

Universidad Nacional Abierta y a Distancia

UNAD

Diplomado de profundización Cisco

CCNA2 R&S UNIDAD 4

Magda Niño Rocha Cód. 52373378  
Jeison Haver Cuervo Cód. 86086608  
Omar Hernando González Cód. 79578671  
Oscar Hernán Cortez Cód. 17688765  
Cristian Sebastián Pérez Cód. 1038359384

Tutor  
Efraín Alejandro Pérez

Julio de 2017

**Resumen**

En este trabajo se logra describir cómo crear y configurar un nuevo servidor de Protocolo de configuración dinámica de host (DHCP). El servicio DHCP ofrece a los clientes direcciones IP e información como la ubicación de su puerta de enlace, o gateway, predeterminada, servidores de Sistema de nombres de dominio (DNS).

## Tabla de contenido

|   |     |
|---|-----|
| Resumen.....  | 2   |
| Introducción .....  | 4   |
| 4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks ..... | 5   |
| 7.3.2.4 Lab - Configuring Basic RIPv2 and RIPv6 .....               | 12  |
| 8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2.....             | 36  |
| 8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3.....             | 73  |
| 9.2.1.10 Packet Tracer Configuring Standard ACLs .....              | 115 |
| 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs .....      | 119 |
| 9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines.....        | 125 |
| 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs .....                 | 131 |
| 10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router .....           | 141 |
| 10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch .....           | 152 |
| 10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6.....       | 168 |
| 10.3.1.1 IoE and DHCP Instructions .....                            | 192 |
| 11.2.2.6 Lab - Configuring Dynamic and Static NAT.....              | 197 |
| 11.2.3.7 Lab - Configuring NAT Pool Overload and PAT.....           | 218 |
| Conclusiones.....   | 226 |
| Bibliografía .....  | 227 |

## **Introducción**

El protocolo Internet versión 6 (IPv6) es una nueva versión de IP (*Internet Protocol*), diseñada para reemplazar a la versión 4 (IPv4), que actualmente está implementada en la gran mayoría de dispositivos que acceden a Internet. IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso.

Se calcula que, actualmente, las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas

El reciente crecimiento exponencial de Internet y el agotamiento inminente del espacio de direcciones IPv4. Las direcciones IPv4 han empezado a escasear relativamente, lo que ha obligado a algunas organizaciones a utilizar un traductor de direcciones de red (NAT, Network Address Translator) para asignar múltiples direcciones privadas a una única dirección IP pública. Si bien los NAT fomentan la reutilización del espacio de direcciones privadas.

#### 4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks

### Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

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

- From the command prompt, ping **PC-C** (192.168.3.3).
- From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username SSHadmin and password ciscosshpa55. When finished, exit the SSH session.

```
PC> ssh -l SSHadmin 192.168.2.1
```

```
C:\>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=3ms 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 = 3ms, Average = 2ms

C:\>ssh -l SSHadmin 192.168.2.1
Invalid Command.

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

R2#exit
```

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

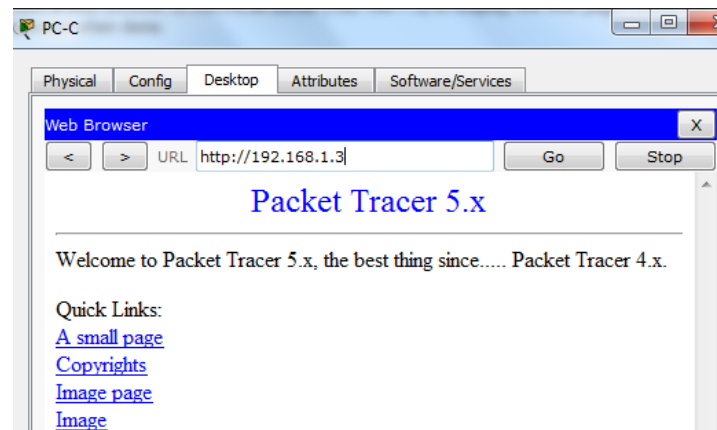
- From the command prompt, ping **PC-A** (192.168.1.3).
- From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username SSHadmin and password ciscosshpa55. Close the SSH session when finished.

```

PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>pnig 192.168.1.3
Invalid Command.
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=13ms TTL=125
Reply from 192.168.1.3: bytes=32 time=14ms TTL=125
Reply from 192.168.1.3: bytes=32 time=12ms TTL=125
Reply from 192.168.1.3: bytes=32 time=11ms TTL=125
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 14ms, Average = 12ms
C:\>ssh -l SSHAdmin 192.168.2.1
Open
Password:

```

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



## Part 2: Secure Access to Routers

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

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

```

Press RETURN to get started!

User Access Verification

Password:

R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3
R1(config)#

```

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

```
R3>enable
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#
```

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

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

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

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

```
C:\>ssh -l SSHadmin 192.168.2.1
Open
Password:
% Password: timeout expired!
% Login invalid

[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.2.1
Open
Password:
a. R2#exit
```

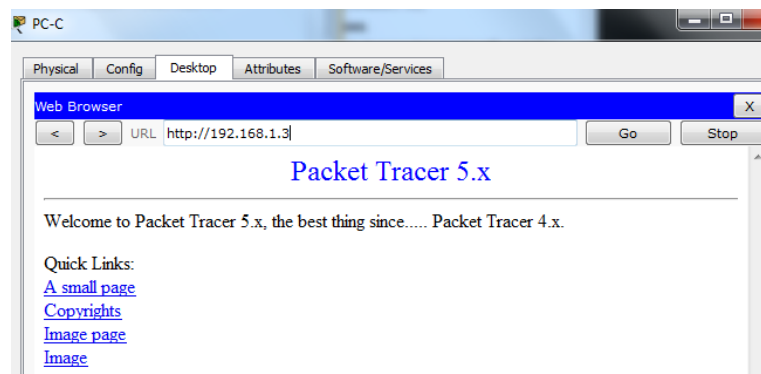
```
C:\>ssh -l SSHadmin 192.168.2.1
% Connection refused by remote host
C:\>
```

## Part 3: Create a Numbered IP ACL 120 on R1

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

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

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



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

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

```
R1#line vty 0 4
  ^
% Invalid input detected at '^' marker.

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#
R1(config-line)#exit
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
```

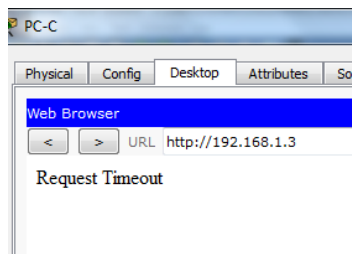
## Step 3: Apply the ACL to interface S0/0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0.

```
R1(config)#access-list 120 permit tcp host 192.168.3.3 host
10.1.1.1 eq 22
R1(config)#
```

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

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



## Part 4: Modify An Existing ACL on R1

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



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

```
C:\>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.

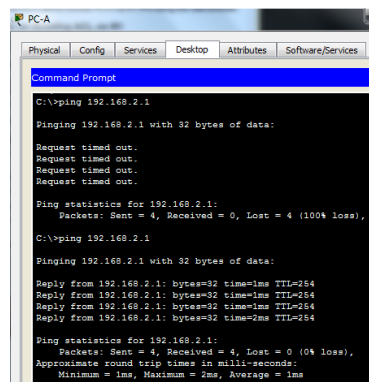
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

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

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

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



```
PC-A
Physical Config Services Desktop Attributes Software/Services
Command Prompt
C:\>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),

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=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
Reply from 192.168.2.1: bytes=32 time=2ms 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
```

## Part 5: Create a Numbered IP ACL 110 on R3

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

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

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

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

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

## Part 6: Create a Numbered IP ACL 100 on R3

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

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

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).

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

### Step 2: Apply the ACL to interface Serial 0/0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.

```
R3(config)#interface f0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#exit
R3(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255
% Incomplete command.
R3(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq
22host 192.168.3.3

% Invalid input detected at '^' marker.

R3(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq
22 host 192.168.3.3
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 15.255.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.255.255.255 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)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#
```

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

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

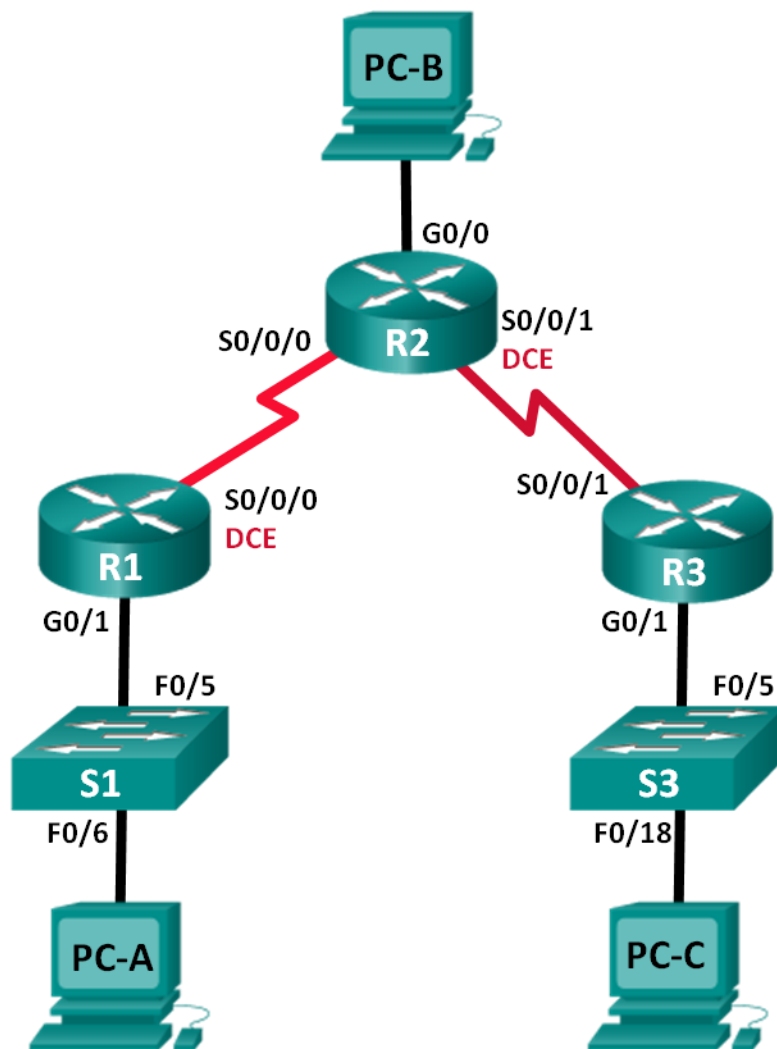
### Step 4: Check results.

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

```
R3(config-if)#do sh access-list
Standard IP access list 10
 10 permit host 192.168.3.3
Extended IP access list 110
 10 permit ip 192.168.3.0 0.0.0.255 any (4 match(es))
Extended IP access list 100
 10 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
 20 deny ip 10.0.0.0 0.255.255.255 any (559 match(es))
 30 deny ip 160.0.0.0 15.255.255.255 any
 40 deny ip 192.0.0.0 0.255.255.255 any
 50 deny ip 127.0.0.0 0.255.255.255 any
 60 deny ip 224.0.0.0 15.255.255.255 any
 70 permit ip any any
```

### 7.3.2.4 Lab - Configuring Basic RIPv2 and RIPvng

#### Topología



### Tabla de direccionamiento

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

### Objetivos

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

#### Parte 2: configurar y verificar el routing RIPv2

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

#### Parte 3: configurar IPv6 en los dispositivos

#### Parte 4: configurar y verificar el routing RIPv2

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

### Información básica/situación

RIP versión 2 (RIPv2) se utiliza para enrutar direcciones IPv4 en redes pequeñas. RIPv2 es un protocolo de routing vector distancia sin clase, según la definición de RFC 1723. Debido a

que RIPv2 es un protocolo de routing sin clase, las máscaras de subred se incluyen en las actualizaciones de routing. De manera predeterminada, RIPv2 resume automáticamente las redes en los límites de redes principales. Cuando se deshabilita la sumarización automática, RIPv2 ya no resume las redes a su dirección con clase en routers fronterizos.

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

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

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

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

## Recursos necesarios

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

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

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

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

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

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

- a. Desactive la búsqueda del DNS.
- b. Configure los nombres de los dispositivos como se muestra en la topología.

- c. Configurar la encriptación de contraseñas.
- d. Asigne **class** como la contraseña del modo EXEC privilegiado.
- e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- g. Configure **logging synchronous** para la línea de consola.

```

Router#config t
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd !
Enter TEXT message. End with the character '!'.

*****
*****
*****ACCESO SOLO A USUARIOS AUTORIZADOS*****
*****
!

R1(config)#LINE CON 0
R1(config-line)#LOGGING SYNCHRONOUS
R1(config-line)#interface vlan 1
R1(config-if)#description vlan 1
R1(config-if)#exit
R1(config)#
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

```

- h. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- i. Configure una descripción para cada interfaz con una dirección IP.
- j. Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.
- k. Copie la configuración en ejecución en la configuración de inicio.

```

R1(config)#int g0/1
R1(config-if)#ip address 172.30.10.1
R1(config-if)#ip address 172.30.10.1 255.255.255.0

% Invalid input detected at '^' marker.

R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#no shutdown

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

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

R1(config-if)#int s0/0/0
R1(config-if)#ip address 10.1.1.1
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

```

#### Paso 4. configurar los equipos host.

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

| IP Configuration           |   |
|----------------------------|---|
| IP Configuration           |   |
| <input type="radio"/> DHCP | <input checked="" type="radio"/> Static |
| IP Address                 | 172.30.10.3                             |
| Subnet Mask                | 255.255.255.0                           |
| Default Gateway            | 172.30.10.1                             |
| DNS Server                 |   |

#### Paso 5. Probar la conectividad.

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

- Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.
- Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.



```

R1#ping 172.30.10.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.10.3, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3
ms

```

## Parte 2: configurar y verificar el routing RIPv2

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

### Paso 1. Configurar el enrutamiento RIPv2.

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

```

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

```

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

- b. Configure RIPv2 en el R3 y utilice la instrucción **network** para agregar las redes apropiadas y evitar actualizaciones de routing en la interfaz LAN.
- c. Configure RIPv2 en el R2. No anuncie la red 209.165.201.0.

```

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.1.1.0
R2(config-router)#network 10.2.2.0
R2(config-router)#
R2(config-router)#exit|

router rip
version 2
passive-interface GigabitEthernet0/0
network 10.0.0.0
network 172.30.0.0

```

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

## Paso 2. examinar el estado actual de la red.

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

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

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

- b. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? no\_ ¿Por qué? No esta publicada la dir de b aun\_\_\_\_\_

¿Es posible hacer ping de la PC-A a la PC-C? si ¿Por qué? \_por esta notificada\_\_

¿Es posible hacer ping de la PC-C a la PC-B? \_no\_ ¿Por qué? \_\_\_\_\_

¿Es posible hacer ping de la PC-C a la PC-A? \_si\_ ¿Por qué? \_\_esta publicada y xuste un camino para comunicarse\_\_\_\_\_

- c. Verifique que RIPv2 se ejecute en los routers.

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

```
R1# show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
```

```

Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0        2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway           Distance      Last Update
  10.1.1.2           120
Distance: (default is 120)

```

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

```

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

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

```

---

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

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

```

interface GigabitEthernet0/1
 ip address 172.30.30.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
!
interface Vlan1
 description vlan 1
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface GigabitEthernet0/1
 network 10.0.0.0
 network 172.30.0.0

```

d. Examinar el sumarización automática de las rutas.

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

R2# **show ip route**

<Output Omitted>

```

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

```

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

R1# **show ip route**

<Output Omitted>

```

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1

```

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

R3# **show ip route**

<Output Omitted>

```

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

```

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

```

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

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#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#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.0.0/16 via 0.0.0.0 in 1 hops

```

---

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

### Paso 3. Desactivar la sumarización automática.

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

```

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

```

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

```

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

```

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

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

R2# **show ip route**

<Output Omitted>

Gateway of last resort is not set

```

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

```

R1# **show ip route**

<Output Omitted>

Gateway of last resort is not set

```

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

```

R3# **show ip route**

<Output Omitted>

```

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

```

```

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.2/32 is directly connected, Serial0/0/0
C    10.2.2.0/30 is directly connected, Serial0/0/1
L    10.2.2.2/32 is directly connected, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
R    172.30.0.0/16 [120/1] via 10.1.1.1, 00:02:51, Serial0/0/0
      [120/1] via 10.2.2.1, 00:00:11, Serial0/0/1
R    172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:05,
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
--More-- 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#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.10.0/24 via 0.0.0.0 in 1 hops

```

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

R2# **debug ip rip**

```

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
      172.30.0.0/16 via 0.0.0.0, metric 2, 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
      172.30.0.0/16 via 0.0.0.0, metric 2, tag 0

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

```

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

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

\_10.2.2.2 172.30.30.0 \_\_\_\_\_

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

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

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

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

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#router rip
```

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

```
R2(config)# router rip
```

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

```

      P - periodic downloaded static route

Gateway of last resort is 209.165.201.2 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C   10.1.1.0/30 is directly connected, Serial0/0/0
L   10.1.1.2/32 is directly connected, Serial0/0/0
C   10.2.2.0/30 is directly connected, Serial0/0/1
L   10.2.2.2/32 is directly connected, Serial0/0/1
 172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
R   172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:24, Serial0/0/1
R   172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:12,
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
S*  0.0.0.0/0 [1/0] via 209.165.201.2

```

### Paso 5. Verificar la configuración de enrutamiento.

- c. Consulte la tabla de routing en el R1.

```
R1# show ip route
```



```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
R    10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:18, Serial0/0/0
172.30.0.0/16 is variably subnetted, 3 subnets, 3 masks
R    172.30.0.0/16 [120/2] via 10.1.1.2, 00:00:18, Serial0/0/0
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R*  0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:18, Serial0/0/0

R1#

```

<Output Omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

R\* 0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0

172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks

C 172.30.10.0/24 is directly connected, GigabitEthernet0/1

L 172.30.10.1/32 is directly connected, GigabitEthernet0/1

R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0

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

\_la ruta estática esta publicada en los routers 1 y 3\_

- d. Consulte la tabla de routing en el R2.

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

\_\_\_publicando a los demás router la ruta estática\_\_\_\_\_

## Paso 6. Verifique la conectividad.

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

```

C:\>tracert 172.30.30.3

Tracing route to 172.30.30.3 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    172.30.10.1
  1  0 ms    *        0 ms    172.30.10.1
  2  *        1 ms    *        Request timed out.
  3  0 ms    *        0 ms    172.30.10.1
  4  *        0 ms

Control-C
^C
C:\>
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=10ms TTL=126
Reply from 209.165.201.2: bytes=32 time=11ms TTL=126
Reply from 209.165.201.2: bytes=32 time=11ms TTL=126
Reply from 209.165.201.2: bytes=32 time=12ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 12ms, Average = 11ms

```

¿Tuvieron éxito los pings? si

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

```

C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=14ms TTL=125
Reply from 172.30.30.3: bytes=32 time=11ms TTL=125
Reply from 172.30.30.3: bytes=32 time=12ms TTL=125
Reply from 172.30.30.3: bytes=32 time=11ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 14ms, Average = 12ms

```

¿Tuvieron éxito los pings? si

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

### 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<br>FE80::1 link-local  | No aplicable           |
|             | S0/0/0   | 2001:DB8:ACAD:12::1/64<br>FE80::1 link-local | No aplicable           |
| R2          | G0/0     | 2001:DB8:ACAD:B::2/64<br>FE80::2 link-local  | No aplicable           |
|             | S0/0/0   | 2001:DB8:ACAD:12::2/64<br>FE80::2 link-local | No aplicable           |
|             | S0/0/1   | 2001:DB8:ACAD:23::2/64<br>FE80::2 link-local | No aplicable           |
| R3          | G0/1     | 2001:DB8:ACAD:C::3/64<br>FE80::3 link-local  | No aplicable           |
|             | S0/0/1   | 2001:DB8:ACAD:23::3/64<br>FE80::3 link-local | No aplicable           |
| PC-A        | NIC      | 2001:DB8:ACAD:A::A/64                        | FE80::1                |
| PC-B        | NIC      | 2001:DB8:ACAD:B::B/64                        | FE80::2                |
| PC-C        | NIC      | 2001:DB8:ACAD:C::C/64                        | FE80::3                |

#### Paso 1. configurar los equipos host.

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

#### Paso 2. configurar IPv6 en los routers.

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

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

```

R1#config 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)#FE80::1 link-local
^
% Invalid input detected at '^' marker.

R1(config-if)#ipv6 FE80::1 link-local
^
% Invalid input detected at '^' marker.

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

```

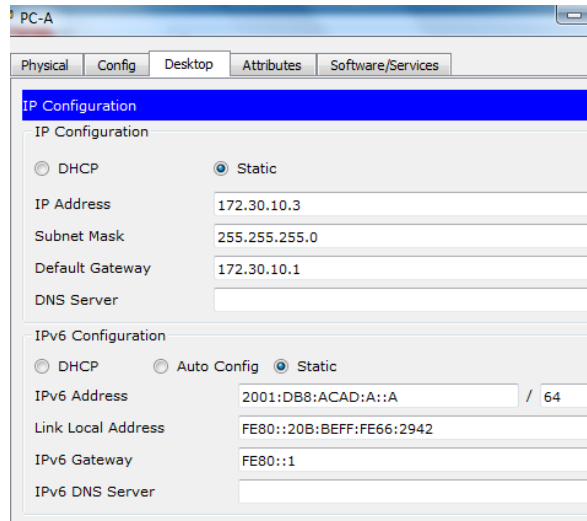
---

```

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

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

```



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

```
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]
---
```

\_\_\_\_\_ show ipv6 interface  
brief \_\_\_\_\_

- d. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.
- e. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

```

C:\>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=40ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time<1ms 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 = 40ms, Average = 10ms

```

#### 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.

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

```

R1(config)# interface g0/1
R1(config)# ipv6 rip Test1 enable
R1(config)# interface s0/0/0
R1(config)# ipv6 rip Test1 enable

```
- Configure RIPng para las interfaces seriales en el R2, con **Test2** como el nombre de proceso. No lo configure para la interfaz G0/0
- Configure RIPng para cada interfaz en el R3, con **Test3** como el nombre de proceso.
- Verifique que RIPng se esté ejecutando en los routers.

```

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

```

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

```

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

```

¿En qué forma se indica RIPng en el resultado?

\_\_\_\_\_ IPv6 Routing Protocol is "rip Test1"

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

```

R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 314
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 1, trigger updates 0
  Full Advertisement 0, Delayed Events 0
  Interfaces:
    GigabitEthernet0/1

```

```

Serial0/0/0
Redistribution:
None

```

¿Cuáles son las similitudes entre RIPv2 y RIPng?

\_ Métrica cuenta de saltos, 16 saltos significan infinito , Actualizaciones completas periódicamente cada 30 segundos (ligeramente variable), sirve para saber que el vecino sigue “vivo” ,Actualizaciones cada 30 segundos\_\_\_\_\_

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

```

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

```

\_\_\_\_\_ show ipv6 route \_\_\_\_\_

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

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

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

- g. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? \_\_\_\_\_ no \_\_\_\_\_

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

¿Es posible hacer ping de la PC-C a la PC-B? \_\_\_\_\_ no \_\_\_\_\_

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

¿Por qué algunos pings tuvieron éxito y otros no?

\_\_\_\_\_ no se activado rip \_\_\_\_\_

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

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



```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::0/64 2001:DB8:ACAD:B::B
```

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

```
R2(config)# int s0/0/0
R2(config-rtr)# ipv6 rip Test2 default-information originate
R2(config)# int s0/0/1
R2(config-rtr)# ipv6 rip Test2 default-information originate
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ipv6 rip test2 default-information originate
```

### Paso 3. Verificar la configuración de enrutamiento.

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

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

```

    via ::, Serial0/0/1
L   FF00::/8 [0/0]
    via ::, Null0

```

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

\_\_lo a prende por rip \_\_\_\_\_

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

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

\_\_la ruta se hace pública para los demás routers\_\_\_\_\_

#### 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.

```

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

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

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=3ms 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 = 3ms, Maximum = 11ms, Average = 9ms

```

¿Tuvieron éxito los pings? \_\_sí\_\_\_\_\_

#### Reflexión

- ¿Por qué desactivaría la sumarización automática para RIPv2?  
\_\_optimiza los recursos del router, para identificación y actualización de las rutas conectadas, para q detecte las redes y no una sola
- En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3?  
\_\_creando una ruta en R2 y además difundirla hacerla pública\_\_\_\_\_
- ¿En qué se diferencian la configuración de RIPv2 y la de RIPv6?  
Son muy parecidos pero tiene q activarse rip por interfaces y la otra global

RIPv6 es un protocolo de enrutamiento vector distancia con un límite de 15 saltos que usa actualizaciones de envenenamiento en reversa y horizonte dividido para evitar routing loops RIPv6 proviene del hecho de que no requiere ningún conocimiento global de la red. Sólo los routers vecinos intercambian mensajes locales, debe ser implementado solo en routers

\_\_\_\_\_

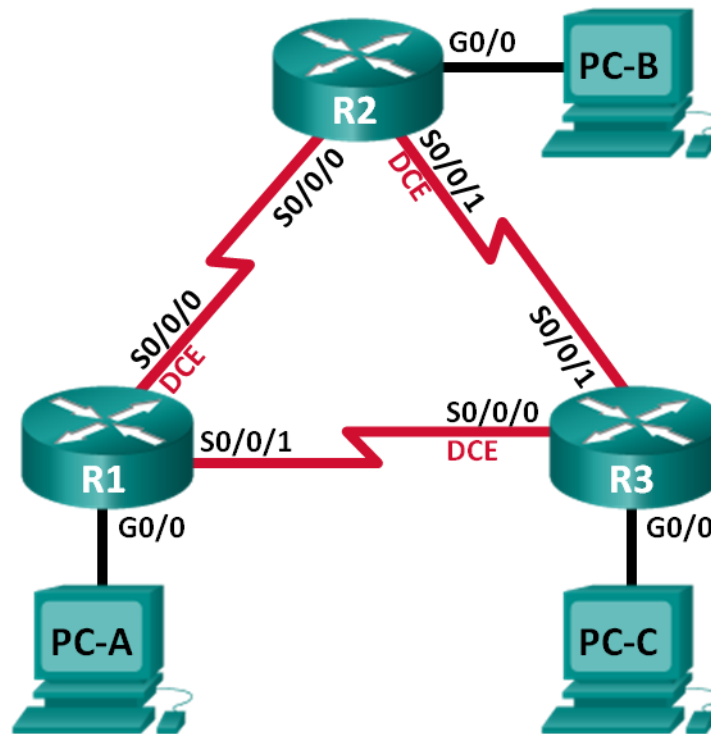
**Tabla de resumen de interfaces del router**

| Resumen de interfaces del router |                             |                             |                       |                       |
|----------------------------------|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de router                 | Interfaz Ethernet #1        | Interfaz Ethernet n.º 2     | Interfaz serial #1    | Interfaz serial n.º 2 |
| 1800                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

**Nota:** para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

### 8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2

## Topología



## Tabla de direccionamiento

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

## Objetivos

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

**Parte 2: configurar y verificar el routing OSPF**

**Parte 3: cambiar las asignaciones de ID del router**

**Parte 4: configurar interfaces OSPF pasivas**

**Parte 5: cambiar las métricas de OSPF**

## Información básica/situación

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

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

**Nota:** los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen 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

### 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.

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

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

**Step 4: configurar los parámetros básicos para cada router.**

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- e. Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.
- f. Configure **logging synchronous** para la línea de consola.
- g. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.
- i. Copie la configuración en ejecución en la configuración de inicio

```

R1
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: NO

Press RETURN to get started!

Router>ENABLE
Router#CONFIGURE T
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#hostname R1
R1 (config)#int g0/0
R1 (config-if)#ip address 192.168.12.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
R1 (config-if)#int s0/0/1
R1 (config-if)#ip address 192.168.12.1 255.255.255.252
R1 (config-if)#clock rate 128000
R1 (config-if)#no shutdown
R1 (config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1 (config-if)#int s0/0/1
R1 (config-if)#ip address 192.168.12.1 255.255.255.252
% 192.168.12.0 overlaps with Serial0/0/0
R1 (config-if)#no shutdown
% 192.168.12.0 overlaps with Serial0/0/0
Serial0/0/1: incorrect IP address assignment
R1 (config-if)#ip address 192.168.13.1 255.255.255.252
R1 (config-if)#no shutdown
R1 (config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1 (config-if)#
  
```

## Step 5: configurar los equipos host.

## Step 6: Probar la conectividad.

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

## 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.

### Step 1: Configure el protocolo OSPF en R1.

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

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

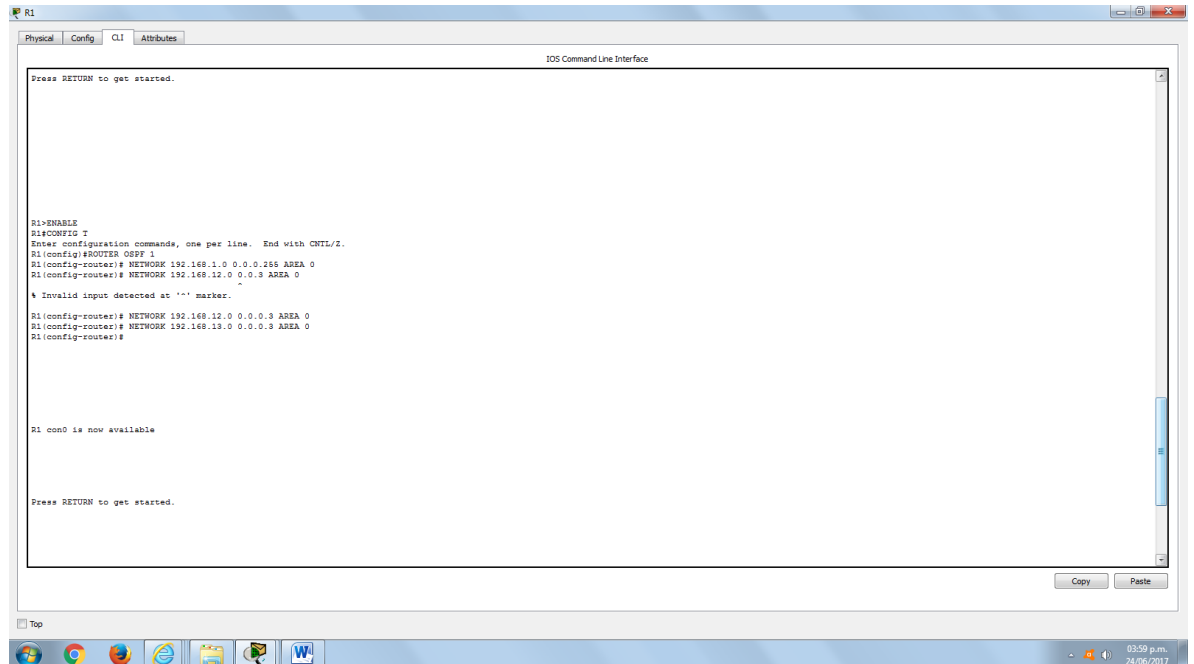
**Nota:** la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

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

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

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

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



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

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

```

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

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

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

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

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



```

R1
Physical Config CLI Attributes
IOS Command Line Interface

# Invalid input detected at "" marker.
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)#

R1 con0 is now available

Press RETURN to get started.

