Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD**

**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**

# DIPLOMADO DE PROFUNDIZACION CISCO

## TRABAJO COLABORATIVO 4


**CHRISTIAN LEANDRO INFANTE – 1.114.875.895**

**ANDRÉS FELIPE SALGADO – 16.867.083**

**GERMAN ANDRÉS BARRIOS – 1.143.829.298**

**ANDRÉS GUSTAVO ZAMBRANO – 1.115.077.528**

**CARLOS ALBERTO CUERVO – 1.116.250.868**


**GRUPO:**

**203092_23**

**TUTOR:**

**JOSE IGNACIO CARDONA**

**CEAD PALMIRA**

**NOVIEMBRE DE 2017**

# INTRODUCCION

Durante este proceso de aprendizaje continuado con el desarrollo del curso de CCNA2 de CISCO y como parte del trabajo colaborativo cuatro, se presenta el siguiente informe como producto de las prácticas realizadas con Packet Tracer propuestas para esta fase final. El trabajo colaborativo cuatro se han dividido en varias partes, de las cuales están desarrolladas en el presente informe, y además se profundiza en los aspectos prácticos de Cisco y de la configuración de los routers.

Cada práctica presenta los pantallazos que evidencian la realización de cada uno de los pasos sugeridos para una correcta comprensión y un correcto aprendizaje. Además al final de cada una de ellas se encuentra el pantallazo del resultado de la actividad con su respectivo puntaje.

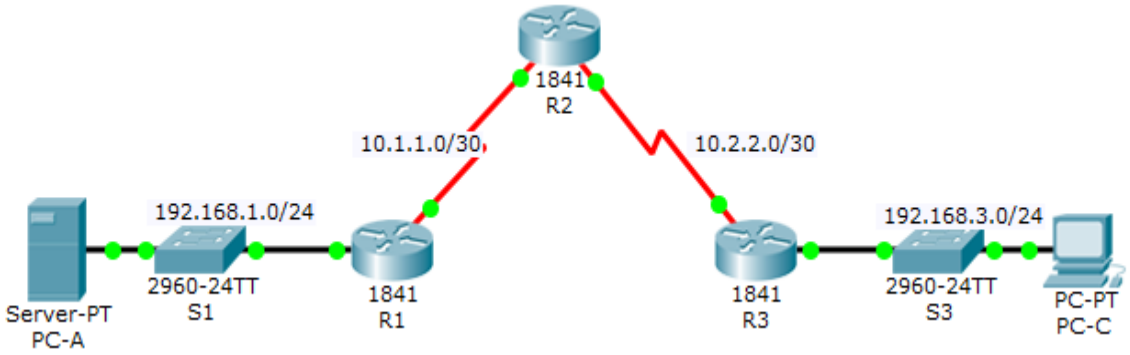
Para los miembros de este grupo colaborativo obtener la certificación CCNA Cisco es importante para una carrera profesional exitosa en IT-Networking, debido a que mejora las habilidades practicas del perfil profesional. Las empresas prefieren profesionales con conocimientos en CCNA sobre otros es porque Cisco es discutible el jugador más grande cuando viene a IT-Networking y la mayoría de las organizaciones tienen equipo de Cisco. Por lo tanto la certificación de Cisco tiene valor importante para el futuro y presente profesional.

CCNA es virtualmente una puerta de entrada al establecimiento de una red mientras que explica conceptos fundamentales claramente y es además un requisito previo para otros cursos como CCNP. Para los integrantes de este grupo

obtener esta certificación cisco ayuda indiscutidamente a fortalecer otros campos de interés en el campo practico (seguridad, centro de datos, proveedor de servicios, inalámbrico). En el campo personal y profesional permite crecer en la empresa o permite cambiar a otra empresa, y o trabajo debido a que CCNA es necesario y requerido en el campo IT.

## 4.4.1.2 PACKET TRACER: Configure IP ACLs to Mitigate Attacks

### Topología




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

### Objectives

- Verify connectivity among devices before firewall configuration.
- Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- Configure ACLs on R1 and R3 to mitigate attacks.

- Verify ACL functionality.

## Background / Scenario

Access to routers R1, R2, and R3 should only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, a server providing DNS, SMTP, FTP, and HTTPS services.
Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and/or destination IP address. In this activity, you create ACLs on edge routers R1 and R3 to achieve this goal. You then verify ACL functionality from internal and external hosts.
The routers have been pre-configured with the following:

- Enable password: ciscoenpa55
- Password for console: ciscoconpa55
- Username for VTY lines: SSHadmin
- Password for VTY lines: ciscosshpa55
- IP addressing
- Static routing

## Part 1: Verify Basic Network Connectivity

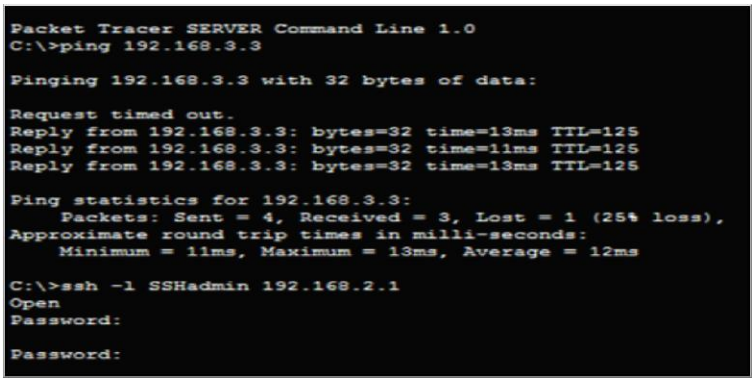
Verify network connectivity prior to configuring the IP ACLs.

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

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

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

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




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

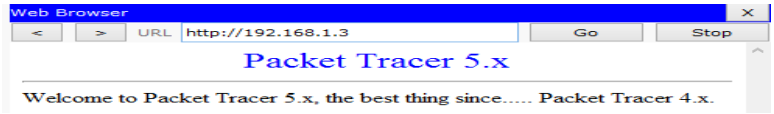
a. From the command prompt, ping PC-A (192.168.1.3).

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

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

```
Packet Tracer PC Command Line 1.0
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=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=6ms 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 = 2ms, Maximum = 6ms, Average = 3ms

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


R2#
```

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




## Part 2: Secure Access to Routers

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

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

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R1(config)#
```

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)#
```

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#
```

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

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

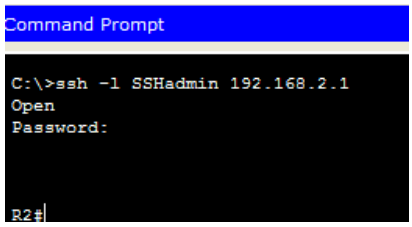
```
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#
```

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

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

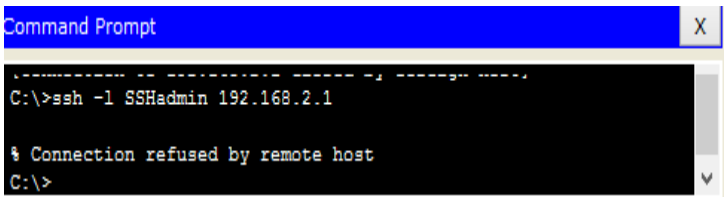
**Step 3: Verify exclusive access from management station PC-C.**

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




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

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

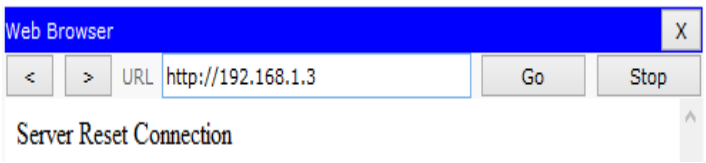



## Part 3: Create a Numbered IP ACL 120 on R1

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

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

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

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

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

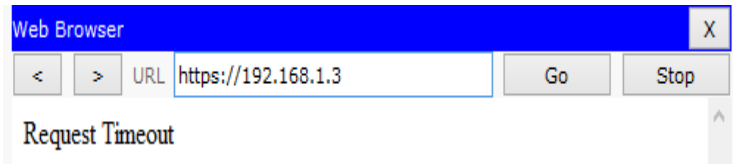
```
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit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

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

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

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

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




## Part 4: Modify An Existing ACL on R1

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

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

```
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:\>
```

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

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

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

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

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

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

C:\>
```

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

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

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

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

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

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

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

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

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#int f0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#
```

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

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

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

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

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

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

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

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

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

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

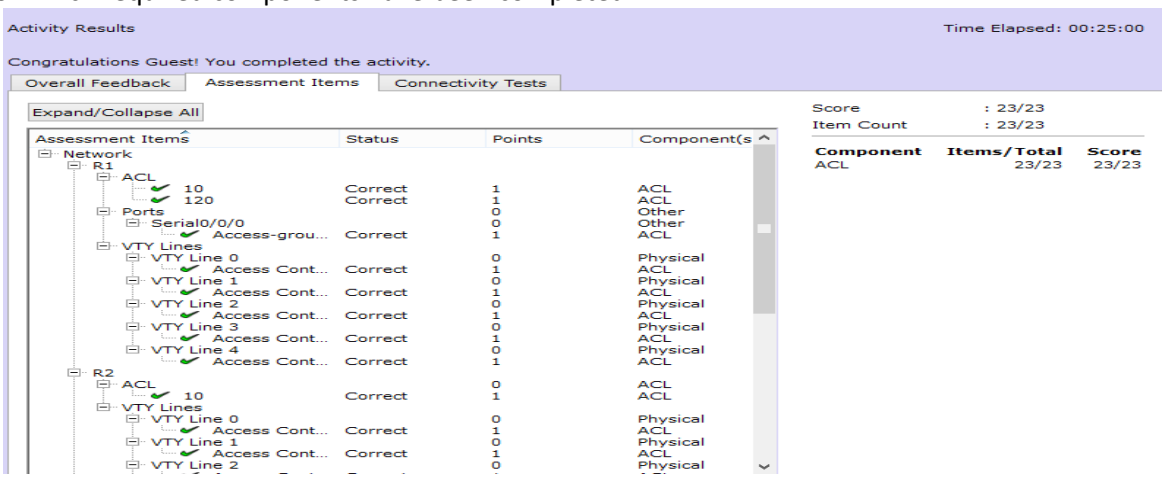
## Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

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.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

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

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

C:\>
```

## Step 4: Check results.

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



## SRIPTS

!!!Script for R1

```
access-list 10 permit 192.168.3.3 0.0.0.0
line vty 0 4
access-class 10 in
access-list 120 permit udp any host 192.168.1.3 eq domain
access-list 120 permit tcp any host 192.168.1.3 eq smtp
access-list 120 permit tcp any host 192.168.1.3 eq ftp
access-list 120 deny tcp any host 192.168.1.3 eq 443
access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
interface s0/0/0
ip access-group 120 in
access-list 120 permit icmp any any echo-reply
access-list 120 permit icmp any any unreachable
access-list 120 deny icmp any any
access-list 120 permit ip any any
```

!!!Script for R2

```
access-list 10 permit 192.168.3.3 0.0.0.0
line vty 0 4
access-class 10 in
```

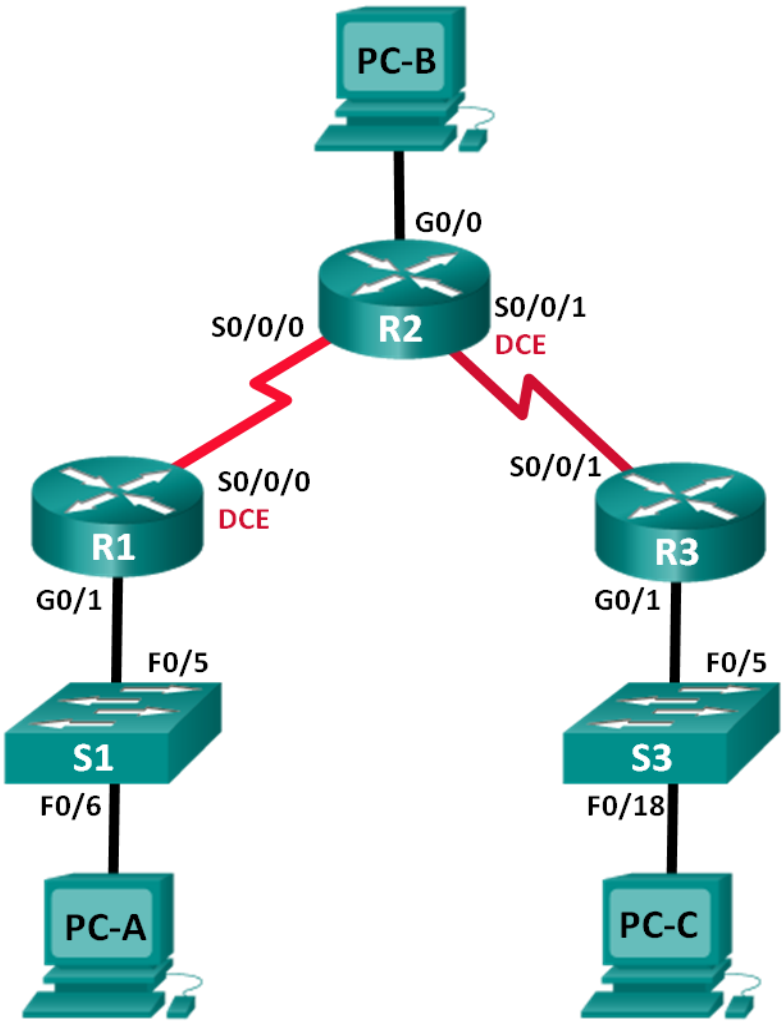
!!!Script for R3

```
access-list 10 permit 192.168.3.3 0.0.0.0
line vty 0 4
access-class 10 in
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 224.0.0.0 15.255.255.255 any
access-list 100 permit ip any any
interface s0/0/1
ip access-group 100 in
access-list 110 permit ip 192.168.3.0 0.0.0.255 any
interface fa0/1
ip access-group 110 in
```

# 7.3.2.4 Práctica de laboratorio: configuración básica de RIPv2 y RIPng

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

## Topología



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

## Objetivos

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

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

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

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

**Parte 4: configurar y verificar el routing RIPng**

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

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

## 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

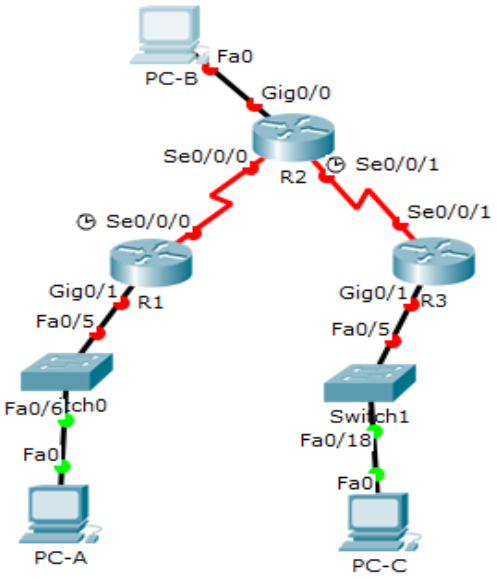
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar 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.

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

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




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

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

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

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hosname S1
                ^
% Invalid input detected at '^' marker.

Switchosname S1hohhostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "Solamente acceso Autorizado"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#no ip  domain-lookup
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd " Solamente Acceso Autorizado"
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
S3#
```

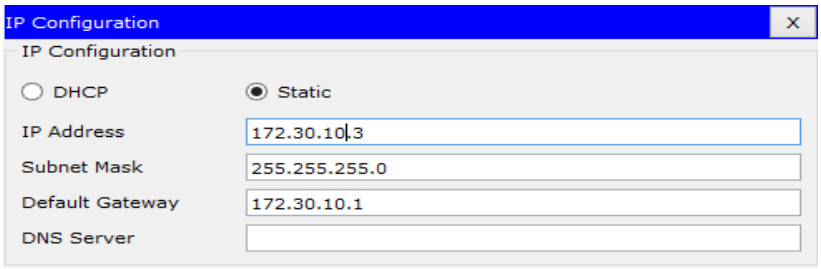
```
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "Solamente Acceso Autorizado"
R1(config)#int g0/1
R1(config-if)#ip add 172.30.10.1 255.255.255.0
R1(config-if)#description connection to S1
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 add 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#description connection to R2
R1(config-if)#no shutdown

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

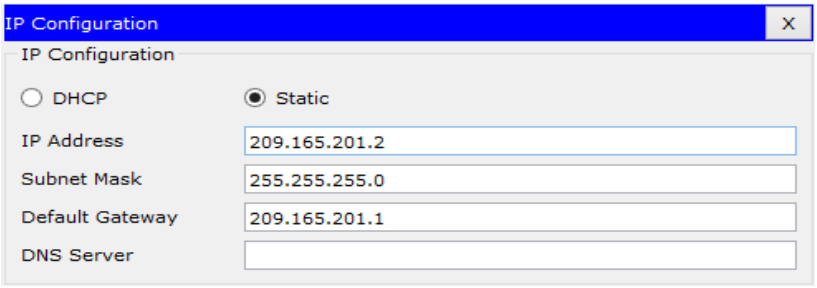
```
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd " Solamente Acceso Autorizado"
R2(config)#int g0/0
R2(config-if)#ip add 209.165.201.1 255.255.255.0
R2(config-if)#description connection to PC-B
R2(config-if)#no shutdown

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

R2(config-if)#int s0/0/0
R2(config-if)#ip add 10.1.1.2 255.255.255.252
R2(config-if)#description connection to R1
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)#ip
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

R2(config-if)#ip add 10.2.2.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#description connection to R3
R2(config-if)#no shutdown
```

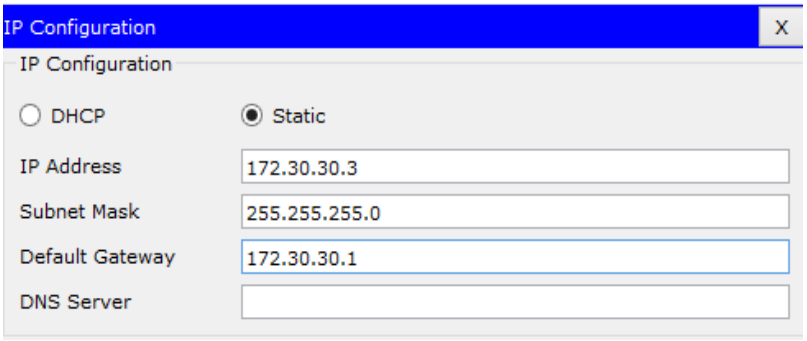
```
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd "Solamente Acceso Autorizado"
R3(config)#int g0/1
R3(config-if)#ip add 172.30.30.1 255.255.255.0
R3(config-if)#description connection to S3
R3(config-if)#no shutdown

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

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

R3(config-if)#int s0/0/1
R3(config-if)#ip add 10.2.2.1 255.255.255.252
R3(config-if)#description connection to R2
R3(config-if)#no shutdown

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

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

R3#cop r s
Destination filename [startup-config]?
Building configuration
```

## Paso 4. configurar los equipos host.

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

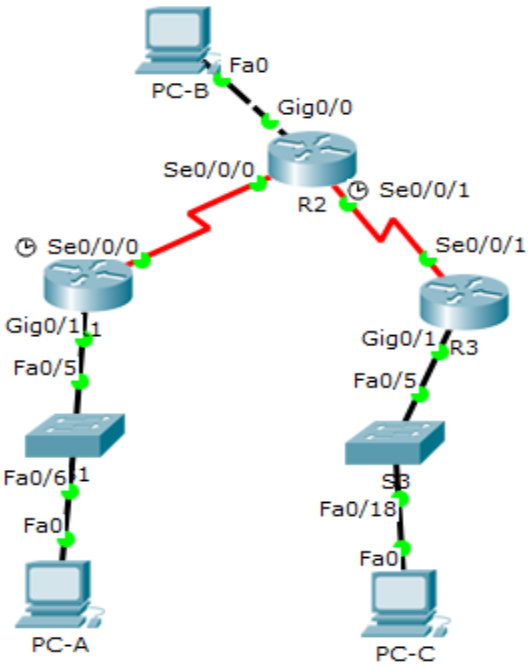


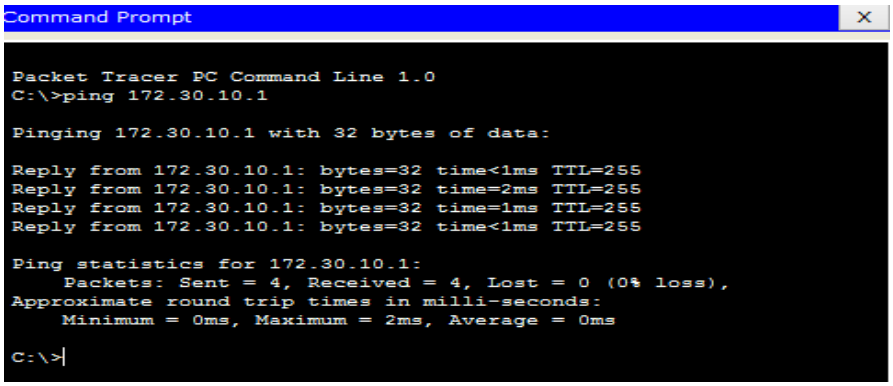



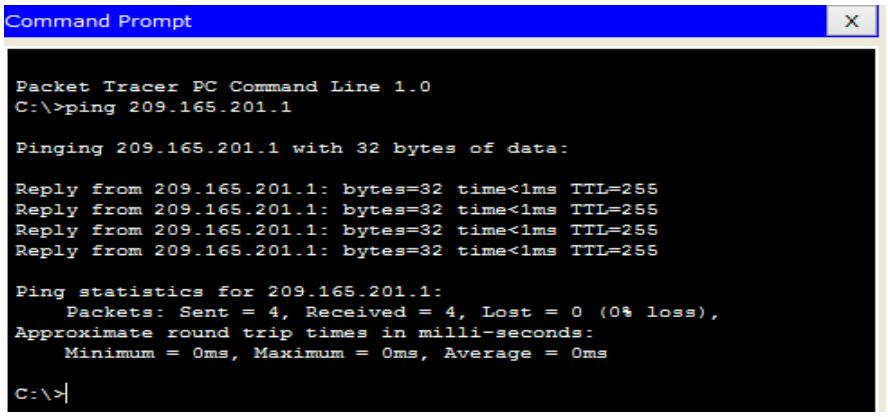

## Paso 5. Probar la conectividad.

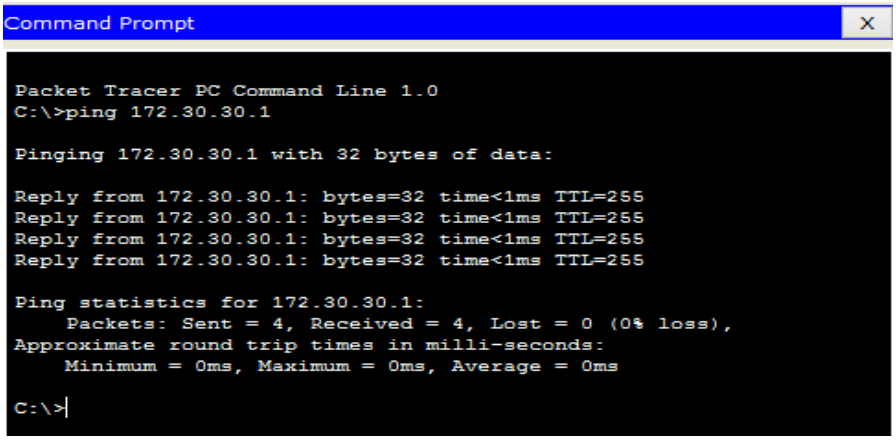
En este momento, las computadoras no pueden hacerse ping entre sí.




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






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

```
R1>ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6
ms
```

```
R2>ping 10.2.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6
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 LA sumarización automática, configurará una ruta predeterminada y verificará la conectividad de extremo a extremo.

### Paso 1. Configurar el enrutamiento RIPv2.

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

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

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

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

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#passive-interface g0/1
R3(config-router)#network 172.30.0.0
R3(config-router)#network 10.0.0.0
R3(config-router)#
```

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

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

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

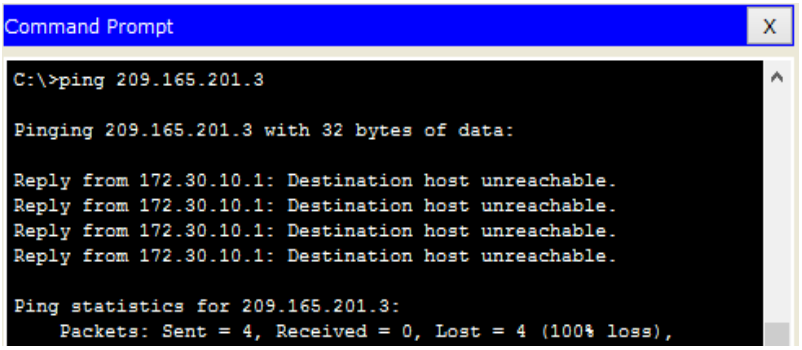
## Paso 2. examinar el estado actual de la red.

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

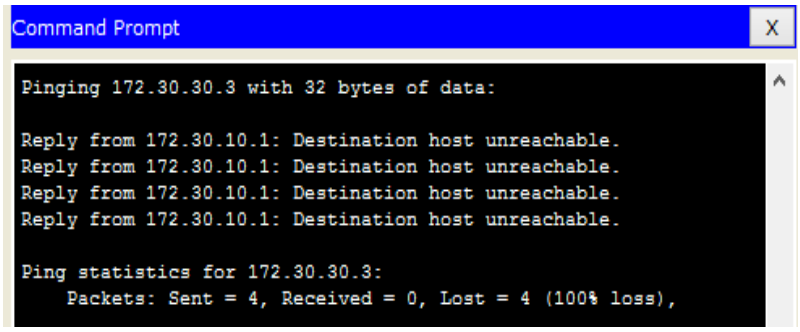
```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     209.165.201.1   YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.1.1.2     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

b. Verifique la conectividad entre las computadoras.

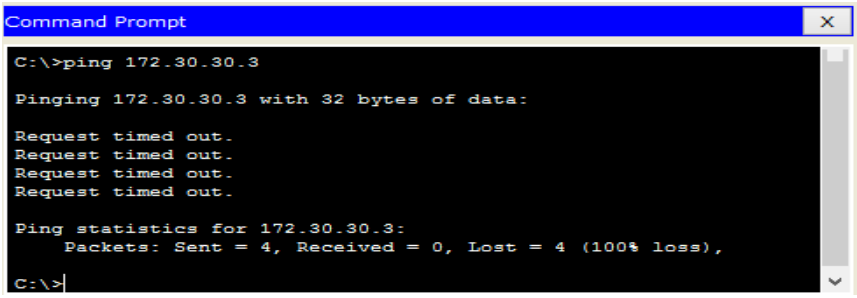
¿Es posible hacer ping de la PC-A a la PC-B? No ¿Por qué? Porque no se anunció la red 209.165.0.0 con la habilitación del RIP en R2




¿Es posible hacer ping de la PC-A a la PC-C?No ¿Por qué? Porque en el router R2 no se especifica la red 172.30.0.0




¿Es posible hacer ping de la PC-C a la PC-B?NO ¿Por qué? Porque el R2 no se especifica la red del PC-C




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

No ¿Por qué? Por la misma situación del primer caso. No se especifica la red en el router R2

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"
Sending updates every 30 seconds, next due in 10 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
            10.0.0.0
            172.30.0.0
Passive Interface(s):
            GigabitEthernet0/1
Routing Information Sources:
            Gateway         Distance      Last Update
            10.1.1.2              120      00:00:10
Distance: (default is 120)
```

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

RIP protocol debugging is on

```
R2#debug ip rip
RIP protocol debugging is on
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: 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: 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
```

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

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

Router rip

versión 2

Passive-interface GigabitEthernet0/1

Network  10.0.0.0

Network 172.30.0.0

```
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.

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R    172.30.0.0/16 [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
                   [120/1] via 10.2.2.1, 00:00:10, 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
```

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 R3

```
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, 00:00:18, Serial0/0/0
     172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1

R1#
```

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

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:13, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1

R3#
```

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

10.2.2.1 on Serial 0/0/1

10.1.1.1 on serial 0/0/0

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

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.

e. 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.

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

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

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

R1#clear ip route *
```

```
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#clear ip rpute *
             ^
% Invalid input detected at '^' marker.

R2#clear ip route *
```

```
R3(config)#router rip
R3(config-router)#no auto-summary
R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#clear ip route *
```

g. 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
```

```
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
     172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:01, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:25, Serial0/0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0

R2#
```

R1# **show ip route**

<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, 00:00:10, 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, 00:00:10, Serial0/0/0

R1#
```

R3# **show ip route**

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:17, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:17, Serial0/0/1
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1

R3#
```

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

**R2# debug ip rip**

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

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

172.30.10.0/24

172.30.30.0/24

```
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0

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

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

¿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.

i. 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
```

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

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

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#router rip
R2(config-router)#default-information originate
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

## Paso 5. Verificar la configuración de enrutamiento.

k. Consulte la tabla de routing en el R1.

```
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, 00:00:10, 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, 00:00:10, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:10, Serial0/0/0

R1#
```

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

Porque ya hay establecida un Gateway o puerta de enlace de último recurso.

l. Consulte la tabla de routing en el R2.

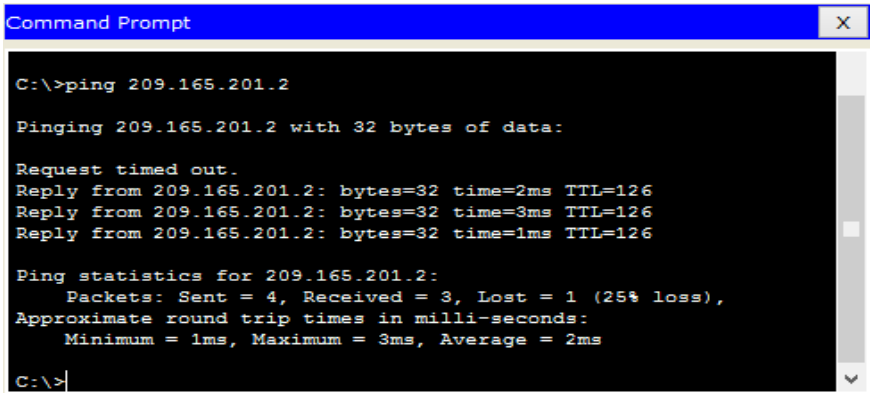
¿En qué forma se proporciona la ruta para el tráfico de Internet en la tabla de routing?

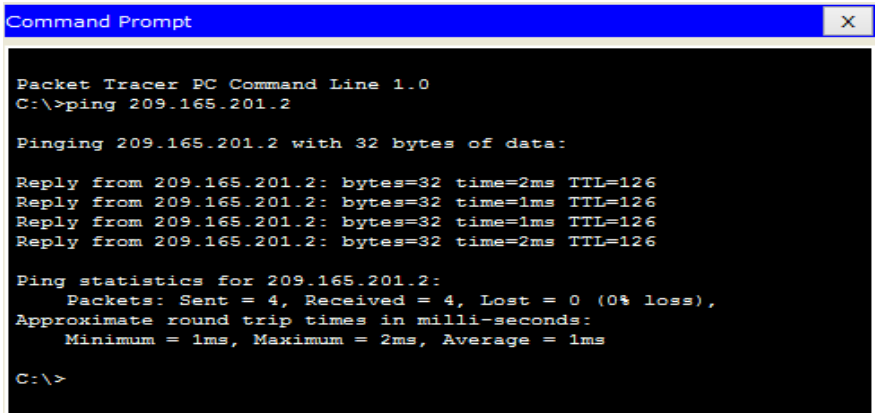
```
Gateway of last resort is 209.165.201.2 to network 0.0.0.0

     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
     172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:19, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:00, 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
S*   0.0.0.0/0 [1/0] via 209.165.201.2

R2#
```

## Paso 6. Verifique la conectividad.

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

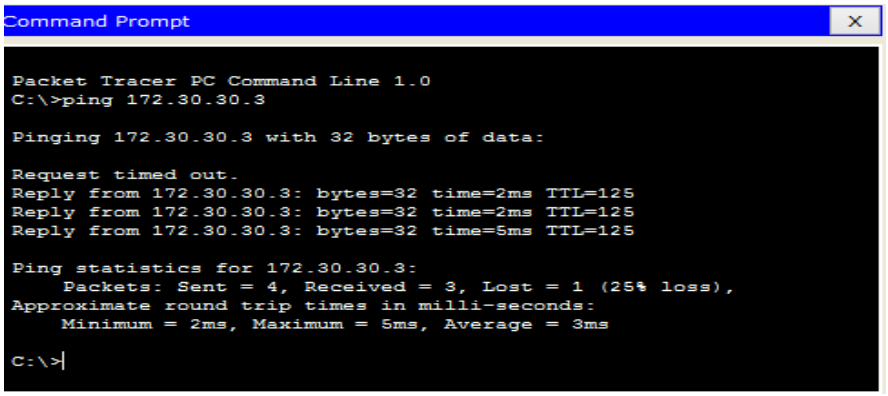
¿Tuvieron éxito los pings? Si




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

¿Tuvieron éxito los pings? Sí




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

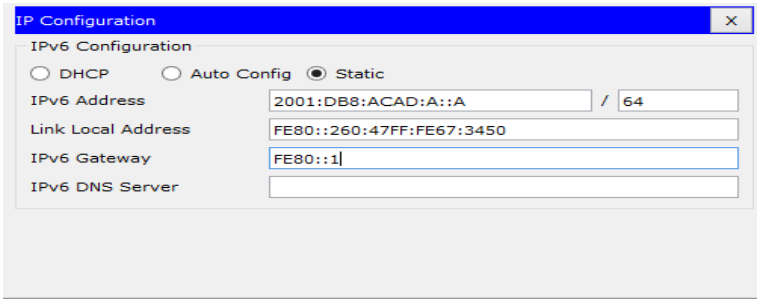
## Parte 3: configurar IPv6 en los dispositivos

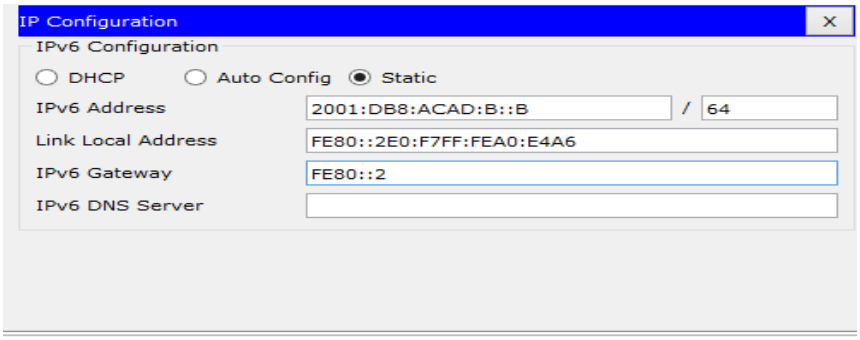
En la parte 3, configurará todas las interfaces con direcciones IPv6 y verificará la conectividad.

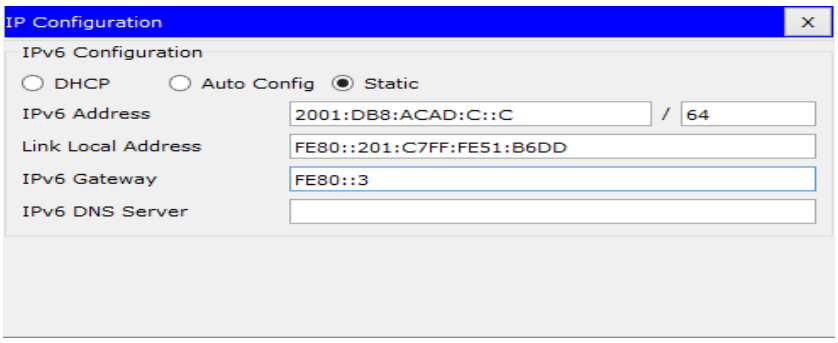
| Dispositivo | Interfaz | Dirección IPv6/longitud de prefijo | Gateway predeterminado |
|---|---|---|---|
| R1 | G0/1 | 2001:DB8:ACAD:A::1/64<br>FE80::1 link-local | No aplicable |
| | S0/0/0 | 2001:DB8:ACAD:12::1/64<br>FE80::1 link-local | No aplicable |
| R2 | G0/0 | 2001:DB8:ACAD:B::2/64<br>FE80::2 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.

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

d. Habilite el routing IPv6 en cada router.

```
R1(config)#int g0/1
R1(config-if)#ipv6 add 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 add FE80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#int s0/0/0
R1(config-if)#ipv6 add 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 add FE80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#end
R1(config)#ipv6 unicast-routing
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

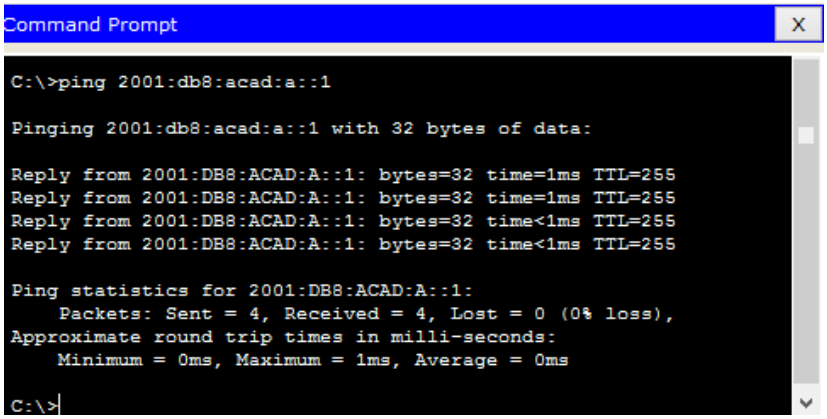
```
R2(config)#int g0/0
R2(config-if)#ipv6 add 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 add FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#int s0/0/0
R2(config-if)#ipv6 add 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 add FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 add 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 add FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

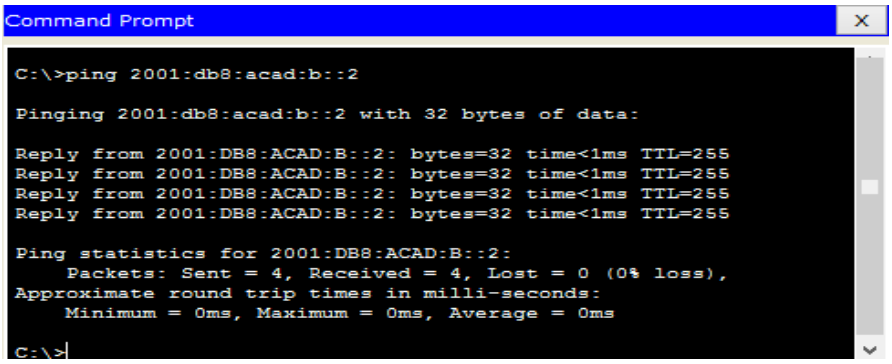
```
R3(config)#int g0/1
R3(config-if)#ipv6 add 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 add FE80::3 link-local
R3(config-if)#no shutdown
R3(config-if)#exit
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int s0/0/1
R3(config-if)#ipv6 add 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 add FE80::3 link-local
R3(config-if)#no shutdown
R3(config-if)#ipv6 unicast-routing
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

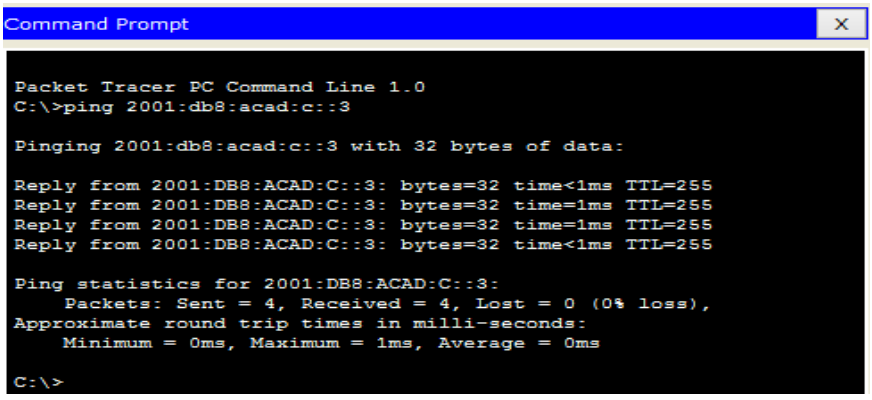
e. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.

Show ipv6 interface

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






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

```
R1>ping 2001:db8:acad:12::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:12::2, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7
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 = 2/3/5
ms
```

```
R3>ping 2001:db8:acad:23::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:23::2, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/5
ms
```

# 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.

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

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

```
R1(config)#int g0/1
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#int s0/0/0
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
R3(config)#int g0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

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

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

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

¿En qué forma se indica RIPng en el resultado?

IPv6 Routing Protocol is “rip Test1”

l. 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?

La distancia administrativa es 120

Updates every 30 seconds

Expire after 180 sec

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

Show ipv6 route

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

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

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

```
       D - EIGRP, EX - EIGRP external
R   2001:DB8:ACAD:A::/64 [120/2]
     via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
     via GigabitEthernet0/0, receive
R   2001:DB8:ACAD:C::/64 [120/2]
     via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R2#
```

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

```
       D - EIGRP, EX - EIGRP external
R    2001:DB8:ACAD:A::/64 [120/3]
      via FE80::2, Serial0/0/1
C    2001:DB8:ACAD:C::/64 [0/0]
      via GigabitEthernet0/1, directly connected
L    2001:DB8:ACAD:C::3/128 [0/0]
      via GigabitEthernet0/1, receive
R    2001:DB8:ACAD:12::/64 [120/2]
      via FE80::2, Serial0/0/1
C    2001:DB8:ACAD:23::/64 [0/0]
      via Serial0/0/1, directly connected
L    2001:DB8:ACAD:23::3/128 [0/0]
      via Serial0/0/1, receive
L    FF00::/8 [0/0]
      via Null0, receive
R3#
```

n. Verifique la conectividad entre las computadoras.

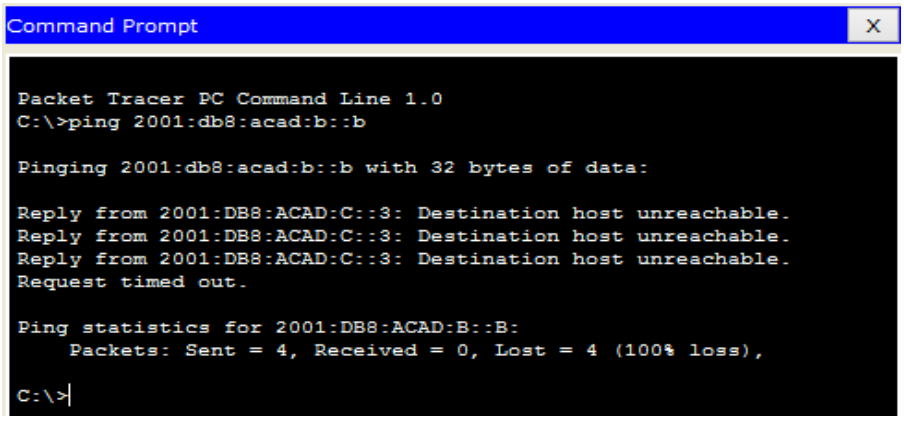
¿Es posible hacer ping de la PC-A a la PC-B? NO

```
Command Prompt

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

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

C:\>
```

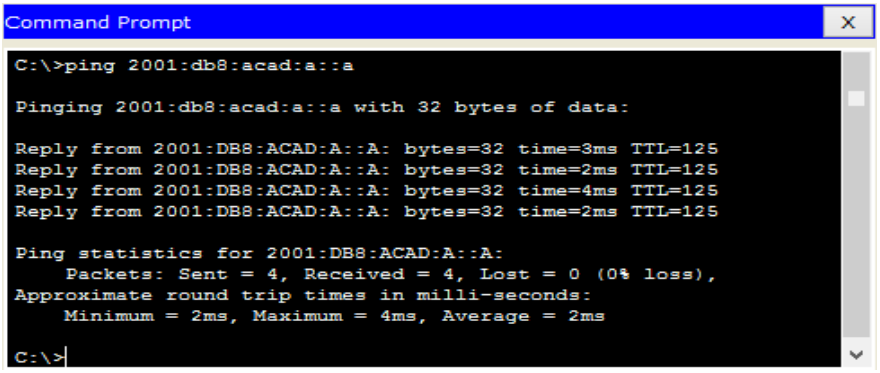
¿Es posible hacer ping de la PC-A a la PC-C?SI

```
Command Prompt

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=11ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 6ms

C:\>
```

¿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?

