

Actividad colaborativa cuatro
Enrutamiento en soluciones de red

Lucero Chamorro Serna - Código 29119841

Omar Montaña - Código 16792094

Edward Hernando Guzmán - Código 14704599

María Yojana Daza – Código 31927910

Omar Fabián Castillo - Código 14798114

Curso: Diplomado de Profundización Cisco
Tutor: José Ignacio Cardona
Grupo: 203092_21

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
PROGRAMA INGENIERÍA DE SISTEMAS
CEAD PALMIRA
NOVIEMBRE, 2017

INTRODUCCIÓN

El presente documento tiene como propósito el desarrollo de la Actividad Colaborativa cuatro del diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN), aplicando las temáticas y los conceptos vistos en el material bibliográfico de la unidad cuatro: Enrutamiento en Soluciones de Red: Enrutamiento Dinámico, OSPF de una sola área, Listas de control de acceso, DHCP y Traducción de direcciones IP para IPv4, de acuerdo a lo indicado en la guía de actividades entregada por la UNAD a través del entorno de colaborativo del diplomado.

Las competencias a desarrollar con la realización de la presente actividad, son: Identificar y solucionar problemas propios de enrutamiento mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces.

El documento contiene el desarrollo de las tareas (prácticas de laboratorio) que en total son catorce (14) ejercicios indicados en la guía, correspondientes a las temáticas que forman parte de la Unidad 4 y los cuales son resueltos mediante el uso de la herramienta de Simulación PACKET TRACER.

Para su elaboración, se tomó en cuenta el material sugerido por la UNAD en la guía de actividades, en el entorno de aprendizaje práctico y en el entorno de conocimiento del curso, así como lo indicado por los tutores en las web conferencias y el contenido temático inmerso en el curso de CCNA 2 de CISCO.

OBJETIVOS

Objetivo general

Desarrollar las actividades correspondientes al trabajo colaborativo cuatro del diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN), con el fin de comprender y aplicar los conceptos fundamentales relacionados con el Enrutamiento en Soluciones de Red.

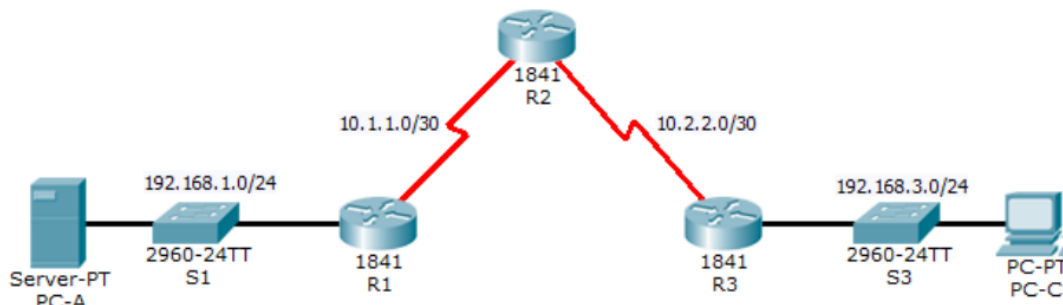
Objetivos específicos

1. Resolver todas las tareas (prácticas de laboratorio) que conforman los catorce (14) ejercicios indicados en la guía de la actividad.
2. Aplicar los conocimientos adquiridos en la unidad cuatro del diplomado, para el desarrollo de cada uno de los ejercicios planteados.
3. Realizar los ejercicios haciendo uso de la herramienta de Simulación PACKET TRACER.

DESARROLLO DE LA ACTIVIDAD

Packet tracer 4.4.1.2 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

Antecedentes / escenario

El acceso a los enrutadores R1, R2 y R3 solo debe permitirse desde PC-C, la estación de administración. PC-C también se utiliza para realizar pruebas de conectividad a PC-A, un servidor que proporciona servicios DNS, SMTP, FTP y HTTPS.

El procedimiento operativo estándar es aplicar ACL en los enrutadores de borde para mitigar las amenazas comunes en función de la dirección IP de origen y / o de destino. En esta actividad, crea ACL en los enrutadores de borde R1 y R3 para lograr este objetivo. A continuación, verifica la funcionalidad de ACL de los hosts internos y externos.

Los enrutadores se han pre configurado con lo siguiente:

Habilitar contraseña: ciscoenpa55

Contraseña para la consola: ciscoconpa55

Nombre de usuario para líneas VTY: SSHadmin

Contraseña para líneas VTY: ciscosshpa55

direccionamiento IP

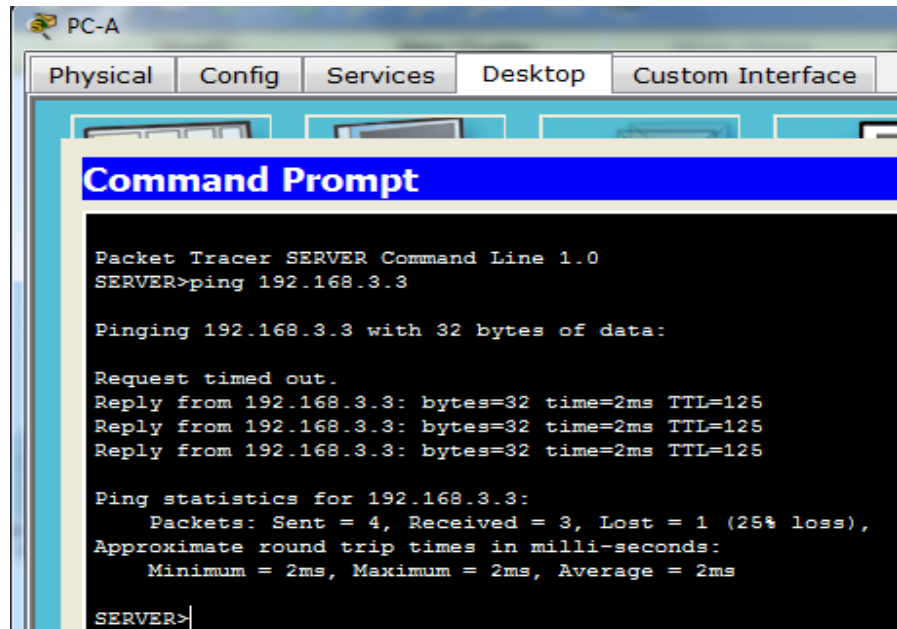
Enrutamiento estático

Parte 1: verificar la conectividad de red básica

Verifique la conectividad de la red antes de configurar las ACL de IP.

Paso 1: desde la PC-A, verifique la conectividad con PC-C y R2.

a. Desde el símbolo del sistema, haga ping a PC-C (192.168.3.3).



```
PC-A
Physical Config Services Desktop Custom Interface
Command Prompt
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

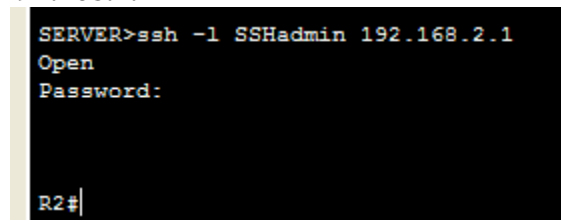
Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

SERVER>
```

b. Desde el símbolo del sistema, establezca una sesión SSH a la interfaz R2 Lo0 (192.168.2.1) utilizando un nombre de usuario Administrador SSH y contraseña **cisco** shpa55. Cuando termine, salga de la sesión SSH.

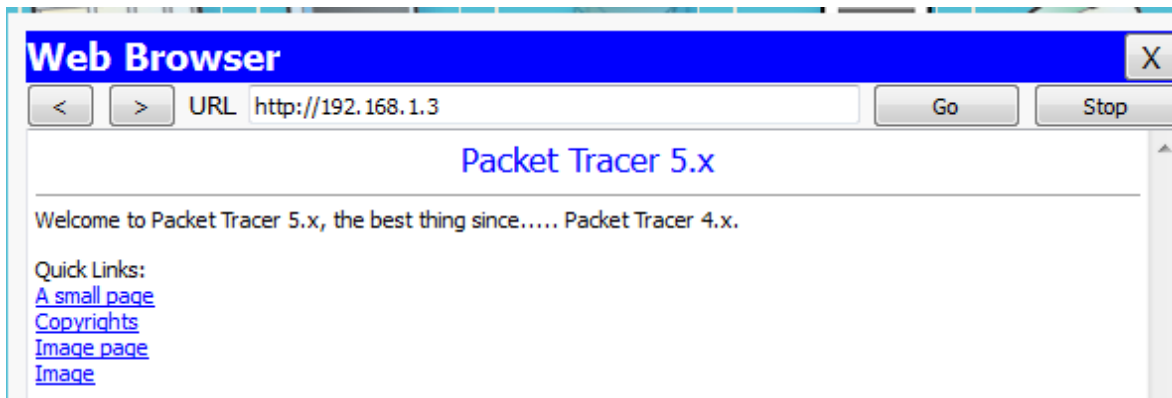
PC> **ssh -l SSHadmin 192.168.2.1**



```
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#
```

c. Abra un navegador web en el servidor PC-A (192.168.1.3) para visualizar la página web. Cierre el navegador cuando termine.



Parte 2: Acceso seguro a enrutadores

Paso 1: Configure la ACL 10 para bloquear todo el acceso remoto a los enrutadores, excepto desde PC-C.

Use el comando access-list para crear una IP ACL numerada en R1, R2 y R3.

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

```
User Access Verification
|
Password:

R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#
```

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

```
User Access Verification

Password:
Password:

R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#
```

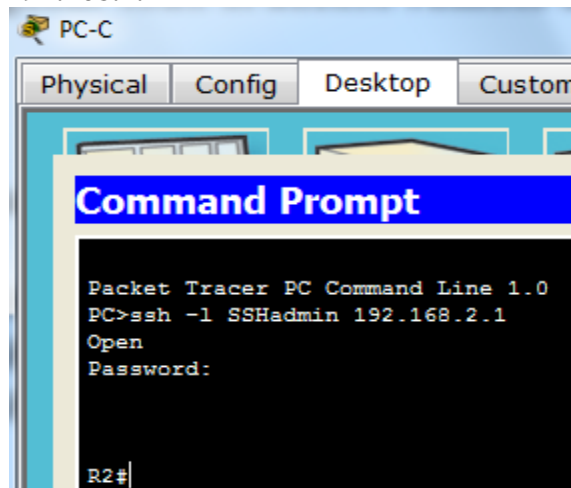
R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0

```
Password:  
R3>en  
Password:  
R3#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0  
R3(config)#line vty 0 4  
R3(config-line)#access-class 10 in  
R3(config-line)#
```

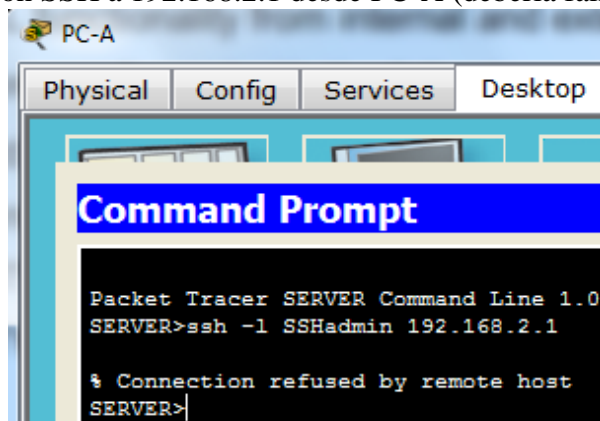
Paso 3: Verifique el acceso exclusivo desde la estación de administración PC-C.

a. Establezca una sesión SSH en 192.168.2.1 desde PC-C (debería tener éxito).

PC> ssh -l SSHAdmin 192.168.2.1



b. Establezca una sesión SSH a 192.168.2.1 desde PC-A (debería fallar)

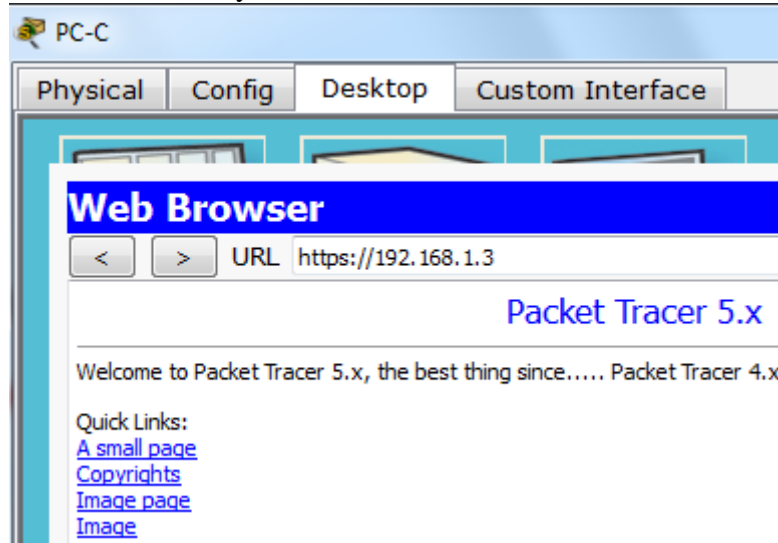


Parte 3: Cree una ACL IP numerada 120 en R1

Permita que cualquier servidor externo acceda a los servicios DNS, SMTP y FTP en el servidor PC-A, niegue cualquier acceso de host externo a los servicios HTTPS en PC-A y permita que PC-C tenga acceso a R1 a través de SSH.

Paso 1: Verifique que PC-C pueda acceder a la PC-A a través de HTTPS usando el navegador web.

Asegúrese de deshabilitar HTTP y habilitar HTTPS en el servidor PC-A



Paso 2: configure la ACL 120 para permitir y denegar específicamente el tráfico especificado. Use el comando access-list para crear una ACL IP numerada.

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

Paso 3: aplique la ACL a la interfaz S0/0/0

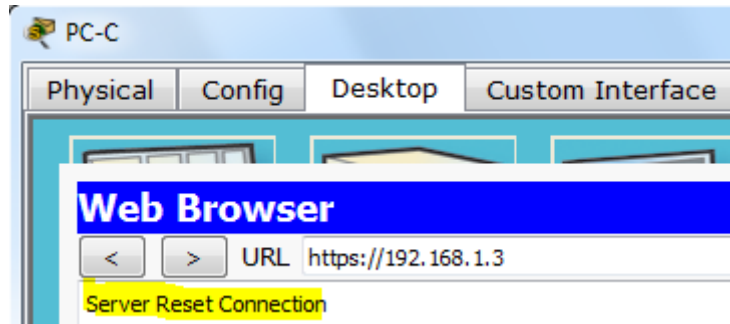
Utilice el comando **ip access-group** para aplicar la lista de acceso al tráfico entrante en la **interfaz S0/0/0**

```
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)#exit
R1 (config)#
```


Paso 4: Verifique que PC-C no pueda acceder a PC-A a través de HTTPS utilizando el navegador web.



Parte 4: Modificar una ACL existente en R1

Permitir respuestas de eco ICMP y mensajes inalcanzables de destino desde la red externa (en relación con R1); denegar todos los demás paquetes ICMP entrantes.

Paso 1: Verifique que la PC-A no pueda hacer ping exitosamente en la interfaz loopback en R2.

```
SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

SERVER>
```

Paso 2: Realice los cambios necesarios en la ACL 120 para permitir y denegar el tráfico especificado.

Use el comando access-list para crear una ACL IP numerada.

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

Paso 3: Verifique que PC-A pueda hacer ping con éxito en la interfaz loopback en R2.

```

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

SERVER>

```

Parte 5: Crear una ACL IP numerada 110 en R3

Denegar todos los paquetes salientes con la dirección de origen fuera del rango de direcciones IP internas en R3.

Paso 1: Configure la ACL 110 para permitir solo el tráfico desde la red interna. Use el comando access-list para crear una ACL IP numerada.

```

User Access Verification

Password:

R3>en
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#

```

Paso 2: aplique la ACL a la interfaz F0 / 1

Use el comando ip access-group para aplicar la lista de acceso al tráfico entrante en la interfaz F0 / 1.

```

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

```

Parte 6: Crear una ACL 100 de IP numerada en R3

En R3, bloquee todos los paquetes que contengan la dirección IP de origen del siguiente grupo de direcciones: 127.0.0.0/8, cualquier dirección privada RFC 1918 y cualquier dirección de multidifusión IP.

Paso 1: configure la ACL 100 para bloquear todo el tráfico especificado de la red externa. También debe bloquear el tráfico proveniente de su propio espacio de direcciones internas si no es una dirección RFC 1918 (en esta actividad, su espacio de direcciones internas es parte del espacio de direcciones privadas especificado en RFC 1918).

Use el comando access-list para crear una ACL IP numerada

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
```

```
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)#
```

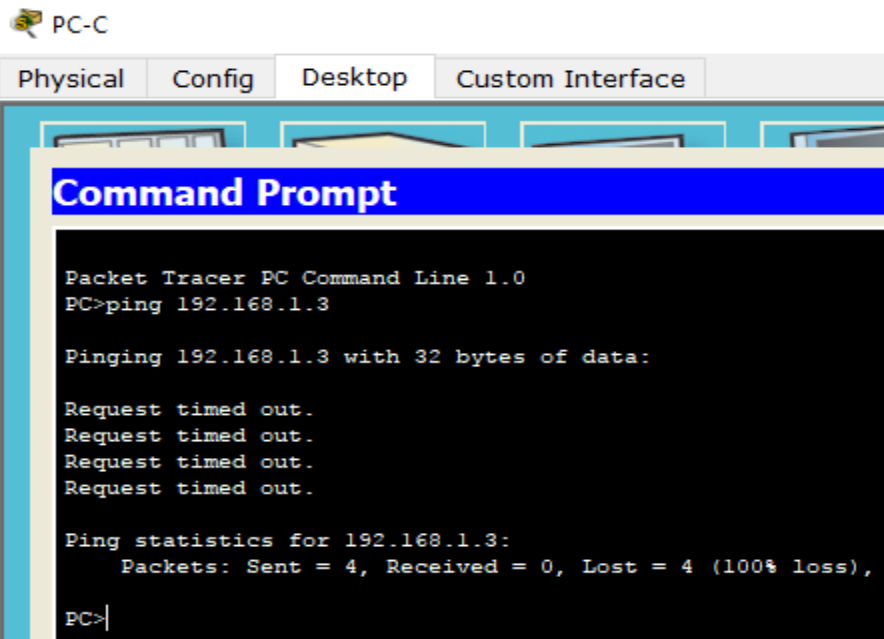
Paso 2: aplique la ACL a la interfaz Serial 0/0/1.

Use el comando ip access-group para aplicar la lista de acceso al tráfico entrante en la interfaz Serial 0/0/1.

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

Paso 3: Confirme que la interfaz de entrada de tráfico especificada Serial 0/0/1 se elimine

Desde el indicador de comando de PC-C, haga ping al servidor PC-A. Las respuestas de eco ICMP están bloqueadas por la ACL ya que se obtienen del espacio de direcciones 192.168.0.0/16



The screenshot shows the Packet Tracer PC Command Line interface for PC-C. The window has tabs for Physical, Config, Desktop, and Custom Interface. The Command Prompt window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Paso 4: verifica los resultados

Su porcentaje de finalización debe ser del 100%. Haga clic en Comprobar resultados para ver los comentarios y la verificación de cuáles componentes requeridos se han completado.

Cisco Packet Tracer Student - C:\Users\Omar\Google Drive\UNAD\DIPLOMADO\COLABORATIVO 4\Aporte1_Omar MON... — □ ×

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 02:00:10

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component
Network			
R1			
ACL			
10	Correct	1	ACL
120	Correct	1	ACL
Ports			
Serial0/0/0		0	Other
Access-group ...	Correct	1	Other
VTY Lines			
VTY Line 0		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 1		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 2		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 3		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 4		0	Physical
Access Contro...	Correct	1	ACL
R2			
ACL		0	ACL
10	Correct	1	ACL
VTY Lines			
VTY Line 0		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 1		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 2		0	Physical

Score : 23/23

Item Count : 23/23

Component	Items/Total	Score
ACL	23/23	23/23

Cisco Packet Tracer Student - C:\Users\Omar\Google Drive\UNAD\DIPLOMADO\COLABORATIVO 4\Aporte1_Omar MON... — □ ×

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 02:02:12

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component
R3			
Access Contro...	Correct	1	ACL
VTY Line 1		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 2		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 3		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 4		0	Physical
Access Contro...	Correct	1	ACL
R3			
ACL			
10	Correct	1	ACL
100	Correct	1	ACL
110	Correct	1	ACL
Ports			
FastEthernet0/1		0	Other
Access-group ...	Correct	1	ACL
VTY Lines			
VTY Line 0		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 1		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 2		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 3		0	Physical
Access Contro...	Correct	1	ACL
VTY Line 4		0	Physical
Access Contro...	Correct	1	ACL

Score : 23/23

Item Count : 23/23

Component	Items/Total	Score
ACL	23/23	23/23

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

Topología

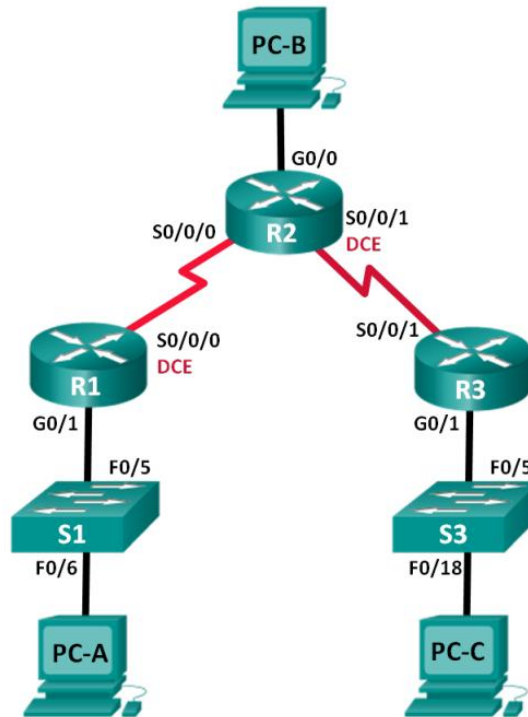


Tabla de direccionamiento

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

Información básica/situación

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

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

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

Recursos necesarios

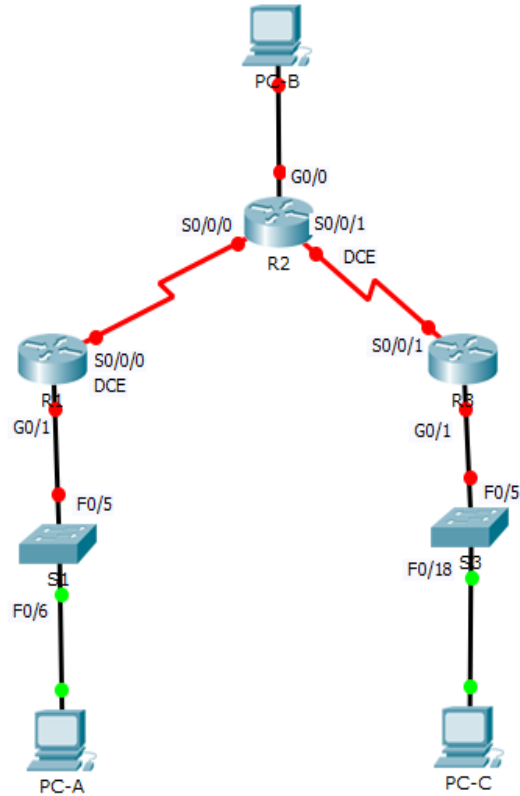
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

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

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

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

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



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

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

Configuración R1

```

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#service password-encryption
R1(config)#enable password class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd "Se Prohbe el Acceso No Autorizado"
R1(config)#int g0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#no shutdown

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

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

R1(config-if)#

```

```

R1(config)#int s0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#clock rate 128000
R1(config-if)#no shut

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

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

```

Configuración R2


```
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)#service password-encryption
R2(config)#enable password class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#banner motd "Se Prohibe el Acceso No Autorizado"
R2(config)#int g0/0
R2(config-if)#ip address 209.165.201.1 255.255.255.0
R2(config-if)#no shutdown

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

```
R2(config-if)#int s0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown

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

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

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut|
R2(config-if)#int s0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shut

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

Configuración R3

```
R3(config)#int s0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial10/0/1, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/1, changed state to up

R3(config-if)#
```

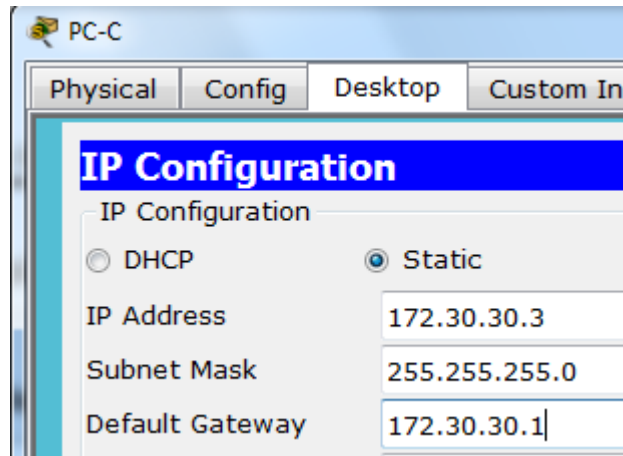
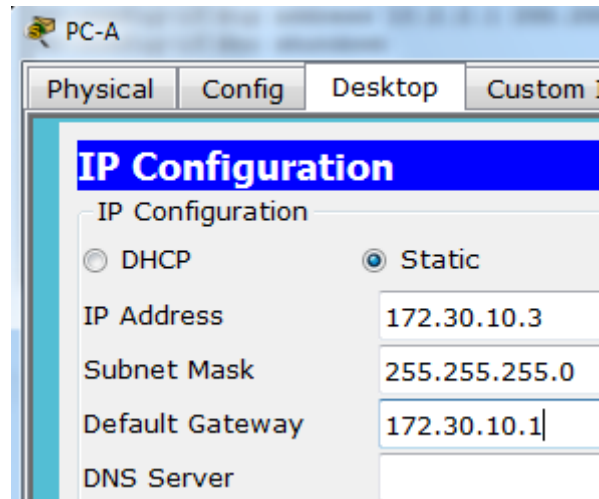
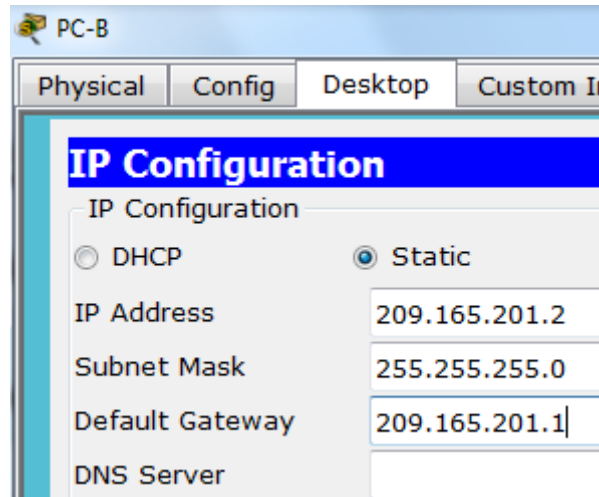
```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#service password-encryption
R3(config)#enable password class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#banner motd "Se Prohibe el Acceso No Autorizado"
R3(config)#int g0/1
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#no shutdown

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

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

R3(config-if)#
```

Paso 4. Configurar los equipos host.

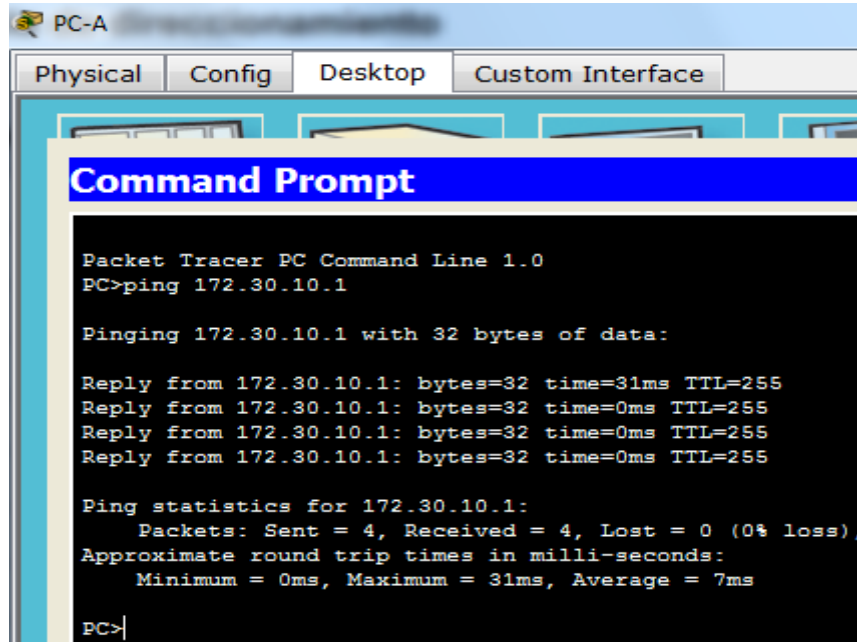


Paso 5. Probar la conectividad.

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.

Ping del PC-A al R1



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.30.10.1

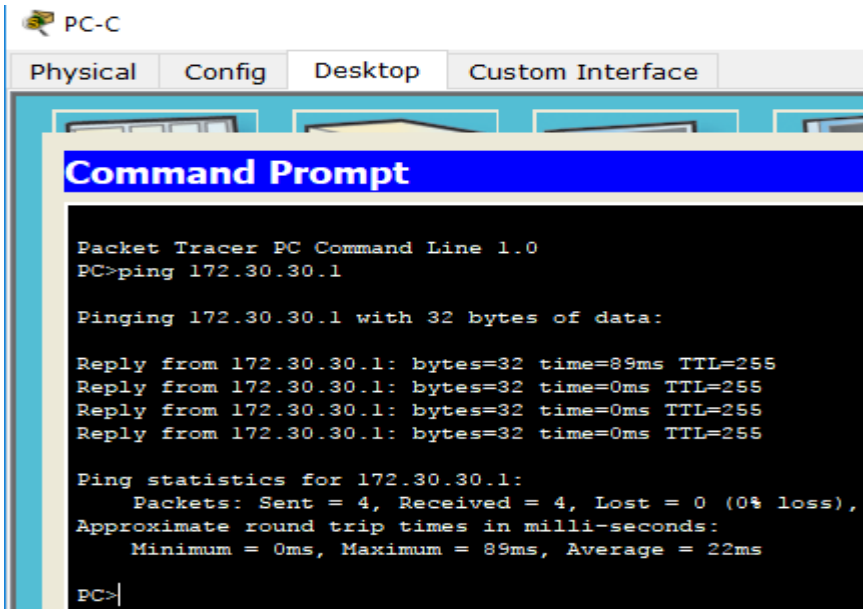
Pinging 172.30.10.1 with 32 bytes of data:

Reply from 172.30.10.1: bytes=32 time=31ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms 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 = 31ms, Average = 7ms

PC>
```

Ping del PC-C al R3



```
PC-C
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

Reply from 172.30.30.1: bytes=32 time=89ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms 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 = 89ms, Average = 22ms

PC>
```

Ping del PC-B al R2

The screenshot shows a Packet Tracer PC Command Line window for PC-B. The window has tabs for Physical, Config, Desktop, and Custom Interface. The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms 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 = 0ms, Average = 0ms

PC>|
```

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#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)#
```

m. 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#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)#

```

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

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2

```

Paso 6. 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.

show ip interface brief

```

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
Serial10/0/0             10.1.1.2        YES manual up      up
Serial10/0/1             10.2.2.2        YES manual up      up
Vlan1                    unassigned      YES unset  administratively down down
R2#

```

R2#

o. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? **NO** ¿Por qué? **El R2 no anuncia la ruta a la PC-B**

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.

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

PC>
```

¿Es posible hacer ping de la PC-A a la PC-C? **NO** ¿Por qué? **El R1 y el R3 no tienen rutas a las subredes específicas en el router remoto**

```
PC>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.

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

PC>
```

¿Es posible hacer ping de la PC-C a la PC-B? **NO** ¿Por qué? **El R2 no anuncia la ruta a la PC-C**

```
PC-C
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

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

PC>
```

¿Es posible hacer ping de la PC-C a la PC-A? **NO** ¿Por qué? **El R1 y el R3 no tienen rutas a las subredes específicas en el router remoto**

```
PC>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

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

PC>
```

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.

Verificación de ejecución del RIP en el R1


```

R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 26 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0        2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway            Distance      Last Update
  10.1.1.2           120          00:00:09
Distance: (default is 120)
R1#

```

Verificación de ejecución del RIP en el R2

```

R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 27 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0        2     2
  Serial0/0/1        2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway            Distance      Last Update
  10.2.2.1           120          00:00:09
  10.1.1.1           120          00:00:24
Distance: (default is 120)
R2#

```

Verificación de ejecución del RIP en el R3

```

R3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/1        2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway            Distance      Last Update
  10.2.2.2           120           00:00:10
Distance: (default is 120)
R3#

```

Al emitir el comando **debug ip rip** en el R2, ¿qué información se proporciona que confirma que RIPv2 está en ejecución? R/sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)

```

R2#debug ip rip
RIP protocol debugging is on
R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
  10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
  10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
R2#

```

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

```

R2#undebug all
All possible debugging has been turned off
R2#

```

Al emitir el comando **show run** en el R3, ¿qué información se proporciona que confirma que RIPv2 está en ejecución? R/ **router rip version 2**

```

router rip
version 2
passive-interface GigabitEthernet0/1
network 10.0.0.0
network 172.30.0.0
!
ip classless
R3#

```

d. Examinar el sumarización automática de las rutas.

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

```

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:19, Serial0/0/1
                   [120/1] via 10.1.1.1, 00:00:04, Serial0/0/0
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
R2#

```

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

```

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C       10.1.1.0/24 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:05, Serial0/0/0
       172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
R1#

```

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

```

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:19, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
       172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1
R3#

```

Utilice el comando **debug ip rip** en el **R2** para determinar las rutas recibidas en las actualizaciones RIP del **R3** e indíquelas a continuación. **R/172.30.0.0/16**

```

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

```

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 7. 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
```

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

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

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

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

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

R1# clear ip route *
R1#
```

s. 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
```

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

Gateway of last resort is not set

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

```
R1# show ip route
```

```

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

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
R1#

```

R3# show ip route

```

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

Gateway of last resort is not set

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

```

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

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

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

172.30.30.0/24

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

Paso 8. 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

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

u. 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
```

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

Paso 9. Verificar la configuración de enrutamiento.

v. Consulte la tabla de routing en el R1.