00:58:52: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to FULL, Loading Done

R1>END
Translating "END"...domain server (255.255.255.255)
# Unknown command or computer name, or unable to find computer address
R1>ENABLE
R1#SHOW IP OSPF NEIGHBOR

Neighbor ID      Pri  State           Dead Time   Address      Interface
192.168.23.2    0    FULL/ -         00:00:38   192.168.13.2 Serial0/0/1
R1#

```

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

R1# **show ip route**

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

Gateway of last resort is not set

```

          192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.1.0/24 is directly connected, GigabitEthernet0/0
L         192.168.1.1/32 is directly connected, GigabitEthernet0/0
O         192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O         192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
          192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.12.0/30 is directly connected, Serial0/0/0
L         192.168.12.1/32 is directly connected, Serial0/0/0
          192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.13.0/30 is directly connected, Serial0/0/1
L         192.168.13.1/32 is directly connected, Serial0/0/1
          192.168.23.0/30 is subnetted, 1 subnets
O         192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0

```

[110/128] via 192.168.13.2, 00:31:38, Serial0/0/1

```

R1>END
Translating "END"...domain server (256.256.256.256)
% Unknown command or computer name, or unable to find computer address
R1>ENABLE
R1#SHOW IP OSPF NEIGHBOR
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.2    0     FULL/-         00:00:38    192.168.13.2    Serial0/0/1
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 [110/128] via 192.168.13.2, 00:07:50, Serial0/0/1
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:08:10, Serial0/0/1
L    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
C    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.168.13.0/30 is directly connected, Serial0/0/1
L    192.168.13.1/32 is directly connected, Serial0/0/1
O    192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0/30 [110/128] via 192.168.13.2, 00:08:00, Serial0/0/1
R1#
  
```

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

```

R1>END
Translating "END"...domain server (256.256.256.256)
% Unknown command or computer name, or unable to find computer address
R1>ENABLE
R1#SHOW IP OSPF NEIGHBOR
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.2    0     FULL/-         00:00:38    192.168.13.2    Serial0/0/1
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 [110/128] via 192.168.13.2, 00:07:50, Serial0/0/1
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:08:10, Serial0/0/1
L    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
C    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.168.13.0/30 is directly connected, Serial0/0/1
L    192.168.13.1/32 is directly connected, Serial0/0/1
O    192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0/30 [110/128] via 192.168.13.2, 00:08:00, Serial0/0/1
R1#SHOW IP ROUTE OSPF
O    192.168.2.0 [110/128] via 192.168.13.2, 00:10:06, Serial0/0/1
O    192.168.3.0 [110/65] via 192.168.13.2, 00:10:26, Serial0/0/1
O    192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0 [110/128] via 192.168.13.2, 00:10:16, Serial0/0/1
R1#
  
```

#### Step 4: verificar la configuración del protocolo OSPF.

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

```
R1# show ip protocols
*** IP Routing is NSF aware ***
```

Routing Protocol is "ospf 1"

```
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
```

Router ID 192.168.13.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

```
192.168.1.0 0.0.0.255 area 0
192.168.12.0 0.0.0.3 area 0
192.168.13.0 0.0.0.3 area 0
```

Routing Information Sources:

| Gateway      | Distance | Last Update |
|--------------|----------|-------------|
| 192.168.23.2 | 110      | 00:19:16    |
| 192.168.23.1 | 110      | 00:20:03    |

Distance: (default is 110)

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

NL - OSPF NESA external type 1, N2 - OSPF NESA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, I1 - IS-IS level-1, I2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, O - per-user static route, o - ODR
D - 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 [110/129] via 192.168.13.2, 00:07:50, Serial0/0/1
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:08:10, Serial0/0/1
C 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
L 192.168.12.0/24 is directly connected, Serial0/0/0
L 192.168.12.1/32 is directly connected, Serial0/0/0
C 192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
L 192.168.13.0/30 is directly connected, Serial0/0/1
L 192.168.13.1/32 is directly connected, Serial0/0/1
O 192.168.23.0/30 is subnetted, 1 subnets
L 192.168.23.0/30 [110/128] via 192.168.13.2, 00:09:00, Serial0/0/1

R1#SHOW IP ROUTE OSPF
O 192.168.2.0 [110/129] via 192.168.13.2, 00:10:06, Serial0/0/1
O 192.168.3.0 [110/65] via 192.168.13.2, 00:10:26, Serial0/0/1
O 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:10:16, Serial0/0/1

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          00:12:59
    192.168.23.1          110          00:12:41
    192.168.23.2          110          00:12:41
  Distance: (default is 110)

R1#
```

#### Step 5: verificar la información del proceso OSPF.

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

R1# **show ip ospf**

```
Routing Process "ospf 1" with ID 192.168.13.1
Start time: 00:20:23.260, Time elapsed: 00:25:08.296
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
```

**Area BACKBONE(0)**

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

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

0 192.168.3.0 [110/68] via 192.168.13.2, 00:10:26, Serial0/0/1
0 192.168.23.0/30 is summarized, 1 subnets
0 192.168.23.0 [110/128] via 192.168.13.2, 00:10:16, Serial0/0/1

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           00:12:59
    192.168.23.1     110           00:12:41
    192.168.23.2     110           00:12:41
  Distance: (default is 110)

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 7 times
    Area ranges are
      Number of LSA 3, Checksum Sum 0x013276
      Number of opaque link LSA 0, Checksum Sum 0x000000
      Number of DCbitless LSA 0
      Number of Indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0

```

## Step 6: verificar la configuración de la interfaz OSPF.

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

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

| Interface | PID | Area | IP Address/Mask | Cost | State | Nbrs |
|-----------|-----|------|-----------------|------|-------|------|
| F/C       |     |      |                 |      |       |      |
| Se0/0/1   | 1   | 0    | 192.168.13.1/30 | 64   | P2P   | 1/1  |
| Se0/0/0   | 1   | 0    | 192.168.12.1/30 | 64   | P2P   | 1/1  |
| Gi0/0     | 1   | 0    | 192.168.1.1/24  | 1    | DR    | 0/0  |

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

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

```

Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID      Cost      Disabled   Shutdown   Topology Name
  0                  64        no         no         Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled

```

```

Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.1/30, Area 0, Attached via Network
Statement
  Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT,
Cost: 64
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
                0          64          no            no            Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:03
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.1
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
                0          1          no            no            Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0

```

Suppress hello for 0 neighbor(s)

```

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 00:00:08
Index 1/1, Flood queue length 0
Hex 0x0/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
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 00:00:08
Index 1/2, Flood queue length 0
Hex 0x0/0x0(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)
Serial0/0/1 is up, line protocol is up
Internet address is 192.168.13.1/30, 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 00:00:09
Index 2/3, Flood queue length 0
Hex 0x0/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
R1#
R1#
R1#
  
```

## Step 7: Verificar la conectividad de extremo a extremo.

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

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

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.8: bytes=32 time=3ms TTL=125
Reply from 192.168.2.8: bytes=32 time=3ms TTL=125
Reply from 192.168.2.3: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 3ms
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.8: bytes=32 time=3ms TTL=126
Reply from 192.168.3.8: bytes=32 time=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=3ms TTL=126
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms
C:\>
  
```

### 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.

#### Step 8: Cambie las ID de router con direcciones de loopback.

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

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

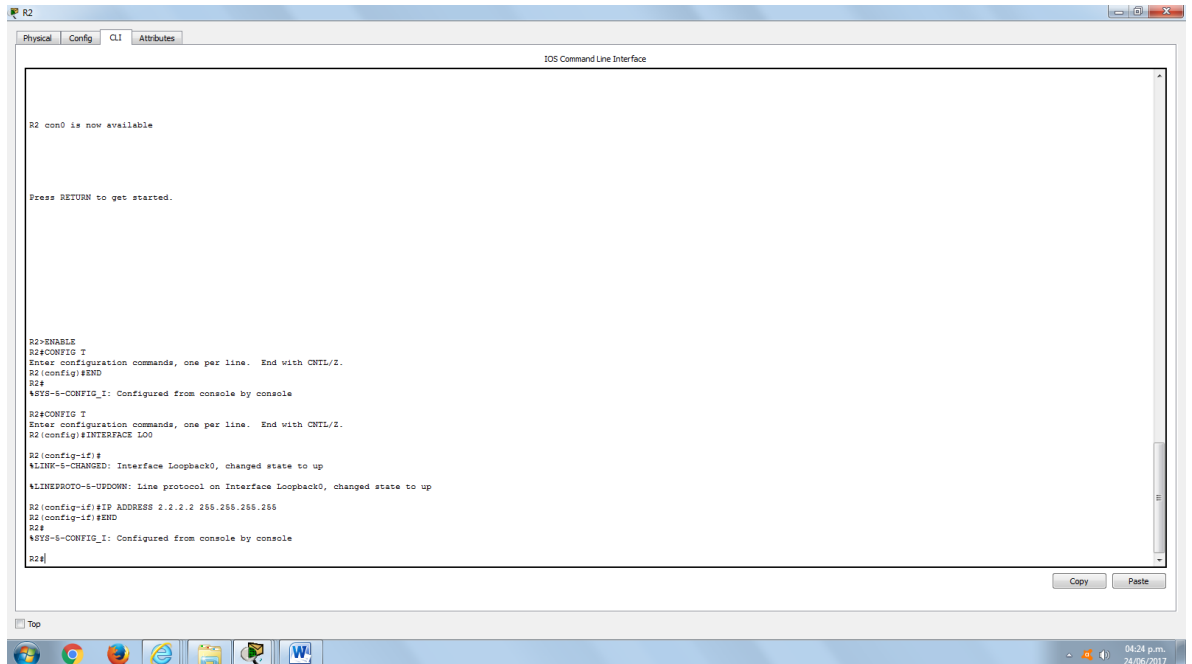
```

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 00:00:05
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)
Serial0/0/1 is up, line protocol is up
Internet address is 192.168.13.1/30, 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 00:00:09
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
R1#
R1#
R1#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#INTERFACE LO0
R1(config-if)#
%LINK-3-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)#
R1(config-if)#END
R1#
%SYS-6-CONFIG_I: Configured from console by console
R1#

```

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





The screenshot shows the CLI of router R2. The text in the terminal window is as follows:

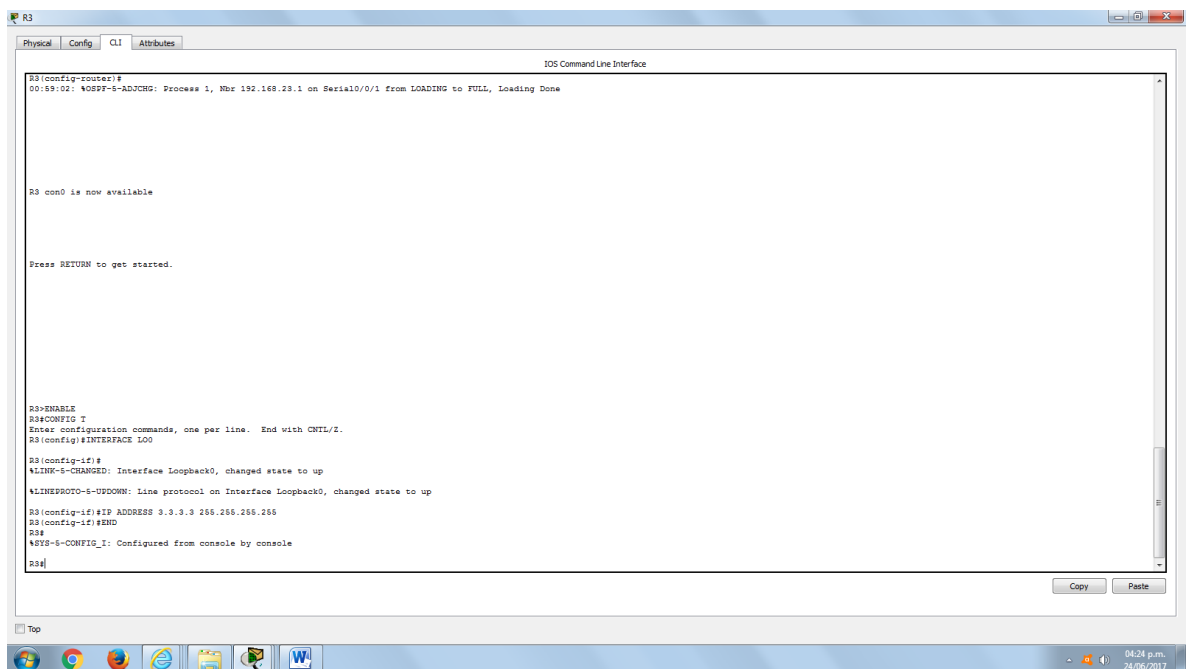
```

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

R2 con0 is now available

Press RETURN to get started.

R2>ENABLE
R2#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#END
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#INTERFACE 100
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#
R2#
  
```



The screenshot shows the CLI of router R3. The text in the terminal window is as follows:

```

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

R3 (config-router)#
00:59:02: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial10/0/1 from LOADING to FULL, Loading Done

R3 con0 is now available

Press RETURN to get started.

R3>ENABLE
R3#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R3 (config)#INTERFACE 100
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#
R3#
  
```

- c. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.
- d. Debe volver a cargar los routers para restablecer la ID del router a la dirección de loopback. Emita el comando **reload** en los tres routers. Presione Enter para confirmar la recarga.
- e. Una vez que se haya completado el proceso de recarga del router, emita el comando **show ip protocols** para ver la nueva ID del router.

```
R1# show ip protocols
*** IP Routing is NSF aware ***
```

Routing Protocol is "ospf 1"

```
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
```

Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

```
192.168.1.0 0.0.0.255 area 0
```

```
192.168.12.0 0.0.0.3 area 0
```

```
192.168.13.0 0.0.0.3 area 0
```

Routing Information Sources:

| Gateway | Distance | Last Update |
|---------|----------|-------------|
| 3.3.3.3 | 110      | 00:01:00    |
| 2.2.2.2 | 110      | 00:01:14    |

Distance: (default is 110)

```

R1
R1#
R1#CONF T
R1#
R1#CONF T
Error: configuration commands, one per line. End with CNTL/Z.
R1(config)#INTERFACE LOO
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)#
R1(config-if)#END
R1#
%SYS-5-CONFIG_I: Configured from console by console
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          00:29:48
    192.168.23.1    110          00:29:30
    192.168.23.2    110          00:29:30
  Distance: (default is 110)
R1#
  
```

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

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

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

R1 #

```

R1#
R1#
R1#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#INTERFACE LOOP
R1(config-if)#
%LINKS-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)#
R1(config-if)#END
R1#
%SYS-5-CONFIG_I: Configured from console by console
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          00:29:49
  192.168.23.1         110          00:29:30
  192.168.23.2         110          00:29:30
  Distance: (default is 110)

R1#SHOW IP OSPF NEIGHBOR
Neighbor ID Pri State Dead Time Address Interface
192.168.23.2 0 FULL/- 00:00:37 192.168.13.2 Serial0/0/1
R1#

```

### Step 9: 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**.

- 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
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)#
R1(config-if)#END
R1#
%SYS-5-CONFIG_I: Configured from console by console
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           00:29:48
    192.168.23.1     110           00:29:30
    192.168.23.2     110           00:29:30
  Distance: (default is 110)

R1#SHOW IP OSPF NEIGHBOR
Neighbor ID     Pri   State           Dead Time   Address        Interface
192.168.23.2    0     FULL/ -         00:00:37    192.168.13.2   Serial0/0/1
R1#CONFIG 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.
- 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(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#

R2 con0 is now available

Press RETURN to get started.

R2>>ENABLE
R2#CONFIG 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 (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#

R3 con0 is now available

Press RETURN to get started.

R3>ENABLE
R3#CONFIG
R3#CONFIG
Configuring from terminal, memory, or network [terminal]?
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
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
```

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

```
Routing Protocol is "ospf 1"
```

```
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set
```

```
Router ID 11.11.11.11
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

```
Maximum path: 4
```

```
Routing for Networks:
```

```
192.168.1.0 0.0.0.255 area 0
```

```
192.168.12.0 0.0.0.3 area 0
```

```
192.168.13.0 0.0.0.3 area 0
```

```
Passive Interface(s):
```

```
GigabitEthernet0/1
```

```
Routing Information Sources:
```

| Gateway     | Distance | Last Update |
|-------------|----------|-------------|
| 33.33.33.33 | 110      | 00:00:19    |
| 22.22.22.22 | 110      | 00:00:31    |
| 3.3.3.3     | 110      | 00:00:41    |
| 2.2.2.2     | 110      | 00:00:41    |

```
Distance: (default is 110)
```

```

R3
R3(config-if)#IP ADDRESS 33.33.33.266 266.266.266.266
R3(config-if)#END
R3#
*SYS-5-CONFIG_I: Configured from console by console
R3#

R3 con0 is now available

Press RETURN to get started.

R3>ENABLE
R3#CONFIG
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ROUTER OSPF 3
R3(config-router)#ROUTERS-ID 33.33.33.33
R3(config-router)#Reload or use "clear ip ospf process" command, for this to take effect
END
R3#
*SYS-5-CONFIG_I: Configured from console by console
R3#

```

- 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<br>Interface   | Pri | State   | Dead Time | Address      |
|----------------------------|-----|---------|-----------|--------------|
| 33.33.33.33<br>Serial0/0/1 | 0   | FULL/ - | 00:00:36  | 192.168.13.2 |
| 22.22.22.22<br>Serial0/0/0 | 0   | FULL/ - | 00:00:32  | 192.168.12.2 |

```

R1# show ip ospf neighbors
Routing Information Sources:
Gateway         Distance      Last Update
192.168.13.1    110           00:29:49
192.168.23.1    110           00:29:30
192.168.23.2    110           00:29:30
Distance: (default is 110)

R1# show ip ospf neighbors
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.2    0     FULL/ -         00:00:37    192.168.13.2    Serial0/0/1
R1# config 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# show ip protocols
Routing Protocol is "ospf 1"
  Output 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           00:10:28
192.168.23.1    110           00:10:09
192.168.23.2    110           00:10:09
Distance: (default is 110)

R1# show ip ospf neighbors
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.2    0     FULL/ -         00:00:37    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.

### Step 10: configurar una interfaz pasiva.

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

```

R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
  0                   1         no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:02
  Supports Link-local Signaling (LLS)

```

```

Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

```

R1
#SYS-5-CONFIG_I: Configured from console by console
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           00:10:26
    192.168.23.1     110           00:10:09
    192.168.23.2     110           00:10:09
  Distance: (default is 110)

R1#SHOW IP OSPF NEIGHBOR

Neighbor ID  Pri  State           Dead Time   Address       Interface
192.168.23.2    0  FULL/ -         00:00:37    192.168.13.2  Serial0/0/1
R1#SHOW IP OSPF INTERFACE G0/0
-
% Invalid input detected at '^' marker.

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 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 00:00:06
  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)
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
Physical Config CLI Attributes
IOS Command Line Interface

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           00:10:25
  192.168.23.1      110           00:10:08
  192.168.23.2      110           00:10:08
  Distance: (default is 110)

R1#SHOW IP OSPF NEIGHBOR

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.2    0     FULL/0         00:00:37    192.168.13.2    Serial0/0/1
R1#SHOW IP OSPF INTERFACE G0/0
^
* Invalid input detected at '^' marker.

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 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 00:00:06
  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)

R1#CONFIG 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
```

```

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

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

Neighbor ID Pri State Dead Time Address Interface
192.168.23.2 0 FULL/- 00:00:37 192.168.13.2 Serial0/0/1
R1#SHOW IP OSPF INTERFACE G0/0
-
! Invalid input detected at '^' marker.
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 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 00:00:06
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)
R1#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ROUTER OSPF 1
R1(config-router)#SPRITE-INTERFACE G0/0
R1(config-router)#END
R1#
R1#S-CONFIG_I: Configured from console by console
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 192.168.13.1, 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# **show ip route**

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

Gateway of last resort is not set

```

2.0.0.0/32 is subnetted, 1 subnets
C      2.2.2.2 is directly connected, Loopback0
O      192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.2.0/24 is directly connected, GigabitEthernet0/0
L      192.168.2.1/32 is directly connected, GigabitEthernet0/0
O      192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.12.0/30 is directly connected, Serial0/0/0
L      192.168.12.2/32 is directly connected, Serial0/0/0
192.168.13.0/30 is subnetted, 1 subnets

```

```

O   192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
    [110/128] via 192.168.12.1, 00:58:32, Serial0/0/0
    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.23.0/30 is directly connected, Serial0/0/1
L   192.168.23.1/32 is directly connected, Serial0/0/1

```

```

R1#
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 192.168.1.1, 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 1/7, Flood queue length 0
Next 0x010/0x010
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#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 - IGP, l1 - IGP level-1, l2 - IGP level-2, ia - IGP 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    192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/128] via 192.168.13.1, 00:46:34, Serial0/0/1
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:46:14, Serial0/0/1
C    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.1/32 is directly connected, Serial0/0/0
C    192.168.19.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.168.19.0/30 is directly connected, Serial0/0/1
L    192.168.19.1/32 is directly connected, Serial0/0/1
O    192.168.23.0/30 is subnetted, 1 subnets
L    192.168.23.0/30 [110/128] via 192.168.13.2, 00:46:04, Serial0/0/1

R1#
R1#

```

## Step 11: establecer la interfaz pasiva como la interfaz predeterminada en un router.

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

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

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

```

R1
Physical Config CLI Attributes
IOS Command Line 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 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#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
NI - 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 1.1.1.0/32 is directly connected, Loopback0
C 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
L 192.168.1.0/24 is directly connected, GigabitEthernet0/0
O 192.168.2.0/24 [110/129] via 192.168.13.2, 00:48:14, Serial0/0/1
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:46:14, Serial0/0/1
L 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
L 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
O 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0/30 [110/128] via 192.168.13.2, 00:46:04, Serial0/0/1

R1#
R1#SHOW IP OSPF NEIGHBOR
Neighbor ID Pri State Dead Time Address Interface
192.168.13.2 0 FULL/ - 00:00:38 192.168.13.2 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)#
```

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

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

```

Codes: I - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EK - 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 [110/129] via 192.168.13.1, 00:45:54, Serial0/0/1
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:46:14, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.12.0/30 is directly connected, Serial0/0/0
L 192.168.12.1/32 is directly connected, Serial0/0/0
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.13.0/30 is directly connected, Serial0/0/1
L 192.168.13.1/32 is directly connected, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0/30 [110/128] via 192.168.13.2, 00:46:04, Serial0/0/1

R1#
R1#SHOW IP OSPF NEIGHBOR

Neighbor ID      Pri   State           Dead Time   Address      Interface
192.168.13.2     0    FULL/ -         00:00:38    192.168.13.2 Serial0/0/1
R1#CONFIG T
* Invalid input detected at '^' marker.
R1#CONFIG T
-
* Invalid input detected at '^' marker.
R1#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ROUTER OSPF 1
R1(config-router)#PASSIVE-INTERFACE DEFAULT
R1(config-router)#
01:47:09: %OSPF-6-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
R1(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
192.168.13.2     0    FULL/ -         00:00:34    192.168.13.2 Serial0/0/1

```

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

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

```

Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.2/30, Area 0, Attached via Network
Statement
  Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost:
64
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
  0                  64        no            no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)

```

```
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

- e. Si todas las interfaces en el R2 son pasivas, no se anuncia ninguna información de routing. En este caso, el R1 y el R3 ya no deberían tener una ruta a la red 192.168.2.0/24. Esto se puede verificar mediante el comando **show ip route**.
- f. En el R2, emita el comando **no passive-interface** para que el router envíe y reciba actualizaciones de routing OSPF. Después de introducir este comando, verá un mensaje informativo que explica que se estableció una adyacencia de vecino con el R1.

```
R2(config)# router ospf 1
R2(config-router)# no passive-interface s0/0/0
R2(config-router)#
*Apr  3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from LOADING to FULL, Loading Done
```

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

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? S0/0/0

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3? 128

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

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

¿Qué indica esta información? El tráfico a la red desde R3 192.168.2.0/24 serán enviados a través de R1. La interfaz S0/0/1 en R2 todavía está configurado como una interfaz pasiva, por lo que la información de enrutamiento OSPF no se está anunciando a través de esta interfaz.

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

```
R2(CONFIG)#ROUTER OSPF 1
R2(CONFIG-ROUTER)#NO PASIVE-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? s/0/0/1

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

65 (One T1 (1.544 Mb/s) serial link (at a cost of 64) plus the R2 Gigabit 0/0 LAN link (at a cost of 1).

¿El R2 aparece como vecino OSPF del R3? 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.

### Step 12: cambiar el ancho de banda de referencia en los routers.

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

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

```
R1# show interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia
c471.fe45.7520)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:17:31, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    279 packets output, 89865 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    1 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

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

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

```
R1# show ip route ospf
```

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

```
Gateway of last resort is not set
```

```
O      192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O          192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
          [110/128] via 192.168.12.2, 00:01:08, Serial0/0/0
```

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

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

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

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

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



```

R1# show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network
Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
                0        64         no         no         Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)

```

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

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

```

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

```

- f. Emita el comando **auto-cost reference-bandwidth 10000** en los routers R2 y R3.
- g. Vuelva a emitir el comando **show ip ospf interface** para ver el nuevo costo de G0/0 en el R3 y de S0/0/1 en el R1.

```

R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
                0        10         no         no         Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

```

```

oob-resync timeout 40
Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

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

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

```

Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network
Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost:
6476
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
                   0         6476         no            no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)

```

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

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

```
R1# show ip route ospf
```

```

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

```

```

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

```

Gateway of last resort is not set

```

O      192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
O      192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O          192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
          [110/12952] via 192.168.12.2, 00:05:17, Serial0/0/

```

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

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

```

R1(config)# router ospf 1
R1(config-router)# auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
      Please ensure reference bandwidth is consistent across all
routers.

```

¿Por qué querría cambiar el ancho de banda de referencia OSPF predeterminado? PARA OBTENER UN CÁLCULO DE COSTOS MÁS PRECISA PARA ESTOS ENLACES MÁS RÁPIDOS

### Step 13: cambiar el ancho de banda de una interfaz.

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

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

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

```

R1# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.12.1/30

```

```

MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
<Output Omitted>

```

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

```

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

Gateway of last resort is not set

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

```

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

```

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

```

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

```

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

Gateway of last resort is not set

```

```

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

```

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

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

| Interface F/C | PID | Area | IP Address/Mask | Cost | State | Nbrs |
|---------------|-----|------|-----------------|------|-------|------|
| Se0/0/1       | 1   | 0    | 192.168.13.1/30 | 64   | P2P   | 1/1  |
| Se0/0/0       | 1   | 0    | 192.168.12.1/30 | 781  | P2P   | 1/1  |
| Gi0/0         | 1   | 0    | 192.168.1.1/24  | 1    | DR    | 0/0  |

- f. Cambie el ancho de banda de la interfaz S0/0/1 a la misma configuración que S0/0/0 en el R1.
- g. Vuelva a emitir el comando **show ip route ospf** para ver el costo acumulado de ambas rutas a la red 192.168.23.0/24. Observe que otra vez hay dos rutas con el mismo costo (845) a la red 192.168.23.0/24: una a través de S0/0/0 y otra a través de S0/0/1.

```
R1# show ip route ospf
```

```

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

```

```
Gateway of last resort is not set
```

```

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

```

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

El costo para 192.168.3.0/24: R1 S0 / 0/1 + R3 G0 / 0 (781 + 1 = 782).

El costo para 192.168.23.0/30: R1 S0 / 0/1 y R3 S0 / 0/1 (781 + 64 = 845).

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

```
R3# show ip route ospf
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

```

Gateway of last resort is not set

```

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

```

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

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

1562. Cada enlace serie ahora tiene un costo de 781, y la ruta a la red 192.168.23.0/24 viaja sobre dos enlaces seriales.  $781 + 781 = 1.562$ .

#### Step 14: cambiar el costo de la ruta.

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

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

```

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

```

Gateway of last resort is not set

```

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

```

```

O      192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
      [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0

```

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

```

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

```

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

```

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

```

Gateway of last resort is not set

```

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

```

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

Explique la razón por la que la ruta a la red 192.168.3.0/24 en el R1 ahora atraviesa el R2. OSPF elegirá la ruta con el menor costo acumulado.

## Reflexión

1. ¿Por qué es importante controlar la asignación de ID de router al utilizar el protocolo OSPF? Asignaciones de ID Router controlan el router designado (DR) y BDR (BDR) elección / proceso en una red de acceso múltiple.
2. ¿Por qué el proceso de elección de DR/BDR no es una preocupación en esta práctica de laboratorio? El proceso de elección DR / BDR es sólo un problema en una red multiacceso como Ethernet o Frame Relay
3. ¿Por qué querría configurar una interfaz OSPF como pasiva? Elimina innecesaria información de enrutamiento OSPF en esa interfaz, liberando ancho de banda

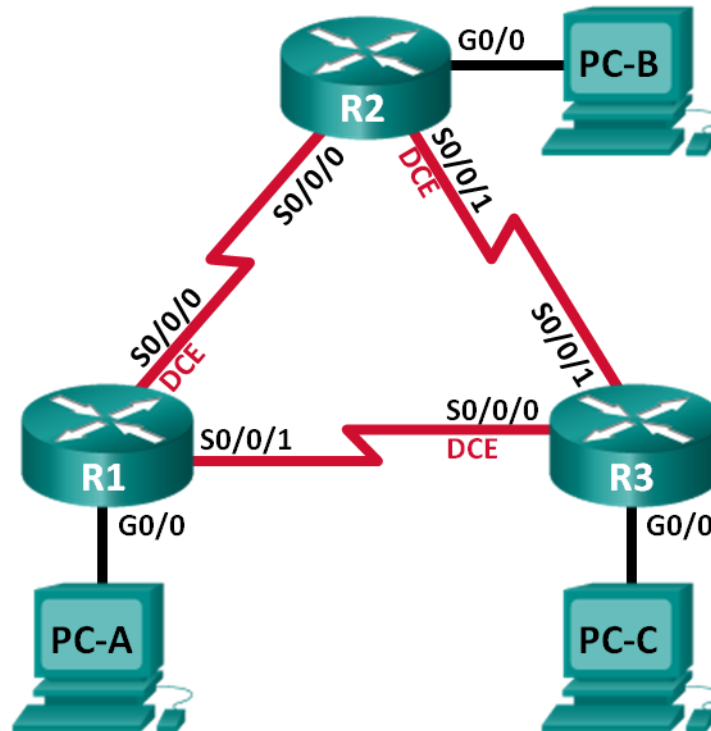
**Tabla de resumen de interfaces del router**

| Resumen de interfaces del router  |                             |                             |                       |                       |
|---|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de router  | Interfaz Ethernet #1        | Interfaz Ethernet n.º 2     | Interfaz serial #1    | Interfaz serial n.º 2 |
| 1800  | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900  | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801  | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811  | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900  | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| <p><b>Nota:</b> para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.</p> |                             |                             |                       |                       |



### 8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3

#### Topología



### Tabla de direccionamiento

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

### Objetivos

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

**Parte 2: configurar y verificar el routing OSPFv3**

**Parte 3: configurar interfaces pasivas OSPFv3**

### Información básica/situación

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

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

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

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

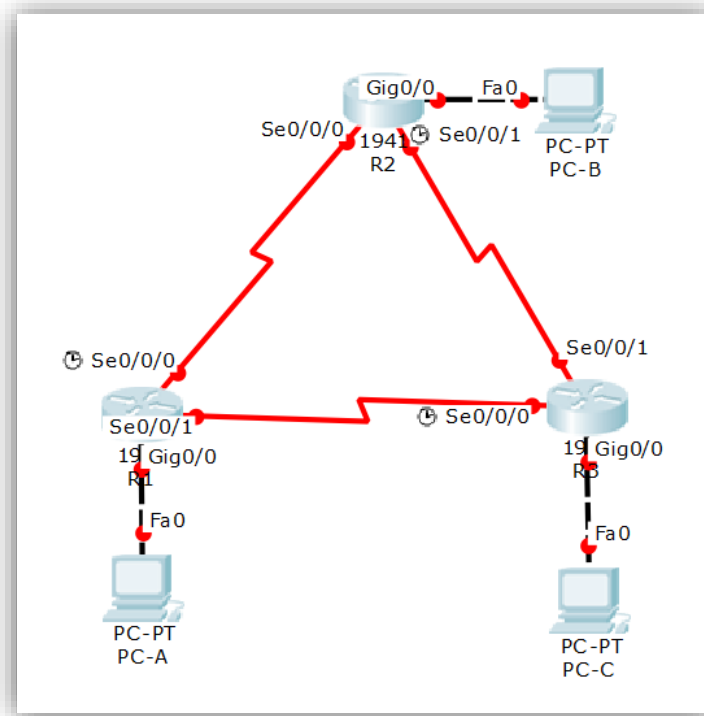
### Recursos necesarios

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

### 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.

**Step 15: realizar el cableado de red tal como se muestra en la topología.**



**Step 16: inicializar y volver a cargar los routers según sea necesario.**

**Step 17: configurar los parámetros básicos para cada router.**

- Desactive la búsqueda del DNS.  
(config)# no ip domain-lookup
- Configure el nombre del dispositivo como se muestra en la topología.  
(config)# hostname xx
- Asigne **class** como la contraseña del modo EXEC privilegiado.  
(config)# enable secret class
- Asigne **cisco** como la contraseña de vty.  
(config)# line vty 0 15  
(config-line)# pass cisco  
(config-line)# login  
(config-line)# exit

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

```
(config)# banner motd x ¡Prohibido el acceso no autorizado! X
```

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

```
(config)# line console 0
(config-line)# login synchronous
(config-line)# exit
```

- g. Cifre las contraseñas de texto no cifrado.

```
(config)# service password-encryption
```

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

```
(config)# int gx/x
(config-if)# ipv6 address xxxx:xxx:xxxx:xx::x/xx
(config-if)# ipv6 address xxxx::x link-local
(config-if)# No shutdown
```

```
(config)# int sx/x/x
(config-if)# ipv6 address xxxx:xxx:xxxx:xx::x/xx
(config-if)# ipv6 address xxxx::x link-local
(config-if)# clock rate xxxxxx
(config-if)# No shutdown
```

```
(config)# int sx/x/x
(config-if)# ipv6 address xxxx:xxx:xxxx:xx::x/xx
(config-if)# ipv6 address xxxx::x link-local
(config-if)# No shutdown
(config-if)# exit
```

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

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

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

```
(config)# copy run start Router
```

```

Router#enable
Router#conf te
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 vty 0 15
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd x Prohibido el acceso no autorizado! x
R1(config)#line console 0
R1(config-line)#login synchronous
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#int 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)#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)#clock rate 128000
R1(config-if)#No shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#int 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)#
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#copy run start Router
^
% Invalid input detected at '^' marker.

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

R1#copy run start Router
^
% Invalid input detected at '^' marker.