Porque la ruta para la PC-B no se anunció en el RIPng

## 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.

Ipv6 route ::0/64 2001:DB8:ACAD:B::B

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

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

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

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

```
R2(config)#ipv6 route ::0/64 2001:DB8:ACAD:B::B
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

## Paso 3. Verificar la configuración de enrutamiento.

c. 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 GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
     via GigabitEthernet0/0, receive
R   2001:DB8:ACAD:C::/64 [120/2]
     via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R2#
```

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

Porque tiene la ruta estática ::/64 por defecto

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

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

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

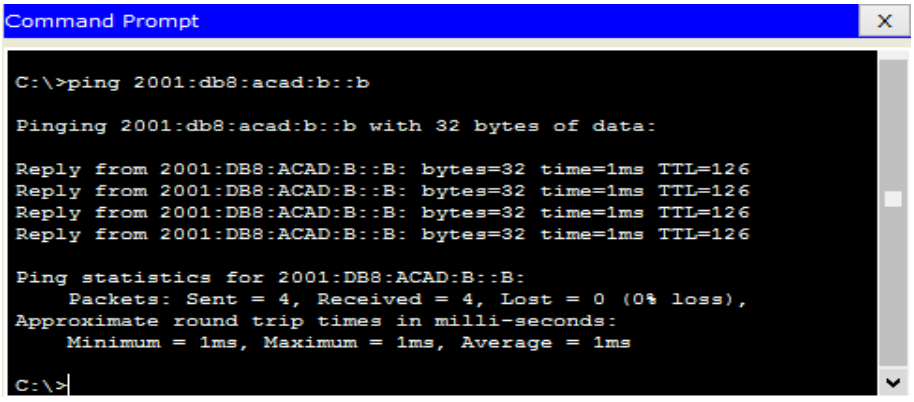
```
Password:
R1#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1,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

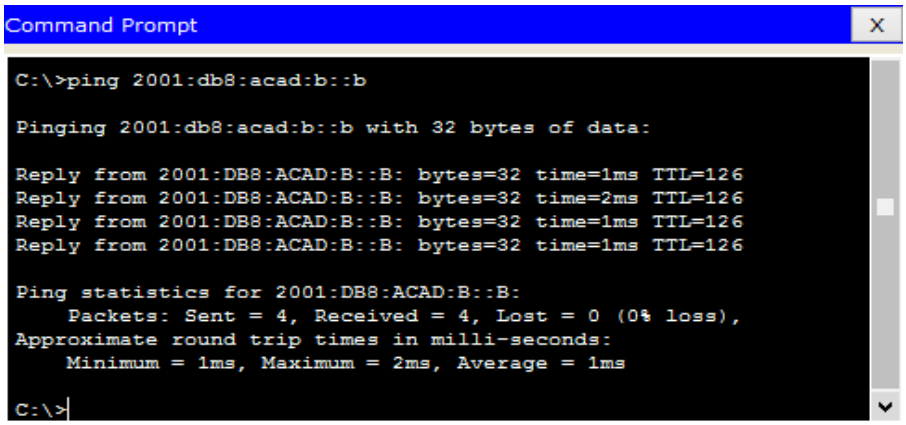
```
R3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF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

### Paso 4. Verifique la conectividad.

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

¿Tuvieron éxito los pings? SI






## Reflexión

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

   Para evitar que los router hagan sumarización de acuerdo a la clase mayor

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

   Con las actualizaciones realizadas por el rip que se recibieron del router R2 donde se configuró la ruta por defecto

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

   Con el RIPv2 la configuración se hace identificando las redes y con RIPng se hace identificando las interfaces

## Tabla de resumen de interfaces del router

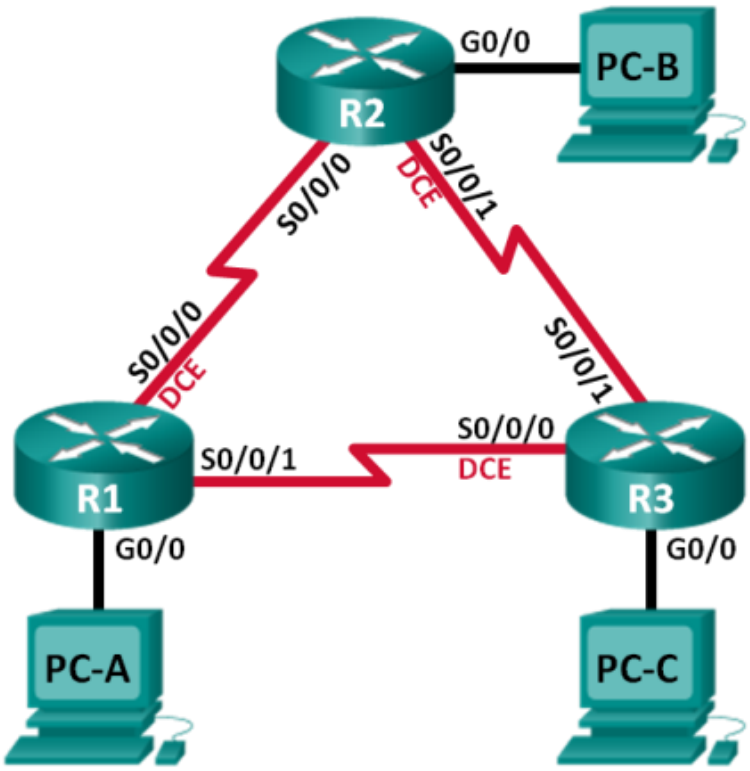
| Resumen de interfaces del router | | | | |
|---|---|---|---|---|
| **Modelo de router** | **Interfaz Ethernet #1** | **Interfaz Ethernet n.º 2** | **Interfaz serial #1** | **Interfaz serial n.º 2** |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1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

Universidad Nacional Abierta y a Distancia

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

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

## Topología



| 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.

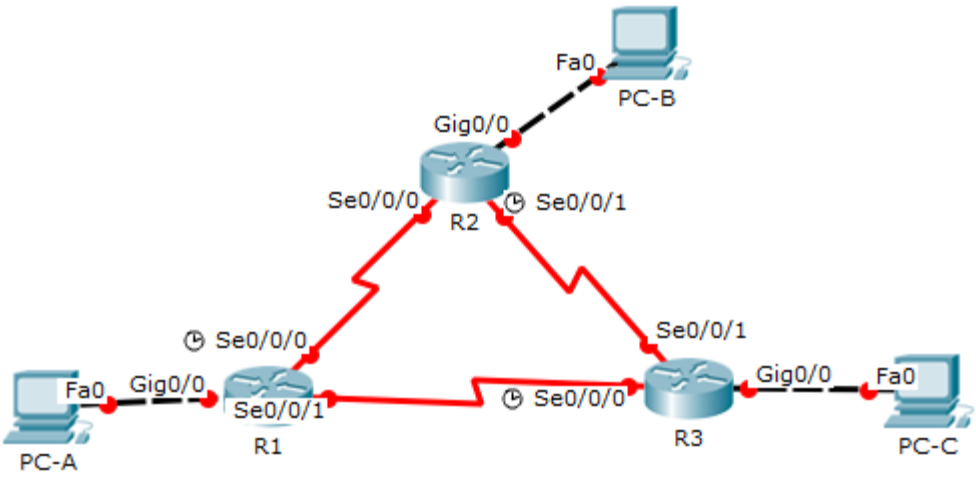
### Recursos necesarios

- 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

## Part 2: armar la red y configurar los parámetros básicos de los dispositivos

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

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




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

### Paso 3. configurar los parámetros básicos para cada router.

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**.

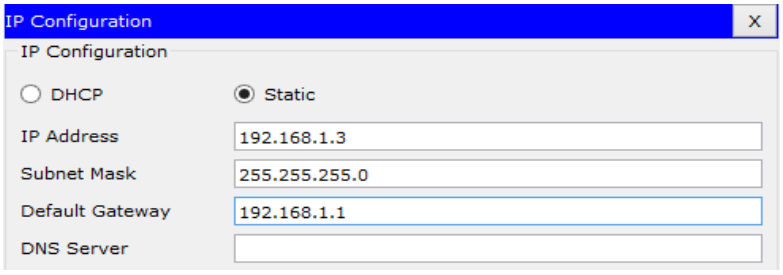
i. Copie la configuración en ejecución en la configuración de inicio

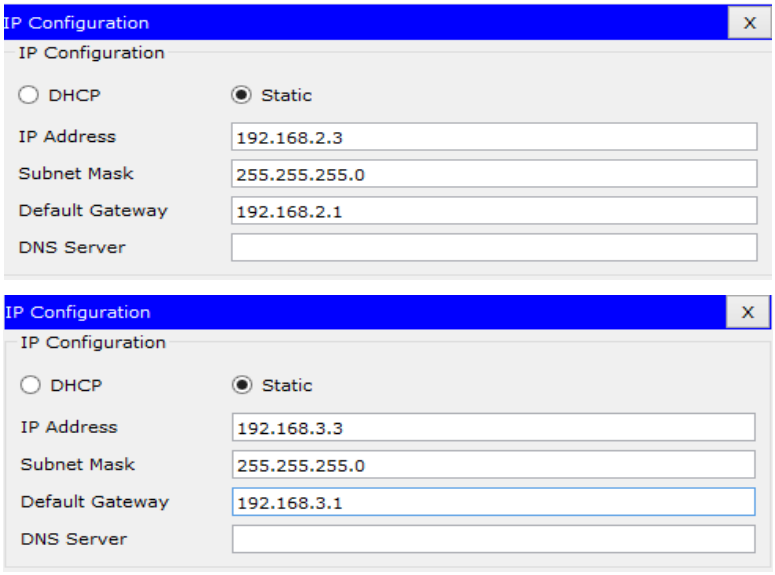
```
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd "Solamente Acceso Autorizado"
R1(config)#service password-encryption
R1(config)#int g0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#description connection to PC-A
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)#ip add 192.168.12.1 255.255.255.252
R1(config-if)#description connection to R2
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)#ip add 192.168.13.1 255.255.255.252
R1(config-if)#description connection to R3
R1(config-if)#no shutdown
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#banner motd "Solamente Acceso Autorizado"
R2(config)#service password-encryption
R2(config)#int g0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#description connection to PC-B
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)#ip add 192.168.12.2 255.255.255.252
R2(config-if)#description connection to R1
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
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
```

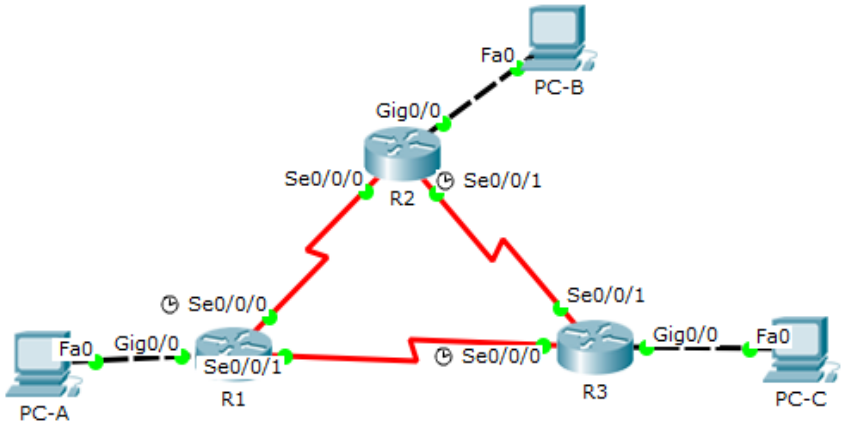
```
R3(config)#no ip domain-lookup
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#banner motd "Solamente Acceso Autorizado"
R3(config)#service password-encryption
R3(config)#int g0/0
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#description connection to PC-C
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)#ip add 192.168.13.2
% Incomplete command.
R3(config-if)#ip add 192.168.13.2 255.255.255.252
R3(config-if)#description conenection to R1
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)#
```

**Paso 4. configurar los equipos host.**






## Paso 5. Probar la conectividad.




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

```
R1>ping 192.168.12.2
```
**ping a R2**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6
ms
```

```
R1>ping 192.168.13.2
```
**ping a R3**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7
ms
```

```
R2>ping 192.168.12.1
```
**ping a R1**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4
ms
```

```
R2>ping 192.168.23.2
```
**ping a R3**

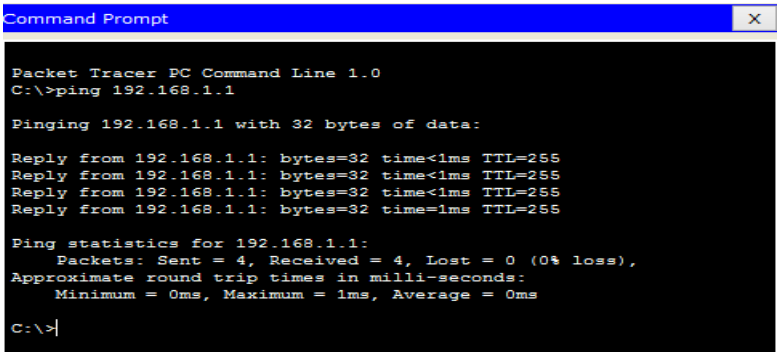
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6
ms
```

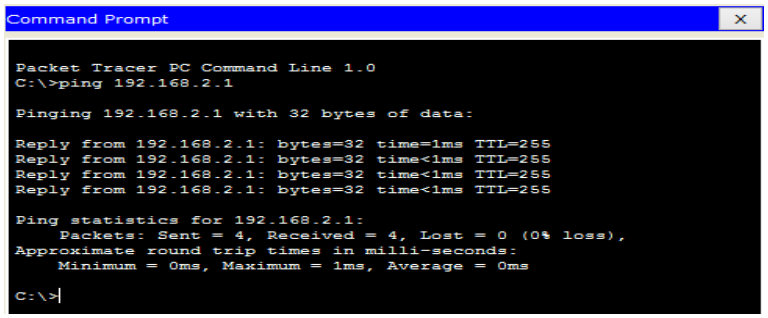
```
R3>ping 192.168.13.1
```
**ping a R1**

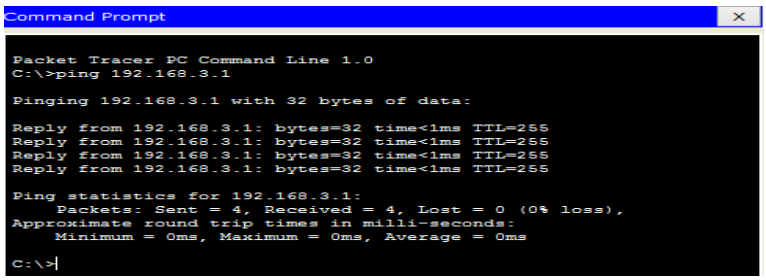
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6
ms
```

```
R3>ping 192.168.23.1
```
**ping a R2**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms
```




# Parte 3. Configurar y verificar el enrutamiento OSPF

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

## Paso 1. Configure el protocolo OSPF en R1.

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

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

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

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

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.3 area 0
R1(config-router)#network 192.168.13.0 0.0.0.3 area 0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

## Paso 2. Configure OSPF en el R2 y el R3.

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

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
01:00:59: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R2(config-router)#network 192.168.23.0 0.0.0.3 area 0
R2(config-router)#end
R2#
```

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0
R3(config-router)#
01:05:18: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R3(config-router)#network 192.168.23.0 0.0.0.3 area 0
R3(config-router)#
01:05:40: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on
Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-router)#end
R3#
```

```
R1#
01:01:19: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done

R1#
01:05:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to FULL, Loading Done
```

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

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

```
R1#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
192.168.23.1      0   FULL/  -        00:00:31    192.168.12.2    Serial0/0/0
```

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.13.1      0   FULL/  -        00:00:39    192.168.12.1    Serial0/0/0
192.168.23.2      0   FULL/  -        00:00:39    192.168.23.2    Serial0/0/1
```

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.13.1      0   FULL/  -        00:00:36    192.168.13.1    Serial0/0/0
192.168.23.1      0   FULL/  -        00:00:38    192.168.23.1    Serial0/0/1
```

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

      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, 00:11:08, Serial0/0/0
O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:07:00, 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, 00:06:38, Serial0/0/0
                         [110/128] via 192.168.13.2, 00:06:38, Serial0/0/1

R1#
```

```
Gateway of last resort is not set

O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:13:46, 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, 00:09:06, 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       192.168.13.0/30 [110/128] via 192.168.12.1, 00:09:06, Serial0/0/0
                        [110/128] via 192.168.23.2, 00:09:06, Serial0/0/1
     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

R2#
```

```
Gateway of last resort is not set

O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:10:56, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:10:34, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:10:34, Serial0/0/0
                        [110/128] via 192.168.23.1, 00:10:34, Serial0/0/1
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1

R3#
```

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

Show ip route ospf

```
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 03:47:46, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 03:43:38, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.12.2, 03:43:16, Serial0/0/0
                     [110/128] via 192.168.13.2, 03:43:16, Serial0/0/1
```

## Paso 4. verificar la configuración del protocolo OSPF.

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

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

```
R1# show ip protocols
```

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.13.1         110      00:14:37
    192.168.23.1         110      00:14:15
    192.168.23.2         110      00:14:15
  Distance: (default is 110)
```

## Paso 5. verificar la información del proceso OSPF.

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

```
R1#show ip ospf
 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 15 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x009baf
        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
```

## Paso 6. verificar la configuración de la interfaz OSPF.

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

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

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

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

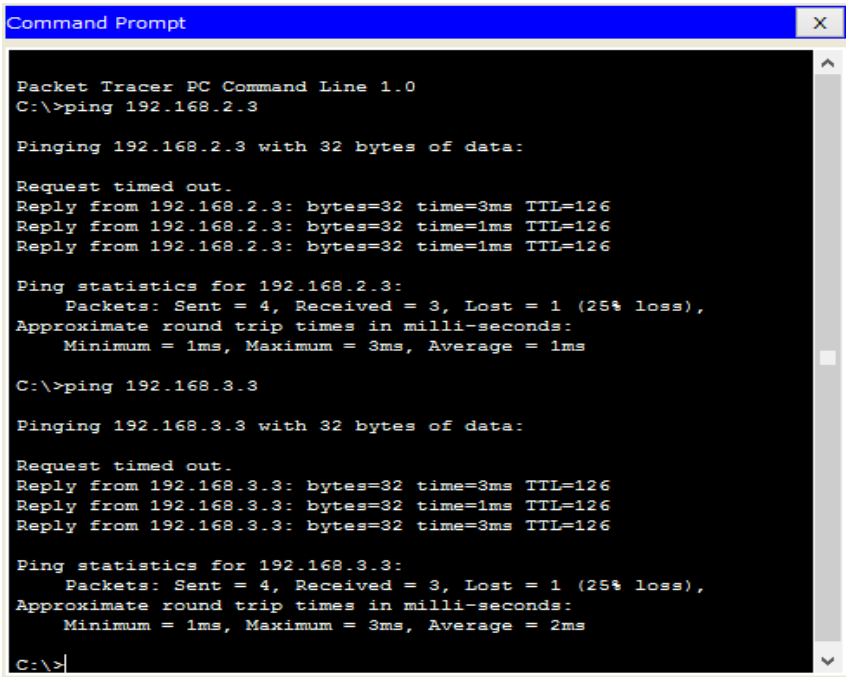
```
R1# show ip ospf interface
```

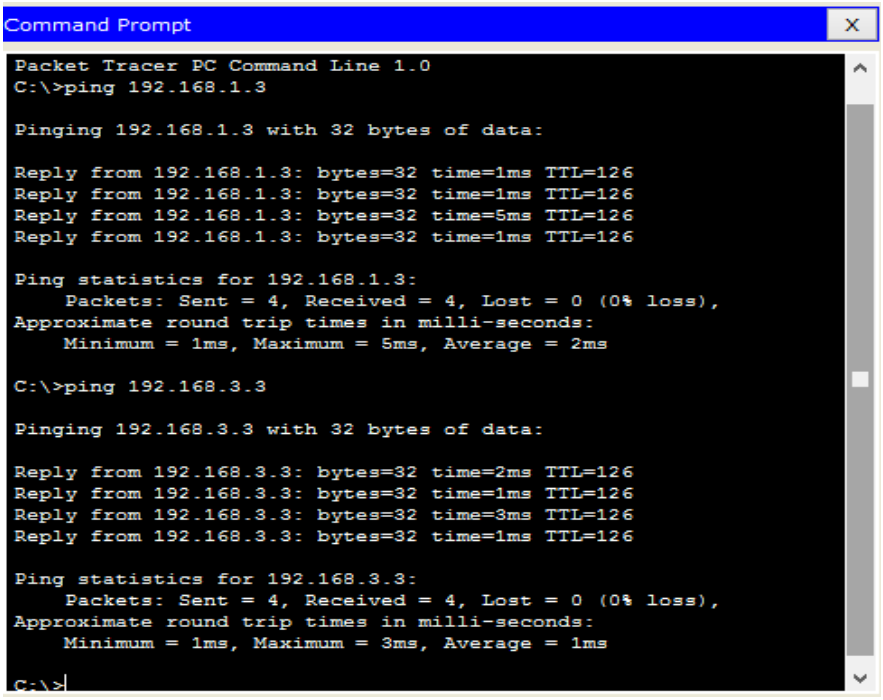
```
R1#show ip ospf interface

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 00:00:02
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  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 00:00:02
  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)
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 00:00:02
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)
R1#
```

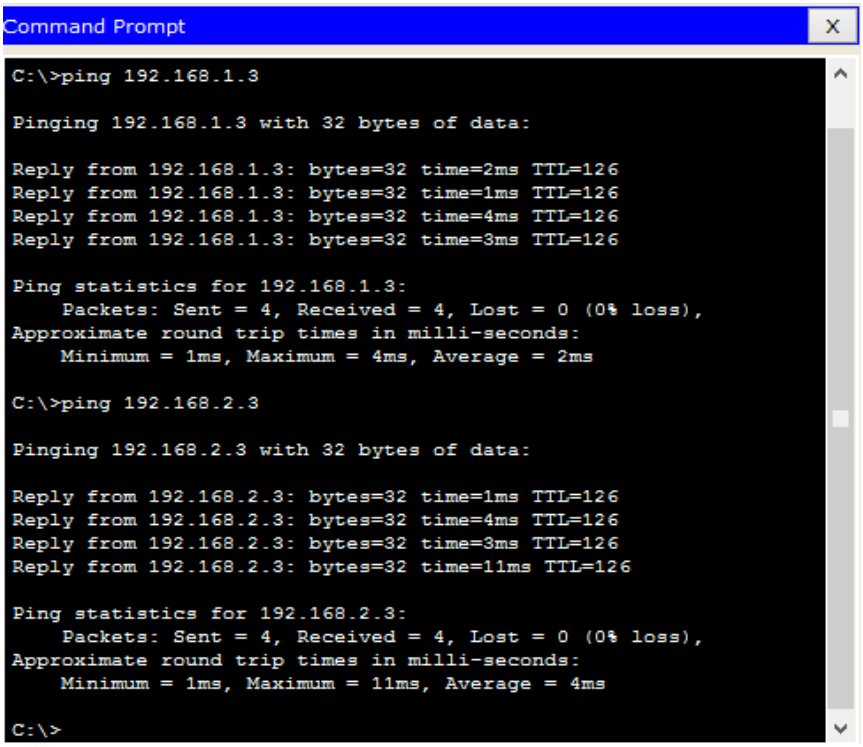
## Paso 7. Verificar la conectividad de extremo a extremo.

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

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


Command Prompt
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 192.168.2.3: bytes=32 time=3ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.2.3:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 1ms
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=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms 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 = 1ms, Maximum = 3ms, Average = 2ms
C:\>


Command Prompt
Packet Tracer PC Command Line 1.0
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=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=5ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 1ms
C:\>




## Parte 4. cambiar las asignaciones de ID del router

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

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

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

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

### Paso 1. Cambie las ID de router con direcciones de loopback.

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

```
R1(config)#interface lo0

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

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.

```
R2(config)#interface lo0

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

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

R2(config-if)#ip add 2.2.2.2 255.255.255.255
R2(config-if)#end
R2#
```

```
R3(config)#interface lo0

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

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

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

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
```

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:01:48
    2.2.2.2              110      00:01:48
    3.3.3.3              110      00:01:48
    192.168.13.1         110      00:15:41
    192.168.23.1         110      00:02:32
    192.168.23.2         110      00:02:17
  Distance: (default is 110)

R2#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 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:03:31
    2.2.2.2              110      00:03:31
    3.3.3.3              110      00:03:31
    192.168.13.1         110      00:17:24
    192.168.23.1         110      00:04:15
    192.168.23.2         110      00:04:00
  Distance: (default is 110)

R3#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 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.3.0 0.0.0.255 area 0
    192.168.13.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:04:33
    2.2.2.2              110      00:04:33
    3.3.3.3              110      00:04:33
    192.168.13.1         110      00:18:26
    192.168.23.1         110      00:05:17
    192.168.23.2         110      00:05:02
  Distance: (default is 110)
```

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

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:30    192.168.12.2    Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:39    192.168.13.2    Serial0/0/1
```

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

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

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

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

```
R1(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#
```

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

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

R1#
00:26:14: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:26:14: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached

00:26:14: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:26:14: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached

R1#
00:26:29: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done

R1#
00:26:30: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0
from LOADING to FULL, Loading Done
```

```
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R2#
00:28:09: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:28:09: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached

00:28:09: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:28:09: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached

R2#
00:28:10: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done

R2#
00:28:11: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from LOADING to FULL, Loading Done

R2#
00:28:55: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done


R3#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R3#
00:28:29: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:28:29: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached

00:28:29: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:28:29: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached

R3#
00:28:30: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from LOADING to FULL, Loading Done

R3#
00:28:36: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done
```

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(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
```

```
R3(config)#router ospf 1
R3(config-router)#router-id 33.33.33.33
R3(config-router)#Reload or use "clear ip ospf process" command,
for this to take effect


R3(config-router)#end
```

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

```
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
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:36:43
    2.2.2.2              110      00:02:44
    3.3.3.3              110      00:08:33
    11.11.11.11          110      00:02:03
    22.22.22.22          110      00:02:03
    33.33.33.33          110      00:02:03
    192.168.13.1         110      00:50:36
    192.168.23.1         110      00:37:27
    192.168.23.2         110      00:37:12
  Distance: (default is 110)

R1#
```

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

```
R1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       0   FULL/  -        00:00:30    192.168.12.2    Serial0/0/0
33.33.33.33       0   FULL/  -        00:00:30    192.168.13.2    Serial0/0/1
```

## Parte 5. configurar las interfaces pasivas de OSPF

El comando **passive-interface** evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. En la parte 4, utilizará el comando **passive-interface** para configurar una única interfaz como pasiva.

También configurará OSPF para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

## Paso 1. configurar una interfaz pasiva.

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

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

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

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST,
Cost: 1
  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
    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)
```

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

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

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

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

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

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

```
Gateway of last resort is not set

     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:23:19,
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, 00:23:59,
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       192.168.13.0/30 [110/128] via 192.168.12.1, 00:23:19,
Serial0/0/0
                        [110/128] via 192.168.23.2, 00:23:19,
Serial0/0/1
     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

R2#
```

```
Gateway of last resort is not set

     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:39:26,
Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:30:16,
Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:30:16,
Serial0/0/1
                        [110/128] via 192.168.13.1, 00:30:16,
Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1

R3#
```

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

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

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       0   FULL/  -        00:00:36    192.168.12.2    Serial0/0/0
33.33.33.33       0   FULL/  -        00:00:35    192.168.13.2    Serial0/0/1
```

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)#
01:19:11: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached

01:19:11: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
```

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

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:36    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 is 192.168.12.2/30, Area 0
  Process ID 1, Router ID 22.22.22.22, Network Type POINT-TO-
POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    No Hellos (Passive interface)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
```

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**.

```
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    192.168.3.0/24 [110/65] via 192.168.13.2, 00:01:14, 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, 00:01:14, Serial0/0/1

R1#
```

```
Gateway of last resort is not set

     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:02:50, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:02:50, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1

R3#
```

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)#
00:07:30: %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 ip ospf neighbor** en el R1 y el R3, y busque una ruta a la red 192.168.2.0/24.

```
Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:02:23, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:09:43, 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, 00:02:23, Serial0/0/0
                        [110/128] via 192.168.13.2, 00:02:23, Serial0/0/1
```

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       0   FULL/  -        00:00:30    192.168.12.2    Serial0/0/0
33.33.33.33       0   FULL/  -        00:00:32    192.168.13.2    Serial0/0/1
R1#
```

```
Gateway of last resort is not set

     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:12:10, Serial0/0/0
O    192.168.2.0/24 [110/129] via 192.168.13.1, 00:04:40, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:12:10, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1

R3#
```

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
11.11.11.11       0   FULL/  -        00:00:39    192.168.13.1
Serial0/0/0
R3#
```

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

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

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

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

¿Qué indica esta información?

Esto nos indica que la interface S0/0/1 del R2 aun sigue siendo pasiva y que el costo de 129 de la métrica para la red 192.168.2.0/24 es debido a que la ruta es travez de las dos interfaces seriales que van desde R3 a R1 y desde R1 a R2. Como el costo de cada una de ellas vale 64 y el costo de la interfaz G0/0 vale 1 entonces al sumarlas da 64+64+1 = 129

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 passive-interface S0/0/1

```
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/1
R2(config-router)#
01:36:47: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on
Serial0/0/1 from LOADING to FULL, Loading Done
```

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

```
Gateway of last resort is not set

     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:12:25, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:00:55, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:00:55, Serial0/0/1
                        [110/128] via 192.168.13.1, 00:00:55, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1

R3#
```

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? S0/0/1

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

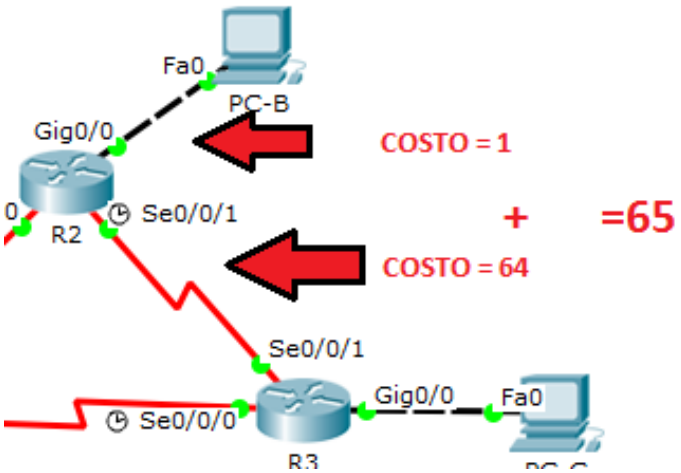
La métrica es 65.

El cálculo es la suma del costo del enlace G0/0 que es igual a 1

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

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
```

Más el costo del enlace S0/0/1que es igua a 64

```
R3#show ip ospf interface s0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.23.2/30, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
```




OSPF utiliza el costo como métrica. Cuando el costo es menor, la ruta es mejor que una con un costo mayor.

El costo de una interfaz es inversamente proporcional al ancho de banda de la interfaz. Por lo tanto, cuanto mayor es el ancho de banda, menor es el costo. Cuanto más sobrecarga y retraso, mayor es el costo. Por lo tanto, una línea Ethernet de 10 Mb/s tiene un costo mayor que una línea Ethernet de 100 Mb/s.

**Costo = *ancho de banda de referencia / ancho de banda de la interfaz***

El ancho de banda de referencia predeterminado es 10^8 (100 000 000); por lo tanto, la fórmula es la siguiente:

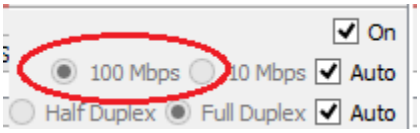
**Costo = 100 000 000 bps /ancho de banda de la interfaz en bps**

100.000.000/BW

Entonces el costo del enlace S0/0/1 = 100.000.000/1.544.000=64.76

Y el costo del enlace G0/0 = 100.000.000/100.000.000=1

NOTA: Como el ancho de banda que soporta la tarjeta Ethernet del PC es 100Mbs, entonces el cálculo del costo del enlace G0/0 se hace co n ese valor y no con 1Gbs




**Valores de costo de OSPF predeterminados de Cisco**

| Tipo de interfaz | Ancho de banda de referencia en bps | | Ancho de banda predeterminado en bps | Costo |
|---|---|---|---|---|
| 10 Gigabit Ethernet<br>10 Gbps | 100,000,000 | ÷ | 10,000,000,000 | 1 |
| Gigabit Ethernet<br>1 Gbps | 100,000,000 | ÷ | 1,000,000,000 | 1 |
| Fast Ethernet<br>100 Mbps | 100,000,000 | ÷ | 100,000,000 | 1 |
| Ethernet<br>10 Mbps | 100,000,000 | ÷ | 10,000,000 | 10 |
| Serial<br>1,544 Mbps | 100,000,000 | ÷ | 1,544,000 | 64 |
| Serial<br>128 kbps | 100,000,000 | ÷ | 128,000 | 781 |
| Serial<br>64 kbps | 100,000,000 | ÷ | 64,000 | 1562 |

El mismo costo debido al ancho de banda de referencia

Imagen recuperada de: http://ecovi.uagro.mx/ccna2/course/module8/8.2.3.1/8.2.3.1.html

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       0   FULL/  -        00:00:36    192.168.23.1    Serial0/0/1
11.11.11.11       0   FULL/  -        00:00:36    192.168.13.1    Serial0/0/0
```

¿El R2 aparece como vecino OSPF del R3? Si

# Parte 6. cambiar las métricas de OSPF

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

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

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

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

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

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

```
R1#show interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 000c.cf14.3b01 (bia
000c.cf14.3b01)
  Description: connection to PC-A
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is
unsupported
```

**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
```

```
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 01:03:12, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 01:03:12, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 01:03:12,
Serial0/0/1
                     [110/128] via 192.168.12.2, 01:03:12,
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 is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

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 is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  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
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 33.33.33.33
  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.

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

```
R3(config)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
```

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

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

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 100
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

**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 is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 6476
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  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
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 33.33.33.33
  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
O    192.168.2.0 [110/6576] via 192.168.12.2, 00:06:27, Serial0/0/0
O    192.168.3.0 [110/6576] via 192.168.13.2, 00:04:50, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/12952] via 192.168.13.2, 00:04:40, Serial0/0/1
                     [110/12952] via 192.168.12.2, 00:04:40, Serial0/0/0
```

**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.


R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
```

```
R3(config)#router ospf 1
R3(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 admitir redes con enlaces más rápidos que 100Mbits que es el ancho de banda de referencia por defecto

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

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

**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 (connected)
  Hardware is HD64570
  Description: connection to R2
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
```

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

```
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 00:07:53, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:07:53, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.12.2, 00:07:53,
Serial0/0/0
                     [110/128] via 192.168.13.2, 00:07:53,
Serial0/0/1
```

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)#bandwith 128
                       ^
% Invalid input detected at '^' marker.

R1(config-if)#bandwidth 128
R1(config-if)#end
```

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
O    192.168.2.0 [110/129] via 192.168.13.2, 00:01:18, Serial0/0/1
O    192.168.3.0 [110/65] via 192.168.13.2, 00:13:44, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 00:01:18, Serial0/0/1
```

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

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

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

```
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 11.11.11.11, Network Type BROADCAST, Cost: 1
  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
    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)
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 781
  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 00:00:02
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 22.22.22.22
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
```

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

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

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
O    192.168.2.0 [110/782] via 192.168.12.2, 00:01:03, Serial0/0/0
O    192.168.3.0 [110/782] via 192.168.13.2, 00:01:03, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/845] via 192.168.12.2, 00:01:03, Serial0/0/0
                     [110/845] via 192.168.13.2, 00:01:03, Serial0/0/1

R1#
```

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.

Primero se cambio el ancho de banda de la interfaz S0/0/0 de 1544Kb/s a 128Kb/s, entonces el costo sería:

Para el caso de la red 192.168.3.0/24 el cálculo fue el siguiente:

$$\frac{100000000}{128000} = 781$$

El costo del enlace S0/0/0 es 781

Para el costo de la interfaz G0/0 hay que trabajar con 100Mb/s que es la velocidad que soporta, entonces:

$$\frac{100000000}{100000000} = 1$$

El costo acumulado para la red 192.168.3.0/24 sería 782

Para el caso de la red 192.168.23.0/30 el cálculo fue el siguiente:

$$\frac{100000000}{128000} = 781$$

El costo del enlace S0/0/0 es 781

Como el costo del enlace S0/0/1 vale:

$$\frac{100000000}{1544000} = 64$$

Entonces el costo acumulado para la red 192.168.23.0/30 es 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
O    192.168.1.0 [110/65] via 192.168.13.1, 02:19:11, Serial0/0/0
O    192.168.2.0 [110/65] via 192.168.23.1, 02:19:11, Serial0/0/1
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0 [110/845] via 192.168.13.1, 02:19:11, Serial0/0/0
```

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

```
R2(config)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#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)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#end
```

```
R3(config)#int s0/0/0
R3(config-if)#bandwidth 128
R3(config-if)#exit
R3(config)#int s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#end
```

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

El costo es 1562. Porque es el acumulado se sumar al interfaz S0/0/1 de R1 que vale 781 más la interfaz S0/0/1 de R3 cuyo costo es 781 también. Es decir 781+781=1562

Todo lo anterior debido a que se cambió en ancho de banda de las interfaces seriales a 128Kb/s en tonces:

$$\frac{100000000}{128000} = 781$$

## Paso 3. cambiar el costo de la ruta.

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

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

```
R1#show ip route ospf
O    192.168.2.0 [110/782] via 192.168.12.2, 02:57:07, Serial0/0/0
O    192.168.3.0 [110/782] via 192.168.13.2, 02:57:07, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.13.2, 00:32:28, Serial0/0/1
                     [110/1562] via 192.168.12.2, 00:32:28, 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
O    192.168.2.0 [110/782] via 192.168.12.2, 02:59:50, Serial0/0/0
O    192.168.3.0 [110/1563] via 192.168.12.2, 00:00:46, Serial0/0/0
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:00:46, 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.

La razón de esto es que como el costo del enlace S0/0/1 es mayor que el costo del enlace S0/0/0 que es 1563 entonces la mejor ruta es por R2

## Reflexión

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

Porque las asignaciones de ID del router controlan el proceso de elección del router asignado y router designado de respaldo en una red de acceso multiples.Si la ID del router está asociado a una interfaz activa ésta puede ser cambiada si la interface se cae.

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

   Porque el proceso de elección de DR/BDR es solo un problema en una red de acceso múltiples, como Ethernet o Frame Relay.

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

   Porque es una forma práctica de liberar ancho de banda ya que al configurar la interfaz como pasiva no se genera routing OSPF de esa interfaz..

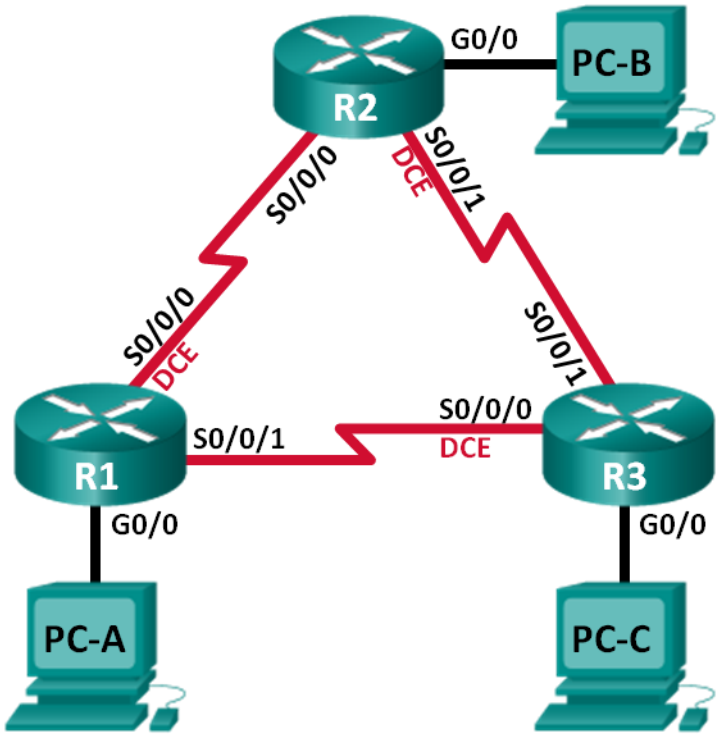
## Tabla de resumen de interfaces del router

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

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

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

## a. Topología




Topología

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

# 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 |

## b. 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**

## c. 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.

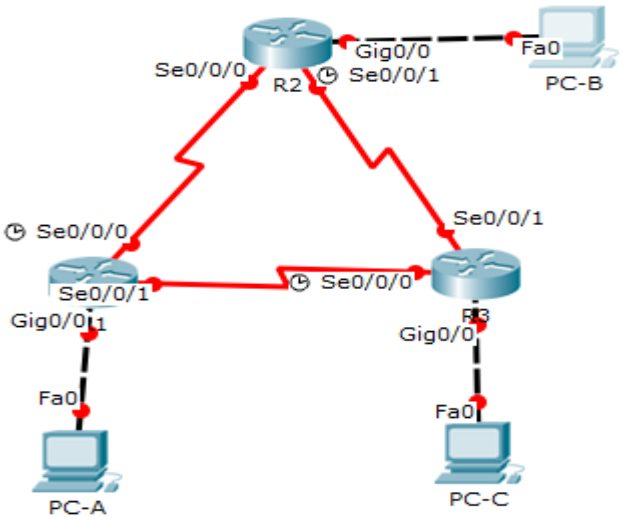
### d. Recursos necesarios

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

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

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

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




Ensamble de topología

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

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

i. Desactive la búsqueda del DNS.

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

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

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

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

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

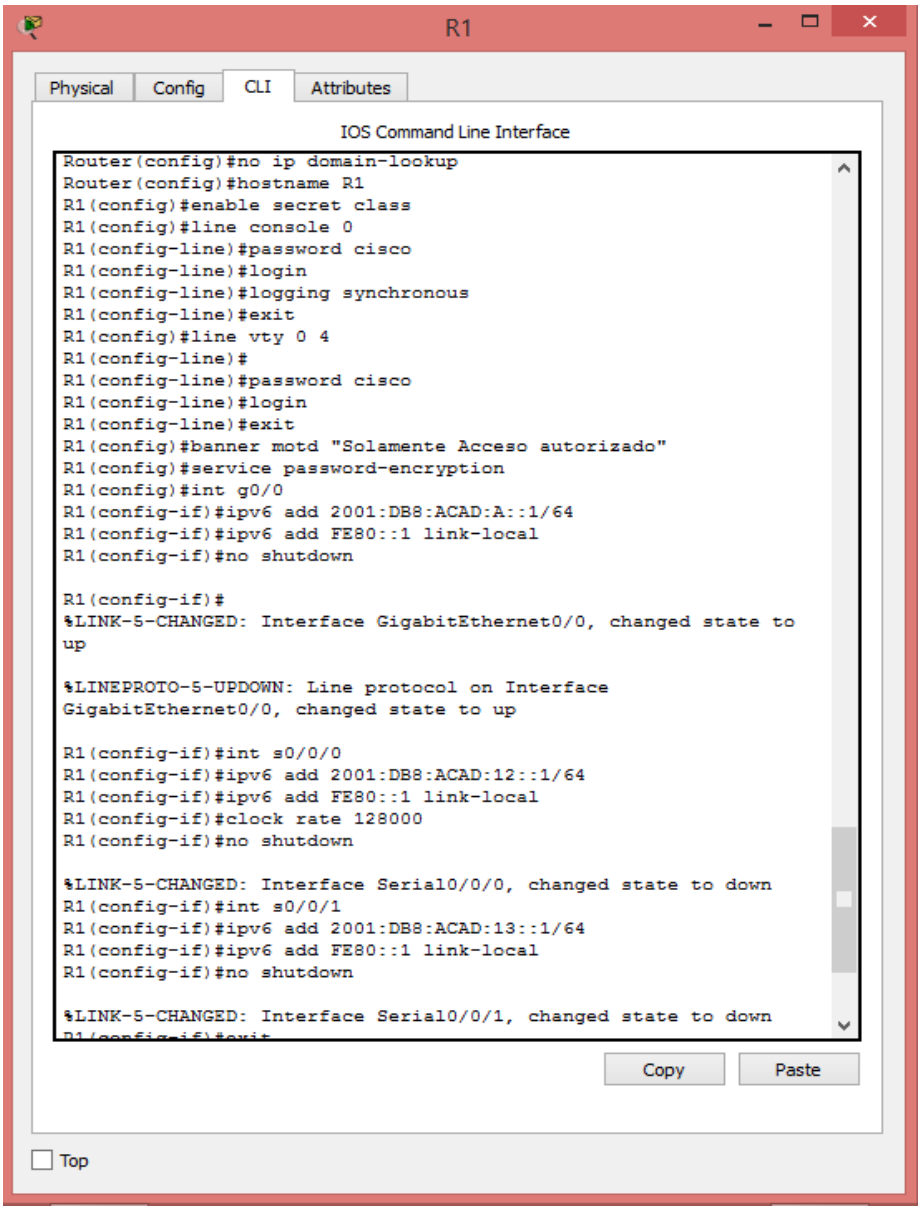
vii. Cifre las contraseñas de texto no cifrado.

