Universidad Nacional Abierta Y A Distancia – Unad

Escuela De Ciencias Básicas, Tecnología E Ingeniería

Diplomado De Profundización Cisco

# Trabajo Colaborativo 4


Presentado Por:

Luis Eduardo Urreste Melo Cód. 6322073

John Jairo Montoya Cortes Cód. 16862376

Camilo José Pedroza Sánchez Cód. 1112100280

Edinso Rojas Cód. 94403387

Juan Carlos Merchán Rubiano Cód. 16798483


Grupo:

203092_25

Tutor:

José Ignacio Cardona


Universidad Nacional Abierta Y A Distancia – Unad

Escuela De Ciencias Básicas Tecnología E Ingeniería (Ecbti)

Noviembre De 2017

# Contenido

## Introducción

Continuando con el desarrollo del curso de CCNA de CISCO y como parte del trabajo colaborativo cuatro (4), se presenta el siguiente informe como producto de las prácticas realizadas con Packet Tracer propuestas para esta fase.

Este informe corresponde a la parte CCNA Principios básicos de Routing y Switching. En esta parte centra en routing dinámico, OSPF de área única, lista de control de acceso, DHCP, entre otras actividades; En cada una de las practicas el grupo presentará 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. Además del informe, se anexan los archivos. pka de Packet Tracer como prueba de su ejecución.

Asimismo, en esta fase el alumno adquirirá las destrezas y habilidades en la configuración tanto de router y switch estableciendo un esquema de direccionamiento adecuado junto con un direccionamiento que permita enviar un paquete de extremo a extremo optando por una un protocolo adecuado menos saltos.

# Objetivos

## Objetivos Generales

Adquirir las destrezas necesarias en configuración de switches y router, protocolos de enrutamiento, y proponer un esquema de direccionamiento acorde con los estándares internacionales

## Objetivos Específicos

- Explorar los diferentes protocolos de routing dinámico, indicando los beneficios de utilizar esta clase de protocolos.
- Analizar el protocolo de routing OSPF y los beneficios que ofrece en su configuración
- Proponer un esquema de donde se incluye lista de acceso permitiendo de esa forma que solo los usuarios autorizados pueden utilizar la red empresarial.
- Aprender a configurar el servicio de DHCP en los routers

## 4.4.1.2 Packet Tracer: Configure Ip Acls To Mitigate Attacks

**Topología**

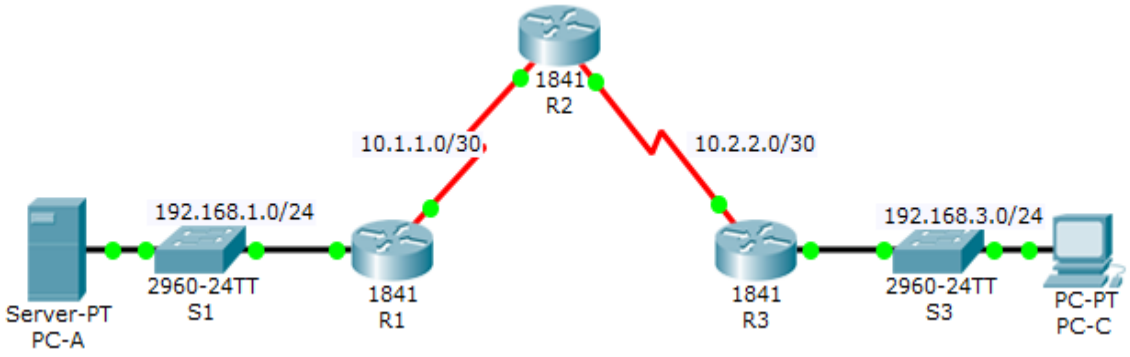



Figura 1. Topología

Tabla 1. Tabla de direccionamiento 4.4.1.2

| 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

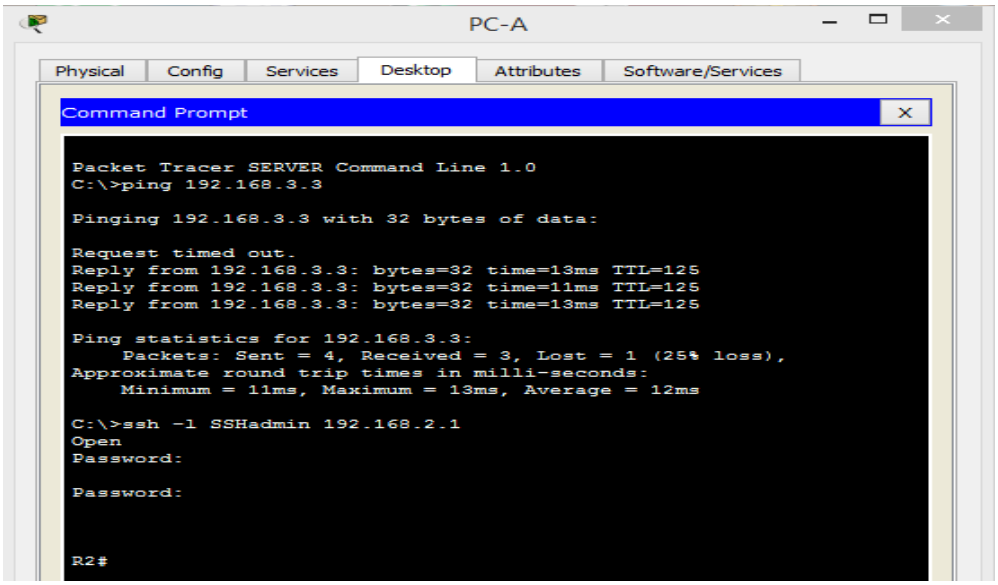



Figura 2. Verificación de ping y entrada SSH a R2 desde PC-A

**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

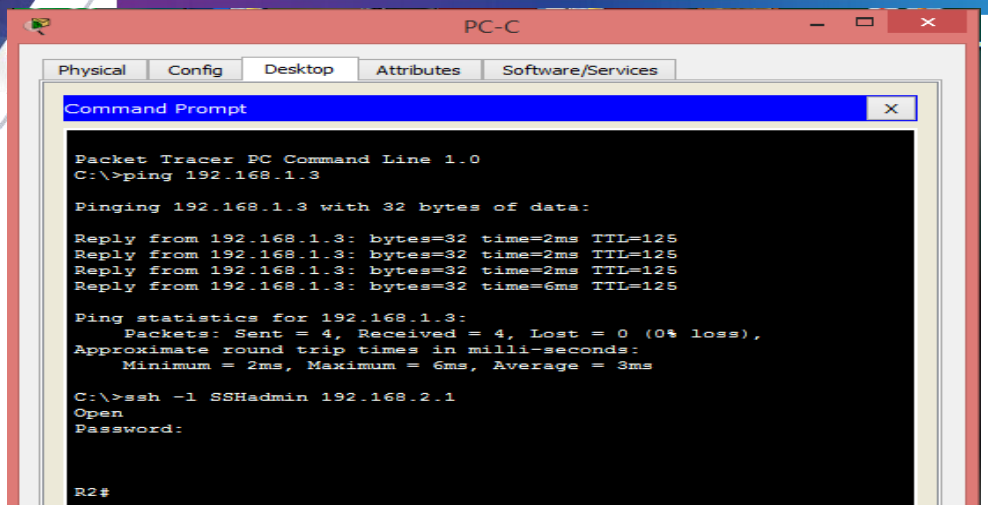



Figura 3. Verificación de ping y entrada SSH a R2 desde PC-C

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

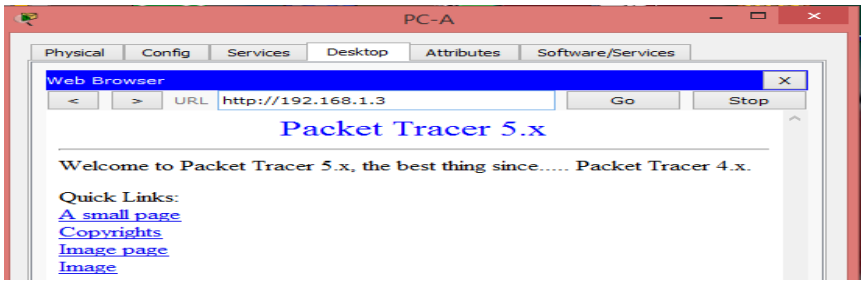



Figura 4. Acceso a lapágina web del servidor

**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)#
```

Figura 5. Configuración de las listas de acceso 10 para cada router

**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.

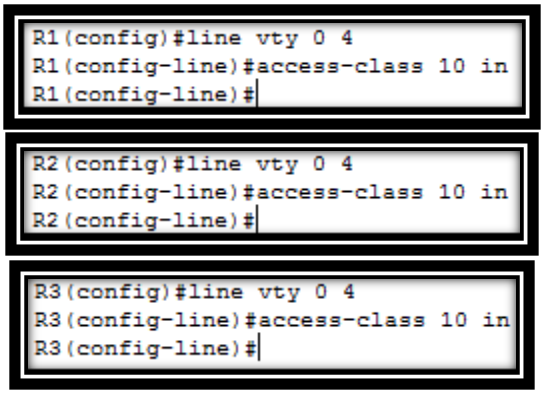



Figura 6.Aplicando las ACL 10 a las interfaces de cada router

**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).

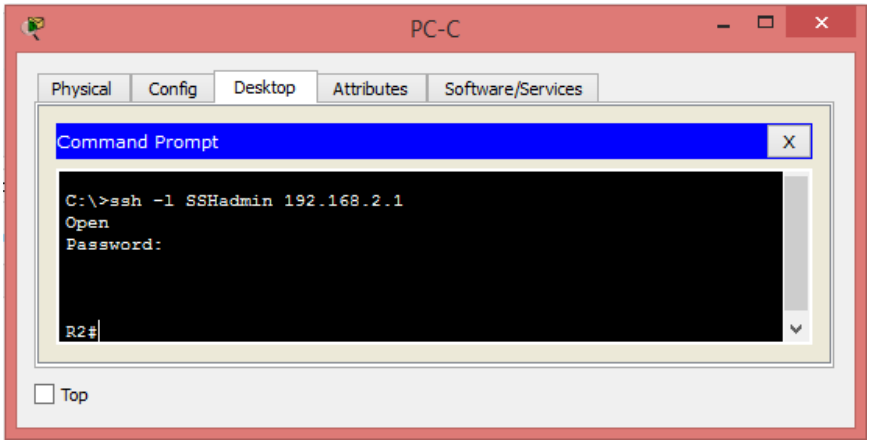



Figura 7. Estableciendo sesión ssh en el PC-C hacia R2

PC> ssh –l SSHadmin 192.168.2.1

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

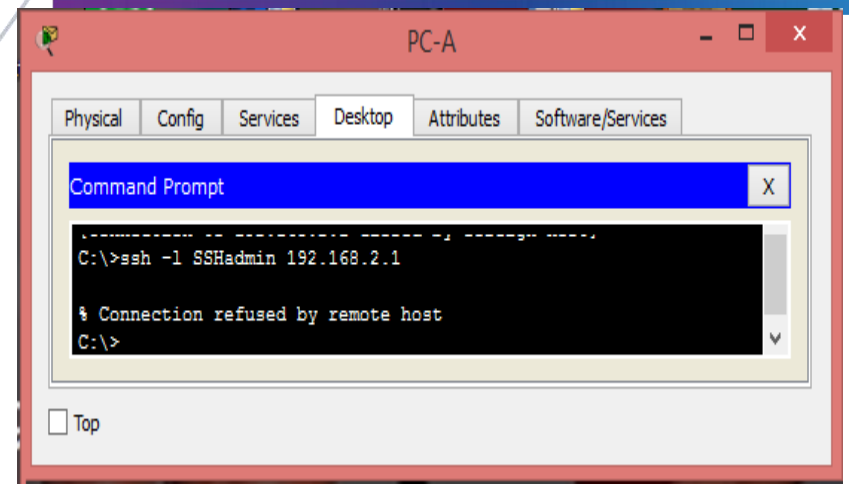



Figura 8. Inicio de sesión ssh en PC-A bloqueado

**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.

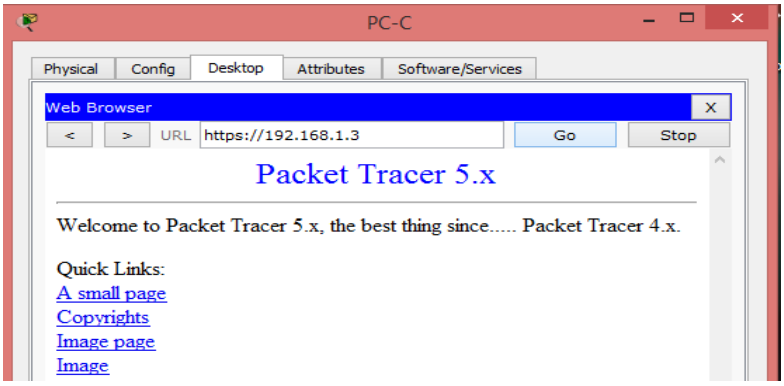
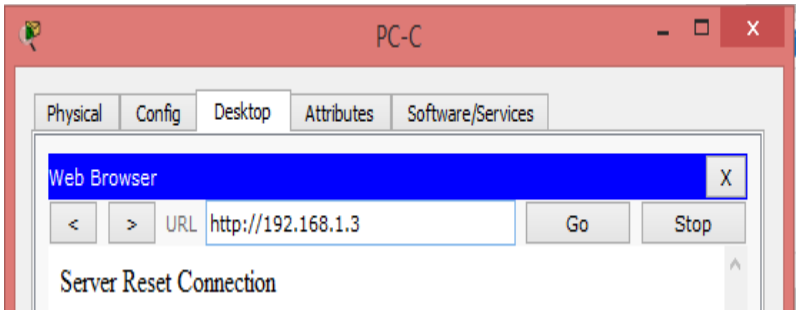



Figura 9. Acceso seguro (HTTPS) al servidor por web desde PC-C habilitado




Acceso seguro (HTTP) al servidor por web desde PC-C deshabiltado

**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
```

Figura 10.Configuración de la ACL 120 en R1 para permitir y denegar tráfico específico

**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)#
```

Figura 11. Asignanado la ACL 120 a la interfaz en R1

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

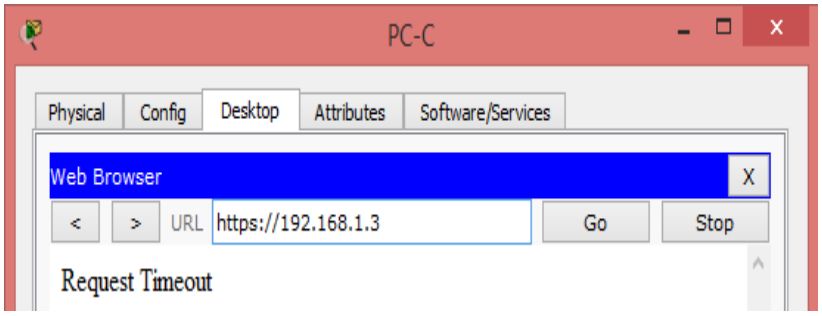



Figura 12. Acceso HTTPS desde PC-C hacia el servidor deshabilitado

**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.**

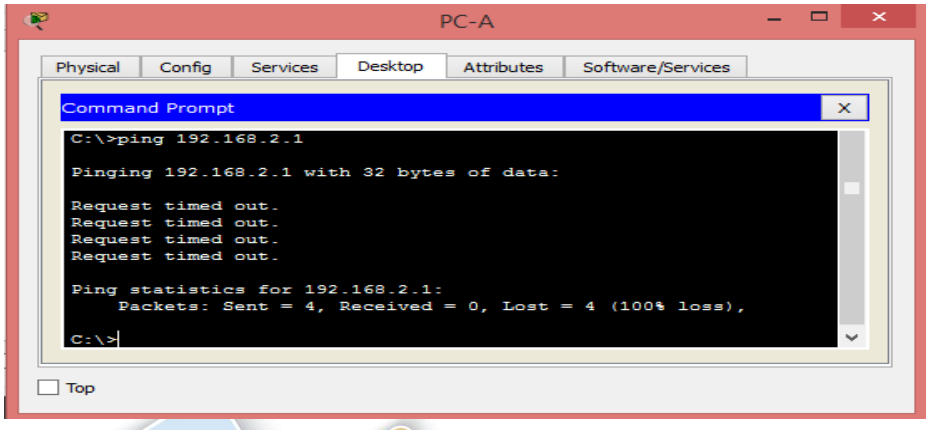


Figura 13. Ping fallido desde PC-A al R2

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

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

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

Figura 14. Permitiendo y denegando tráfico específico en R1

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

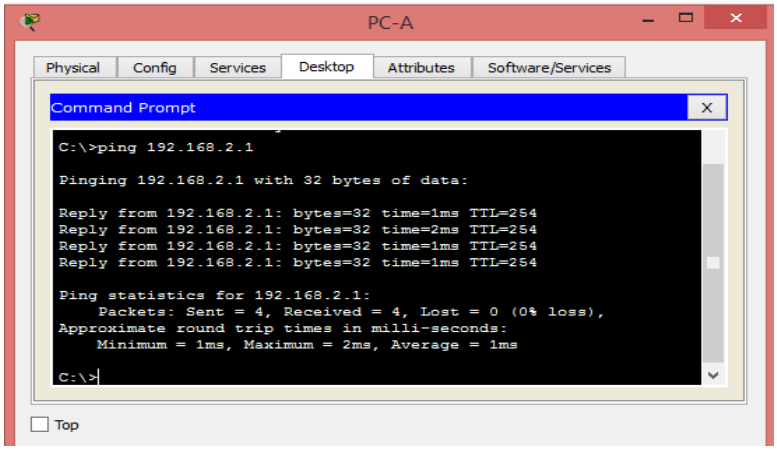



Figura 15. Ping exitoso desde la PC-A al R2

**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)#
```

Figura 16. Permitiendo tráfico sólo desde la red interna en R3

**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
```

Figura 17. Bloqueando el tráfico especificado de la red externa

**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)#
```

Figura 18. Asignando la ACL 100 a la interfaz de R3

**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.

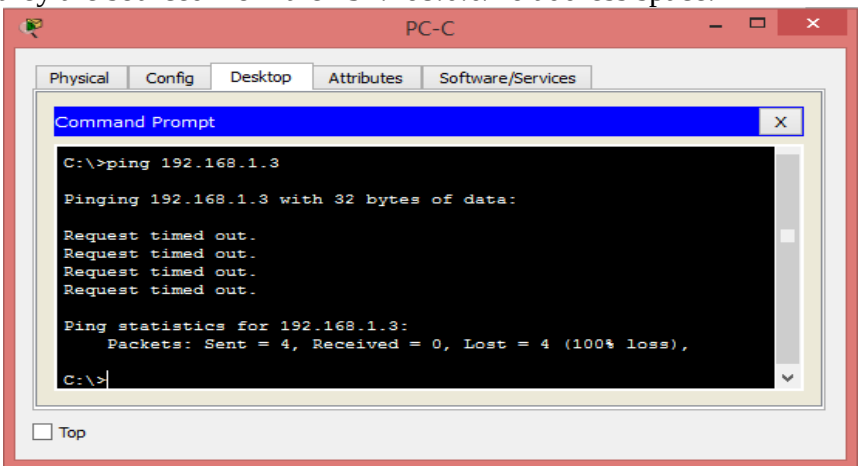



Figura 19. Conectividad bloqueda desde PC-C al servidor

**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.

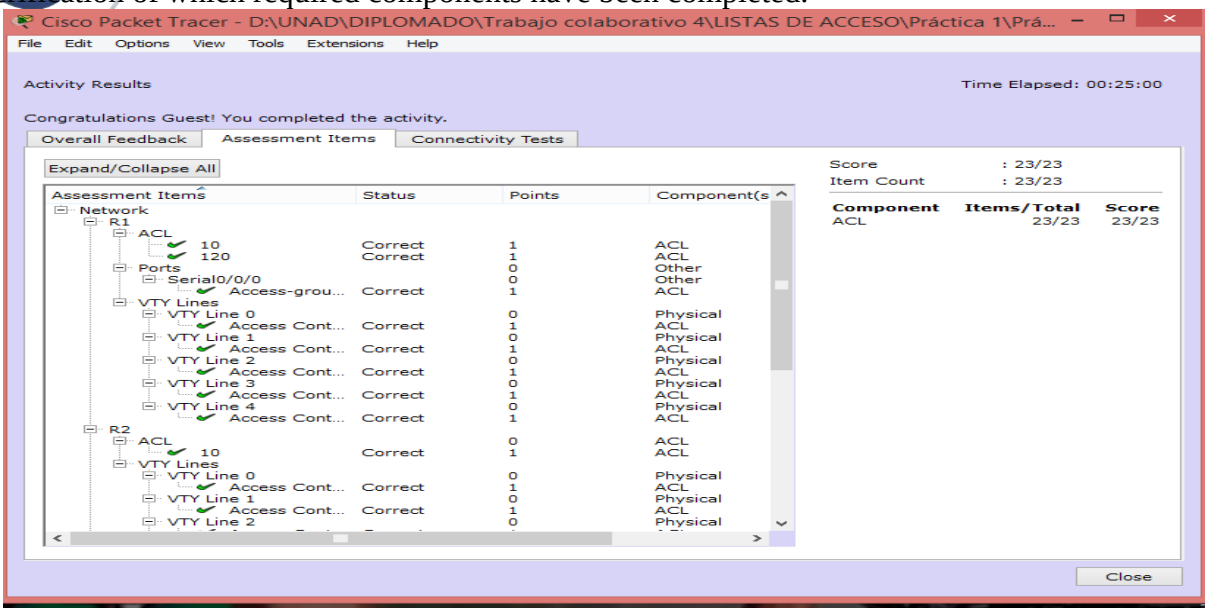



Figura 20. Resultado Actividad

**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
```

## 9.2.1.10 Packet Tracer: Configuring Stantdard Acls

**Topología**

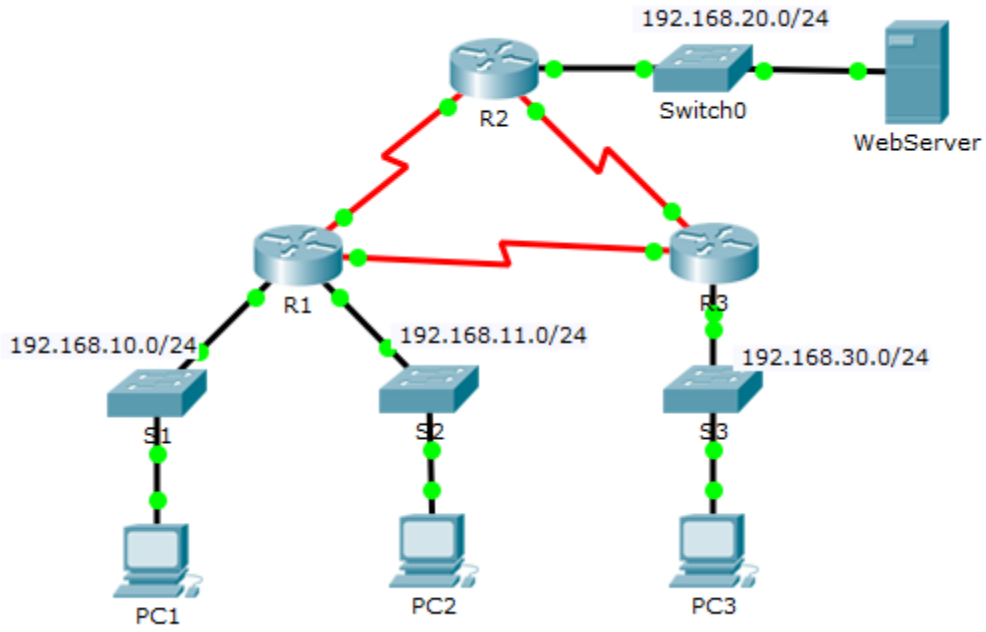



Figura 21. Topología

Tabla 2. Tabla de direccionamiento 9.2.1.10

| Device | Interface | IP Address | Subnet Mask | Default Gateway | Switchport |
|---|---|---|---|---|---|
| R1 | G0/0 | 192.168.10.1 | 255.255.255.0 | N/A | S1 Fa0/5 |
| | G0/1 | 192.168.11.1 | 255.255.255.0 | N/A | N/A |
| | S0/0/0 | 10.1.1.1 | 255.255.255.252 | | |
| | S0/0/1 | 10.3.3.1 | 255.255.255.252 | | |
| R2 | G0/0 | 192.168.20.1 | 255.255.255.0 | N/A | N/A |
| | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
| | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| R3 | G0/0 | 192.168.33.1 | 255.255.255.0 | N/A | S3 Fa0/5 |
| | S0/0/0 | 10.3.3.2 | 255.255.255.252 | N/A | N/A |
| | S0/0/1 | 10.2.2.2 | 255.255.255.252 | | |
| PC1 | NIC | 192.168.10.10 | 255.255.255.0 | 192.168.10.1 | S1 Fa0/6 |
| PC2 | NIC | 192.168.11.10 | 255.255.255.0 | 192.168.11.1 | S3 Fa0/18 |
| PC3 | | 192.168.30.10 | 255.255.255.0 | 192.168.30.1 | k |
| WebServer | | 192.168.20.254 | 255.255.255.0 | 192.168.20.1 | |

**Objectives**

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

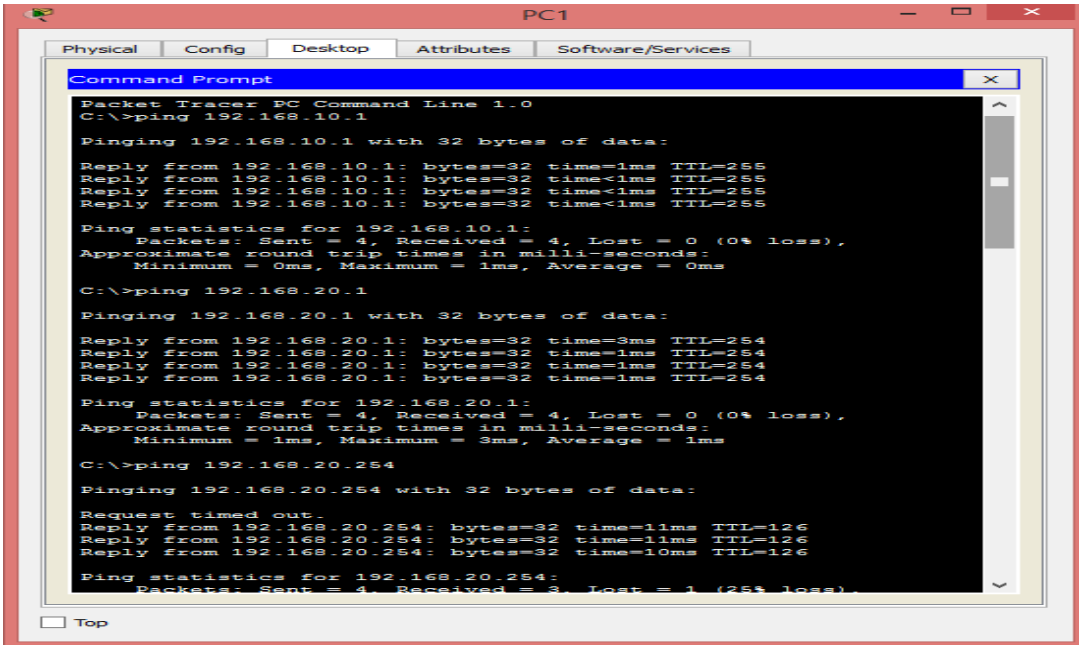
**Background / Scenario**

Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

**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.



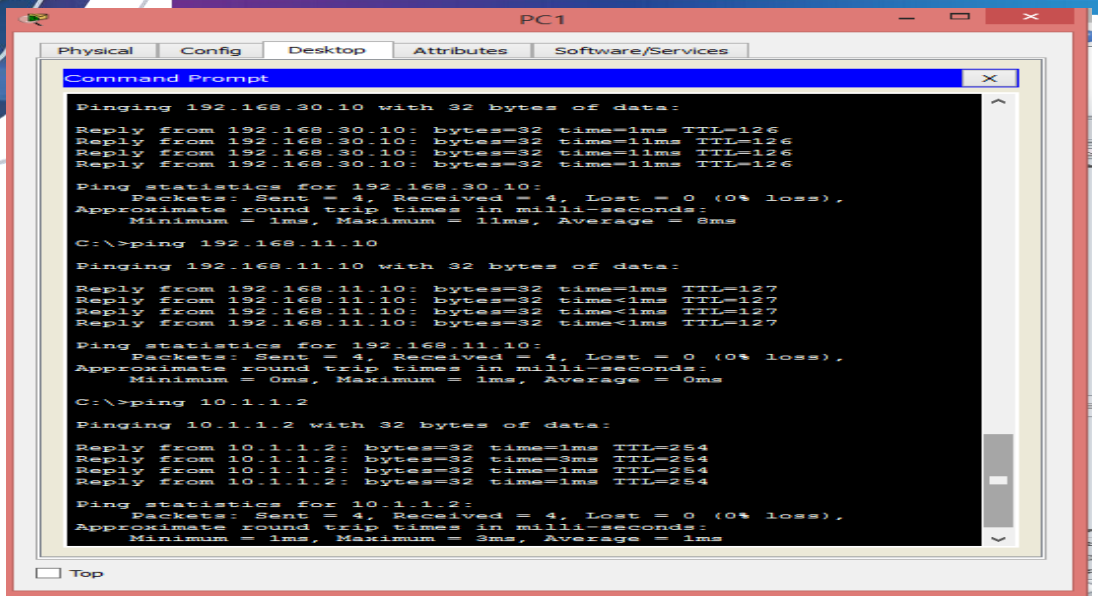



Figura 22. Verificación de conectividad

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

**a.** The following network policies are implemented on R2:

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

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

**b.** The following network policies are implemented on R3:

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

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

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

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

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

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

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

R2(config)# access-list 1 permit any

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

R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out

```
R2>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)#int g0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

Figura 23. Configuración de lista de acceso en R2 y asignación de la interfaz

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

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

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

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

R3(config)# access-list 1 permit any

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

R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out

```
R3>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
R3(config)#access-list 1 permit any
R3(config)#int g0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
```

Figura 24. Creación de lista de acceso en R3 y asignación de la interfaz

**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
```

Figura 25. Verificación de las ACLs creadas en R2

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

Figura 26. Verificación de las ACLs creadas en R3

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

- A ping from 192.168.10.10 to 192.168.11.10 succeeds.
- A ping from 192.168.10.10 to 192.168.20.254 succeeds.

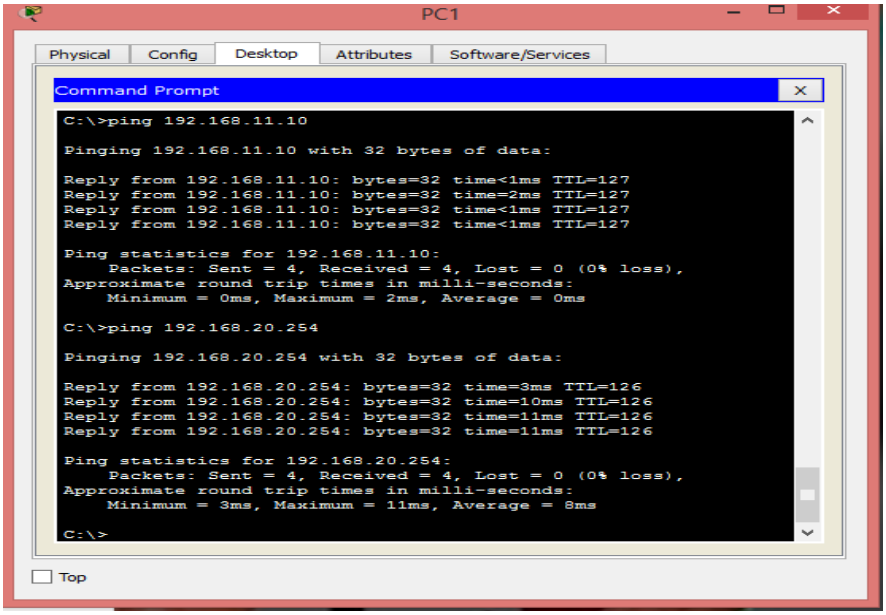



Figura 27. Conectividad exitosa del PC1 con la red 192.168.11.0 y 192.168.20.0

- A ping from 192.168.11.10 to 192.168.20.254 fails.

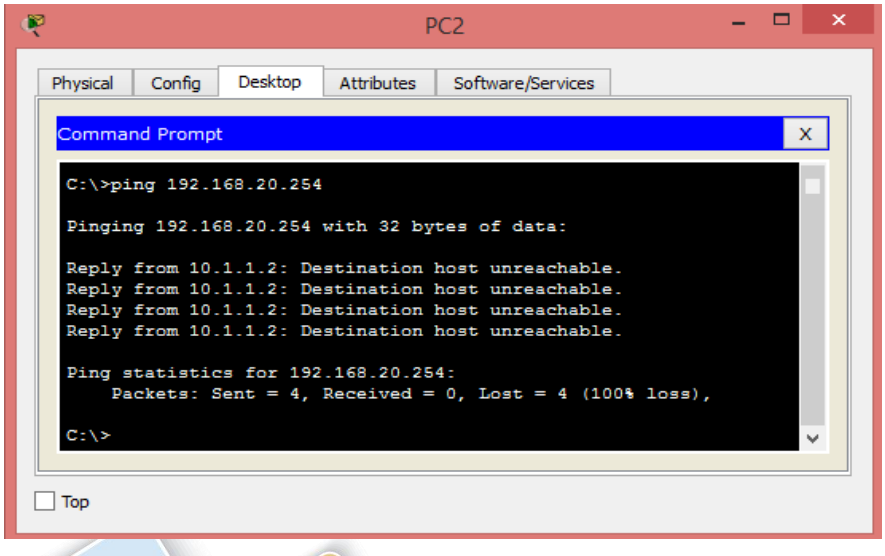


Figura 28. Conectividad bloqueada en la PC2 hacia la red 192.168.20.0

- A ping from 192.168.10.10 to 192.168.30.10 fails.

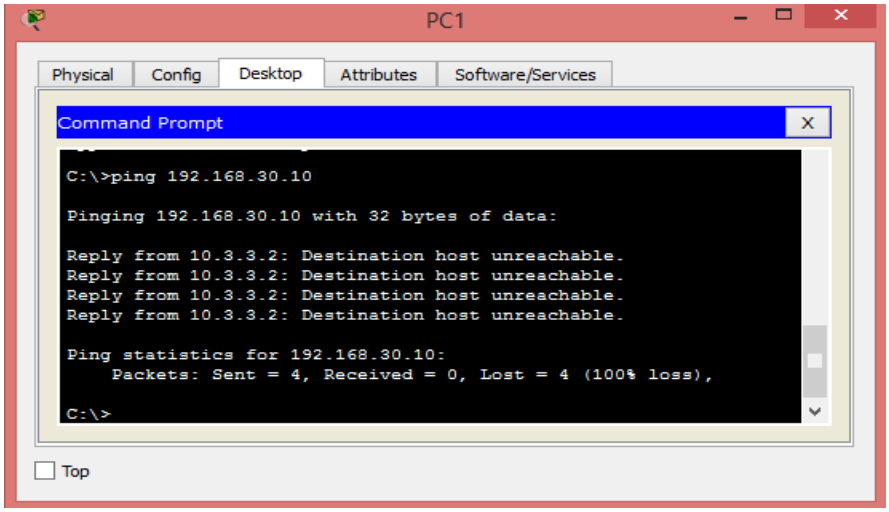



Figura 29. Conectividad bloqueda en la PC1 hacia la red 192.168.30.0

- A ping from 192.168.11.10 to 192.168.30.10 succeeds.

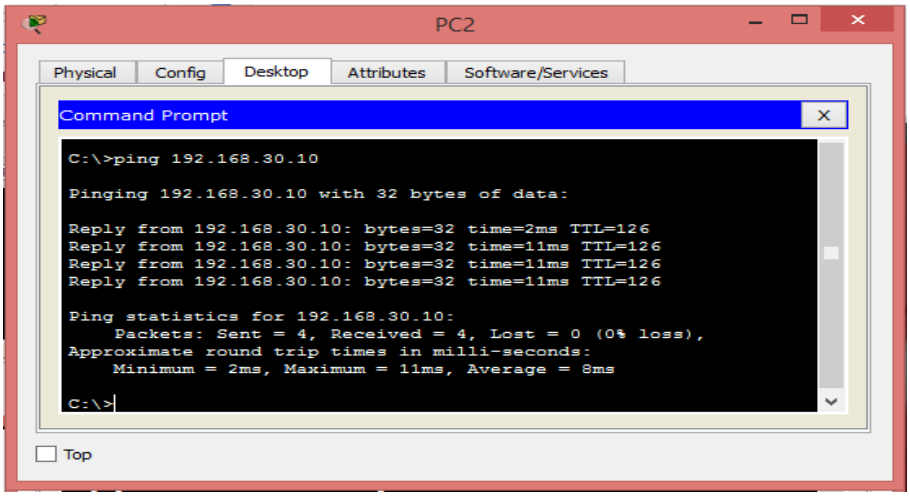



Figura 30. Conectividad exitosa de la PC2 con la red 192.168.30.0

- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

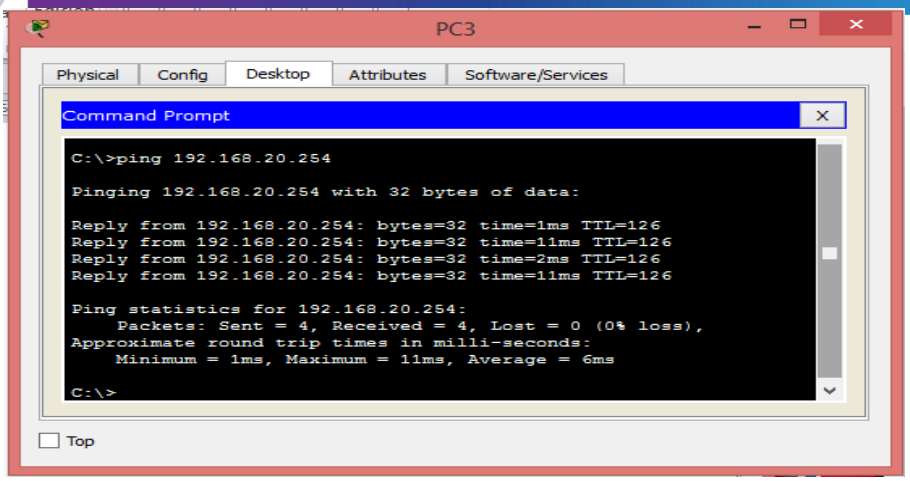



Figura 31. Conectividad exitosa en la PC3 hacia la red 192.168.20

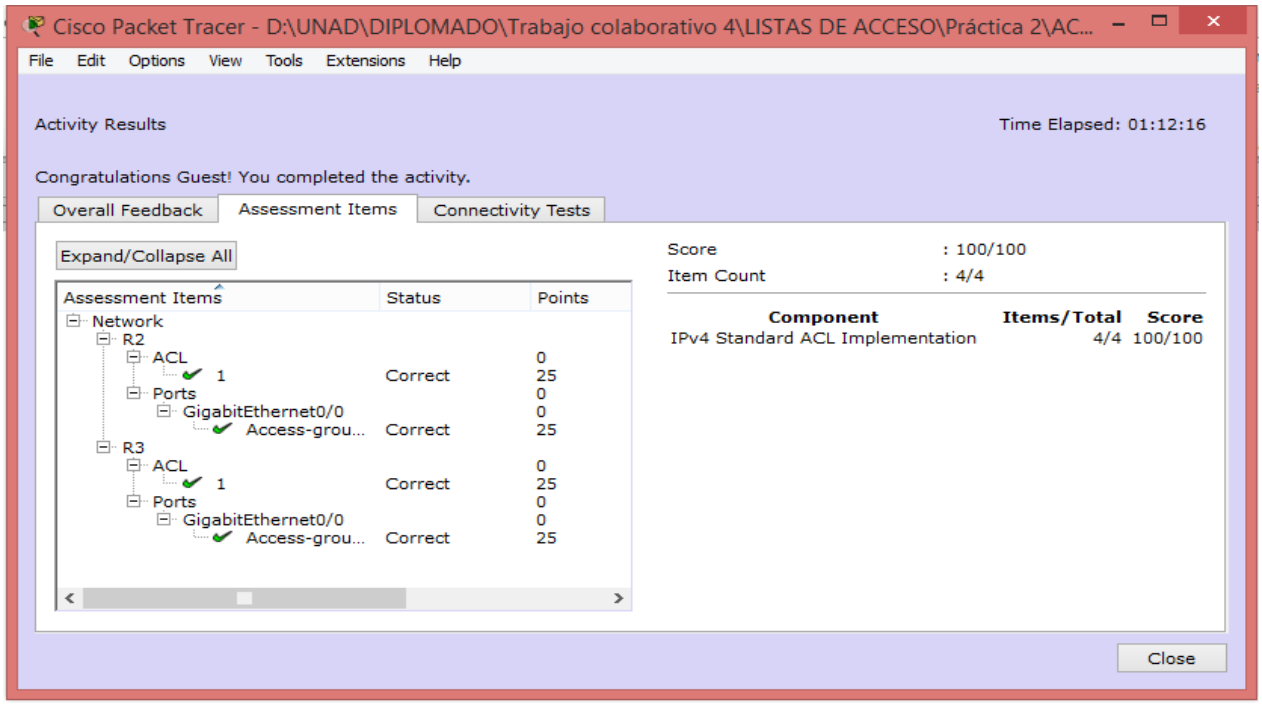



Figura 32. Resultado Actividad

## 9.2.1.11 Packet Tracer: Configuring Named Standard Acls

### Topología

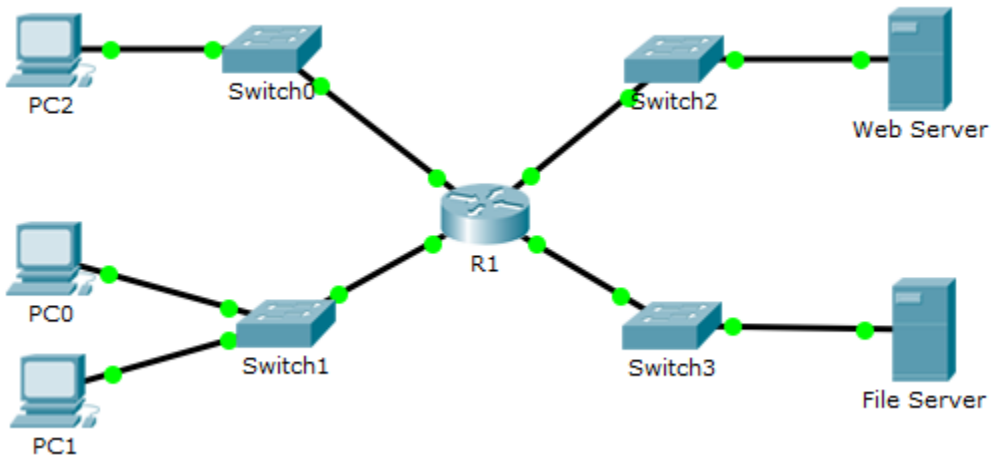



Figura 33. Topología

Tabla 3. Tabla de direccionamiento 9.2.1.11

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

### Objectives

- Part 1: Configure and Apply a Named Standard ACL
- Part 2: Verify the ACL Implementation

### Background / Scenario

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

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

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

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

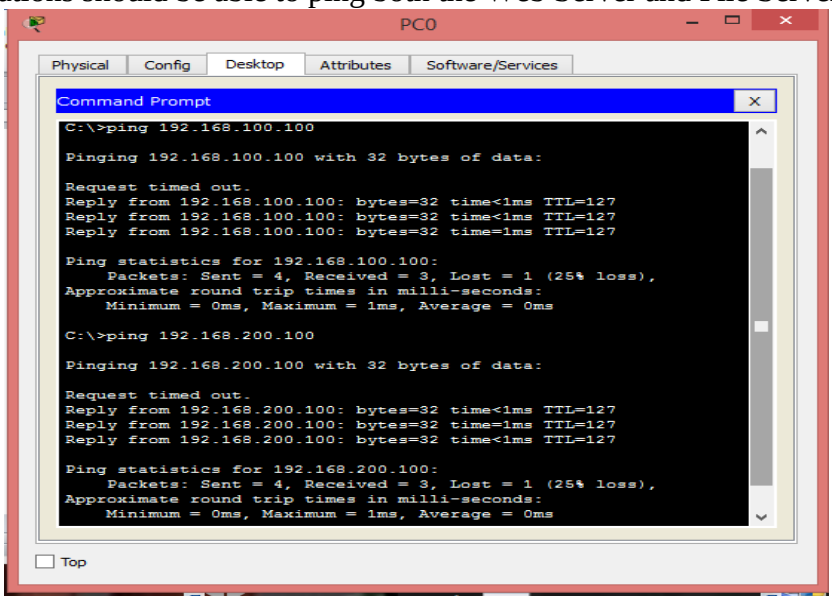



Figura 34. Verificación de conectividad del PC0 con los servidores

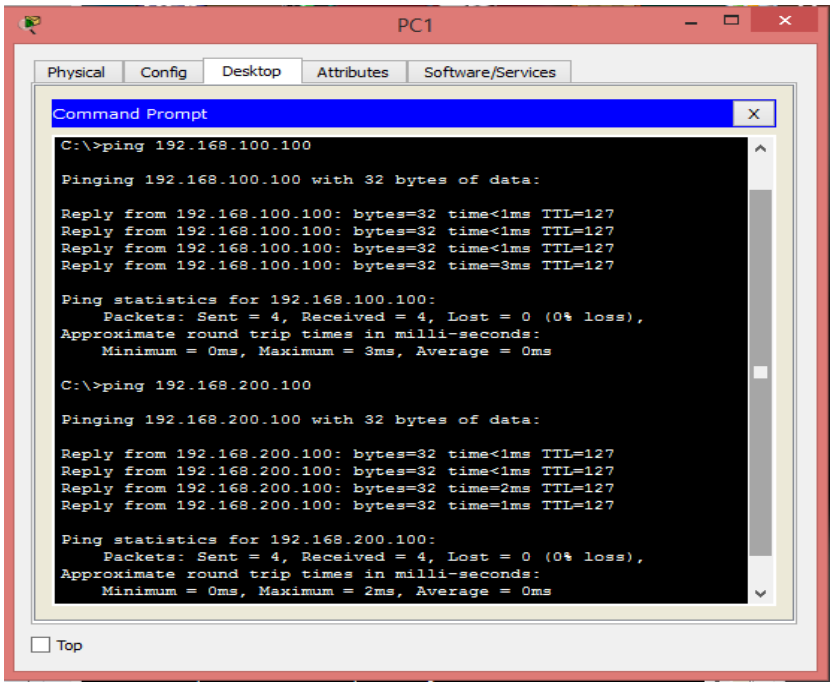



Figura 35. Verificación de conectividad del PC1 con los servidores

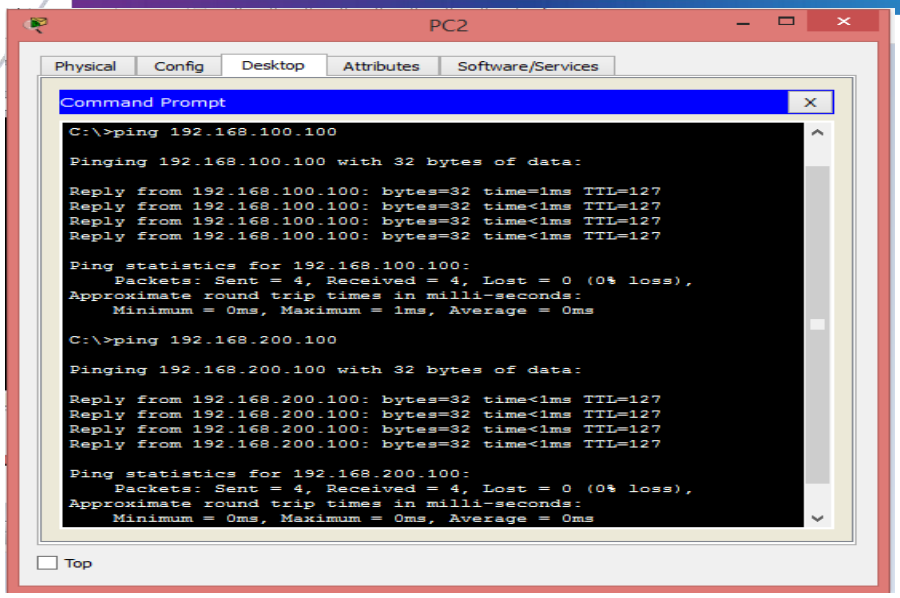



Figura 36. Verificación de conectividad del PC2 con los servidores

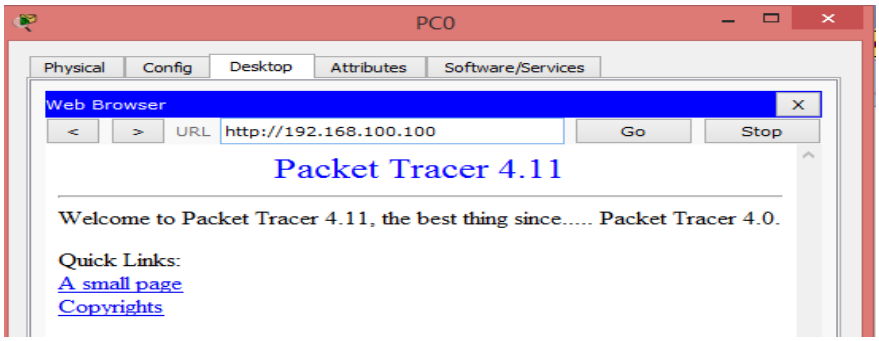



Figura 37. Acceso ala página web del servidor

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

Configure the following named ACL on R1.

R1(config)# ip access-list standard File_Server_Restrictions

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

R1(config-std-nacl)# deny any

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

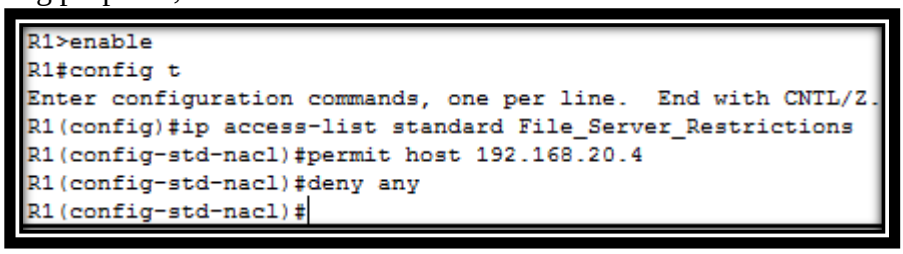



Figura 38. Configuración la ACL estándar con nombre en R1

**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
co
% Ambiguous command: "co"
R1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Figura 39Asignando la ACL a la interfaz F0/1 de R1

**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
```