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

```

```
Router>enable
Router#conf te
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line vty 0 15
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#banner motd x Prohibido el acceso no autorizado! x
R2(config)#line console 0
R2(config-line)#loggin synchronous
R2(config-line)#exit
R2(config)#service password-encryption
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)#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)#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)#No shutdown

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

R2(config-if)#int s0/0/1
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

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)#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)#
R2(config)#ipv6 unicast-routing
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

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



```

Router#conf te
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line vty 0 15
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#banner motd x Prohibido el acceso no autorizado! x
R3(config)#line console 0
R3(config-line)#login synchronous
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#int 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)#int 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
R3(config-if)#No shutdown

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

R3(config-if)#int s0/0/1
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)#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

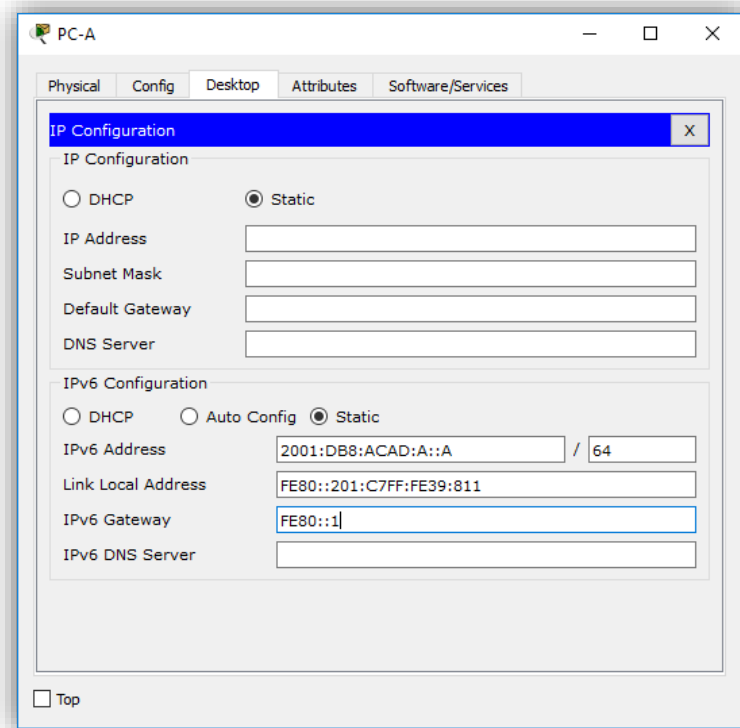
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

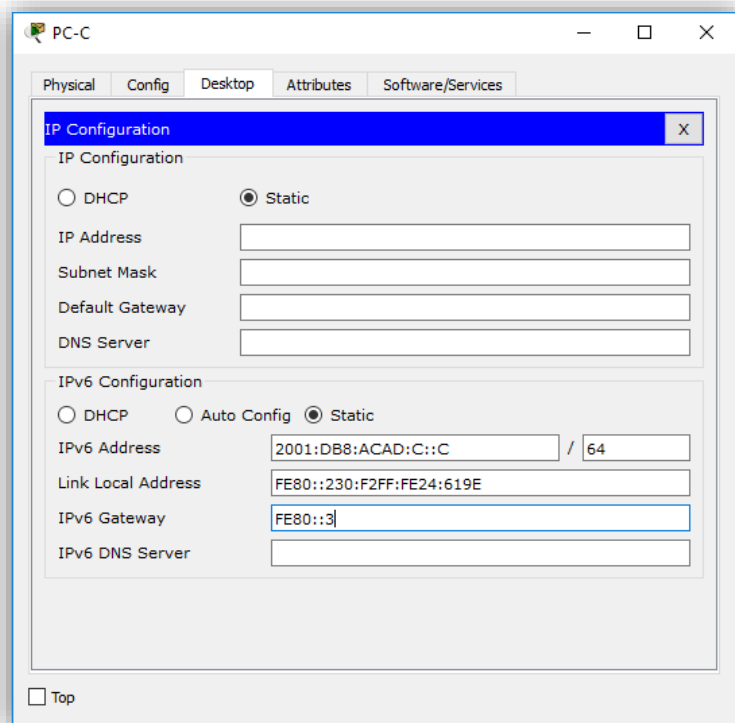
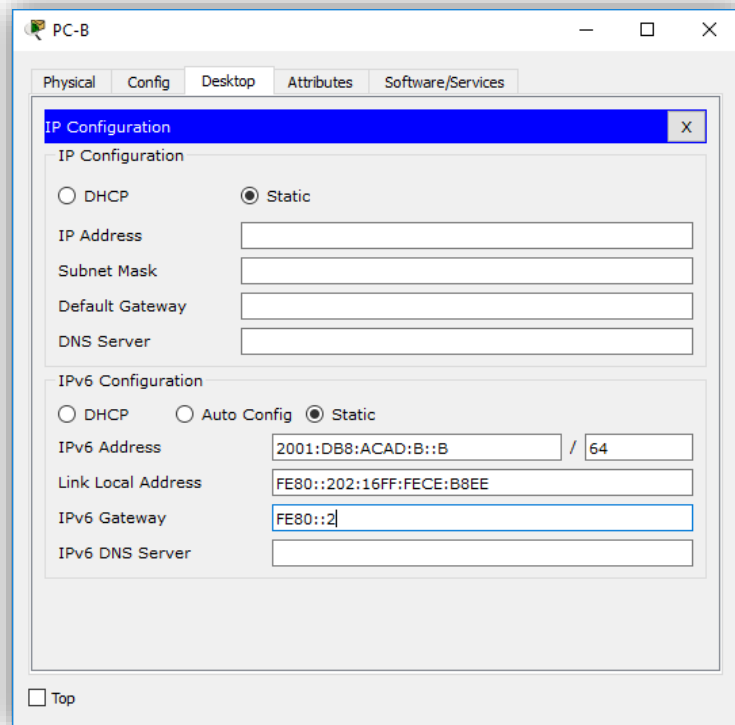
R3(config-if)#exit
R3(config)#copy running-config startup-config
^
% Invalid input detected at '^' marker.

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

R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

```

**Step 18: configurar los equipos host.**



**Step 19: 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.

```
Prohibido el acceso no autorizado!

R1>conf te
^
% Invalid input detected at '^' marker.

R1>enable
Password:
R1#ping 2001:DB8:ACAD:12::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::2, timeout is
2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
2/6/18 ms

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

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::3, timeout is
2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/9/16 ms

R1#
```

```
Prohibido el acceso no autorizado!  
  
R2>enable  
Password:  
R2#ping 2001:DB8:ACAD:12::1  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::1, timeout is  
2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max =  
5/10/16 ms  
  
R2#ping 2001:DB8:ACAD:23::3  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::3, timeout is  
2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max =  
1/10/26 ms  
  
R2#
```

```

Prohibido el acceso no autorizado!

R3>enable
Password:
R3#ping 2001:DB8:ACAD:23::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::2, timeout is
2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/5
ms

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

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::1, timeout is
2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/5/12 ms

R3#

```

## Parte 2. configurar el routing OSPFv3

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

### Step 20: 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
```

```
R1#conf te
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-
id,please configure manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#
```

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

```
R2>enable
Password:
R2#conf te
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-
id,please configure manually
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

```
R3#conf te
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-
id,please configure manually
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
R2# show ipv6 ospf
```

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

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

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

```
<Output Omitted>
```



```
R1#show ipv6 ospf
Routing Process "ospfv3 1" with ID 1.1.1.1
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
```

```
R2#show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
```

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

### Step 21: configurar OSPFv6 en el R1.

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

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

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

```

R1#conf te
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#

```

- Nota:** la ID del proceso debe coincidir con la ID del proceso que usó en el paso 1a.
- b. Asigne las interfaces en el R2 y el R3 al área 0 de OSPFv3. Al agregar las interfaces al área 0, debería ver mensajes de adyacencia de vecino.

R1#

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

R1#

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

```

R2#
R2#enable
R2#conf te
Enter configuration commands, one per line. End with CNTL/Z.
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)#
02:08:25: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
02:10:54: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done

R2(config-if)#

```

```

R3#conf te
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
02:10:35: %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)#
02:10:54: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done

R3(config-if)#

```

### Step 22: 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<br>Interface | Pri | State   | Dead Time | Interface ID |
|--------------------------|-----|---------|-----------|--------------|
| 3.3.3.3<br>Serial0/0/1   | 0   | FULL/ - | 00:00:39  | 6            |
| 2.2.2.2<br>Serial0/0/0   | 0   | FULL/ - | 00:00:36  | 6            |

```
R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID
Interface
2.2.2.2          0    FULL/ -         00:00:31   3
Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:39   3
Serial0/0/1
R1#
```

```
R2#
R2#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID
Interface
1.1.1.1          0    FULL/ -         00:00:33   3
Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:36   4
Serial0/0/1
R2#
```

```
R3#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID
Interface
2.2.2.2          0    FULL/ -         00:00:36   4
Serial0/0/1
1.1.1.1          0    FULL/ -         00:00:37   4
Serial0/0/0
R3#
```

### Step 23: 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"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
```

```
R2#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
```

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

#### Step 24: verificar las interfaces OSPFv3.

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

```
R1#show ipv6 ospf interface
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)
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 00:00:07
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 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 00:00:08
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
R1#
```

```
R2#show ipv6 ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, local address FE80::2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:06
  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::2, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:06
  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 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 4
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:09
  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)
R2#
```

```

R3#show ipv6 ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, local address FE80::3
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:00
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:01
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 4
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:08
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
R3#

```

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

```

R1# show ipv6 ospf interface brief

```

| Interface | PID | Area | Intf ID | Cost | State | Nbrs | F/C |
|-----------|-----|------|---------|------|-------|------|-----|
| Se0/0/1   | 1   | 0    | 7       | 64   | P2P   | 1/1  |     |
| Se0/0/0   | 1   | 0    | 6       | 64   | P2P   | 1/1  |     |



Gi0/0            1        0                    3            1        DR        0/0

### Step 25: verificar la tabla de routing IPv6.

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

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

```
R2>en
Password:
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#
```

```

R3>en
Password:
R3#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O  2001:DB8:ACAD:A::/64 [110/65]
   via FE80::1, Serial0/0/0
O  2001:DB8:ACAD:B::/64 [110/65]
   via FE80::2, Serial0/0/1
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
   via FE80::2, Serial0/0/1
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#

```

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

Utilizaría el comando

R1# **show ipv6 route ospf**

```

R1#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF
ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O  2001:DB8:ACAD:B::/64 [110/65]
   via FE80::2, Serial0/0/0
O  2001:DB8:ACAD:C::/64 [110/65]
   via FE80::3, Serial0/0/1
O  2001:DB8:ACAD:23::/64 [110/128]
   via FE80::2, Serial0/0/0
   via FE80::3, Serial0/0/1
R1#

```

```

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#

```

```

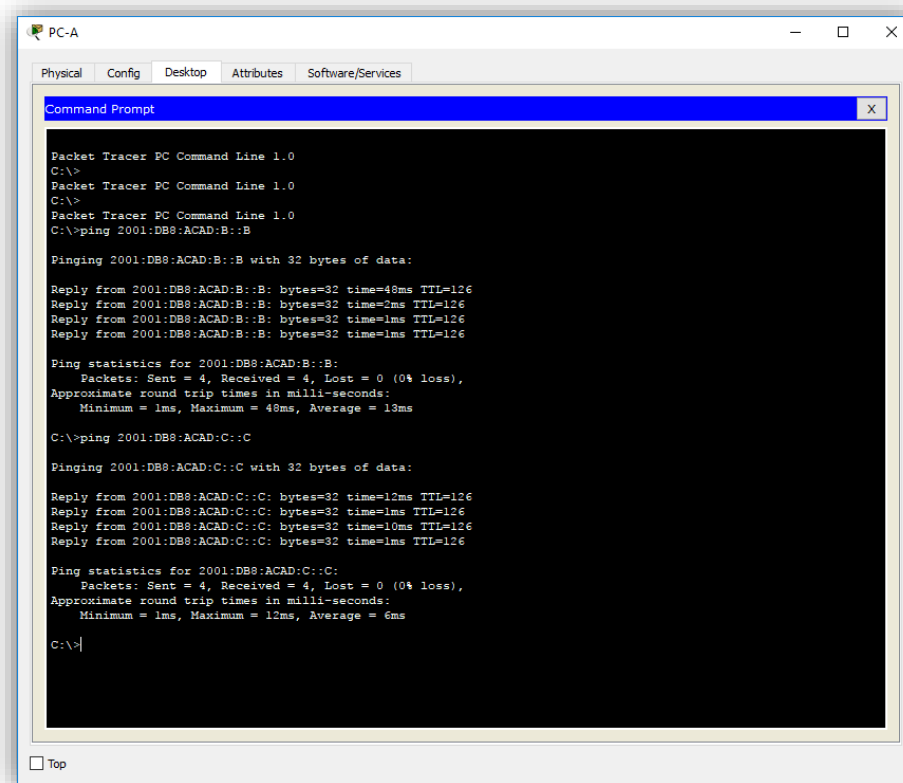
R3#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O   2001:DB8:ACAD:A::/64 [110/65]
    via FE80::1, Serial0/0/0
O   2001:DB8:ACAD:B::/64 [110/65]
    via FE80::2, Serial0/0/1
O   2001:DB8:ACAD:12::/64 [110/128]
    via FE80::1, Serial0/0/0
    via FE80::2, Serial0/0/1
R3#

```

### Step 26: 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.



The image shows a screenshot of a Windows PC-A desktop environment. The desktop has several tabs: Physical, Config, Desktop, Attributes, and Software/Services. A Command Prompt window is open, displaying the output of a Packet Tracer PC Command Line 1.0. The user has entered the command 'ping 2001:DB8:ACAD:B::B' and received the following output:

```
Packet Tracer PC Command Line 1.0
C:\>
Packet Tracer PC Command Line 1.0
C:\>
Packet Tracer PC Command Line 1.0
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=48ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
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 = 48ms, Average = 13ms

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

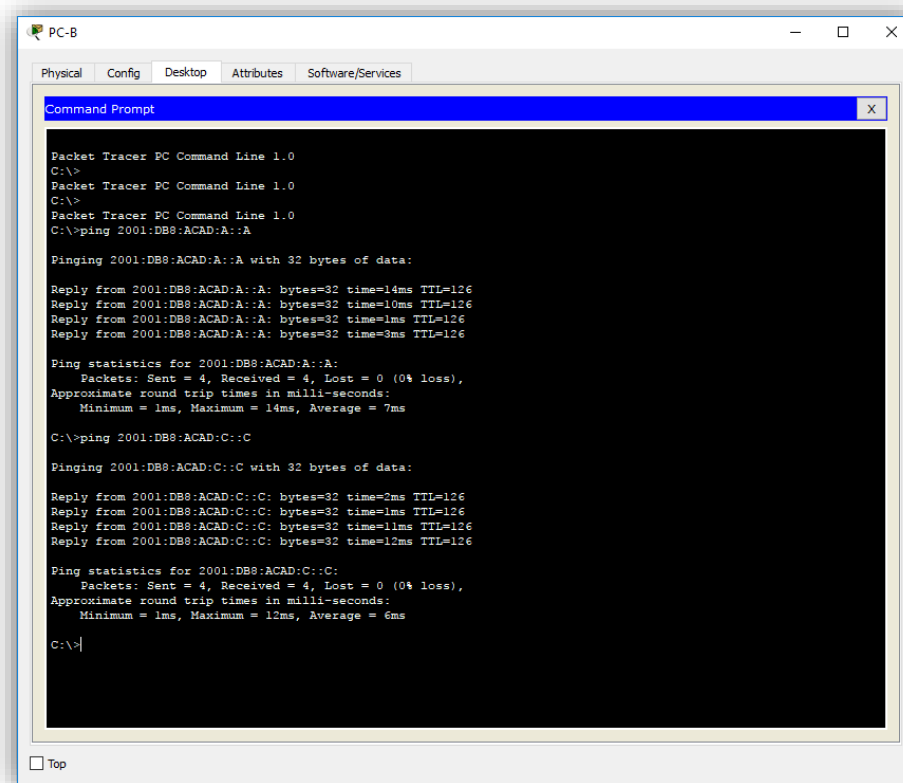
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms 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=10ms 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 = 12ms, Average = 6ms

C:\>
```

At the bottom left of the Command Prompt window, there is a 'Top' button.



The screenshot shows a Windows desktop environment with a window titled "PC-B". Inside the window, there is a "Command Prompt" application. The command prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>
Packet Tracer PC Command Line 1.0
C:\>
Packet Tracer PC Command Line 1.0
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=14ms TTL=126
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=10ms 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=3ms 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 = 14ms, Average = 7ms

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=2ms 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=11ms TTL=126
Reply from 2001:DB8:ACAD:C:C: bytes=32 time=12ms 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 = 12ms, Average = 6ms

C:\>
```

At the bottom left of the Command Prompt window, there is a "Top" button.

```

PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>
Packet Tracer PC Command Line 1.0
C:\>
Packet Tracer PC Command Line 1.0
C:\>
C:\>ping 2001:DB8:ACAD:A:A
Pinging 2001:DB8:ACAD:A:A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:A:A: bytes=32 time=17ms 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=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 = 17ms, Average = 8ms
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=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
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 = 1ms, Average = 1ms
C:\>

```

### Parte 3. configurar las interfaces pasivas de OSPFv3

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

#### Step 27: configurar una interfaz pasiva.

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

```
R1>en
Password:
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 00:00:09
  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#
```

```
R2>en
Password:
R2#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, local address FE80::2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:08
  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)
R2#
```

```
R3>en
Password:
R3#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, local address FE80::3
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:06
  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)
R3#
```



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

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

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

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

```
R2(config)#ipv6 router ospf 1  
R2(config-rtr)#passive-interface g0/0
```

```
R3(config)#ipv6 router ospf 1  
R3(config-rtr)#passive-interface g0/0
```

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

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

```
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#
```

```
R2#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State 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)
R2#
```

```
R3#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State 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)
R3#
```

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

```
R2# show ipv6 route ospf
```

```

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#

```

```

R3#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:B::/64 [110/65]
  via FE80::2, Serial0/0/1
O 2001:DB8:ACAD:12::/64 [110/128]
  via FE80::1, Serial0/0/0
  via FE80::2, Serial0/0/1
R3#

```

### Step 28: 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

```

```

R2#conf te
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
03:37:21: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached

03:37:21: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface 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

```

```
R1#show ipv6 ospf neighbor

Neighbor ID      Pri   State           Dead Time   Interface ID
Interface
3.3.3.3          0    FULL/ -         00:00:35   3
Serial0/0/1
R1#
```

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

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

```
R2#show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
  No Hellos (Passive interface)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
R2#
```

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

```
R1#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
```

```

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

```

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

```

R2(config)# ipv6 router ospf 1
R2(config-rtr)# no passive-interface s0/0/1
*Apr  8 19:21:57.939: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on
Serial0/0/1 from LOADING to FULL, Loading Done

```

```

R2#conf te
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
03:43:01: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done

```

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

```

R1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
  via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:B::/64 [110/129]
  via FE80::3, Serial0/0/1
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#

```

```

R3#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O  2001:DB8:ACAD:A::/64 [110/65]
   via FE80::1, Serial0/0/0
O  2001:DB8:ACAD:B::/64 [110/65]
   via FE80::2, Serial0/0/1
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
   via FE80::2, Serial0/0/1
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#show ipv6 ospf neighbor

Neighbor ID      Pri   State           Dead Time   Interface ID
Interface
2.2.2.2          0    FULL/ -         00:00:38   4
Serial0/0/1
1.1.1.1          0    FULL/ -         00:00:39   4
Serial0/0/0
R3#

```

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

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

¿El R2 aparece como vecino OSPFv3 en el R1? **SI**

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

¿Qué indica esta información?

**Todo el tráfico hacia la red 2001:DB8:ACAD:B::/64 desde R1 será enrutado a través de R3.**



La interfaz S0/0/0 en R2 está configurada como pasiva de tal manera que OSPFv3 no manda información de ruteo notificándose a través de esta interfaz.

El costo 129 acumulado resulta del tráfico que pasa por R3

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)#
03:59:40: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
```

- g. 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/ -         00:00:38   3
Serial0/0/0
3.3.3.3        0    FULL/ -         00:00:31   4
Serial0/0/1
R2#
```

## Reflexión

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

Si, se puede intercambiar, porque el ID del proceso OSPFv3 se usa solo localmente en el router, y no es necesario que este coincida con la ID del proceso que se usa en los otros routers en el área OSPFv3

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

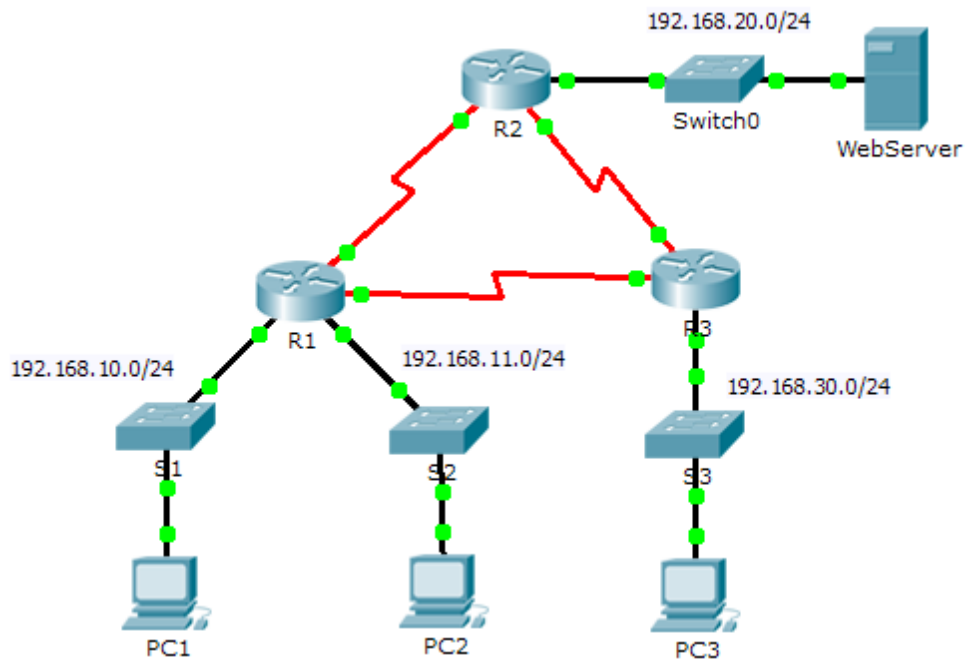
Eliminar la instrucción network ayuda a evitar errores en la dirección de IPv6

**Tabla de resumen de interfaces del router**

| Resumen de interfaces del router |                             |                             |                       |                       |
|----------------------------------|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de router                 | Interfaz Ethernet #1        | Interfaz Ethernet n.º 2     | Interfaz serial #1    | Interfaz serial n.º 2 |
| 1800                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

**Nota:** para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

### 9.2.1.10 Packet Tracer Configuring Standard ACLs



```

R2
  Physical Config CLI
  IOS Command Line Interface
  %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
  %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
  %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
  %DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency
  %DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.2 (Serial0/0/1) 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 192.168.11.0.0.0.255
  % Invalid input detected at '^' marker.
  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)#
  
```

Completion: 50/100

ES 02:58 p.m. 21/11/2016

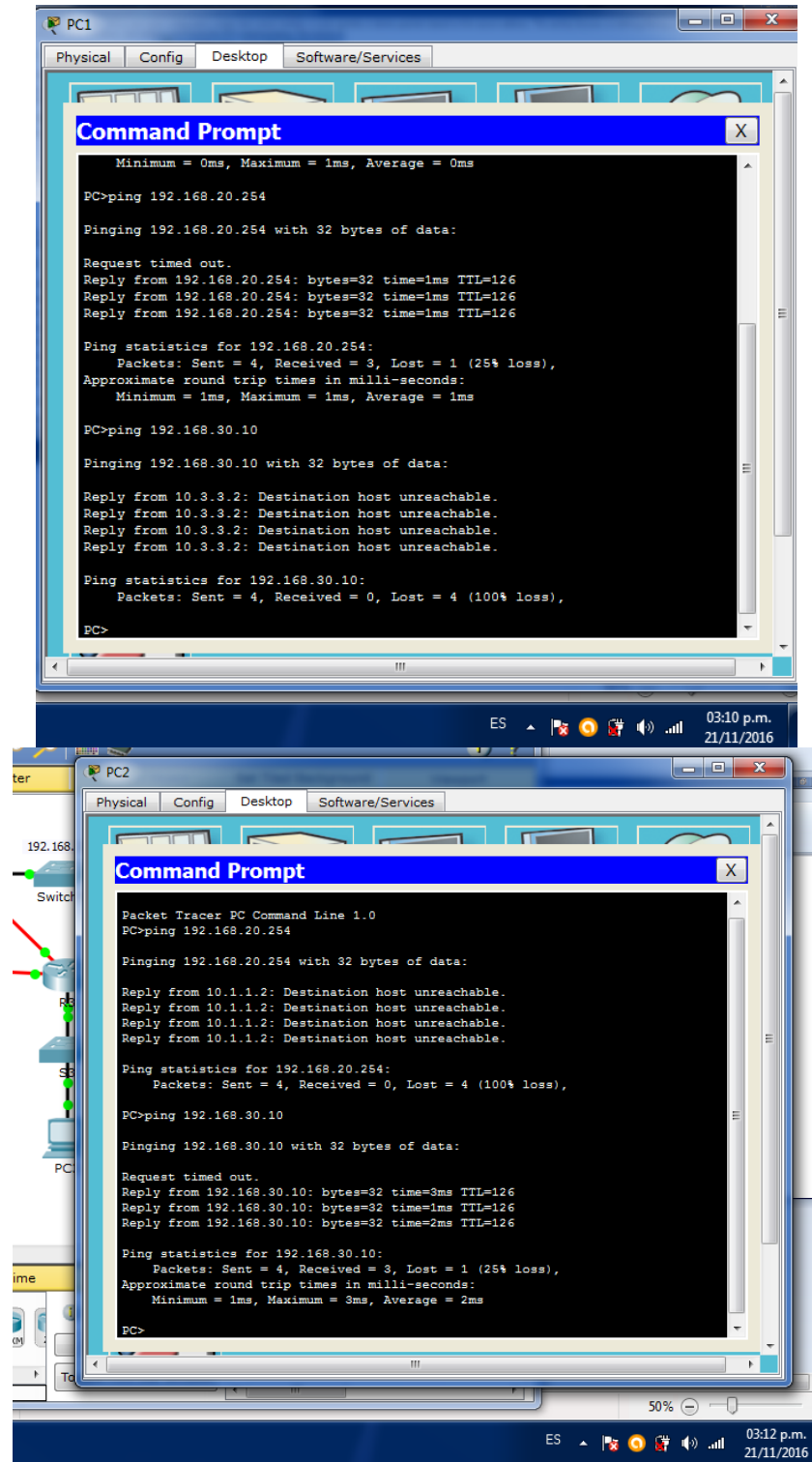
denies packets based on the source address. This activity focuses on defining hitting criteria, configuring standard ACLs, and configuring Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

IOS Command Line Interface

```
Press RETURN to get started!  
  
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up  
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up  
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.1 (Serial0/0/1) is up: new adjacency  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up  
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.3.3.1 (Serial0/0/0) is up: new adjacency  
  
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)#
```

Command Prompt

```
PC>ping 192.168.11.10  
Pinging 192.168.11.10 with 32 bytes of data:  
Request timed out.  
Reply from 192.168.11.10: bytes=32 time=0ms TTL=127  
Reply from 192.168.11.10: bytes=32 time=0ms 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 = 3, Lost = 1 (25% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
PC>ping 192.168.20.254  
Pinging 192.168.20.254 with 32 bytes of data:  
Request timed out.  
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=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 = 1ms, Average = 1ms  
  
PC>
```



RESULTADO FINAL

The screenshot shows the 'Activity Results' window in Cisco Packet Tracer. The window title is 'Cisco Packet Tracer - D:\10 SEMESTRE\DIPLOMADO CISCO\UNIDAD 4\CCNA2 R&S UNIDAD 4\LISTAS DE ACCESO\9.2.1.10 Pack...'. The main heading is 'Activity Results' with a sub-heading 'Time Elapsed: 00:27:21'. Below this, it says 'Congratulations Guest! You completed the activity.' There are three tabs: 'Overall Feedback', 'Assessment Items', and 'Connectivity Tests'. The 'Assessment Items' tab is active, showing a tree view of the network configuration and a summary table.

| Assessment Items   | Status  | Points |
|--------------------|---------|--------|
| Network            |         |        |
| R2                 |         |        |
| ACL 1              | Correct | 25     |
| Ports              |         | 0      |
| GigabitEthernet0/0 |         | 0      |
| Access-group ...   | Correct | 25     |
| R3                 |         |        |
| ACL 1              | Correct | 25     |
| Ports              |         | 0      |
| GigabitEthernet0/0 |         | 0      |
| Access-group ...   | Correct | 25     |

| Component                        | Items/Total | Score   |
|----------------------------------|-------------|---------|
| IPv4 Standard ACL Implementation | 4/4         | 100/100 |

Score : 100/100  
Item Count : 4/4

Close

## CONCLUSIÓN

Con esta práctica logramos entender la gran utilidad que se puede realizar con una configuración básica con el estándar ACL, estos nos generan listas de condiciones que se aplica a un tráfico de comunicación que viaja a través del router.

En pocas palabras indica al router que tipo de paquetes se puede aceptar o rechazar en base de las condiciones establecidas que para este caso son las direcciones origen y destino o cierto momento un protocolo de capa superior o número de puerto.

Cabe mencionar que los objetivos de las ACL son:

- Limitar el tráfico de red y mejorar el rendimiento de la red.
- Controlar el flujo de tráfico.
- Proporcionar un nivel básico de seguridad para el acceso de red.
- Establecer qué tipo de tráfico se envía o se bloquea en las interfaces del router.

Otorgar y denegar permiso a los usuarios para acceder a ciertos tipos de archivos.

### 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs

#### Addressing Table

| Device      | Interface | IP Address      | Subnet Mask   | Default Gateway |
|-------------|-----------|-----------------|---------------|-----------------|
| R1          | F0/0      | 192.168.10.1    | 255.255.255.0 | N/A             |
|             | F0/1      | 192.168.20.1    | 255.255.255.0 | N/A             |
|             | E0/0/0    | 192.168.100.1   | 255.255.255.0 | N/A             |
|             | E0/1/0    | 192.168.200.1   | 255.255.255.0 | N/A             |
| File Server | NIC       | 192.168.200.100 | 255.255.255.0 | 192.168.200.1   |
| Web Server  | NIC       | 192.168.100.100 | 255.255.255.0 | 192.168.100.1   |
| PC0         | NIC       | 192.168.20.3    | 255.255.255.0 | 192.168.20.1    |
| PC1         | NIC       | 192.168.20.4    | 255.255.255.0 | 192.168.20.1    |
| PC2         | NIC       | 192.168.10.3    | 255.255.255.0 | 192.168.10.1    |

#### Objectives

**Part 1: Configure and Apply a Named Standard ACL**

**Part 2: Verify the ACL Implementation**

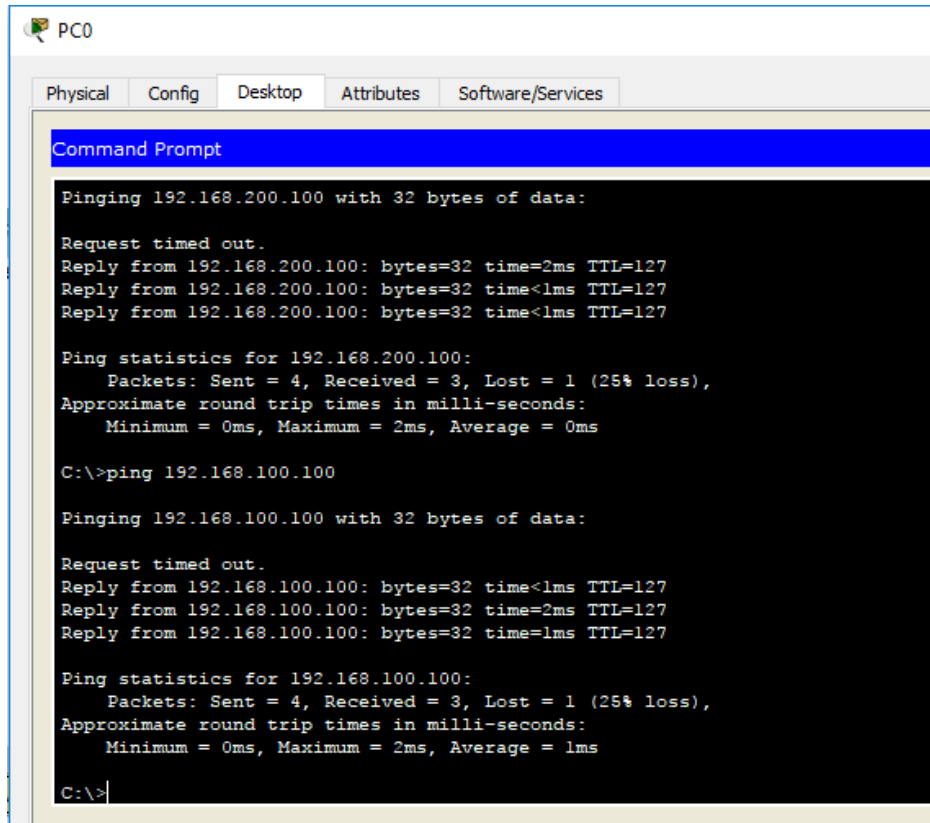
#### Background / Scenario

The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied access.

#### Part 1: Configure and Apply a Named Standard ACL

**Step 1: Verify connectivity before the ACL is configured and applied.**

All three workstations should be able to ping both the **Web Server** and **File Server**.



PC0

Physical Config Desktop Attributes Software/Services

Command Prompt

```
Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

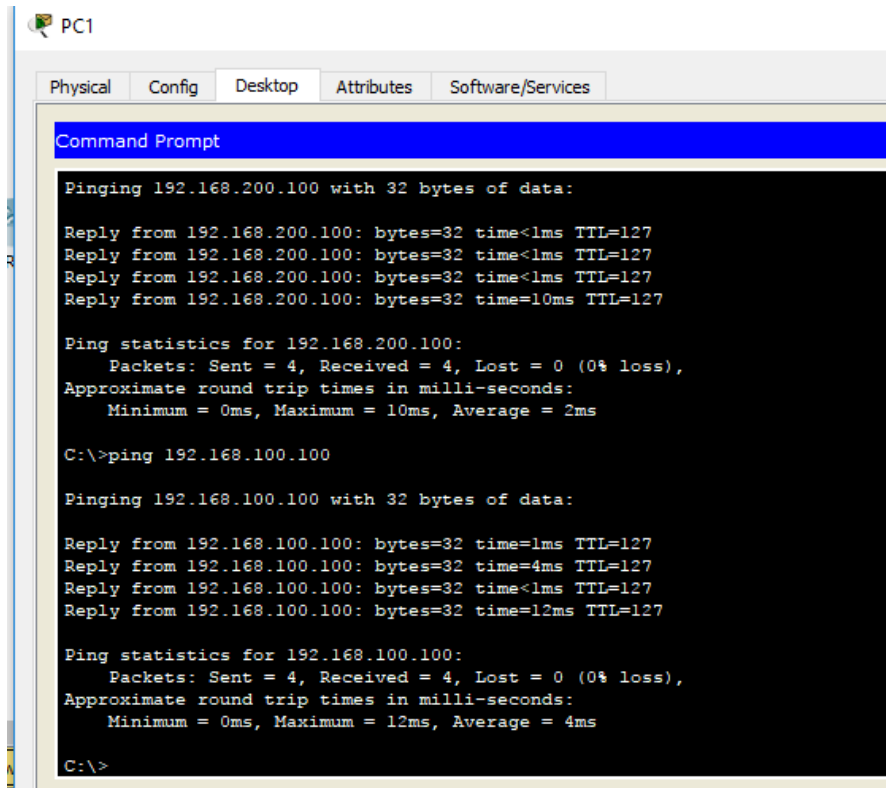
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\>
```



PC1

Physical Config Desktop Attributes Software/Services

Command Prompt

```
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=10ms 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 = 10ms, Average = 2ms

C:\>ping 192.168.100.100

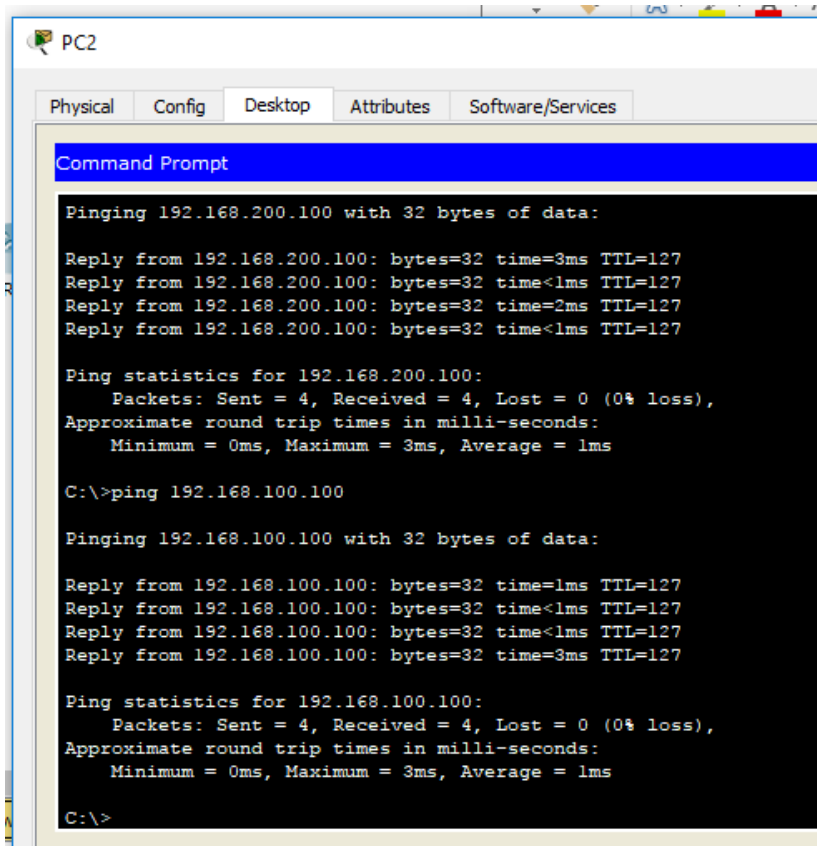
Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=4ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms 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 = 12ms, Average = 4ms

C:\>
```





The screenshot shows a Windows PC2 window with a Command Prompt open. The window title is 'PC2' and it has tabs for 'Physical', 'Config', 'Desktop', 'Attributes', and 'Software/Services'. The Command Prompt displays the following text:

```
Command Prompt

Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.200.100: bytes=32 time=3ms TTL=127
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

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 = 3ms, 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=3ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```

## Step 2: Configure a named standard ACL.

Configure the following named ACL on R1.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# deny any
```

**Note:** For scoring purposes, the ACL name is case-sensitive.

The screenshot shows the R1 CLI interface with the following text:

```

Compiled Mon 15-May-06 14:54 by pt_team

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1/0,
changed state to up

R1>en
R1#conf t
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)#

```

### Step 3: Apply the named ACL.

- a. Apply the ACL outbound on the interface Fast Ethernet 0/1.  
R1(config-if)# **ip access-group File\_Server\_Restrictions out**
- b. Save the configuration.