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

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

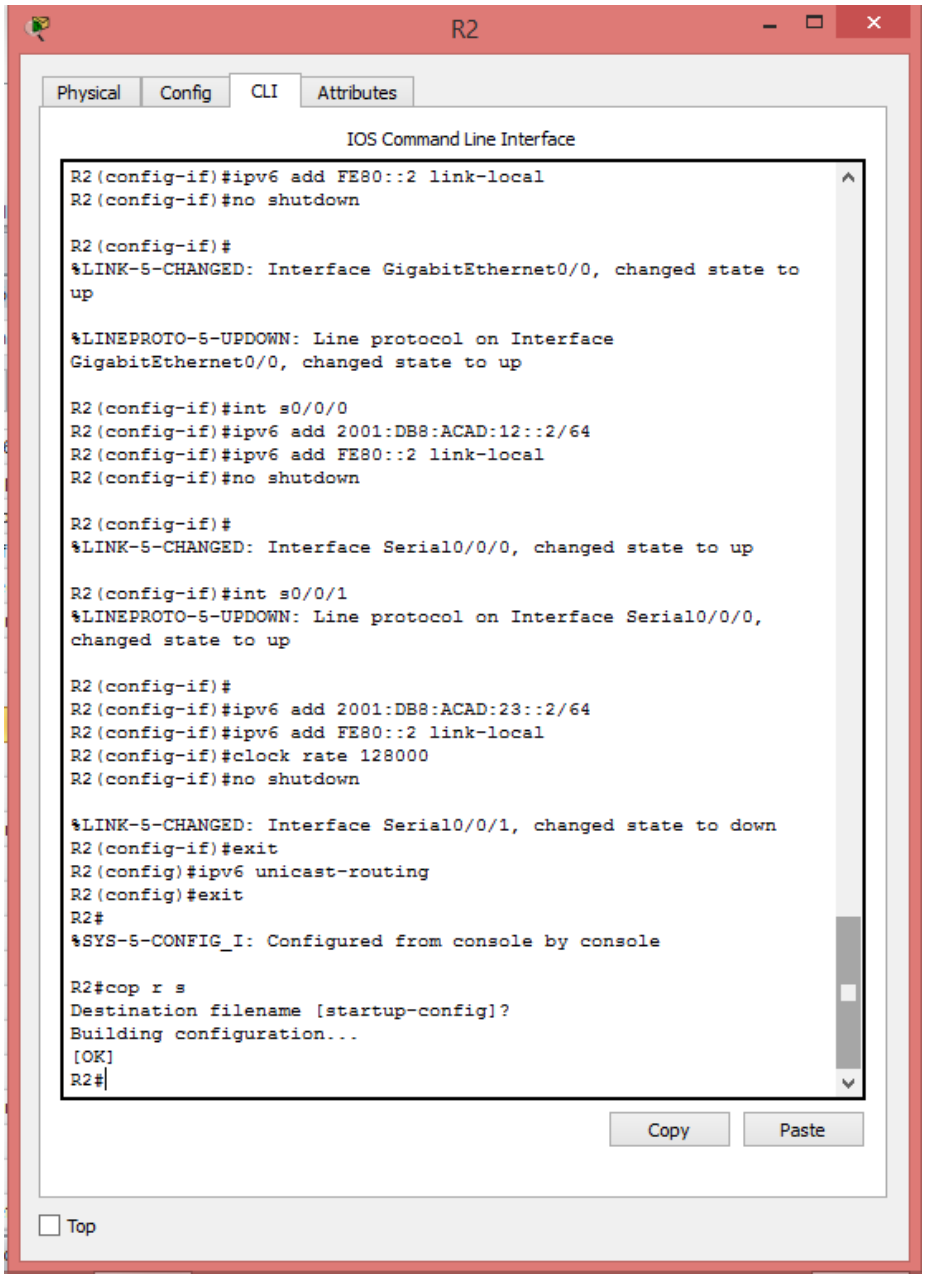
x. Copie la configuración en ejecución en la configuración de inicio

d.




Configuración básica R1

e.




Configuración básica R2

f.

g.

h.

i.

j.

k.

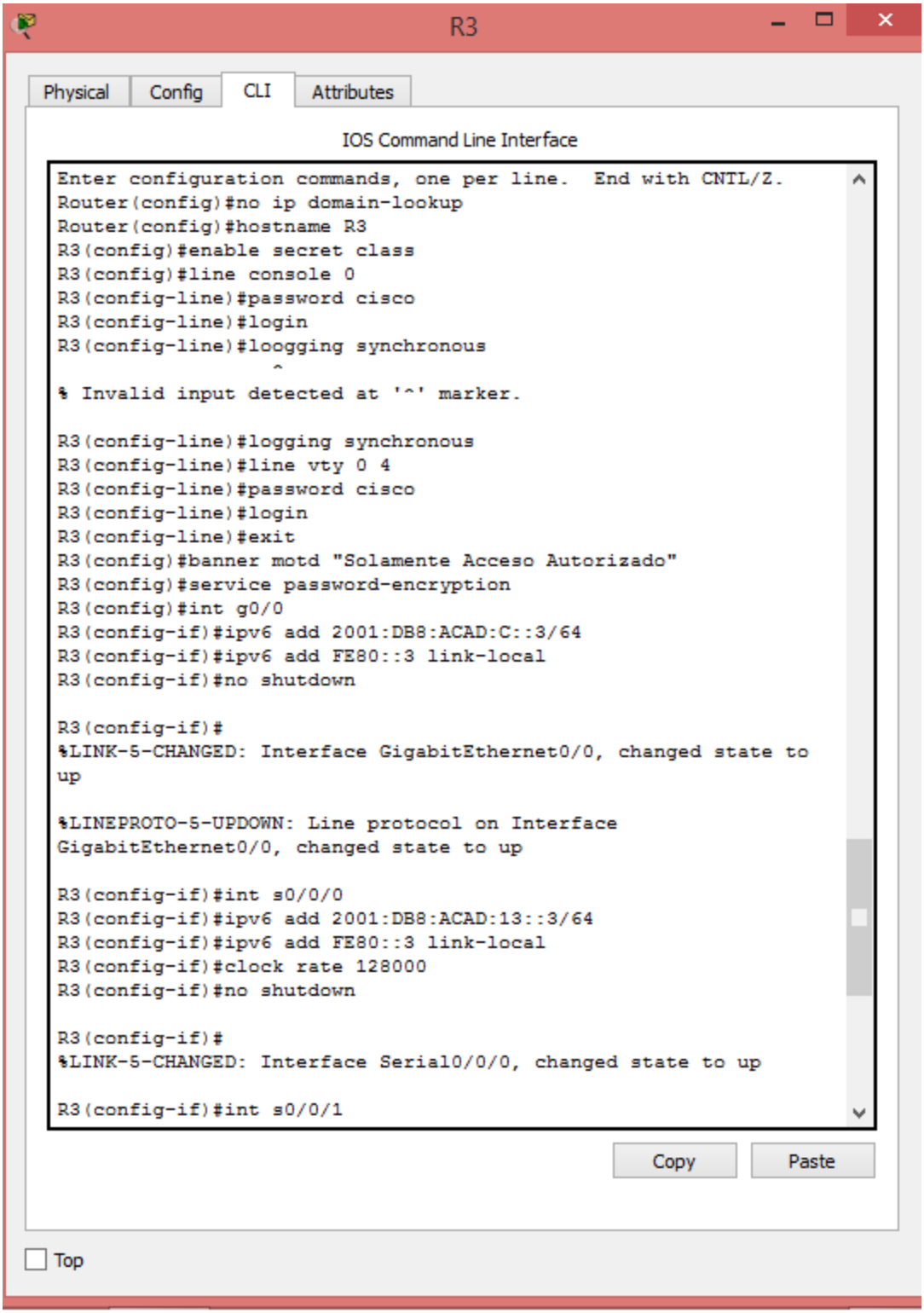
l.

m.

n.

o.

p.

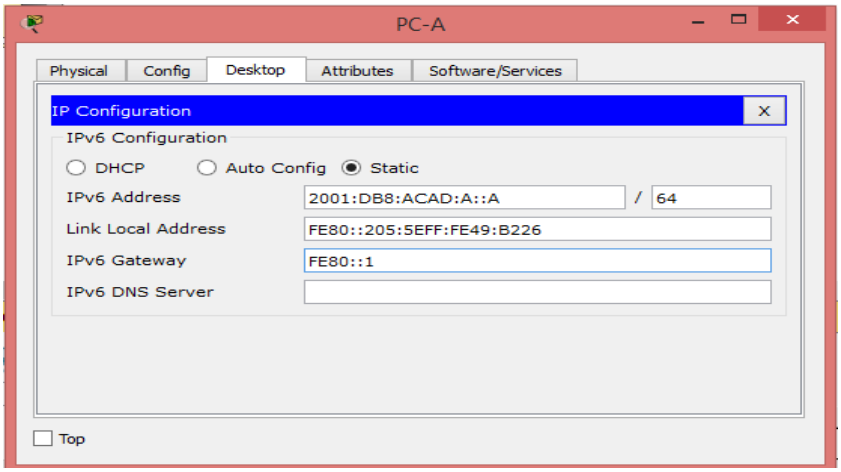

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#loogging synchronous
^
% Invalid input detected at '^' marker.
R3(config-line)#logging synchronous
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#banner motd "Solamente Acceso Autorizado"
R3(config)#service password-encryption
R3(config)#int g0/0
R3(config-if)#ipv6 add 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 add 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 add 2001:DB8:ACAD:13::3/64
R3(config-if)#ipv6 add 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
Copy
Paste
Top

q.

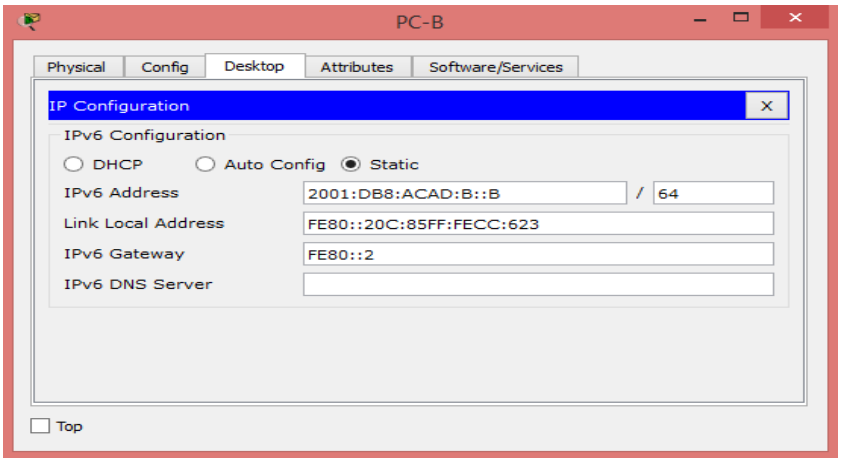
Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

Configuración básica R3

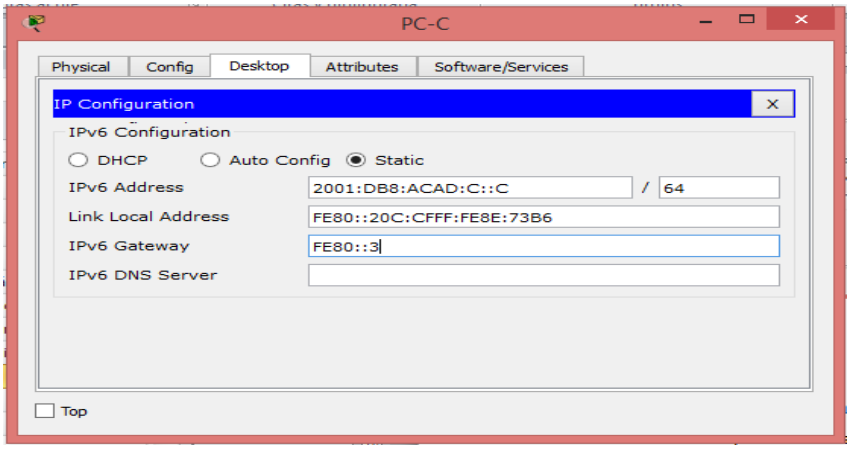
## Paso 1. configurar los equipos host.




PC-A




PC-B




PC-C

### Paso 2. 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.

```
R1>ping 2001:db8:acad:12::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:12::2, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6
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 =
1/4/10 ms
```

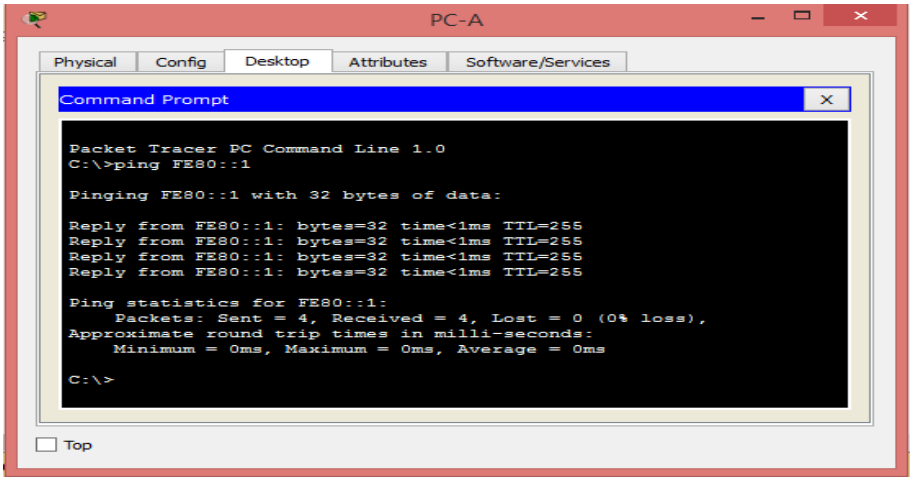
Prueba de Conectividad exitosa de R1 con R2 y R3

```
R2>ping 2001:db8:acad:12::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:12::1, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4
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 = 3/4/6
ms
```

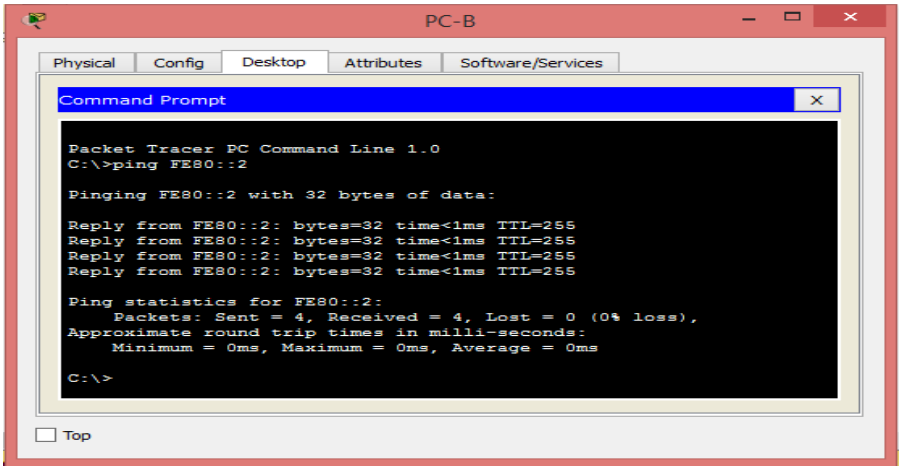
Prueba de Conectividad exitosa de R2 con R1 y R3

```
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 = 1/4/6
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 = 3/5/9
ms
```

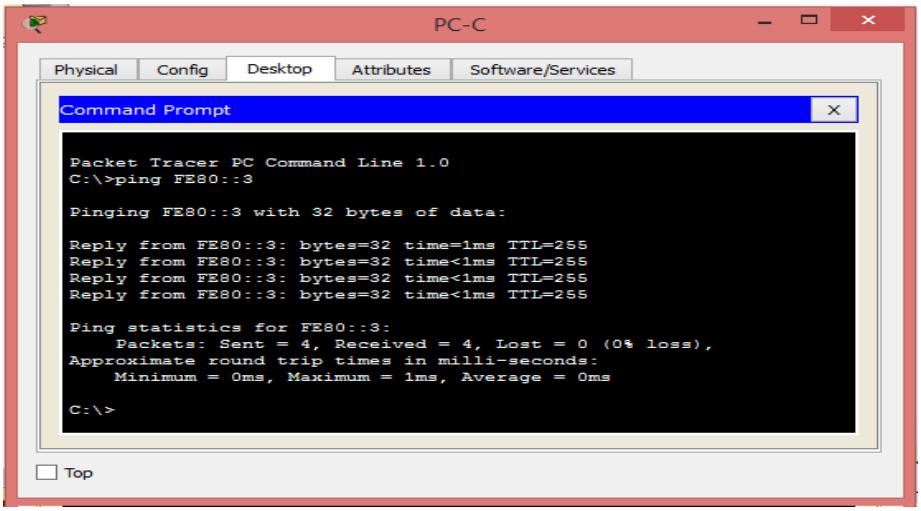
Prueba de Conectividad exitosa de R3 con R1 y R2




Prueba de Ping desde PC-A a R1 exitoso



Prueba de Ping desde PC-B a R2 exitoso




Prueba de Ping desde PC-C a R3 exitoso

## 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.

### Paso 1. asignar ID a los routers.

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

i. 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.

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

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

```
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-
id,please configure manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
```

Asignación del ID de proceso OSPFv3 al R1

iii. 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.

r.
```
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
```

Asignación del ID de proceso OSPFv3 al R2

s.
```
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
```

Asignación del ID de proceso OSPFv3 al R3

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

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

Verifcación ID R2

u.
```
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 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 Reference bandwidth unit is 100 mbps
```

Verifcación ID R1

v.
```
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 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 Reference bandwidth unit is 100 mbps
```

Verifcación ID R3

### Paso 2. configurar OSPFv6 en el R1.

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

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

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

Configuración OSPFv3 de G0/0 en R1

x.

**Nota**: la ID del proceso debe coincidir con la ID del proceso que usó en el paso 1a.

ii. 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.

y.
```
R2(config)#int g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#int s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#int s0/0/1
R2(config-if)#
02:09:53: %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
```

Configuración OSPFv3 de G0/0 en R2

z.
```
R3(config)#int g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int s0/0/1
02:11:10: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

R3(config-if)#int s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
```

Configuración OSPFv3 de G0/0 en R3

aa.

```
00:00:10: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

00:00:10: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
```

Mensajes de adyacencia recibidas en R1

### Paso 3. verificar vecinos de OSPFv3.

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

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

```
            OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
R1#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           0   FULL/  -        00:00:34    3               Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:31    3               Serial0/0/0
```

Verificación de vecindad de R1 con R2 y R3

### Paso 4. verificar la configuración del protocolo OSPFv3.

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

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

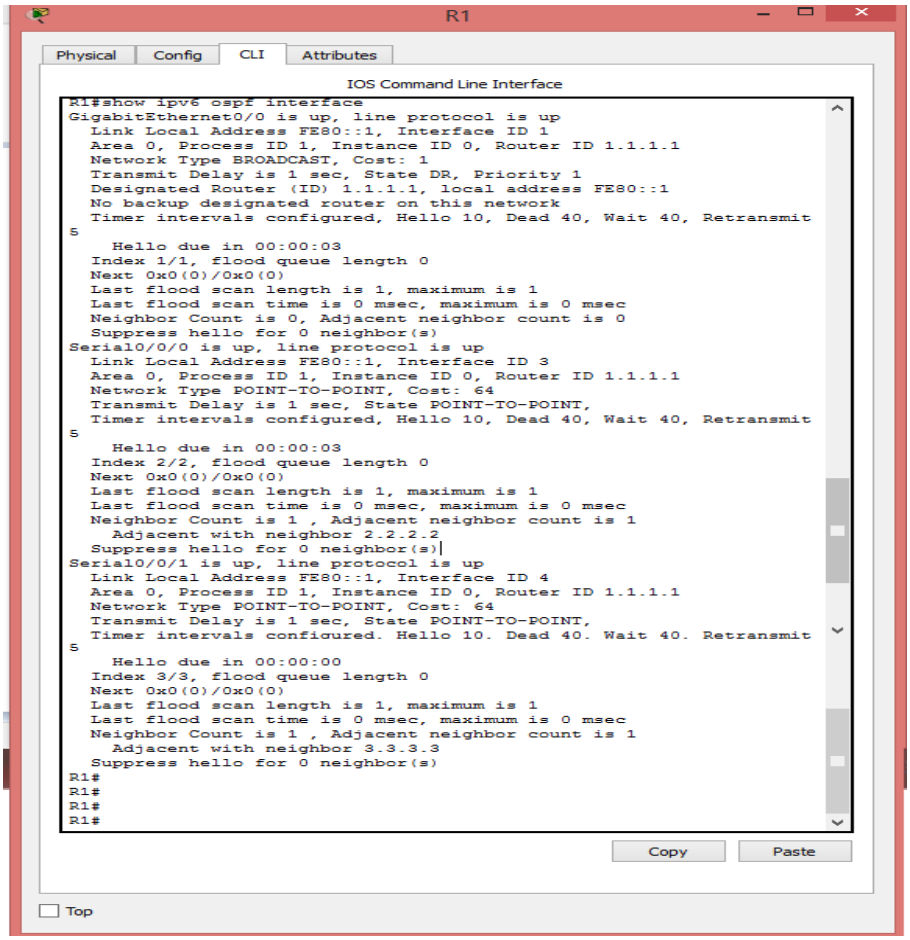
Verificación del protocolos OSPFv3

### Paso 5. verificar las interfaces OSPFv3.

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

bb.

cc.




Lista detallada interfaces OSPF en R1

dd.

ii. 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
```

### Paso 6. verificar la tabla de routing IPv6.

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

```
R2#show ipv6 route
IPv6 Routing Table - 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::3, Serial0/0/1
     via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Tabla de routing de R2

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

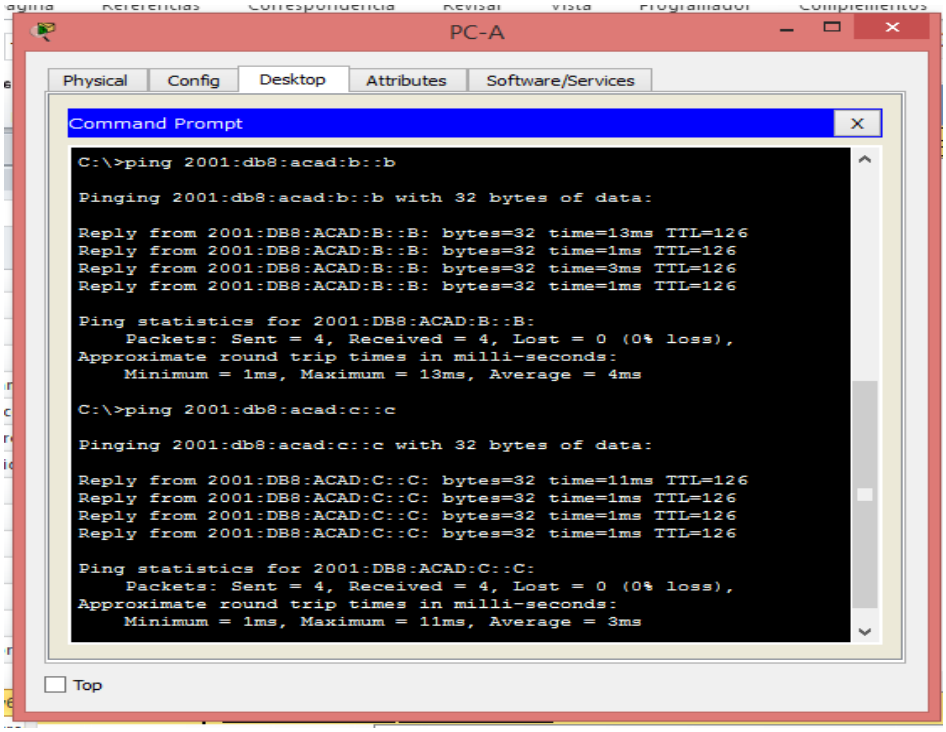
Show ipv6 route ospf

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

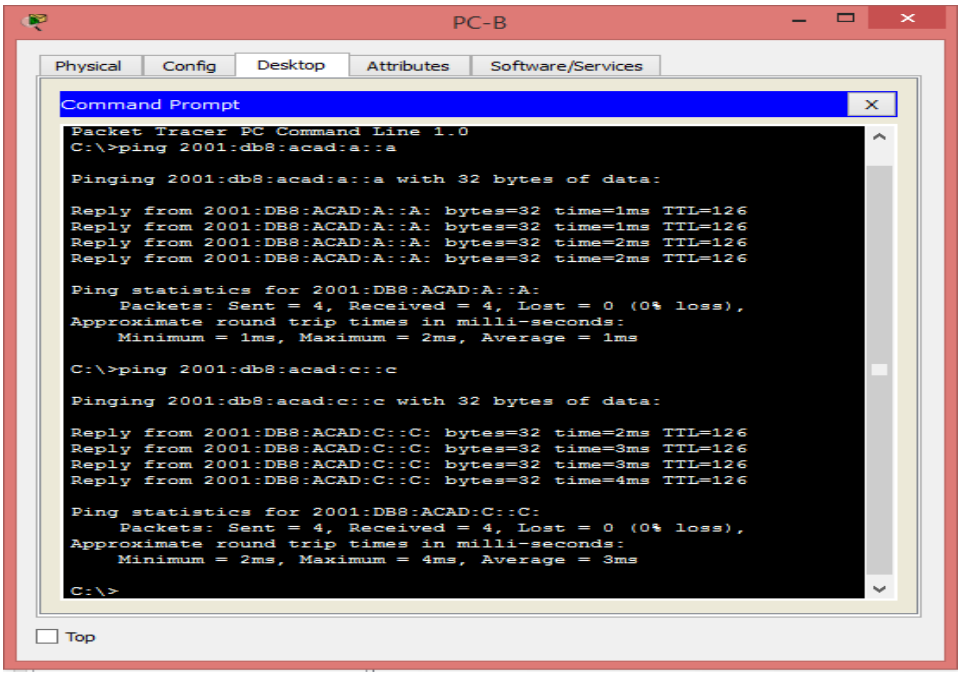
Tabla de routing con solo OSPF

### Paso 7. Verificar la conectividad de extremo a extremo.

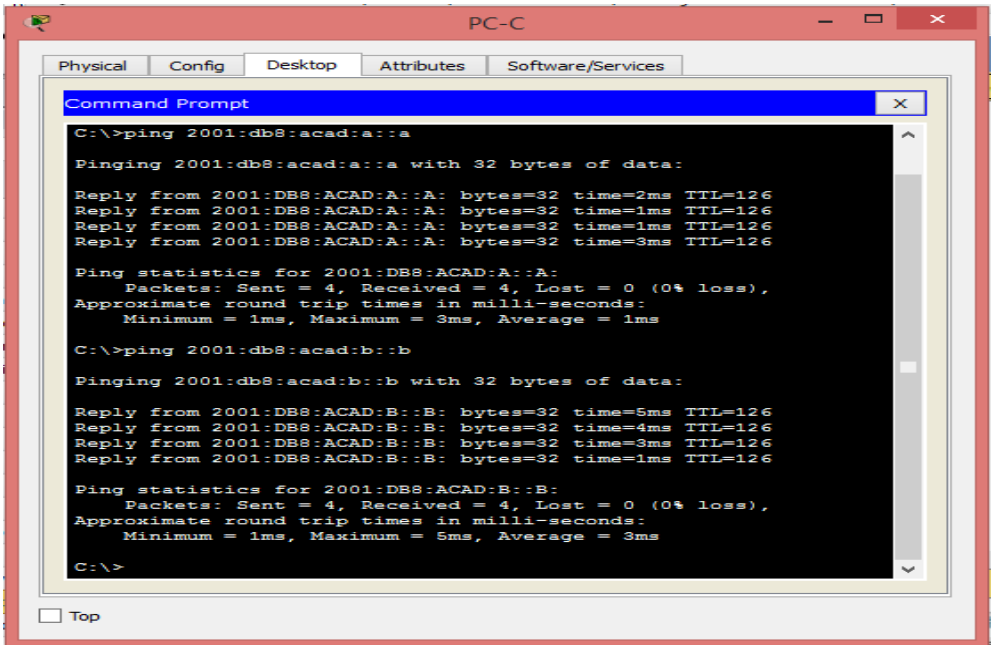
Se debería poder hacer ping entre todas las computadoras de la topología. Verifique y resuelva los problemas, si es necesario.




Prueba de conectividad de extremos PC-A exitosa




Prueba de conectividad de extremos PC-B exitosa




Prueba de conectividad de extremos PC-C exitosa

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

## 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.

### Paso 1. configurar una interfaz pasiva.

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

```
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 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 00:00:00
  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)
```

ee.

ff. Verificación interfaz G0/0 en estado active en R1

gg.

ii. 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-rtr)#exit
R1(config)#exit
```

hh.

Configuración interfaz G0/0 como pasiva en R1

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

```
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 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)
```

ii.

Verificación interfaz G0/0 en estado pasivo en R1

jj.

iv. 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.

kk.

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

Verificando ruta disponible a a la red 2001:DB8:ACAD:A::/64. En R2

ll.

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

Verificando ruta disponible a a la red 2001:DB8:ACAD:A::/64. En R3

**Paso 2. establecer la interfaz pasiva como la interfaz predeterminada en el router.**

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

mm.

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
01:01:43: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached

01:01:43: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
```

Estableciendo la interfaz pasiva como predeterminada en R2

ii. 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.

nn.

```
R1#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           0   FULL/  -        00:00:34    3               Serial0/0/1
```

Efecto de la interfaz pasiva predeterminada en R1

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

oo.

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

Verificación interfaz S0/0/0 en R2 como pasiva

iv. 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**.

pp.

```
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
```

Red 2001:DB8:ACAD:B::/64 fuera de la tabla de routing en R1

qq.

```
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
```

Red 2001:DB8:ACAD:B::/64 fuera de la tabla de routing en R3

v. 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.

rr.

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
01:10:31: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done
```

Activación de la interfaz S0/0/1 en R2

vi. 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.

ss.

```
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]
```

Red 2001:DB8:ACAD:B::/64 en la tabla de routing en R1

tt.

```
R1#show ipv6 ospf neighbor

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

R1 sin vecindad con R2

uu.

```
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
```

Red 2001:DB8:ACAD:B::/64 en la tabla de routing en R3

vv.

```
R3#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
1.1.1.1           0   FULL/  -        00:00:32    4               Serial0/0/0
2.2.2.2           0   FULL/  -        00:00:34    4               Serial0/0/1
```

Vecindad de R3 con R2

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64? S0/0/1

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

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

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

¿Qué indica esta información?

Lo anterior nos indica que la interfaz S0/0/0 de R2 todavía está configurada como pasiva, por lo tanto no hay tráfico hacia ella. Debido a lo anterior entonces el valor de la métrica de 129 es porque el costo de la interfaz S0/0/1 de R1 vale 64 y el costo de la interfaz S0/0/1 de R3 vale 64 más el costo de la interfaz G0/0 que vale 1 entonces dá: 64+64+1 =129 y ésta será la ruta para la red red 2001:DB8:ACAD:B::/64

vii. 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.

ww.

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#
01:35:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
```

Activación de interfaz S0/0/0 en R2

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

```
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           0   FULL/  -        00:00:33    3               Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:32    3               Serial0/0/0
```

Restauración de la vecindad de R2 con R1

## e. Reflexión

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

Si porque no es necesario que la ID de proceso de un router coincida con la ID de proceso de otro u otros routers, ya que la ID del proceso OSPFv3 se usa sólo localmente

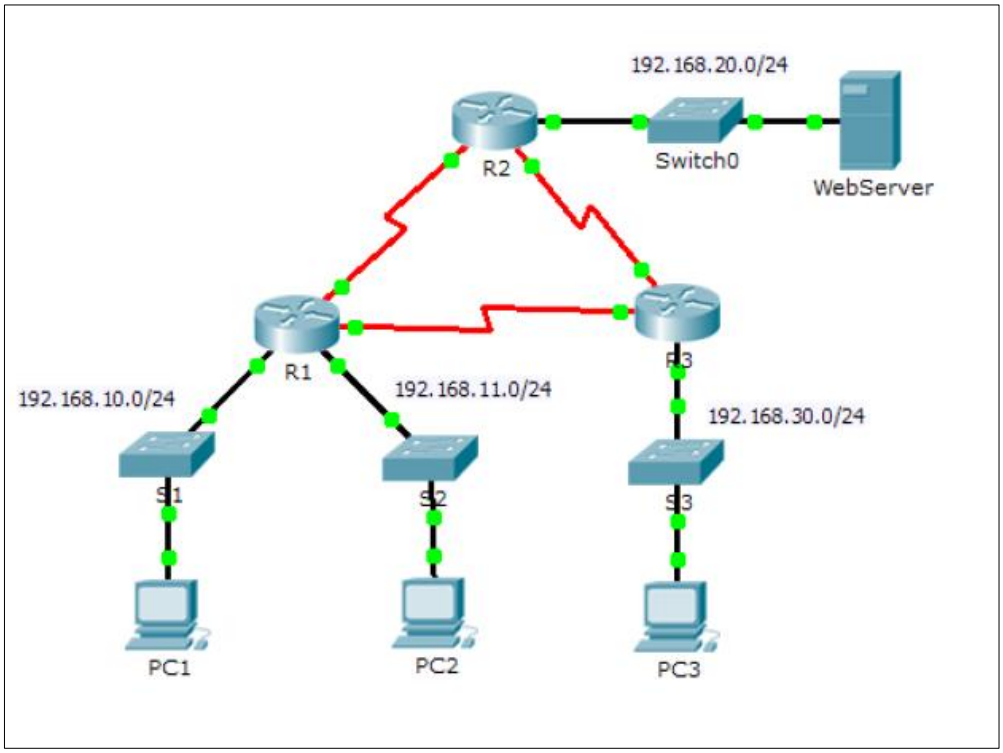
b. ¿Cuál podría haber sido la razón para eliminar el comando **network** en OSPFv3?

Porque con su eliminación se evitan los errores en la dirección IPv6

## f. 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 Instructions IG**




| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| R1 | F0/0 | 192.168.10.1 | 255.255.255.0 | N/A |
| | F0/1 | 192.168.11.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A |
| | S0/0/1 | 10.3.3.1 | 255.255.255.252 | N/A |
| R2 | F0/0 | 192.168.20.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| R3 | F0/0 | 192.168.30.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 10.3.3.2 | 255.255.255.252 | N/A |
| | S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A |

| | | | | |
|---|---|---|---|---|
| PC1 | NIC | 192.168.10.10 | 255.255.255.0 | 192.168.10.1 |
| PC2 | NIC | 192.168.11.10 | 255.255.255.0 | 192.168.11.1 |
| PC3 | NIC | 192.168.30.10 | 255.255.255.0 | 192.168.30.1 |
| WebServer | NIC | 192.168.20.254 | 255.255.255.0 | 192.168.20.1 |

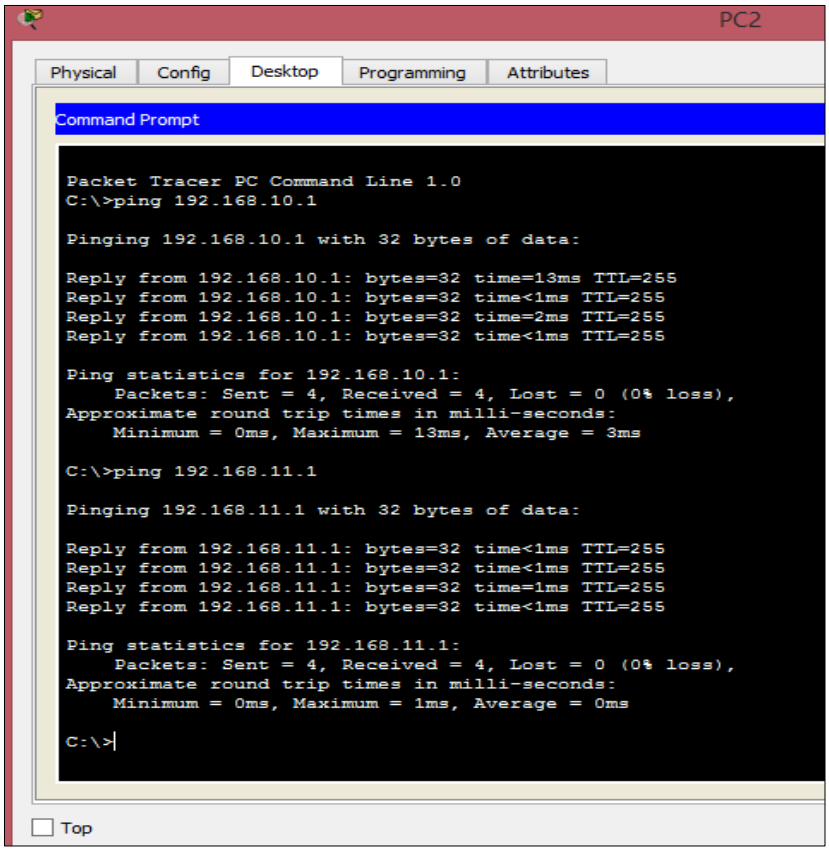
**Objetivos**

**Part 1:** Plan an ACL Implementation
**Part 2:** Configure, Apply, and Verify a Standard ACL

**Part 1: Plan an ACL Implementation**

**Step 1:** Investigate the current network configuration.

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



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

a. The following network policies are implemented on R2:

- ✓ The 192.168.11.0/24 network is not allowed access to the WebServer on the 192.168.20.0/24 network.
- ✓ All other access is permitted.

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

b. The following network policies are implemented on R3:

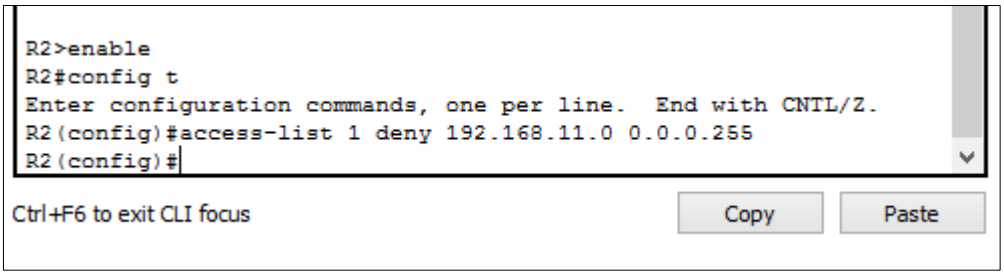
- ✓ The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
- ✓ All other access is permitted.

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

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

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

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



b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:

```
R2>enable
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#
```

Ctrl+F6 to exit CLI focus  Copy  Paste

c. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

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

Ctrl+F6 to exit CLI focus  Copy  Paste

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

a. Create an ACL using the number 1 on R3 with a statement that denies access to the 192.168.30.0/24 network from the PC1 (192.168.10.0/24) network.

```
R3>enable
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 1 deny 192-168-10.0 0.0.0.255
                               ^
% Invalid input detected at '^' marker.

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

Ctrl+F6 to exit CLI focus  Copy  Paste

b. b. By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, create a second rule for ACL 1.

```
R3>enable
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 1 deny 192-168-10.0 0.0.0.255
                               ^
% Invalid input detected at '^' marker.

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

c. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface

```
R3>enable
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 1 deny 192-168-10.0 0.0.0.255
                               ^
% Invalid input detected at '^' marker.

R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
```

Ctrl+F6 to exit CLI focus  Copy  Paste

**Step 3:** Verify ACL configuration and functionality.

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

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

R2#
```

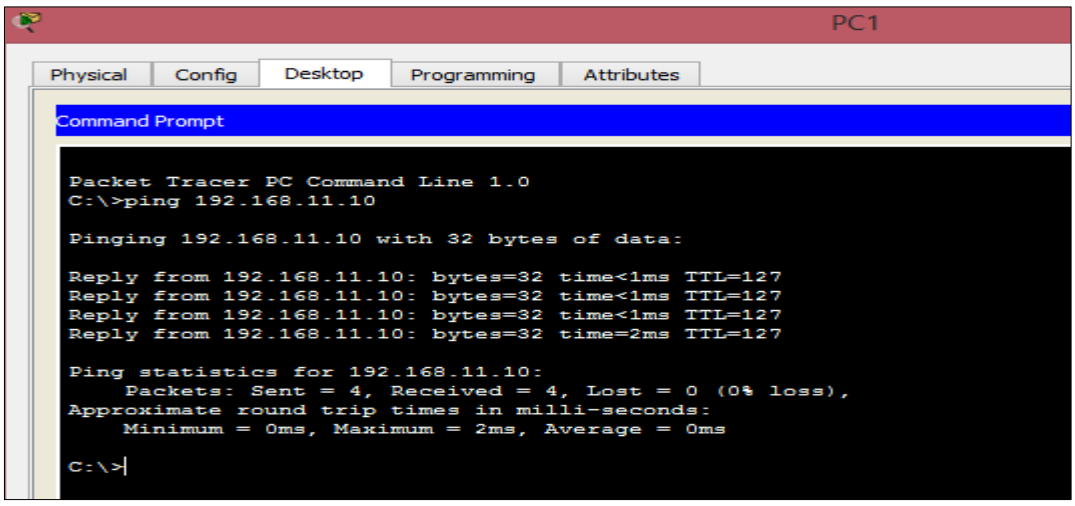
Ctrl+F6 to exit CLI focus  Copy  Paste

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

R3#
```

Ctrl+F6 to exit CLI focus  Copy  Paste

b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:

✓ ping from 192.168.10.10 to 192.168.11.10 succeeds.




✓ A ping from 192.168.10.10 to 192.168.20.254 succeeds.

```
C:\>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=10ms TTL=126
Reply from 192.168.20.254: bytes=32 time=2ms 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 = 10ms, Average = 4ms

C:\>
```

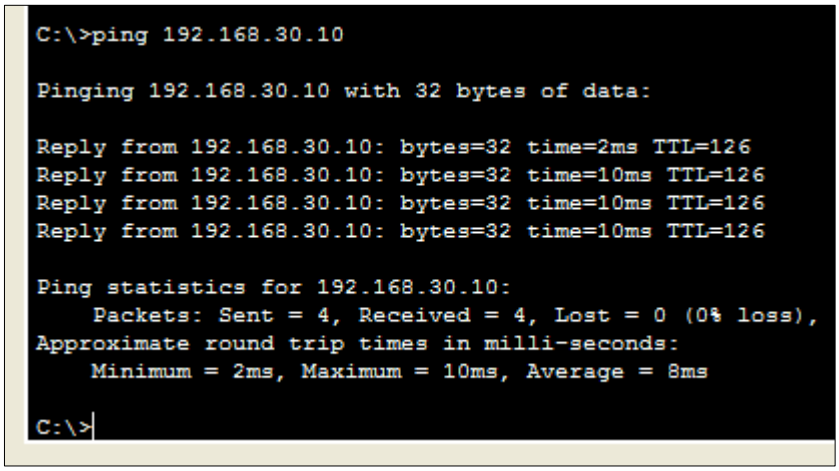
- ✓ A ping from 192.168.11.10 to 192.168.20.254 fails.

