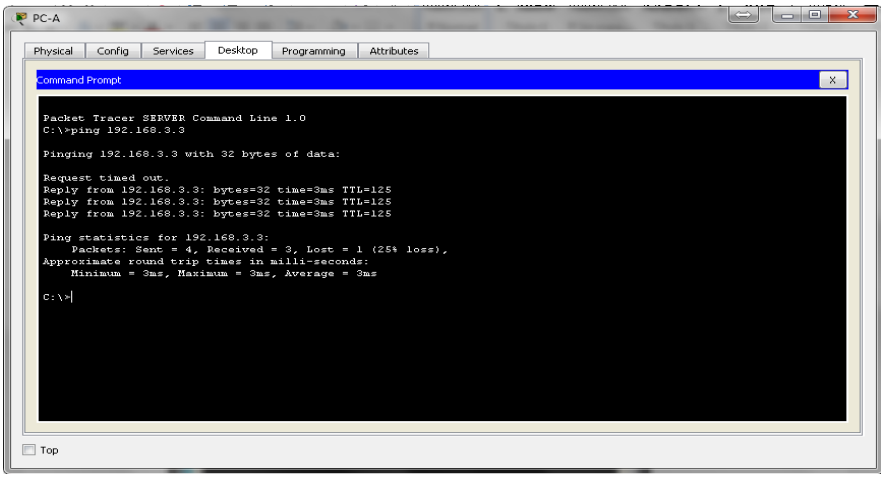
Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

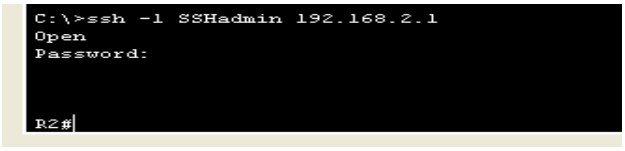
Step 1: From PC-A, verify connectivity to PC-C and R2.

a. From the command prompt, ping **PC-C** (192.168.3.3).



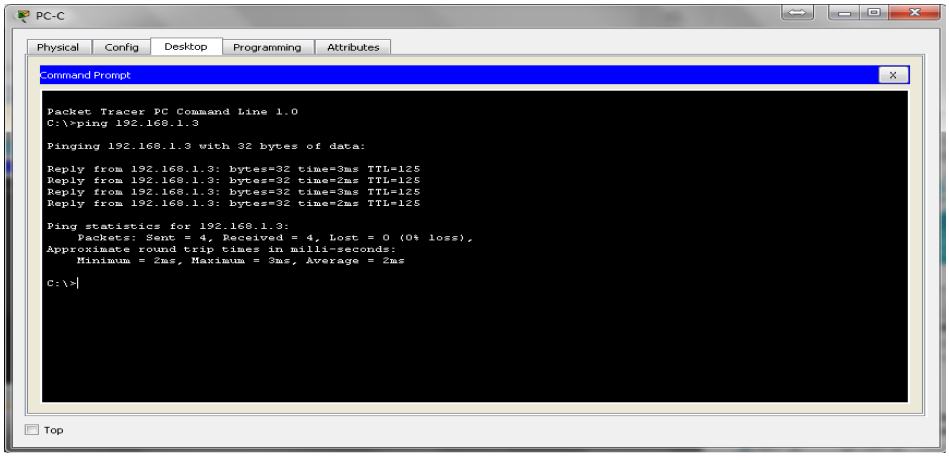
b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. When finished, exit the SSH session.

PC> **ssh -l SSHadmin 192.168.2.1**



Step 2: From PC-C, verify connectivity to PC-A and R2.

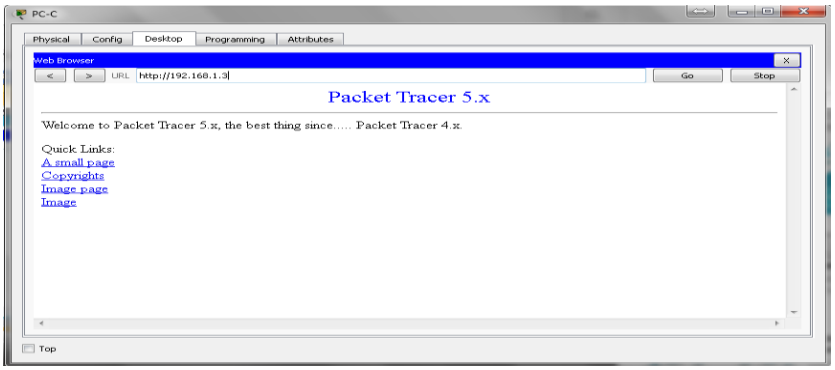
a. From the command prompt, ping **PC-A** (192.168.1.3).



b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. Close the SSH session when finished.

PC> **ssh -l SSHadmin 192.168.2.1**

c. Open a web browser to the **PC-A** server (192.168.1.3) to display the web page. Close the browser when done.

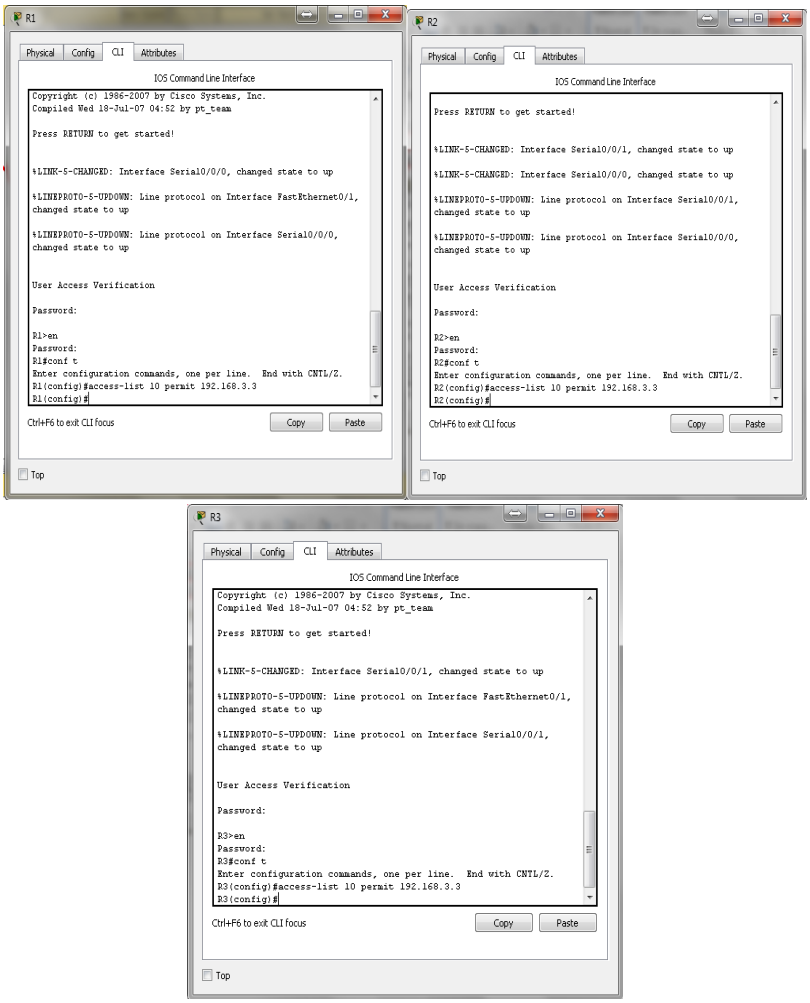


Part 2: Secure Access to Routers

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.

Use the **access-list** command to create a numbered IP ACL on **R1**, **R2**, and **R3**.

R1(config)# **access-list 10 permit 192.168.3.3 0.0.0.0**
R2(config)# **access-list 10 permit 192.168.3.3 0.0.0.0**
R3(config)# **access-list 10 permit 192.168.3.3 0.0.0.0**



Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.
R1(config-line)# access-class 10 in
R2(config-line)# access-class 10 in
R3(config-line)# access-class 10 in

```
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#
```

```
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#
```

```
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#
```

Step 3: Verify exclusive access from management station PC-C.

a. Establish a SSH session to 192.168.2.1 from **PC-C** (should be successful).

PC> **ssh –l SSHadmin 192.168.2.1**

```
[Connection to 192.168.2.1 closed by foreign host]
C:\>
C:\>en
Invalid Command.

C:\>ssh -l SSHadmin 192.168.2.1
Open
Password:



R2#exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

b. Establish a SSH session to 192.168.2.1 from **PC-A** (should fail).

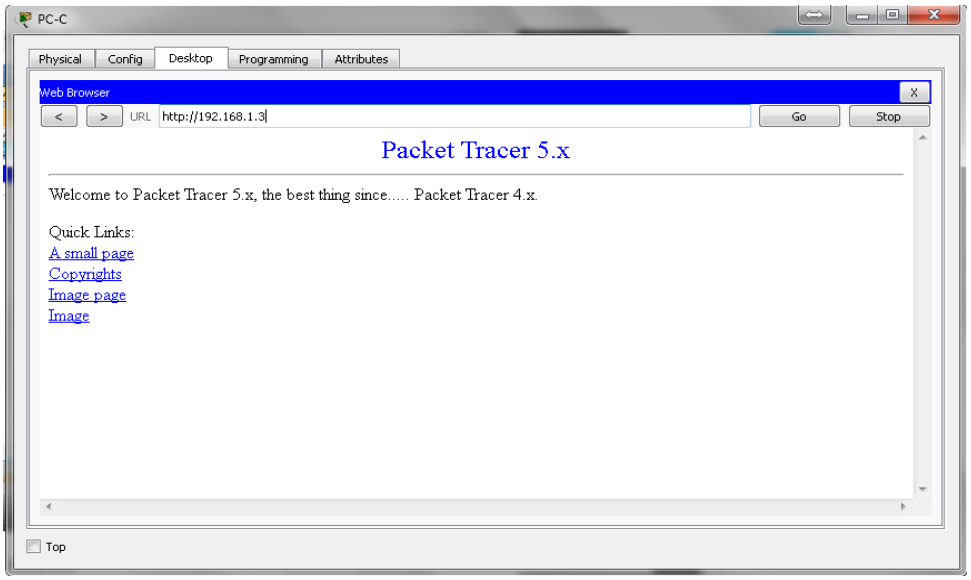
```
[Connection to 192.168.2.1 closed by foreign host]
C:\>
C:\>ssh -l SSHadmin 192.168.2.1

% Connection refused by remote host
C:\>
```

Part 3: Create a Numbered IP ACL 120 on R1

Permit any outside host to access DNS, SMTP, and FTP services on server **PC-A**, deny any outside host access to HTTPS services on **PC-A**, and permit **PC-C** to access **R1** via SSH.

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server **PC-A**.



Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

R1(config)# **access-list 120 permit udp any host 192.168.1.3 eq domain**
R1(config)# **access-list 120 permit tcp any host 192.168.1.3 eq smtp**
R1(config)# **access-list 120 permit tcp any host 192.168.1.3 eq ftp**
R1(config)# **access-list 120 deny tcp any host 192.168.1.3 eq 443**
R1(config)# **access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22**

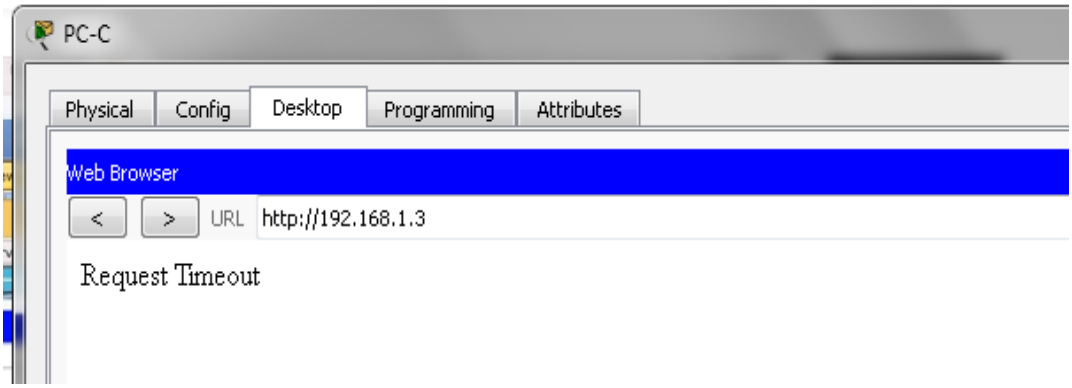
```
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq
domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq
smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host
10.1.1.1 eq 22
R1(config)#
```

Step 3: Apply the ACL to interface S0/0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0. R1(config)# interface s0/0/0
R1(config-if)# ip access-group 120 in

```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 120 in
R1(config-if)#
```

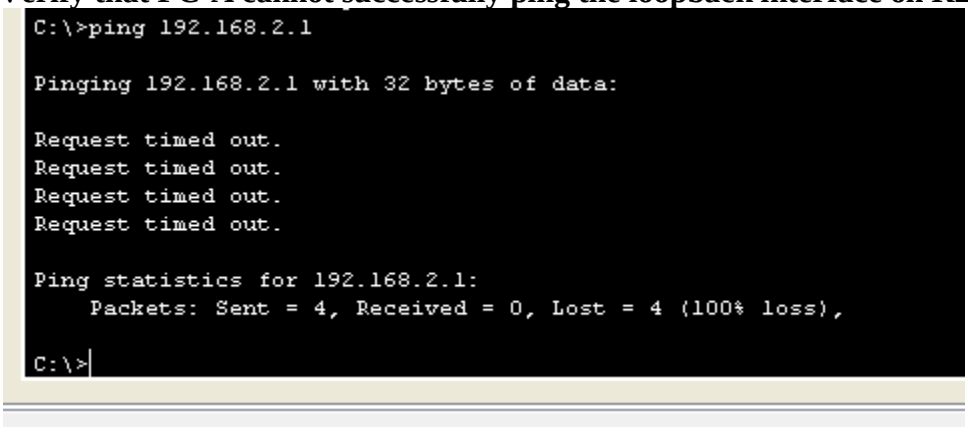
Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.



Part 4: Modify An Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to **R1**); deny all other incoming ICMP packets.

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.



Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

R1(config)# **access-list 120 permit icmp any any echo-reply**
R1(config)# **access-list 120 permit icmp any any unreachable**
R1(config)# **access-list 120 deny icmp any any**
R1(config)# **access-list 120 permit ip any any**

```
R1(config)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#
```

Ctrl+F6 to exit CLI focus Copy

Step 3: Verify that PC-A can successfully ping the loopback interface on R2.

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=2ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Part 5: Create a Numbered IP ACL 110 on R3

Deny all outbound packets with source address outside the range of internal IP addresses on **R3**.

Step 1: Configure ACL 110 to permit only traffic from the inside network.

Use the **access-list** command to create a numbered IP ACL.

R3(config)# **access-list 110 permit ip 192.168.3.0 0.0.0.255 any**

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#
```

Step 2: Apply the ACL to interface F0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface F0/1.

R3(config)# **interface fa0/1**
R3(config-if)# **ip access-group 110 in**

```
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#
```

Part 6: Create a Numbered IP ACL 100 on R3

On **R3**, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

Step 1: Configure ACL 100 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).
Use the **access-list** command to create a numbered IP ACL.

R3(config)# **access-list 100 deny ip 10.0.0.0 0.255.255.255 any**
R3(config)# **access-list 100 deny ip 172.16.0.0 0.15.255.255 any**
R3(config)# **access-list 100 deny ip 192.168.0.0 0.0.255.255 any**
R3(config)# **access-list 100 deny ip 127.0.0.0 0.255.255.255 any**
R3(config)# **access-list 100 deny ip 224.0.0.0 15.255.255.255 any**
R3(config)# **access-list 100 permit ip any any**

```
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#
```

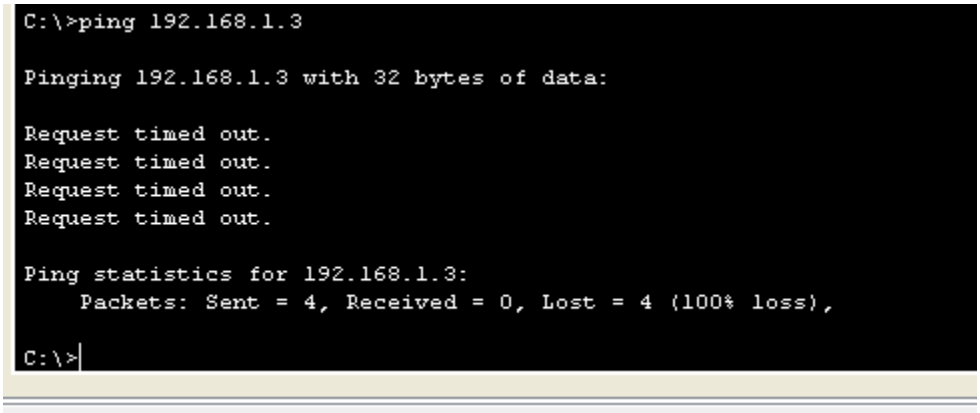
Ctrl+F6 to exit CLI focus Copy Paste

Step 2: Apply the ACL to interface Serial 0/0/1.
Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.
R3(config)# **interface s0/0/1**
R3(config-if)# **ip access-group 100 in**

```
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#
```

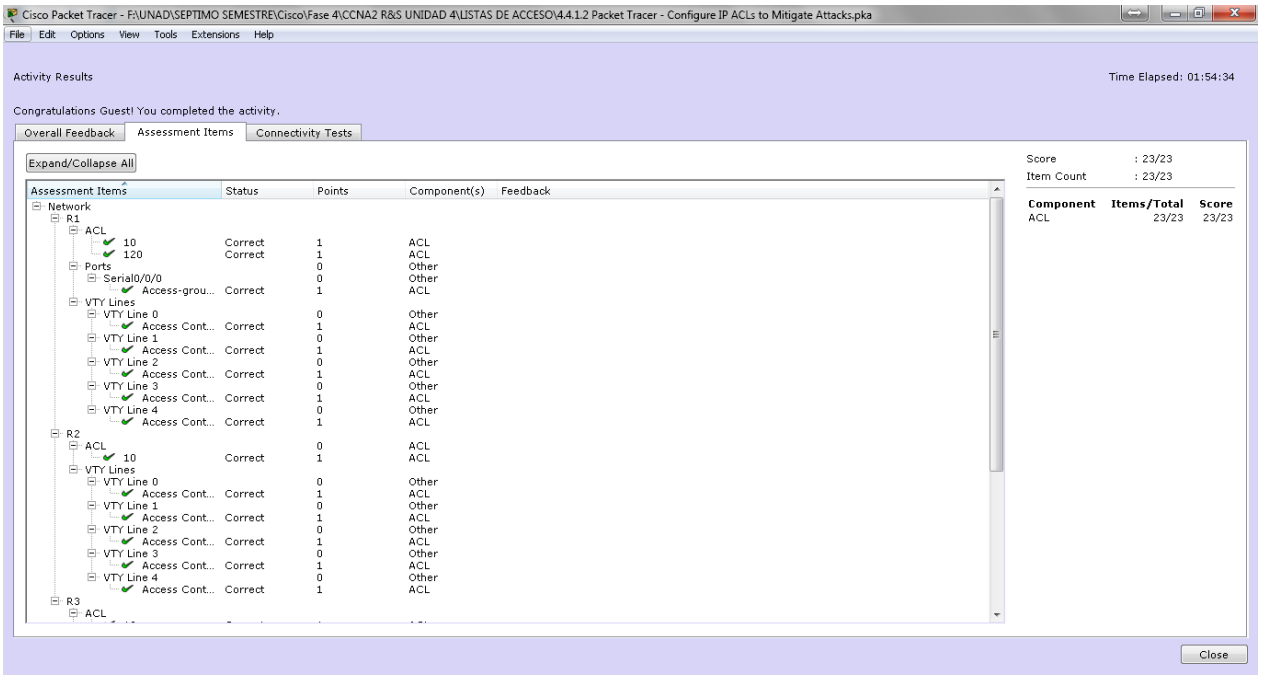
Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

From the **PC-C** command prompt, ping the **PC-A** server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.



Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.


Cisco Packet Tracer - F:\UNAD\SEPTIMO SEMESTRE\Cisco\Fase 4\CCNA2 R&S UNIDAD 4\LISTAS DE ACCESO\4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks.pka
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:54:34
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items Status Points Component(s) Feedback
Network
R1
ACL
10 Correct 1 ACL
120 Correct 1 ACL
Ports 0 Other
Serial0/0/0 0 Other
Access-grou... Correct 1 ACL
VTY Lines
VTY Line 0 0 Other
Access Cont... Correct 1 ACL
VTY Line 1 0 Other
Access Cont... Correct 1 ACL
VTY Line 2 0 Other
Access Cont... Correct 1 ACL
VTY Line 3 0 Other
Access Cont... Correct 1 ACL
VTY Line 4 0 Other
Access Cont... Correct 1 ACL
R2
ACL 0 ACL
10 Correct 1 ACL
VTY Lines
VTY Line 0 0 Other
Access Cont... Correct 1 ACL
VTY Line 1 0 Other
Access Cont... Correct 1 ACL
VTY Line 2 0 Other
Access Cont... Correct 1 ACL
VTY Line 3 0 Other
Access Cont... Correct 1 ACL
VTY Line 4 0 Other
Access Cont... Correct 1 ACL
R3
ACL
Score : 23/23
Item Count : 23/23
Component Items/Total Score
ACL 23/23 23/23
Close

7.3.2.4 Packet Tracer: Configuración básica de RIPv2 y RIPng

Topología

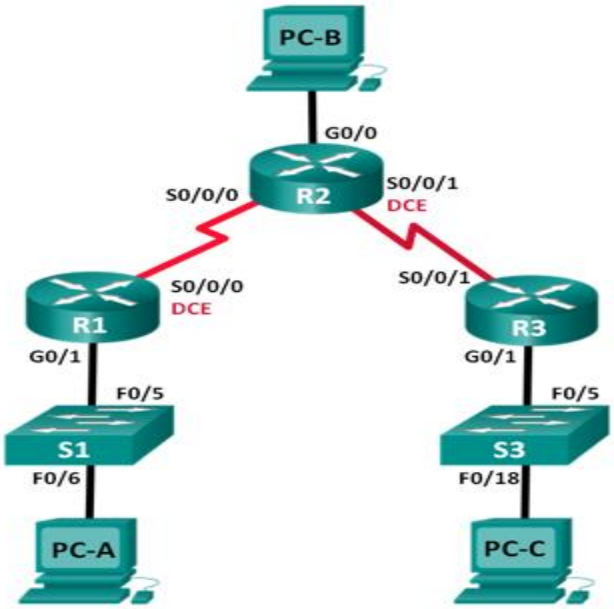


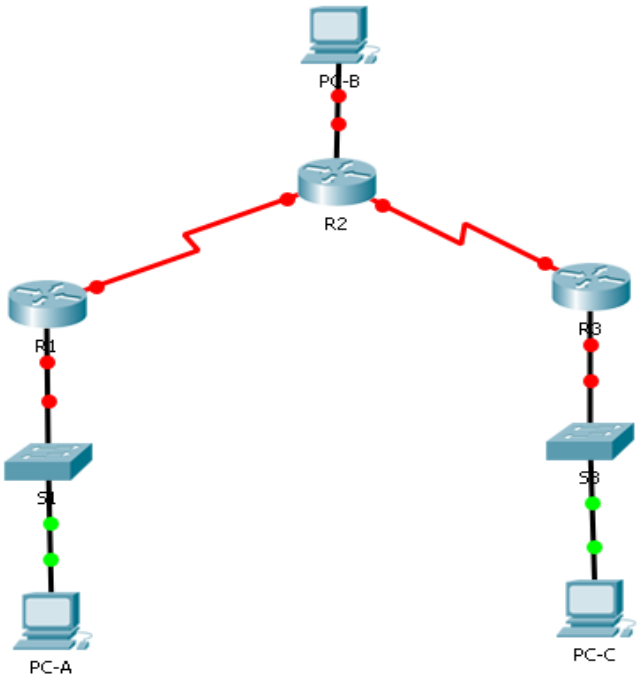
Tabla de direccionamiento

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

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

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

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



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

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

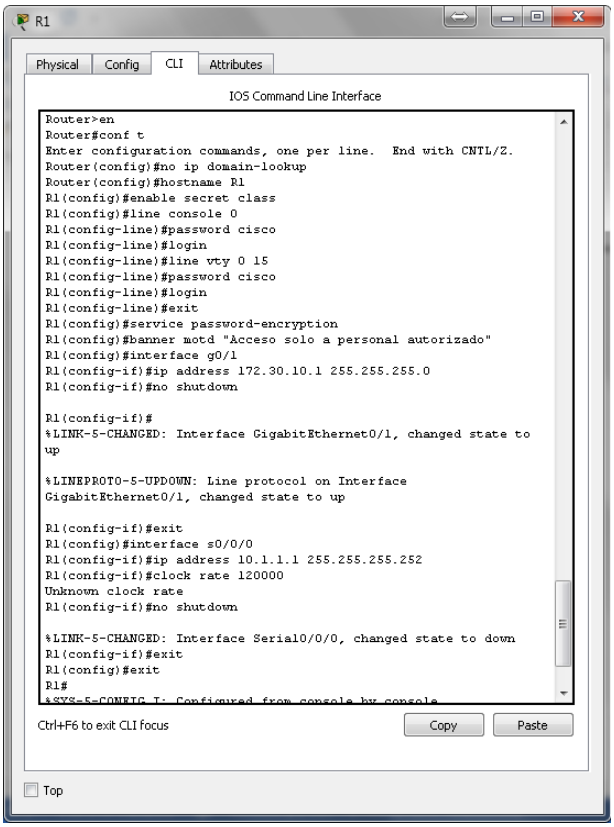
a. Desactive la búsqueda del DNS.
b. Configure los nombres de los dispositivos como se muestra en la topología.
c. Configurar la encriptación de contraseñas.
d. Asigne **class** como la contraseña del modo EXEC privilegiado.
e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
g. Configure **logging synchronous** para la línea de consola.
h. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.

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

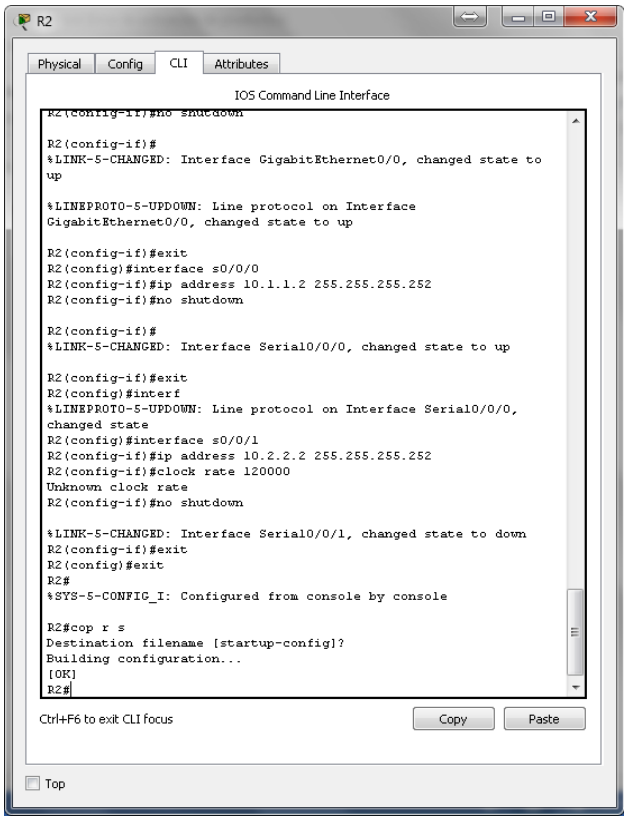
j. Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.

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

Configuración R1

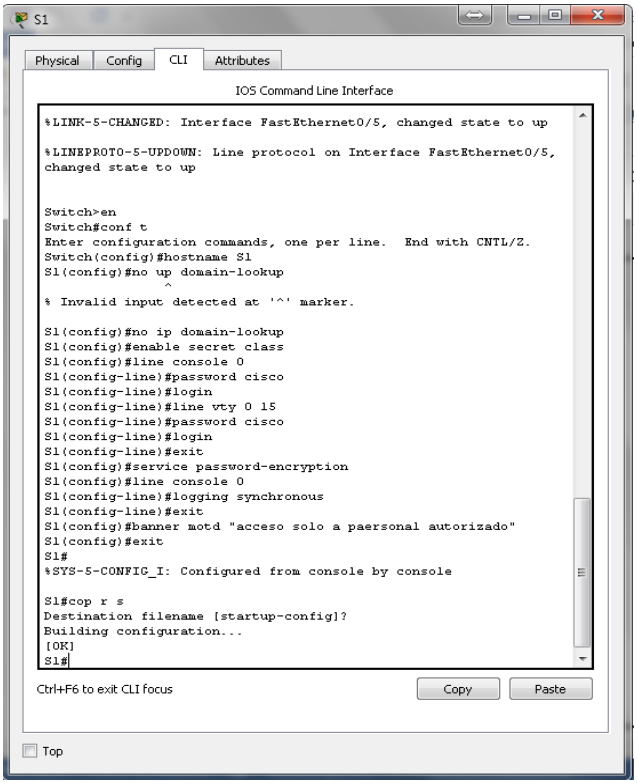


Configuración R2

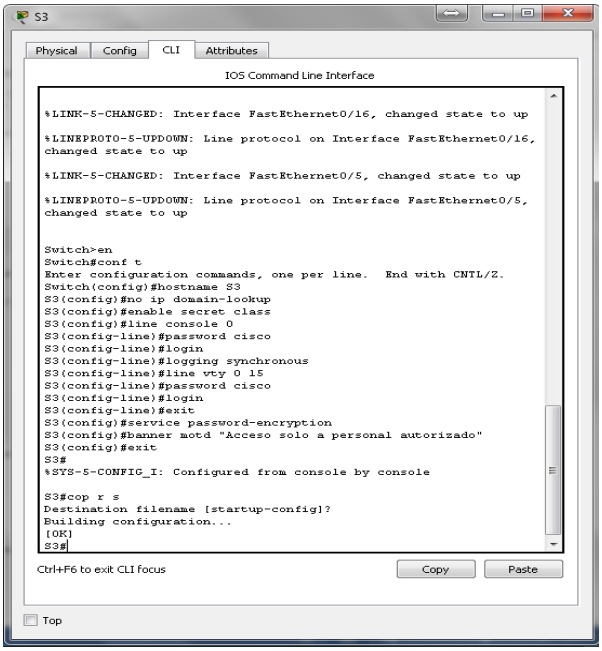


Configuración R3

Configuración S1

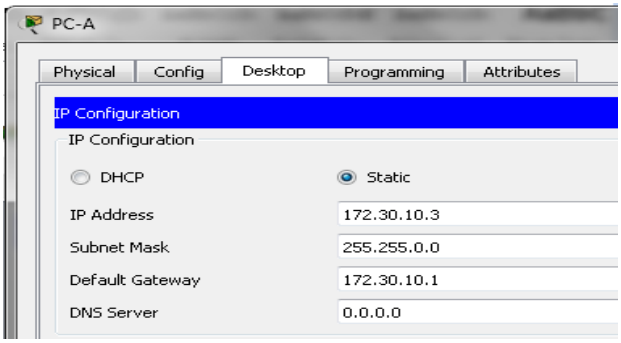


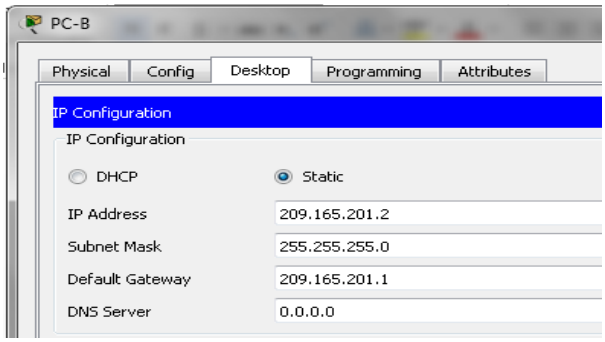
Configuración S3

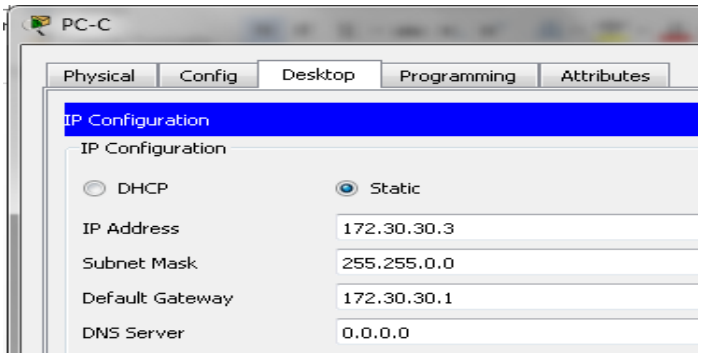


Paso 4. configurar los equipos host.

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



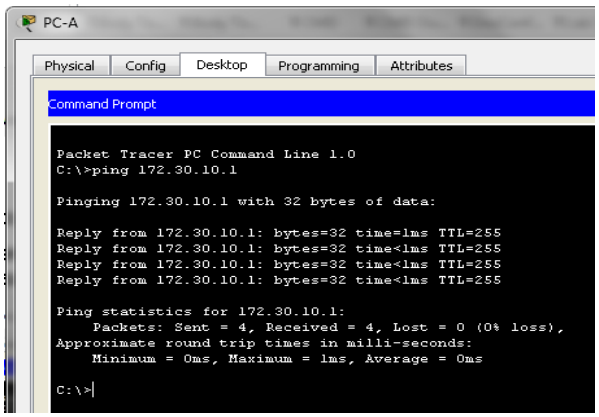


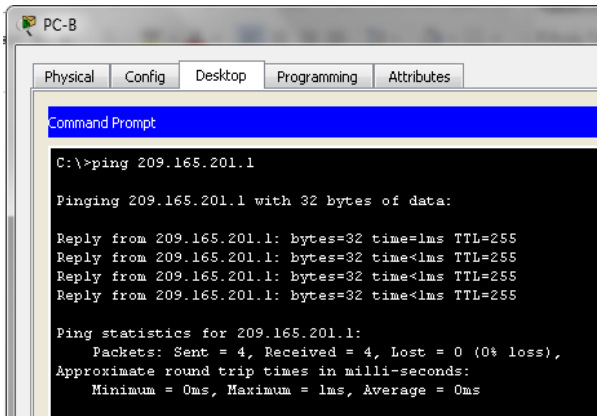


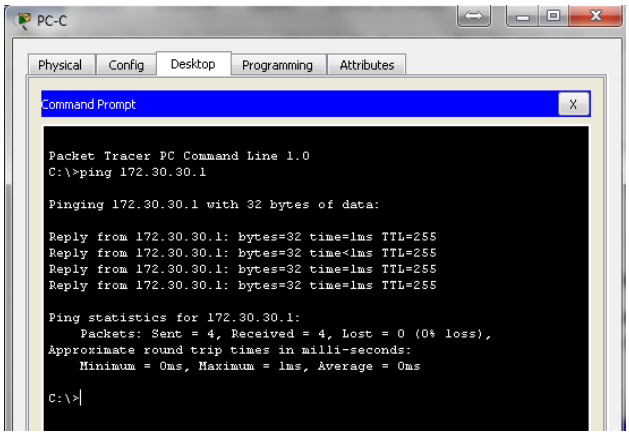
Paso 5. Probar la conectividad.

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

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

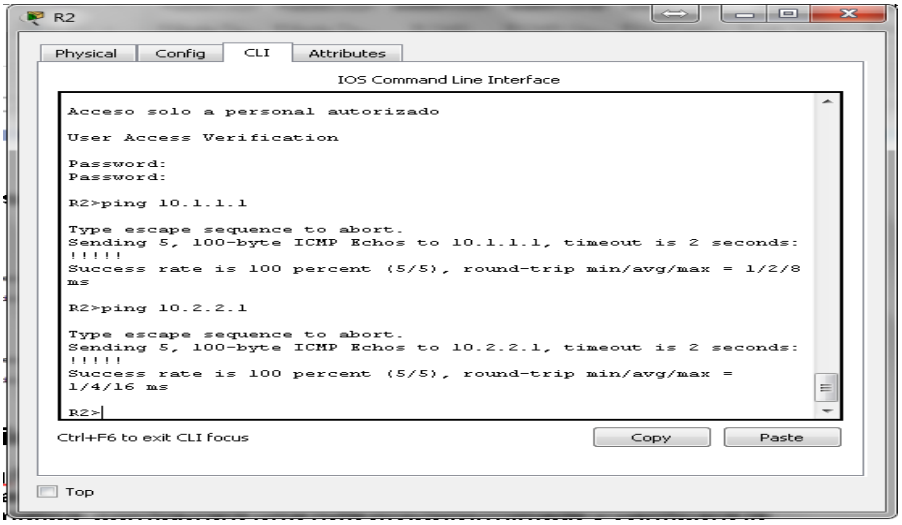

PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.30.10.1
Pinging 172.30.10.1 with 32 bytes of data:
Reply from 172.30.10.1: bytes=32 time=1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<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 = 1ms, Average = 0ms
C:\>


PC-B
Physical
Config
Desktop
Programming
Attributes
Command Prompt
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


PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
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:\>

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

Ping R2 a R1 y R2 a R3



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**

```
R1>en
Password:
R1#conf 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)#
```

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.

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.

```
R3>en
Password:
R3#conf 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)#
```

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

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#exit
R2(config)#
```

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.

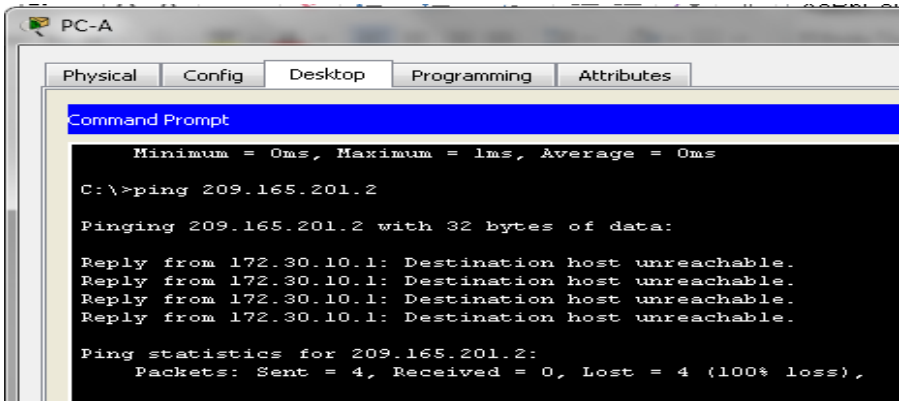
Paso 2. examinar el estado actual de la red.

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

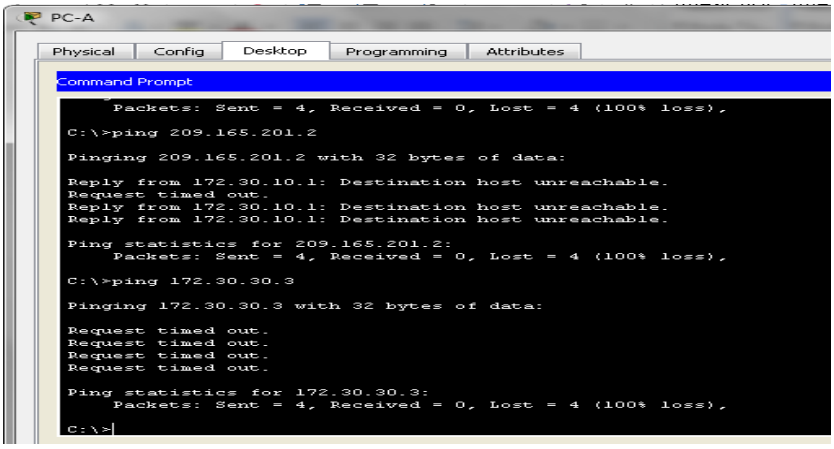
```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0         209.165.201.1   YES manual up
up
GigabitEthernet0/1         unassigned      YES unset
administratively down down
Serial0/0/0                10.1.1.2        YES manual up
up
Serial0/0/1                10.2.2.2        YES manual up
up
Vlan1                      unassigned      YES unset
administratively down down
R2#
```

b. Verifique la conectividad entre las computadoras.

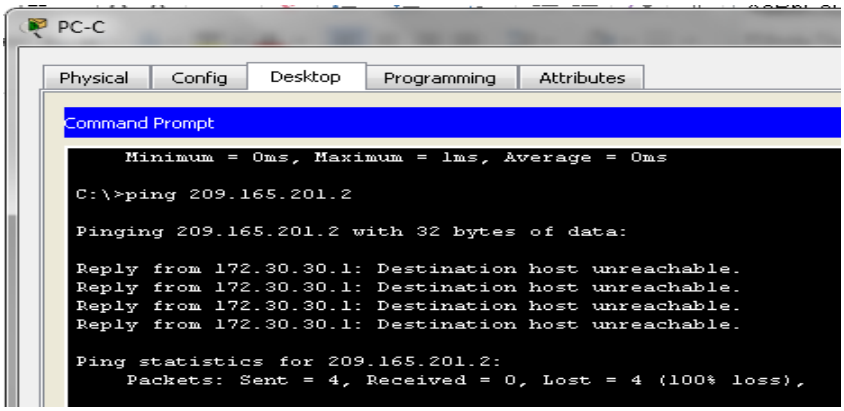
¿Es posible hacer ping de la PC-A a la PC-B? NO ¿Por qué? porque R2 no tiene una ruta que llegue a PC-B esta LAN no está participando en RIP



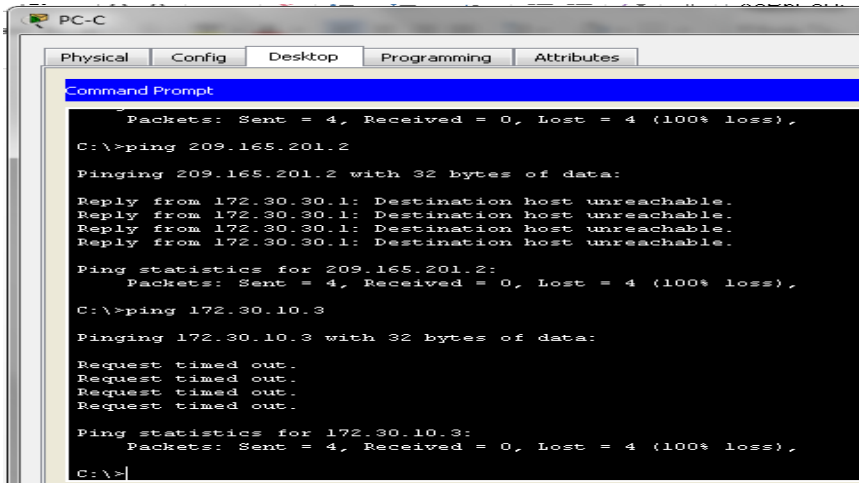
¿Es posible hacer ping de la PC-A a la PC-C? NO ¿Por qué? Porque R1 y R3 no tienen rutas hacia la redes especificadas en el router remoto



¿Es posible hacer ping de la PC-C a la PC-B? NO ¿Por qué? La LAN donde se encuentra PC-B no participa en RIP y R2 no tiene una ruta especificada hacia este equipo

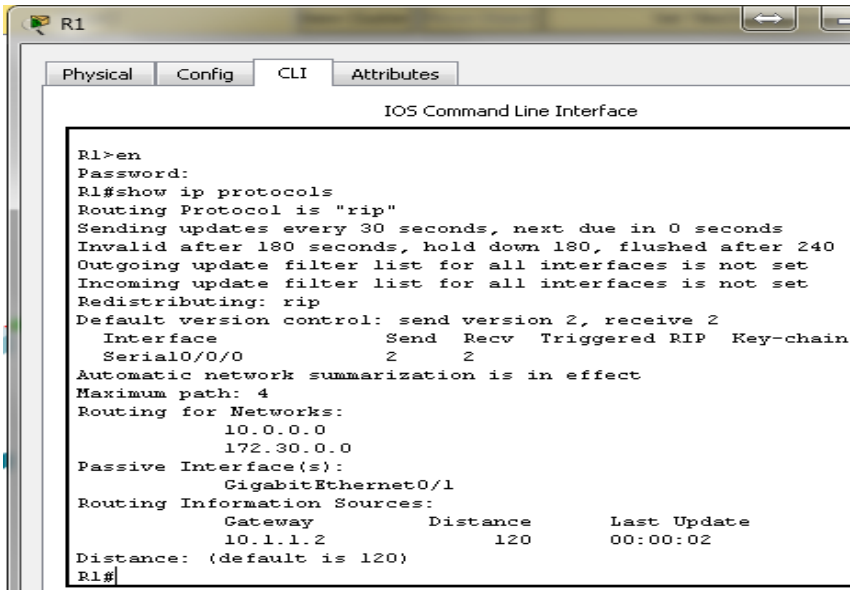


¿Es posible hacer ping de la PC-C a la PC-A? NO ¿Por qué? R1 y R3 no tienen rutas hacia la subred el router remoto.

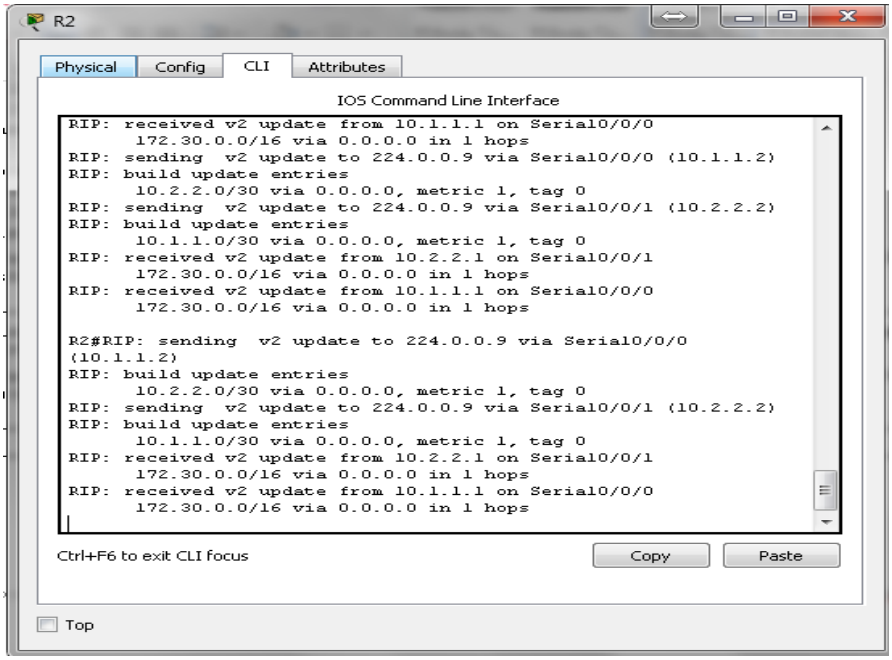


c. Verifique que RIPv2 se ejecute en los routers.

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.



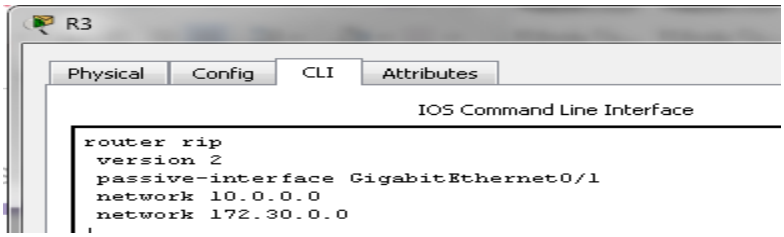
Al emitir el comando **debug ip rip** en el R2, ¿qué información se proporciona que confirma que RIPv2 está en ejecución?



RIP nos envía actualizaciones verison dos a 224.0.0.9via serial 0/0/0y serial 0/0/1

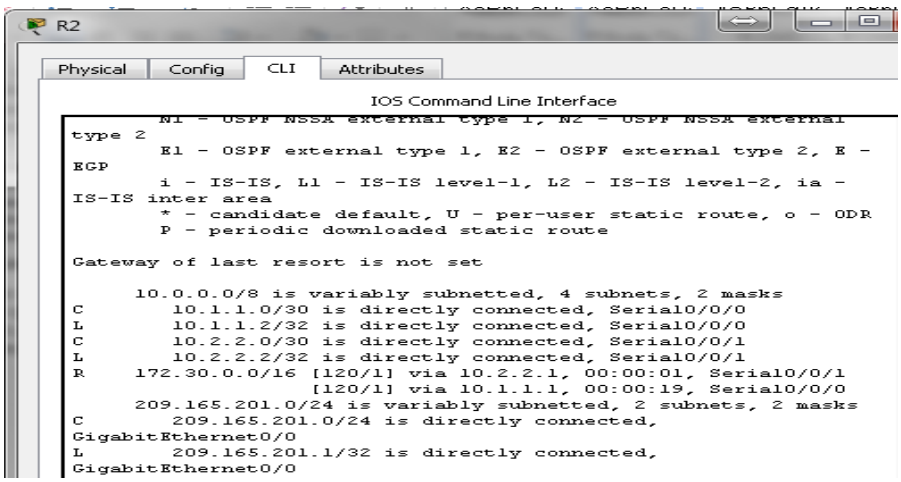
Cuando haya terminado de observar los resultados de la depuración, emita el comando **undebug all** en la petición de entrada del modo EXEC privilegiado

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

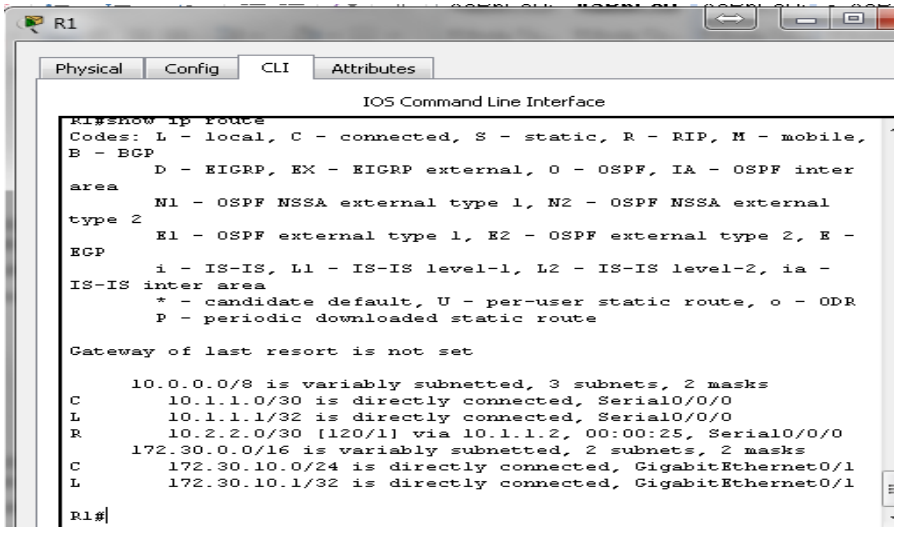


d. Examinar el sumarización automática de las rutas.

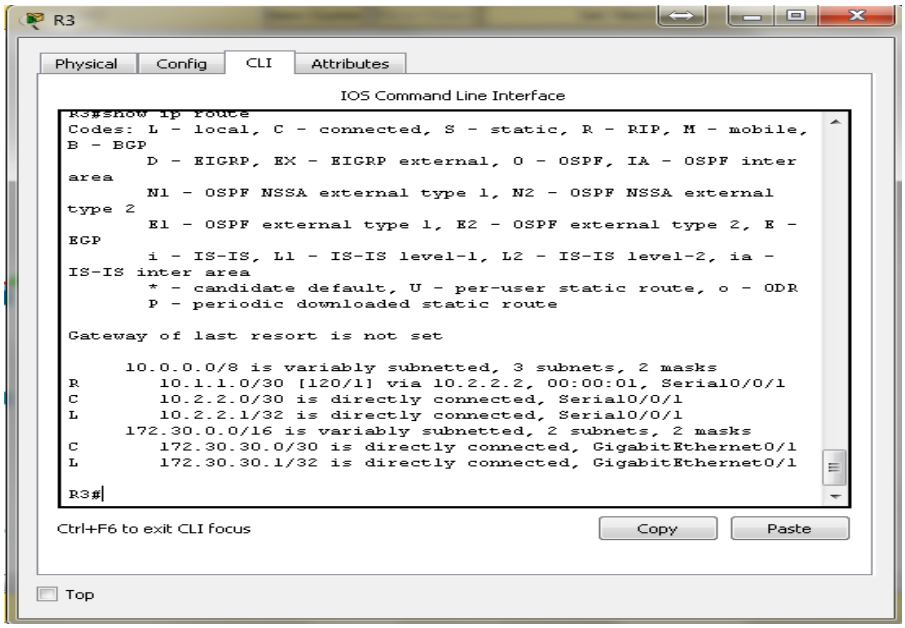
Las LAN conectadas al R1 y el R3 se componen de redes no contiguas. El R2 muestra dos rutas de igual costo a la red 172.30.0.0/16 en la tabla de routing. El R2 solo muestra la dirección de red principal con clase 172.30.0.0 y no muestra ninguna de las subredes de esta red



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.

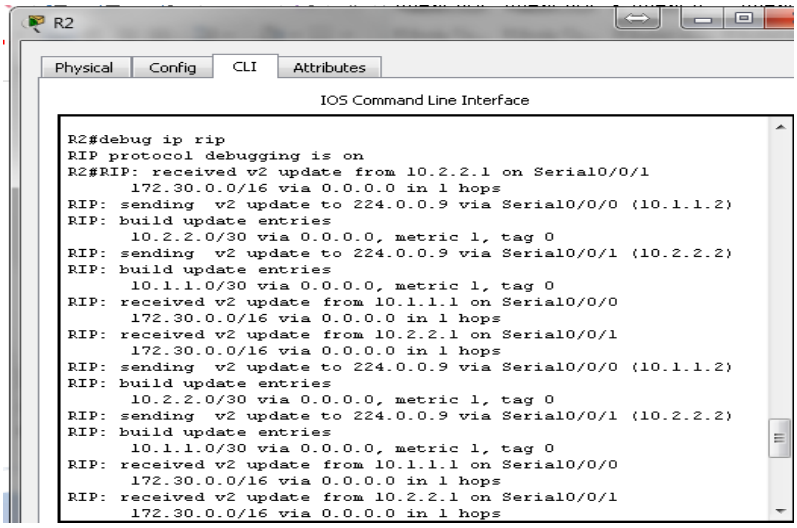


El R3 solo muestra sus propias subredes para la red 172.30.0.0. El R3 no tiene ninguna ruta para las subredes 172.30.0.0 en el R1.



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

<u>received v2 update from 10.1.1.1 on Serial0/0/0</u>
<u>received v2 update from 10.2.2.1 on Serial0/0/1</u>



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.

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

R1(config)# **router rip**

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

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

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

R1# **clear ip route ***