Figura 40. Verificación de la ACL creada

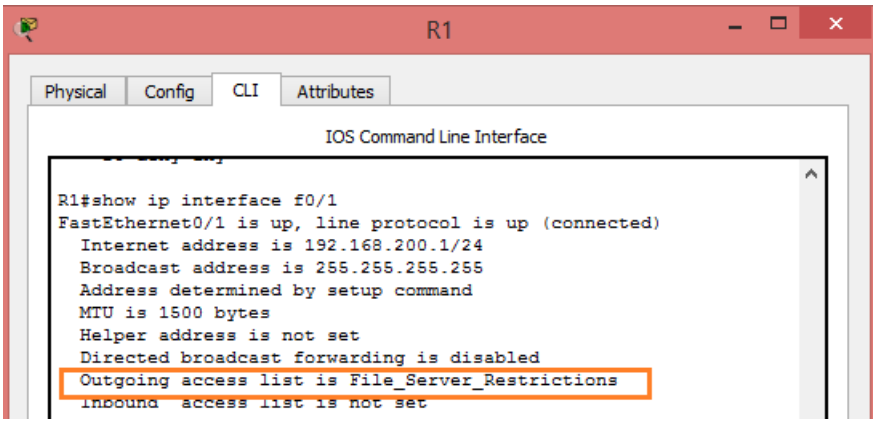



Figura 41. Verificación asignación de la ACL a la interfaz F0/1

**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**.

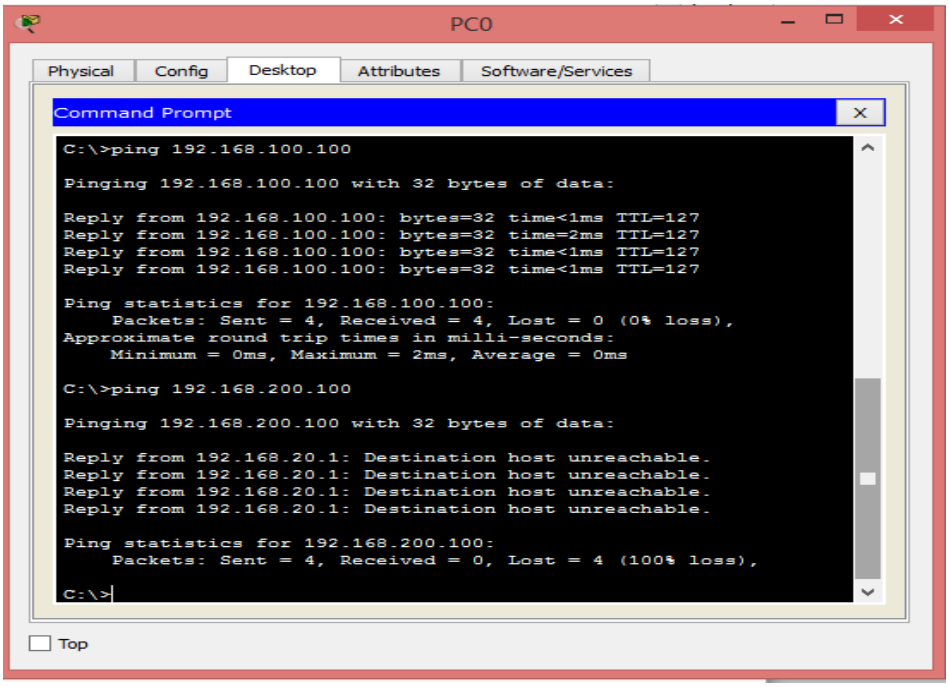



Figura 42. Acceso desde la PC0 al File server bloqueado por la ACL

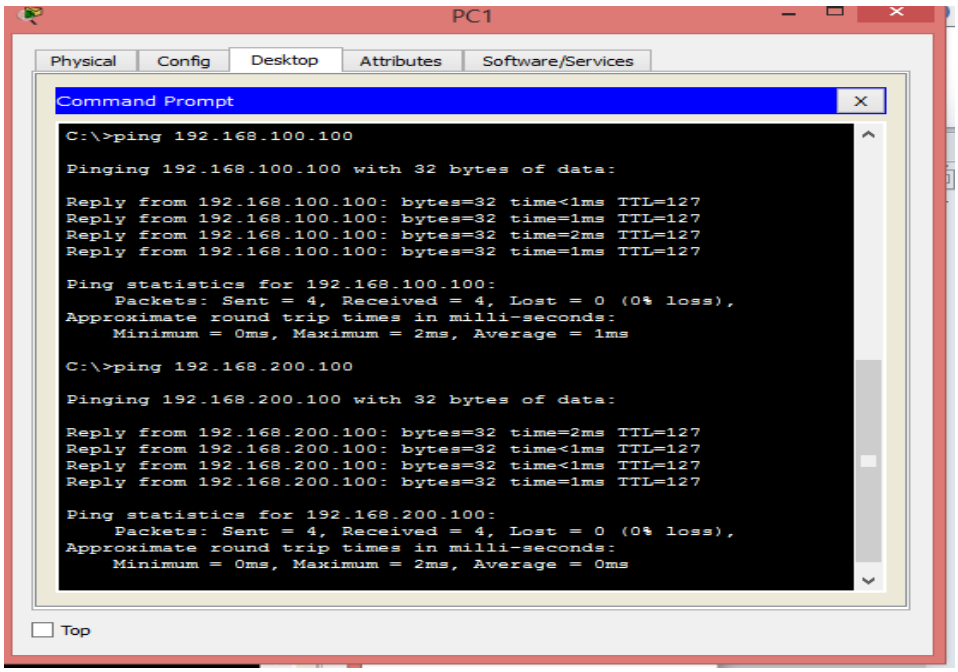



Figura 43. Acceso a los dos servidores desde la PC1

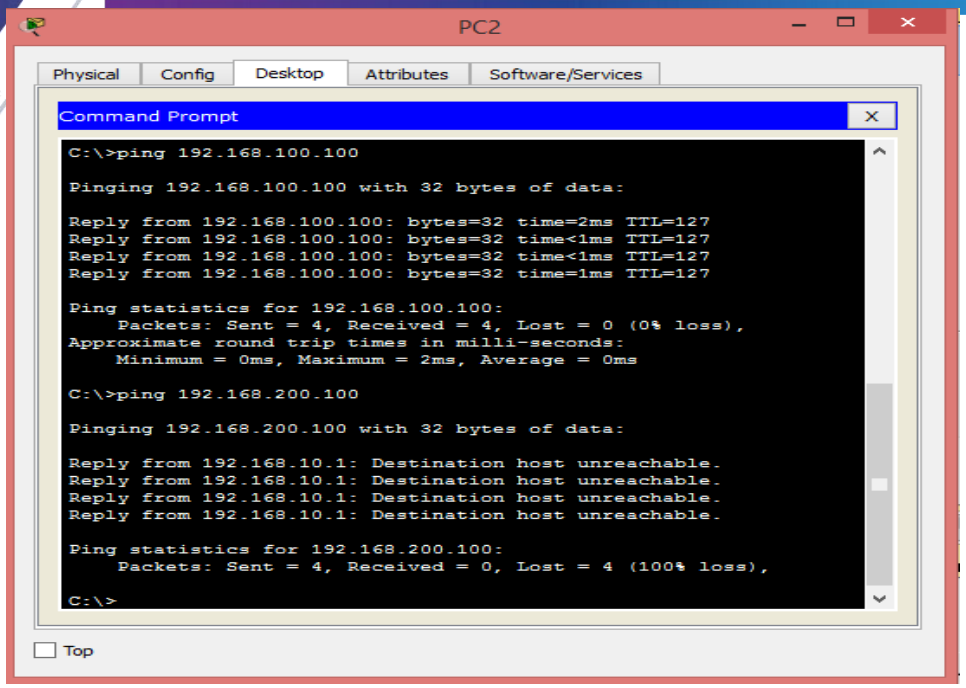



Figura 44. Acceso desde la PC2 al File server bloqueado por la ACL

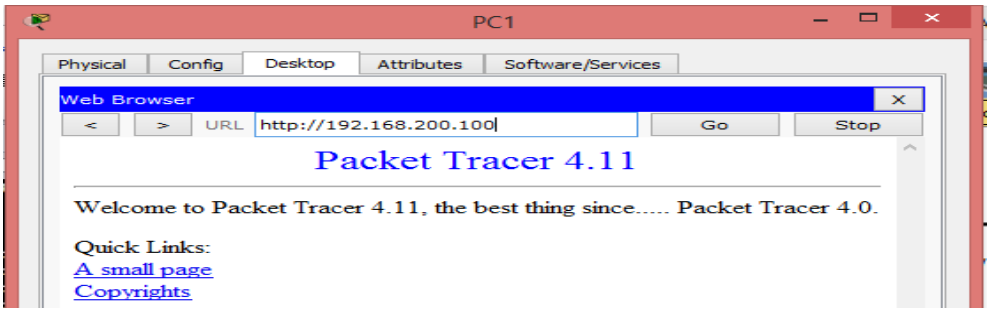



Figura 45. Acceso a la página web del File server desde la PC1

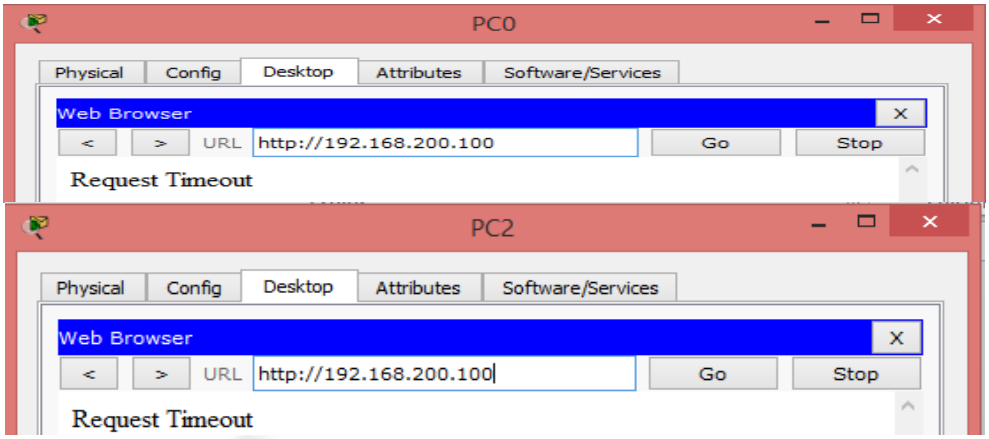



Figura 46. Acceso Web restringido al FileServer para los PC0 y PC2

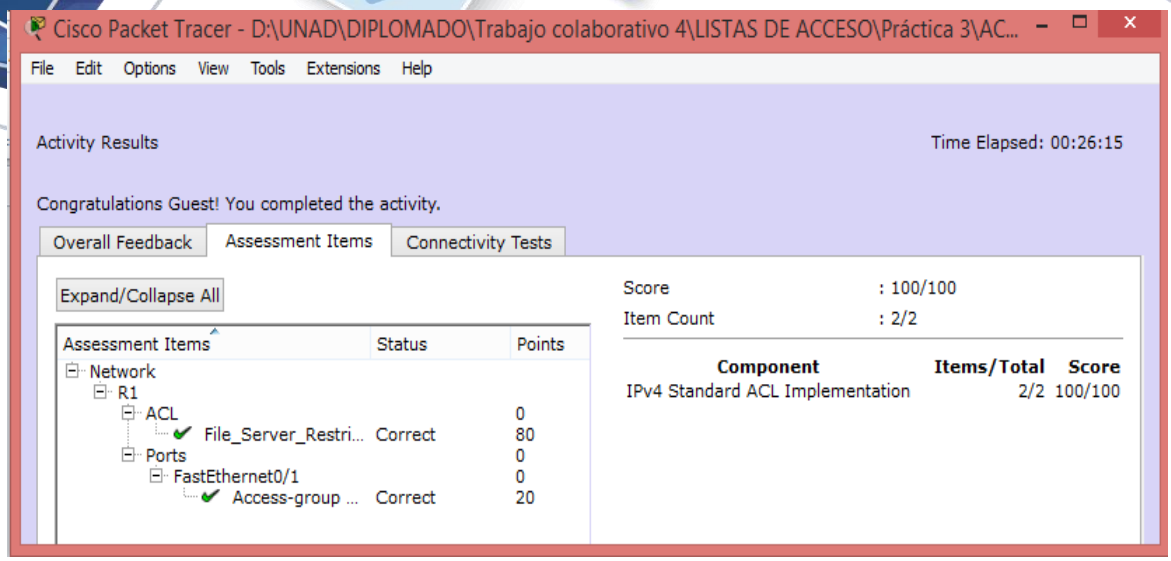
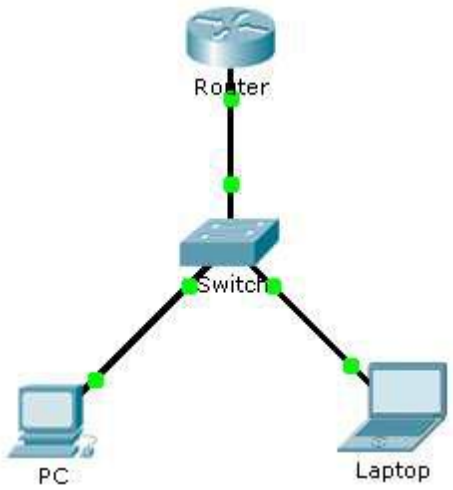



Figura 47. Resultado Actividad

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

## Topology




## Addressing Table

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

## Objectives

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

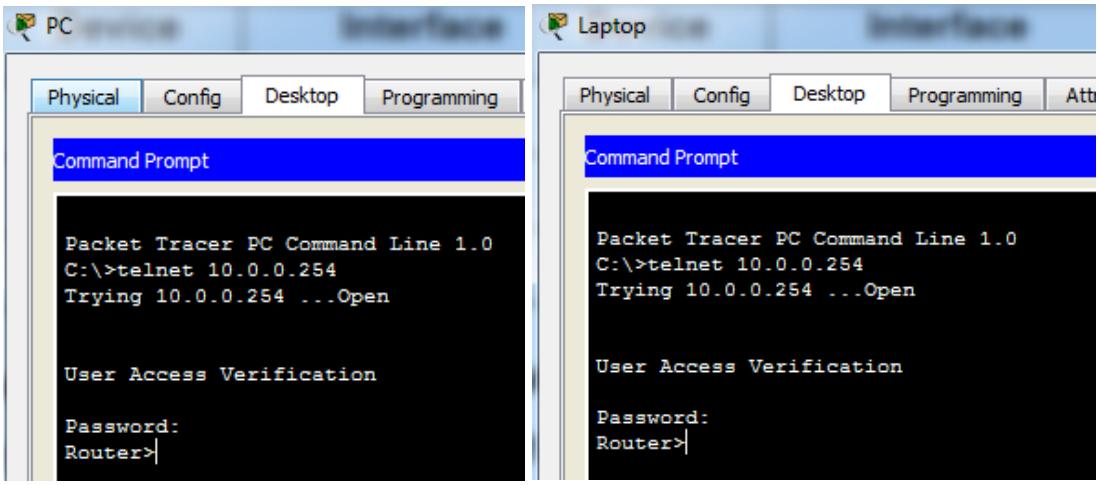
## Background

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

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

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

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




## 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
```

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

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

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

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

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

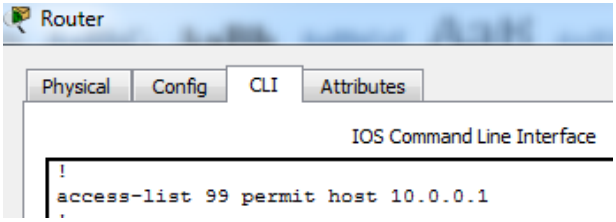
```
Router(config)#line vty 0 4
Router(config-line)#ac
Router(config-line)#acc
Router(config-line)#access
Router(config-line)#access-class 99 in
Router(config-line)#
```

## 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.

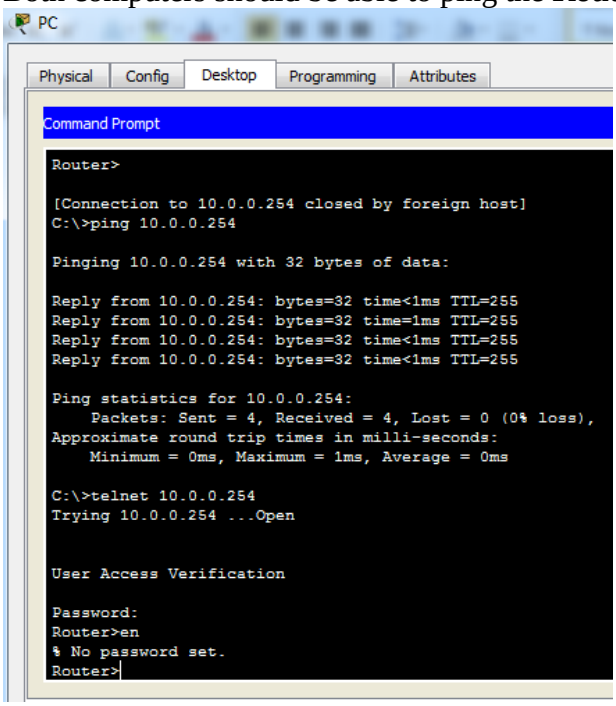
```
Router#
Router#show access-lists
Standard IP access list 99
    10 permit host 10.0.0.1
```




```
line vty 0 4
 access-class 99 in
 password cisco
 login
line vty 5 15
 password cisco
 login
```

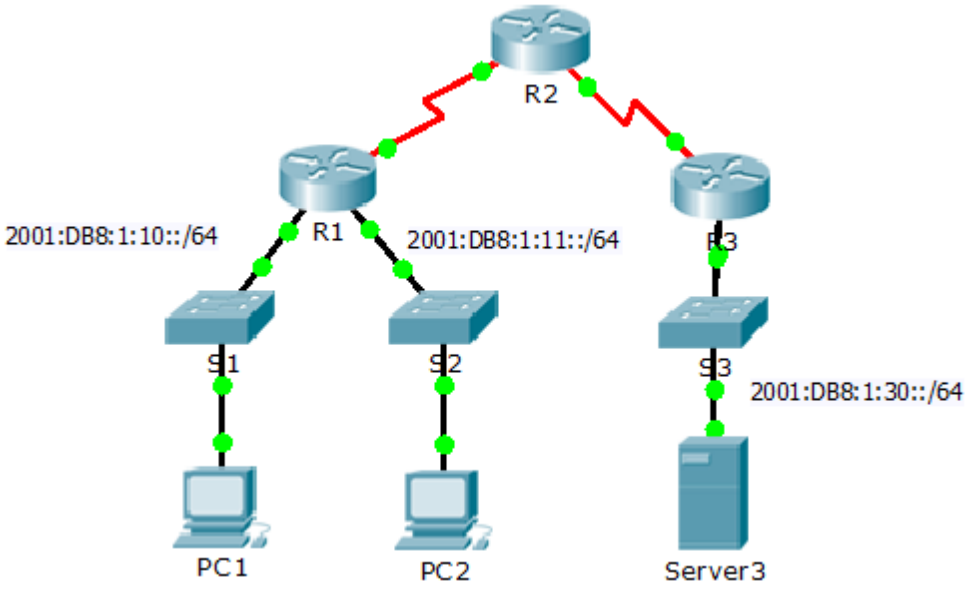
## Step 2: Verify that the ACL is working properly.

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



# 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs Instructions IG

## Topology




## Addressing Table

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

## Objectives

**Part 1: Configure, Apply, and Verify an IPv6 ACL**
**Part 2: Configure, Apply, and Verify a Second IPv6 ACL**

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

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

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

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

Configure an ACL named BLOCK_HTTP on R1 with the following statements.

a. Block HTTP and HTTPS traffic from reaching Server3.

R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq 443

b. Allow all other IPv6 traffic to pass.

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

```
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#
R1#
```

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

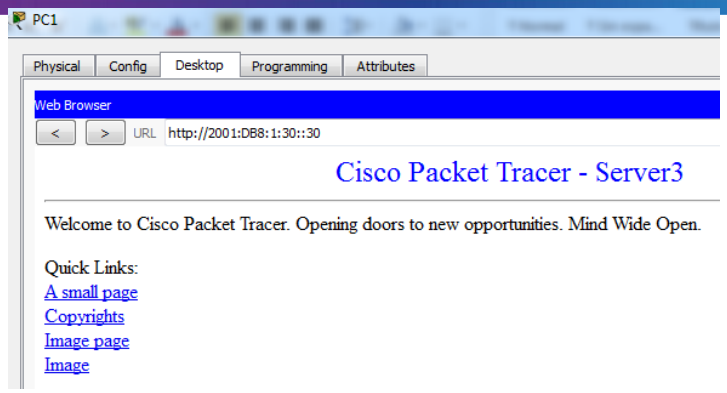
Apply the ACL on the interface closest the source of the traffic to be blocked.

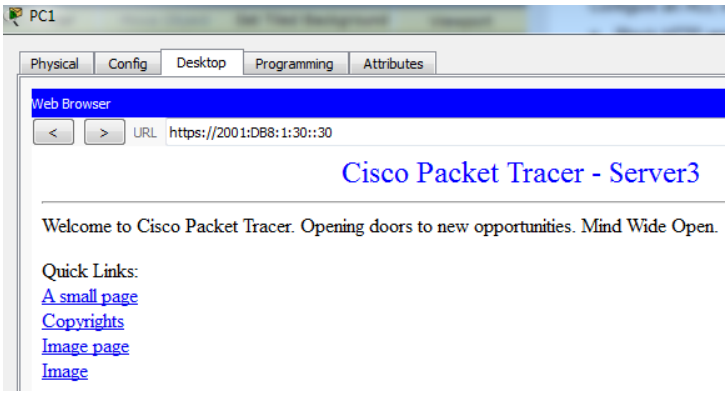
R1(config)# **interface GigabitEthernet0/1**
R1(config-if)# **ipv6 traffic-filter BLOCK_HTTP in**

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

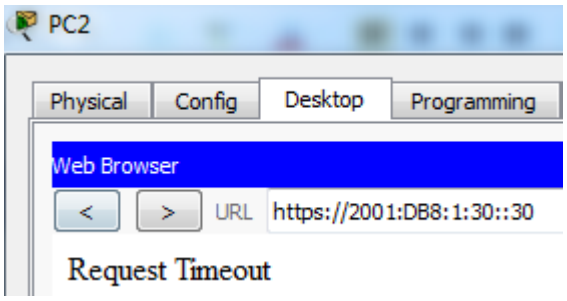
Verify the ACL is operating as intended by conducting the following tests:

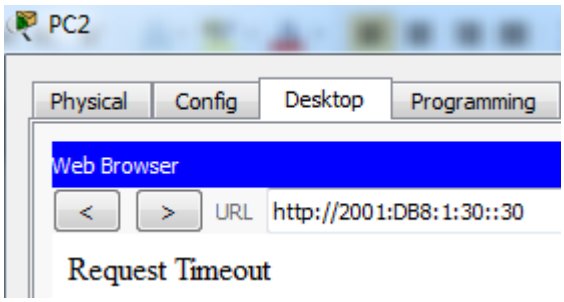
- Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.



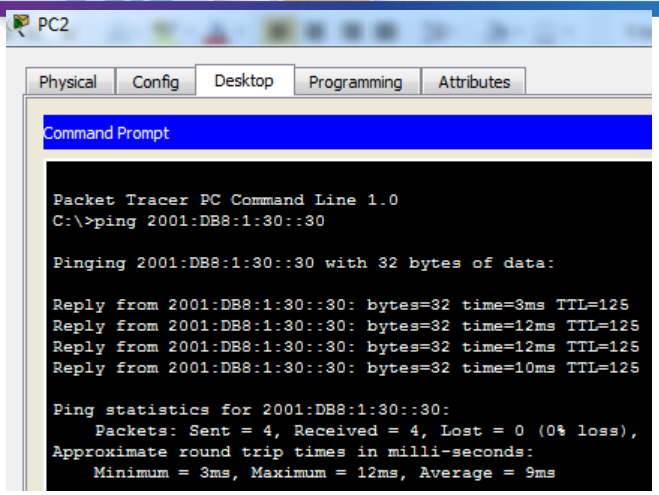




- Open the **web browser** of **PC2** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked




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




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

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

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

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

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

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

b. Allow all other IPv6 traffic to pass.

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

```
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#PER
R3(config-ipv6-acl)#PERmit ipv
R3(config-ipv6-acl)#PERmit ipv6 any
R3(config-ipv6-acl)#PERmit ipv6 any an
R3(config-ipv6-acl)#PERmit ipv6 any any
R3(config-ipv6-acl)#
```

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

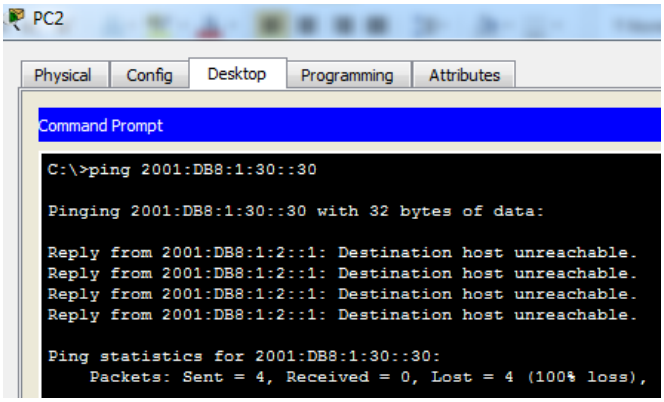
In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked regardless of its source or changes that occur to the network topology, apply the ACL closest to the destination.

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

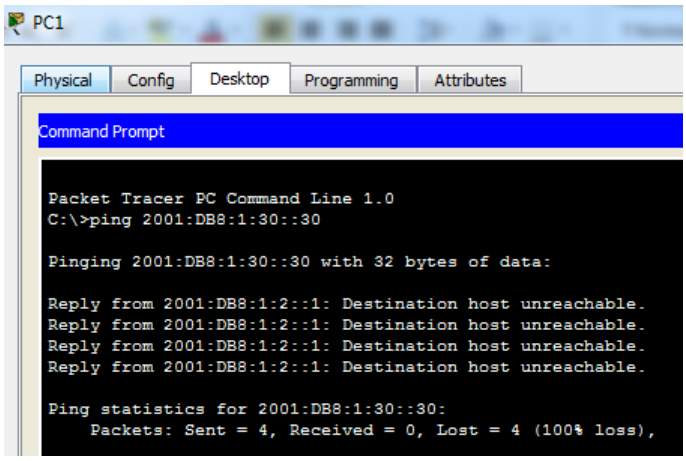
```
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ipv
R3(config-if)#ipv6 tr
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
```

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

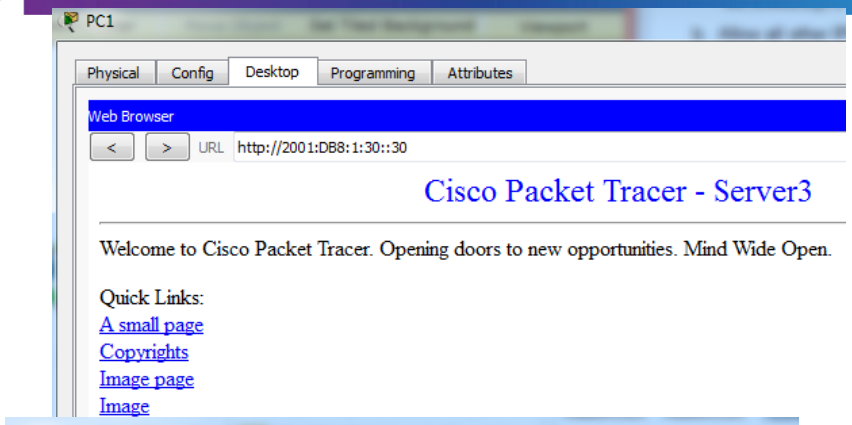
a. Ping from **PC2** to 2001:DB8:1:30::30. The ping should fail.

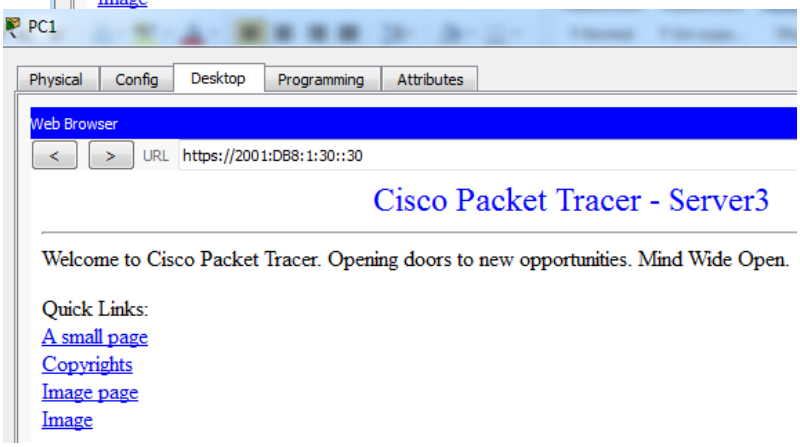



b. Ping from **PC1** to 2001:DB8:1:30::30. The ping should fail.




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


PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://2001:DB8:1:30::30
Cisco Packet Tracer - Server3
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
https://2001:DB8:1:30::30
Cisco Packet Tracer - Server3
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

**7.3.2.4 Lab - Configuring Basic RIPv2 and RIPng**

**Práctica de laboratorio: configuración básica de RIPv2 y RIPng**

**Topología**

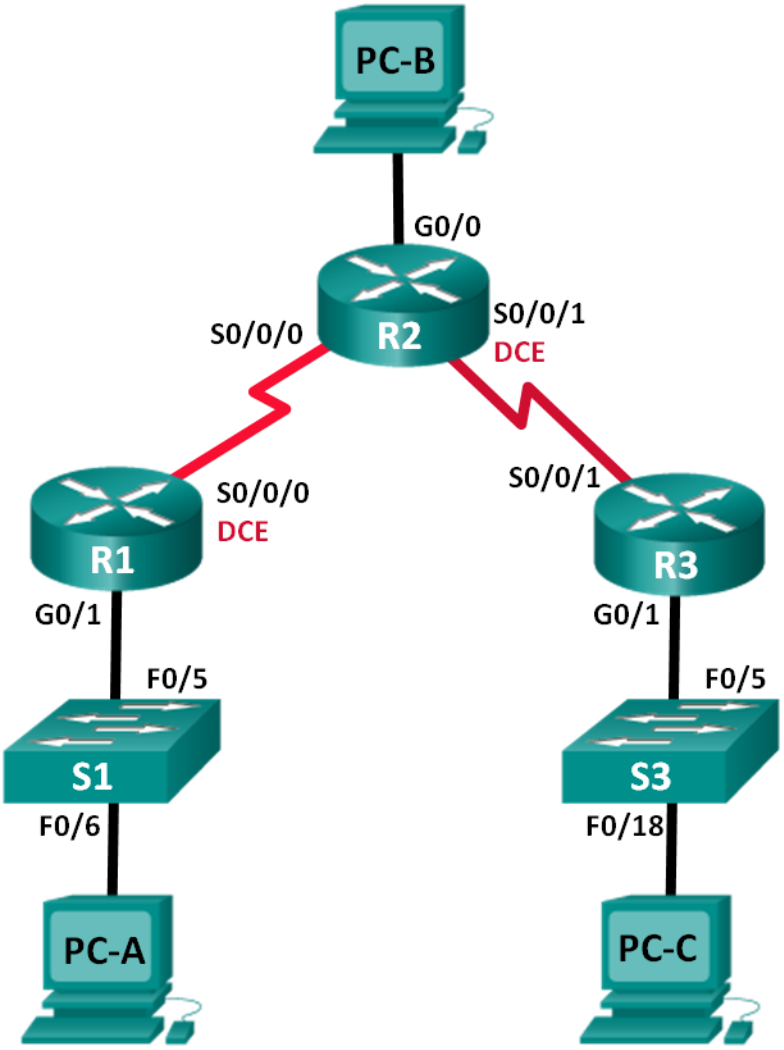



**Tabla de direccionamiento**

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

**Objetivos**

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

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

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

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

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

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

- Verificar la conectividad de extremo a extremo.

**Información básica/situación**

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

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

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

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

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

**Recursos necesarios**

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

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

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

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

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

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

a. Desactive la búsqueda del DNS.

**Este procedimiento de realiza para los Router(1,2,3) y Switch(1,3)**

**(config)#no ip domain-lookup**

b. Configure los nombres de los dispositivos como se muestra en la topología.

**Router(config)#hostname R1 →→ R1(config)#**

**Router(config)#hostname R2 →→ R2(config)#**

**Router(config)#hostname R3 →→ R3(config)#**

**Switch(config)#hostname S1 →→ S1(config)#**

**Switch(config)#hostname S3 →→ S3(config)#**

c. Configurar la encriptación de contraseñas.

**Este procedimiento de realiza para los Router(1,2,3) y Switch(1,3)**

**R1(config)#service password-encryption**

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

**Este procedimiento de realiza para los Router(1,2,3) y Switch(1,3)**

**(config)#enable secret class**

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

**Este procedimiento de realiza para los Router(1,2,3) y Switch(1,3)**