```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

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

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

C:\>
```

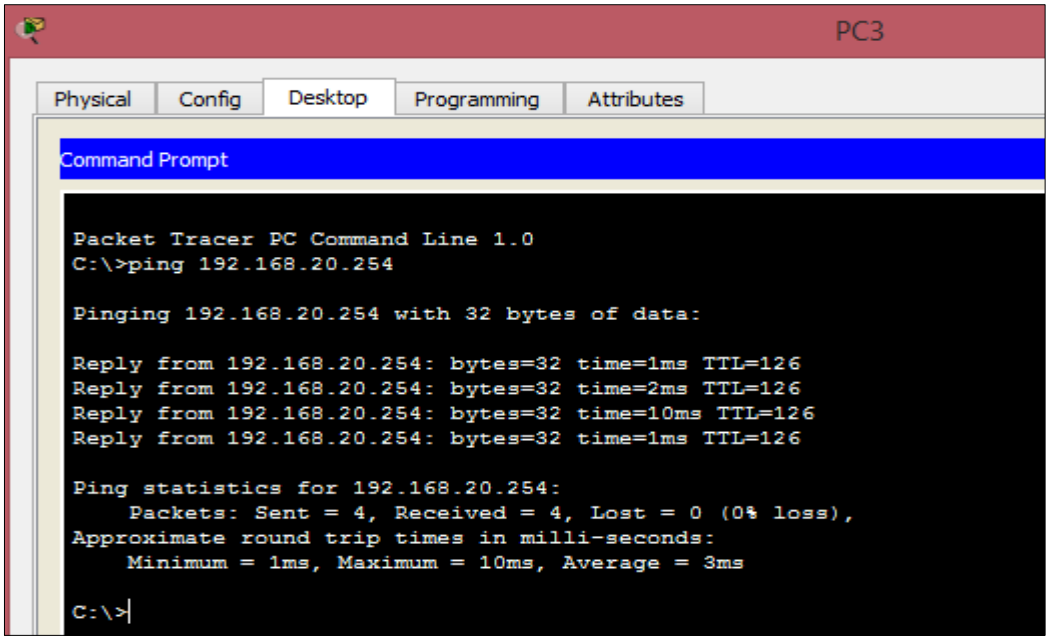
- ✓ A ping from 192.168.10.10 to 192.168.30.10 fails.

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

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

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

C:\>
```

- ✓ A ping from 192.168.11.10 to 192.168.30.10 succeeds

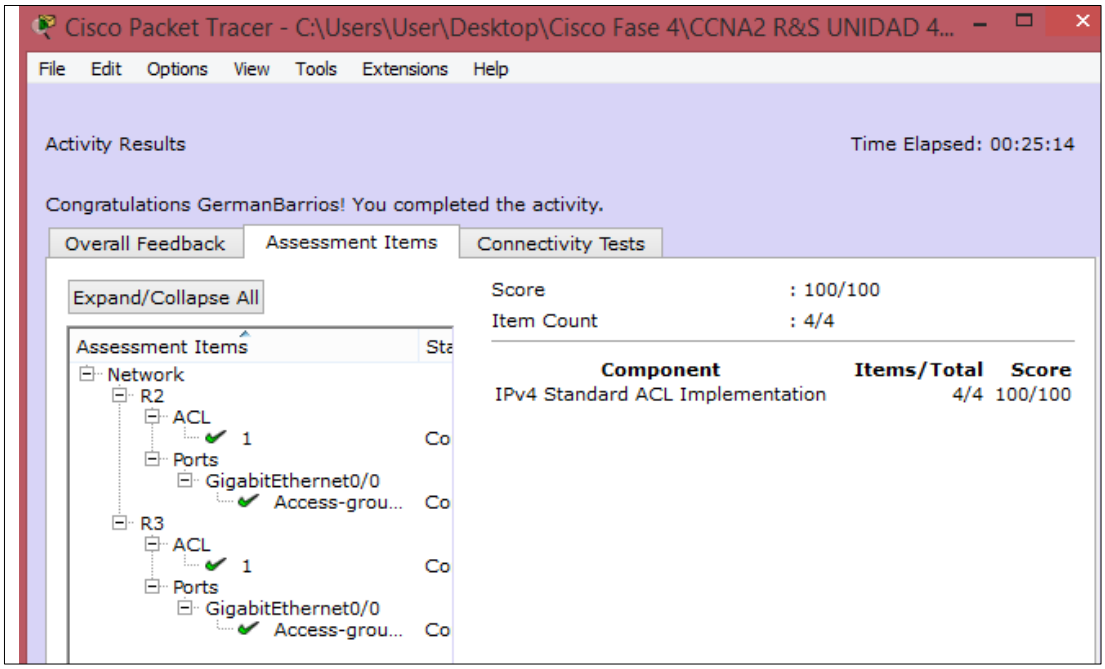



- ✓ A ping from 192.168.30.10 to 192.168.20.254 succeeds



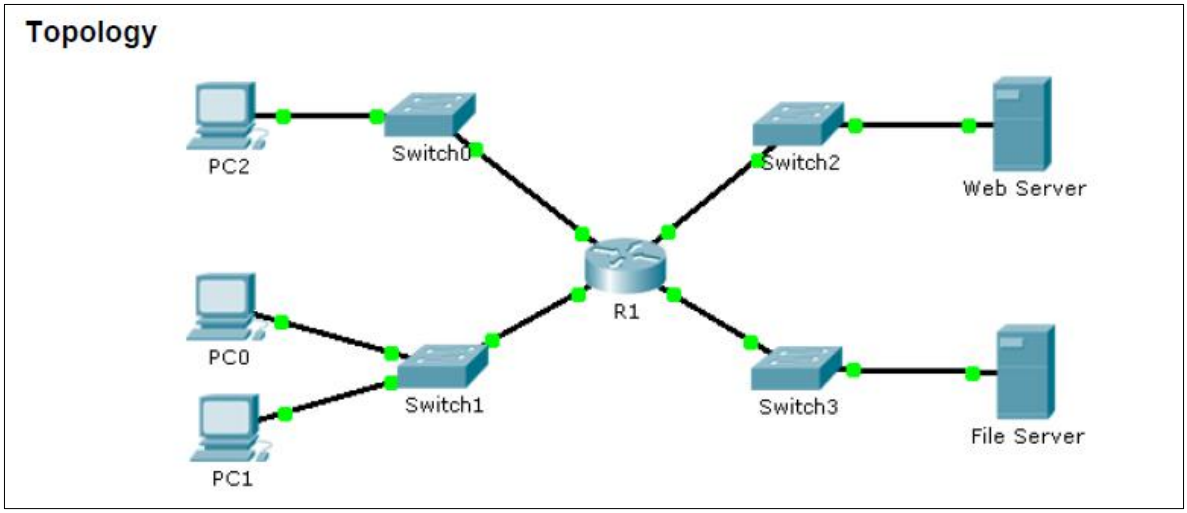

**Resultados**

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2



Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

# 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs Instructions IG




| 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**

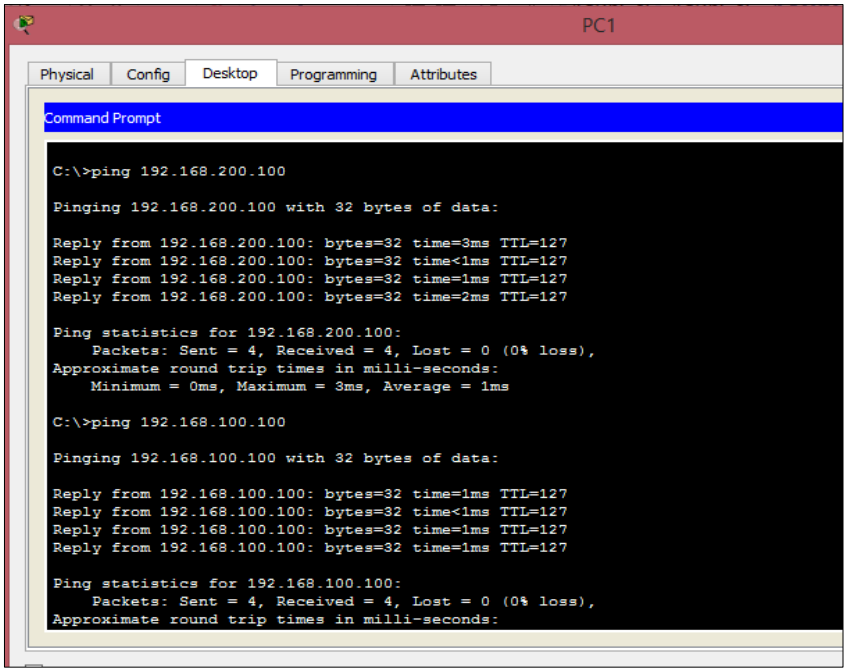
Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

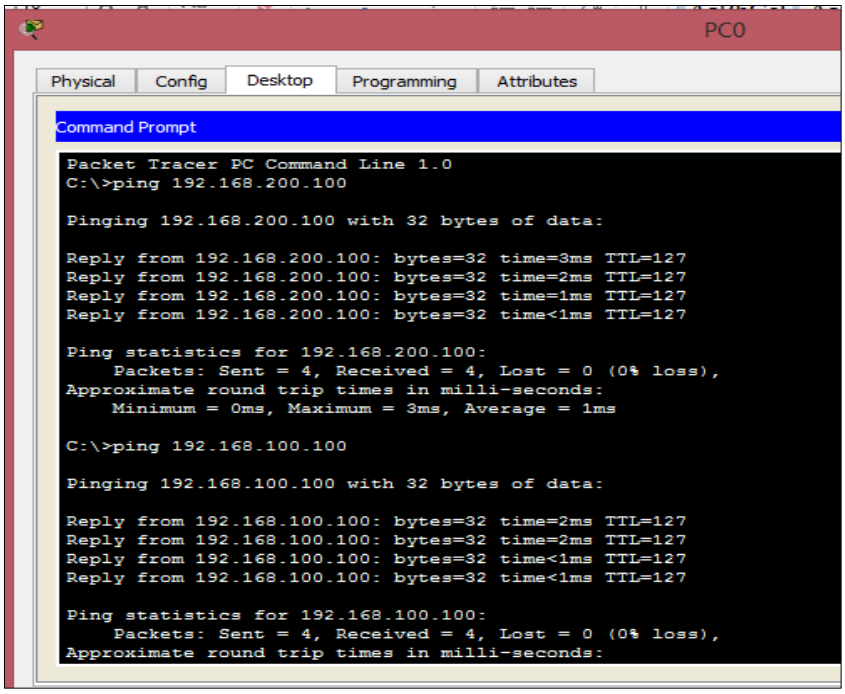
The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied access.

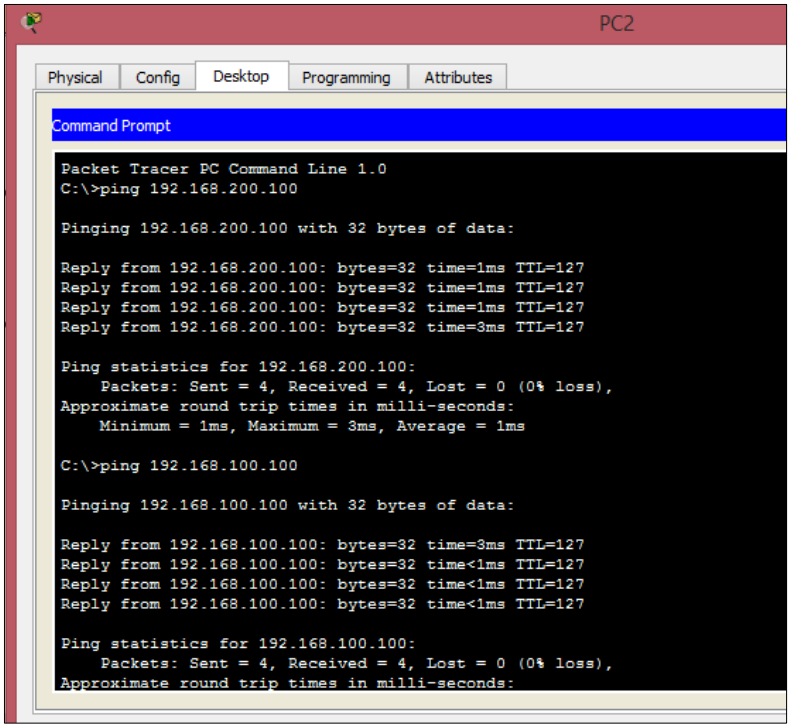
**Part 1: Configure and Apply a Named Standard ACL**

**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






**Step 2:** Configure a named standard ACL.

```
R1>enable
R1#config 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)#
```

Ctrl+F6 to exit CLI focus  Copy  Paste

**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)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Ctrl+F6 to exit CLI focus  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.

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

R1#
```

Ctrl+F6 to exit CLI focus Copy

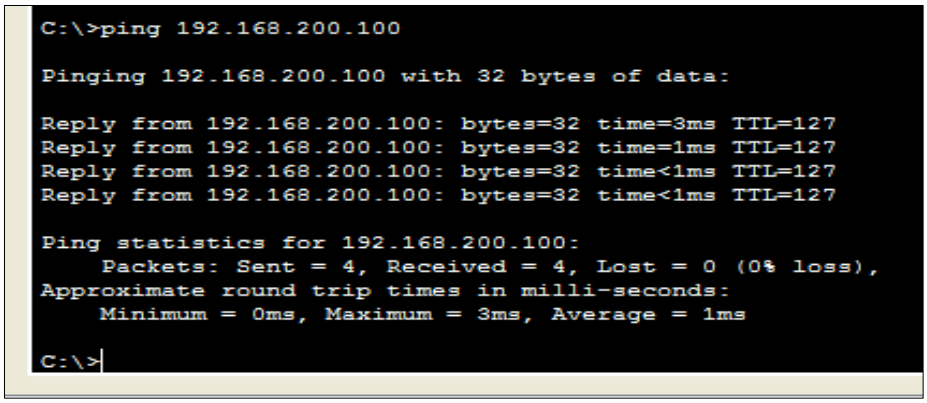
```
R1#show ip interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.200.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is File_Server_Restrictions
  Inbound  access list is not set
  Proxy ARP is enabled
```

Ctrl+F6 to exit CLI focus Copy Paste

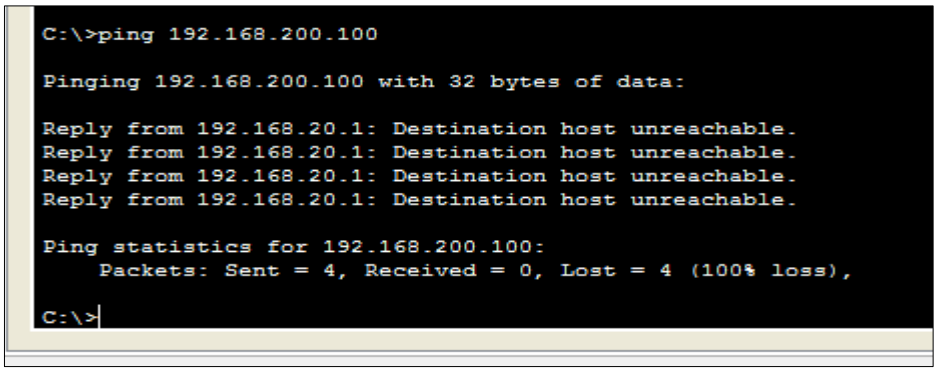
**Step 2:** Verify that the ACL is working properly.

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

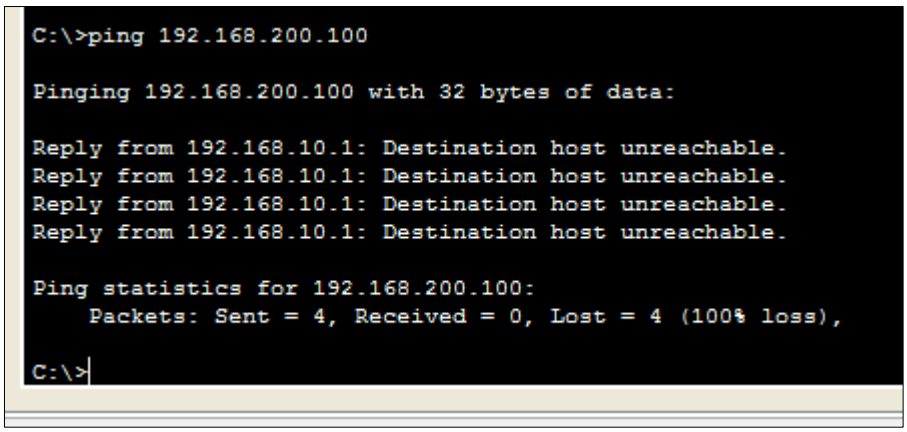
**PC 1 ping hacia File Server**




**PC0 ping hacia File Server**

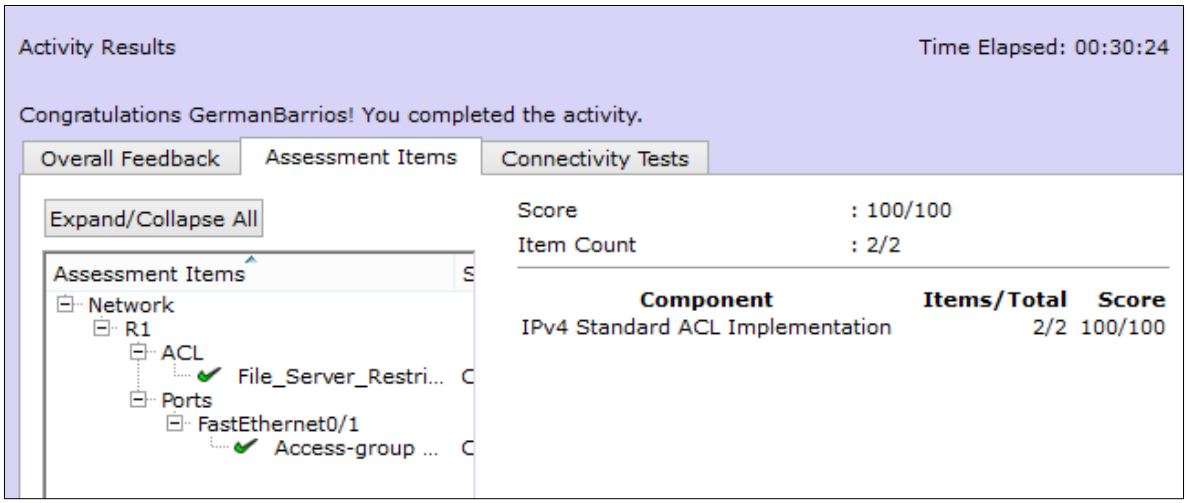



**PC2 ping hacia File server**



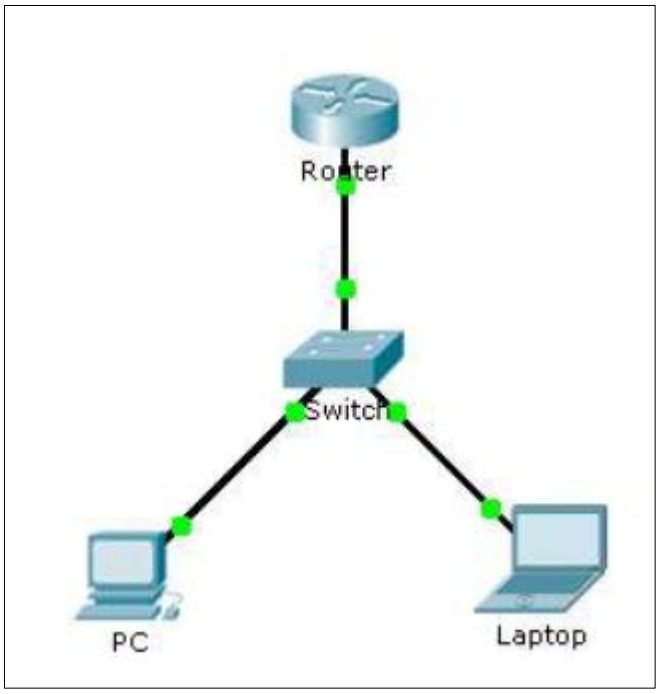

**Resultados**

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2




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

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2




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

**Objectives**

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

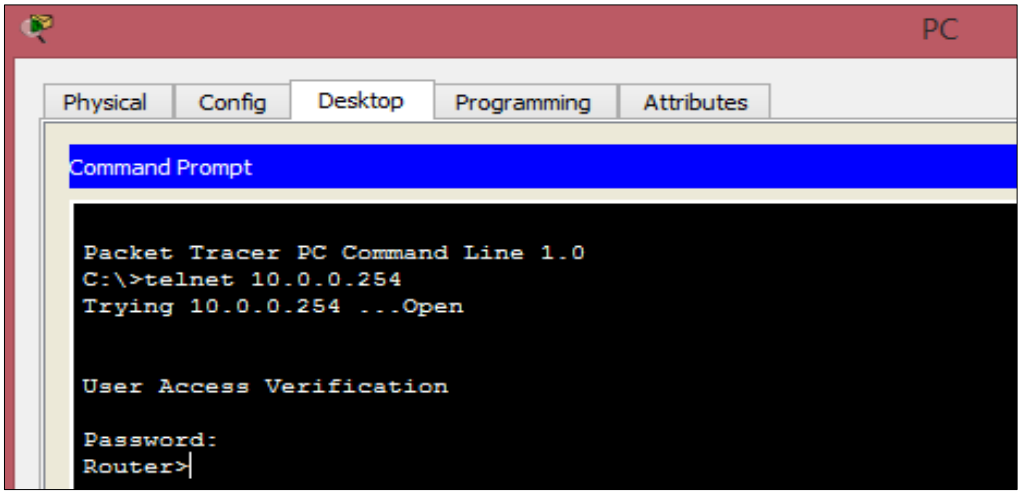
**Background**

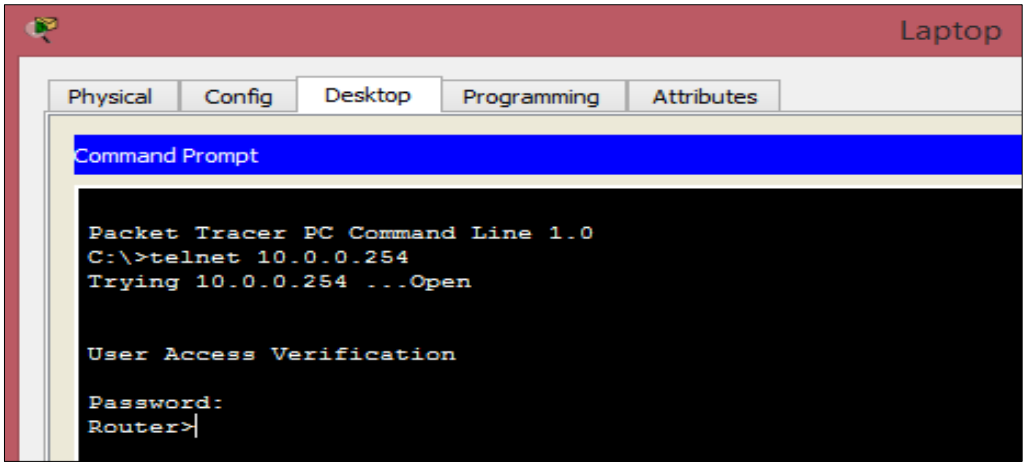
As network administrator, you must have remote access to your router. This access should not be available to other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows PC access to the Telnet lines, but denies all other source IP addresses.

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

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

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




**Step 2:** Configure a numbered standard ACL.

Configure the following numbered ACL on Router.

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

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

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#
```

Ctrl+F6 to exit CLI focus

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

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

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

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#exit
Router(config)#
```

Ctrl+F6 to exit CLI focus

**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.

```
Router#show access-lists
Standard IP access list 99
    10 permit host 10.0.0.1

Router#
```

Ctrl+F6 to exit CLI focus

**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.

**PC ping hacia el router**

```
C:\>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time=1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

**PC acceso por telnet al router**

```
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open


User Access Verification

Password:
Router>
```

Top

**Laptop ping hacia el router**

```
C:\>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Laptop acceso por telnet al router**

```
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
C:\>
```

**Resultados**

Activity Results — Time Elapsed: 00:13:09

Congratulations GermanBarrios! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

| Assessment Items | Sta |
|---|---|
| Network | |
| Router | |
| ACL | |
| 99 | Cor |
| VTY Lines | |
| VTY Line 0 | |
| Access Cont... | Cor |
| VTY Line 1 | |
| Access Cont... | Cor |
| VTY Line 2 | |
| Access Cont... | Cor |
| VTY Line 3 | |
| Access Cont... | Cor |
| VTY Line 4 | |
| Access Cont... | Cor |

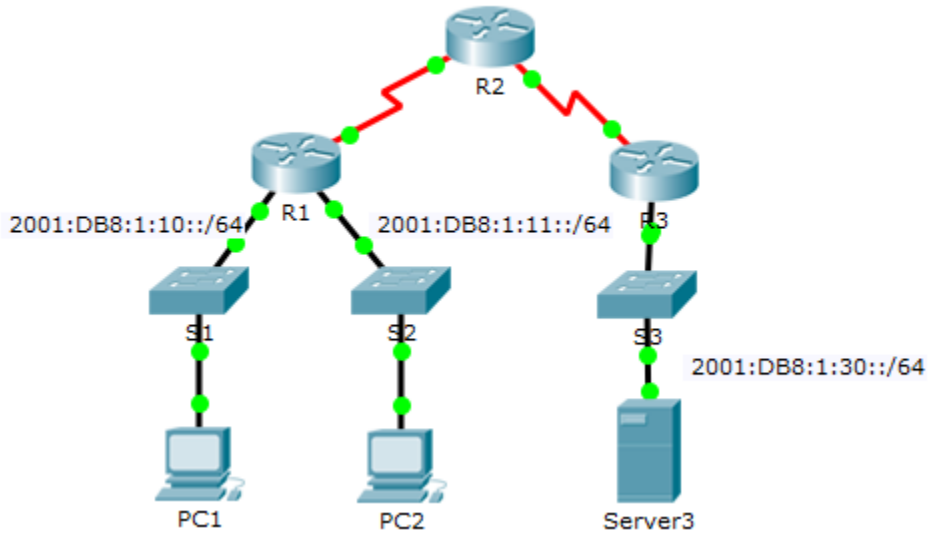
Score : 100/100

Item Count : 6/6

| Component | Items/Total | Score |
|---|---|---|
| IPv4 Standard ACL Implementation | 6/6 | 100/100 |

# 9.5.2.6 PACKET TRACER: Configuring IPV6 ACLs

## Topología




Topología

Tabla de direccionamiento 9.5.2.6

| Device | Interface | IP Address | 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
```

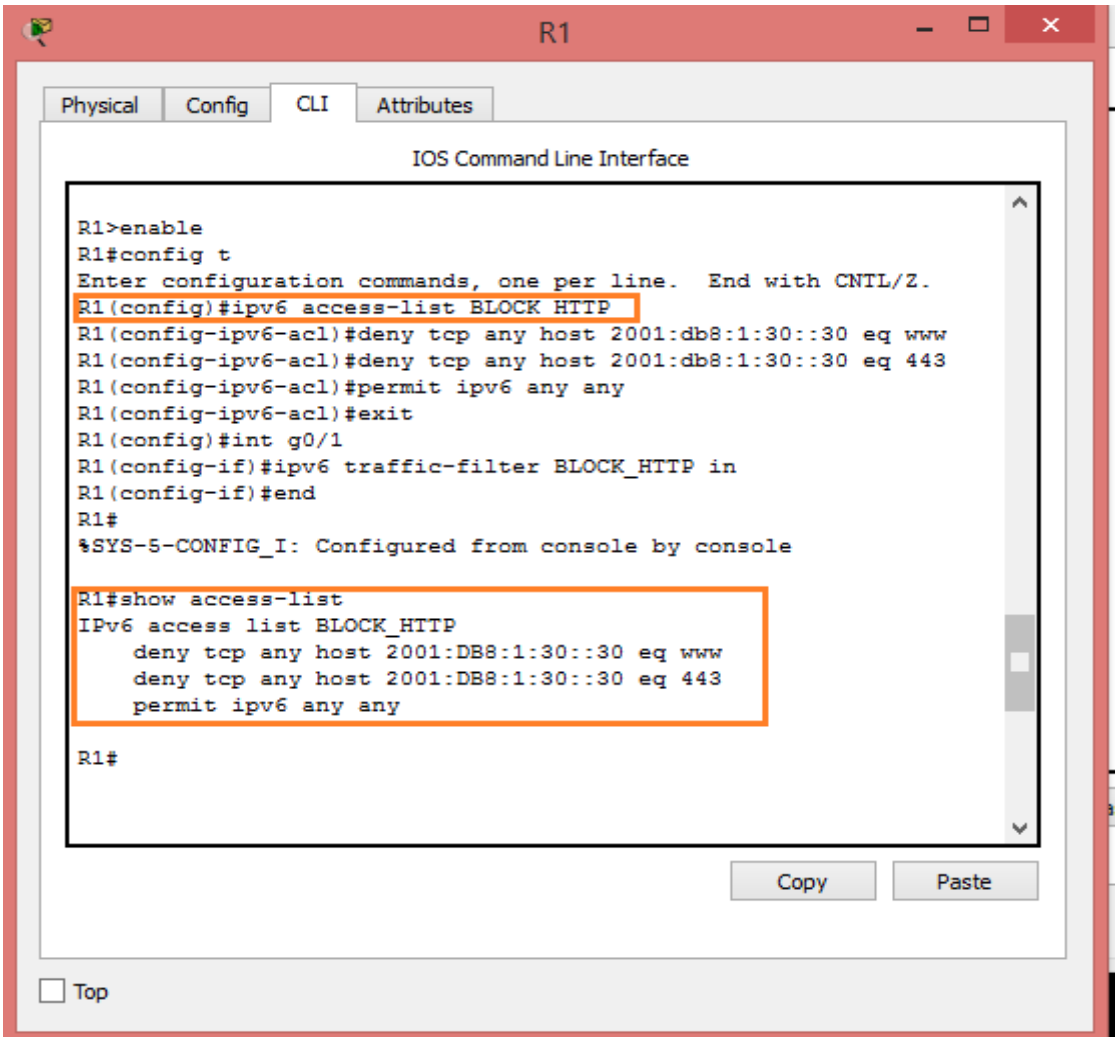
b. Allow all other IPv6 traffic to pass.

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

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

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

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

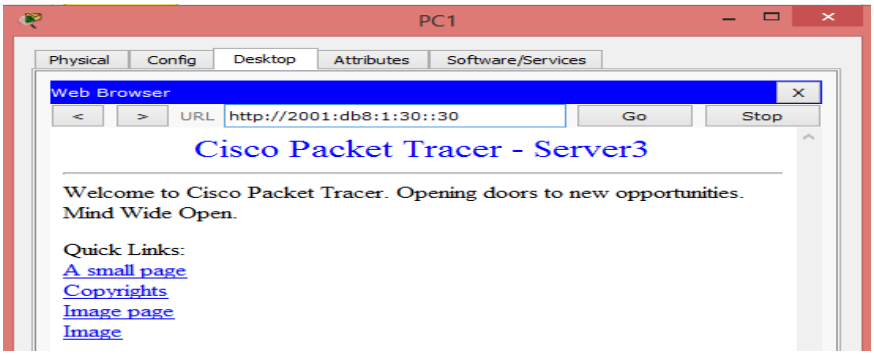



Configuración de la ACL para bloque de HTTP en R1

**Step 3: Verify the ACL implementation.**

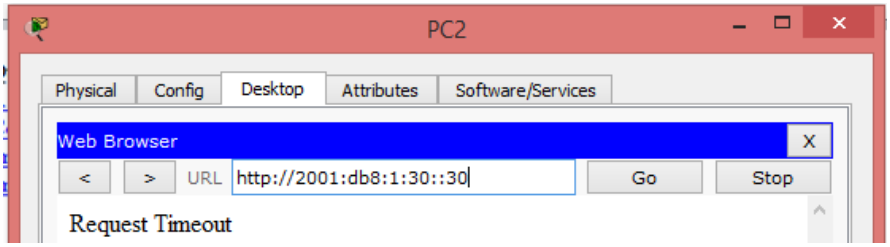
Verify the ACL is operating as intended by conducting the following tests:

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



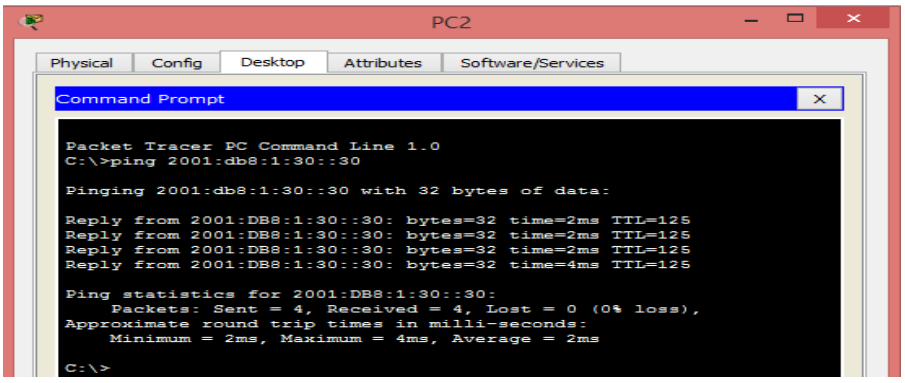

Verificación de acceso al servidor 3 desde PC1

- 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




Acceso al Servidor 3 desde PC2 bloqueado

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




Tráfico IPV6 desde PC2 al servidor funcional

## 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.

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

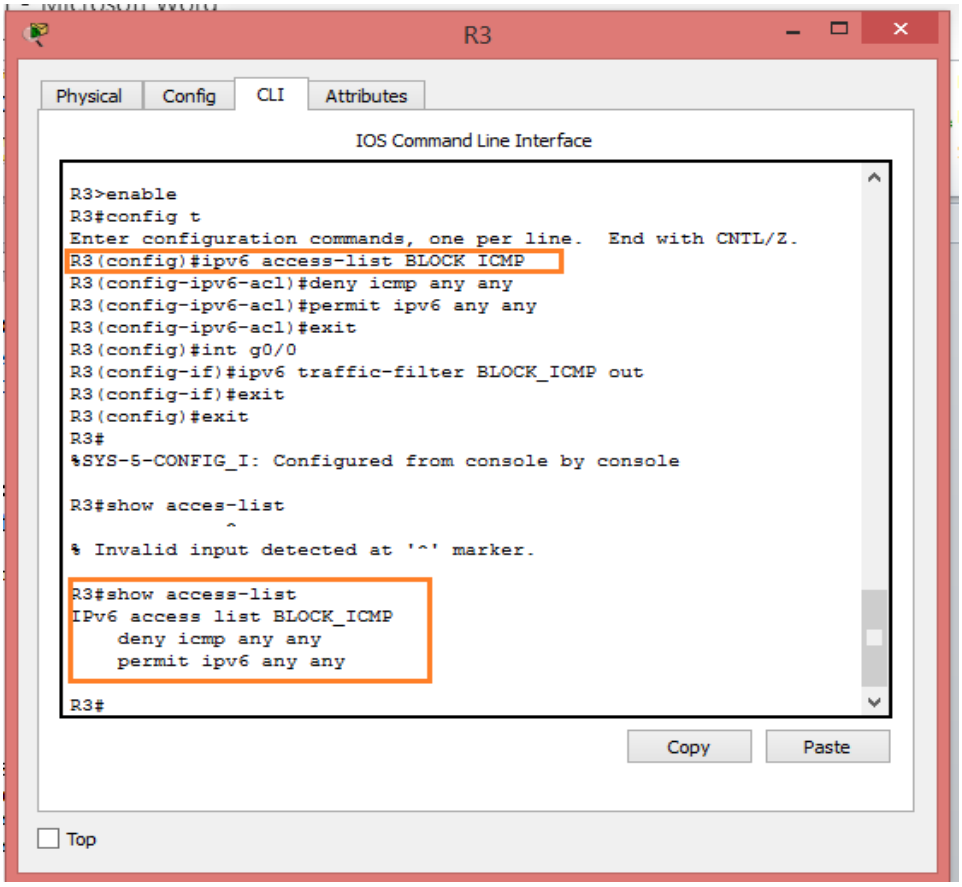
b. Allow all other IPv6 traffic to pass.

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

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

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

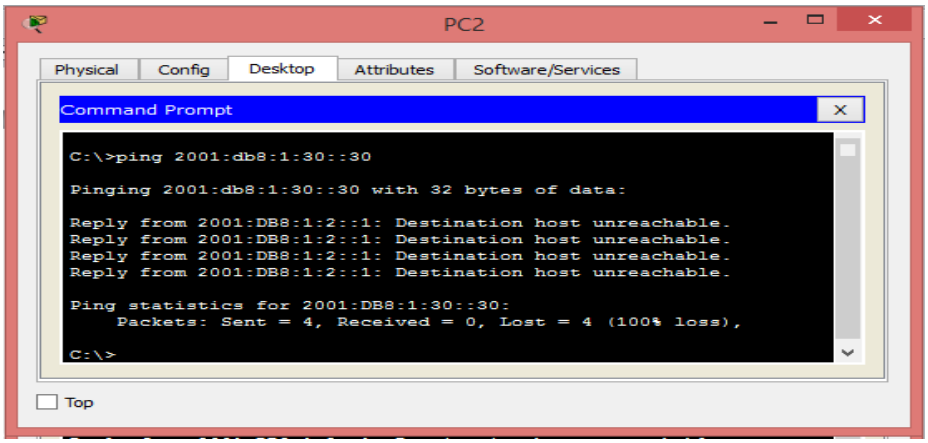
```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ipv6 traffic-filter BLOCK_ICMP out
```




Creacción de ACL en R3 para el bloqueo de ICMP

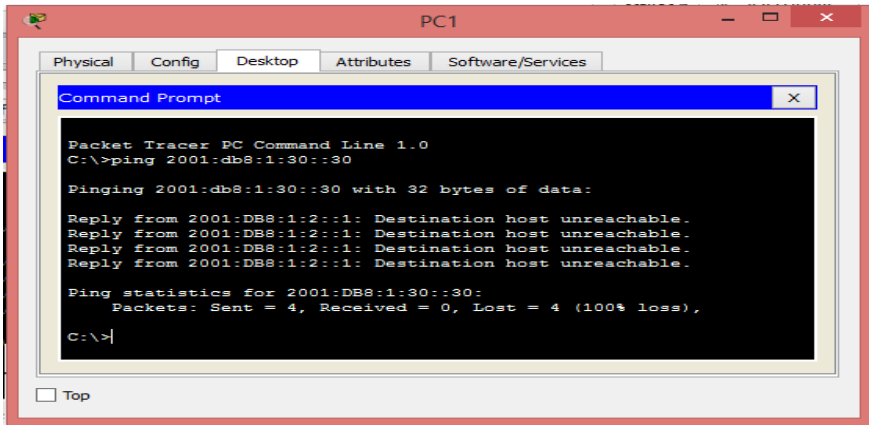
**Step 3: Verify that the proper access list functions.**

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




Tráfico entre PC2 y servidor 3 bloqueado

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




Tráfico entre PC1 y el servidor 3 bloqueado

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


Acceso web al servidor 3 habilitado para el PC1

# 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.

### 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
```

### Step 3: Verify the ACL implementation.

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

- Open the **web browser** of **PC1** to http:// 2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.
- Open the **web browser** of **PC2** to http:// 2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked
- Ping from **PC2** to 2001:DB8:1:30::30. The ping should be successful.

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

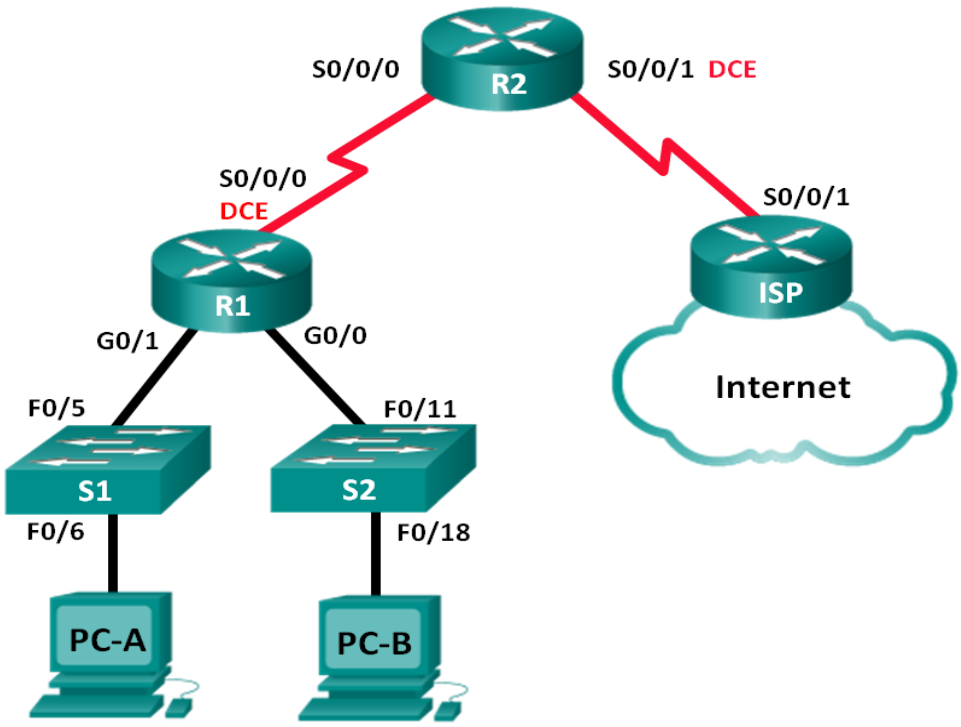
The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

Time Elapsed: 00:37:22 Completion: 100/100

Resultado Actividad

# 10.1.2.4 Práctica de laboratorio: configuración de DHCPv4 básico en un router

## Topología




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.

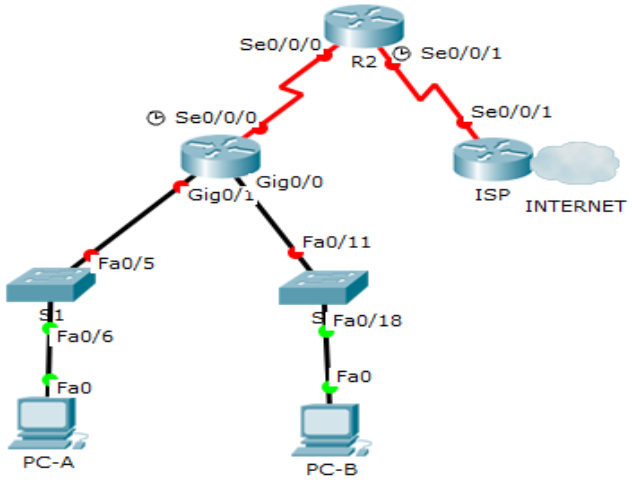
### Recursos necesarios

- 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

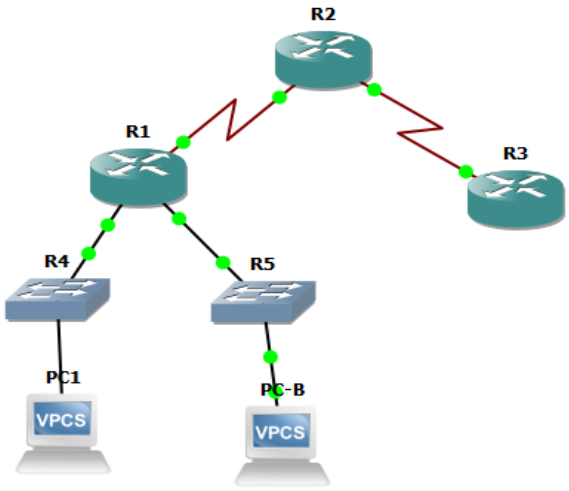
## Parte 1. Armar la red y configurar los parámetros básicos de los dispositivos

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.

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




Ensamble topología en Packet Tracer




Ensamble topología en GNS3

**Paso 2. inicializar y volver a cargar los routers y los switches.**

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

a. Desactive la búsqueda DNS.

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

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

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

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

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

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

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
```