```

R1(config-std-nacl)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#do wr
Building configuration...
[OK]
R1(config-if)#

```

Copy

Paste

## Part 2: Verify the ACL Implementation

### Step 1: Verify the ACL configuration and application to the interface.

Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface fastethernet 0/1** command to verify that the ACL is applied correctly to the interface.

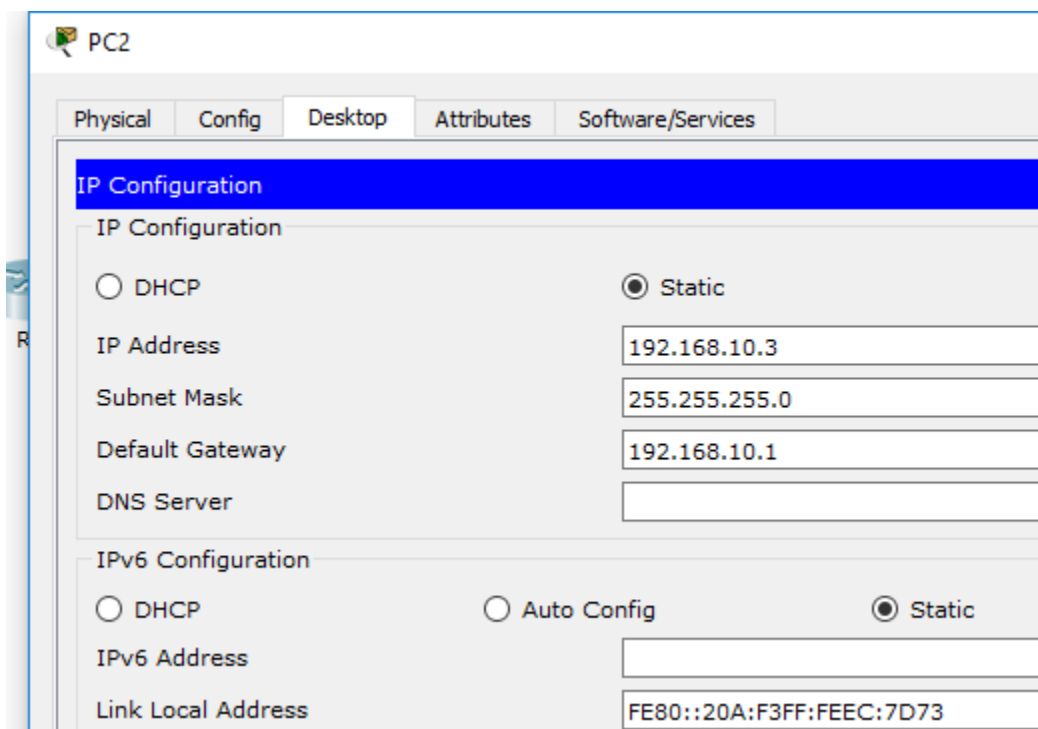
### Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the **Web Server**, but only **PC1** should be able to ping the **File Server**.

The image displays two screenshots of network configuration windows for PC0 and PC1. Both windows show the 'Config' tab selected, with 'IP Configuration' highlighted in blue. The 'IP Configuration' section is expanded, showing radio buttons for 'DHCP' and 'Static'. The 'Static' option is selected in both. The fields for IP Address, Subnet Mask, and Default Gateway are populated with the following values:

| Field           | PC0 Value     | PC1 Value     |
|-----------------|---------------|---------------|
| IP Address      | 192.168.20.3  | 192.168.20.4  |
| Subnet Mask     | 255.255.255.0 | 255.255.255.0 |
| Default Gateway | 192.168.20.1  | 192.168.20.1  |
| DNS Server      |               |               |

Below the IP Configuration section, the 'IPv6 Configuration' section is also visible. It shows radio buttons for 'DHCP', 'Auto Config', and 'Static'. The 'Static' option is selected. The 'Link Local Address' field is populated with the value FE80::204:9AFF:FE44:2267.



**Solo el PC1 puede tener acceso al FILE SERVER**

### 9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines

#### Addressing Table

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

#### Objectives

**Part 1: Configure and Apply an ACL to VTY Lines**

**Part 2: Verify the ACL Implementation**

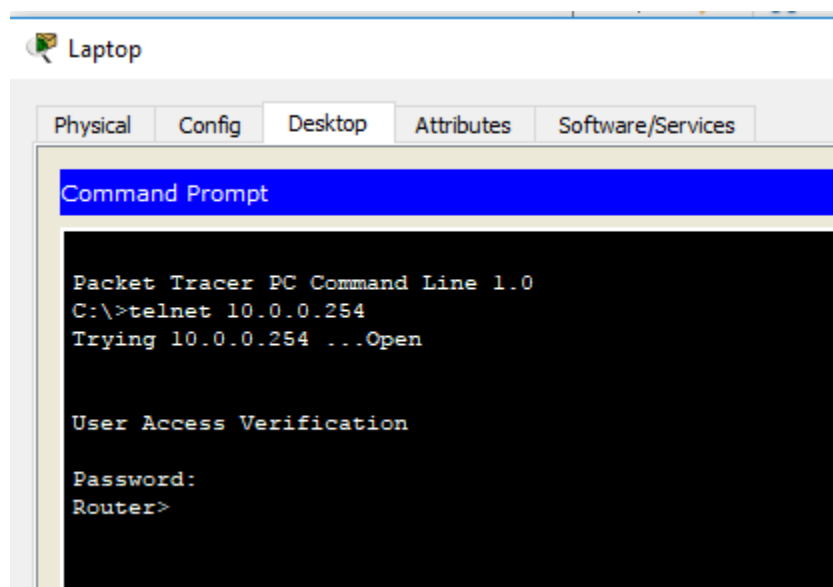
#### Background

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

#### Part 1: Configure and Apply an ACL to VTY Lines

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

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



The screenshot shows a Packet Tracer PC Command Line window for a Laptop. The window title is "Laptop" and it has tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The "Command Prompt" window is open, displaying the following text:

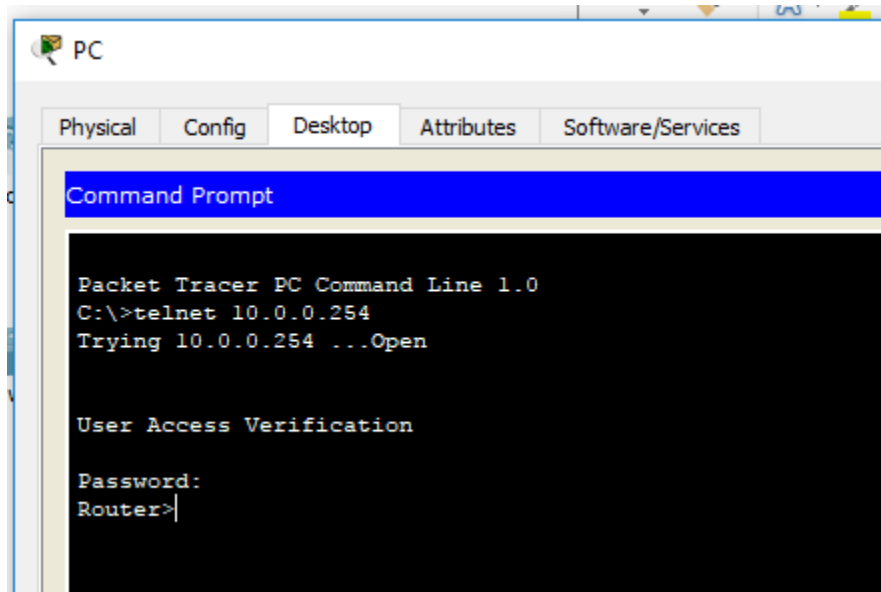
```

Packet Tracer PC Command Line 1.0
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>

```



The image shows a screenshot of a Packet Tracer PC Command Prompt window. The window title is "PC" and it has tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The "Desktop" tab is active, and the "Command Prompt" window is open. The command prompt shows the following text:

```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

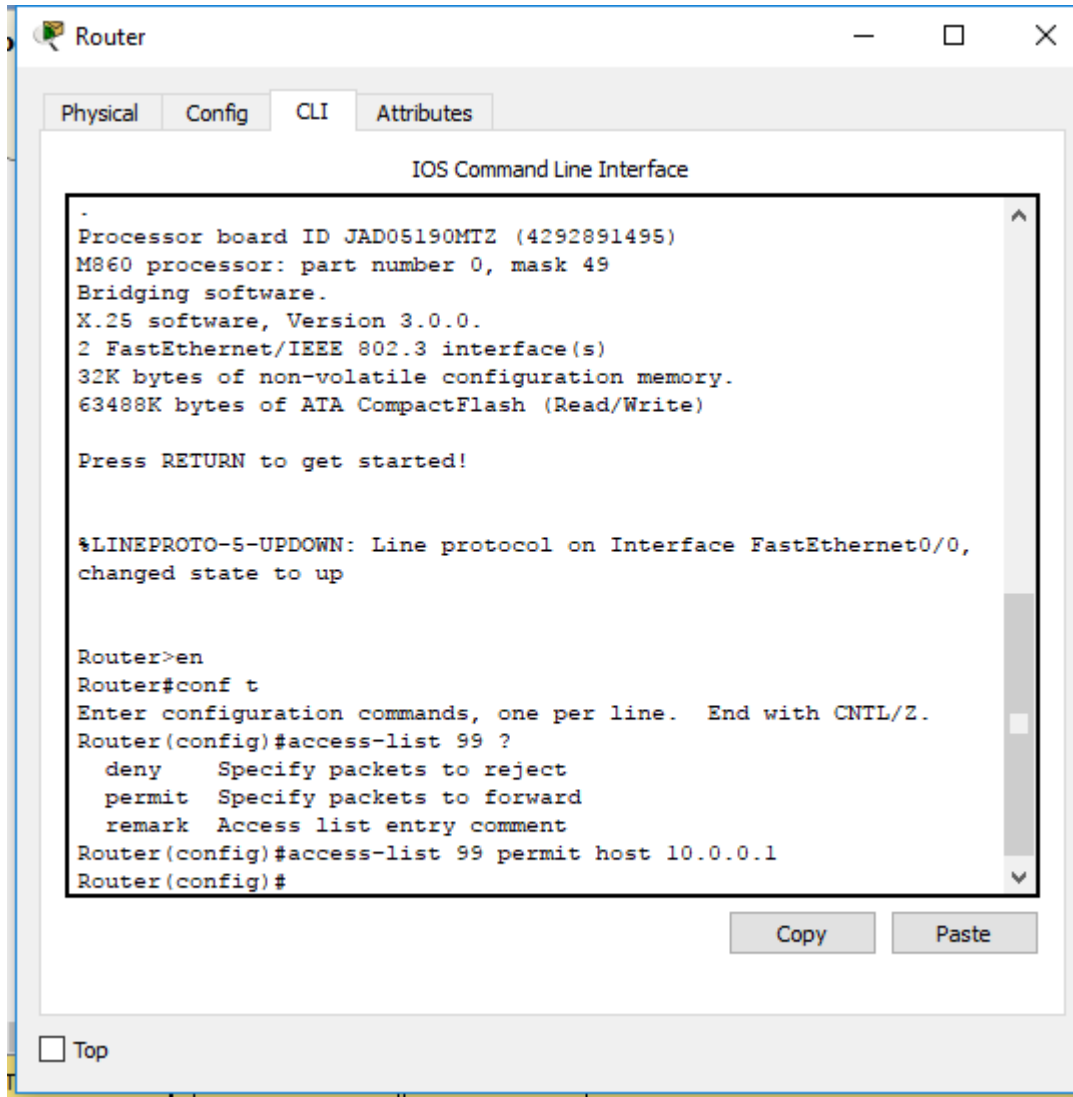
Password:
Router>
```

## Step 2: Configure a numbered standard ACL.

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

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

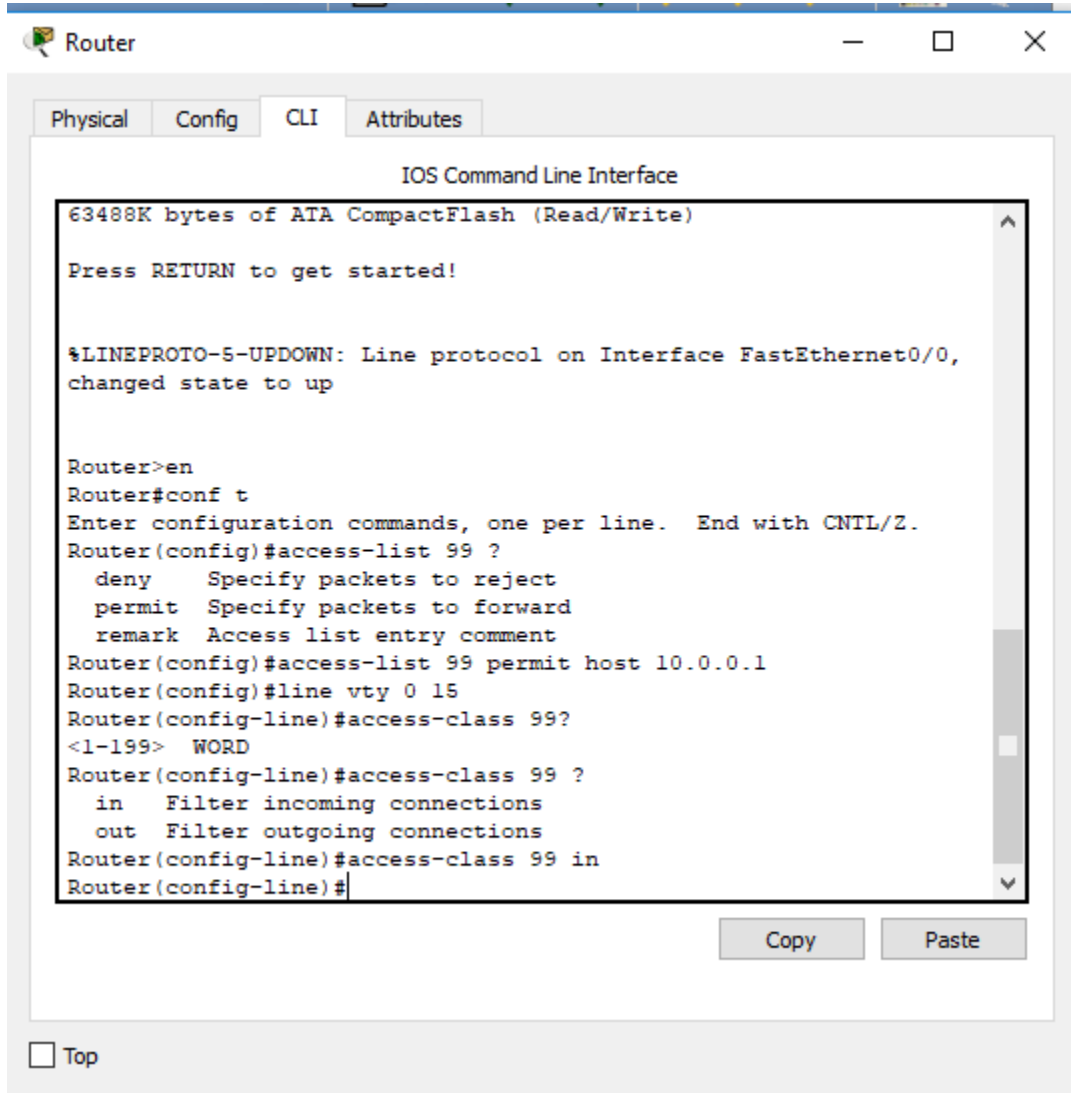
Because we do not want to permit access from any other computers, the implicit deny property of the access list satisfies our requirements.



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

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

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



The screenshot shows a window titled "Router" 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:

```
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 99 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99?
<1-199> WORD
Router(config-line)#access-class 99 ?
  in     Filter incoming connections
  out    Filter outgoing connections
Router(config-line)#access-class 99 in
Router(config-line)#
```

At the bottom of the terminal window, there are "Copy" and "Paste" buttons. Below the terminal window, there is a checkbox labeled "Top".

## Part 2: Verify the ACL Implementation

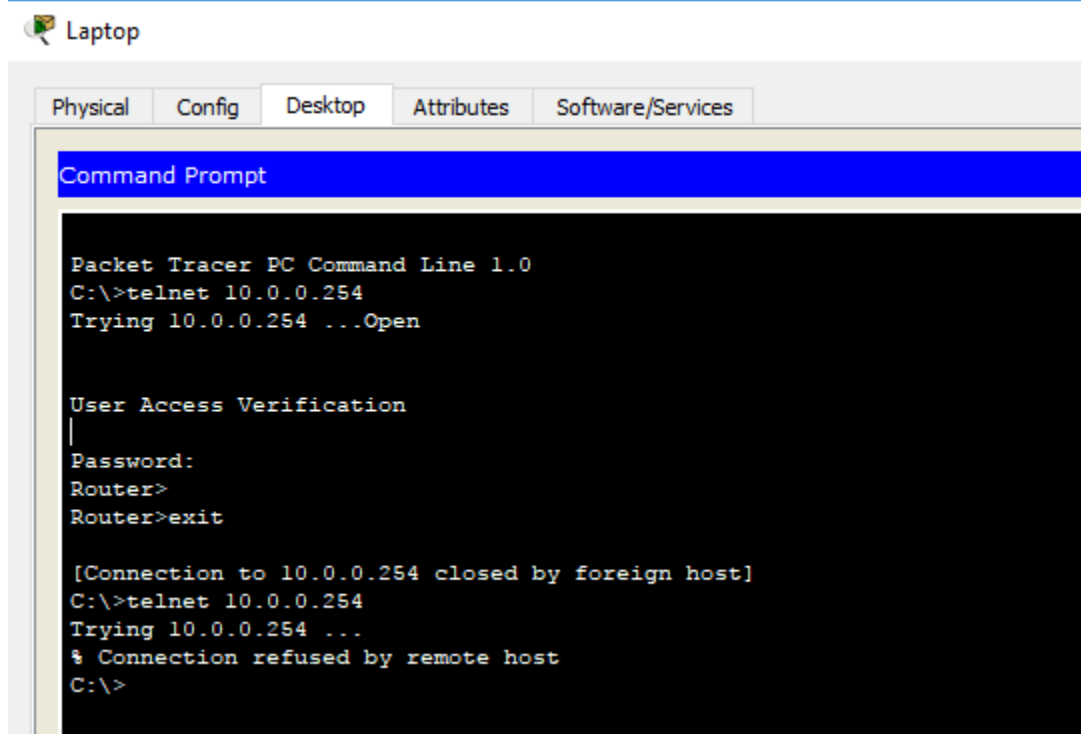
### Step 1: Verify the ACL configuration and application to the VTY lines.

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

### Step 2: Verify that the ACL is working properly.

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



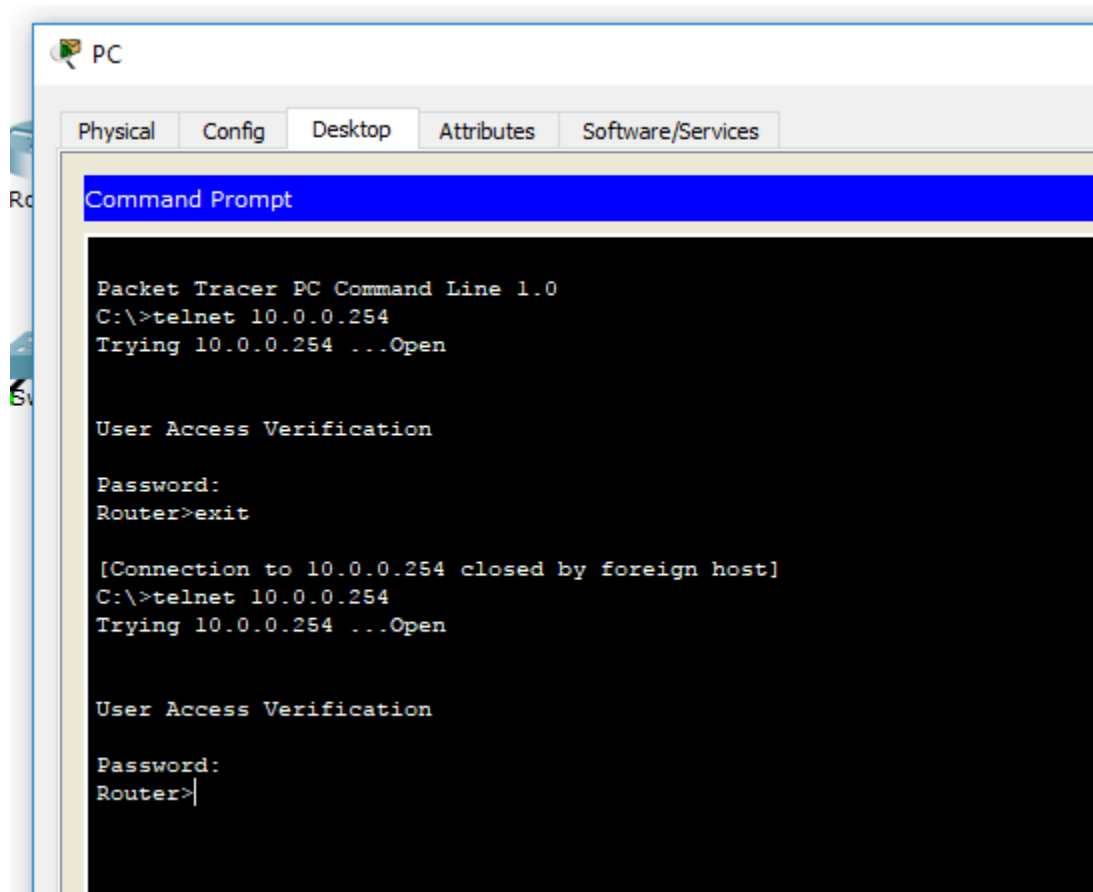


The screenshot shows a Packet Tracer PC Command Line window titled "Laptop". The window has tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The "Command Prompt" window is active, displaying the following text:

```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification
|
Password:
Router>
Router>exit

[Connection to 10.0.0.254 closed by foreign host]
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
C:\>
```



The image shows a screenshot of a Packet Tracer PC Command Prompt window. The window title is "PC" and it has tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The "Desktop" tab is active, and the "Command Prompt" window is open. The command prompt shows the following text:

```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>exit

[Connection to 10.0.0.254 closed by foreign host]
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>|
```

## 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs

### Addressing Table

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

### Objectives

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

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

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

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

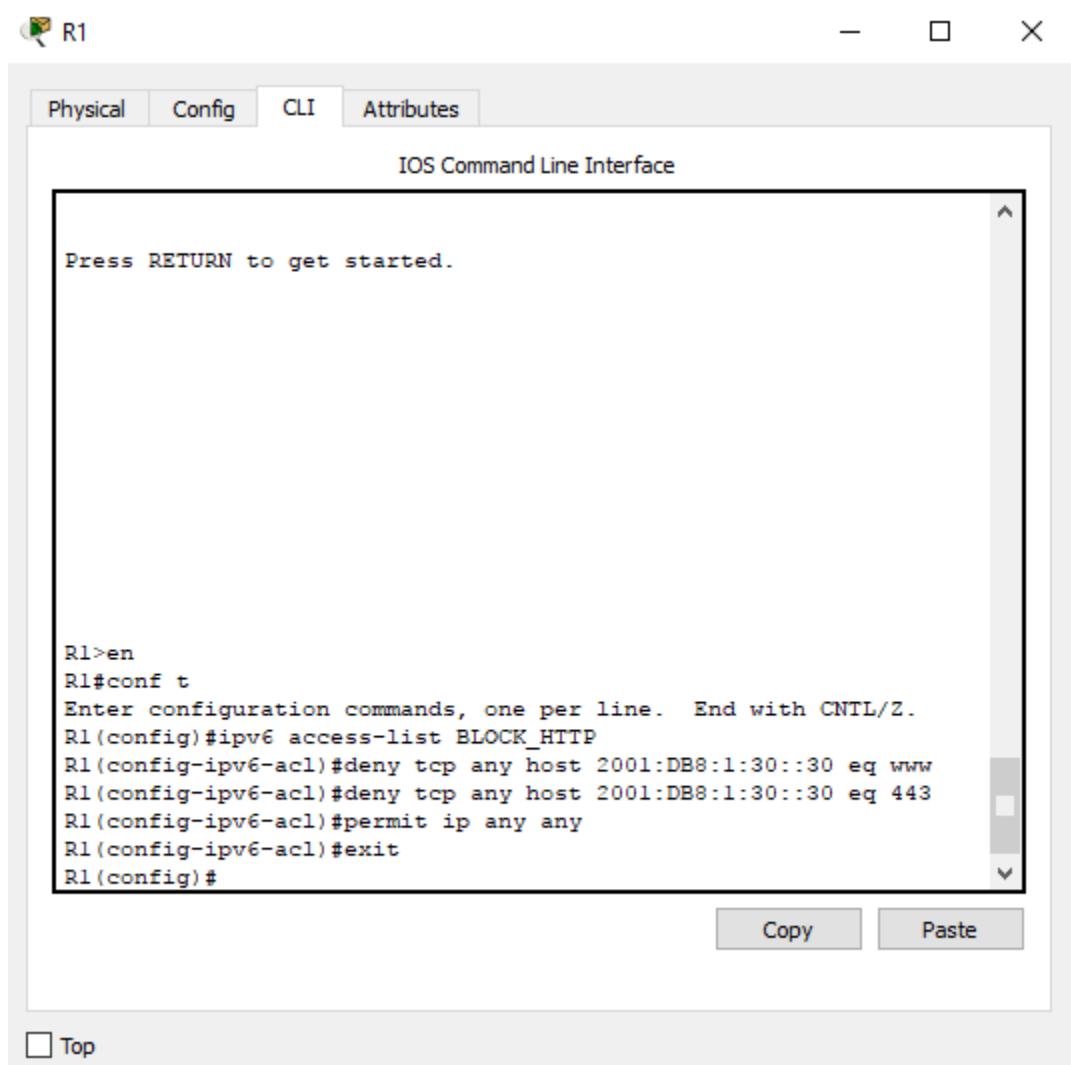
#### Step 1: Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named **BLOCK\_HTTP** on **R1** with the following statements.

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

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

- b. Allow all other IPv6 traffic to pass.



The screenshot shows a window titled "R1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The interface shows the following commands and their outputs:

```
Press RETURN to get started.