```
(config)#line console 0
(config-line)#password cisco
(config-line)#login
(config-line)#logging synchronous
(config-line)#line vty 0 15
(config-line)#password cisco
(config-line)#login
```

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

**Este procedimiento de realiza para los Router(1,2,3) y Switch(1,3)**

**(config)#banner motd 'Este es un sistema protegido, solo esta permitido el acceso a usuarios autorizados!'**

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

**Este procedimiento de realiza para los Router(1,2,3) y Switch(1,3)**

**(config)#line console 0**
**(config-line)#logging synchronous**

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

**R1(config)#interface gigabitEthernet 0/1**
**R1(config-if)#ip address 172.30.10.1 255.255.255.0**
**R1(config-if)#no shutdown**
**R1(config)#interface serial 0/0/0**
**R1(config-if)#ip address 10.1.1.1 255.255.255.252**
**R1(config-if)#no shutdown**

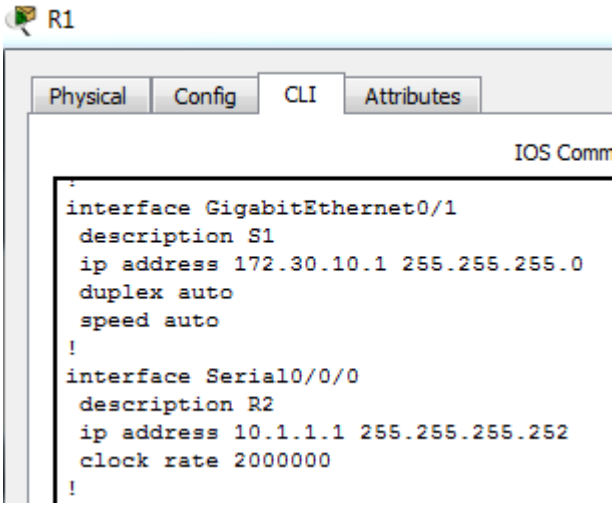
**R2(config)#interface gigabitEthernet 0/0**
**R2(config-if)#ip address 209.165.201.1 255.255.255.0**
**R2(config-if)#no shutdown**
**R2(config)#interface serial 0/0/0**
**R2(config-if)#ip address 10.1.1.2 255.255.255.252**
**R2(config-if)#no shutdown**
**R2(config)#interface serial 0/0/1**
**R2(config-if)#ip address 10.2.2.2 255.255.255.252**
**R2(config-if)#no shutdown**

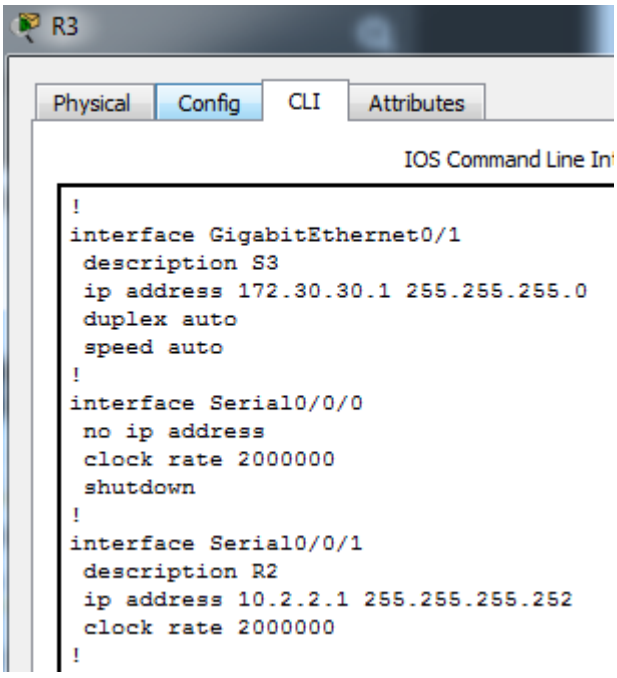
**R3(config)#inter gigabitEthernet 0/1**
**R3(config-if)#ip address 172.30.30.1 255.255.255.0**
**R3(config-if)#no shutdown**
**R3(config)#interface serial 0/0/1**
**R3(config-if)#ip address 10.2.2.1 255.255.255.252**
**R3(config-if)#no shutdown**

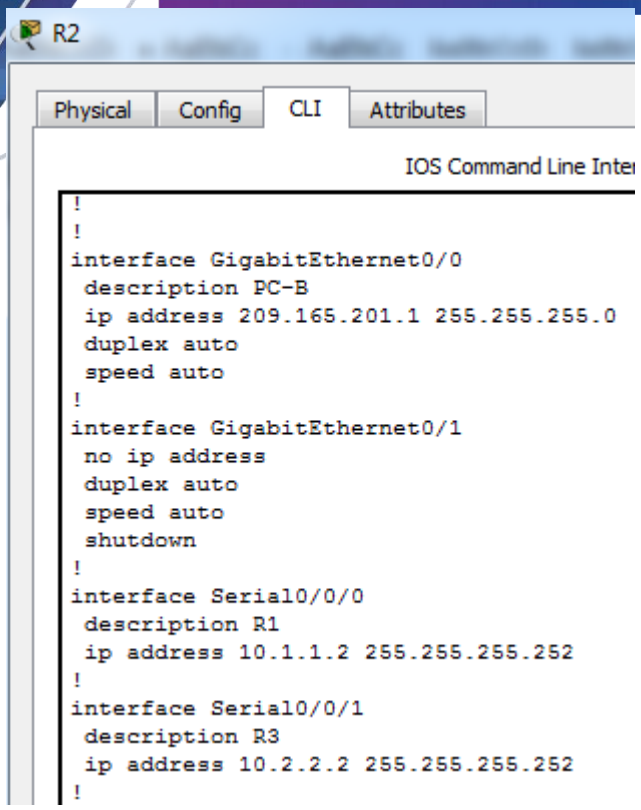
i. Configure una descripción para cada interfaz con una dirección IP.

**R1(config)#interface gigabitEthernet 0/1**

**R1(config-if)#description S1**




R2
Physical
Config
CLI
Attributes
IOS Command Line Inter
!
!
interface GigabitEthernet0/0
 description PC-B
 ip address 209.165.201.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description R1
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 description R3
 ip address 10.2.2.2 255.255.255.252
!

S3

Physical | Config | CLI | Attributes

IOS C

```
interface FastEthernet0/5
 description R3
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
 description PC-C
!
```

S1

Physical | Config | CLI | Attributes

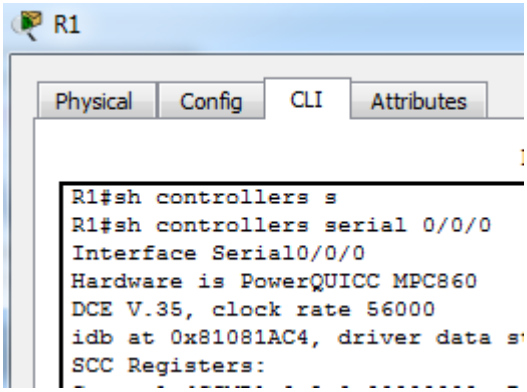
IOS C

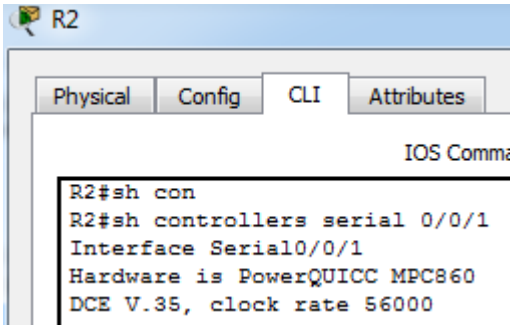
```
!
interface FastEthernet0/5
 description R1
!
interface FastEthernet0/6
 description PC-A
!
```

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

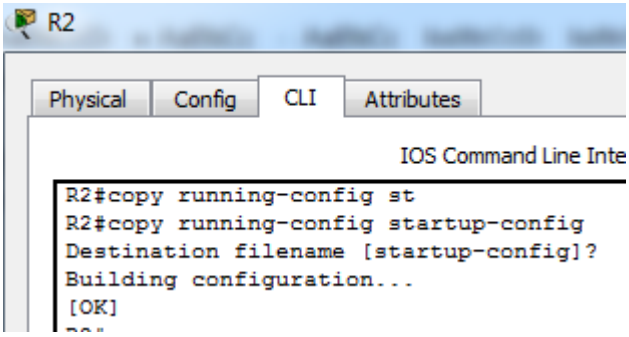
R2(config-if)#clock rate 56000

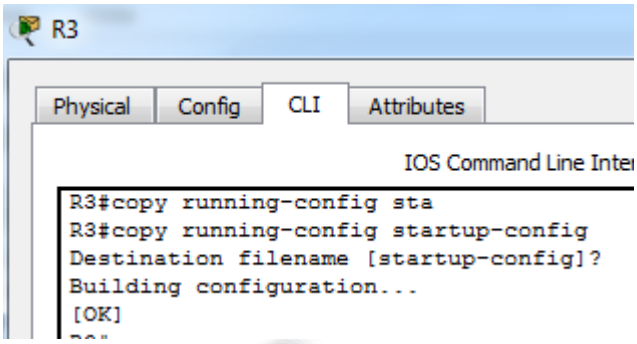
R1(config-if)#clock rate 56000

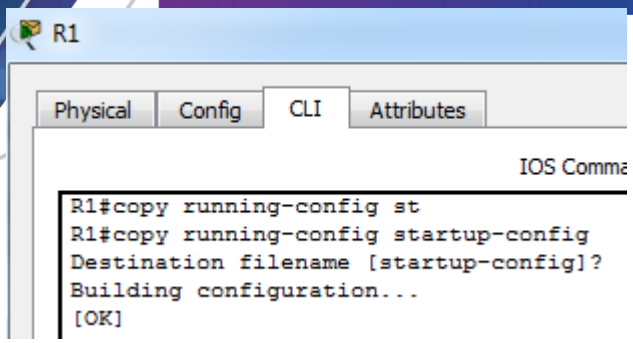


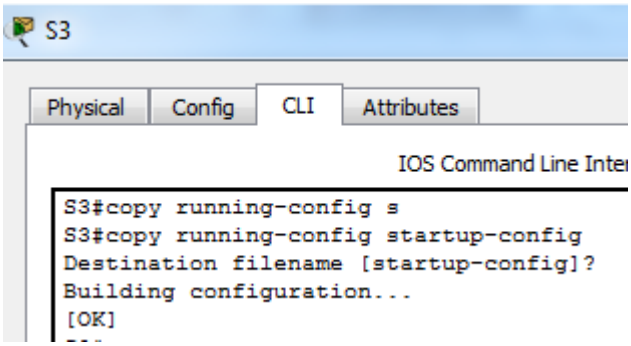



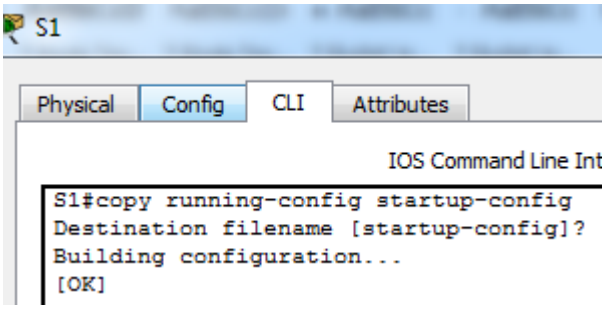

k. Copie la configuración en ejecución en la configuración de inicio.



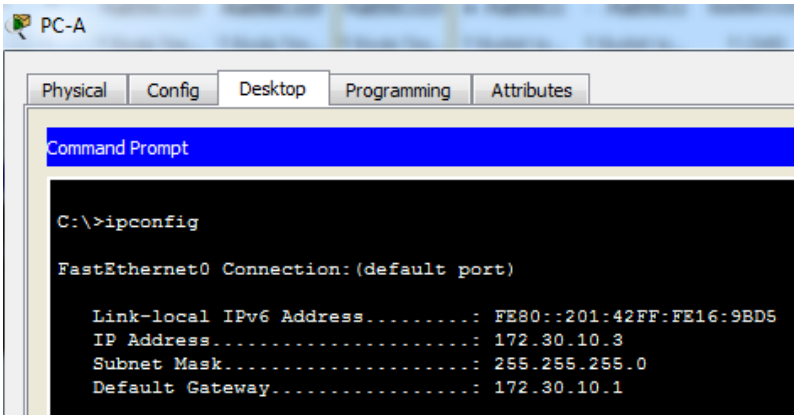


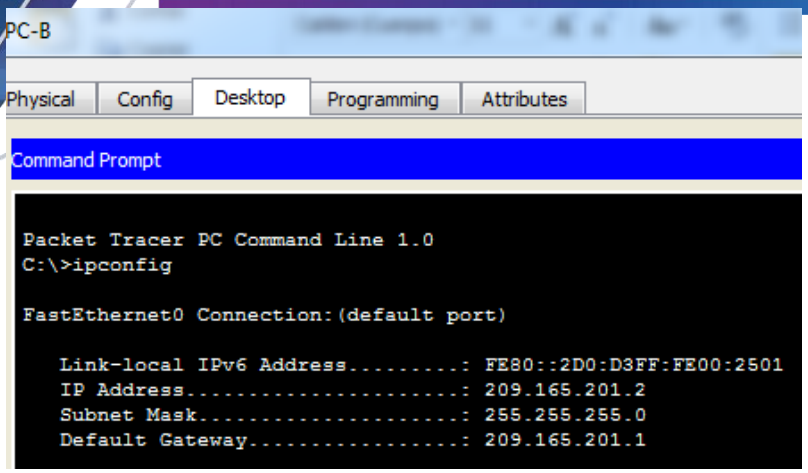



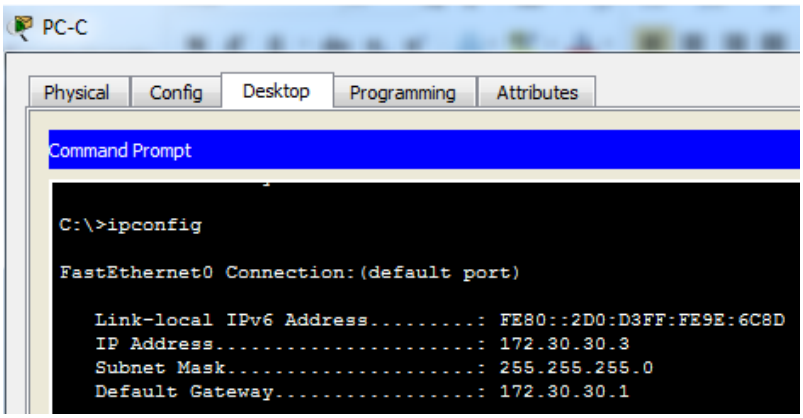




**Paso 1. configurar los equipos host.**

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



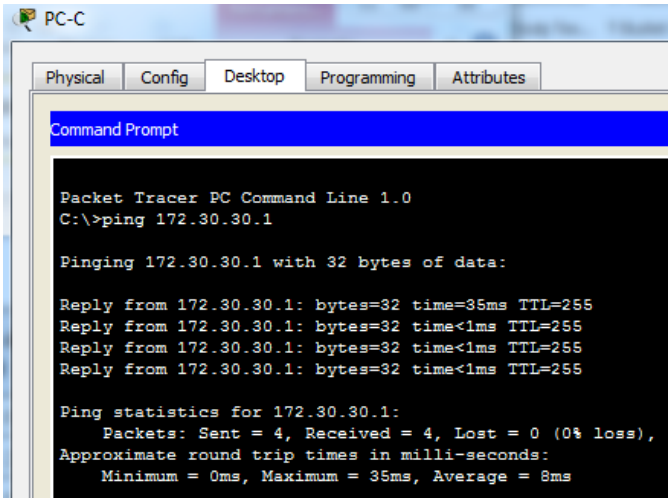


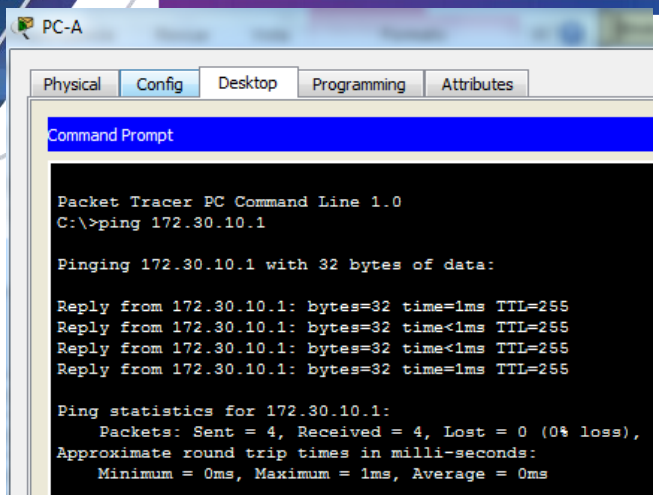



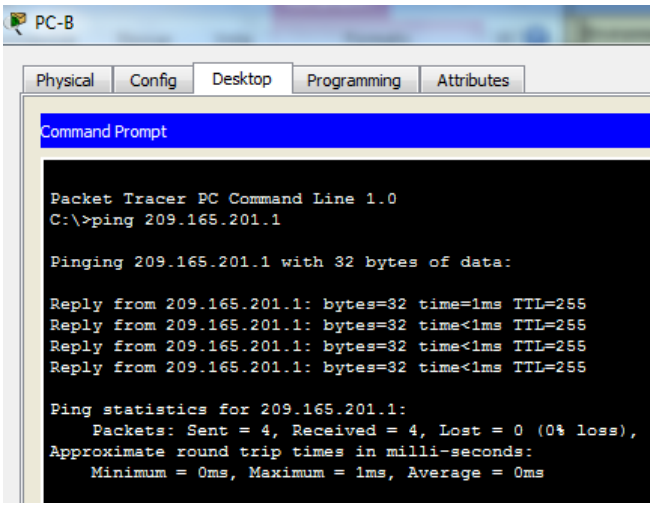

**Paso 2. Probar la conectividad.**

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.

## Parte 2: configurar y verificar el routing RIPv2

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

### Paso 1. Configurar el enrutamiento RIPv2.

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

R1# **config t**

R1(config)# **router rip**

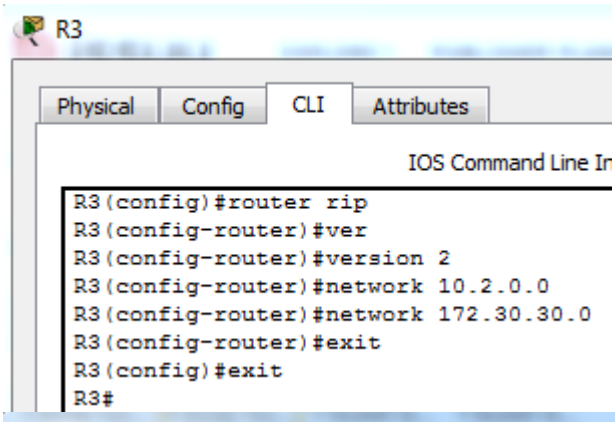
R1(config-router)# **version 2**
R1(config-router)# **passive-interface g0/1**
R1(config-router)# **network 172.30.0.0**
R1(config-router)# **network 10.0.0.0**

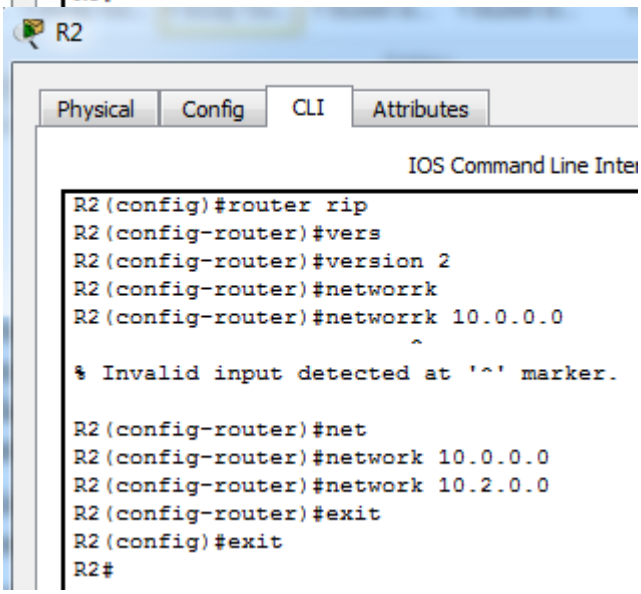
El comando **passive-interface** evita que las actualizaciones de routing se envíen a través de la interfaz especificada. Este proceso evita tráfico de routing innecesario en la LAN. Sin embargo, la red a la que pertenece la interfaz especificada aún se anuncia en las actualizaciones de routing enviadas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

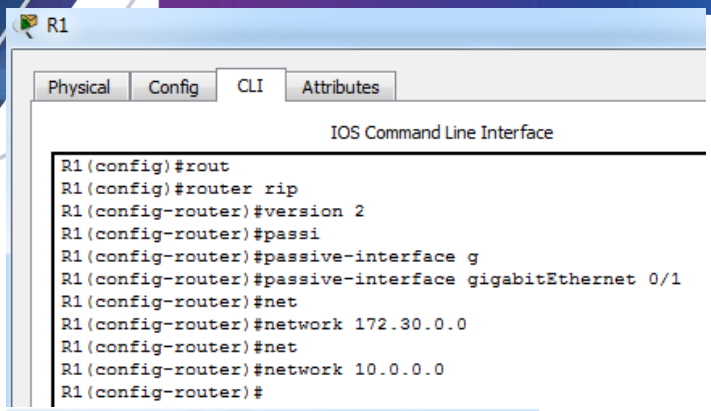
b. Configure RIPv2 en el R3 y utilice la instrucción **network** para agregar las redes apropiadas y evitar actualizaciones de routing en la interfaz LAN.

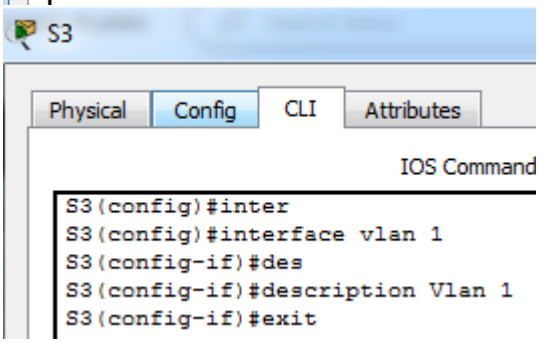
c. Configure RIPv2 en el R2. No anuncie la red 209.165.201.0.

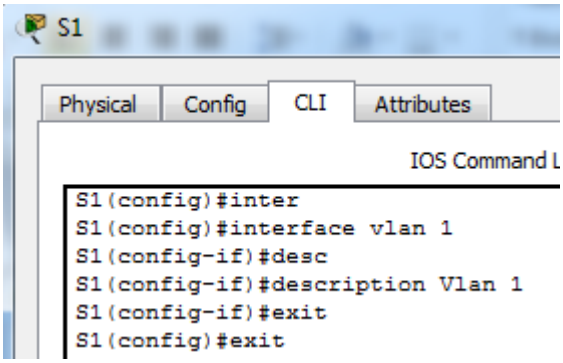
**Nota:** no es necesario establecer la interfaz G0/0 como pasiva en el R2, porque la red asociada a esta interfaz no se está anunciando.






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

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

R2# **show ip interface brief**

| Interface | IP-Address | OK? | Method | Status | Protocol |
|---|---|---|---|---|---|
| Embedded-Service-Engine0/0 | unassigned | YES | unset | administratively down | down |
| GigabitEthernet0/0 | 209.165.201.1 | YES | manual | up | up |
| GigabitEthernet0/1 | unassigned | YES | unset | administratively down | down |
| Serial0/0/0 | 10.1.1.2 | YES | manual | up | up |
| Serial0/0/1 | 10.2.2.2 | YES | manual | up | up |

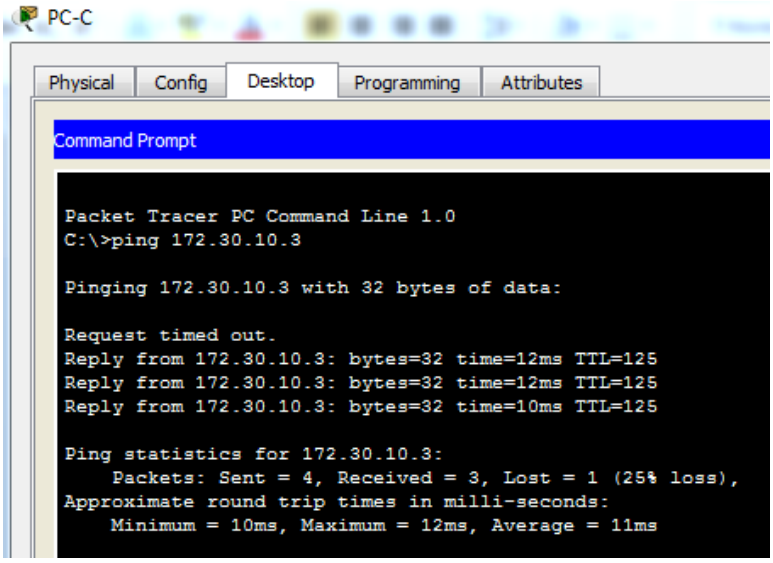
b. Verifique la conectividad entre las computadoras.

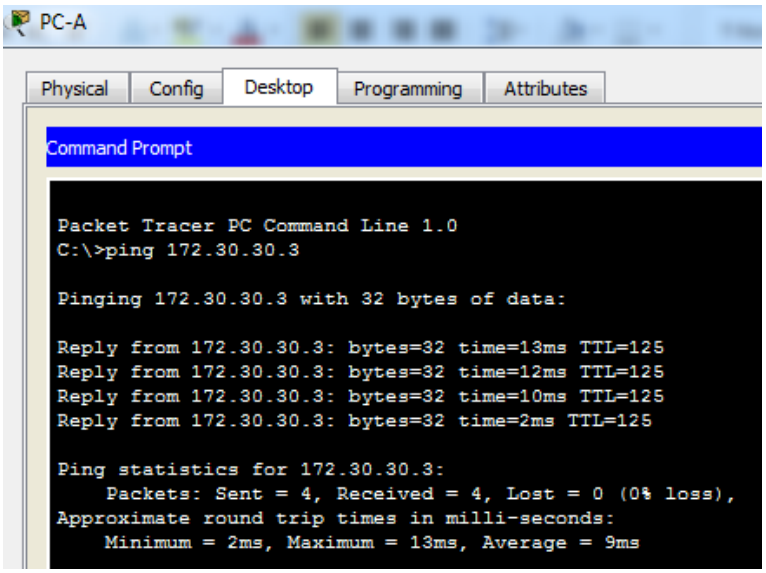
¿Es posible hacer ping de la PC-A a la PC-B? _NO

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

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

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



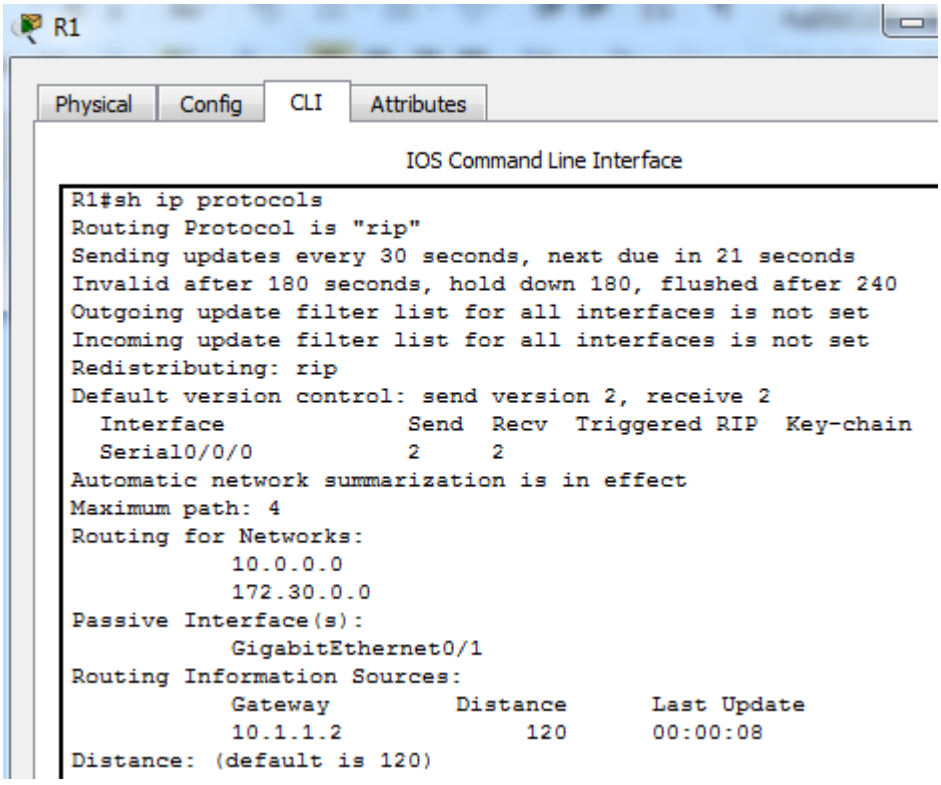

c. Verifique que RIPv2 se ejecute en los routers.

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

R1# **show ip protocols**

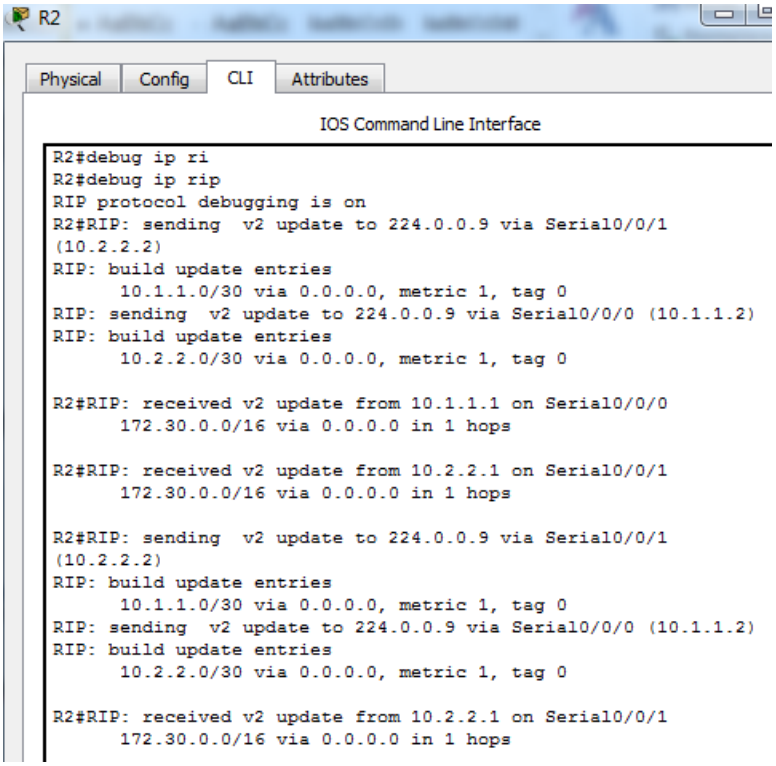
Routing Protocol is "rip"

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 2, receive 2
  Interface  Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0  2  2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway  Distance  Last Update
  10.1.1.2  120
Distance: (default is 120)



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

_ nos muestra la metrica y las redes y el puerto de comunicacion que estan en con este protocolo_




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?

_ Nos muestra toda la configuración que se hizo en este router a lo que respecta al protocolo_

d. Examinar el sumarización automática de las rutas.

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

R2# **show ip route**

<Output Omitted>

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

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

L 10.1.1.2/32 is directly connected, Serial0/0/0

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

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

R1# **show ip route**

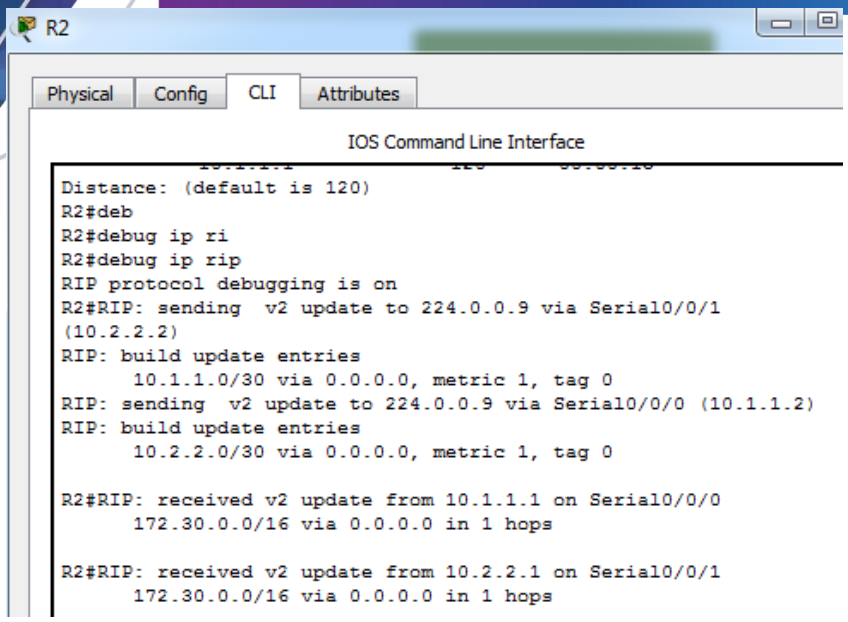
<Output Omitted>
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.30.10.0/24 is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

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

R3# **show ip route**

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

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




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

**Paso 3. Desactivar la sumarización automática.**

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

R1(config)# **router rip**

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

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

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

R1# **clear ip route ***

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

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

R2# **show ip route**

<Output Omitted>

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

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

L 10.1.1.2/32 is directly connected, Serial0/0/0

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

R1# **show ip route**
<Output Omitted>
Gateway of last resort is not set

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

R3# **show ip route**
<Output Omitted>
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.2.2.0/30 is directly connected, Serial0/0/1
L 10.2.2.1/32 is directly connected, Serial0/0/1
R 10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.30.30.0/24 is directly connected, GigabitEthernet0/1
L 172.30.30.1/32 is directly connected, GigabitEthernet0/1
R 172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1

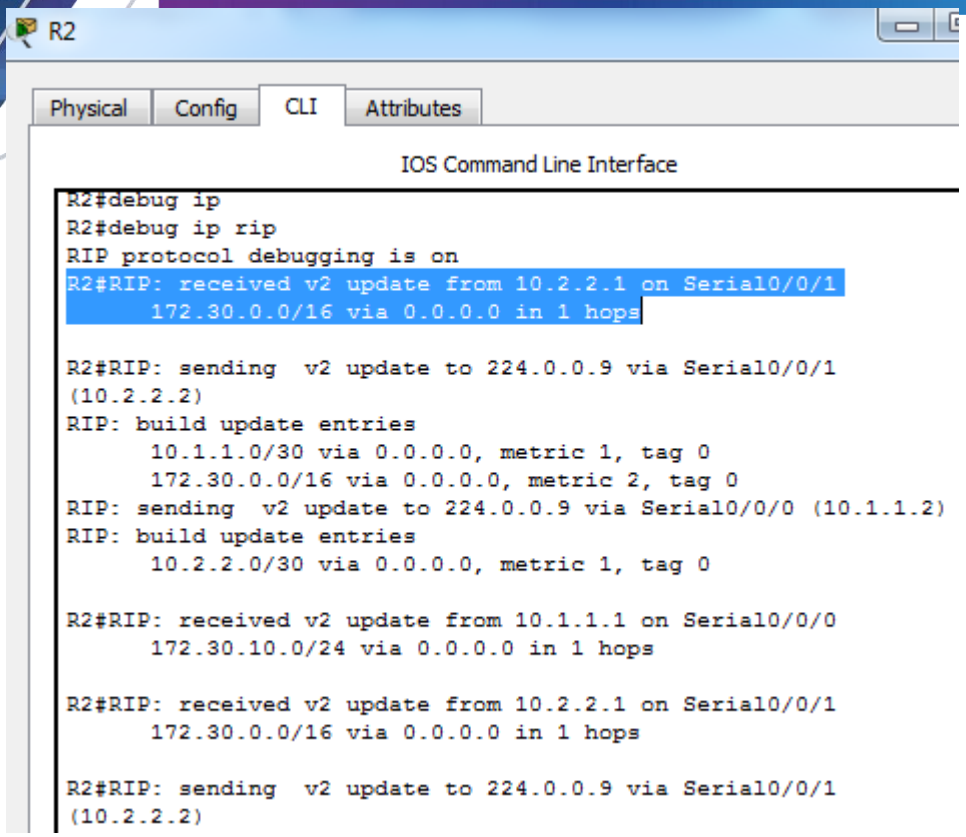
d. Utilice el comando **debug ip rip** en el R2 para examinar las actualizaciones RIP.

**R2# debug ip rip**

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

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

__10.2.2.2 y 172.30.10.0_____




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

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

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

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

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

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

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

c. Consulte la tabla de routing en el R1.

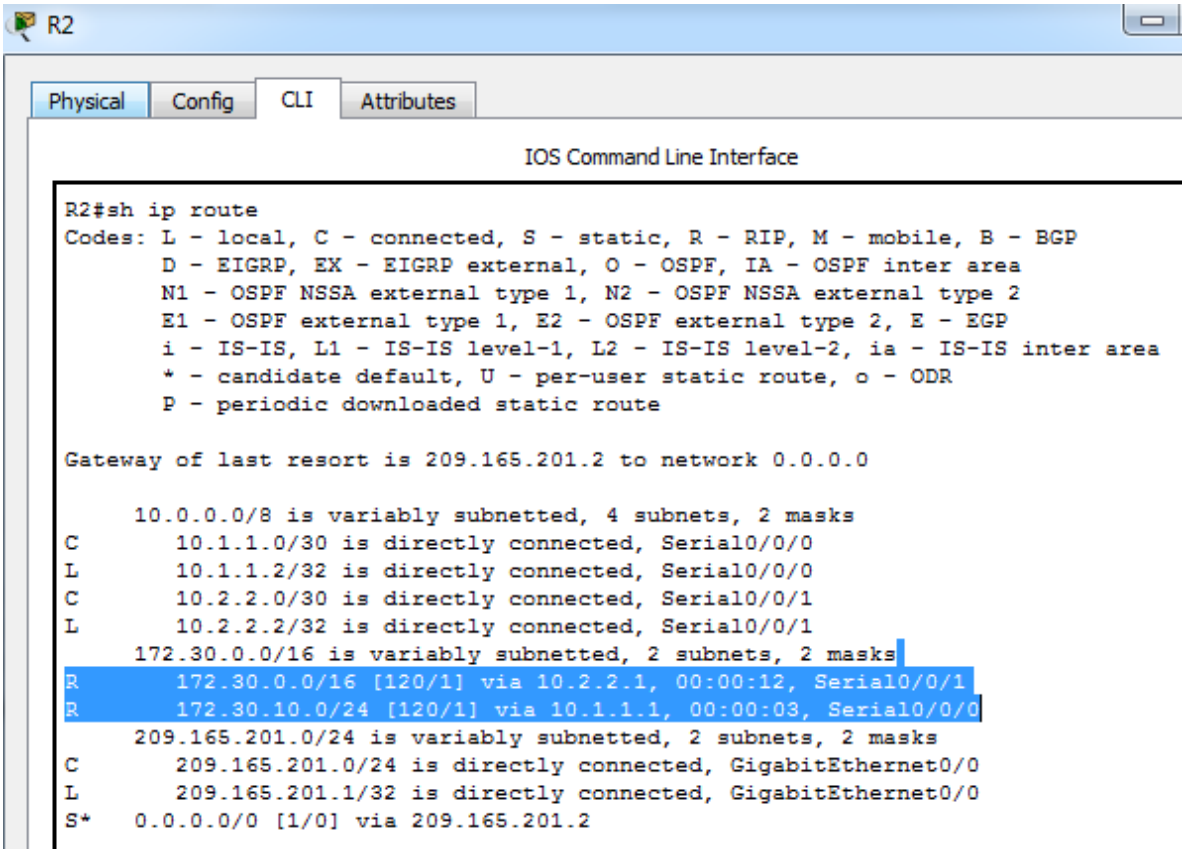
R1# **show ip route**
<Output Omitted>
Gateway of last resort is 10.1.1.2 to network 0.0.0.0

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

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 172.30.10.0/24 is directly connected, GigabitEthernet0/1
L 172.30.10.1/32 is directly connected, GigabitEthernet0/1
R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0

¿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?

___SE VISUALIZA QUE LA DIRECCION DEL R1 Y 3R3 __




d. Consulte la tabla de routing en el R2.

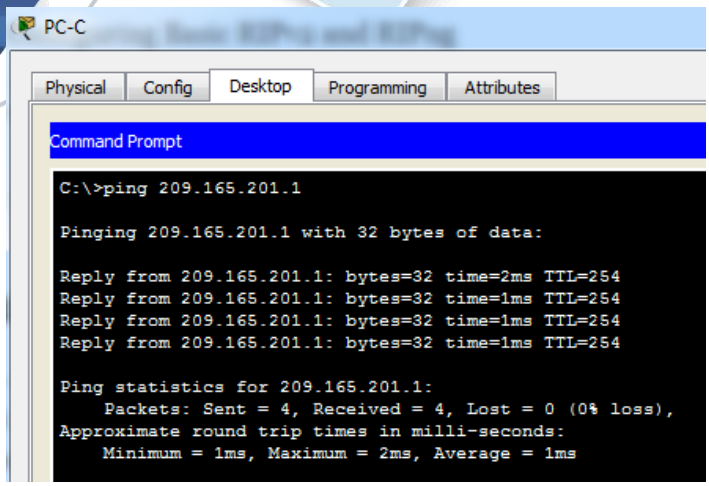
¿En qué forma se proporciona la ruta para el tráfico de Internet en la tabla de routing?

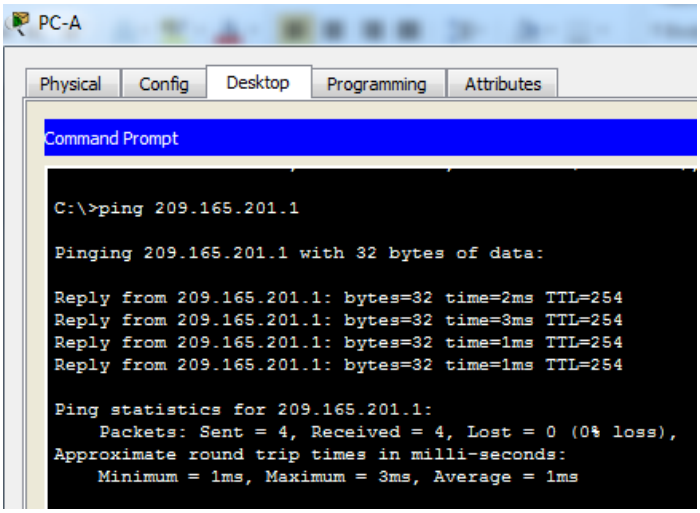
__ por las rutas estaticas _

**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.

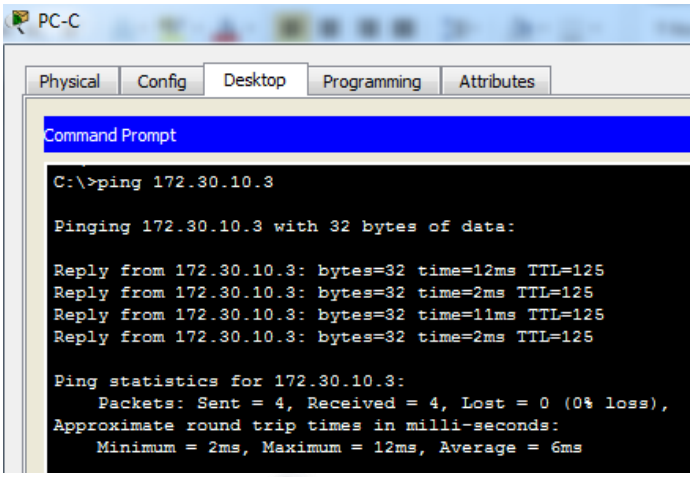
¿Tuvieron éxito los pings? __SI___




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? __SI___




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

## Parte 3: configurar IPv6 en los dispositivos

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

**Tabla de direccionamiento**

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

### Paso 1. configurar los equipos host.

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

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

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

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

R2

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
R2(config)#inte
R2(config)#interface g0/0
R2(config-if)#ip?
ip  ipv6
R2(config-if)#ipv6 ad
R2(config-if)#ipv6 address 2001:db8:acad:b::2/64
R2(config-if)#ipv6 ad
R2(config-if)#ipv6 address fe80::2 li
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#exit
R2(config)#int s
R2(config)#int
R2(config)#interface se
R2(config)#interface serial 0/0/0
R2(config-if)#ipv6 address 2001:db8:acad:12::2/64
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#exit
R2(config)#interface serial 0/0/1
R2(config-if)#ipv6 address 2001:db8:acad:23::2/64
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

R1

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#inter g
R1(config)#inter gigabitEthernet 0/1
R1(config-if)#ipv6 ad
R1(config-if)#ipv6 address 2001:db8:acad:a::1/64
R1(config-if)#ipv6 address fe80::1 li
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#inter se
R1(config)#inter serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:12::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

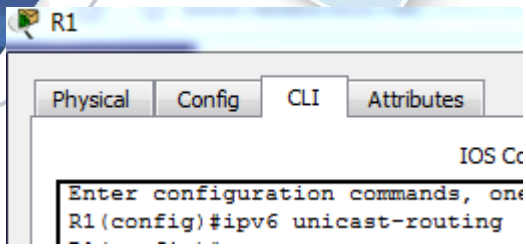
R3

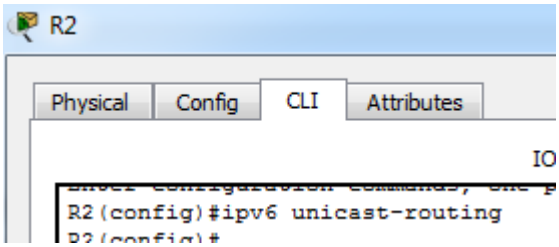
Physical | Config | CLI | Attributes

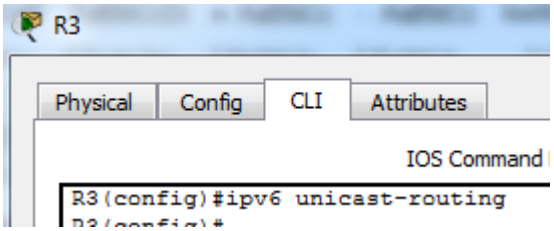
IOS Command Line Interface