```
R1# show ip route
```

<Output Omitted>

```
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

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/24 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
 172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R1#
```

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

R/ Hay un Gateway de último recurso, y la ruta predeterminada aparece en la tabla como detectada a través de RIP

w. Consulte la tabla de routing en el R2.

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

R/ El R2 tiene una ruta estática predeterminada a 0,0,0,0 a través de 209.165.201.2 que está conectada directamente a G0/0

Paso 10. Verifique la conectividad.

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

¿Tuvieron éxito los pings? **R/ SI**

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

¿Tuvieron éxito los pings? R/ SI

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.

PC-A

IPv6 Configuration

DHCP
 Auto Config
 Static

IPv6 Address: /

Link Local Address:

IPv6 Gateway:

IPv6 DNS Server:

PC-B

IPv6 Configuration	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	2001:DB8:ACAD:B::B / 64
Link Local Address	FE80::2D0:97FF:FEB3:B12A
IPv6 Gateway	FE80::2
IPv6 DNS Server	

PC-C

IPv6 Configuration	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	2001:DB8:ACAD:C::C / 64
Link Local Address	FE80::260:47FF:FE32:97C9
IPv6 Gateway	FE80::3
IPv6 DNS Server	

Paso 11. Configurar IPv6 en los routers.

- Para cada interfaz del router, asigne la dirección global y la dirección link local de la tabla de direccionamiento.
- Habilite el routing IPv6 en cada router.

Configuración IPv6 R1

```
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)#
```

Configuración IPv6 R2

```

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)#

```

Configuración IPv6 R3

```

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

```

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

R/ show ipv6 interface brief

Verificación de IPv6 en R1

```

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#

```

Verificación de IPv6 en R2

```

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#

```

Verificación de IPv6 en R3

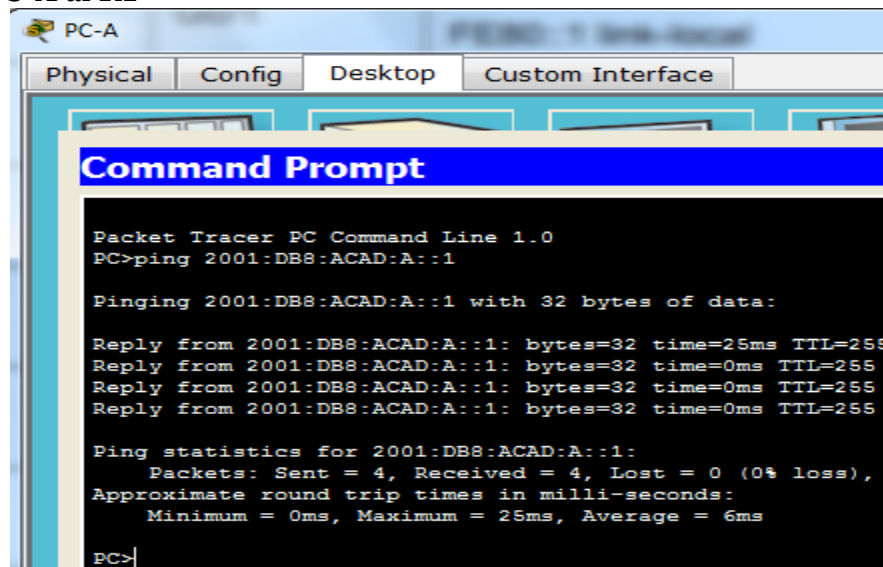
```

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#

```

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

Ping del PC-A al R1



Ping del PC-B al R2

```
PC-B
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:ACAD:B::2

Pinging 2001:DB8:ACAD:B::2 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::2: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time=0ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Ping del PC-C al R3

```
PC-C
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:ACAD:C::3

Pinging 2001:DB8:ACAD:C::3 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::3: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

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#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)#
```

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

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

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

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

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

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

```
R2#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test2"
  Interfaces:
    Serial0/0/0
    Serial0/0/1|
  Redistribution:
    None
R2#
```

```
R3#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test3"
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/1
  Redistribution:
    None
R3#
```

¿En qué forma se indica RIPng en el resultado?

R/ **El RIPng se indica por el nombre de los procesos**

ff. Emita el comando show ipv6 rip Test1.

R1# show show ipv6 rip database

```
R1#show ipv6 rip database
RIP process "Test1" local RIB
  2001:DB8:ACAD:C::/64, metric 3, installed
    Serial0/0/0/FE80::2, expires in 167 sec
  2001:DB8:ACAD:12::/64, metric 2
    Serial0/0/0/FE80::2, expires in 167 sec
  2001:DB8:ACAD:23::/64, metric 2, installed
    Serial0/0/0/FE80::2, expires in 167 sec
R1#
```

¿Cuáles son las similitudes entre RIPv2 y RIPng?

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

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

R/ **show ipv6 route**

R1

```

R1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
  via GigabitEthernet0/1, receive
R 2001:DB8:ACAD:C::/64 [120/3]
  via FE80::2, Serial0/0/0, receive
C 2001:DB8:ACAD:12::/64 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
  via Serial0/0/0, receive
R 2001:DB8:ACAD:23::/64 [120/2]
  via FE80::2, Serial0/0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
R1#

```

R2

```

R2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
R 2001:DB8:ACAD:A::/64 [120/2]
  via FE80::1, Serial0/0/0, receive
C 2001:DB8:ACAD:B::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:B::2/128 [0/0]
  via GigabitEthernet0/0, receive
R 2001:DB8:ACAD:C::/64 [120/2]
  via FE80::3, Serial0/0/1, receive
C 2001:DB8:ACAD:12::/64 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::2/128 [0/0]
  via Serial0/0/0, receive
C 2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::2/128 [0/0]
  via Serial0/0/1, receive
L FF00::/8 [0/0]
  via Null0, receive
R2#

```

R3

```

R3#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R 2001:DB8:ACAD:A::/64 [120/3]
   via FE80::2, Serial0/0/1, receive
C 2001:DB8:ACAD:C::/64 [0/0]
   via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:C::3/128 [0/0]
   via GigabitEthernet0/1, receive
R 2001:DB8:ACAD:12::/64 [120/2]
   via FE80::2, Serial0/0/1, receive
C 2001:DB8:ACAD:23::/64 [0/0]
   via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::3/128 [0/0]
   via Serial0/0/1, receive
L FF00::/8 [0/0]
   via Null0, receive
R3#

```

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

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

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

hh. Verifique la conectividad entre las computadoras.

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

```

PC>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

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

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

PC>

```

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


```

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

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

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=5ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 2ms

PC>

```

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

```

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

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

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

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

PC>

```

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

```

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

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

Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

PC>

```

¿Por qué algunos pings tuvieron éxito y otros no?

R/ No se anunció ninguna ruta a la red 2001:DB8:ACAD:B::/64

Paso 12. 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.

R/ **ipv6 route ::/64 2001:db8:acad:b::b**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/64 2001:db8:acad:b::b
R2(config)#
```

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

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

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

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

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

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z
R2(config)#ipv6 route ::/64 2001:db8:acad:b::b
R2(config)#
R2(config)#
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#
```

Paso 13. Verificar la configuración de enrutamiento.

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

```
R2# show ipv6 route
```

```

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

```

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

R/ La ruta estática predeterminada aparece en la tabla con routing del R2

S::/64[1/0] via 2001:DB8:ACAD::B

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

Consulta tabla routing **R1**

```

R1#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   ::/0 [120/2]
    via FE80::2, Serial0/0/0, receive
C   2001:DB8:ACAD:A::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:A::1/128 [0/0]
    via GigabitEthernet0/1, receive
R   2001:DB8:ACAD:C::/64 [120/3]
    via FE80::2, Serial0/0/0, receive
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::1/128 [0/0]
    via Serial0/0/0, receive
R   2001:DB8:ACAD:23::/64 [120/2]
    via FE80::2, Serial0/0/0, receive
L   FF00::/8 [0/0]
--More--

```

Consulta tabla routing R3

```

R3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   ::/0 [120/2]
    via FE80::2, Serial0/0/1, receive
R   2001:DB8:ACAD:A::/64 [120/3]
    via FE80::2, Serial0/0/1, receive
C   2001:DB8:ACAD:C::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:C::3/128 [0/0]
    via GigabitEthernet0/1, receive
R   2001:DB8:ACAD:12::/64 [120/2]
    via FE80::2, Serial0/0/1, receive
C   2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::3/128 [0/0]
    via Serial0/0/1, receive
L   FF00::/8 [0/0]
    via Null0, receive
R3#

```

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

R/ La ruta predeterminada aparece como una ruta RIPng distribuida con el valor de métrica

2. **R1: R::/0 [120/2] via FE::2, s 0/0/0**

R3: R::/0 [120/2] via FE::2, s 0/0/1

Paso 4. Verifique la conectividad.

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

¿Tuvieron éxito los pings? **R/SI**

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

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

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>
```

Reflexión

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

R/ Para que los routers no resuman las rutas en los límites de las redes principales con clase

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

R/ Por actualizaciones del routing recibidas del router en el que estaba configurada la ruta predeterminada (R2)

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

R/ RIPv2 se configura mediante instrucciones de network, mientras que RIPv6 se configura en las interfaces

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

Topología

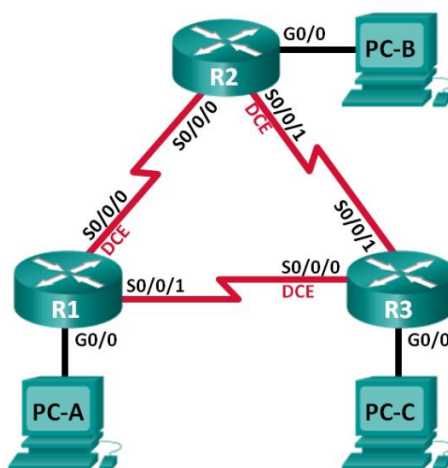


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

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.

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

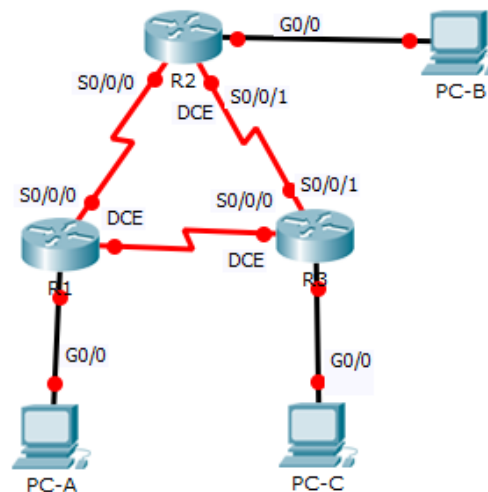
Cables Ethernet y seriales, como se muestra en la topología

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 en los equipos host y los routers.

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

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



Paso 3: configurar los parámetros básicos para cada router.

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

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

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

Configuración R1

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable password class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#no ip domain-lookup
R1(config)#banner motd "Se Prohibe el Acceso No Autorizado"
R1(config)#int g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

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

R1(config-if)#
```

```
R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#int s0/0/1
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#
```

Configuración R2


```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#enable password class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#no ip domain-lookup
R2(config)#banner motd "Se Prohibe el Acceso No Autorizado"
R2(config)#int g0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut

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

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

R2(config-if)#
```

```
R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.12.2 255.255.255.252
R1(config-if)#no shut

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

R1(config-if)#in
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R1(config-if)#
R1(config-if)#int s0/0/1
R1(config-if)#ip address 192.168.23.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#
```

Configuración R3

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#enable password class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#no ip domain-lookup
R3(config)#banner motd "Se Prohibe el Acceso No Autorizado"
R3(config)#int g0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R3(config-if)#
```

```
R3(config-if)#int s0/0/0
R3(config-if)#ip address 192.168.13.2 255.255.255.252
R3(config-if)#clock rate 128000
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

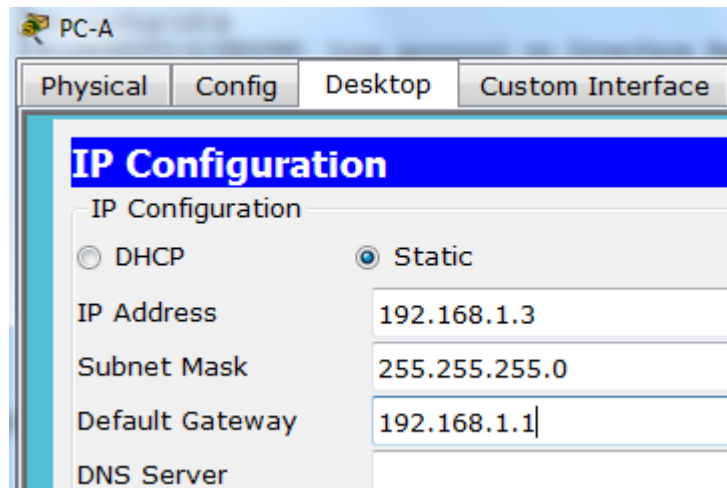
R3(config-if)#int s0/0/1
R3(config-if)#ip address 192.168.23.2 255.255.255.252
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

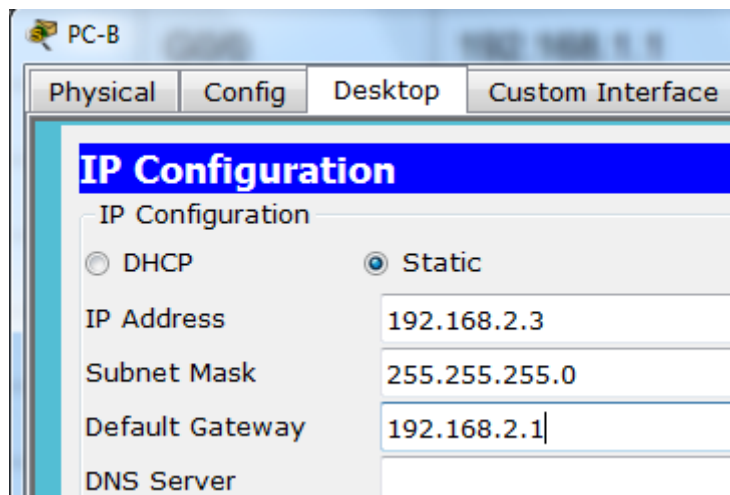
R3(config-if)#
```

Paso 4: configurar los equipos host.

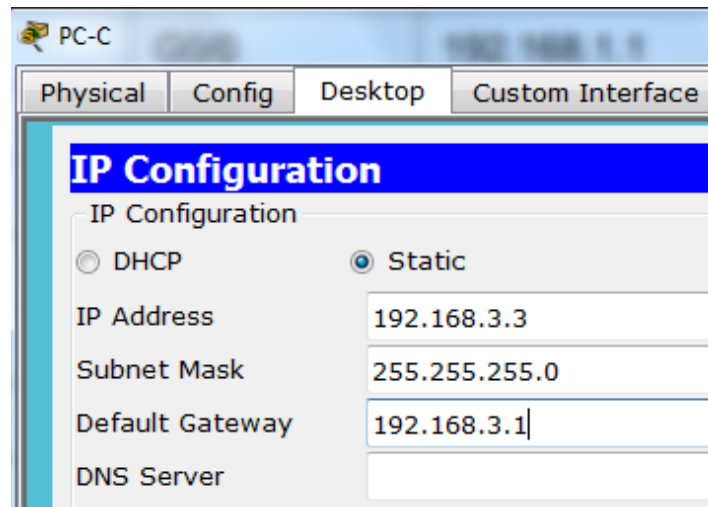
Configuración PC-A



Configuración PC-B



Configuración PC-C



Paso 5: Probar la conectividad.

Ping del R1 al R2

```
R1#ping 192.168.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/25/121 ms

R1#
```

Ping del R1 al R3

```
R1#ping 192.168.13.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

R1#
```

Ping del R2 al R3

Parte 2: 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.

Paso 1: Configure el protocolo OSPF en R1.

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

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

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

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
```

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

Paso 2: Configure OSPF en el R2 y el R3

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

Configure OSPF en el R2

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.255 area 0
R2(config-router)#
00:48:59: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on Serial0/0/0 from LOADING
to FULL, Loading Done

R2(config-router)#network 192.168.23.0 0.0.0.255 area 0
R2(config-router)#

```

Configure OSPF en el R3

```

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#
R3(config)#network 192.168.3.0 0.0.0.255 area 0
^
% Invalid input detected at '^' marker.

R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.13.0 0.0.0.255 area 0
R3(config-router)#
00:53:20: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on Serial0/0/0 from LOADING
to FULL, Loading Done

R3(config-router)#network 192.168.23.0 0.0.0.255 area 0
R3(config-router)#

```

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

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

R1

```

R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
192.168.23.1     0     FULL/ -         00:00:39   192.168.12.2   Serial0/0/0
192.168.13.2     0     FULL/ -         00:00:37   192.168.13.2   Serial0/0/1
R1#

```

R2

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.13.1	0	FULL/ -	00:00:30	192.168.12.1	Serial0/0/0

```
R2#
```

R3

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.13.1	0	FULL/ -	00:00:38	192.168.13.1	Serial0/0/0

```
R3#
```

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

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, 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, 00:14:32, Serial0/0/0  
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:10:11, 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
```

```
R1#
```

R2

```

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

Gateway of last resort is not set

O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:15:57, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, GigabitEthernet0/0
L    192.168.2.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/129] via 192.168.12.1, 00:11:27, Serial0/0/0
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.2/32 is directly connected, Serial0/0/0
     192.168.13.0/30 is subnetted, 1 subnets
O    192.168.13.0/30 [110/128] via 192.168.12.1, 00:15:57, Serial0/0/0
R2#

```

R3

```

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

Gateway of last resort is not set

O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:12:35, Serial0/0/0
O    192.168.2.0/24 [110/129] via 192.168.13.1, 00:12:35, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, GigabitEthernet0/0
L    192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O    192.168.12.0/30 [110/128] via 192.168.13.1, 00:12:35, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/0
L    192.168.13.2/32 is directly connected, Serial0/0/0
R3#

```

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

R/ show ip route ospf

Paso 4: verificar la configuración del protocolo OSPF.

El comando show ip protocols es una manera rápida de verificar información fundamental de configuración de OSPF. Esta información incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.

R1# show ip protocols

```
R1#show ip protocols
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
    192.168.13.1    110          00:26:58
    192.168.13.2    110          00:26:58
    192.168.23.1    110          00:01:16
  Distance: (default is 110)

R1#
```

Paso 5: verificar la información del proceso OSPF.

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

R1# show ip ospf

```
R1#show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
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
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 2 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x01d9e4
    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

R1#
```

Paso 6: verificar la configuración de la interfaz OSPF

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

R1# **show ip ospf interface brief** → este comando no funciona

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**

```

R1#show ip ospf interface

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
  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
    Hello due in 00:00:01
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 192.168.13.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01

R1#

```

Paso 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.

Ping del PC-A al PC-B

```

PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

PC>

```

Ping del PC-A al PC-C

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=4ms TTL=126
Reply from 192.168.2.3: bytes=32 time=2ms TTL=126
Reply from 192.168.2.3: bytes=32 time=2ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

PC>|
```

Ping del PC-B al PC-C

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=11ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=6ms TTL=125
Reply from 192.168.3.3: bytes=32 time=4ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 5ms

PC>|
```

Parte 3: 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.

Paso 1: Cambie las ID de router con direcciones de loopback

b. 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
```

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface lo0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

c. 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.

Asignación IP loopback 0 en R2

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface lo0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#

```

Asignación IP loopback 0 en R3

```

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface lo0

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R3(config-if)#ip address 3.3.3.3 255.255.255.255
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#

```

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

R1

```

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

```

```

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

```

```

R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#

```

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

R1

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

Readonly ROMMON initialized
```

R2

```
R2#reload
Proceed with reload? [confirm]
00:54:17: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done

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

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

R3

```
R3#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
```

f. 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

```

R1>show ip protocols

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
    1.1.1.1          110          00:06:29
    2.2.2.2          110          00:06:29
    3.3.3.3          110          00:08:29
    192.168.13.1     110          00:32:59
    192.168.13.2     110          00:09:03
    192.168.23.1     110          00:09:03
  Distance: (default is 110)

R1>

```

g. 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
2.2.2.2        0    FULL/ -         00:00:31   192.168.12.2   Serial0/0/0
3.3.3.3        0    FULL/ -         00:00:39   192.168.13.2   Serial0/0/1
R1>

```

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

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

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

R1(config)# `router ospf 1`

R1(config-router)# `router-id 11.11.11.11`

Reload or use "clear ip ospf process" command, for this to take effect

R1(config)# `end`


```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 11.11.11.11
R1(config-router)#Reload or use "clear ip ospf process" command, for this to take
effect

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

R1#

```

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`.

```

R1#clear ip ospf process
Reset ALL OSPF processes? [no]:

R1#clear ip ospf
% Incomplete command.
R1#
R1#clear ip ospf process
Reset ALL OSPF processes? [no]:

R1#

```

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.

R2

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 22.22.22.22
R2(config-router)#Reload or use "clear ip ospf process" command, for this to take
effect

R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#

```

R3

```

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 33.33.33.33
R3(config-router)#Reload or use "clear ip ospf process" command, for this to take
effect

R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#

```

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

```

R1#show ip protocols

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
    1.1.1.1          110          00:26:21
    2.2.2.2          110          00:26:21
    3.3.3.3          110          00:28:21
    192.168.13.1     110          00:52:51
    192.168.13.2     110          00:28:55
    192.168.23.1     110          00:28:55
  Distance: (default is 110)

R1#

```

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

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:33	192.168.12.2	Serial0/0/0
3.3.3.3	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1

R1#

Parte 4: 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.

Paso 1: configurar una interfaz pasiva.

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

R1# show ip ospf interface g0/0

```
R1#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, 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, Interface address 192.168.1.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:09
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
R1#
```

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
```

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#passive-interface g0/0
R1(config-router)#
```

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`

```
R1#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State WAITING, Priority 1
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
R1#
```

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

```

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

Gateway of last resort is not set

    2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.12.1, 00:40:52, Serial0/0/0
O       192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O       192.168.3.0/24 [110/129] via 192.168.12.1, 00:40:52, Serial0/0/0
O       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
O       192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0/30 [110/128] via 192.168.12.1, 00:40:52, Serial0/0/0
R2#

```

R3

```

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

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:46:40, Serial0/0/0
O       192.168.2.0/24 [110/129] via 192.168.13.1, 00:44:30, Serial0/0/0
O       192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
O       192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:44:50, Serial0/0/0
O       192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
R3#

```

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

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

R1# `show ip ospf neighbor`

```
Neighbor ID      Pri   State           Dead Time   Address      Interface
2.2.2.2          0    FULL/ -         00:00:37   192.168.12.2 Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:35   192.168.13.2 Serial0/0/1
R1#
```

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)#

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#
R2(config)#router ospf 1
R2(config-router)#passive-interface default
R2(config-router)#
00:52:02: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
R2(config-router)#
```

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
3.3.3.3          0    FULL/ -         00:00:34   192.168.13.2 Serial0/0/1
R1#
```

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`

```

R2#show ip ospf interface s0/0/0

Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.12.2/30, Area 0
 Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Suppress hello for 0 neighbor(s)
R2#

```

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**.

R2

```

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

Gateway of last resort is not set

 2.0.0.0/32 is subnetted, 1 subnets
 C       2.2.2.2/32 is directly connected, Loopback0
 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
 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
R2#

```

R3

```

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

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 01:03:01, Serial0/0/0
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
    192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 01:01:10, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
R3#

```

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)#
```

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#
00:04:36: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING
to FULL, Loading Done
R2(config-router)#

```

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**

```
show ip route 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, 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

    1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
    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, 00:02:46, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 00:07:13, 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
R1#

```

show ip route R3

```

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

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:14:12, Serial0/0/0
O       192.168.2.0/24 [110/129] via 192.168.13.1, 00:09:36, Serial0/0/0
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
    192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:14:12, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
R3#

```

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? R/ la interfaz s0/0/0

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3? R/ La métrica es 129

¿El R2 aparece como vecino OSPF en el R1? R/ SI

¿El R2 aparece como vecino OSPF en el R3? R/ NO

¿Qué indica esta información? R/ Indica que no manda por esa interface paquetes Hello, el r2 tiene esa interface pasiva

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

R/ **router ospf 1**

no passive-interface s0/0/1

```
R2(config-router)#router ospf 1
R2(config-router)#no passive-interface s0/0/1
R2(config-router)#
```

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/ La s0/0/0

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

Gateway of last resort is not set

  3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:57, Serial0/0/0
O       192.168.2.0/24 [110/129] via 192.168.13.1, 00:26:21, Serial0/0/0
       192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
       192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:30:57, Serial0/0/0
       192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
R3#
```

¿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 es 65, esta se calcula de una link de 1.544 cuesta 64 más 1 que es la gigabyte son 65 que es la métrica que da

¿El R2 aparece como vecino OSPF del R3? R/ SI

Parte 5: 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.

Paso 1: cambiar el ancho de banda de referencia en los routers.

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**

```

R1#show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Hardware is CN Gigabit Ethernet, address is 000c.cf8b.dc01 (bia 000c.cf8b.dc01)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); 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 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 watchdog, 1017 multicast, 0 pause input
  0 input packets with dribble condition detected
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
R1#

```

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

```

R1#show ip route ospf
O   192.168.2.0 [110/65] via 192.168.12.2, 00:13:51, Serial0/0/0
O   192.168.3.0 [110/65] via 192.168.13.2, 00:13:51, Serial0/0/1
R1#

```

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

```

R3#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.3.1/24, Area 0
Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R3#

```

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.

```

R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#

```

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

Comando **auto-cost reference-bandwidth 10000** en R2

```
R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all routers.
R2(config-router)#
```

Comando **auto-cost reference-bandwidth 10000** en R3

```
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all routers.
R3(config-router)#
```

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

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

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 100
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R3#
```

R1# **show ip ospf interface s0/0/1**

```

R1#show ip ospf interface s0/0/1

Serial0/0/1 is up, line protocol is up
 Internet address is 192.168.13.1/30, Area 0
 Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 6476
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:04
 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 33.33.33.33
 Suppress hello for 0 neighbor(s)
R1#

```

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

R1# show ip route ospf

```

R1#show ip route ospf
O   192.168.2.0 [110/6576] via 192.168.12.2, 00:11:50, Serial0/0/0
O   192.168.3.0 [110/6576] via 192.168.13.2, 00:10:26, Serial0/0/1
R1#

```

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

```

R1#show ip route ospf
O   192.168.2.0 [110/6576] via 192.168.12.2, 00:11:50, Serial0/0/0
O   192.168.3.0 [110/6576] via 192.168.13.2, 00:10:26, Serial0/0/1
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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.
R1(config-router)#

```

Paso 2: cambiar el ancho de banda de una interfaz.

En la mayoría de los enlaces seriales, la métrica del ancho de banda será 1544 Kbits de manera predeterminada (la de un T1). Si esta no es la velocidad real del enlace serial, se

deberá cambiar la configuración del ancho de banda para que coincida con la velocidad real, a fin de permitir que el costo de la ruta se calcule correctamente en OSPF. Use el comando `bandwidth` para ajusta la configuración del ancho de banda de una interfaz.

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**

```
R1#show interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 192.168.12.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
5 minute input rate 54 bits/sec, 0 packets/sec
5 minute output rate 54 bits/sec, 0 packets/sec
478 packets input, 32692 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
501 packets output, 34284 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
R1#
```

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
O    192.168.2.0 [110/164] via 192.168.12.2, 00:12:59, Serial0/0/0
O    192.168.3.0 [110/164] via 192.168.13.2, 00:12:59, Serial0/0/1
R1#
```

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
```

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

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
```

```
1.0.0.0/32 is subnetted, 1 subnets  
C    1.1.1.1/32 is directly connected, Loopback0  
    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 [110/782] via 192.168.12.2, 00:00:10, Serial0/0/0  
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:10, 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  
R1#
```

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 interface brief  
Interface                IP-Address      OK? Method Status Protocol  
GigabitEthernet0/0      192.168.1.1    YES manual up      up  
GigabitEthernet0/1      unassigned      YES unset  administratively down down  
Serial0/0/0             192.168.12.1   YES manual up      up  
Serial0/0/1             192.168.13.1   YES manual up      up  
Loopback0               1.1.1.1        YES manual up      up  
Vlan1                   unassigned      YES unset  administratively down down  
R1#
```

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

```

R1(config)#int s0/0/1
R1(config-if)#bandwidth 128
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
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`

```

Gateway of last resort is not set

 1.0.0.0/32 is subnetted, 1 subnets
C    1.1.1.1/32 is directly connected, Loopback0
 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 [110/782] via 192.168.12.2, 00:16:42, Serial0/0/0
O    192.168.3.0/24 [110/782] via 192.168.13.2, 00:04:13, 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
R1#

```

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`

```

R3#show ip route ospf
O    192.168.1.0 [110/65] via 192.168.13.1, 00:23:15, Serial0/0/0
O    192.168.2.0 [110/846] via 192.168.13.1, 00:23:05, Serial0/0/0
 192.168.12.0/30 is subnetted, 1 subnets
O    192.168.12.0 [110/845] via 192.168.13.1, 00:23:15, Serial0/0/0
R3#

```

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

```

R2(config)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#en
% Ambiguous command: "en"
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#

```

¿Cuál es el nuevo costo acumulado a la red 192.168.23.0/24 en el R1? ¿Por qué?

R/ El nuevo costo es el acumulado es 1562 por que la suma es $781+781=1562$

Paso 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

```

Gateway of last resort is not set

  1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
  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 [110/782] via 192.168.12.2, 00:32:58, Serial0/0/0
O       192.168.3.0/24 [110/782] via 192.168.13.2, 00:20:29, 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

R1#

```

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

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

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

```
Gateway of last resort is not set

  1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
  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 [110/782] via 192.168.12.2, 00:40:28, Serial0/0/0
O       192.168.3.0/24 [110/1566] via 192.168.13.2, 00:04:17, 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
R1#
```

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

R/ **Porque ahora el costo es mayor al ir por la serial s0/0/01, de 1565. Se va por la serial 0/0/0**

Reflexión

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

R/ **porque si no hay un nombre de router ID usa una look back más alta, sino hay usa la ip más alta dentro de sus interfaces activas, y si esta se desactiva cambia el nombre o ID del route, por lo tanto va a ver problemas al elegir el DR y el BDR.**

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

R/ Porque la elección del router designado (DR) y del router designado de respaldo (BDR) se hace en redes Ethernet y en este laboratorio estamos usando redes punto a punto y no hay problemas en elegir el DR o BDR

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

R/ Porque una interface pasiva me permite hacer que si no hay un route en esa interface no es necesario enviar paquetes hello por seguridad lo que ahorrar recurso de red como ancho de banda, etc.

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

Topología

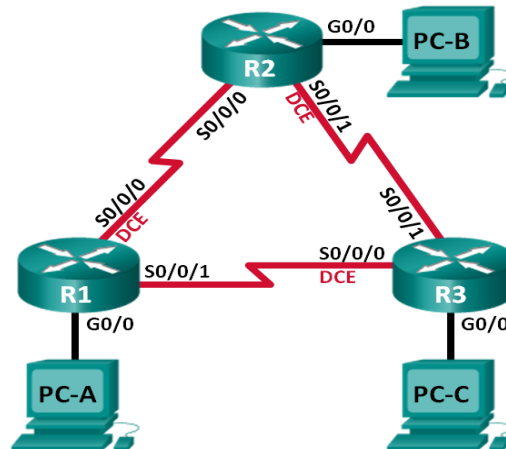


Tabla de direccionamiento

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

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)

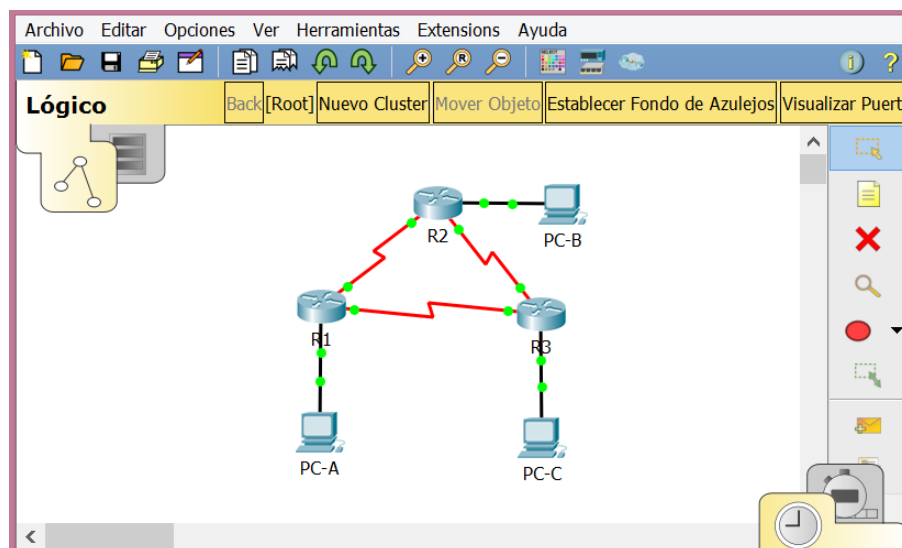
Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet y seriales, como se muestra en la topología

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.

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



Inicializar y volver a cargar los routers según sea necesario.

Configurar los parámetros básicos para cada router.

Desactive la búsqueda del DNS.

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

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

Asigne **cisco** como la contraseña de vty.

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

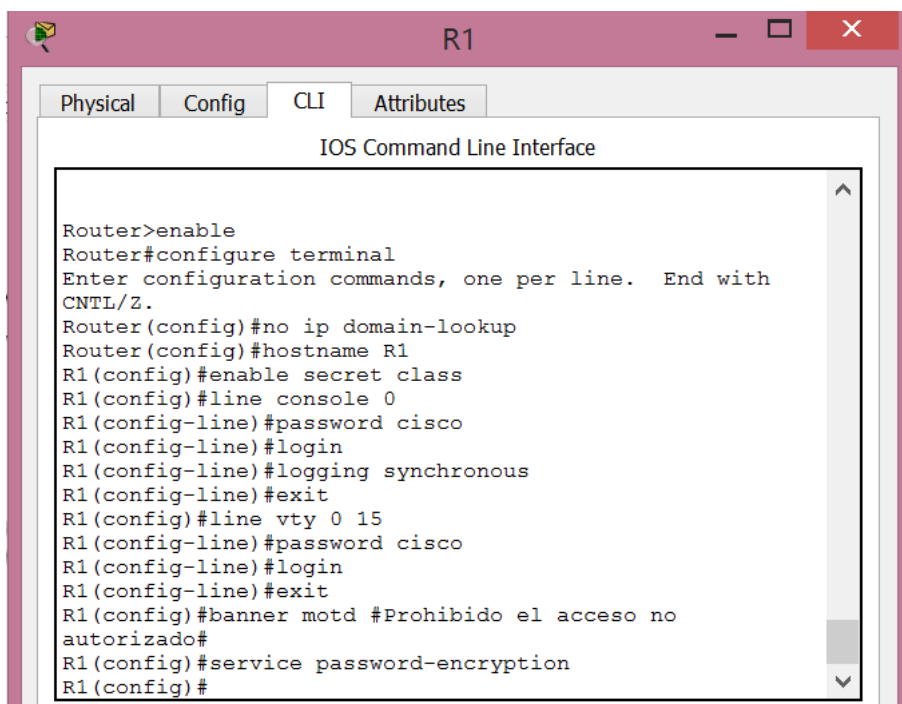
Configure **logging synchronous** para la línea de consola.

Cifre las contraseñas de texto no cifrado.

Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.

Habilite el routing de unidifusión IPv6 en cada router.

Copie la configuración en ejecución en la configuración de inicio



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd #Prohibido el acceso no
autorizado#
R1(config)#service password-encryption
R1(config)#
```