```
R1>en
Password:
R1#conf 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
% Incomplete command.
R1#clear ip route *
R1#
```

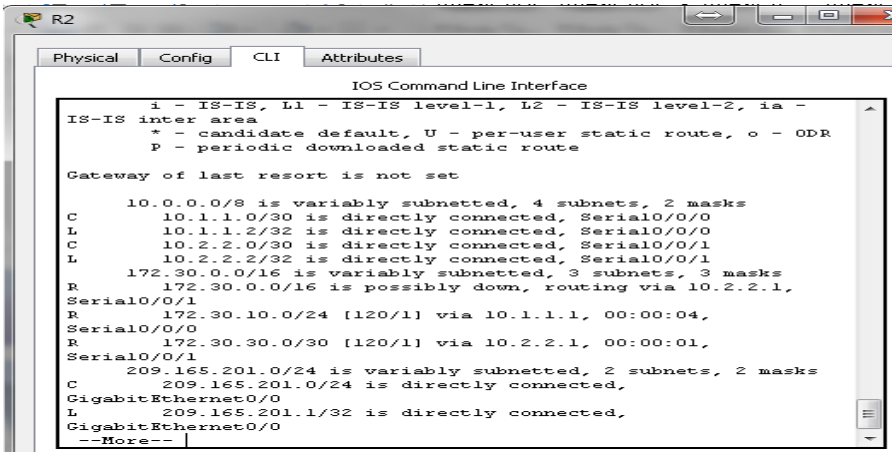
```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#clear ip route *
R2#
```

```
R3>en
Password:
R3#undebug all
All possible debugging has been turned off
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#no auto-summary
R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#clear ip route *
R3#
```

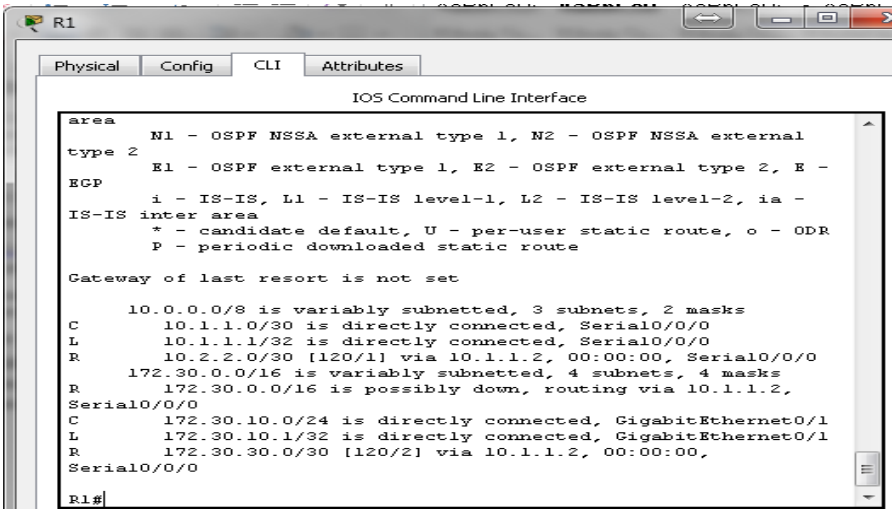
c. Examinar las tablas de enrutamiento Recuerde que la convergencia de las tablas de routing demora un tiempo después de borrarlas.

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

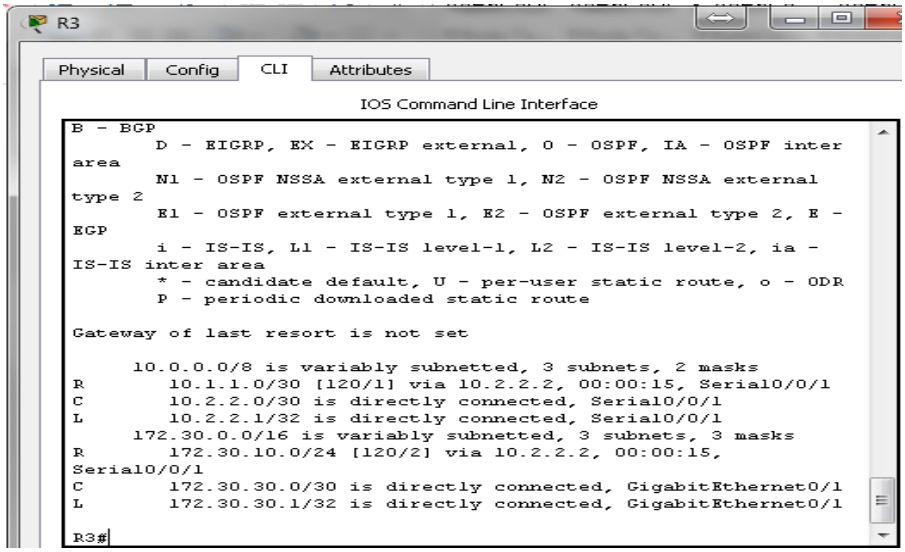
R2# **show ip route**



R1# **show ip route**



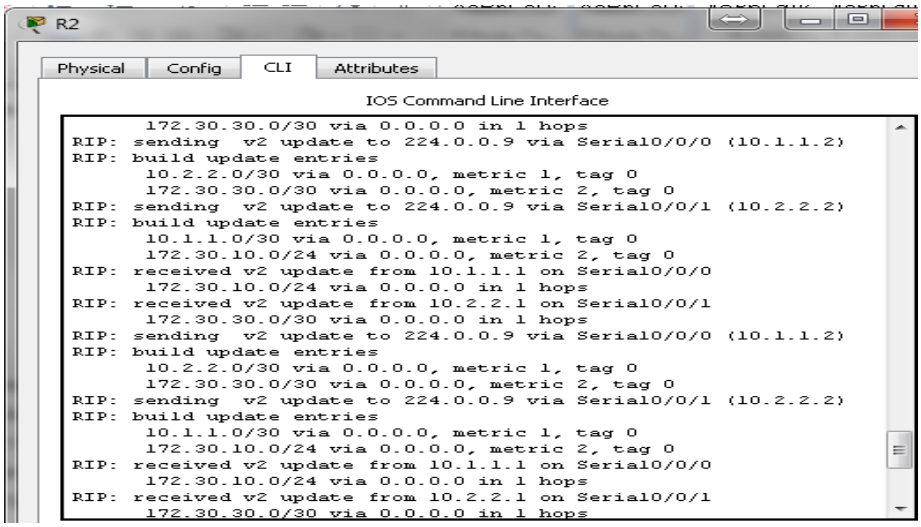
R3# **show ip route**



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?

172.30.30.0/24

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

Si

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

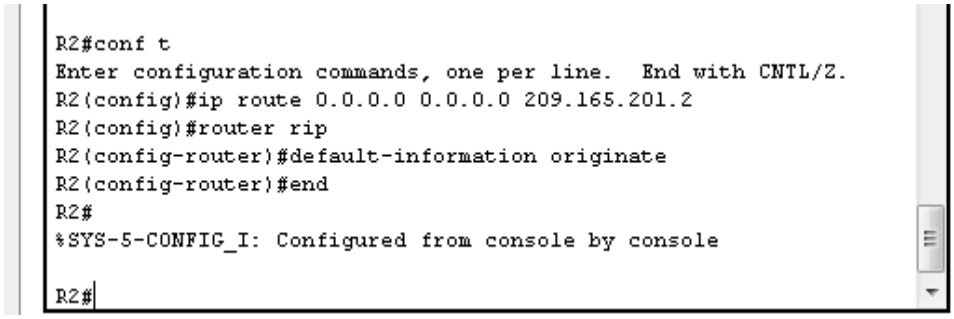
a. Desde el R2, cree una ruta estática a la red 0.0.0.0 0.0.0.0, con el comando **ip route**. Esto envía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet al establecer un gateway de último recurso en el router R2.

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

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

R2(config)# **router rip**

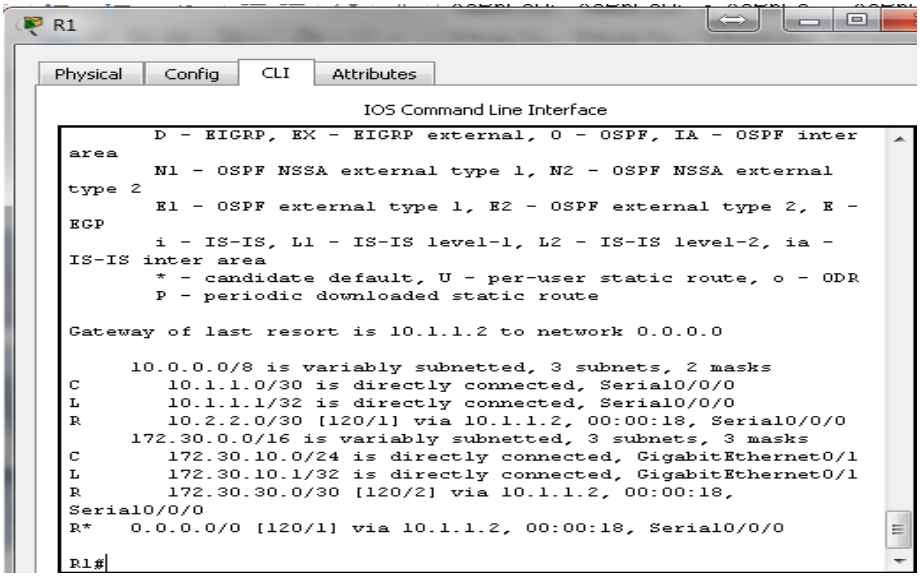
R2(config-router)# **default-information originate**



Paso 5. Verificar la configuración de enrutamiento.

a. Consulte la tabla de routing en el R1.

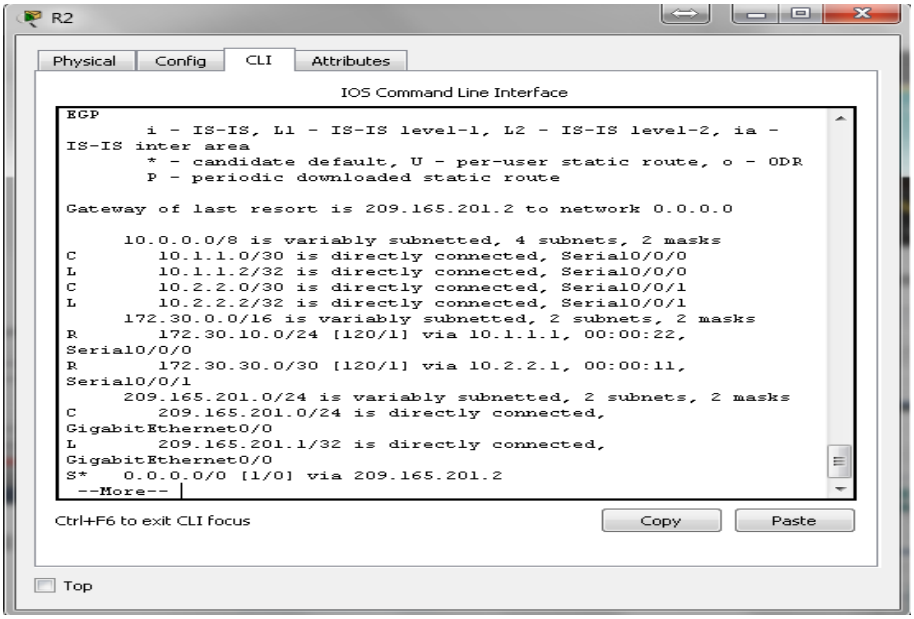
R1# **show ip route**



¿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?

Hay un gateway de último alcance es decir una puerta de enlace que nos conecta a internet y la ruta por defecto que se muestra en la tabla de ruteo esta prendida por RIP

b. Consulte la tabla de routing en el R2.

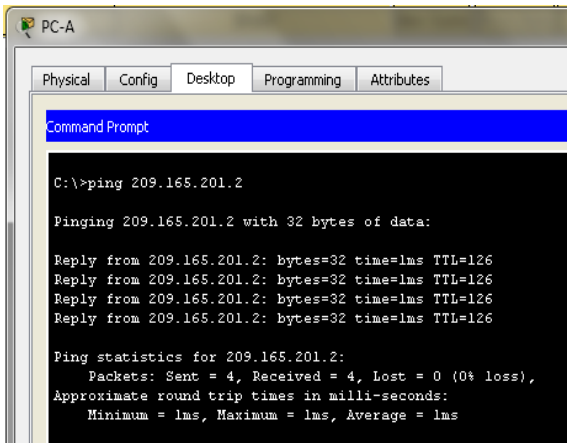


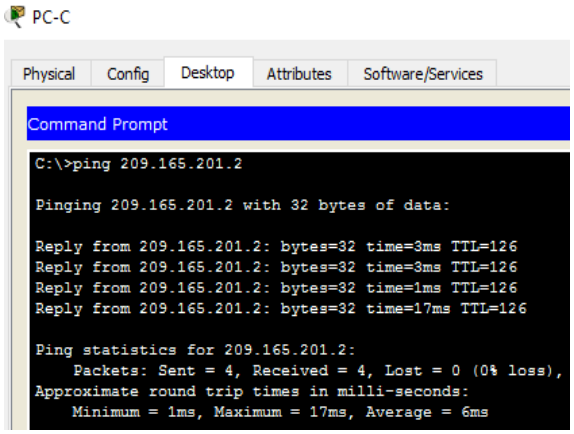
¿En qué forma se proporciona la ruta para el tráfico de Internet en la tabla de routing?

Esta ruta S* 0.0.0.0/0 [1/0] via 209.165.201.2, R2 tiene una ruta estática por defecto a través de la ruta 209.165.201.2 la cual está directamente conectada a G0/0

Paso 6. Verifique la conectividad.

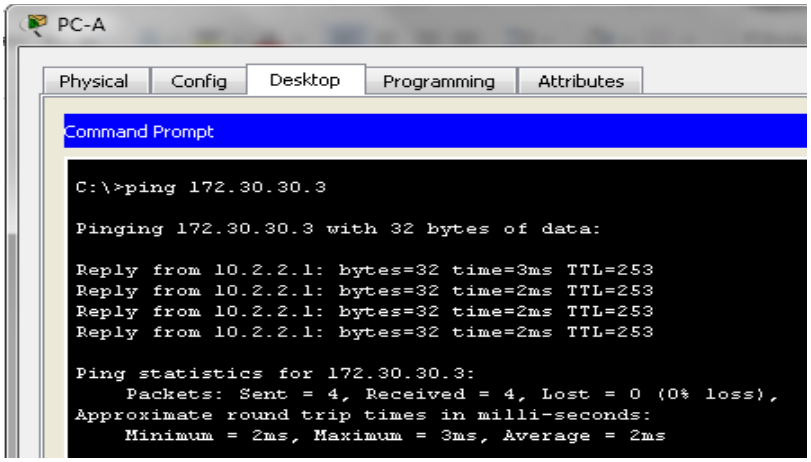
iii. Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 209.165.201.2





iv. Verifique que los hosts dentro de la red dividida en subredes tengan posibilidad de conexión entre ¿Tuvieron éxito los pings?

Nota: quizá sea necesario deshabilitar el firewall de las computadoras sí haciendo ping entre la PC-A y la PC-C.



¿Tuvieron éxito los pings?

SI

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.

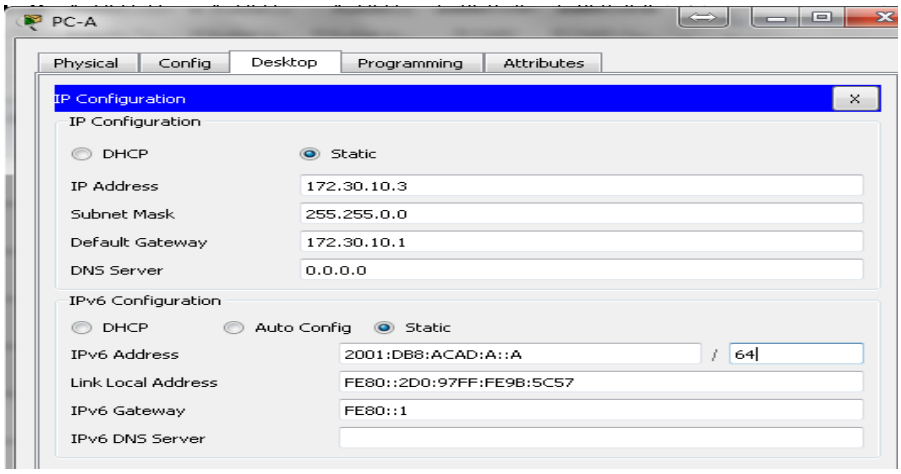
Nota: la asignación de una dirección IPv6 además de una dirección IPv4 en una interfaz se conoce como “dual-stacking” (o apilamiento doble). Esto se debe a que las pilas de protocolos IPv4 e IPv6 están activas.

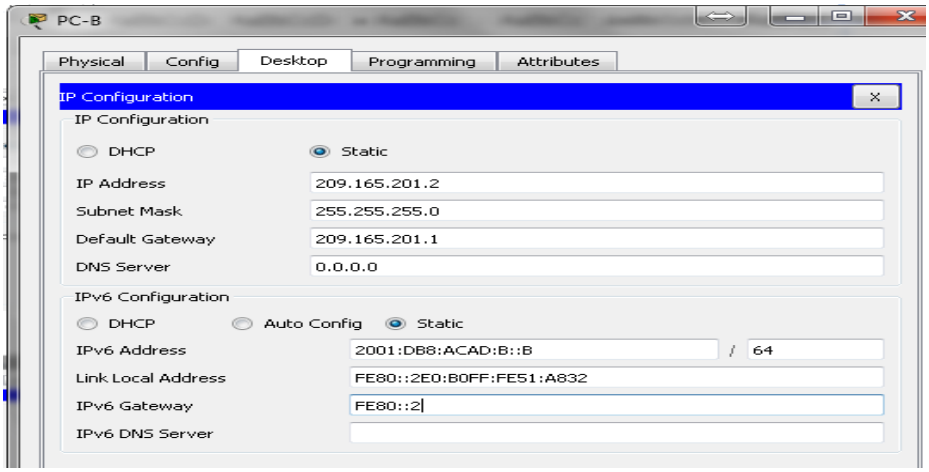
a. Para cada interfaz del router, asigne la dirección global y la dirección link local de la tabla de direccionamiento.

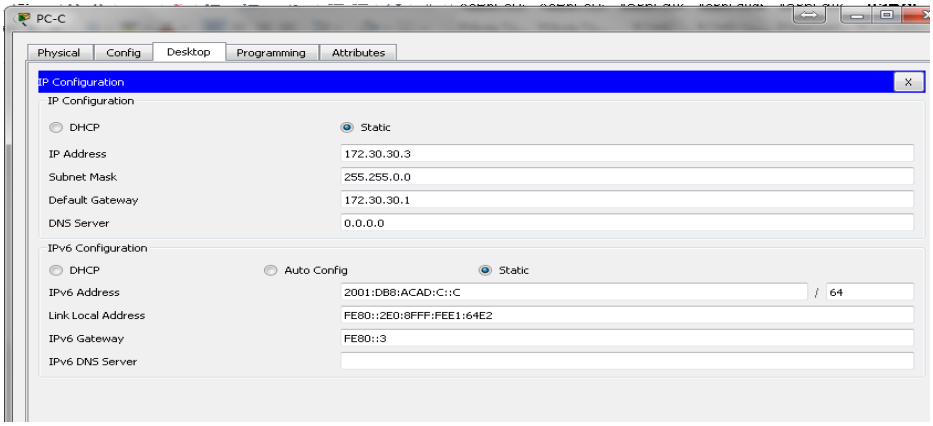
```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#
```

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int 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)#int 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)#int 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)#
```

```
R3>en
Password:
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int g0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#FE80::3 link-local
               ^
% Invalid input detected at '^' marker.

R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#
```







b. Habilite el routing IPv6 en cada router

```
R1(config)#ipv6 unicast-routing
R1(config)#
```

```
R2(config)#ipv6 unicast-routing
R2(config)#
```

```
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

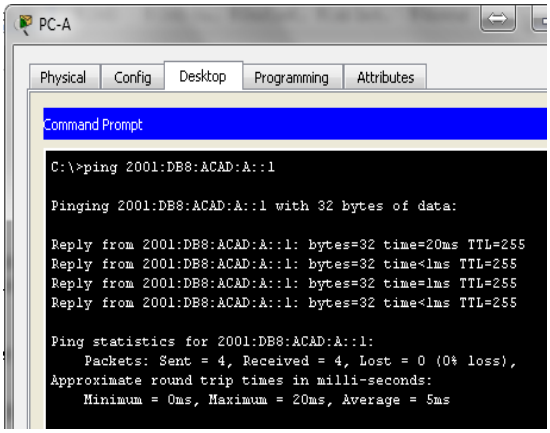
show ipv6 interface brief

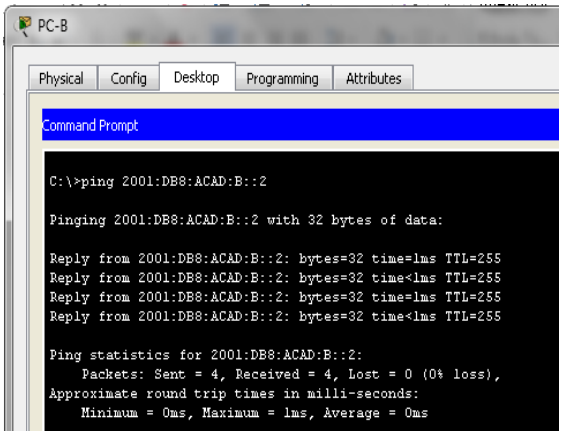
```
R1#show ipv6 interface brief
GigabitEthernet0/0          [administratively down/down]
GigabitEthernet0/1          [up/up]
    FE80::1
    2001:DB8:ACAD:A::1
Serial0/0/0                 [up/up]
    FE80::1
    2001:DB8:ACAD:12::1
Serial0/0/1                 [administratively down/down]
Vlan1                       [administratively down/down]
R1#
```

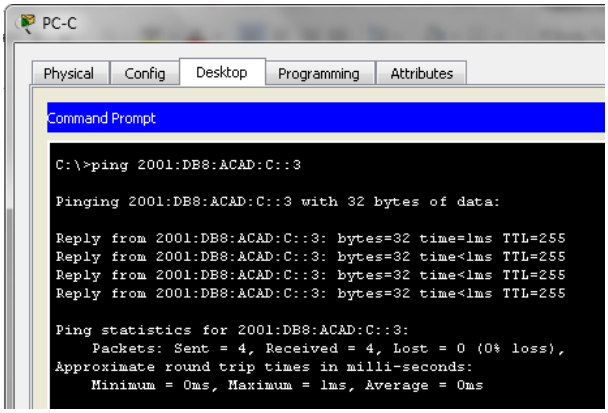
```
R2#show ipv6 interface brief
GigabitEthernet0/0          [up/up]
    FE80::2
    2001:DB8:ACAD:B::2
GigabitEthernet0/1          [administratively down/down]
Serial0/0/0                 [up/up]
    FE80::2
    2001:DB8:ACAD:12::2
Serial0/0/1                 [up/up]
    FE80::2
    2001:DB8:ACAD:23::2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

```
R3#show ipv6 interface 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#
```

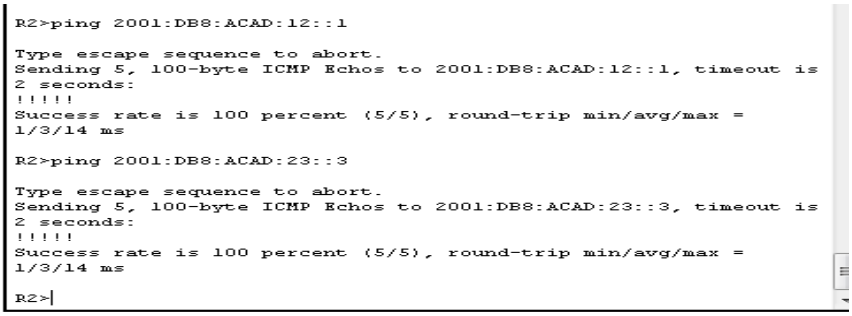
c. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.







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



Parte 4: configurar y verificar el routing RIPng

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

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**

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface 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

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface s0/0/0
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
```

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

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

R3#
```

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**

```
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#
```

¿En qué forma se indica RIPng en el resultado?

RIPng esta listado por el nombre del proceso

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

R1# **show ipv6 rip Test1**

```
R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 31
     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:
```

¿Cuáles son las similitudes entre RIPv2 y RIPng?

RIPv2 y RIPng tienen una distancia administrativa de 120 y usan en 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.

Show ipv6 route

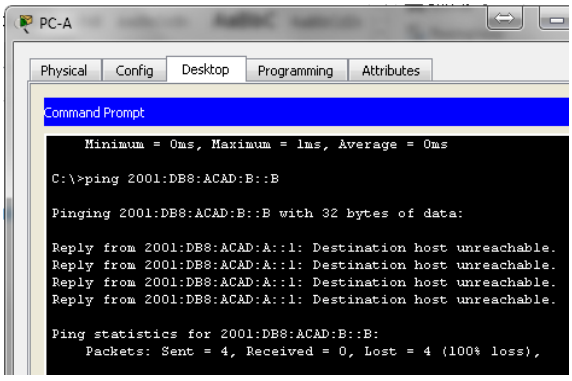
En el R1, ¿cuántas rutas se descubrieron mediante RIPng? **2**

En el R2, ¿cuántas rutas se descubrieron mediante RIPng? **2**

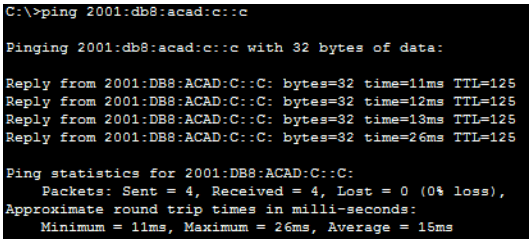
En el R3, ¿cuántas rutas se descubrieron mediante RIPng? **2**

g.Verifique la conectividad entre las computadoras.

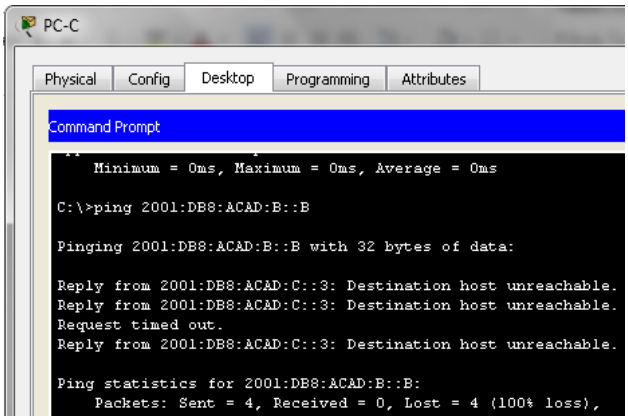
¿Es posible hacer ping de la PC-A a la PC-B? **NO**



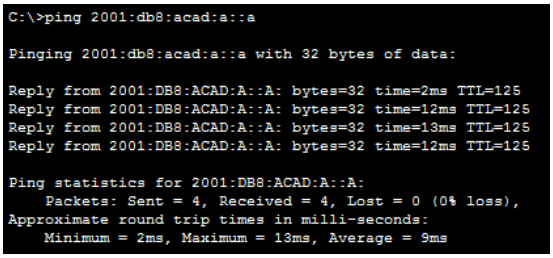
¿Es posible hacer ping de la PC-A a la PC-C? **SI**



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



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



¿Por qué algunos pings tuvieron éxito y otros no?

No ha sido asignada una ruta para la red 2001:DB8:ACAD:B::/64

Pas0 2. Configurar y volver a distribuir una ruta predeterminada.

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

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#Ipv6 route ::0/64 2001:DB8:ACAD:B::B
```

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

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

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

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

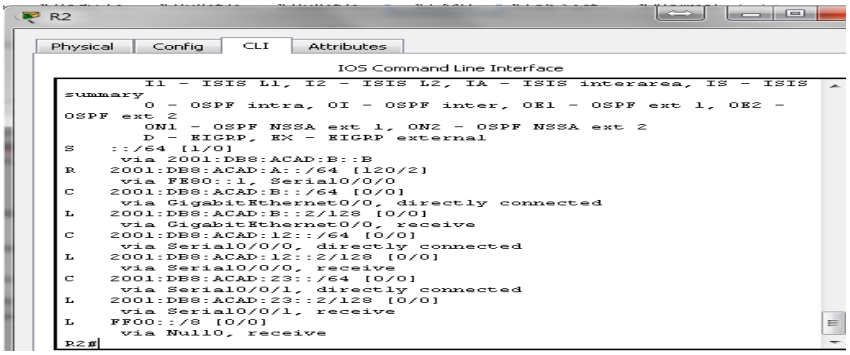
R2(config-rtr)# **ipv6 rip Test2 default-information originate**

```
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)#
```

Paso3. Verificar la configuración de enrutamiento.

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

R2# **show ipv6 route**



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

Ya que presenta la ruta estática ::/64 por defecto

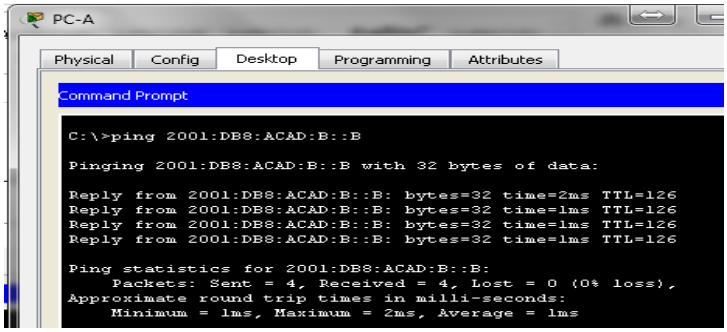
b.Consulte las tablas de routing del R1 y el R3.

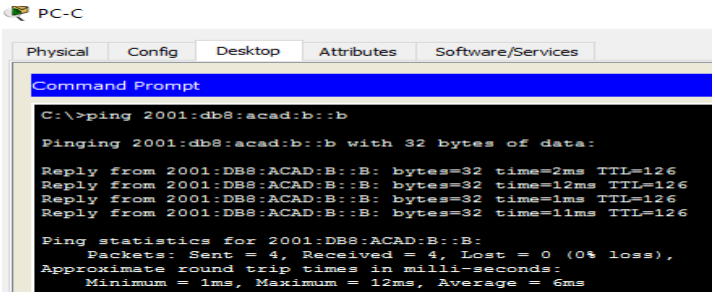
¿Cómo se proporciona la ruta para el tráfico de Internet en sus tablas de enrutamiento?

R ::/0 [120/2] via FE80::2, serial 0/0/0

Paso4. Verifique la conectividad.

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





¿Tuvieron éxito los pings? **SI**

Reflexión

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

   Para que los routers no sumaricen las rutas de acuerdo a la clase mayor

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

   De acuerdo a actualizaciones de rip recibidas desde el router donde fue configurada la ruta por defecto

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

   RIPv2 se configura identificando las redes y RIPng 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.

8.2.4.5 Práctica de laboratorio: configuración de OSPFv2 básico de área única

Topología

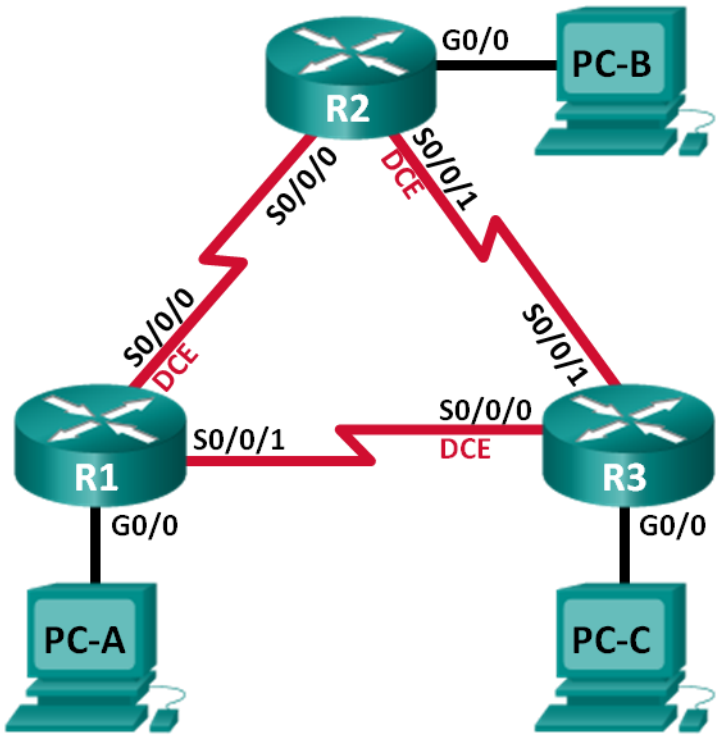


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/1/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/1/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/1/0	192.168.12.2	255.255.255.252	N/A
	S0/1/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/1/1 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/1/0	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 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 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. **OK**

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

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

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

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

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

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

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

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

Step 4: configurar los equipos host. OK

Step 5: Probar la conectividad. OK

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. OK

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

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

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

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

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

Step 2: Configure OSPF en el R2 y el R3. OK

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. OK

a. 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
```

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

```
R1# show ip route
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?

R/

El comando adecuado para visualizar solo rutas ospf es: **show ip route ospf**

Step 4: verificar la configuración del protocolo OSPF. OK

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. OK

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 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of 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. OK

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

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

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

```
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. OK

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. OK

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. OK

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. OK

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.
OK

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

```
R1# show ip ospf neighbor

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
```

b. 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/

Utiliza la interface **serial0/1/1**

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

R/

El costo para la conexión de la red 192.168.2.0/24 en el R3 es: **129**, distribuido así: 64 enlace serial0/1/1 R3, 64 enlace serial0/1/0 R1, 1 interface GR R2.

¿El R2 aparece como vecino OSPF en el R1?

R/

El R2 **SI** aparece como vecino OSPF del R1, mediante la ID Neighbor 22.22.22.22. IP 192.168.12.2 y serial0/10

¿El R2 aparece como vecino OSPF en el R3?

R/

El R2 **NO** aparece como vecino OSPF del R3, lo cual puede indicar que si bien R3 puede encontrar una ruta hacia R2 es mediante R1.

¿Qué indica esta información?

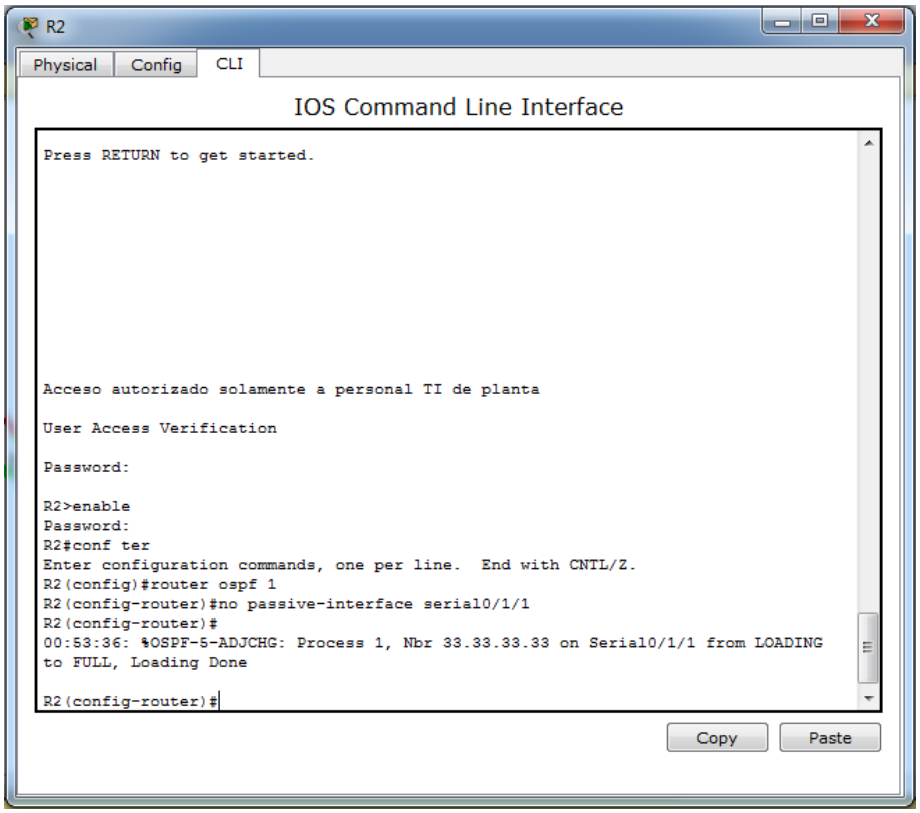
R/

La información anterior en conjunto indica que para que un paquete de datos enviado desde la LAN de R3 alcance la LAN de R2, se debe enrutar a través de la interface serial0/1/1 del R3 por medio de las interfaces seriales de R1. Esto lo confirma el costo de la métrica que es 129.

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

R/

A continuación pantallzo de la CLI de R2, donde se han emitido los comandos suficientes y necesarios para habilitar la interface serial0/1/1 (en nuestro caso).



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/

Utiliza la interface **serial0/1/0**

¿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 para la conexión de la red 192.168.2.0/24 en el R3 es: **65**, distribuido así: 64 enlace serial0/1/0 R3, 1 interface GE R2.

Calculado así: $costo = BW\ Referencia \div BW\ Interfaz$

$$costo_{G0/0} = 100.000.000 \div 100.000.000 = 1$$

$$costo_{serial\ 0\ /\ 1\ /0} = 100.000.000 \div 1.544.000 = 64$$

¿El R2 aparece como vecino OSPF del R3?

R/

El R2 **SI** aparece como vecino OSPF del R3, mediante la ID Neighbor 22.22.22.22. IP 192.168.23.1 y serial0/10

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. OK

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?

R/

Es necesario cambiar el ancho de banda predeterminado dado que para el cálculo del costo de las métricas se utiliza la siguiente formula: $costo = BW\ Referencia \div BW\ Interfaz$, luego cualquier valor mayor o igual al ancho de banda de referencia tendrá como costo el valor de 1. Cando queremos tener una métrica mejor ajustada para efectos de cálculo del cost, es indispensable ampliar el ancho de banda de referencia.

Step 2: cambiar el ancho de banda de una interfaz. OK

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.

R/

El costo para la conexión de la red 192.168.3.0/24 en el R1 es: **782**, distribuido así: 781 enlace serial0/1/1 R1, 1 interface GE R3.

Calculado así: $costo = BW\ Referencia \div BW\ Interfaz$

$$\boldsymbol{costo_{G0/0} = 100.000.000 \div 100.000.000 = 1}$$

$$\boldsymbol{costo_{serial\ 0\ /\ 1\ /\ 1} = 100.000.000 \div 128.000 = 781}$$

El costo para la conexión de la red 192.168.23.0/30 en el R1 es: **845**, distribuido así: 781 enlace serial0/1/1 R1, 64 interface serial0/1/0 R3.

Calculado así: $costo = BW\ Referencia \div BW\ Interfaz$

$$\boldsymbol{costo_{serial\ 0\ /\ 1\ /\ 0} = 100.000.000 \div 1.544.000 = 64}$$

$$\boldsymbol{costo_{serial\ 0\ /\ 1\ /\ 1} = 100.000.000 \div 128.000 = 781}$$

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?

R/

El nuevo costo acumulado para la conexión de la red 192.168.23.0/30 en el R1 es: **1562**, distribuido así: 781 enlace serial0/1/1 R1, 781 interface serial0/1/0 R3.

Calculado así: $costo = BW\ Referencia \div BW\ Interfaz$

$$costo_{serial\,0/1/0} = 100.000.000 \div 128.000 = 781$$

$$costo_{serial\,0/1/1} = 100.000.000 \div 128.000 = 781$$

Lo anterior se debe a que todos los enlaces seriales ahora se encuentra con un BW configurado de 128 kbps.

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.

R/

Se debe básicamente al costo de la ruta, es decir, al configurar la interface serial0/1/1 del R1 con un valor de costo igual a 1565, el router prefiere la ruta que pasa a travez de R2 ya que el costo de esta ruta es menor 1562, por ésta razón la ruta hacia la red 192.168.3.0/24 que utilizaba el enlace serial0/1/1 entre R1 y R2, ahora sale de la tabla de routing de R1 y se prefiere la ruta a través del R2.

Reflexión

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

   R/

   La ID de ruoter le permite al equipo participar en el dominio OSPF, además que suministra identificación exclusiva, y participación en la elección del router designado o DR.

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

   R/

   Por que la red de topología utilizada en la presente práctica de laboratorio no incluye redes de accesos multiples que conectan a los routers. Los routers de la topología se encuentran enlazados mendite WAN seriales que no requieren la designación DR o BDR.

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

   R/

El motivo fundamental por el cual deseamos configurar una interfaz como pasiva radica en el hecho de evitar propgaciones de dato innecesarias, como por ejemplo en las redes LAN. Esto a su vez constituye uso eficiente de la interfaz y el ancho de banda, suministra mejor seguridad ya que un paquete de datos OSPF si se propaga por una LAN puede ser interceptado, modificado y vuelto a entregar al router quien inició la solicitud, generando tablas de routing y arboles con información poco confiable que afecta el enrutamiento de la información.

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.				

8.3.3.6 Práctica de laboratorio: configuración de OSPFv3 básico de área única

Topología

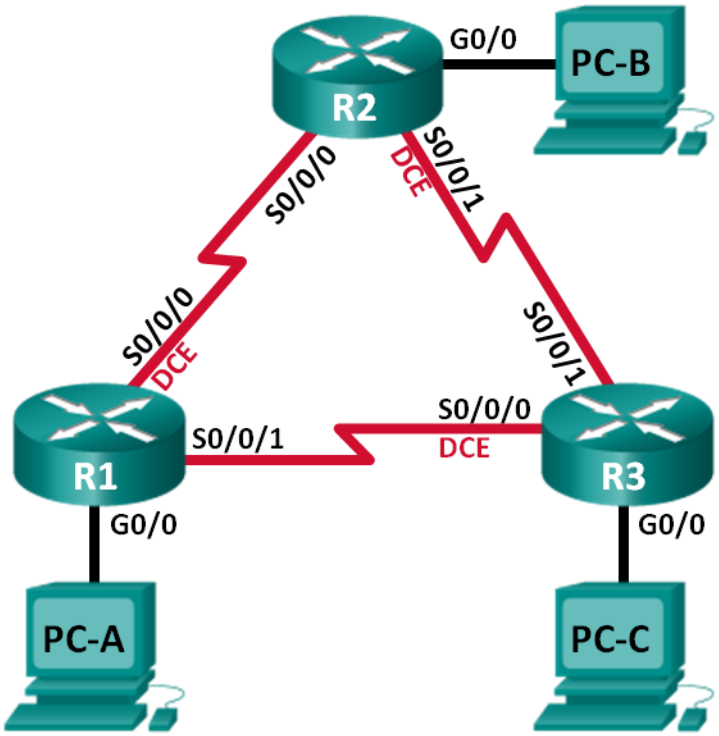


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

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 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 en los equipos host y los routers.

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

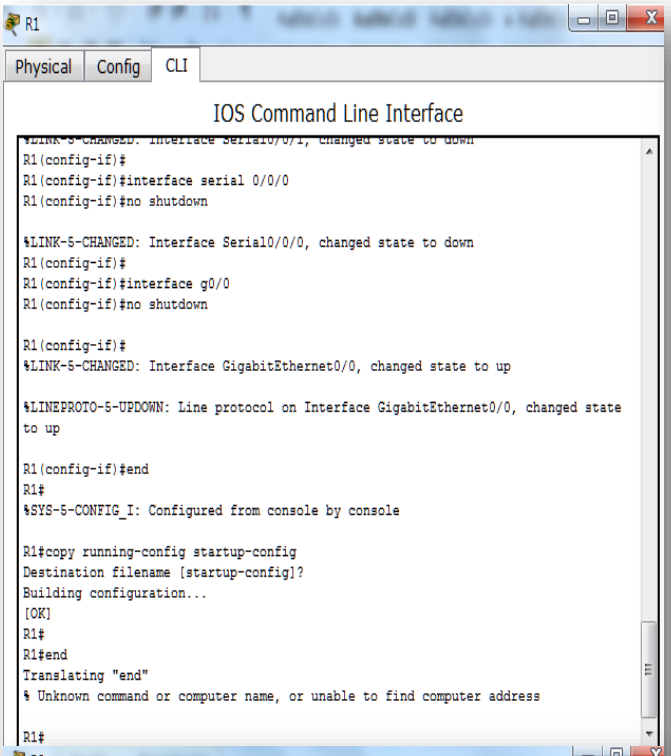
Step 2: inicializar y volver a cargar los routers según sea necesario.

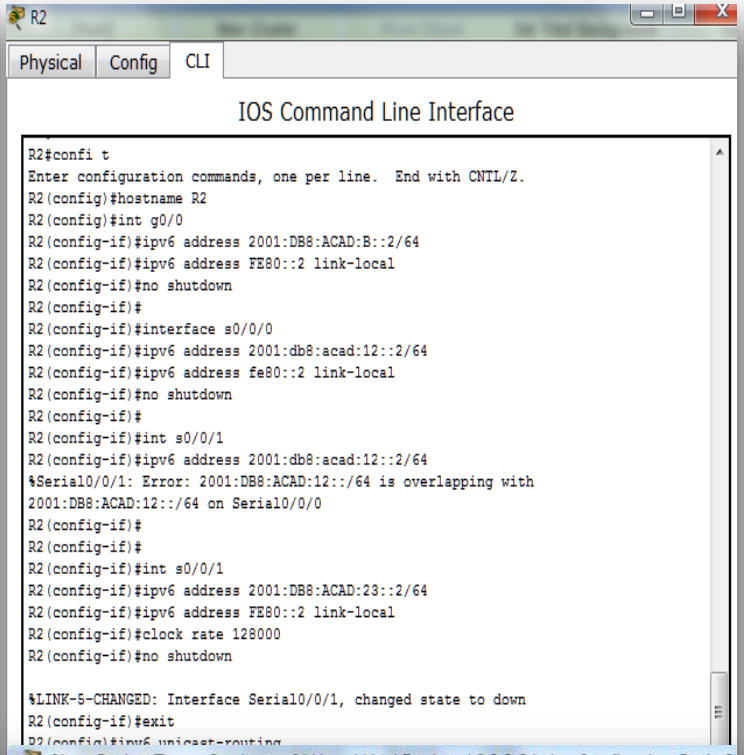
Step 3: configurar los parámetros básicos para cada router.

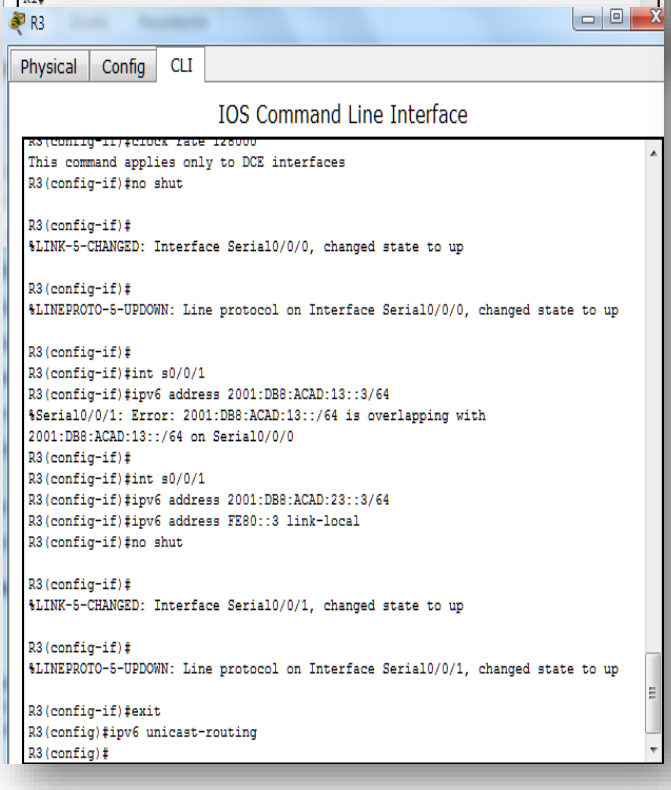
a. Desactive la búsqueda del DNS.
b. Configure el nombre del dispositivo como se muestra en la topología.
c. Asigne **class** como la contraseña del modo EXEC privilegiado.
d. Asigne **cisco** como la contraseña de vty.
e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso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

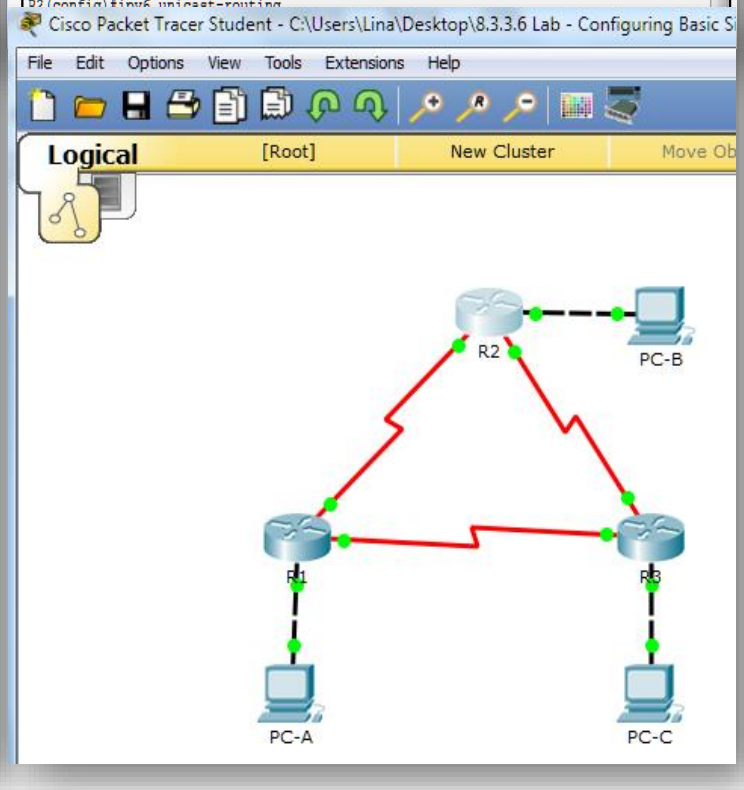
i. Habilite el routing de unidifusión IPv6 en cada router.