```
R3(config)#inter g
R3(config)#inter gigabitEthernet 0/1
R3(config-if)#ipv
R3(config-if)#ipv6 ad
R3(config-if)#ipv6 address 2001:db8:acad:c::3/64
R3(config-if)#ipv6 ad
R3(config-if)#ipv6 address fe80::3 li
R3(config-if)#ipv6 address fe80::3 link-local
R3(config-if)#exit
R3(config)#inter s0/0/1
R3(config-if)#ipv6 address 2001:db8:acad:23::3/64
R3(config-if)#ipv6 address fe80::3 link-local
```

b. Habilite el routing IPv6 en cada router.




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

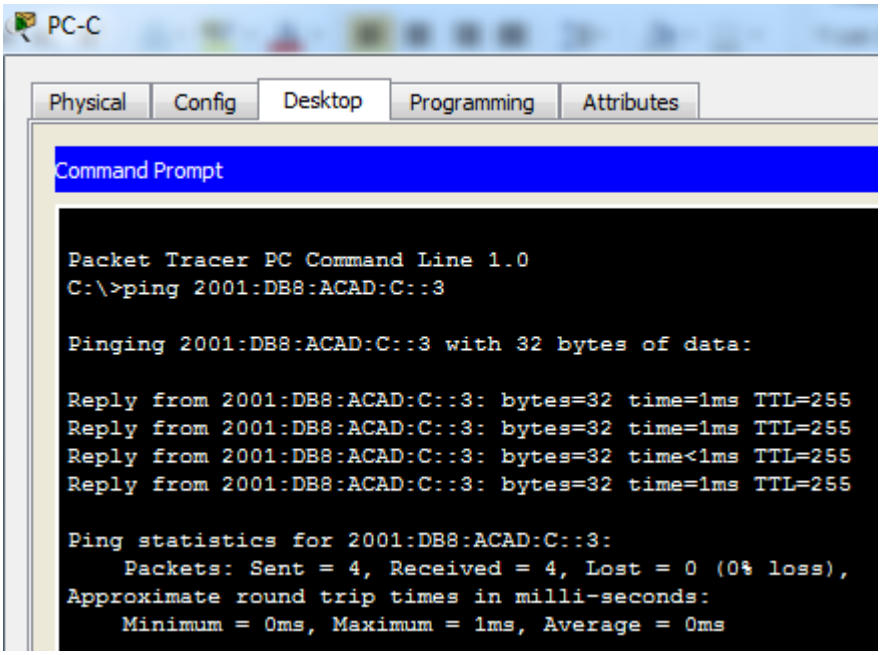
___ show ipv6 interface brief _____

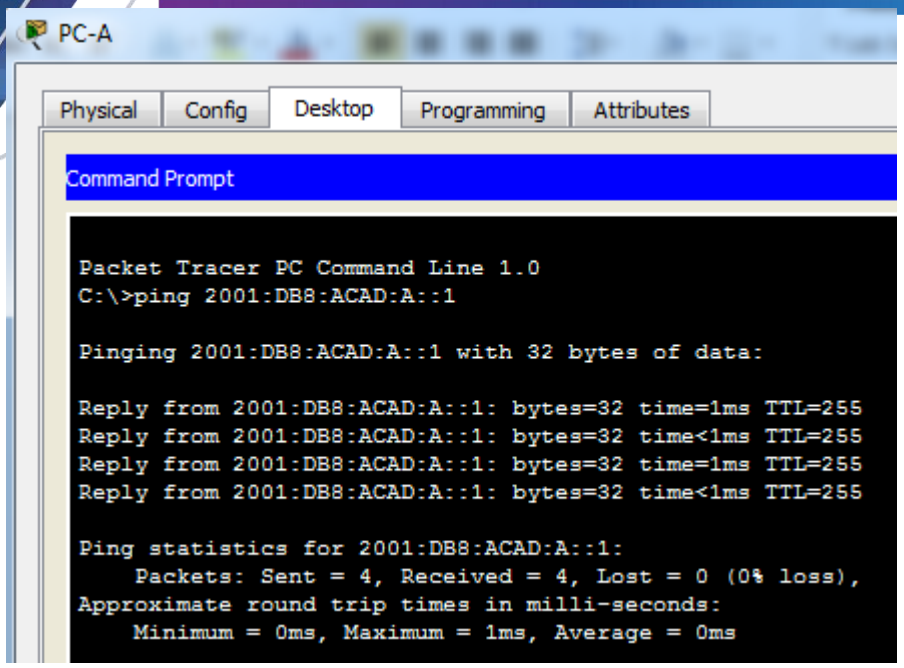
```
R1#show ipv6 interface brief
GigabitEthernet0/0         [administratively down/down]
GigabitEthernet0/1         [up/up]
    FE80::1
    2001:DB8:ACAD:A::1
Serial0/0/0                [up/up]
    FE80::1
    2001:DB8:ACAD:12::1
Serial0/0/1                [administratively down/down]
Vlan1         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

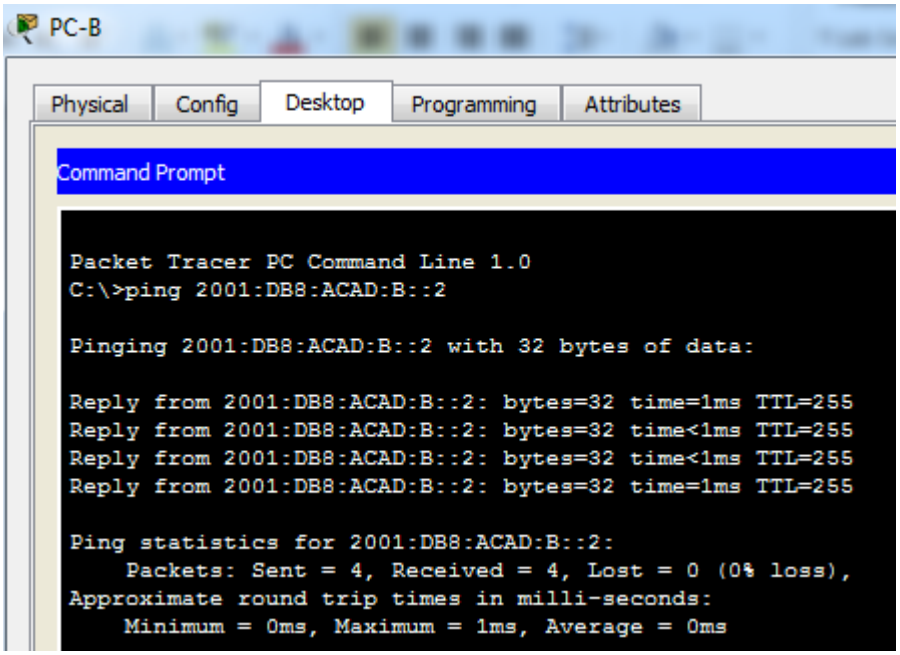
```
R2#sh ipv6 interface brief
GigabitEthernet0/0         [up/up]
    FE80::2
    2001:DB8:ACAD:B::2
GigabitEthernet0/1         [administratively down/down]
Serial0/0/0                [up/up]
    FE80::2
    2001:DB8:ACAD:12::2
Serial0/0/1                [up/up]
    FE80::2
    2001:DB8:ACAD:23::2
Vlan1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

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

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






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

Ping del R3 → R2

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

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::2, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6
ms
```

Ping del R2 → R1

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

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::1, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8
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.

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

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

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

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

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

```
R1(config)#inter
R1(config)#interface g
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ipv
R1(config-if)#ipv6 rip t
R1(config-if)#ipv6 rip te
R1(config-if)#ipv6 rip Test1 en
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#exit
R1(config)#inter
R1(config)#interface de
R1(config)#interface s
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 rip Test1 enable
```

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

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip
R2(config-if)#ipv6 rip Test2 en
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#interface serial 0/0/1
R2(config-if)#ipv6 rip Test2 enable
```

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

```
R3(config)#interface gigabitEthernet 0/1
R3(config-if)#ipv6 rip Test3 en
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#inter
R3(config-if)#interface s/0/0/1
                 ^
% Invalid input detected at '^' marker.

R3(config-if)#exit
R3(config)#inte
R3(config)#interface se
R3(config)#interface serial 0/0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#exit
```

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

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

R1# **show ipv6 protocols**

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "rip Test1"

Interfaces:

Serial0/0/0

GigabitEthernet0/1

Redistribution:

None

¿En qué forma se indica RIPng en el resultado?

Show ipv6 rip Test1

```
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
```

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

R1# **show ipv6 rip Test1**

RIP process "Test1", port 521, multicast-group FF02::9, pid 314

Administrative distance is 120. Maximum paths is 16

Updates every 30 seconds, expire after 180

Holddown lasts 0 seconds, garbage collect after 120

Split horizon is on; poison reverse is off
Default routes are not generated
Periodic updates 1, trigger updates 0
Full Advertisement 0, Delayed Events 0
Interfaces:
GigabitEthernet0/1
Serial0/0/0
Redistribution:
None

¿Cuáles son las similitudes entre RIPv2 y RIPng?

___similitud como la difusión de rutas____

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

___show ipv6 router_____

```
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
```

En el R1, ¿cuántas rutas se descubrieron mediante RIPng? ____2_____

En el R2, ¿cuántas rutas se descubrieron mediante RIPng? ____3____

En el R3, ¿cuántas rutas se descubrieron mediante RIPng? ____2_____

g. Verifique la conectividad entre las computadoras.

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

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

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

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

¿Por qué algunos pings tuvieron éxito y otros no?

__rip estaba desactivado_____

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

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

__ R2(config)#ipv6 route 0:0:0:0::0/64 gigabitEthernet 0/0 _____

```
R2(config)#ipv6 route 0:0:0:0::0/64 gigabitEthernet 0/0
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**

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

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

R2# **show ipv6 route**

IPv6 Routing Table - 10 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

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

D - EIGRP, EX - EIGRP external

S ::/64 [1/0]

via 2001:DB8:ACAD:B::B

R 2001:DB8:ACAD:A::/64 [120/2]

via FE80::1, Serial0/0/0

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

via ::, GigabitEthernet0/1

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

via ::, GigabitEthernet0/1

R 2001:DB8:ACAD:C::/64 [120/2]

via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
via ::, Serial0/0/0
L 2001:DB8:ACAD:12::2/128 [0/0]
via ::, Serial0/0/0
C 2001:DB8:ACAD:23::/64 [0/0]
via ::, Serial0/0/1
L 2001:DB8:ACAD:23::2/128 [0/0]
via ::, Serial0/0/1
L FF00::/8 [0/0]
via ::, Null0

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

__Porque las rutas se publican en los demas Router y estableciendo rutas estaticas_____

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

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

__El Router que tiene el acceso a internet envia la ruta a los demas routers y se proporcionan por medio de Rip por ruta estatica_____

**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____

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

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

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=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 = 3ms, Average = 2ms
```

**Reflexión**

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

- Permite optimizar los recursos del router, manteniendo una red con mayor estabilidad y confiabilidad.

- Porque en versión 2 para la sumarizacion necesaria clases completas para que detecte las redes.
- Para que identifique y actualice con las rutas directamente conectadas.

2. En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3?
   - Las rutas se inicia con la letra R
   - Con la ruta estatica configurada con ip router.
3. ¿En qué se diferencian la configuración de RIPv2 y la de RIPng?
   - RIPng se habilita en una interfaz, no en la configuración del router.
   - En RIPv2 admite actualizaciones RIPv1, RIPng no.
   - En RIPv2 podemos colocar etiquetas a las rutas
   - RIPv2 codifica el siguiente salto en cada entrada en la ruta, mientras que con RIPng se requiere de una codificación especifica
   - RIPng puede configurar varias redes en cada interfaz con un proceso.

Tabla de resumen de interfaces del router

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

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

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

**Topología**

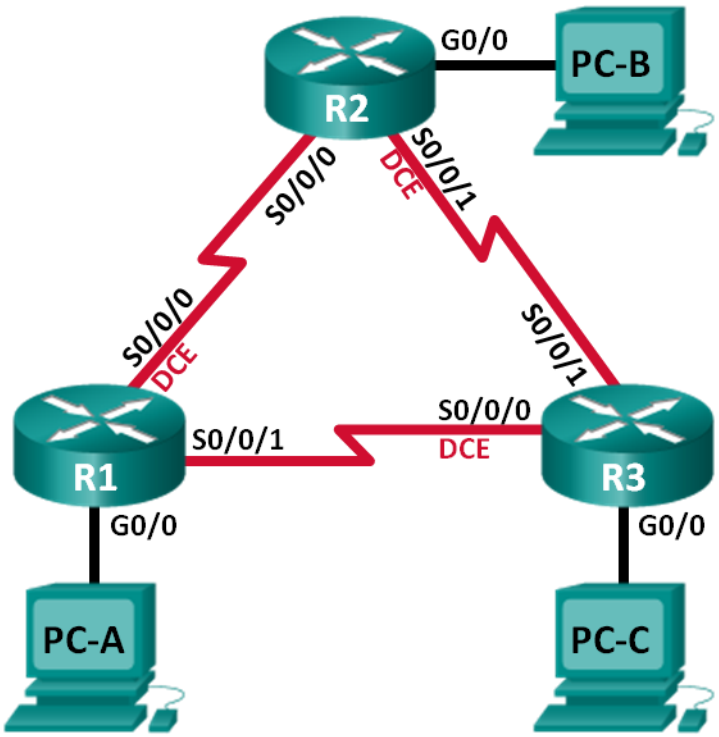


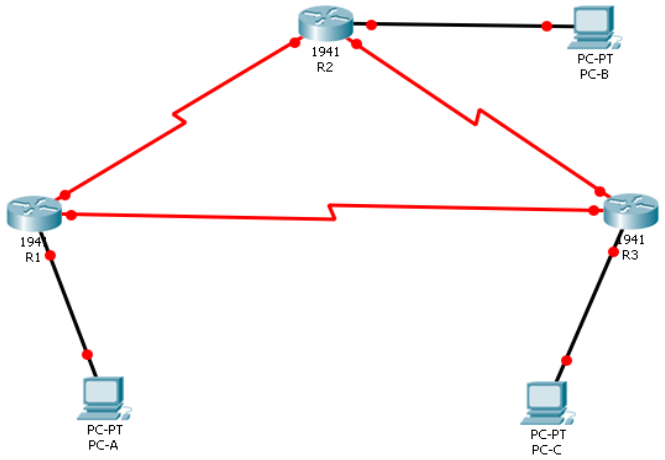
**Tabla de direccionamiento**

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
|---|---|---|---|---|
| R1 | G0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| | S0/0/0 (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 |

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

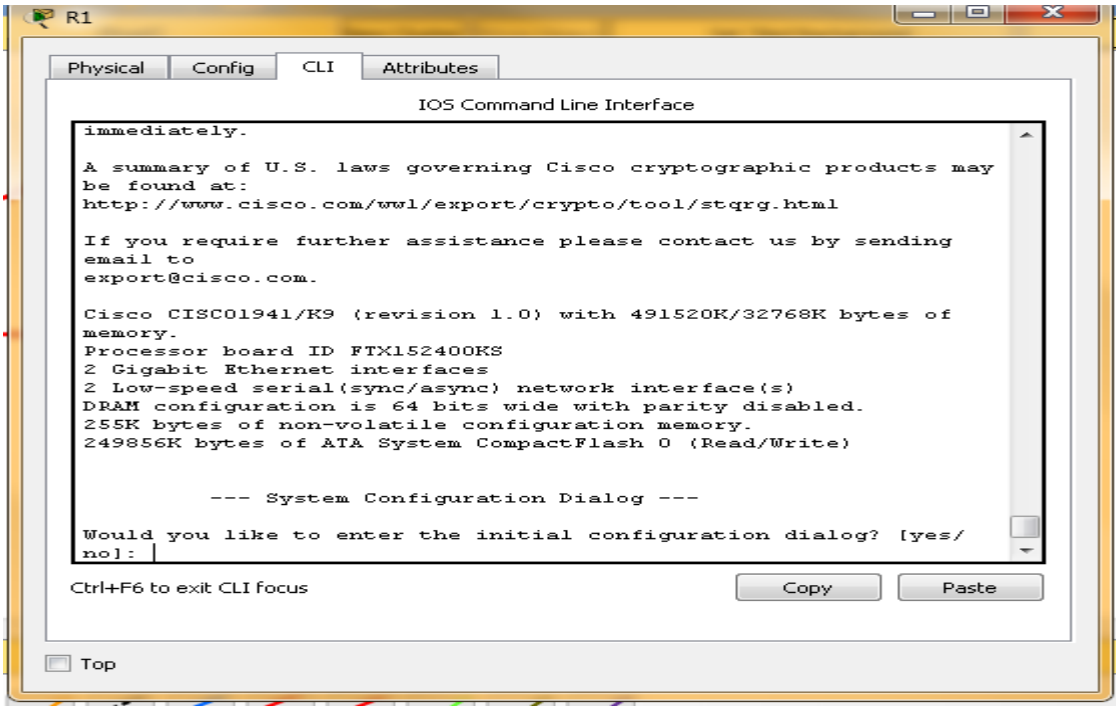
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

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

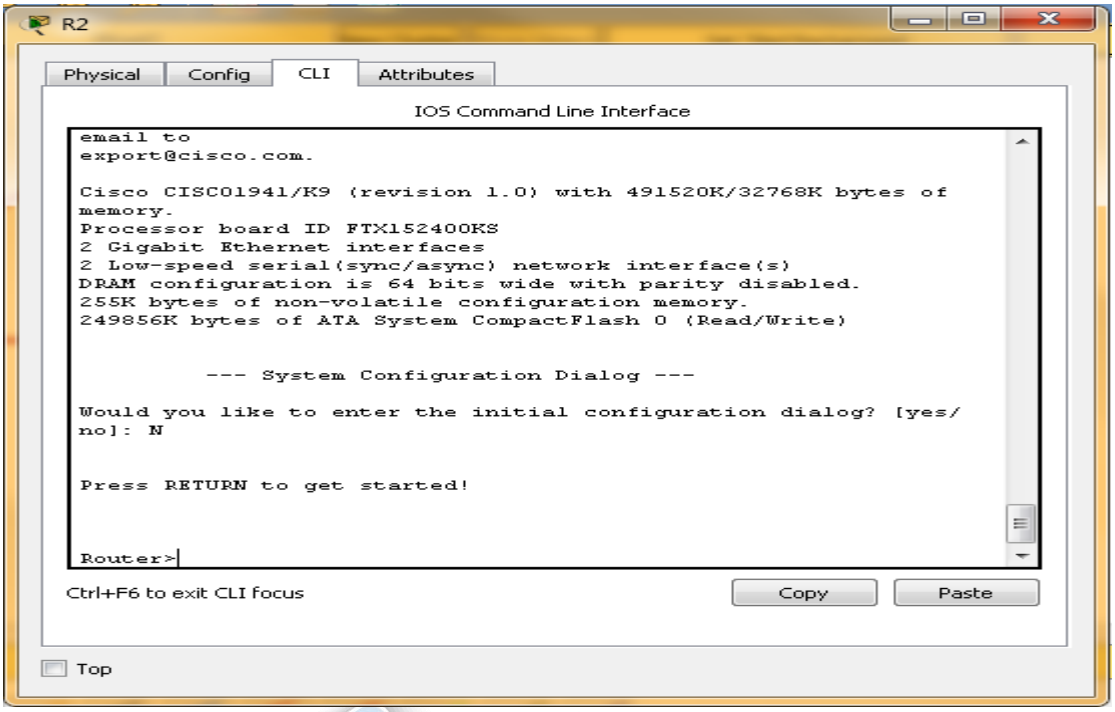


**Step 2: inicializar y volver a cargar los routers según sea necesario.**

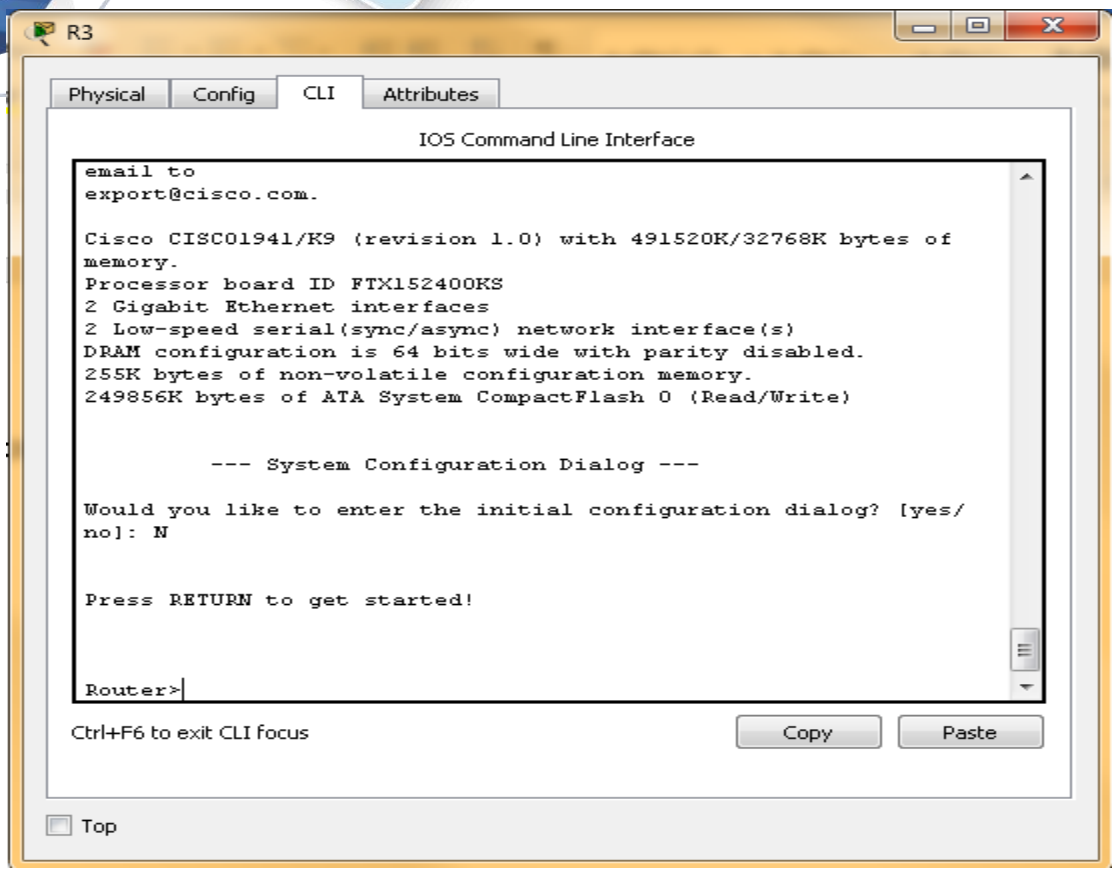
**ROUTER 1**




**ROUTER 2**



**ROUTER 3**




**Step 3: configurar los parámetros básicos para cada router.**

a. Desactive la búsqueda del DNS.

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

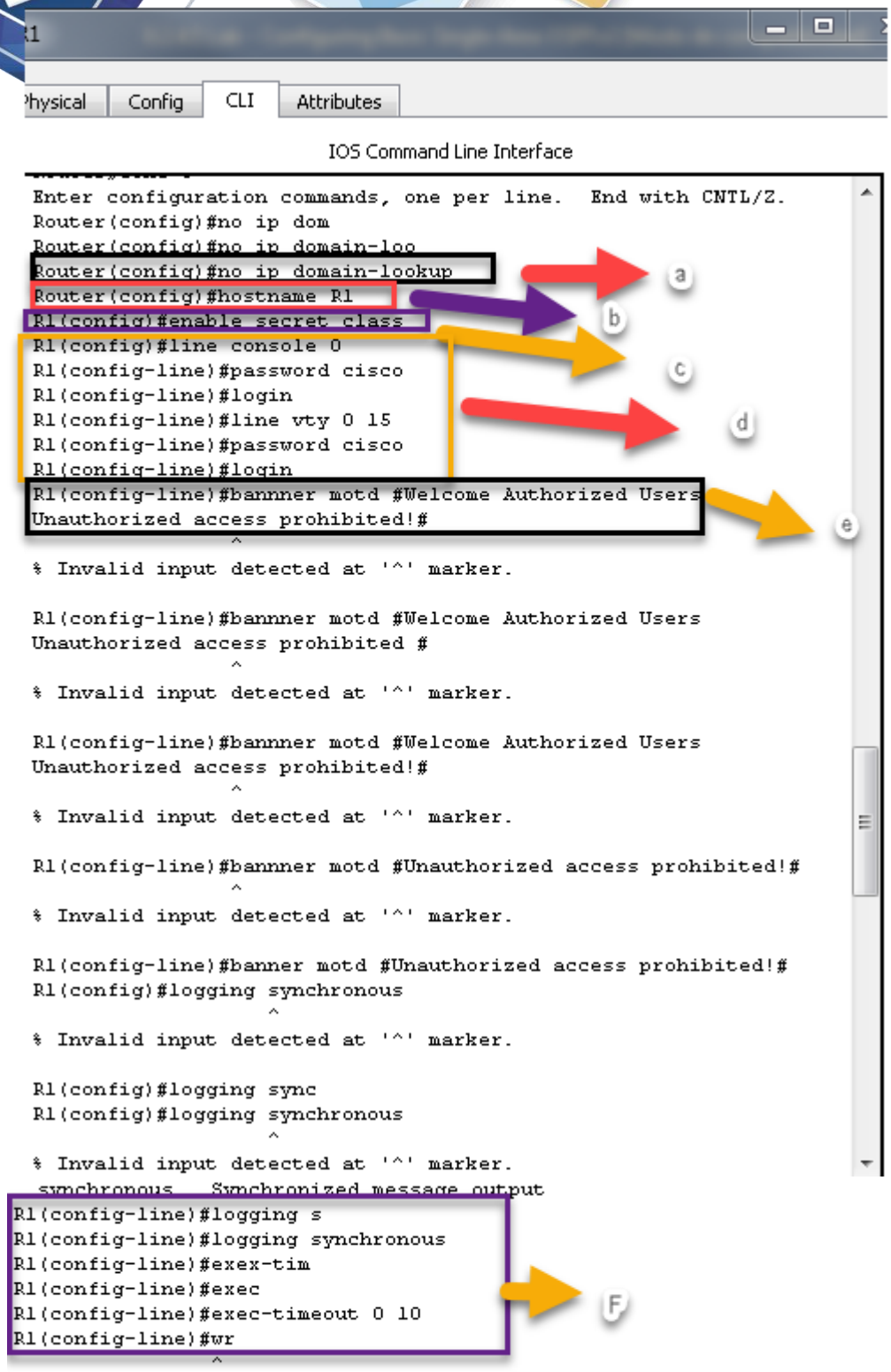
c. Asigne **class** como la contraseña del modo EXEC privilegiado.

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

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

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

Router 1 Puntos a-b-c-d-e-f




**Router 2 Puntos a-b-c-d-e-f**

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-l
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console o
                          ^
% Invalid input detected at '^' marker.

R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#banner motd #unathorized access prohibited!#
R2(config)#line console 0
R2(config-line)#lo
R2(config-line)#loggi
R2(config-line)#logging s
R2(config-line)#logging synchronous
R2(config-line)#exec-time
R2(config-line)#exec-timeout 0 10
```

a

b

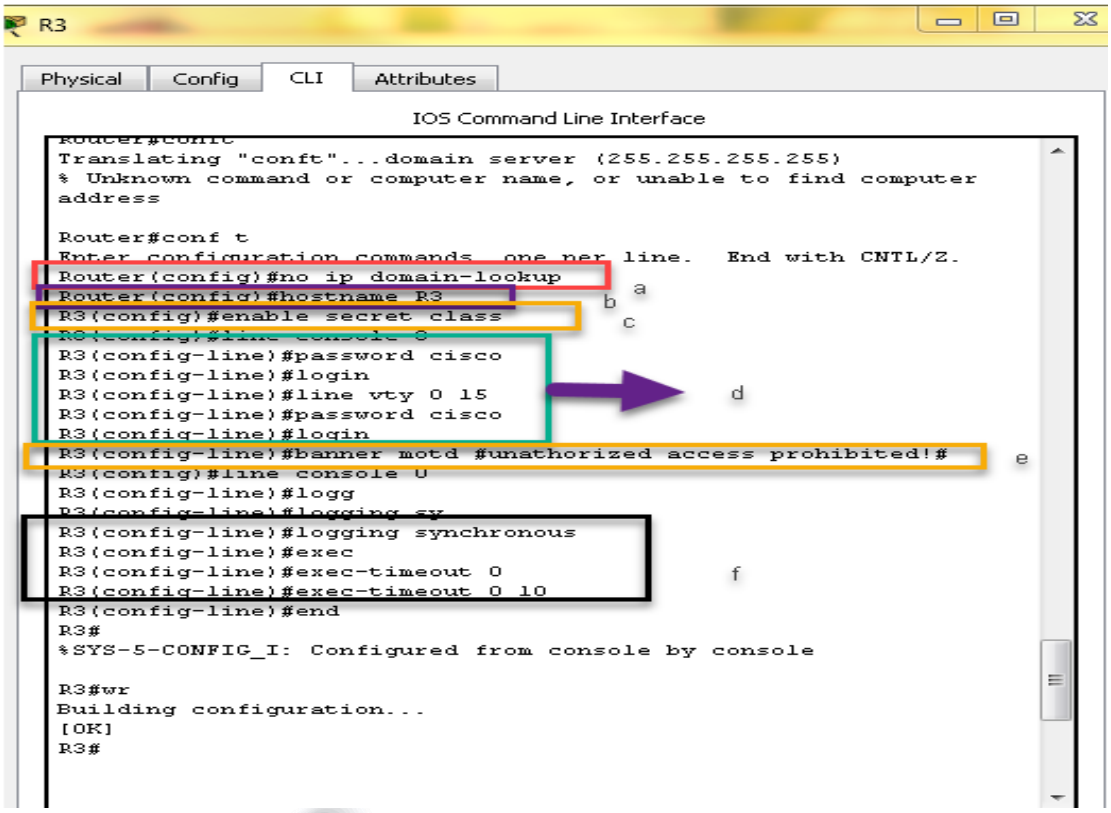
c

d

e

F

**Router 3  Puntos a-b-c-d-e-f**

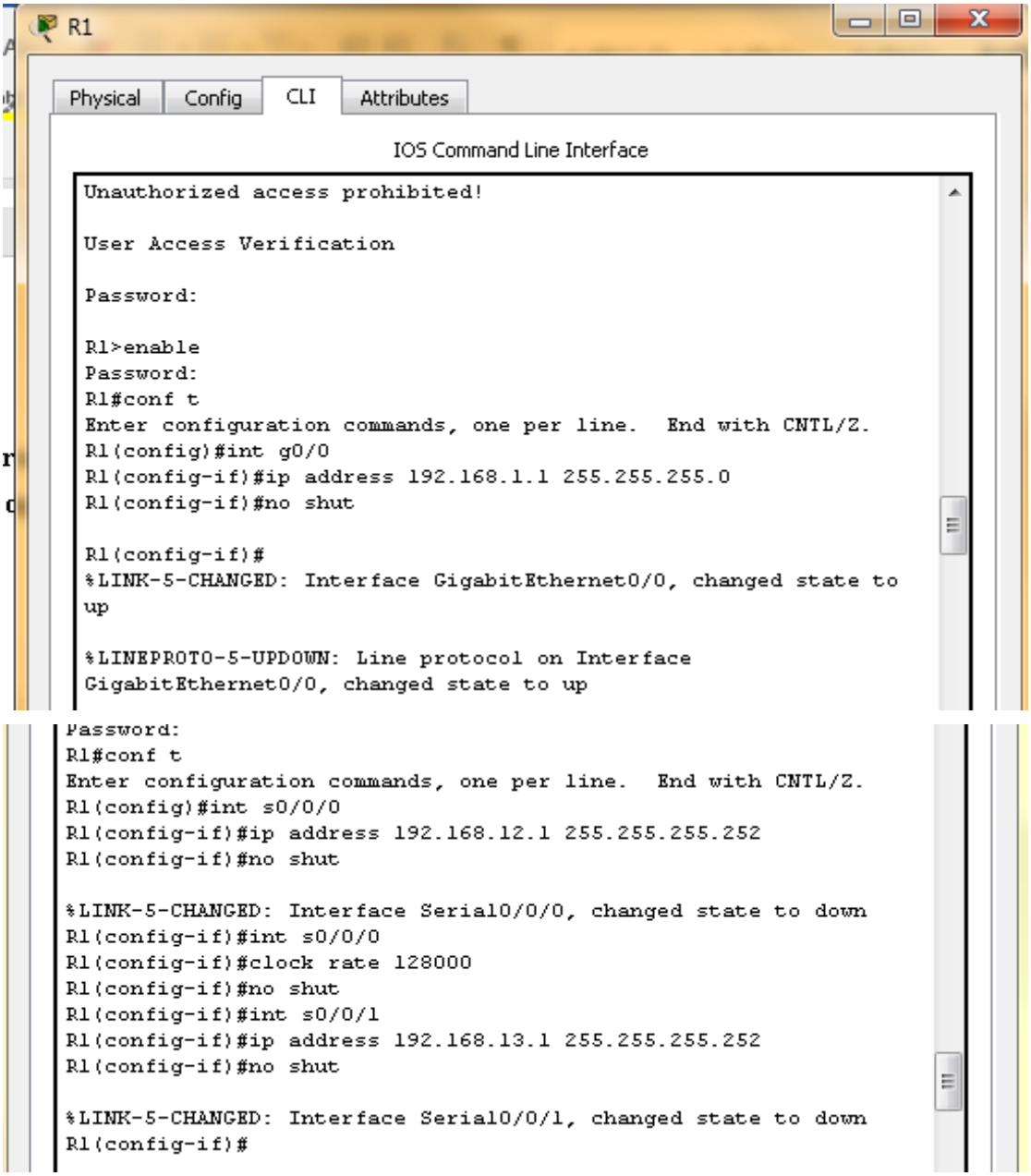


g. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces

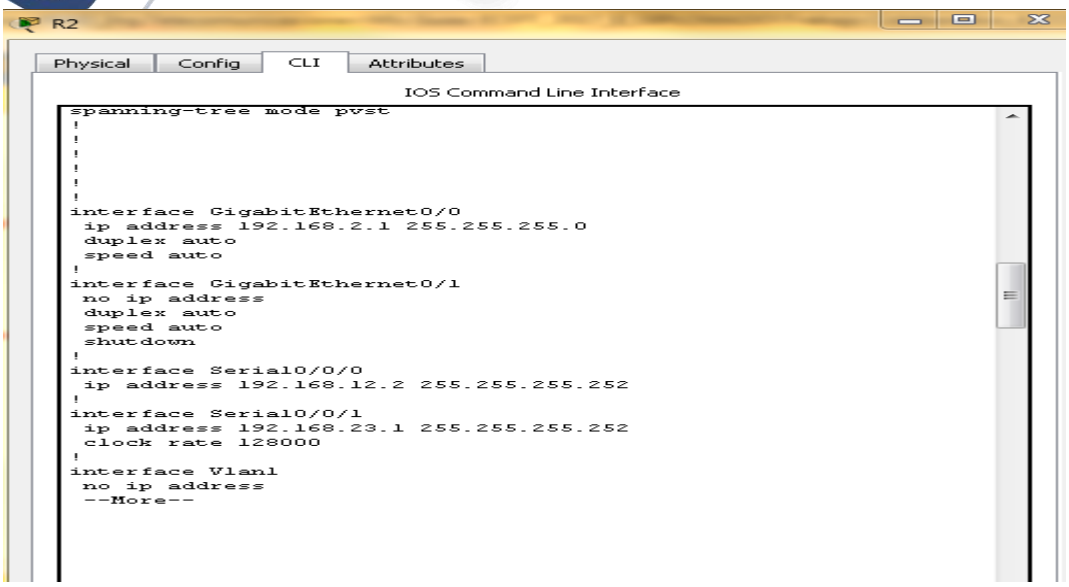
h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.