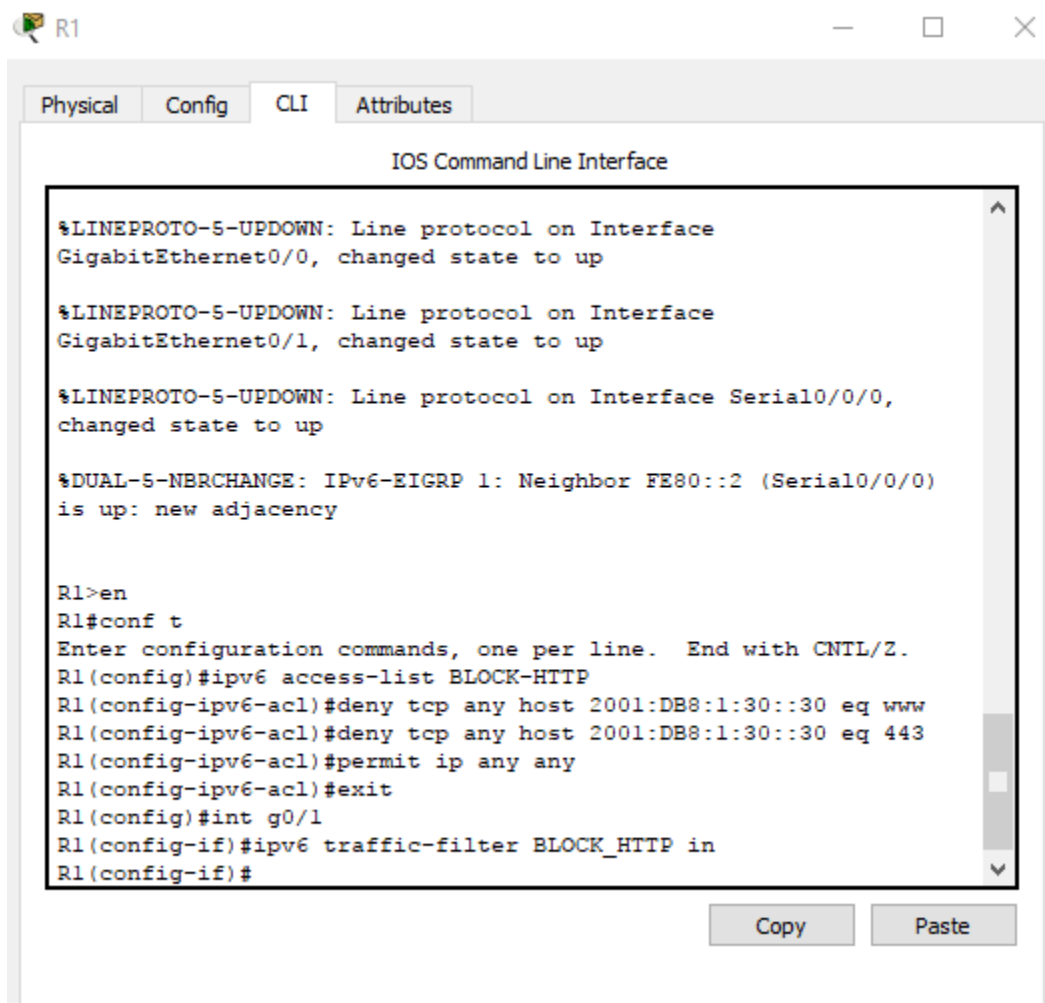
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ip any any
R1(config-ipv6-acl)#exit
R1(config)#
```

At the bottom of the CLI window, there are "Copy" and "Paste" buttons, and a "Top" button with a checkbox.

## Step 2: Apply the ACL to the correct interface.

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

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



The screenshot shows a network device CLI window titled "R1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The output shows several status messages indicating that line protocols on GigabitEthernet0/0, GigabitEthernet0/1, and Serial0/0/0 have changed state to up. It also shows an IPv6-EIGRP neighbor adjacency being established. The user then enters the configuration mode and configures an IPv6 access list named "BLOCK-HTTP" with two deny rules for TCP traffic to 2001:DB8:1:30::30 on ports 80 and 443, followed by a permit rule for all other traffic. Finally, the user applies this access list to interface GigabitEthernet0/1.

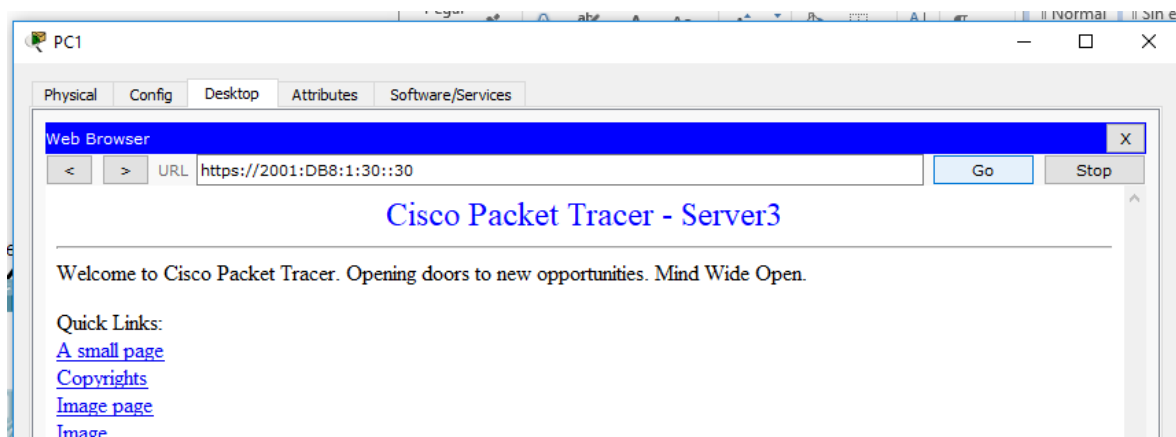
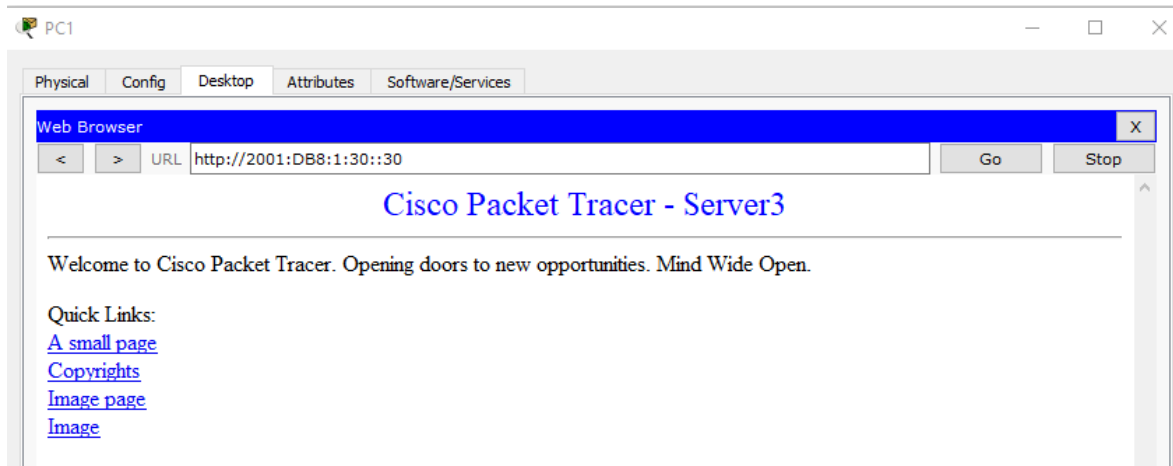
```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK-HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ip any any
R1(config-ipv6-acl)#exit
R1(config)#int g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

Copy Paste

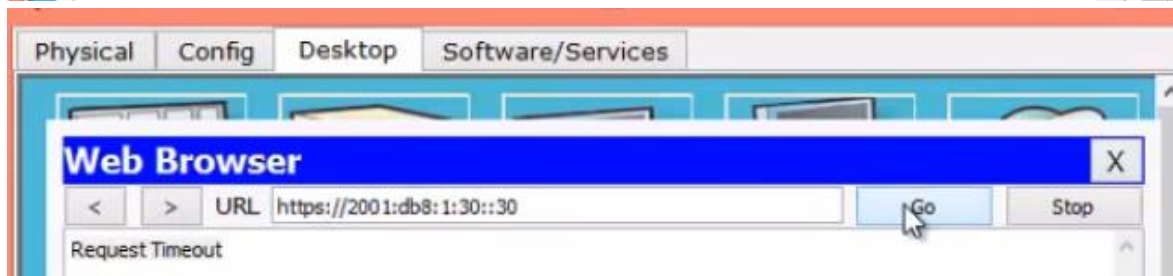
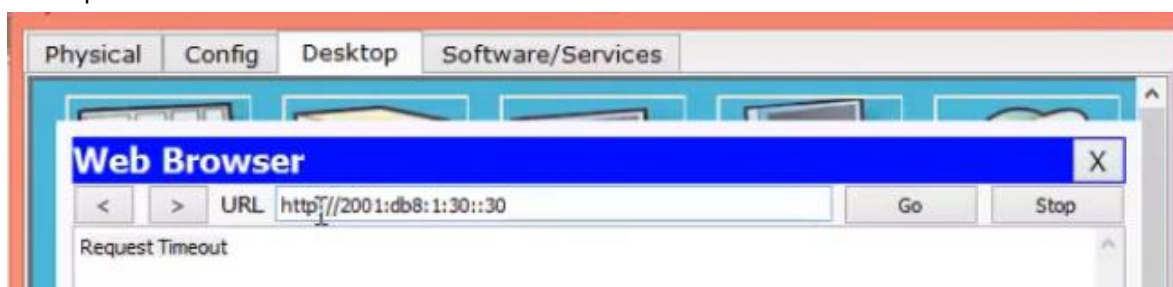
### Step 3: Verify the ACL implementation.

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

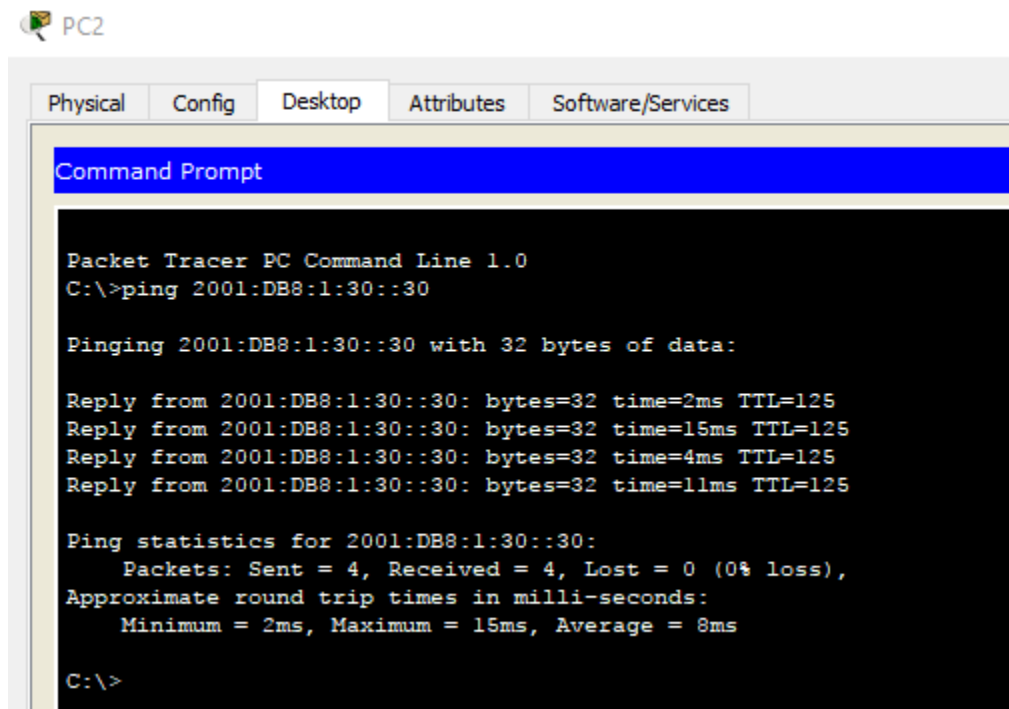
- Open the **web browser** of **PC1** to [http:// 2001:DB8:1:30::30](http://2001:DB8:1:30::30) or <https://2001:DB8:1:30::30>. The website should appear.



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



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



The screenshot shows a Packet Tracer PC Command Line window for PC2. The window has tabs for Physical, Config, Desktop, Attributes, and Software/Services. The Desktop tab is active, displaying a Command Prompt. The Command Prompt shows the following output:

```
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=15ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=4ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=11ms 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 = 15ms, Average = 8ms

C:\>
```

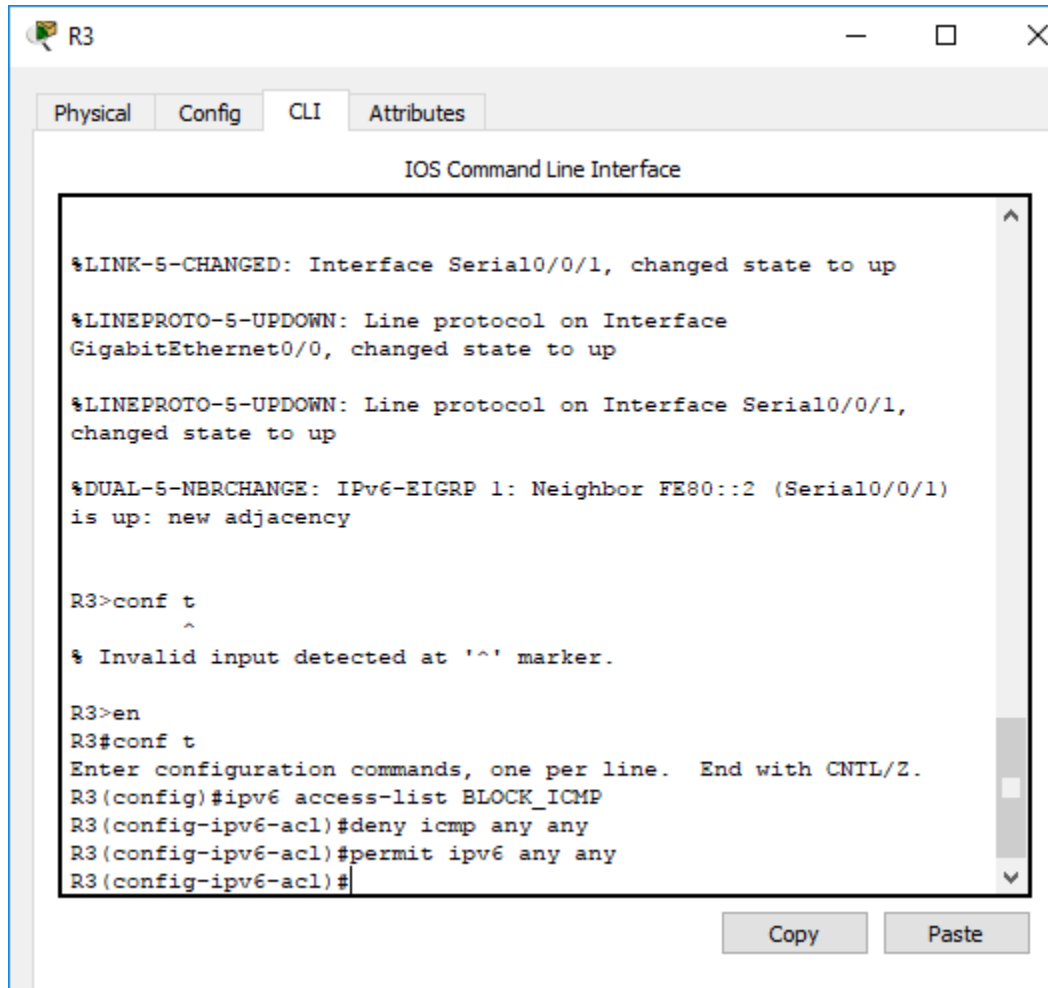
## Part 2: Configure, Apply, and Verify a Second IPv6 ACL

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

### Step 1: Create an access list to block ICMP.

Configure an ACL named **BLOCK\_ICMP** on **R3** with the following statements:

- a. Block all ICMP traffic from any hosts to any destination.
- b. Allow all other IPv6 traffic to pass.



The screenshot 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 several system messages indicating interface state changes and a new IPv6 EIGRP adjacency. The user enters the command "conf t", which is interpreted as "en" (enable), resulting in an "Invalid input detected at '^' marker." message. The user then enters "en" to return to user EXEC mode, followed by "conf t" to enter configuration mode. In configuration mode, the user enters the following commands: "ipv6 access-list BLOCK\_ICMP", "deny icmp any any", and "permit ipv6 any any". The prompt is currently "R3(config-ipv6-acl)#".

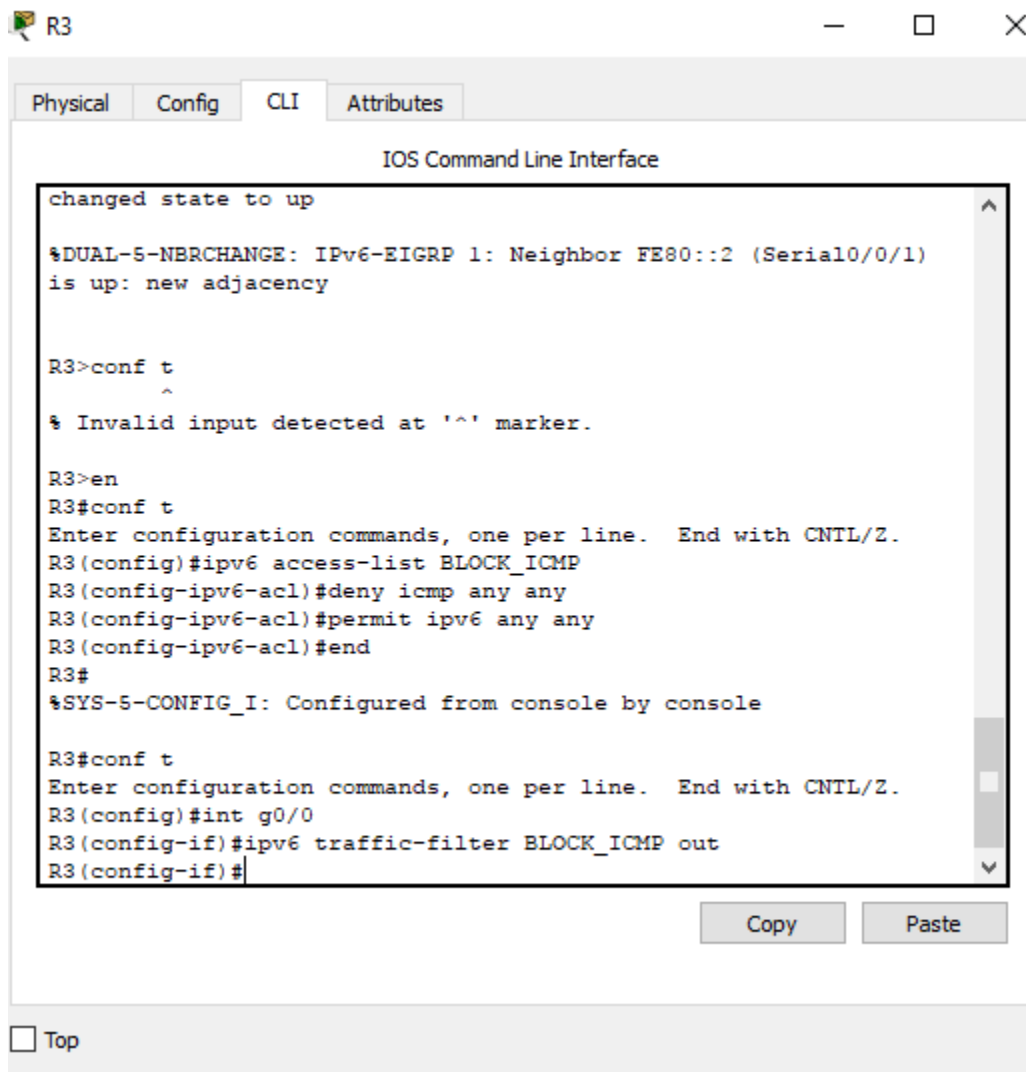
```
R3>conf t
^
% Invalid input detected at '^' marker.

R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#
```

## Step 2: Apply the ACL to the correct interface.

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





The screenshot shows a terminal window titled "R3" with tabs for "Physical", "Config", "CLI", and "Attributes". The main content is the "IOS Command Line Interface" showing the following sequence of commands and outputs:

```
changed state to up
%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::2 (Serial0/0/1)
is up: new adjacency

R3>conf t
^
% Invalid input detected at '^' marker.

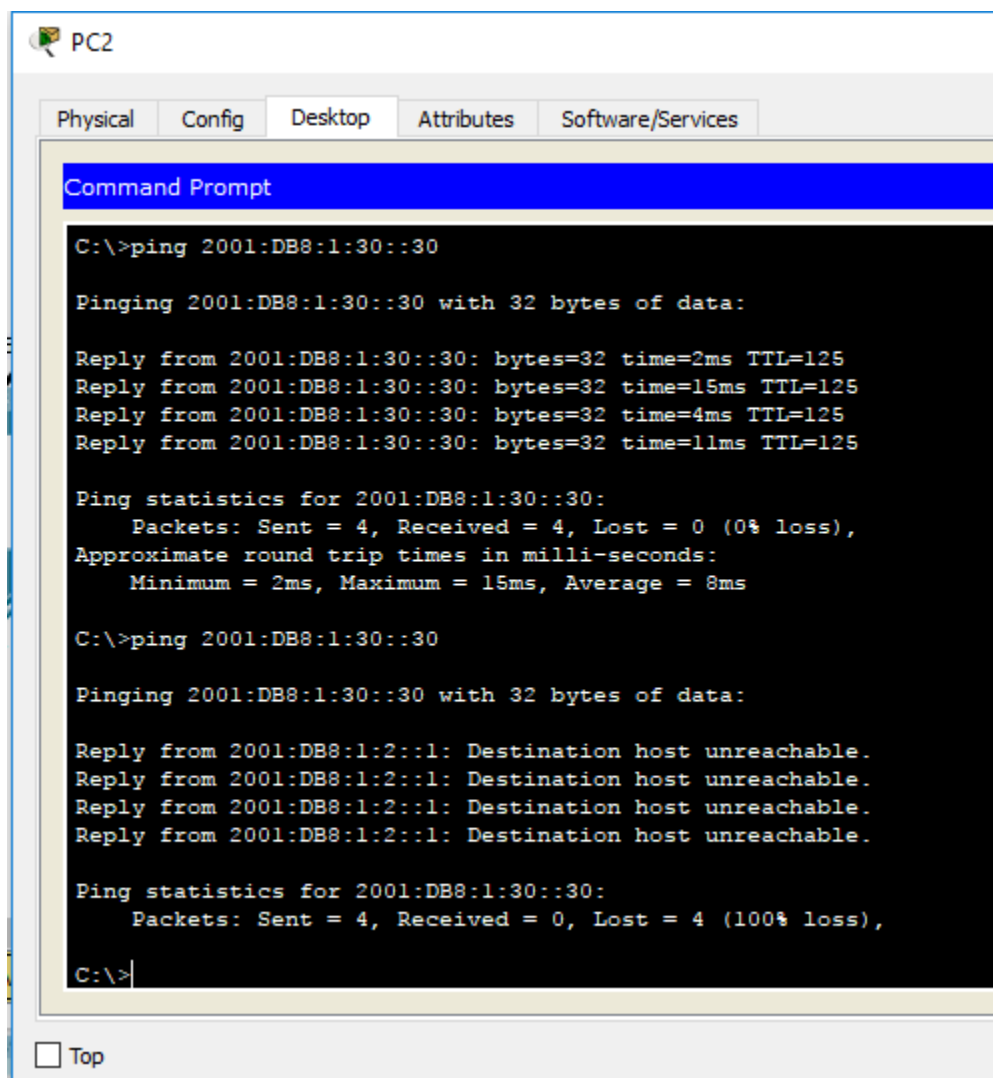
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

At the bottom of the terminal window, there are "Copy" and "Paste" buttons, and a "Top" button with a checkbox.

### Step 3: Verify that the proper access list functions.

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



```
PC2
Physical Config Desktop Attributes Software/Services
Command Prompt
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=15ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=4ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=11ms 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 = 15ms, Average = 8ms

C:\>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

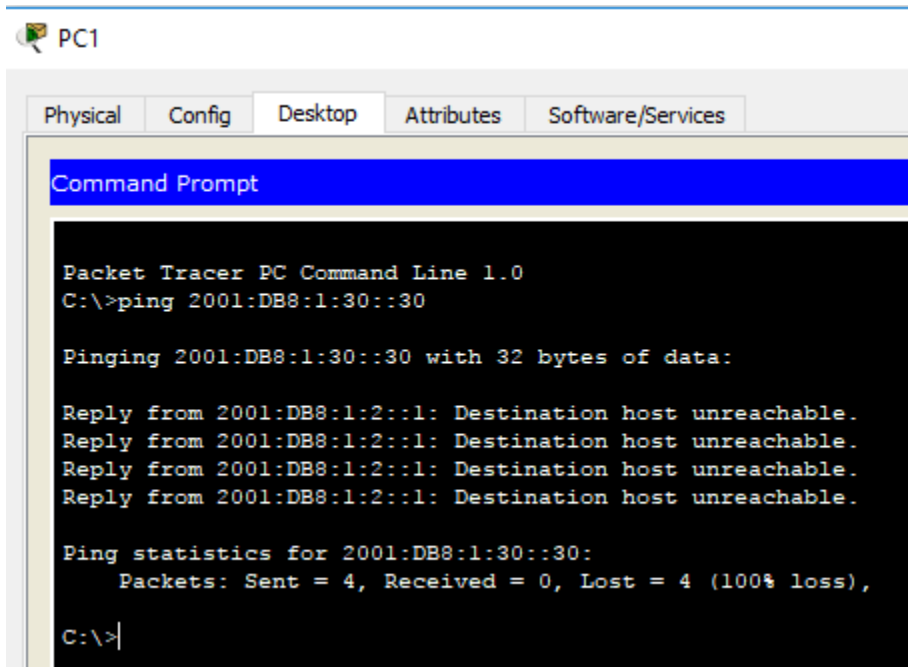
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

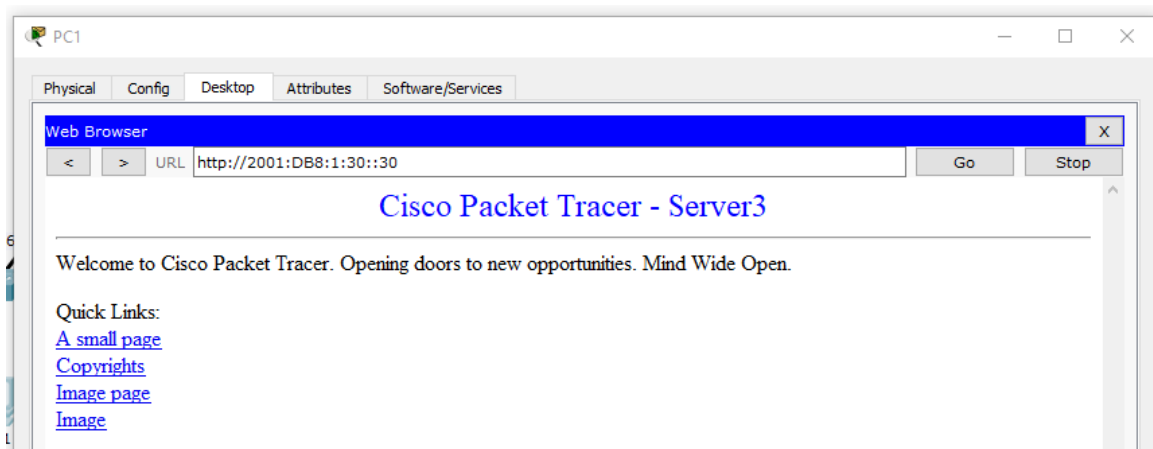
C:\>
```

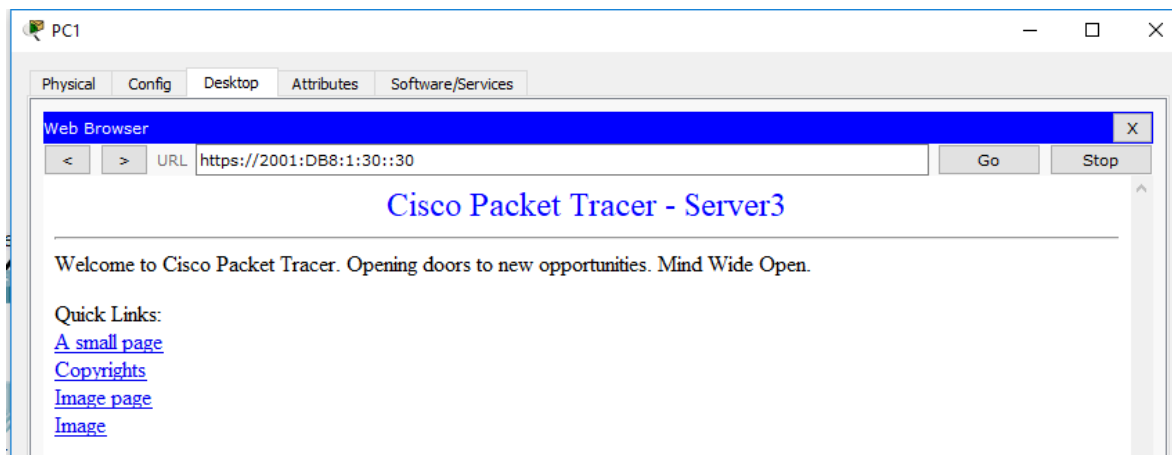
Top

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



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





### 10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router

## Topología

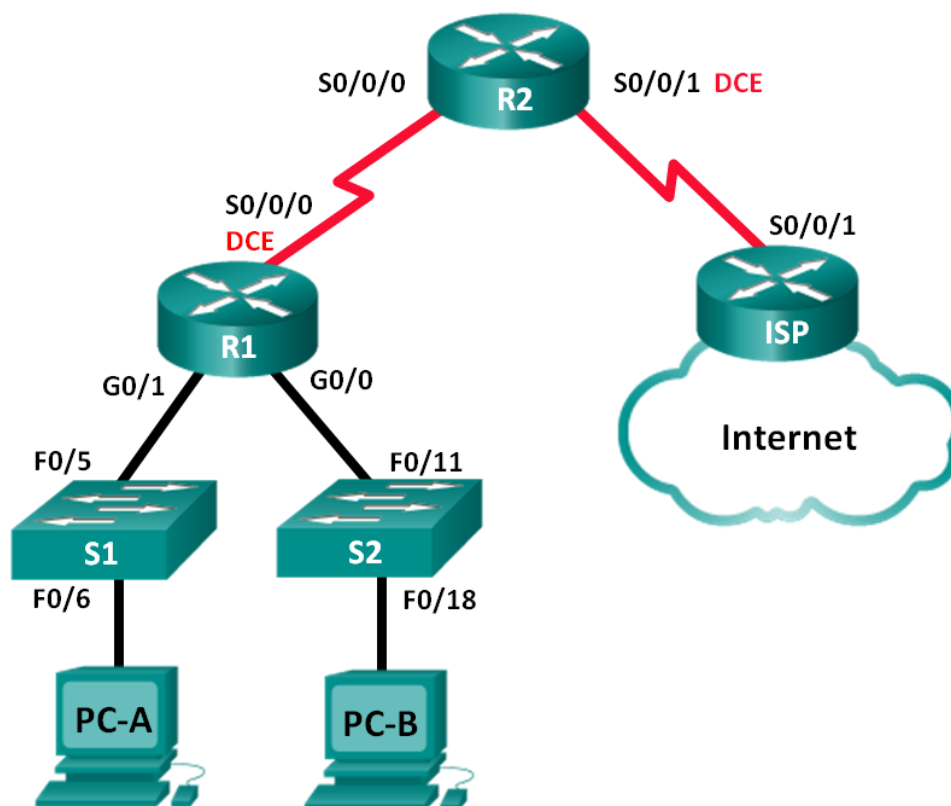


Tabla de direccionamiento

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

## Objetivos

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

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

## Información básica/situación

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

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

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

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

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

## Recursos necesarios

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

## 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.

**Step 29:** realizar el cableado de red tal como se muestra en la topología.

**Step 30:** inicializar y volver a cargar los routers y los switches.

**Step 31:** configurar los parámetros básicos para cada router.

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

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

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
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)#logging synchronous
R1(config-line)#
```

```
R1(config-if)#int g0/1
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 GigabitEthernet0/1, 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)#clock rate 128000
R1(config-if)#ip address 192.168.2.253 255.255.255.252
R1(config-if)#no shut
```

```

R2(config)#int s0/0/0
R2(config-if)#ip address 192.168.2.254 255.255.255.252
^
% Invalid input detected at '^' marker.

R2(config-if)#ip address 192.168.2.254 255.255.255.252
R2(config-if)#no shut

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

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

R2(config-if)#int 0/0/1
^
% Invalid input detected at '^' marker.

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

ISP>enable
Password:
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/1
ISP(config-if)#ip address 209.165.200.225 255.255.255.224
ISP(config-if)#no shut

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

ISP(config-if)#
%LINEPROTO-S-UPDOWN: Line protocol on 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>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 192.168.2.252 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#|

```

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

```

R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.252 0.0.0.3
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225

```



- 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>enable
Password:
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 192.168.0.0 255.255.255.0 209.165.200.226
ISP(config)#
```

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

### Step 32: 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.

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/31/149 ms

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 =
1/11/54 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 =
2/12/56 ms
```

### Step 33: 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.

### Step 34: 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.

```
-----
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
```

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?

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix... :
Physical Address. . . . . : 00E0.B000.C352
Link-local IPv6 Address . . . . . : FE80::2E0:B0FF:FE00:C352
Autoconfiguration IP Address. . . . : 169.254.195.82
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. . . . . : 00-01-00-01-9A-48-C2-46-00-E0-B0-00-C3-52
```

---

\_\_no por q R1 se debe configurar como un agente de retransmisión DHCP \_\_

### Step 35: 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.

## User Access Verification

Password:

R1&gt;enable

Password:

R1#config t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#int g0/0

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

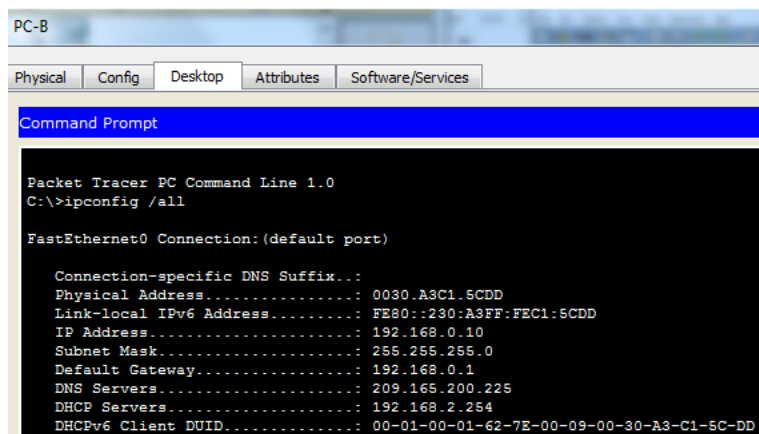
R1(config-if)#int g0/1

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

R1(config-if)#|

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.

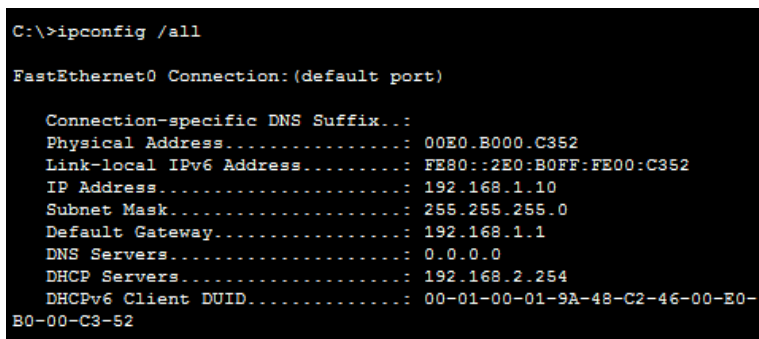


```

PC-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. . . . .: 0030.A3C1.5CDD
    Link-local IPv6 Address . . . . .: FE80::230:A3FF:FEC1:5CDD
    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. . . . .: 00-01-00-01-62-7E-00-09-00-30-A3-C1-5C-DD
  
```



```

C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address. . . . .: 00E0.B000.C352
    Link-local IPv6 Address . . . . .: FE80::2E0:B0FF:FE00:C352
    IP Address. . . . .: 192.168.1.10
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: 192.168.1.1
    DNS Servers . . . . .: 0.0.0.0
    DHCP Servers . . . . .: 192.168.2.254
    DHCPv6 Client DUID. . . . .: 00-01-00-01-9A-48-C2-46-00-E0-
    B0-00-C3-52
  
```

---

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?

\_\_190.168.0.10 y 192.168.1.10\_\_\_\_\_

### Step 36: 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?