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
```

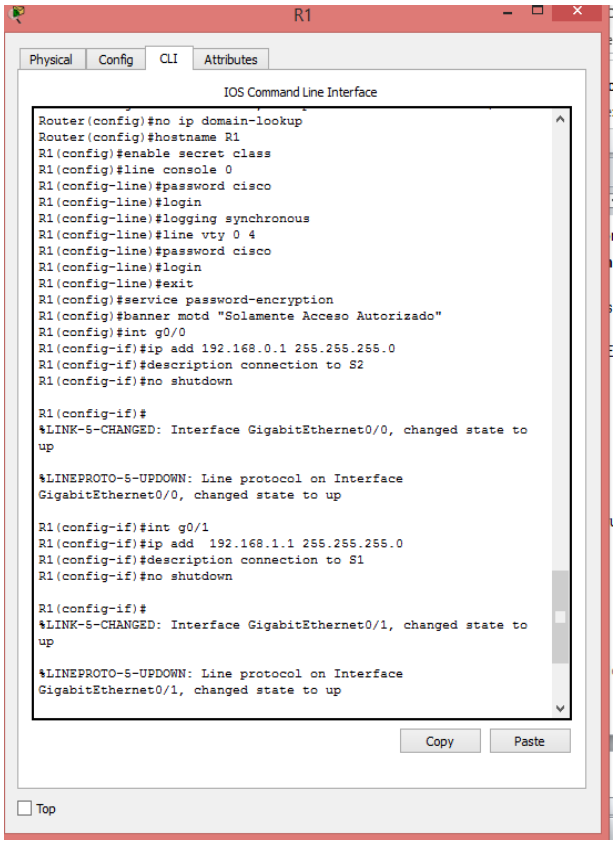
j. Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.

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

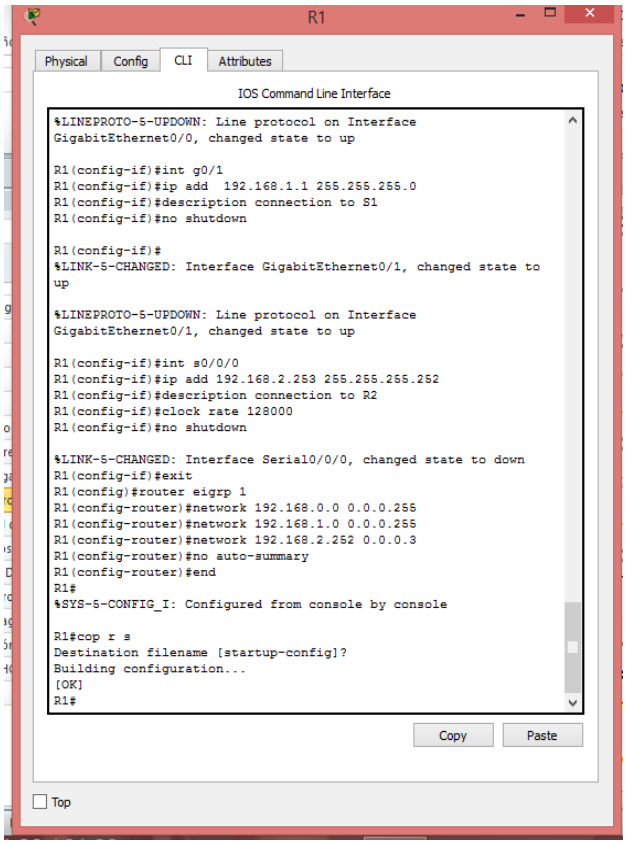
k. Copie la configuración en ejecución en la configuración de inicio

xx.

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

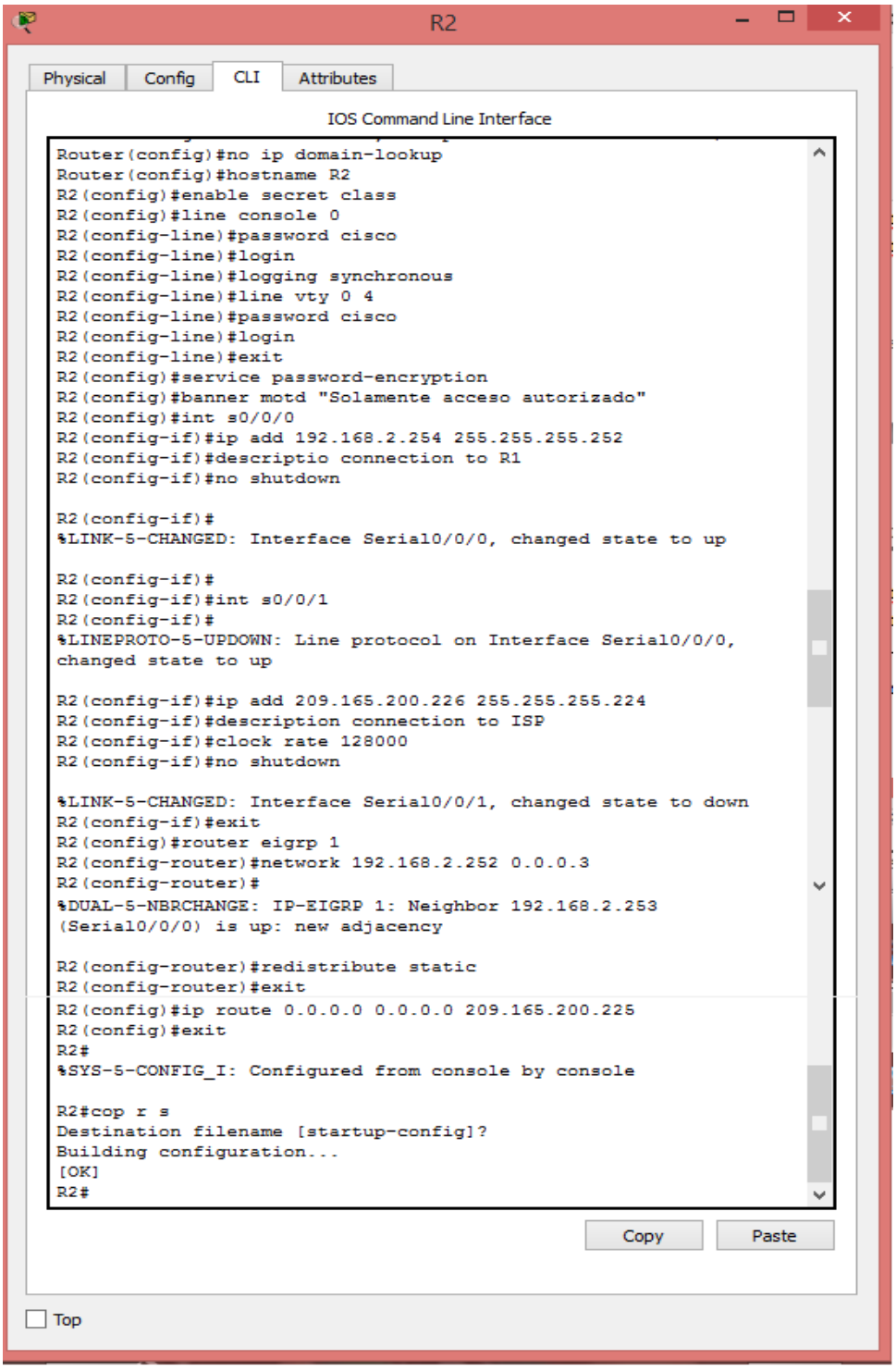



yy.

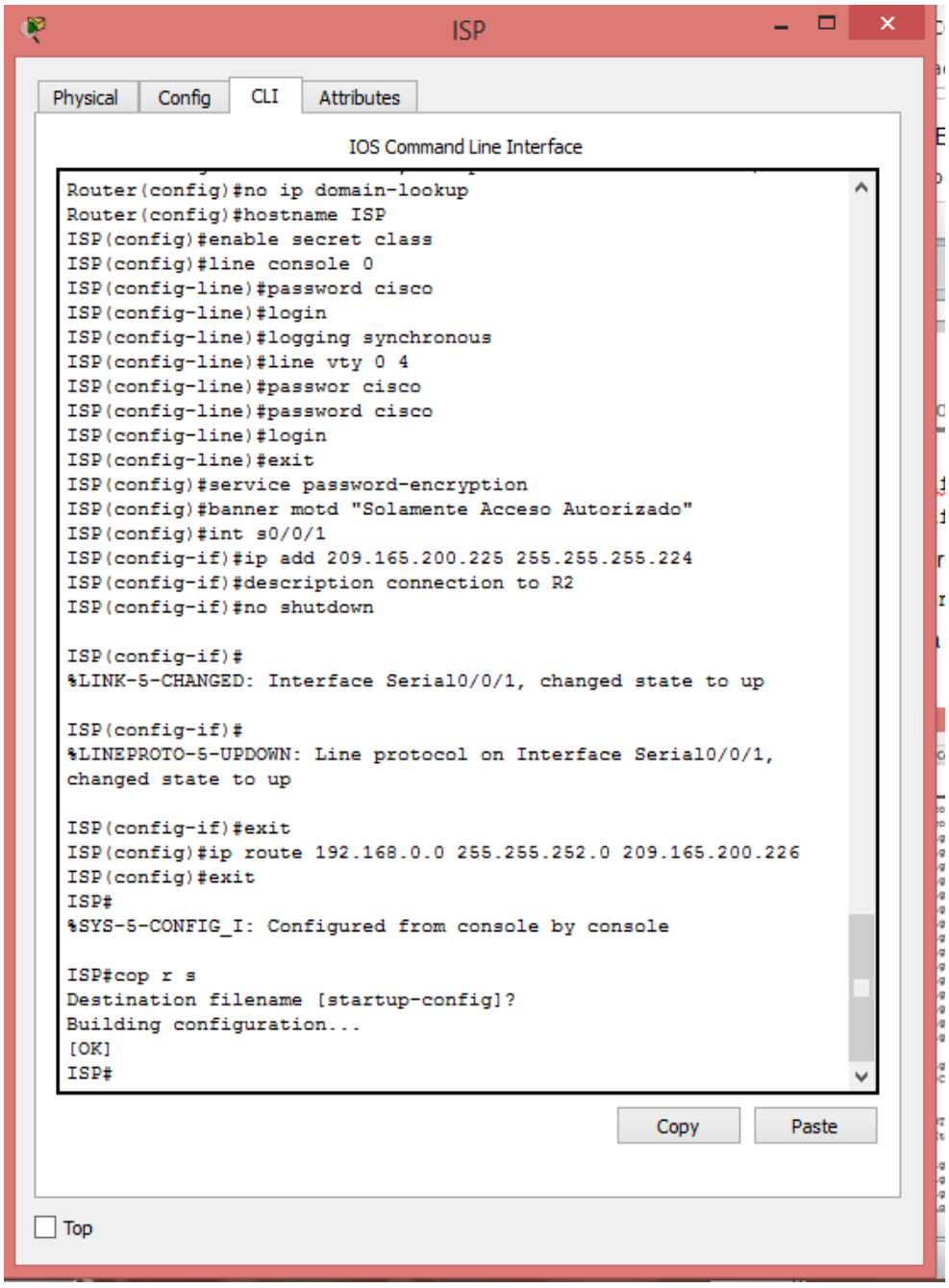



Configuración de R1

zz.




Configuración de R2




aaa.

Configuración R3

## Paso 4. verificar la conectividad de red entre los routers.

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

```
R1>ping 192.168.2.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4
ms
```

Conectividad exitosa entre R1 y R2

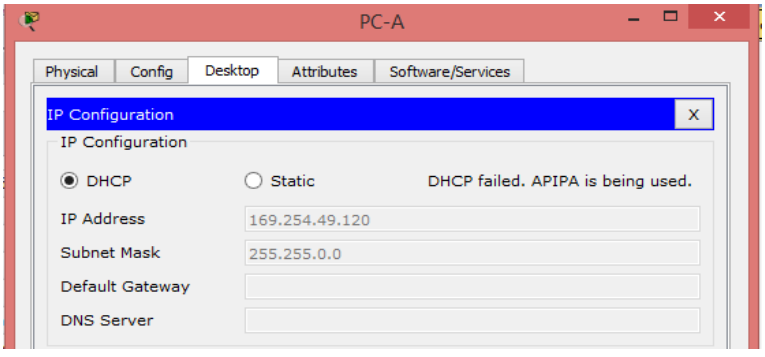
```
R2>ping 209.165.200.225

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

Conectividad exitosa entre R2 y R3

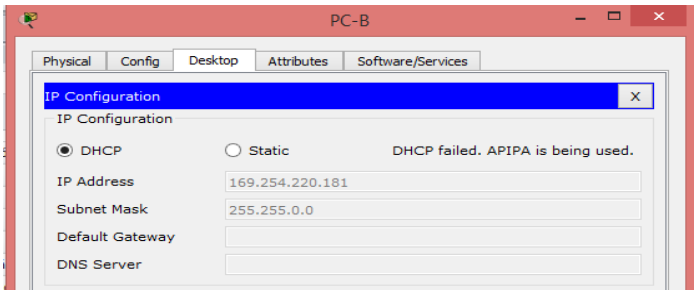
```
ISP#ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6
ms
```

Conectividad exitosa entre R3 y R2

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




Configuración de DHCP en PC-A




Configuración de DHCP en PC-B

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

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

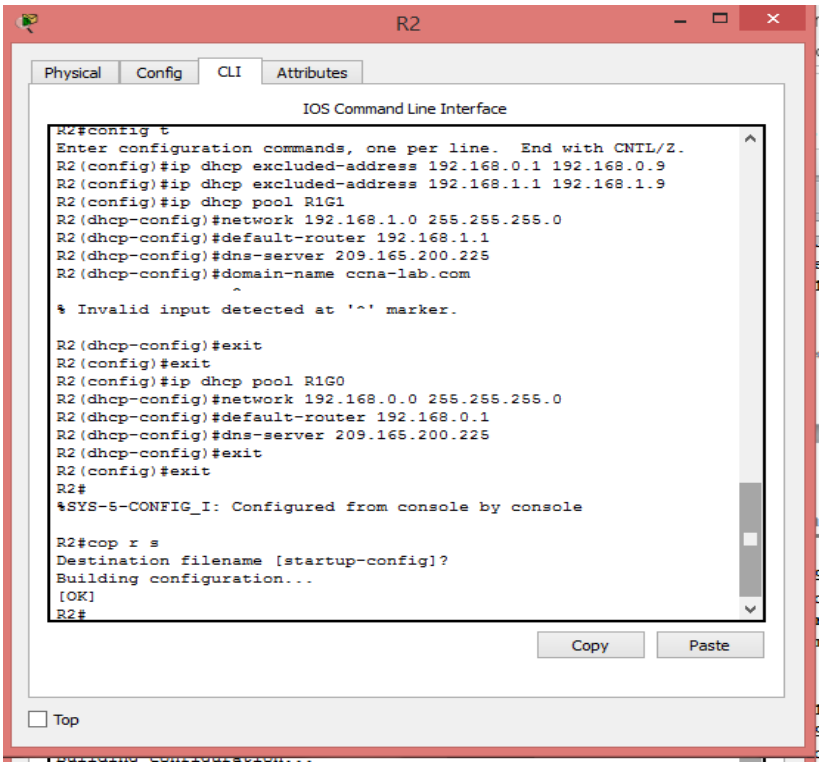
## Paso 1. configurar los parámetros del servidor de DHCPv4 en el router R2.

En el R2, configure un conjunto de direcciones DHCP para cada LAN del R1. Utilice el nombre de conjunto **R1G0** para G0/0 LAN y **R1G1** para G0/1 LAN. Asimismo, configure las direcciones que se excluirán de los conjuntos de direcciones. La práctica recomendada indica que primero se deben configurar las direcciones excluidas, a fin de garantizar que no se arrienden accidentalmente a otros dispositivos.

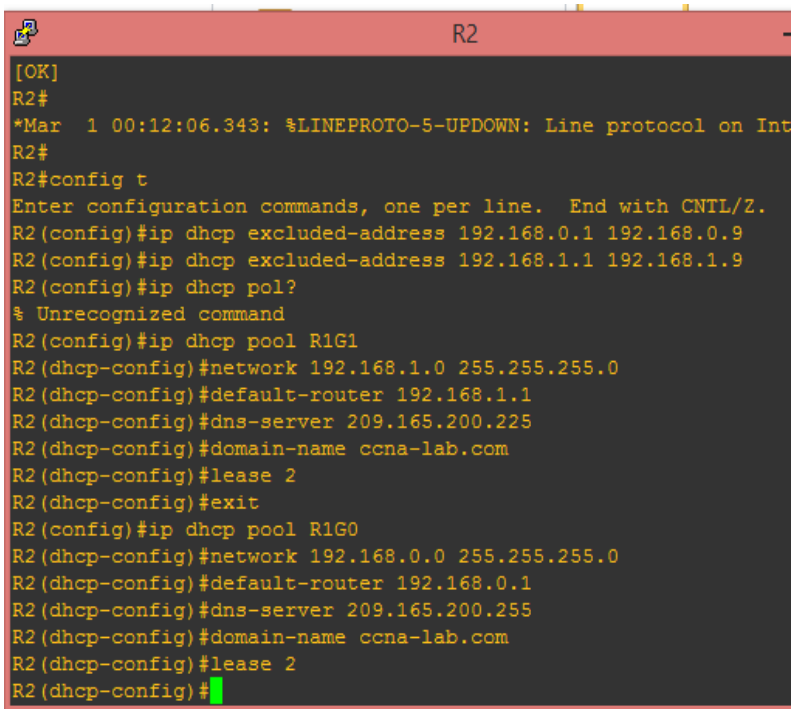
Excluya las primeras nueve direcciones en cada LAN del R1; empiece por .1. El resto de las direcciones deben estar disponibles en el conjunto de direcciones DHCP. Asegúrese de que cada conjunto de direcciones DHCP incluya un gateway predeterminado, el dominio **ccna-lab.com**, un servidor DNS (209.165.200.225)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

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

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



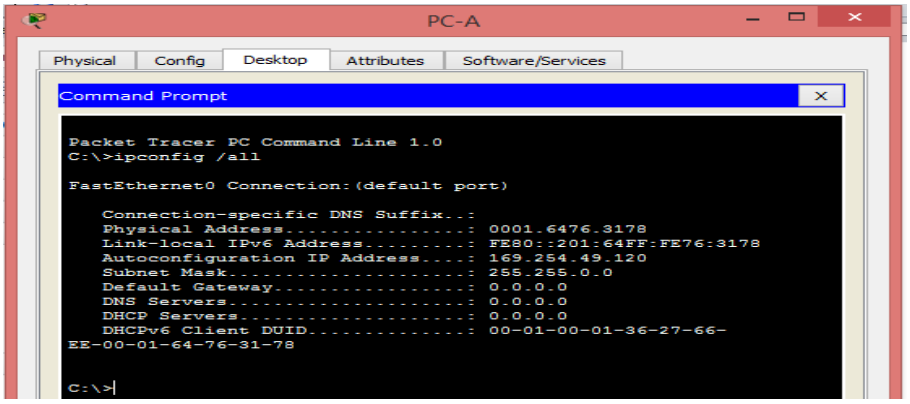

Configuración de R2 como servidor DHCP en Packet Tracer



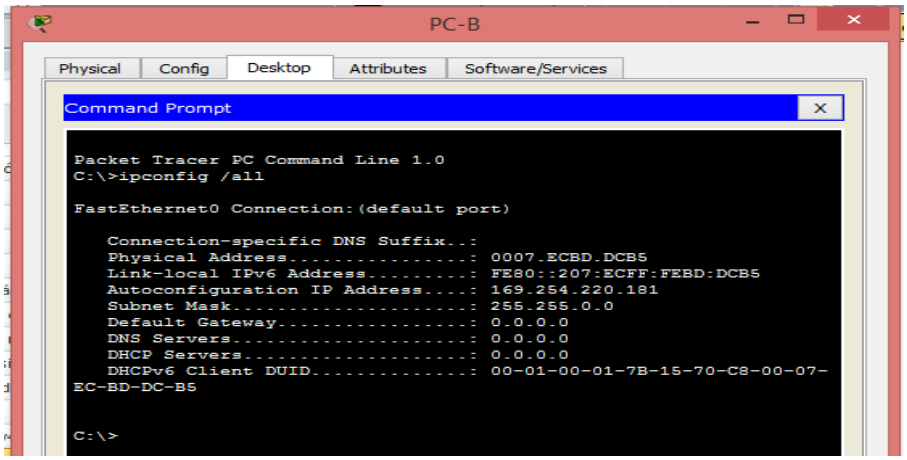

Configuración de R2 como servidor DHCP en GNS3

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

No, porque el router R2 está en otra red




Verificación direcionamiento DHCP en PC-A




Verificación direcionamiento DHCP en PC-B

## Paso 2. configurar el R1 como agente de retransmisión DHCP.

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

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

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

Configuración R1 como agente de retransmisión DHCP

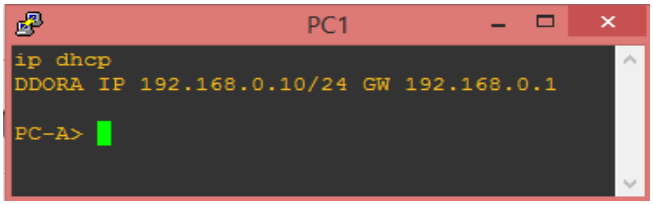
## Paso 3. registrar la configuración IP para la PC-A y la PC-B.

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

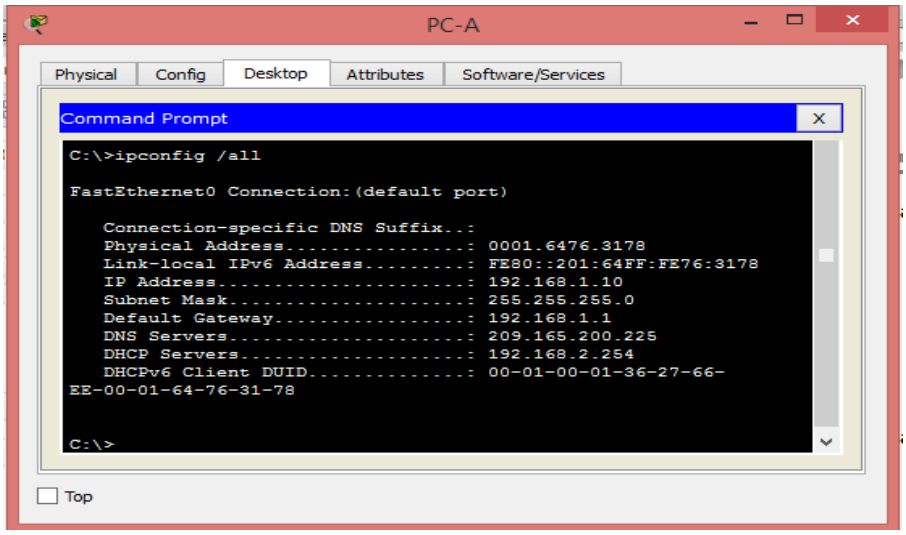
PC-A

IP DHCP 192.168.1.10

MAC address 0001.6476.3178



Dirección recibida en el PC-A del servidor en GNS3

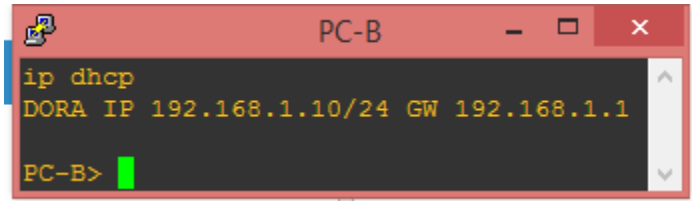



Dirección recibida en el PC-A del servidor

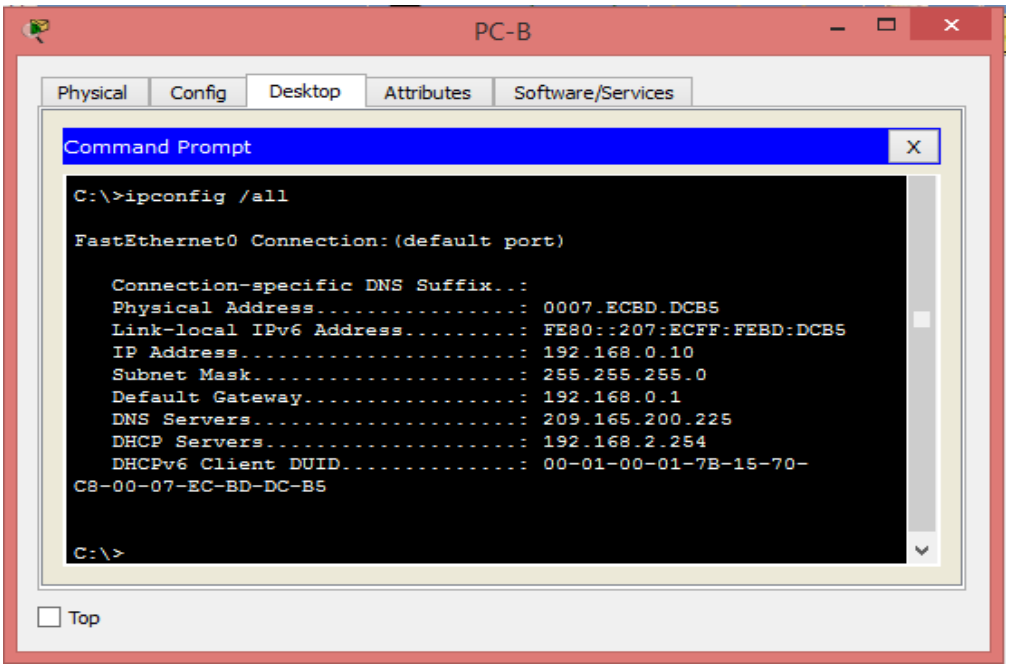
PC-B

IP DHCP 192.168.0.10

MAC address 0007.ECBD.DCB5




Dirección recibida en el PC-B del servidor en GNS3




Dirección recibida en el PC-B del servidor

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?

En la PCA es la 192.168.1.10 y en la PC-b la 192.168.0.10

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

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

bbb. Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado? El tiempo de expiración del arrendamiento el tipo y y la MAC address

ccc.

```
R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.10     0001.6476.3178          2                       Automatic
192.168.0.10     0007.ECBD.DCB5          2                       Automatic
R2#
```

ddd.

```
R2#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.0.10        0100.5079.6668.00       Mar 03 2002 12:21 AM    Automat
ic
192.168.1.10        0100.5079.6668.01       Mar 03 2002 12:24 AM    Automat
ic
```

Verificación de los servicios DHCP

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?

Dos tipos de mensajes, los que se envían y los que se reciben

```
R2#show ip dhcp server statistics
Memory usage         25719
Address pools        2
Database agents      0
Automatic bindings   2
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         5
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            5
DHCPACK              3
DHCPNAK              0
R2#
```

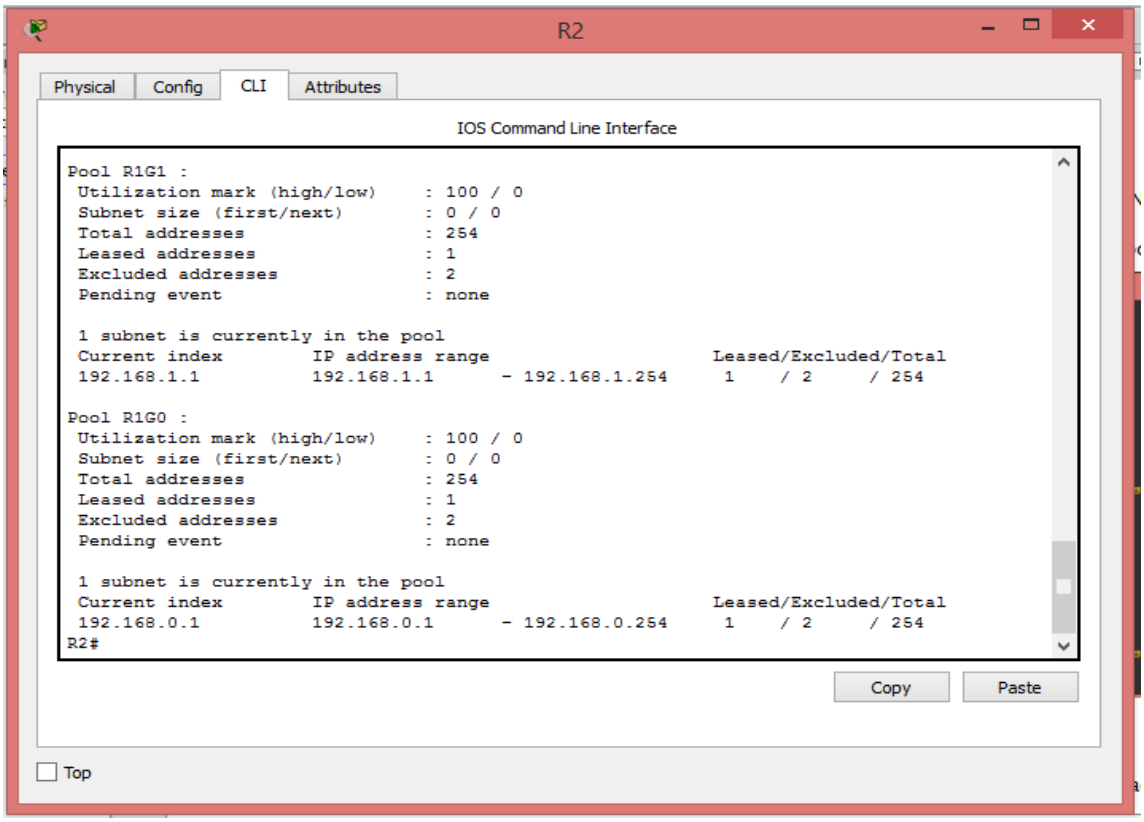
Visualización de las estadisticas de DHCP en R2 con GNS3

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

```
R2
DHCPACK             3
DHCPNAK             0
R2#show ip dhcp pool

Pool R1G1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased addresses
 192.168.1.11         192.168.1.1      - 192.168.1.254     1

Pool R1G0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased addresses
 192.168.0.11         192.168.0.1      - 192.168.0.254     1
R2#
```

eee.

Visualizando la configuración del pool de DHCP en GNS3




Visualizando la configuración del pool de DHCP en PT

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

ggg. Hace referencia a la dirección ip de la interfaz G0/0 y G0/1 del R1

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

hhh.

```
R2#show run | section dhcp
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
ip dhcp pool R1G1
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 209.165.200.225
   domain-name ccna-lab.com
   lease 2
ip dhcp pool R1G0
   network 192.168.0.0 255.255.255.0
   default-router 192.168.0.1
   dns-server 209.165.200.255
   domain-name ccna-lab.com
   lease 2
```

Visualizando configuración DHCP en R2 con GNS3

iii.

jjj.

kkk.

```
R2#show run | begin dhcp
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 209.165.200.225
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 209.165.200.225
```

Visualizando configuración DHCP en R2 con PT

lll.

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

mmm.

nnn.

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

Visualizando la configuración de retransmisión en G0/0 de R1

ooo.

```
R1#show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.2.254
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
```

Visualizando la configuración de retransmisión en G0/1 de R1

```
R1
R1#show run interface f0/0
Building configuration...

Current configuration : 129 bytes
!
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip helper-address 192.168.2.254
 duplex auto
 speed auto
end

R1#show run interface f0/1
Building configuration...

Current configuration : 129 bytes
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.2.254
 duplex auto
 speed auto
end

R1#
```

Show run interface en GNS3

## Reflexión

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

El principal beneficio es que se puede ahorrar recursos de hardware al tener concentrados todos los DHCP en un solo router.

## 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
```

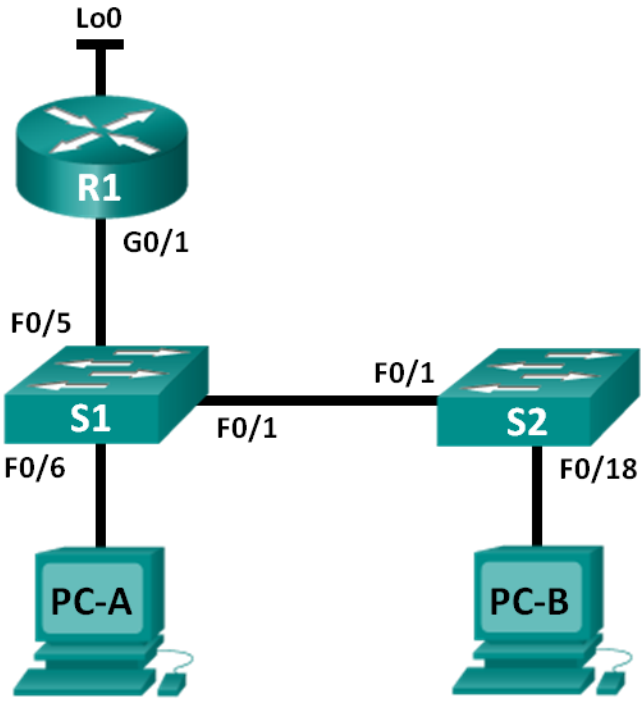
Universidad Nacional Abierta y a Distancia

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

# 10.1.2.5

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

## Topología



## Tabla de direccionamiento

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

## Objetivos

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

**Parte 2: cambiar la preferencia de SDM**

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

**Parte 3: configurar DHCPv4**

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

**Parte 4: configurar DHCP para varias VLAN**

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

**Parte 5: habilitar el routing IP**

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

## Información básica/situación

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

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

**Nota**: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión

15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

### Recursos necesarios

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

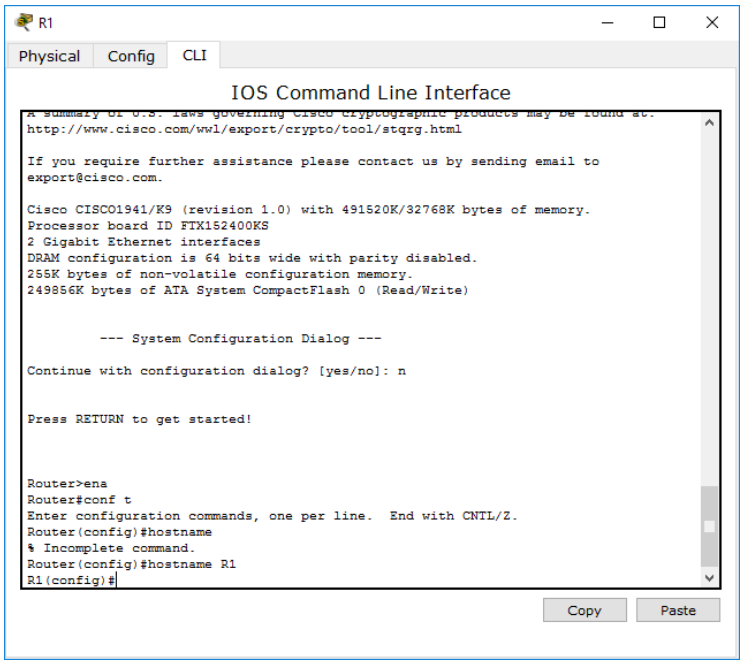
## Parte 7: armar la red y configurar los parámetros básicos de los dispositivos

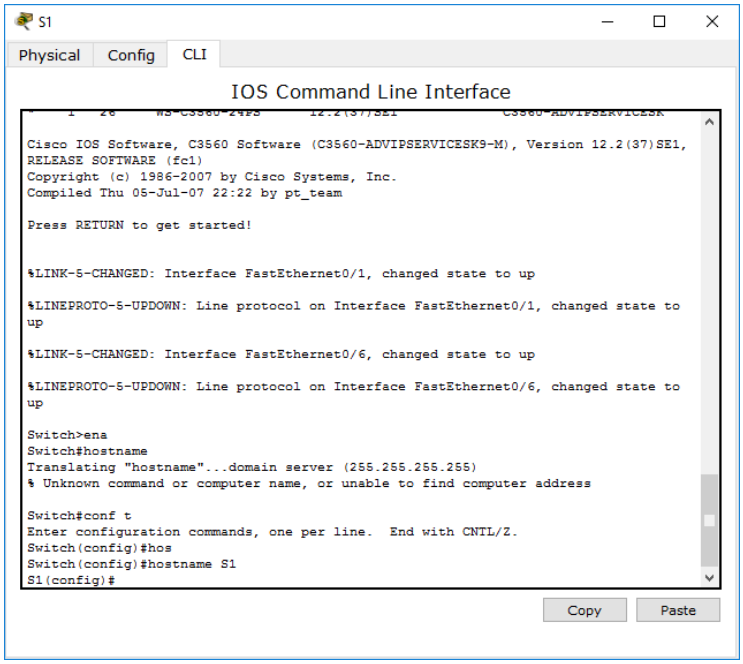
### Paso 1: realizar el cableado de red tal como se muestra en la topología.

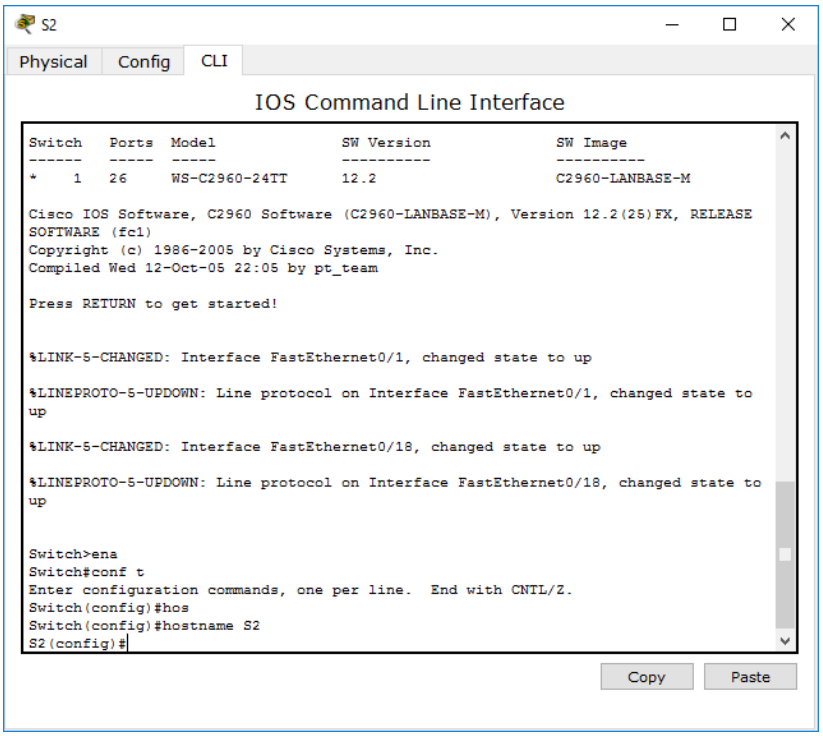
### Paso 2: inicializar y volver a cargar los routers y switches.

### Paso 3: configurar los parámetros básicos en los dispositivos.

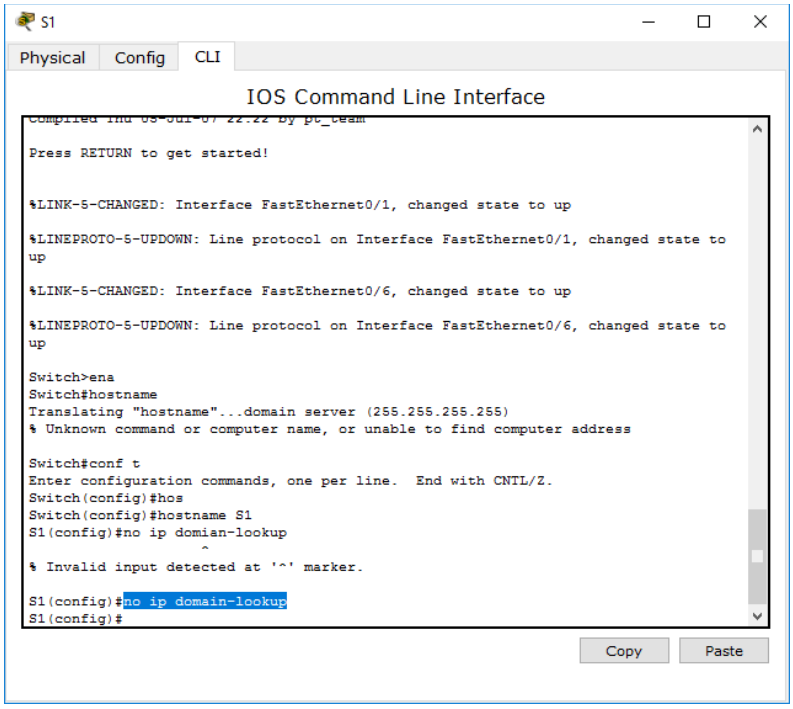
a. Asigne los nombres de dispositivos como se muestra en la topología.

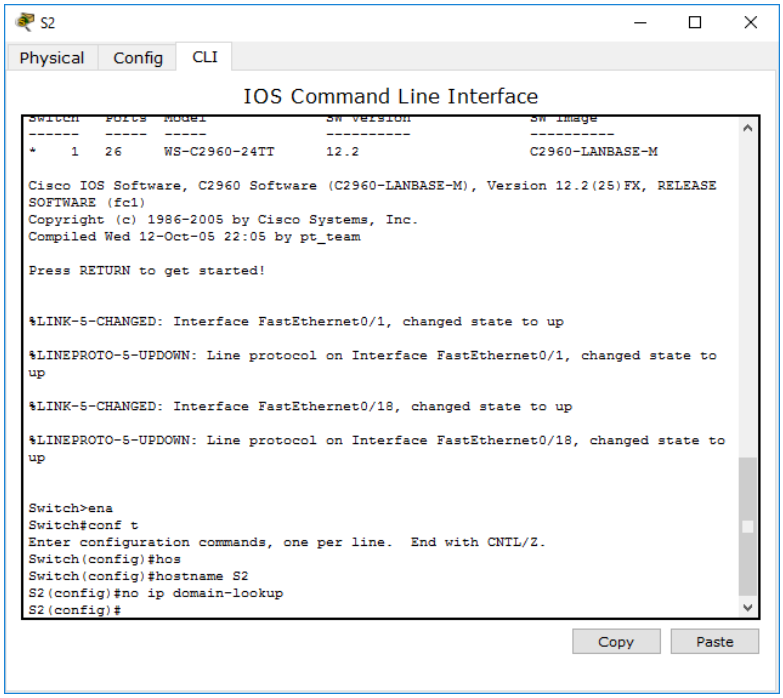

R1
Physical
Config
CLI
IOS Command Line Interface
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname
% Incomplete command.
Router(config)#hostname R1
R1(config)#
Copy
Paste

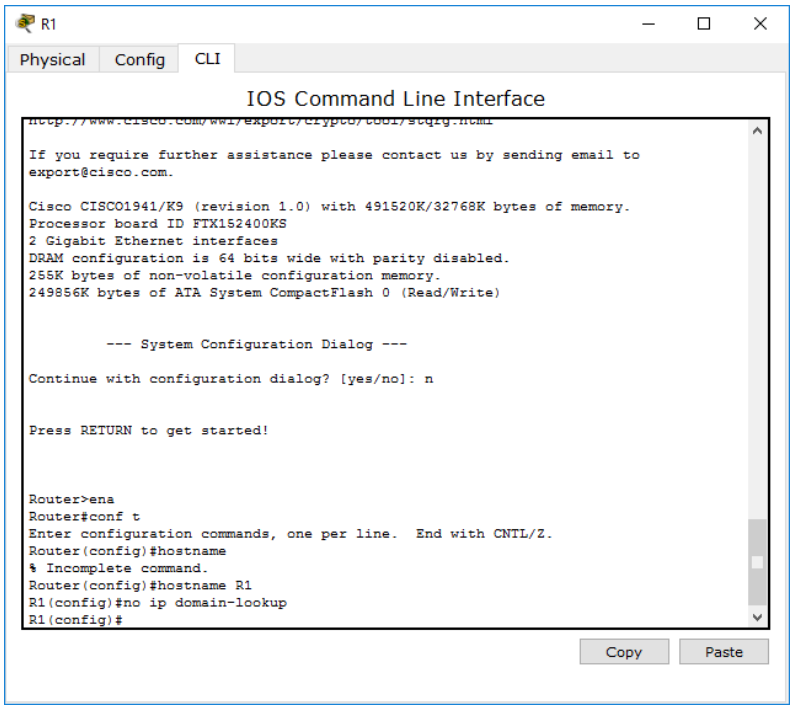

S1
Physical
Config
CLI
IOS Command Line Interface
Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to
up
Switch>ena
Switch#hostname
Translating "hostname"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname S1
S1(config)#
Copy
Paste



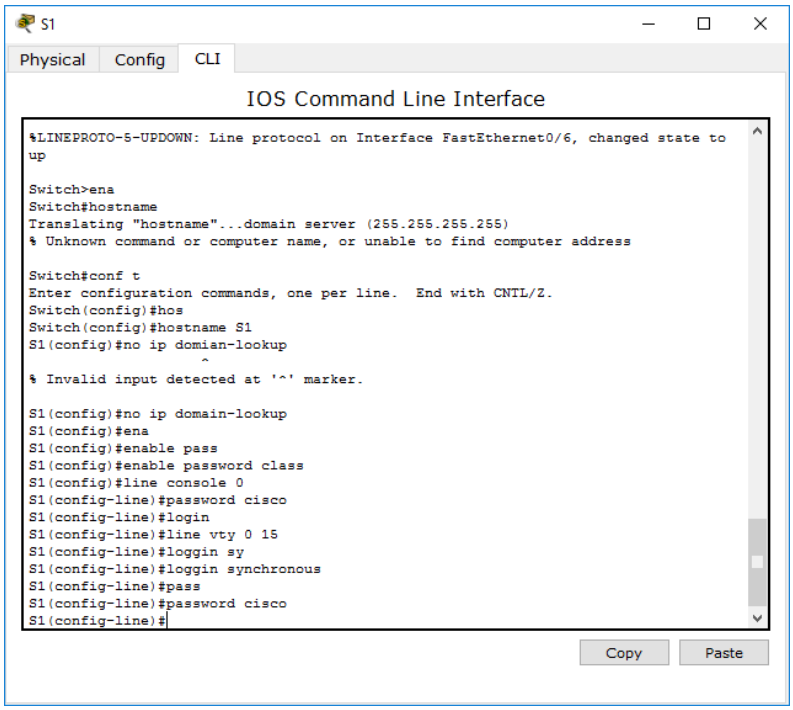

b. Desactive la búsqueda del DNS.

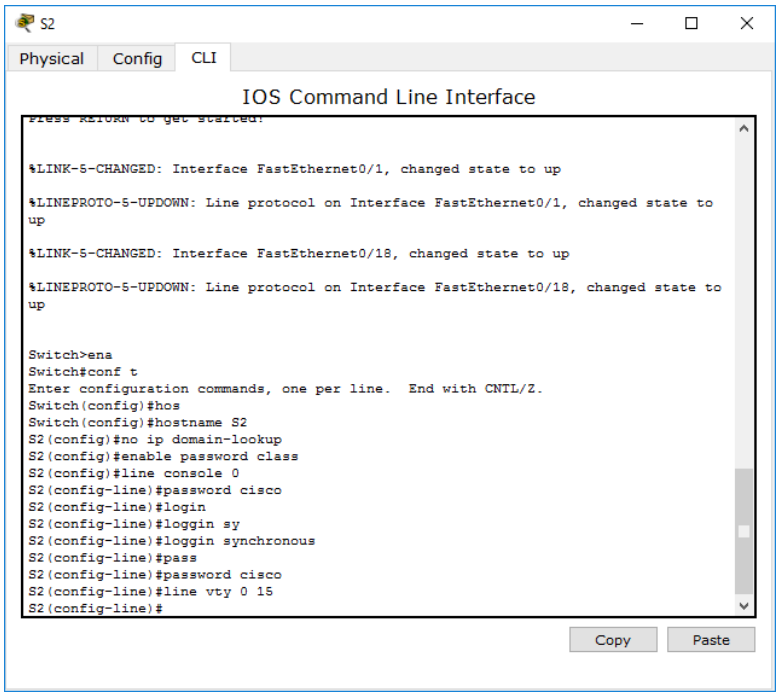


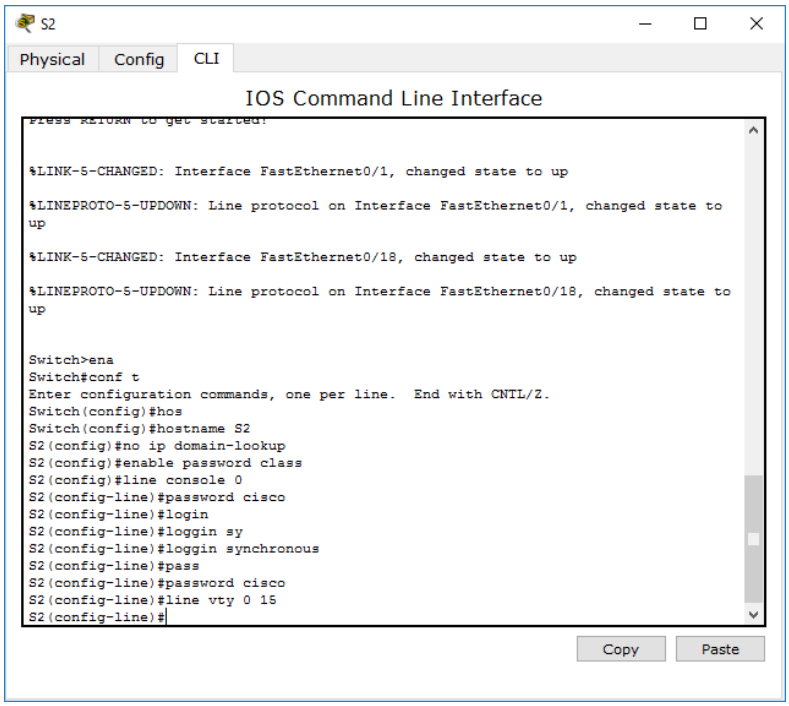

S2
Physical
Config
CLI
IOS Command Line Interface
Switch  Ports  Model  SW Version  SW Image
------  -----  -----  ----------  ----------
*  1  26  WS-C2960-24TT  12.2  C2960-LANBASE-M
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#
Copy
Paste



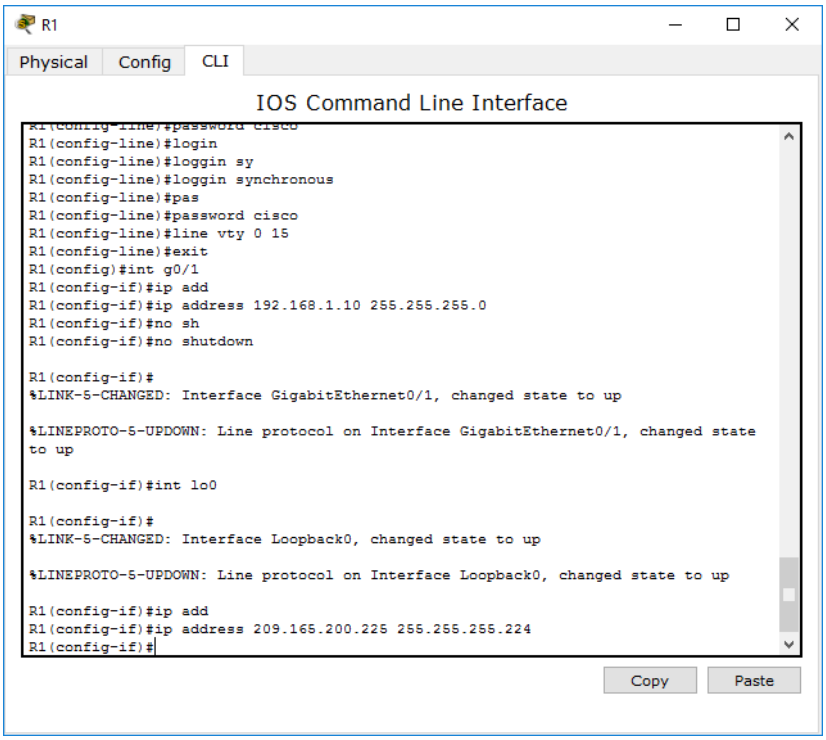

c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.


S1
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
Switch>ena
Switch#hostname
Translating "hostname"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname S1
S1(config)#no ip domian-lookup
^
% Invalid input detected at '^' marker.
S1(config)#no ip domain-lookup
S1(config)#ena
S1(config)#enable pass
S1(config)#enable password class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#loggin sy
S1(config-line)#loggin synchronous
S1(config-line)#pass
S1(config-line)#password cisco
S1(config-line)#
Copy
Paste

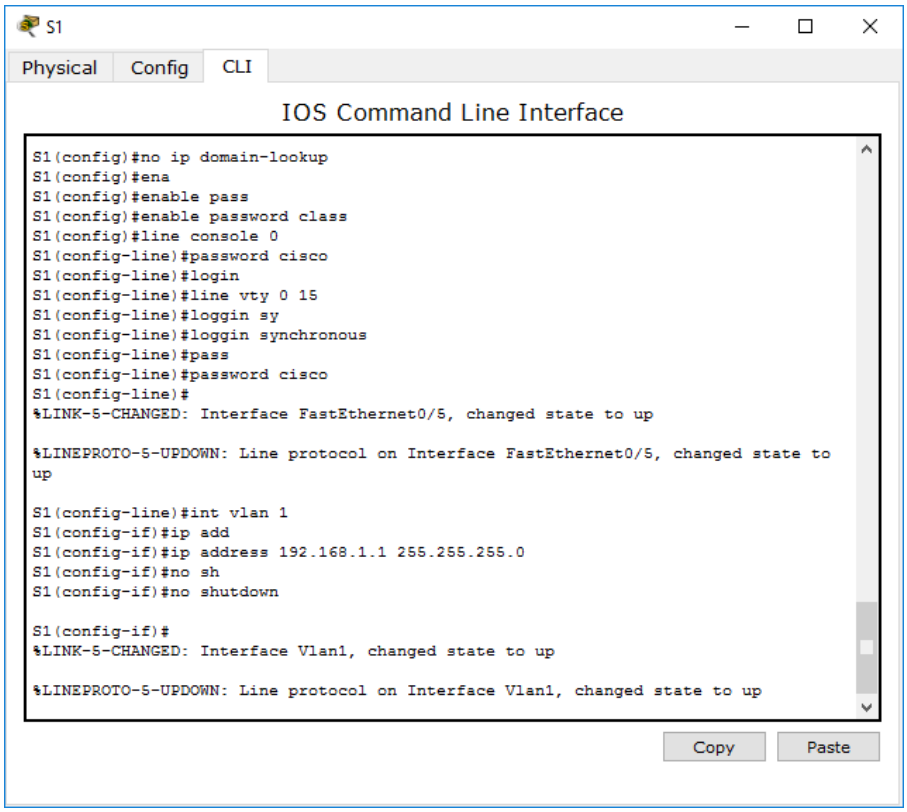

S2
Physical
Config
CLI
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#enable password class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#loggin sy
S2(config-line)#loggin synchronous
S2(config-line)#pass
S2(config-line)#password cisco
S2(config-line)#line vty 0 15
S2(config-line)#
Copy
Paste

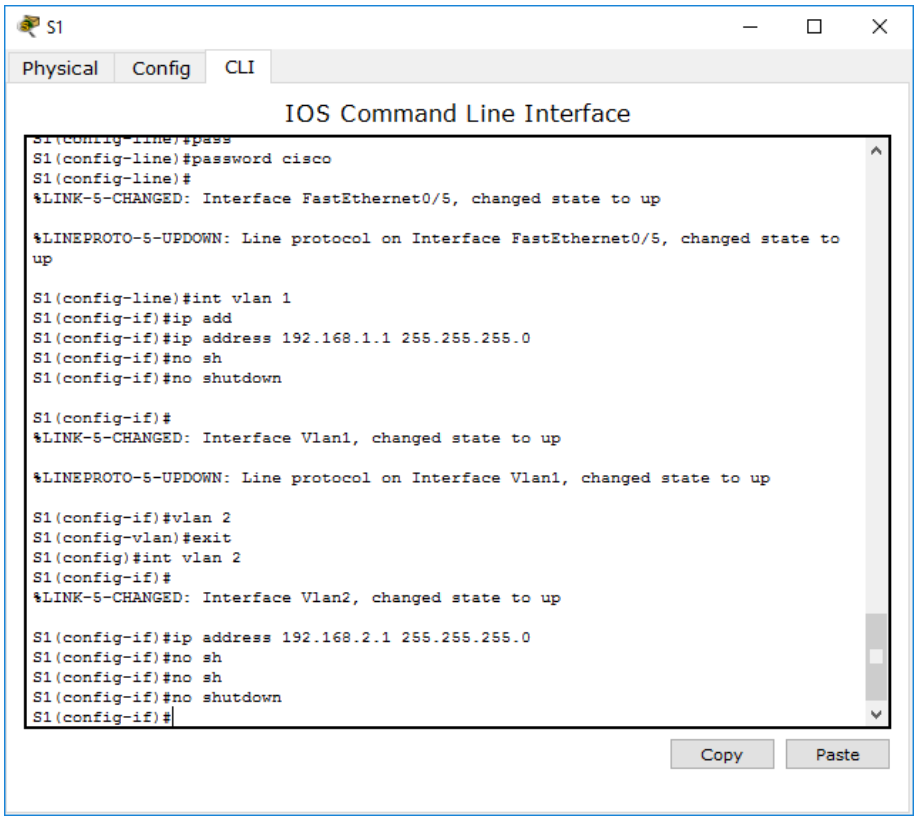



d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

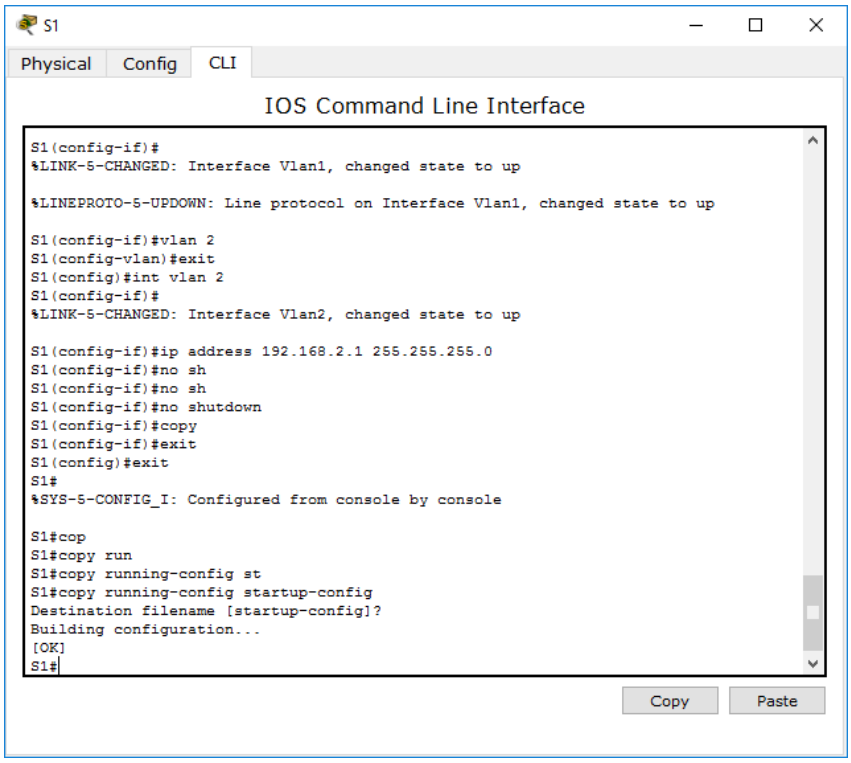



e. Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.


S1
Physical
Config
CLI
IOS Command Line Interface
S1(config)#no ip domain-lookup
S1(config)#ena
S1(config)#enable pass
S1(config)#enable password class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#loggin sy
S1(config-line)#loggin synchronous
S1(config-line)#pass
S1(config-line)#password cisco
S1(config-line)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
S1(config-line)#int vlan 1
S1(config-if)#ip add
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no sh
S1(config-if)#no shutdown
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Copy
Paste




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




## Parte 8: cambiar la preferencia de SDM

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

### Paso 1: mostrar la preferencia de SDM en el S1.

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

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

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

¿Cuál es la plantilla actual?

_____

## Paso 2: cambiar la preferencia de SDM en el S1.

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

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

¿Qué plantilla estará disponible después de la recarga?

_____

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
```