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

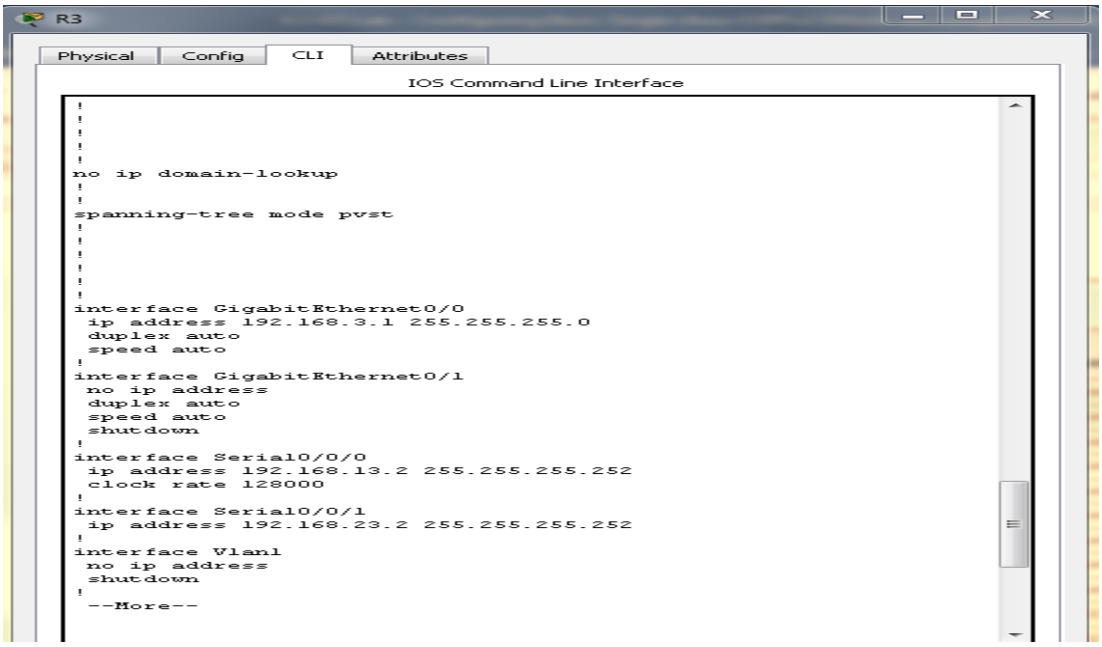
**ROUTER 1 G-H-I**



**ROUTER 2 G-H-I**

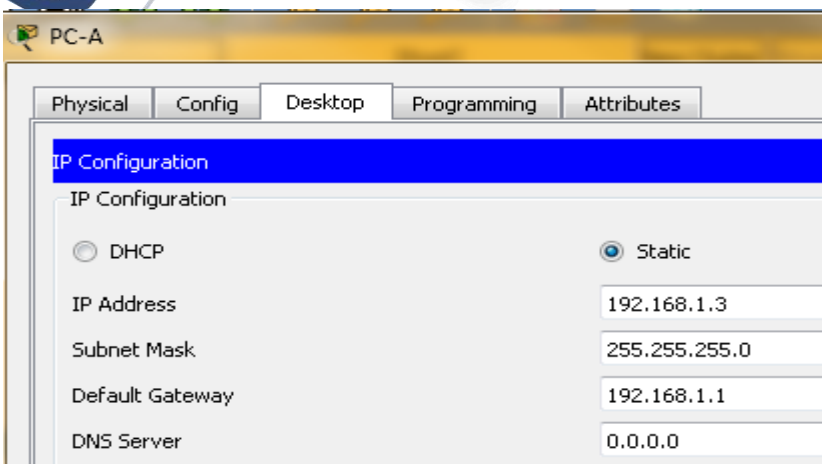



**ROUTER 3 G-H-I**

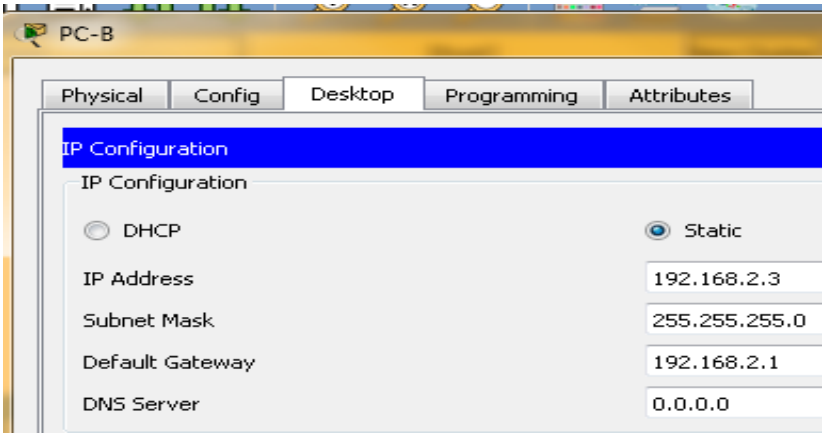


**Paso 4: Configurar los equipos host**

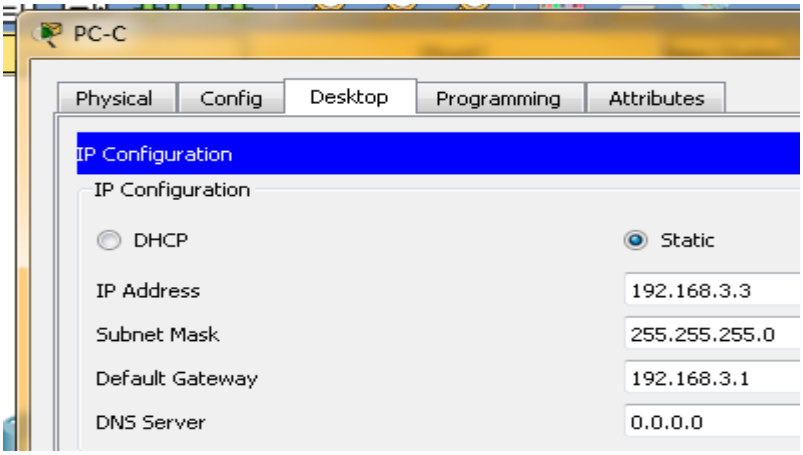
**PC-A**




**PC-B**

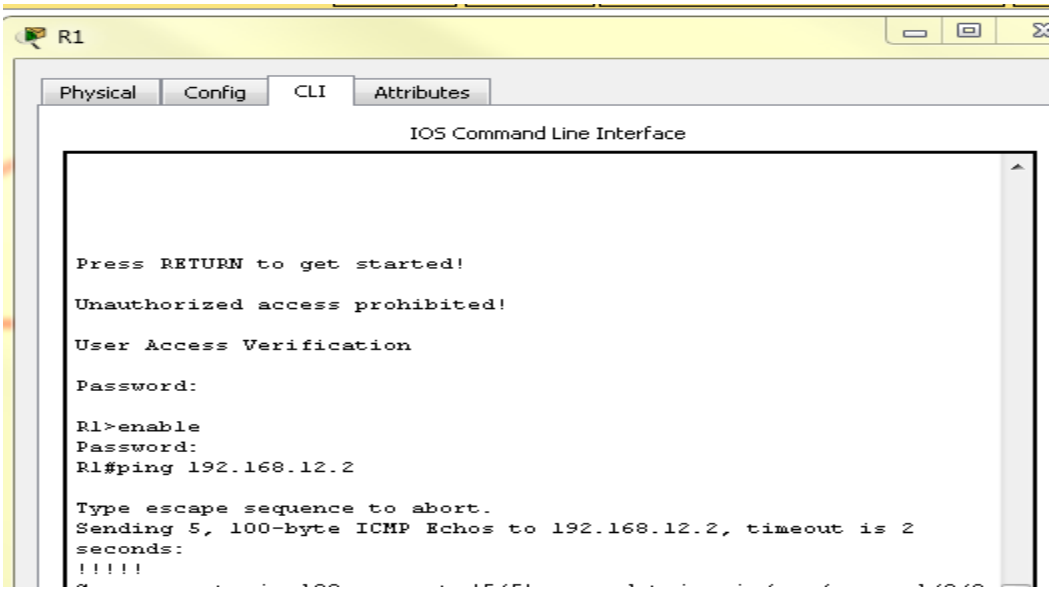


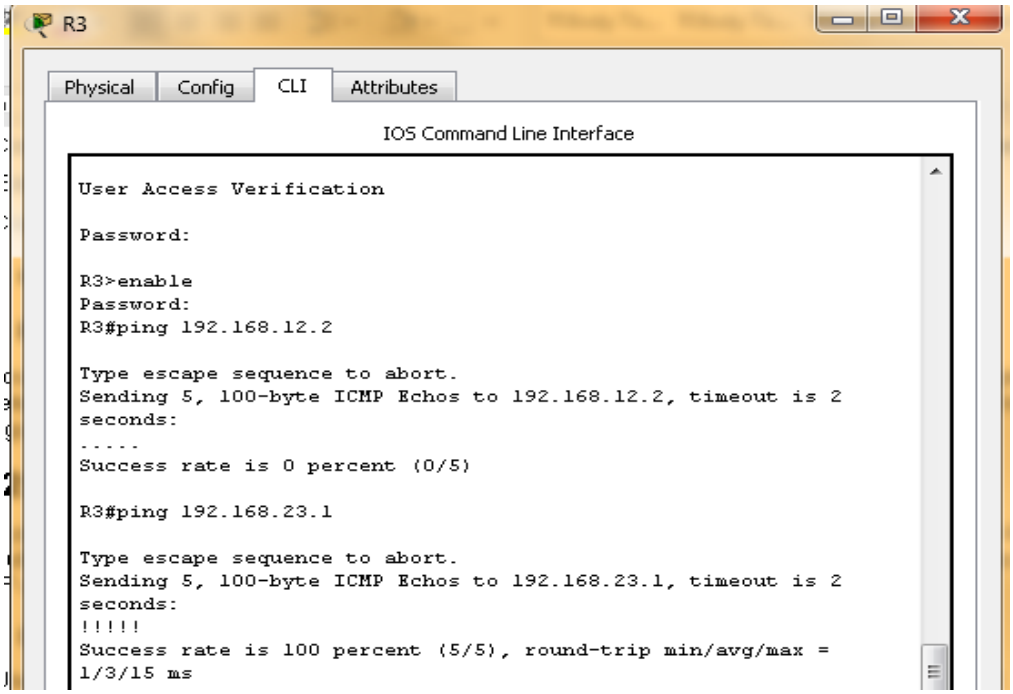

**PC-C**

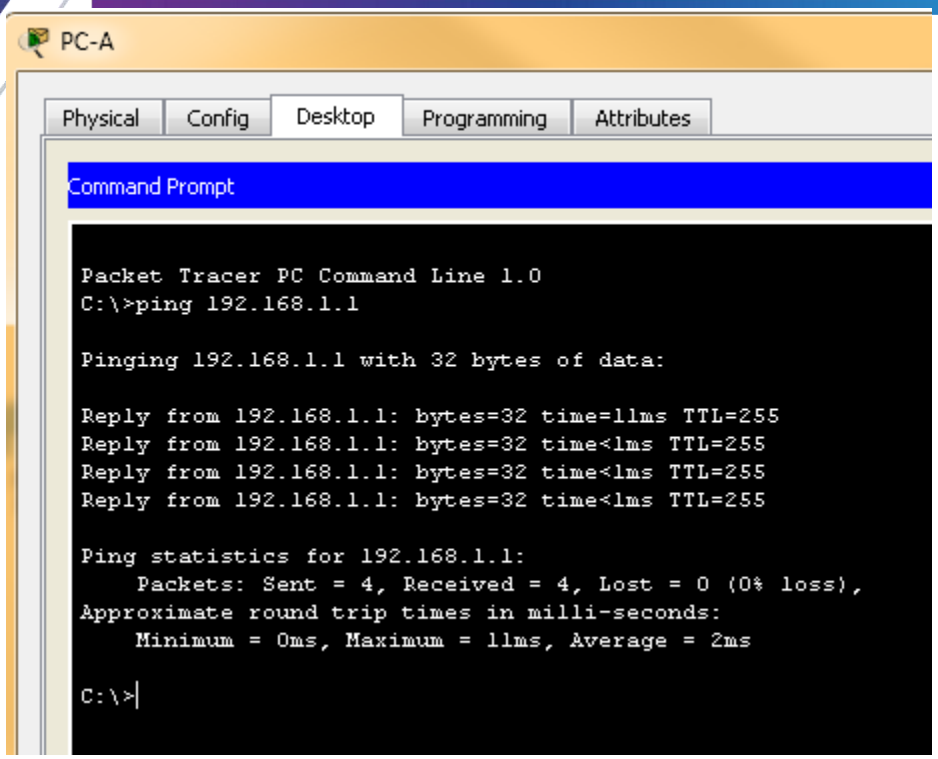


**Paso 5: Probar la conectividad.**

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.



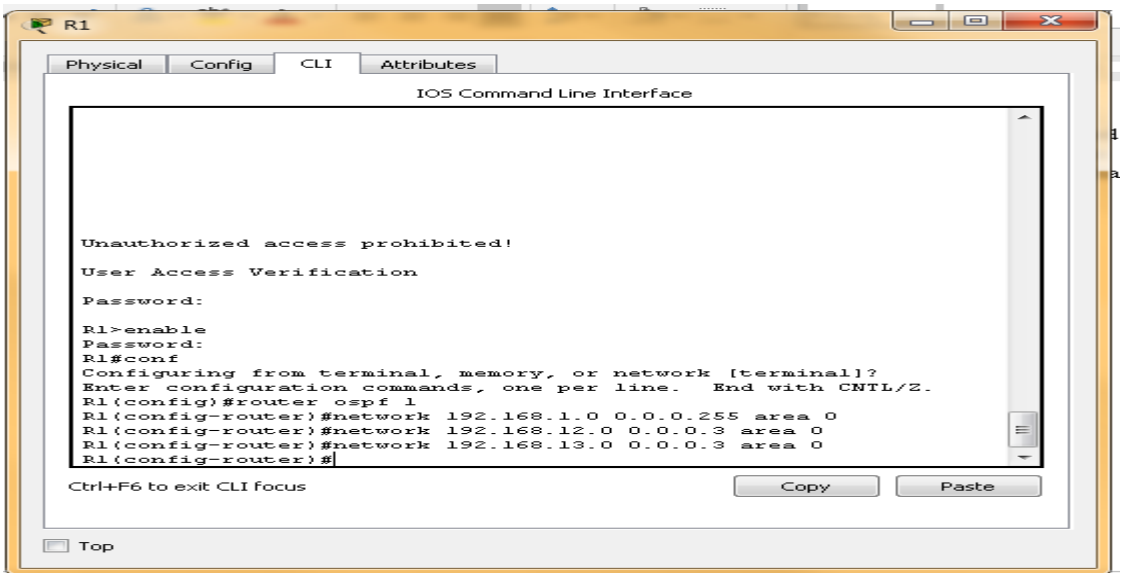






## Part 3: Configurar y verificar el enrutamiento OSPF

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

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



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

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

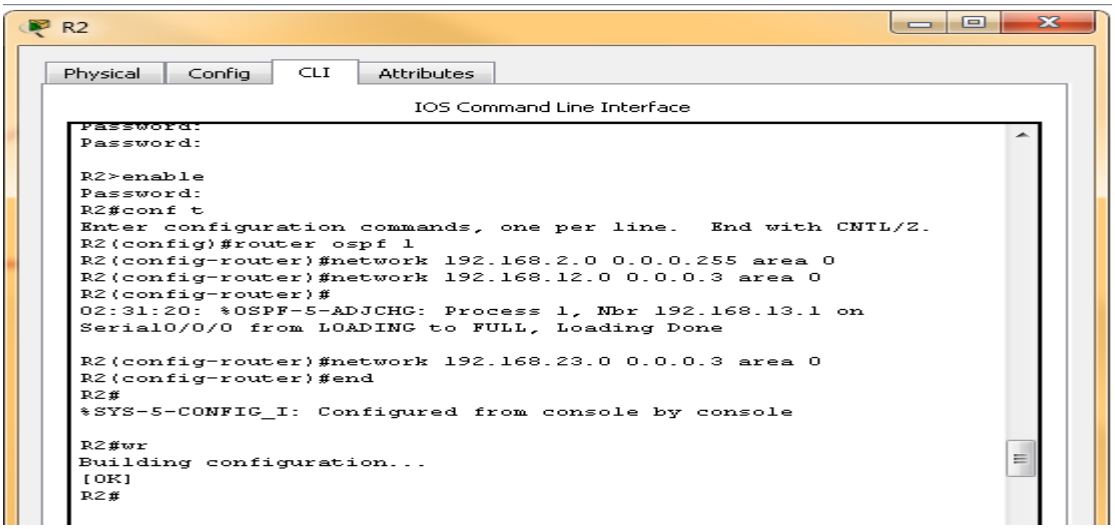
R1#

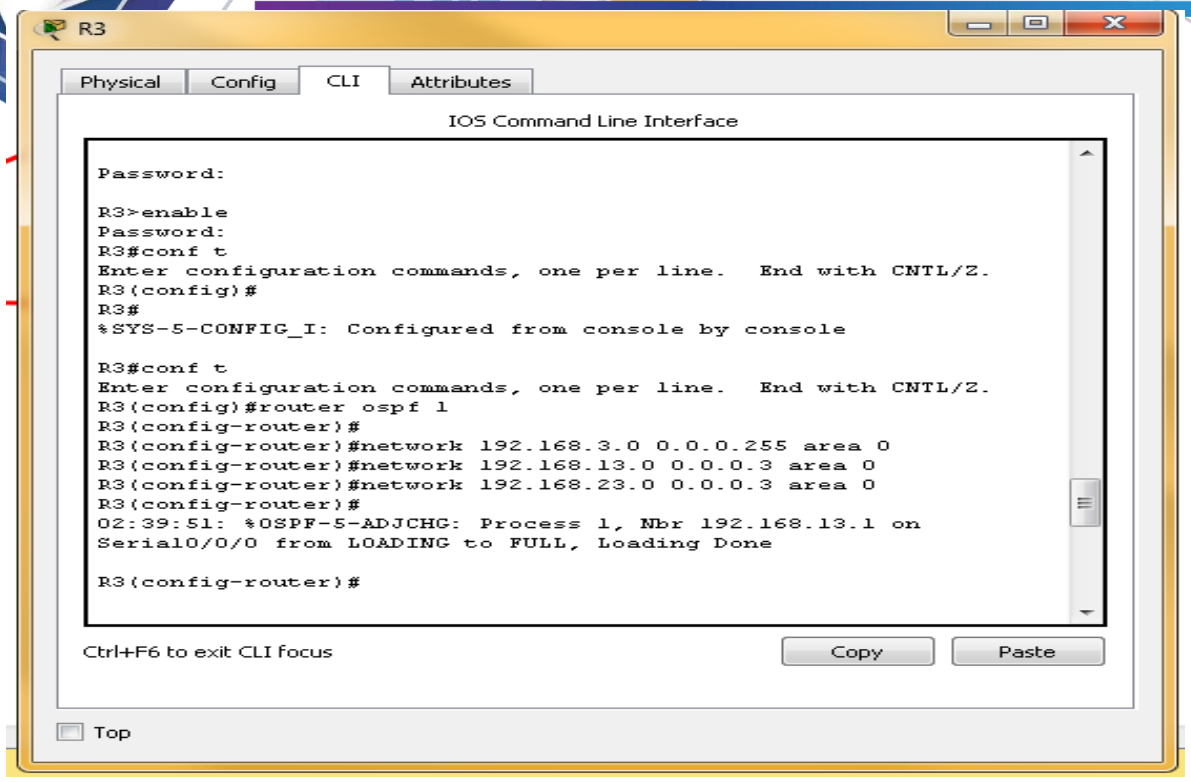
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done

R1#

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

R1#



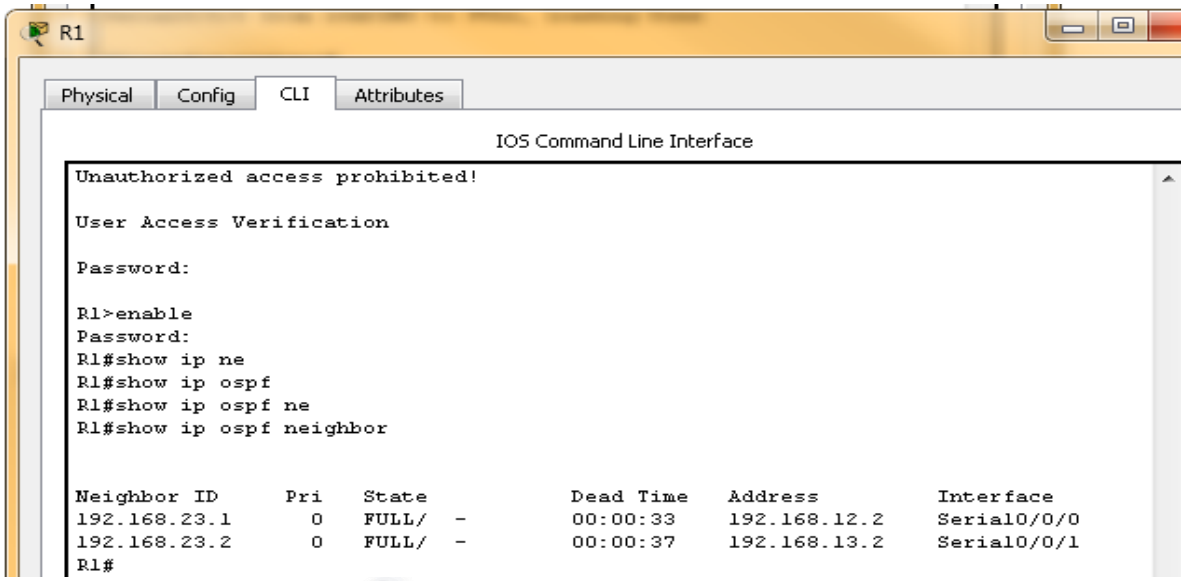



**Step 3: verificar los vecinos OSPF y la información de routing.**

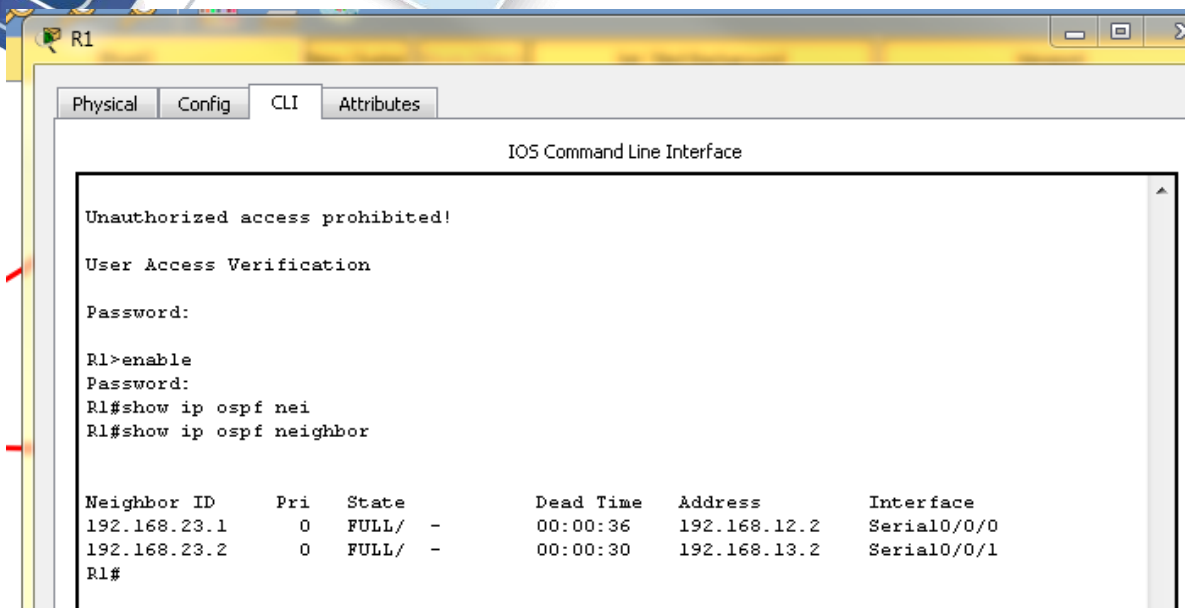
a. Emita el comando **show ip ospf neighbor** para verificar que cada router indique a los demás routers en la red como vecinos.

R1# **show ip ospf neighbor**

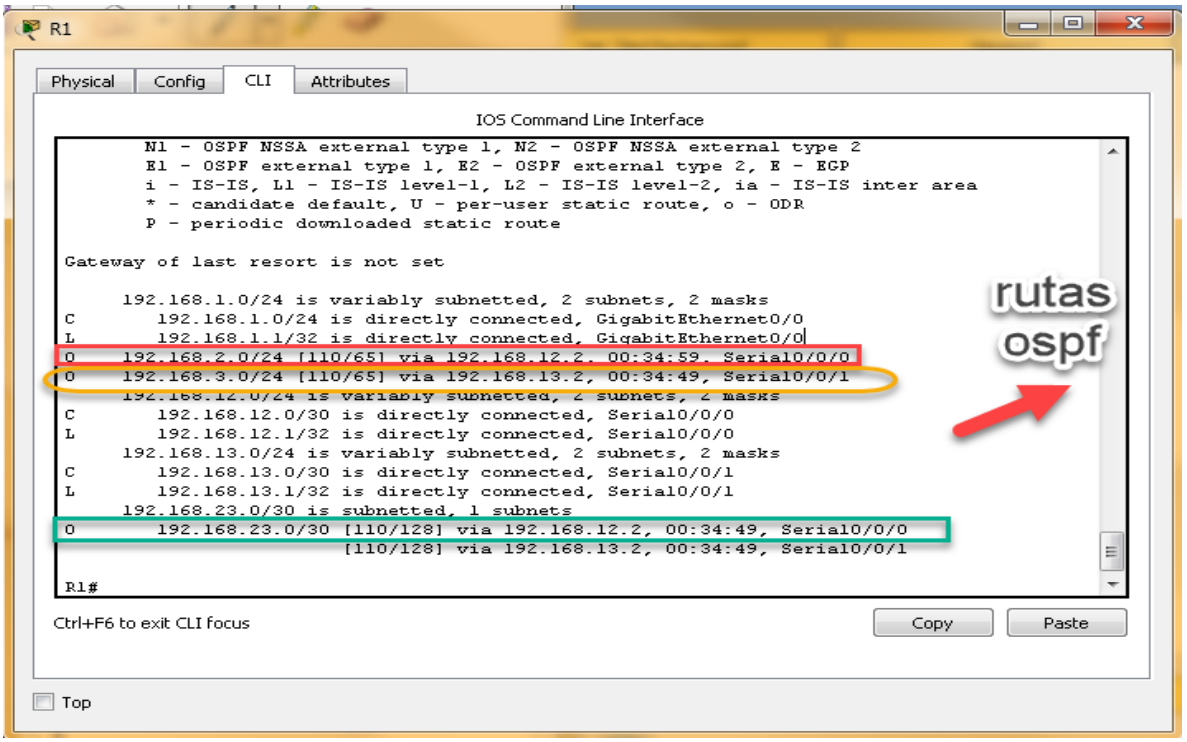
**Router 1**



**Router R1 OSPF NEIGHBOR**




**Show ip route R1**

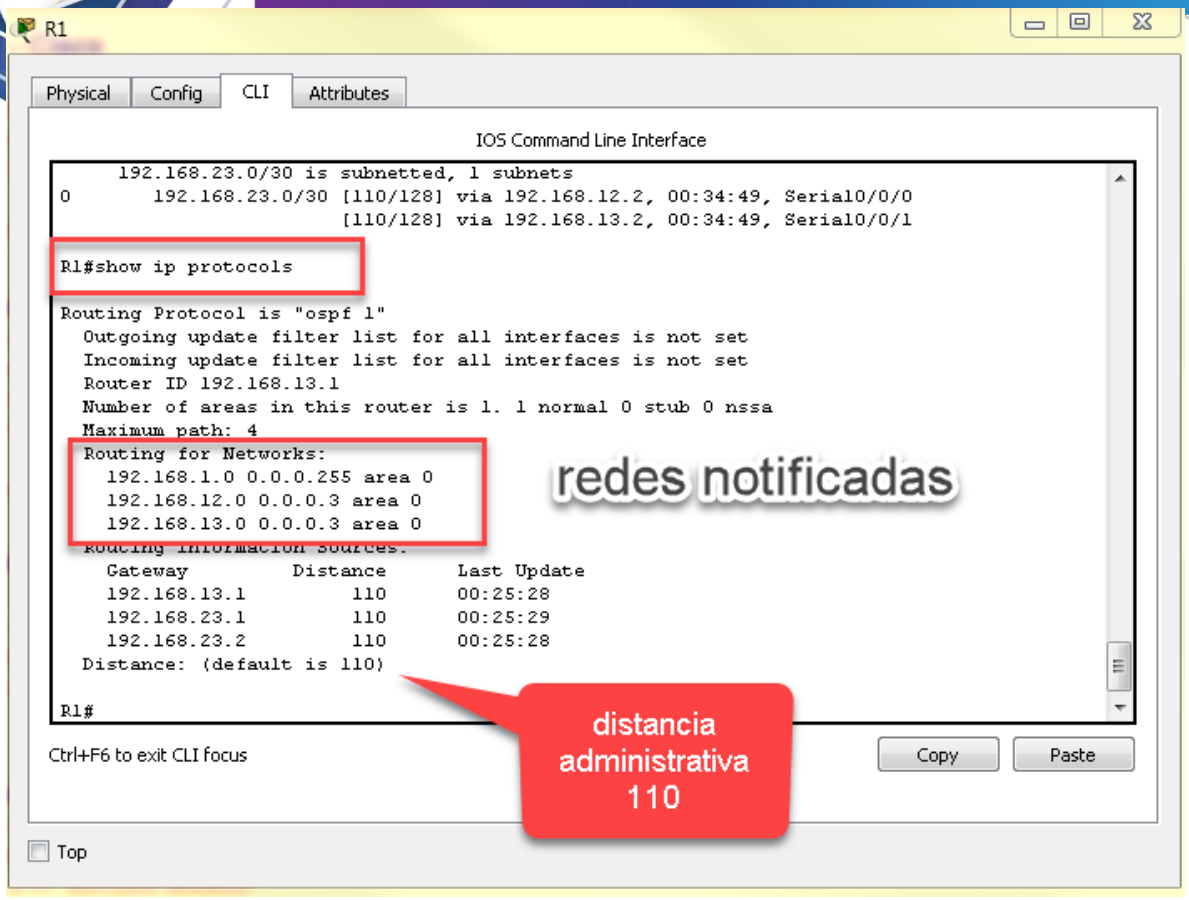


**¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?**

**Show ip route ospf**

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

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


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
192.168.23.0/30 is subnetted, 1 subnets
0 192.168.23.0/30 [110/128] via 192.168.12.2, 00:34:49, Serial0/0/0
[110/128] via 192.168.13.2, 00:34:49, Serial0/0/1
R1#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.168.13.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.1.0 0.0.0.255 area 0
192.168.12.0 0.0.0.3 area 0
192.168.13.0 0.0.0.3 area 0
Gateway Distance Last Update
192.168.13.1 110 00:25:28
192.168.23.1 110 00:25:29
192.168.23.2 110 00:25:28
Distance: (default is 110)
R1#
redes notificadas
distancia administrativa 110
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

```
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      00:25:28
    192.168.23.1         110      00:25:29
    192.168.23.2         110      00:25:28
  Distance: (default is 110)

R1#show ip ospf
 Routing Process "ospf 1" with ID 192.168.13.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
```

protocolos OSPF

id router

rutas notificadas

distancia administrativas

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

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

```
R1#show ip ospf
 Routing Process "ospf 1" with ID 192.168.13.1
 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 5 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x00b0a6
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

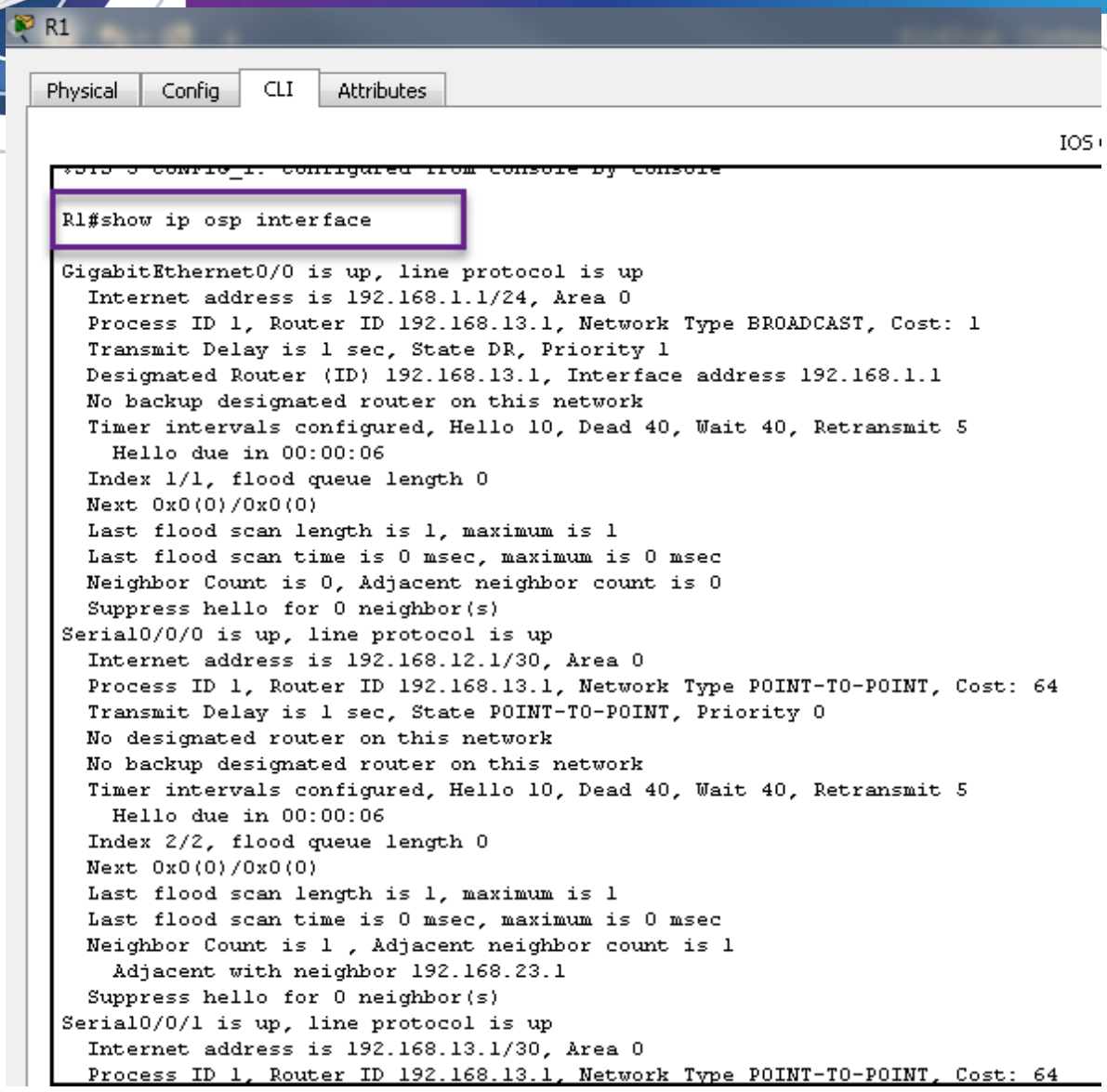
**Step 6: verificar la configuración de la interfaz OSPF.**

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

```
        Number of DoNotAge LSA 0
        Flood list length 0

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

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#show ip ospf interface brief
             ^
% Invalid input detected at '^' marker.