```
R2#show ip dhcp binding
IP address      Client-ID/
                Hardware address      Lease expiration      Type
192.168.0.10    0030.A3C1.5CDD              --                    Automatic
192.168.1.10    00E0.B000.C352              --                    Automatic
R2#
```

\_\_\_\_las direcciones del hardware del cliente las cuales nos indican cuales computadores se unen a la red \_\_\_\_\_

- 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?

\_10

BOOTREQUEST,DHCPDISCOVER,DHCPRESQUEST,DHCPDECLINE,DHCPRELEASE,DHCPINFORM,BOOTREPLY,DHCPPPOFFER,DHCPACK,DHCPNAK\_\_\_\_\_

- 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 la siguiente ip disponible para arrendarse

```
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

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
R2#
```

- 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 R1G0
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 209.165.200.225
ip dhcp pool R1G1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
```

- e. En el R2, introduzca el comando **show run interface** para las interfaces G0/0 y G0/1 para ver la configuración de retransmisión DHCP en la configuración en ejecución.

```
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
ip helper-address 192.168.2.254
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.254
duplex auto
speed auto
!
interface Serial0/0/0
ip address 192.168.2.253 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
```

## Reflexión

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

DHCP no se tiene que dedicar mucho tiempo a configurar una red TCP/IP ni a la administración diaria de dicha red. Facilita la administración de las direcciones IP.

DHCP permite disminuir la carga administrativa asociada a la configuración manual de cada host con una dirección IP. Además, si un host se mueve a una subred IP diferente, debe utilizar una dirección de IP diferente de la que empleaba antes. DHCP se hace cargo de esto automáticamente, lo que permite al host elegir una dirección IP en la subred IP correcta.

## Tabla de resumen de interfaces del router

| Resumen de interfaces del router |                             |                             |                       |                       |
|----------------------------------|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de router                 | Interfaz Ethernet #1        | Interfaz Ethernet n.º 2     | Interfaz serial #1    | Interfaz serial n.º 2 |
| 1800                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

**Nota:** para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

## Apéndice A: comandos de configuración de DHCP

### Router R1

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

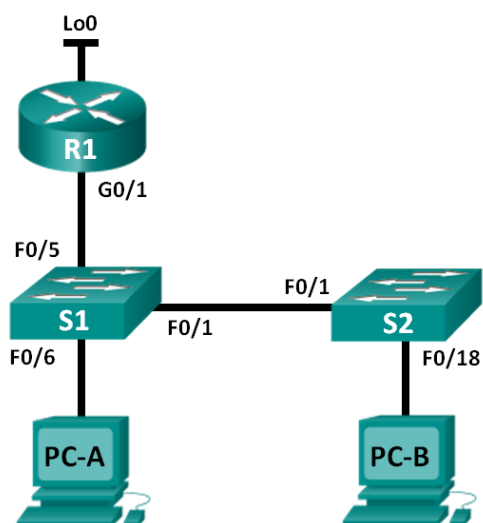
### Router R2

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
```

```
R2(dhcp-config)# network 192.168.0.0 255.255.255.0  
R2(dhcp-config)# default-router 192.168.0.1  
R2(dhcp-config)# dns-server 209.165.200.225  
R2(dhcp-config)# domain-name ccna-lab.com  
R2(dhcp-config)# lease 2
```

### 10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch

#### Topología

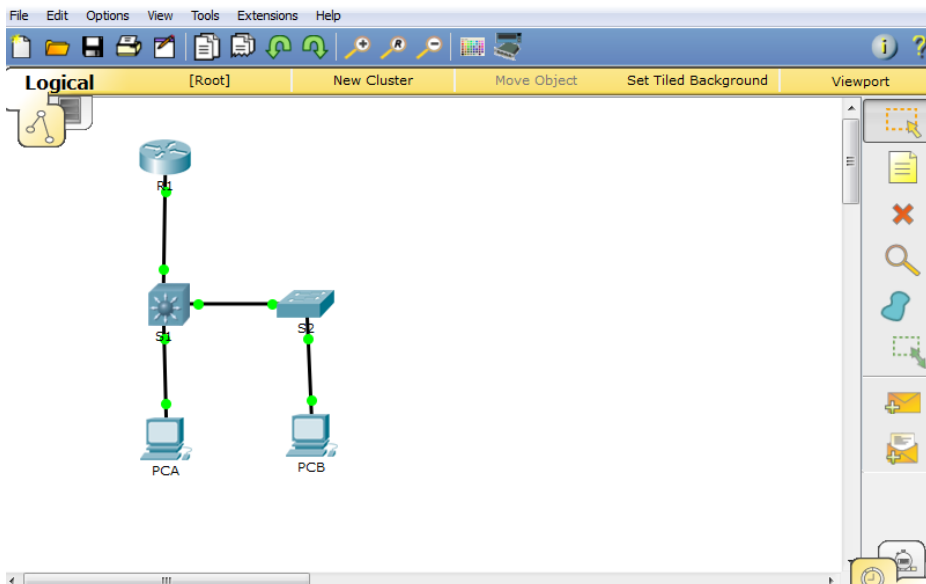


#### Tabla de direccionamiento

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

#### Objetivos





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

### **Parte 2: cambiar la preferencia de SDM**

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

### **Parte 3: configurar DHCPv4**

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

### **Parte 4: configurar DHCP para varias VLAN**

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

### **Parte 5: habilitar el routing IP**

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

### **Información básica/situación**

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

**Nota:** en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos

se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

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

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

### Recursos necesarios

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

### Parte 1. Armar la red y configurar los parámetros básicos de los dispositivos

**Paso 37:** realizar el cableado de red tal como se muestra en la topología.

**Paso 38:** inicializar y volver a cargar los routers y switches.

**Paso 39:** configurar los parámetros básicos en los dispositivos.

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

### 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.

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

**S1# show sdm prefer**

The current template is "dual-ipv4-and-ipv6 default" template.  
The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

|  |        |
|--|--------|
| number of unicast mac addresses:               | 4K     |
| number of IPv4 IGMP groups + multicast routes: | 0.25K  |
| number of IPv4 unicast routes:                 | 0      |
| number of IPv6 multicast groups:               | 0.375k |
| number of directly-connected IPv6 addresses:   | 0      |
| number of indirect IPv6 unicast routes:        | 0      |
| 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:                       | 0.625k |
| number of IPv6 security aces:                  | 125    |

**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

```

¿Cuál es la plantilla actual? Las soluciones cambian. “default” o “default dual-ipv4-and-ipv6” o “lanbase-routing”.

### Paso 2: cambiar la preferencia de SDM en el S1.

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

```
S1(config)# sdm prefer lanbase-routing
```

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

#### S1# show sdm prefer

```

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

```

```

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

```

On next reload, template will be "lanbase-routing" template.

¿Qué plantilla estará disponible después de la recarga? lanbase-routing

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

```
S1# reload
```

System configuration has been modified. Save? [yes/no]: **no**

Proceed with reload? [confirm]

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

### 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.

- Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó. S1(config)# **ip dhcp excluded-address 192.168.1.1 192.168.1.10**
- Cree un pool de DHCP con el nombre **DHCP1**. En el espacio proporcionado, escriba el comando que utilizó. S1(config)# **ip dhcp pool DHCP1**
- Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó. S1(dhcp-config)# **network 192.168.1.0 255.255.255.0**
- Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó. S1(dhcp-config)# **default-router 192.168.1.1**
- Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó. S1(dhcp-config)# **dns-server 192.168.1.9**
- Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó. S1(dhcp-config)# **lease 3**
- Guarde la configuración en ejecución en el archivo de configuración de inicio.

**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

Para la PC-B, incluya lo siguiente:

Dirección IP: 192.168.1.12

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1

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

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

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

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

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

**Paso 1: asignar un puerto a la VLAN 2.**

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

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

S1(config-if)# **switchport access vlan 2**

**Paso 2: configurar DHCPv4 para la VLAN 2.**

Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó. S1(config)# **ip dhcp excluded-address 192.168.2.1 192.168.2.10**

Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó. S1(config)# **ip dhcp pool DHCP2**

Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó. S1(dhcp-config)# **network 192.168.2.0 255.255.255.0**

Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó. S1(dhcp-config)# **default-router 192.168.2.1**

Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó. S1(dhcp-config)# **dns-server 192.168.2.9**

Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó. S1(dhcp-config)# **lease 3**

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

### **Paso 3: verificar la conectividad y DHCPv4.**

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

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.2.11

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.2.1

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

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

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

¿Los pings eran correctos? ¿Por qué? el gateway predeterminado está en la misma red que la PC-A, esta puede hacer ping al gateway predeterminado. La PC-B está en una red diferente; por lo tanto, el ping de la PC-A no es correcto.

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

#### **S1# show ip route**

Default gateway is not set

Host Gateway Last Use Total Uses Interface

ICMP redirect cache is empty

¿Qué resultado arrojó este comando? No se instauró un gateway predeterminado y no hay una tabla de routing presente en el switch.

### **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.**

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

S1(config)# **ip routing**

- b. Verificar la conectividad entre las VLAN.  
 ¿Es posible hacer ping de la PC-A a la PC-B? Sí  
 ¿Qué función realiza el switch? El switch hace routing entre VLAN.
- c. Vea la información de la tabla de routing para el S1.  
 ¿Qué información de la ruta está incluida en el resultado de este comando?  
 El switch nos enseña una tabla de routing que muestra las VLAN como las redes conectadas directamente 192.168.1.0/24 y 192.168.2.0/24.
- d. Vea la información de la tabla de routing para el R1.  
 ¿Qué información de la ruta está incluida en el resultado de este comando?  
 El producto del router muestra las redes conectadas directamente 192.168.1.0 y 209.165.200.224, pero no tiene ninguna entrada para la red 192.168.2.0.
- e. ¿Es posible hacer ping de la PC-A al R1? No  
 ¿Es posible hacer ping de la PC-A a la interfaz Lo0? No  
 Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?  
 Para que haya comunicación entre todas las redes, se deben agregar rutas a las tablas de routing.

## Paso 2: asignar rutas estáticas.

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

- a. En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.  
**S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10**
- b. En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.  
**R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1**
- c. Vea la información de la tabla de routing para el S1.  
 ¿Cómo está representada la ruta estática predeterminada?  
 Gateway of last resort is 192.168.1.10 to network 0.0.0.0
- d. Vea la información de la tabla de routing para el R1.  
 ¿Cómo está representada la ruta estática?  
 S 192.168.2.0/24 está conectada directamente, GigabitEthernet0/1
- e. ¿Es posible hacer ping de la PC-A al R1? Sí  
 ¿Es posible hacer ping de la PC-A a la interfaz Lo0? Si



## Reflexión

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

Si las trayectorias estáticas se excluyeran después de la creación del pool de DHCPv4, existiría un lapso durante el cual las direcciones excluidas podrían pasarse dinámicamente a hosts.

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

El switch ofrece las configuraciones IP según la asignación que haga la VLAN del puerto al que el host está conectado.

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

El switch puede trabajar como un servidor de DHCP y puede hacer routing estático y entre VLAN.

**Tabla de resumen de interfaces del router**

| Resumen de interfaces del router |                             |                             |                       |                       |
|----------------------------------|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de router                 | Interfaz Ethernet #1        | Interfaz Ethernet n.º 2     | Interfaz serial #1    | Interfaz serial n.º 2 |
| 1800                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

**Nota:** para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

## Apéndice A: comandos de configuración

### Configurar DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

```
S1(config)# ip dhcp pool DHCP1
```

```
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

### Configurar DHCPv4 para varias VLAN

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

### Habilitar routing IP

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

### Configuraciones de dispositivos

#### Router R1

```
R1#show run
Building configuration...
Current configuration : 1489 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
```

```
!  
!  
no ip domain lookup  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
!  
interface Loopback0  
ip address 209.165.200.225 255.255.255.0  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
ip address 192.168.1.10 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/0/0  
no ip address  
shutdown  
clock rate 2000000  
!  
interface Serial0/0/1  
no ip address  
shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
ip route 192.168.2.0 255.255.255.0 GigabitEthernet0/1  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
password cisco  
login  
line aux 0
```

```
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Switch S1

```
S1#show run
Building configuration...
Current configuration : 3636 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
ip routing
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.2.1 192.168.2.10
!
ip dhcp pool DHCP1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 192.168.1.9
lease 3
!
ip dhcp pool DHCP2
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 192.168.2.9
lease 3
```

```
!  
!  
no ip domain-lookup  
!  
!  
crypto pki trustpoint TP-self-signed-2531409152  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-2531409152  
revocation-check none  
rsakeypair TP-self-signed-2531409152  
!  
!  
crypto pki certificate chain TP-self-signed-2531409152  
certificate self-signed 01  
3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030  
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274  
69666963 6174652D 32353331 34303931 3532301E 170D3933 30333031 30303030  
35365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649  
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 35333134  
30393135 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281  
8100CA1B 27DE634E CF9FE284 C86127EF 41E7A52F 0A82FA2B 7C5448B7 184EA1AB  
C22510E1 38A742BC D9F416FD 93A52DC6 BA77A928 B317DA75 1B3E2C66 C2D9061B  
806132D9 E3189012 467C7A2C DCAC3EF4 4C419338 790AA98B C7A81D73 8621536C  
4A90659E 267BA2E3 36F801A4 F06BEC65 386A40DA 255D9790 F9412706 9E73A660  
45230203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603  
551D2304 18301680 14A7356A D364AE65 E1E9D42F 9B059B27 B69BB9C6 FD301D06  
03551D0E 04160414 A7356AD3 64AE65E1 E9D42F9B 059B27B6 9BB9C6FD 300D0609  
2A864886 F70D0101 05050003 8181002A D78919E7 0D75567C EF60036C 6C4B051A  
2ABC5B9C DA1C1E48 AF33C405 5C64E074 B954C5B5 D825BE61 7340C695 03049797  
D869E516 3936D0EC C871F140 66A1DEB2 BA57AB0D D2AB2706 17674B3A 7423C276  
B96CFB88 DE98A86E 7B539B68 7DEE53BB ED16BFA0 A89A5CA4 79F15F49 59DDF6E5  
E716514A 5CFC7522 8E76778E 029E8F  
quit  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3
```

```
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
switchport access vlan 2  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
ip address 192.168.1.1 255.255.255.0  
!  
interface Vlan2  
ip address 192.168.2.1 255.255.255.0
```

```
!  
ip http server  
ip http secure-server  
ip route 0.0.0.0 0.0.0.0 192.168.1.10  
!  
!  
!  
line con 0  
password cisco  
login  
line vty 0 4  
password cisco  
login  
line vty 5 15  
password cisco  
login  
!  
end
```

### 10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6

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

#### Topología



#### Tabla de direccionamiento

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

#### Objetivos

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

**Parte 2: configurar la red para SLAAC**

**Parte 3: configurar la red para DHCPv6 sin estado**

**Parte 4: configurar la red para DHCPv6 con estado**

#### Información básica/situación

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

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

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

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



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

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

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

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

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

### S1# show sdm prefer

```

S1
-----
System serial number      : FOC133311EY
Top Assembly Part Number  : 800-24671-02
Top Assembly Revision Number : 80
Version ID                : V02
CLEI Code Number         : COM3K0082A
Hardware Board Revision Number : 0x01

Switch  Ports  Model          SW Version      SW Image
-----  -
* 1    26    WS-C2960-24FT  15.2            C2960-LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 15.2(2)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch#ENABLE
Switch#HOSTNAME S1
Switch#CONFIGURE T
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#HOSTNAME S1
S1(config)#END
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

number of unicast mac addresses:      8K
number of IPv4 IGMP groups:          256
number of IPv4/MSC qos aces:         128
number of IPv4/MSC security aces:    384

S1#

```

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

```

The screenshot shows a terminal window titled "S1" with tabs for Physical, Config, CLI, and Attributes. The main content is the IOS Command Line Interface output, which includes system information and a table of switch ports.

```

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:06 by pt_team
Image text-base: 0x00000098, data-base: 0x014129C4

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0001.6420.CC3A
Motherboard assembly number     : 73-8932-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MCP
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                     : WS-C2960-24TT
System serial number            : FOC10321EY
Top Assembly Part Number        : 820-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
Class Code Number               : COM9008DA
Hardware Board Revision Number  : 0x01

Switch  Ports  Model          SW Version      SW Image
-----  -
* 1    24    WS-C2960-24TT  12.2            C2960-LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:06 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

```

## 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.

**Step 3:** realizar el cableado de red tal como se muestra en la topología.

**Step 4:** inicializar y volver a cargar el router y el switch según sea necesario.

**Step 5: Configurar R1**

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

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
San Jose, California 95134-1706
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 8-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24728040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wai/export/crypto/qa/tqa.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTK12400E2
2 Gigabit Ethernet interfaces
2 low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
256K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>ENABLE
Router>CONFIG Y
% Invalid input detected at '^' marker.
Router>CONFIG ?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
% Invalid input detected at '^' marker.
Router(config)#hostname R1
R1(config)#
  
```

**Step 6: configurar el S1.**

- Desactive la búsqueda del DNS.
- Configure el nombre del dispositivo.
- Cifre las contraseñas de texto no cifrado.
- Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.

- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Desactive administrativamente todas las interfaces inactivas.
- i. Guarde la configuración en ejecución en la configuración de inicio.

```

S1
Physical Config CLI Attributes
IOS Command Line Interface

Power supply serial number : DTR1036C7UB
Model revision number      : P0
Motherboard revision number : A0
Model number                : WS-C3560-24PS-E
System serial number        : CAT10379J7F
Top Assembly Part Number    : 820-26380-04
Top Assembly Revision Number : 80
Version ID                  : V06
CISX Code Number           : C081100A3C
Hardware Board Revision Number : 0x01

Switch Ports Model          SW Version      SW Image
-----
* 1 24 WS-C3560-24PS      12.2(37)SE1     C3560-ADVIPSERVICESK

Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

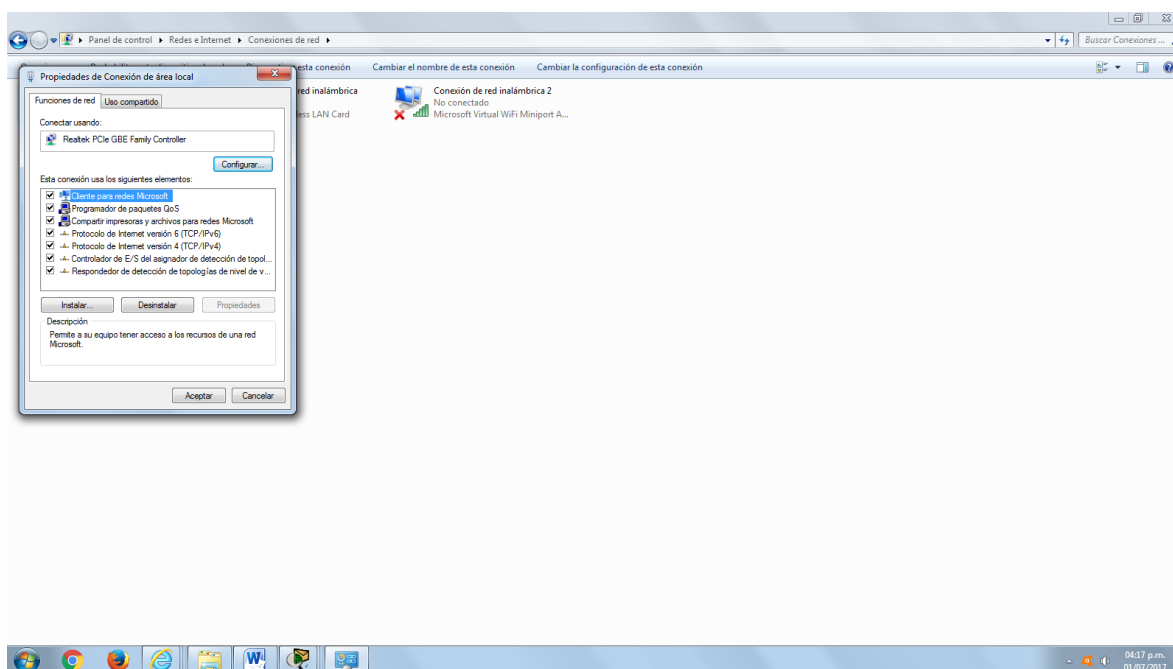
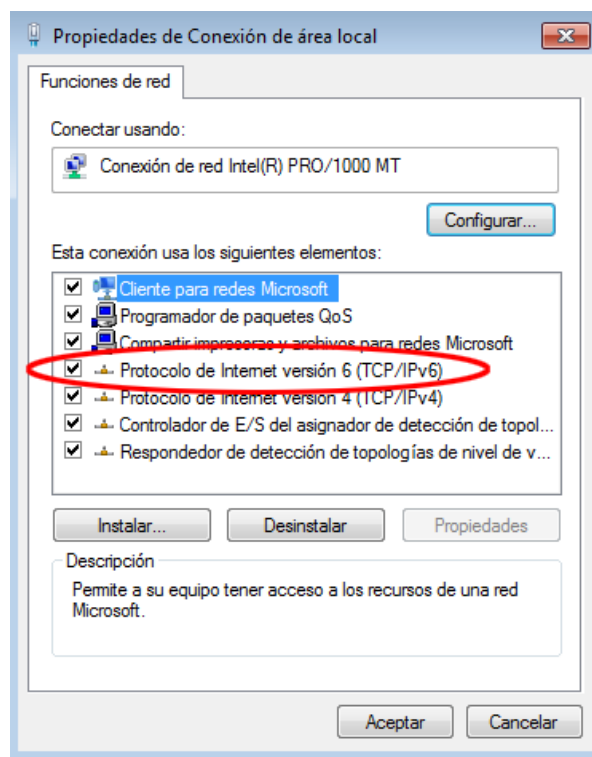
Switch>ENABLE
Switch#SHOW SIM PREFER
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.
number of unicast mac addresses: 6K
number of IPv4 IGMP groups + multicast sources: 1K
number of IPv4 unicast routes: 8K
number of directly-connected IPv4 hosts: 6K
number of indirect IPv4 routes: 2K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.5K
number of IPv4/MAC security aces: 1K

Switch#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
  
```

## Parte 2. configurar la red para SLAAC

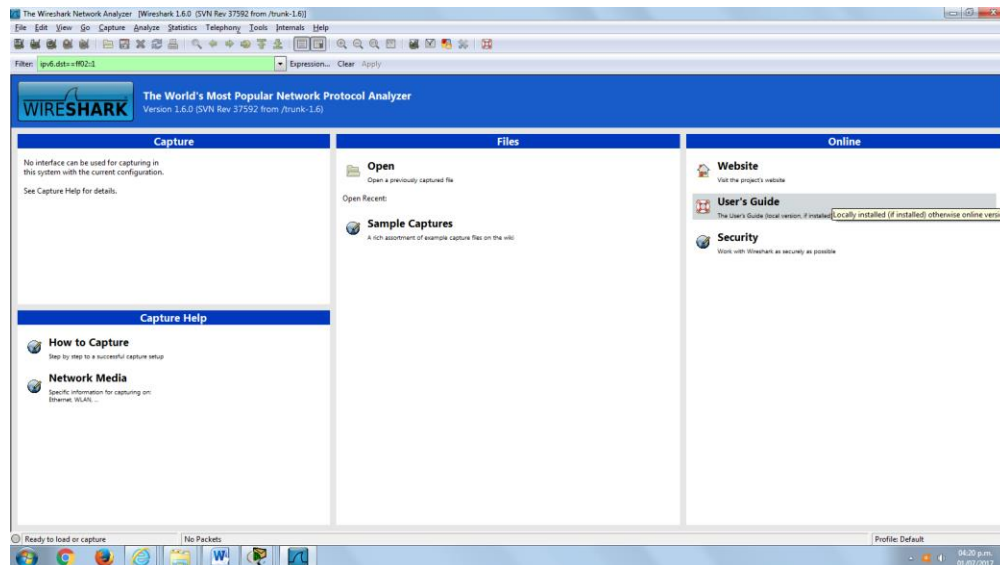
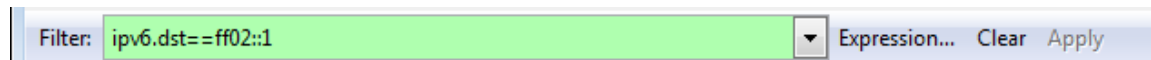
### Step 7: preparar la PC-A.

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



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

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



## Step 8: Configurar R1

- a. Habilite el routing de unidifusión IPv6.

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wai/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco C1900-1941-K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400K2
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
256K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>ENABLE
Router#CONFIG Y
-
% Invalid input detected at *** marker.
Router#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#HOSTNAME R1
-
% Invalid input detected at *** marker.
Router(config)#HOSTNAME R1
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
Physical Config CLI Attributes
IOS Command Line Interface

Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wai/export/crypto/tool/stqrg.html

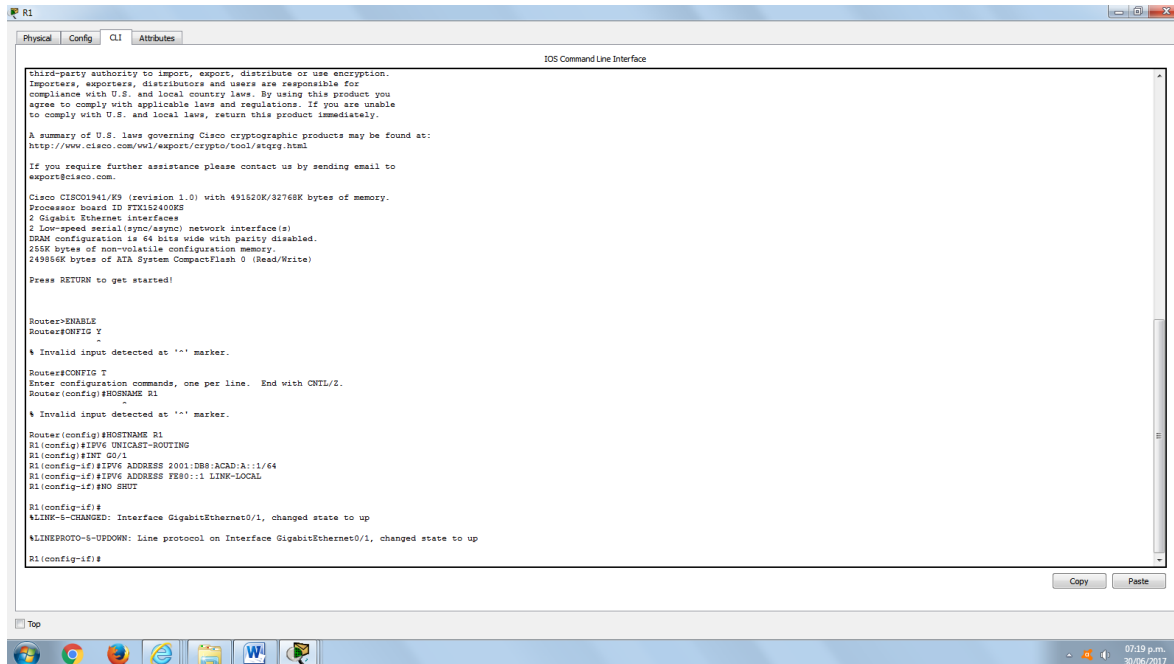
If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco C1900-1941-K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400K2
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
256K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>ENABLE
Router#CONFIG Y
-
% Invalid input detected at *** marker.
Router#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#HOSTNAME R1
-
% Invalid input detected at *** marker.
Router(config)#HOSTNAME R1
R1(config)#IPV6 UNICAST-ROUTING
R1(config)#INT G0/1
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.  
 d. Active la interfaz G0/1.



### Step 9: 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
-----
Physical Config CLI Attributes
IOS Command Line Interface

* Invalid input detected at '^' marker.
Router#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
* Invalid input detected at '^' marker.

Router(config)#hostname R1
R1(config)#ipv6 unicast-routing
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)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#SHOW IPV6 INTERFACE G0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FE80::1
  FE80::1:FE80::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 retirement interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1200 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#

```

### Step 10: configurar el S1.

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

```

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

```

### Step 11: verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

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

```

S1# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
No Virtual link-local address(es):
Stateless address autoconfig enabled
Global unicast address(es):
  2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]
    valid lifetime 2591988 preferred lifetime 604788
Joined group address(es):
  FF02::1
  FF02::1:FE8:8A40

```

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

Output features: Check hwidb

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND NS retransmit interval is 1000 milliseconds

**Default router is FE80::1 on Vlan1**

```

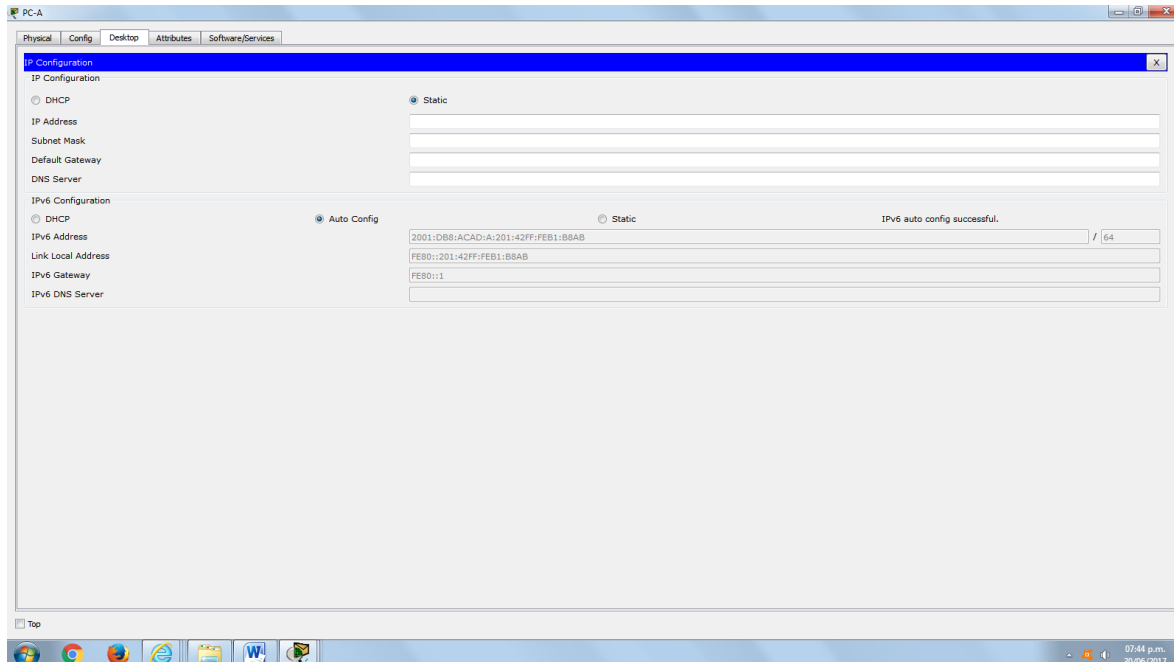
S1
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

S1#
*SYS-5-CONFIG_I: Configured from console by console
S1#show ipv6 interface
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan 1
S1(config-if)#no shut

S1(config-if)#
*LINE-5-CHANGED: Interface Vlan1, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#end
S1#
*SYS-5-CONFIG_I: Configured from console by console
S1#show ipv6 interface brief
FastEthernet0/1          [down/down]
FastEthernet0/2          [down/down]
FastEthernet0/3          [down/down]
FastEthernet0/4          [down/down]
FastEthernet0/5          [up/up]
FastEthernet0/6          [up/up]
FastEthernet0/7          [down/down]
FastEthernet0/8          [down/down]
FastEthernet0/9          [down/down]
FastEthernet0/10         [down/down]
FastEthernet0/11         [down/down]
FastEthernet0/12         [down/down]
FastEthernet0/13         [down/down]
FastEthernet0/14         [down/down]
FastEthernet0/15         [down/down]
FastEthernet0/16         [down/down]
FastEthernet0/17         [down/down]
FastEthernet0/18         [down/down]
FastEthernet0/19         [down/down]
FastEthernet0/20         [down/down]
FastEthernet0/21         [down/down]
FastEthernet0/22         [down/down]
FastEthernet0/23         [down/down]
FastEthernet0/24         [down/down]
GigabitEthernet0/1       [down/down]
GigabitEthernet0/2       [down/down]
Vlan1                    [up/up]
S1#

```



**Step 12: verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.**

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

```

Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . : 
    Descripción . . . . . : Conexión de red Intel(R) PRO/1000
    MT
    Dirección física. . . . . : 00-0C-29-E3-23-17
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Preferido)
    Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11(Preferido)
    Dirección IPv4. . . . . : 192.168.96.139(Preferido)
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : fe80::1:11
    Servidores DNS . . . . . : fec0:0:0:ffff::1%1
    : fec0:0:0:ffff::2%1
    : fec0:0:0:ffff::3%1
    NetBIOS sobre TCP/IP. . . . . : habilitado
  
```

```

PC-A
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. . . . .: 0001.4281.B8AB
Link-local IPv6 Address . . . . .: FE80::201:42FF:FEB1:B8AB
IP Address. . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: 0.0.0.0
DNS Servers . . . . .: 0.0.0.0
DHCP Servers . . . . .: 0.0.0.0
DHCPv6 Client GUID . . . . .: 00-01-00-01-3E-55-DB-02-00-01-42-B1-B8-AB

C:\>

```

```

PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>IPCONFIG

FastEthernet0 Connection: (default port)
Link-local IPv6 Address . . . . .: FE80::201:42FF:FEB1:B8AB
IP Address . . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: 0.0.0.0

C:\>IPV6CONFIG

FastEthernet0 Connection: (default port)
Link-local IPv6 Address . . . . .: FE80::201:42FF:FEB1:B8AB
IPv6 Address . . . . .: 2001:DB8:ACAD:A:201:42FF:FEB1:B8AB/64
Default Gateway . . . . .: FE80::1
DHCPv6 Client GUID . . . . .: 00-01-00-01-3E-55-DB-02-00-01-42-B1-B8-AB

C:\>

```

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

se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.

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

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

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

- Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast\_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
  - Type: Router Advertisement (134)
  - Code: 0
  - Checksum: 0x1816 [correct]
  - Cur hop limit: 64
  - Flags: 0x00
    - 0... .. = Managed address configuration: Not set
    - .0... .. = Other configuration: Not set
    - ..0... .. = Home Agent: Not set
    - ...0 0... = Prf (Default Router Preference): Medium (0)
    - ....0.. = Proxy: Not set
    - .... ..0. = Reserved: 0
  - Router lifetime (s): 1800
  - Reachable time (ms): 0
  - Retrans timer (ms): 0
  - ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
  - ICMPv6 Option (MTU : 1500)
  - ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)
    - Type: Prefix information (3)
    - Length: 4 (32 bytes)
    - Prefix Length: 64
    - Flag: 0xc0
    - Valid Lifetime: 2592000
    - Preferred Lifetime: 604800
    - Reserved
    - Prefix: 2001:db8:acad:a:: (2001:db8:acad:a::)

### Parte 3. configurar la red para DHCPv6 sin estado

#### Step 13: configurar un servidor de DHCP IPv6 en el R1.