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

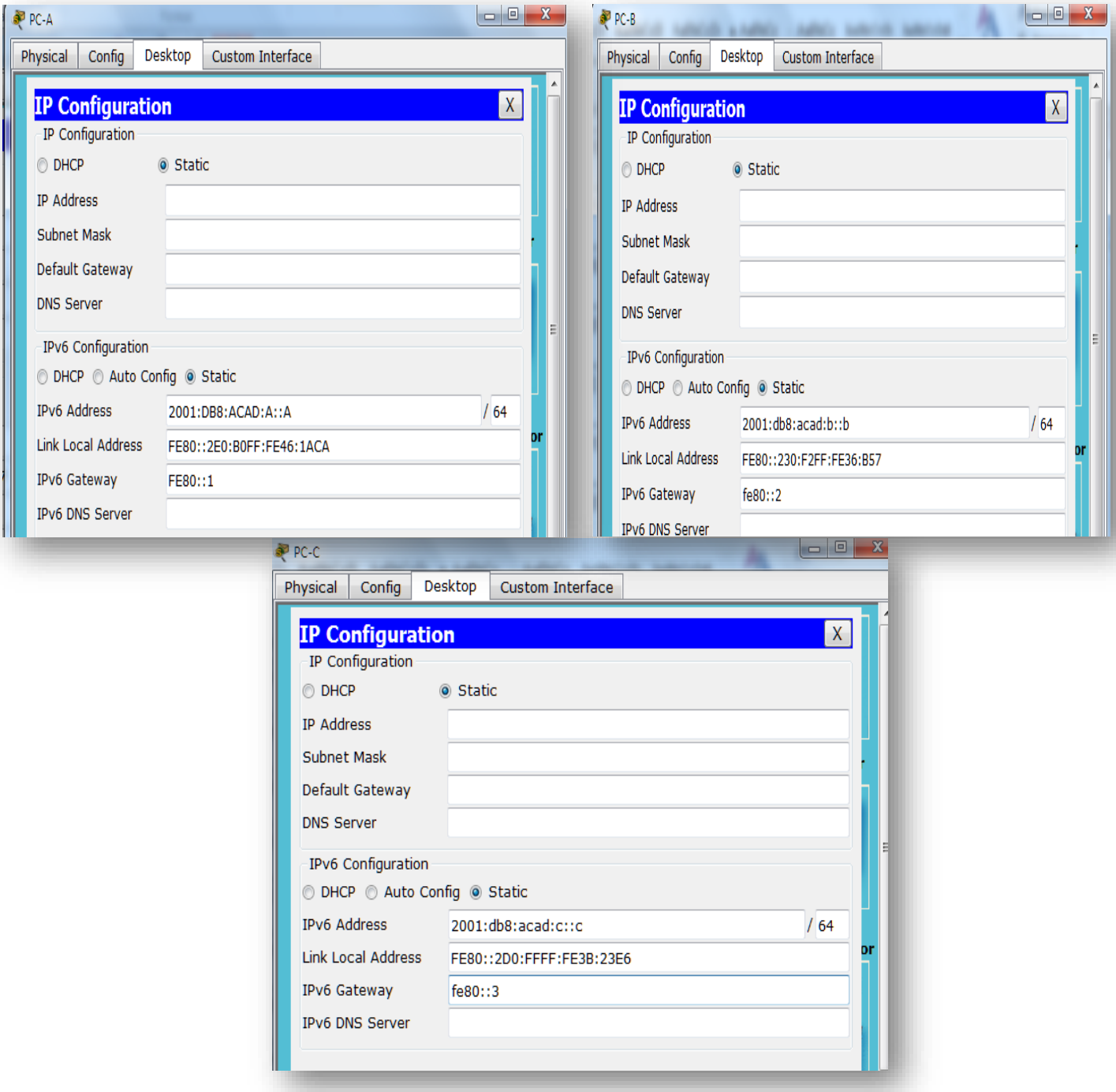






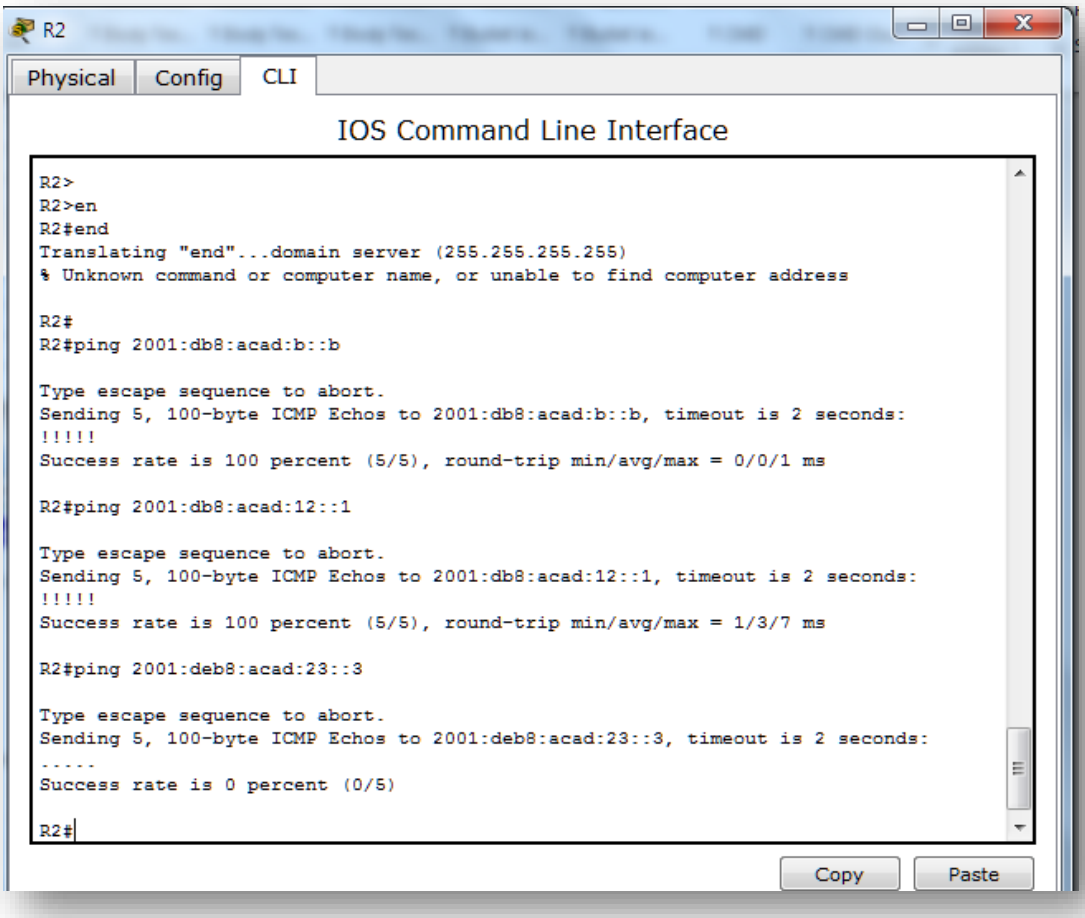


Step 4: configurar los equipos host.



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



Part 2: 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**.

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

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

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

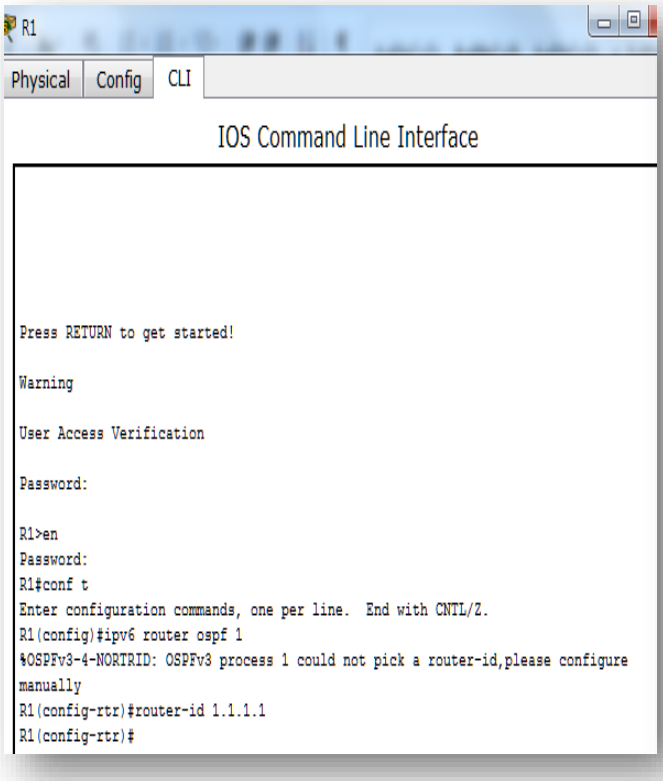
b. Asigne la ID de router OSPFv3 **1.1.1.1** al R1.

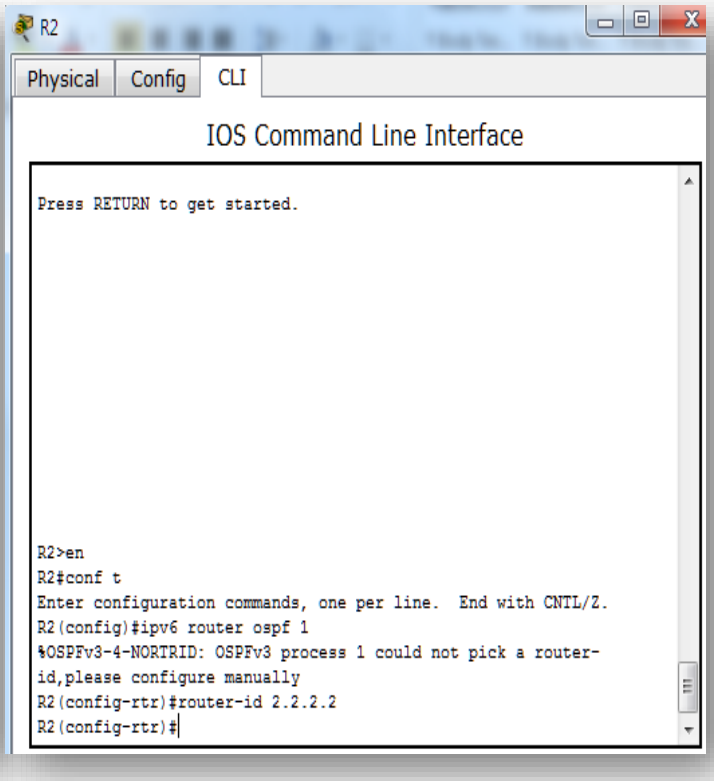
```
R1(config-rtr)# router-id 1.1.1.1
```

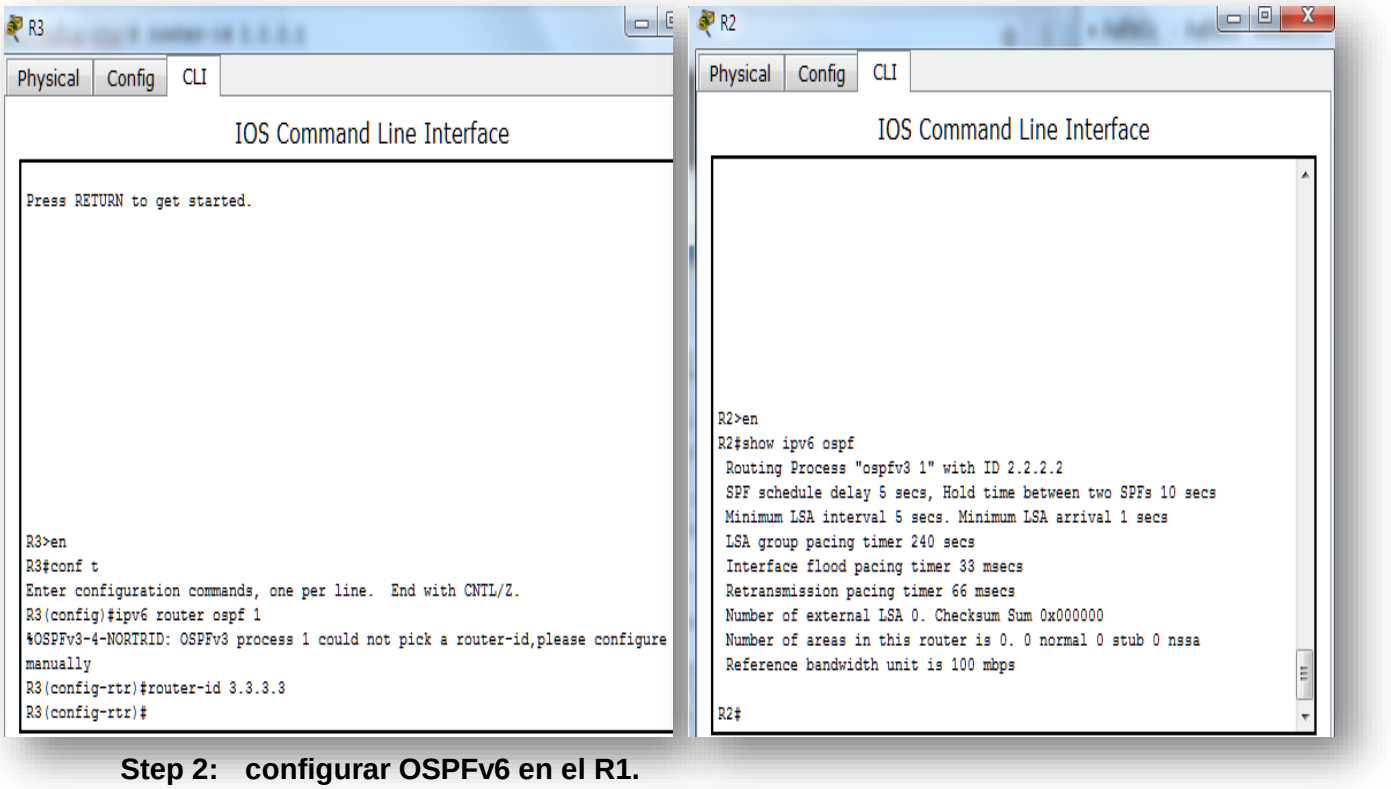
c. Inicie el proceso de routing de OSPFv3 y asigne la ID de router **2.2.2.2** al R2 y la ID de router **3.3.3.3** al R3.

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

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







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
```

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.

```
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
```

R1

Physical | Config | CLI

IOS Command Line Interface

```
Warning

User Access Verification

Password:
Password:
Password:

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

R2

Physical | Config | CLI

IOS Command Line Interface

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

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


R2>en
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#int s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
00:05:00: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

R2(config-if)#int s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
```

R3

Physical | Config | CLI

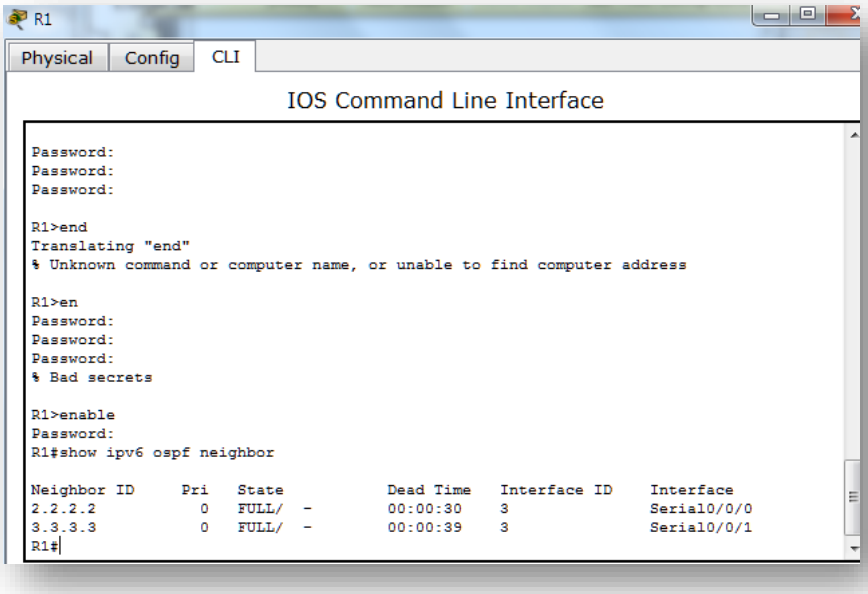
IOS Command Line Interface

```
%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

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


R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int g0/0
R3(config-if)# ipv6 ospf 1 area 0
R3(config-if)#int s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int s0/
00:11:50: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

               ^
% Invalid input detected at '^' marker.

R3(config-if)#int s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
00:12:51: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 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
```

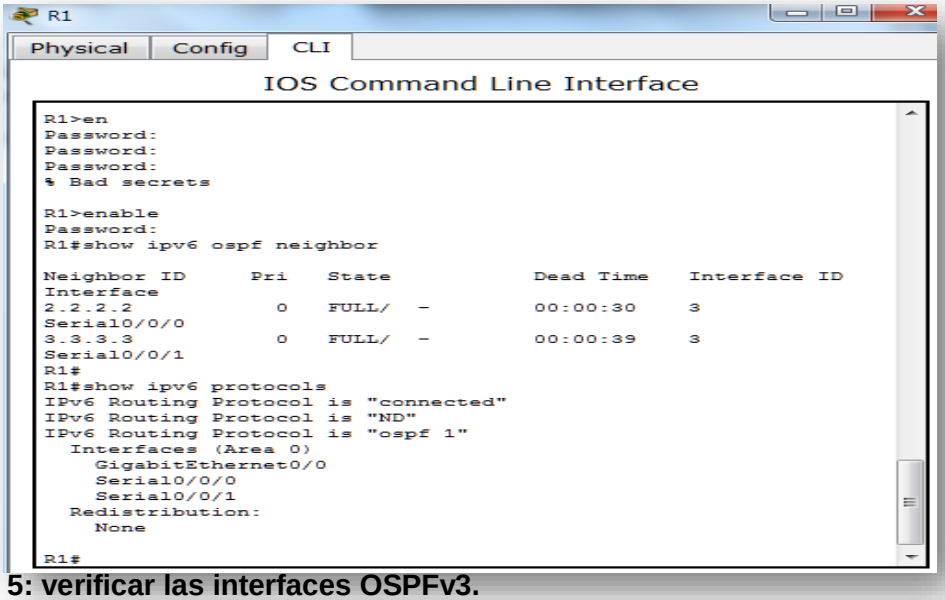


Step 4: verificar la configuración del protocolo OSPFv3.

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
```

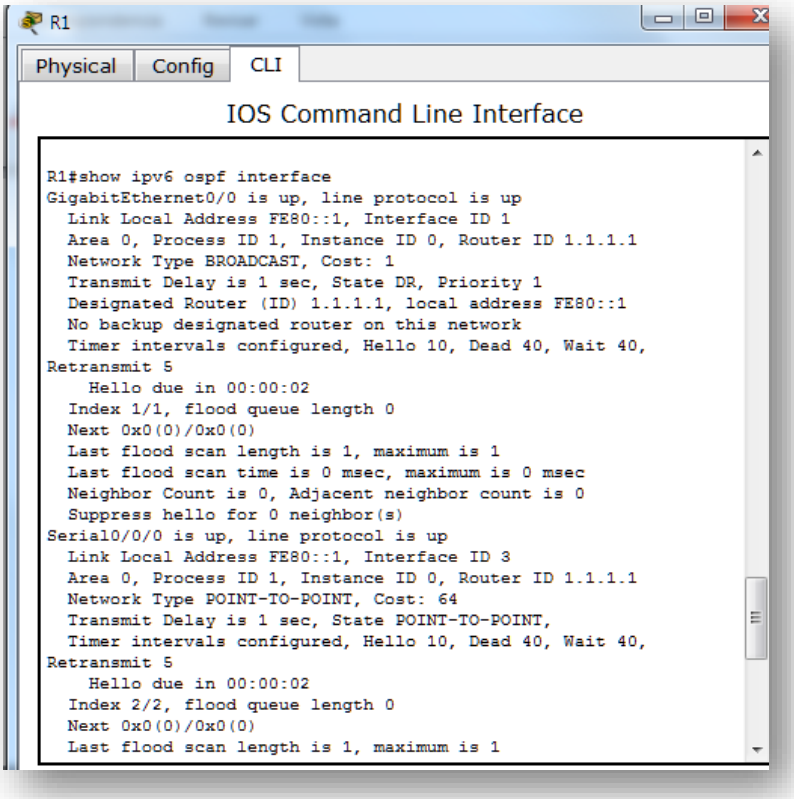


Step 5: verificar las interfaces OSPFv3.

a. 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)
```



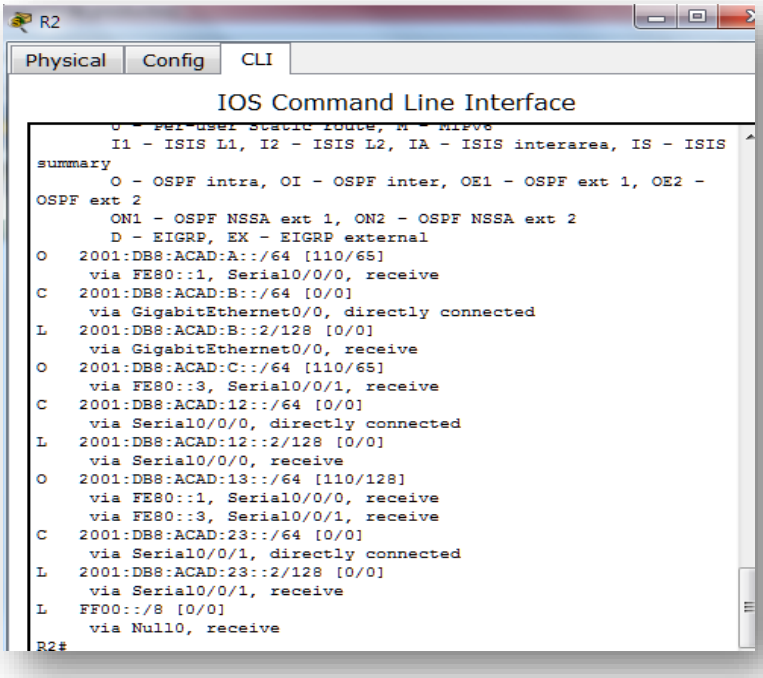
a. Para mostrar un resumen de las interfaces con OSPFv3 habilitado, emita el comando **show ipv6 ospf interface brief**.

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

Step 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
```



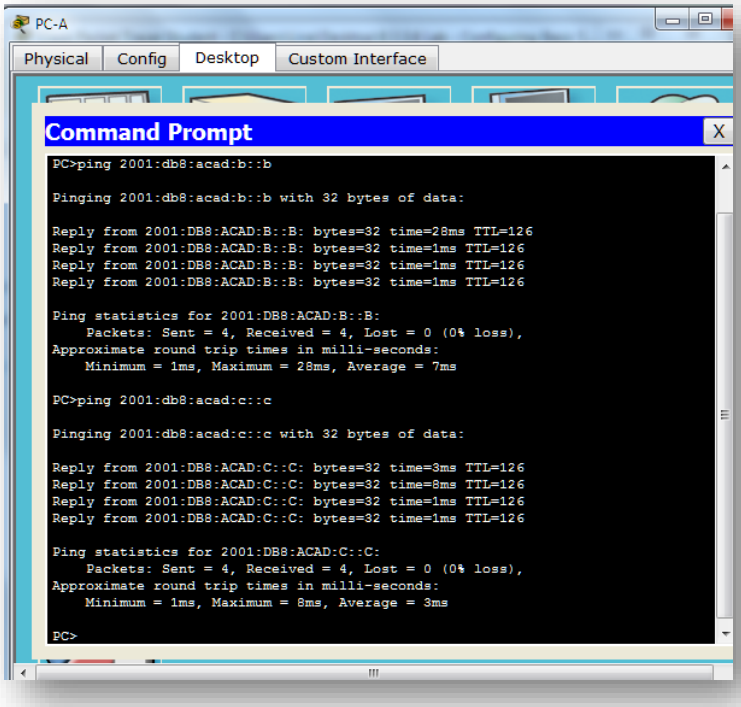
¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?

- **Show ipv6 route ospf**

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.



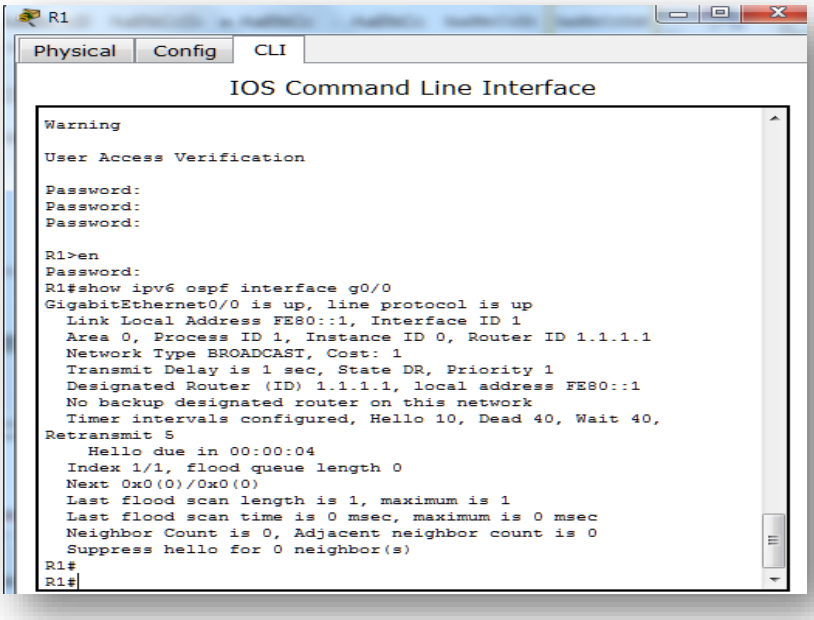
Part 3: configurar las interfaces pasivas de OSPFv3

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.

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

```
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)
```

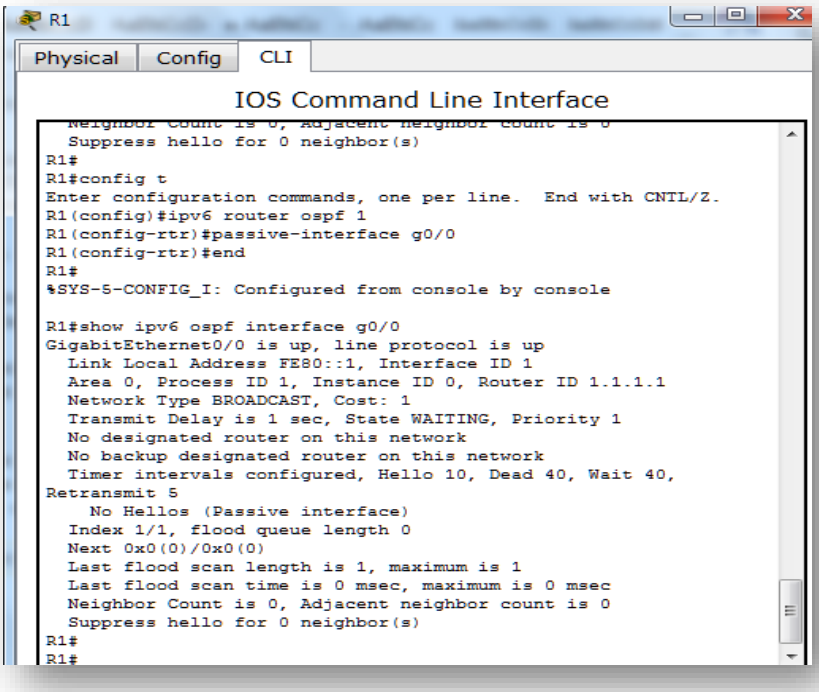


b. Emita el comando **passive-interface** para cambiar la interfaz G0/0 en el R1 a pasiva.

```
R1(config)# ipv6 router ospf 1
R1(config-rtr)# passive-interface g0/0
```

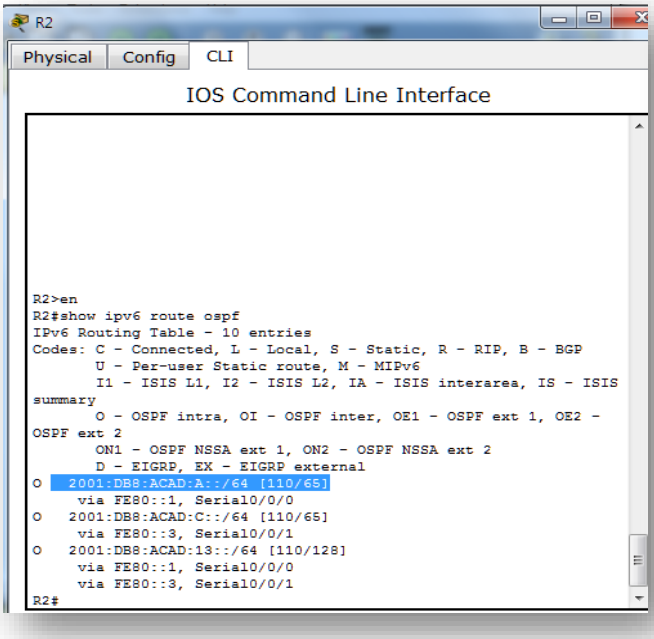
c. Vuelva a emitir el comando **show ipv6 ospf interface g0/0** para verificar que la interfaz G0/0 ahora sea pasiva.

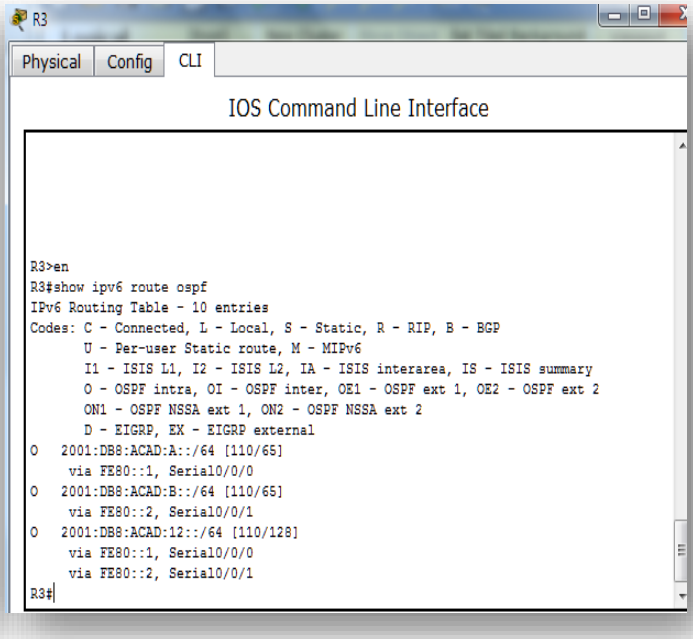
```
R1# show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this 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)
```



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
```

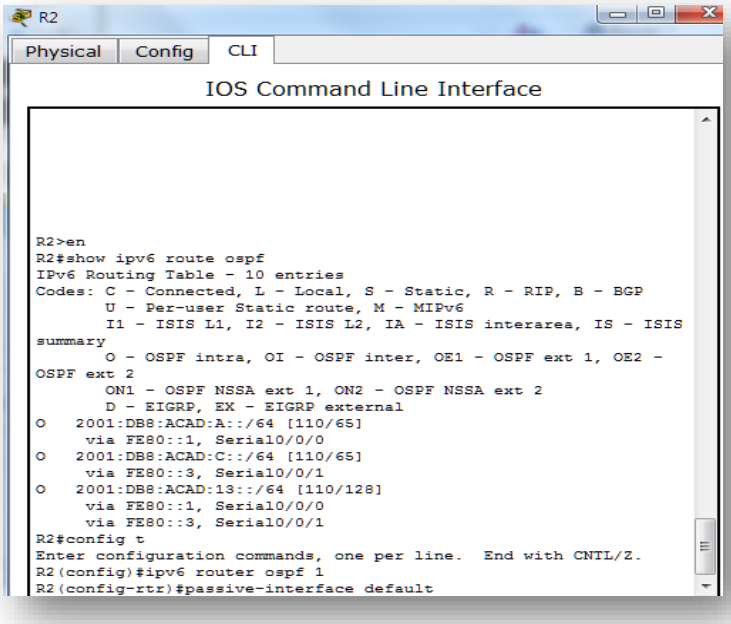




Step 2: establecer la interfaz pasiva como la interfaz predeterminada en el router.

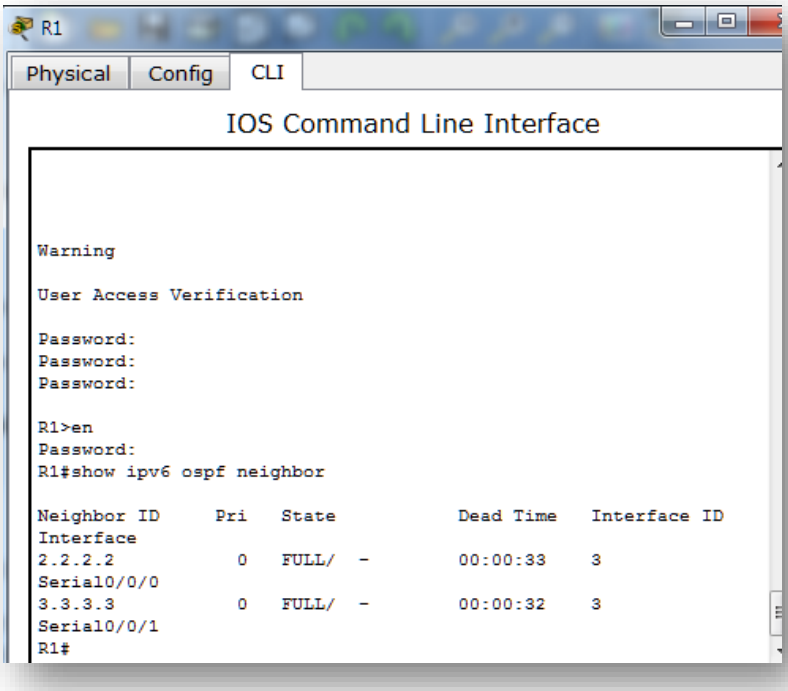
a. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPFv3 como pasivas de manera predeterminada.

```
R2(config)# ipv6 router ospf 1
R2(config-rtr)# passive-interface default
```



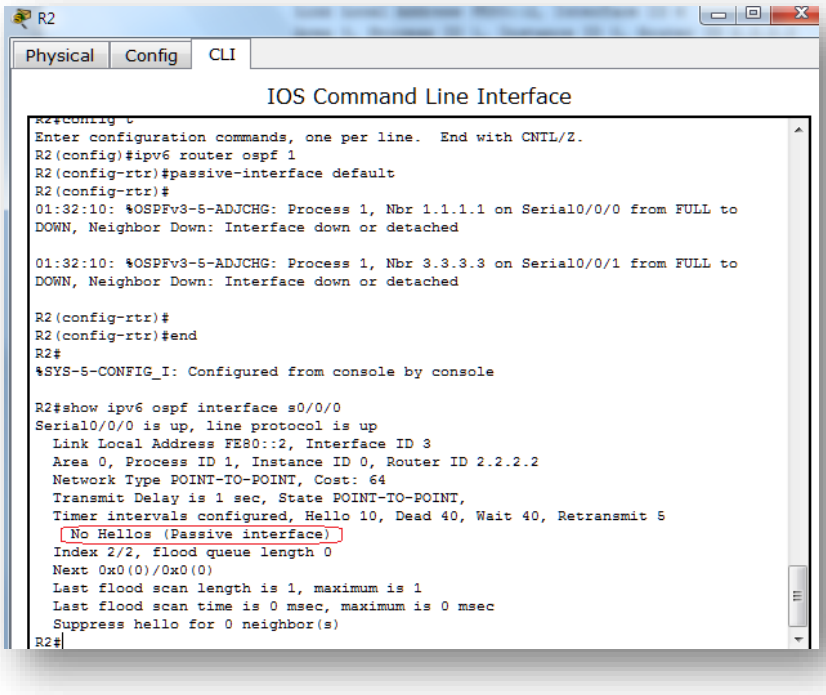
b. Emita el comando **show ipv6 ospf neighbor** en el R1. Una vez que el temporizador de tiempo muerto caduca, el R2 ya no se muestra como un vecino OSPF.

```
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
```

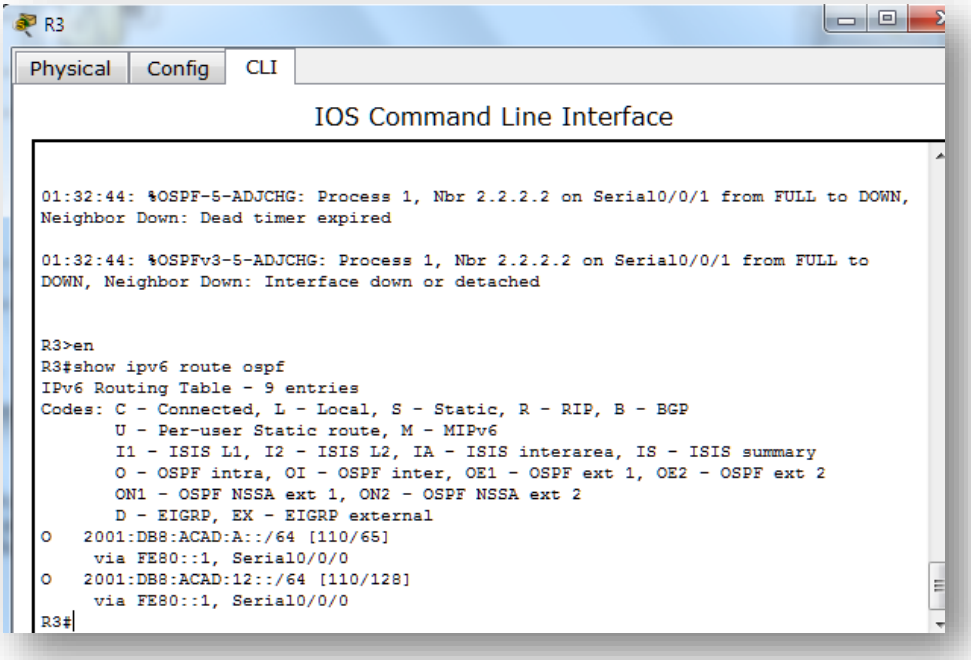


c. En el R2, emita el comando **show ipv6 ospf interface s0/0/0** para ver el estado OSPF de la interfaz S0/0/0.

```
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)
```



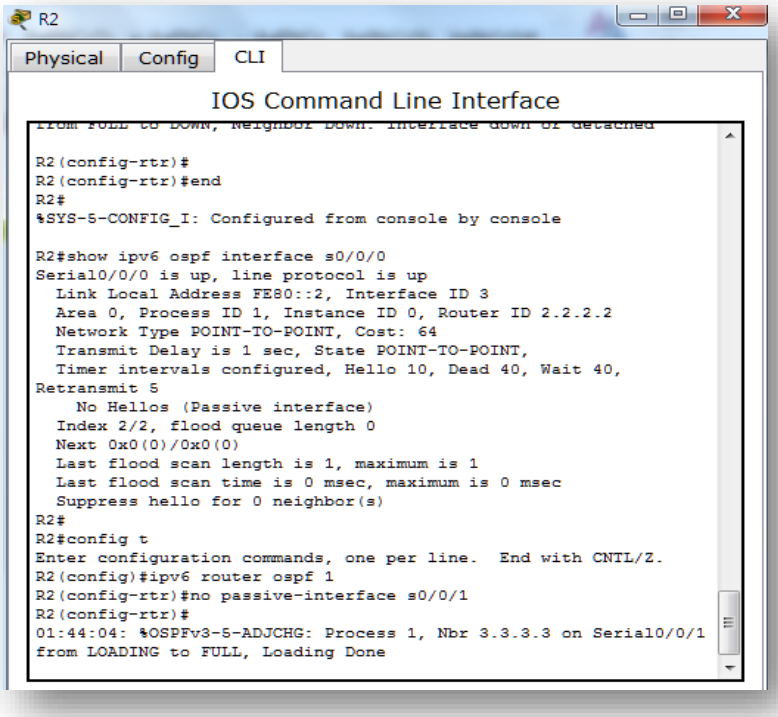
d. Si todas las interfaces OSPFv3 en el R2 son pasivas, no se anuncia ninguna información de routing. Si este es el caso, el R1 y el R3 ya no deberían tener una ruta a la red 2001:DB8:ACAD:B::/64. Esto se puede verificar mediante el comando **show ipv6 route**.



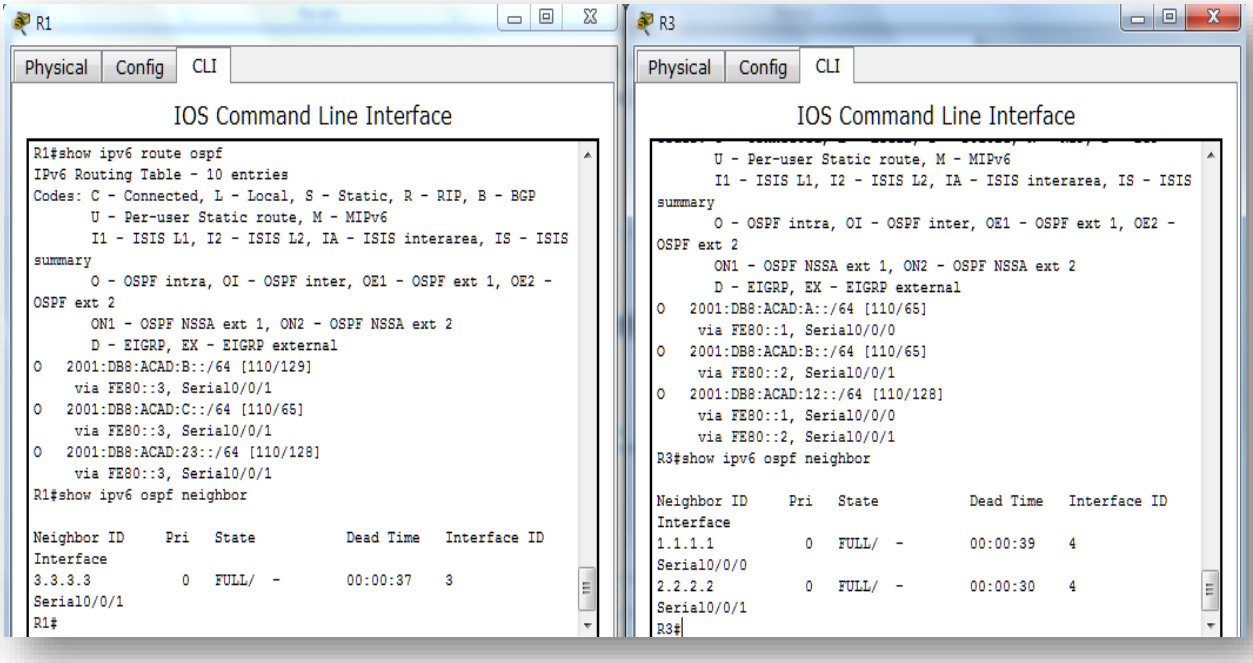
e. Ejecute el comando **no passive-interface** para cambiar S0/0/1 en el R2 a fin de que envíe y reciba actualizaciones de routing OSPFv3. Después de introducir este comando, aparece un mensaje informativo que explica que se estableció una adyacencia de vecino con el R3.

```
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



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



¿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

- Únicamente R3

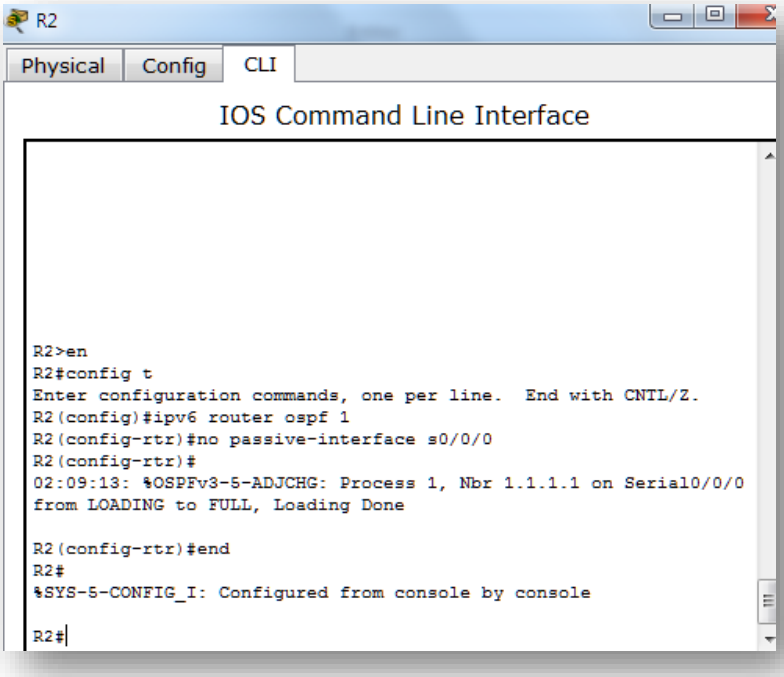
¿El R2 aparece como vecino OSPFv3 en el R3?

- Si

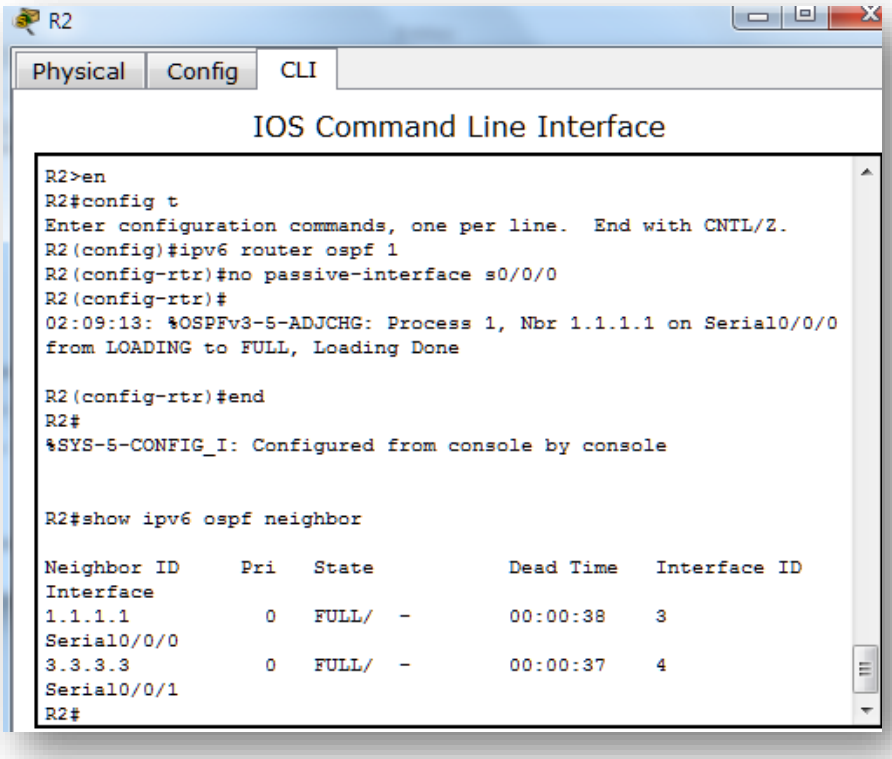
¿Qué indica esta información?

- Todo el tráfico hacia la red b desde R1 será ruteado a través de R3. La interface serial 0 en R2 está un configurada como pasiva, de tal manera que ospfv3 no envía información de ruteo notificándose a través de esta interfaz

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.



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



Reflexión

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

    - Sí, porque el proceso de ospf es solamente usado y es significativamente usado en un router. No necesita coincidir el proceso usado en otro router en la misma área; no tiene que coincidir.

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

    - Removiendo la entrada network ayuda a prevenir los errores en las direcciones ipv6.

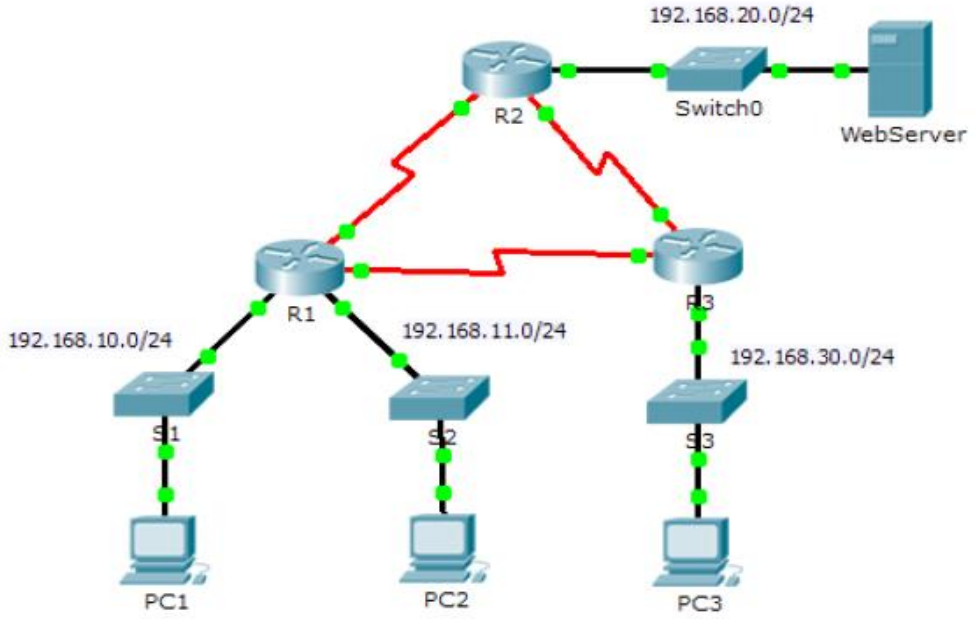
Tabla de resumen de interfaces del router

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.

9.2.1.10 Packet Tracer - Configuring Standard ACLs

Topology



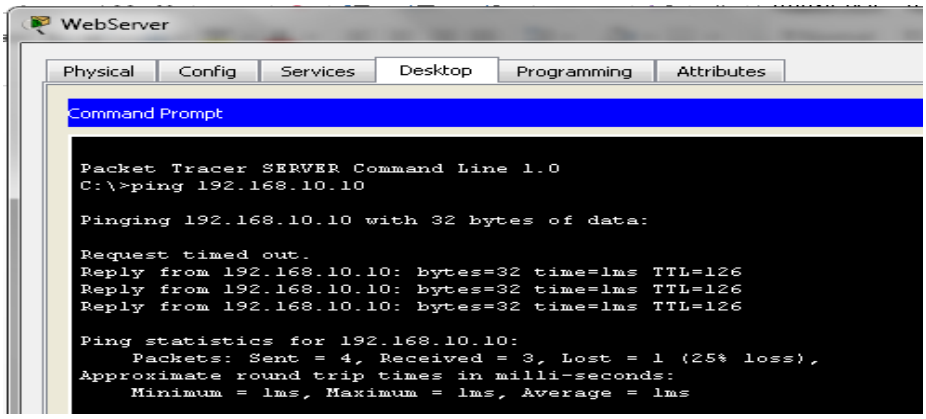
Addressing Table

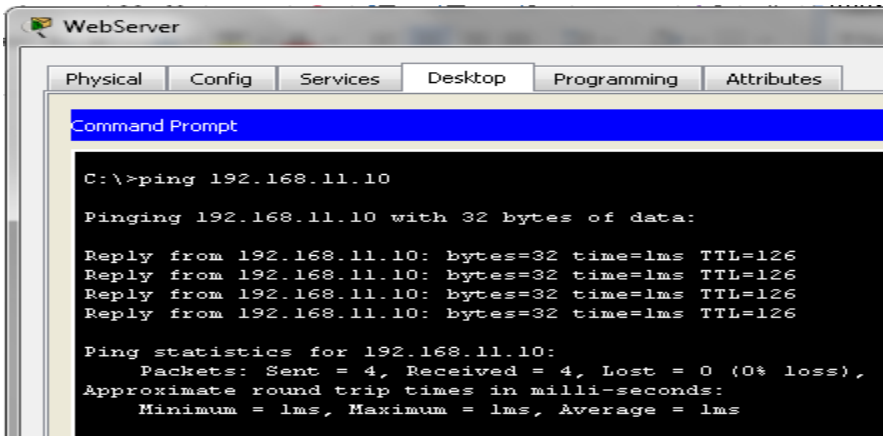
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

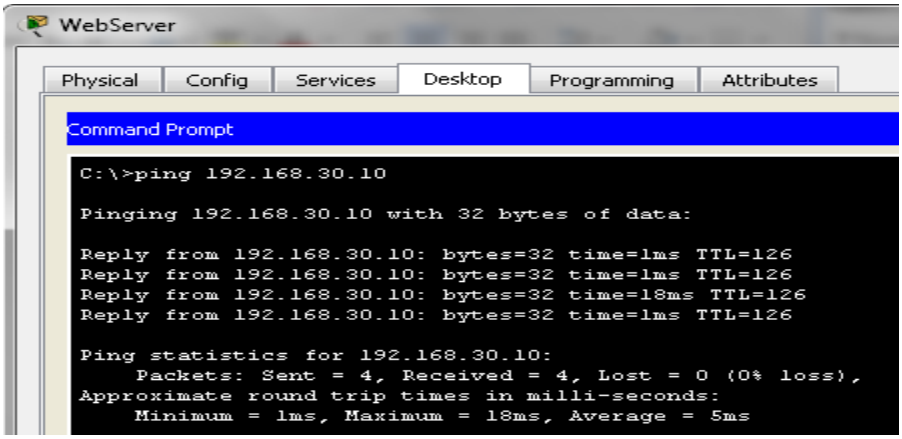
Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device







Step 2: Evaluate two network policies and plan ACL implementations.

a. The following network policies are implemented on **R2**:
   - The 192.168.11.0/24 network is not allowed access to the **WebServer** on the 192.168.20.0/24 network.
   - All other access is permitted.

   To restrict access from the 192.168.11.0/24 network to the **WebServer** at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic

b. The following network policies are implemented on **R3**:
   - The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
   - All other access is permitted.