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#service password-encryption
R1(config)#
R1(config)#interface g0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no 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

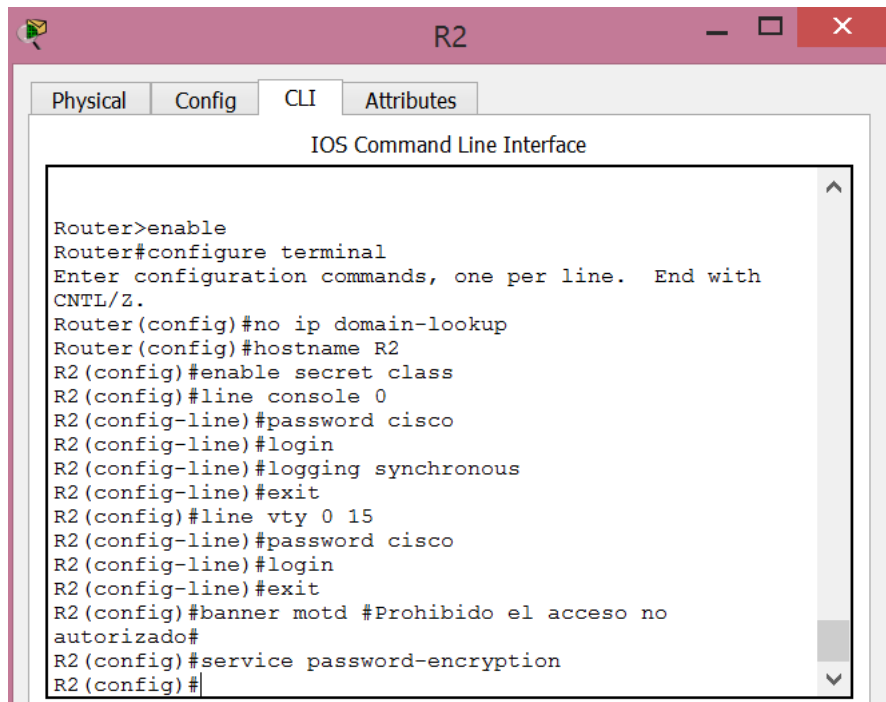
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

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

R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:13::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

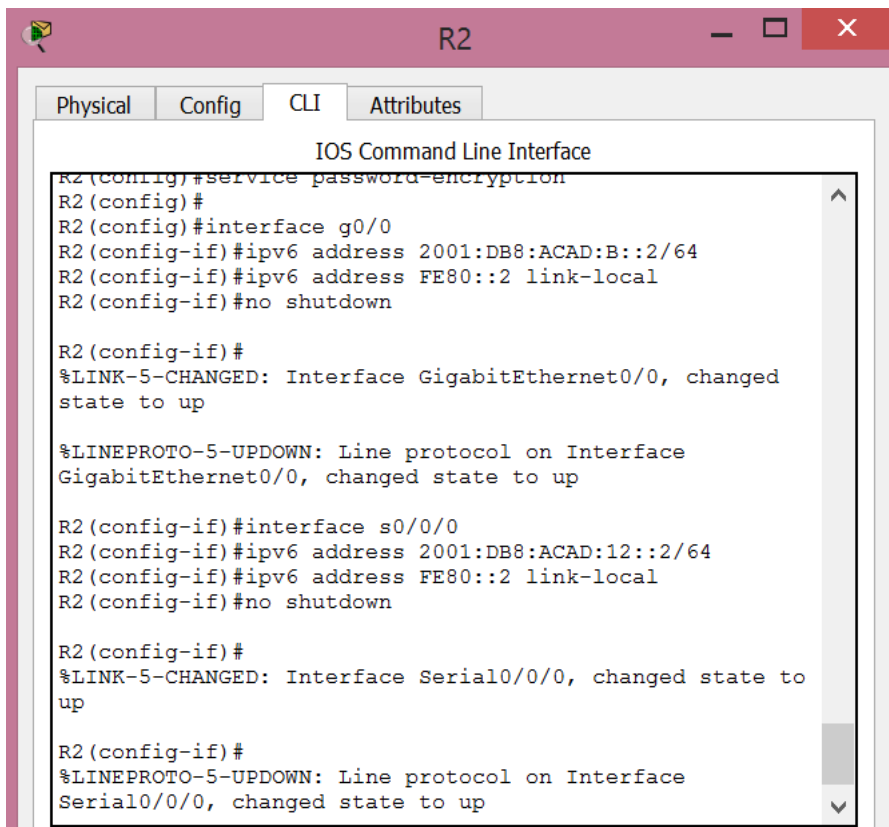
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to
down
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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



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

```
Router>enable
Router#configure terminal
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)#logging synchronous
R2(config-line)#exit
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#banner motd #Prohibido el acceso no
autorizado#
R2(config)#service password-encryption
R2(config)#
```



The screenshot shows the same "R2" window with the "CLI" tab active. The terminal output continues with interface configuration commands and status messages:

```
R2(config)#service password-encryption
R2(config)#
R2(config)#interface g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

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

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

R2(config-if)#interface s0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

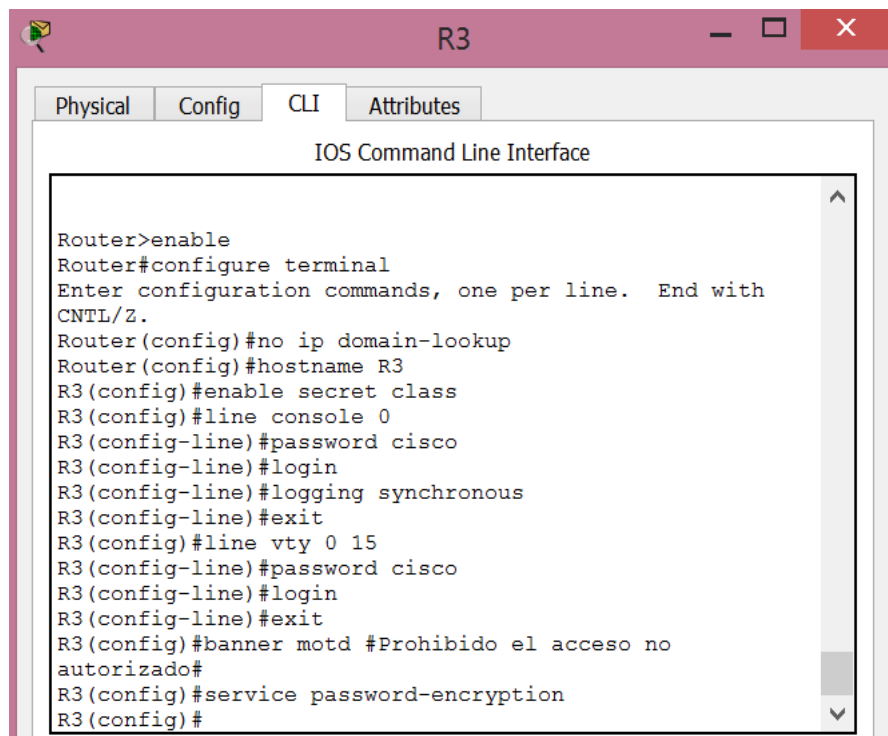
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to
up

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

```
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to
down
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

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



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

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#banner motd #Prohibido el acceso no
autorizado#
R3(config)#service password-encryption
R3(config)#
```

The image shows a window titled "R3" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the configuration of interfaces g0/0, s0/0/0, and serial0/0/1 with IPv6 addresses and link-local addresses. It also shows the execution of "copy run start" to save the configuration.

```
R3(config)#
R3(config)#interface g0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed
state to up

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

R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:13::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#clock rate 128000
This command applies only to DCE interfaces
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to
up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up

R3(config-if)#

R3(config-if)#interface serial0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown

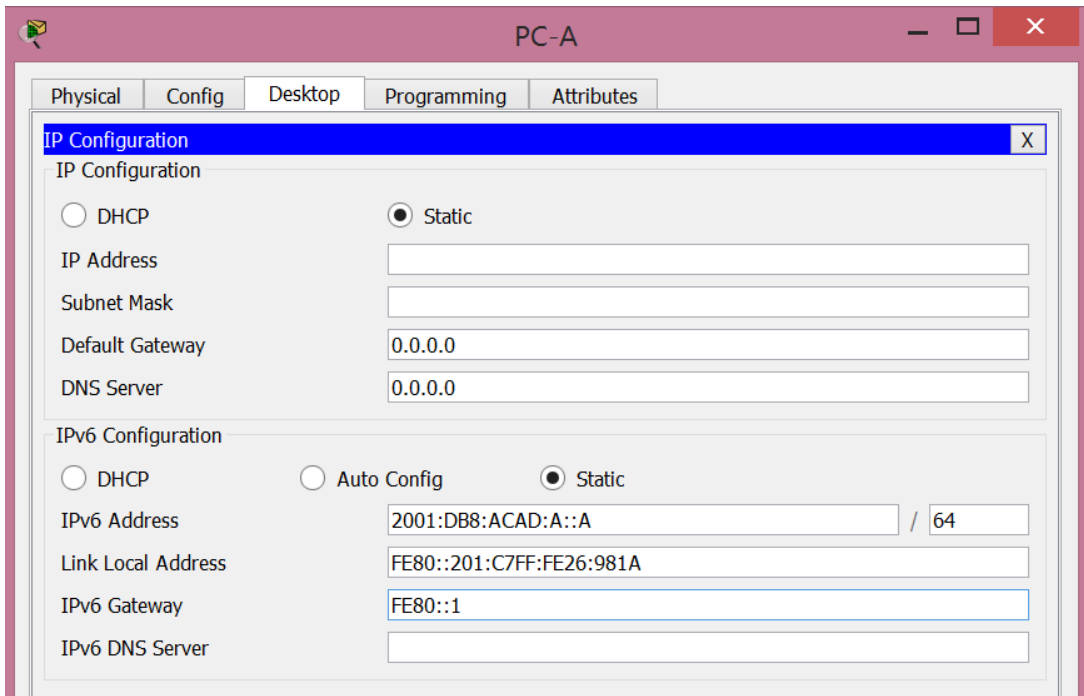
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to
up

R3(config-if)#exit
R3(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up

R3(config)#ipv6 unicast-routing
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

configurar los equipos host.



PC-A

Physical Config Desktop Programming Attributes

IP Configuration

DHCP Static

IP Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

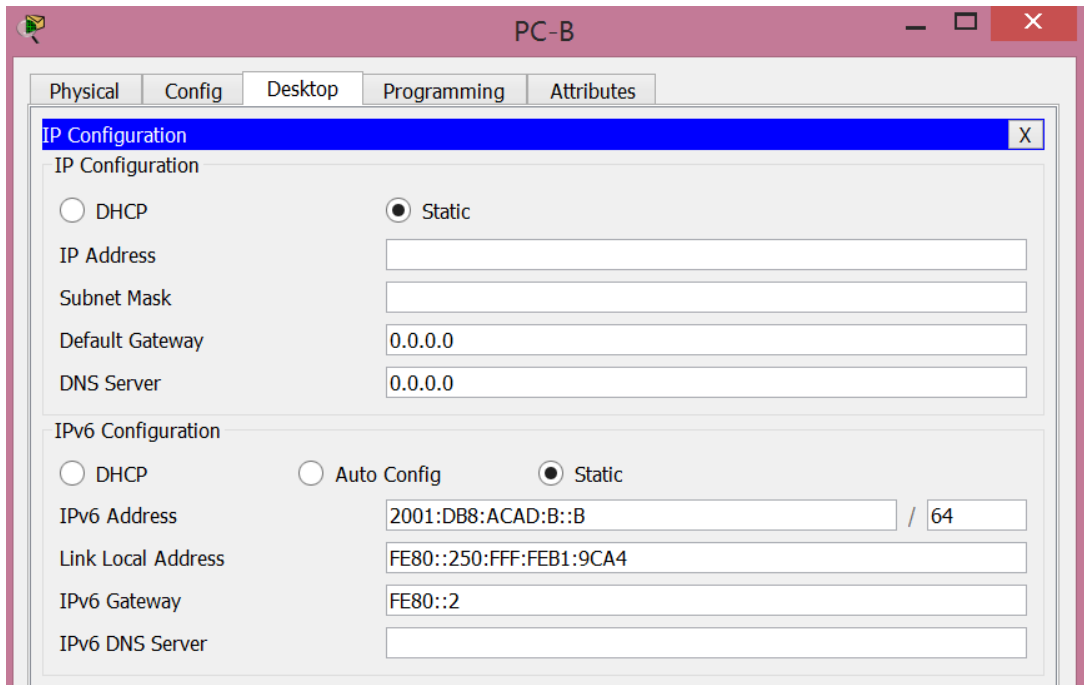
DHCP Auto Config Static

IPv6 Address 2001:DB8:ACAD:A::A / 64

Link Local Address FE80::201:C7FF:FE26:981A

IPv6 Gateway FE80::1

IPv6 DNS Server



PC-B

Physical Config Desktop Programming Attributes

IP Configuration

DHCP Static

IP Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

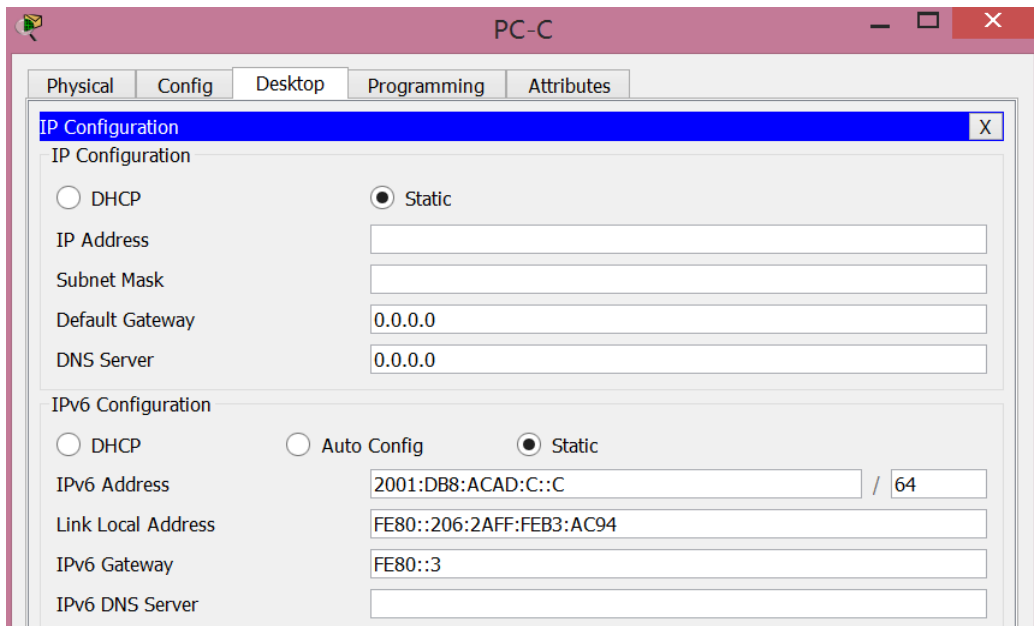
DHCP Auto Config Static

IPv6 Address 2001:DB8:ACAD:B::B / 64

Link Local Address FE80::250:FFF:FEB1:9CA4

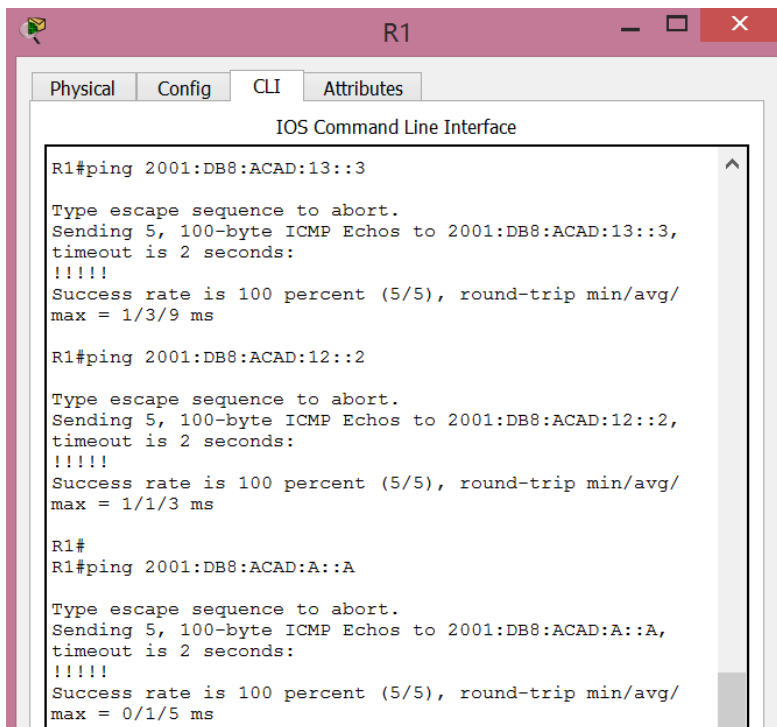
IPv6 Gateway FE80::2

IPv6 DNS Server



Probar la conectividad.

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



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

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::3,
timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/
max = 1/2/5 ms

R2#ping 2001:DB8:ACAD:12::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::1,
timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/
max = 1/3/7 ms

R2#
R2#ping 2001:DB8:ACAD:B::B

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:B::B,
timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/
max = 0/0/2 ms

R2#
```

```
R3
R3#ping 2001:DB8:ACAD:13::1

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

R3#ping 2001:DB8:ACAD:23::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::2,
timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/
max = 1/2/8 ms

R3#ping 2001:DB8:ACAD:C::C

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:C::C,
timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/
max = 0/2/8 ms

R3#
```

PC-C

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
Packet Tracer PC Command Line 1.0
C:\>ping FE80::3

Pinging FE80::3 with 32 bytes of data:

Reply from FE80::3: bytes=32 time<1ms TTL=255
Reply from FE80::3: bytes=32 time<1ms TTL=255
Reply from FE80::3: bytes=32 time<1ms TTL=255
Reply from FE80::3: bytes=32 time<1ms TTL=255

Ping statistics for FE80::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

PC-B

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
Packet Tracer PC Command Line 1.0
C:\>ping FE80::2

Pinging FE80::2 with 32 bytes of data:

Reply from FE80::2: bytes=32 time=1ms TTL=255
Reply from FE80::2: bytes=32 time<1ms TTL=255
Reply from FE80::2: bytes=32 time<1ms TTL=255
Reply from FE80::2: bytes=32 time<1ms TTL=255

Ping statistics for FE80::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

PC-A

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
Packet Tracer PC Command Line 1.0
C:\>ping FE80::1

Pinging FE80::1 with 32 bytes of data:

Reply from FE80::1: bytes=32 time=1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255

Ping statistics for FE80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```


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.

Asignar ID a los routers.

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

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

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

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

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

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

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

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

```
R2# show ipv6 ospf
```

```
Routing Process "ospfv3 1" with ID 2.2.2.2
```

```
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
```

```
Router is not originating router-LSAs with maximum metric
```

```
<Output Omitted>
```

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
CNTL/Z.  
R1(config)#  
R1(config)#ipv6 router ospf 1  
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a  
router-id, please configure manually  
R1(config-rtr)#router-id 1.1.1.1  
R1(config-rtr)#exit  
R1(config)#exit  
R1#  
%SYS-5-CONFIG_I: Configured from console by console  
  
R1#show ipv6 ospf  
Routing Process "ospfv3 1" with ID 1.1.1.1  
SPF schedule delay 5 secs, Hold time between two SPFs  
10 secs  
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs  
LSA group pacing timer 240 secs  
Interface flood pacing timer 33 msec  
Retransmission pacing timer 66 msec  
Number of external LSA 0. Checksum Sum 0x000000  
Number of areas in this router is 0. 0 normal 0 stub 0  
nssa  
Reference bandwidth unit is 100 mbps  
  
R1#|
```

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
R2(config)#  
R2(config)#ipv6 router ospf 1  
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a  
router-id, please configure manually  
R2(config-rtr)#router-id 2.2.2.2  
R2(config-rtr)#exit  
R2(config)#exit  
R2#  
%SYS-5-CONFIG_I: Configured from console by console  
  
R2#show ipv6 ospf  
Routing Process "ospfv3 1" with ID 2.2.2.2  
SPF schedule delay 5 secs, Hold time between two SPFs  
10 secs  
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs  
LSA group pacing timer 240 secs  
Interface flood pacing timer 33 msec  
Retransmission pacing timer 66 msec  
Number of external LSA 0. Checksum Sum 0x000000  
Number of areas in this router is 0. 0 normal 0 stub 0  
nssa  
Reference bandwidth unit is 100 mbps  
  
R2#|
```

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config)#
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a
router-id, please configure manually
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
SPF schedule delay 5 secs, Hold time between two SPFs
10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0
nssa
Reference bandwidth unit is 100 mbps

R3#
```

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.

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
```

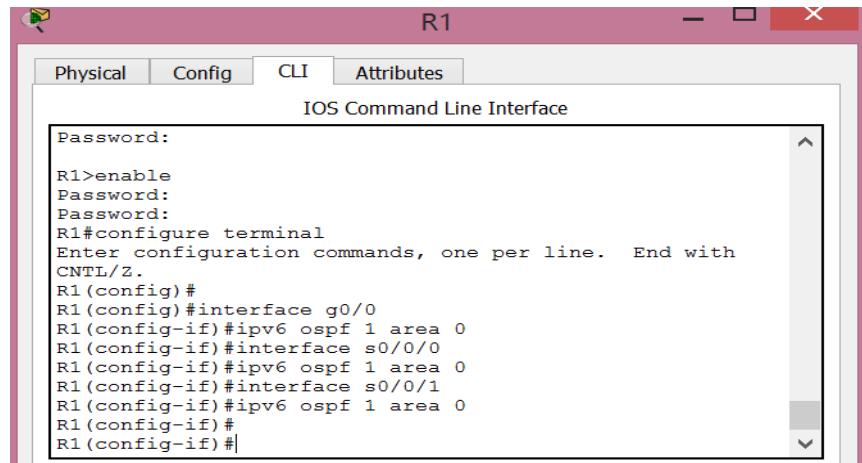
```
R1(config-if)# interface s0/0/0
```

```
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.

A screenshot of a network device terminal window titled 'R1'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The main area is titled 'IOS Command Line Interface'. The terminal shows the following commands and output:

```
Password:
R1>enable
Password:
Password:
R1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)#
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)#
R1(config-if)#
```

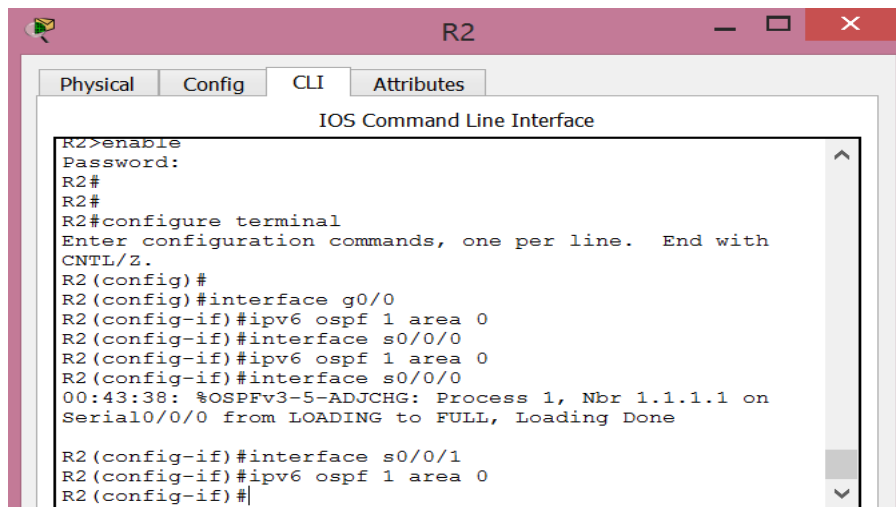
Asigne las interfaces en el R2 y el R3 al área 0 de OSPFv3. Al agregar las interfaces al área 0, debería ver mensajes de adyacencia de vecino.

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

A screenshot of a network device terminal window titled 'R2'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The main area is titled 'IOS Command Line Interface'. The terminal shows the following commands and output:

```
R2>enable
Password:
R2#
R2#
R2#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R2(config)#
R2(config)#interface g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/0
00:43:38: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
```

```

R3#
R3#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R3(config)#
R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
00:49:59: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
00:50:10: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on
Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-if)#

```

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

```
Physical Config CLI Attributes
IOS Command Line Interface

Prohibido el acceso no autorizado
User Access Verification
Password:
R1>enable
Password:
R1#
R1#show ipv6 ospf neighbor

Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
2.2.2.2          0     FULL/ -         00:00:30   3             Serial0/0/0
3.3.3.3          0     FULL/ -         00:00:39   3             Serial0/0/1
R1#
```

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

```
R1#
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
R1#
```

Verificar las interfaces OSPFv3.

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

R1# **show ipv6 ospf interface**

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

Link Local Address FE80::1, Interface ID 7

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

Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

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

Hello due in 00:00:05

Graceful restart helper support enabled

Index 1/3/3, flood queue length 0

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

Last flood scan length is 1, maximum is 1

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

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 3.3.3.3

Suppress hello for 0 neighbor(s)

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

Link Local Address FE80::1, Interface ID 6

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

Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

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

Hello due in 00:00:00

Graceful restart helper support enabled

Index 1/2/2, flood queue length 0

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

Last flood scan length is 1, maximum is 2

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

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 2.2.2.2

Suppress hello for 0 neighbor(s)

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3

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

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

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

No backup designated router on this network

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

Hello due in 00:00:03

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

```
R1#show ipv6 ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  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 2.2.2.2
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 4
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
```

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	

```
R1#  
R1#show ipv6 ospf interface brief  
% Invalid input detected at '^' marker.  
R1#
```

Packet Tracer no soporta este comando.

Verificar la tabla de routing IPv6.

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

R2# show ipv6 route

IPv6 Routing Table - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

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

via FE80::1, Serial0/0/0

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

via GigabitEthernet0/0, directly connected

L 2001:DB8:ACAD:B::2/128 [0/0]

via GigabitEthernet0/0, receive

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

via FE80::3, Serial0/0/1

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

via Serial0/0/0, directly connected

- L 2001:DB8:ACAD:12::2/128 [0/0]
via Serial0/0/0, receive
- O 2001:DB8:ACAD:13::/64 [110/128]
via FE80::3, Serial0/0/1
via FE80::1, Serial0/0/0
- C 2001:DB8:ACAD:23::/64 [0/0]
via Serial0/0/1, directly connected
- L 2001:DB8:ACAD:23::2/128 [0/0]
via Serial0/0/1, receive
- L FF00::/8 [0/0]
via Null0, receive

```

R2#
R2#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
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::1, Serial0/0/0
  via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::2/128 [0/0]
  via Serial0/0/1, receive
L FF00::/8 [0/0]
  via Null0, receive
R2#

```

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

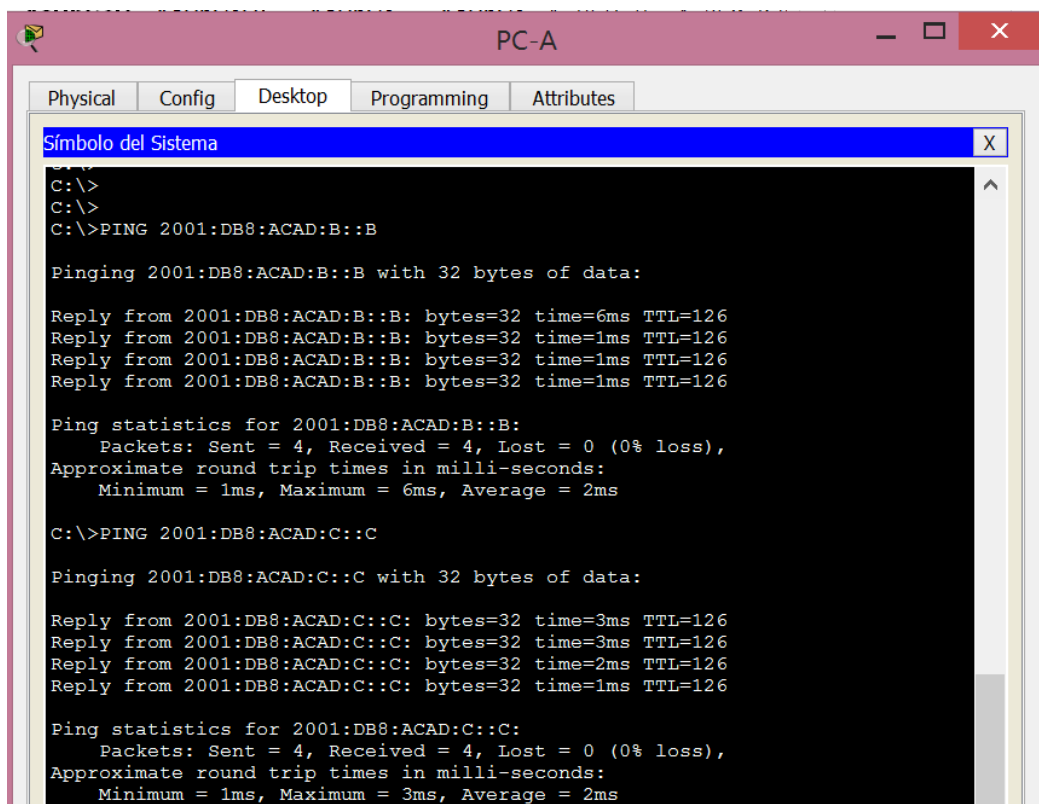
Show ipv6 route ospf

```
R2#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:13::/64 [110/128]
  via FE80::1, Serial0/0/0
  via FE80::3, Serial0/0/1
R2#
```

Verificar la conectividad de extremo a extremo.

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

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



```
PC-A
Physical Config Desktop Programming Attributes
Símbolo del Sistema
C:\>
C:\>
C:\>PING 2001:DB8:ACAD:B::B

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

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=6ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>PING 2001:DB8:ACAD:C::C

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

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

PC-B

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 1ms, Average = 0ms

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

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

Reply from 2001:DB8:ACAD:A:A: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:A:A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>PING 2001:DB8:ACAD:C:C

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

Reply from 2001:DB8:ACAD:C:C: bytes=32 time=4ms TTL=126
Reply from 2001:DB8:ACAD:C:C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C:C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C:C: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:C:C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

PC-C

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

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

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

Reply from 2001:DB8:ACAD:A:A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=5ms TTL=126
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=8ms TTL=126

Ping statistics for 2001:DB8:ACAD:A:A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 4ms

C:\>PING 2001:DB8:ACAD:C:C

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

Reply from 2001:DB8:ACAD:C:C: bytes=32 time=5ms TTL=128
Reply from 2001:DB8:ACAD:C:C: bytes=32 time=1ms TTL=128
Reply from 2001:DB8:ACAD:C:C: bytes=32 time<1ms TTL=128
Reply from 2001:DB8:ACAD:C:C: bytes=32 time=4ms TTL=128

Ping statistics for 2001:DB8:ACAD:C:C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 2ms
```

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.

configurar una interfaz pasiva.