R1(config)#
```

el packet tracer no soporta este comando show ip ospf interface brief

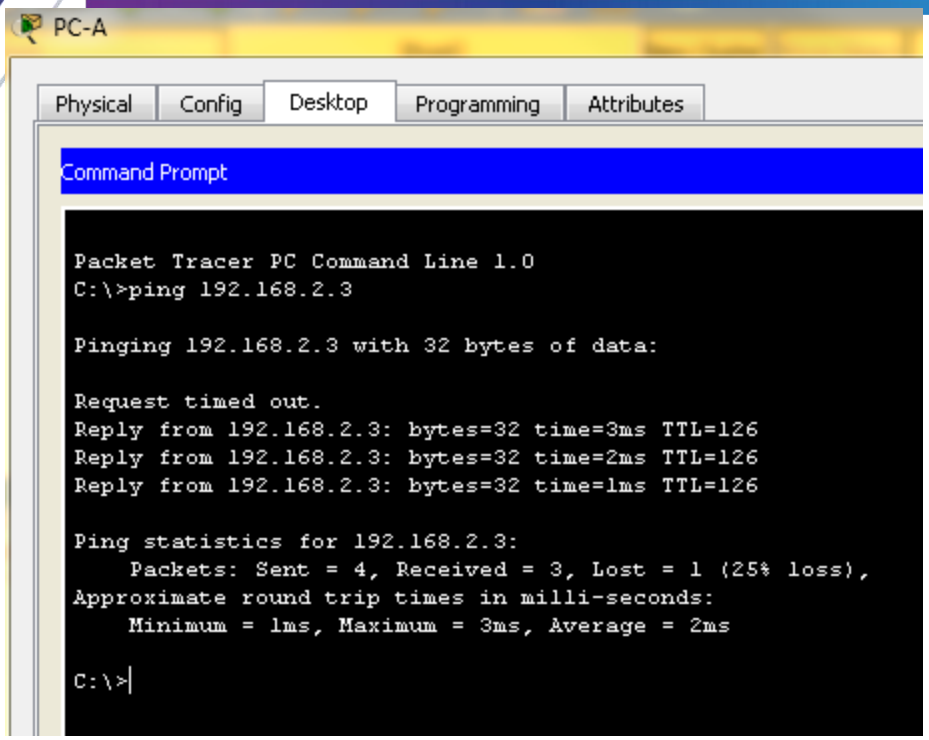
b. Para obtener una lista detallada de todas las interfaces con OSPF habilitado, emita el comando **show ip ospf interface**.

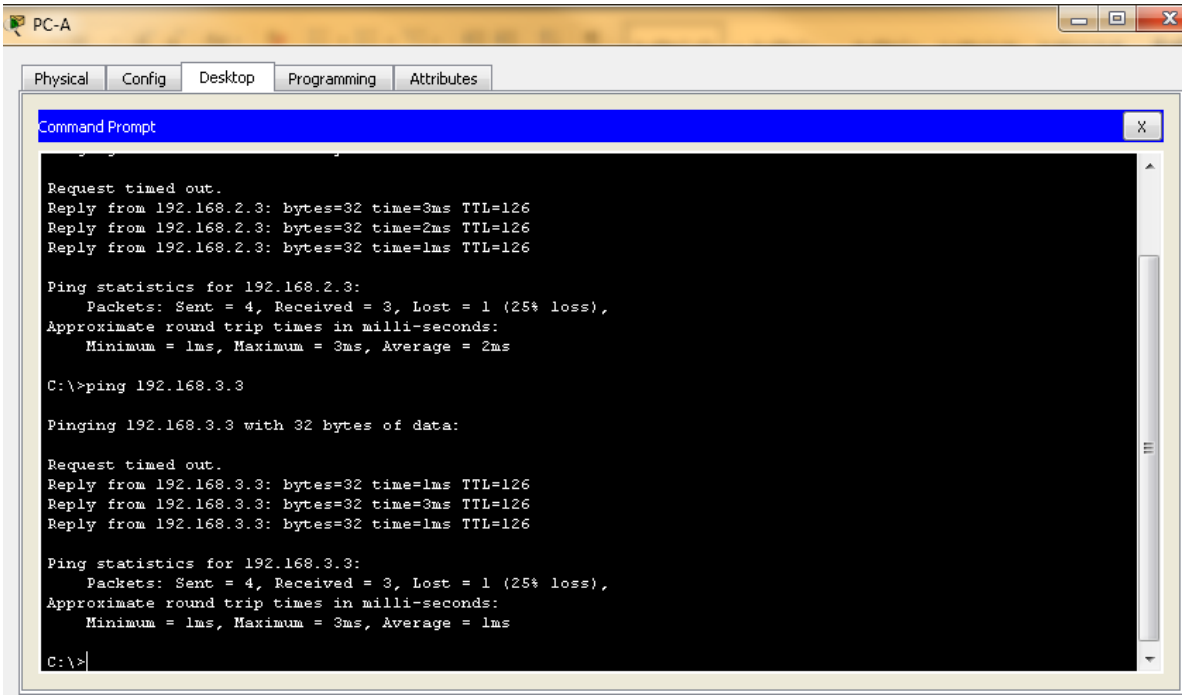



**Step 7: Verificar la conectividad de extremo a extremo.**

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

Ping's 192.168.2.3 y 192.168.3.3




## Part 4: cambiar las asignaciones de ID del router

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

1) Dirección IP configurada con el comando de OSPF **router-id**, si la hubiera

2) Dirección IP más alta de cualquiera de las direcciones de loopback del router, si la hubiera

3) Dirección IP activa más alta de cualquiera de las interfaces físicas del router

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

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

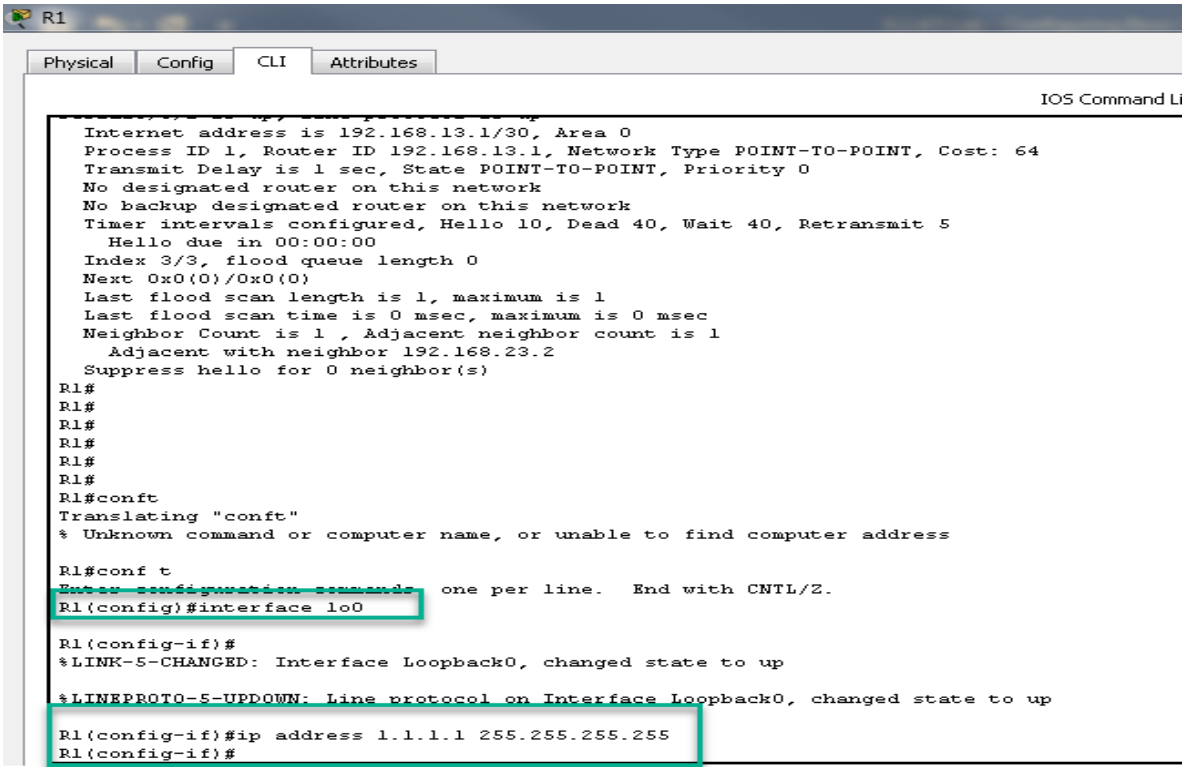
**Step 1: Cambie las ID de router con direcciones de loopback.**

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

R1(config)# **interface lo0**

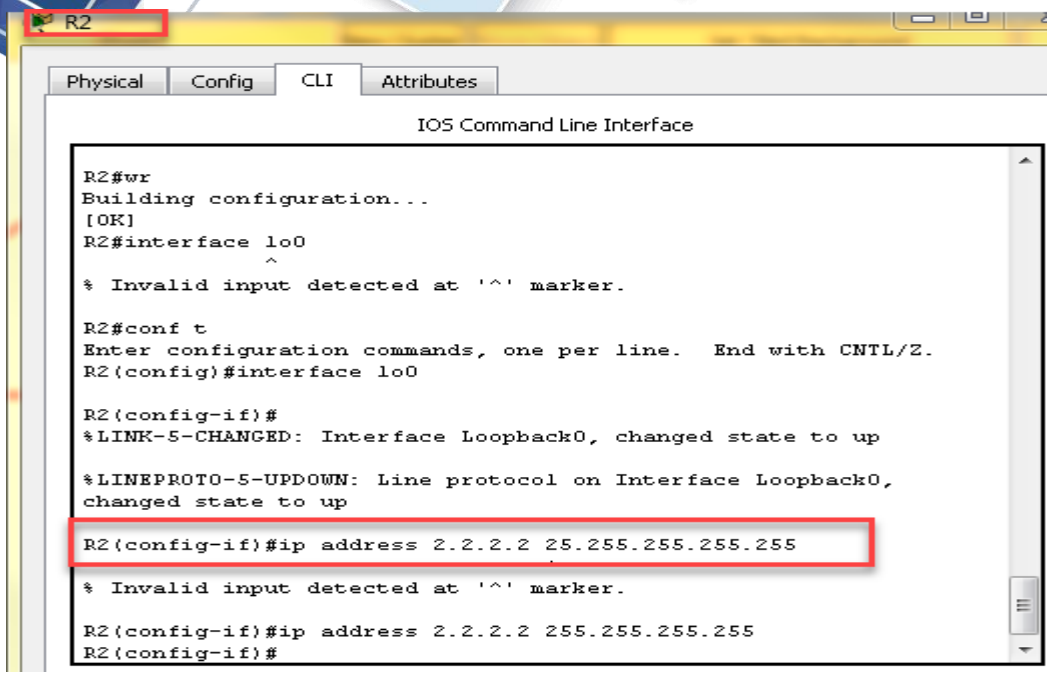
R1(config-if)# **ip address 1.1.1.1 255.255.255.255**

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

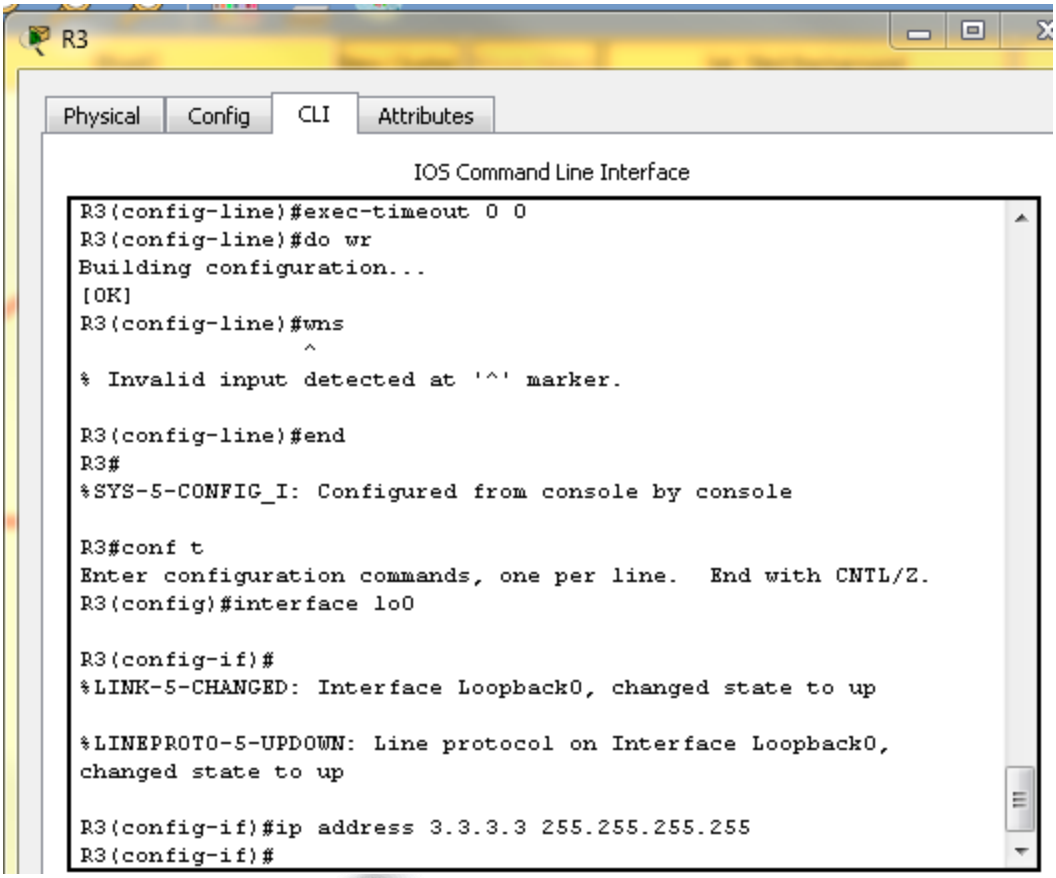



b. Asigne direcciones IP al loopback 0 en el R2 y el R3. Utilice la dirección IP 2.2.2.2/32 para el R2 y 3.3.3.3/32 para el R3.

Lookpack en R2

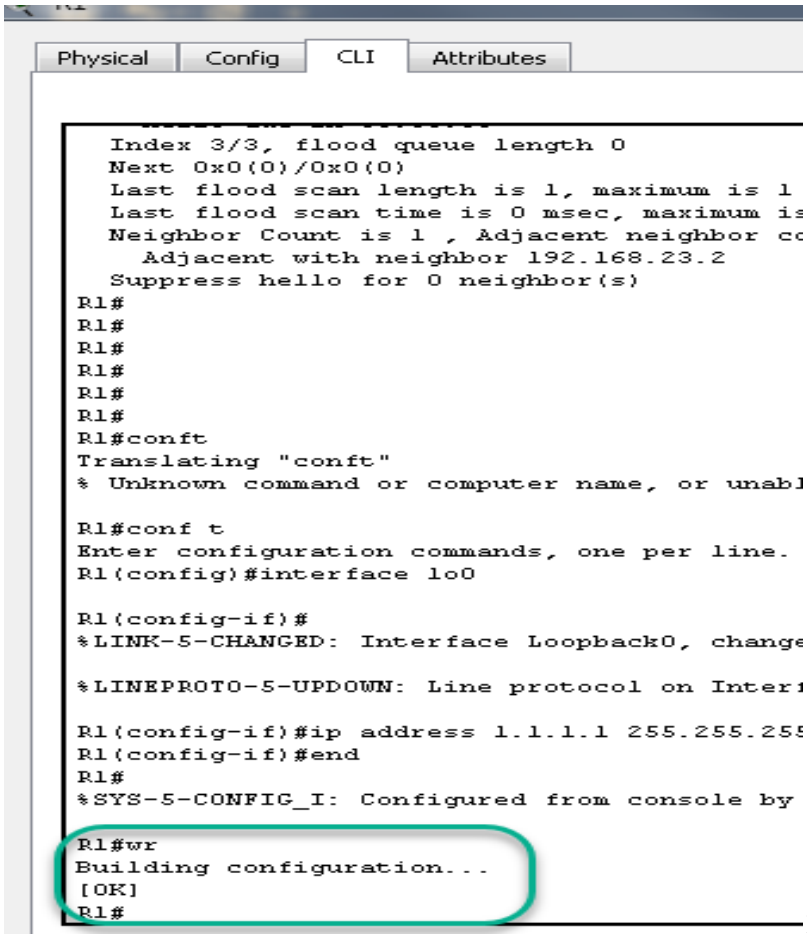



Loopback En Router 3

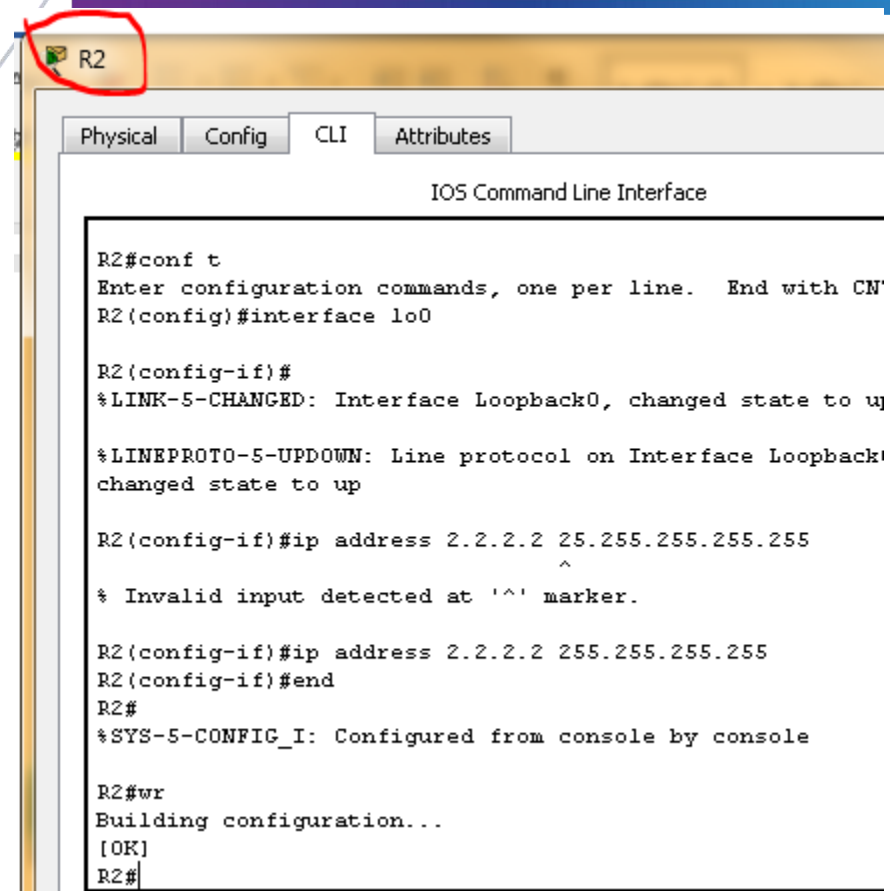


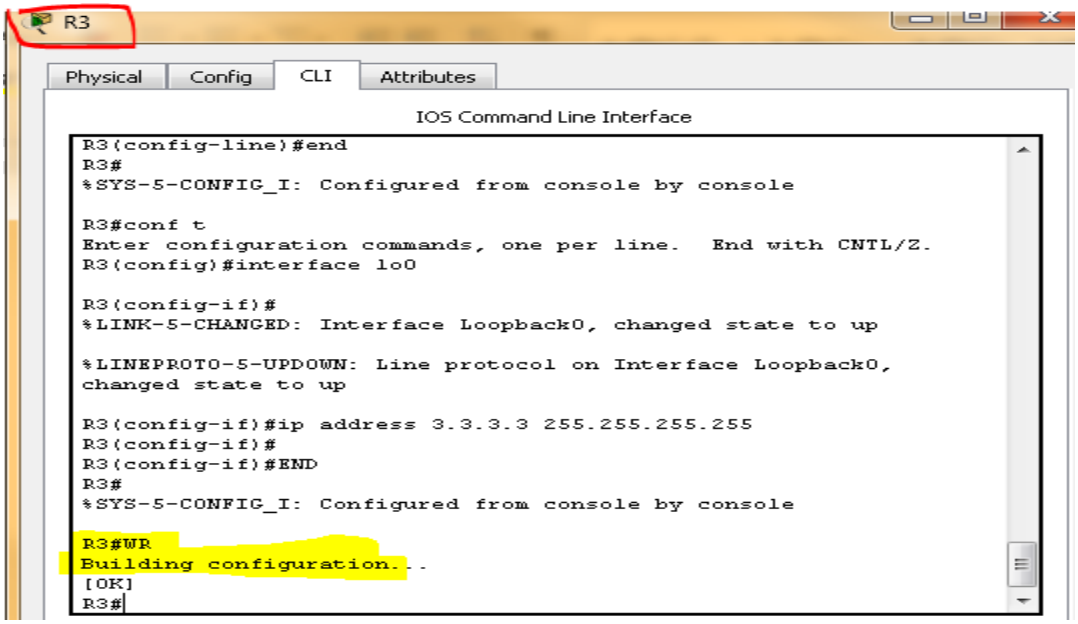
c. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.

Guardar Configuracion Router



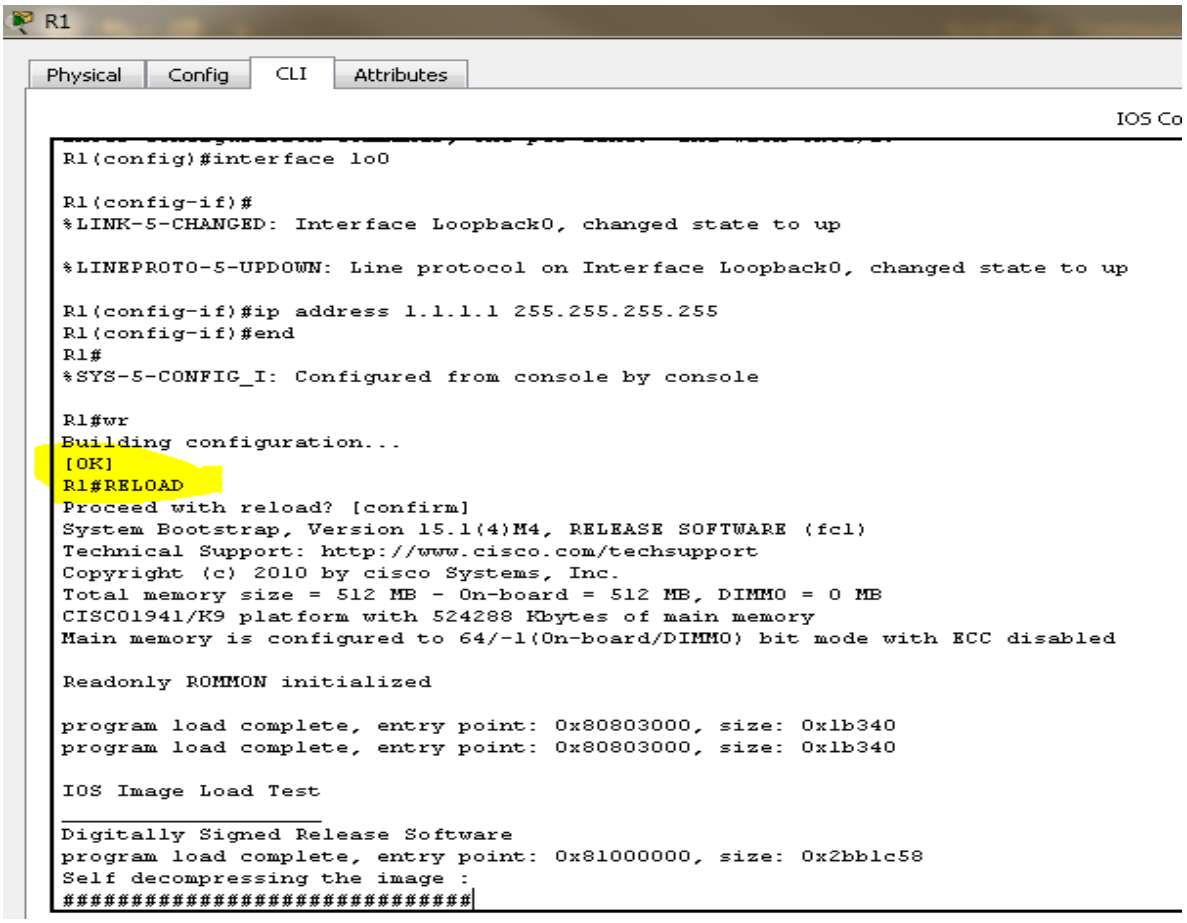

1-2-3

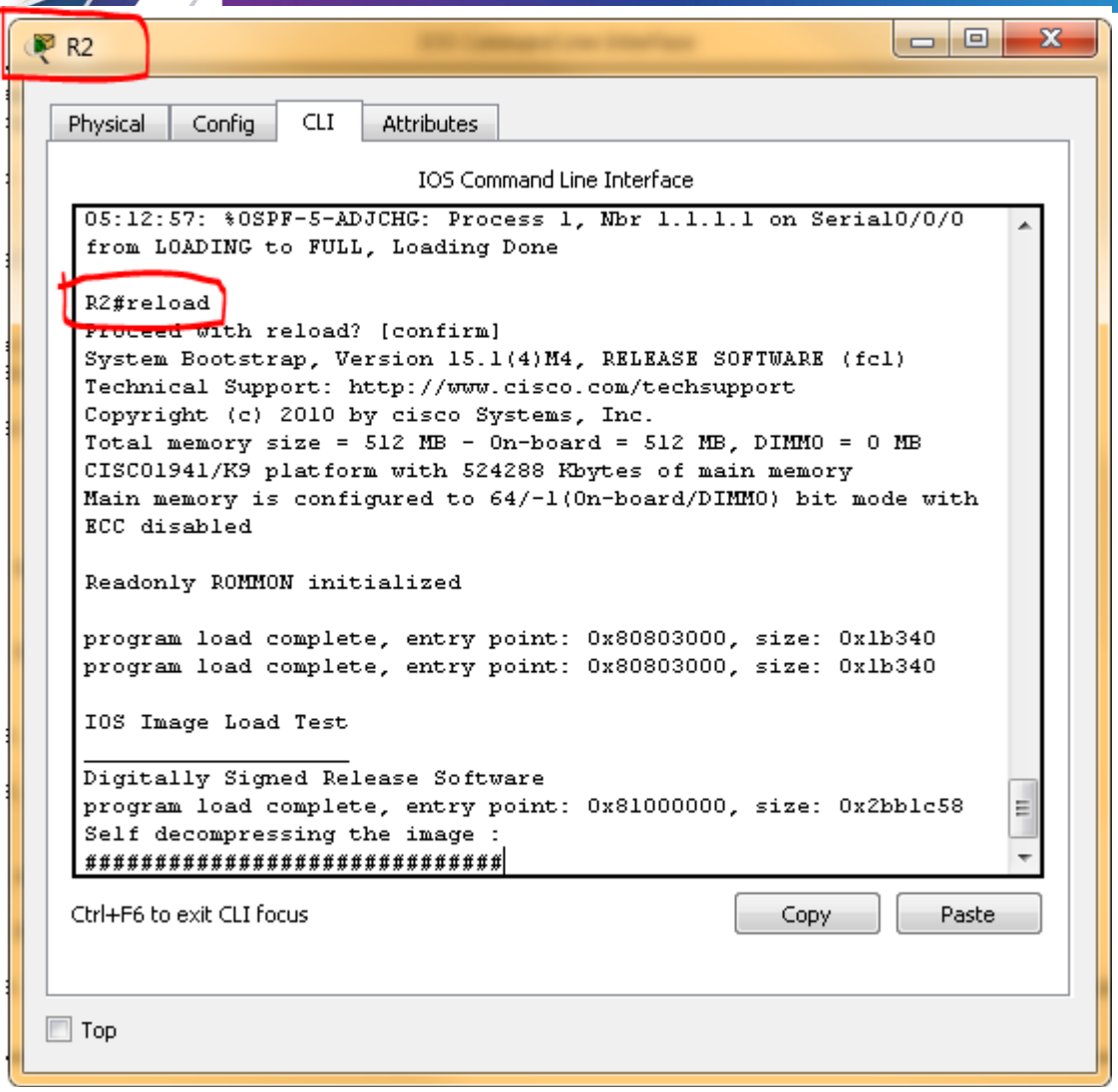

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2#conf t
Enter configuration commands, one per line. End with CN
R2(config)#interface lo0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to u
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback
changed state to up
R2(config-if)#ip address 2.2.2.2 25.255.255.255.255
^
% Invalid input detected at '^' marker.
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#wr
Building configuration...
[OK]
R2#

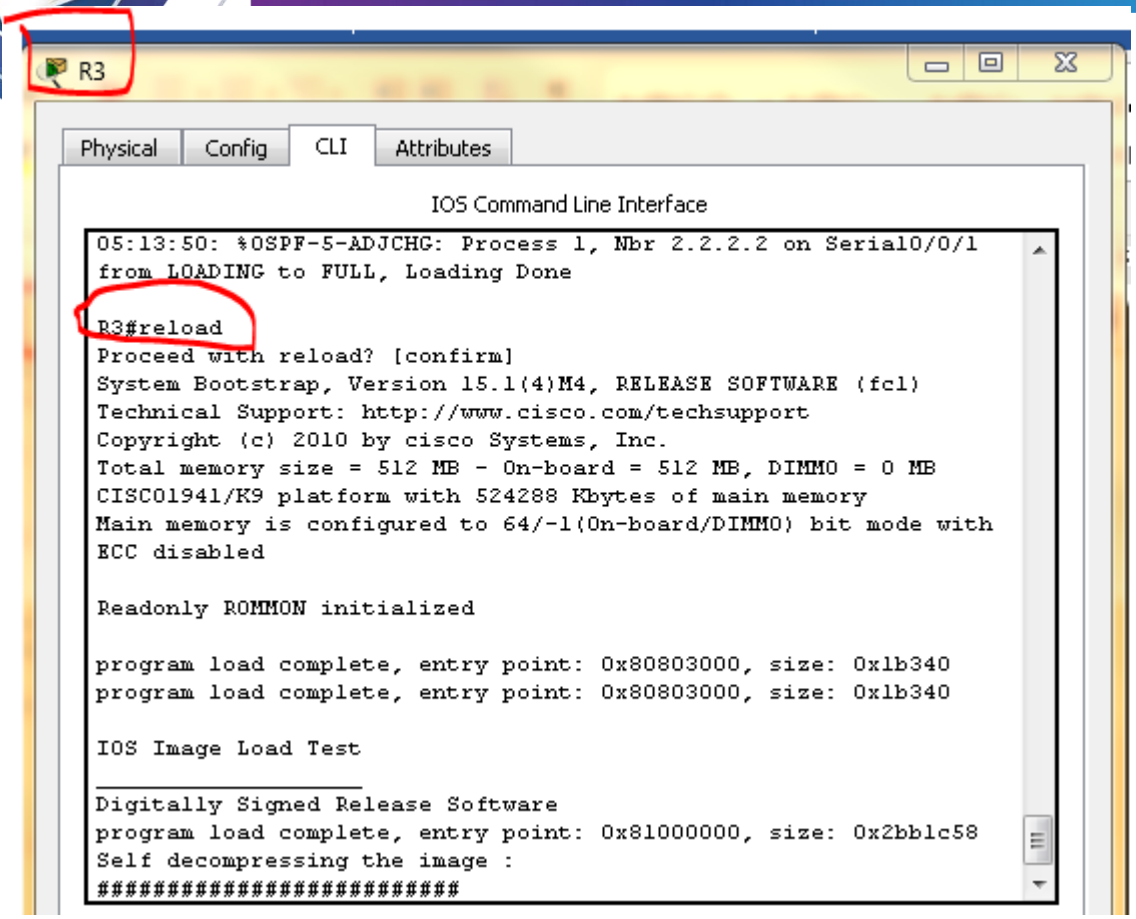

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3(config-line)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface lo0
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R3(config-if)#ip address 3.3.3.3 255.255.255.255
R3(config-if)#
R3(config-if)#END
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#WR
Building configuration...
[OK]
R3#

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.

Reload en los router R1-R2-R3




R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
05:12:57: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R2#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
IOS Image Load Test
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

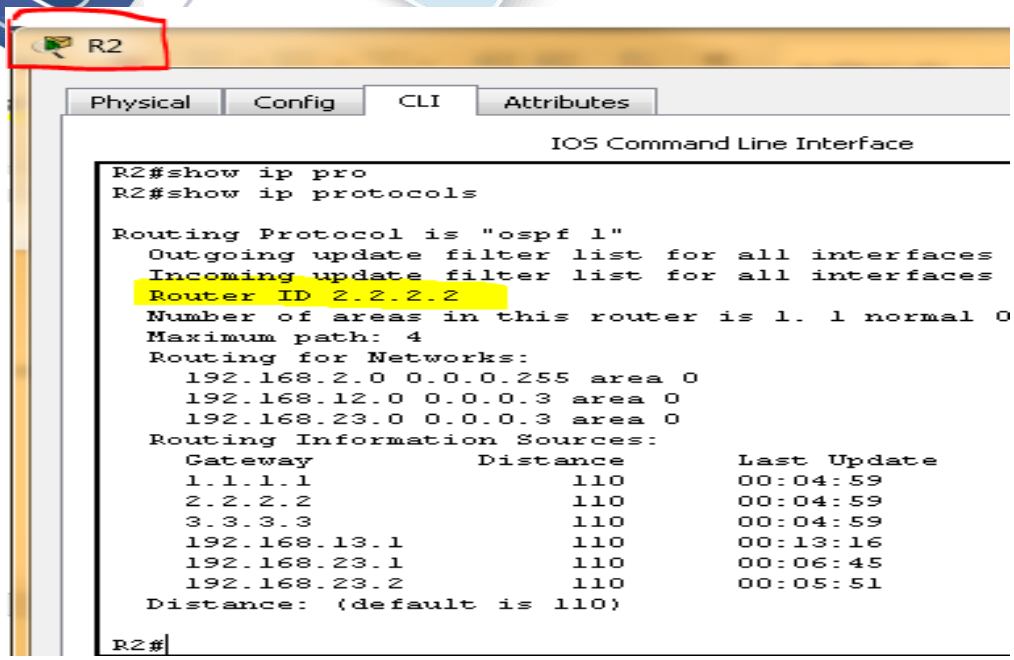



e. Una vez que se haya completado el proceso de recarga del router, emita el comando **show ip protocols** para ver la nueva ID del router.

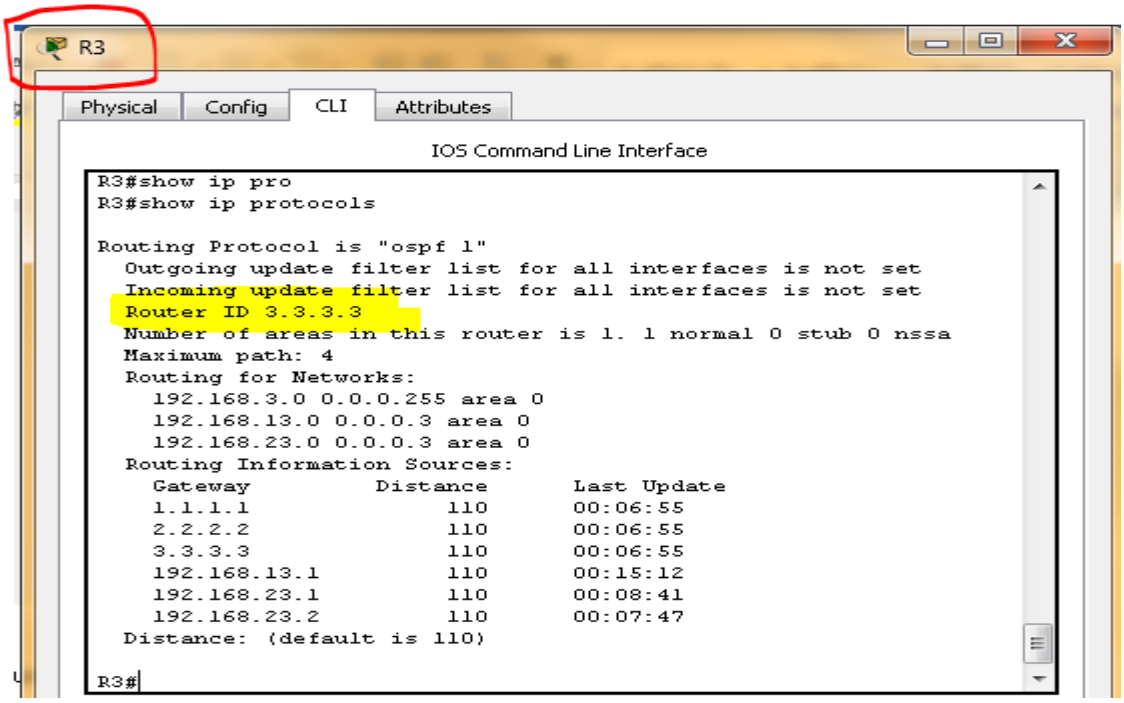
Nuevo id del router 1

```
R1#show ip pro
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      00:02:46
    2.2.2.2              110      00:02:46
    3.3.3.3              110      00:02:46
    192.168.13.1         110      00:11:03
    192.168.23.1         110      00:04:32
    192.168.23.2         110      00:03:38
  Distance: (default is 110)
```

Nuevo id del router 2




Nuevo id del router 3




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**

```
Password:

R1>enable
Password:
R1#show ip pro
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      00:02:46
    2.2.2.2              110      00:02:46
    3.3.3.3              110      00:02:46
    192.168.13.1         110      00:11:03
    192.168.23.1         110      00:04:32
    192.168.23.2         110      00:03:38
  Distance: (default is 110)