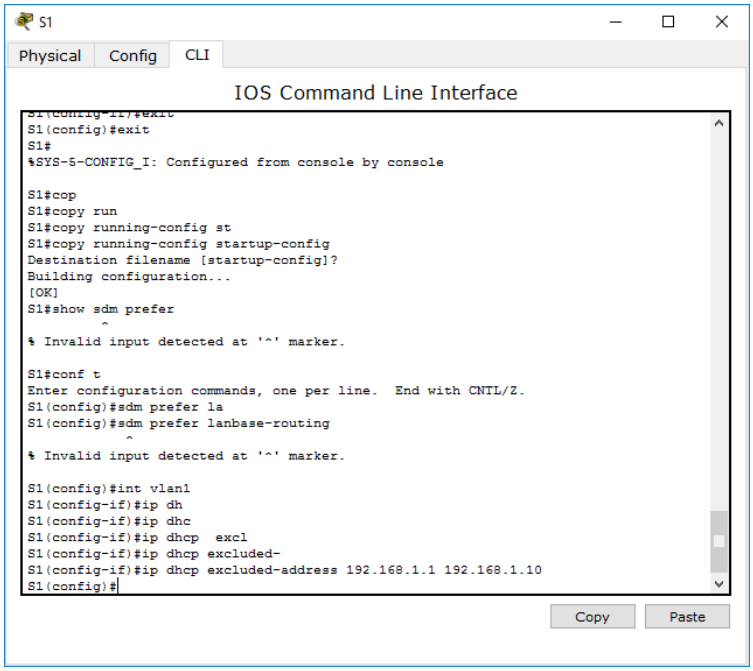
```
number of IPv4/MAC security aces:                0.375k
number of IPv6 policy based routing aces:        0
number of IPv6 qos aces:                         0.375k
number of IPv6 security aces:                    127
```

# Parte 9: configurar DHCPv4

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

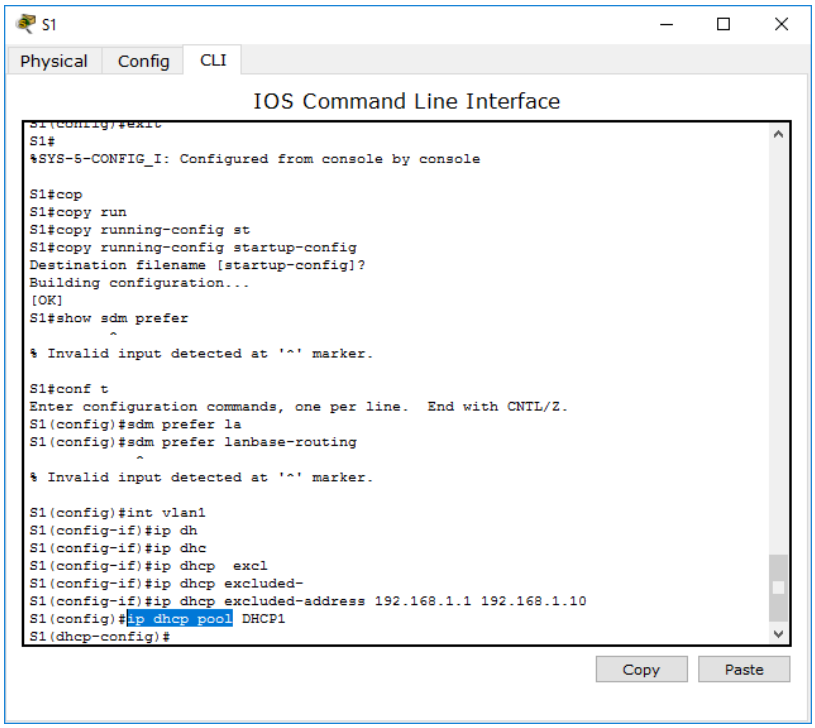
## Paso 1: configurar DHCP para la VLAN 1.

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



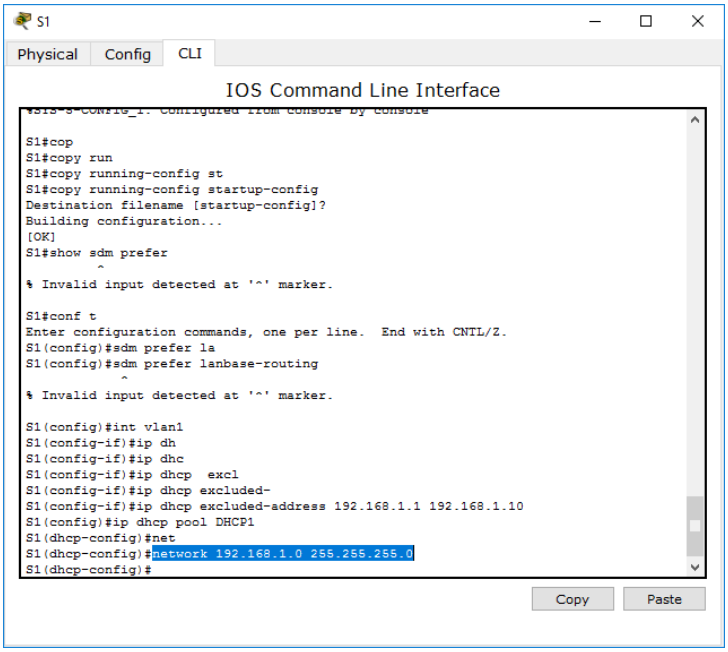

_____

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

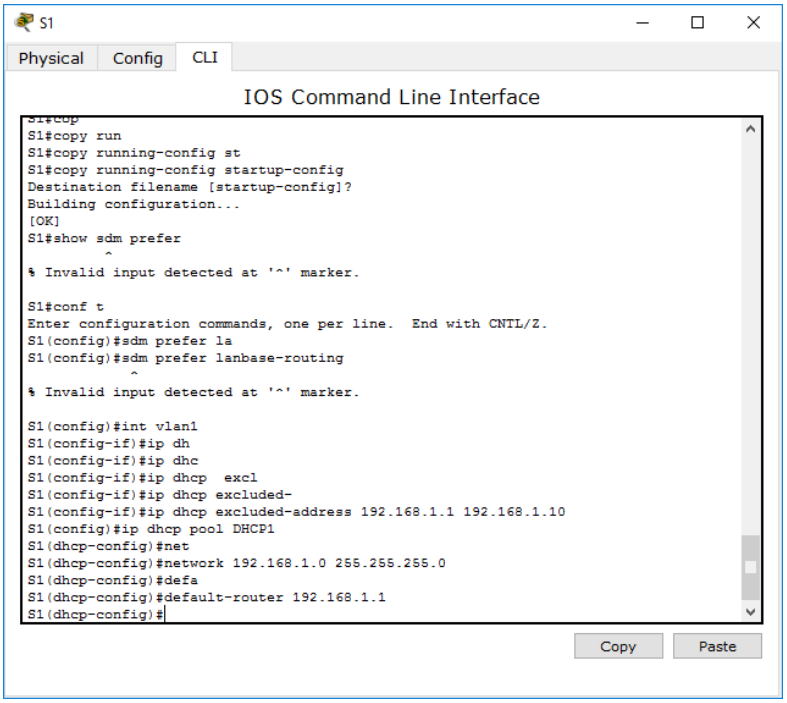



_____

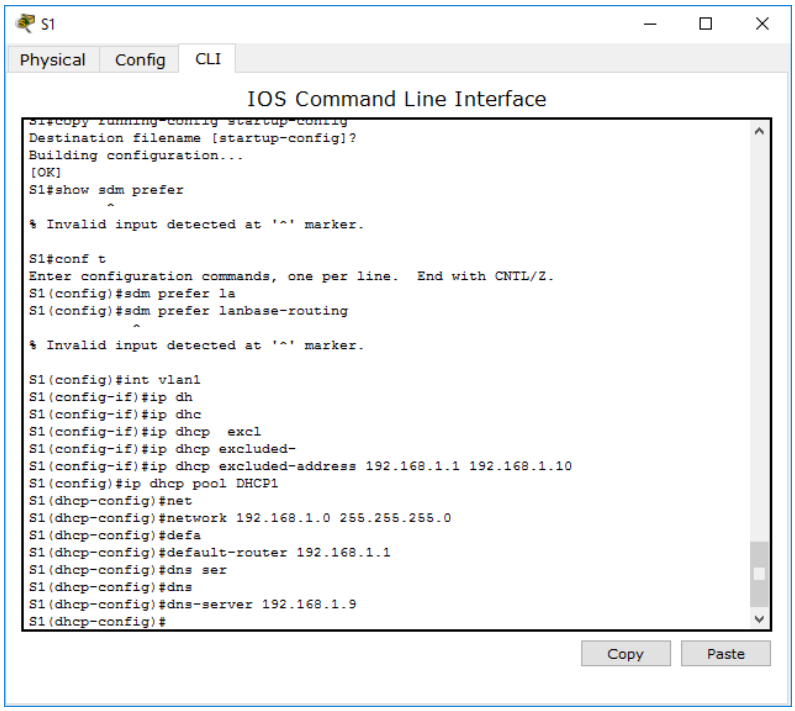
c. Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.



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



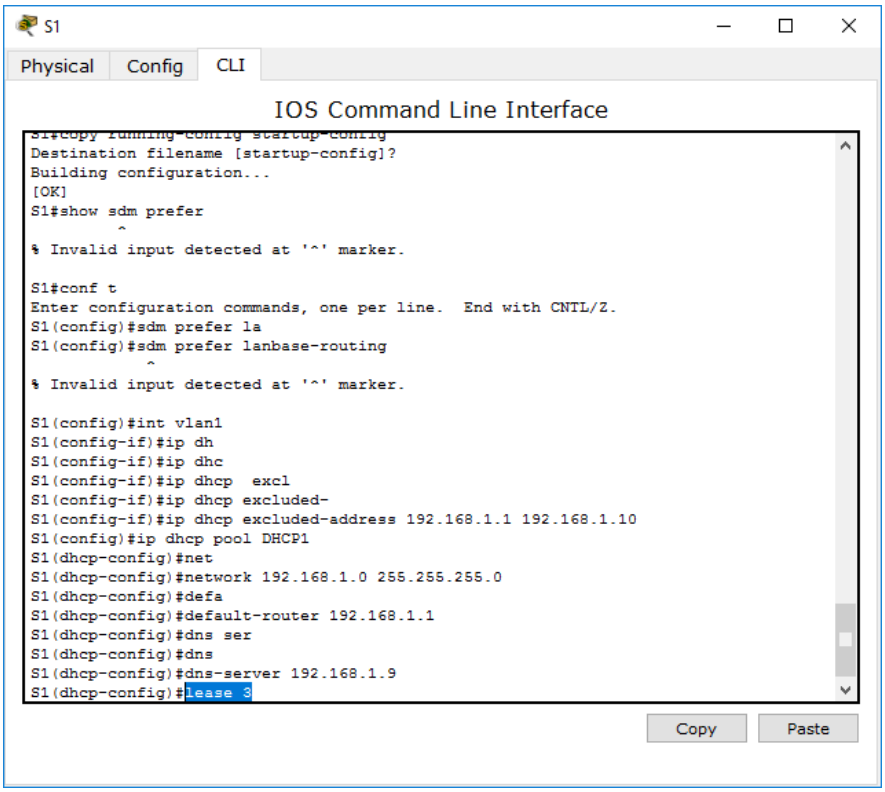
e. Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.



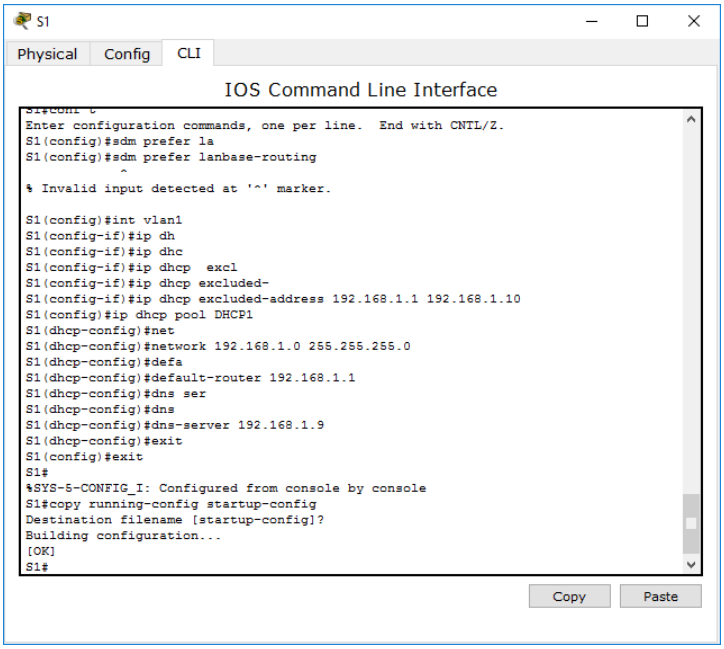

_____

_____

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




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



## Paso 2: verificar la conectividad y DHCP.

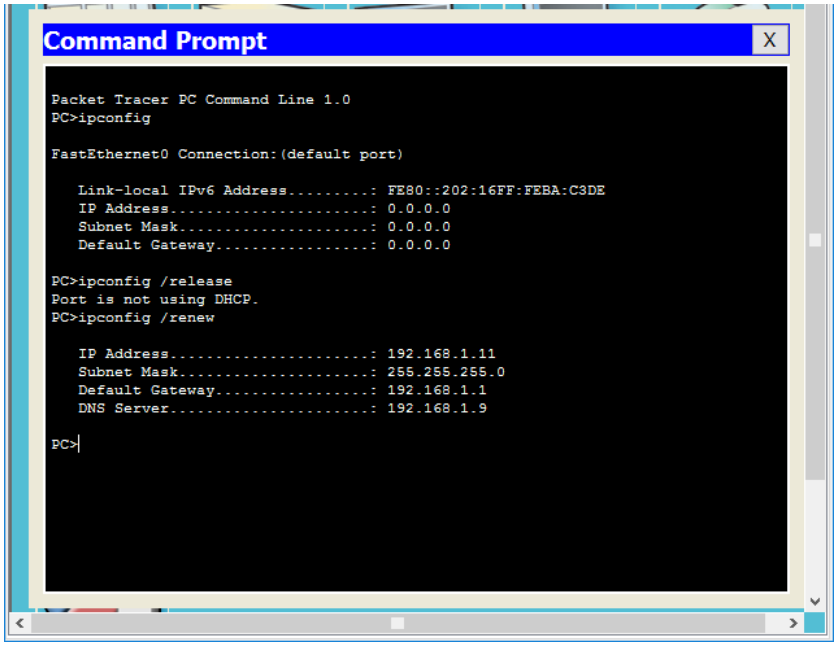
a. En la PC-A y la PC-B, abra el símbolo del sistema y emita el comando **ipconfig**. Si la información de IP no está presente, o si está incompleta, emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: _____

Máscara de subred: _____

Gateway predeterminado: _____

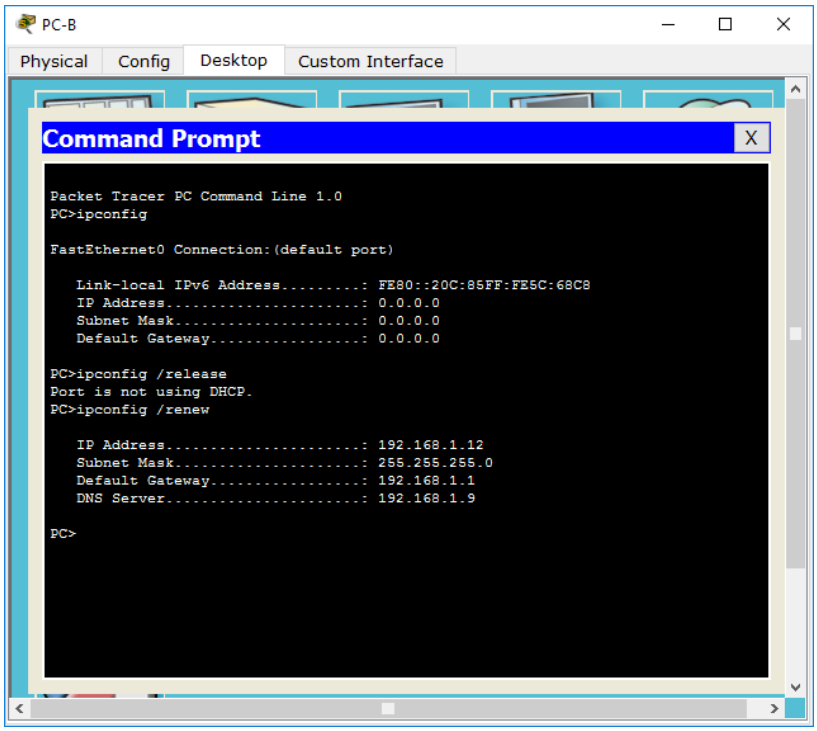



Para la PC-B, incluya lo siguiente:

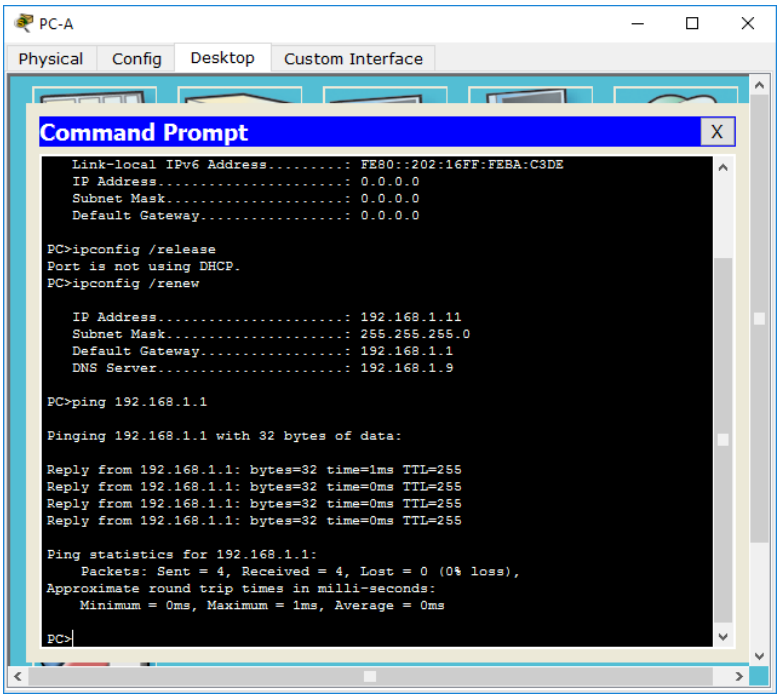
Dirección IP: _____

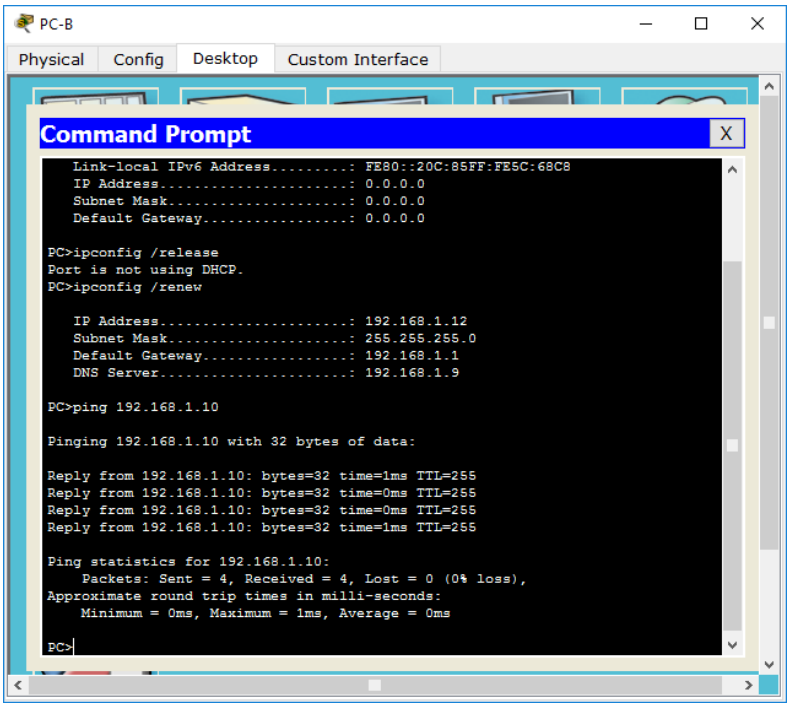
Máscara de subred: _____

Gateway predeterminado: _____




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






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

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

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

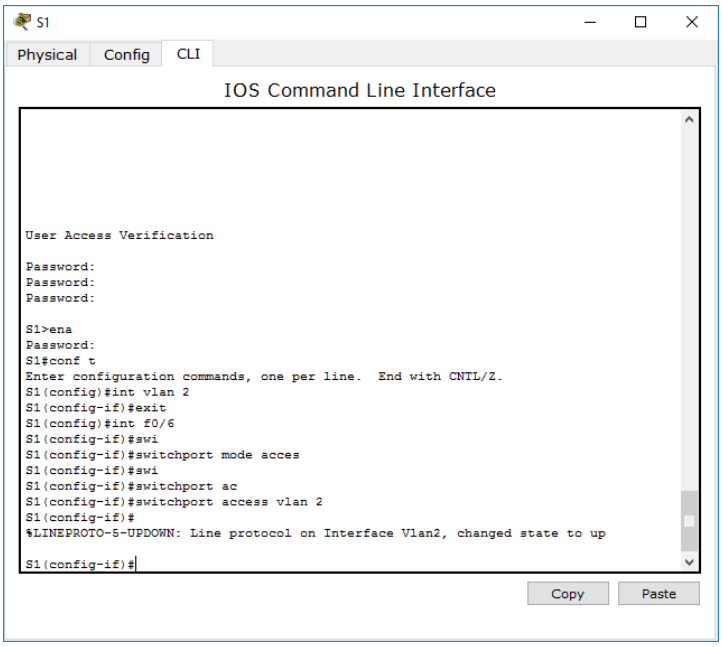
Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.

## Parte 10:configurar DHCPv4 para varias VLAN

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

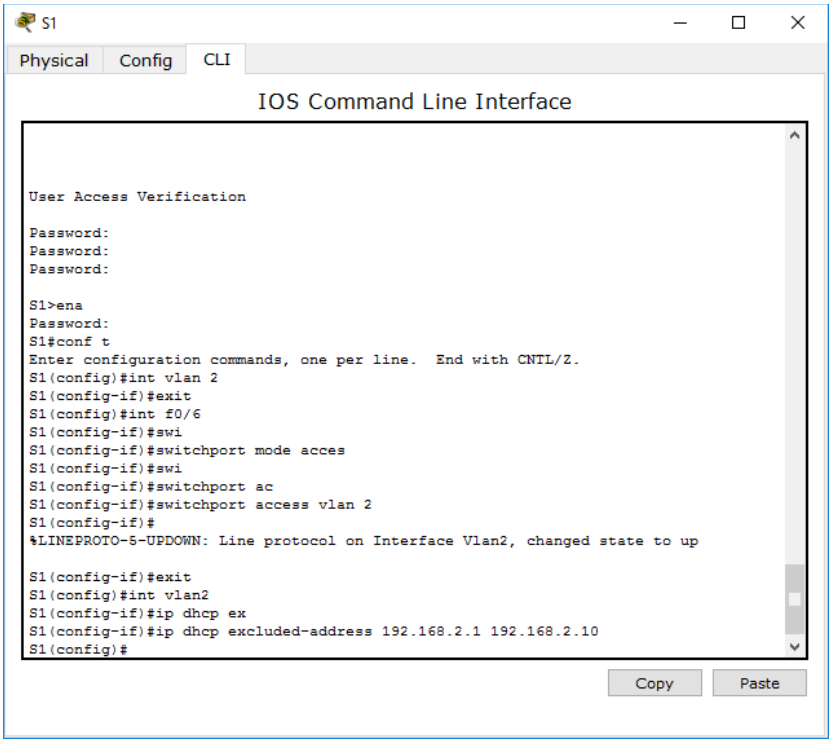
### Paso 1: asignar un puerto a la VLAN 2.

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

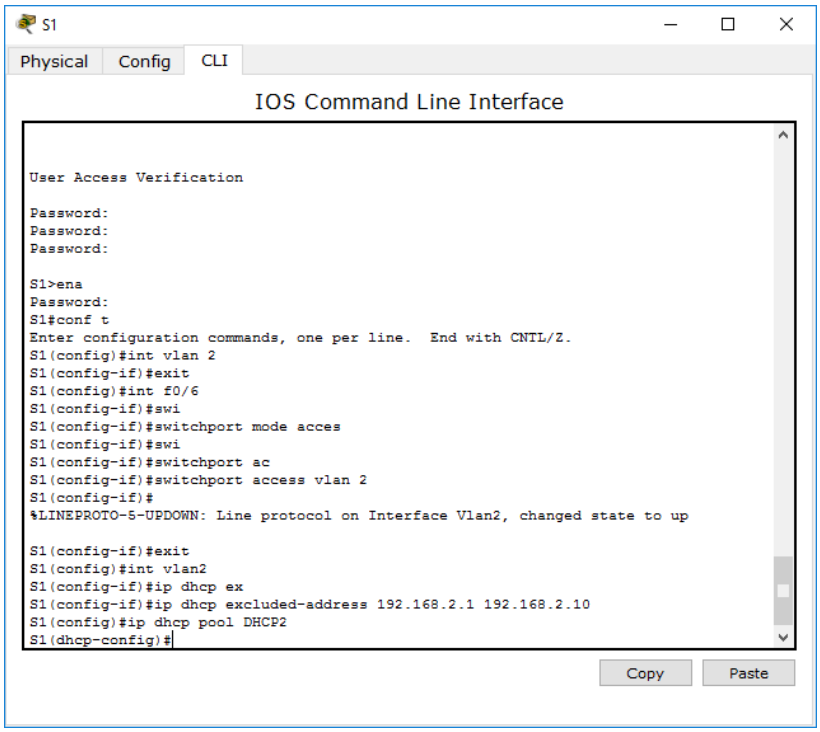



## Paso 2: configurar DHCPv4 para la VLAN 2.

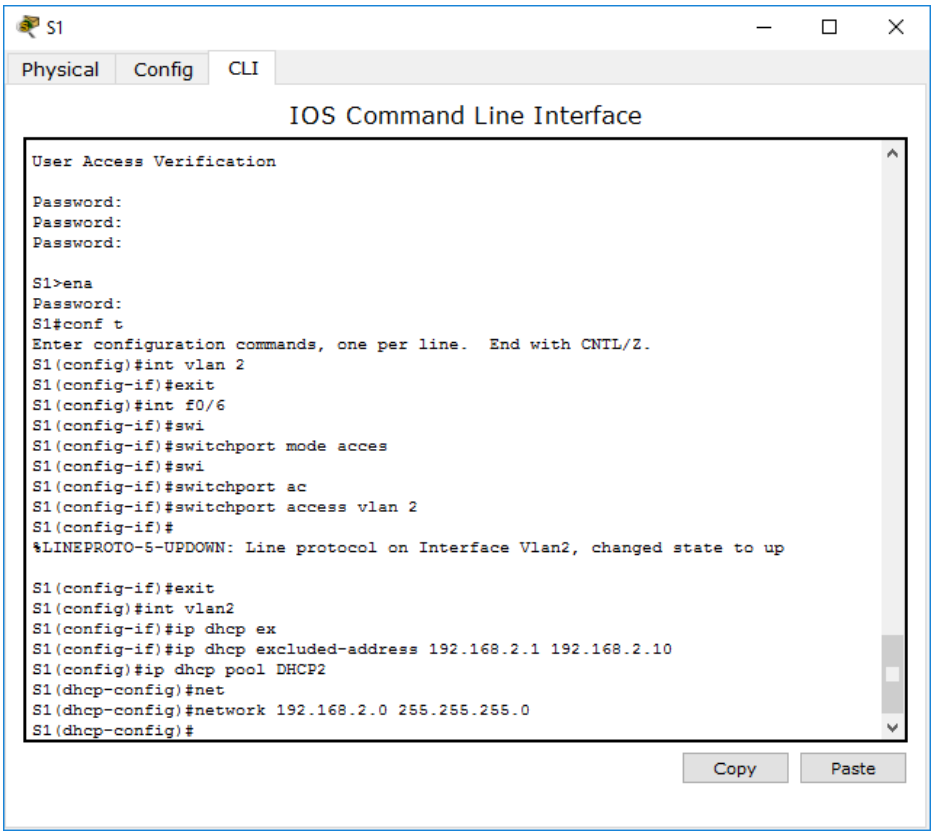
a. Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.



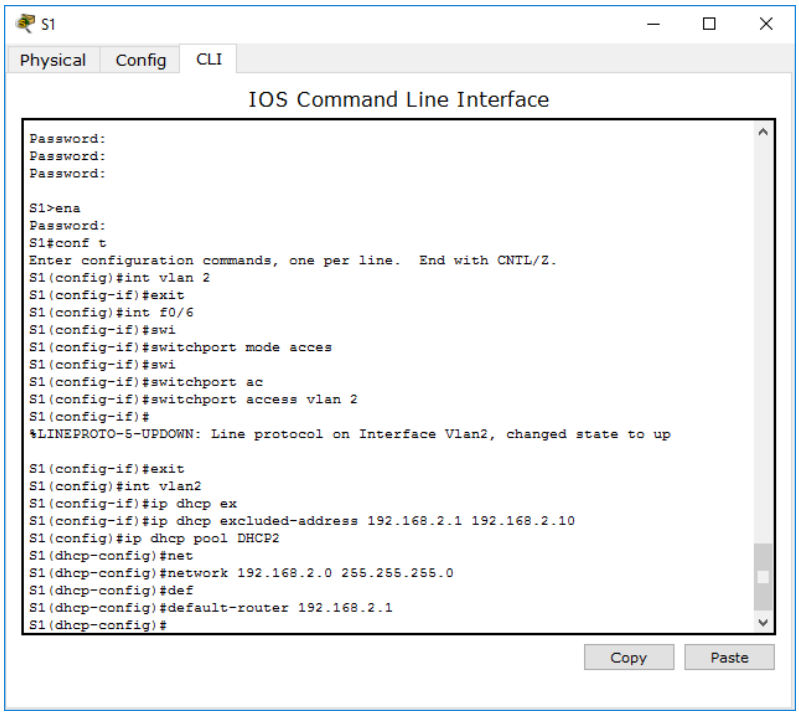
b. Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó.




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

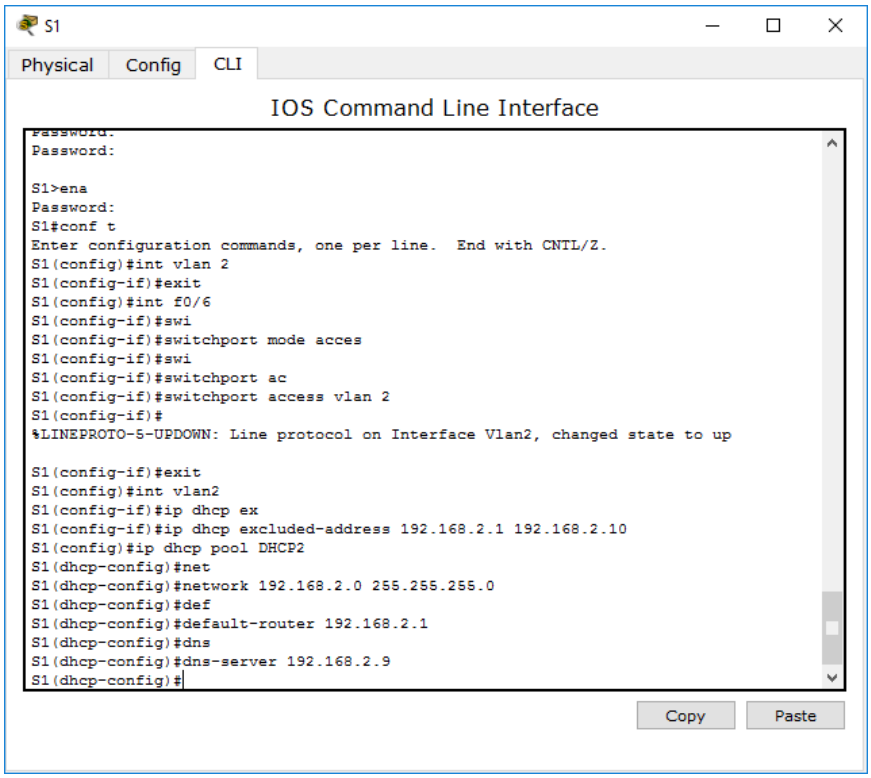



d. Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.

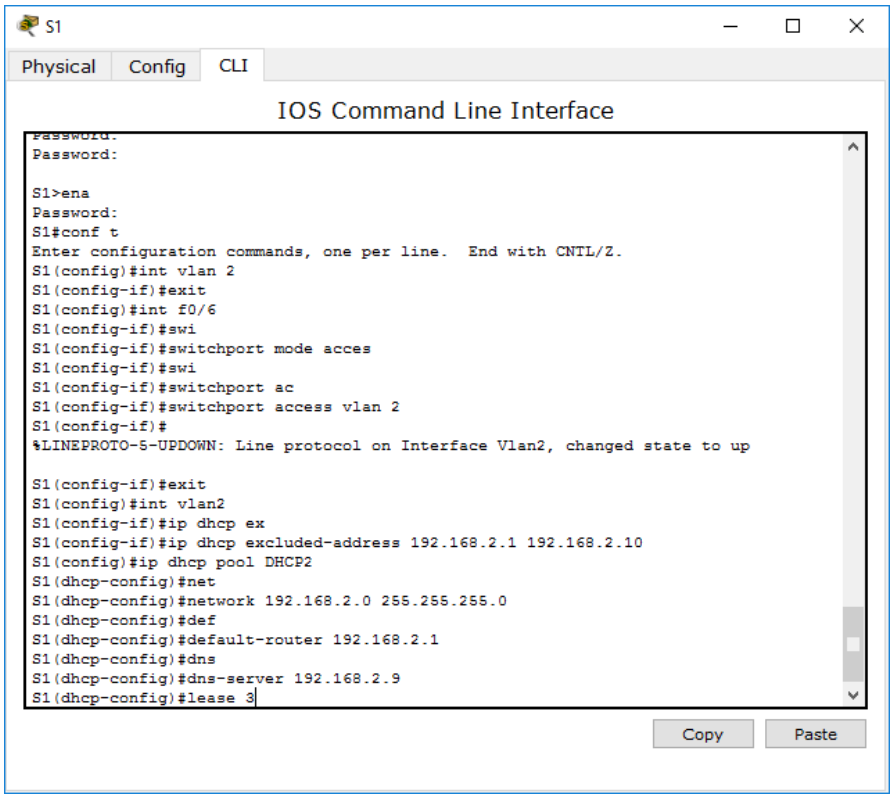



_____

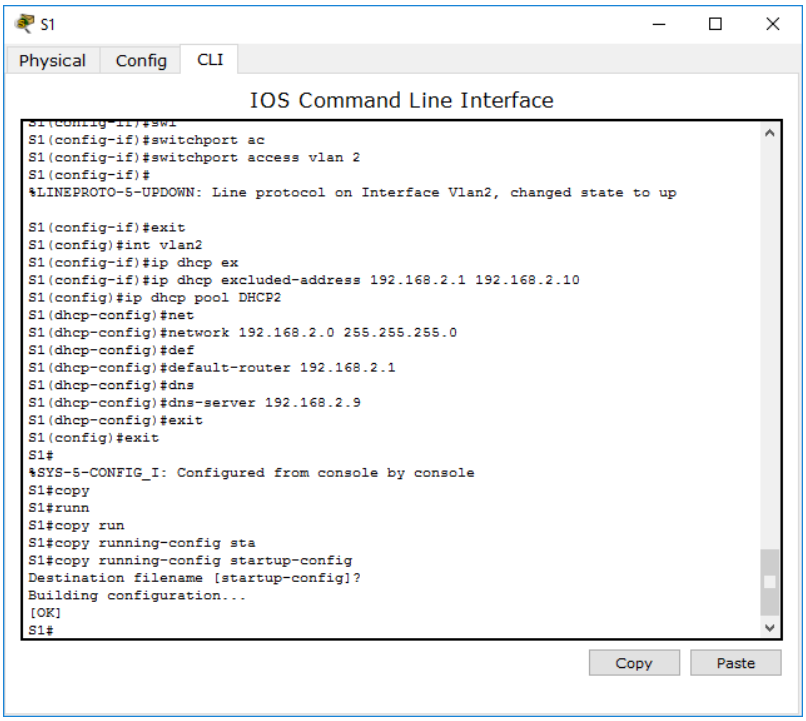
e. Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.