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

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

```
GigabitEthernet0/0 is up, line protocol is up
```

```
Link Local Address FE80::1, Interface ID 3
```

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

```
Network Type BROADCAST, Cost: 1
```

```
Transmit Delay is 1 sec, State DR, Priority 1
```

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

```
No backup designated router on this network
```

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

```
Hello due in 00:00:05
```

```
Graceful restart helper support enabled
```

```
Index 1/1/1, flood queue length 0
```

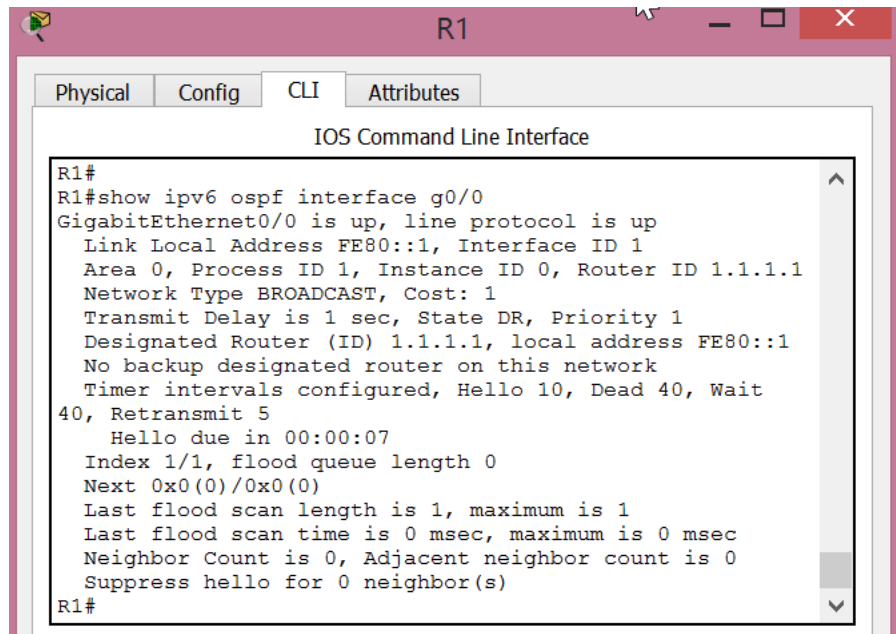
```
Next 0x0(0)/0x0(0)/0x0(0)
```

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

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

```
Neighbor Count is 0, Adjacent neighbor count is 0
```

Suppress hello for 0 neighbor(s)

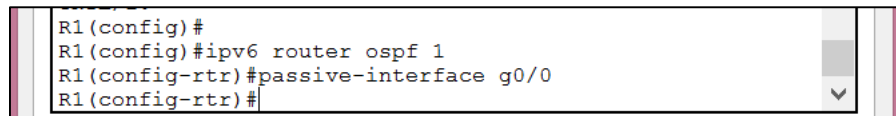


```
R1#  
R1#show ipv6 ospf interface g0/0  
GigabitEthernet0/0 is up, line protocol is up  
  Link Local Address FE80::1, Interface ID 1  
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1  
  Network Type BROADCAST, Cost: 1  
  Transmit Delay is 1 sec, State DR, Priority 1  
  Designated Router (ID) 1.1.1.1, local address FE80::1  
  No backup designated router on this network  
  Timer intervals configured, Hello 10, Dead 40, Wait  
  40, Retransmit 5  
    Hello due in 00:00:07  
  Index 1/1, flood queue length 0  
  Next 0x0(0)/0x0(0)  
  Last flood scan length is 1, maximum is 1  
  Last flood scan time is 0 msec, maximum is 0 msec  
  Neighbor Count is 0, Adjacent neighbor count is 0  
  Suppress hello for 0 neighbor(s)  
R1#
```

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

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

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



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

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

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

```
GigabitEthernet0/0 is up, line protocol is up
```

```
  Link Local Address FE80::1, Interface ID 3
```

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

```
  Network Type BROADCAST, Cost: 1
```

```
  Transmit Delay is 1 sec, State WAITING, Priority 1
```

```
  No designated router on this network
```

```
  No backup designated router on this network
```

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

No Hellos (Passive interface)

Wait time before Designated router selection 00:00:34

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

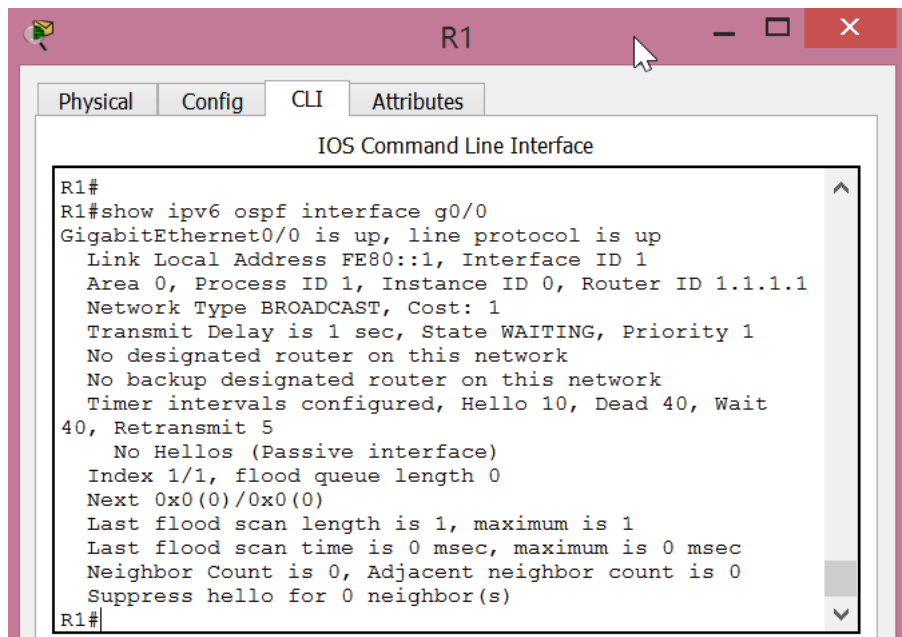
Next 0x0(0)/0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)



```
R1#
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait
  40, Retransmit 5
  No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1#
```

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

R2# show ipv6 route ospf

IPv6 Routing Table - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

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

via FE80::1, Serial0/0/0

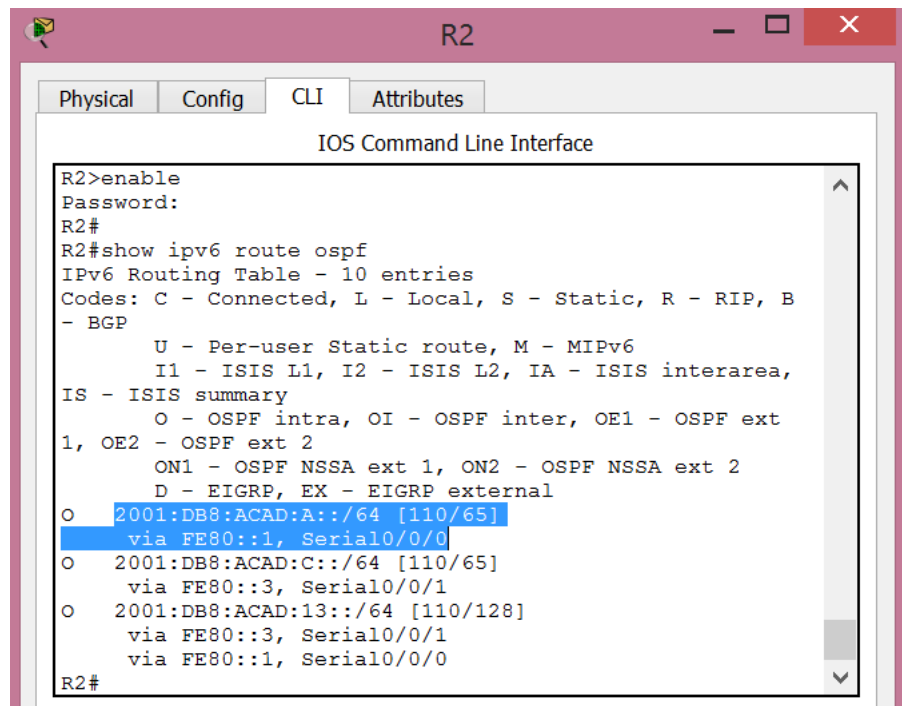
O 2001:DB8:ACAD:C::/64 [110/65]

via FE80::3, Serial0/0/1

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

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0



```
R2>enable
Password:
R2#
R2#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B
- BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea,
IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext
1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:13::/64 [110/128]
  via FE80::3, Serial0/0/1
  via FE80::1, Serial0/0/0
R2#
```

The screenshot shows the CLI of router R3. The user has entered the command `R3#show ipv6 route ospf`. The output displays the IPv6 routing table with 10 entries. The first entry is highlighted in blue: `O 2001:DB8:ACAD:A::/64 [110/65] via FE80::1, Serial0/0/0`. Other entries include routes for 2001:DB8:ACAD:B::/64 and 2001:DB8:ACAD:12::/64.

Establecer la interfaz pasiva como la interfaz predeterminada en el router.

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

The screenshot shows the CLI of router R2. The user has entered the commands `R2(config)# ipv6 router ospf 1` and `R2(config-rtr)# passive-interface default`. The output shows the status of the OSPFv3 process, indicating that the interfaces are down or detached.

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

```

R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
3.3.3.3         0    FULL/ -        00:00:31   3            Serial0/0/1
R1#

```

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

R2# show ipv6 ospf interface s0/0/0

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

Link Local Address FE80::2, Interface ID 6

Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2

Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

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

No Hellos (Passive interface)

Graceful restart helper support enabled

Index 1/2/2, flood queue length 0

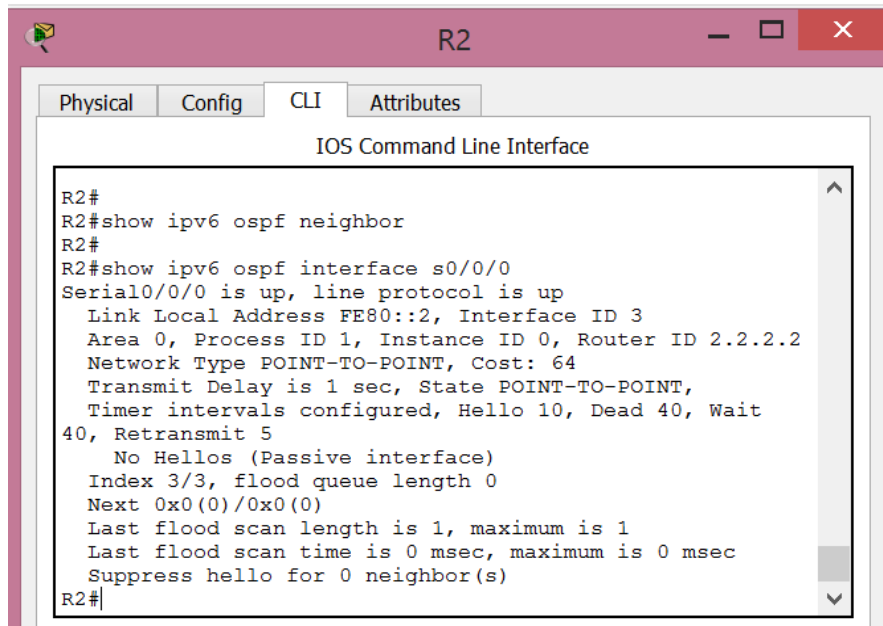
Next 0x0(0)/0x0(0)/0x0(0)

Last flood scan length is 2, maximum is 3

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

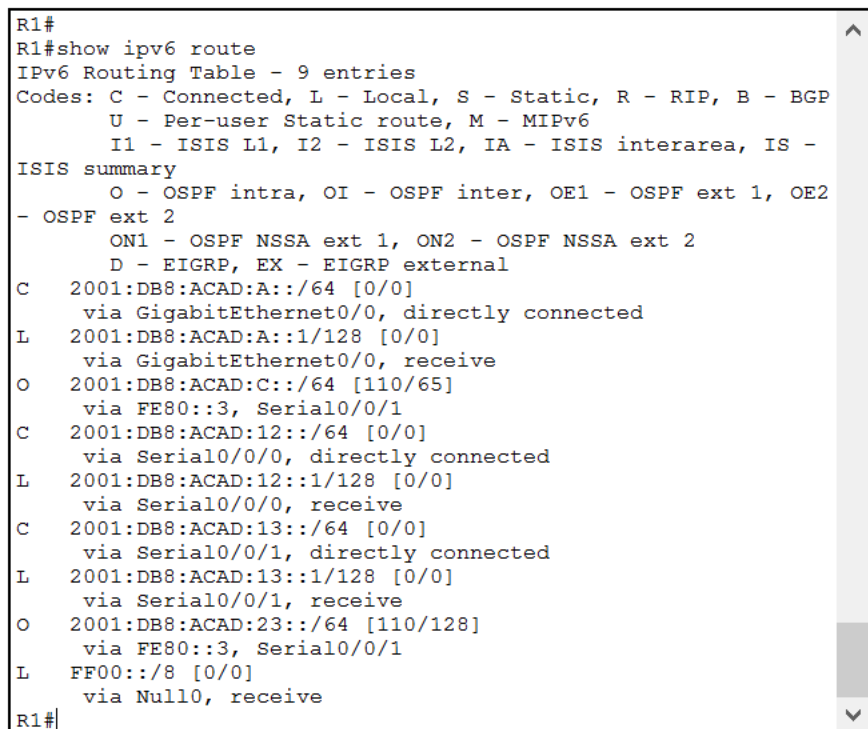
Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)



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

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



```
R1#
R1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS -
ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2
- OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:C::/64 [110/65]
via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
via Serial0/0/0, receive
C 2001:DB8:ACAD:13::/64 [0/0]
via Serial0/0/1, directly connected
L 2001:DB8:ACAD:13::1/128 [0/0]
via Serial0/0/1, receive
O 2001:DB8:ACAD:23::/64 [110/128]
via FE80::3, Serial0/0/1
L FF00::/8 [0/0]
via Null0, receive
R1#
```

```

R3#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B
- BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea,
IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext
1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
O  2001:DB8:ACAD:A::/64 [110/65]
   via FE80::1, Serial0/0/0
C  2001:DB8:ACAD:C::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:C::3/128 [0/0]
   via GigabitEthernet0/0, receive
O  2001:DB8:ACAD:12::/64 [110/128]
   via FE80::1, Serial0/0/0
C  2001:DB8:ACAD:13::/64 [0/0]
   via Serial0/0/0, directly connected
L  2001:DB8:ACAD:13::3/128 [0/0]
   via Serial0/0/0, receive
C  2001:DB8:ACAD:23::/64 [0/0]
   via Serial0/0/1, directly connected
L  2001:DB8:ACAD:23::3/128 [0/0]
   via Serial0/0/1, receive
L  FF00::/8 [0/0]
   via Null0, receive
R3#

```

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
```

```

R2(config)#
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
02:25:46: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-rtr)#

```

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?

Usa la interface Serial0/0/1

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

La métrica es de 129

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
- ISIS summary
  O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1,
OE2 - OSPF ext 2
  ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
  D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
  via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:B::/64 [110/129]
  via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
  via Serial0/0/0, receive
C 2001:DB8:ACAD:13::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:13::1/128 [0/0]
  via Serial0/0/1, receive
O 2001:DB8:ACAD:23::/64 [110/128]
  via FE80::3, Serial0/0/1
L FF00::/8 [0/0]
  via Null0, receive
R1#show ipv6 ospf neighbor

Neighbor ID      Pri  State           Dead Time
Interface ID    Interface
3.3.3.3          0   FULL/ -         00:00:37    3
Serial0/0/1
R1#
```

```
R2#
R2#show ipv6 ospf neighbor

Neighbor ID      Pri  State           Dead Time
Interface ID    Interface
3.3.3.3          0   FULL/ -         00:00:33    4
Serial0/0/1
R2#
```

```
R3#
R3#show ipv6 ospf neighbor

Neighbor ID      Pri  State           Dead Time  Interface ID
Interface
2.2.2.2          0   FULL/ -         00:00:30    4
Serial0/0/1
1.1.1.1          0   FULL/ -         00:00:30    4
Serial0/0/0
R3#
```

¿El R2 aparece como vecino OSPFv3 en el R1? NO

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

¿Qué indica esta información?

Todo el tráfico que va hacia la red “B” desde R1 será enrutado a través de R3. La interface serial 0/0/0 de R2 está aún configurada como pasiva, entonces OSPFv3 no manda información de ruteo notificándose a través de esta interface.

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

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface S0/0/0
R2(config-rtr)#
03:11:59: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-rtr)#
```

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

```
R2#show ipv6 ospf neighbor
Neighbor ID      Pri  State           Dead Time
Interface ID    Interface
1.1.1.1          0   FULL/ -         00:00:35   3
Serial0/0/0
3.3.3.3          0   FULL/ -         00:00:33   4
Serial0/0/1
R2#
```

Reflexión

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

Si se puede, por que el proceso de OSPFv3 solo es usado localmente en el router y no afecta a los demás routers, ya que no necesita coincidir con el proceso usado en otros routers en el área OSPFv3.

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

Eliminando la entrada network ayuda a prevenir los errores en las direcciones IPV6.

9.2.1.10 Packet Tracer: configuración de ACL estándar

Topología

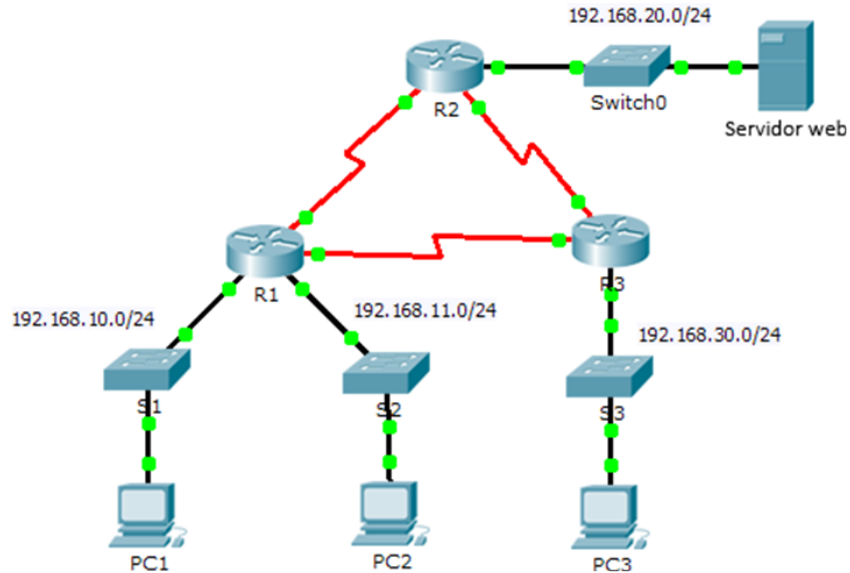


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1

PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Información básica/situación

Las listas de control de acceso (ACL) estándar son scripts de configuración del router que controlan si un router permite o deniega paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, incluidas las direcciones IP y el routing del protocolo de routing de gateway interior mejorado (EIGRP).

Parte 1: planificar una implementación de ACL

Paso 1: investigar la configuración actual de red.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tenga conectividad completa. Elija una computadora y haga ping a otros dispositivos en la red para verificar que la red tenga plena conectividad.

Debería poder hacer ping correctamente a todos los dispositivos.

```
PC1
Physical Config Desktop Programming Attributes
Símbolo del Sistema X
C:\>
C:\>
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time=1ms TTL=127
Reply from 192.168.11.10: bytes=32 time=1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=10ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 5ms

C:\>
```

```
PC1
Physical Config Desktop Programming Attributes
Símbolo del Sistema X
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 5ms

C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=2ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=1ms TTL=254
Reply from 10.1.1.2: bytes=32 time=1ms TTL=254
Reply from 10.1.1.2: bytes=32 time=1ms TTL=254
Reply from 10.1.1.2: bytes=32 time=2ms TTL=254

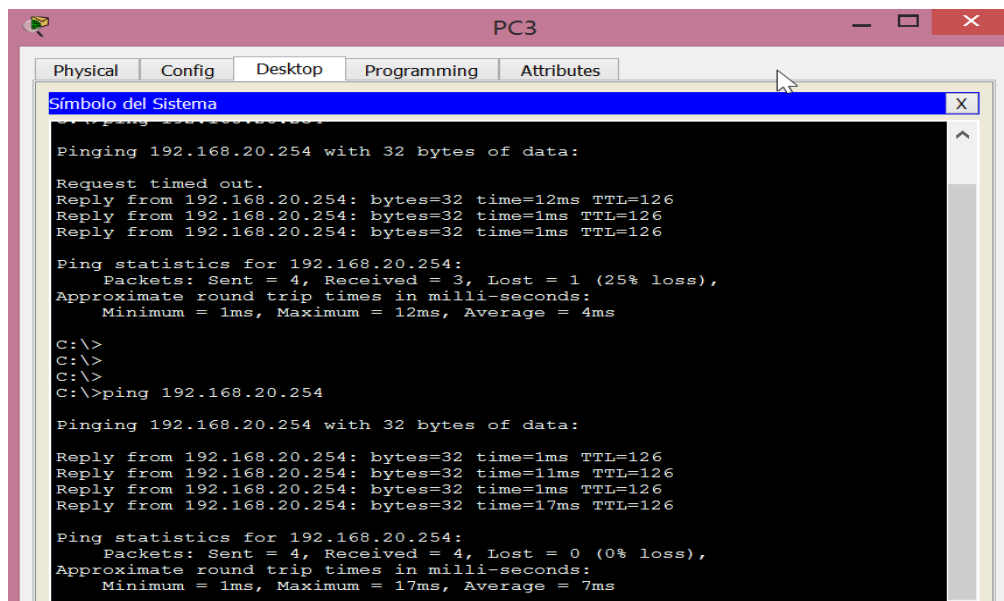
Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
C:\>ping 10.3.3.1

Pinging 10.3.3.1 with 32 bytes of data:

Reply from 10.3.3.1: bytes=32 time=1ms TTL=255
Reply from 10.3.3.1: bytes=32 time<1ms TTL=255
Reply from 10.3.3.1: bytes=32 time<1ms TTL=255
Reply from 10.3.3.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.3.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



```
PC3
Physical Config Desktop Programming Attributes
Símbolo del Sistema
Pinging 192.168.20.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.254: bytes=32 time=12ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms

C:\>
C:\>
C:\>
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=11ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=17ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 17ms, Average = 7ms
```

Paso 2: evaluar dos políticas de red y planificar las implementaciones de ACL.

a. En el **R2** están implementadas las siguientes políticas de red:

- La red 192.168.11.0/24 no tiene permiso para acceder al **servidor web** en la red 192.168.20.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.11.0/24 al **servidor web** en 192.168.20.254 sin interferir con otro tráfico, se debe crear una ACL en el **R2**. La lista de acceso se debe colocar en la interfaz de salida hacia el **servidor web**. Se debe crear una segunda regla en el **R2** para permitir el resto del tráfico.

b. En el **R3** están implementadas las siguientes políticas de red:

- La red 192.168.10.0/24 no tiene permiso para comunicarse con la red 192.168.30.0/24.

- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.10.0/24 a la red 192.168.30/24 sin interferir con otro tráfico, se debe crear una lista de acceso en el **R3**. La ACL se debe colocar en la interfaz de salida hacia la **PC3**. Se debe crear una segunda regla en el **R3** para permitir el resto del tráfico.

Parte 2: configurar, aplicar y verificar una ACL estándar

Paso 1: configurar y aplicar una ACL estándar numerada en el R2.

- a. Cree una ACL con el número 1 en el **R2** con una instrucción que deniegue el acceso a la red 192.168.20.0/24 desde la red 192.168.11.0/24.

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

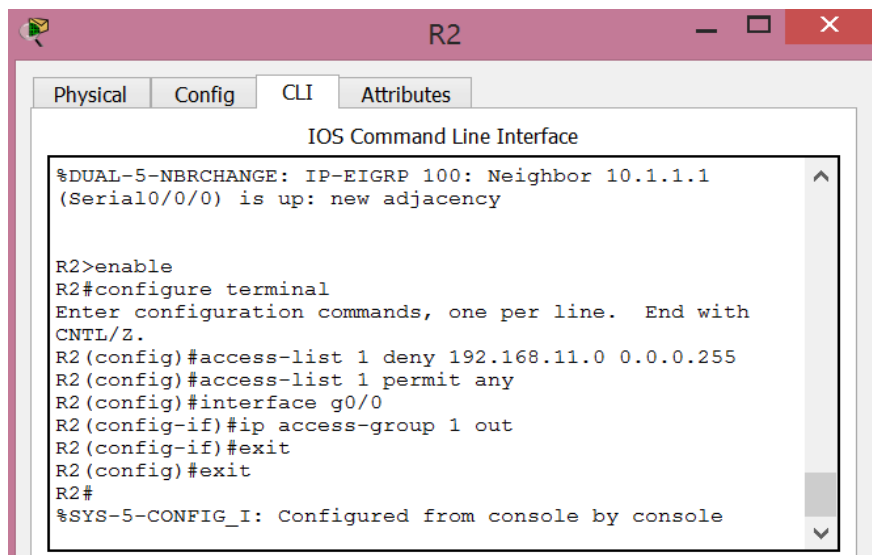
- b. De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con una regla. Para permitir el resto del tráfico, configure la siguiente instrucción:

```
R2(config)# access-list 1 permit any
```

- c. Para que la ACL realmente filtre el tráfico, se debe aplicar a alguna operación del router. Para aplicar la ACL, colóquela en la interfaz Gigabit Ethernet 0/0 para el tráfico saliente.

```
R2(config)# interface GigabitEthernet0/0
```

```
R2(config-if)# ip access-group 1 out
```



```
R2
Physical Config CLI Attributes
IOS Command Line Interface
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1
(Serial0/0/0) is up: new adjacency

R2>enable
R2#configure terminal
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 g0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 2: configurar y aplicar una ACL estándar numerada en el R3.

- Cree una ACL con el número 1 en el **R3** con una instrucción que deniegue el acceso a la red 192.168.30.0/24 desde la red de la **PC1** (192.168.10.0/24).

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

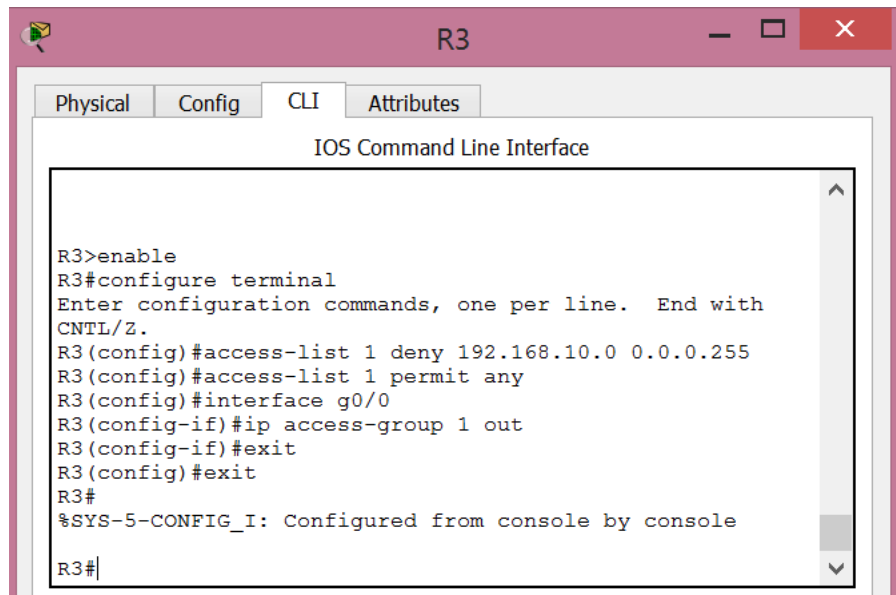
- De manera predeterminada, las ACL deniegan todo el tráfico que no coincide con una regla. Para permitir el resto del tráfico, cree una segunda regla para la ACL 1.

```
R3(config)# access-list 1 permit any
```

- Para aplicar la ACL, colóquela en la interfaz Gigabit Ethernet 0/0 para el tráfico saliente.

```
R3(config)# interface GigabitEthernet0/0
```

```
R3(config-if)# ip access-group 1 out
```



```
R3
R3>enable
R3#configure terminal
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 g0/0
R3 (config-if)#ip access-group 1 out
R3 (config-if)#exit
R3 (config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

Paso 3: verificar la configuración y la funcionalidad de la ACL.

- En el **R2** y el **R3**, introduzca el comando **show access-list** para verificar las configuraciones de la ACL. Introduzca el comando **show run** o **show ip interface gigabitethernet 0/0** para verificar la colocación de las ACL.

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

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

```
R2#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.20.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is 1
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
```

```
R3#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.30.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is 1
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
```

- b. Una vez colocadas las dos ACL, el tráfico de la red se restringe según las políticas detalladas en la parte 1. Utilice las siguientes pruebas para verificar las implementaciones de ACL:
- Un ping de 192.168.10.10 a 192.168.11.10 se realiza correctamente.
 - Un ping de 192.168.10.10 a 192.168.20.254 se realiza correctamente.
 - Un ping de 192.168.11.10 a 192.168.20.254 falla.
 - Un ping de 192.168.10.10 a 192.168.30.10 falla.
 - Un ping de 192.168.11.10 a 192.168.30.10 se realiza correctamente.
 - Un ping de 192.168.30.10 a 192.168.20.254 se realiza correctamente.

PC1

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
C:\>
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time=1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=11ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms
```

PC1

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```


PC2

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=2ms TTL=126
Reply from 192.168.30.10: bytes=32 time=2ms TTL=126
Reply from 192.168.30.10: bytes=32 time=10ms TTL=126
Reply from 192.168.30.10: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 4ms
```

PC3

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 17ms, Average = 7ms

C:\>
C:\>
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=10ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 3ms

C:\>
```

9.2.1.11 Packet Tracer: configuración de ACL estándar con nombre

Topología

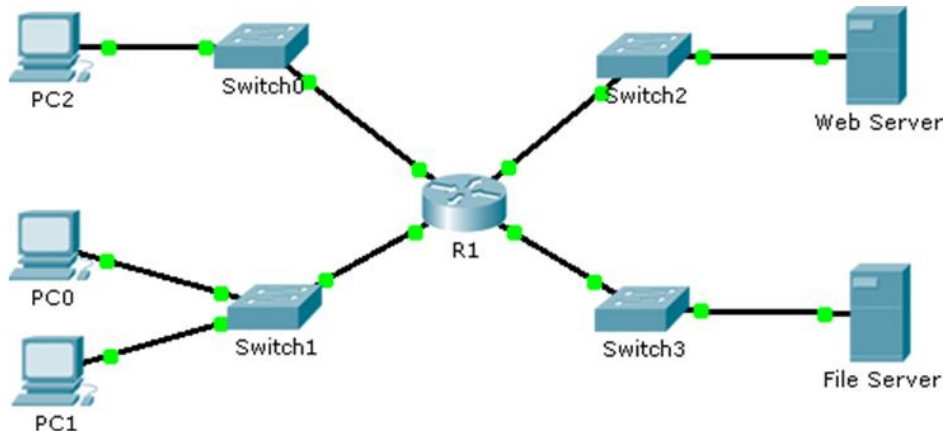


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
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

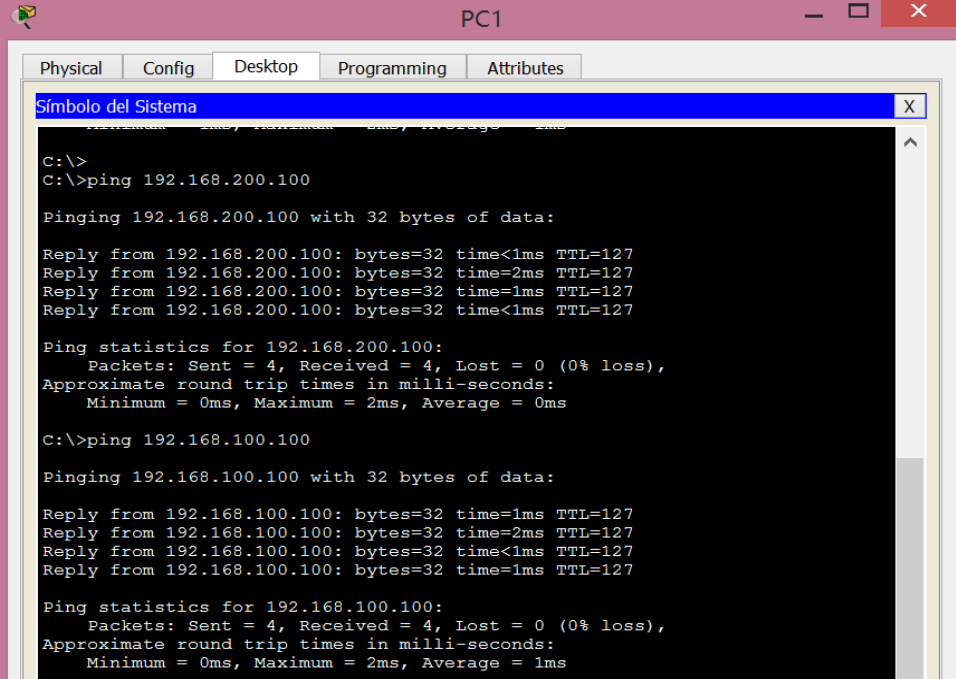
Información básica/situación

El administrador de red sénior le solicitó que cree una ACL estándar con nombre 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**.



```
PC1
-----
Physical  Config  Desktop  Programming  Attributes
Símbolo del Sistema
C:\>
C:\>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=2ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

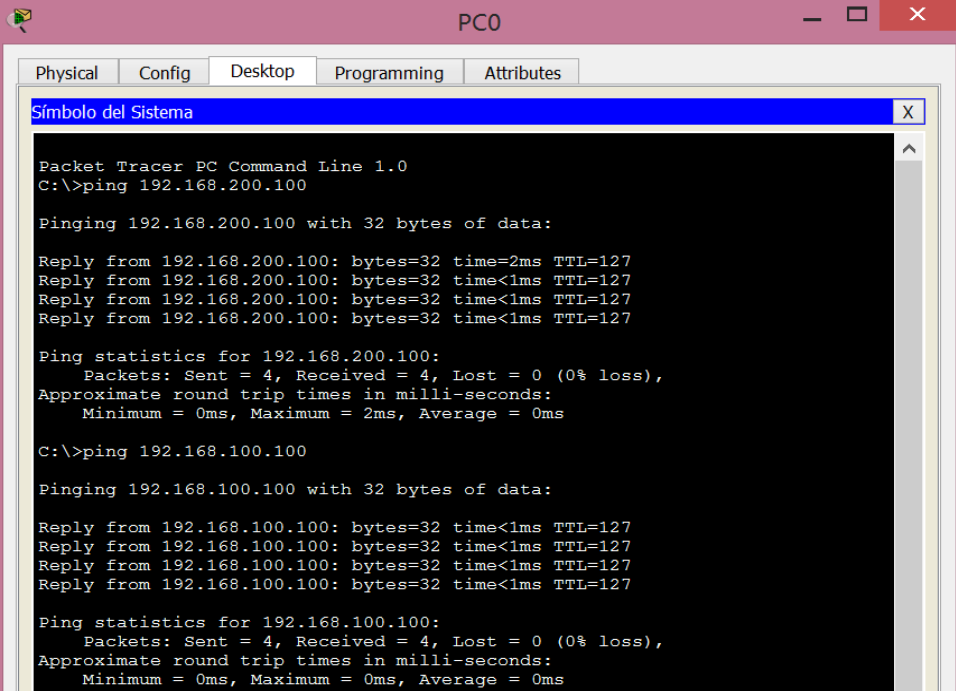
Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>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<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms 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
```



```
PC0
-----
Physical  Config  Desktop  Programming  Attributes
Símbolo del Sistema
Packet Tracer PC Command Line 1.0
C:\>
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=2ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms 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 = 2ms, Average = 0ms

C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms 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
```

The image shows a Packet Tracer PC Command Line window titled "PC2". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, showing a "Símbolo del Sistema" window. The command prompt displays the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms 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

C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms 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 = 1ms, Maximum = 2ms, 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.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1/0,
changed state to up
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
R1(config-std-nacl)#
R1(config-std-nacl)#
```

Paso 3: aplicar la ACL con nombre.

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

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

- b. Guarde la configuración.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#
R1(config)#interface f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Parte 2: verificar la implementación de la ACL

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

Utilice 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 haya aplicado de forma correcta a la interfaz.

```
R1#show access-lists
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.20.4
 20 deny any
R1#
```

```
R1#show ip interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
 Internet address is 192.168.200.1/24
 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 File_Server_Restrictions
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
 IP output packet accounting is disabled
 IP access violation accounting is disabled
 TCP/IP header compression is disabled
 RTP/IP header compression is disabled
 Probe proxy name replies are disabled
 Policy routing is disabled
 Network address translation is disabled
 BGP Policy Mapping is disabled
 Input features: MCI Check
 WCCP Redirect outbound is disabled
 WCCP Redirect inbound is disabled
 WCCP Redirect exclude is disabled
R1#
```

Paso 2: verificar que la ACL funcione correctamente.

Aunque las tres estaciones de trabajo deberían poder hacer ping al **servidor web**, pero sólo **PC1** debería poder hacer ping al **servidor web**.