   To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

a. Create an ACL using the number 1 on **R2** with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network

R2(config)# **access-list 1 deny 192.168.11.0 0.0.0.255**

b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:
R2(config)# **access-list 1 permit any**

c. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.
R2(config)# **interface GigabitEthernet0/0**
R2(config-if)# **ip access-group 1 out**

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

Step 2: Configure and apply a numbered standard ACL on R3.

a. Create an ACL using the number 1 on **R3** with a statement that denies access to the 192.168.30.0/24 network from the **PC1** (192.168.10.0/24) network.
R3(config)# **access-list 1 deny 192.168.10.0 0.0.0.255**

b. By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, create a second rule for ACL 1.
R3(config)# **access-list 1 permit any**

c. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.
R3(config)# **interface GigabitEthernet0/0**
R3(config-if)# **ip access-group 1 out**

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
```

Step 3: Verify ACL configuration and functionality.

a. On **R2** and **R3**, enter the **show access-list** command to verify the ACL configurations. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.

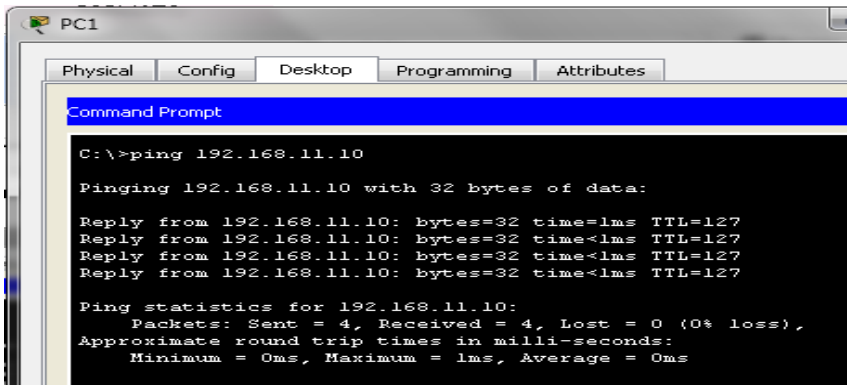
```
R2#show access-list
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255
    20 permit any

R2#
```

```
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 unreachables 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
```

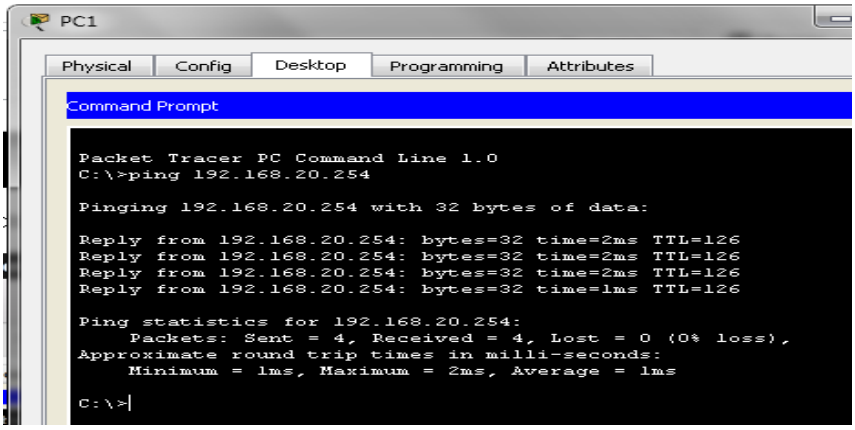
```
R3#show access-list
Standard IP access list 1
    10 deny 192.168.10.0 0.0.0.255
    20 permit any

R3#
```

```
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 unreachables 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
```

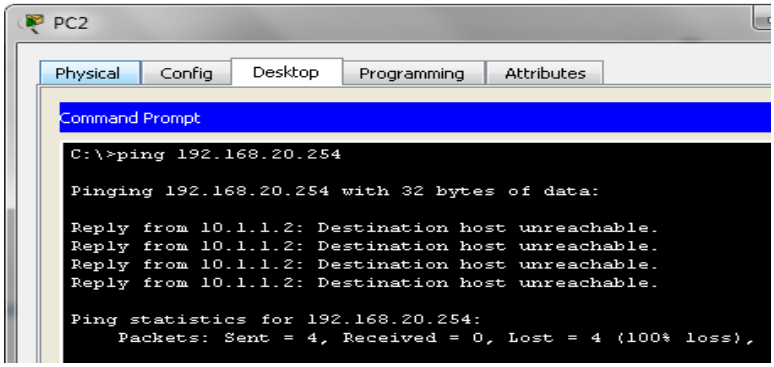
b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:
   - A ping from 192.168.10.10 to 192.168.11.10 succeeds.



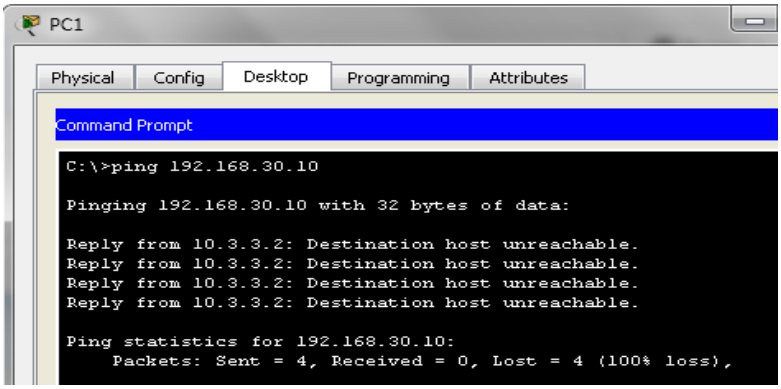
   - A ping from 192.168.10.10 to 192.168.20.254 succeeds.



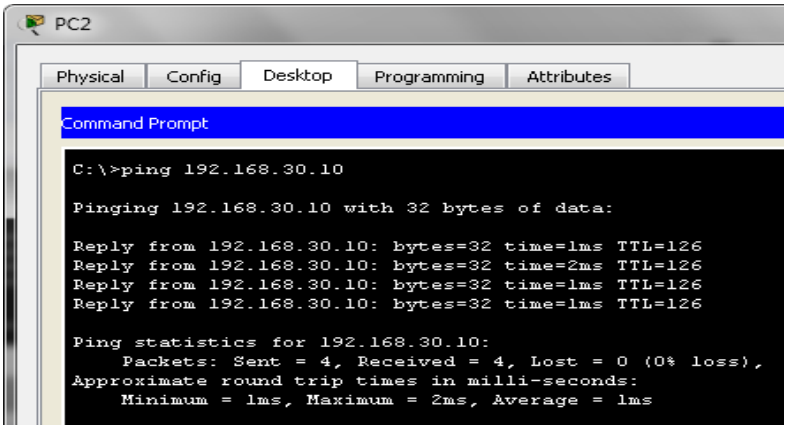
- A ping from 192.168.11.10 to 192.168.20.254 fails.



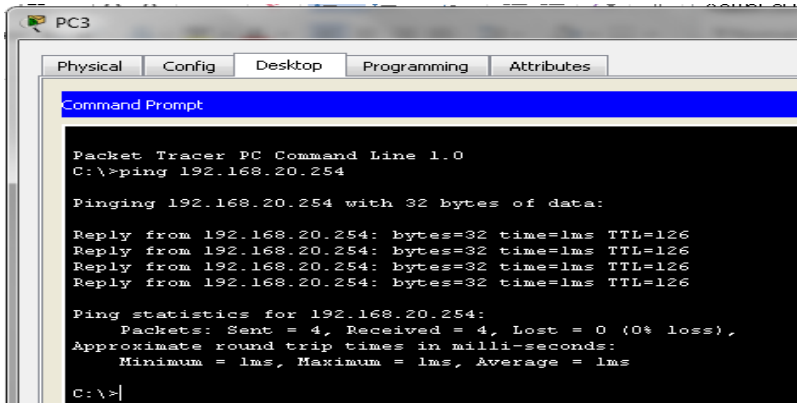
- A ping from 192.168.10.10 to 192.168.30.10 fails.

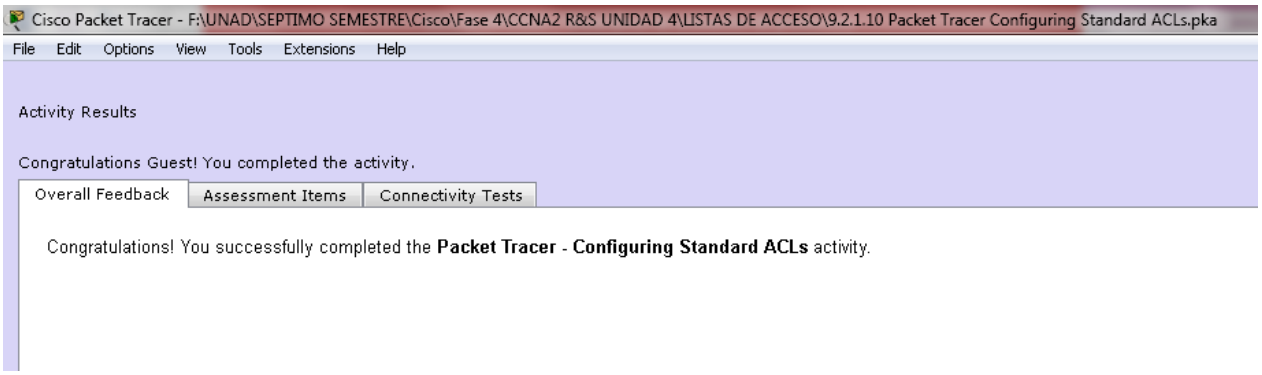


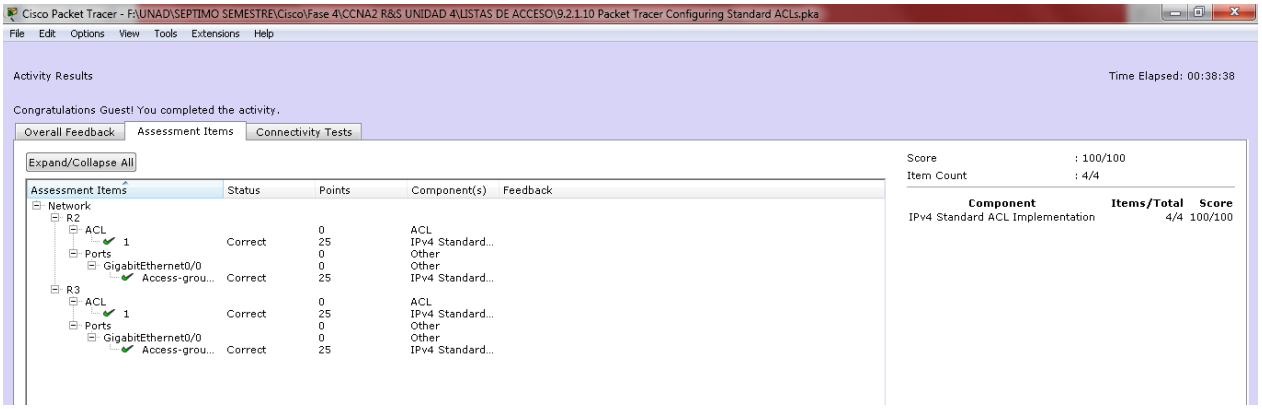
- A ping from 192.168.11.10 to 192.168.30.10 succeeds.



- A ping from 192.168.30.10 to 192.168.20.254 succeeds.







Actividad 9.2.1.11 – Configuración de ACL estándares nombradas.

Tabla de Direccionamiento.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	F0/0	192.168.10.1	255.255.255.0	No aplicable
	F0/1	192.168.20.1	255.255.255.0	No aplicable
	E0/0/0	192.168.100.1	255.255.255.0	No aplicable
	E0/1/0	192.168.200.1	255.255.255.0	No aplicable
Servidor de archivos	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Servidor web	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objetivos

Parte 1: configurar y aplicar una ACL estándar con nombre

Parte 2: verificar la implementación de la ACL

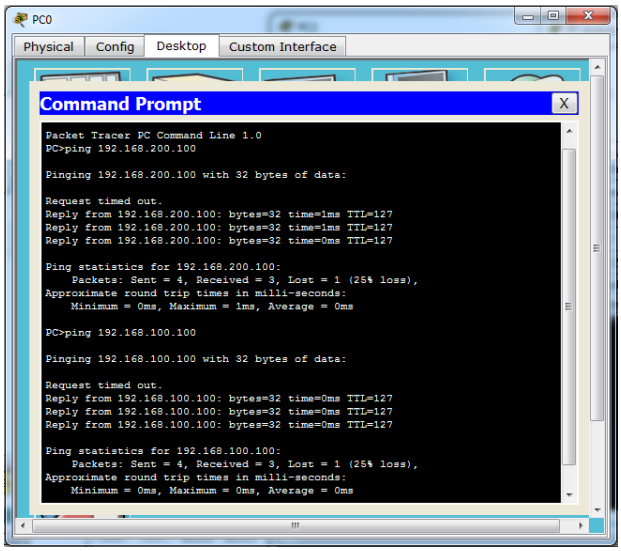
Información básica/Situación

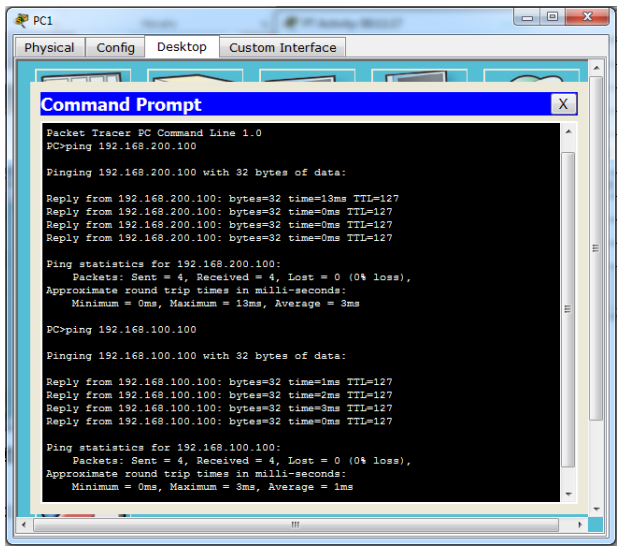
El administrador de red ejecutivo le ha solicitado que cree una ACL nombrada estándar para impedir el acceso a un servidor de archivos. Se debe denegar el acceso de todos los clientes de una red y de una estación de trabajo específica de una red diferente.

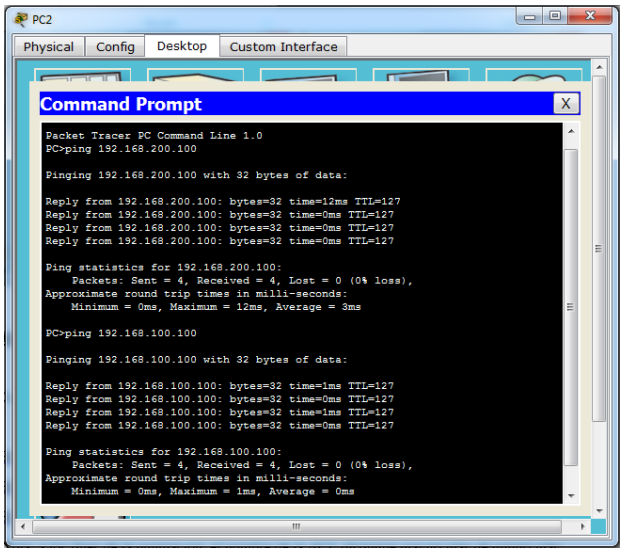
Parte 1: configurar y aplicar una ACL estándar con nombre

Paso 1: verificar la conectividad antes de configurar y aplicar la ACL.

Las tres estaciones de trabajo deben poder hacer ping tanto al Servidor web como al Servidor de archivos .


PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms


PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.200.100: bytes=32 time=13ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 13ms, Average = 3ms
PC>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time=3ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 1ms



Paso 2: configurar una ACL estándar con nombre.

Configure la siguiente ACL con nombre en el R1 .

R1(config)# ip access-list standard File_Server_Restrictions

R1(config-std-nacl)# permit host 192.168.20.4

R1(config-std-nacl)# deny any

Nota: a los fines de la puntuación, el nombre de la ACL distingue mayúsculas de minúsculas.

Paso 3: aplicar la ACL con nombre.

a. Aplique la salida de la ACL en la interfaz Fast Ethernet 0/1.

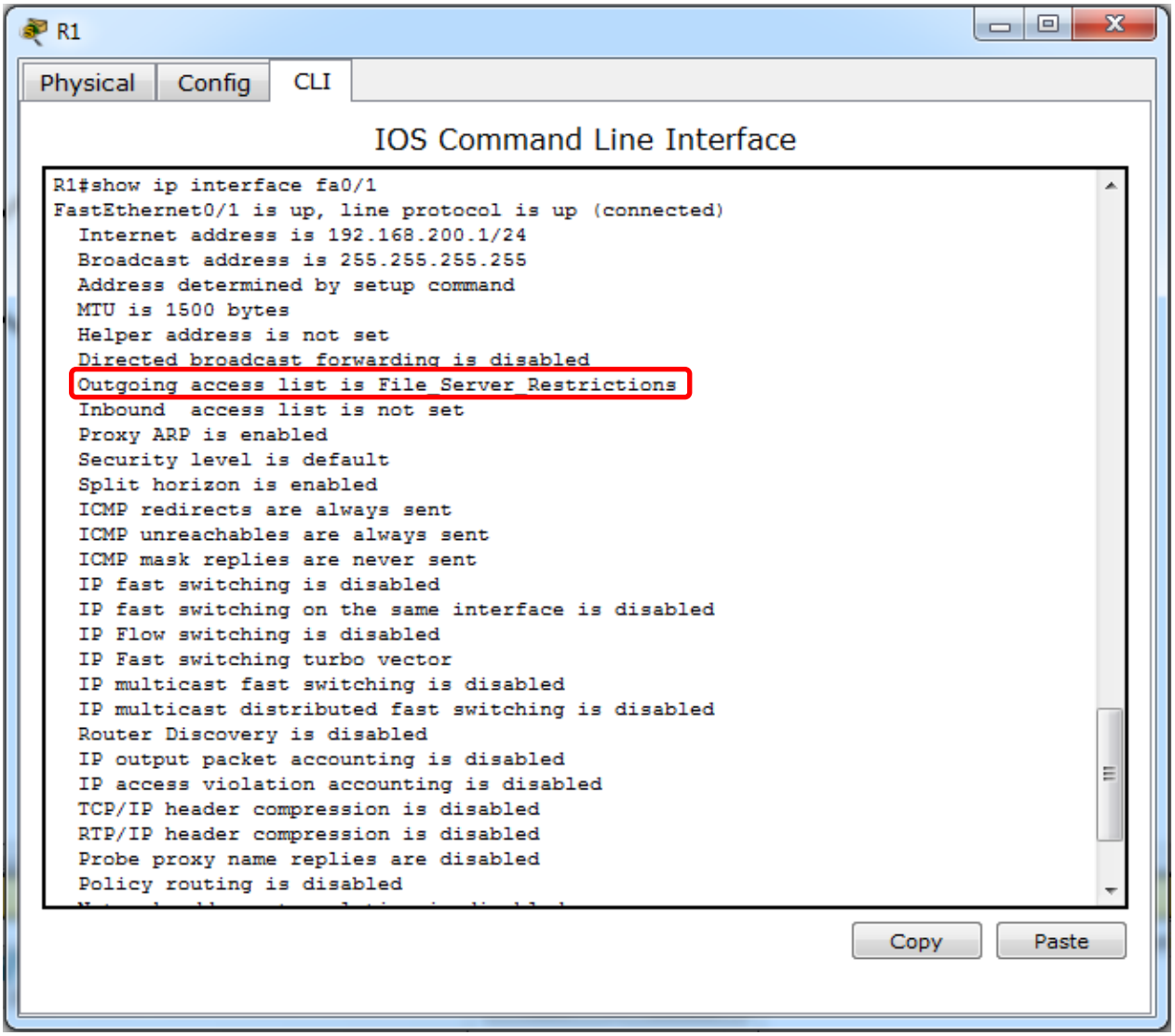
R1(config-if)# ip access-group File_Server_Restrictions out

b. Guarde la configuración.

Parte 2: verificar la implementación de la ACL

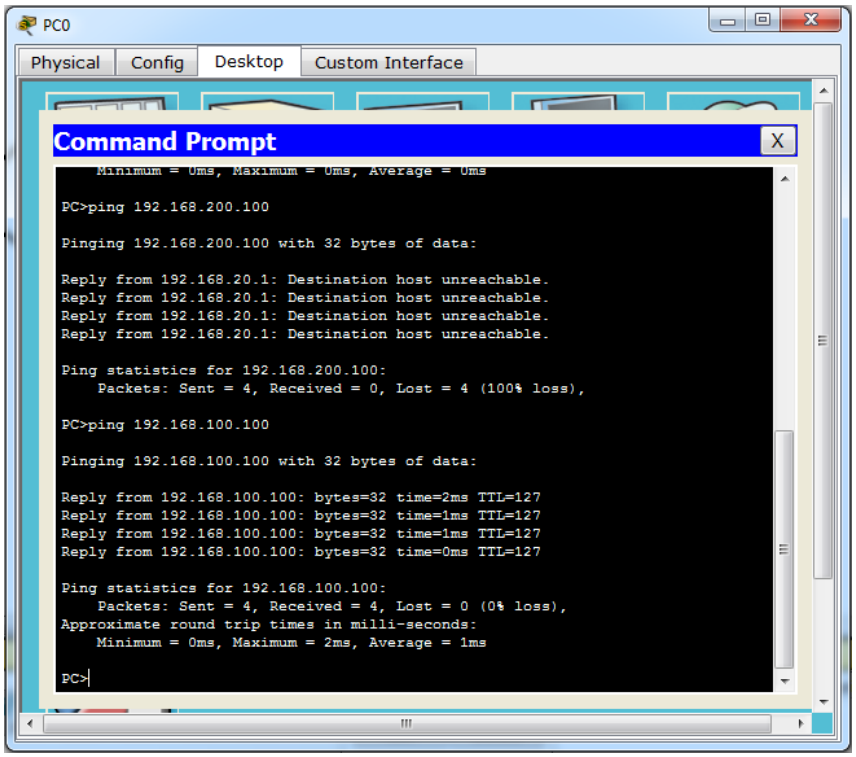
Paso 1: verificar la configuración de la ACL y su aplicación a la interfaz.

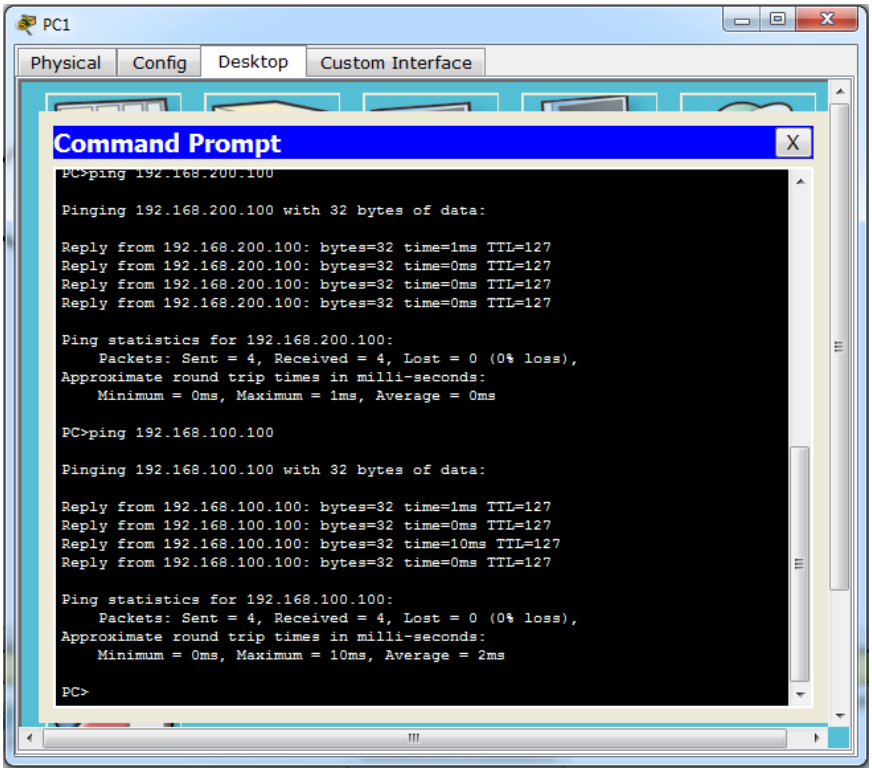
Use el comando show access-lists para verificar la configuración de la ACL. Utilice el comando show run o show ip interface fastethernet 0/1 para verificar que la ACL se aplicó correctamente a la interfaz.

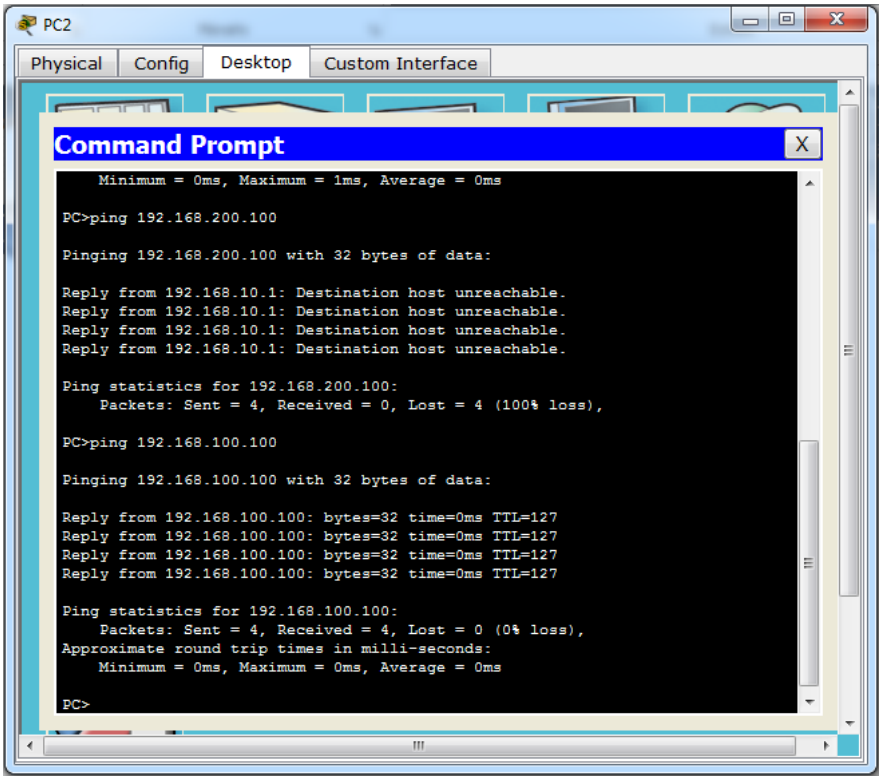


Paso 2: verificar que la ACL funcione correctamente.

Las tres estaciones de trabajo deben poder hacer ping al Servidor web , pero solo la PC1 debe poder hacer ping al Servidor de archivos .


PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 1ms
PC>


PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=10ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms
PC>


PC2
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>

9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines

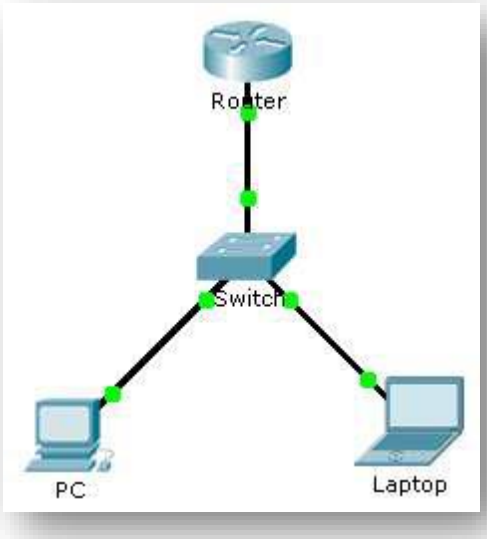


Tabla de Direcciones

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Laptop	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Objectives

Part 1: Configure and Apply an ACL to VTY Lines
Part 2: Verify the ACL Implementation

Background

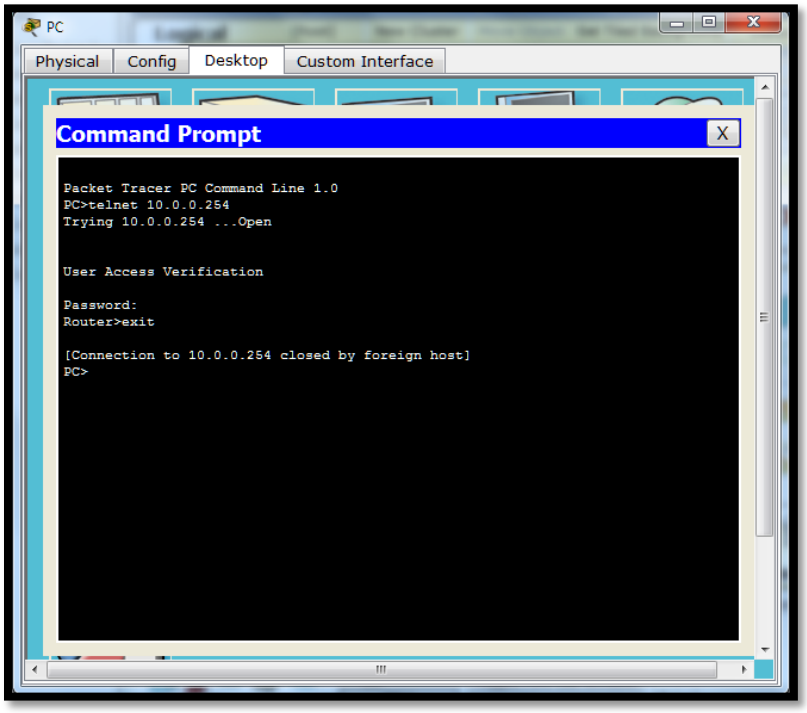
As network administrator, you must have remote access to your router. This access should not be available to
other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows **PC**
access to the Telnet lines, but denies all other source IP addresses.

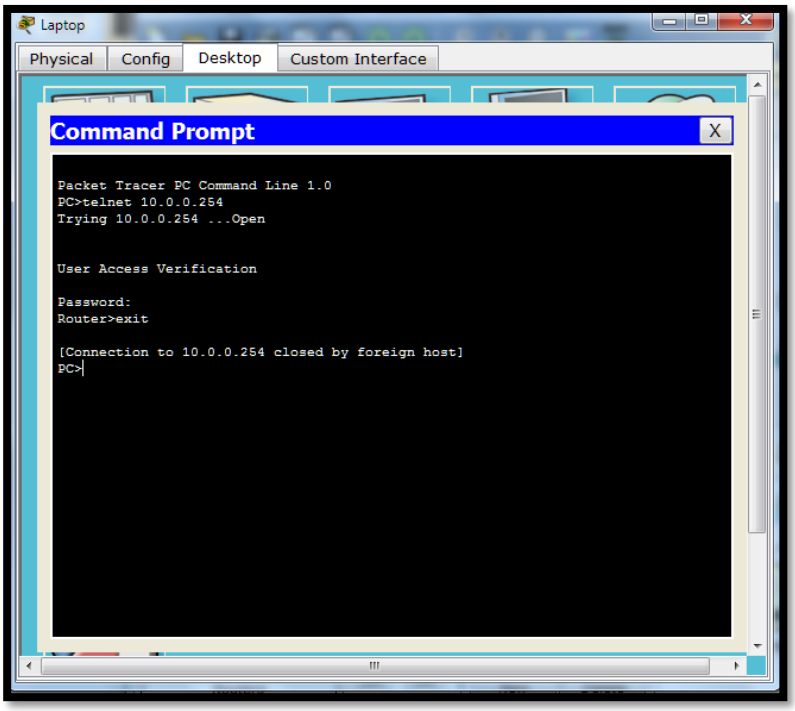
Part 1: Configure and Apply an ACL to VTY Lines

Step 1: Verify Telnet access before the ACL is configured.

Both computers should be able to Telnet to the **Router**. The password is **cisco**

.


PC
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>telnet 10.0.0.254
Trying 10.0.0.254 ...Open
User Access Verification
Password:
Router>exit
[Connection to 10.0.0.254 closed by foreign host]
PC>

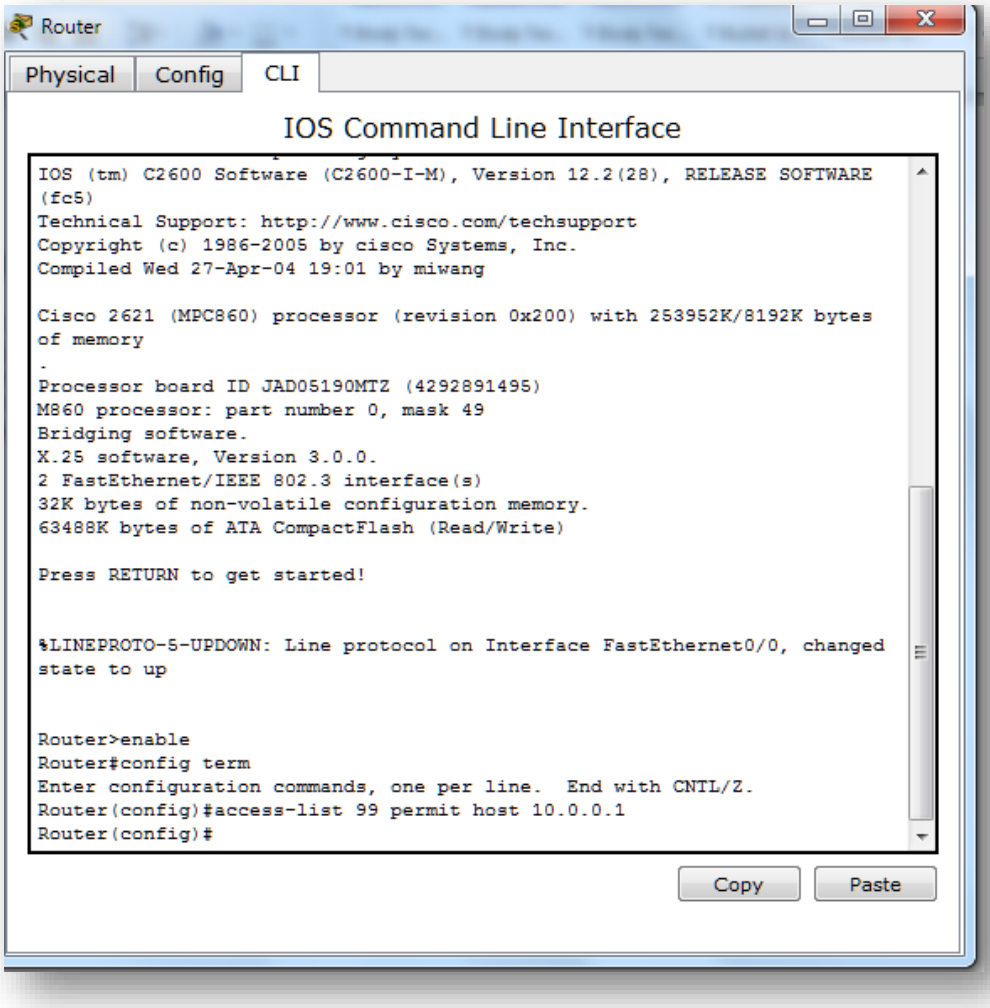

Laptop
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>telnet 10.0.0.254
Trying 10.0.0.254 ...Open
User Access Verification
Password:
Router>exit
[Connection to 10.0.0.254 closed by foreign host]
PC>

Step 2: Configure a numbered standard ACL

Configure the following numbered ACL on **Router**.

```
Router(config)# access-list 99 permit host 10.0.0.1
```

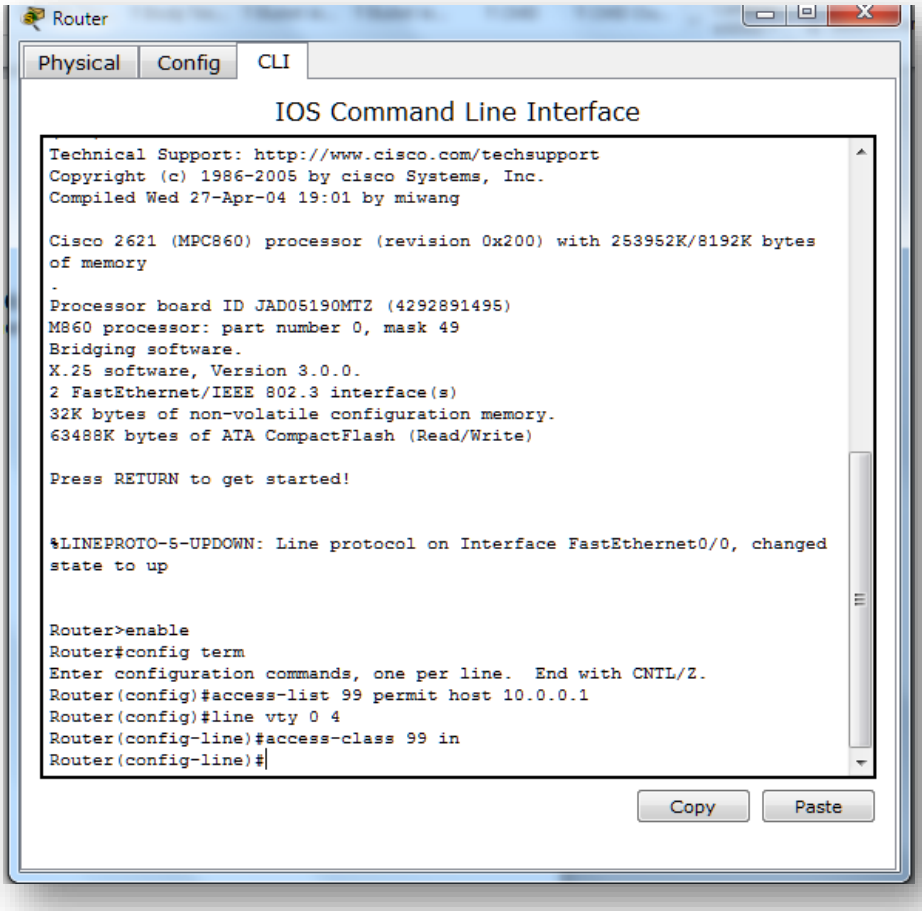
Because we do not want to permit access from any other computers, the implicit deny property of the access
list satisfies our requirements.



Step 3: Place a named standard ACL on the router.

Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must
place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration
mode for lines 0 – 4 and use the **access-class** command to apply the ACL to all the VTY lines:

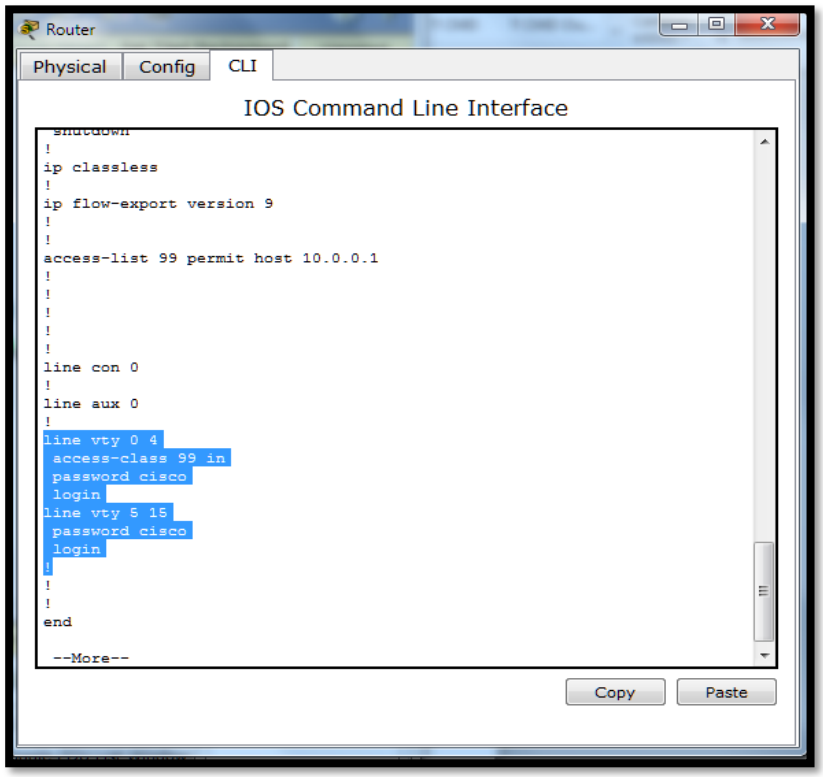
```
Router(config)# line vty 0 15
Router(config-line)# access-class 99 in
```



Part 2: Verify the ACL Implementation

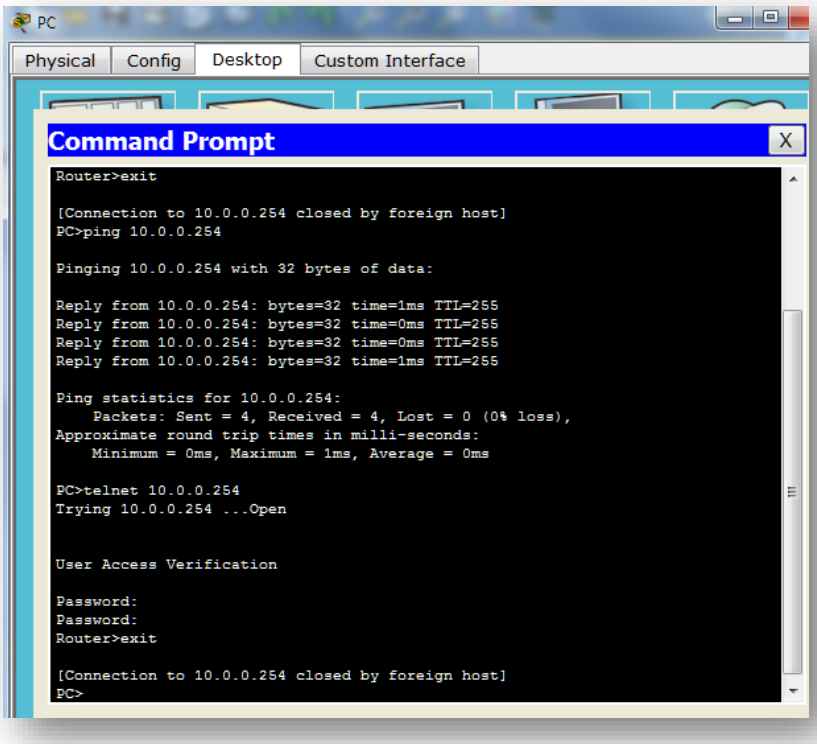
Step 1: Verify the ACL configuration and application to the VTY lines.

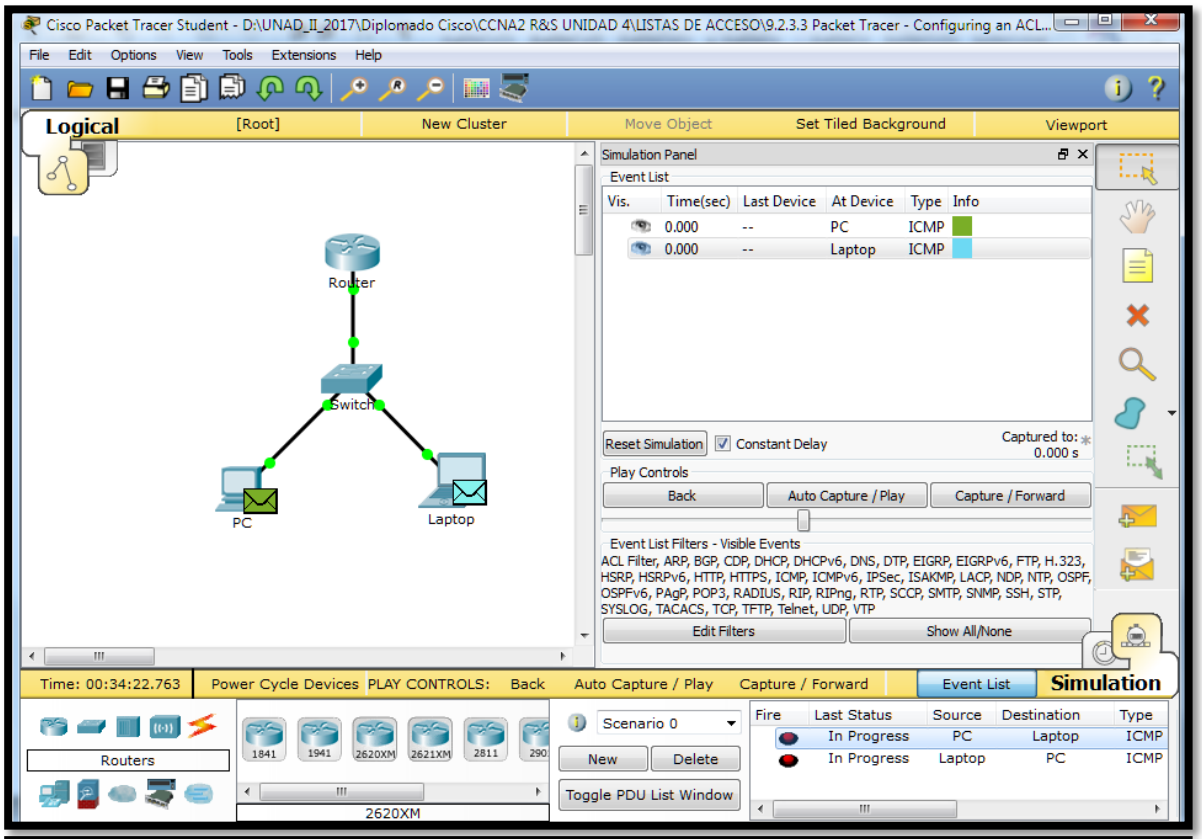
Use the **show access-lists** to verify the ACL configuration. Use the **show run** command to verify the ACL is
applied to the VTY lines.

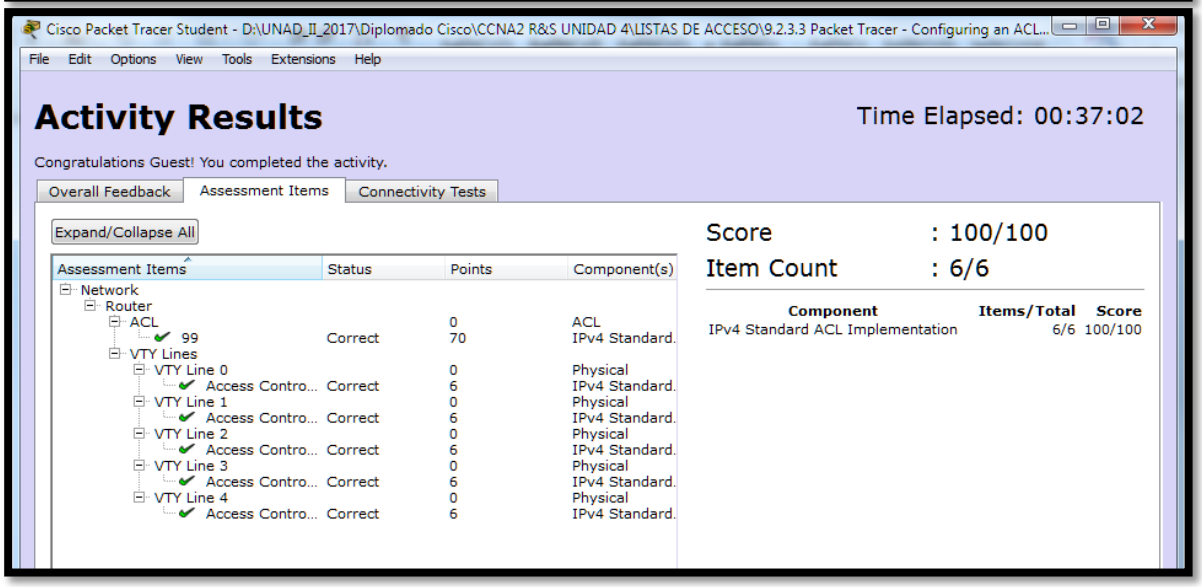


Step 2: Verify that the ACL is working properly.

Both computers should be able to ping the **Router**, but only **PC** should be able to Telnet to it.



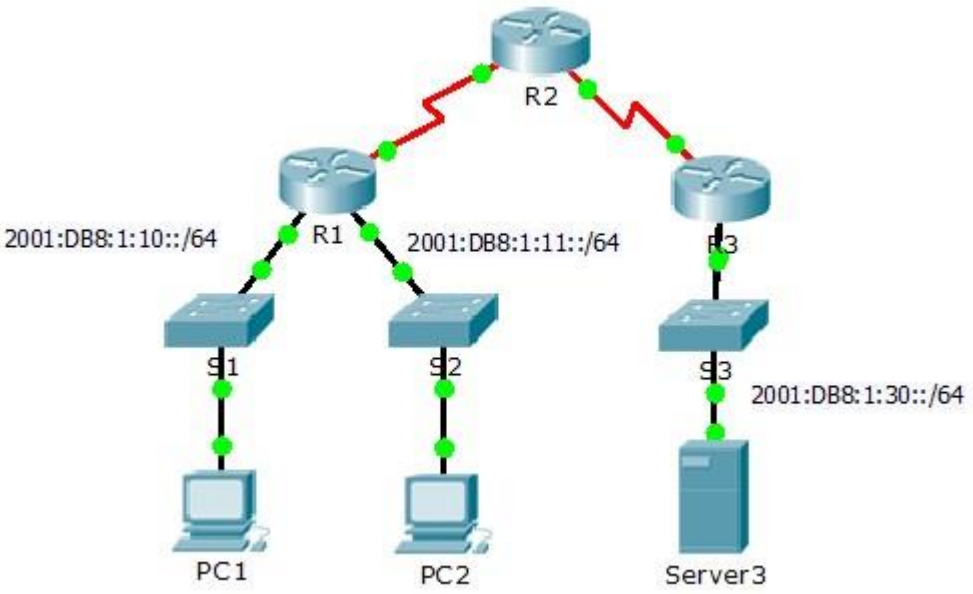

Cisco Packet Tracer Student - D:\UNAD_II_2017\Diplomado Cisco\CCNA2 R&S UNIDAD 4\LISTAS DE ACCESO\9.2.3.3 Packet Tracer - Configuring an ACL...
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Router
Switch
PC
Laptop
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC ICMP
0.000 -- Laptop ICMP
Reset Simulation
Constant Delay
Captured to: 0.000 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:34:22.763
Power Cycle Devices
PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation
Routers
1841 1941 2620XM 2621XM 2811
2620XM
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type
In Progress PC Laptop ICMP
In Progress Laptop PC ICMP


Cisco Packet Tracer Student - D:\UNAD_II_2017\Diplomado Cisco\CCNA2 R&S UNIDAD 4\LISTAS DE ACCESO\9.2.3.3 Packet Tracer - Configuring an ACL...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:37:02
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items Status Points Component(s)
Network
Router
ACL 0 ACL
99 Correct 70 IPv4 Standard.
VTY Lines
VTY Line 0 0 Physical
Access Contro... Correct 6 IPv4 Standard.
VTY Line 1 0 Physical
Access Contro... Correct 6 IPv4 Standard.
VTY Line 2 0 Physical
Access Contro... Correct 6 IPv4 Standard.
VTY Line 3 0 Physical
Access Contro... Correct 6 IPv4 Standard.
VTY Line 4 0 Physical
Access Contro... Correct 6 IPv4 Standard.
Score : 100/100
Item Count : 6/6
Component Items/Total Score
IPv4 Standard ACL Implementation 6/6 100/100

9.5.2.6 Packet Tracer - Configuring IPv6 ACLs (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectives

Part 1: Configure, Apply, and Verify an IPv6 ACL

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Part 1: Configure, Apply, and Verify an IPv6 ACL

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be

identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

Step 1: Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named **BLOCK_HTTP** on **R1** with the following

statements.

```
R1(config)#ipv6 address list BLOCK_HTTP
                             ^
```

a. Block HTTP and HTTPS traffic from reaching **Server3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

```
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::30 443
                                                        ^
```

b. Allow all other IPv6 traffic to pass.