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




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



## Paso 3: verificar la conectividad y DHCPv4.

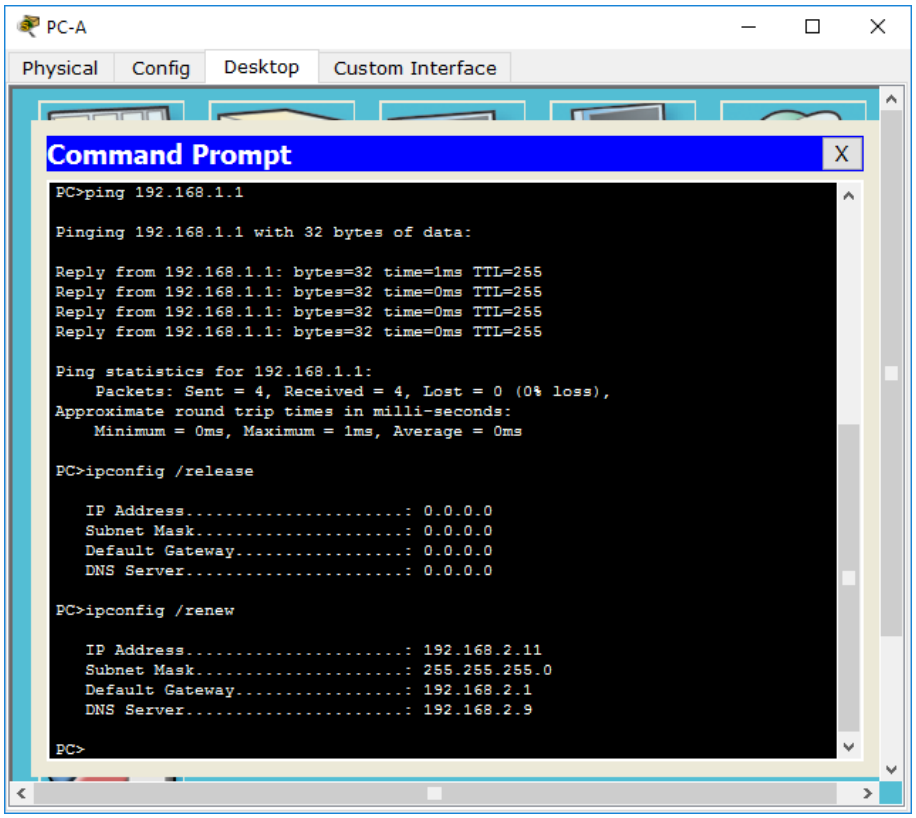
a. En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: _____

Máscara de subred: _____

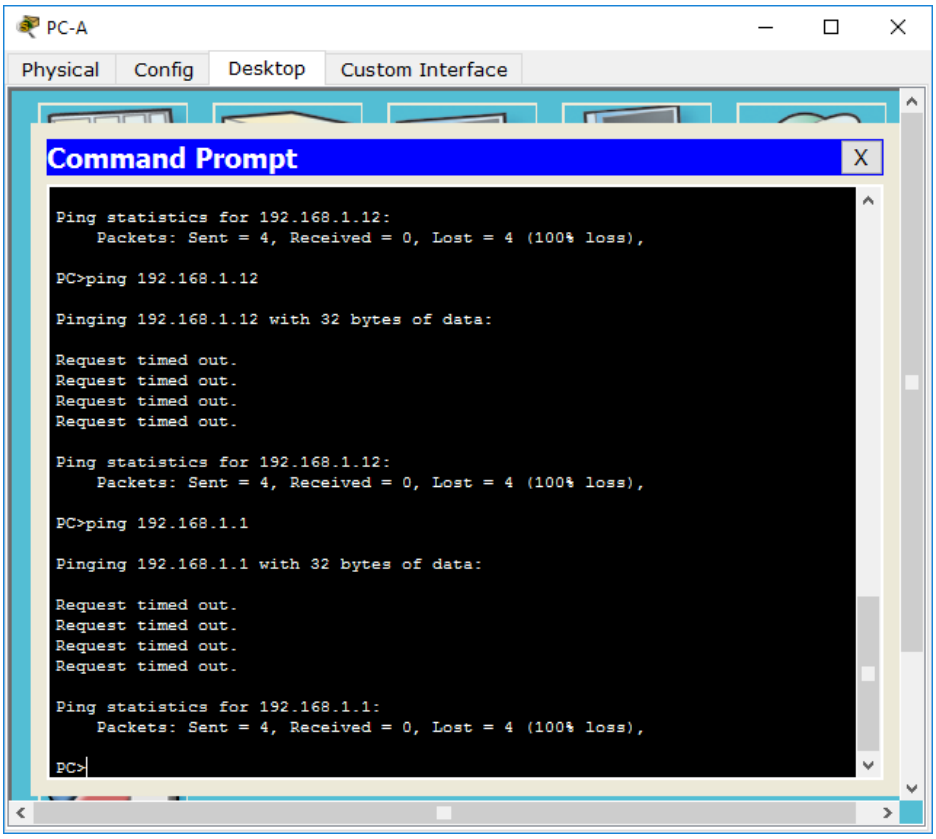
Gateway predeterminado: _____

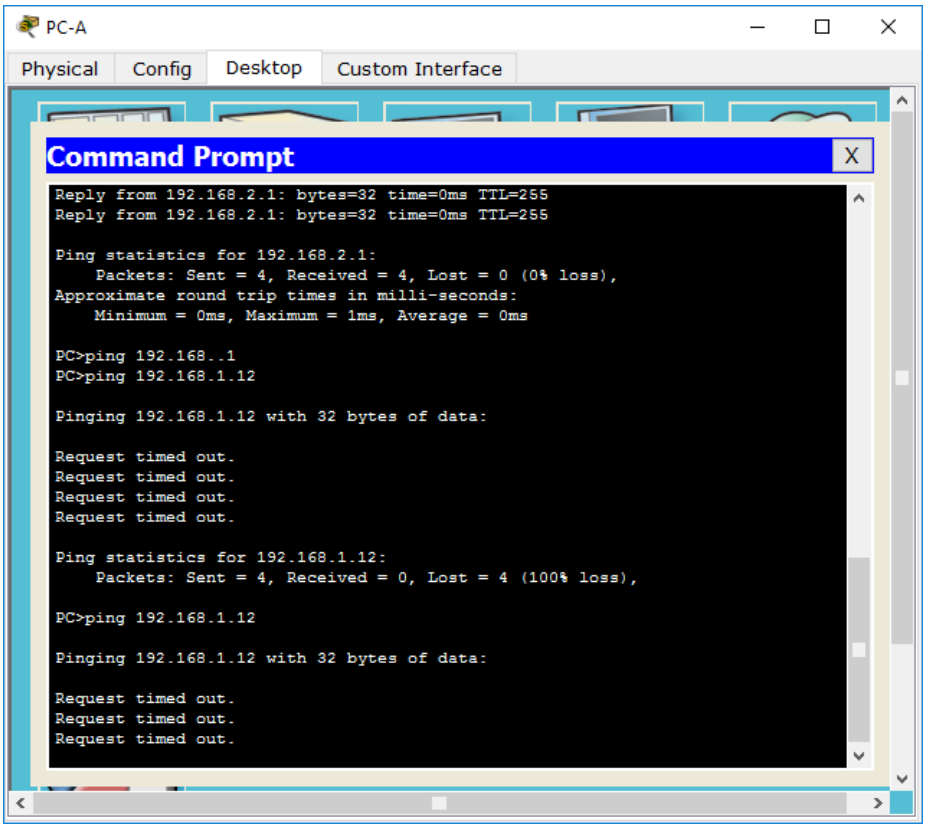



b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado de la VLAN 2 y a la PC-B.

¿Es posible hacer ping de la PC-A al gateway predeterminado? No

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


PC-A
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Ping statistics for 192.168.1.12:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.1.12
Pinging 192.168.1.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.12:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>

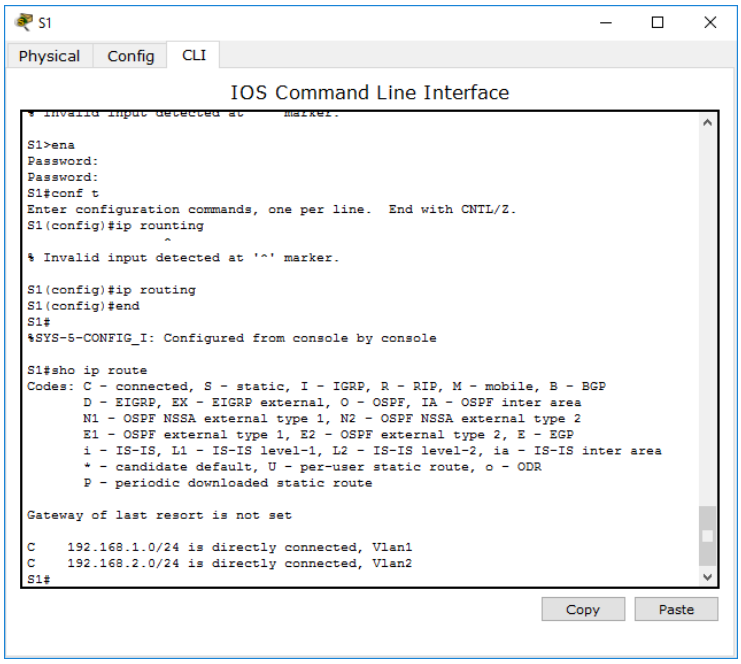



¿Los pings eran correctos? ¿Por qué?

No se alcanzan los pings por que los equipos están configurados en Vlan diferentes

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

¿Qué resultado arrojó este comando?



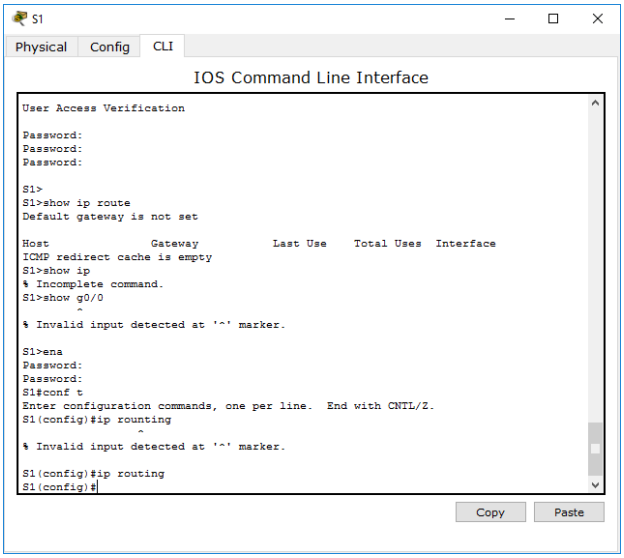

# Parte 11:habilitar el routing IP

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.

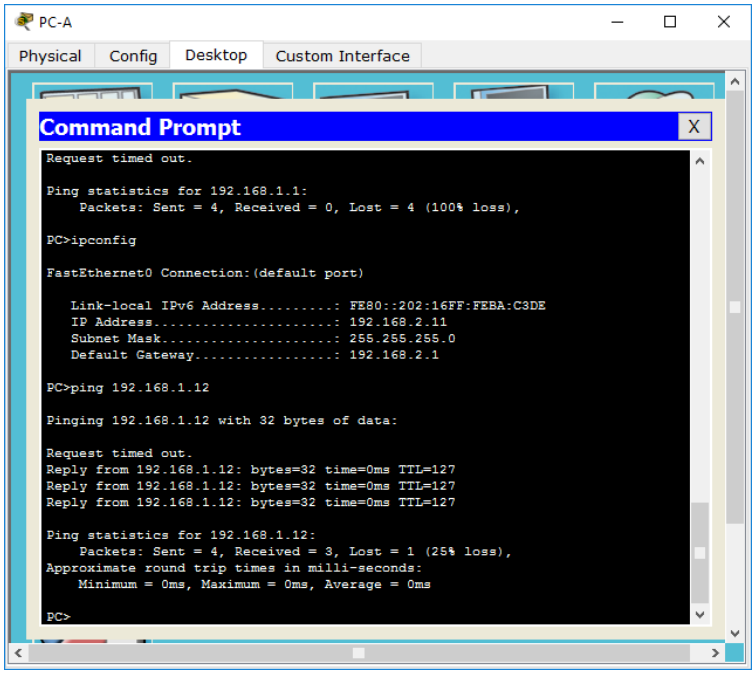
```
S1(config)# ip routing
```



b. Verificar la conectividad entre las VLAN.

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

¿Qué función realiza el switch? Router

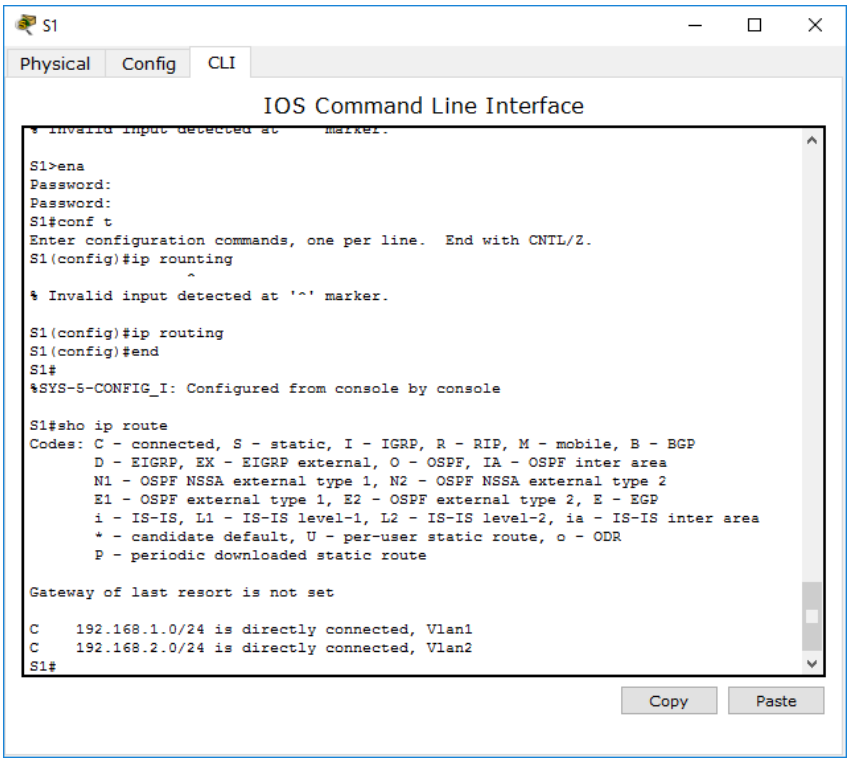



_____

_____

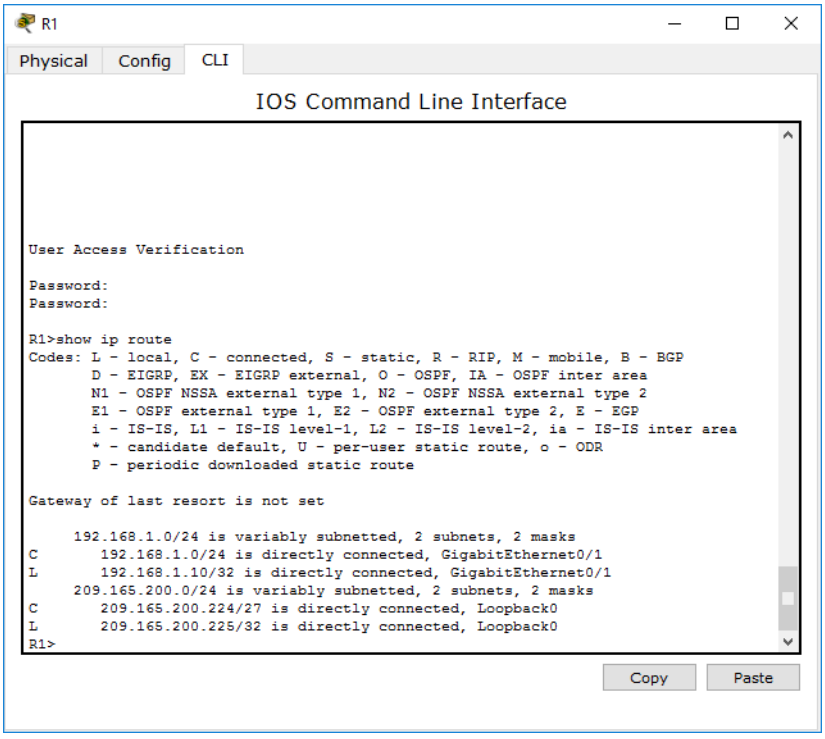
c. Vea la información de la tabla de routing para el S1.

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



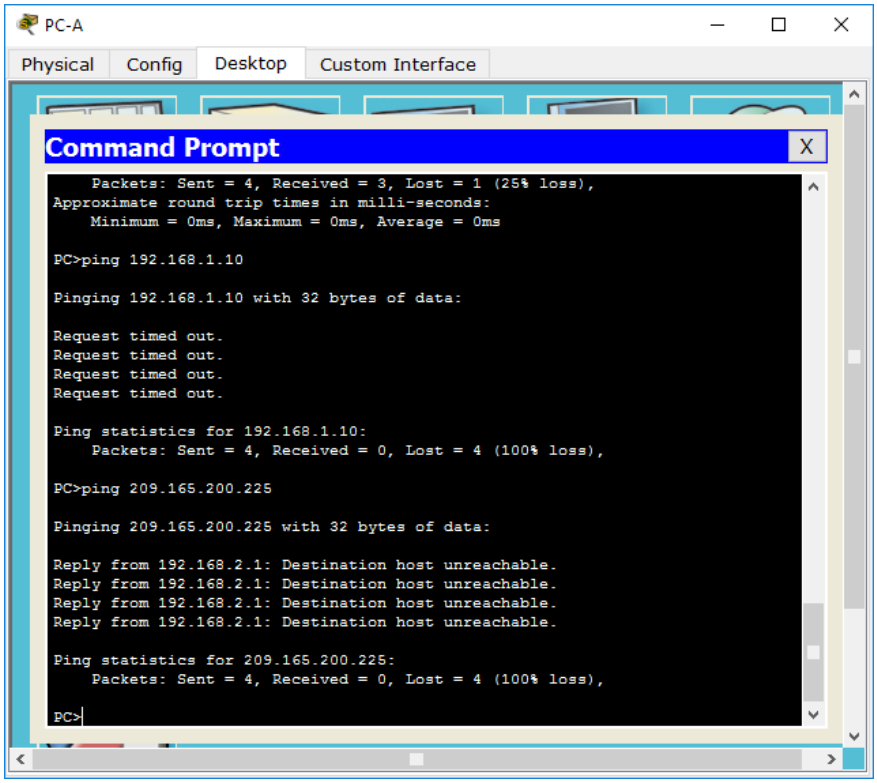

d. Vea la información de la tabla de routing para el R1.

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



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



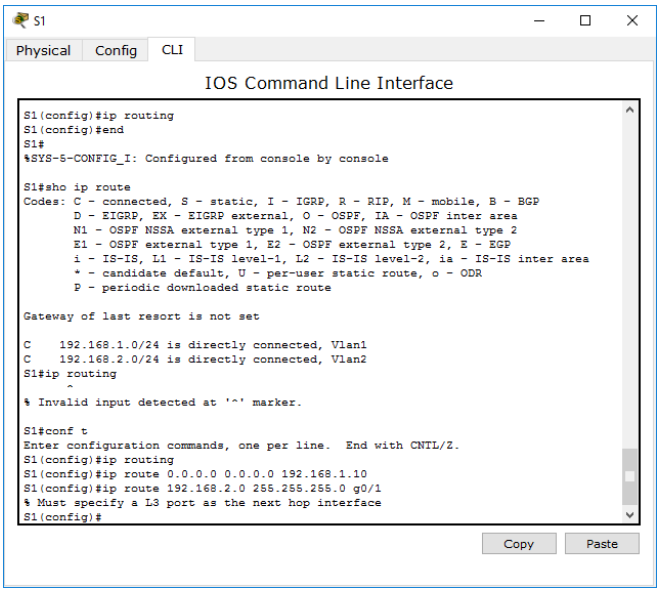

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Una ruta estatica

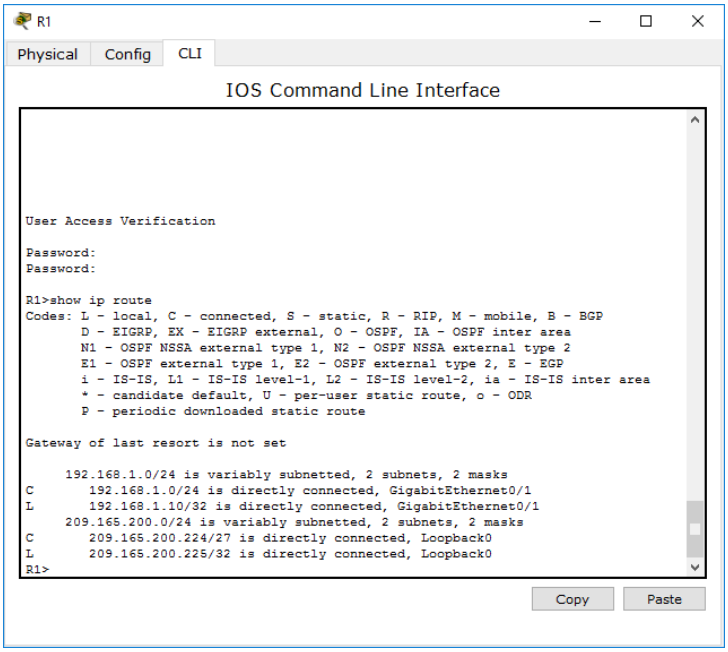
## Paso 2: asignar rutas estáticas.

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.




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

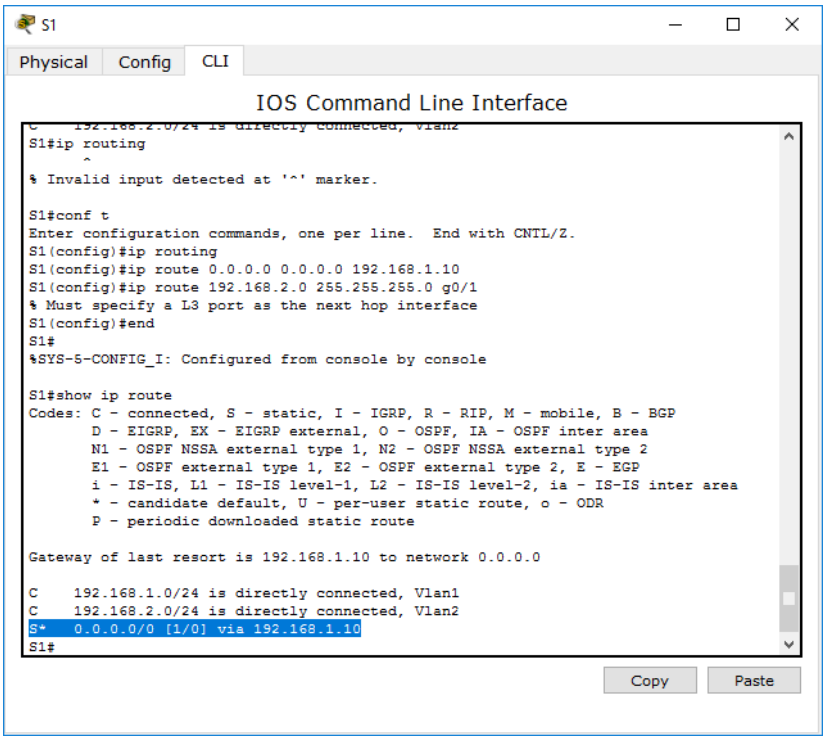



_____

_____

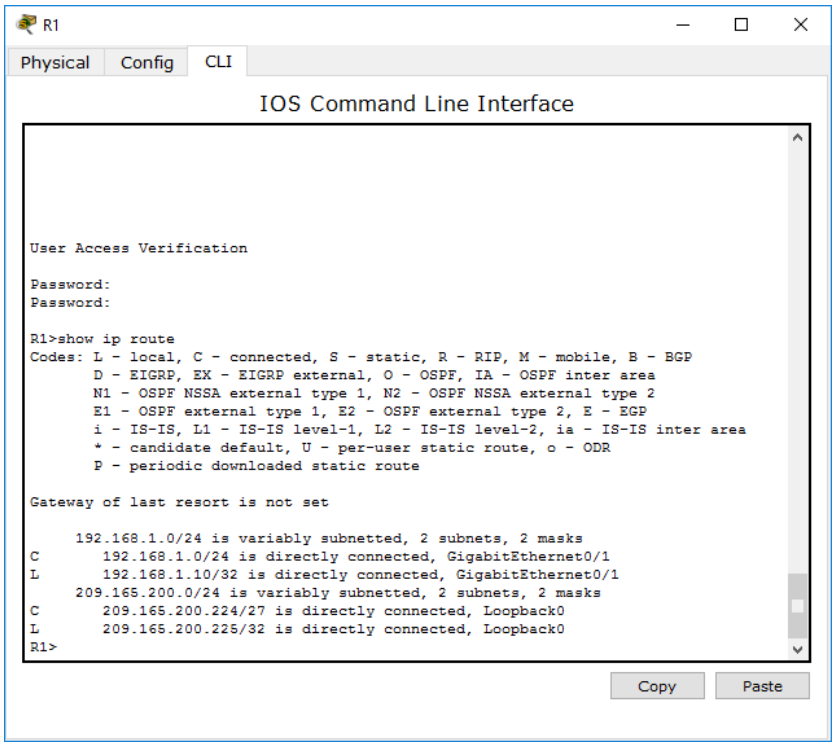
c. Vea la información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?




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

¿Cómo está representada la ruta estática?



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

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

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

   Reservas para no crear conflictos con los equipos de ruteo

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

   Dependiendo de la Vlan en la que este

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

   Ruteo capa 3

## 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
```

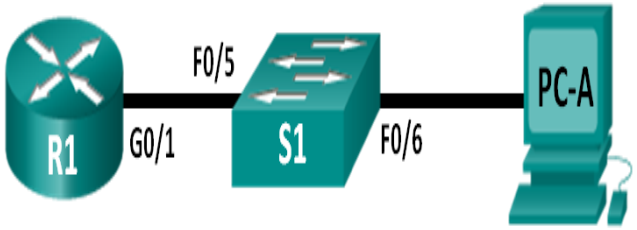
Universidad Nacional Abierta y a Distancia

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

# 10.2.3.5

# Práctica de laboratorio: configuración de dhcpv6 sin estado y con estado

## Topología



## Tabla de direccionamiento

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

## Objetivos

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

**Parte 2: configurar la red para SLAAC**

**Parte 3: configurar la red para DHCPv6 sin estado**

**Parte 4: configurar la red para DHCPv6 con estado**

## Información básica/situación

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

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

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

dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

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

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

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

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

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

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

S1# **show sdm prefer**

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

S1# **config t**

S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**

S1(config)# **end**

S1# **reload**

**Recursos necesarios**

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

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

## Parte 12. armar la red y configurar los parámetros básicos de los dispositivos

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

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

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

**Paso 3. Configurar R1**

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo.

c. Cifre las contraseñas de texto no cifrado.

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

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

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

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

h. Guardar la configuración en ejecución en la configuración de inicio.

**Paso 4. configurar el S1.**

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo.

c. Cifre las contraseñas de texto no cifrado.

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

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

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

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

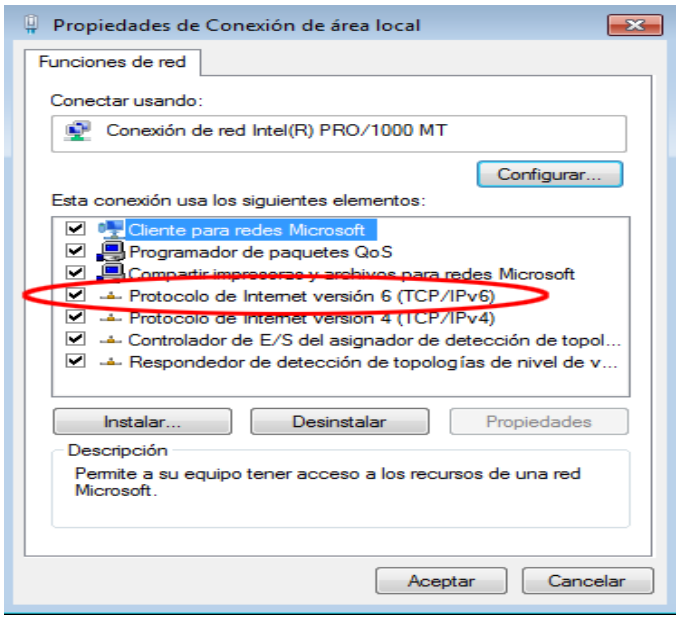
h. Desactive administrativamente todas las interfaces inactivas.

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

## Parte 13. configurar la red para SLAAC

### Paso 1. preparar la PC-A.

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



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

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


**Paso 2. Configurar R1**

a. Habilite el routing de unidifusión IPv6.

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

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

d. Active la interfaz G0/1.

**Paso 3. verificar que el R1 forme parte del grupo de multidifusión de todos los routers.**

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

R1# **show ipv6 interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::1

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF00:1

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.

**Paso 4. configurar el S1.**

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

S1(config)# **interface vlan 1**

S1(config-if)# **ipv6 address autoconfig**

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

**Paso 5. verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.**

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

S1# **show ipv6 interface**

Vlan1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40

No Virtual link-local address(es):

Stateless address autoconfig enabled

Global unicast address(es):

2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]

valid lifetime 2591988 preferred lifetime 604788

Joined group address(es):

FF02::1

FF02::1:FFE8:8A40

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

Output features: Check hwidb

ND DAD is enabled, number of DAD attempts: 1

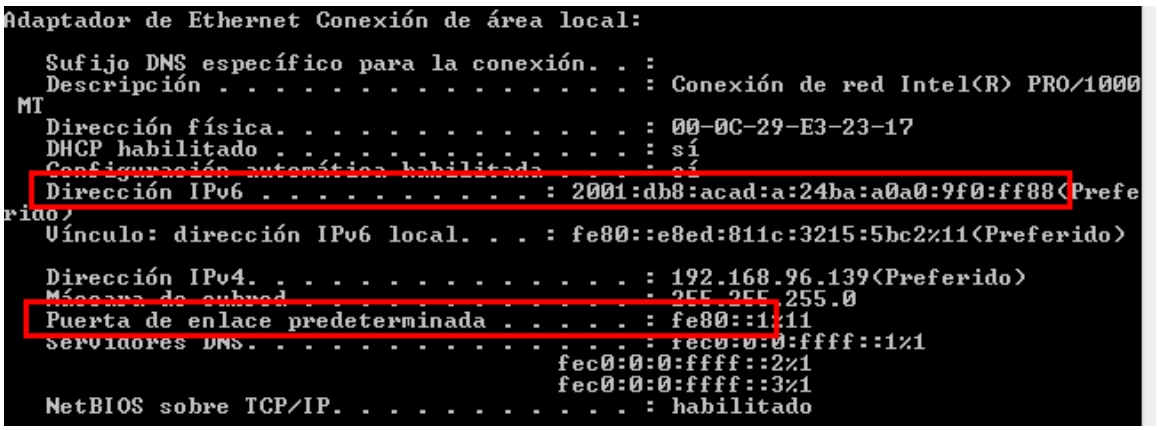
ND reachable time is 30000 milliseconds (using 30000)

ND NS retransmit interval is 1000 milliseconds

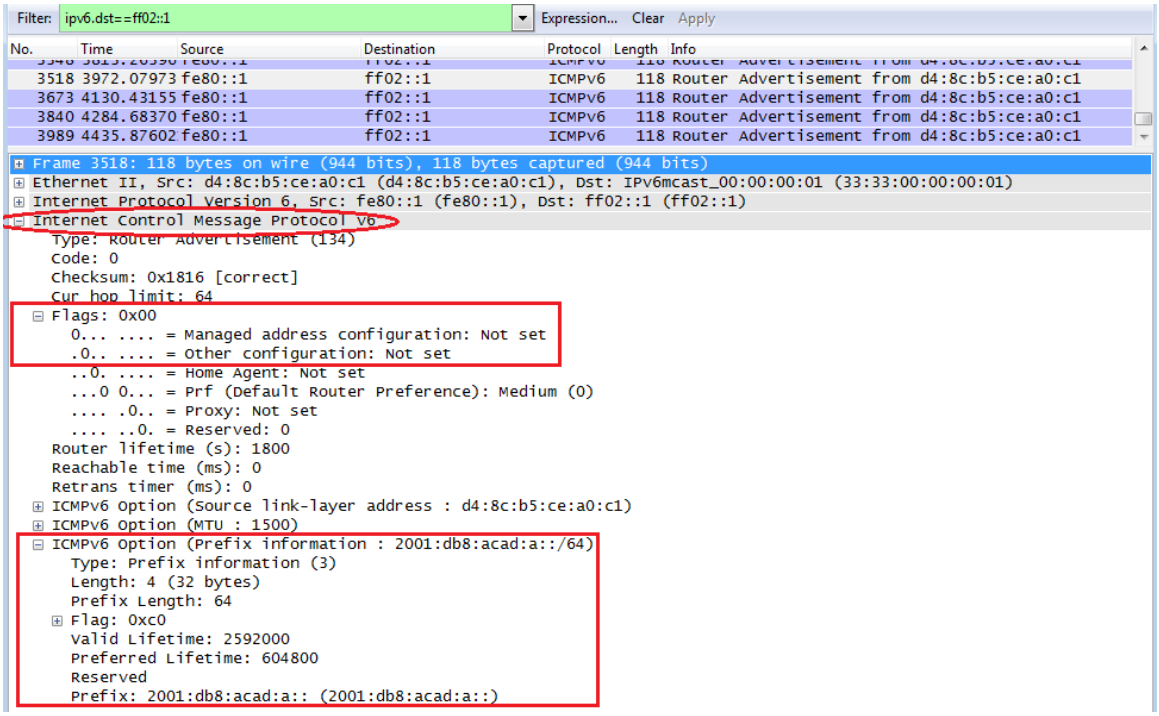
Default router is FE80::1 on Vlan1

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

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




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




## Parte 14. configurar la red para DHCPv6 sin estado

### Paso 1. configurar un servidor de DHCP IPv6 en el R1.

a. Cree un pool de DHCP IPv6.

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

b. Asigne un nombre de dominio al pool.

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

c. Asigne una dirección de servidor DNS.

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

R1(config-dhcpv6)# **exit**

d. Asigne el pool de DHCPv6 a la interfaz.

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

R1(config-if)# **ipv6 dhcp server IPV6POOL-A**

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

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

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

**Paso 2. verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.**

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

R1# **show ipv6 interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::1

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:2

FF02::1:FF00:1

FF05::1:3

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.

Hosts use DHCP to obtain other configuration.

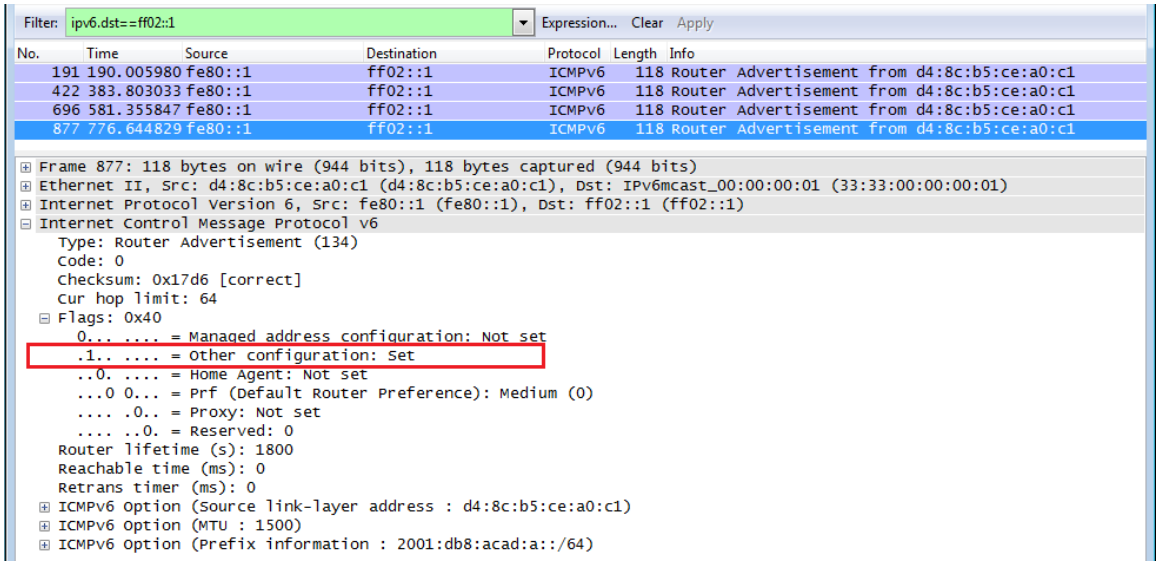
**Paso 3. ver los cambios realizados en la red en la PC-A.**

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

```
Adaptador de Ethernet Conexión de área local:

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

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

Adaptador de túnel isatap.localdomain:

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

**Paso 4. ver los mensajes RA en Wireshark.**

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




**Paso 5. verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.**

Use los comandos **show ipv6 dhcp binding** y **show ipv6 dhcp pool** para verificar que la 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

**Paso 6. restablecer la configuración de red IPv6 de la PC-A.**

a. Desactive la interfaz F0/6 del S1.

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

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

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

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

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

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

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

## Parte 15. configurar la red para DHCPv6 con estado

### Paso 1. preparar la PC-A.

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

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


### Paso 2. cambiar el pool de DHCPv6 en el R1.

a. Agregue el prefijo de red al pool.

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

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

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

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

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

R1(config-dhcpv6)# **domain-name ccna-StatefulDHCPv6.com**

R1(config-dhcpv6)# **end**

c. Verifique la configuración del pool de DHCPv6.

R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

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

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

Domain name: ccna-StatefulDHCPv6.com

Active clients: 0

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

R1# **debug ipv6 dhcp detail**

IPv6 DHCP debugging is on (detailed)

**Paso 3. establecer el indicador en G0/1 para DHCPv6 con estado.**

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

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

R1(config-if)# **shutdown**

R1(config-if)# **ipv6 nd managed-config-flag**

R1(config-if)# **no shutdown**

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

**Paso 4. habilitar la interfaz F0/6 en el S1.**

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

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

S1(config-if)# **no shutdown**

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

**Paso 5. verificar la configuración de DHCPv6 con estado en el R1.**

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

R1# **show ipv6 interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::1

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:2

FF02::1:FF00:1

FF05::1:3

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use DHCP to obtain routable addresses.

Hosts use DHCP to obtain other configuration.

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

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

R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

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

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

Domain name: ccna-StatefulDHCPv6.com

Active clients: 1

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

comando **show** con la dirección IPv6 que se indica con el comando **ipconfig /all** en la PC-A.