PC1

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

```
Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\>
C:\>
C:\>
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=4ms 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=1ms 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 = 4ms, Average = 1ms

C:\>
```

PC0

Physical Config Desktop Programming Attributes

Símbolo del Sistema X

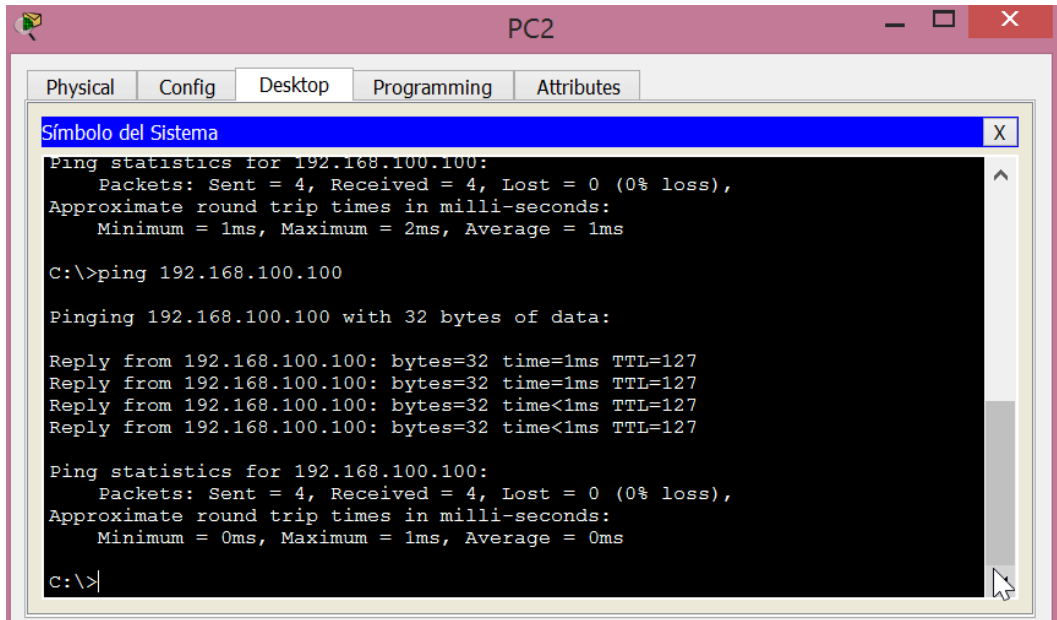
```
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```



```
PC2
Physical Config Desktop Programming Attributes
Símbolo del Sistema
Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

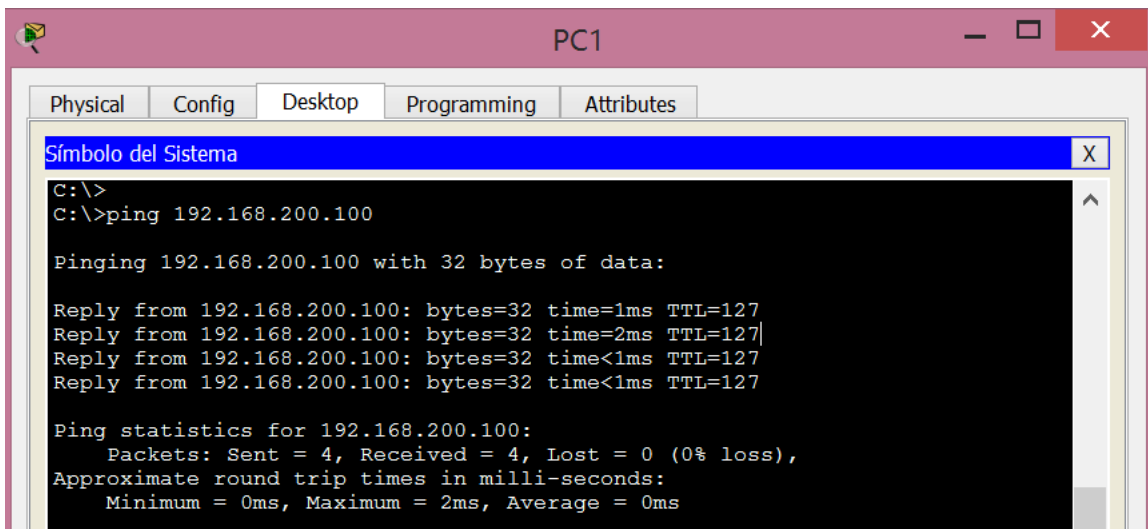
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Se verifica y evidencia que las tres estaciones o PC pueden hacer ping al servidor web.

En las siguientes imágenes se verifica y evidencia que solamente la PC1 puede hacer ping al servidor de archivos.



```
PC1
Physical Config Desktop Programming Attributes
Símbolo del Sistema
C:\>
C:\>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=2ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

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 = 2ms, Average = 0ms
```



```
PC0
Physical Config Desktop Programming Attributes
Símbolo del Sistema X
Packet Tracer PC Command Line 1.0
C:\>
C:\>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),
```

```
PC2
Physical Config Desktop Programming Attributes
Símbolo del Sistema X
Packet Tracer PC Command Line 1.0
C:\>
C:\>ping 192.168.200.100

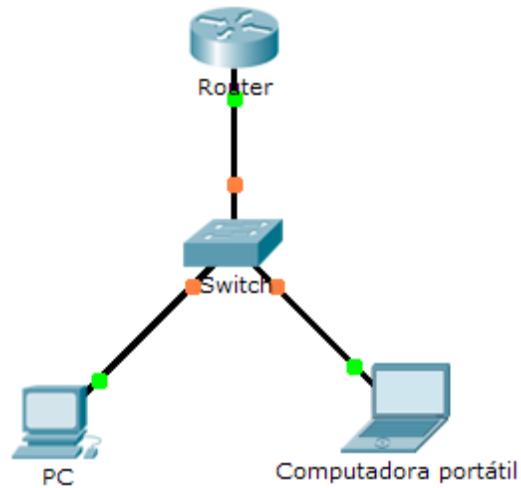
Pinging 192.168.200.100 with 32 bytes of data:

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),
```

9.2.3.3 Packet Tracer: configuración de una ACL en líneas VTY

Topología:

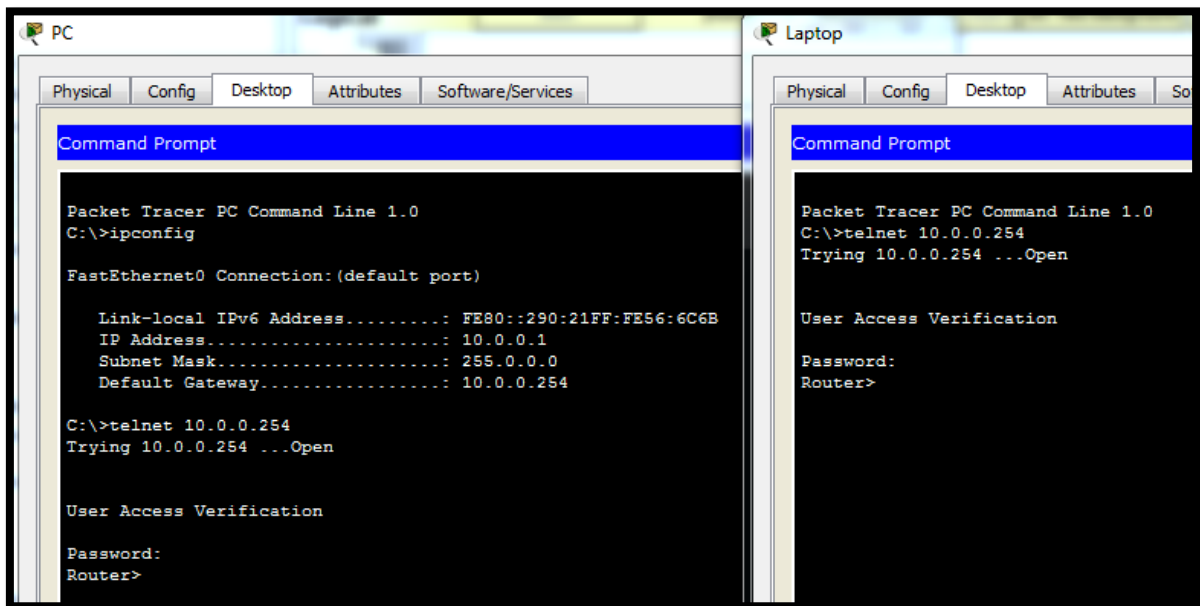


Información básica: Como administrador de red, debe tener acceso remoto al router. Este acceso no debe estar disponible para otros usuarios de la red. Por lo tanto, configurará y aplicará una lista de control de acceso (ACL) que permita el acceso de una computadora (PC) a las líneas Telnet, pero que deniegue el resto de las direcciones IP de origen.

Parte 1: configurar y aplicar una ACL a las líneas VTY

Paso 1: verificar el acceso por Telnet antes de configurar la ACL.

Ambas computadoras deben poder acceder al Router mediante Telnet. La contraseña es cisco.



Paso 2: configurar una ACL estándar numerada.

Configure la siguiente ACL numerada en el Router.

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

Ya que no deseamos permitir el acceso desde ninguna otra computadora, la propiedad de denegación implícita de la lista de acceso cumple nuestros requisitos.

Paso 3: colocar una ACL estándar con nombre en el router.

Se debe permitir el acceso a las interfaces del Router y se debe restringir el acceso por Telnet. Por lo tanto, debemos colocar la ACL en las líneas Telnet que van de 0 a 4. Desde la petición de entrada de configuración del Router, acceda al modo de configuración de línea de las líneas 0 a 4 y utilice el comando access-class para aplicar la ACL a todas las líneas VTY: Router(config)# line vty 0 4 Router(config-line)# access-class 99 in

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#acc
% Incomplete command.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
```

Parte 2: verificar la implementación de la ACL

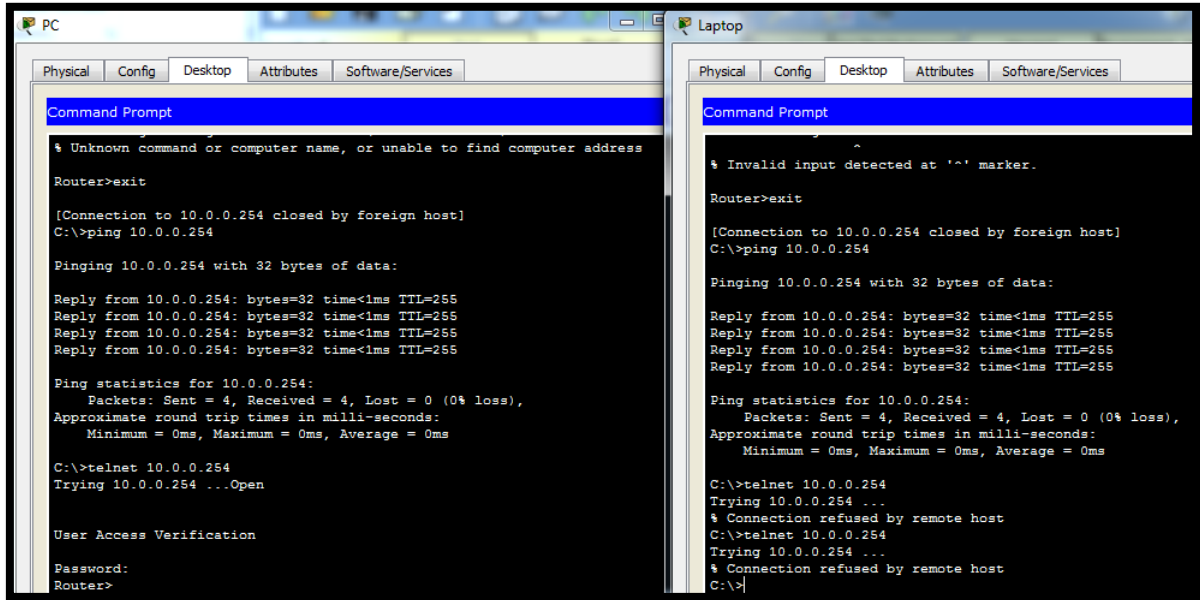
Paso 1: verificar la configuración de la ACL y su aplicación a las líneas VTY.

Utilice el comando show access-lists para verificar la configuración de la ACL. Utilice el comando show run para verificar que la ACL esté aplicada a las líneas VTY.

```
Router(config-line)#do show access-lists
Standard IP access list 99
 10 permit host 10.0.0.1
```

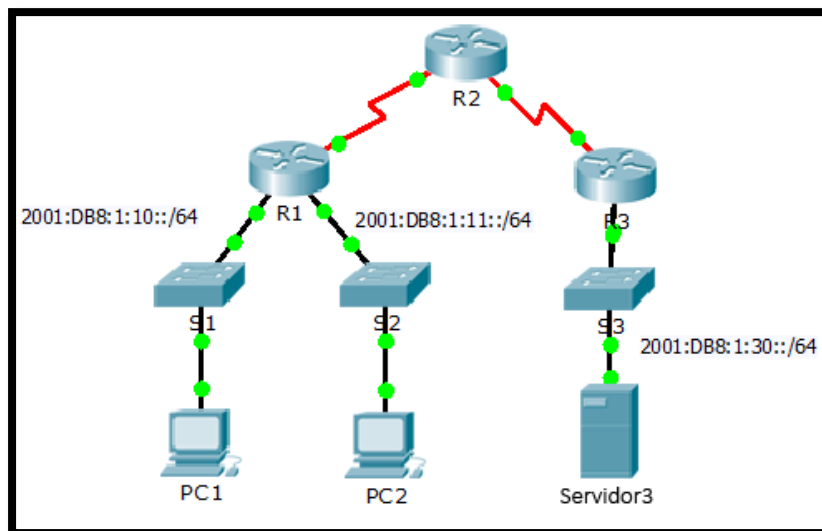
Paso 2: verificar que la ACL funcione correctamente.

Ambas computadoras deben poder hacer ping al Router, pero solo la computadora PC debería poder acceder al Router mediante Telnet.



9.5.2.6 Packet Tracer: configuración de ACL de IPv6

Topología



Parte 1: configurar, aplicar y verificar una ACL de IPv6

Según los registros, una computadora en la red 2001:DB8:1:11::0/64 actualiza repetidamente su página web, lo que ocasiona un ataque por denegación de servicio (DoS) contra el Servidor3. Hasta que se pueda identificar y limpiar el cliente, debe bloquear el acceso HTTP y HTTPS a esa red mediante una lista de acceso.

Paso 1: configurar una ACL que bloquee el acceso HTTP y HTTPS.

Configure una ACL con el nombre BLOCK_HTTP en el R1 con las siguientes instrucciones.

a. Bloquear el tráfico HTTP y HTTPS para que no llegue al Servidor3.

```
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
```

b. Permitir el paso del resto del tráfico IPv6.

```
R1>enable
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list block_http
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq 80
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
```

Paso 2: aplicar la ACL a la interfaz correcta.

Aplice la ACL a la interfaz más cercana al origen del tráfico que se desea bloquear.

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

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

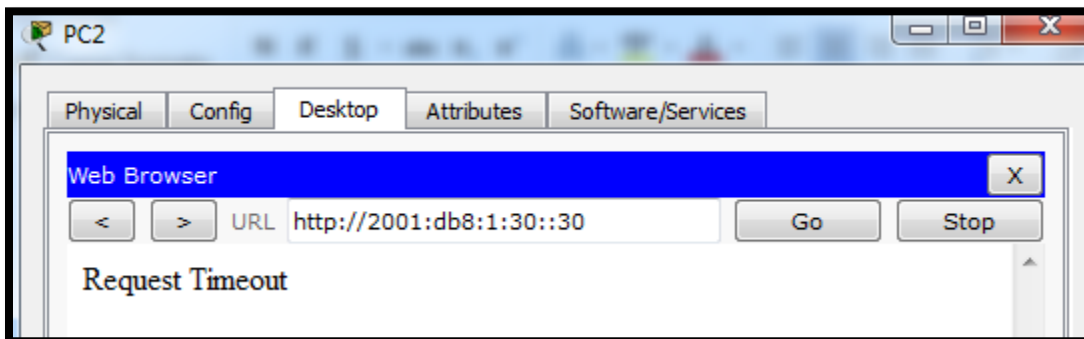
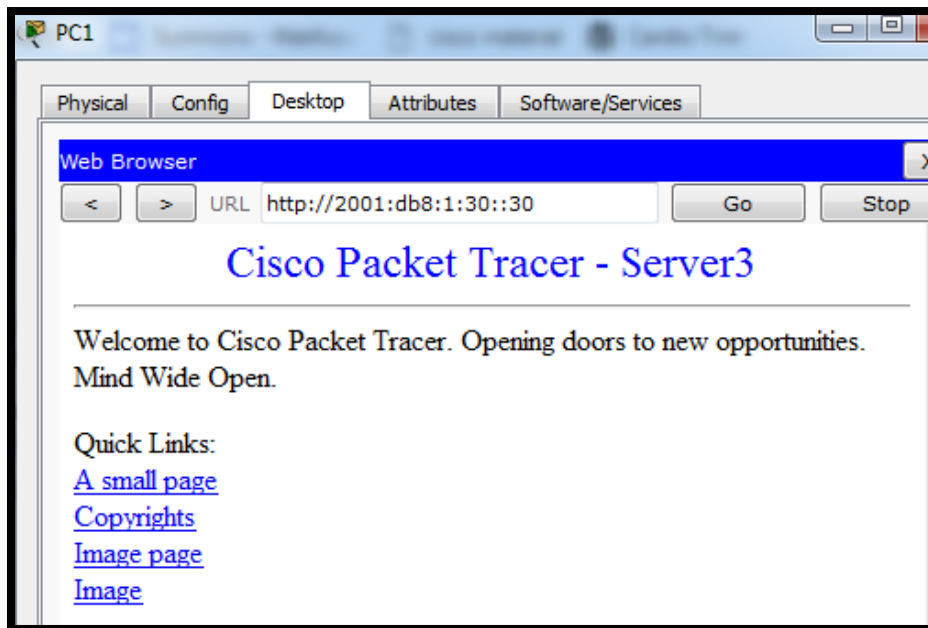
Paso 3: verificar la implementación de la ACL.

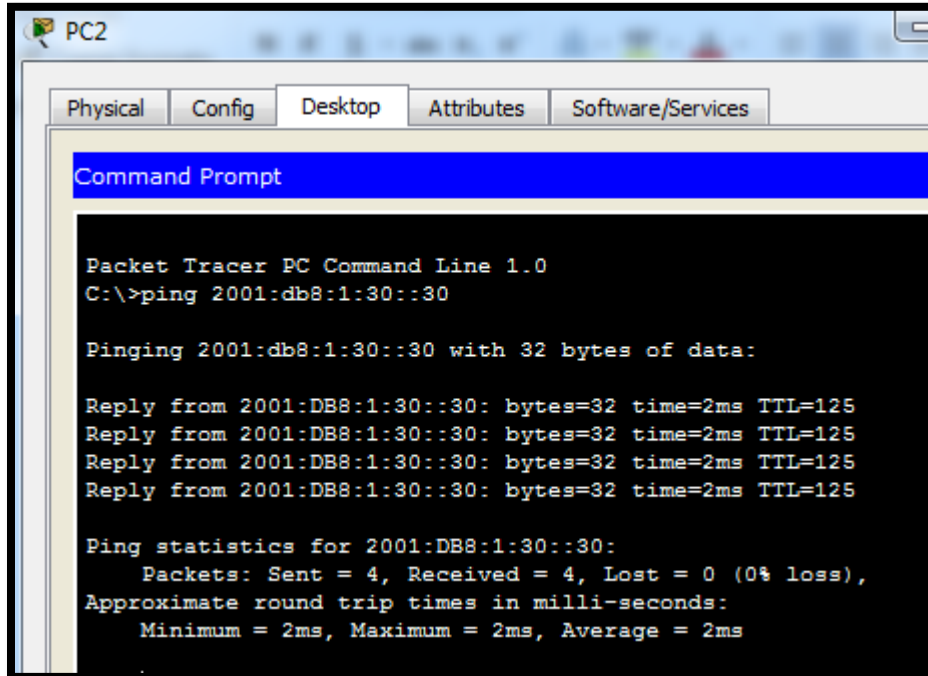
Realice las siguientes pruebas para verificar que la ACL funcione de manera correcta:

- Abra el navegador web de la PC1 con la dirección <http://2001:DB8:1:30::30> o <https://2001:DB8:1:30::30>. Debería aparecer el sitio web.

- Abra el navegador web de la PC2 con la dirección `http://2001:DB8:1:30::30` o `https://2001:DB8:1:30::30`. El sitio web debería estar bloqueado.
- Haga ping de la PC2 a `2001:DB8:1:30::30`. El ping debería realizarse correctamente.

```
R1#show ipv6 access-list
IPv6 access list block_http
deny tcp any host 2001:DB8:1:30::30 eq www
deny tcp any host 2001:DB8:1:30::30 eq 443
permit ipv6 any any
```





```
PC2
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:1:30::30

Pinging 2001:db8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Ahora, en los registros se indica que su servidor recibe pings de diversas direcciones IPv6 en un ataque por denegación de servicio distribuido (DDoS). Debe filtrar las solicitudes de ping ICMP a su servidor.

Paso 1: crear una lista de acceso para bloquear ICMP.

Configure una ACL con el nombre BLOCK_ICMP en el R3 con las siguientes instrucciones:

- a. Bloquear todo el tráfico ICMP desde cualquier host hasta cualquier destino.
- b. Permitir el paso del resto del tráfico IPv6.

```
R3>enable
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list block_icmp
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
```

Paso 2: aplicar la ACL a la interfaz correcta.

En este caso, el tráfico ICMP puede provenir de cualquier origen. Para asegurar que el tráfico ICMP esté bloqueado, independientemente de su origen o de los cambios que se produzcan en la topología de la red, aplique la ACL lo más cerca posible del destino.

```
R3(config-ipv6-acl)#interface gig0/0
R3(config-if)#ipv6 traffic-filter block_icmp out
^
% Invalid input detected at '^' marker.
R3(config-if)#ipv6 traffic-filter block_icmp out
```

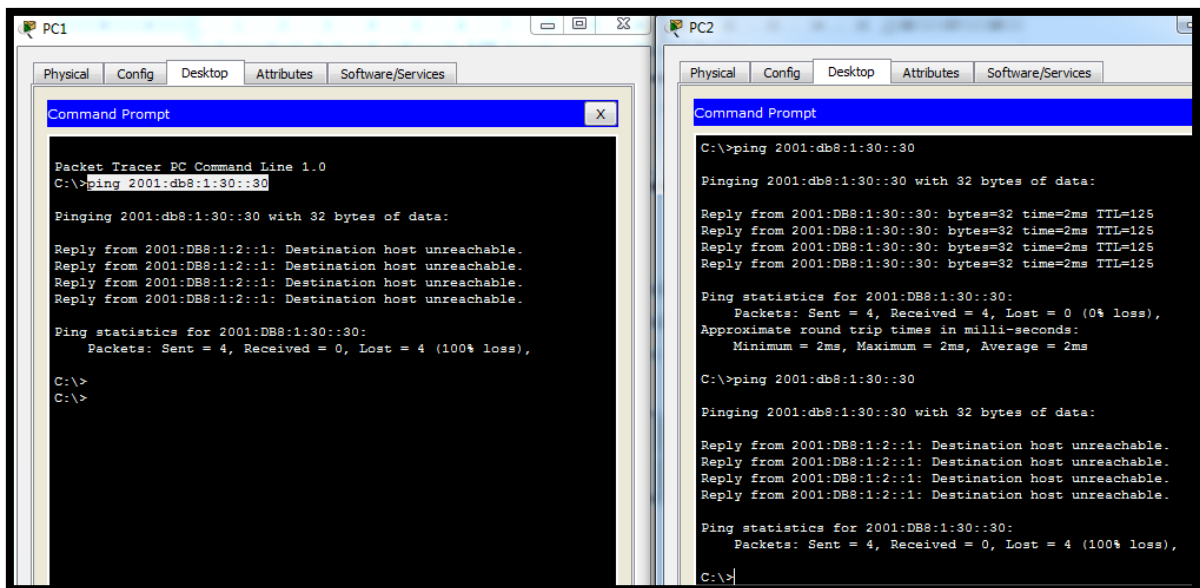
Paso 3: verificar que la lista de acceso adecuada funcione.

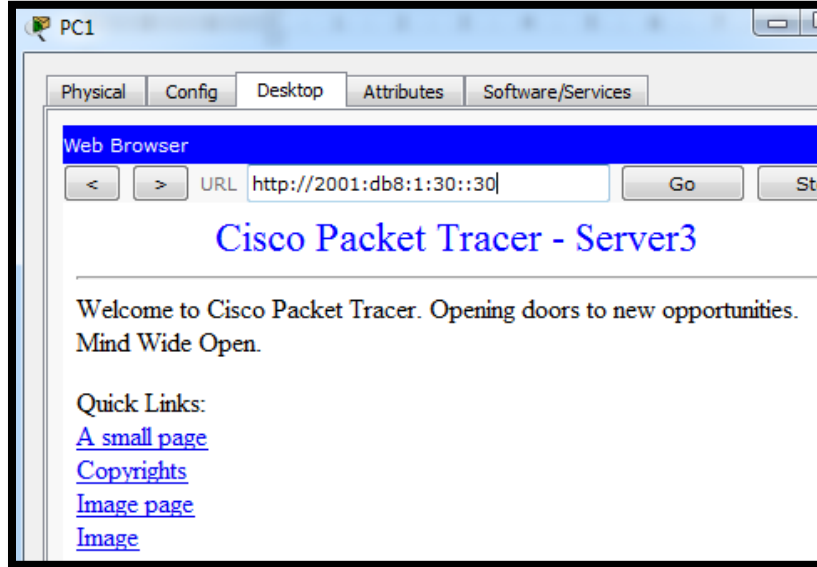
a. Haga ping de la PC2 a 2001:DB8:1:30::30. El ping debe fallar.

b. Haga ping de la PC1 a 2001:DB8:1:30::30. El ping debe fallar.

Abra el navegador web de la PC1 con la dirección <http://2001:DB8:1:30::30> o <https://2001:DB8:1:30::30>. Debería aparecer el sitio web.

```
R3#show ipv6 access-list
IPv6 access list block_icmp
deny icmp any any
permit ipv6 any any
```





10.1.2.4 Práctica de laboratorio: configuración de DHCPv4 básico en un router

Topología

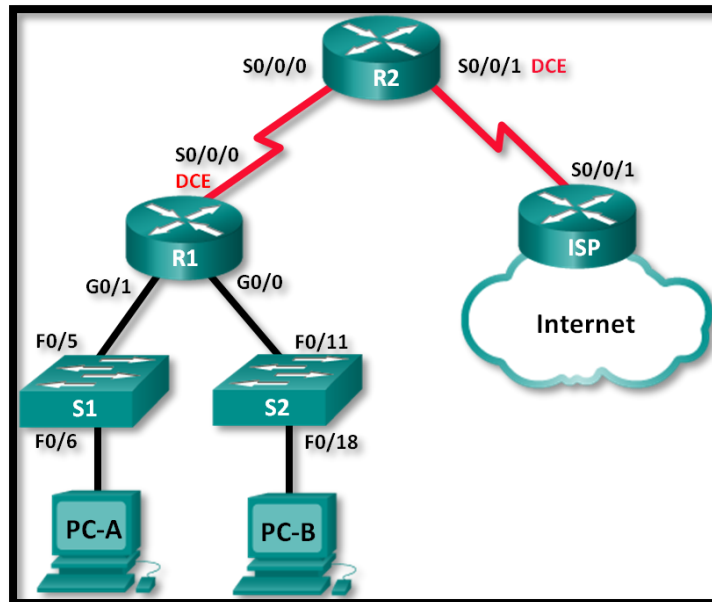


Tabla de direccionamiento

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

Recursos necesarios

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

2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

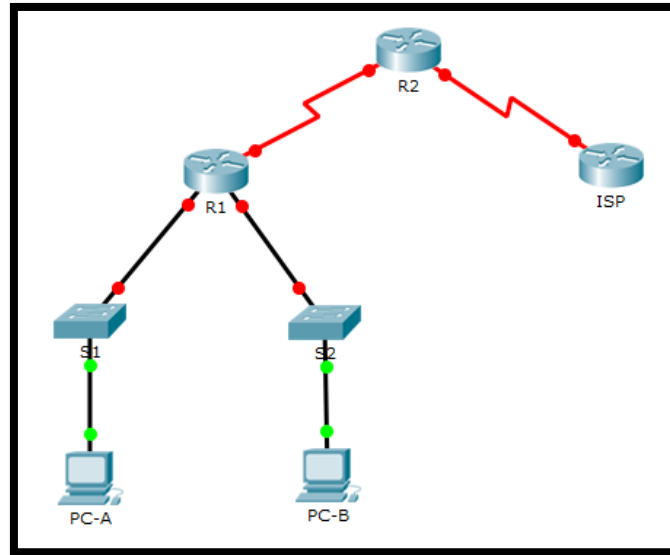
Cables Ethernet y seriales, como se muestra en la topología

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

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

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

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



Paso 3 configurar los parámetros básicos para cada router.

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

```
Router(config)#hostname R1
R1(config)#interface g0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
^
% Invalid input detected at '^' marker.

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

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

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

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

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

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

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

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

```

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

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

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

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

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

```

```

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

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

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

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

```

h) Configure EIGRP for R1.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Paso 4 verificar la conectividad de red entre los routers.

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

```
R1#ping 192.168.2.254

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

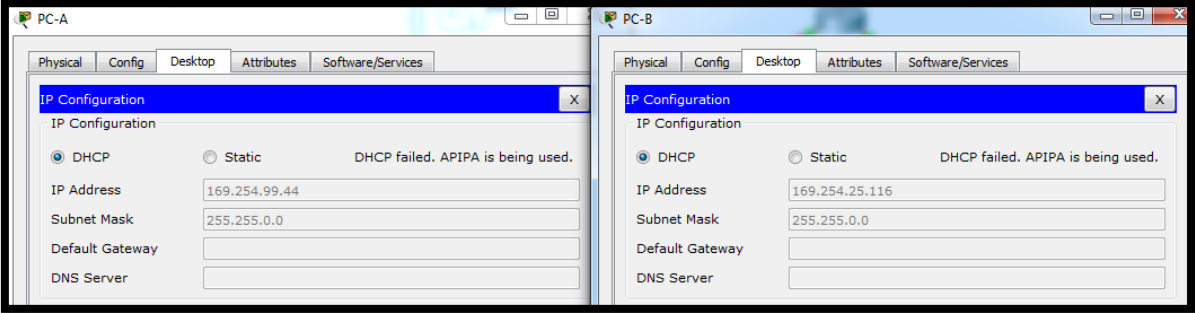
R1#ping 209.165.200.225

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

```
R2#ping 209.165.200.225

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

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



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

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

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

En el R2, configure un conjunto de direcciones DHCP para cada LAN del R1. Utilice el nombre de conjunto **R1G0** para G0/0 LAN y **R1G1** para G0/1 LAN. Asimismo, configure las direcciones que se excluirán de los conjuntos de direcciones. La práctica recomendada indica que primero se deben configurar las direcciones excluidas, a fin de garantizar que no se arrienden accidentalmente a otros dispositivos.

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

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

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

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

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

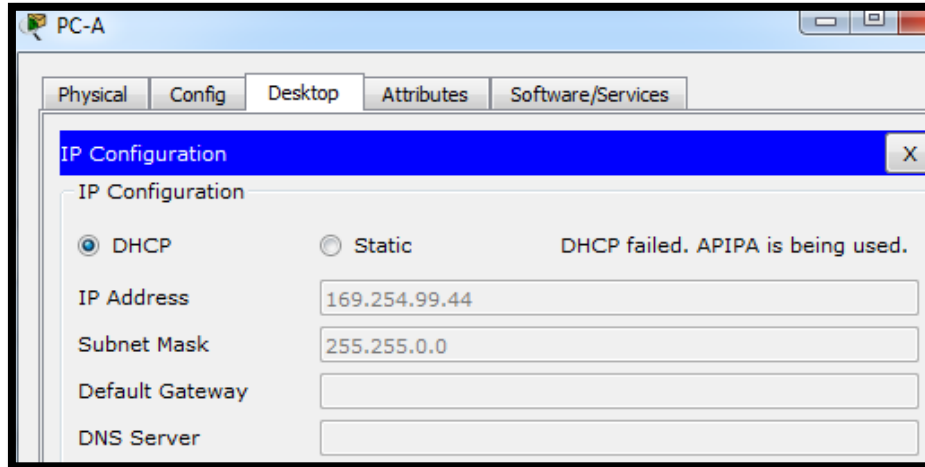
R2(dhcp-config)#lease 2
^
% Invalid input detected at '^' marker.

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

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

R2(dhcp-config)#exit
```

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



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

Paso 2 configurar el R1 como agente de retransmisión DHCP.