```

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

R1>config t
-
% Invalid input detected at '^' marker.

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

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

- a. Cree un pool de DHCP IPv6.

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

- b. Asigne un nombre de dominio al pool.

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

- c. Asigne una dirección de servidor DNS.

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

```
R1(config-dhcpv6)# exit
```

```

R1
-----
R1>config t
-
% Invalid input detected at '^' marker.
R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FE02::1
  FE02::2
  FE02::1:FE00:1
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
Routers use stateless autoconfig for addresses.
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool ipv6pool-a
R1(config-dhcpv6)#domain-name ccna-statelessDHCPv6.COM
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
```

- 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 t
% Invalid input detected at '^' marker.
R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
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
Routers use stateless autoconfig for addresses.
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#domain-name ccna-statelessDHCPV6.COM
R1(config-dhcpv6)#dhcp-server 2001:DB8:ACAD:A::ABCD
R1(config-dhcpv6)#EXIT
R1(config)#INTERFACE G0/1
R1(config-if)#IPv6 DHCP SERVER IPV6POOL-AQ
R1(config-if)#IPv6 DHCP SERVER IPV6POOL-A
R1(config-if)#ipv6 ND OTHER-CONFIG-FLAG
R1(config-if)#END
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

```

#### Step 14: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

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

R1# **show ipv6 interface g0/1**

```

GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF02::1:FF00:1
  FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds

```

ND router advertisements live for 1800 seconds  
 ND advertised default router preference is Medium  
 Hosts use stateless autoconfig for addresses.  
**Hosts use DHCP to obtain other configuration.**

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

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(config)#
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool ipv6pool-a
R1(config-dhcpv6)#domain-name ccsa-statelessNDHCPv6.COM
R1(config-dhcpv6)#DNS-SERVER 2001:DB8:ACAD:A::ABCD
R1(config-dhcpv6)#EXIT
R1(config)#INTERFACE G0/1
R1(config-if)#IPv6 DHCP SERVER IPV6POOL-AQ
R1(config-if)#IPv6 DHCP SERVER IPV6POOL-A
R1(config-if)#ipv6 ND CONFIG-STATUS
R1(config-if)#END
R1#
NEWS-6-CONFIG_I: Configured from console by console

R1#SHOW IPV6 INTERFACE G0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FE02::1
  FE02::2
  FE02::1:2
  FE02::1:FE00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#
  
```

### Step 15: ver los cambios realizados en la red en la PC-A.

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



```

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

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

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

```

### Step 16: 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)

```

### Step 17: verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.

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

```
R1# show ipv6 dhcp binding
```

R1# show ipv6 dhcp pool

DHCPv6 pool: IPV6POOL-A

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

Domain name: ccna-statelessDHCPv6.com

Active clients: 0

```

R1#show ipv6 dhcp pool
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#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool ipv6pool-a
R1(config-dhcpv6)#domain-name ccna-statelessDHCPv6.COM
R1(config-dhcpv6)#dns-server 2001:DB8:ACAD:A::ABCD
R1(config-dhcpv6)#EXIT
R1(config)#interface G0/1
R1(config-if)#ipv6 dhcp server IPV6POOL-AQ
R1(config-if)#ipv6 dhcp server IPV6POOL-A
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#END
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#SHOW IPV6 INTERFACE G0/1
Sysctlksharmer0/1 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 retrasmrvt 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 dhcp BINDING
R1#show ipv6 dhcp POOL
DHCPv6 pool: ipv6pool-a
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.COM
Active clients: 0
R1#

```

## Step 18: 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

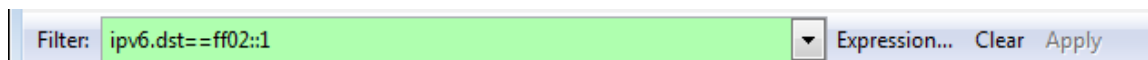
S1(config-if)# shutdown

- Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.
- Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.
  - 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.
  - Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

## Parte 4. configurar la red para DHCPv6 con estado

### Step 19: preparar la PC-A.

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



### Step 20: cambiar el pool de DHCPv6 en el R1.

- Agregue el prefijo de red al pool.  

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```
- Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.

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

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

- Verifique la configuración del pool de DHCPv6.  

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (0 in use, 0 conflicts)
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
```
- Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

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

### Step 21: establecer el indicador en G0/1 para DHCPv6 con estado.

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

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

**Step 22: habilitar la interfaz F0/6 en el S1.**

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

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

**Step 23: verificar la configuración de DHCPv6 con estado en el R1.**

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

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

- b. En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.
- c. Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
```

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

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

Domain name: ccna-StatefulDHCPv6.com

Active clients: 1

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

R1# **show ipv6 dhcp binding**

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

DUID: 0001000117F6723D000C298D5444

Username : unassigned

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

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

preferred lifetime 86400, valid lifetime 172800

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

```

Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión. . . : ccna-StatefulDHCPv6.com
  Descripción . . . . . : Conexión de red Intel(R) PRO/1000
  MT
  Dirección física. . . . . : 00-0C-29-E3-23-17
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Dirección IPv6 . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce<Preferido>
  Concesión obtenida. . . . . : jueves, 05 de septiembre de 2013
  16:07:59
  La concesión expira . . . . . : jueves, 05 de septiembre de 2013
  16:38:03
  Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
  Vínculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a%11<Preferido>
  Dirección IPv4. . . . . : 192.168.96.139<Preferido>
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : fe80::1%11
  IAID DHCPv6 . . . . . : 234884137
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-E3-23-17
  Servidores DNS . . . . . : 2001:db8:acad:a::abcd
  NetBIOS sobre TCP/IP. . . . . : habilitado

```

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

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

R1# **u all**

Se ha desactivado toda depuración posible

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

\*Mar 5 16:42:39.779: 00030001FC994775C3E0

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

\*Mar 5 16:42:39.779: 00010001

R1#17F6723D000C298D5444

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

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

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

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

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

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

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

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

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

#### Step 24: verificar DHCPv6 con estado en la PC-A.

- a. Detenga la captura de Wireshark en la PC-A.
- b. Expanda el mensaje RA más reciente que se indica en Wireshark. Verifique que se haya establecido el indicador **Managed address configuration** (Configuración de dirección administrada).

| No. | Time       | Source  | Destination | Protocol | Length | Info  |
|-----|------------|---------|-------------|----------|--------|---|
| 36  | 54.582255  | Fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from fc:99:47:75:c3:e1 |
| 265 | 215.309226 | Fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from fc:99:47:75:c3:e1 |
| 425 | 373.272435 | Fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from fc:99:47:75:c3:e1 |
| 553 | 554.893786 | Fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from fc:99:47:75:c3:e1 |
| 664 | 730.139576 | Fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from fc:99:47:75:c3:e1 |
| 775 | 922.720109 | Fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from fc:99:47:75:c3:e1 |

|   |  |  |  |  |  |  |
|---|--|--|--|--|--|--|
| <b>Frame 775: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)</b>                           |  |  |  |  |  |  |
| Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), 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: 0x3a82 [correct]  |  |  |  |  |  |  |
| Cur hop limit: 64   |  |  |  |  |  |  |
| Flags: 0xc0   |  |  |  |  |  |  |
| 1... .. = Managed address configuration: Set  |  |  |  |  |  |  |
| ..1... .. = Other configuration: Set  |  |  |  |  |  |  |
| ..0... .. = Home Agent: Not set   |  |  |  |  |  |  |
| ...0 0... = Prf (Default Router Preference): Medium (0)   |  |  |  |  |  |  |
| .... 0... = Proxy: Not set  |  |  |  |  |  |  |
| .... ..0 = Reserved: 0  |  |  |  |  |  |  |
| Router lifetime (<): 1800   |  |  |  |  |  |  |

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

| No. | Time       | Source                       | Destination                  | Protocol | Length | Info   |
|-----|------------|------------------------------|------------------------------|----------|--------|--|
| 250 | 443.078236 | fe80::d428:7de2:997ff02::1:2 | ff02::1:2                    | DHCPv6   | 146    | Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2   |
| 267 | 475.083284 | fe80::d428:7de2:997ff02::1:2 | ff02::1:2                    | DHCPv6   | 146    | Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2   |
| 425 | 656.281211 | fe80::d428:7de2:997ff02::1:2 | ff02::1:2                    | DHCPv6   | 146    | Solicit XID: 0xc86c32 CID: 0001000117f6723d000c2   |
| 429 | 656.282249 | fe80::1                      | fe80::d428:7de2:997ff02::1:2 | DHCPv6   | 191    | Advertise XID: 0xc86c32 CID: 0001000117f6723d000c2 |
| 460 | 657.292018 | fe80::d428:7de2:997ff02::1:2 | ff02::1:2                    | DHCPv6   | 188    | Request XID: 0xc86c32 CID: 0001000117f6723d000c2   |
| 462 | 657.292638 | fe80::1                      | fe80::d428:7de2:997ff02::1:2 | DHCPv6   | 191    | Reply XID: 0xc86c32 CID: 0001000117f6723d000c298   |

|   |  |  |  |  |  |  |
|---|--|--|--|--|--|--|
| 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: 0e000c290000a8c000010e000005001820010db8acad00a...   |  |  |  |  |  |  |
| 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: 20010db8acad00a00000000000abcd   |  |  |  |  |  |  |
| 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

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

DHCPv6 con estado utiliza más recursos de memoria. Las respuestas varían, pero DHCPv6 con estado requiere que el router almacene la información de estado

dinámico de los clientes DHCPv6. Los clientes DHCPv6 sin estado no utilizan el servidor de DHCP para obtener información de dirección, de modo que no es necesario almacenarla.

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

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

### Tabla de resumen de interfaces del router

| Resumen de interfaces del router |                             |                             |                       |                       |
|----------------------------------|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de router                 | Interfaz Ethernet #1        | Interfaz Ethernet n.º 2     | Interfaz serial #1    | Interfaz serial n.º 2 |
| 1800                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

**Nota:** para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

#### 10.3.1.1 IoE and DHCP Instructions

## IdT y DHCP

### Objetivo

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

### Situación

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

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



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

- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.

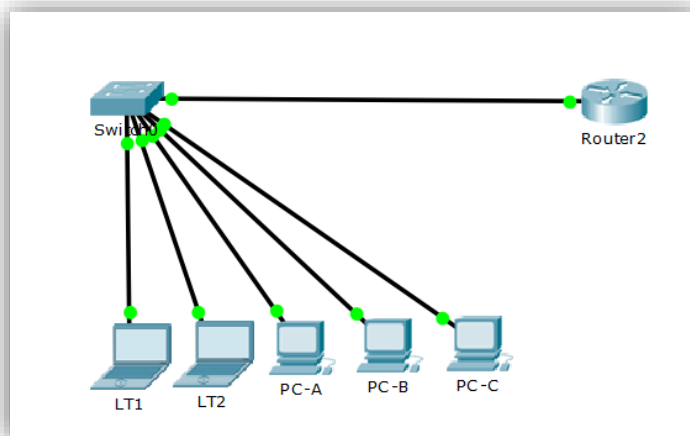
```
Router>en
Router#conf te
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no sh

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

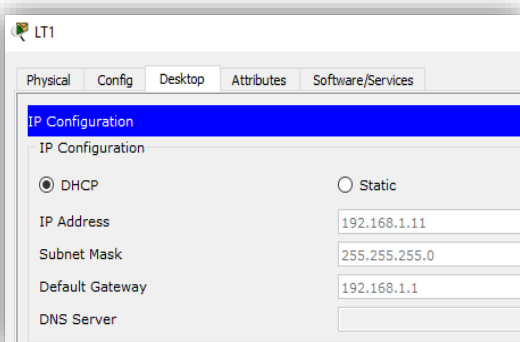
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
Router(config)#ip dhcp pool lan
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#exit
Router(config)#end
Router#
```

- 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**.



LT1

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

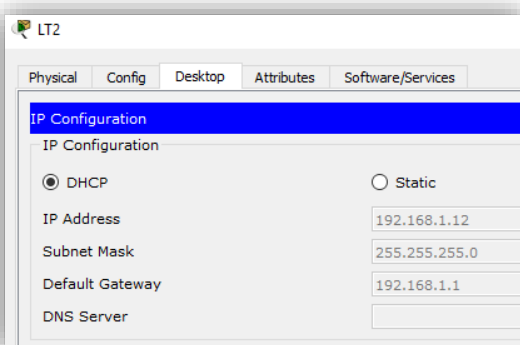
DHCP  Static

IP Address 192.168.1.11

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server



LT2

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

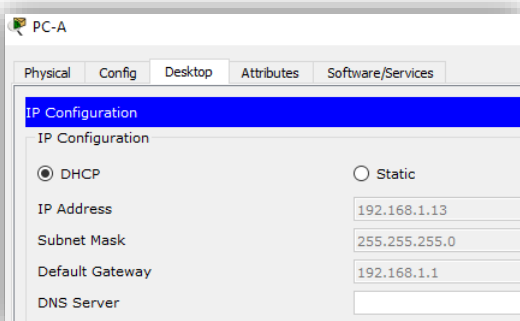
DHCP  Static

IP Address 192.168.1.12

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server



PC-A

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

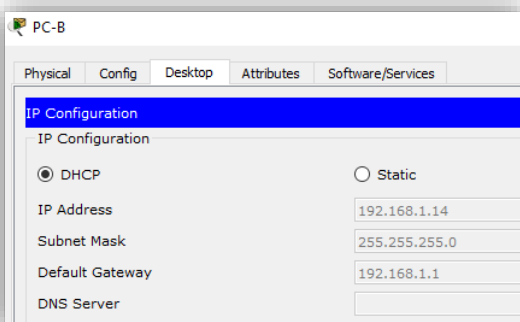
DHCP  Static

IP Address 192.168.1.13

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server



PC-B

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

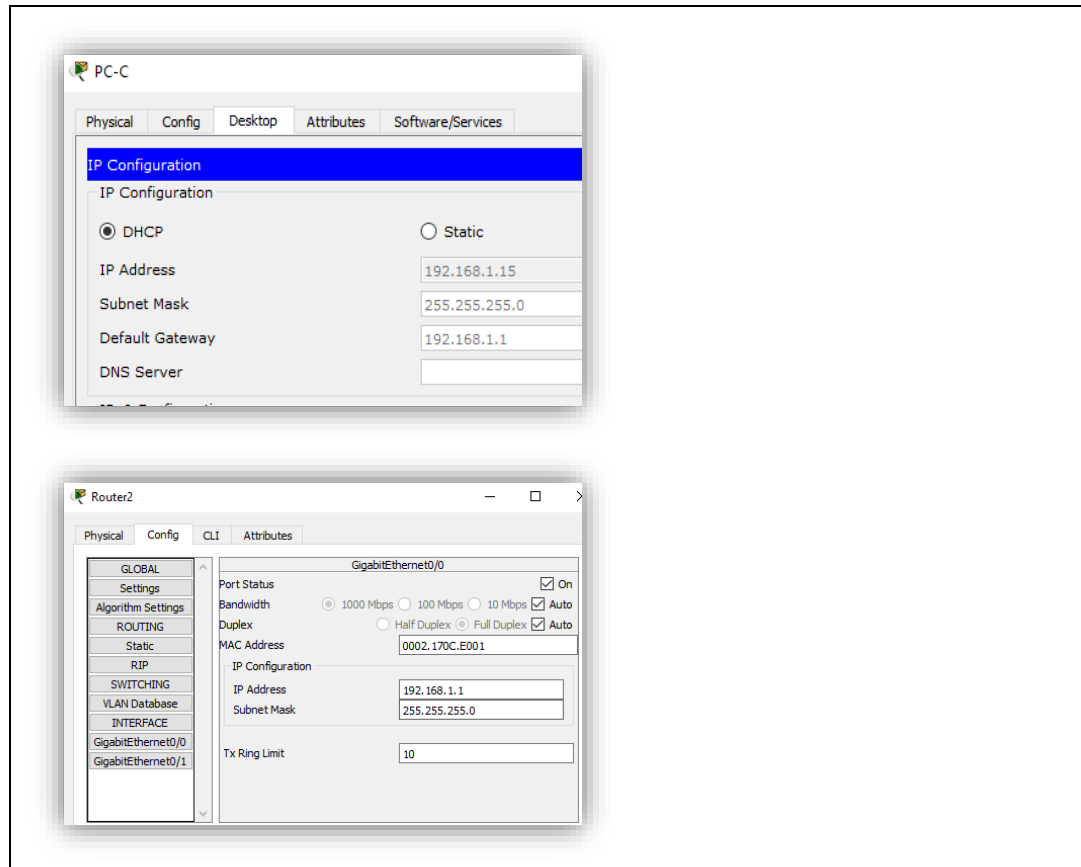
DHCP  Static

IP Address 192.168.1.14

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server



## Recursos necesarios

Software de Packet Tracer

## Reflexión

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

El router 1941 es fácil de configurar para enrutamiento con DHCP y su costo es bajo, comparado con los ISR. Estos últimos tienen muchas más funcionalidades que quizá las pequeñas empresas no necesitarán, esto es un punto importante para tomar como opción el 1941.

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.

IPv6 permite más direccionamiento, por lo tanto, más dispositivos finales, pero con una configuración similar en el enrutador.

IPv6 es generalmente dinámico, por lo que configurarlo una vez en el enrutador evita que los técnicos de red tengan que configurar cada dispositivo.

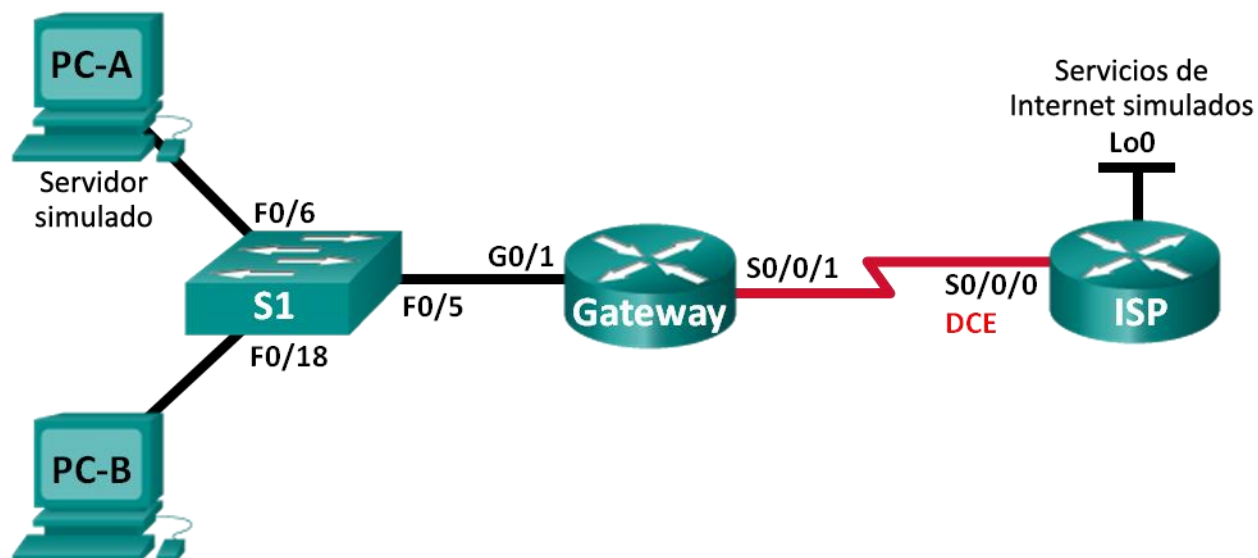
IPv6 se puede configurar con seguridad mejorada en comparación con IPv4 y permite a los administradores de red controlar mejor los recursos y la conectividad de red / dispositivo y el acceso a los recursos.

Permite a las empresas soportar múltiples tipos de dispositivos, como teléfonos IP y portátiles.

Permite a los administradores de red configurar algunos dispositivos para facilitar el acceso remoto.

## 11.2.2.6 Lab - Configuring Dynamic and Static NAT

### Topología



### Tabla de direccionamiento

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

### Objetivos

**Parte 1: armar la red y verificar la conectividad**

**Parte 2: configurar y verificar la NAT estática**

**Parte 3: configurar y verificar la NAT dinámica**

### Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red

privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

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

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

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

## Recursos necesarios

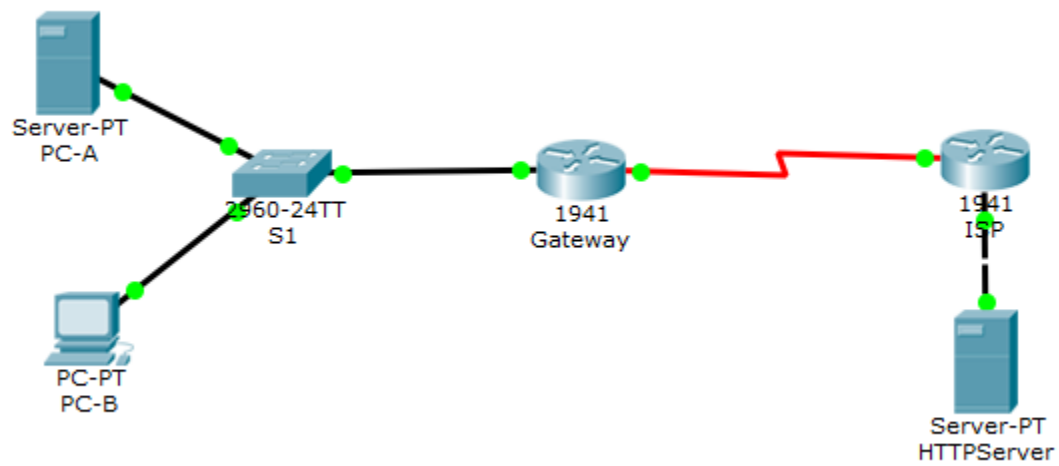
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

## 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.

### Step 25: realizar el cableado de red tal como se muestra en la topología.

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



### Step 26: configurar los equipos host.

PC-B

Physical Config Desktop Attributes Software/Services

IP Configuration

IP Configuration

DHCP  Static

IP Address: 192.168.1.21

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server:

IPv6 Configuration

DHCP  Auto Config  Static

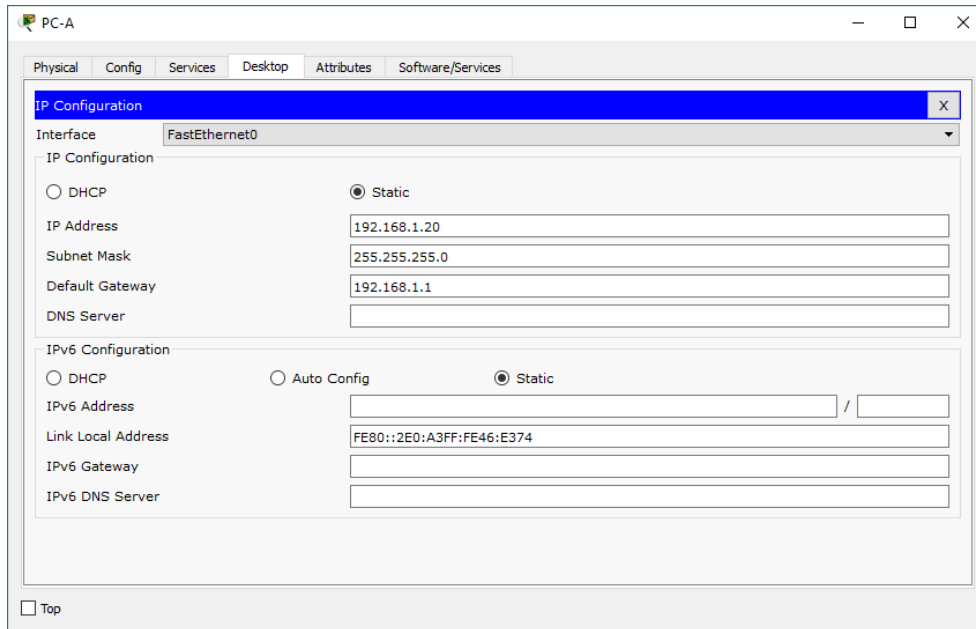
IPv6 Address: /

Link Local Address: FE80::201:64FF:FE48:CC4E

IPv6 Gateway:

IPv6 DNS Server:

Top



**Step 27: inicializar y volver a cargar los routers y los switches según sea necesario.**

**Step 28: 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.



```
Router>en
Router#conf te
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#int g0/1
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

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

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

Router(config-if)#int s0/0/1
Router(config-if)#ip add 209.165.201.18 255.255.255.252
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#exit
Router(config)#hostname Gateway
Gateway(config)#line console 0
Gateway(config-line)#pass cisco
Gateway(config-line)#login
Gateway(config-line)#logging synchronous
Gateway(config-line)#line vty 0 15
Gateway(config-line)#pass cisco
Gateway(config-line)#login
Gateway(config-line)#exit
Gateway(config)#enable secret class
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console
```

```

Router>en
Router#conf
Configuring from terminal, memory, or network [terminal]? te
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#int s0/0/0
Router(config-if)#ip add 209.165.201.17 255.255.255.252
Router(config-if)#clock rate 128000
Router(config-if)#no shutdown

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

Router(config-if)#int g0/0
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router(config-if)#int g0/0
Router(config-if)#ip add 192.31.7.1 255.255.255.255
Bad mask /32 for address 192.31.7.1
Router(config-if)#ip add 192.31.7.1 255.255.255.0
Router(config-if)#exit
Router(config)#hostname ISP
ISP(config)#line console 0
ISP(config-line)#
ISP(config-line)#pass cisco
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#line vty 0 15
ISP(config-line)#pass cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#enable secret class
ISP(config)#exit
ISP#
%SYS-5-CONFIG_I: Configured from console by console

```

### Step 29: crear un servidor web simulado en el ISP.

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

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

- Habilite el servicio del servidor HTTP en el ISP.

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

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

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

**Packet tracer no soporta estos comandos**

### Step 30: configurar el routing estático.

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

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

```
ISP#
ISP#conf te
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 209.165.200.224 255.255.255.224
209.165.201.18
```

- 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
```

```
Password:
```

```
Gateway>en
Password:
Gateway#conf te
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

### Step 31: Guardar la configuración en ejecución en la configuración de inicio.

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

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

### Step 32: Verificar la conectividad de la red

- a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

PC-B

Physical Config Desktop Attributes Software/Services

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:\>
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|

```

Recorte de ventana

Top

PC-A

Physical Config Services Desktop Attributes Software/Services

Command Prompt

```

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

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

Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|

```

Top

- 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.

```

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

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1
L      192.168.1.1/32 is directly connected, GigabitEthernet0/1
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.201.16/30 is directly connected, Serial0/0/1
L      209.165.201.18/32 is directly connected, Serial0/0/1
S*    0.0.0.0/0 [1/0] via 209.165.201.17

```

Gateway#

---

```

ISP#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

      192.31.7.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.31.7.0/24 is directly connected, GigabitEthernet0/0
L      192.31.7.1/32 is directly connected, GigabitEthernet0/0
      209.165.200.0/27 is subnetted, 1 subnets
S      209.165.200.224/27 [1/0] via 209.165.201.18
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.201.16/30 is directly connected, Serial0/0/0
L      209.165.201.17/32 is directly connected, Serial0/0/0

```

ISP#

## 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.

### Step 33: configurar una asignación estática.

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20
209.165.200.225
```

```
Gateway#conf te
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip nat inside source static 192.168.1.20 209.165.200.225
```

### Step 34: Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

```
Gateway(config)#interface g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface s0/0/0
Gateway(config-if)#ip nat outside
```

### Step 35: probar la configuración.

- Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside
global
--- 209.165.200.225    192.168.1.20     ---                ---

Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.200.225    192.168.1.20     ---                ---
```

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

192.168.1.20 = 209.165.200.225

¿Quién asigna la dirección global interna?

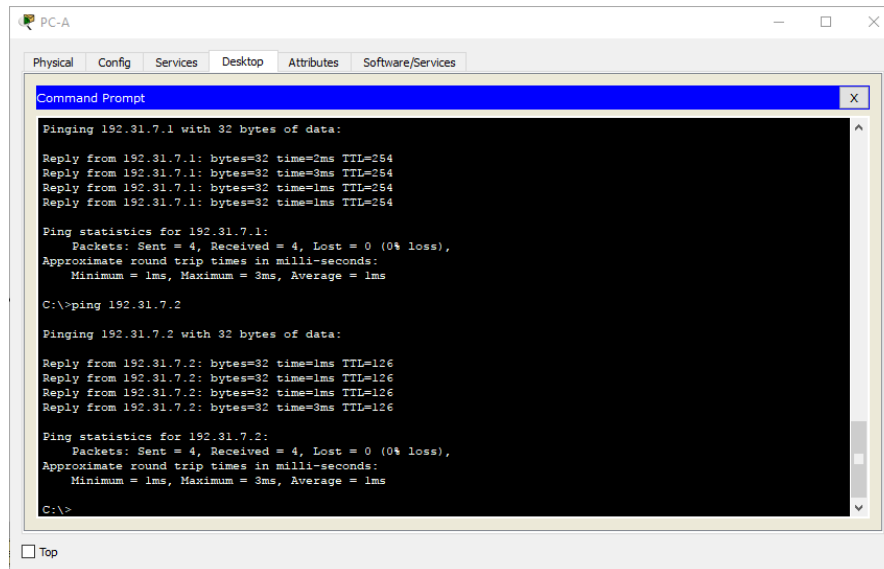
Es asignada por el Router desde el pool de NAT.

¿Quién asigna la dirección local interna?

Es asignada por el administrador de red.

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

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



```
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:28 192.168.1.20:28  192.31.7.2:28     192.31.7.2:28
icmp 209.165.200.225:29 192.168.1.20:29  192.31.7.2:29     192.31.7.2:29
icmp 209.165.200.225:30 192.168.1.20:30  192.31.7.2:30     192.31.7.2:30
icmp 209.165.200.225:31 192.168.1.20:31  192.31.7.1:31     192.31.7.1:31
icmp 209.165.200.225:32 192.168.1.20:32  192.31.7.1:32     192.31.7.1:32
icmp 209.165.200.225:33 192.168.1.20:33  192.31.7.1:33     192.31.7.1:33
icmp 209.165.200.225:34 192.168.1.20:34  192.31.7.1:34     192.31.7.1:34
icmp 209.165.200.225:35 192.168.1.20:35  192.31.7.1:35     192.31.7.1:35
icmp 209.165.200.225:36 192.168.1.20:36  192.31.7.1:36     192.31.7.1:36
icmp 209.165.200.225:37 192.168.1.20:37  192.31.7.1:37     192.31.7.1:37
icmp 209.165.200.225:38 192.168.1.20:38  192.31.7.1:38     192.31.7.1:38
icmp 209.165.200.225:39 192.168.1.20:39  192.31.7.2:39     192.31.7.2:39
icmp 209.165.200.225:40 192.168.1.20:40  192.31.7.2:40     192.31.7.2:40
icmp 209.165.200.225:41 192.168.1.20:41  192.31.7.2:41     192.31.7.2:41
icmp 209.165.200.225:42 192.168.1.20:42  192.31.7.2:42     192.31.7.2:42
--- 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?

**Utilizó los puertos 28 al 42**

**Nota:** puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

- c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

| Pro  | Inside global        | Inside local      | Outside local | Outside global |
|------|----------------------|-------------------|---------------|----------------|
| icmp | 209.165.200.225:1    | 192.168.1.20:1    | 192.31.7.1:1  |                |
| tcp  | 209.165.200.225:1034 | 192.168.1.20:1034 | 192.31.7.1:23 |                |
| ---  | 209.165.200.225      | 192.168.1.20      | ---           | ---            |

```
C:\>telnet 192.31.7.1
Trying 192.31.7.1 ...Open

User Access Verification

Password:
ISP>exit

[Connection to 192.31.7.1 closed by foreign host]
C:\>
```

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

Gateway#
```

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

¿Qué protocolo se usó para esta traducción? **TCP**

¿Cuáles son los números de puerto que se usaron?