```
R1(config)# permit ipv6 any any
```

```
R1(config-ipv6-acl)#permit ipv6 any any
```

Step 2: Apply the ACL to the correct interface.

Apply the ACL on the interface closest the source of the traffic to be blocked.

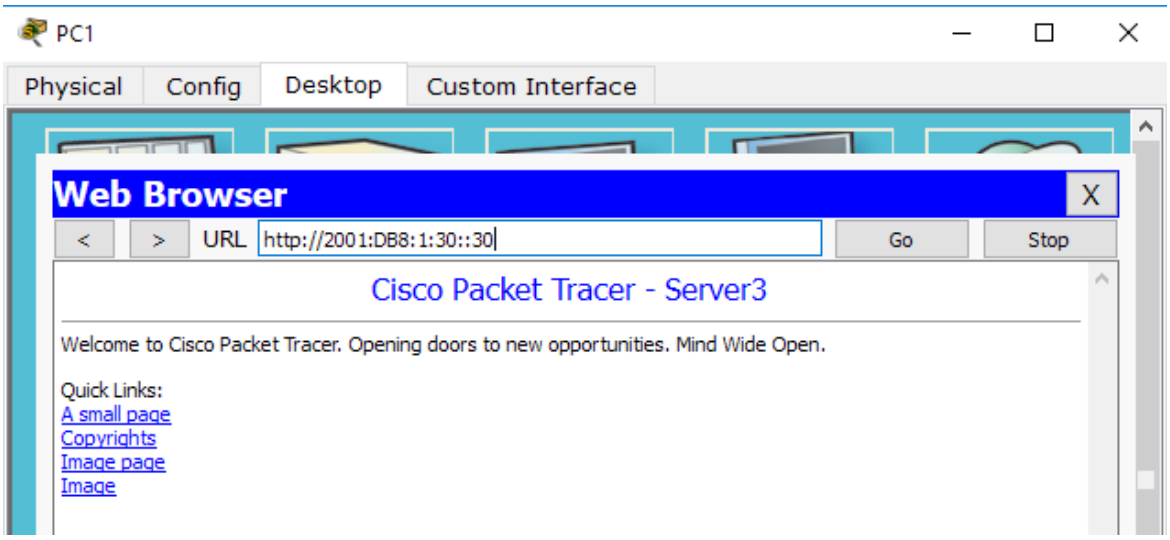
```
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ipv6 traffic-filter
BLOCK_HTTP in
```

```
R1(config-ipv6-acl)#interface g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
```

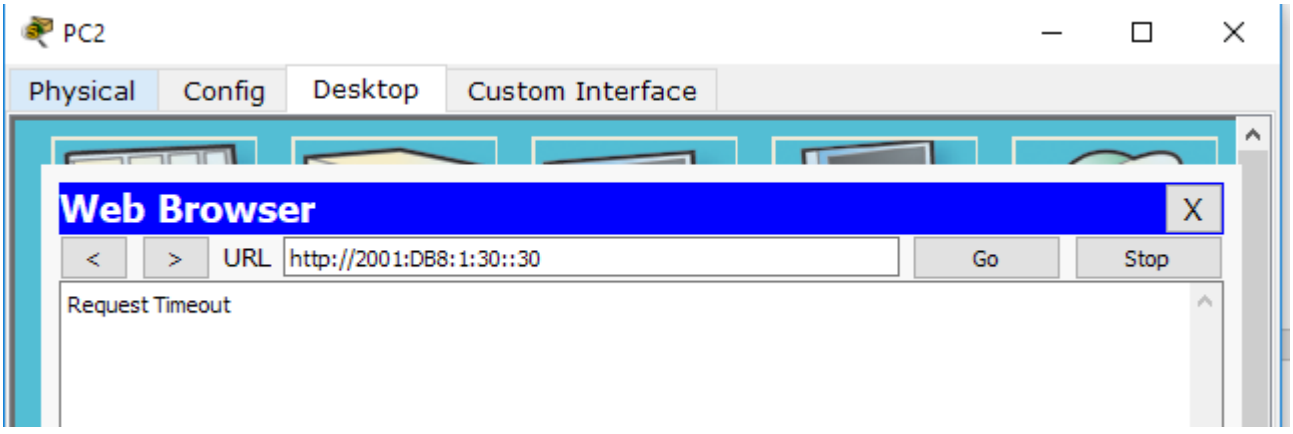
Step 3: Verify the ACL implementation.

Verify the ACL is operating as intended by conducting the following tests:

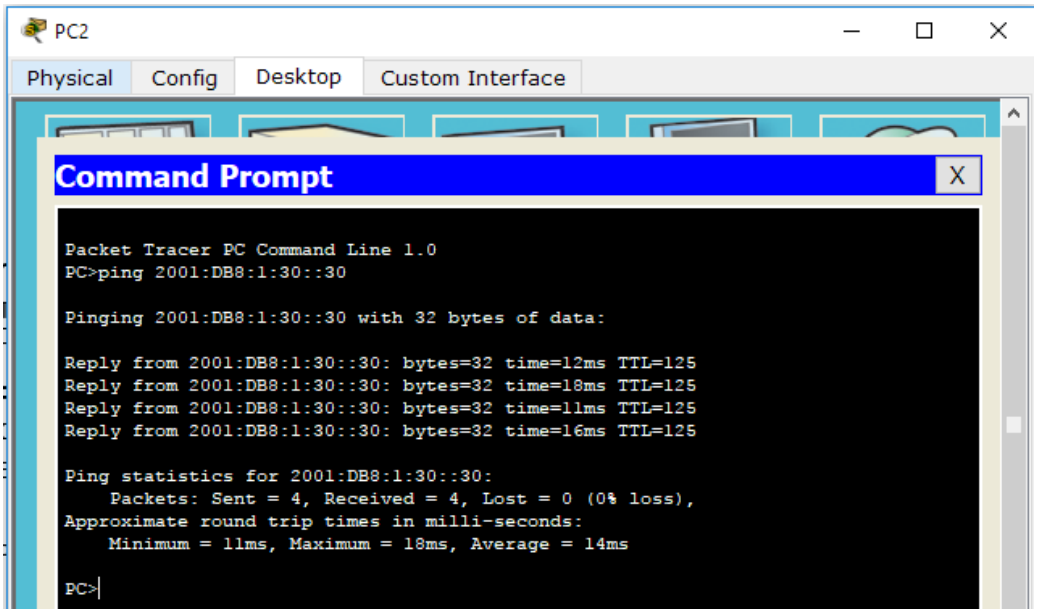
- Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.



- Open the **web browser** of **PC2** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked



- Ping from **PC2** to 2001:DB8:1:30::30. The ping should be successful.



Part 2: Configure, Apply, and Verify a Second IPv6 ACL

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

Step 1: Create an access list to block ICMP.

Configure an ACL named **BLOCK_ICMP** on **R3** with the following

statements:

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
```

a. Block all ICMP traffic from any hosts to any destination.

```
R3(config)# deny icmp any any
```

b. Allow all other IPv6 traffic to pass.

```
R3(config)# permit ipv6 any any
```

```
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#exit
```

Step 2: Apply the ACL to the correct interface.

In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked regardless of its source or changes that occur to the network topology, apply the ACL closest to the destination.

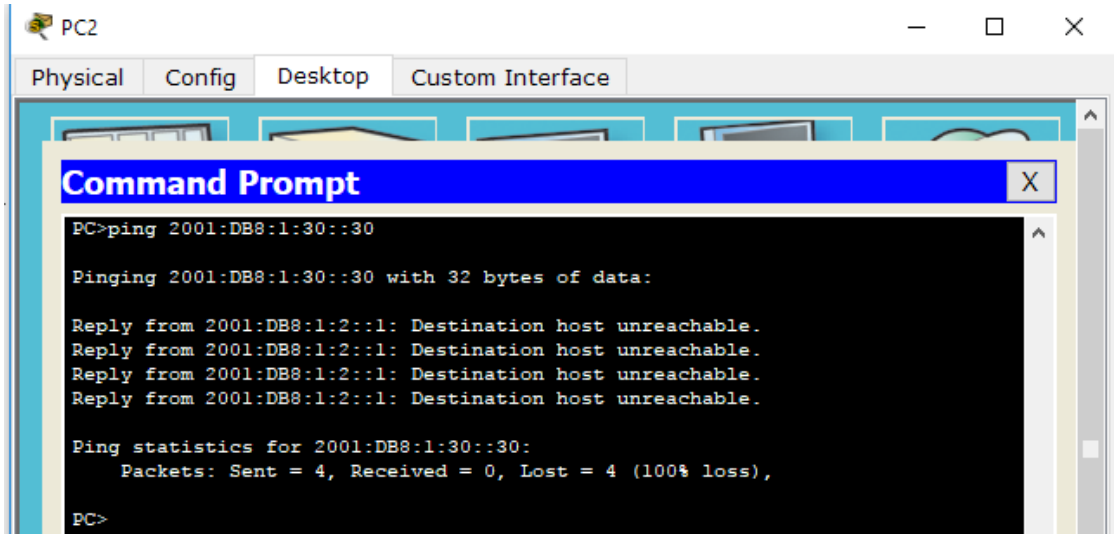
```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ipv6 traffic-filter
```

BLOCK_ICMP out

```
R3(config)#int g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
```

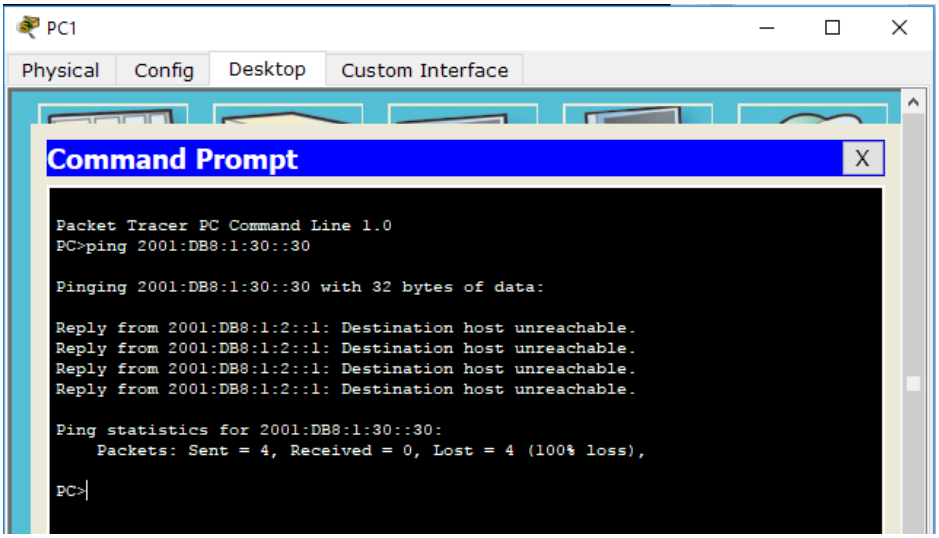
Step 3: Verify that the proper access list functions.

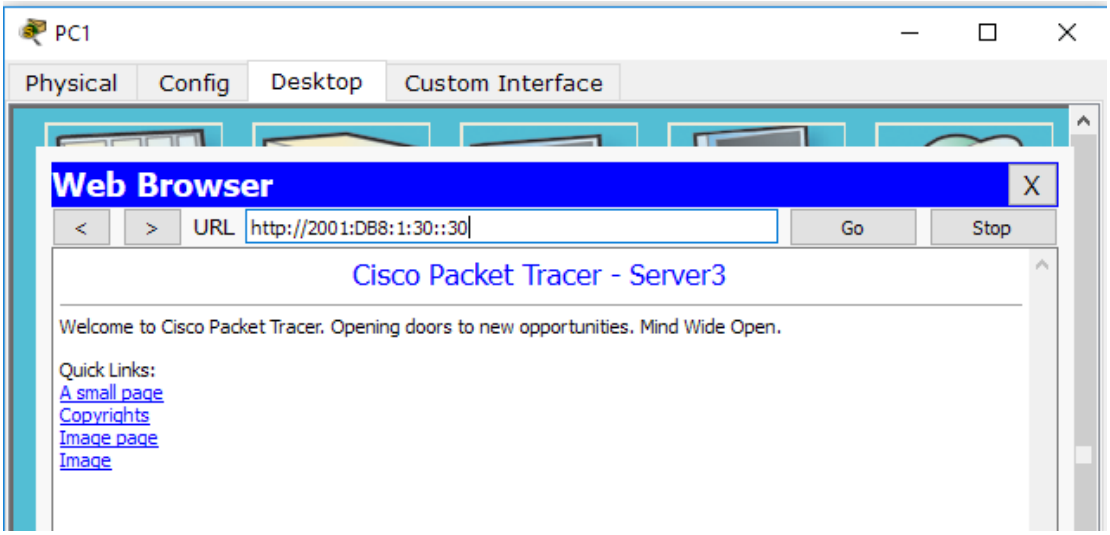
a. Ping from **PC2** to 2001:DB8:1:30::30. The ping should fail.

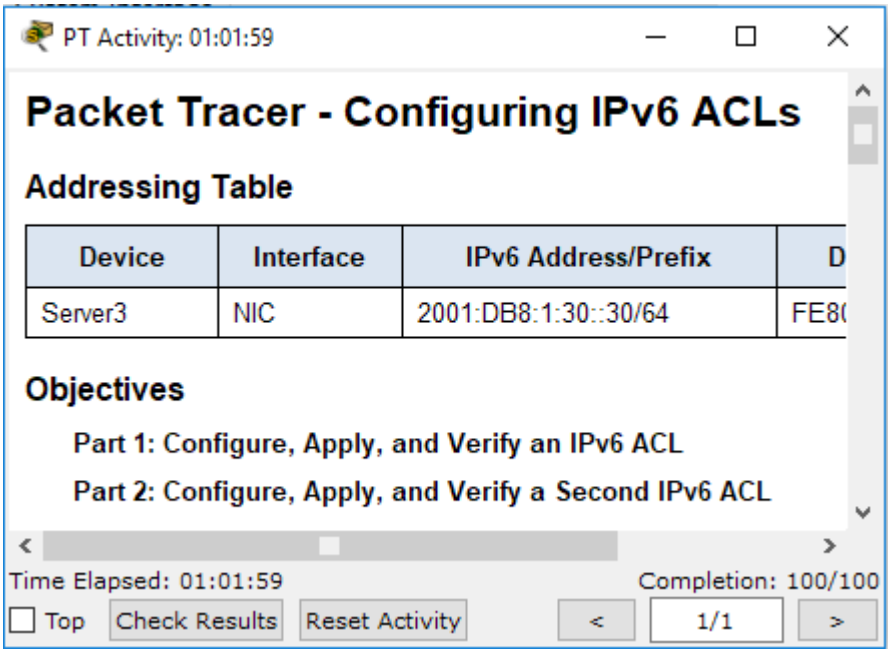


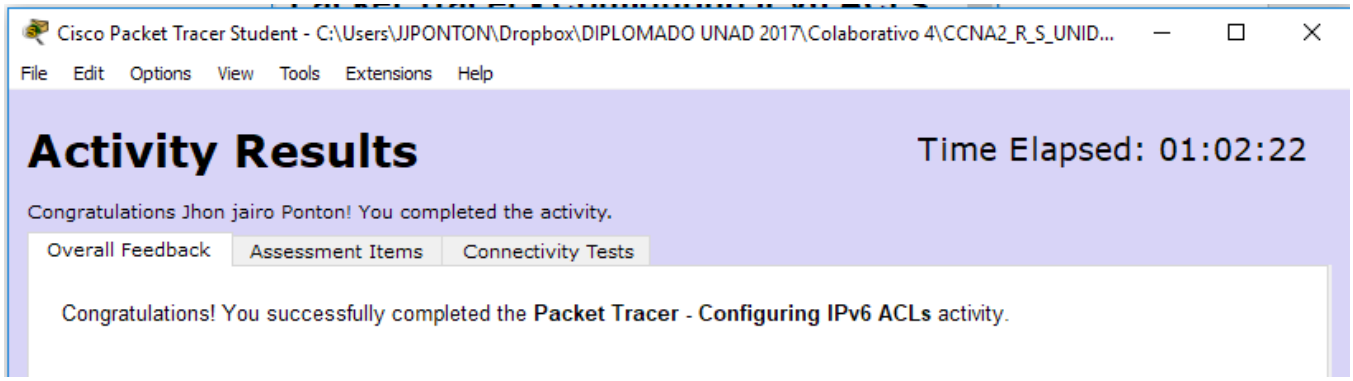
b. Ping from **PC1** to 2001:DB8:1:30::30. The ping should fail.

Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should display.






PT Activity: 01:01:59
Packet Tracer - Configuring IPv6 ACLs
Addressing Table
Device
Interface
IPv6 Address/Prefix
Server3
NIC
2001:DB8:1:30::30/64
Objectives
Part 1: Configure, Apply, and Verify an IPv6 ACL
Part 2: Configure, Apply, and Verify a Second IPv6 ACL
Time Elapsed: 01:01:59
Completion: 100/100
Top
Check Results
Reset Activity
1/1


Cisco Packet Tracer Student - C:\Users\JJPONTON\Dropbox\DIPLOMADO UNAD 2017\Colaborativo 4\CCNA2_R_S_UNID...
File
Edit
Options
View
Tools
Extensions
Help
Activity Results
Time Elapsed: 01:02:22
Congratulations Jhon jairo Ponton! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations! You successfully completed the Packet Tracer - Configuring IPv6 ACLs activity.

10.1.2.4 Packet Tracer - Configuración de DHCPv4 básico en un router

Topología

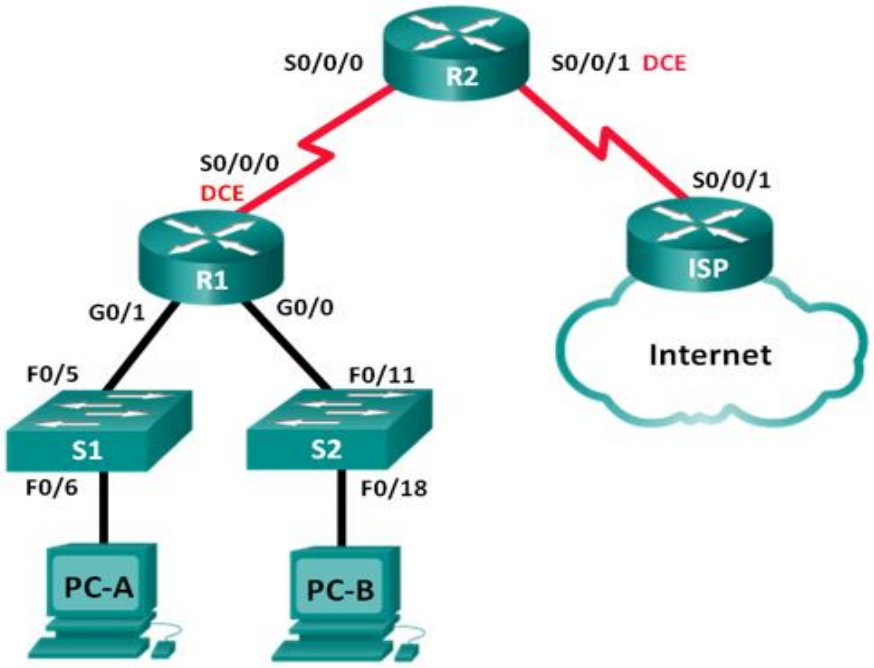


Tabla de direccionamiento

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

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

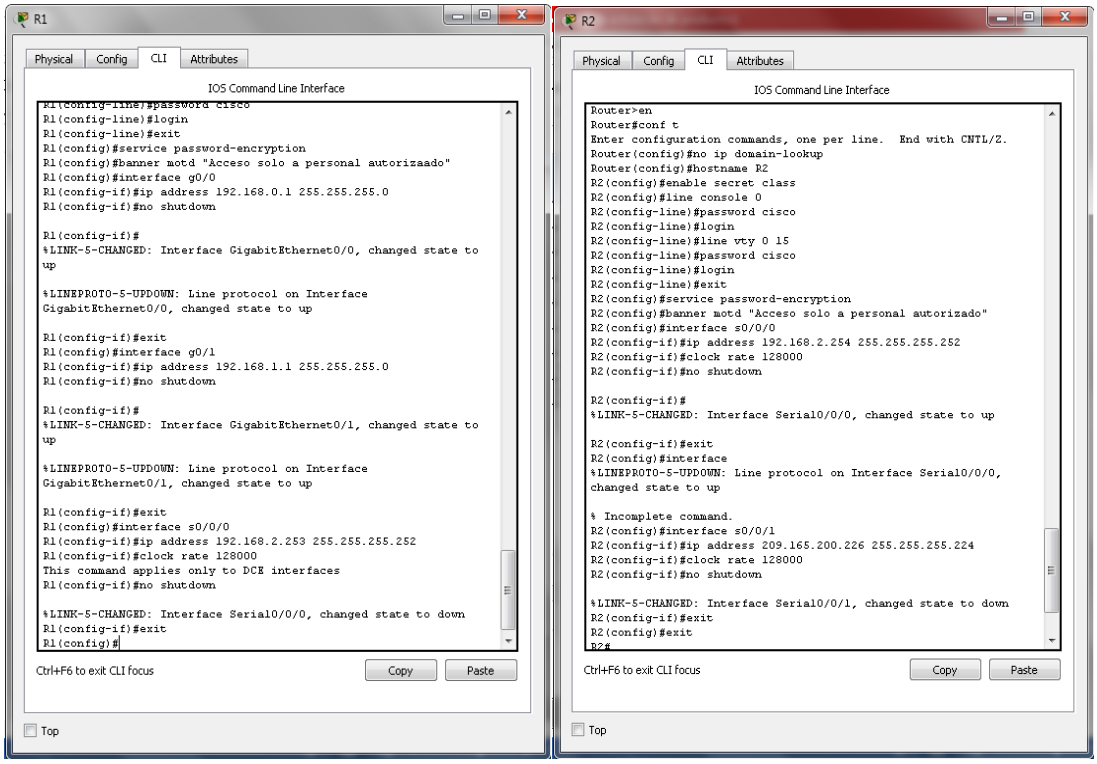
En la parte 1, establecerá la topología de la red y configurará los routers y switches con los parámetros básicos, como las contraseñas y las direcciones IP. Además, configurará los parámetros de IP de las computadoras en la topología.

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.

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


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "Acceso solo a personal autorizaado"
R1(config)#interface g0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#interface g0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)#exit
R1(config)#interface s0/0/0
R1(config-if)#ip address 192.168.2.253 255.255.255.252
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)#exit
R1(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd "Acceso solo a personal autorizado"
R2(config)#interface s0/0/0
R2(config-if)#ip address 192.168.2.254 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#exit
R2(config)#interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
% Incomplete command.
R2(config)#interface s0/0/1
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit
R2(config)#exit
R2#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


ISP
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#banner motd "Acceso solo a personal autorizado"
ISP(config)#interface s0/0/1
ISP(config-if)#ip address 209.165.200.225 255.255.255.224
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
ISP(config-if)#exit
ISP(config)#exit
ISP#
%SYS-5-CONFIG_I: Configured from console by console
ISP#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
ISP#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

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>en
Password:
R1#conf t
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>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router eigrp 1
R2(config-router)#network 192.168.2.252 0.0.0.3
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253
(Serial0/0/0) is up: new adjacency

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

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#conf t
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

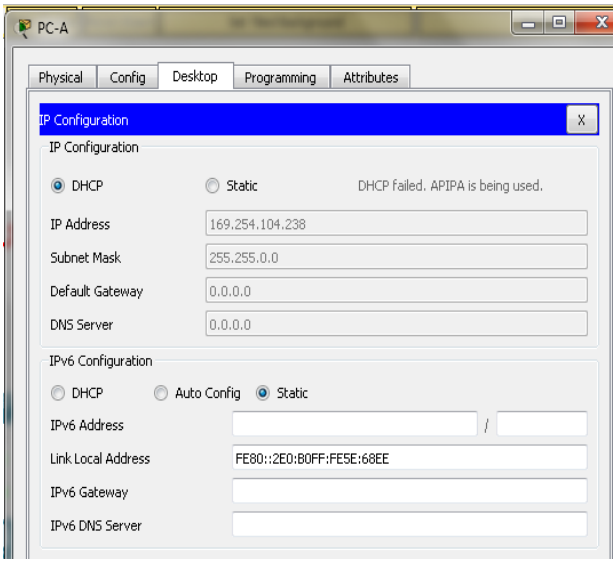
Step 4: verificar la conectividad de red entre los routers.

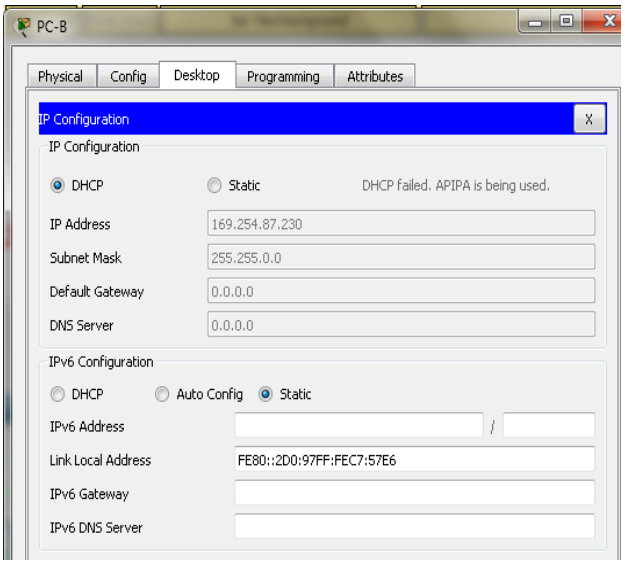
Si algún ping entre los routers falla, corrija los errores antes de continuar con el siguiente paso. Use los comandos **show ip route** y **show ip interface brief** para detectar posibles problemas.

Ping ISP a 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 = 2/3/8
ms

ISP#
```

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





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

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

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.

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

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

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

R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9

R2(config)#ip dhcp pool R1G1

R2(dhcp-config)#network 192.168.1.0 255.255.255.0

R2(dhcp-config)#default-router 192.168.1.1

R2(dhcp-config)#dns-server 209.165.200.225

R2(dhcp-config)#exit

R2(config)#ip dhcp pool R1G0

R2(dhcp-config)#network 192.168.0.0 255.255.255.0

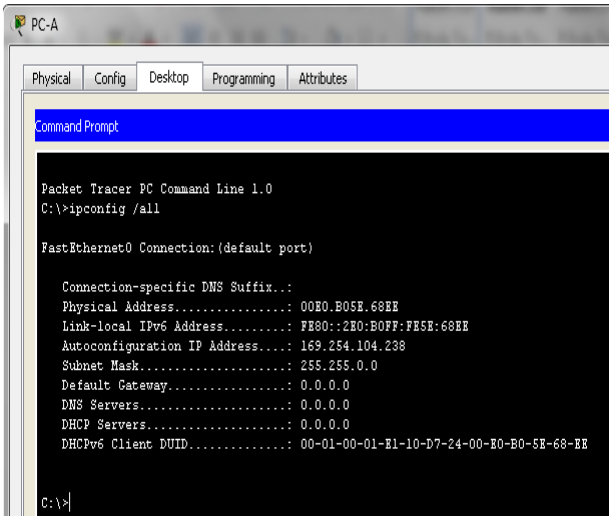
R2(dhcp-config)#default-router 192.168.0.1

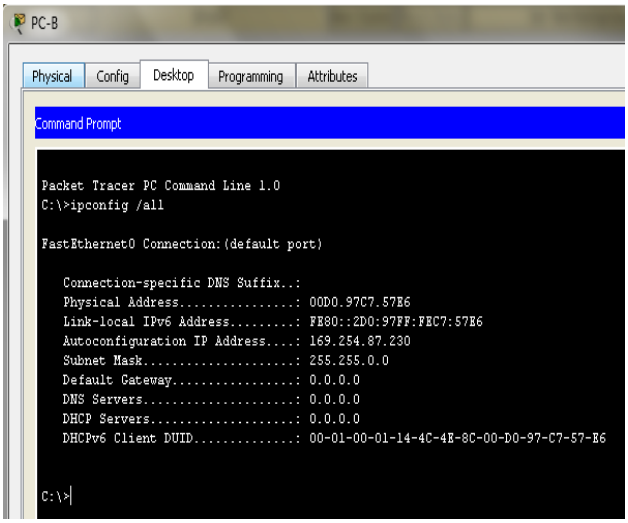
R2(dhcp-config)#dns-server 209.165.200.225

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
                  ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#exit
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#
```

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

No, Porque el R2 esta en otra red





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.

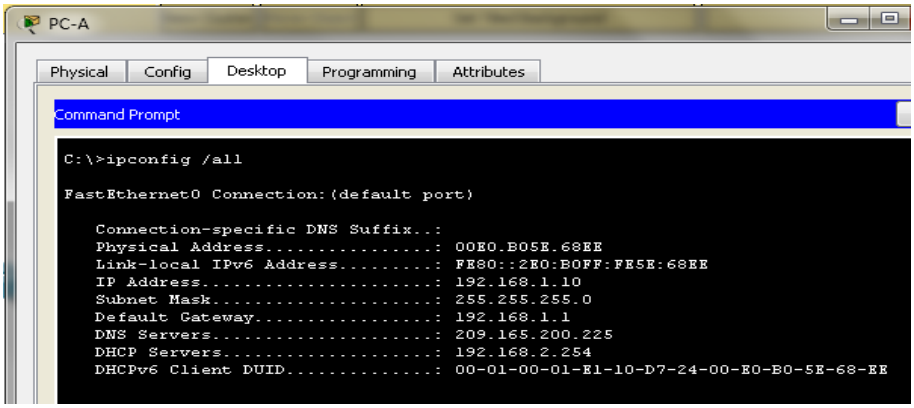
R1(config)#interface g0/0
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
R1(config)#interface g0/1
R1(config-if)#ip helper-address 192.168.2.254

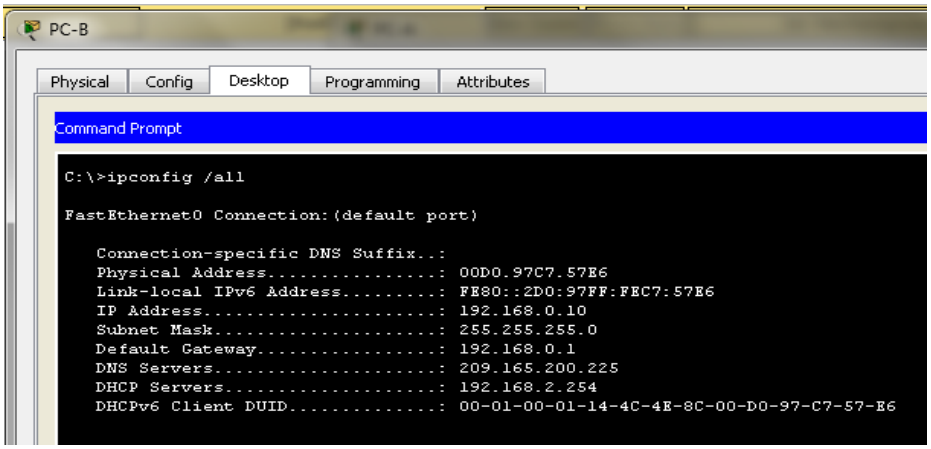
R1(config-if)#

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

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.





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?

A partir de la 192.168.0.10

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

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

```
R2>en
Password:
R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration
Type
                 Hardware address
192.168.1.10     00E0.B05E.68EE           --
Automatic
192.168.0.10     00D0.97C7.57E6           --
Automatic
R2#
```

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

Las direcciones MAC de los equipos PC-A y PC-B

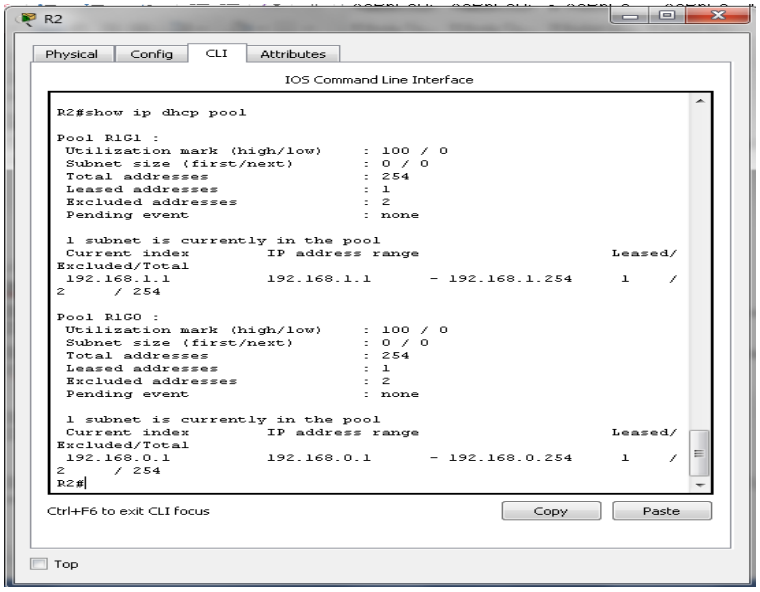
b. En el R2, introduzca el comando **show ip dhcp server statistics** para ver la actividad de mensajes y las estadísticas del pool de DHCP.

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

R2#
```

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

Packet Tracer no tiene esta funcion

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)?

Al Rango de direcciones IP que fueron excluidas en el Router

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

```
R2#show run
Building configuration...

Current configuration : 1425 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 209.165.200.225
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 209.165.200.225
!
!
!
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
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.2.254 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 ip address 209.165.200.226 255.255.255.224
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 1
 redistribute static
 network 192.168.2.252 0.0.0.3

!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.225
!
```

Reflexión

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

Ahorro de recursos de hardware de los router, al tener un servidor DHCP del router independiente para cada sub red sería más complejo y la administración centralizada de la red sería más difícil porque tocaría a entrar a cada router

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

Topología

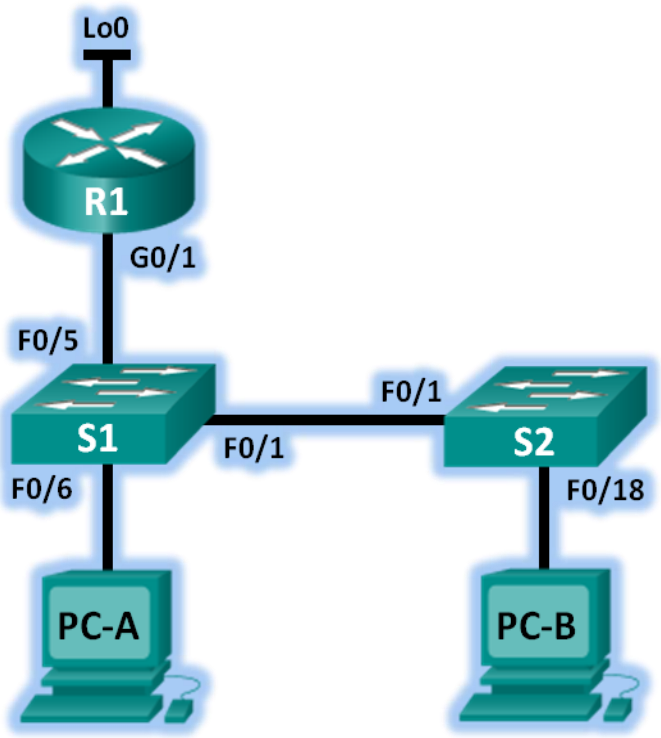


Tabla de direccionamiento

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

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
Parte 2: cambiar la preferencia de SDM

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

Parte 3: configurar DHCPv4

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

Parte 4: configurar DHCP para varias VLAN

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

Parte 5: habilitar el routing IP

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

Información básica/situación

Un switch Cisco 2960 puede funcionar como un servidor de DHCPv4. El servidor de DHCPv4 de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones identificados que están asociados a VLAN específicas e interfaces virtuales de switch (SVI). El switch Cisco 2960 también puede funcionar como un dispositivo de capa 3 y hacer routing entre VLAN y una cantidad limitada de rutas estáticas. En esta práctica de laboratorio, configurará DHCPv4 para VLAN únicas y múltiples en un switch Cisco 2960, habilitará el routing en el switch para permitir la comunicación entre las VLAN y agregará rutas estáticas para permitir la comunicación entre todos los hosts.
Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.
Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.
Nota: asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

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

Part 1: 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.
Step 3: Configurar los parámetros básicos en los dispositivos.

a. Asigne los nombres de dispositivos como se muestra en la topología.
b. Desactive la búsqueda del DNS.
c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.
e. Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.
f. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Part 2: 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.

Step 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?

- default
- default dual-ipv4-and-ipv6
- lanbase-routing

Step 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?

- lanbase-routing

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

```
S1# reload

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

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

Step 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
```

Part 3: 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.

Step 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.
   - 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.
   - 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.
   - 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.
   - S1(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.
   - 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.
   - S1(dhcp-config)# lease 3

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

```
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.2.1 192.168.2.10
!ip dhcp pool DHCP1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 192.168.1.9
ip dhcp pool DHCP2
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 192.168.2.9
ip routing
```

```
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.2.1 192.168.2.10
!
ip dhcp pool DHCP1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.1.9
ip dhcp pool DHCP2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 192.168.2.9
```

Step 2: verificar la conectividad y DHCP.

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

PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address.....: 0090.0C7A.8C8D
Link-local IPv6 Address.....: FE80::290:CFF:FE7A:8C8D
IP Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 192.168.2.9
DHCP Servers.....: 192.168.2.1
DHCPv6 Client DUID.....: 00-01-00-01-6D-4E-85-AC-00-90-0C-7A-8C-8D

PC>

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:
PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address.....: 0005.5E12.4E28
Link-local IPv6 Address.....: FE80::205:5EFF:FE12:4E28
IP Address.....: 192.168.1.12
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 192.168.1.9
DHCP Servers.....: 192.168.1.1
DHCPv6 Client DUID.....: 00-01-00-01-39-2B-10-21-00-05-5E-12-4E-28

PC>

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?
Sí
¿Es posible hacer ping de la PC-A a la PC-B?
Sí
¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1
Sí
Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.

Part 4: 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.

Step 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)# interface f0/6
S1(config-if)# switchport access vlan 2
```

```
interface FastEthernet0/6
 switchport access vlan 2
 switchport mode access
!
```

Step 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.

```
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.

```
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.

```
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.

```
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.

S1(dhcp-config)# lease 3

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

```
ip dhcp pool DHCP2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 192.168.2.9
ip routing
```

Step 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:

PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address.....: 0090.0C7A.8C8D
Link-local IPv6 Address.....: FE80::290:CFF:FE7A:8C8D
IP Address.....: 192.168.2.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.1
DNS Servers.....: 192.168.2.9
DHCP Servers.....: 192.168.2.1
DHCPv6 Client DUID.....: 00-01-00-01-6D-4E-85-AC-00-90-0C-7A-8C-8D
PC>

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?
Sí
¿Es posible hacer ping de la PC-A a la PC-B?
No
¿Los pings eran correctos? ¿Por qué?
Como la PC-A estaba dentro de la misma red del Gateway predeterminado por esto el PING es correcto, pero en el caso del PING a la PC-B como están en redes diferente no es correcto.

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

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

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

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

¿Qué resultado arrojó este comando?
Solo las redes conectadas directamente.

Part 5: 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.

Step 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`

```
S1#
S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip routing
S1(config)#
```

b. Verificar la conectividad entre las VLAN.
¿Es posible hacer ping de la PC-A a la PC-B?
Sí
¿Qué función realiza el switch?
Realiza el intercambio de mensajes entre las VLAN diferentes.

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

```
S1# 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

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1
L        192.168.1.1/32 is directly connected, Vlan1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Vlan2
L        192.168.2.1/32 is directly connected, Vlan2
```

¿Qué información de la ruta está incluida en el resultado de este comando?
El switch exhibe una tabla de routing que muestra las VLAN como las redes conectadas directamente:

- 192.168.1.0/24
- 192.168.2.0/24.

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

```
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
       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

      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
      209.165.200.0/27 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/27 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?

Redes conectadas directamente:

- 192.168.1.0
- 209.165.200.224

Si observamos aún no tenemos una ruta 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?

Debemos agregar rutas estáticas que permitan enrutar estos paquetes.

Step 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 0.0.0.0 192.168.1.10

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

R1(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.

```
S1# 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 192.168.1.10 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.10
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1
L        192.168.1.1/32 is directly connected, Vlan1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Vlan2
L        192.168.2.1/32 is directly connected, Vlan2
```

¿Cómo está representada la ruta estática predeterminada?

Gateway of last resort is S* 0.0.0.0/0 [1/0] via 192.168.1.10

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

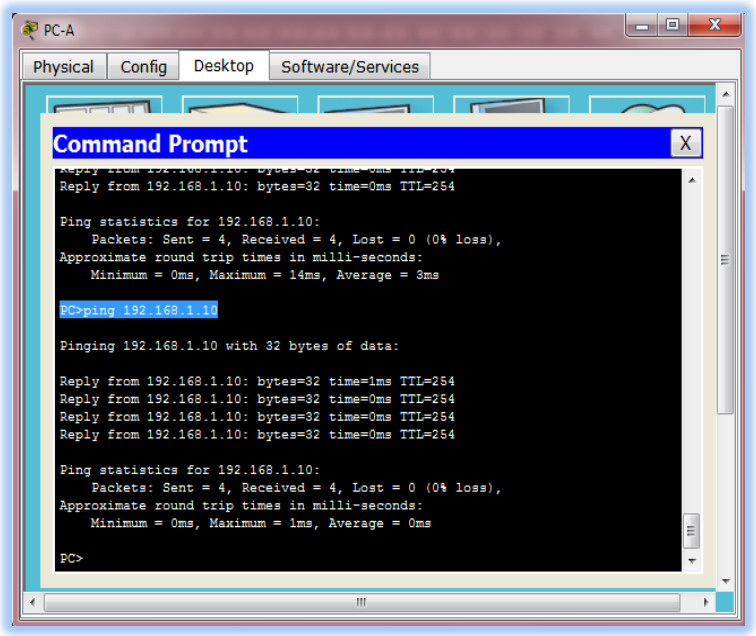
```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
    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

      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
S     192.168.2.0/24 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/27 is directly connected, Loopback0
L        209.165.200.225/32 is directly connected, Loopback0
```

¿Cómo está representada la ruta estática?

S 192.168.2.0/24 está conectada directamente, GigabitEthernet0/1

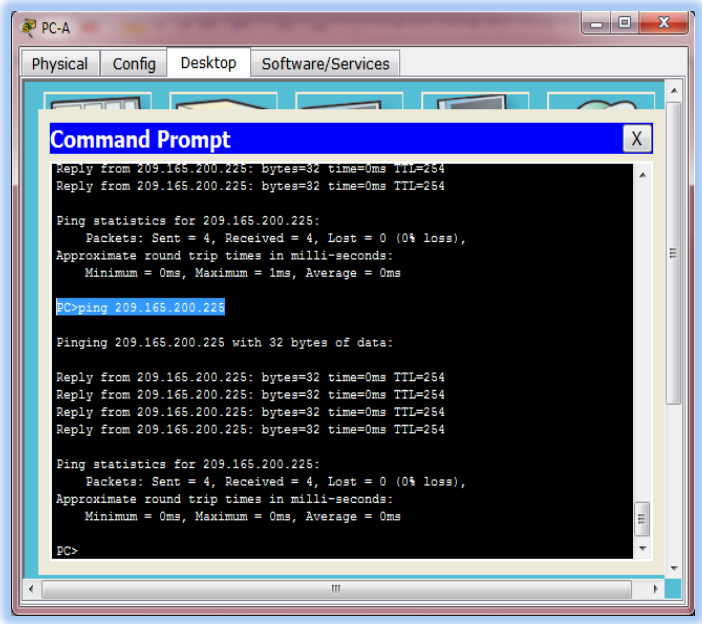
e. ¿Es posible hacer ping de la PC-A al R1?

Sí



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

Sí



Reflexión

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

   Si no realizamos este proceso podemos crear una duplicidad de direcciones IP generando conflictos entre los dispositivos que están configurados y los que le estamos asignando la IP por DHCP.

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

   Esto lo hacen de acuerdo a la asignación de cada una de las interfaces a determinada VLAN.

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

   Este lo podemos configurar como router, para que desempeñe algunas de sus funciones.

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**

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

Topología

Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación

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

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

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

uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

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

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

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

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

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

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

```
S1# show sdm prefer
```

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

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

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

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

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.

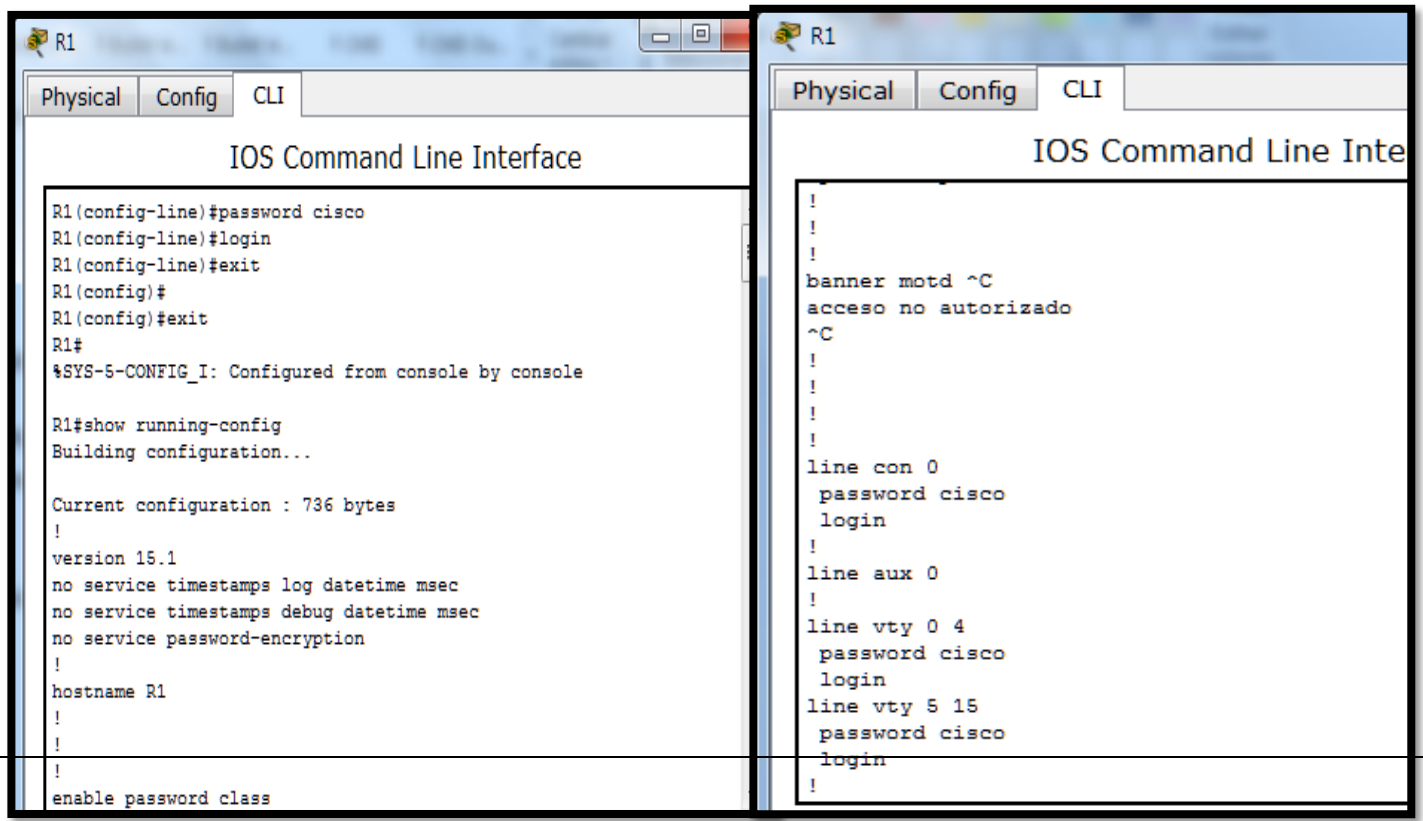
d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.

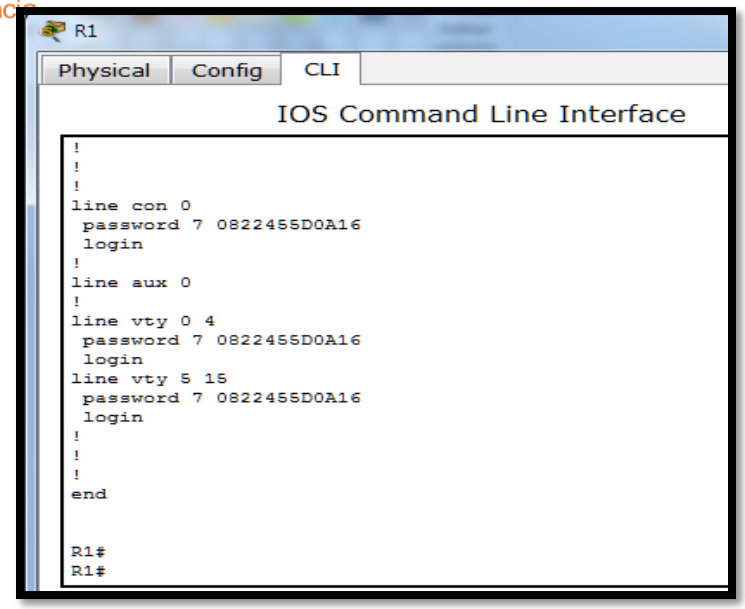
e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

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.

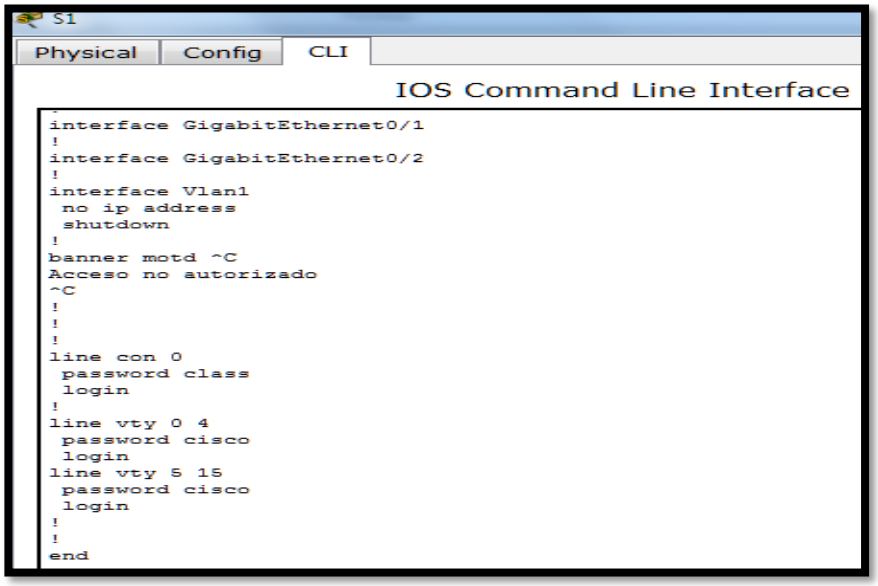
e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

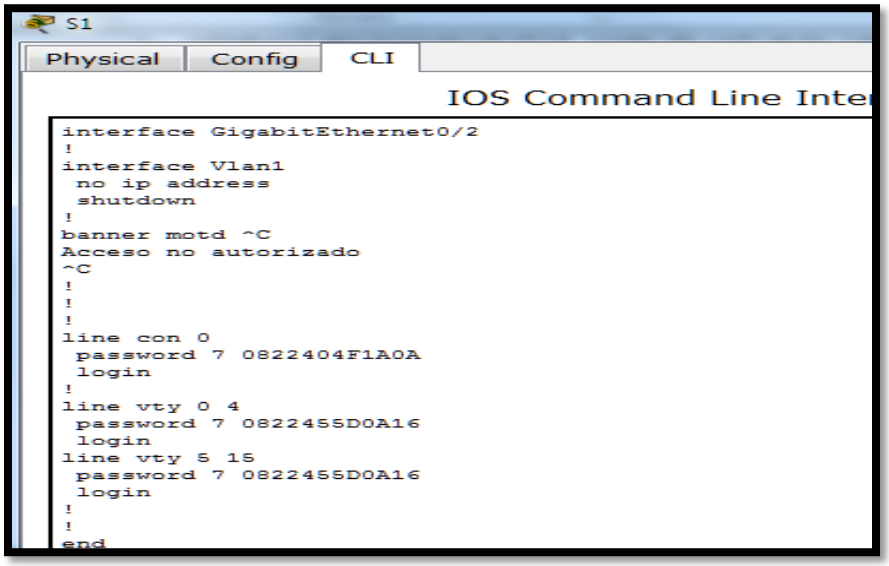
f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

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

h. Desactive administrativamente todas las interfaces inactivas.

Guarde la configuración en ejecución en la configuración de inicio

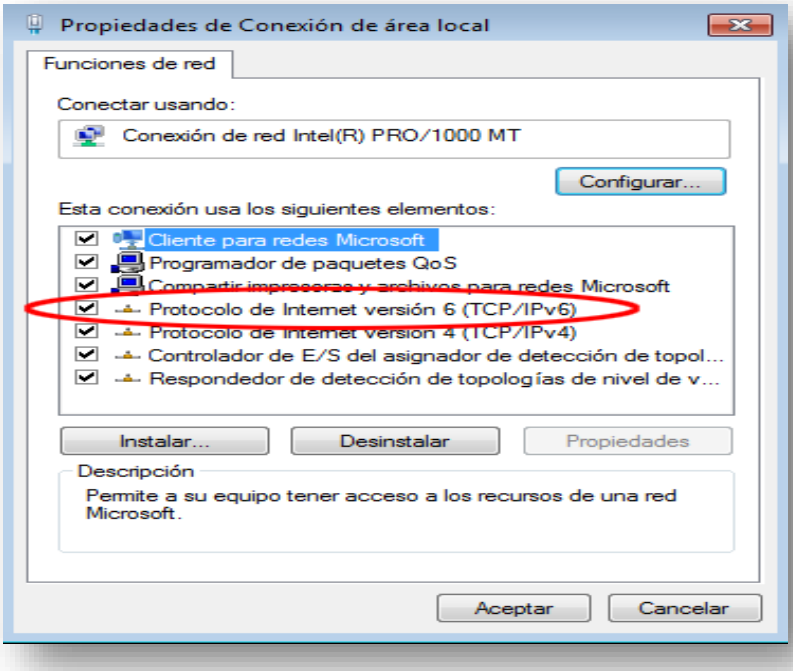




Part 2: configurar la red para SLAAC

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.

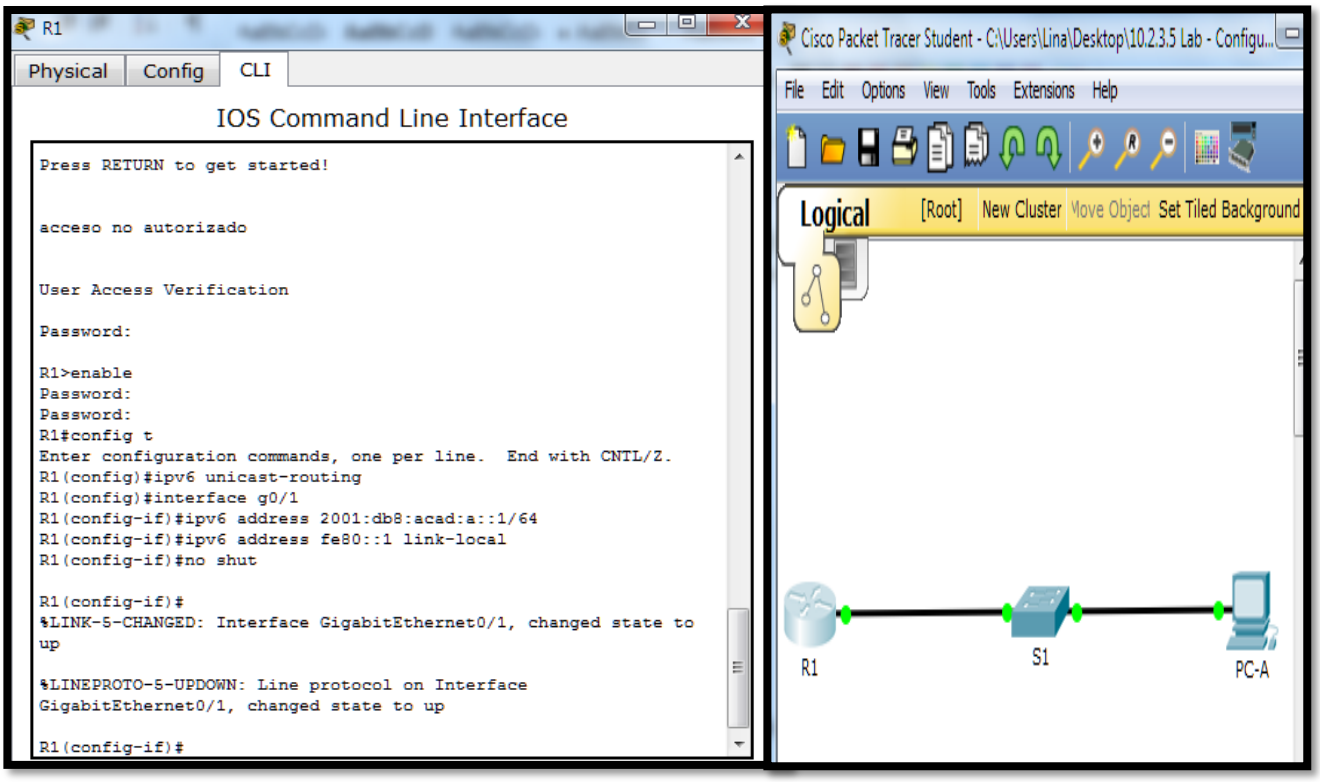
Step 2: Configurar R1

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.

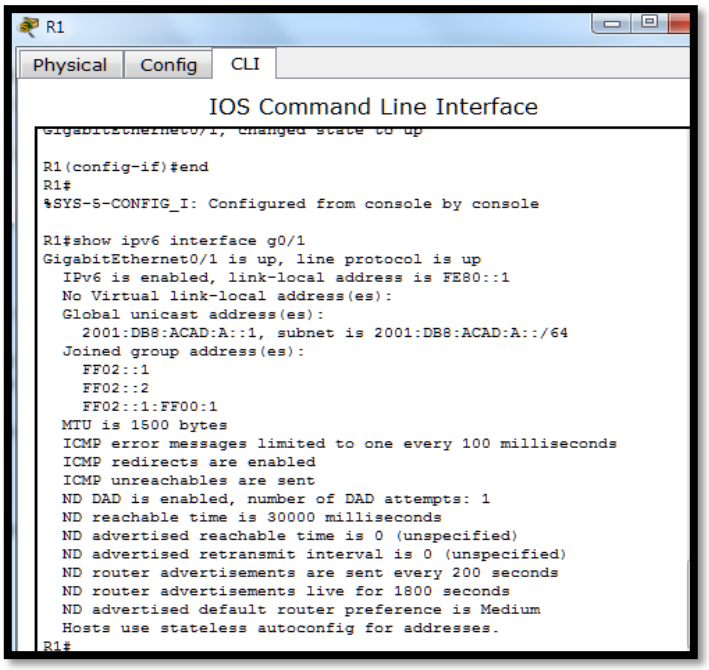
d. Active la interfaz G0/1.



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.

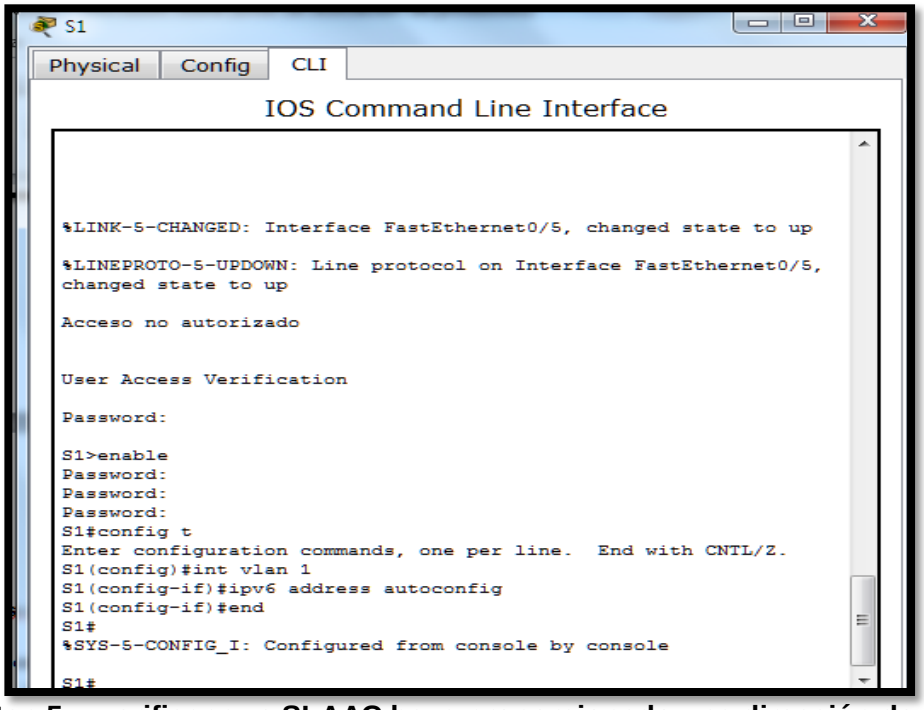
```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2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