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

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

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

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

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

PC-A

Physical Config Desktop Attributes Software/Services

Command Prompt

```
Link-local IPv6 Address.....: FE80::207:ECFF:FE74:632C
Autoconfiguration IP Address....: 169.254.99.44
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....:
00-01-00-01-1A-06-96-6D-00-07-EC-74-63-2C

C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0007.EC74.632C
Link-local IPv6 Address.....: FE80::207:ECFF:FE74:632C
IP Address.....: 192.168.1.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 209.165.200.225
DHCP Servers.....: 192.168.2.254
DHCPv6 Client DUID.....:
00-01-00-01-1A-06-96-6D-00-07-EC-74-63-2C
```

PC-B

Physical Config Desktop Attributes Software/Services

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0001.63DA.1974
Link-local IPv6 Address.....: FE80::201:63FF:FEDA:1974
IP Address.....: 192.168.0.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.0.1
DNS Servers.....: 209.165.200.225
DHCP Servers.....: 192.168.2.254
DHCPv6 Client DUID.....: 00-01-00-01-C3-E1-
CE-1E-00-01-63-DA-19-74
```

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

192.168.1.10 y 192.168.0.10

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

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

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

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

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

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

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

Comando no soportado por packet tracer.

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

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

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

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

```

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

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

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

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

```

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

```

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

```

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

```

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

```

```

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

```

Reflexión

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

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

Ejercicio 10.1.2.5 configuración de dhcpv4 básico en un switch

Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.22 5	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

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.

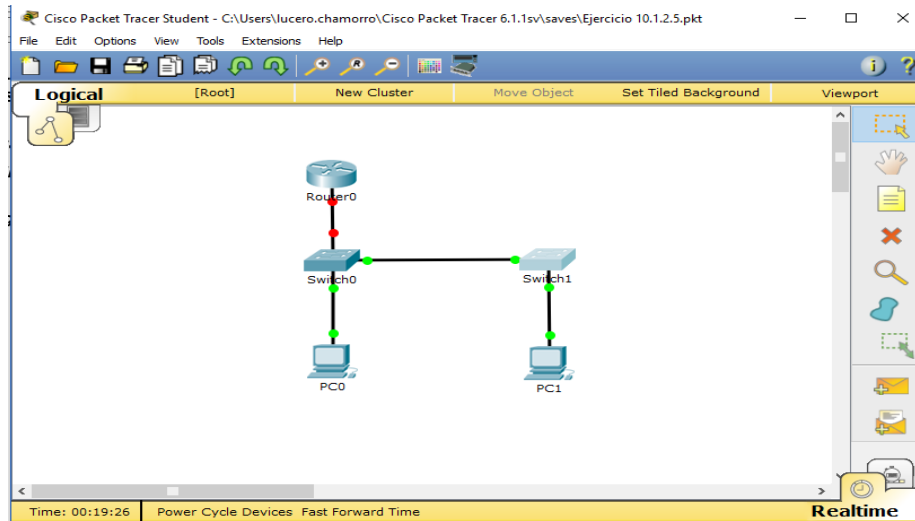
Nota: asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

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

Parte 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.

Paso 3 Configurar los parámetros básicos en los dispositivos.

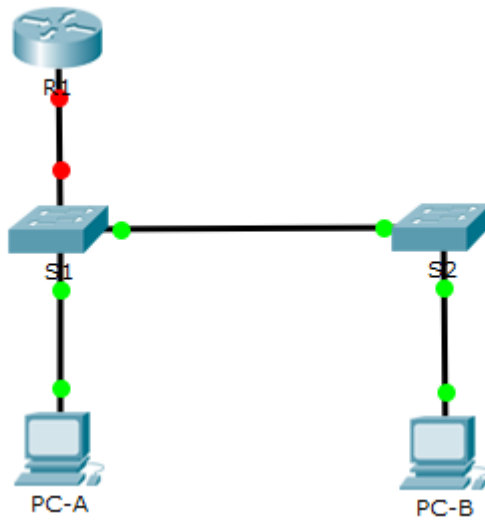
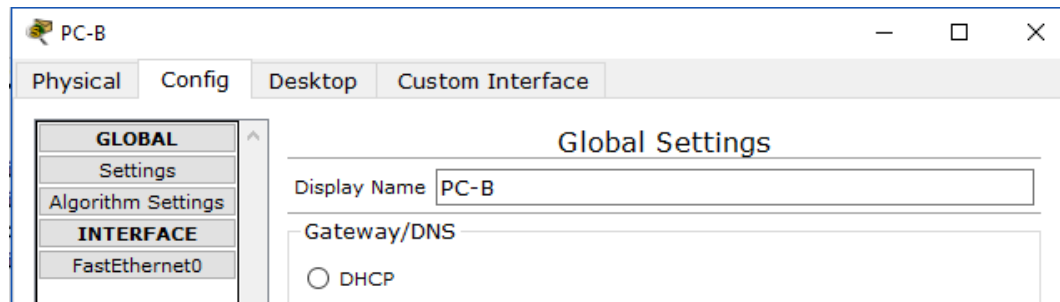
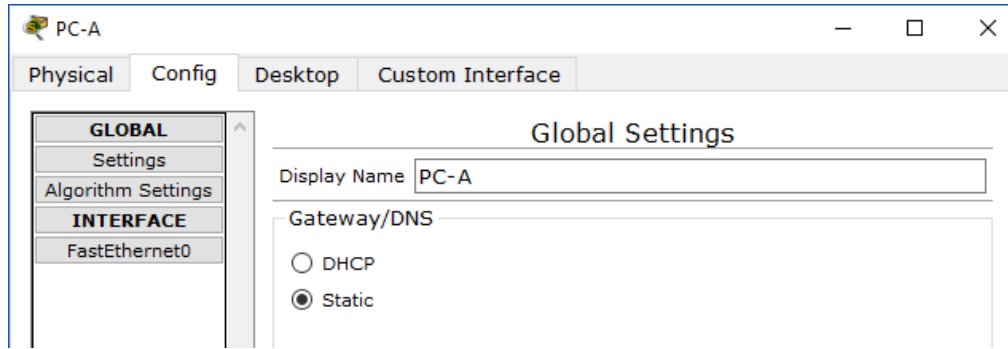
- a. Asigne los nombres de dispositivos como se muestra en la topología.

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

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
```

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
^
% Invalid input detected at '^' marker.

Switch(config)#hostname S2
S2(config)#
```

- b. Desactive la búsqueda del DNS.

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#
```

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

```
R1(config)#enable password class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

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

```
R1(config)#interface g0/1
R1(config-if)#ip address 192.168.1.10 255.255.255.0
R1(config-if)#no shutdown

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

R1(config-if)#
```

```
R1(config-if)#exit
R1(config)#interface lo0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

IP de las interfaces configuradas

```
R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/1 192.168.1.10   YES manual up          down
Loopback0          209.165.200.225 YES manual up          up
Vlan1              unassigned      YES unset  administratively down down
R1#
```

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

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 2
S1(config-if)#ip address 192.168.2.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#exit
```

Vlan1	192.168.1.1	YES manual up	up
Vlan2	192.168.2.1	YES manual down	down

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

```
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Parte 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.

Paso 1 Mostrar la preferencia de SDM en el S1.

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

S1# show sdm prefer

The current template is "default" template.

The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

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

¿Cuál es la plantilla actual?

Paso 2 Cambiar la preferencia de SDM en el S1.

- 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?

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

S1# reload

System configuration has been modified. Save? [yes/no]: no

Proceed with reload? [confirm]

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

Paso 3 Verificar que la plantilla lanbase-routing esté cargada.

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

S1# show sdm prefer

The current template is "lanbase-routing" template.

The selected template optimizes the resources in

the switch to support this level of features for

0 routed interfaces and 255 VLANs.

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

number of IPv4/MAC qos aces: 0.125k
number of IPv4/MAC security aces: 0.375k
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 0.375k
number of IPv6 security aces: 127

Parte 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.

Paso 1 Configurar DHCP para la VLAN 1.

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

R/ el comando es **ip dhcp excluded-address 192.168.1.1 192.168.1.10**

```
S1> enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#
```

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

R/ El comando es **ip dhcp pool LAN-POOL-1**

```
S1(config)#ip dhcp pool LAN-POOL-1
S1(dhcp-config)#
```

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

R/ El comando es **network 192.168.1.0 255.255.255.0**

```
S1(config)#ip dhcp pool LAN-POOL-1
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#
```

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

R/ El comando es **default-router 192.168.1.1**

```
S1(config)#ip dhcp pool LAN-POOL-1
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.1.1
S1(dhcp-config)#
```

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

R/ El comando es **dns-server 192.168.1.9**

```
S1(dhcp-config)#dns-server 192.168.1.9
S1(dhcp-config)#
```

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

R/ el comando es lease 3

```
S1(dhcp-config)#lease 3
^
% Invalid input detected at '^' marker.

S1(dhcp-config)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

El comando no es soportado por el packet tracer

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

R/ El comando es **copy running-config startup-config**

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Paso 2 Verificar la conectividad y DHCP.

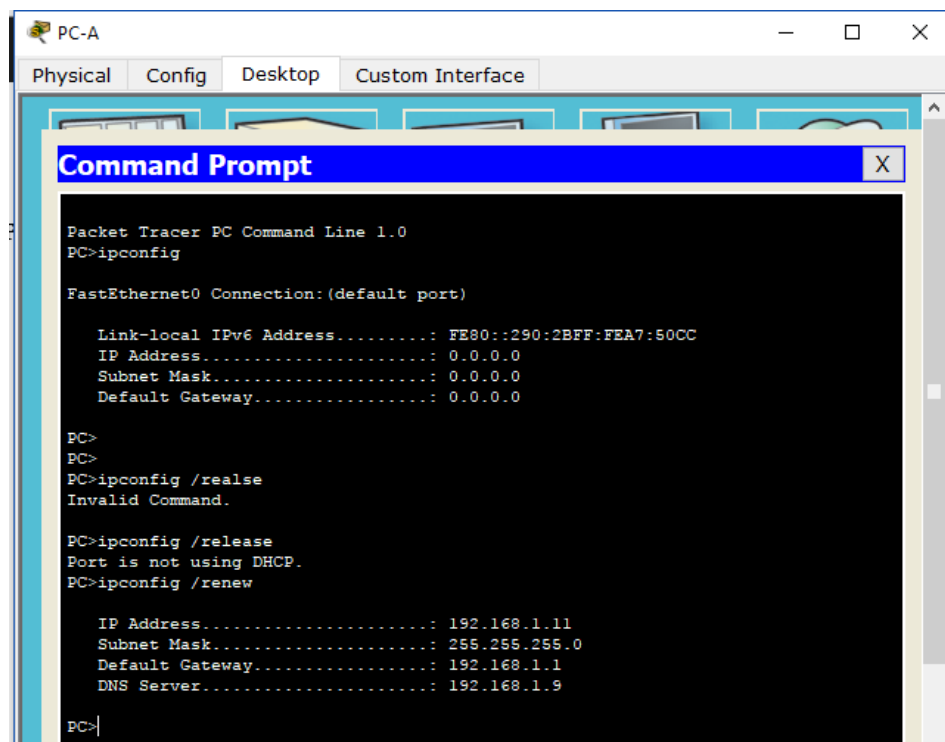
- a. En la PC-A y la PC-B, abra el símbolo del sistema y emita el comando ipconfig. Si la información de IP no está presente, o si está incompleta, emita el comando ipconfig /release, seguido del comando ipconfig /renew.

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.1.11

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.1.1**



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::290:2BFF:FEA7:50CC
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

PC>
PC>
PC>ipconfig /realse
Invalid Command.

PC>ipconfig /release
Port is not using DHCP.
PC>ipconfig /renew

IP Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Server.....: 192.168.1.9

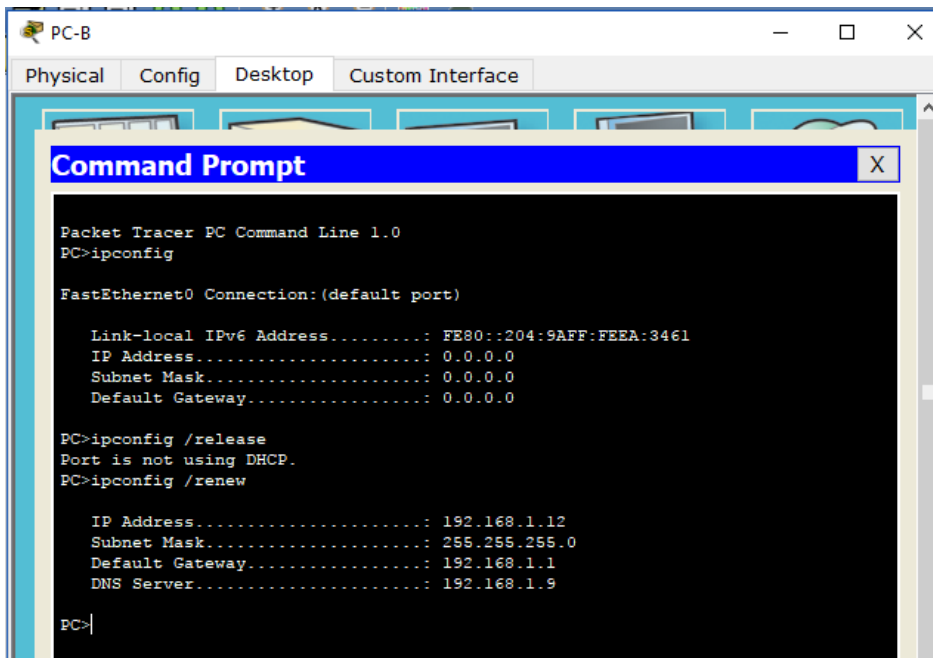
PC>
```


Para la PC-B, incluya lo siguiente:

Dirección IP: **192.168.1.12**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.1.1**



```
PC-B
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default port)

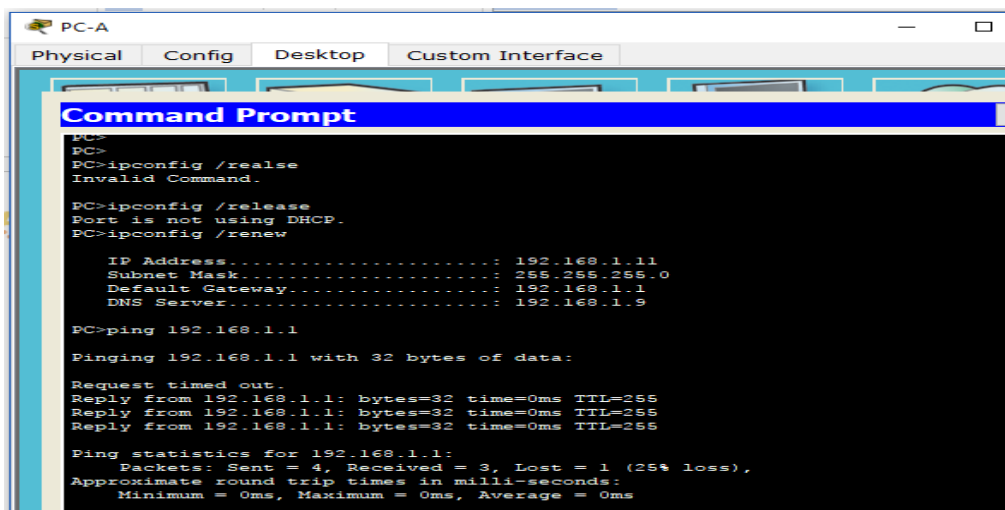
Link-local IPv6 Address.....: FE80::204:9AFF:FEEA:3461
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

PC>ipconfig /release
Port is not using DHCP.
PC>ipconfig /renew

IP Address.....: 192.168.1.12
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Server.....: 192.168.1.9

PC>
```

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



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>
PC>
PC>ipconfig /realse
Invalid Command.

PC>ipconfig /release
Port is not using DHCP.
PC>ipconfig /renew

IP Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Server.....: 192.168.1.9

PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time=0ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
PC-B
Physical Config Desktop Custom Interface
Command Prompt
Link-local IPv6 Address . . . . . FE80::204:9AFF:FEEA:3461
IP Address . . . . . 0.0.0.0
Subnet Mask . . . . . 0.0.0.0
Default Gateway . . . . . 0.0.0.0

PC>ipconfig /release
Port is not using DHCP.
PC>ipconfig /renew

IP Address . . . . . 192.168.1.12
Subnet Mask . . . . . 255.255.255.0
Default Gateway . . . . . 192.168.1.1
DNS Server . . . . . 192.168.1.9

PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=3ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

```
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#
```

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

R/ Si es satisfactorio el ping

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.1.1

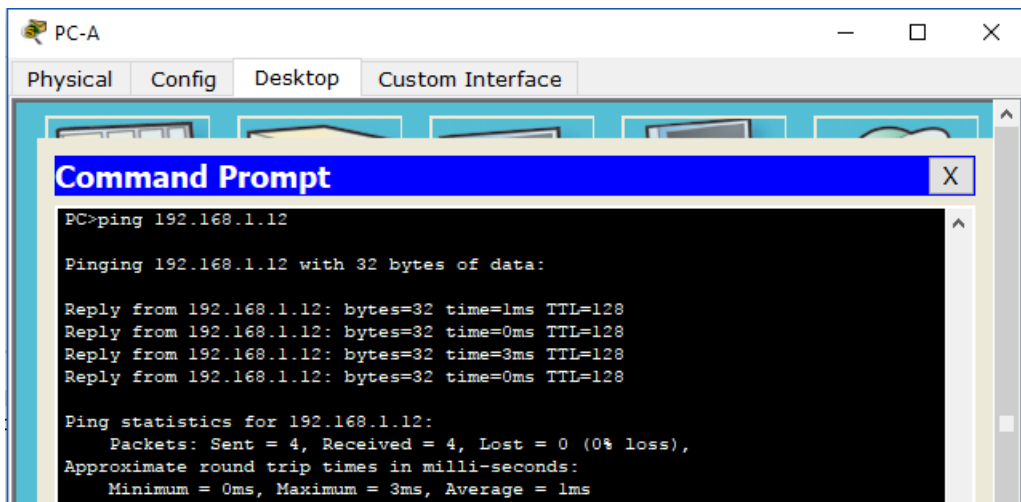
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time=0ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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

R/ Si es posible el ping



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.1.12

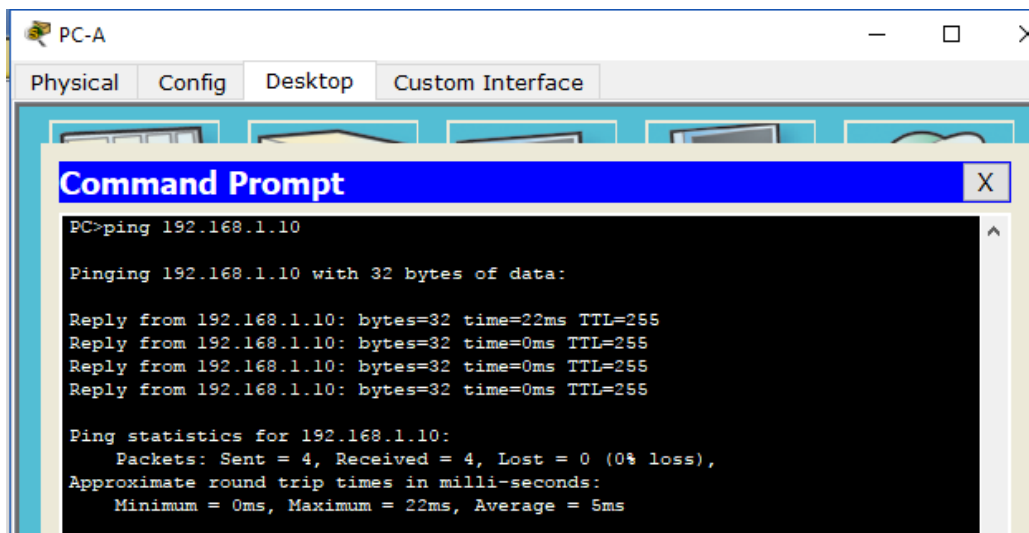
Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

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

R/ Si es posible el ping.



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=22ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 22ms, Average = 5ms
```

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

Parte 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.

Paso 1 Asignar un puerto a la VLAN 2.

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

R/ Para asignar el puerto F0/6 a la vlan 2 usamos los siguientes comandos

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

```
S1(config-if)#switchport mode access
```

```
S1(config-if)#switchport access vlan 2
```

```
% Access VLAN does not exist. Creating vlan 2
```

```
S1(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

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

```
S1(config-if)#end
```

```
S1>enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

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

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

Paso 2 Configurar DHCPv4 para la VLAN 2.

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

R/ el comando que se utiliza es *ip dhcp excluded-address 192.168.2.1 192.168.2.10*

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)#
```

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

R/ El comando que se utiliza es *ip dhcp pool DHCP2*

```
S1(config)#ip dhcp pool DHCP2
S1(dhcp-config)#
```

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

R/ El comando que se utiliza es *network 192.168.2.0 255.255.255.0*

```
S1(dhcp-config)#network 192.168.2.0 255.255.255.0
S1(dhcp-config)#
```

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

R/ El comando que se utiliza es *default-router 192.168.2.1*

```
S1(dhcp-config)#default-router 192.168.2.1
S1(dhcp-config)#
```

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

R/ El comando que se utiliza es *dns-server 192.168.2.9*

```
S1(dhcp-config)#dns-server 192.168.2.9
S1(dhcp-config)#
```

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

R/ El comando que se utiliza es *lease 3*

```
S1(dhcp-config)#lease 3
      ^
% Invalid input detected at '^' marker.
S1(dhcp-config)#
```

Comando no soportado por Packet Trace

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

R/ El comando que se utiliza es *copy running-config startup-config*

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Paso 3 Verificar la conectividad y DHCPv4.

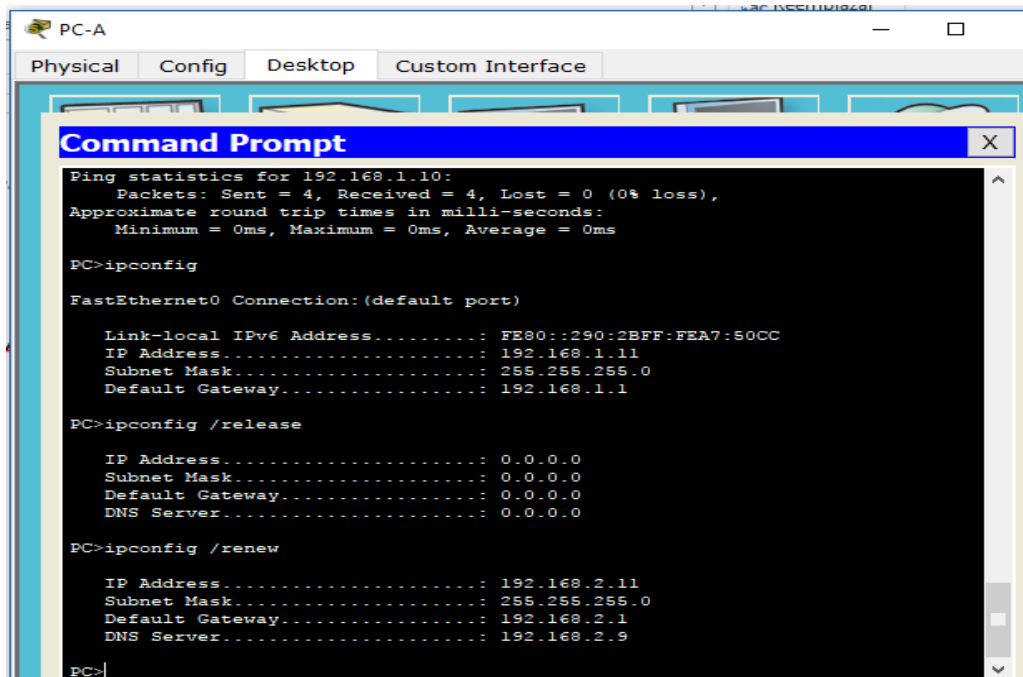
- a. En la PC-A, abra el símbolo del sistema y emita el comando `ipconfig /release`, seguido del comando `ipconfig /renew`.

Para la PC-A, incluya lo siguiente:

Dirección IP: ***192.168.2.11***

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.2.1**



```
PC-A
Physical Config Desktop Custom Interface

Command Prompt
Ping statistics for 192.168.1.10:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ipconfig

FastEthernet0 Connection: (default port)

  Link-local IPv6 Address . . . . . : FE80::290:2BFF:FEA7:50CC
  IP Address. . . . . : 192.168.1.11
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1

PC>ipconfig /release

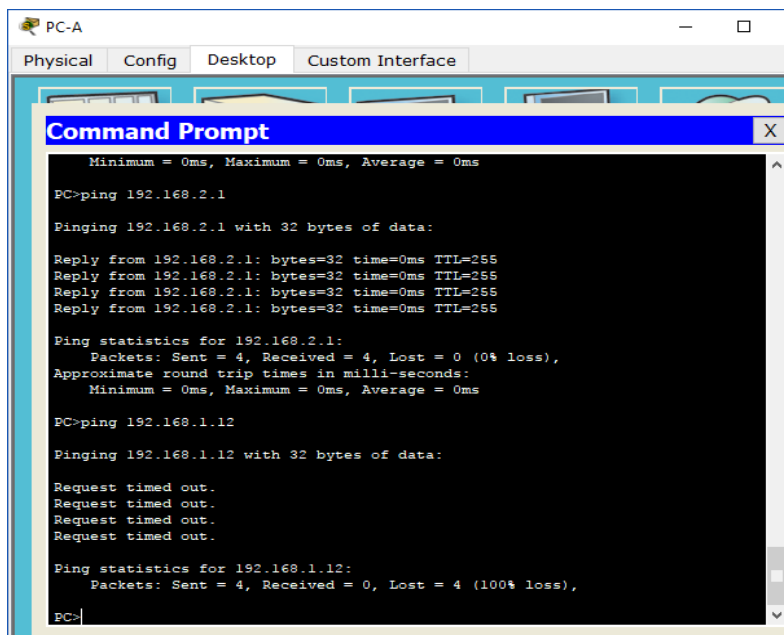
  IP Address . . . . . : 0.0.0.0
  Subnet Mask . . . . . : 0.0.0.0
  Default Gateway . . . . . : 0.0.0.0
  DNS Server . . . . . : 0.0.0.0

PC>ipconfig /renew

  IP Address . . . . . : 192.168.2.11
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.2.1
  DNS Server . . . . . : 192.168.2.9

PC>
```

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



```
PC-A
Physical Config Desktop Custom Interface

Command Prompt
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255

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

PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

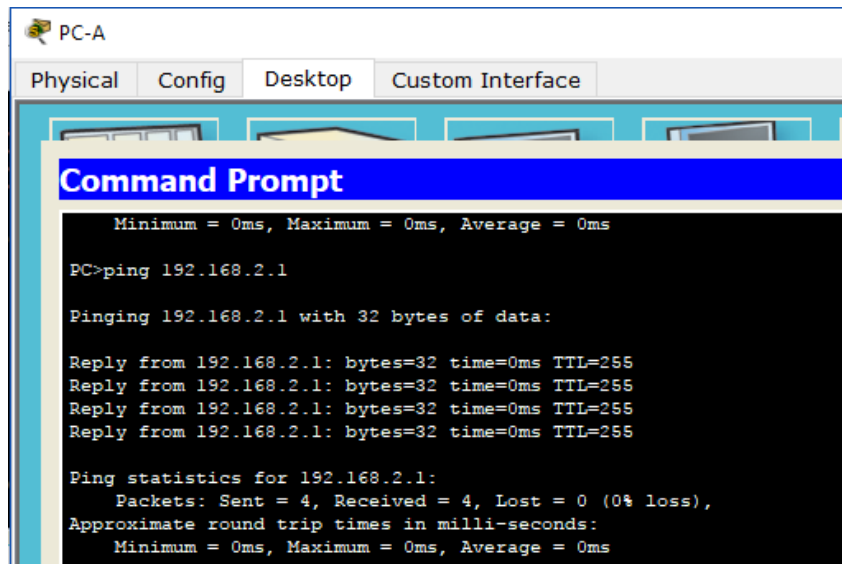
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.12:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

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

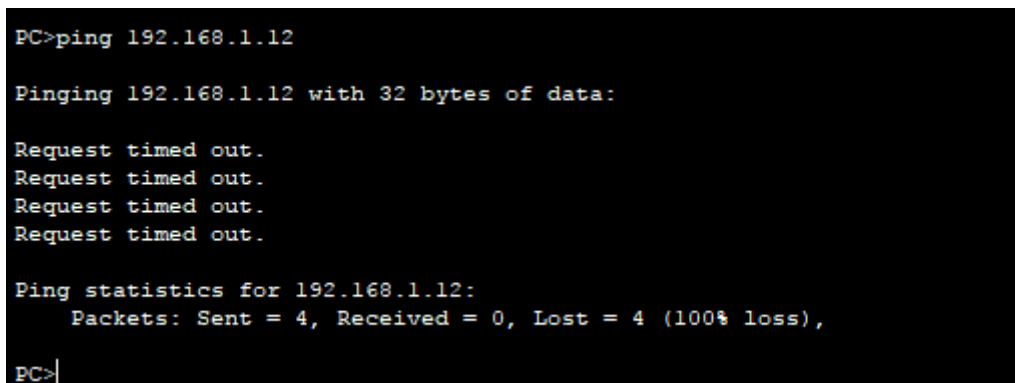
R/ Si responde a ping el Gateway predeterminado desde el PC-A



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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

R/ No es posible el ping del PC-A al PC-B



```
PC>ping 192.168.1.12
Pinging 192.168.1.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

¿Los pings eran correctos? ¿Por qué?

R/ El ping al gateway es satisfactorio desde la PC-A por estar en la misma red de la PC-A, caso contrario de la PC-B, por esta razón este segundo ping de PC-A a PC-B no respondió.

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

¿Qué resultado arrojó este comando?

R/ Se emite el comando pero este no es soportado ya que no arroja ningún resultado.

```
S1#show ip route
Default gateway is not set
Host          Gateway      Last Use    Total Uses  Interface
ICMP redirect cache is empty
S1#
```

Parte 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.

Paso 1 Habilitar el routing IP en el S1.

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

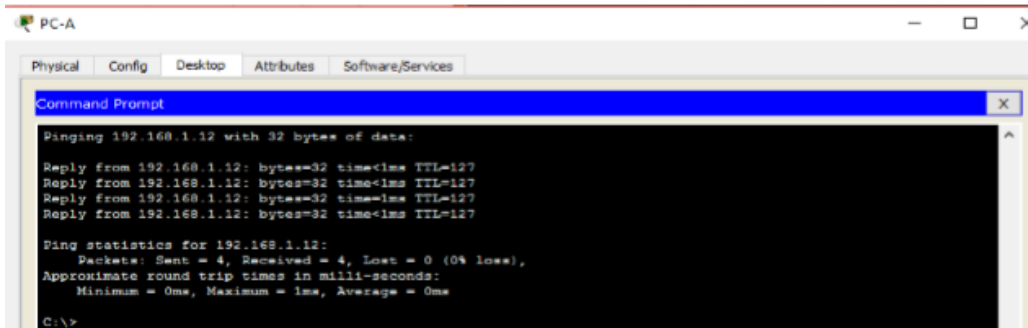
S1(config)# ip routing

```
S1#configure ter
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip rout
S1(config)#ip routing
```

- Verificar la conectividad entre las VLAN.

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

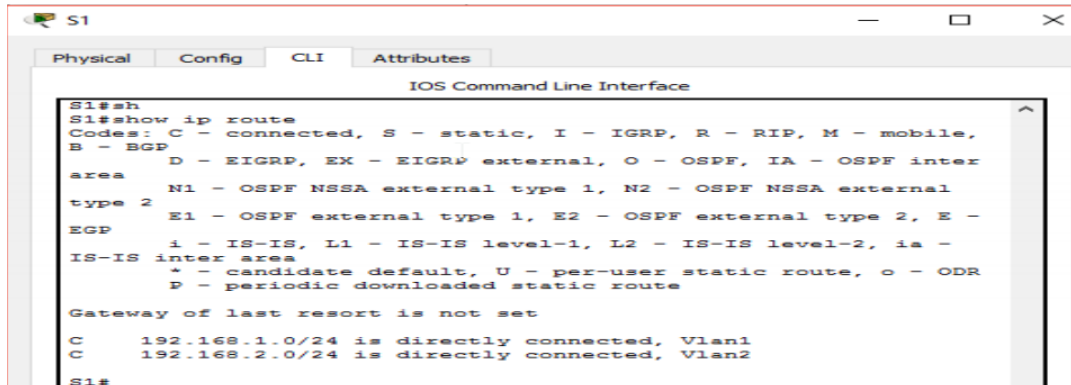
R/ Si, el ping realizado del PC-A al PC-B fue exitoso



¿Qué función realiza el switch?

R/ Cumple la función de enrutador entre las dos VLAN

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

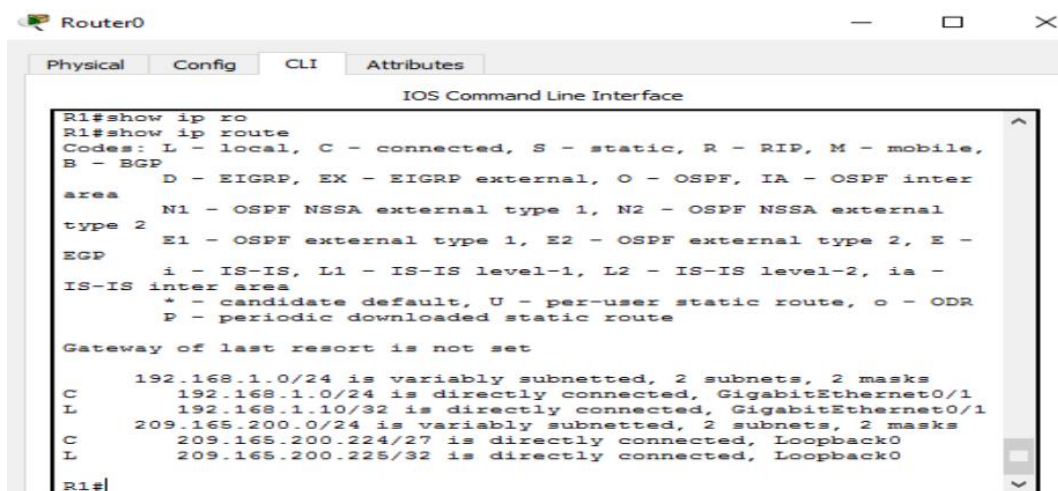


```
S1#  
S1#show ip route  
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,  
B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter  
area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external  
type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E -  
EGP  
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 not set  
  
C    192.168.1.0/24 is directly connected, Vlan1  
C    192.168.2.0/24 is directly connected, Vlan2  
  
S1#
```

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

R/ Se observan dos redes directamente conectadas (vlan 1 - 2).

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



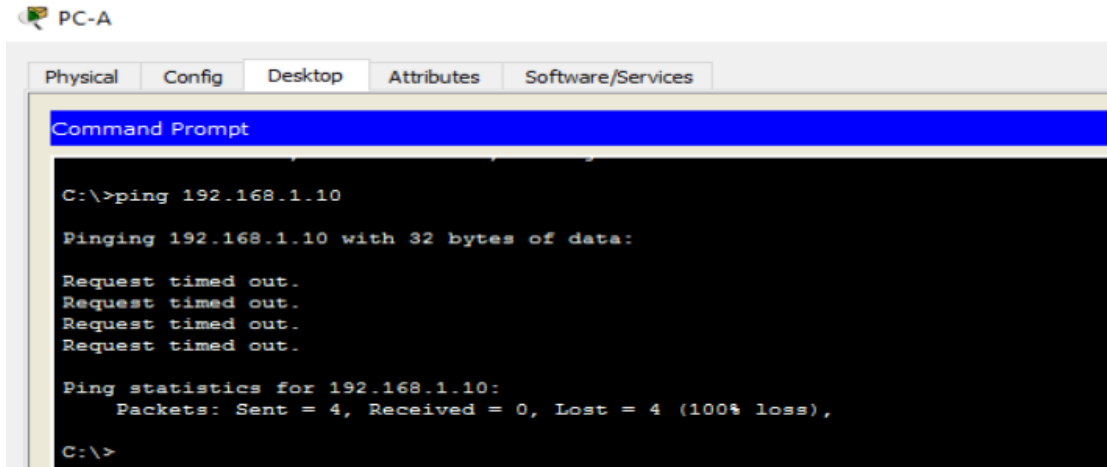
```
Router0  
R1#show ip ro  
R1#show ip route  
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,  
B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter  
area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external  
type 2  
E1 - OSPF external type 1, E2 - OSPF external 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, GigabitEthernet0/1  
L    192.168.1.10/32 is directly connected, GigabitEthernet0/1  
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks  
C    209.165.200.224/27 is directly connected, Loopback0  
L    209.165.200.225/32 is directly connected, Loopback0  
  
R1#
```

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

R/ De igual forma que el S1 se muestran dos redes directamente conectadas, solo que este muestra la red 1 (192.168.1.0) y la publica 209.165.200.224, y no se evidencia la entrada para la red 2 (192.168.2.0).