R1#show ip ospf ne
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:36    192.168.12.2    Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:38    192.168.13.2    Serial0/0/1
R1#
```

**Step 2: cambiar la ID del router R1 con el comando router-id.**

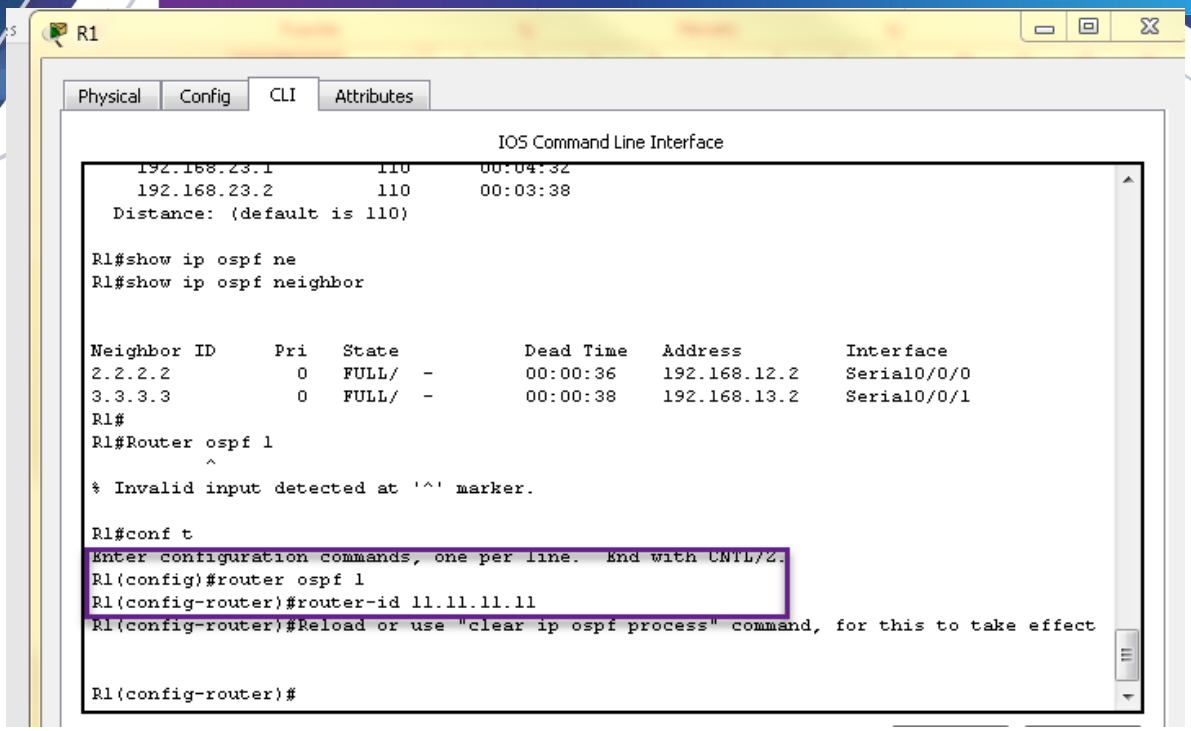
a. Emita el comando **router-id 11.11.11.11** en el R1 para reasignar la ID del router. Observe el mensaje informativo que aparece al emitir el comando **router-id**.

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

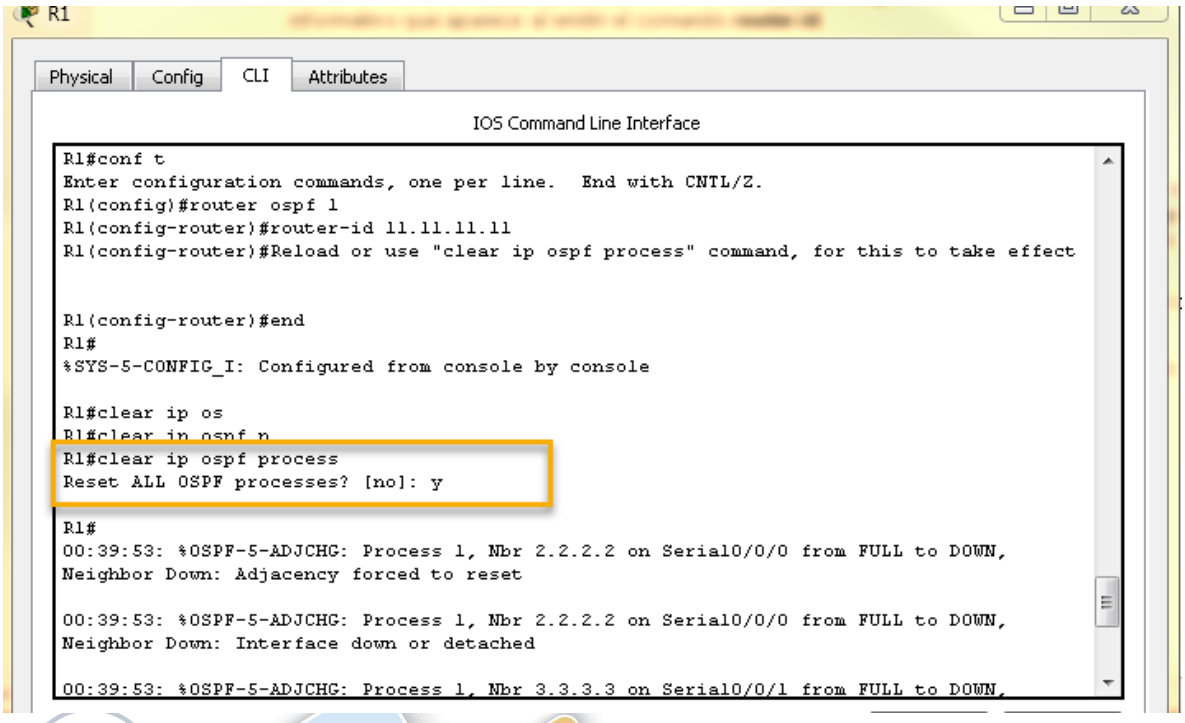
R1(config-router)# **router-id 11.11.11.11**

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

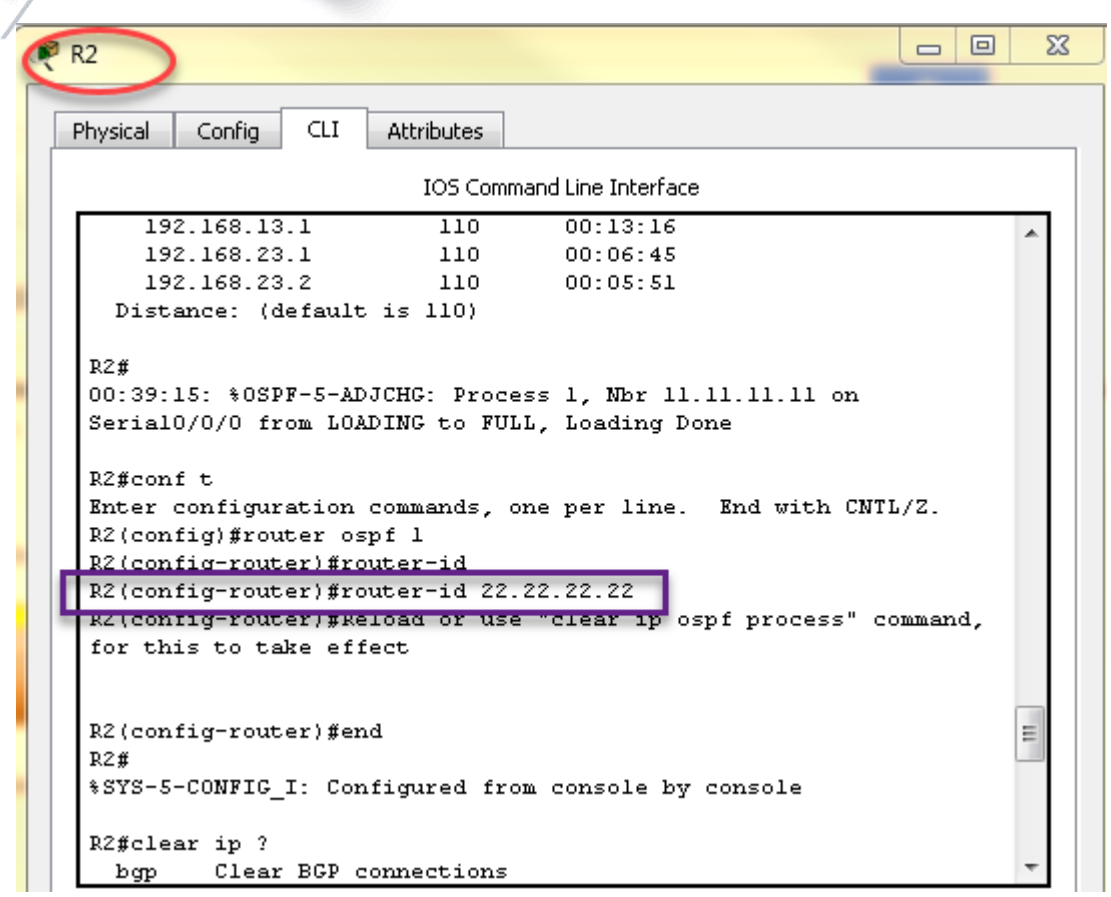
R1(config)# **end**

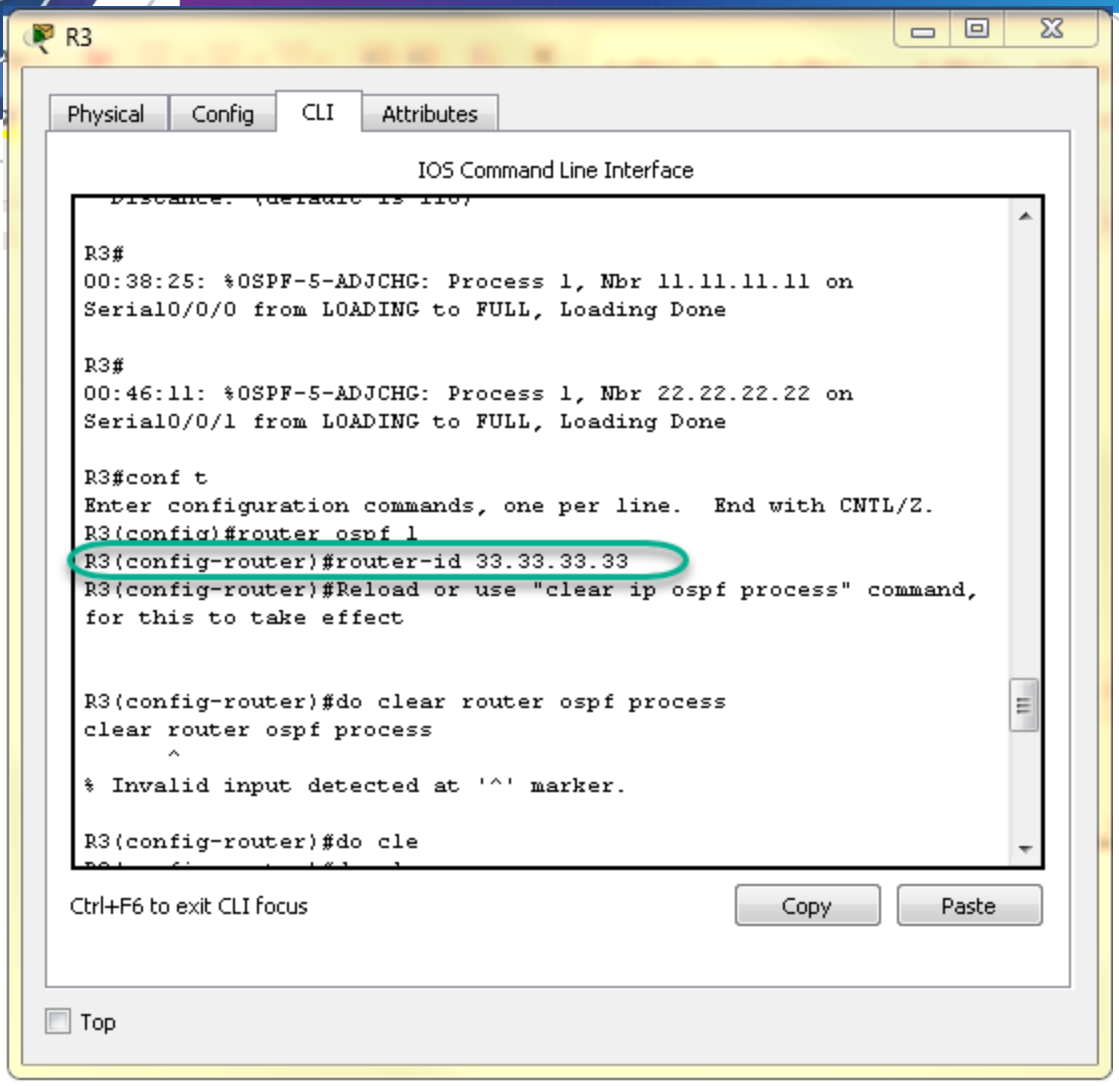



b. Recibirá un mensaje informativo en el que se le indique que debe volver a cargar el router o usar el comando **clear ip ospf process** para que se aplique el cambio. Emita el comando **clear ip ospf process** en los tres routers. Escriba **yes** (sí) como respuesta al mensaje de verificación de restablecimiento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



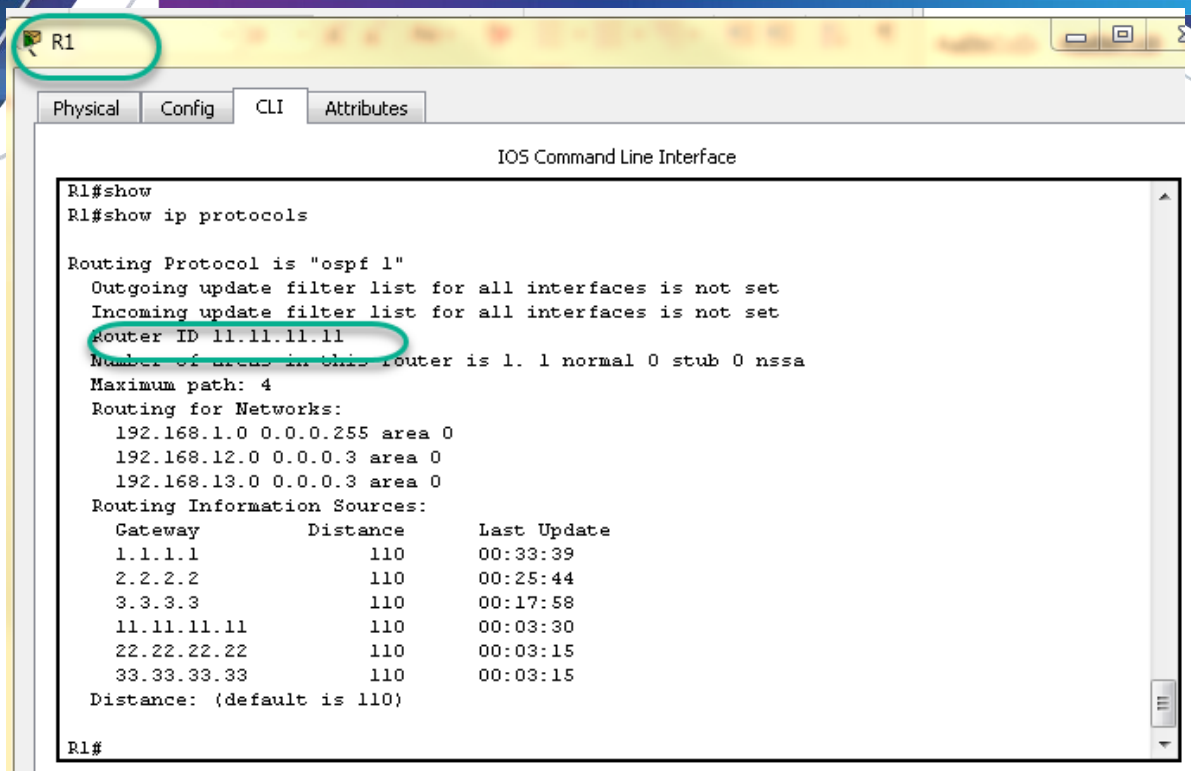
c. Establezca la ID del router R2 **22.22.22.22** y la ID del router R3 **33.33.33.33**. Luego, use el comando **clear ip ospf process** para restablecer el proceso de routing de OSPF.





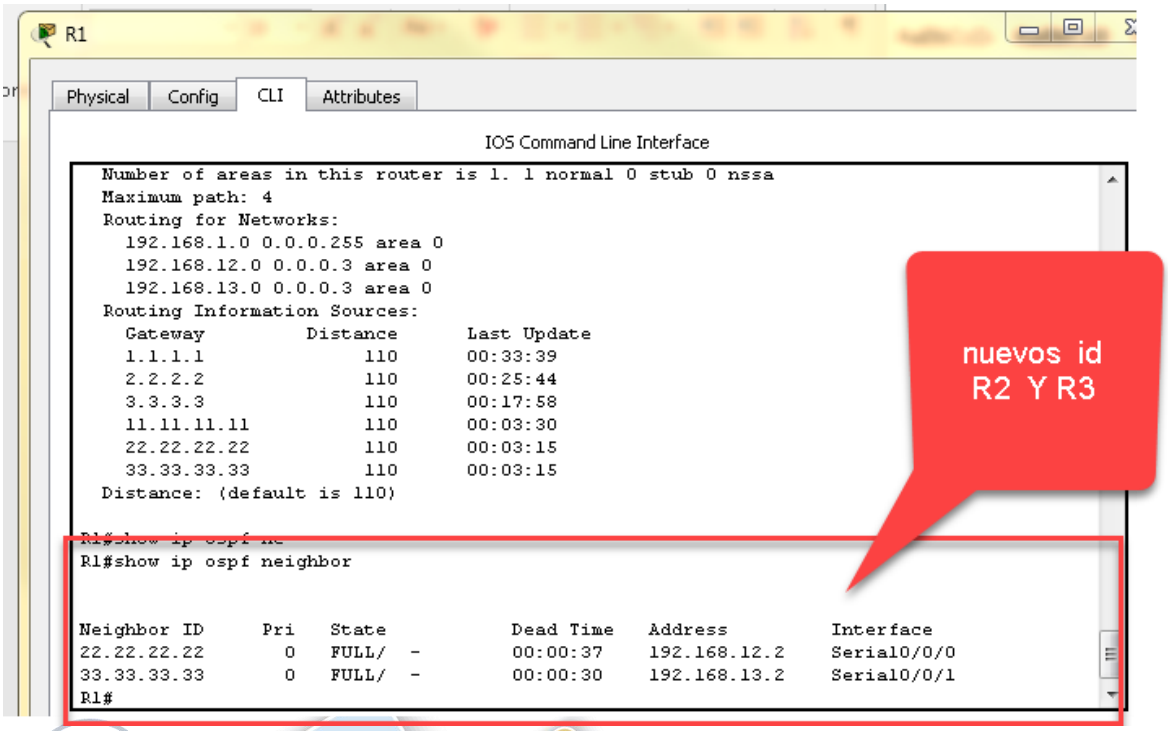

d. Emita el comando **show ip protocols** para verificar que la ID del router R1 haya cambiado.

R1# **show ip protocols**




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**

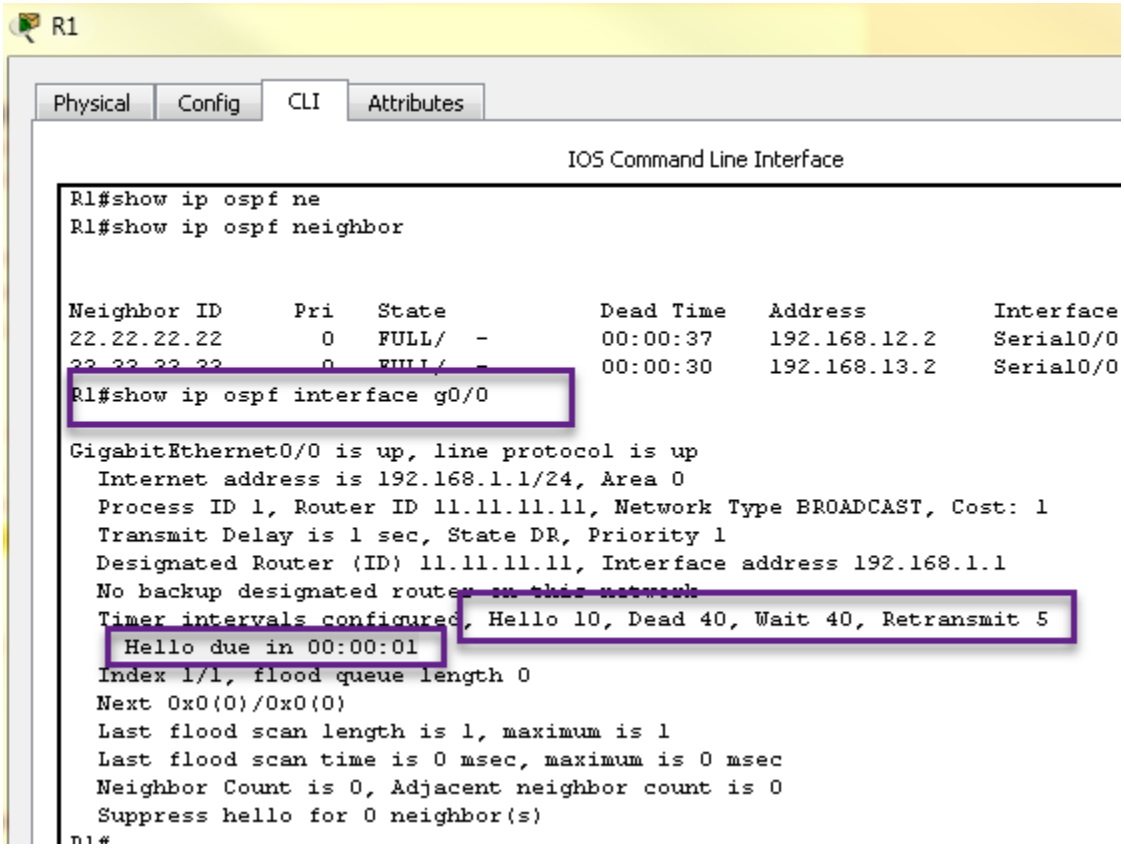


**Part 5: configurar las interfaces pasivas de OSPF**

El comando **passive-interface** evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. En la parte 4, utilizará el comando **passive-interface** para configurar una única interfaz como pasiva. También configurará OSPF para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

**Step 1: configurar una interfaz pasiva.**

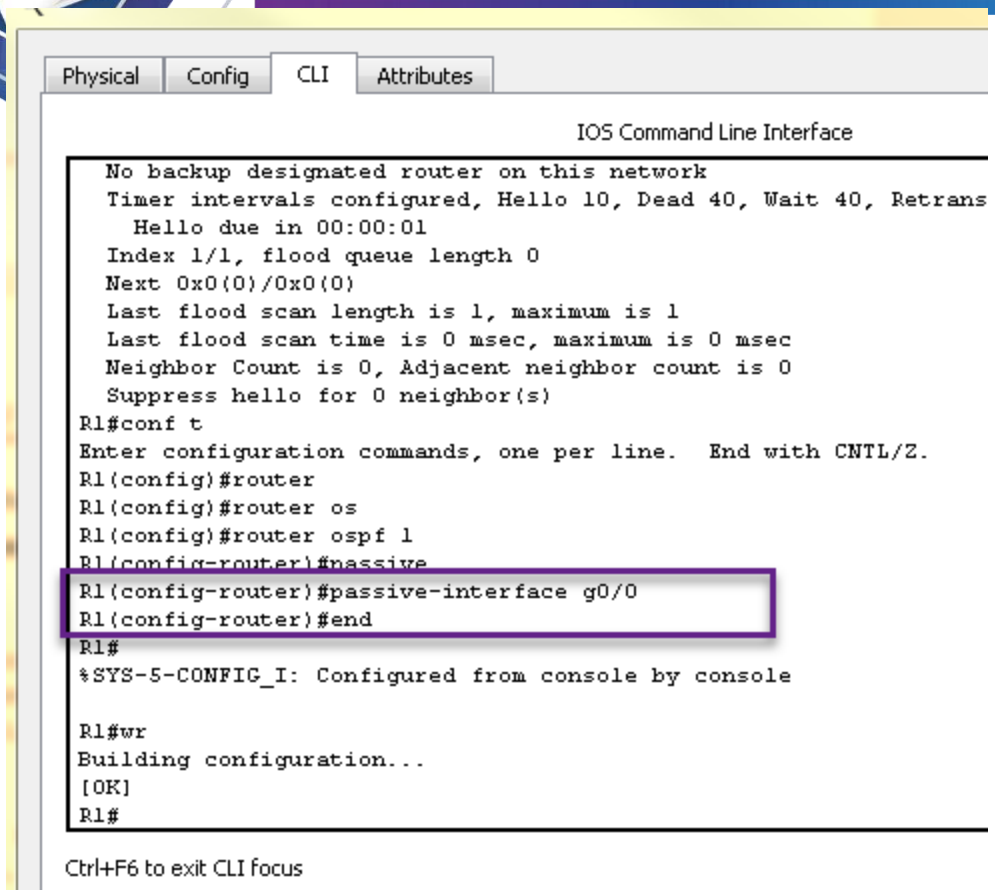
a. Emita el comando **show ip ospf interface g0/0** en el R1. Observe el temporizador que indica cuándo se espera el siguiente paquete de saludo. Los paquetes de saludo se envían cada 10 segundos y se utilizan entre los routers OSPF para verificar que sus vecinos estén activos.




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

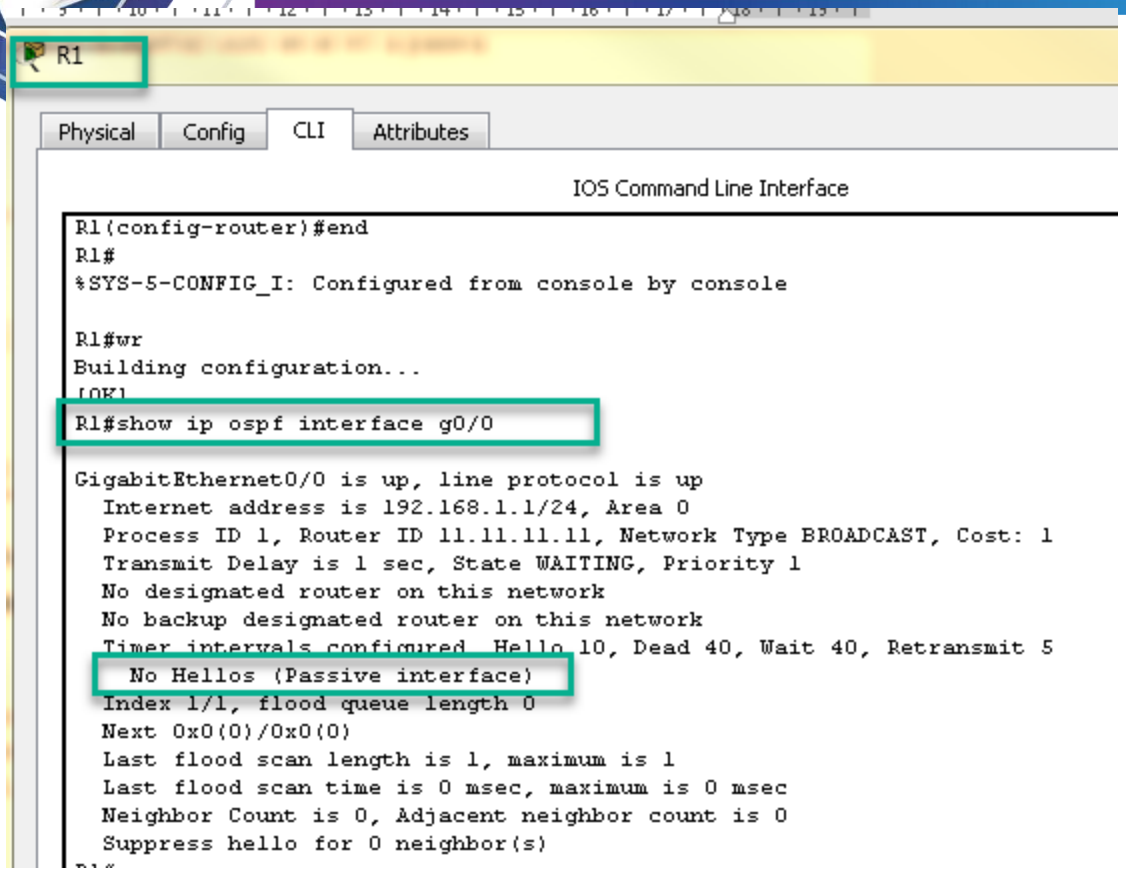
R1(config)# **router ospf 1**

R1(config-router)# **passive-interface g0/0**

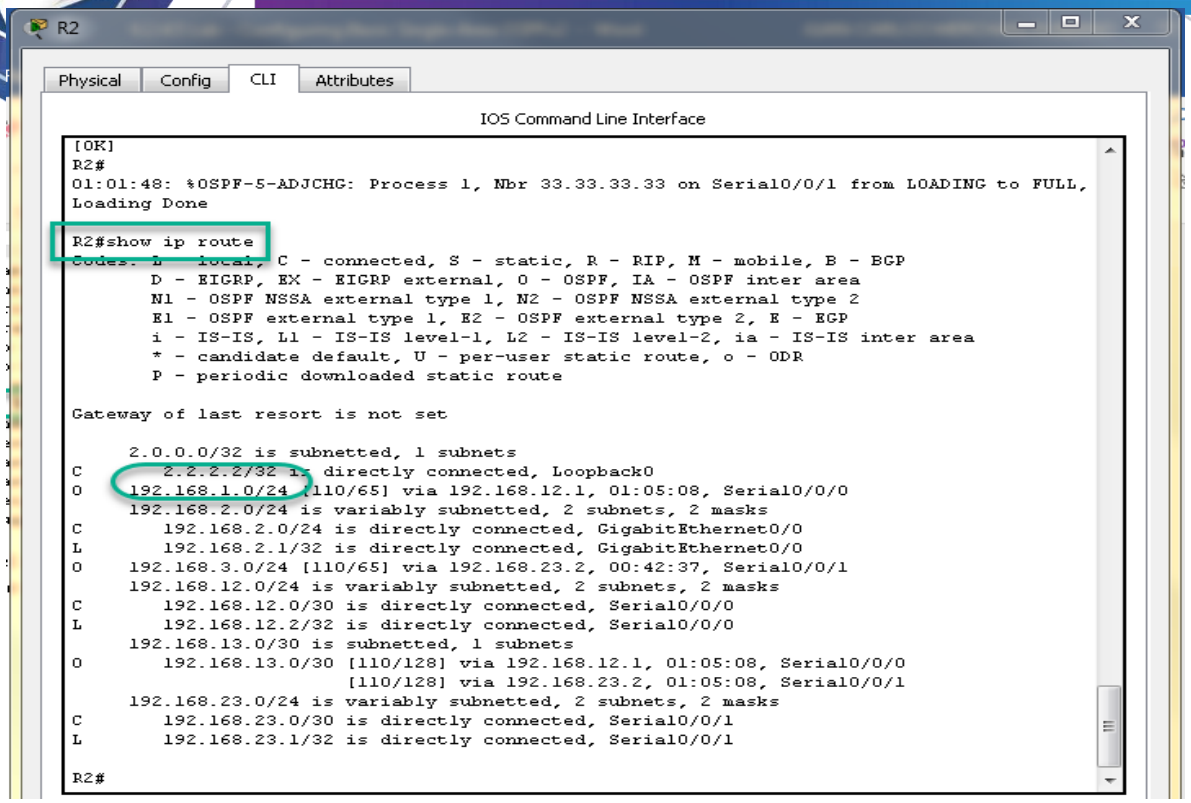


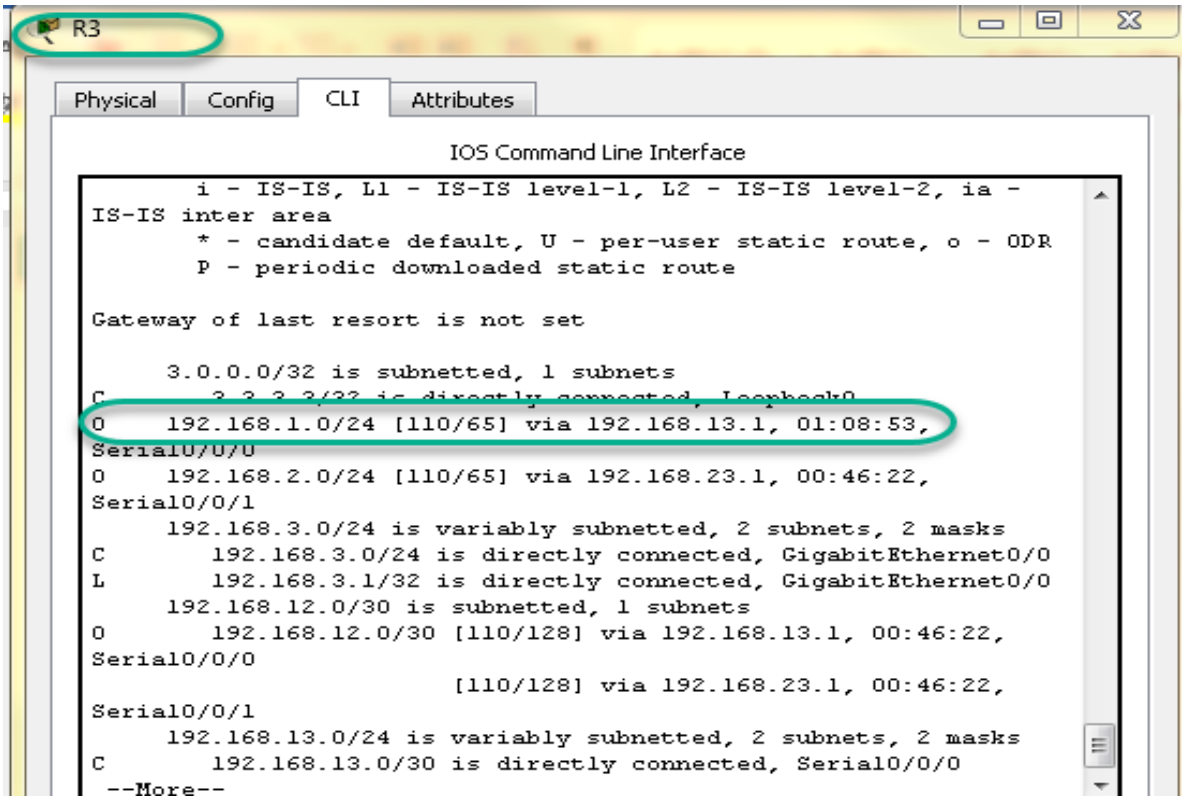

**c. Vuelva a emitir el comando show ip ospf interface g0/0 para verificar que la interfaz G0/0 ahora sea pasiva.**

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




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

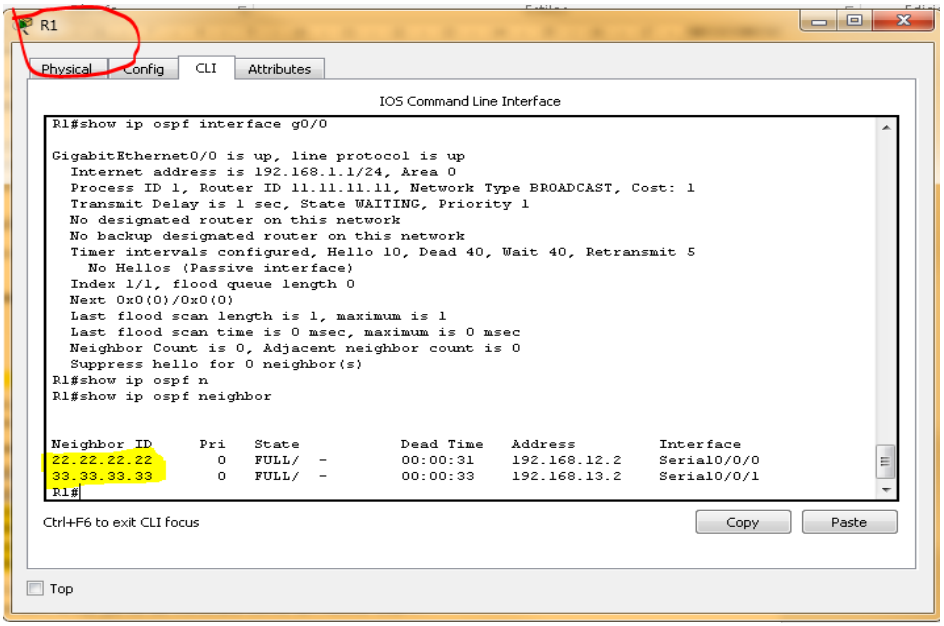

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
[OK]
R2#
01:01:48: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from LOADING to FULL, Loading Done
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
2.0.0.0/32 is subnetted, 1 subnets
C 2.2.2.2/32 is directly connected, Loopback0
O 192.168.1.0/24 [110/65] via 192.168.12.1, 01:05:08, 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, 00:42:37, 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, 01:05:08, Serial0/0/0
[110/128] via 192.168.23.2, 01:05:08, 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#

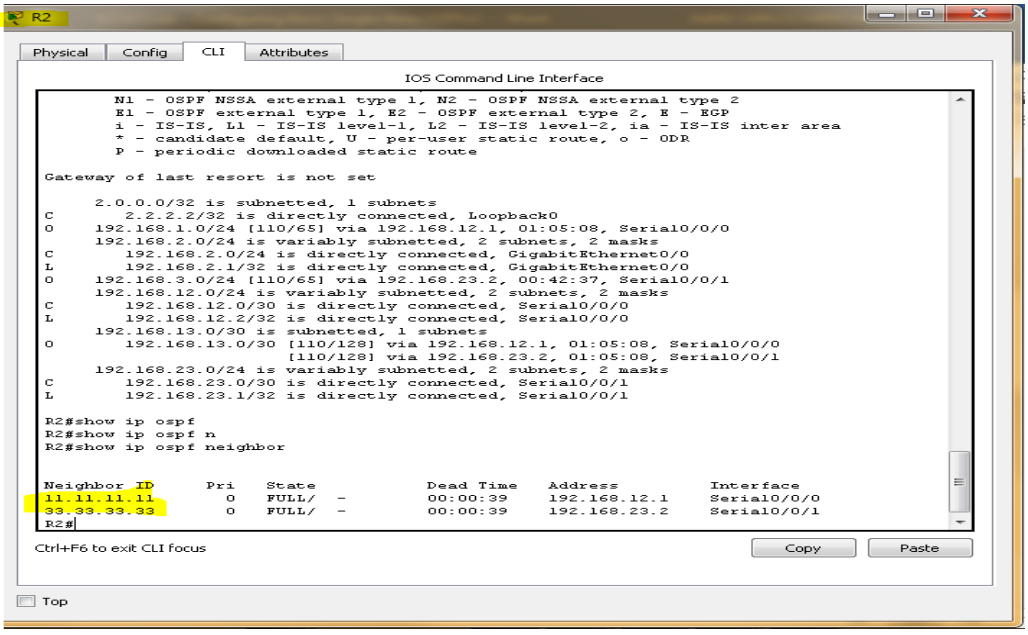

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
3.0.0.0/32 is subnetted, 1 subnets
C 3.3.3.3/32 is directly connected, Loopback0
O 192.168.1.0/24 [110/65] via 192.168.13.1, 01:08:53, Serial0/0/0
O 192.168.2.0/24 [110/65] via 192.168.23.1, 00:46:22, 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, 00:46:22, Serial0/0/0
[110/128] via 192.168.23.1, 00:46:22, 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
--More--

**Step 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.

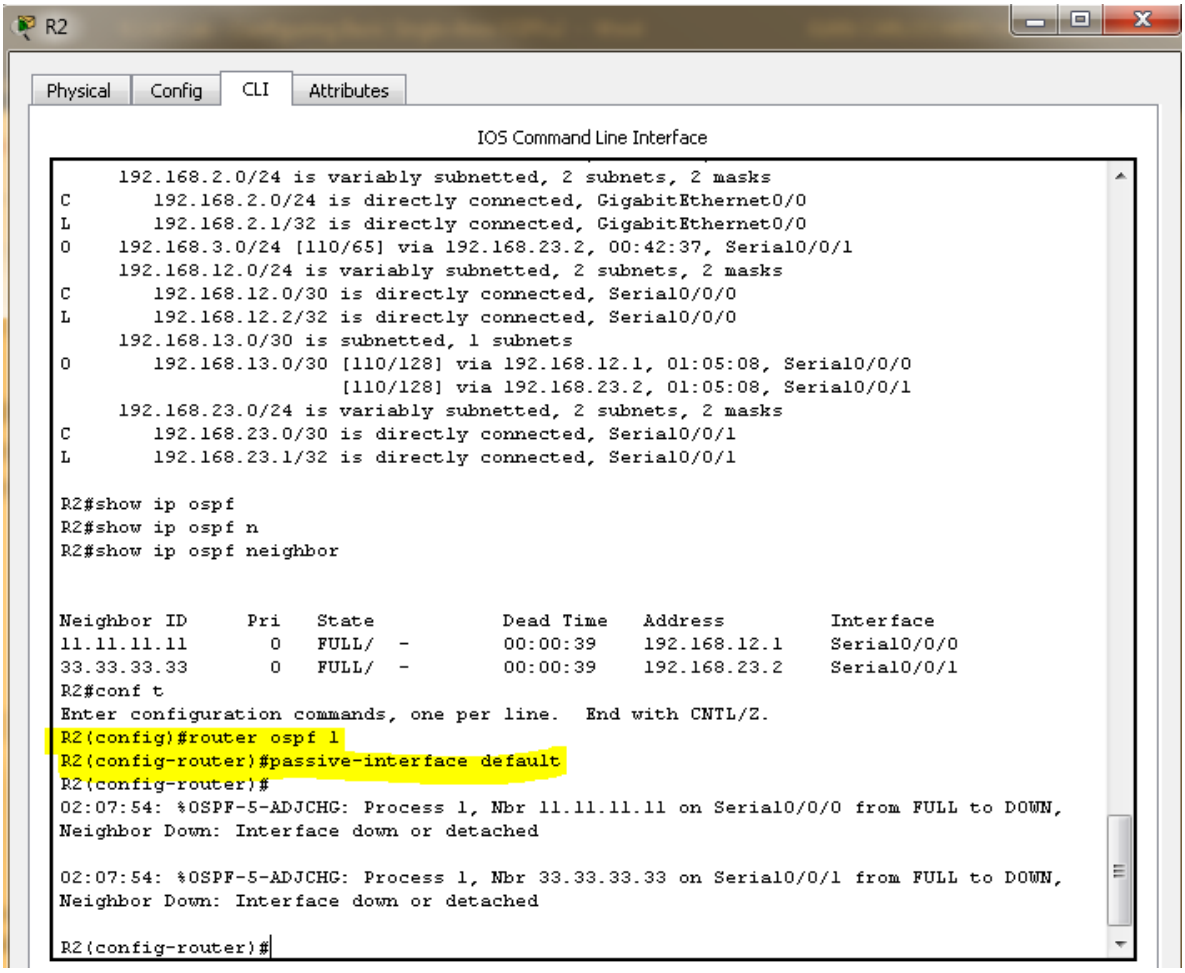
R1# **show ip ospf neighbor**



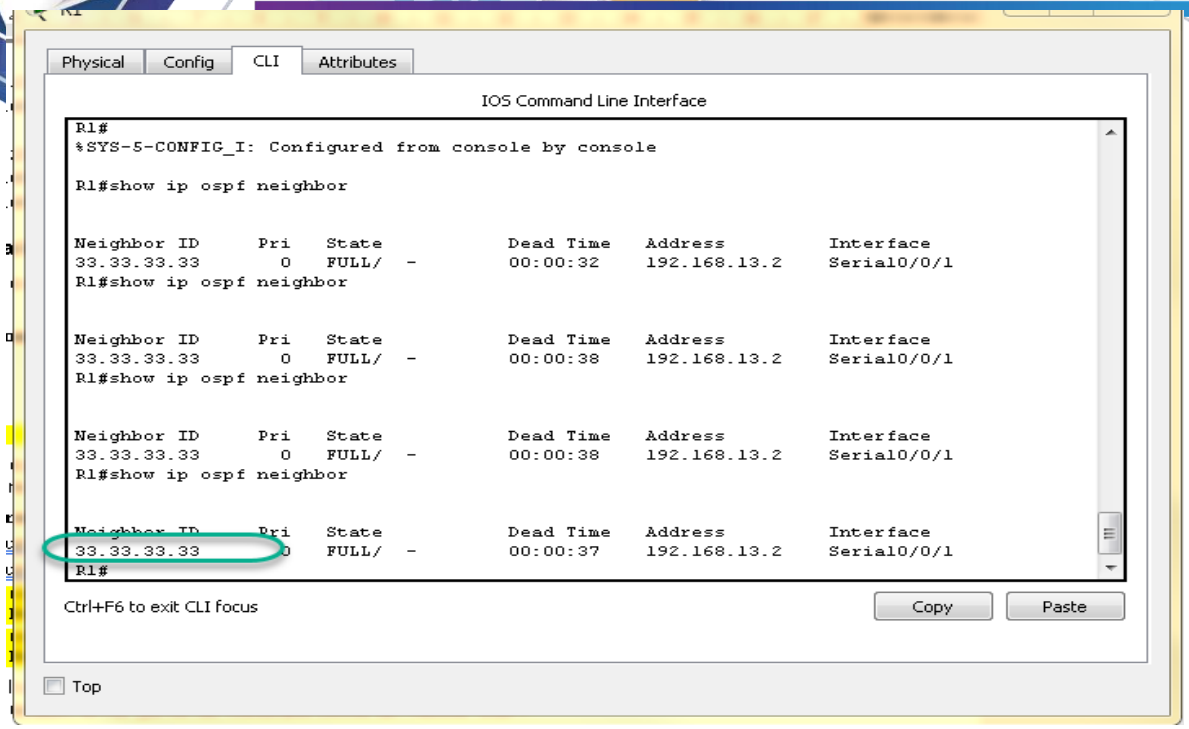

b. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPF como pasivas de manera predeterminada.

R2(config)# **router ospf 1**
R2(config-router)# **passive-interface default**
R2(config-router)#



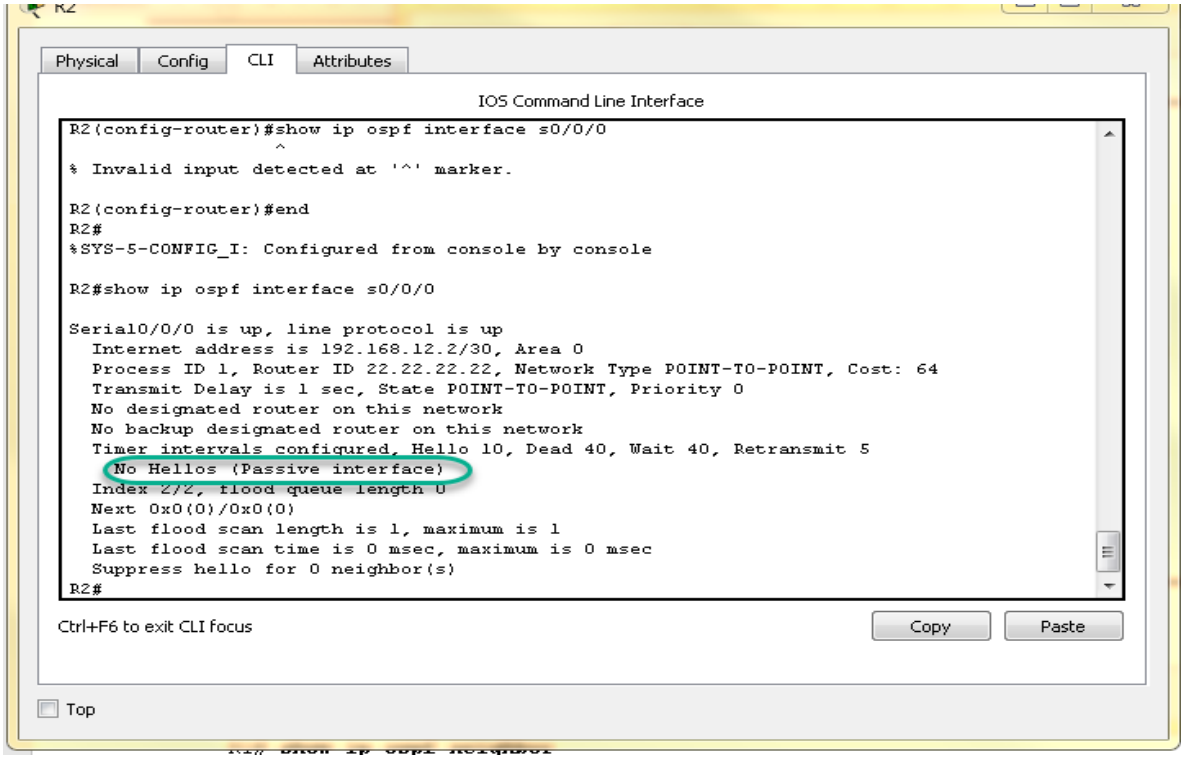

c. Vuelva a emitir el comando **show ip ospf neighbor** en el R1. Una vez que el temporizador de tiempo muerto haya caducado, el R2 ya no se mostrará como un vecino OSPF.

R1# **show ip ospf neighbor**

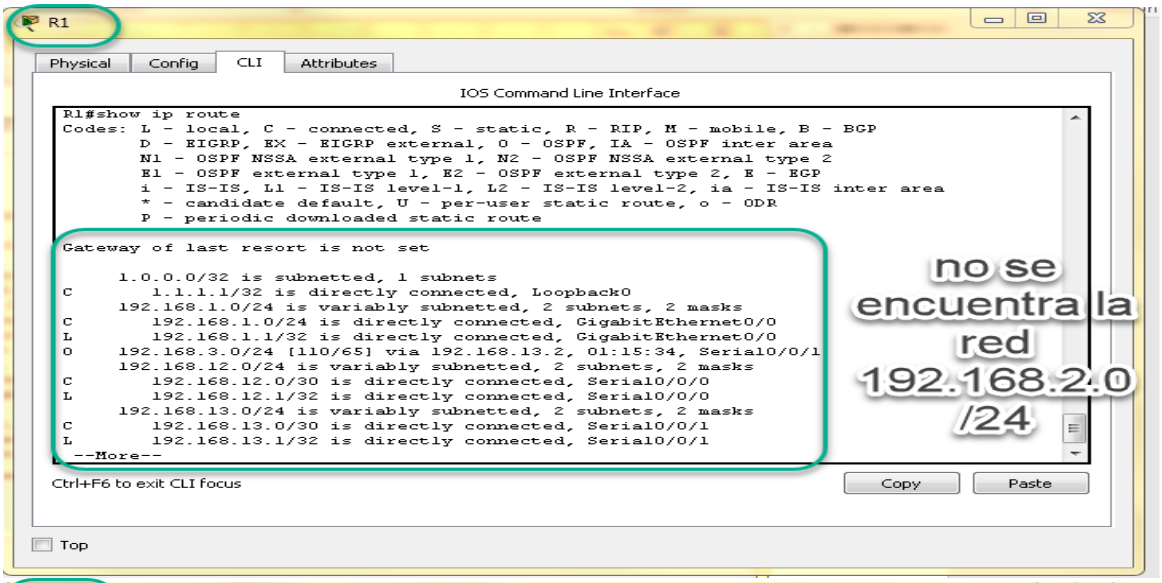


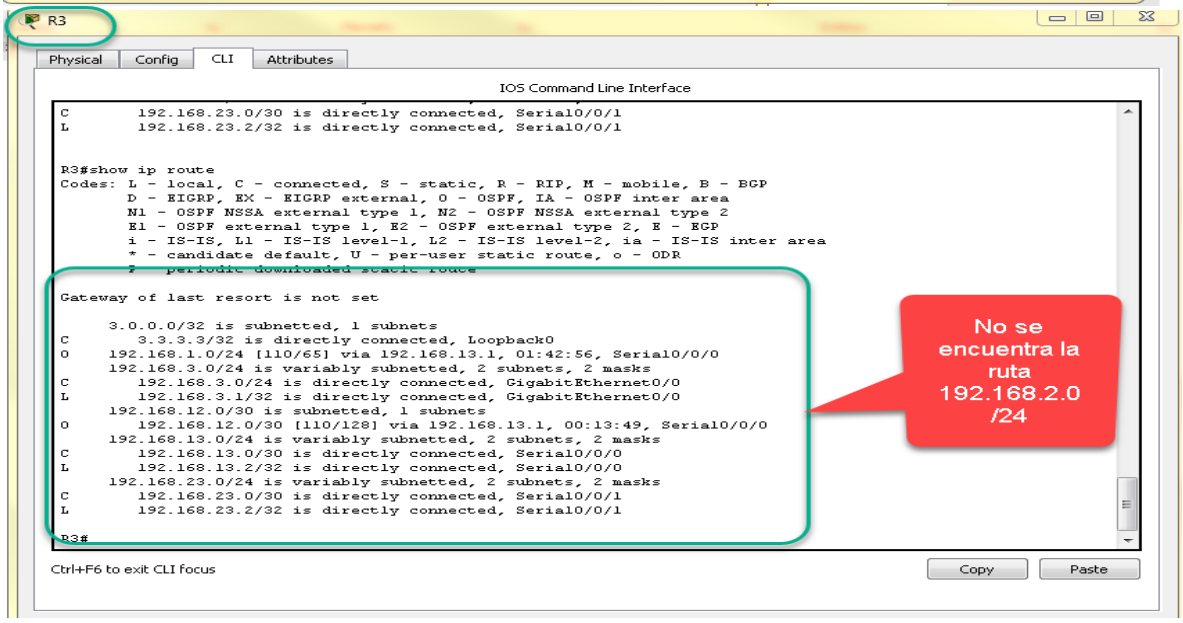

d. Emita el comando **show ip ospf interface S0/0/0** en el R2 para ver el estado de OSPF de la interfaz S0/0/0.

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



e. Si todas las interfaces en el R2 son pasivas, no se anuncia ninguna información de routing. En este caso, el R1 y el R3 ya no deberían tener una ruta a la red 192.168.2.0/24. Esto se puede verificar mediante el comando **show ip route**

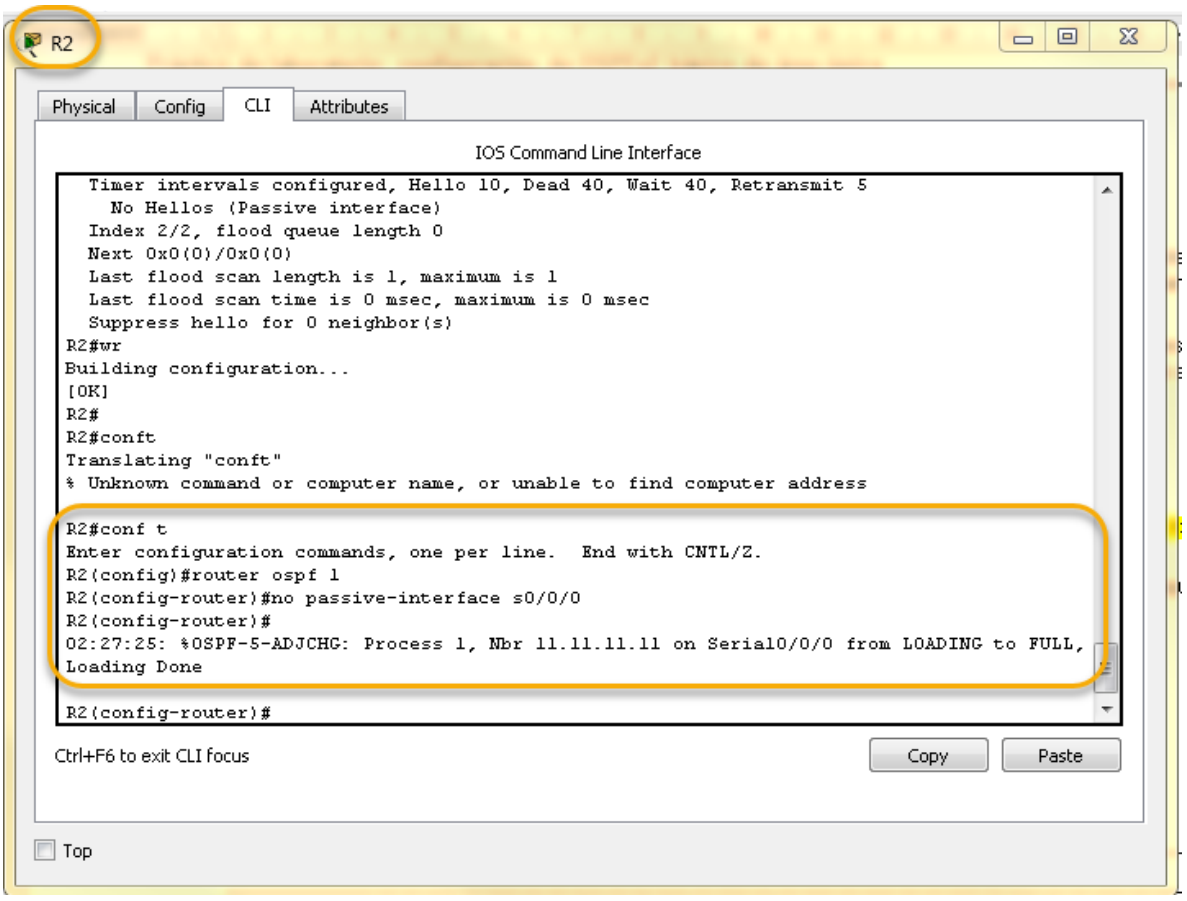



f. En el R2, emita el comando **no passive-interface** para que el router envíe y reciba actualizaciones de routing OSPF. Después de introducir este comando, verá un mensaje informativo que explica que se estableció una adyacencia de vecino con el R1.

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

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




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

R1

Physical | Config | CLI | Attributes

IOS Command Line Int

```
      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
 --More--
02:28:19: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on Serial0/0/0 from LOADING to FULL, Los

      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0/30 [110/128] via 192.168.13.2, 00:09:28, Serial0/0/1


R1#hiw ip route
         ^
% Invalid input detected at '^' marker.