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
```

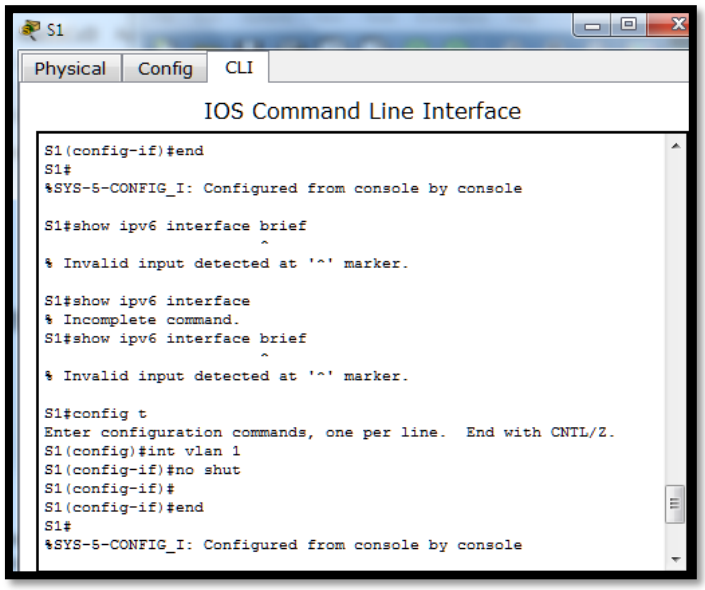


Step 5: verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

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:FFE8:8A40
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
Output features: Check hwidb
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
Default router is FE80::1 on Vlan1
```

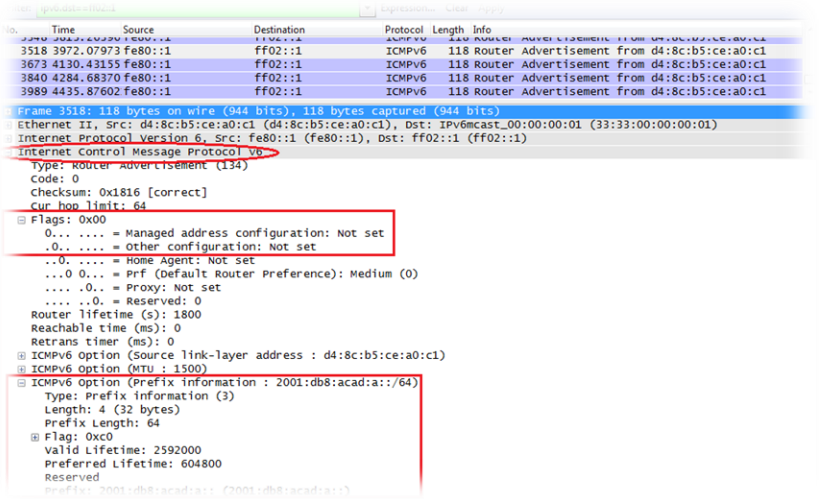


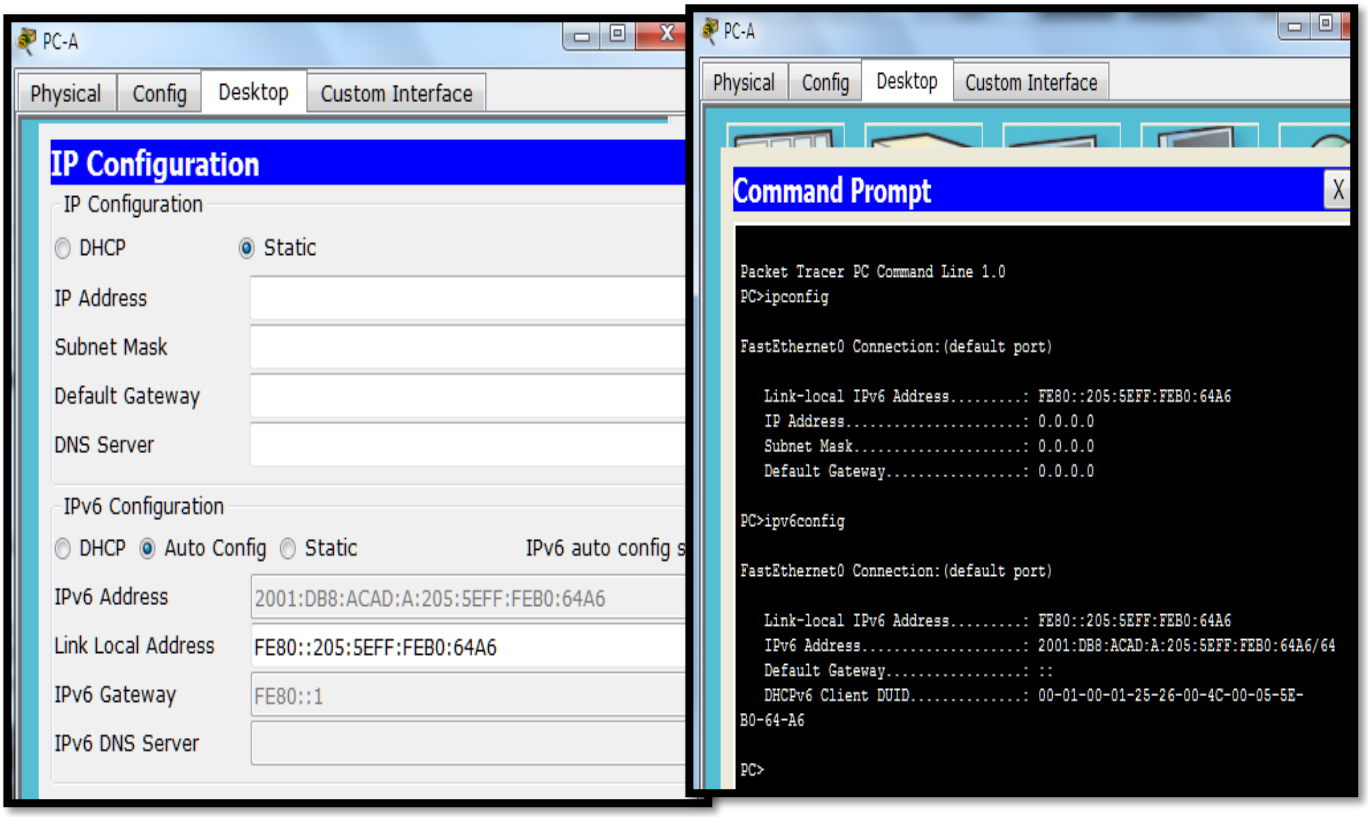
Step 6: verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

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.

```
Adaptador de Ethernet Conexión de área local:

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

   Dirección IPv4. . . . . . . . . . . . . . : 192.168.96.139(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::1%11
   Servidores DNS. . . . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                               fec0:0:0:ffff::2%1
                                               fec0:0:0:ffff::3%1
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

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.





Part 3: configurar la red para DHCPv6 sin estado

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

a. Cree un pool de DHCP IPv6.

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

b. Asigne un nombre de dominio al pool.

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

c. Asigne una dirección de servidor DNS.

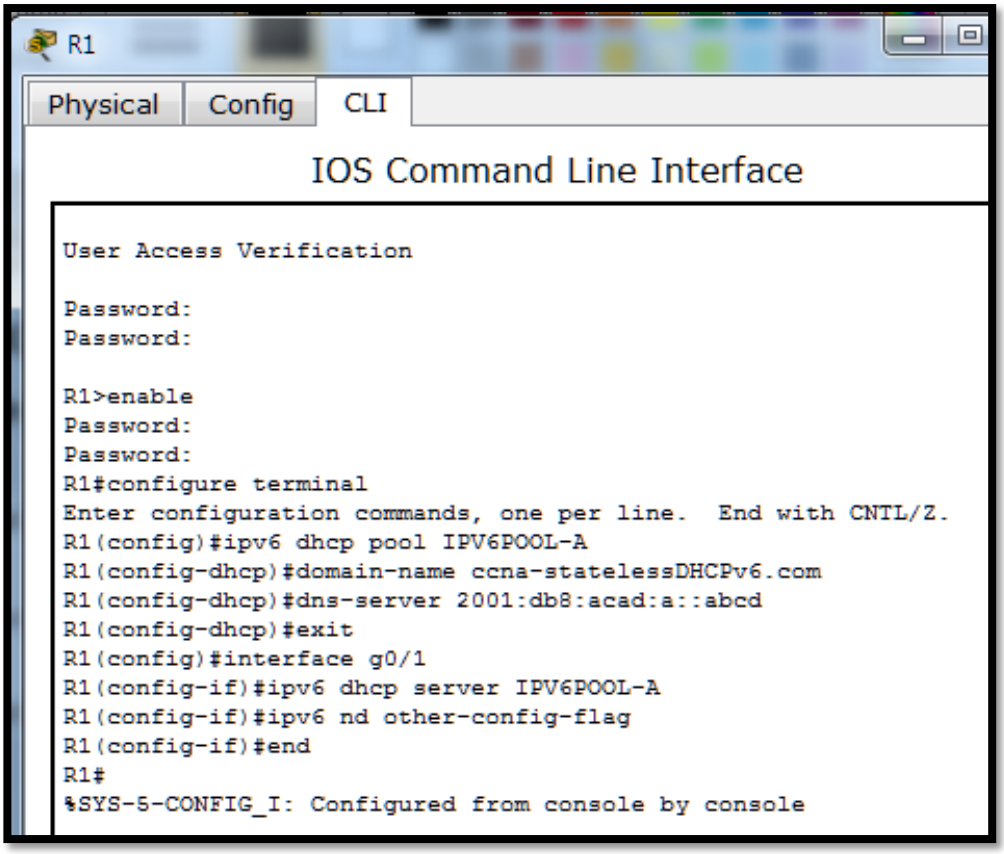
```
R1(config-dhcpv6)# dns-server 2001:db8:acad:a::abcd
R1(config-dhcpv6)# exit
```

d. Asigne el pool de DHCPv6 a la interfaz.

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

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

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



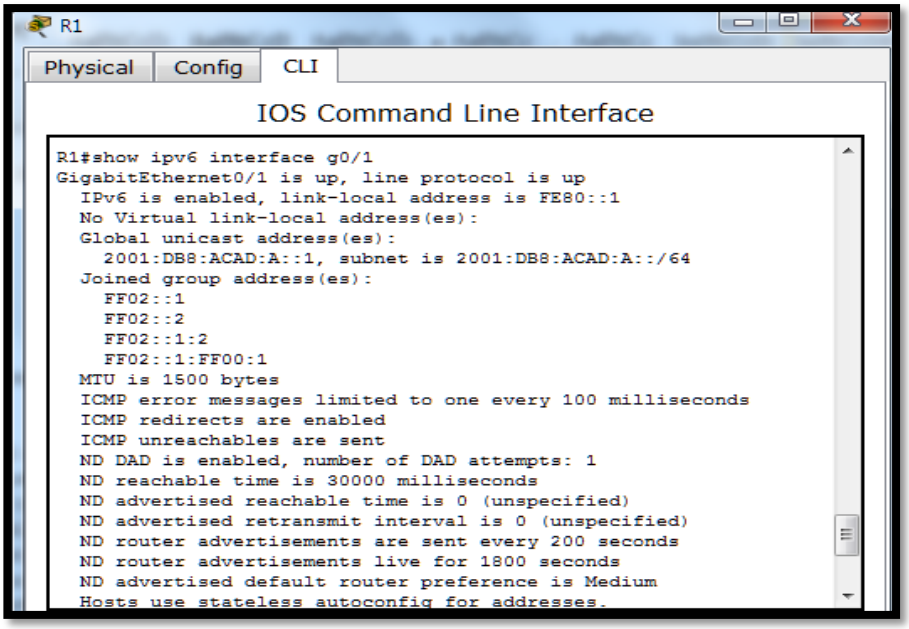
Step 2: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

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 unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

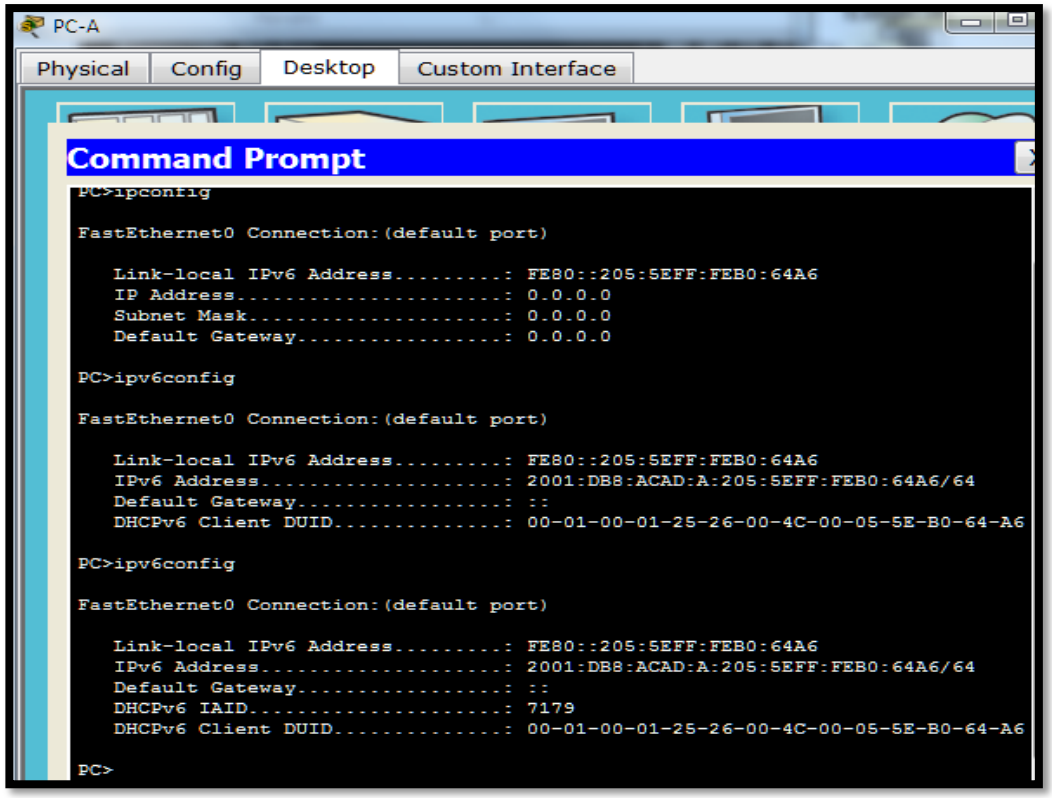
Hosts use DHCP to obtain other configuration.



Step 3: ver los cambios realizados en la red en la PC-A.

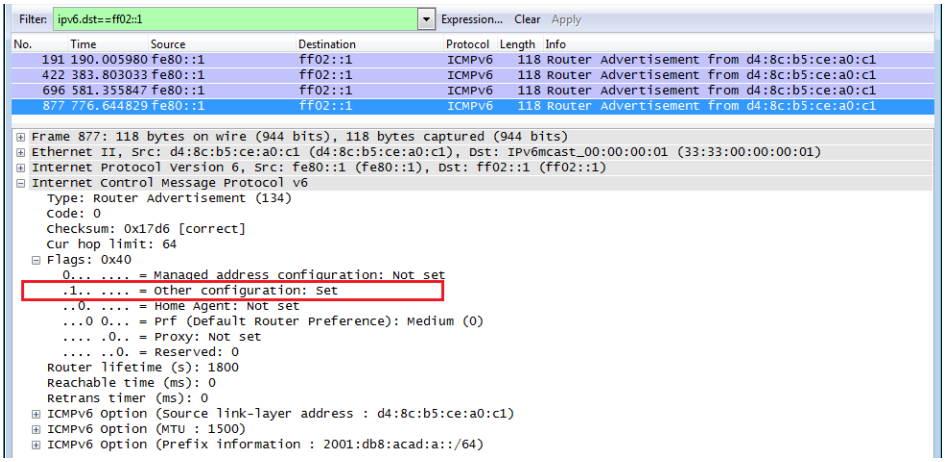
Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente 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
 MT
   Dirección física. . . . . . . . . . . . . : 00-0C-29-E3-23-17
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11(Preferido)

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

Adaptador de túnel isatap.localdomain:

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



Step 4: ver los mensajes RA en Wireshark.

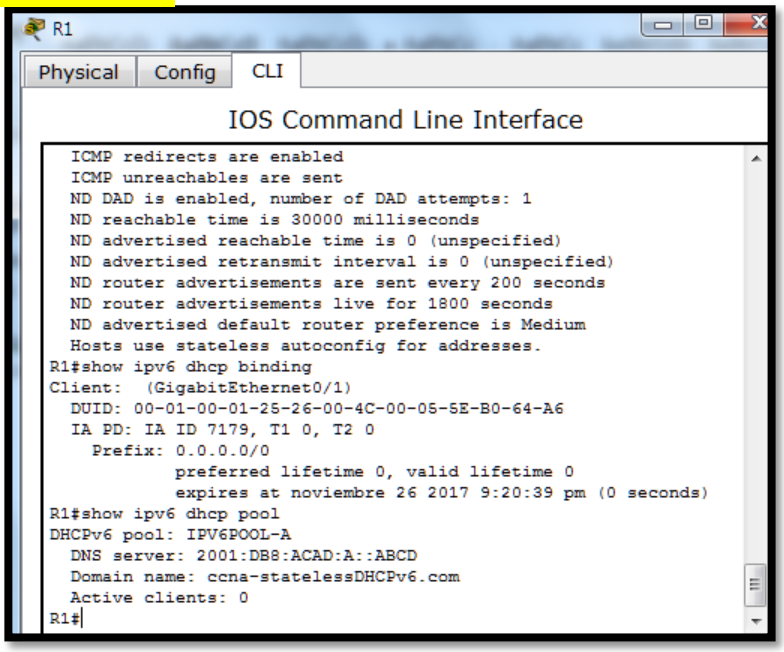
Desplácese hasta el último mensaje RA que se muestra en Wireshark y expándalo para ver la configuración de indicadores ICMPv6. Observe que el indicador Other configuration (Otra configuración) está establecido en 1.



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.

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.

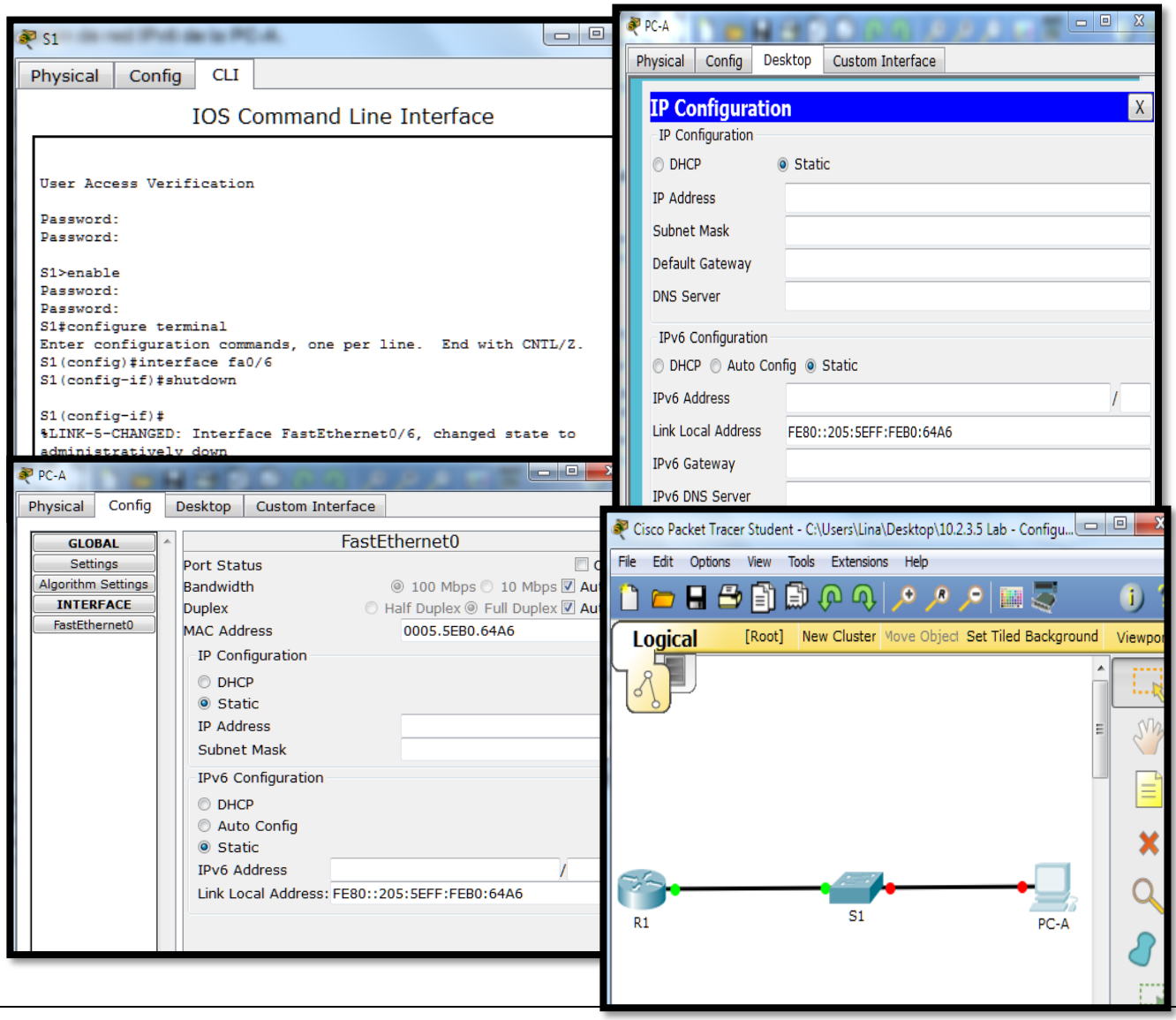
```
S1(config)# interface f0/6
S1(config-if)# shutdown
```

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 4: configurar la red para DHCPv6 con estado

Step 1: cambiar el pool de DHCPv6 en el R1.

a. Agregue el prefijo de red al pool.

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

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

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

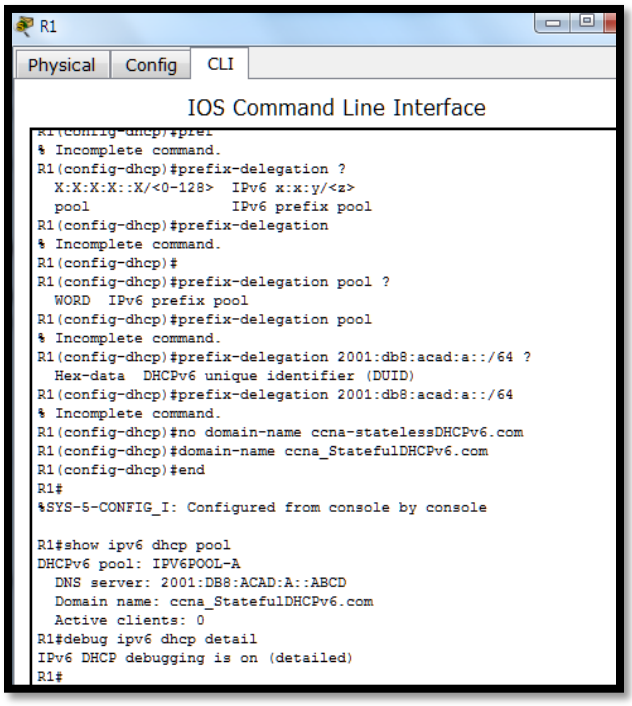
```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)# end
```

c. Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred
86400 (0 in use, 0 conflicts)
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
```

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

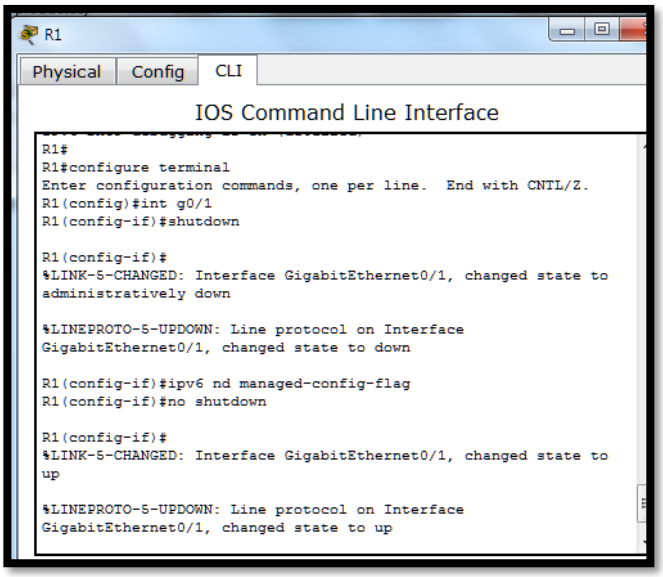
```
R1# debug ipv6 dhcp detail
   IPv6 DHCP debugging is on (detailed)
```



Step 2: 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.

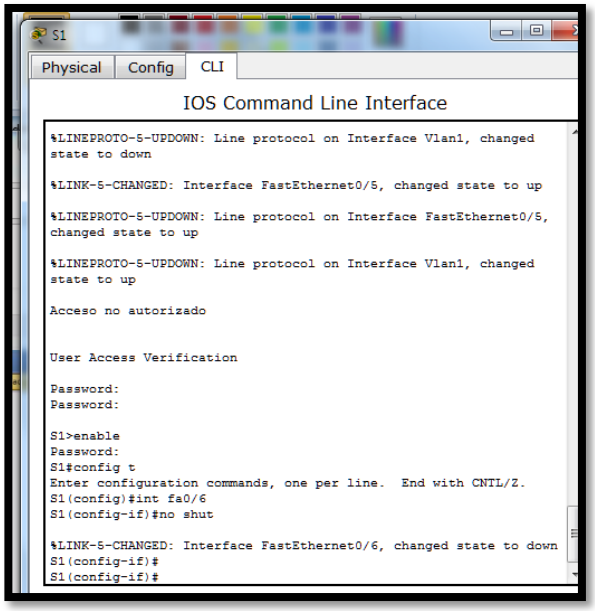
```
R1(config)# interface g0/1
R1(config-if)# shutdown
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# no shutdown
R1(config-if)# end
```



Step 3. 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.

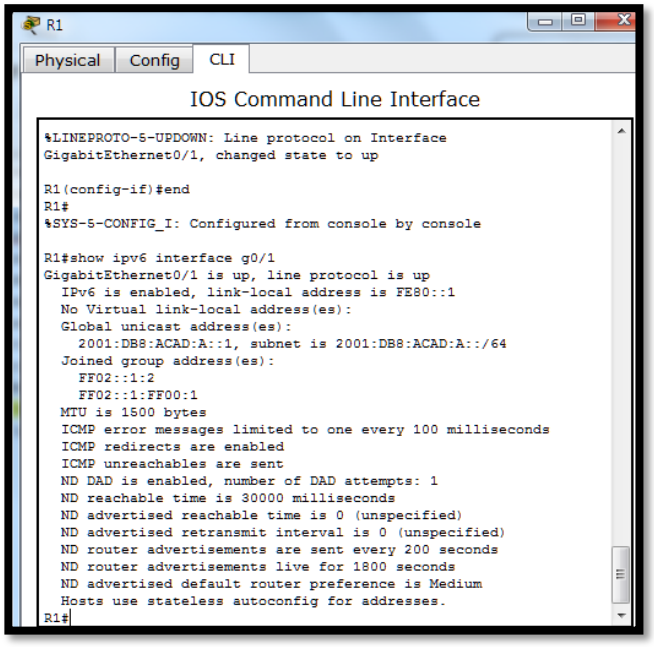
```
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# end
```



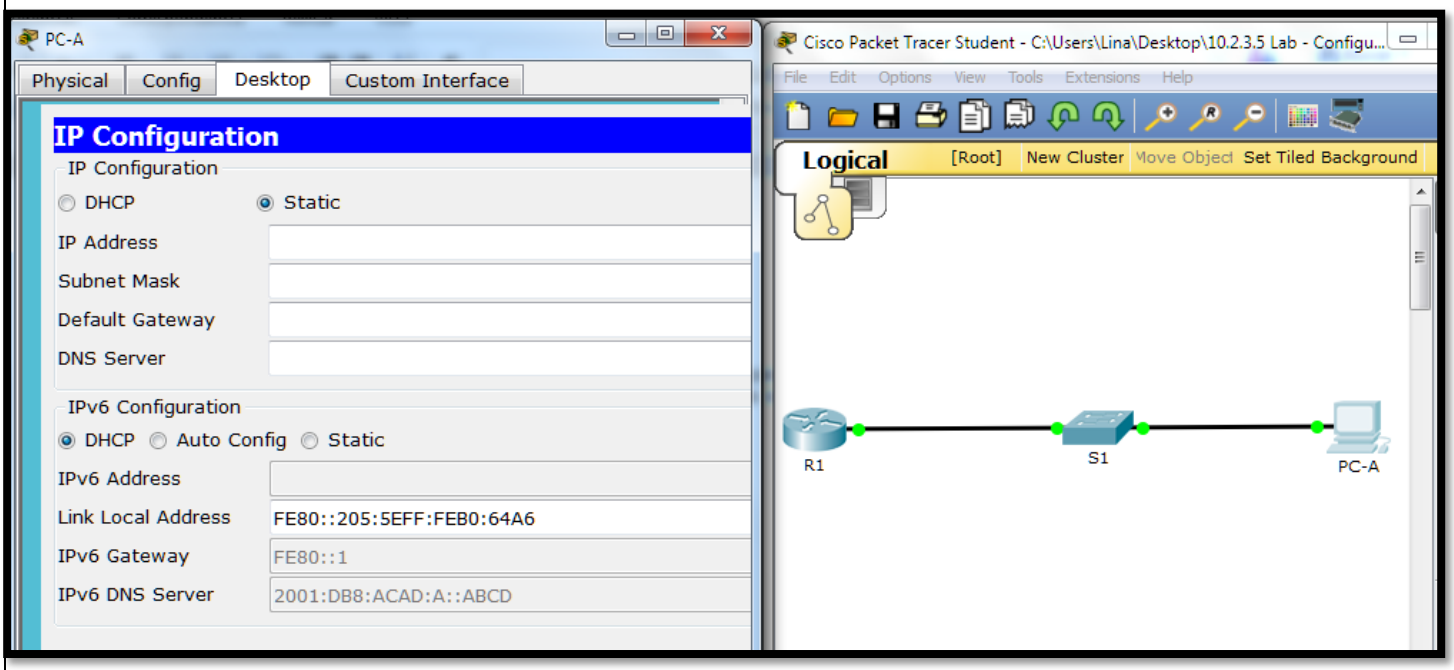
Step 3: verificar la configuración de DHCPv6 con estado en el R1.

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

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



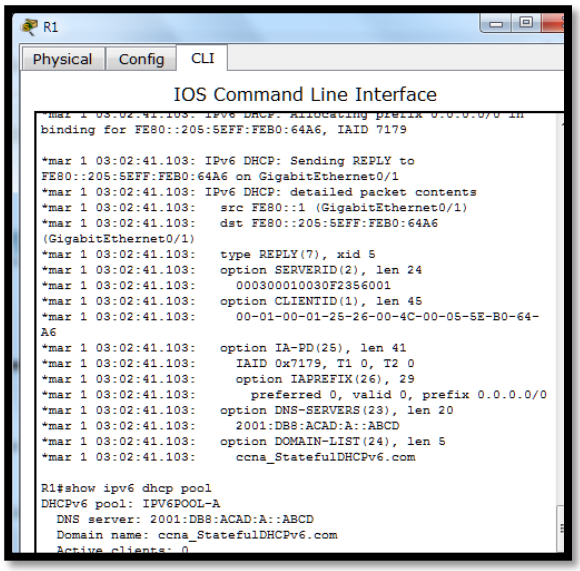
b. En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.



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
```

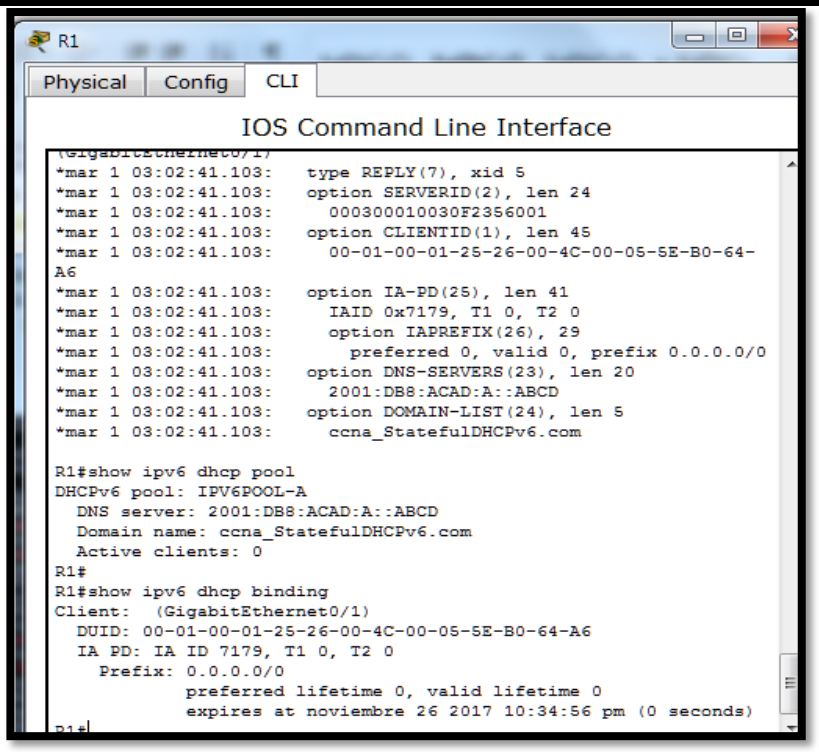
Active clients: 1



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)
```