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

R/ No es posible el ping



```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

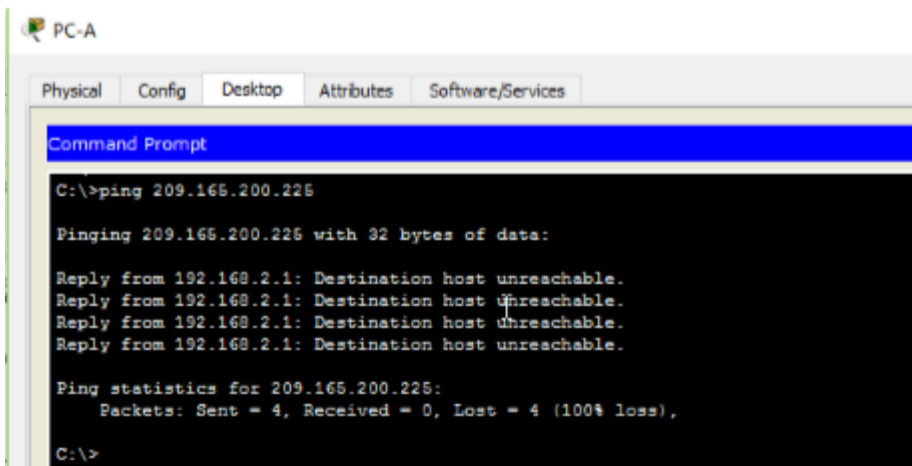
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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

R/ No es posible la realización del ping



```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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

R/ Se deben incluir todas las rutas en la tabla de ruteo para que se pueda garantizar esta comunicación.

Paso 2 Asignar rutas estáticas.

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

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

R/ Se utiliza el comando *ip route 0.0.0.0 0.0.0.0 192.168.1.10*

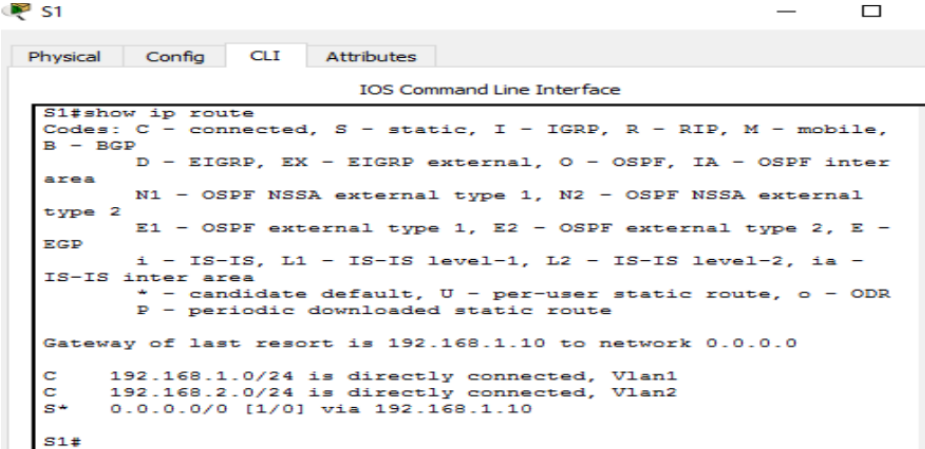
```
S1#configure ter
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.10
S1(config)#
```

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

R/ Se utiliza el comando *ip route 192.168.2.0 255.255.255.0 g0/1*

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip ro
R1(config)#ip route 192.168.2.0 255.255.255.0 g0/1
%Default route without gateway, if not a point-to-point
interface, may impact performance
R1(config)#
```

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



```
S1
Physical Config CLI Attributes
IOS Command Line Interface
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
S*   0.0.0.0/0 [1/0] via 192.168.1.10
S1#
```

¿Cómo está representada la ruta estática predeterminada?

R/ Está representada como: 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, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

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

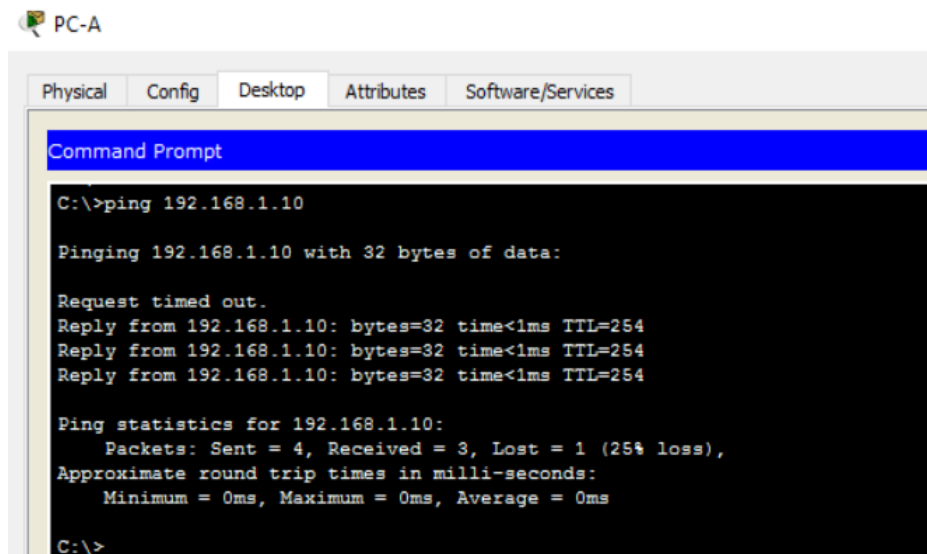
R1#
```

¿Cómo está representada la ruta estática?

R/ La ruta estática está representada como: S 192.168.2.0/24 is directly connected, GigabitEthernet0/1

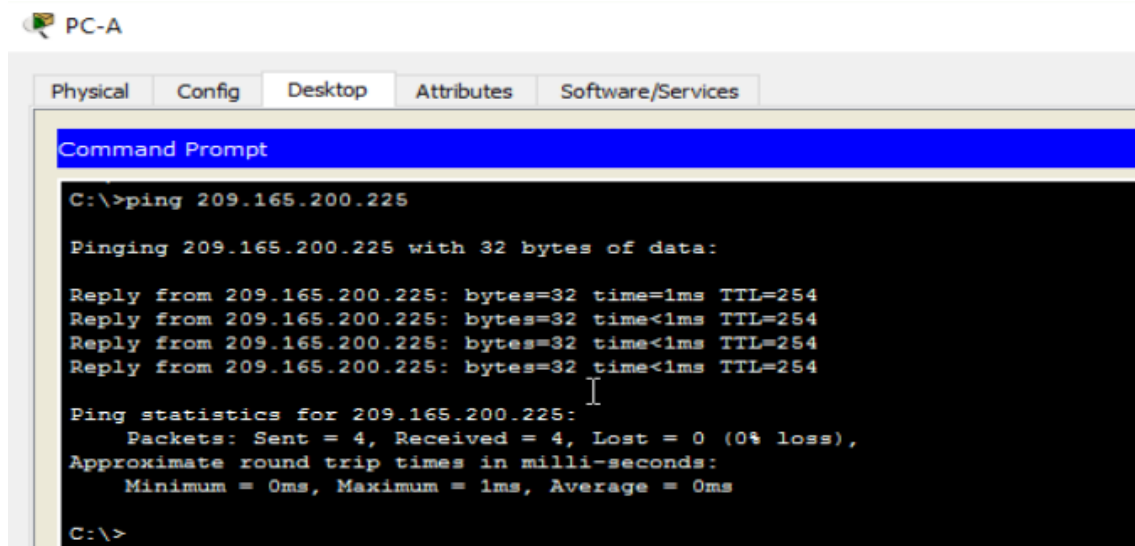
e. ¿Es posible hacer ping de la PC-A al R1?

R/ Se ping que se realiza del PC_A a R1 es exitoso



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

R/ El ping a Lo0 es exitoso



```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254

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

C:\>
```

Reflexión

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

R/ Por la ventana de tiempo que existe cuando se excluyen estas direcciones antes de crear el pool de direcciones y se podrían dar de forma dinámica hacia unos equipos finales (hosts).

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

R/ Las asigna basándose en la vlan de cada vlan con relación a su puerto conectado.

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

R/ Este switch puede tener funciones de dhcp, en mi caso para el ejercicio no lo use, use uno 3560 ya que el 2960 no me soportaba el comando ip route.

Ejercicio 10.2.3.5 configuración de dhcpv6 sin estado y con estado

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

Información básica/situación

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

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

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

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

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

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

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles

y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

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

S1# show sdm prefer

```
Switch#show sdm prefer
The current template is "desktop IPv4 and IPv6 default"
template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:          3K
  number of directly-connected IPv4 hosts: 2K
  number of indirect IPv4 routes:       1K
number of IPv6 multicast groups:        1.125k
number of directly-connected IPv6 addresses: 2K
number of indirect IPv6 unicast routes:  1K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:            0.5K
number of IPv4/MAC security aces:       1K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces:                0.625k
number of IPv6 security aces:           0.5K
```

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

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#reload
```


Recursos necesarios

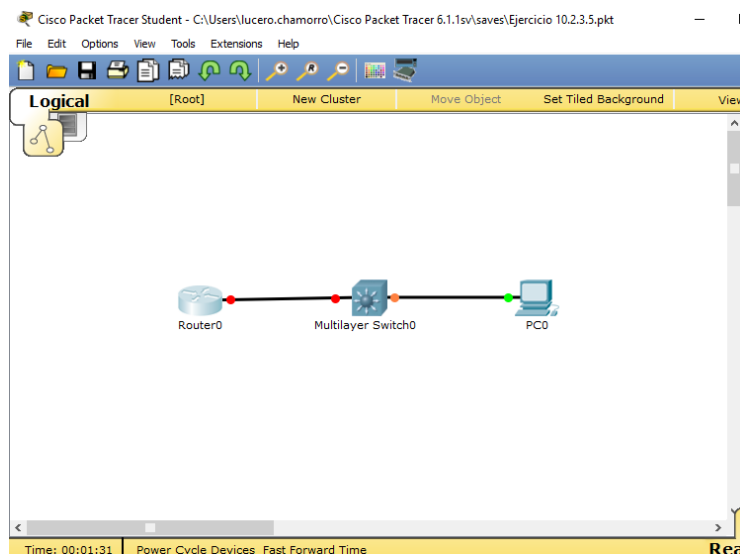
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para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

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

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

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



Paso 2 Inicializar y volver a cargar el router y el switch según sea necesario.

Paso 3 Configurar R1

- a. Desactive la búsqueda del DNS.

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#
```

- b. Configure el nombre del dispositivo.

```
Router(config)#hostname R1
R1(config)#
```

- c. Cifre las contraseñas de texto no cifrado.

```
R1(config)#service password-encryption
R1(config)#
```

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

```
R1(config)#banner motd "No esta Autorizado Comuniquese con el Administrador "
R1(config)#
```

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

```
R1(config)#enable password class
R1(config)#
```

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

```
R1(config)#line vty 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

```
No esta Autorizado Comuniquese con el Administrador
User Access Verification
Password:
R1>enable
Password:
R1#
```

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

```
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#
```

- h. Guardar la configuración en ejecución en la configuración de inicio.

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

Paso 4 Configurar el S1.

- a. Desactive la búsqueda del DNS.

```
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#
```

- b. Configure el nombre del dispositivo.

```
Switch(config)#hostname S1
S1(config)#
```

- c. Cifre las contraseñas de texto no cifrado.

```
S1(config)#service password-encryption
S1(config)#
```

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

```
S1(config)#banner motd " No esta Autorizado Comuniquese con el Administrador "  
S1(config)#
```

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

```
S1(config)#enable password class  
S1(config)#
```

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

```
S1(config)#enable password class  
S1(config)#line console 0  
S1(config-line)#password cisco  
S1(config-line)#login  
S1(config-line)#exit  
S1(config)#line vty 0  
S1(config-line)#password cisco  
S1(config-line)#login  
S1(config-line)#exit  
S1(config)#
```

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

```
S1(config)#line console 0  
S1(config-line)#logging synchronous  
S1(config-line)#exit  
S1(config)#
```

- h. Desactive administrativamente todas las interfaces inactivas.

```
S1#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
S1(config)#Int range f0/1-4, f0/7-24  
S1(config-if-range)#shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively
down
```

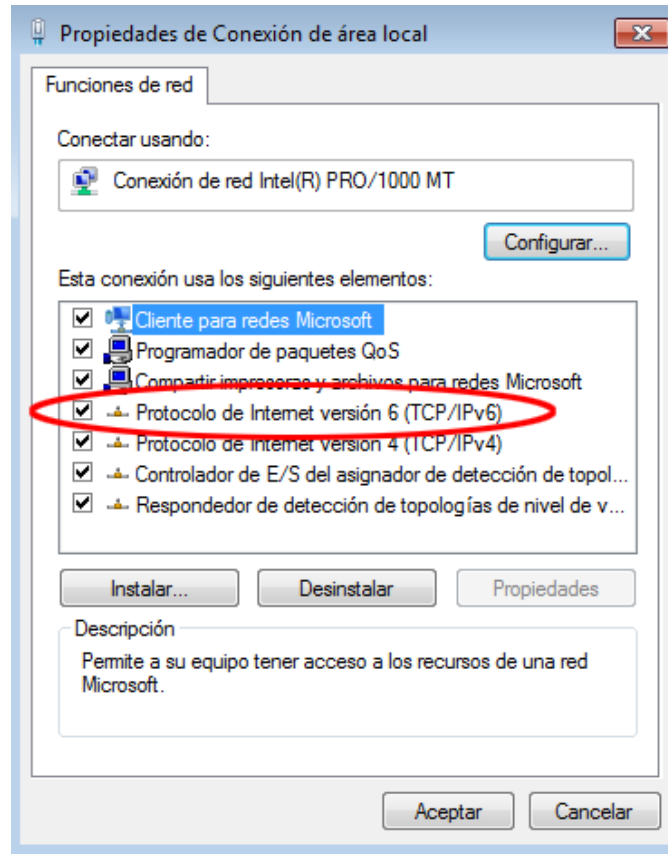
- i. Guarde la configuración en ejecución en la configuración de inicio.

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

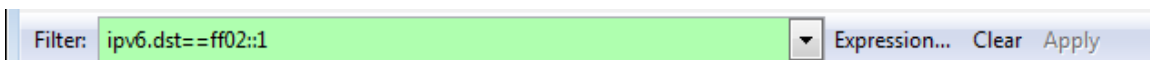
Parte 2 Configurar la red para SLAAC

Paso 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.



Paso 2 Configurar R1

- a. Habilite el routing de unidifusión IPv6.

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

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

```
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#
```

- c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz 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)#
```

- d. Active la interfaz 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)#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)#
```

Paso 3 Verificar que el R1 forme parte del grupo de multidifusión de todos los routers.

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

```
R1# show ipv6 interface g0/1
```

GigabitEthernet0/1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::1

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF00:1

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.

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

Paso 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
```

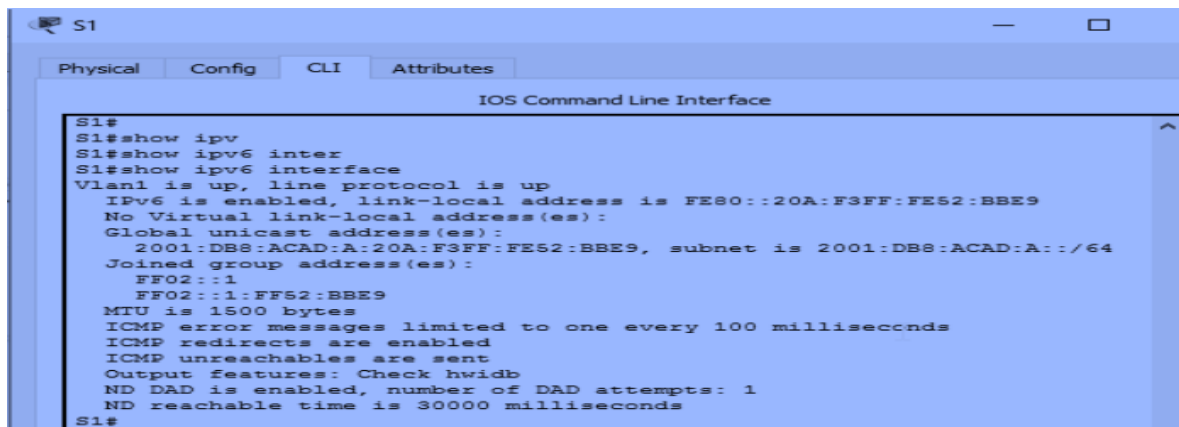
```
S1(config-if)# end
```

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface vlan 1
S1(config-if)#ipv6 address autoconfig
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Paso 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.

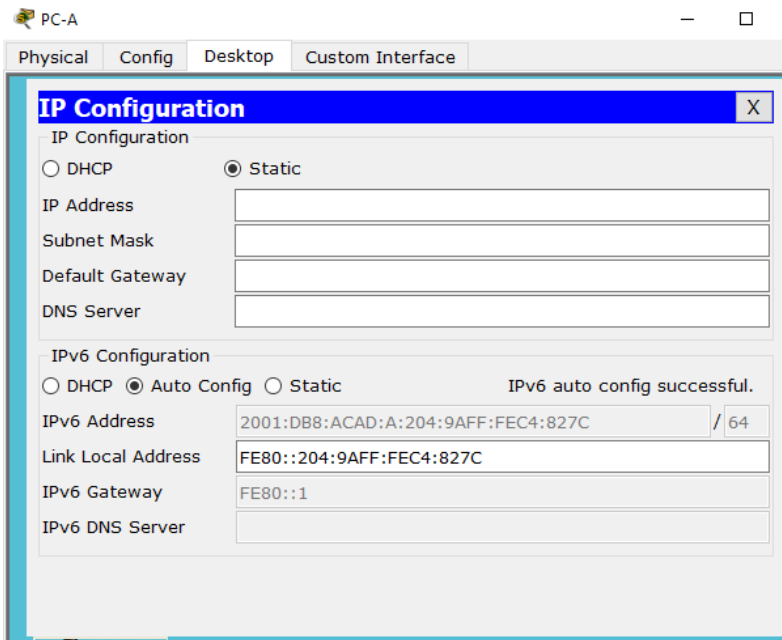
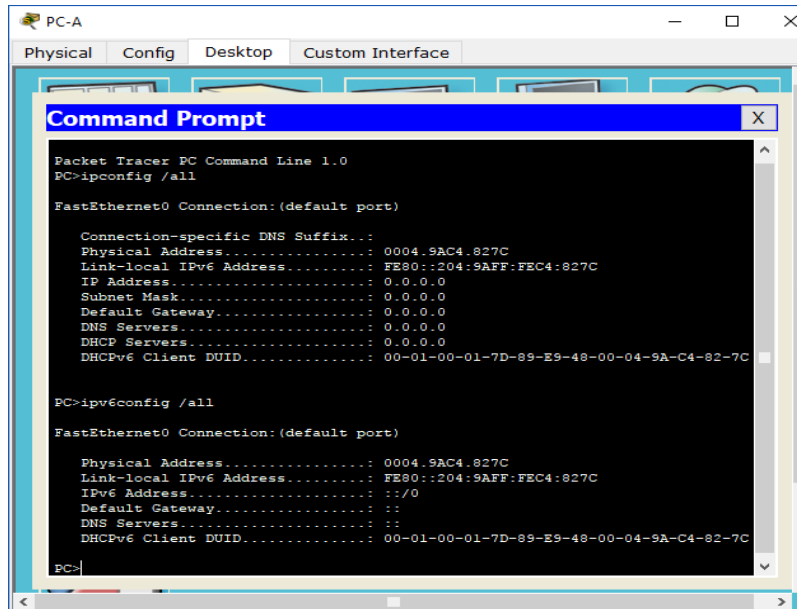
```
S1# show ipv6 interface
```



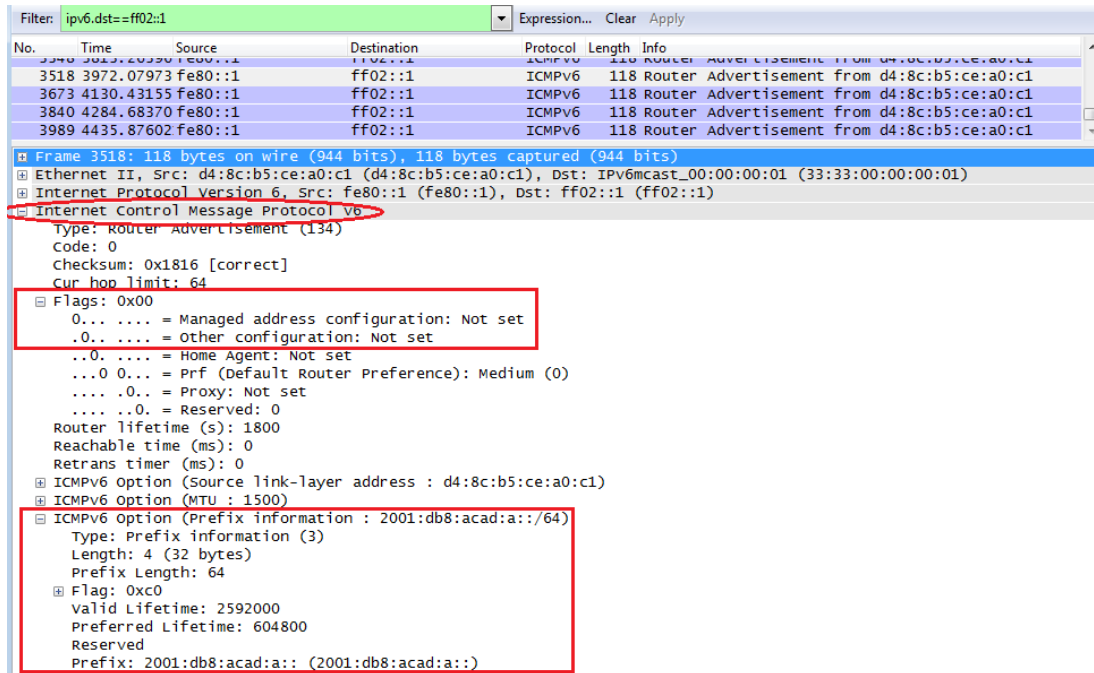
```
S1#
S1#show ipv6
S1#show ipv6 inter
S1#show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20A:F3FF:FES2:BBE9
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A:20A:F3FF:FES2:BBE9, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::1:FF52:BBE9
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
Output features: Check hwidb
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
S1#
```

Paso 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.



Parte 3 Configurar la red para DHCPv6 sin estado

Paso 1 Configurar un servidor de DHCP IPv6 en el R1.

- a. Cree un pool de DHCP IPv6.

R1(config)# ipv6 dhcp pool IPV6POOL-A

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#
```

- b. Asigne un nombre de dominio al pool.

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

```
R1(config-dhcpv6)#domain-name ccna-statelessDHCPV6.com
R1(config-dhcpv6)#
```

c. Asigne una dirección de servidor DNS.

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

R1(config-dhcpv6)# **exit**

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

d. Asigne el pool de DHCPv6 a la interfaz.

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

R1(config-if)# **ipv6 dhcp server IPV6POOL-A**

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

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

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

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

```
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 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**

```
R1#show ipv6 int 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
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

Paso 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.

```

PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
FastEthernet0 Connection: (default port)
Physical Address.....: 0004.9AD1.4A70
Link-local IPv6 Address.....: FE80::204:9AFF:FED1:4A70
IPv6 Address.....: 2001:DB8:ACAD:A:204:9AFF:FED1:4A70/64
Default Gateway.....: FE80::1
DNS Servers.....: ::
DHCPv6 Client DUID.....: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70

C:\>ipv6config /all

FastEthernet0 Connection: (default port)
Physical Address.....: 0004.9AD1.4A70
Link-local IPv6 Address.....: FE80::204:9AFF:FED1:4A70
IPv6 Address.....: 2001:DB8:ACAD:A:204:9AFF:FED1:4A70/64
Default Gateway.....: FE80::1
DNS Servers.....: ::
DHCPv6 Client DUID.....: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70

C:\>ipv6config /all

FastEthernet0 Connection: (default port)
Physical Address.....: 0004.9AD1.4A70
Link-local IPv6 Address.....: FE80::204:9AFF:FED1:4A70
IPv6 Address.....: 2001:DB8:ACAD:A:204:9AFF:FED1:4A70/64
Default Gateway.....: FE80::1
DNS Servers.....: 2001:DB8:ACAD:A::ABCD
DHCPv6 IAID.....: 15057
DHCPv6 Client DUID.....: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70

C:\>

```

Paso 4 Ver los mensajes RA en Wireshark.

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

```

Filter: ipv6.dst==ff02::1
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
191 190.005980 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
422 383.803033 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
696 581.355847 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
877 776.644829 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1

Frame 877: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
Type: Router Advertisement (134)
Code: 0
Checksum: 0x17d6 [correct]
cur hop limit: 64
Flags: 0x40
0... .. = Managed address configuration: Not set
.1... .. = Other configuration: Set
..0... .. = Home Agent: Not set
...0... = Prf (Default Router Preference): Medium (0)
....0.. = Proxy: Not set
....0.. = Reserved: 0
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0
ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
ICMPv6 Option (MTU : 1500)
ICMPv6 option (Prefix information : 2001:db8:acad:a::/64)

```

Paso 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 PCA no haya obtenido una dirección IPv6 del pool de DHCPv6.}

R1# **show ipv6 dhcp binding**

R1# **show ipv6 dhcp pool**

```
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
IA PD: IA ID 15057, T1 0, T2 0
Prefix: 0.0.0.0/0
        preferred lifetime 0, valid lifetime 0
        expires at Noviembre 22 2017 8:26:37 pm (0 seconds)
```

```
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPV6.com
Active clients: 0
```

Paso 6 Restablecer la configuración de red IPv6 de la PC-A.

- Desactive la interfaz F0/6 del S1.

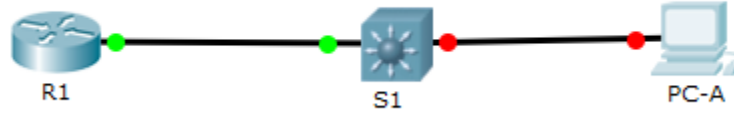
Nota: la desactivación de la interfaz F0/6 evita que la PC-A reciba una nueva dirección IPv6 antes de que usted vuelva a configurar el R1 para DHCPv6 con estado en la parte 4.

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

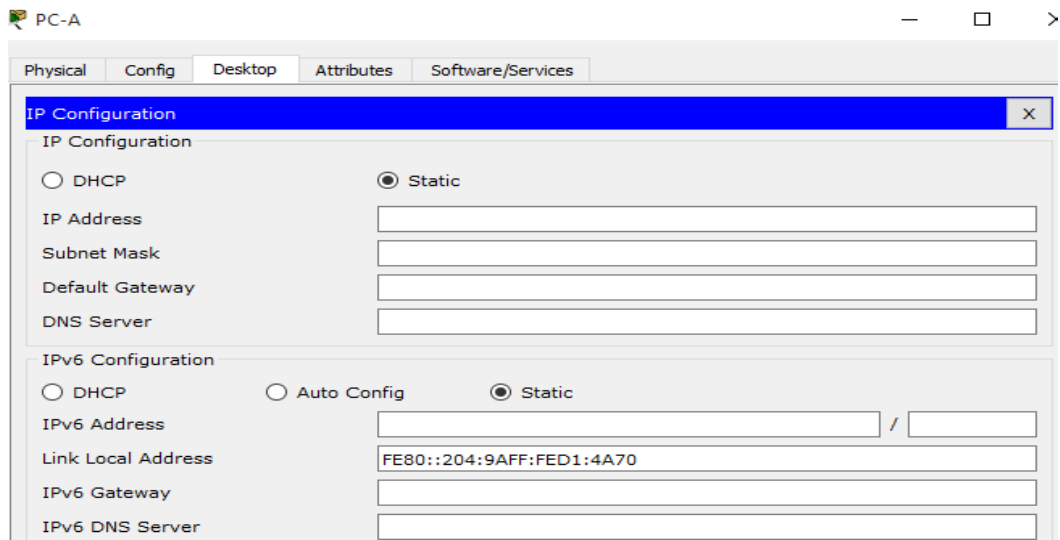
S1(config-if)# **shutdown**

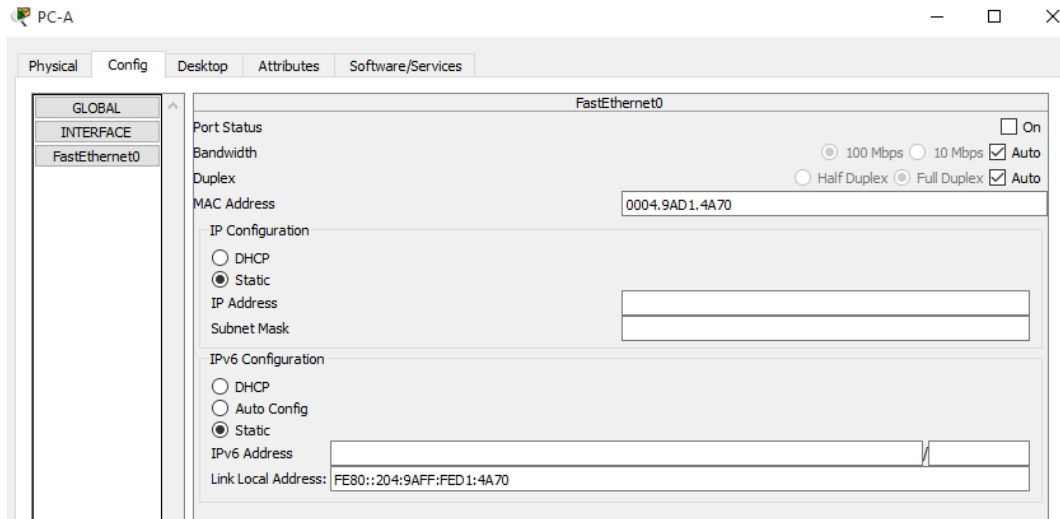
```
S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
changed state to down
```



- 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.



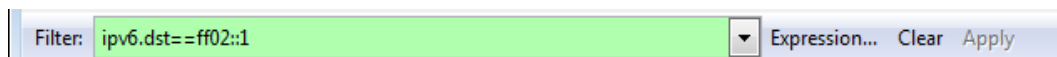


- 2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) y, a continuación, haga clic en Aceptar para aceptar el cambio. configurar la red para DHCPv6 con estado

Parte 4 configurar la red para DHCPv6 con estado

Paso 1 Preparar la PC-A.

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



Paso 2 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
```

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

Nota: El comando no es soportado por packet tracer

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**

```
R1(config-dhcpv6)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

c. Verifique la configuración del pool de DHCPv6.

R1# **show ipv6 dhcp pool**

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

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

R1# **debug ipv6 dhcp detail**

```
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
```

Paso 3 Establecer el indicador en G0/1 para DHCPv6 con estado.

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

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

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

```
R1(config-if)# ipv6 nd managed-config-flag
```

```
R1(config-if)# no shutdown
```

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

```
R1(config-if)#IPV6 nd managed-config-flag
R1(config-if)#no shu

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

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

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

R1#
```

Paso 4 Habilitar la interfaz F0/6 en el S1.

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

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

```
S1(config-if)# no shutdown
```

```
S1(config-if)# end
```

```

S1(config)#int f0/6
S1(config-if)#no shu

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to down
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#

```

Paso 5 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

```

R1#show ipv6 int 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):
  FE02::1:2
  FE02::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
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.

```

- 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.

Nota:

No se pudo asignar una ipv6 unicast por lo que ese comando no se soportó en el punto a, Parte 4, paso 2.

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

R1# show ipv6 dhcp pool

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

Nota: El resultado debería ser 1 como clientes activos, por no haber soportado la asignación de la pv6 unicast no aparece ninguno.

- 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

```
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
  DUID: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
  IA PD: IA ID 15057, T1 0, T2 0
  Prefix: 0.0.0.0/0
           preferred lifetime 0, valid lifetime 0
           expires at Noviembre 22 2017 8:59:10 pm (0 seconds)
```

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

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

R1# u all

Se ha desactivado toda depuración posible

```
R1#u all
All possible debugging has been turned off
R1#
```

- 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. 1 03:42:13.467: elapsed-time 0
*Mar. 1 03:42:13.467: option CLIENTID(1), len 45
*Mar. 1 03:42:13.467: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:13.467: option ORO(6), len 10
*Mar. 1 03:42:13.467: IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 03:42:13.467: option IA-PD(25), len 16
*Mar. 1 03:42:13.467: IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:13.467: IPv6 DHCP: Using interface pool IPV6POOL-A

*Mar. 1 03:42:13.467: IPv6 DHCP: Sending ADVERTISE to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:13.467: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:13.467: src FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467: dst FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467: type ADVERTISE(2), xid 4
*Mar. 1 03:42:13.467: option SERVERID(2), len 24
*Mar. 1 03:42:13.467: 0003000100902B731501
*Mar. 1 03:42:13.467: option CLIENTID(1), len 45
*Mar. 1 03:42:13.467: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:13.467: option IA-PD(25), len 45
*Mar. 1 03:42:13.467: IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:13.467: option IAPREFIX(26), 29
*Mar. 1 03:42:13.467: preferred 0, valid 0, prefix 0.0.0.0/0

*Mar. 1 03:42:13.467: IPv6 DHCP: Received REQUEST from FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:13.467: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:13.467: src FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467: dst FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467: type REQUEST(3), xid 2
*Mar. 1 03:42:13.467: option ELAPSED-TIME(8), len 6
*Mar. 1 03:42:13.467: elapsed-time 0
*Mar. 1 03:42:13.467: option SERVERID(2), len 24
*Mar. 1 03:42:13.467: 0003000100902B731501
*Mar. 1 03:42:13.467: option CLIENTID(1), len 45
*Mar. 1 03:42:13.467: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:13.467: option ORO(6), len 10
*Mar. 1 03:42:13.467: IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 03:42:13.467: option IA-PD(25), len 45
*Mar. 1 03:42:13.467: IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:13.467: option IAPREFIX(26), 29
*Mar. 1 03:42:13.467: preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 03:42:13.467: IPv6 DHCP: Using interface pool IPV6POOL-A
*Mar. 1 03:42:13.467: IPv6 DHCP: Creating binding for FE80::204:9AFF:FED1:4A70 in pool IPV6POOL-A
*Mar. 1 03:42:13.467: IPv6 DHCP: Allocating IA_PD 15057 in binding for FE80::204:9AFF:FED1:4A70
*Mar. 1 03:42:13.467: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for FE80::204:9AFF:FED1:4A70, IAID 15057

*Mar. 1 03:42:13.467: IPv6 DHCP: Sending REPLY to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:13.467: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:13.467: src FE80::1 (GigabitEthernet0/1)
```

```
*Mar. 1 03:42:13.467: IPv6 DHCP: Sending REPLY to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:13.467: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:13.467: src FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467: dst FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467: type REPLY(7), xid 2
*Mar. 1 03:42:13.467: option SERVERID(2), len 24
*Mar. 1 03:42:13.467: 0003000100902B731501
*Mar. 1 03:42:13.467: option CLIENTID(1), len 45
*Mar. 1 03:42:13.467: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:13.467: option IA-PD(25), len 41
*Mar. 1 03:42:13.467: IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:13.467: option IAPREFIX(26), 29
*Mar. 1 03:42:13.467: preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 03:42:13.467: option DNS-SERVERS(23), len 20
*Mar. 1 03:42:13.467: 2001:DB8:ACAD:A:ABCD
*Mar. 1 03:42:13.467: option DOMAIN-LIST(24), len 5
*Mar. 1 03:42:13.467: ccna-StatefulDHCPv6.com

*Mar. 1 03:42:20.981: IPv6 DHCP: Received SOLICIT from FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:20.981: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:20.981: src FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:20.981: dst FF02::1:2 (GigabitEthernet0/1)
*Mar. 1 03:42:20.981: type SOLICIT(1), xid 5
*Mar. 1 03:42:20.981: option ELAPSED-TIME(8), len 6
*Mar. 1 03:42:20.981: elapsed-time 0
*Mar. 1 03:42:20.981: option CLIENTID(1), len 45
*Mar. 1 03:42:20.981: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:20.981: option ORO(6), len 10
*Mar. 1 03:42:20.981: IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 03:42:20.981: option IA-PD(25), len 16
*Mar. 1 03:42:20.981: IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:20.981: IPv6 DHCP: Using interface pool IPV6POOL-A

*Mar. 1 03:42:20.981: IPv6 DHCP: Sending ADVERTISE to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:20.981: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:20.981: src FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:20.981: dst FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:20.981: type ADVERTISE(2), xid 5
*Mar. 1 03:42:20.981: option SERVERID(2), len 24
*Mar. 1 03:42:20.981: 0003000100902B731501
*Mar. 1 03:42:20.981: option CLIENTID(1), len 45
*Mar. 1 03:42:20.981: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:20.981: option IA-PD(25), len 45
*Mar. 1 03:42:20.981: IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:20.981: option IAPREFIX(26), 29
*Mar. 1 03:42:20.981: preferred 0, valid 0, prefix 0.0.0.0/0
```

```

*Mar. 1 03:42:23.515: IPv6 DHCP: Received REQUEST from FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:23.515: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:23.515:   src FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:23.515:   dst FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:23.515:   type REQUEST(3), xid 4
*Mar. 1 03:42:23.515:   option ELAPSED-TIME(8), len 6
*Mar. 1 03:42:23.515:     elapsed-time 0
*Mar. 1 03:42:23.515:   option SERVERID(2), len 24
*Mar. 1 03:42:23.515:     0003000100902B731501
*Mar. 1 03:42:23.515:   option CLIENTID(1), len 45
*Mar. 1 03:42:23.515:     00-01-00-01-67-AS-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:23.515:   option ORO(6), len 10
*Mar. 1 03:42:23.515:     IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 03:42:23.515:   option IA-PD(25), len 45
*Mar. 1 03:42:23.515:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:23.515:   option IAPREFIX(26), 29
*Mar. 1 03:42:23.515:     preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 03:42:23.515: IPv6 DHCP: Using interface pool IPV6POOL-A
*Mar. 1 03:42:23.515: IPv6 DHCP: Creating binding for FE80::204:9AFF:FED1:4A70 in pool IPV6POOL-A
*Mar. 1 03:42:23.515: IPv6 DHCP: Allocating IA_PD 15057 in binding for FE80::204:9AFF:FED1:4A70
*Mar. 1 03:42:23.515: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for FE80::204:9AFF:FED1:4A70, IAID 15057

*Mar. 1 03:42:23.515: IPv6 DHCP: Sending REPLY to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:23.515: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:23.515:   src FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:23.515:   dst FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:23.515:   type REPLY(7), xid 4
*Mar. 1 03:42:23.515:   option SERVERID(2), len 24
*Mar. 1 03:42:23.515:     0003000100902B731501
*Mar. 1 03:42:23.515:   option CLIENTID(1), len 45
*Mar. 1 03:42:23.515:     00-01-00-01-67-AS-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:23.515:   option IA-PD(25), len 41
*Mar. 1 03:42:23.515:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:23.515:   option IAPREFIX(26), 29
*Mar. 1 03:42:23.515:     preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 03:42:23.515:   option DNS-SERVERS(23), len 20
*Mar. 1 03:42:23.515:     2001:DB8:ACAD:A:ABCD
*Mar. 1 03:42:23.515:   option DOMAIN-LIST(24), len 5
*Mar. 1 03:42:23.515:     ccna-StatefulDHCPv6.com

```

Paso 6 Verificar DHCPv6 con estado en la PC-A.