Global/local interno: **Global 1025, Local 23**

Global/local externo: **Global 1025, Local 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.

```
Packet Tracer SERVER Command Line 1.0
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=3ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126
Reply from 209.165.200.225: bytes=32 time=12ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms
```



- e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

```
Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside
global
icmp 209.165.200.225:12 192.168.1.20:12  209.165.201.17:12
209.165.201.17:12
--- 209.165.200.225    192.168.1.20      ---                ---

Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:5 192.168.1.20:5   192.31.7.2:5      192.31.7.2:5
icmp 209.165.200.225:6 192.168.1.20:6   192.31.7.2:6      192.31.7.2:6
icmp 209.165.200.225:7 192.168.1.20:7   192.31.7.2:7      192.31.7.2:7
icmp 209.165.200.225:8 192.168.1.20:8   192.31.7.2:8      192.31.7.2:8
--- 209.165.200.225    192.168.1.20      ---                ---
tcp 209.165.200.225:1025 192.168.1.20:1025 192.31.7.1:23     192.31.7.1:23
```

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

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

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

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

Gateway#show ip nat st
Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 72 Misses: 34
Expired translations: 33
Dynamic mappings:
```

**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.

#### Step 36: borrar las NAT.

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

#### Step 37: definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

#### Step 38: verificar que la configuración de interfaces NAT siga siendo válida.

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

```
Gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 72 Misses: 34
Expired translations: 33
Dynamic mappings:
```

#### Step 39: definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.242
209.165.200.254 netmask 255.255.255.224
```

#### Step 40: definir la NAT desde la lista de origen interna hasta el conjunto externo.

**Nota:** recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

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

#### Step 41: probar la configuración.

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

```
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Gateway# **show ip nat translations**

| Pro    | Inside global     | Inside local   | Outside local | Outside      |
|--------|-------------------|----------------|---------------|--------------|
| global |                   |                |               |              |
| ---    | 209.165.200.225   | 192.168.1.20   | ---           | ---          |
| icmp   | 209.165.200.242:1 | 192.168.1.21:1 | 192.31.7.1:1  | 192.31.7.1:1 |
| ---    | 209.165.200.242   | 192.168.1.21   | ---           | ---          |

Gateway#**show ip nat translations**

| Pro  | Inside global     | Inside local   | Outside local | Outside global |
|------|-------------------|----------------|---------------|----------------|
| icmp | 209.165.200.242:1 | 192.168.1.21:1 | 192.31.7.1:1  | 192.31.7.1:1   |
| icmp | 209.165.200.242:2 | 192.168.1.21:2 | 192.31.7.1:2  | 192.31.7.1:2   |
| icmp | 209.165.200.242:3 | 192.168.1.21:3 | 192.31.7.1:3  | 192.31.7.1:3   |
| icmp | 209.165.200.242:4 | 192.168.1.21:4 | 192.31.7.1:4  | 192.31.7.1:4   |
| ---  | 209.165.200.225   | 192.168.1.20   | ---           | ---            |

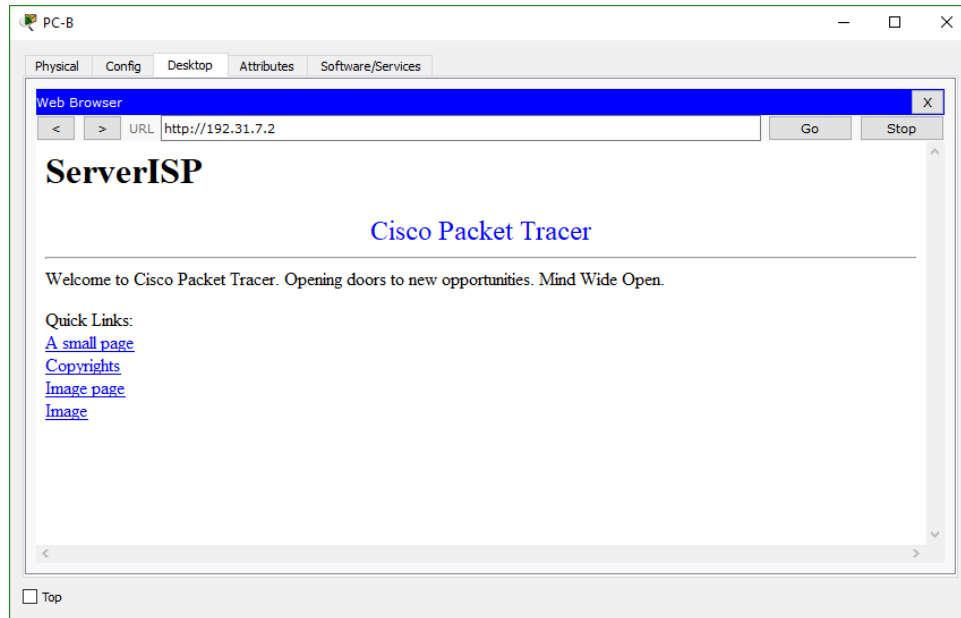
¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = **209.165.200.242**

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? **Los puertos 1 al 4**

- b. En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.



c. Muestre la tabla de NAT.

| Pro           | Inside global        | Inside local      | Outside local | Outside |
|---------------|----------------------|-------------------|---------------|---------|
| ---           | 209.165.200.225      | 192.168.1.20      | ---           | ---     |
| tcp           | 209.165.200.242:1038 | 192.168.1.21:1038 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1039 | 192.168.1.21:1039 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1040 | 192.168.1.21:1040 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1041 | 192.168.1.21:1041 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1042 | 192.168.1.21:1042 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1043 | 192.168.1.21:1043 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1044 | 192.168.1.21:1044 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1045 | 192.168.1.21:1045 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1046 | 192.168.1.21:1046 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1047 | 192.168.1.21:1047 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1048 | 192.168.1.21:1048 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1049 | 192.168.1.21:1049 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1050 | 192.168.1.21:1050 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |
| tcp           | 209.165.200.242:1051 | 192.168.1.21:1051 | 192.31.7.1:80 |         |
| 192.31.7.1:80 |                      |                   |               |         |

```
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80
192.31.7.1:80
```

```
--- 209.165.200.242 192.168.1.22 ---
```

The screenshot shows a Gateway router CLI window with the following content:

```

Gateway
Physical Config CLI Attributes
IOS Command Line Interface
Gateway#show ip nat traslat
Gateway#show ip
Gateway#show ip nat traslations
^
% Invalid input detected at '^' marker.

Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225    192.168.1.20      ---
tcp 209.165.200.242:1026 192.168.1.21:1026 192.31.7.254:80    192.31.7.254:80
tcp 209.165.200.242:1027 192.168.1.21:1027 192.31.7.254:80    192.31.7.254:80
tcp 209.165.200.242:1028 192.168.1.21:1028 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1029 192.168.1.21:1029 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1030 192.168.1.21:1030 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1031 192.168.1.21:1031 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1032 192.168.1.21:1032 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1033 192.168.1.21:1033 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1034 192.168.1.21:1034 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1035 192.168.1.21:1035 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1036 192.168.1.21:1036 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1037 192.168.1.21:1037 192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.2:80      192.31.7.2:80
Gateway#
Copy Paste
 Top

```

¿Qué protocolo se usó en esta traducción? **TCP**

¿Qué números de puerto se usaron?

Interno: **desde el 1026 al 1038**

Externo: 80

¿Qué número de puerto bien conocido y qué servicio se usaron? **El puerto 80 y se usó para acceder al servidor desde la web.**

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

```
Gateway# show ip nat statistics
```

```
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
```

```
Peak translations: 17, occurred 00:06:40 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```

```
GigabitEthernet0/1
```

```
Hits: 345 Misses: 0
```

```
CEF Translated packets: 345, CEF Punted packets: 0
```

```
Expired translations: 20
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 1] access-list 1 pool public_access refcount 2
```

```
pool public_access: netmask 255.255.255.224
```

```
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13, allocated 1 (7%), misses 0
```

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

```
Gateway#show ip nat statistics
Total translations: 14 (1 static, 13 dynamic, 13 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 266 Misses: 52
Expired translations: 38
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 13
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 1 (7%), misses 0
```

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

#### Step 42: eliminar la entrada de NAT estática.

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

- Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

```
Gateway(config)# no ip nat inside source static 192.168.1.20
209.165.200.225
Static entry in use, do you want to delete child entries? [no]:
yes
```

- Borre las NAT y las estadísticas.
- Haga ping al ISP (192.31.7.1) desde ambos hosts.

```
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

- d. Muestre la tabla y las estadísticas de NAT.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16 Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13, allocated 2 (15%), misses 0

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

Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 274 Misses: 60
Expired translations: 46
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13 , allocated 0 (0%),
misses 0
```

```

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

```

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

## Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

El uso de IP NAT nos permite optimizar el uso de direcciones IP públicas en una red, como bien sabemos, estas son limitadas.

2. ¿Cuáles son las limitaciones de NAT?

Se deteriora el rendimiento.

Se deteriora la funcionalidad de extremo a extremo.

Se reduce el seguimiento IP de extremo a extremo.

El tunneling se torna más complicado.

El inicio de las conexiones TCP puede interrumpirse.



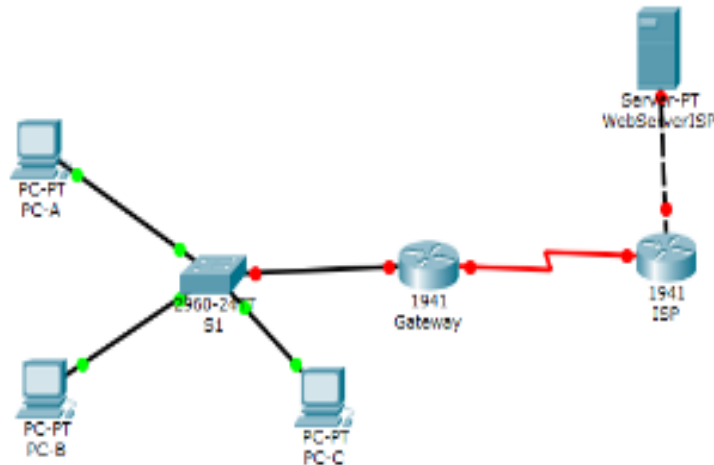
**Tabla de resumen de interfaces del router**

| Resumen de interfaces del router |                             |                             |                       |                       |
|----------------------------------|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de router                 | Interfaz Ethernet #1        | Interfaz Ethernet n.º 2     | Interfaz serial #1    | Interfaz serial n.º 2 |
| 1800                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811                             | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900                             | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

**Nota:** para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

### 11.2.3.7 Lab - Configuring NAT Pool Overload and PAT

#### Topología



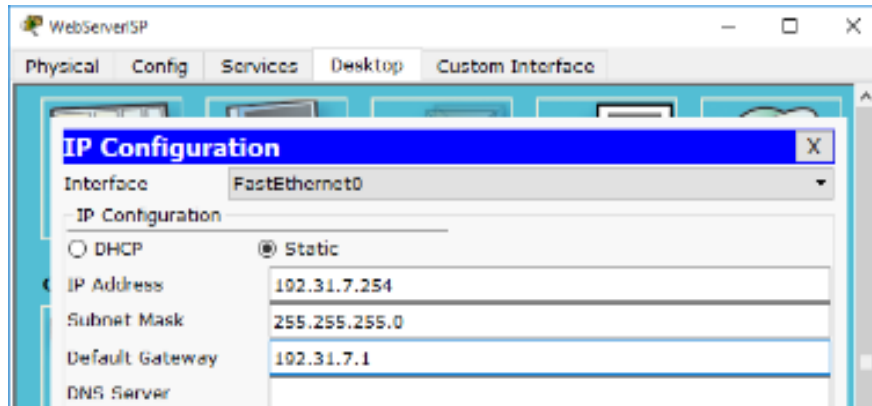
**Nota:** para simular los servicios de internet en PKT, se coloca un servidor web.

#### Tabla de direccionamiento

| Dispositivo | Interfaz     | Dirección IP   | Máscara de subred | Gateway predeterminado |
|-------------|--------------|----------------|-------------------|------------------------|
| Gateway     | G0/1         | 192.168.1.1    | 255.255.255.0     | N/A                    |
|             | S0/0/1       | 209.165.201.18 | 255.255.255.252   | N/A                    |
| ISP         | S0/0/0 (DCE) | 209.165.201.17 | 255.255.255.252   | N/A                    |
|             | Lo0          | 192.31.7.1     | 255.255.255.255   | N/A                    |
| PC-A        | NIC          | 192.168.1.20   | 255.255.255.0     | 192.168.1.1            |
| PC-B        | NIC          | 192.168.1.21   | 255.255.255.0     | 192.168.1.1            |
| PC-C        | NIC          | 192.168.1.22   | 255.255.255.0     | 192.168.1.1            |

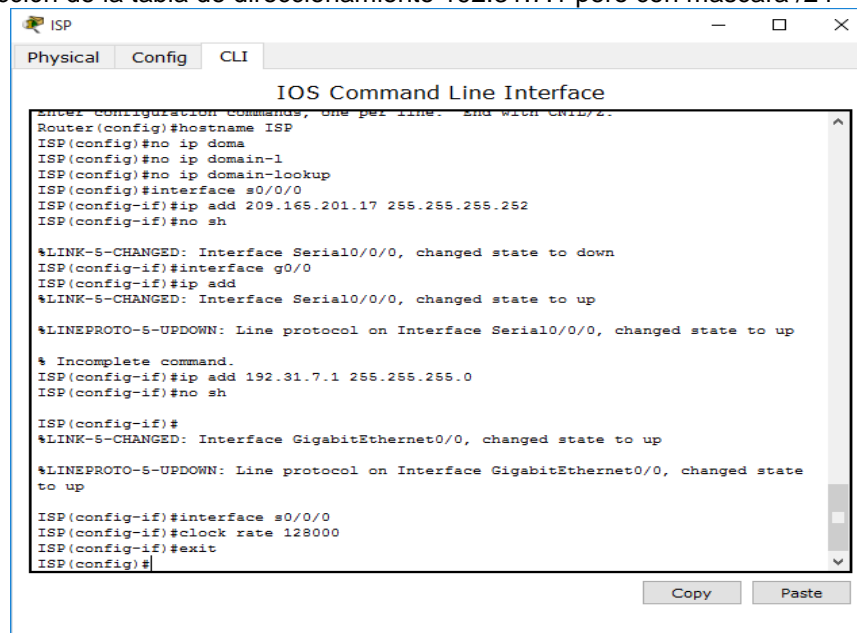
#### Parte 1: Armar la red y verificar la conectividad

Se configuran los host PC-A, PC-B y PC-C de acuerdo a las direcciones de la tabla de direccionamiento, se configura nuestro web server, colocándole una dirección IP que este dentro de la red especificada por la tabla de direccionamiento para el ISP.

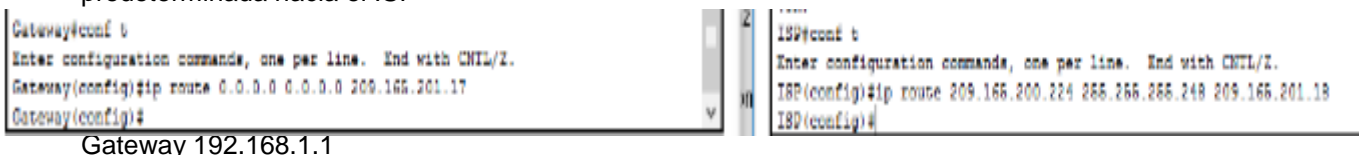


Se configuran los router de acuerdo a las especificaciones.

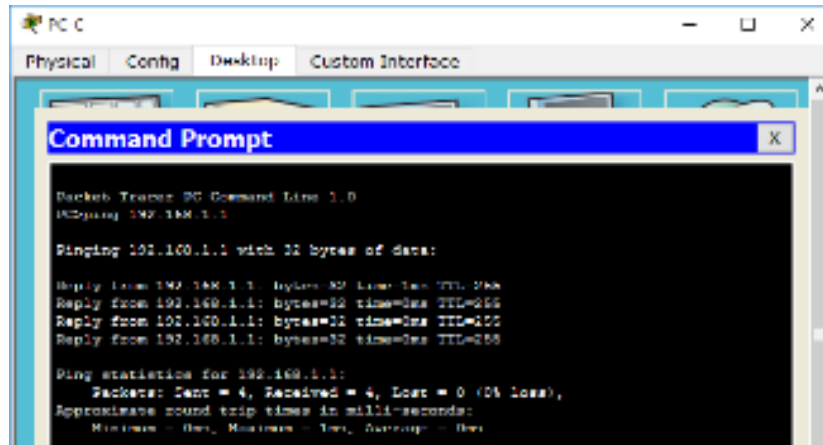
Para ISP se realizan los ajustes de la interface serial s0/0/0 y el clockrate 128000, y en lugar de usar la interface loopback se utiliza la G0/0, para conectar a los servicios de internet, con la misma dirección de la tabla de direccionamiento 192.31.7.1 pero con mascara /24



Se configura el routing estático en ISP para crear la ruta, como en Gateway para la ruta predeterminada hacia el ISP

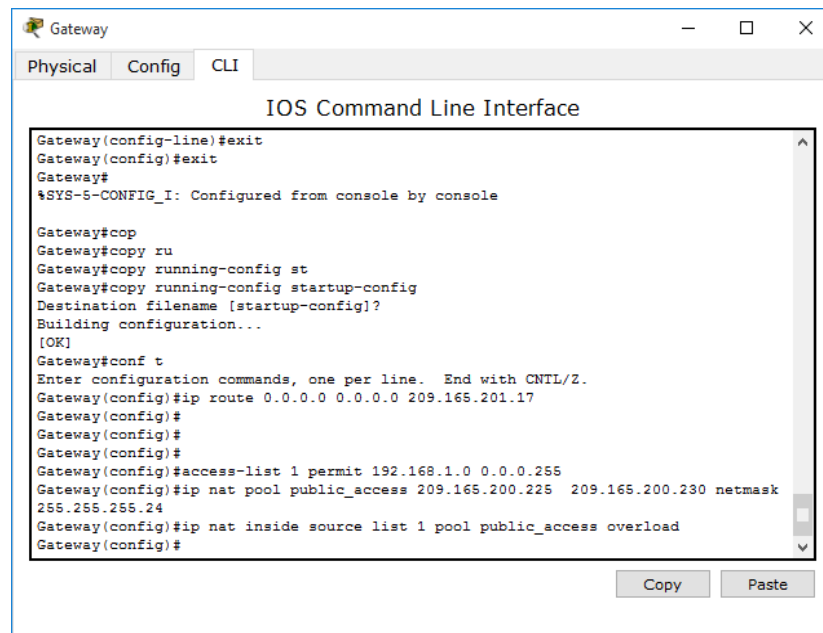


Gateway 192.168.1.1



## Parte 2: Configurar y verificar el conjunto de NAT con sobrecarga

Se configura en Gateway una ACL que permita traducir la red 192.168.1.0/24 y se configuran las direcciones que podrán ser utilizadas, creando el pool y definiendo la NAT desde origen hacia el externo



Para el mismo router se configuran las interfaces que tiene en funcionamiento como inside y outside.

```
Gateway(config)#
Gateway(config)#int g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface s0/0/1
Gateway(config-if)#ip nat outside
Gateway(config-if)#
```

Se verifican las configuraciones del NAT por medio del comando ping, desde los hosts hacia la dirección 192.31.7.1 del ISP

```

PC>ping 192.81.7.1

Pinging 192.81.7.1 with 32 bytes of data:

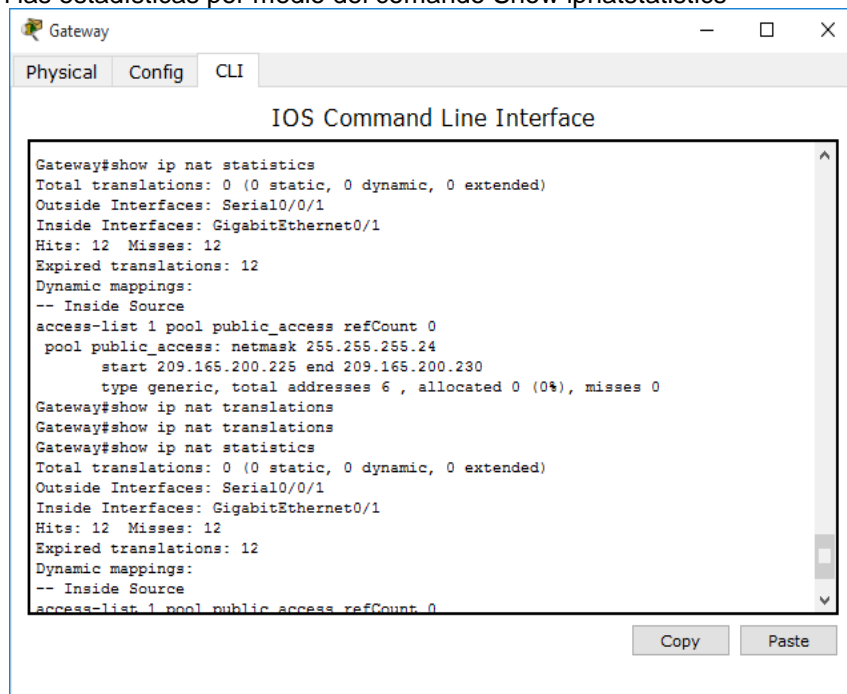
Reply from 192.81.7.1: bytes=32 time=1ms TTL=254
Reply from 192.81.7.1: bytes=32 time=1ms TTL=254
Reply from 192.81.7.1: bytes=32 time=1ms TTL=254
Reply from 192.81.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.81.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>

```

Se muestran las estadísticas por medio del comando Show ipnatstatistics



```

Gateway
Physical Config CLI
IOS Command Line Interface

Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12 Misses: 12
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
pool public_access: netmask 255.255.255.24
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#show ip nat translations
Gateway#show ip nat translations
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12 Misses: 12
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0

```

Por medio del comando show ipnattranslations, se muestran la direcciones NAT del router

The screenshot shows a Gateway router CLI window with the following content:

```

Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 12
pool public_access: netmask 255.255.255.24
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6 , allocated 1 (16%), misses 0
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:1024 192.168.1.21:13  192.31.7.1:13     192.31.7.1:1024
icmp 209.165.200.225:1025 192.168.1.21:14  192.31.7.1:14     192.31.7.1:1025
icmp 209.165.200.225:1026 192.168.1.21:15  192.31.7.1:15     192.31.7.1:1026
icmp 209.165.200.225:1027 192.168.1.21:16  192.31.7.1:16     192.31.7.1:1027
icmp 209.165.200.225:131 192.168.1.22:13  192.31.7.1:13     192.31.7.1:13
icmp 209.165.200.225:141 192.168.1.22:14  192.31.7.1:14     192.31.7.1:14
icmp 209.165.200.225:151 192.168.1.22:15  192.31.7.1:15     192.31.7.1:15
icmp 209.165.200.225:161 192.168.1.22:16  192.31.7.1:16     192.31.7.1:16
icmp 209.165.200.225:171 192.168.1.20:17  192.31.7.1:17     192.31.7.1:17
icmp 209.165.200.225:181 192.168.1.20:18  192.31.7.1:18     192.31.7.1:18
icmp 209.165.200.225:191 192.168.1.20:19  192.31.7.1:19     192.31.7.1:19
icmp 209.165.200.225:201 192.168.1.20:20  192.31.7.1:20     192.31.7.1:20
Gateway#

```

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior?  
**Tres, 192.168.1.20 - 192.168.1.21 - 192.168.1.22**

¿Cuántas direcciones IP globales internas se indican?  
**Solamente una, 209.165.200.225**

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas?  
**Se usan 12 puertos.**

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A?  
 ¿Por qué?  
**El ping falla pues el router solo conoce las direcciones inside global en su tabla de ruteo, dichas direcciones no están notificadas.**

```

ISP>ping 192.168.1.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds:
-----
Success rate is 0 percent (0/5)

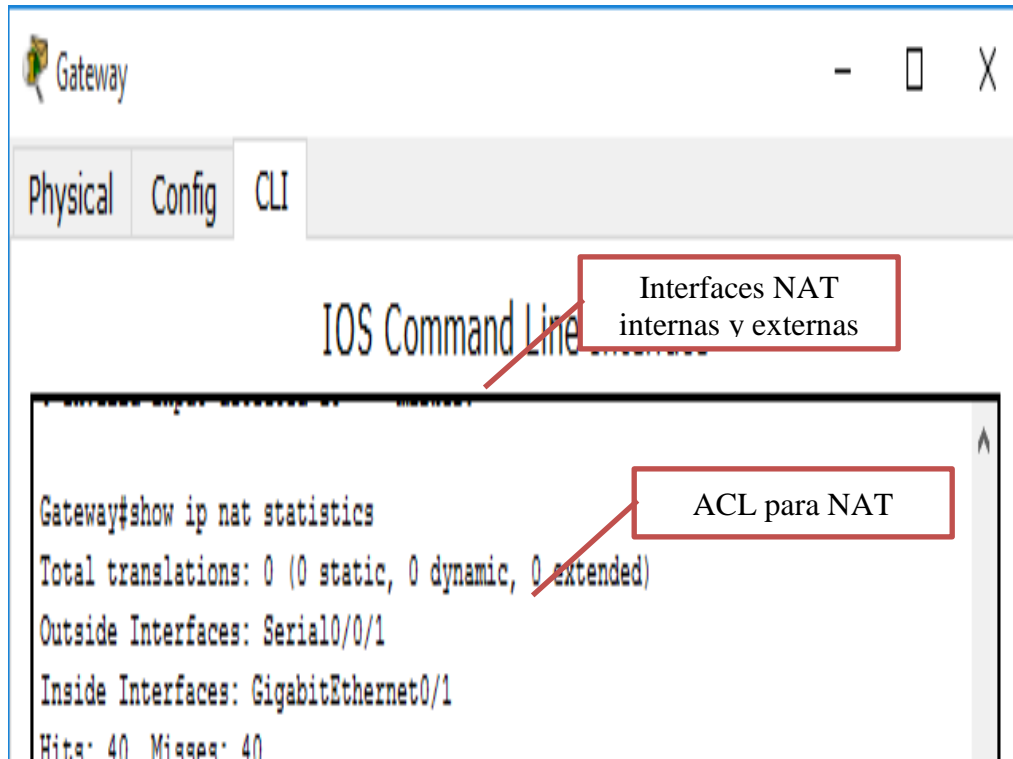
```

### Parte 3: Configurar y verificar PAT

Se deben borrar las NAT y las estadísticas dentro del router Gateway, para lograrlo se usa el comando clearipnattranslations, sin embargo, PKT no soporta este comando.

¿Qué comando usó para confirmar los resultados de los pasos a al c?

Se usa el comando show ipnatstatistics



Ahora se procede a eliminar la configuración para el conjunto de direcciones utilizables, la traducción NAT del origen interno hacia el conjunto interno, y se asocia la lista de origen a la interfaz externa

```

Gateway(config)#no ip nat inside source list 1 pool public_access overload
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 overload
  
```

Ahora se prueba la nueva configuración mostrando las estadísticas y las traducciones NAT en Gateway

The screenshot shows a Cisco Gateway CLI window with the following output:

```

Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 64 Misses: 64
Expired translations: 52
Dynamic mappings:
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.201.18:1024 192.168.1.22:21  192.31.7.1:21     192.31.7.1:1024
icmp 209.165.201.18:1025 192.168.1.22:22  192.31.7.1:22     192.31.7.1:1025
icmp 209.165.201.18:1026 192.168.1.22:23  192.31.7.1:23     192.31.7.1:1026
icmp 209.165.201.18:1027 192.168.1.22:24  192.31.7.1:24     192.31.7.1:1027
icmp 209.165.201.18:21   192.168.1.21:21  192.31.7.1:21     192.31.7.1:21
icmp 209.165.201.18:22   192.168.1.21:22  192.31.7.1:22     192.31.7.1:22
icmp 209.165.201.18:23   192.168.1.21:23  192.31.7.1:23     192.31.7.1:23
icmp 209.165.201.18:24   192.168.1.21:24  192.31.7.1:24     192.31.7.1:24
icmp 209.165.201.18:25   192.168.1.20:25  192.31.7.1:25     192.31.7.1:25
icmp 209.165.201.18:26   192.168.1.20:26  192.31.7.1:26     192.31.7.1:26
icmp 209.165.201.18:27   192.168.1.20:27  192.31.7.1:27     192.31.7.1:27
icmp 209.165.201.18:28   192.168.1.20:28  192.31.7.1:28     192.31.7.1:28
Gateway#

```

## Reflexión

¿Qué ventajas tiene la PAT?

Pat minimiza el uso de direcciones publicas necesarias para acceder a internet, de esta manera PAT al igual que NAT permite esconder las direcciones IP privadas de la red hacia la red externa

## CONCLUSIONES DEL EJERCICIO

- ✓ Al configurar el servidor web se debe tener en cuenta colocar sus direcciones dentro del mismo grupo de la red, para establecer conectividad.
- ✓ Después de cada configuración realizada también se recomienda estar verificando la conectividad por medio de ping realizados desde cualquier host al Gateway. Con ello se evita que al terminar las configuraciones de la red no se lleve una sorpresa insatisfactoria y deba iniciar todas las configuraciones anteriormente realizadas.
- ✓ Cuando se realiza ping desde el Router ISP a una de los hosts, sucede que el ping falla porque solo conoce el lugar de las direcciones ipInside global en su tabla de ruteo, pero las direcciones ipinside local no están notificadas.
- ✓ Para finalizar se recuerda que la importancia de la PAT en una red es minimizar el número de direcciones públicas necesitadas para ingresar a internet, y PAT al igual que NAT sirve para esconder las direcciones privadas hacia la red externa.
- ✓ Por medio de la configuración NAT estamos permitiéndole a una red local, comunicarse con la red externa con una sola IP publica, a través de procesos de traducción de un grupo de direcciones IP privadas a la dirección pública asignada, reduciendo de esta manera el uso de direcciones.



- ✓ Además del gran ahorro de direcciones NAT permite mejorar la seguridad de las redes, pues las terminales internas no serán visibles desde el exterior, reduciendo riesgos de ataques.
- ✓ Para configurar de manera adecuada NAT debe contar con una ACL por medio de la cual se autoricen direcciones para el tráfico.
- ✓ Al usar PAT estamos logrando minimizar el uso de direcciones IP, pues su funcionamiento al igual que NAT es traducir varias direcciones privadas de una red local, a una única dirección pública hacia la red externa, la diferencia es que PAT usa los puertos, pudiendo usar la misma IP pública a la salida, pero con diferente puerto, incrementando la usabilidad de la IP pública.

## Conclusiones

Todos los nodos de una red requieren una dirección IP única que se comunique con otros dispositivos. DHCPv4 utiliza tres métodos diferentes de asignación de direcciones: Asignación manual, asignación automática y asignación dinámica. Existen dos métodos disponibles para la configuración dinámica de las direcciones IPv6 de unidifusión global. Configuración automática de dirección sin estado (SLAAC) y Protocolo de configuración dinámica de host para IPv6 (DHCPv6 con estado). Cuando se resuelven problemas de DHCPv4 o de DHCPv6, se llevan a cabo los mismos pasos: Resolver conflictos de dirección. Verificar la conectividad física. Probar la conectividad con una dirección IP estática. Verificar la configuración de puertos del switch. Probar el funcionamiento en la misma subred o VLAN.

DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP está activo en un servidor donde se centraliza la gestión de las direcciones IP de la red. Hoy en día, muchos sistemas operativos incluyen este servicio dada su importancia.

El DHCP busca automáticamente una dirección, su objetivo principal es simplificar y administrar la red. Se necesita un servidor DHCP para distribuir la IP en los clientes automáticamente. El servidor nos proporciona una configuración que evita conflictos y evita que existan conflictos de direcciones, es decir, asigna direcciones en diferentes dispositivos y enlaces, cada uno de estos de manera que sean independientes y no causan algún conflicto de conexión entre estos. El cliente solicita al servidor y este devuelve un resultado al cliente. Existen 3 maneras de asignación: manual, automática y dinámica.

## Bibliografía

Cisco Networking Academy <https://www.netacad.com/es/>

Unidad 3 - Configuración de Sistemas de red soportados en VLANs

<http://campus06.unad.edu.co/ecbti18/mod/page/view.php?id=143>

Temática: Introducción a redes conmutadas

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>

Temática: Configuración y conceptos básicos de Switching

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

Temática: VLANs

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

Temática: Conceptos de Routing

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

Temática: Enrutamiento entre VLANs

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

Temática: Enrutamiento Estático

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>