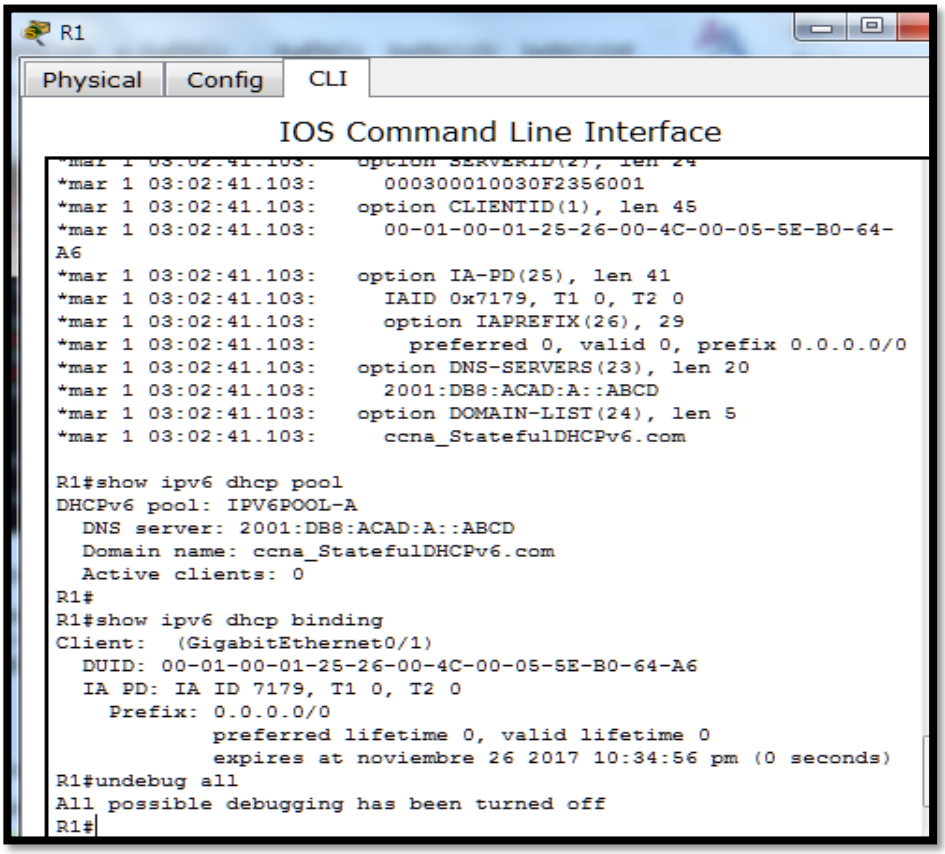
```
Adaptador de Ethernet Conexión de área local:

   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(Pref
erido)
   Concesión obtenida. . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:07:59
   La concesión expira . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:38:03
   Dirección IPv6 . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a:11(Preferido)

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



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.

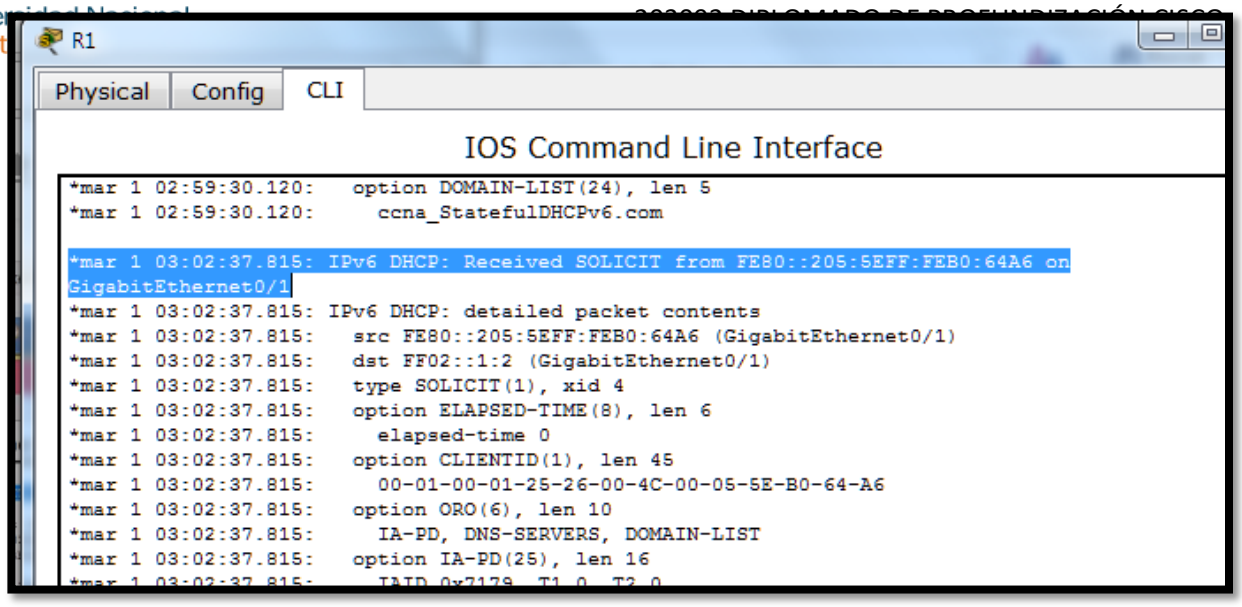
```
R1# u all
Se ha desactivado toda depuración posible
```



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

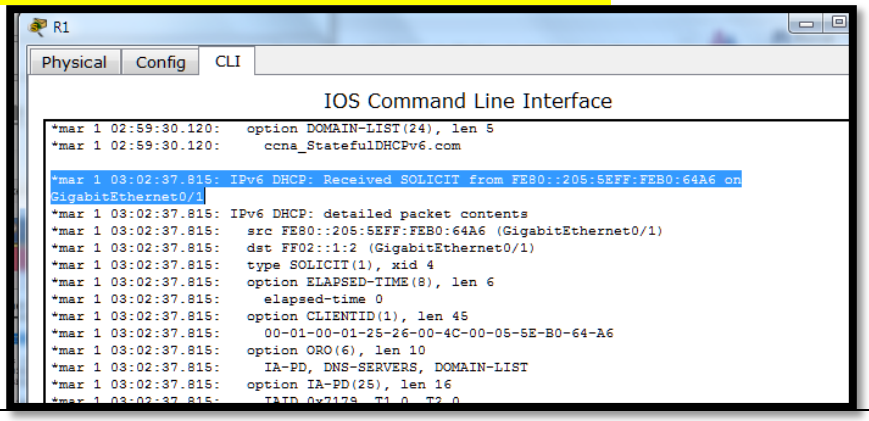
1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

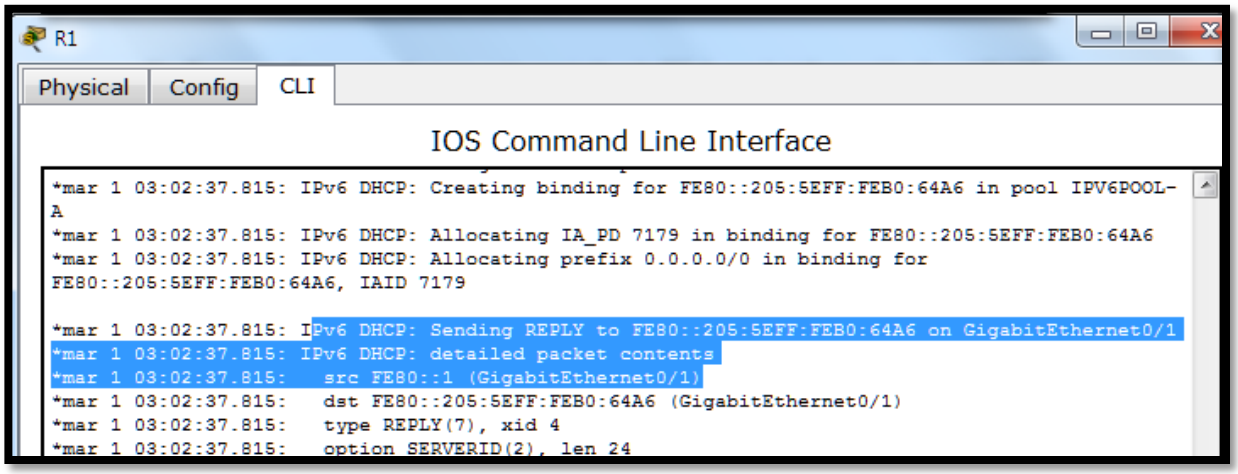
```
*Mar  5 16:42:39.775: IPv6 DHCP: Received SOLICIT from
FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1
*Mar  5 16:42:39.775: IPv6 DHCP: detailed packet contents
*Mar  5 16:42:39.775:   src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar  5 16:42:39.775:   dst FF02::1:2
*Mar  5 16:42:39.775:   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
```

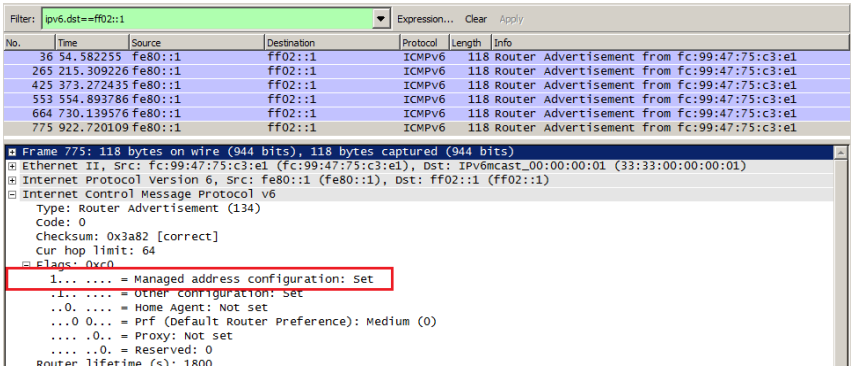




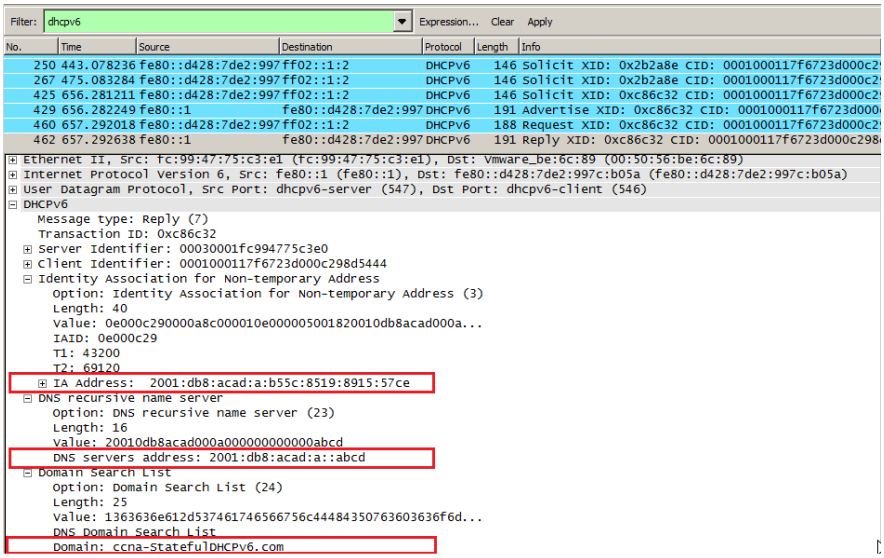
Step 4: verificar DHCPv6 con estado en la PC-A.

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

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



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



Reflexión

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

- El protocolo DHCP permite configurar automáticamente los host de una red TCP/IP durante el arranque de los sistemas. DHCP utiliza un mecanismo de cliente-servidor, a la vez los servidores almacenan y gestionan la información de configuración de los clientes y la suministran cuando éstos la solicitan.

Además el DHCPv6 requiere del router para almacenar la información de estado dinámica sobre los clientes DHCPv6, este método de direccionamiento con estado utiliza más recursos de memoria en el router que el método sin estado.

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

- Se recomienda que los dispositivos ipv6 realicen detección de direcciones duplicadas en cualquier dirección, en la configuración automática de direcciones sin estado se utiliza para configurar las direcciones locales de vínculos y las direcciones no locales de vínculos adicionales mediante el intercambio de mensajes de solicitación de enrutador y anuncio de enrutador con los enrutadores vecinos.

Tabla de Interfaces

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.

10.3.1.1 IdT y DHCP

Objetivo

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

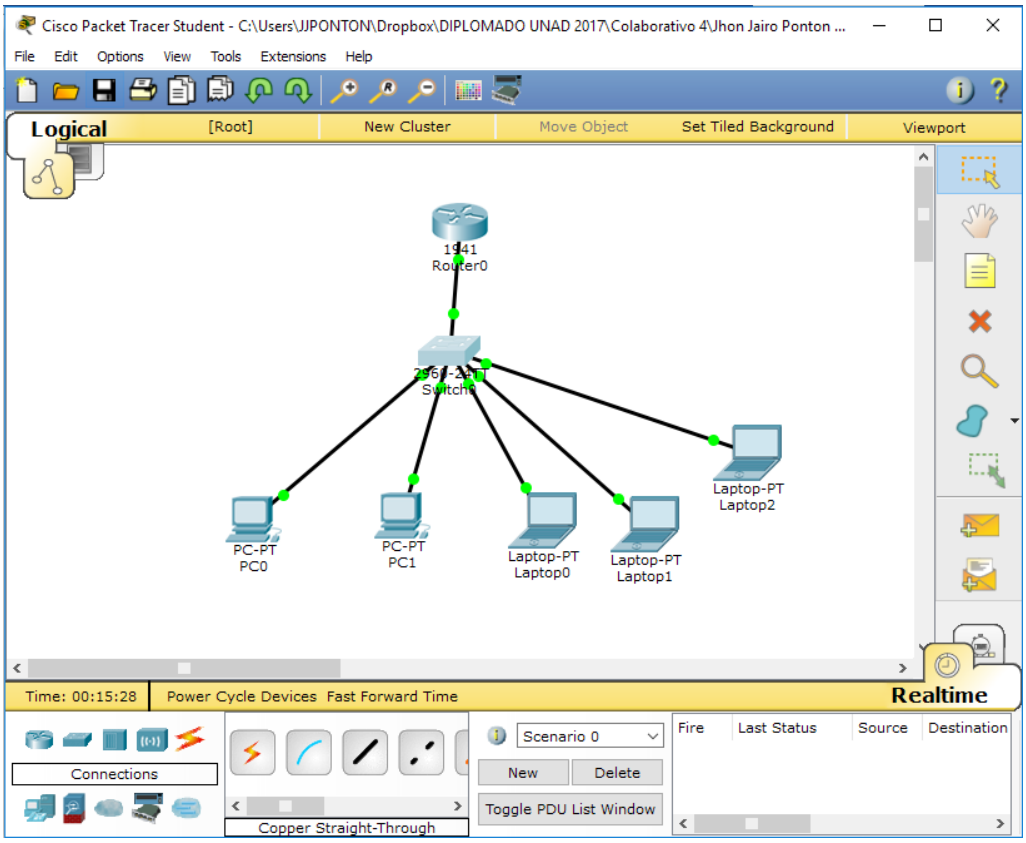
Situación

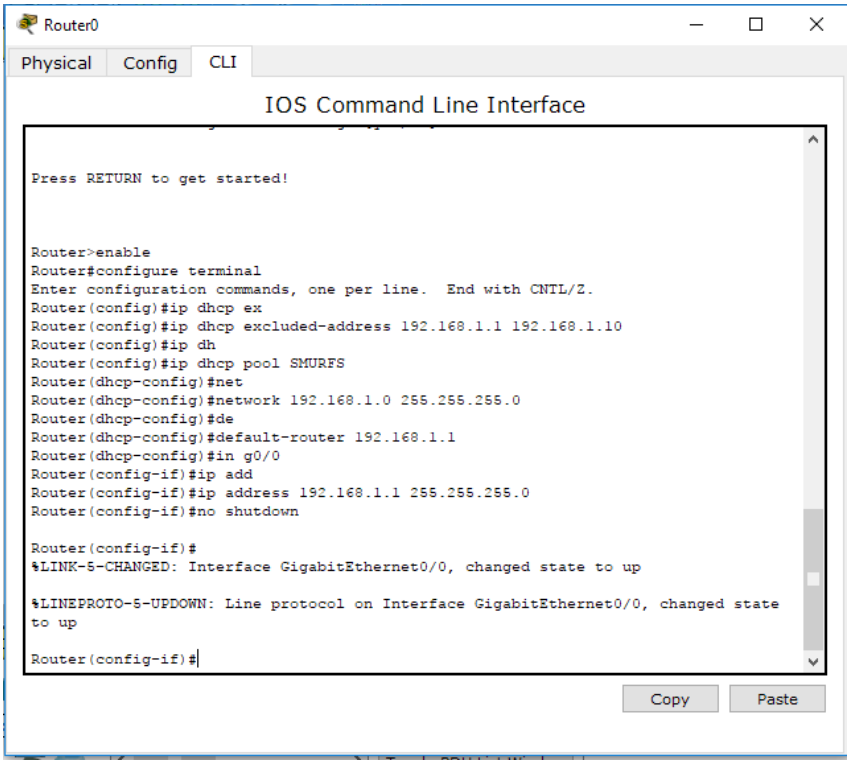
En este capítulo, se presenta el concepto del uso del proceso de DHCP en la red de una pequeña a mediana empresa; sin embargo, el protocolo DHCP también tiene otros usos.

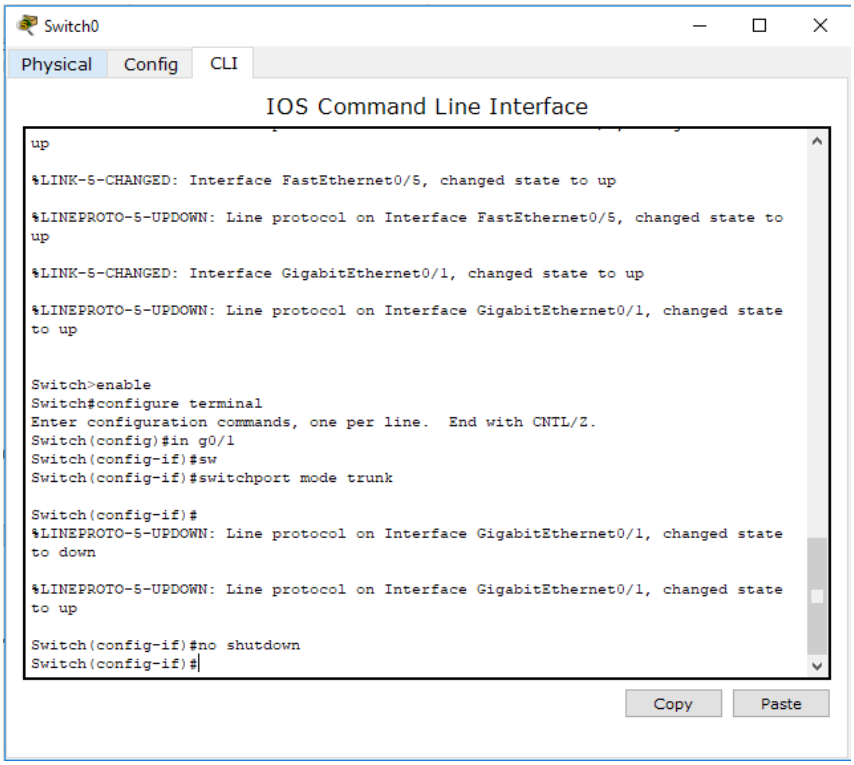
Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

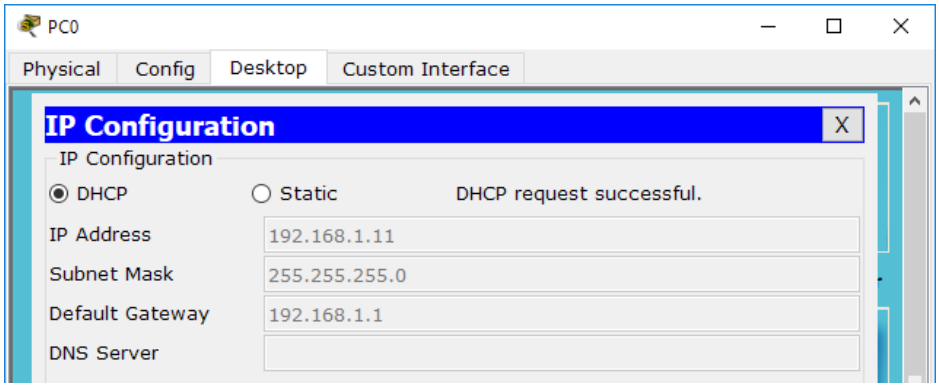
Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

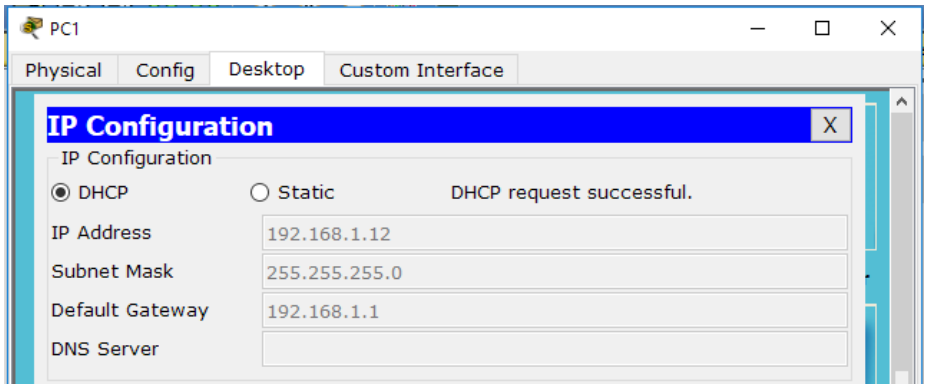
- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.
- Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones 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.

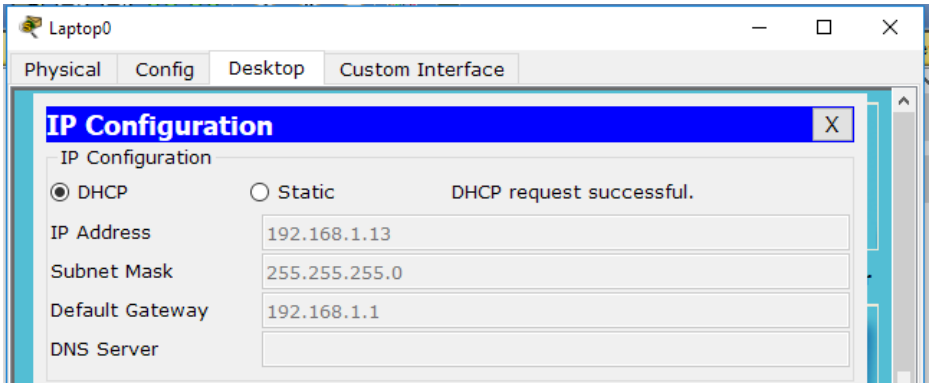

Cisco Packet Tracer Student - C:\Users\JJPONTON\Dropbox\DIPLOMADO UNAD 2017\Colaborativo 4\Jhon Jairo Ponton ...
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
1941 Router0
Switch0
PC-PT PC0
PC-PT PC1
Laptop-PT Laptop0
Laptop-PT Laptop1
Laptop-PT Laptop2
Time: 00:15:28 Power Cycle Devices Fast Forward Time
Realtime
Connections
Copper Straight-Through
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination

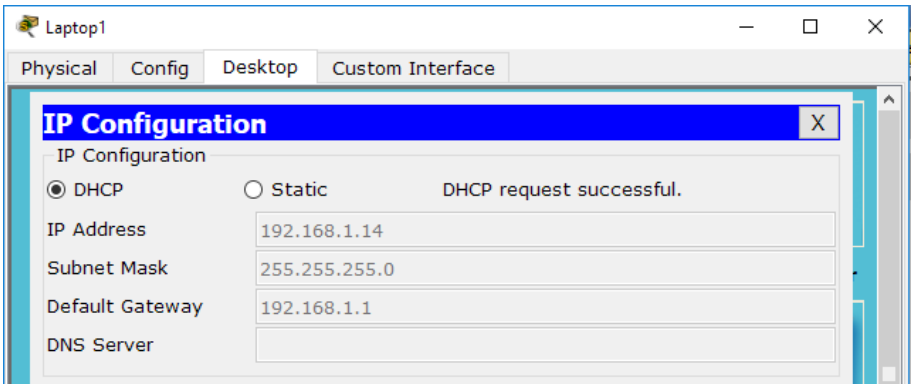

Router0
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started!
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp ex
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
Router(config)#ip dh
Router(config)#ip dhcp pool SMURFS
Router(dhcp-config)#net
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#de
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#in g0/0
Router(config-if)#ip add
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Router(config-if)#
Copy Paste

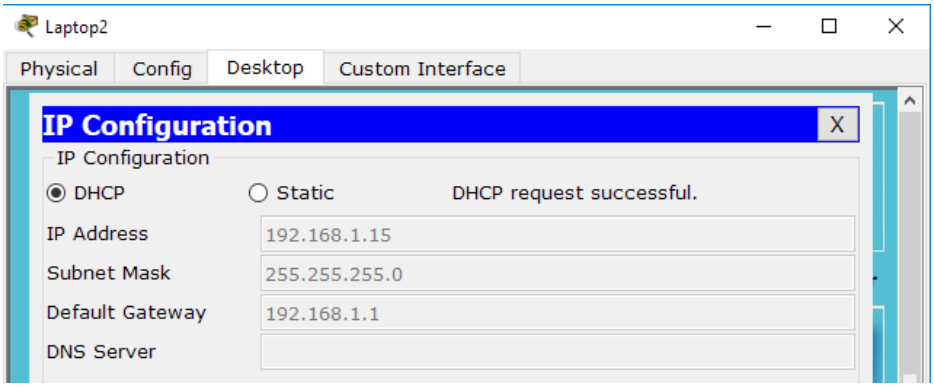

Switch0
Physical
Config
CLI
IOS Command Line Interface
up
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#in g0/1
Switch(config-if)#sw
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Switch(config-if)#no shutdown
Switch(config-if)#
Copy
Paste


PC0
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server


PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server


Laptop0
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.13
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server


Laptop1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server



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?

   Un Router 1941 es de menor costo y lo complementa los 2 puertos para conexión básica a swiches

   ¿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.

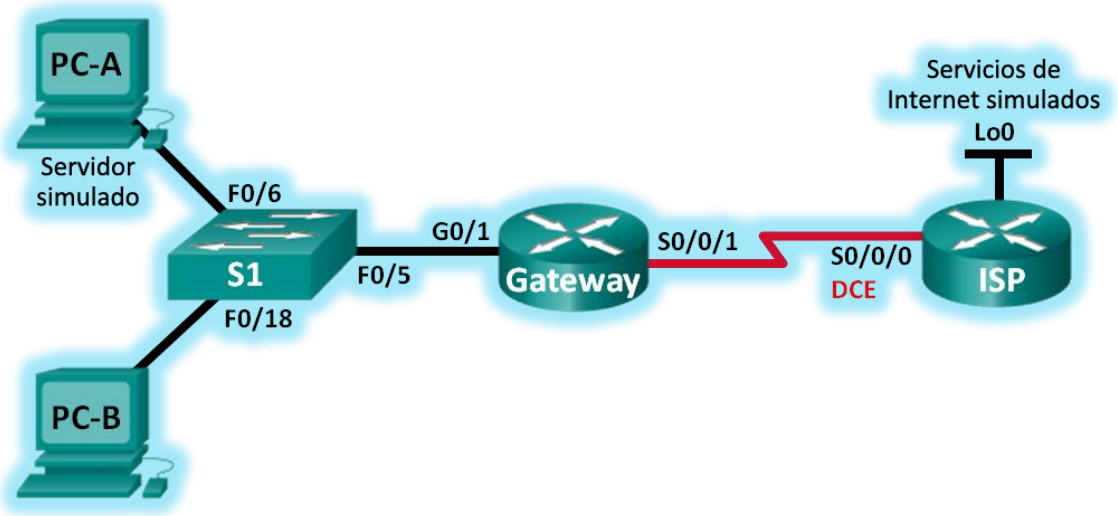
   Ipv6 tiene más direcciones disponibles

   Ipv6 es más dinámica y más fácil de configurar

   Ipv6 da complemento en seguridad a las protecciones básicas de los router

11.2.2.6 Práctica de laboratorio: configuración de NAT dinámica y estática

Topología



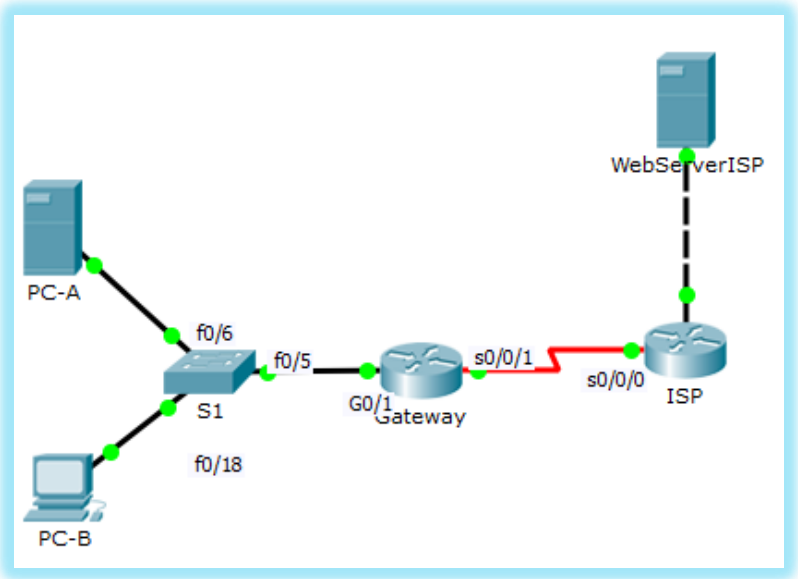


Tabla de direccionamiento

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

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

Información básica/situación

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

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

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

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

Recursos necesarios

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

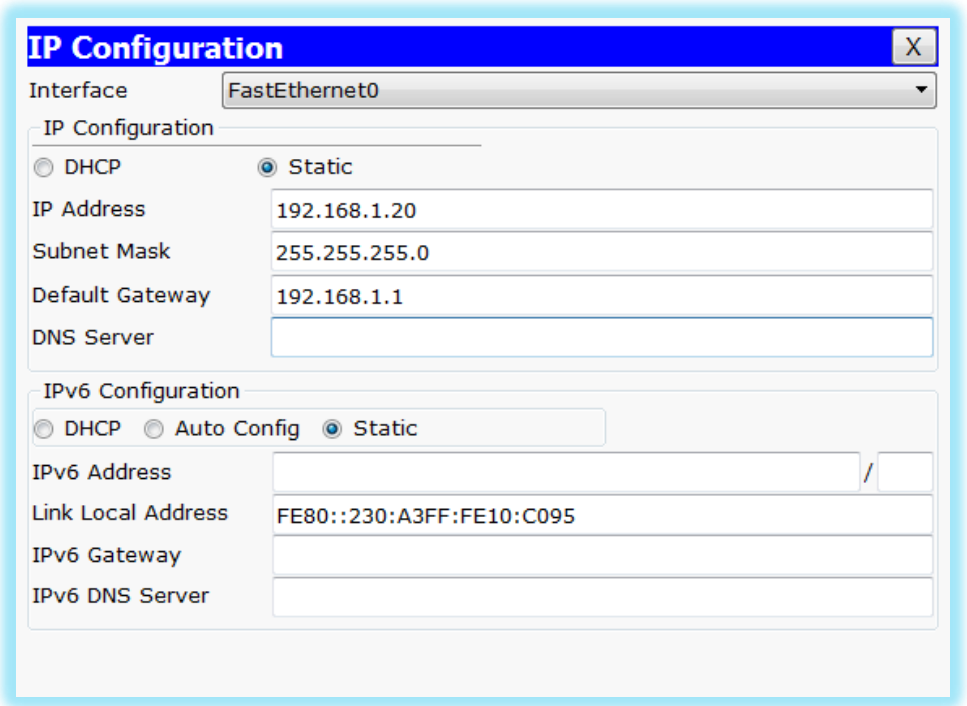
Part 1: armar la red y verificar la conectividad

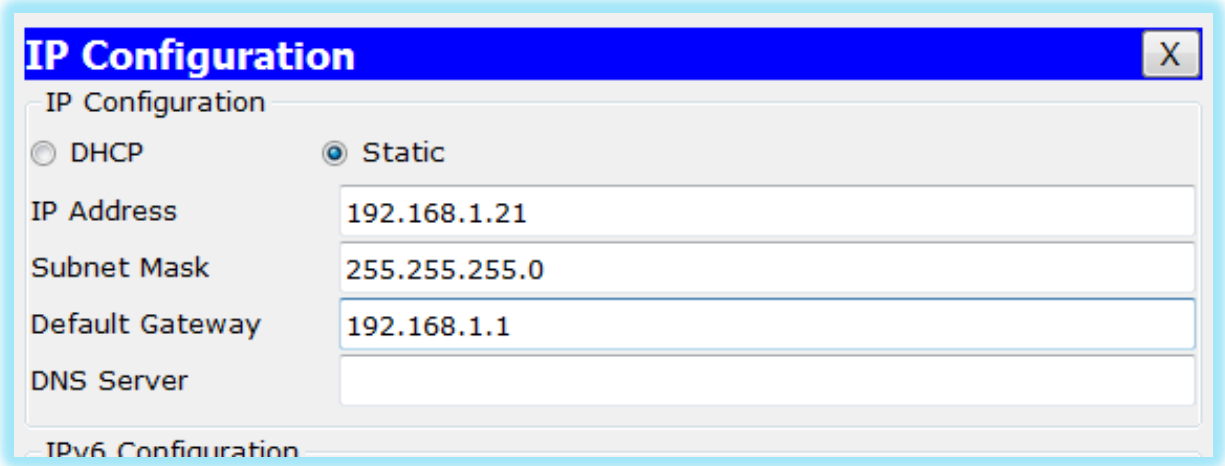
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

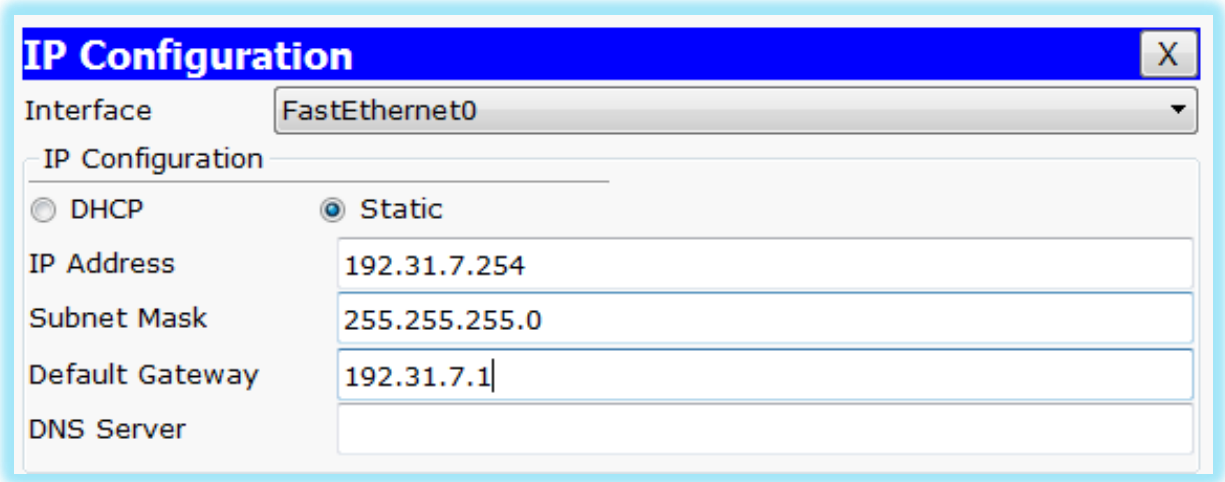
Step 1: realizar el cableado de red tal como se muestra en la topología.

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

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.

a. Desactive la búsqueda del DNS.
b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
c. Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.
d. Configure el nombre del dispositivo como se muestra en la topología.
e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

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

Step 5: crear un servidor web simulado en el ISP.

- No podemos configurar el router ISP como servidor WEB ya que el simulador de Packet Tracer no lo soporta.

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

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

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

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

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

```
ISP(config)# ip http authentication local
```

Step 6: configurar el routing estático.

a. Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

```
ISP#config
Configuring from terminal, memory, or network [terminal]?
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
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>enable
Password:
Gateway#config
Configuring from terminal, memory, or network [terminal]?
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
Gateway(config)#
```

Step 7: Guardar la configuración en ejecución en la configuración de inicio.

Step 8: 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.

Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=62ms TTL=255
Reply from 192.168.1.1: bytes=32 time=14ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms 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 = 62ms, Average = 19ms

SERVER>

Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

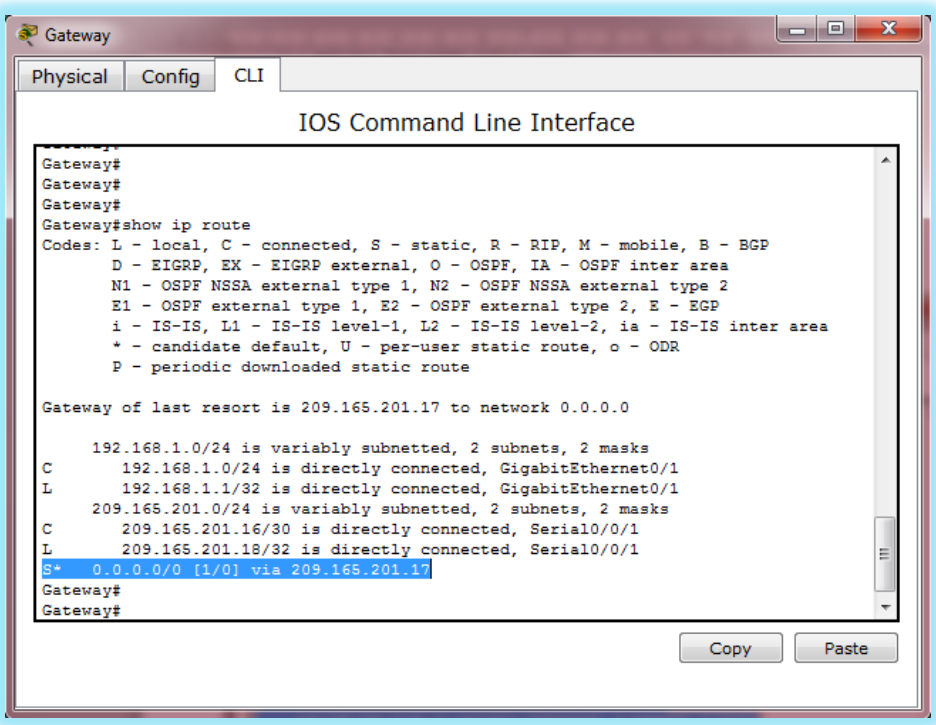
Pinging 192.168.1.1 with 32 bytes of data:

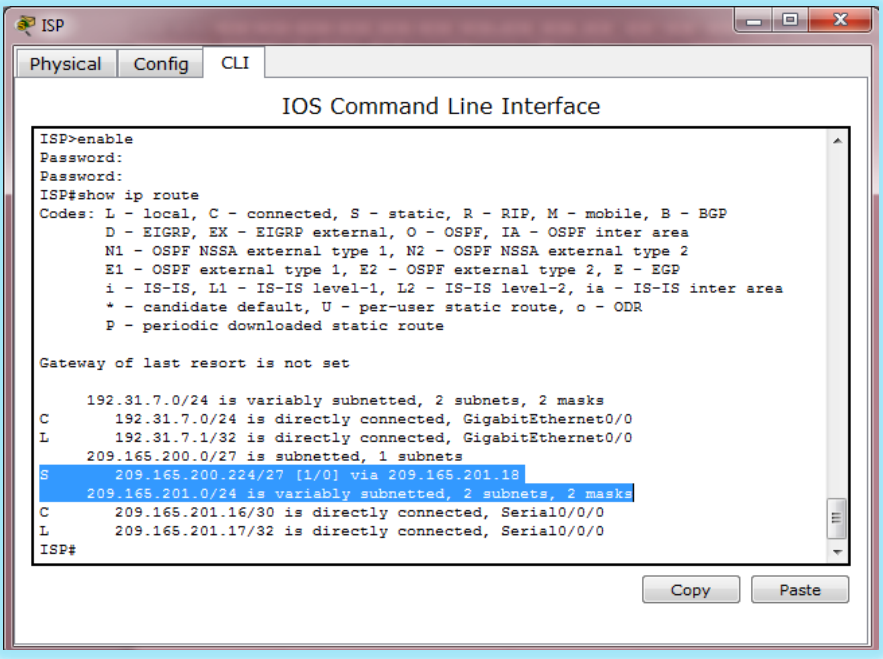
Reply from 192.168.1.1: bytes=32 time=13ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

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 = 13ms, Average = 3ms

PC>

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.





Part 2: 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#config
Configuring from terminal, memory, or network [terminal]?
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)#
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#
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---

Gateway#

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 =

- 209.165.200.225

¿Quién asigna la dirección global interna?

- El router del pool de la NAT.

¿Quién asigna la dirección local interna?

- El administrador de la estación de trabajo.

b. En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

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
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 = 1ms, Average = 1ms

SERVER>

```
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 209.165.200.225:17192.168.1.20:17 192.31.7.1:17 192.31.7.1:17
icmp 209.165.200.225:18192.168.1.20:18 192.31.7.1:18 192.31.7.1:18
icmp 209.165.200.225:19192.168.1.20:19 192.31.7.1:19 192.31.7.1:19
icmp 209.165.200.225:20192.168.1.20:20 192.31.7.1:20 192.31.7.1:20
--- 209.165.200.225 192.168.1.20 --- ---

Gateway#
```

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?

- 17
- 18
- 19
- 20

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       ---                ---
```

```
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.225:1025192.168.1.20:1025 192.31.7.1:23 192.31.7.1:23

Gateway#
```

Nota: es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

¿Qué protocolo se usó para esta traducción?

- TCP

¿Cuáles son los números de puerto que se usaron?

- 1025

Global/local interno:

- 1025.

Global/local externo:

- 23

d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.

```
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=3ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126
Reply from 209.165.200.225: bytes=32 time=3ms TTL=126

Ping statistics for 209.165.200.225:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 2ms

SERVER>
```

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       ---                ---
```

Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:10192.168.1.20:10 192.31.7.254:10 192.31.7.254:10
icmp 209.165.200.225:11192.168.1.20:11 192.31.7.254:11 192.31.7.254:11
icmp 209.165.200.225:12192.168.1.20:12 192.31.7.254:12 192.31.7.254:12
icmp 209.165.200.225:9 192.168.1.20:9 192.31.7.254:9 192.31.7.254:9
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.225:1025192.168.1.20:1025 192.31.7.1:23 192.31.7.1:23

Gateway#

Observe que la dirección local externa y la dirección global externa son iguales. Esta dirección es la dirección de origen de red remota del ISP. Para que el ping del ISP se realice correctamente, la dirección global interna de NAT estática 209.165.200.225 se tradujo a la dirección local interna de la PC-A (192.168.1.20).

f. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

```
Gateway# show ip nat statics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 74 Misses: 29

```
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13 , allocated 0 (0%), misses 0
Gateway#
```

```
Gateway#
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Part 3: 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#clear ip nat translation *
Gateway#clear ip nat statistics
                      ^
% Invalid input detected at '^' marker.

Gateway#
```

- clear ip nat statistics: comando no soportado por Packet Tracer.

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
```

```
Gateway#config
Configuring from terminal, memory, or network [terminal]?
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#
```

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.

```
Gateway# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  FastEthernet0/1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

```
Gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 74  Misses: 29
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13 , allocated 0 (0%), misses 0
Gateway#
```

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
```

```
Gateway#config
```

```
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224
Gateway(config)#
```

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
```

```
Gateway(config)#ip nat inside source list 1 pool public_access
Gateway(config)#
```

Step 6: probar la configuración.

```
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=15ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=20ms 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 = 20ms, Average = 9ms

PC>
```

a. En la PC-B, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242    192.168.1.21       ---                ---
```

```
Gateway#
```

```
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.242:12192.168.1.21:12 192.31.7.1:12 192.31.7.1:12
--- 209.165.200.225 192.168.1.20 --- ---

Gateway#
```

¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 =

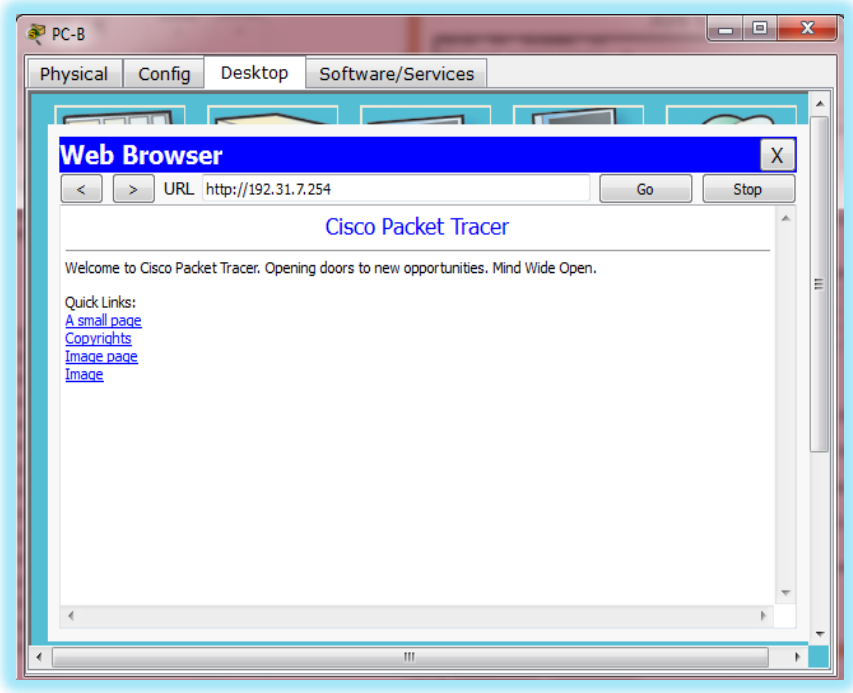
- 209.165.200.242

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?

- 12

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#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.242:1025192.168.1.21:1025 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1026192.168.1.21:1026 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1027192.168.1.21:1027 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1028192.168.1.21:1028 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1029192.168.1.21:1029 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1030192.168.1.21:1030 192.31.7.254:80 192.31.7.254:80

Gateway#
```

¿Qué protocolo se usó en esta traducción?

- TCP

¿Qué números de puerto se usaron?

Interno:

- 1025
- a

- 1030.

Externo:

- 80

¿Qué número de puerto bien conocido y qué servicio se usaron?

- Puerto 80:
- www.
- 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: 12 (1 static, 11 dynamic, 11 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 169 Misses: 53
Expired translations: 41
Dynamic mappings:
-- Inside Source

```
access-list 1 pool public_access refCount 11
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#
```

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
```

```
Gateway#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#no ip nat inside source static 192.168.1.20 209.165.200.225
Gateway(config)#
```

b. Borre las NAT y las estadísticas.

c. Haga ping al ISP (192.31.7.1) desde ambos hosts.

d. Muestre la tabla y las estadísticas de NAT.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16  Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
```

```
[Id: 1] access-list 1 pool public_access refcount 4
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243    192.168.1.20       ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.242    192.168.1.21       ---                ---
```

Gateway#show ip nat statistics
Total translations: 8 (0 static, 8 dynamic, 8 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 177 Misses: 61
Expired translations: 41
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 8
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
Gateway#

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Gateway#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.243:29192.168.1.20:29 192.31.7.1:29 192.31.7.1:29
icmp 209.165.200.243:30192.168.1.20:30 192.31.7.1:30 192.31.7.1:30
icmp 209.165.200.243:31192.168.1.20:31 192.31.7.1:31 192.31.7.1:31
icmp 209.165.200.243:32192.168.1.20:32 192.31.7.1:32 192.31.7.1:32
icmp 209.165.200.244:21192.168.1.21:21 192.31.7.1:21 192.31.7.1:21
icmp 209.165.200.244:22192.168.1.21:22 192.31.7.1:22 192.31.7.1:22
icmp 209.165.200.244:23192.168.1.21:23 192.31.7.1:23 192.31.7.1:23

icmp 209.165.200.244:24192.168.1.21:24 192.31.7.1:24 192.31.7.1:24

Gateway#

Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?
   - Porque con una sola dirección IP pública podemos dar salida a muchos equipos con IP privada dentro de nuestra red para que tengan acceso a internet.
   - NAT puede ser visto también como un método de seguridad para nuestra red local.
2. ¿Cuáles son las limitaciones de NAT?
   - Dentro de los encabezados debe agregar mucha información adicional, lo cual genera retardos superiores a los normales.

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.				

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

Topología

Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación

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

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

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

uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

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

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

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

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

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

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

```
S1# show sdm prefer
```

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

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

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

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

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.

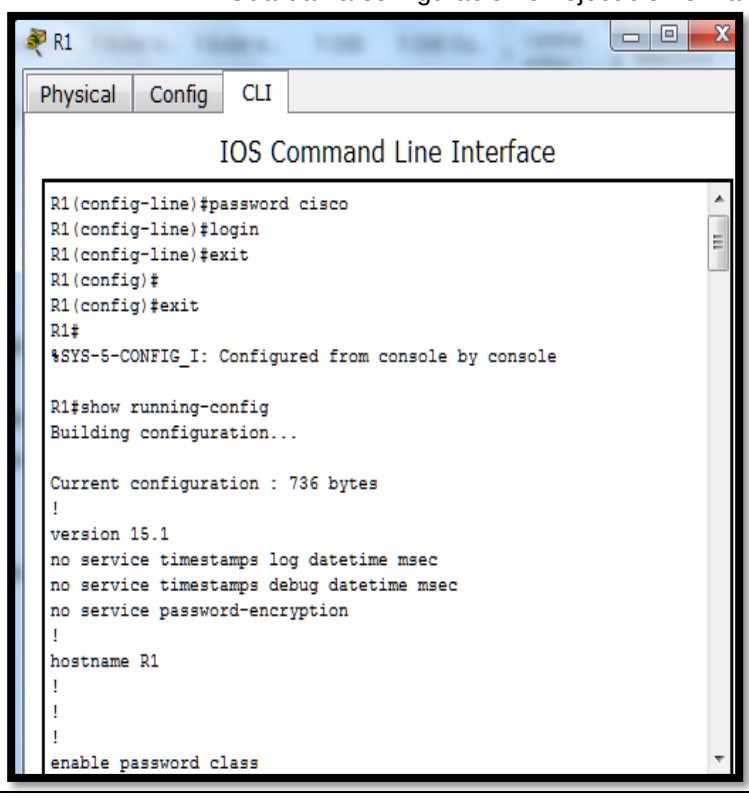
d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.

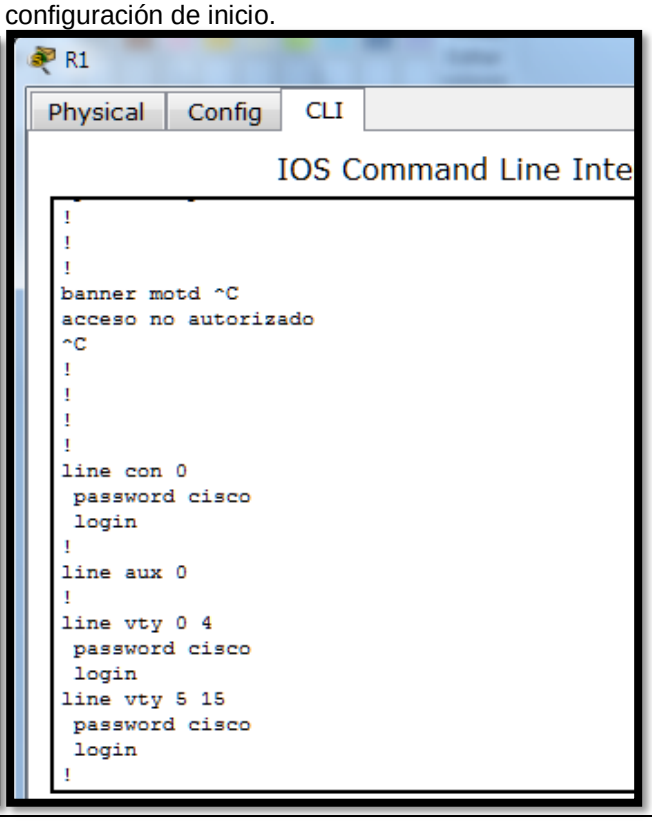
e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

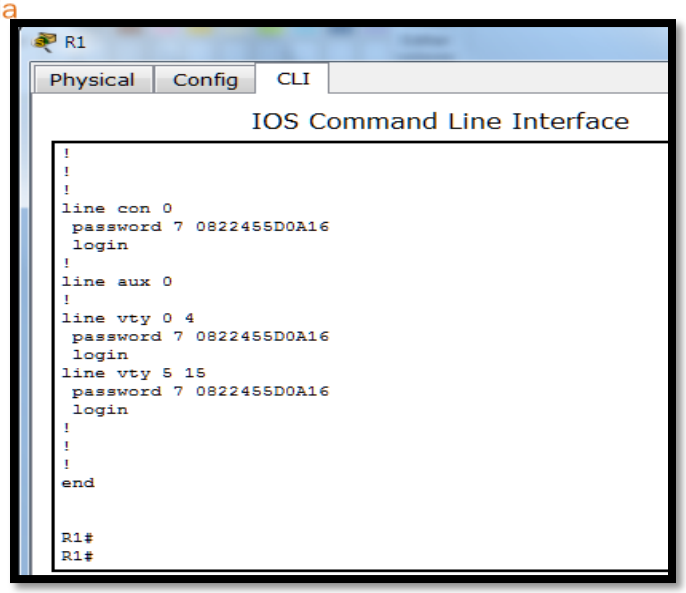
f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

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.

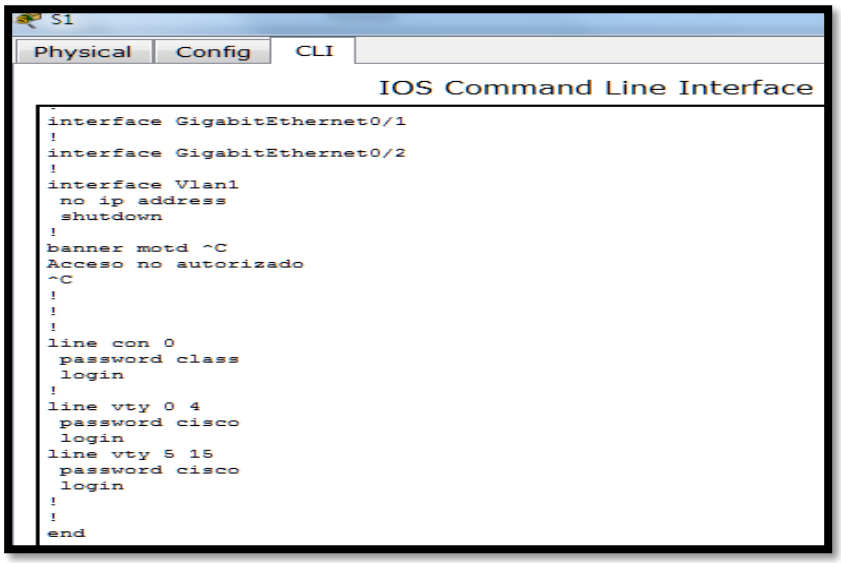
e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

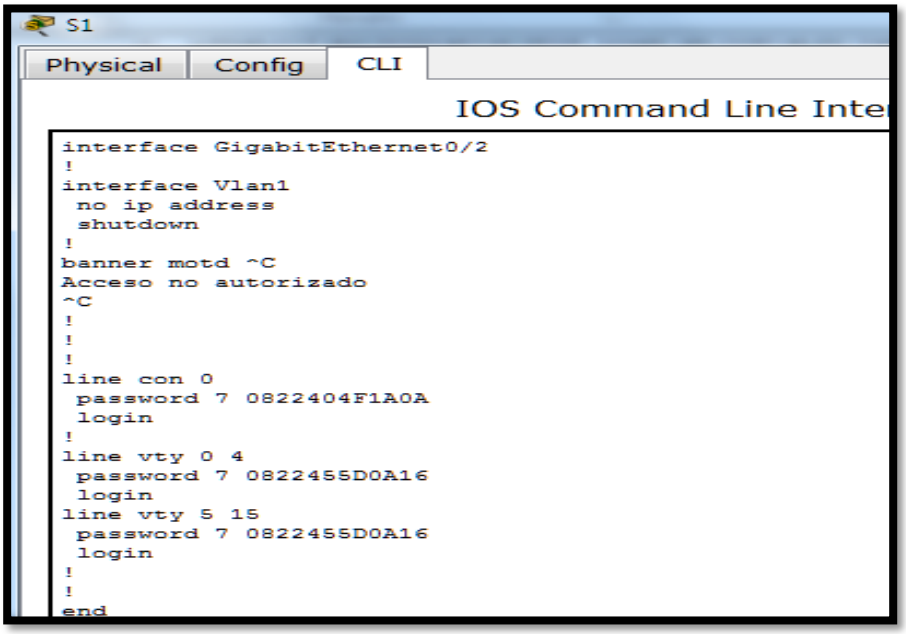
f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

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

h. Desactive administrativamente todas las interfaces inactivas.

Guarde la configuración en ejecución en la configuración de inicio

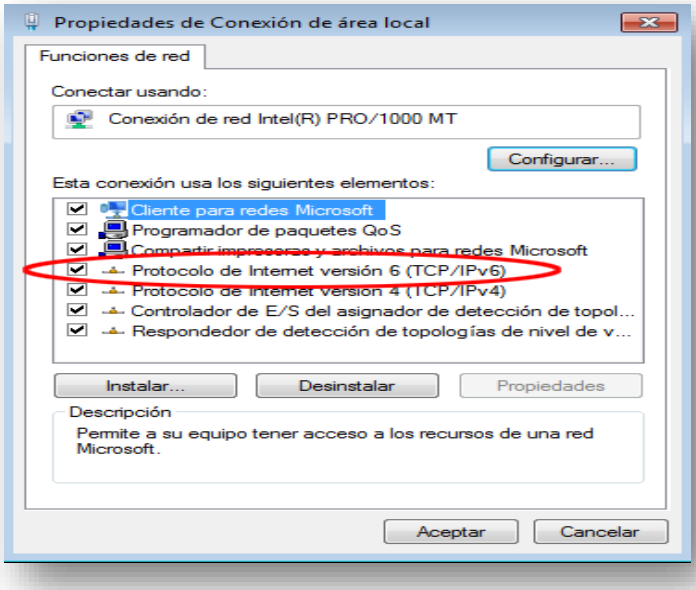




Part 2: configurar la red para SLAAC

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.

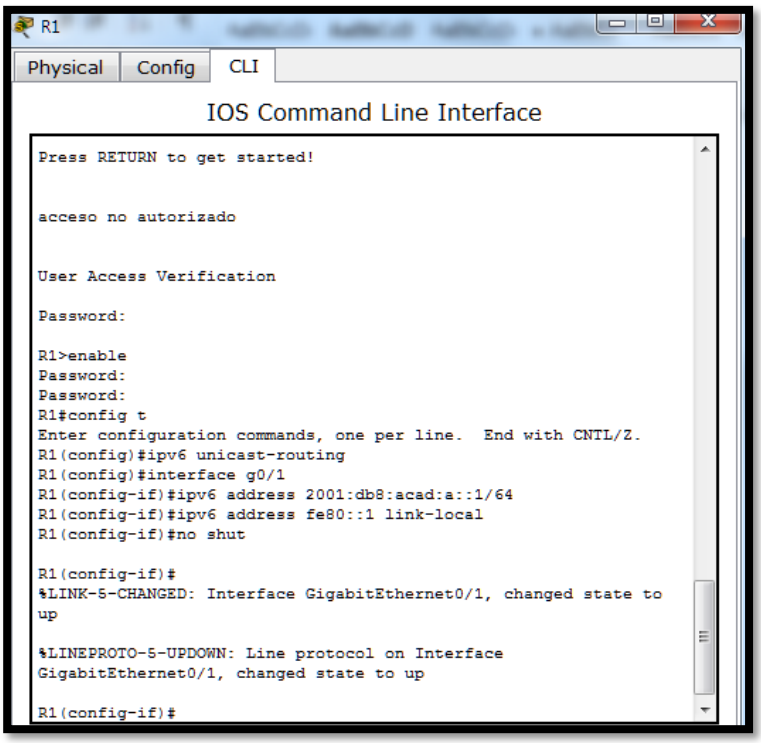
Step 2: Configurar R1

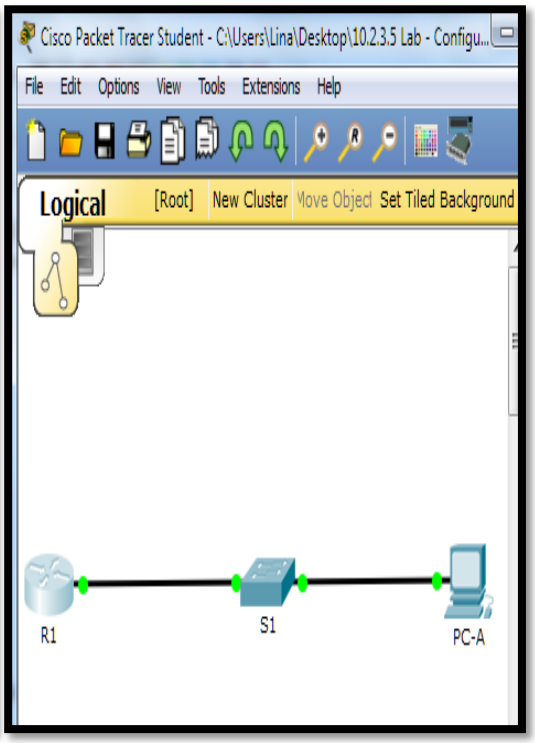
a. Habilite el routing de unidifusión IPv6.

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.

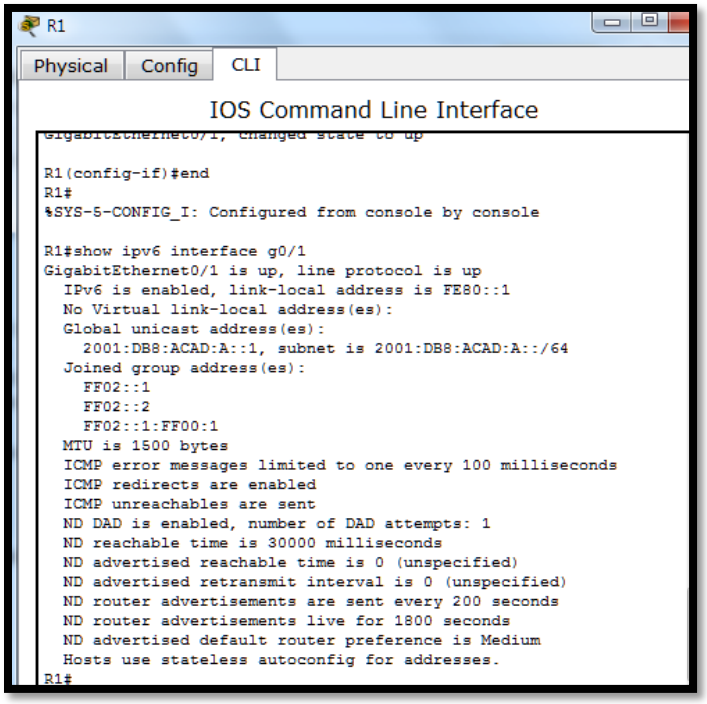




Step 3: verificar que el R1 forme parte del grupo de multidifusión de todos los routers.

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.