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

The screenshot shows a Wireshark capture of ICMPv6 Router Advertisement (RA) messages. The filter is set to 'ipv6.dst==ff02::1'. The packet list shows several RA messages from source fe80::1 to destination ff02::1. The details pane for the selected frame (775) shows the following flags:

- 1... .. = Managed address configuration: Set
- .1... .. = Other configuration: set
- .0... .. = Home Agent: Not set
- ...0... = Prf (Default Router Preference): Medium (0)
-0.. = Proxy: Not set
-0. = Reserved: 0

The 'Managed address configuration: Set' flag is highlighted with a red box, indicating that the router is providing managed addresses to the client.

- 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.

Filter: dhcpv6

No.	Time	Source	Destination	Protocol	Length	Info
250	443.078236	fe80::d428:7de2:997:ff02::1:2	fe80::d428:7de2:997:ff02::1:2	DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
267	475.083284	fe80::d428:7de2:997:ff02::1:2	fe80::d428:7de2:997:ff02::1:2	DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
425	656.281211	fe80::d428:7de2:997:ff02::1:2	fe80::d428:7de2:997:ff02::1:2	DHCPv6	146	Solicit XID: 0xc86c32 CID: 0001000117f6723d000c2
429	656.282249	fe80::1	fe80::d428:7de2:997:ff02::1:2	DHCPv6	191	Advertise XID: 0xc86c32 CID: 0001000117f6723d000c2
460	657.292018	fe80::d428:7de2:997:ff02::1:2	fe80::d428:7de2:997:ff02::1:2	DHCPv6	188	Request XID: 0xc86c32 CID: 0001000117f6723d000c2
462	657.292638	fe80::1	fe80::d428:7de2:997:ff02::1:2	DHCPv6	191	Reply XID: 0xc86c32 CID: 0001000117f6723d000c298

Expanded details for packet 462:

- Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: Vmware_be:6c:89 (00:50:56:be:6c:89)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)
- User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)
- DHCPv6
 - Message type: Reply (7)
 - Transaction ID: 0xc86c32
 - Server Identifier: 00030001fc994775c3e0
 - Client Identifier: 0001000117f6723d000c298d5444
 - Identity Association for Non-temporary Address
 - option: Identity Association for Non-temporary Address (3)
 - Length: 40
 - Value: 0e000c290000a8c000010e000005001820010db8acad000a...
 - IAID: 0e000c29
 - T1: 43200
 - T2: 69120
 - IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce
 - DNS recursive name server
 - option: DNS recursive name server (23)
 - Length: 16
 - Value: 2001:db8:acad:000a:0000:0000:0000:abcd
 - DNS servers address: 2001:db8:acad:a::abcd
 - Domain Search List
 - option: Domain Search List (24)
 - Length: 25
 - Value: 1363636e612d537461746566756c44484350763603636f6d...
 - DNS Domain Search List
 - Domain: ccna-StatefulDHCPv6.com

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?

R/ DHCPv6 con estado utiliza más memoria porque almacena dinámicamente en el router información de los clientes.

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

R/ El tipo de dirección recomendada DHCPv6 es sin estado, por la implementación de redes ipv6 sin necesidad de registro de red cisco.

EJERCICIO 10.3.1.1 idt y DHCP

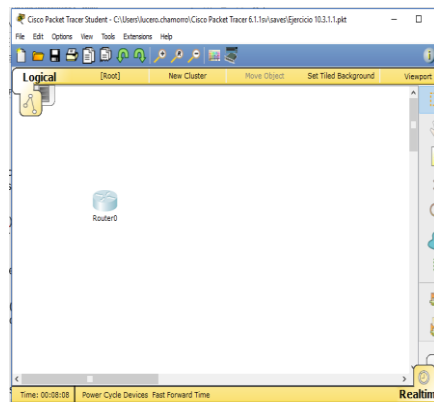
Situación

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.

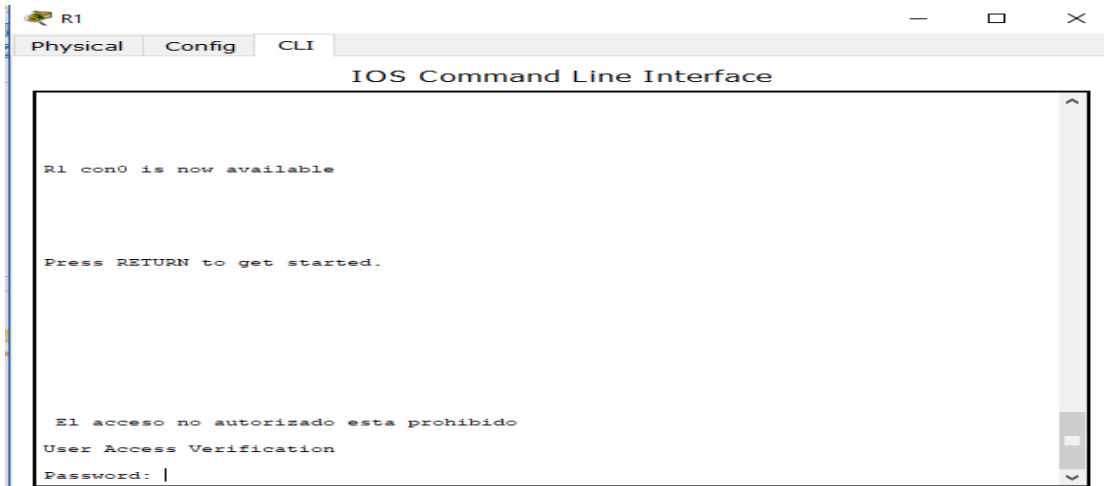
Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

- ❖ Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.



```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd " El acceso no autorizado esta prohibido "
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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



```
R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-add 192.168.1.2 192.168.1.12
R1(config)#ip dhcp pool DHCP1
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-route 192.168.1.1
R1(dhcp-config)#interface g0/1
R1(config-if)#ip add 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

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

Asignación de rango a R1 para direcciones a ser asignadas a clientes por DHCP y configuraciones para DHCP.

Configuración de parámetros DHCP S1 – puertos modo Trunk



```

Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#interface g0/1
S1(config-if)#switchport mode trunk

% Invalid input detected at '^' marker.

S1(config-if)#switchport mode trunk
S1(config-if)#
%LINK-S-CHANGED: Interface FastEthernet0/1, changed state to down

%LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down

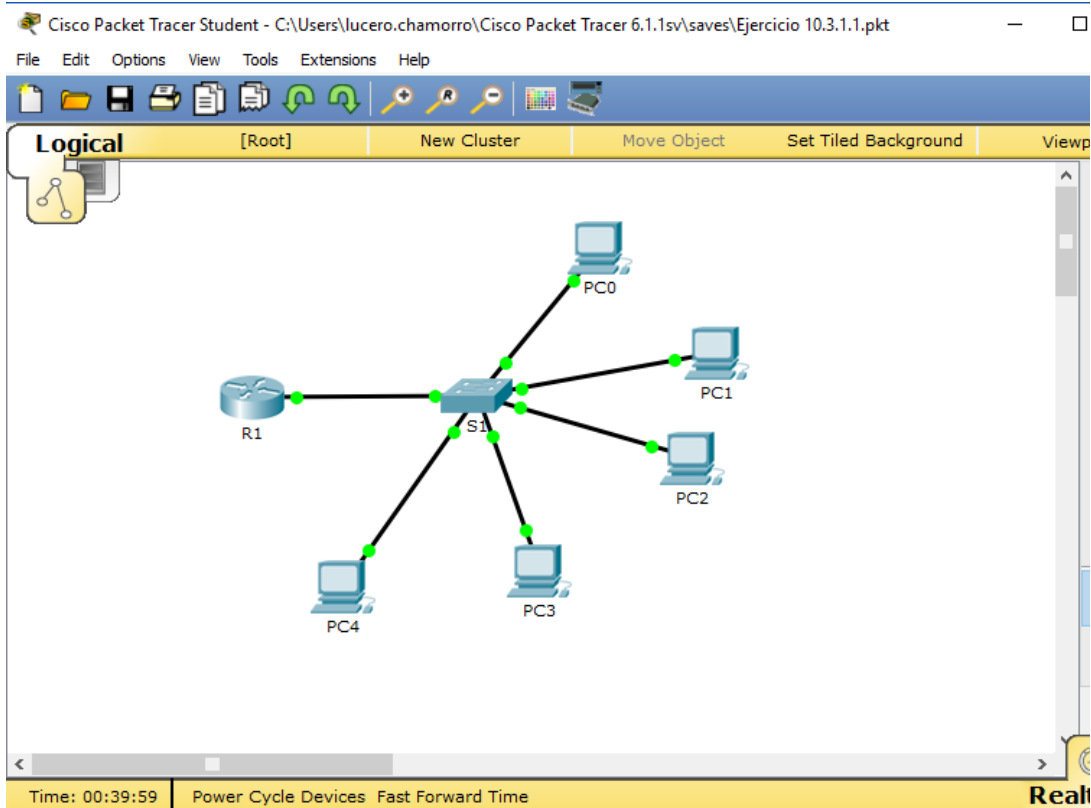
%LINK-S-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

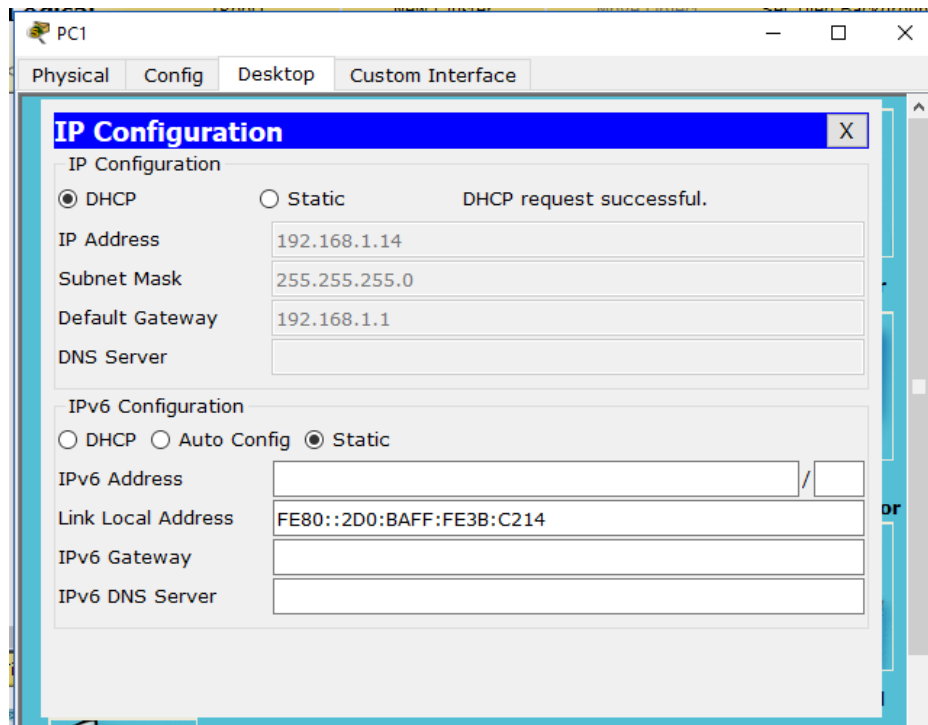
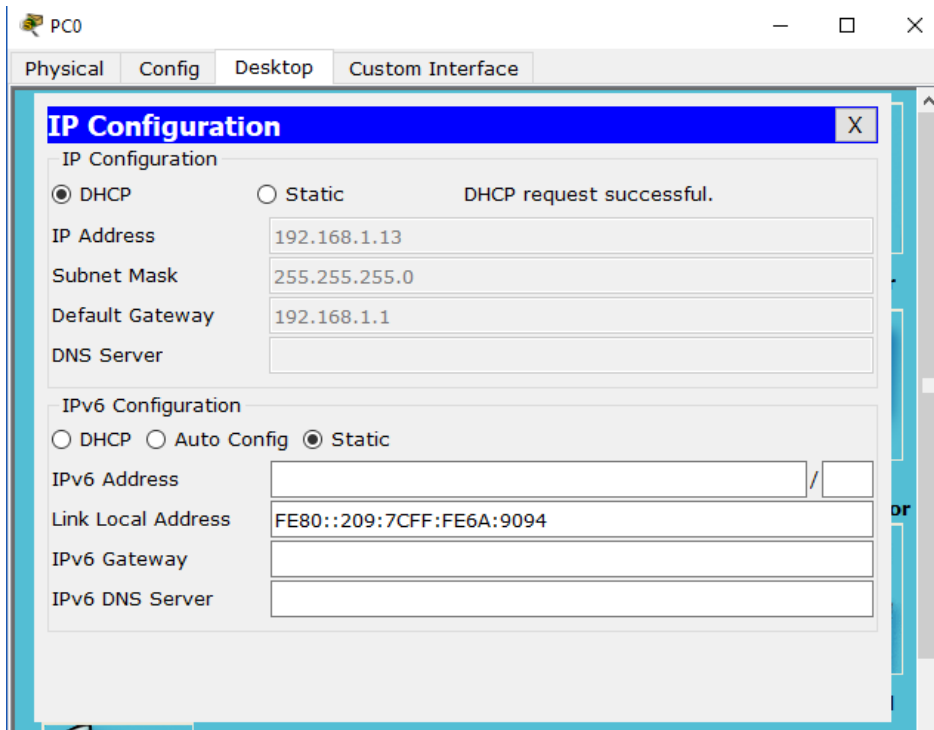
S1(config-if)#no shutdown
S1(config-if)#

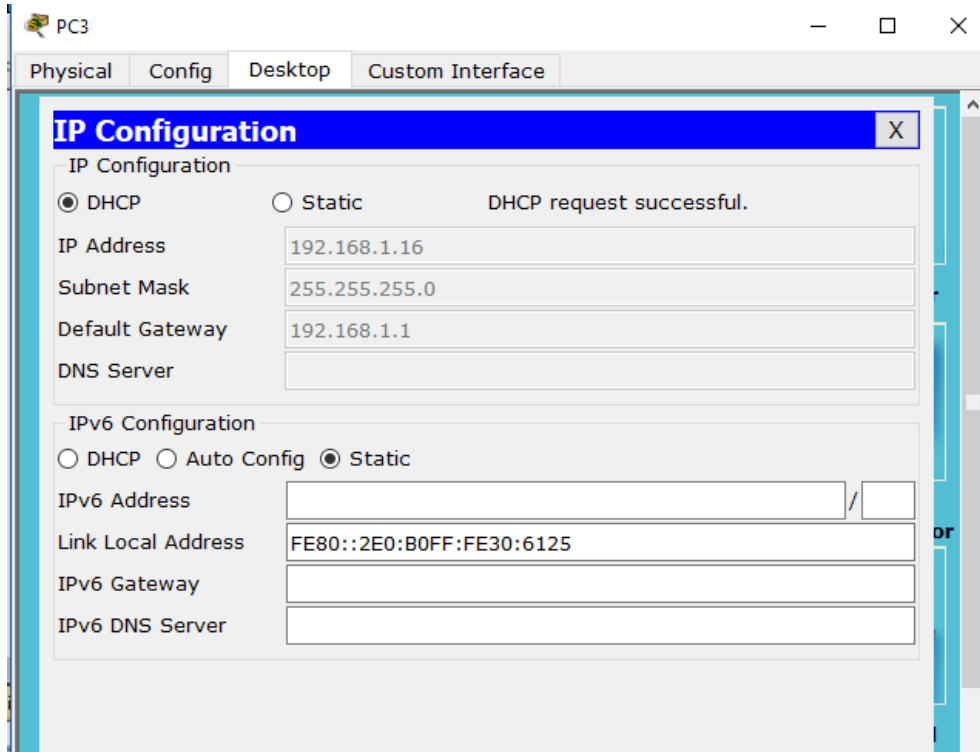
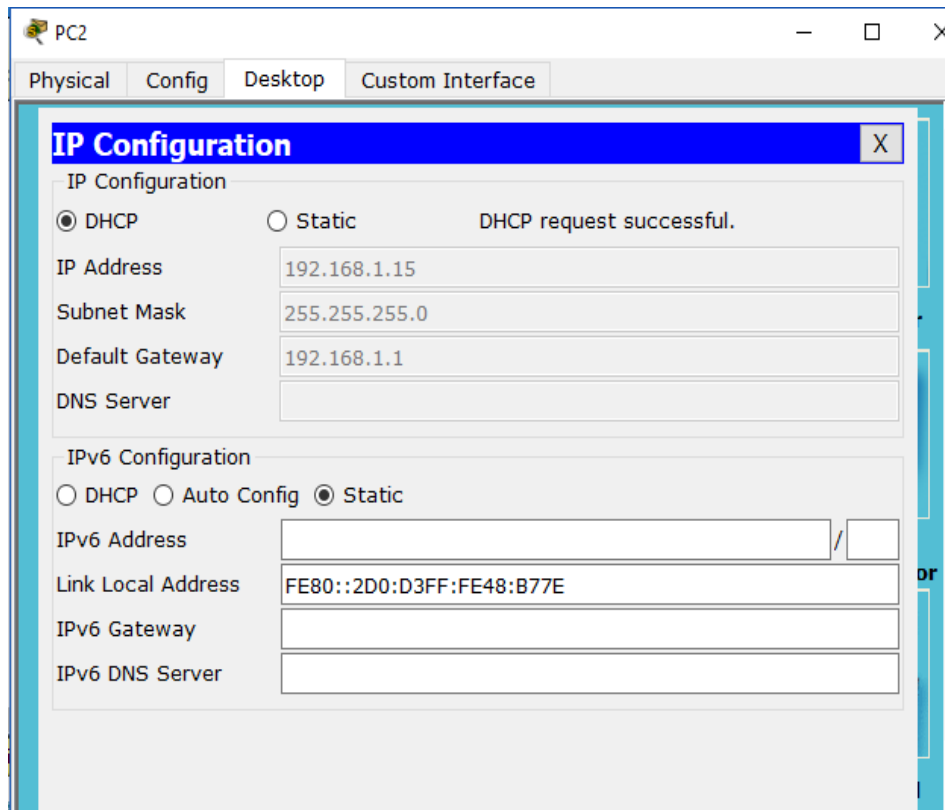
```

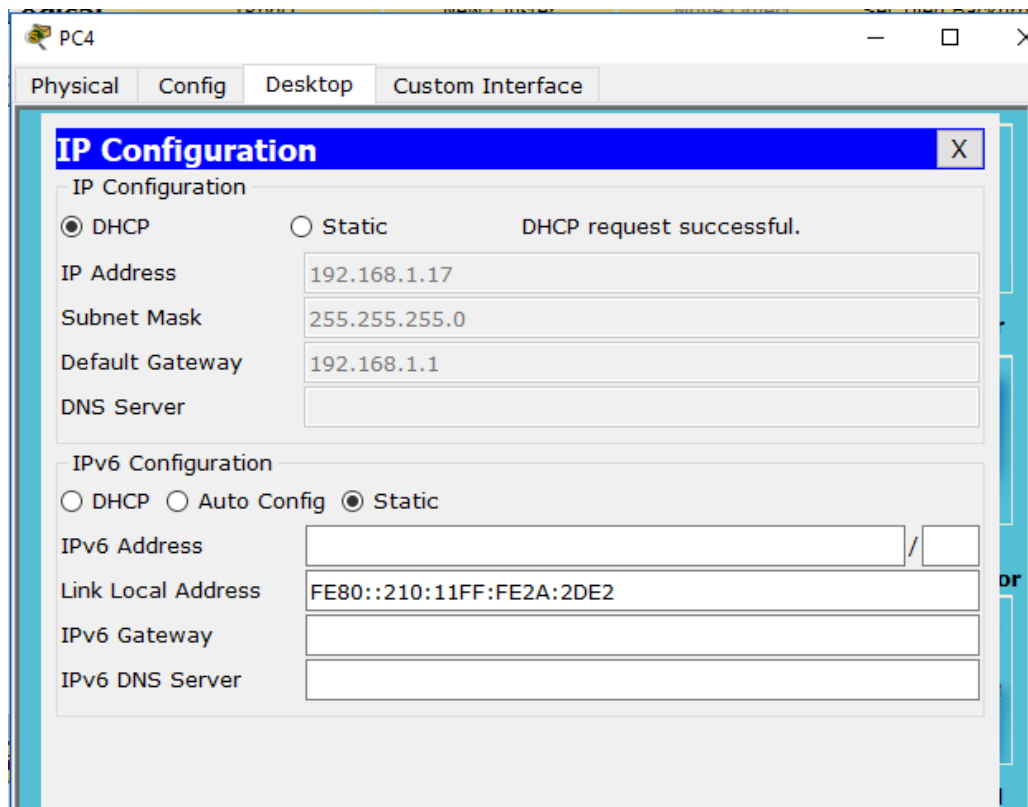
- ❖ Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones DHCP del servidor de DHCP.



- ❖ 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.

R/ Es un protocolo de comunicación realmente muy interesante e importante para optimizar procesos de configuración de grandes redes de comunicación dependiendo las necesidades de los clientes y / u organización.

Recursos necesarios

✓ Software de Packet Tracer

Reflexión

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

R/ Los dispositivos cisco brindan una mayor garantía de seguridad y adicional es fácil de configurar para servidor DHCP.

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

- Para la optimización de administración de redes.
- Para la asignación de rangos específicos a ciertas áreas específicas.
- Para la identificación de grupos de usuarios como visitantes.
- Para configuraciones de clientes en redes centralizadas.
- Por temas de compatibilidad con clientes locales y remotos.

Práctica de laboratorio 11.2.2.6: configuración de NAT dinámica y estática

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

Parte 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.

Paso 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.

Paso 2: configurar los equipos host.

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

Paso 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.

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

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

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

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

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

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

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

Paso 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
```

- 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
```

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

Paso 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.
- 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.

Parte 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.

Paso 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
```

Paso 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
```

Paso 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
```

```
--- 209.165.200.225
```

```
Inside local
```

```
192.168.1.20
```

```
Outside local
```

```
---
```

```
Outside global
```

```
---
```

¿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 administrador de la estación de trabajo

¿Quién asigna la dirección local interna?

El administrador de la estación de trabajo

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

```
Gateway# show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global icmp 209.165.200.225:1  
192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
```

```
--- 209.165.200.225 192.168.1.20 --- ---
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP?

Este número varía

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

icmp 209.165.200.225:1

Inside local

192.168.1.20:1

Outside local

192.31.7.1:1

Outside global

192.31.7.1:1

```
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23 ---
209.165.200.225 192.168.1.20 --- ---
```

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

¿Qué protocolo se usó para esta traducción? tcp

¿Cuáles son los números de puerto que se usaron?

Global/local interno: 1034 (varía)

Global/local externo: 23

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

e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

Gateway# show ip nat translations

```
Pro Inside global Inside local Outside local Outside global icmp 209.165.200.225:12
192.168.1.20:12 209.165.201.17:12 209.165.201.17:12 --- 209.165.200.225 192.168.1.20 --
- ---
```

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

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

```
Gateway# show ip nat statics
```

```
Total active translations: 2 (1 static, 1 dynamic; 1 extended) Peak translations: 2, occurred 00:02:12 ago
```

```
Outside interfaces: Serial0/0/1
```

```
Inside interfaces: GigabitEthernet0/1
```

```
Hits: 39 Misses: 0
```

```
CEF Translated packets: 39, CEF Punted packets: 0 Expired translations: 3
```

```
Dynamic mappings:
```

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

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

Parte 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.

Paso 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
```

Paso 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
```

Paso 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.

Paso 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
```

Paso 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
```

Paso 6: probar la configuración.

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

```
Gateway# show ip nat translations
```

```
Pro Inside global
```

```
--- 209.165.200.225
```

```
Inside local
```

```
192.168.1.20
```

```
Outside local
```

```
---
```

```
Outside global
```

```
---
```

```
icmp 209.165.200.242:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1 --- 209.165.200.242 192.168.1.21 --- ---
```

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

192.168.1.21 = 209.165.200.242

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

¿Qué número de puerto se usó en este intercambio ICMP?

El número es variable

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

--- 209.165.200.225

Inside local

192.168.1.20

Outside local

Outside global

```
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80 tcp 209.165.200.242:1039
192.168.1.21:1039 192.31.7.1:80 tcp 209.165.200.242:1040 192.168.1.21:1040
192.31.7.1:80 tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80 tcp
209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80 tcp 209.165.200.242:1043
192.168.1.21:1043 192.31.7.1:80 tcp 209.165.200.242:1044 192.168.1.21:1044
192.31.7.1:80 tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80 tcp
209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80 tcp 209.165.200.242:1047
192.168.1.21:1047 192.31.7.1:80 tcp 209.165.200.242:1048 192.168.1.21:1048
192.31.7.1:80 tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80 tcp
209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80 tcp 209.165.200.242:1051
192.168.1.21:1051 192.31.7.1:80
```

Tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80

```
192.31.7.1:80 192.31.7.1:80 192.31.7.1:80 192.31.7.1:80 192.31.7.1:80 192.31.7.1:80
192.31.7.1:80 192.31.7.1:80 192.31.7.1:80 192.31.7.1:80 192.31.7.1:80 192.31.7.1:80
192.31.7.1:80 192.31.7.1:80
```

192.31.7.1:80

--- 209.165.200.242 192.168.1.22 --- ---

¿Qué protocolo se usó en esta traducción? tcp

¿Qué números de puerto se usaron?

Interno: 1038 a 1052

Externo: 80

¿Qué número de puerto bien conocido y qué servicio se usaron? Port 80, HTTP

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

Gateway# show ip nat statistics

Total active translations: 3 (1 static, 2 dynamic; 1 extended) Peak translations: 17, occurred 00:06:40 ago

Outside interfaces: Serial0/0/1

Inside interfaces: GigabitEthernet0/1

Hits: 345 Misses: 0

CEF Translated packets: 345, CEF Punted packets: 0 Expired translations: 20

Dynamic mappings: -- Inside Source [Id: 1] access-list 1 pool public_access refcount 2

pool public_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 1 (7%), misses 0

Práctica de laboratorio 11.2.3.7: configuración de un conjunto de NAT con sobrecarga y PAT

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar un conjunto de NAT con sobrecarga

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones

IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

En la parte 2, el ISP asignó una única dirección IP, 209.165.201.18, a su empresa para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Usará la traducción de la dirección del puerto (PAT) para convertir varias direcciones internas en la única dirección pública utilizable. Se probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

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

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

Recursos necesarios

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

1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet y seriales, como se muestra en la topología

armar la red y verificar la conectividad

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

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

Configurar los equipos host.

Inicializar y volver a cargar los routers y los switches.

Configurar los parámetros básicos para cada router.

Desactive la búsqueda del DNS.

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

Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

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

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

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

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

Configurar el routing estático.

Cree una ruta estática desde el router ISP hasta el router Gateway.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

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
```

Verificar la conectividad de la red

Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

Verifique que las rutas estáticas estén bien configuradas en ambos routers.

Configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

Definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
```

definir la NAT desde la lista de origen interna hasta el conjunto externo.

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

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**

Verificar la configuración del conjunto de NAT con sobrecarga.

Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.

Muestre las estadísticas de NAT en el router Gateway.

Gateway# show ip nat statistics

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:25 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 3

pool public_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

Muestre las NAT en el router Gateway.

Gateway# show ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:0 192.168.1.20:1 192.31.7.1:1 192.31.7.1:0

icmp 209.165.200.225:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1

icmp 209.165.200.225:2 192.168.1.22:1 192.31.7.1:1 192.31.7.1:2

Nota: es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? 3

¿Cuántas direcciones IP globales internas se indican? 1

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? 3

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A?
¿Por qué?

El ping fallaría debido a que el router conoce la ubicación de la dirección global interna en la tabla de routing, pero la dirección local interna no se anuncia.

Configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Borrar las NAT y las estadísticas en el router Gateway.

Verificar la configuración para NAT.

Verifique que se hayan borrado las estadísticas.

Verifique que las interfaces externa e interna estén configuradas para NAT.

Verifique que la ACL aún esté configurada para NAT.

¿Qué comando usó para confirmar los resultados de los pasos a al c?

```
show ip nat statistics
```

Eliminar el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
```

Eliminar la traducción NAT de la lista de origen interna al conjunto externo.

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

Asociar la lista de origen a la interfaz externa.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload
```

Probar la configuración PAT.

Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.

Muestre las estadísticas de NAT en el router Gateway.

```
Gateway# show ip nat statistics
```

```
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
```

```
Peak translations: 3, occurred 00:00:19 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```

```
GigabitEthernet0/1
```

```
Hits: 24 Misses: 0
```

```
CEF Translated packets: 24, CEF Punted packets: 0
```

```
Expired translations: 0
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3
```

```
Total doors: 0
```

```
Appl doors: 0
```

```
Normal doors: 0
```

```
Queued Packets: 0
```

Muestre las traducciones NAT en el Gateway.

```
Gateway# show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
```

```
icmp 209.165.201.18:3 192.168.1.20:1 192.31.7.1:1 192.31.7.1:3
```

```
icmp 209.165.201.18:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1
```

```
icmp 209.165.201.18:4 192.168.1.22:1 192.31.7.1:1 192.31.7.1:4
```

Reflexión

¿Qué ventajas tiene la PAT?

Las respuestas varían, pero deben incluir que PAT minimiza la cantidad de direcciones públicas necesarias para proporcionar acceso a Internet y que los servicios de PAT, como los de NAT, sirven para “ocultar” las direcciones privadas de las redes externas.

CONCLUSIONES

Con el desarrollo de la actividad se adquiere los conocimientos para permitir el direccionamiento mediante interfaces específicas en el router que estemos trabajando, y como evidenciamos en la práctica podremos evitar fallas generadas por presencia de bucles en los host.

Con las prácticas realizadas se logró conocer que los ACLs de IPv6 permiten bloquear o impedir el acceso o permitir acceso según configuración de dicha listas, lo que nos favorece redundando en la seguridad de la red que estemos administrando.

La finalidad del desarrollo de los laboratorios, fue el manejo de la configuración de direccionamiento IPV6 en un host mediante SLAACs y la configuración del protocolo DHCPv6 que establece automáticamente los direccionamientos a los host, pero para esta actividad se especificó los dos usos de DHCPv6 que son con estado y sin estado donde con estado toda la información de direccionamiento debe obtenerse desde el servidor DHCPv6 y sin estado no utiliza el servidor.

BIBLIOGRAFÍA

Guías de Packet tracer, capitulos del 7 al 11 del curso CCNA 2. Disponibles en <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html>