R1# **show ipv6 dhcp binding**

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

DUID: 0001000117F6723D000C298D5444

Username : unassigned

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

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

preferred lifetime 86400, valid lifetime 172800

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

```
Adaptador de Ethernet Conexión de área local:

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

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

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

**Nota:** escribir **u all** es la forma más abreviada de este comando y sirve para saber si quiere evitar que los mensajes de depuración se desplacen hacia

abajo constantemente en la pantalla de la sesión de terminal. Si hay varias depuraciones en proceso, el comando **undebug all** las detiene todas.

R1# **u all**

Se ha desactivado toda depuración posible

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Mar 5 16:42:39.779: 00030001FC994775C3E0

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

*Mar 5 16:42:39.779: 00010001

R1#17F6723D000C298D5444

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

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

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

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

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

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

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

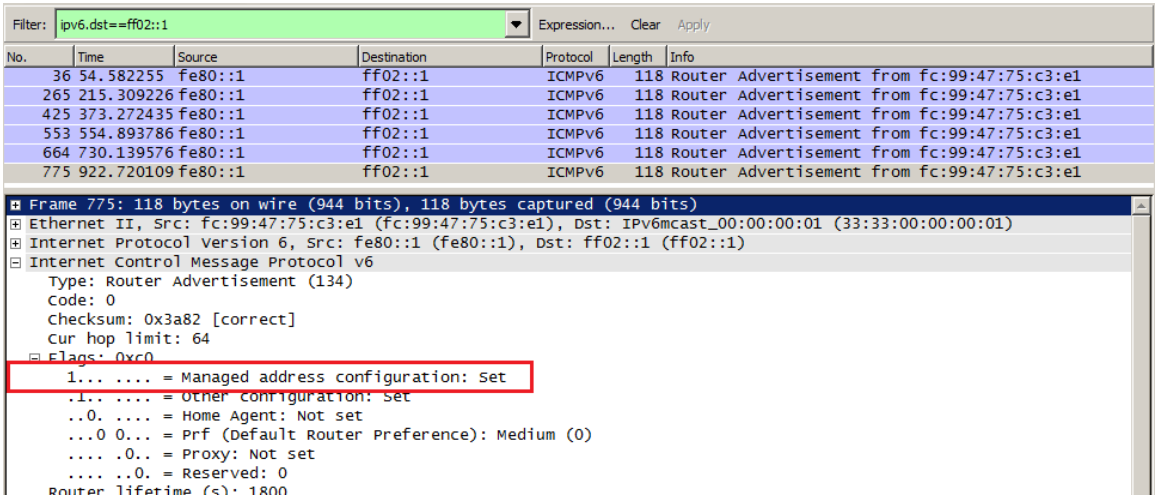
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26

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

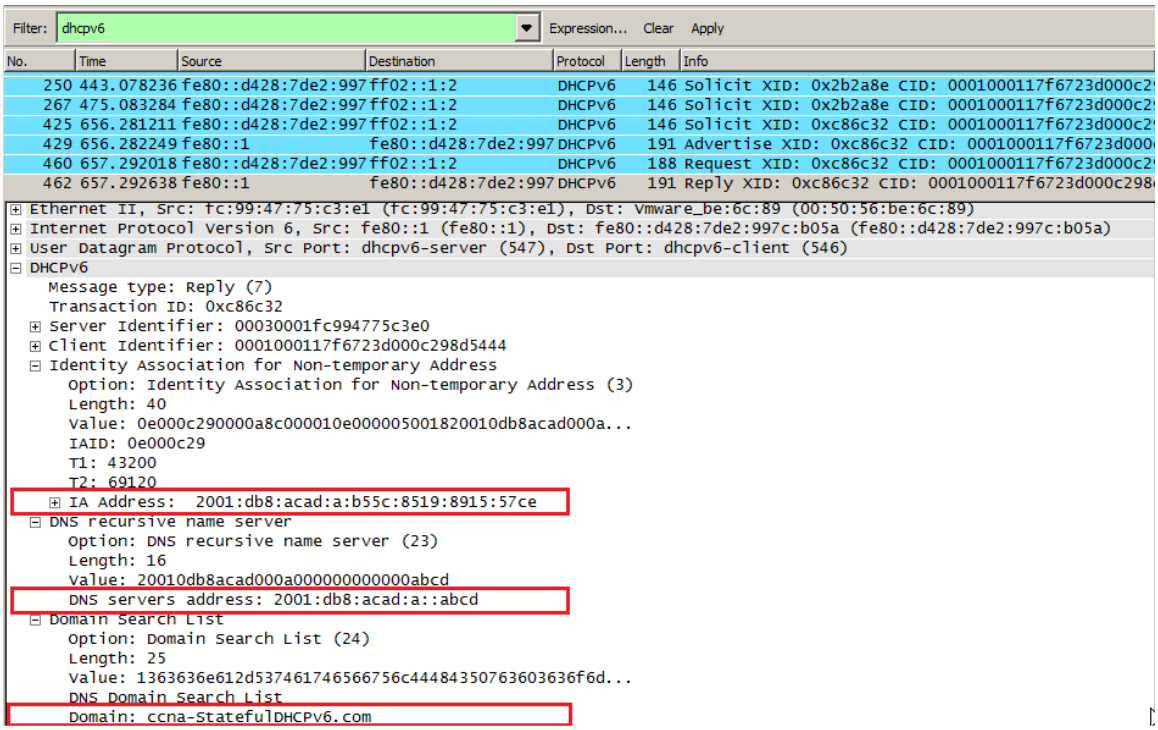
**Paso 6. verificar DHCPv6 con estado en la PC-A.**

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

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




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



**Reflexión**

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

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

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

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

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

**Tabla de 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.

Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

# 10.3.1.1
# IdT y DHCP

## Objetivo

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

## Situación

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

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

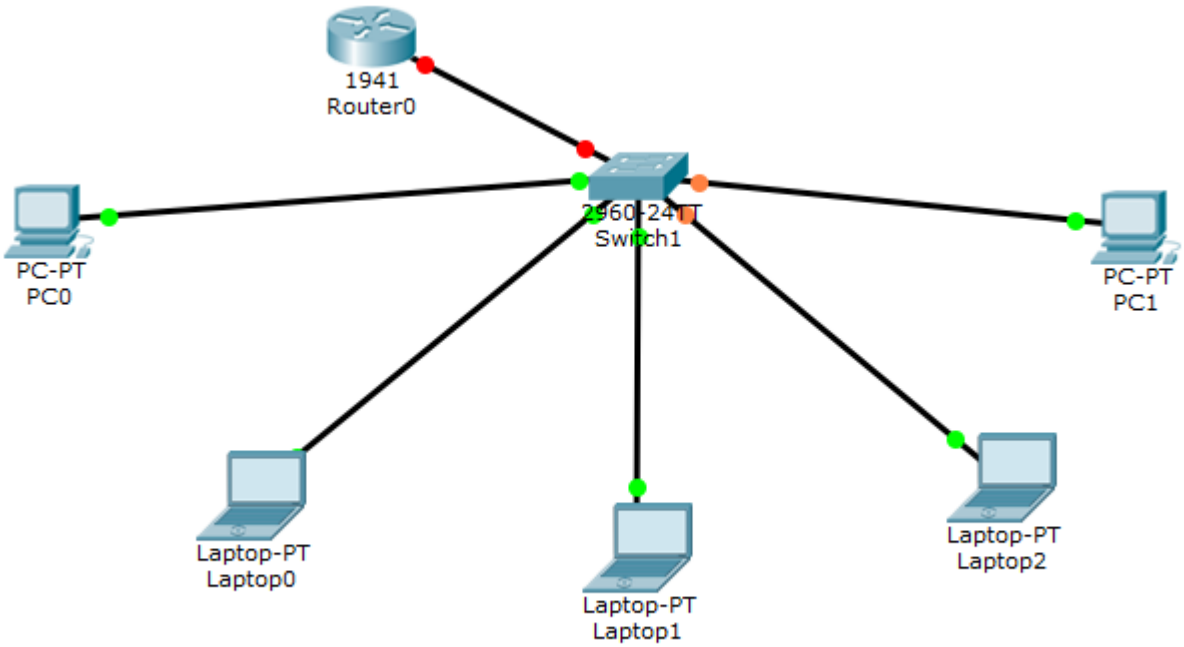
Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

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

## Recursos necesarios

Software de Packet Tracer

**SOLUCION =>**




**Configuración inicial del Router =>**

- Asignamos nombre e IP de la interface G0/1 al router:

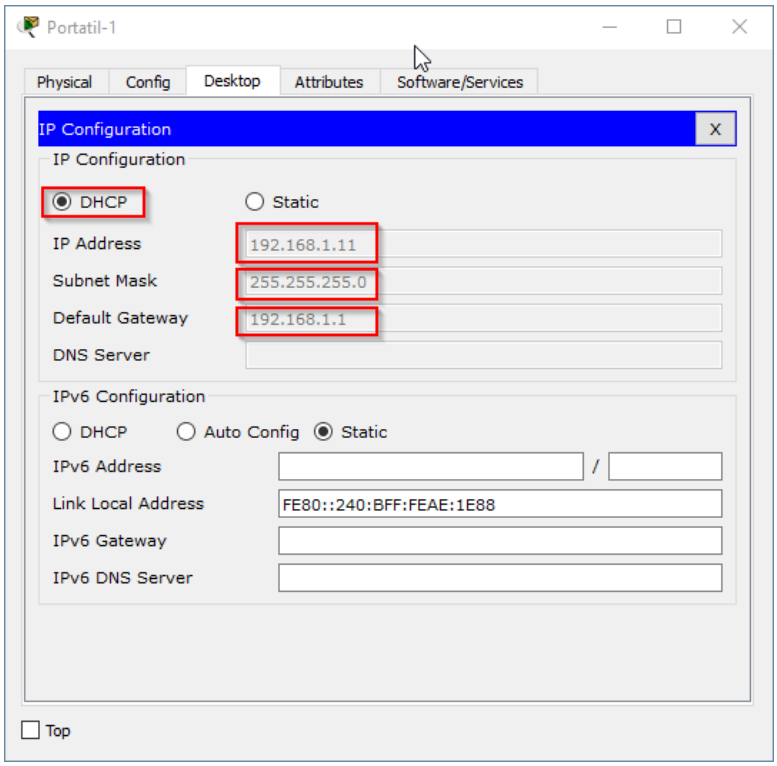
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#Hostname R1
R1(config)#int g0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no Sh

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

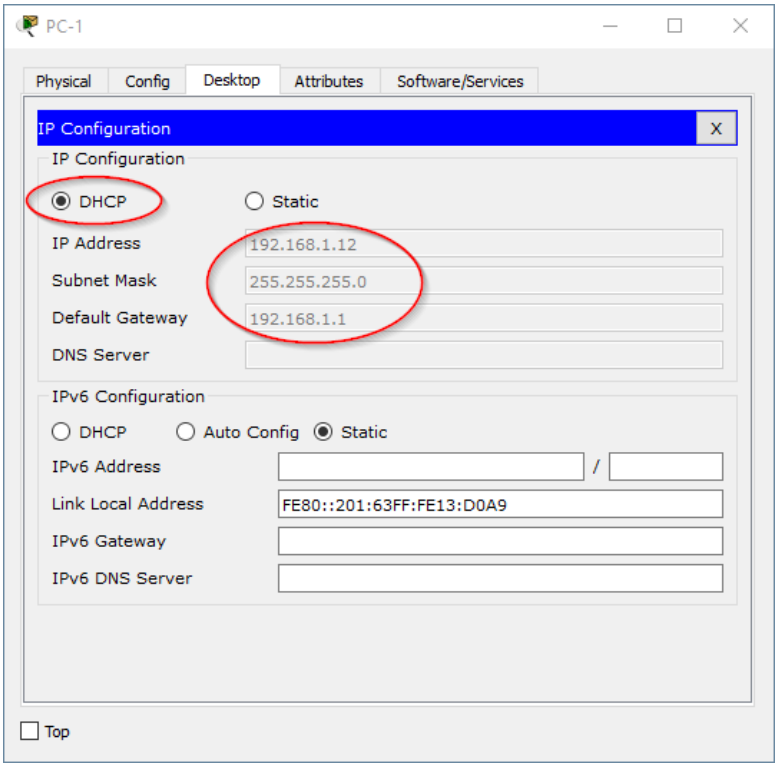
- Configuramos la parte del DHCP(que asigne ip's de la 192.168.1.11 en adelante):

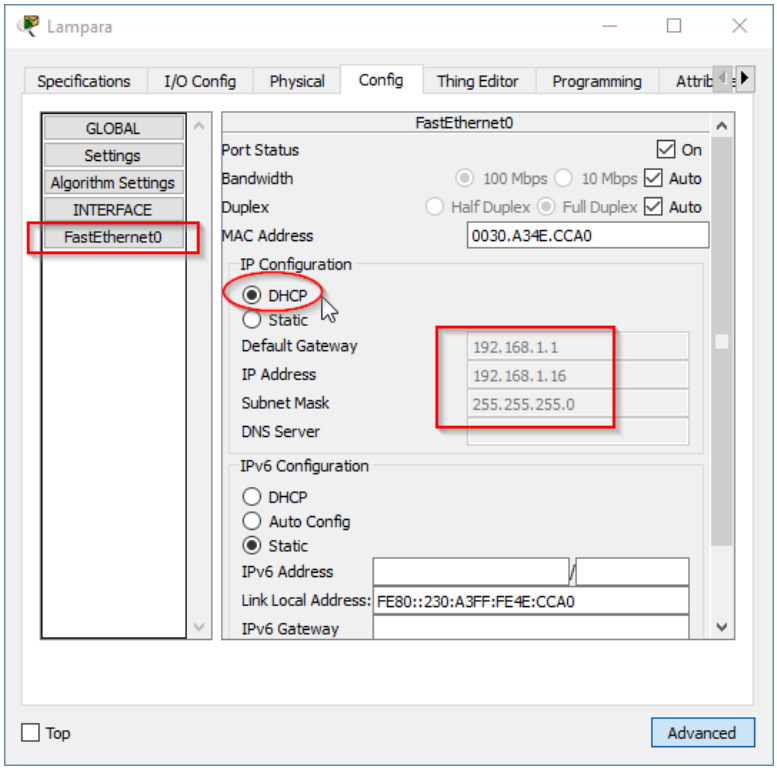
```
R1(config-if)#exit
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
R1(config)#ip dhcp pool LAN
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#exit
R1(config)#
```

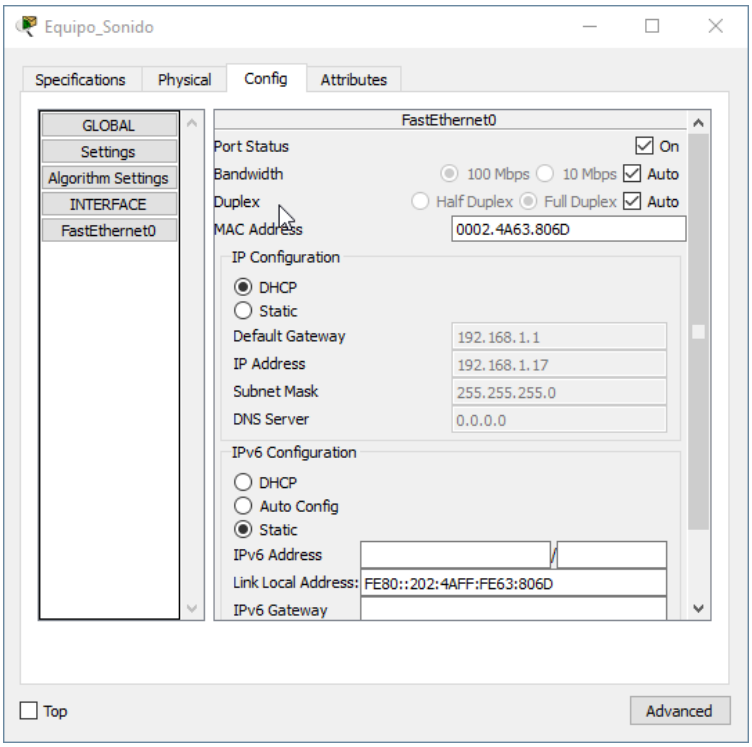
**Configuración de los dispositivos =>**

- Creamos el direccionamiento automático en los diferentes dispositivos:


Portatil-1
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.11
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::240:BFF:FEAE:1E88
IPv6 Gateway
IPv6 DNS Server
Top

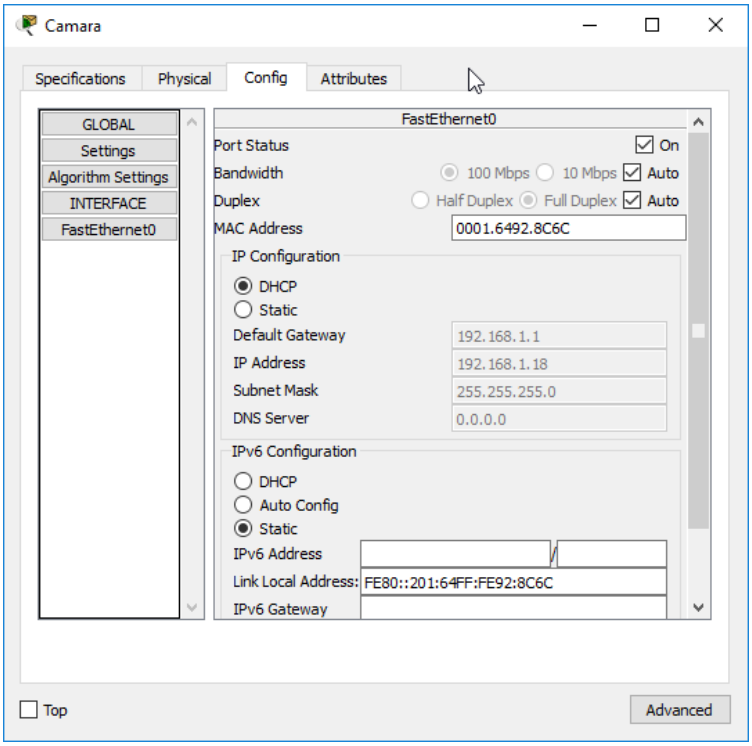

PC-1
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:63FF:FE13:D0A9
IPv6 Gateway
IPv6 DNS Server
Top

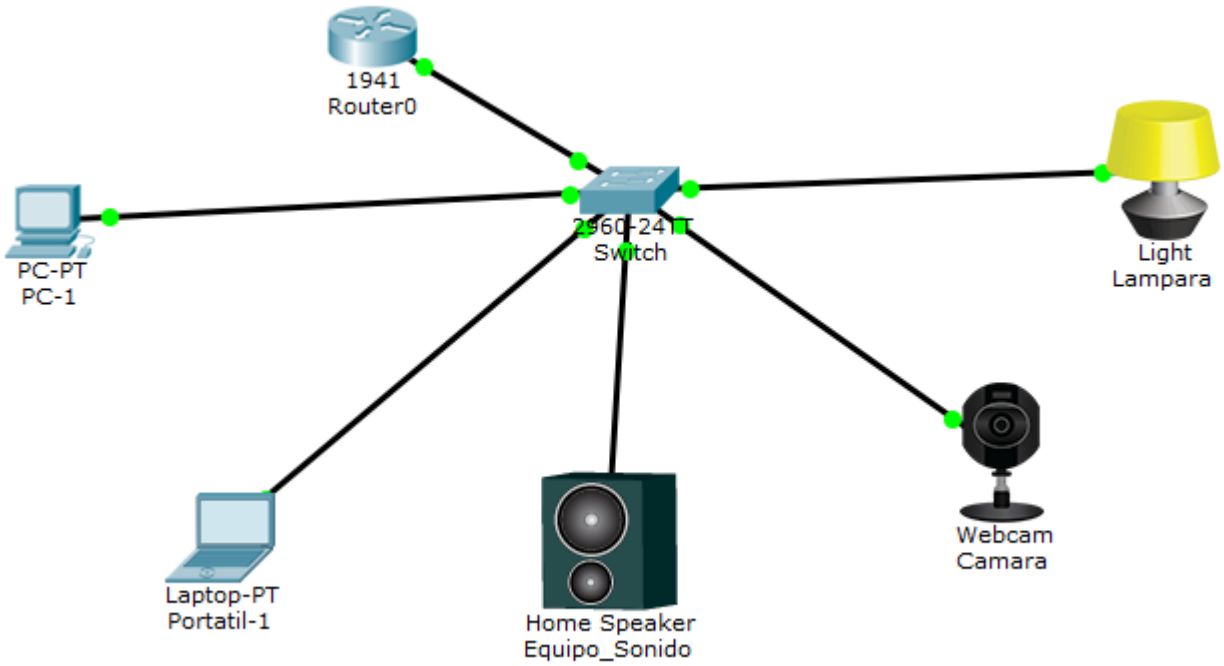

Lampara
Specifications
I/O Config
Physical
Config
Thing Editor
Programming
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0030.A34E.CCA0
IP Configuration
DHCP
Static
Default Gateway
192.168.1.1
IP Address
192.168.1.16
Subnet Mask
255.255.255.0
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address:
FE80::230:A3FF:FE4E:CCA0
IPv6 Gateway
Top
Advanced


Equipo_Sonido
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0002.4A63.806D
IP Configuration
DHCP
Static
Default Gateway
192.168.1.1
IP Address
192.168.1.17
Subnet Mask
255.255.255.0
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address:
FE80::202:4AFF:FE63:806D
IPv6 Gateway
Top
Advanced

Universidad Nacional Abierta y a Distancia

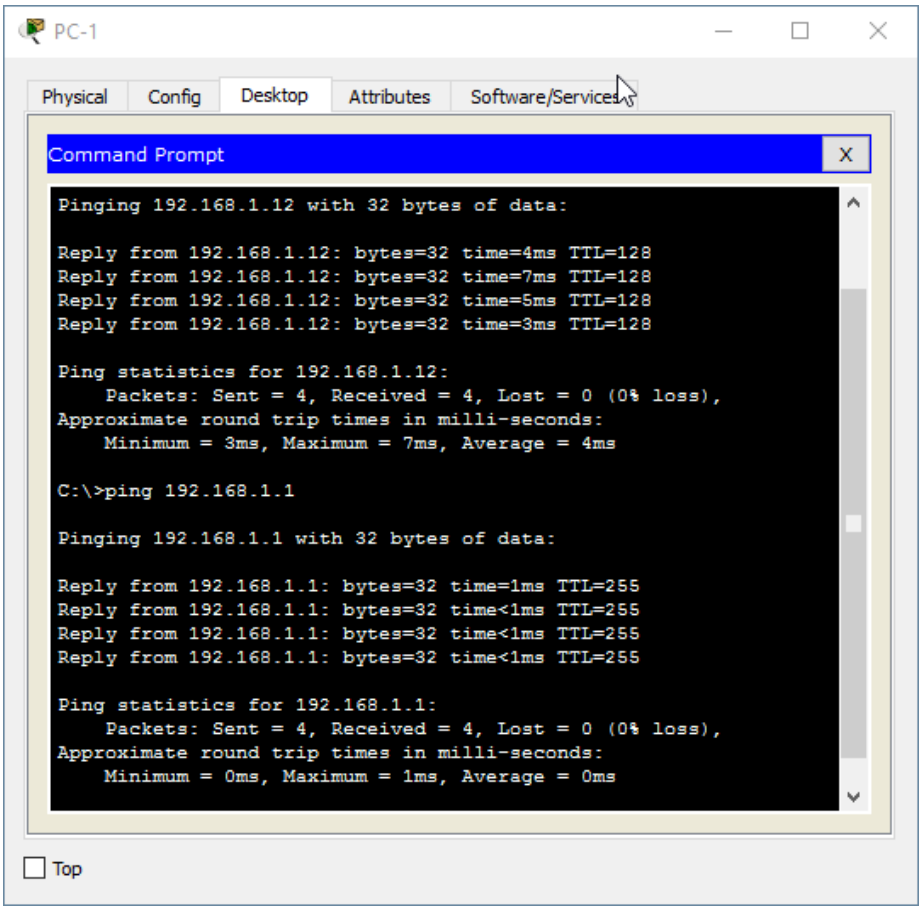
Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2



Diplomado profundización CISCO (Diseño e implementación soluciones integradas LAN/WAN) 2017-2

**Probamos conectividad entre equipos y router =>**




## 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?

   **Porque el Router 1941ofrece una amplia gama de servicios de seguridad en comparacion con otros ISR por lo cual es mas confiable si de prestaciones y seguridad se trata. Pero si se puede usar un ISR mas pequeño como servidor dchp, pero el rendimiento es menor y puede ser vulnerable a ataques informáticos.**

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

   **- Control de Electrodomesticos (Domotica) en el hogar u oficina.**

   **- Identificación de errores de dispositivos de Red para su correspondiente mantenimiento.**

**- Sistemas cerrados de televisión (Vigilancia).**

**- Control de Procesos de una empresa atraves de una red dhcp.**

**- Control y monitoreo de PLC's, IED's y cualquier elemento de una Red en cualquier Empresa**

## 11.2.2.6. Práctica de laboratorio: configuración de NAT dinámica y estática

### Topología


### Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
|---|---|---|---|---|
| Gateway | G0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| | S0/0/1 | 209.165.201.18 | 255.255.255.252 | N/A |
| ISP | S0/0/0 (DCE) | 209.165.201.17 | 255.255.255.252 | N/A |
| | Lo0 | 192.31.7.1 | 255.255.255.255 | N/A |
| Server ISP | NIC | 192.31.7.2 | 255.255.255.0 | 192.31.7.1 |
| 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 |

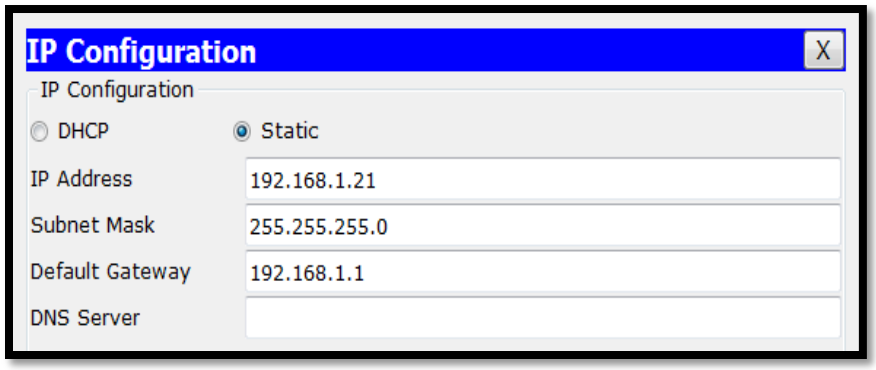
### Parte 1. Armar la red y verificar la conectividad

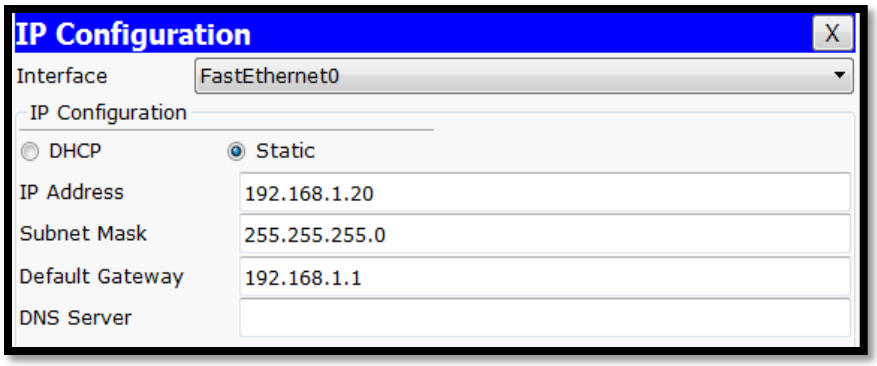
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas

**Paso 7. Realizar el cableado de red tal como se muestra en la topología.**

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

**Paso 8. Configurar los equipos host.**




**Paso 9. Inicializar y volver a cargar los routers y los switches según sea necesario.**

**Paso 10. Configurar los parámetros básicos para cada router.**

**Paso 11. Crear un servidor web simulado en el ISP.**

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

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

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

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

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

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

## Paso 12. Configurar el routing estático.

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

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

b. Cree una ruta predeterminada del router Gateway al router ISP.

```
gateway#conf t
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
```

## Paso 13. Guardar la configuración en ejecución en la configuración de inicio.

## Paso 14. 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>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=19ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=3ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 5ms
```

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
```

```
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

     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
```

**Configurar y verificar la NAT estática.**

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

## Paso 15. Configurar una asignación estática.

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20
209.165.200.225
```

## Paso 16. 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)#ip nat inside source static 192.168.1.20 209.165.200.225
gateway(config)#interface g0/1
gateway(config-if)#ip nat inside
gateway(config-if)#interface s0/0/1
gateway(config-if)#ip nat outside
```

## Paso 17. Probar la configuración.

a. Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
```

¿Cuál es la traducción de la dirección host local interna?
**192.168.1.20 = 209.165.200.225**

¿Quién asigna la dirección global interna?
**Router NAT pool**

¿Quién asigna la dirección local interna?
**El administrador de red**

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

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=12ms TTL=254
Reply from 192.31.7.1: bytes=32 time=13ms TTL=254
Reply from 192.31.7.1: bytes=32 time=13ms TTL=254
Reply from 192.31.7.1: bytes=32 time=12ms 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 = 12ms, Maximum = 13ms, Average = 12ms
```

```
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 209.165.200.225:65192.168.1.20:65    192.31.7.1:65      192.31.7.1:65
icmp 209.165.200.225:66192.168.1.20:66    192.31.7.1:66      192.31.7.1:66
icmp 209.165.200.225:67192.168.1.20:67    192.31.7.1:67      192.31.7.1:67
icmp 209.165.200.225:68192.168.1.20:68    192.31.7.1:68      192.31.7.1:68
icmp 209.165.200.225:69192.168.1.20:69    192.31.7.1:69      192.31.7.1:69
icmp 209.165.200.225:70192.168.1.20:70    192.31.7.1:70      192.31.7.1:70
icmp 209.165.200.225:71192.168.1.20:71    192.31.7.1:71      192.31.7.1:71
icmp 209.165.200.225:72192.168.1.20:72    192.31.7.1:72      192.31.7.1:72
---  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?

**65-66-67-68-69-70-71**

**Nota:** puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

a. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

```
Pro Inside global          Inside local       Outside local      Outside
global
icmp 209.165.200.225:1     192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034  192.31.7.1:23
192.31.7.1:23
--- 209.165.200.225        192.168.1.20       ---                ---
```

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

¿Qué protocolo se usó para esta traducción?

**web**

¿Cuáles son los números de puerto que se usaron?

**Global/local interno: 1034**

**Global/local externo: 23**

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

```
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=12ms TTL=126
Reply from 209.165.200.225: bytes=32 time=15ms TTL=126
Reply from 209.165.200.225: bytes=32 time=12ms TTL=126
Reply from 209.165.200.225: bytes=32 time=12ms 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 = 12ms, Maximum = 15ms, Average = 12ms
```

c. 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
---  209.165.200.225   192.168.1.20       ---                ---
tcp 209.165.200.225:1025192.168.1.20:1025  192.31.7.2:80      192.31.7.2:80
```

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).

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

```
Gateway# show ip nat statics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
```

```
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

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

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

```
gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 82  Misses: 75
Expired translations: 74
Dynamic mappings:
gateway#
```

## Configurar Y Verificar La NAT Dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

### Paso 18. Parte 2. Borrar las NAT.

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

### Paso 19. Definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

**Paso 20. Step 1. Verificar que la configuración de interfaces NAT siga siendo válida.**

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

**Paso 21. definir el conjunto de direcciones IP públicas utilizables.**

```
Gateway(config)# ip nat pool public_access 209.165.200.242
209.165.200.254 netmask 255.255.255.224
```

**Paso 22. definir la NAT desde la lista de origen interna hasta el conjunto externo.**

**Nota:** recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

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

**Paso 23.**

**Paso 24. Probar la configuración.**

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

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=13ms TTL=254
Reply from 192.31.7.1: bytes=32 time=12ms TTL=254
Reply from 192.31.7.1: bytes=32 time=12ms TTL=254
Reply from 192.31.7.1: bytes=32 time=13ms 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 = 12ms, Maximum = 13ms, Average = 12ms
```

```
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 209.165.200.242:5 192.168.1.21:5     192.31.7.1:5       192.31.7.1:5
icmp 209.165.200.242:6 192.168.1.21:6     192.31.7.1:6       192.31.7.1:6
icmp 209.165.200.242:7 192.168.1.21:7     192.31.7.1:7       192.31.7.1:7
icmp 209.165.200.242:8 192.168.1.21:8     192.31.7.1:8       192.31.7.1:8
---  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?

**5 – 6 – 7 – 8**

b. En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.

c. Muestre la tabla de NAT.

```
Pro Inside global        Inside local       Outside local      Outside
global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80     192.31.7.1:80
```

```
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80     192.31.7.1:80
--- 209.165.200.242    192.168.1.22       ---                ---
```

```
gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.225   192.168.1.20       ---                ---
tcp 209.165.200.242:1025192.168.1.21:1025  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1026192.168.1.21:1026  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1027192.168.1.21:1027  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1028192.168.1.21:1028  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1029192.168.1.21:1029  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1030192.168.1.21:1030  192.31.7.2:80      192.31.7.2:80
```

¿Qué protocolo se usó en esta traducción?

**http**

¿Qué números de puerto se usaron?

**Interno: 1025**

**Externo: 80**

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

**80**

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

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 1 (7%), misses 0
Total doors: 0
```

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

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

```
gateway#show ip nat statistics
Total translations: 7 (1 static, 6 dynamic, 6 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 152  Misses: 85
Expired translations: 78
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 6
 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
```

## Paso 25. Eliminar la entrada de NAT estática.

Se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

```
Gateway(config)# no ip nat inside source static 192.168.1.20
209.165.200.225
gateway(config)#no ip nat inside source static 192.168.1.20 209.165.200.225
gateway(config)#

Static entry in use, do you want to delete child entries? [no]: yes
```

b. Borre las NAT y las estadísticas.

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

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=19ms TTL=254
Reply from 192.31.7.1: bytes=32 time=16ms TTL=254
Reply from 192.31.7.1: bytes=32 time=19ms TTL=254
Reply from 192.31.7.1: bytes=32 time=3ms 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 = 3ms, Maximum = 19ms, Average = 14ms
```

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=13ms TTL=254
Reply from 192.31.7.1: bytes=32 time=13ms TTL=254
Reply from 192.31.7.1: bytes=32 time=14ms TTL=254
Reply from 192.31.7.1: bytes=32 time=15ms 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 = 13ms, Maximum = 15ms, Average = 13ms
```

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: 9 (0 static, 9 dynamic, 9 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 160  Misses: 93
Expired translations: 83
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 9
 pool public_access: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13 , allocated 2 (15%), misses 0
```

```
Gateway# 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.

```
gateway#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
tcp 209.165.200.242:1025192.168.1.21:1025  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1026192.168.1.21:1026  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1027192.168.1.21:1027  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1028192.168.1.21:1028  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1029192.168.1.21:1029  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1030192.168.1.21:1030  192.31.7.2:80      192.31.7.2:80
```

**Reflexión**

1. ¿Por qué debe utilizarse la NAT en una red?

   **Por qué se ahorran IP's publicas mayor seguridad debido a que no se muestra la IP de los Host hacia internet por que se usan IP globales asignadas por gateway**

2. ¿Cuáles son las limitaciones de NAT?

   **Hay un tiempo de retraso en el Gateway y algunos servicios no pueden salir hacia internet como por ejemplo SNMP.**

## CONCLUSIONES DEL EJERCICIO

- ✓ En esta actividad se puso en práctica la configuración de NAT estática y dinámica, en el caso de la NAT estática se mapea la dirección IP privada con una dirección IP publica de forma tal que cada equipo en la red privada tiene asignado una IP publica para acceder a internet.

- ✓ Para la NAT dinámica utiliza un pool de IP's privadas que son mapeadas de forma dinámica y a demanda, pero esta solo sirve para establecer conexiones que vayan desde el interior de la red privada hasta la red pública, realizar esta configuración se deben conocer 3 datos.

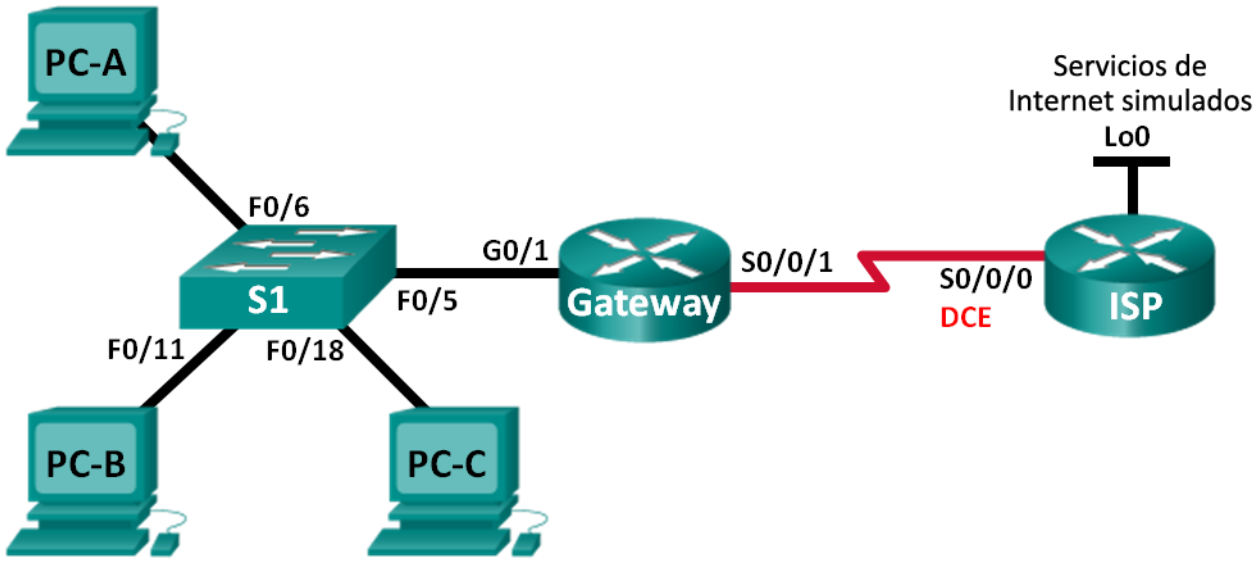
- Direcciones internas a traducir con el fin de limitar el rango

- Direcciones externas globales a traducir
- Interfaces involucradas en el intercambio.

**11.2.3.7**

**Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT**

**Topología**



## Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
|---|---|---|---|---|
| Gateway | G0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| | S0/0/1 | 209.165.201.18 | 255.255.255.252 | N/A |
| ISP | S0/0/0 (DCE) | 209.165.201.17 | 255.255.255.252 | N/A |
| | Lo0 | 192.31.7.1 | 255.255.255.255 | N/A |
| PC-A | NIC | 192.168.1.20 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.1.21 | 255.255.255.0 | 192.168.1.1 |
| PC-C | NIC | 192.168.1.22 | 255.255.255.0 | 192.168.1.1 |

## Objetivos

**Parte 1: armar la red y verificar la conectividad**

**Parte 2: configurar y verificar un conjunto de NAT con sobrecarga**

**Parte 3: configurar y verificar PAT**

## Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

En la parte 2, el ISP asignó una única dirección IP, 209.165.201.18, a su empresa para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Usará la traducción de la dirección del puerto (PAT) para convertir varias direcciones internas en la única dirección pública utilizable. Se

probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

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

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

**Recursos necesarios**

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

**Parte 16. armar la red y verificar la conectividad**

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

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

**Paso 2. configurar los equipos host.**

**Paso 3. inicializar y volver a cargar los routers y los switches.**

**Paso 4. configurar los parámetros básicos para cada router.**

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

**Paso 5. configurar el routing estático.**

a. Cree una ruta estática desde el router ISP hasta el router Gateway.

   ISP(config)# **ip route 209.165.200.224 255.255.255.248 209.165.201.18**

b. Cree una ruta predeterminada del router Gateway al router ISP.

   Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

**Paso 6. Verificar la conectividad de la red**

a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.
b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|---|---|---|---|---|---|---|---|---|---|---|
| | Successful | PC-A | Gateway | ICMP | | 0.000 | N | 0 | (e... | (delete) |
| | Successful | PC-B | Gateway | ICMP | | 0.000 | N | 1 | (e... | (delete) |
| | Successful | PC-C | Gateway | ICMP | | 0.000 | N | 2 | (e... | (delete) |

## Parte 17. configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

### Paso 1. definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

Gateway(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

### Paso 2. definir el conjunto de direcciones IP públicas utilizables.

Gateway(config)# **ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

### Paso 3. definir la NAT desde la lista de origen interna hasta el conjunto externo.

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

### Paso 4. Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

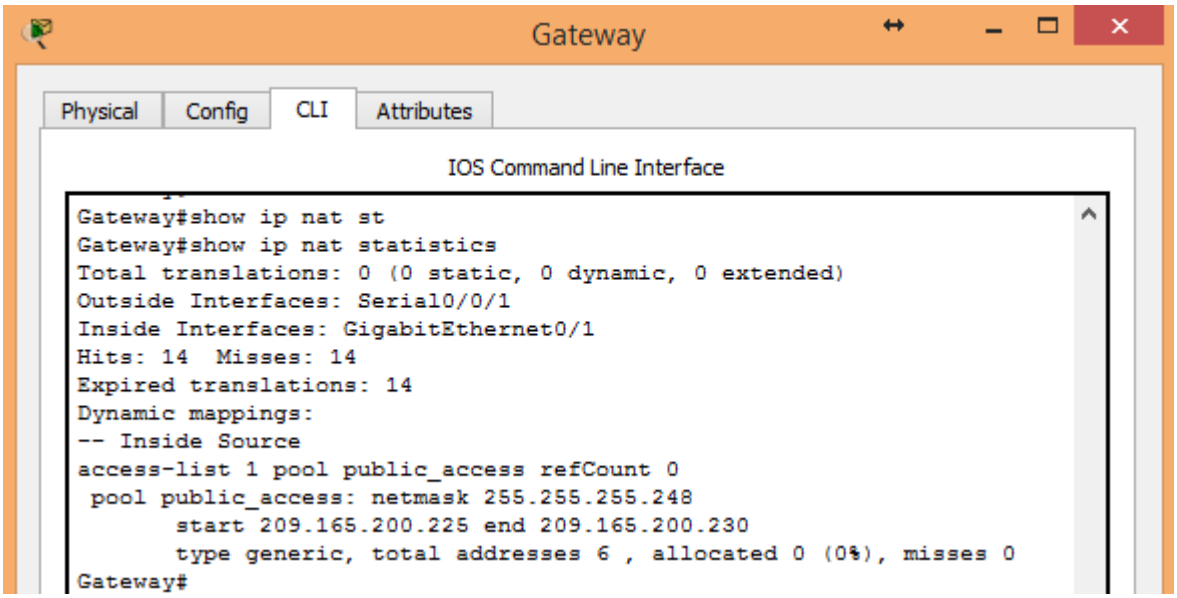
Gateway(config)# **interface g0/1**
Gateway(config-if)# **ip nat inside**
Gateway(config-if)# **interface s0/0/1**
Gateway(config-if)# **ip nat outside**

### Paso 5. verificar la configuración del conjunto de NAT con sobrecarga.

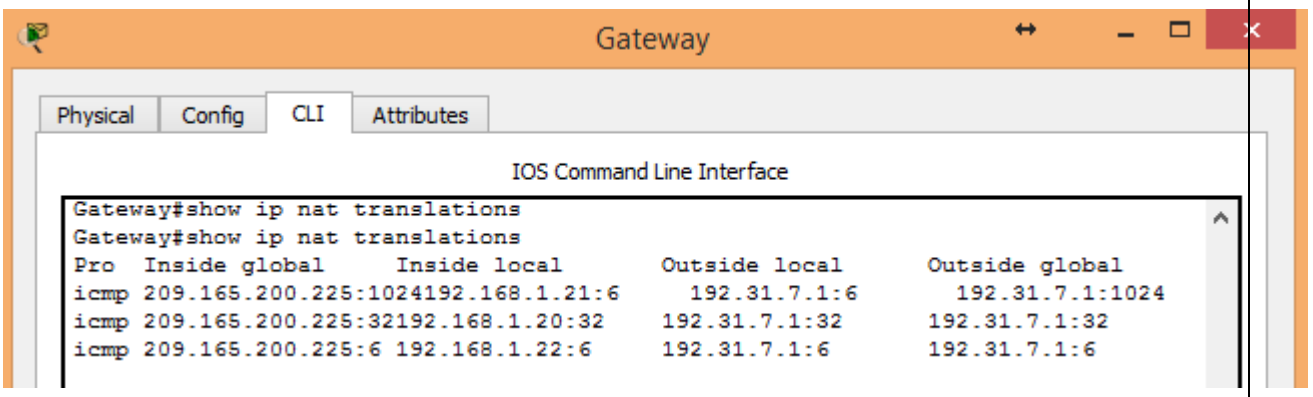
a. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|---|---|---|---|---|---|---|---|---|---|---|
| | Successful | PC-A | 192.31.7.1 | ICMP | | 0.000 | N | 0 | (e... | (delete) |
| | Successful | PC-C | 192.31.7.1 | ICMP | | 0.000 | N | 1 | (e... | (delete) |
| | Successful | PC-B | 192.31.7.1 | ICMP | | 0.000 | N | 2 | (e... | (delete) |

b. Muestre las estadísticas de NAT en el router Gateway.




c. Muestre las NAT en el router Gateway.




**Nota:** es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? 3

¿Cuántas direcciones IP globales internas se indican? 1

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? 3

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

El ping fallaría debido a que el router conoce la ubicación de la dirección global interna en la tabla de routing, pero la dirección local interna no se anuncia.

**Parte 18. configurar y verificar PAT**

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

**Paso 1. borrar las NAT y las estadísticas en el router Gateway.**

**Paso 2. verificar la configuración para NAT.**

a. Verifique que se hayan borrado las estadísticas.
b. Verifique que las interfaces externa e interna estén configuradas para NAT.
c. Verifique que la ACL aún esté configurada para NAT.

¿Qué comando usó para confirmar los resultados de los pasos a al c?

Gateway# show ip nat statistics

**Paso 3. eliminar el conjunto de direcciones IP públicas utilizables.**

Gateway(config)# **no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

**Paso 4. eliminar la traducción NAT de la lista de origen interna al conjunto externo.**

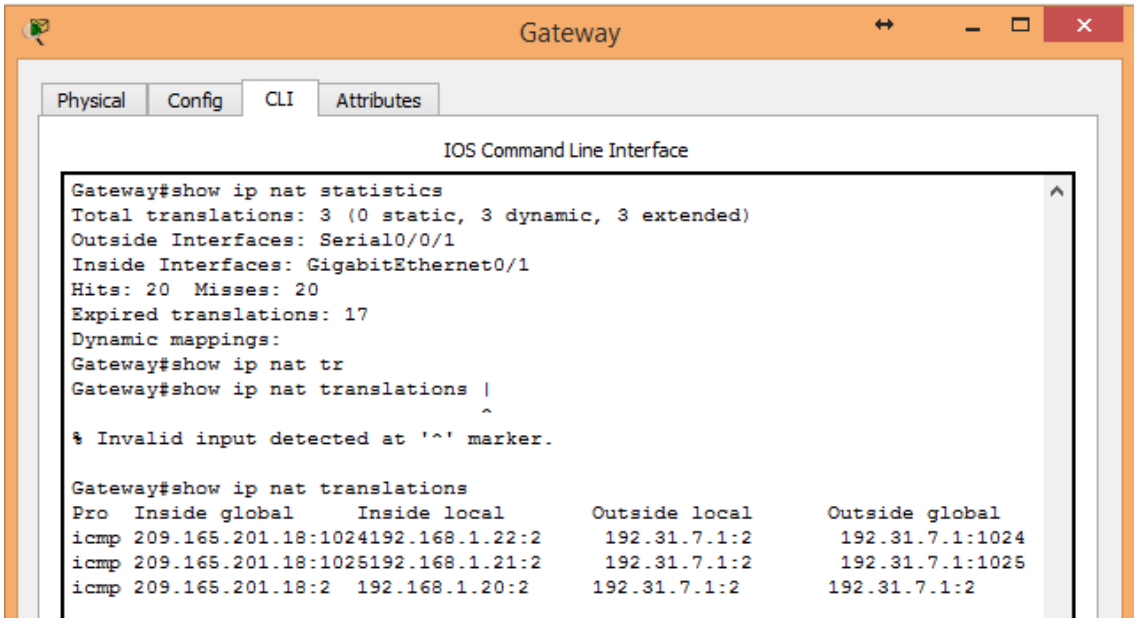
Gateway(config)# **no ip nat inside source list 1 pool public_access overload**

**Paso 5. asociar la lista de origen a la interfaz externa.**

Gateway(config)# **ip nat inside source list 1 interface serial 0/0/1 overload**

**Paso 6. probar la configuración PAT.**

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.
b. Muestre las estadísticas de NAT en el router Gateway.
c. Muestre las traducciones NAT en el Gateway.




**Reflexión**

¿Qué ventajas tiene la PAT?

PAT minimiza la cantidad de direcciones públicas necesarias para proporcionar acceso a Internet y que los servicios de PAT, como los de NAT, sirven para “ocultar” las direcciones privadas de las redes externas.

# CONCLUSIONES

El presente trabajo colaborativo a modo individual permitió la integración de esfuerzos debido a que las prácticas desarrolladas por los miembros del grupo en su mayoría las realizaron todas.

Aprendizaje de cisco con el simulador Packet Tracer y las instrucciones es un modo practico y útil de aprender hacienda y configurar equipos apropiadamente que van estar disponibles en las empresas en el campo de Servicios de Comunicación y telecomunicaciones.

CCNA es importante si desea tener éxito en redes y le dará un buen conocimiento fundamental, el crecimiento y más oportunidades en su carrera de redes.

CCNA es una de las más aceptadas y valoradas certificaciones I.T de hoy.

Obtener CCNA certificado es uno de los mejores movimientos de un principiante en I.T especialmente en redes puede tomar.

Realmente puede aumentar la carrera profesional y llevarlo al siguiente nivel salarial.

La mayoría de las empresas de tecnología ahora están exigiendo certificaciones I.T en un campo específico, incluso para los principiantes.

Aumentar sus conocimientos en redes de Cisco y ampliar su comprensión del concepto de cómo funciona.

Esto solo puede abrir puertas de oportunidades en su carrera en la creación de redes. Incluso un nuevo graduado, pero certificada por CCNA es más probable que contratar a un tipo I.T promedio sin certificación. Así es como funciona ahora.

Los beneficios de ser CCNA certificado es la alta probabilidad del aumento de sueldo. Ya sea en la misma empresa en la que estás o en la siguiente empresa.

Una vez que esté certificado por CCNA, puede aumentar y negociar un salario más alto que un individuo habitual de I.T que solicita la misma posición.

Se cumplieron los objetivos de manera satisfactoria.

# REFERENCIAS BIBLIOGRAFICAS Y CIBERGRAFIA

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1