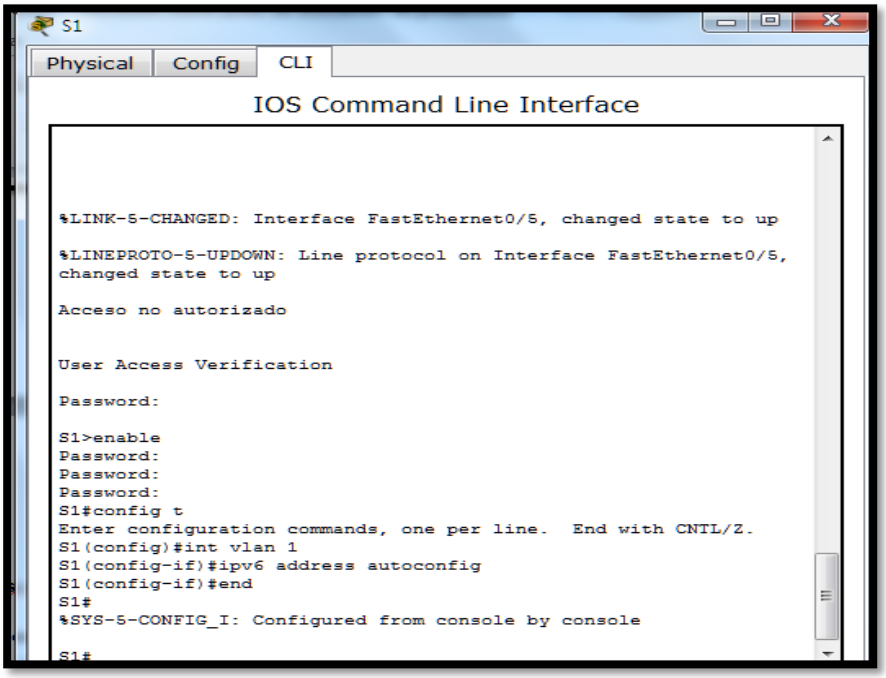
```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2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



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
```

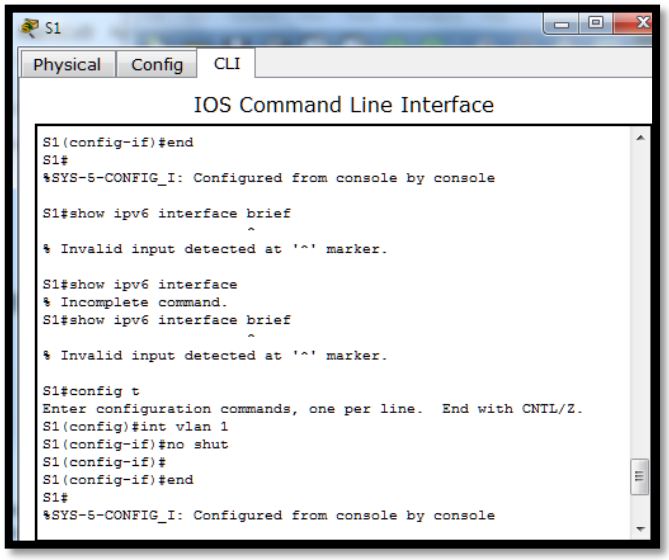


Step 5: verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

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

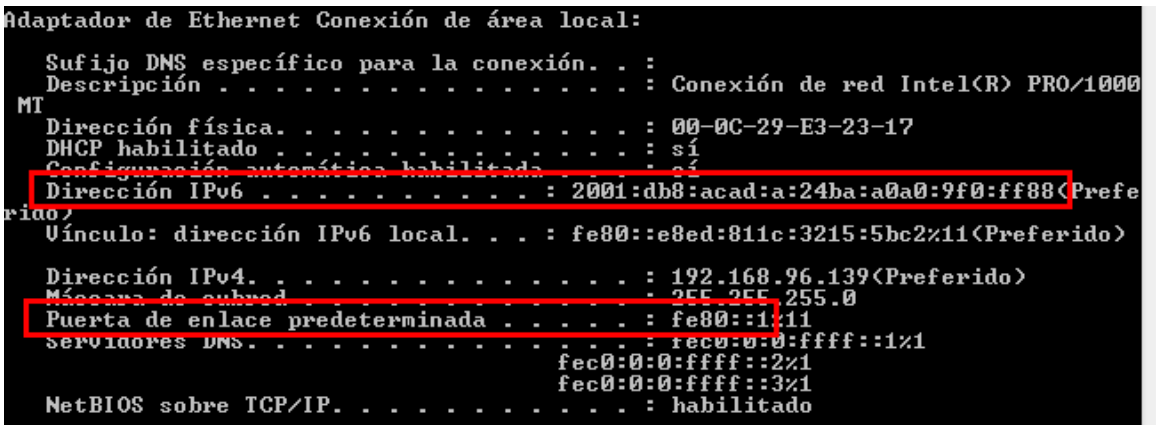
```
S1# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
  No Virtual link-local address(es):
  Stateless address autoconfig enabled
  Global unicast address(es):
    2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64
[EUI/CAL/PRE]
      valid lifetime 2591988 preferred lifetime 604788
  Joined group address(es):
    FF02::1
    FF02::1:FFE8:8A40
  MTU is 1500 bytes
```

```
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
Output features: Check hwidb
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
Default router is FE80::1 on Vlan1
```

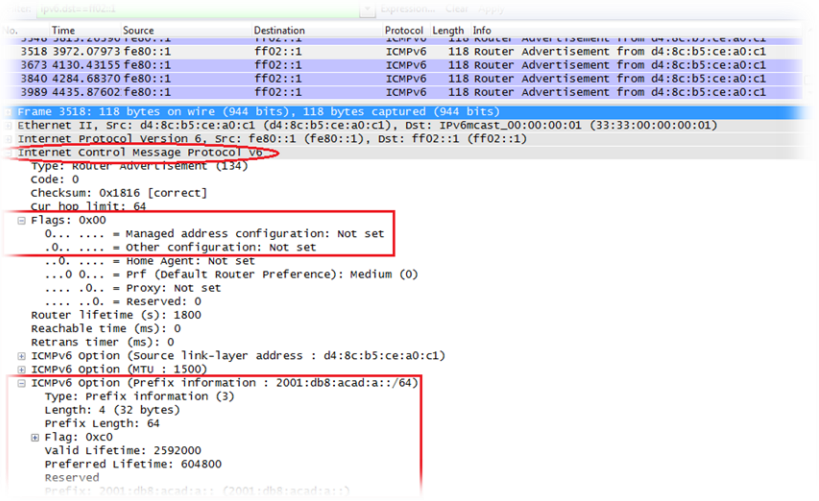


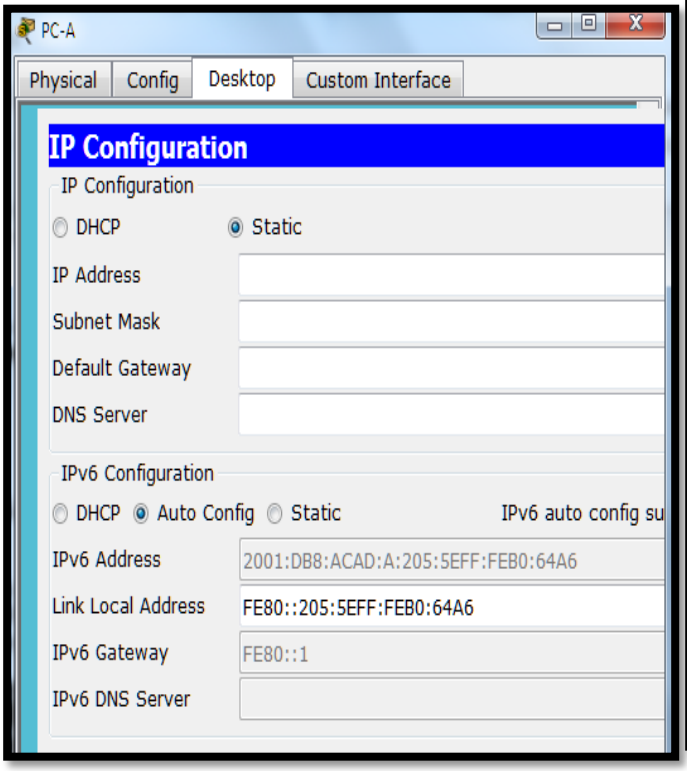
Step 6: verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

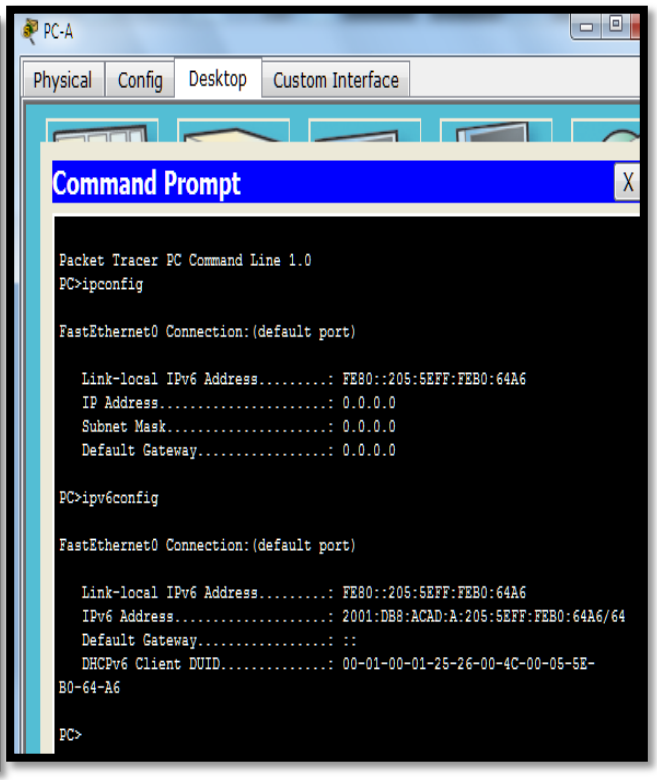
a. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all**. Verifique que la PC-A muestre una dirección IPv6 con el prefijo 2001:db8:acad:a::/64. El gateway predeterminado debe tener la dirección FE80::1.



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.







Part 3: configurar la red para DHCPv6 sin estado

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

a. Cree un pool de DHCP IPv6.

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

b. Asigne un nombre de dominio al pool.

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

c. Asigne una dirección de servidor DNS.

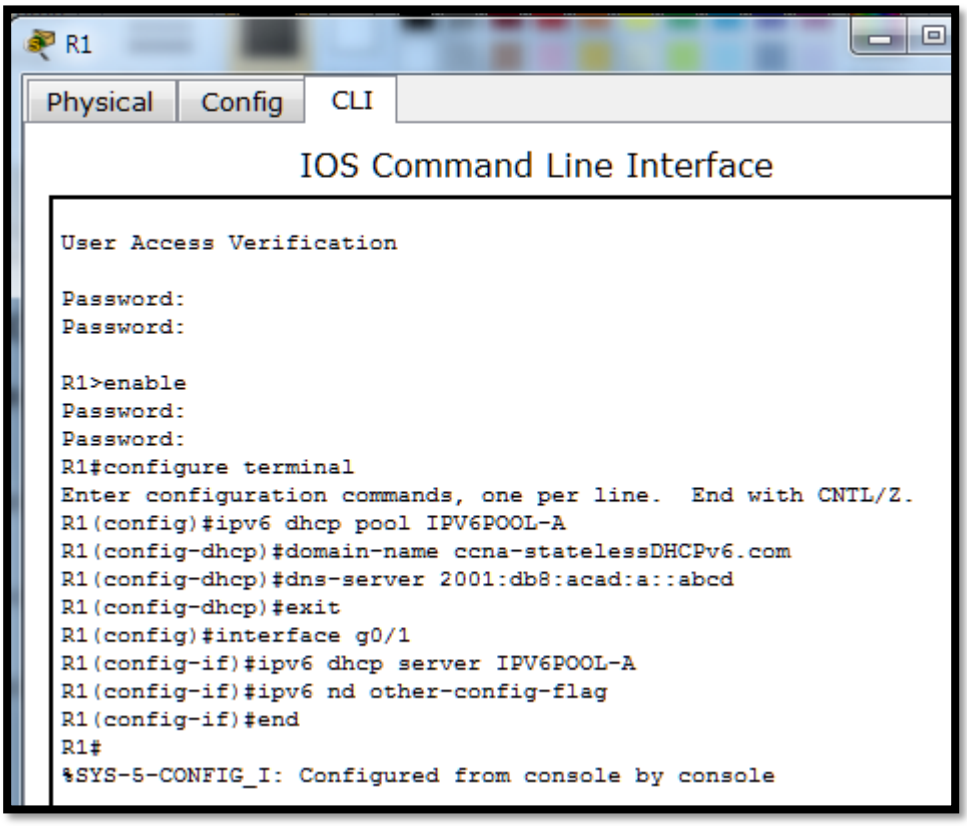
```
R1(config-dhcpv6)# dns-server 2001:db8:acad:a::abcd
R1(config-dhcpv6)# exit
```

d. Asigne el pool de DHCPv6 a la interfaz.

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

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

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

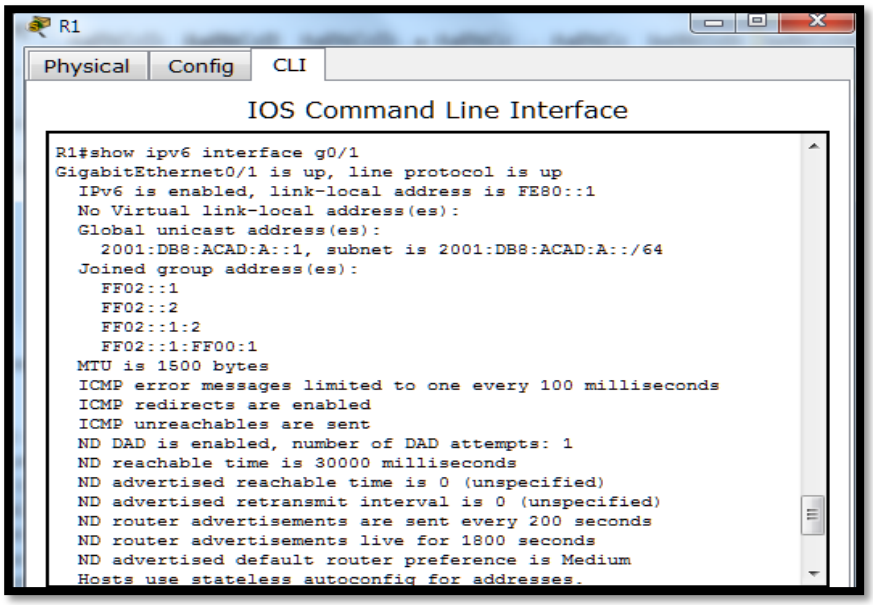


Step 2: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

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 unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

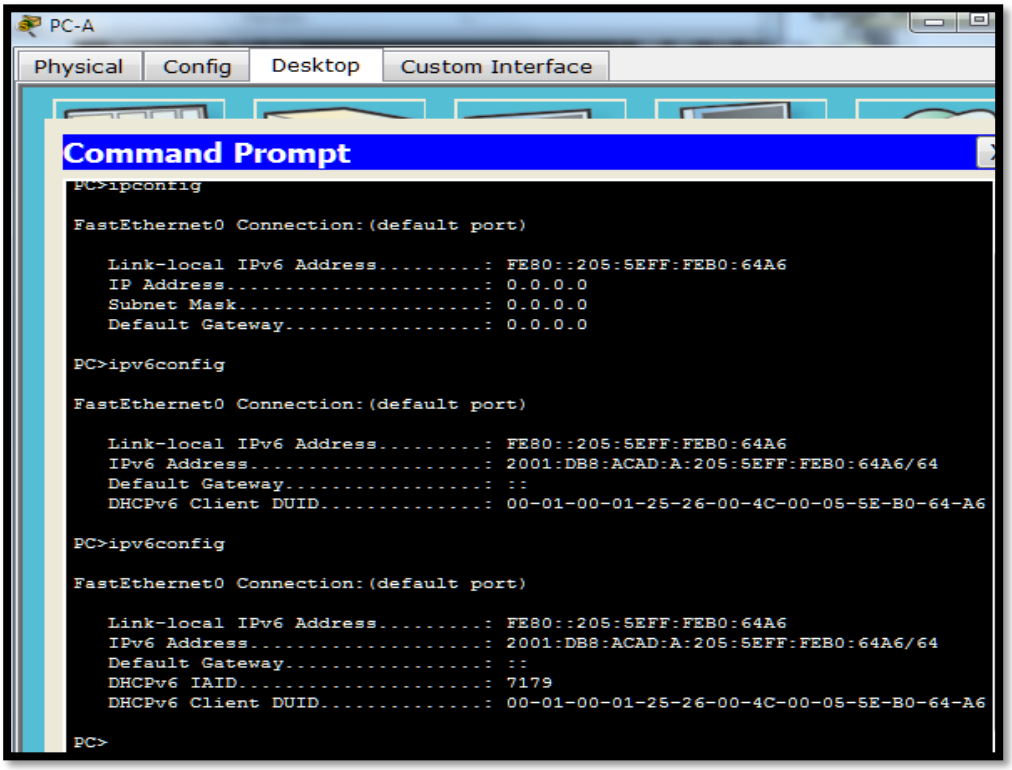
Hosts use DHCP to obtain other configuration.



Step 3: ver los cambios realizados en la red en la PC-A.

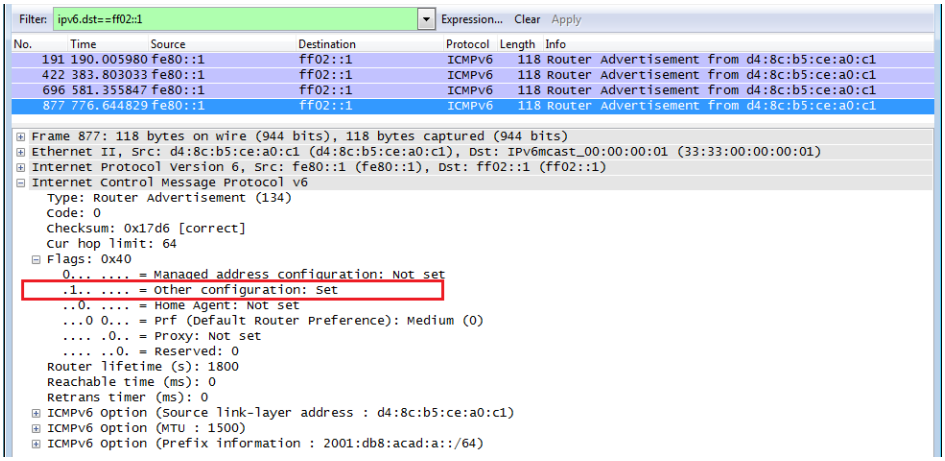
Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente 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
MT
   Dirección física. . . . . . . . . . . . . : 00-0C-29-E3-23-17
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11(Preferido)

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

Adaptador de túnel isatap.localdomain:

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



Step 4: ver los mensajes RA en Wireshark.

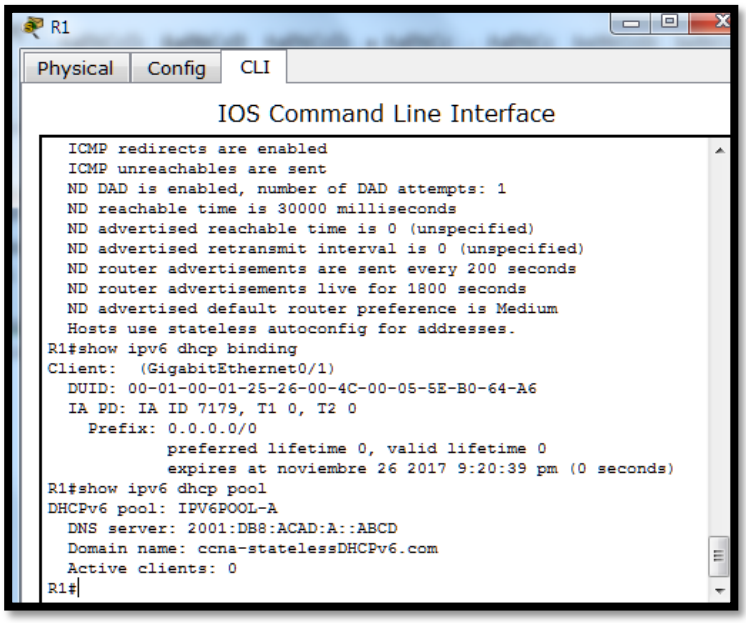
Desplácese hasta el último mensaje RA que se muestra en Wireshark y expándalo para ver la configuración de indicadores ICMPv6. Observe que el indicador Other configuration (Otra configuración) está establecido en 1.



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.

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.

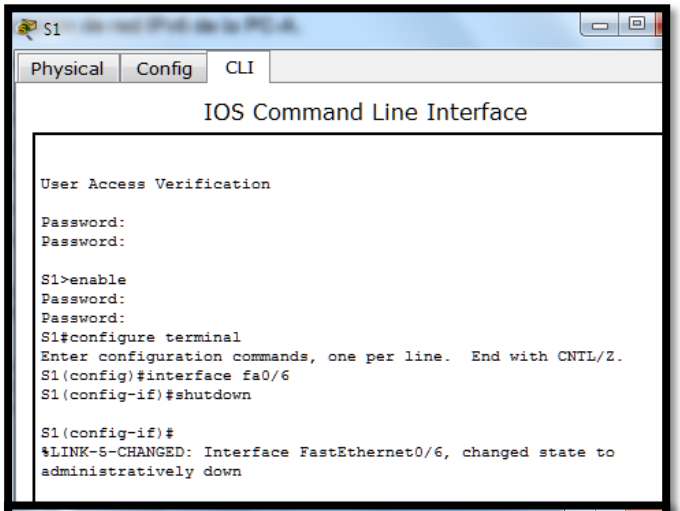
```
S1(config)# interface f0/6
S1(config-if)# shutdown
```

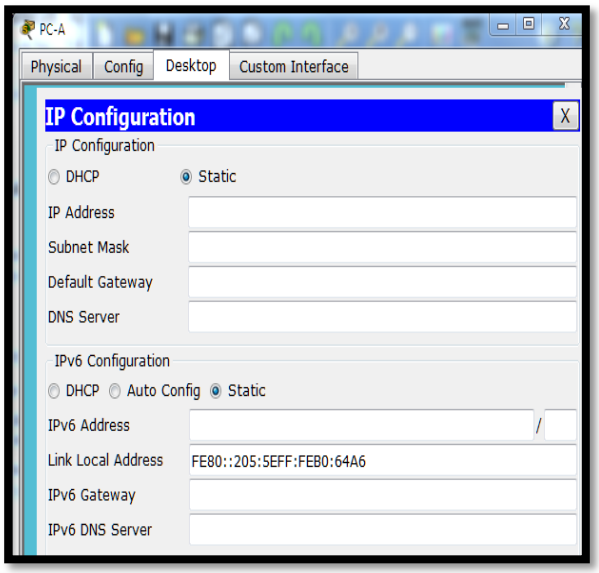
b. Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.

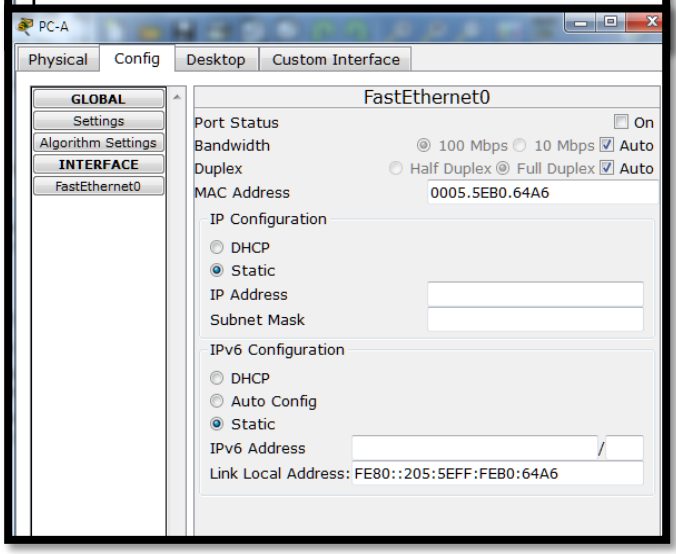
c. Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.

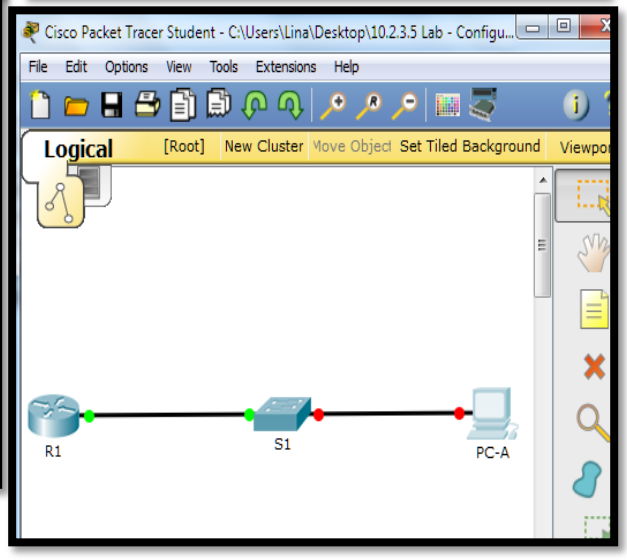
1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.

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 4: configurar la red para DHCPv6 con estado

Step 1: cambiar el pool de DHCPv6 en el R1.

a. Agregue el prefijo de red al pool.

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

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

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

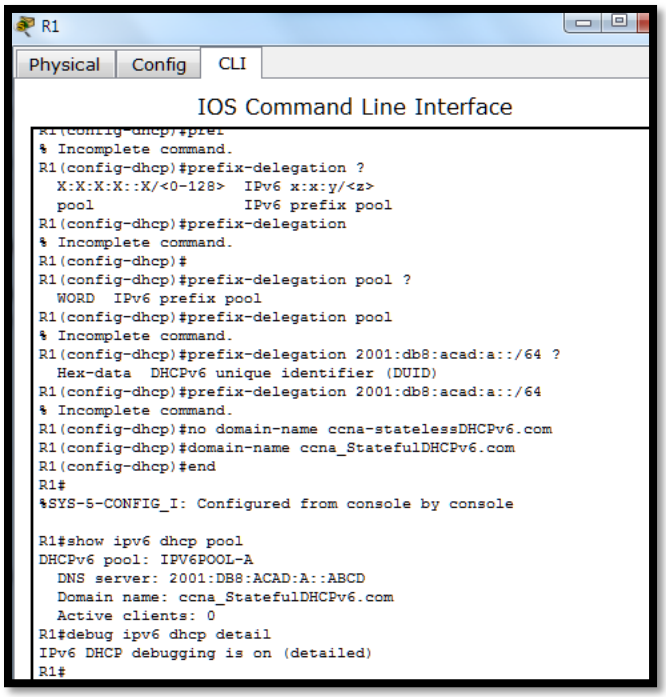
```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)# end
```

c. Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred
86400 (0 in use, 0 conflicts)
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
```

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

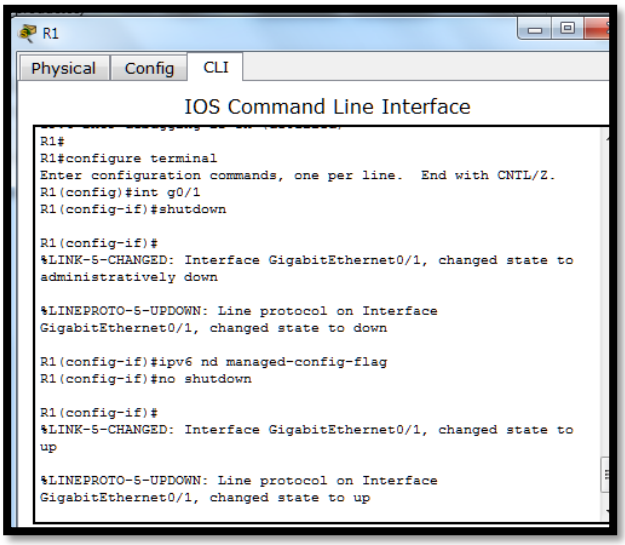
```
R1# debug ipv6 dhcp detail
   IPv6 DHCP debugging is on (detailed)
```



Step 2: 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.

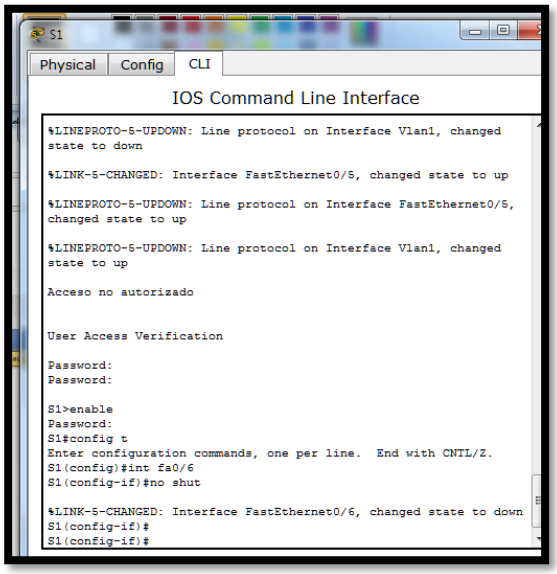
```
R1(config)# interface g0/1
R1(config-if)# shutdown
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# no shutdown
R1(config-if)# end
```



Step 3. 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.

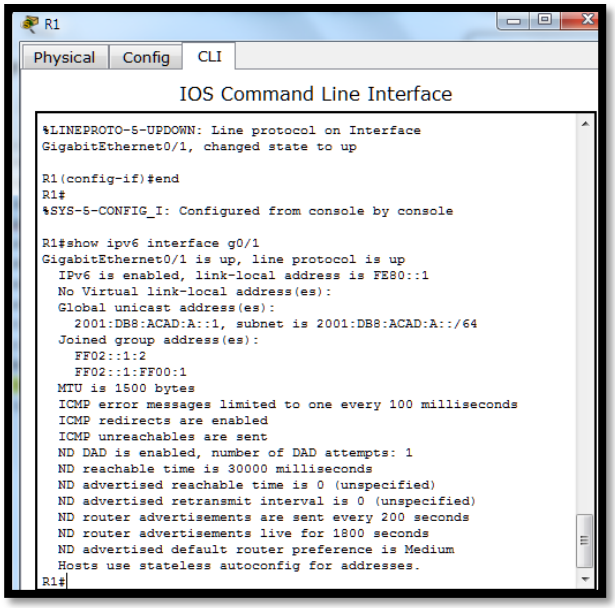
```
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# end
```



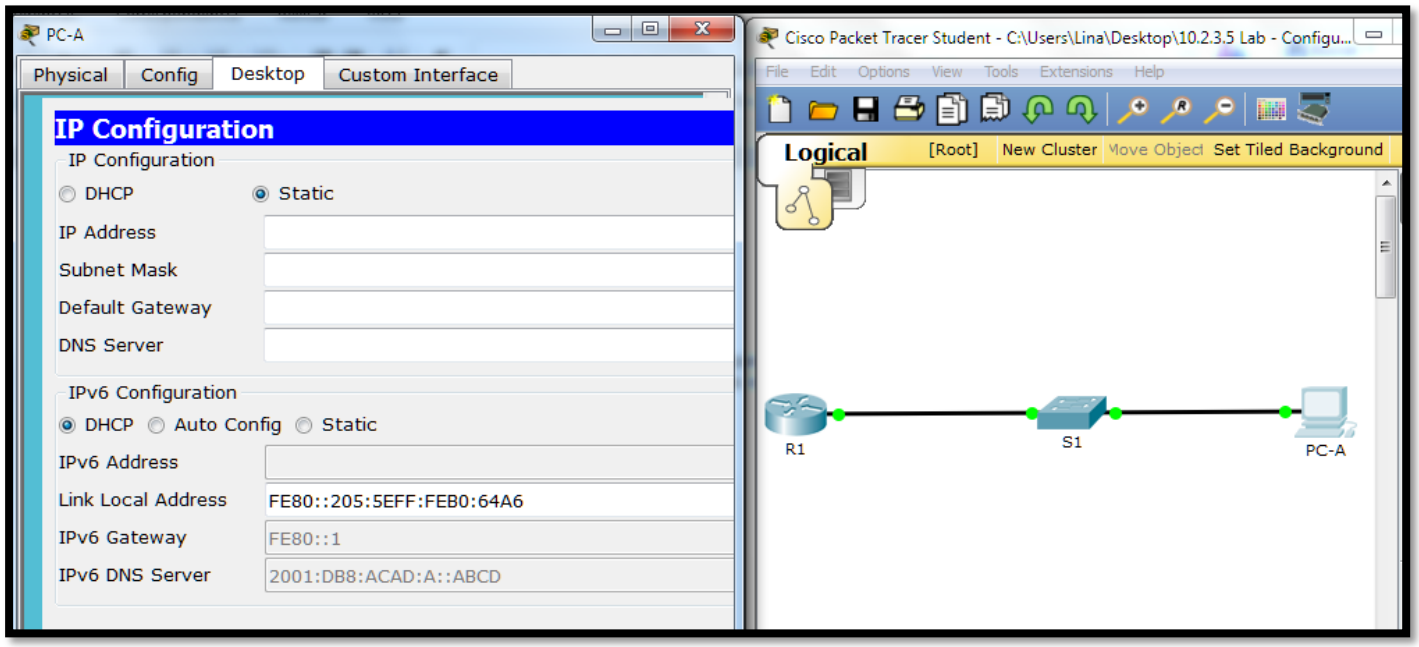
Step 3: verificar la configuración de DHCPv6 con estado en el R1.

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

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



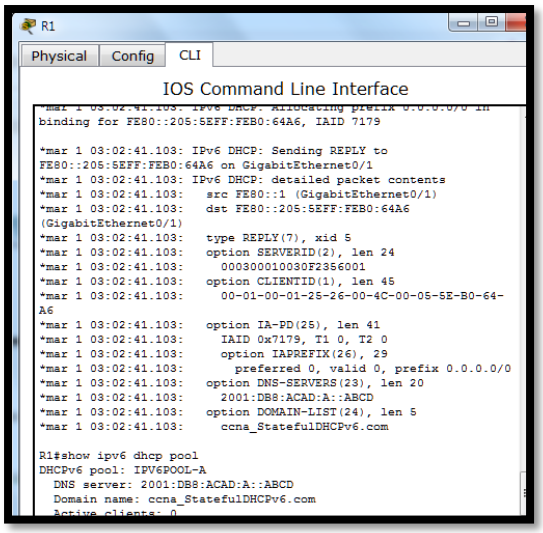
b. En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.



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
```

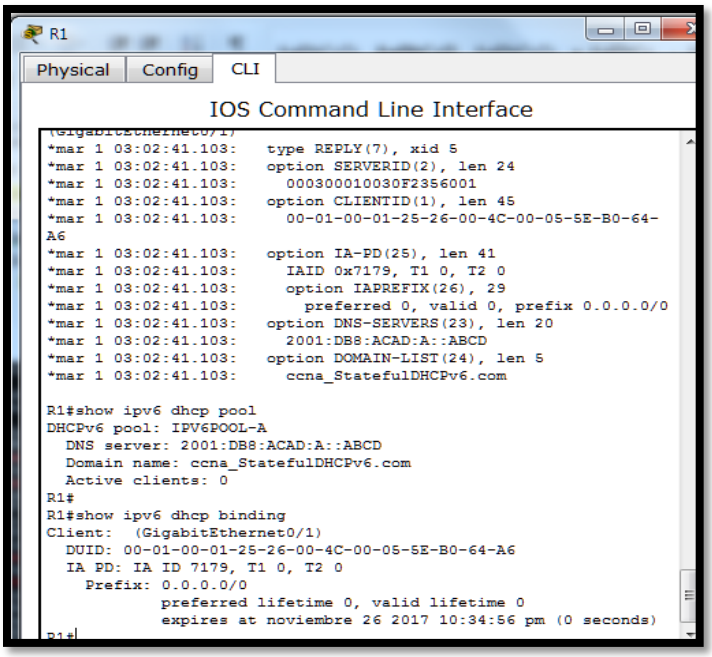
Active clients: 1



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)
```

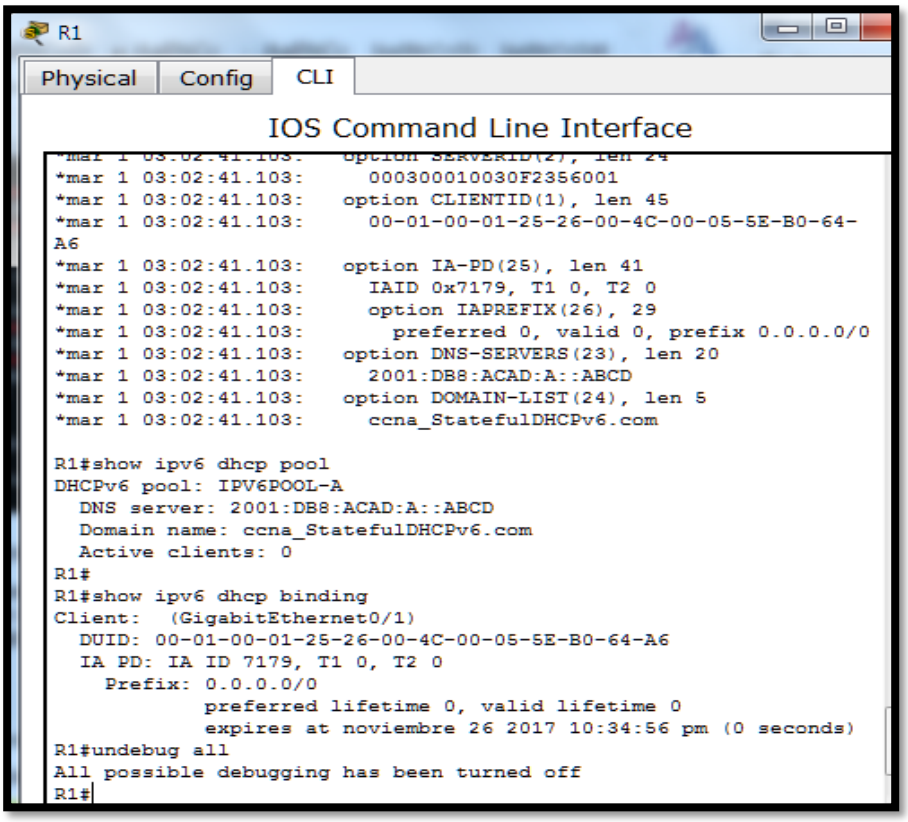
```
Adaptador de Ethernet Conexión de área local:

   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(Pref
erido)
   Concesión obtenida. . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:07:59
   La concesión expira . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:38:03
   Dirección IPv6 . . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a:11(Preferido)

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



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.

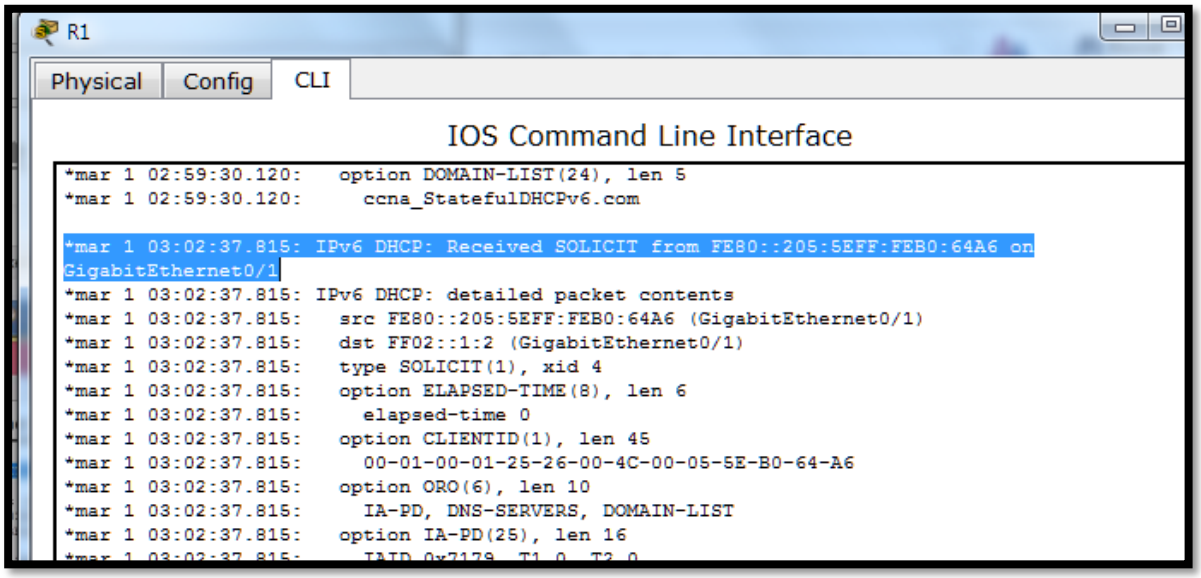
```
R1# u all
Se ha desactivado toda depuración posible
```



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

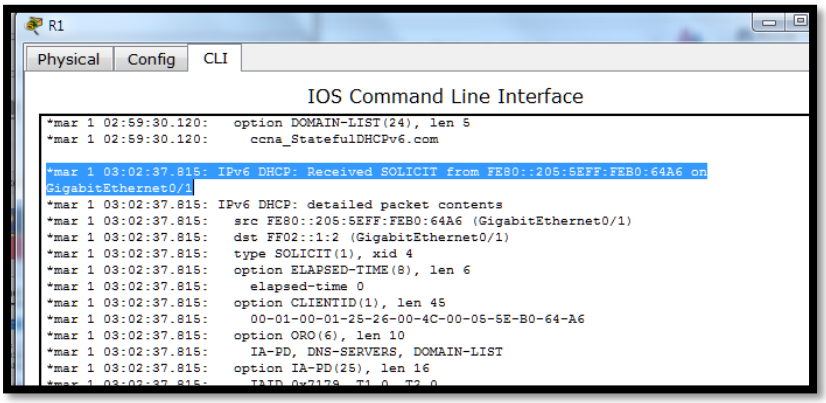
1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

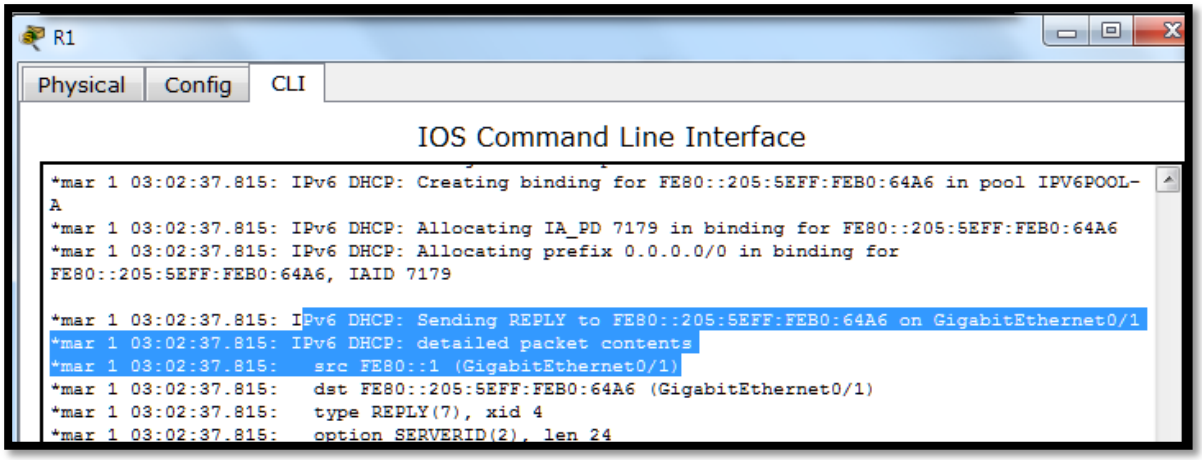
```
*Mar  5 16:42:39.775: IPv6 DHCP: Received SOLICIT from
FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1
*Mar  5 16:42:39.775: IPv6 DHCP: detailed packet contents
*Mar  5 16:42:39.775:   src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar  5 16:42:39.775:   dst FF02::1:2
*Mar  5 16:42:39.775:   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
```

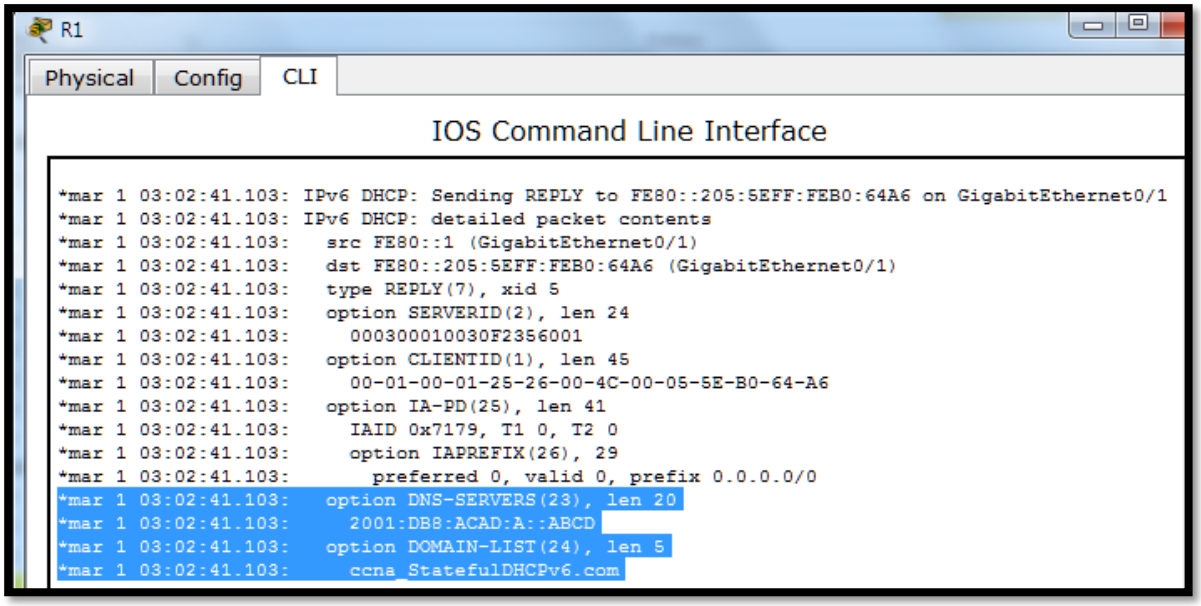


2) Examine el mensaje de respuesta enviado a la PC-A con la información de red DHCP.

```
*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
```


R1
Physical
Config
CLI
IOS Command Line Interface
*mar 1 02:59:30.120: option DOMAIN-LIST(24), len 5
*mar 1 02:59:30.120: ccna_StatefulDHCPv6.com
*mar 1 03:02:37.815: IPv6 DHCP: Received SOLICIT from FE80::205:5EFF:FEB0:64A6 on GigabitEthernet0/1
*mar 1 03:02:37.815: IPv6 DHCP: detailed packet contents
*mar 1 03:02:37.815: src FE80::205:5EFF:FEB0:64A6 (GigabitEthernet0/1)
*mar 1 03:02:37.815: dst FF02::1:2 (GigabitEthernet0/1)
*mar 1 03:02:37.815: type SOLICIT(1), xid 4
*mar 1 03:02:37.815: option ELAPSED-TIME(8), len 6
*mar 1 03:02:37.815: elapsed-time 0
*mar 1 03:02:37.815: option CLIENTID(1), len 45
*mar 1 03:02:37.815: 00-01-00-01-25-26-00-4C-00-05-5E-B0-64-A6
*mar 1 03:02:37.815: option ORO(6), len 10
*mar 1 03:02:37.815: IA-PD, DNS-SERVERS, DOMAIN-LIST
*mar 1 03:02:37.815: option IA-PD(25), len 16

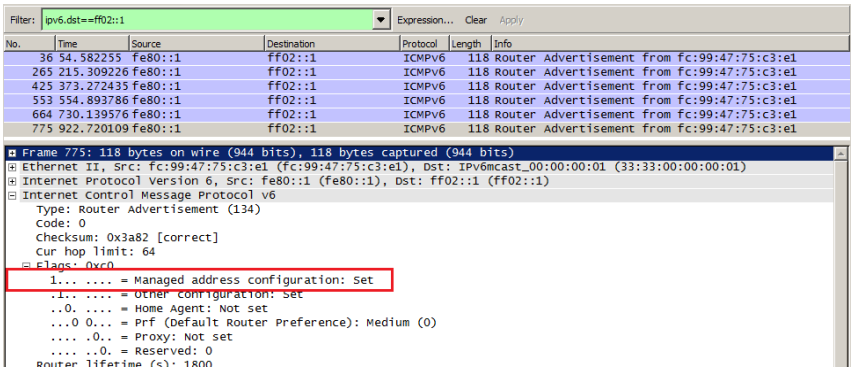

R1
Physical
Config
CLI
IOS Command Line Interface
*mar 1 03:02:37.815: IPv6 DHCP: Creating binding for FE80::205:5EFF:FEB0:64A6 in pool IPV6POOL-A
*mar 1 03:02:37.815: IPv6 DHCP: Allocating IA_PD 7179 in binding for FE80::205:5EFF:FEB0:64A6
*mar 1 03:02:37.815: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for FE80::205:5EFF:FEB0:64A6, IAID 7179
*mar 1 03:02:37.815: IPv6 DHCP: Sending REPLY to FE80::205:5EFF:FEB0:64A6 on GigabitEthernet0/1
*mar 1 03:02:37.815: IPv6 DHCP: detailed packet contents
*mar 1 03:02:37.815: src FE80::1 (GigabitEthernet0/1)
*mar 1 03:02:37.815: dst FE80::205:5EFF:FEB0:64A6 (GigabitEthernet0/1)
*mar 1 03:02:37.815: type REPLY(7), xid 4
*mar 1 03:02:37.815: option SERVERID(2), len 24


R1
Physical
Config
CLI
IOS Command Line Interface
*mar 1 03:02:41.103: IPv6 DHCP: Sending REPLY to FE80::205:5EFF:FEB0:64A6 on GigabitEthernet0/1
*mar 1 03:02:41.103: IPv6 DHCP: detailed packet contents
*mar 1 03:02:41.103: src FE80::1 (GigabitEthernet0/1)
*mar 1 03:02:41.103: dst FE80::205:5EFF:FEB0:64A6 (GigabitEthernet0/1)
*mar 1 03:02:41.103: type REPLY(7), xid 5
*mar 1 03:02:41.103: option SERVERID(2), len 24
*mar 1 03:02:41.103: 0003000100030F2356001
*mar 1 03:02:41.103: option CLIENTID(1), len 45
*mar 1 03:02:41.103: 00-01-00-01-25-26-00-4C-00-05-5E-B0-64-A6
*mar 1 03:02:41.103: option IA-PD(25), len 41
*mar 1 03:02:41.103: IAID 0x7179, T1 0, T2 0
*mar 1 03:02:41.103: option IAPREFIX(26), 29
*mar 1 03:02:41.103: preferred 0, valid 0, prefix 0.0.0.0/0
*mar 1 03:02:41.103: option DNS-SERVERS(23), len 20
*mar 1 03:02:41.103: 2001:DB8:ACAD:A::ABCD
*mar 1 03:02:41.103: option DOMAIN-LIST(24), len 5
*mar 1 03:02:41.103: ccna_StatefulDHCPv6.com

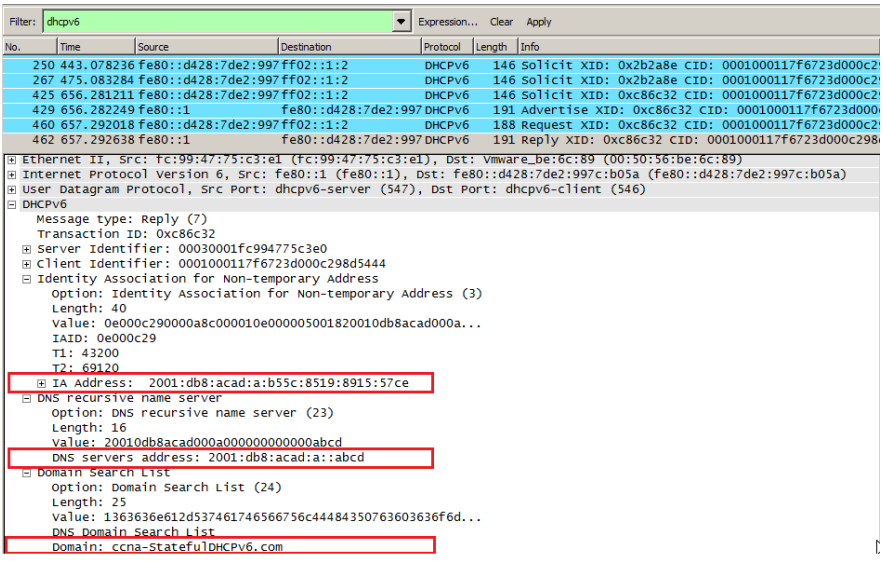
Step 4: verificar DHCPv6 con estado en la PC-A.

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

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



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



Reflexión

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

- El protocolo DHCP permite configurar automáticamente los host de una red TCP/IP durante el arranque de los sistemas. DHCP utiliza un mecanismo de cliente-servidor, a la vez los servidores almacenan y gestionan la información de configuración de los clientes y la suministran cuando éstos la solicitan. Además el DHCPv6 requiere del router para almacenar la información de estado dinámica sobre los clientes DHCPv6, este método de direccionamiento con estado utiliza más recursos de memoria en el router que el método sin estado.

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

- Se recomienda que los dispositivos ipv6 realicen detección de direcciones duplicadas en cualquier dirección, en la configuración automática de direcciones sin estado se utiliza para configurar las direcciones locales de vínculos y las direcciones no locales de vínculos adicionales mediante el intercambio de mensajes de solicitación de enrutador y anuncio de enrutador con los enrutadores vecinos.

Tabla de Interfaces

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.

CONCLUSIONES

- Aprendimos los conceptos de funcionamiento y configuración de Routing dinamico
- Conocimos la función de las listas de control de acceso.
- Aprendimos a configurar el traductor de direcciones NAT en los routers cisco
- Profundizamos en los conceptos de funcionamiento e implementación de DHCPV4 y DHCPV6

BIBLIOGRAFIA

Cisco. (s.f.). *Netacad.com*. Obtenido de https://1314297.netacad.com/courses/548980

Cisco Networking Academy. Introducción a redes conmutadas. Recuperado el 23 de octubre de 2017:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1Cisco

Networking Academy. Configuración y conceptos básicos de Switching. Recuperado el 24 de octubre de 2017:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

Cisco Networking Academy. VLANs. Recuperado el 30 octubre de 2017:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

Cisco Networking Academy. Conceptos de Routing. Recuperado el 30 octubre de 2017:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

Cisco Networking Academy. Enrutamiento entre VLANs. Recuperado el 02 de noviembre de 2017:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

Cisco Networking Academy. Enrutamiento Estático. Recuperado el 02 de noviembre de 2017:

https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1