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

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1/32 is directly connected, Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
O     192.168.2.0/24 [110/65] via 192.168.12.2, 00:05:04, Serial0/0/0
O     192.168.3.0/24 [110/65] via 192.168.13.2, 01:30:41, 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
 --More--
```

R3

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
C        3.3.3.3/32 is directly connected, Loopback0
O     192.168.1.0/24 [110/65] via 192.168.13.1, 01:42:56, 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, 00:13:49, 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# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
C        3.3.3.3/32 is directly connected, Loopback0
O     192.168.1.0/24 [110/65] via 192.168.13.1, 01:56:40, Serial0/0/0
O     192.168.2.0/24 [110/129] via 192.168.13.1, 00:08:32, 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, 00:27:33, 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
 --More--
```

.00%

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

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

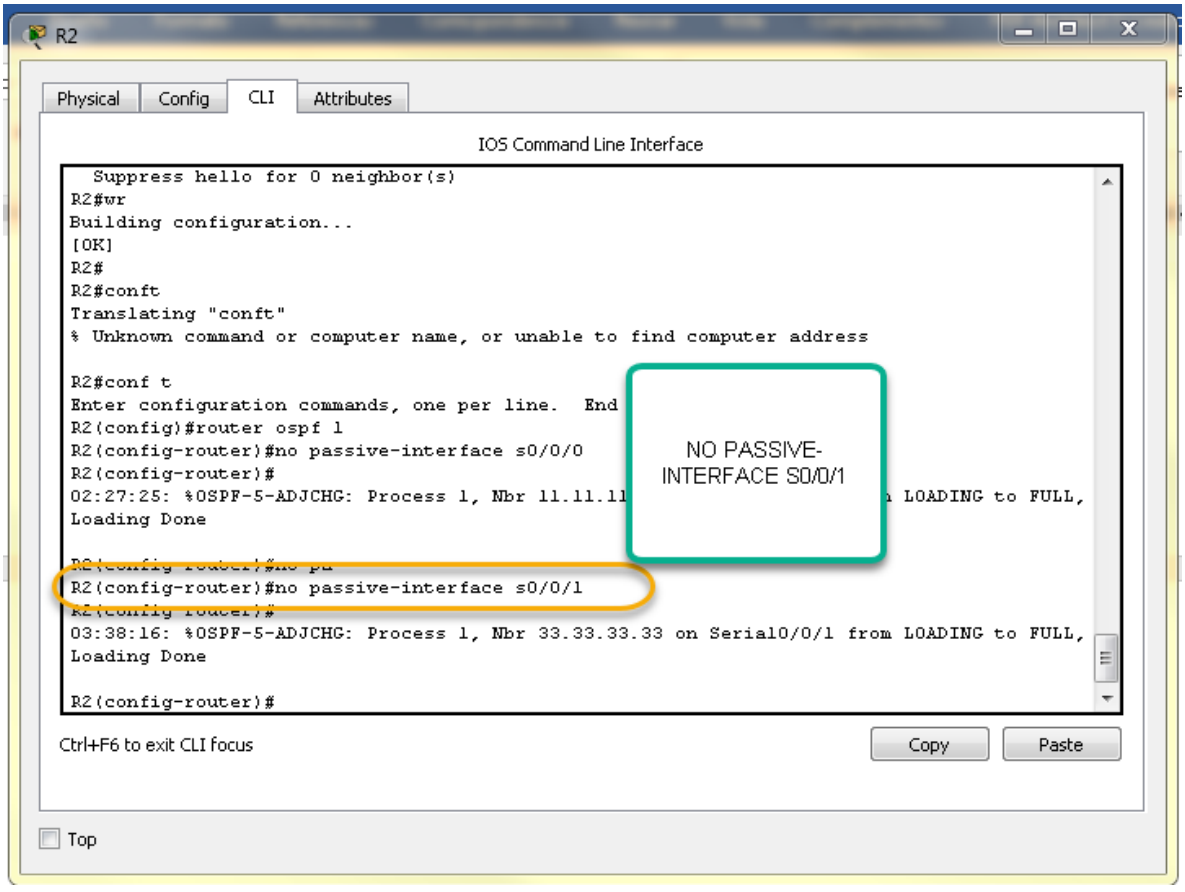
¿El R2 aparece como vecino OSPF en el R1? _SI

¿El R2 aparece como vecino OSPF en el R3? _NO

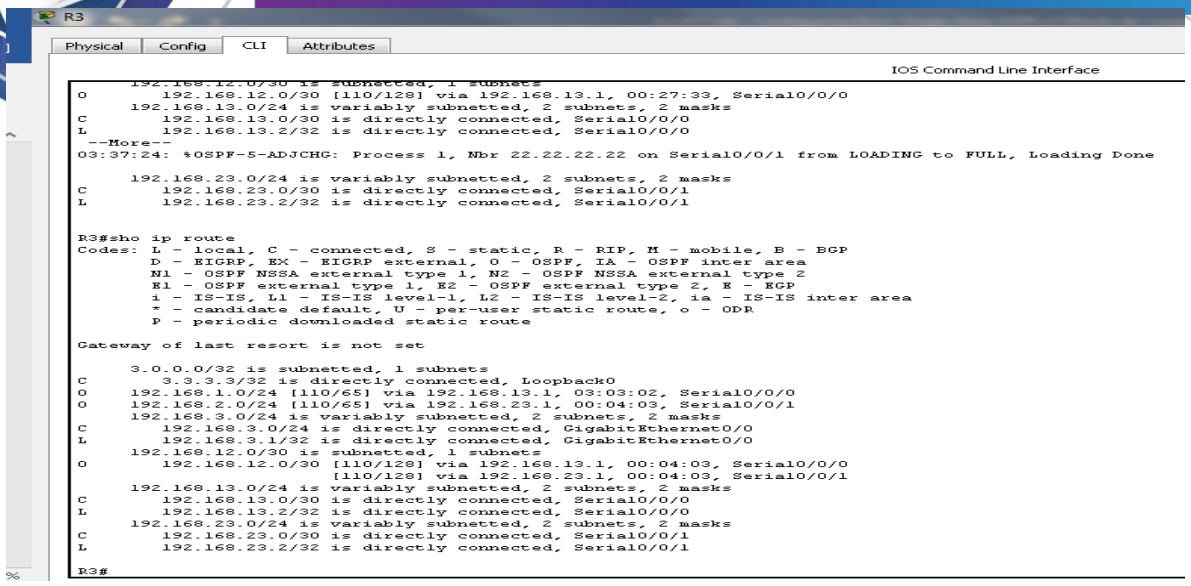
¿Qué indica esta información

Indica que todo el tráfico de la red 192.168.2.0/24 del router 3 deberá ser enrutado a través de R1. La interfaz s0/0/1 en r2 esta aun configurada como una interface pasiva, de tal forma que el enrutamiento ospf no está notificando a través de la la interfaz. El costo acumulado 129 que resulta del tráfico de r3 hacia la red 192.168.2.0 /24 la cual deberá pasar a través de 2 enlaces seriales.

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




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




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

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3 y cómo se calcula? 65

¿El R2 aparece como vecino OSPF del R3? YES

```
R3#shwo ip ospf neigh
R3#show ip ospf neigh
R3#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
11.11.11.11       0   FULL/  -        00:00:31    192.168.13.1    Serial0/0/0
22.22.22.22       0   FULL/  -        00:00:31    192.168.23.1    Serial0/0/1
R3#
```

**Part 6: cambiar las métricas de OSPF**

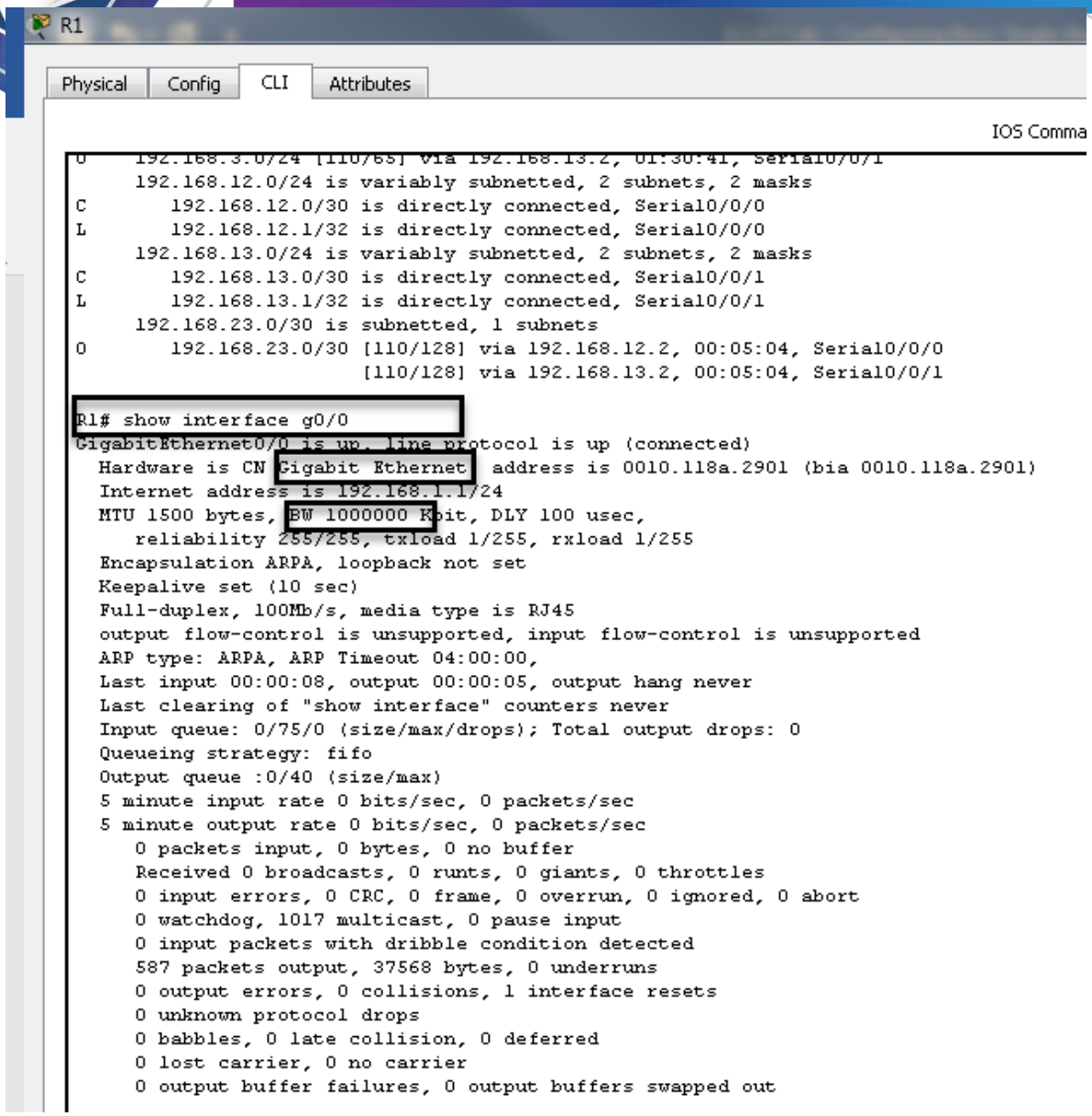
En la parte 3, cambiará las métricas de OSPF con los comandos **auto-cost reference-bandwidth**, **bandwidth** e **ip ospf cost**.

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

**Step 1: Cambiar el ancho de banda de referencia en los routers.**

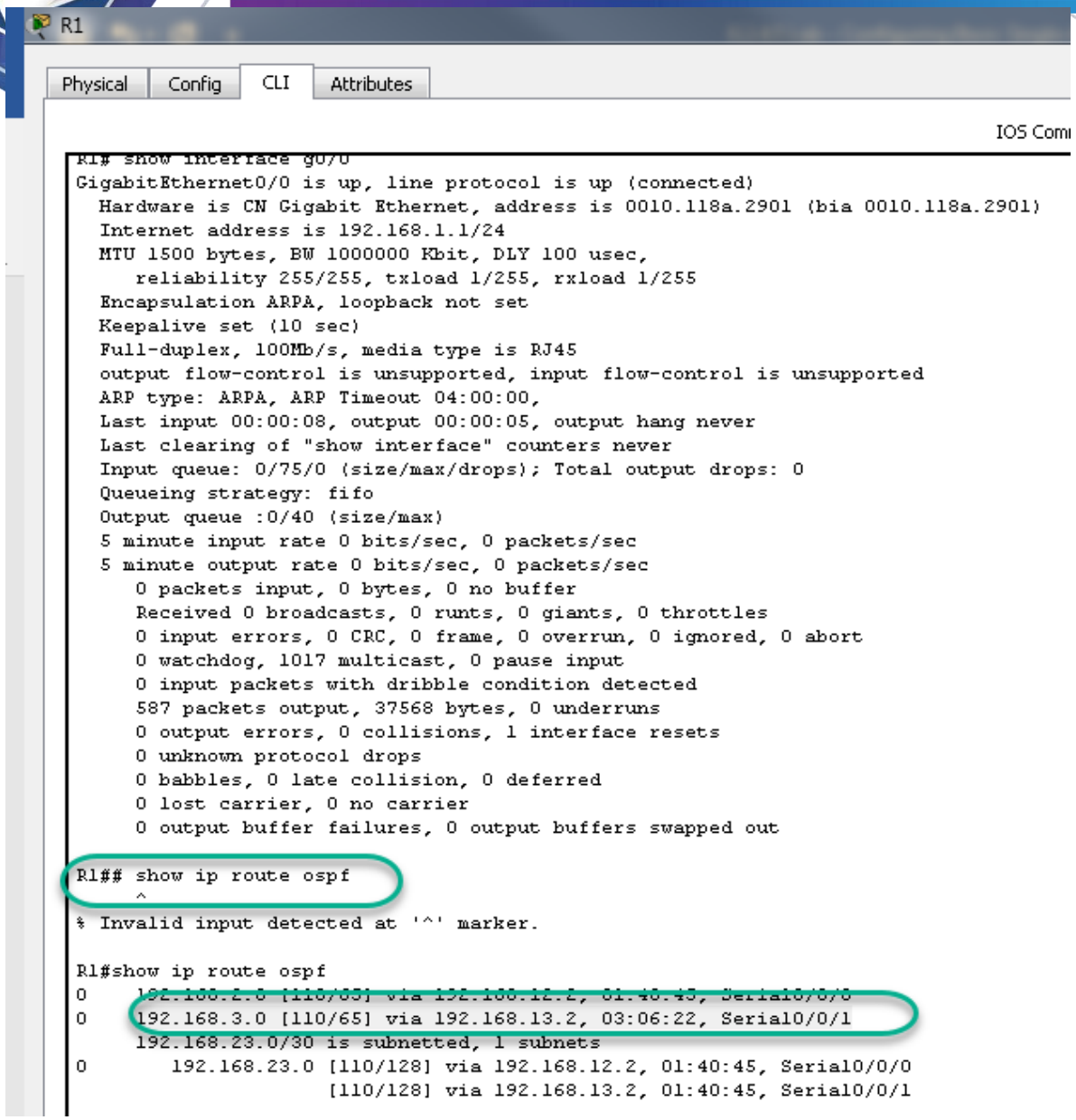
a. Emita el comando **show interface** en el R1 para ver la configuración del ancho de banda predeterminado para la interfaz G0/0.

R1# **show interface g0/0**



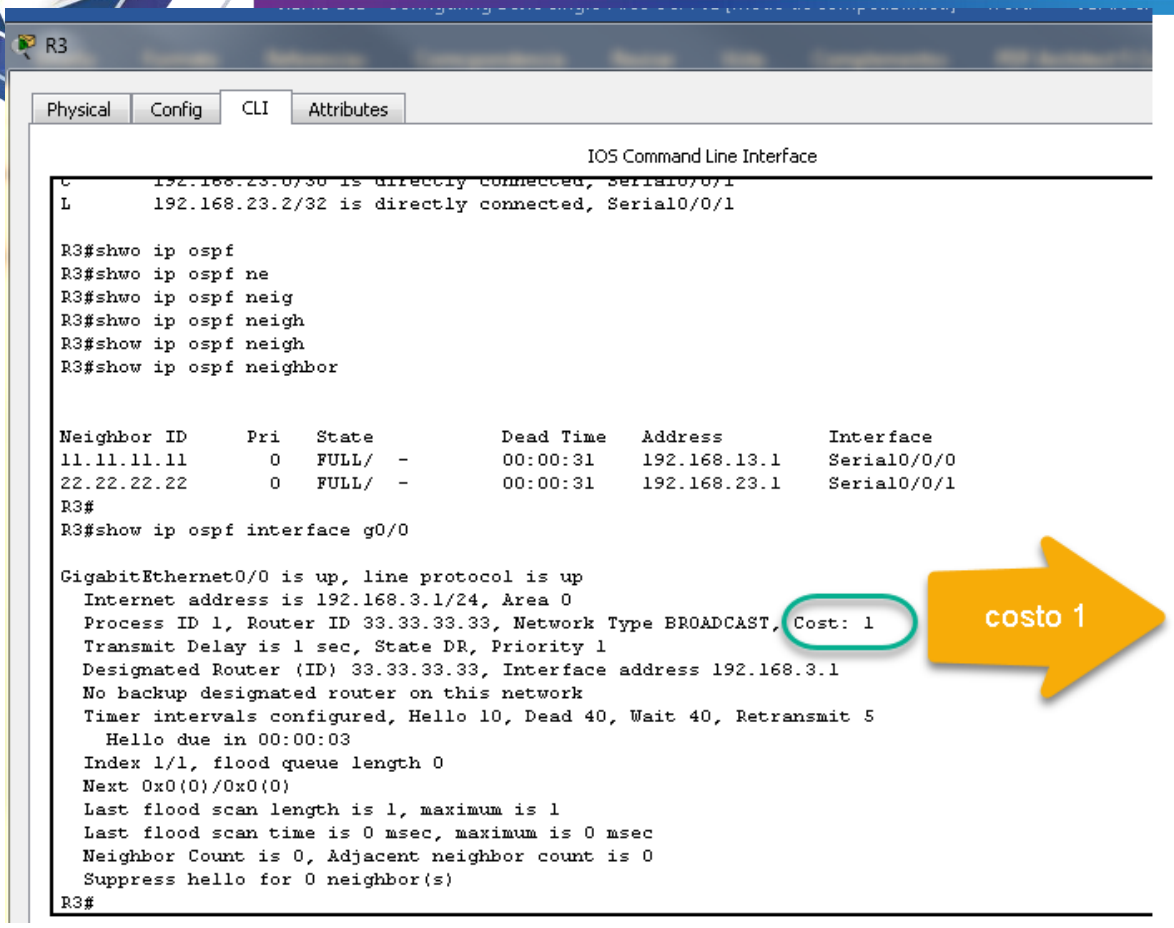

b. Emita el comando **show ip route ospf** en el R1 para determinar la ruta a la red 192.168.3.0/24.

R1# **show ip route ospf**



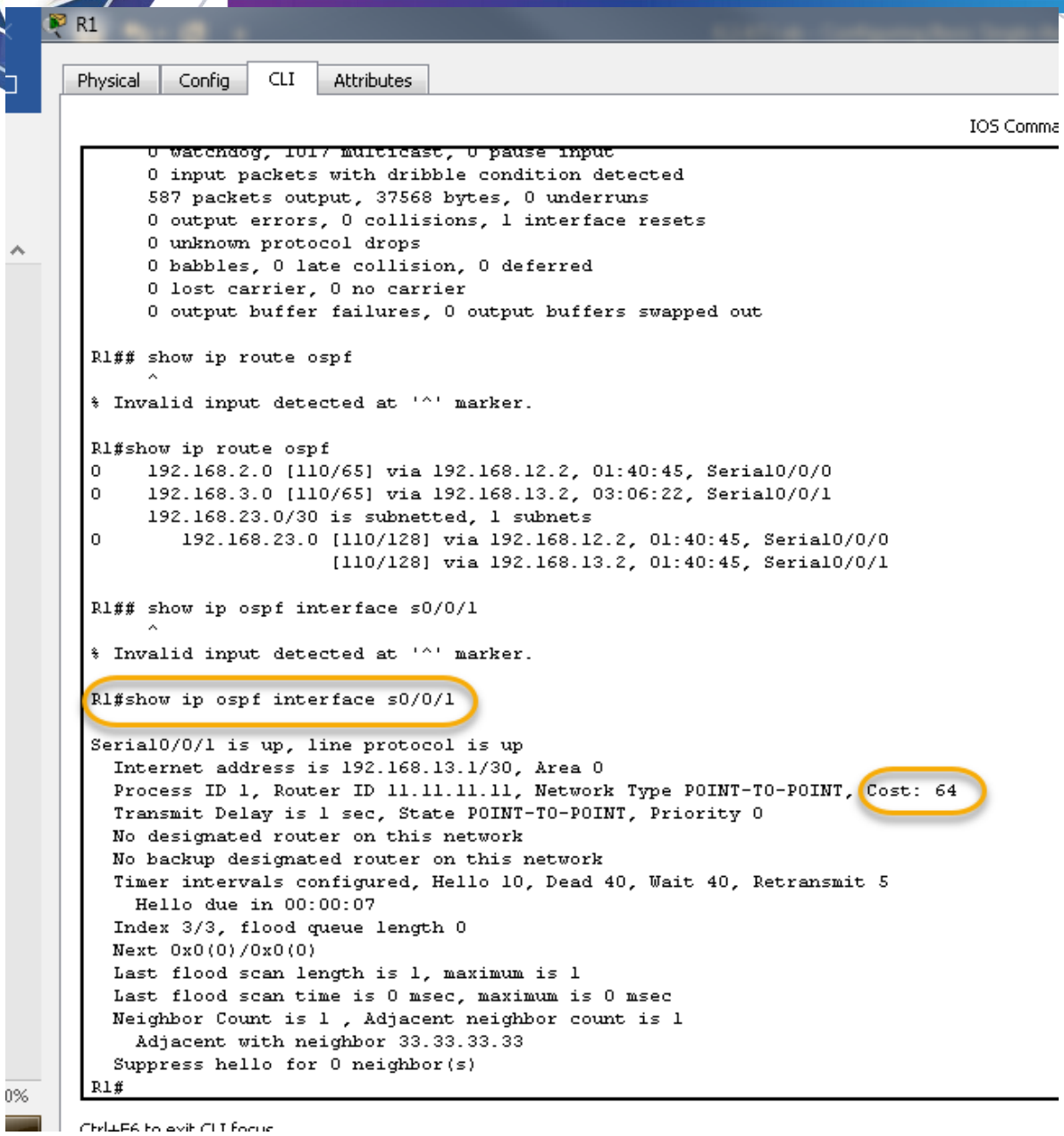

c. Emita el comando **show ip ospf interface** en el R3 para determinar el costo de routing para G0/0.

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




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

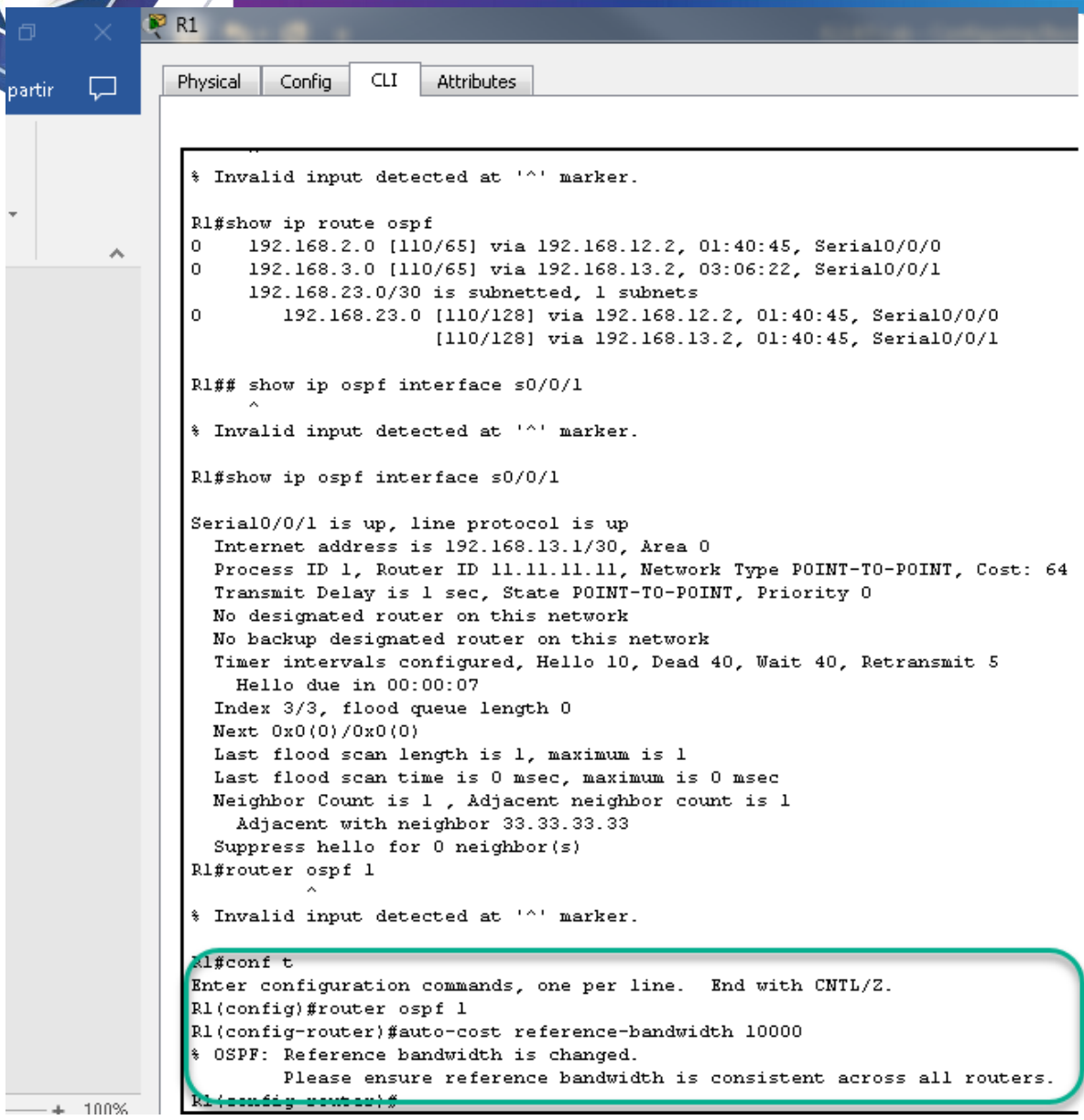
R1# **show ip ospf interface s0/0/1**




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.

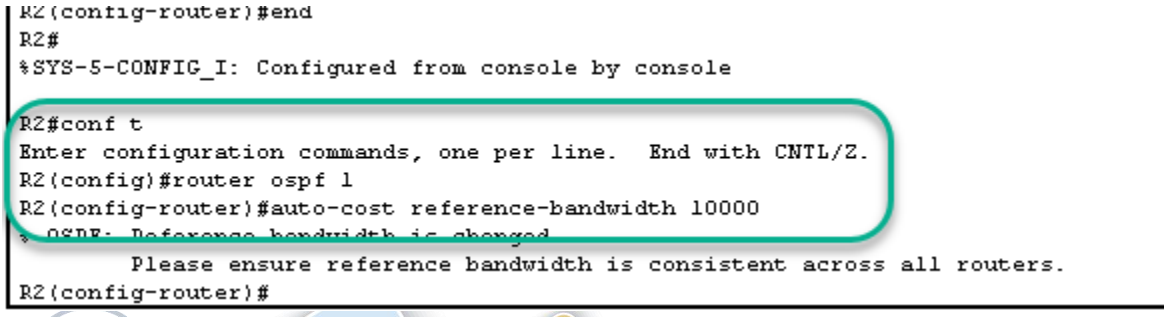
R1(config)# **router ospf 1**

R1(config-router)# **auto-cost reference-bandwidth 10000**

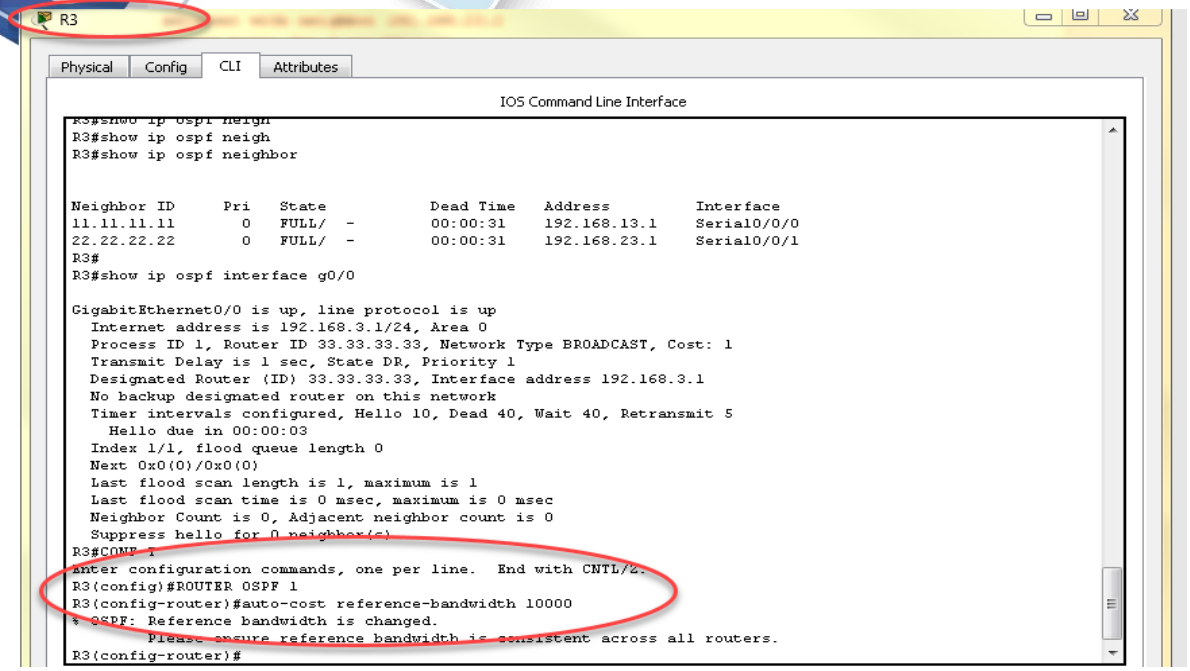



f. Emita el comando **auto-cost reference-bandwidth 10000** en los routers R2 y R3.

Router 2

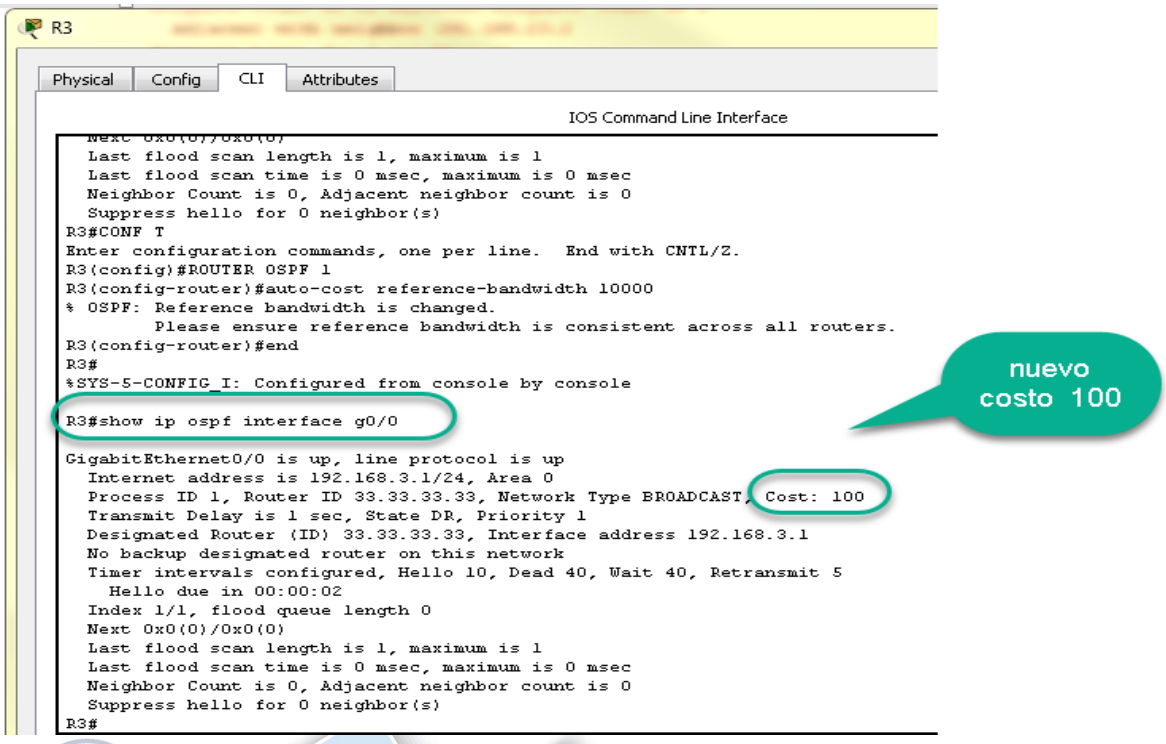


ROUTER 3

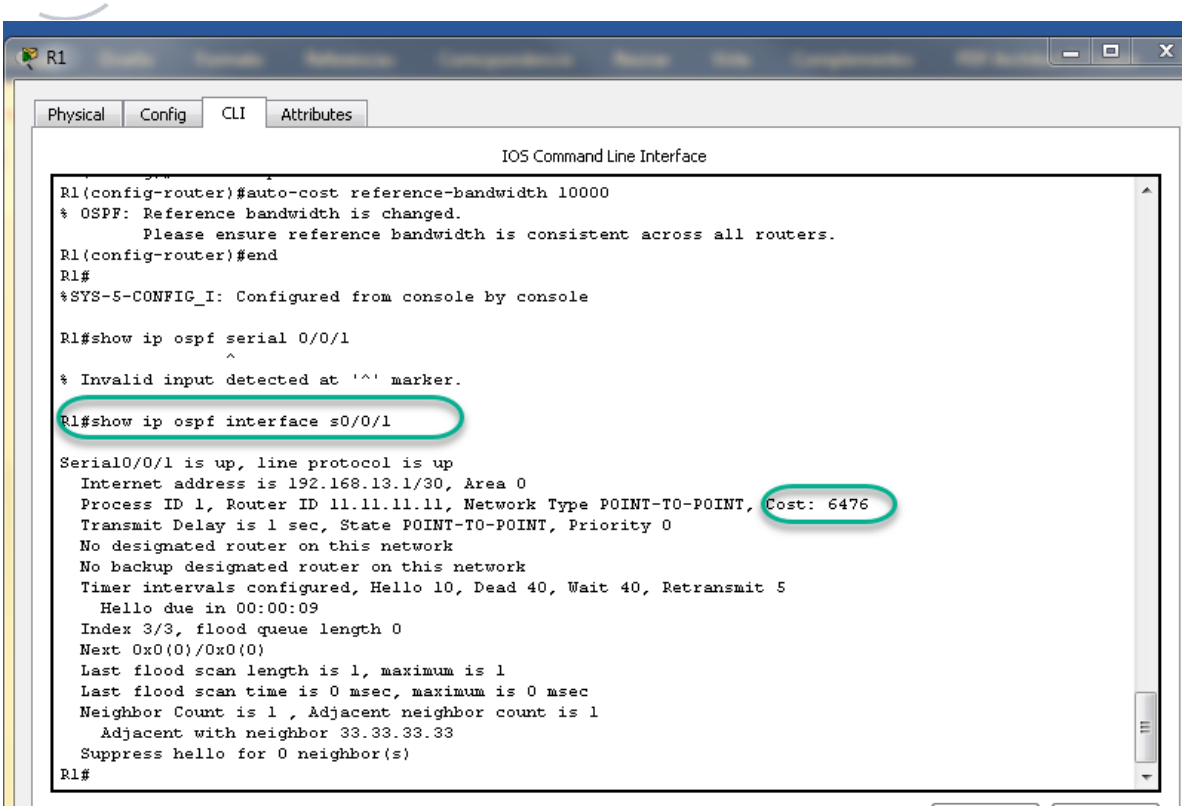



g. Vuelva a emitir el comando **show ip ospf interface** para ver el nuevo costo de G0/0 en el R3 y de S0/0/1 en el R1.

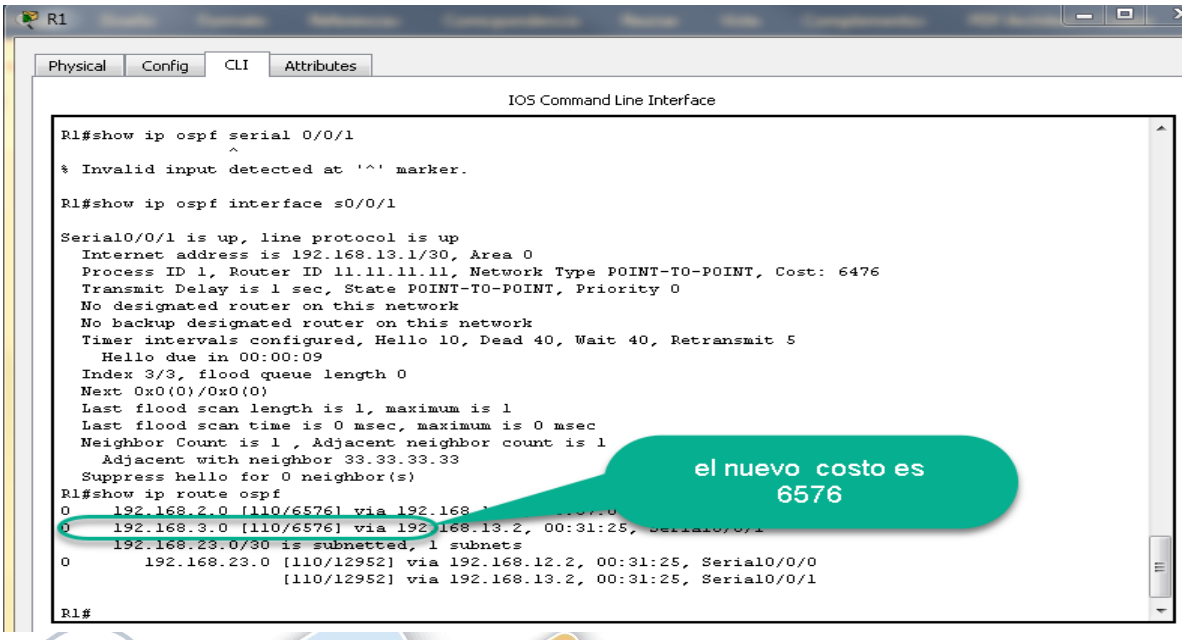
R3# **show ip ospf interface g0/0**



Nos dio 100. Por la velocidad  FAST ETHERNET (100 MB/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).



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**

**ROUTER 1**

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#
```

**ROUTER 2**

```
Enter configuration commands, one per line.  End with CNTL/Z.
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.
R2(config-router)#
```

**ROUTER 3**

```
R3#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
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.
R3(config-router)#
```

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

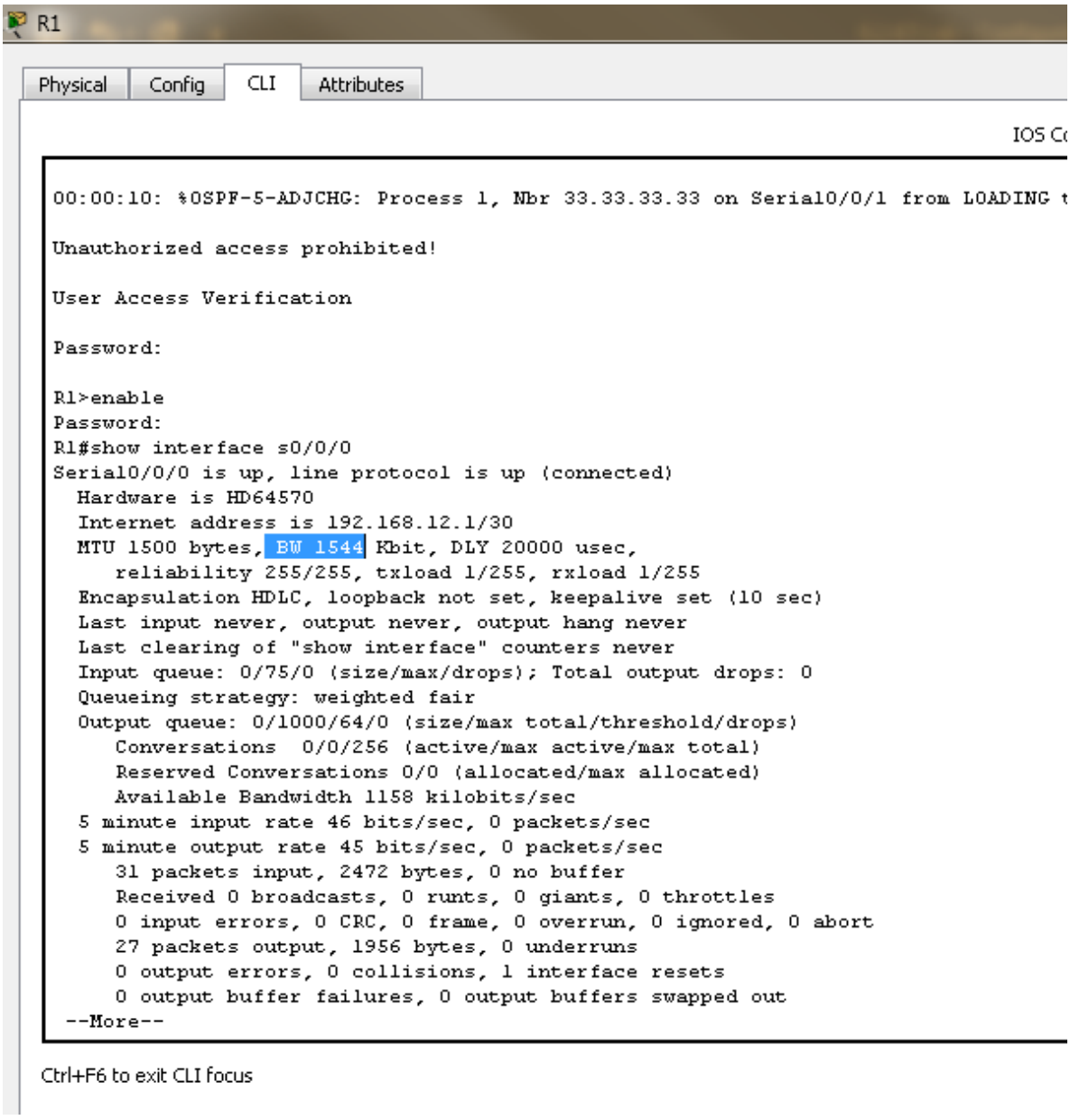
Los equipos de hoy en dia soporta velocidades de mas 100 Mb/s, para obtener un costo más exacto para estas velocidades punto de referencia de ancho de banda es necesario cambiar el ancho.

El cambio del ancho de banda de referencia en realidad no afecta la capacidad de ancho de banda en el enlace, sino que simplemente afecta el cálculo utilizado para determinar la métrica

**Paso2: Cambiar el ancho de banda de una interfaz.**

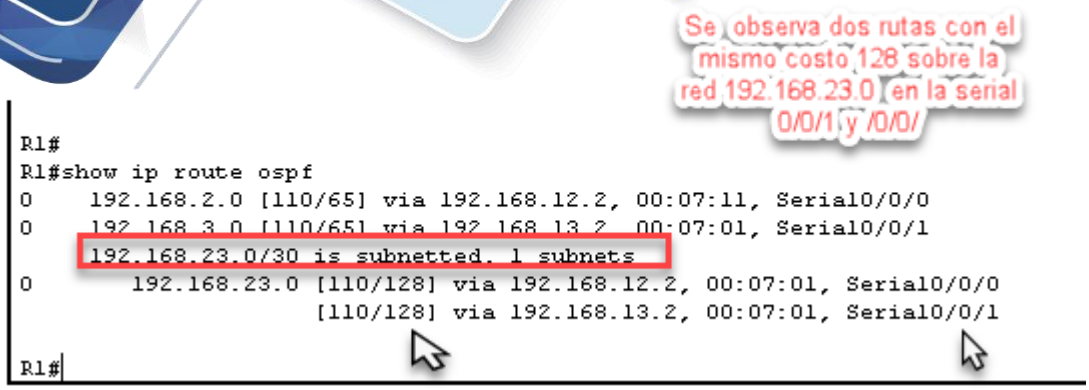
a. Emita el comando **show interface s0/0/0** en el R1 para ver la configuración actual del ancho de banda de S0/0/0. Aunque la velocidad de enlace/frecuencia de reloj en esta interfaz estaba configurada en 128 Kb/s, el ancho de banda todavía aparece como 1544 Kb/s.

R1# **show interface s0/0/0**




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**




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

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

```
R1#WR
Building configuration...
[OK]
R1#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#
```

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

R1# **show ip route ospf**

```
R1#show ip route ospf
O    192.168.2.0 [110/129] via 192.168.13.2, 00:03:55, Serial0/0/1
O    192.168.3.0 [110/65] via 192.168.13.2, 00:29:06, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 00:03:55, Serial0/0/1

R1#
```

192.168.23.0 se encuentra los 128 esto indica que hay una mejor ruta que va por la serial 0/0/1

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**

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

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 00:00:05
  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 22.22.22.22
  Suppress hello for 0 neighbor(s)
R1#
```

```
  Suppress hello for 0 neighbor(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: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 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 33.33.33.33
  Suppress hello for 0 neighbor(s)
R1#
```

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

```
  Suppress hello for 0 neighbor(s)
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s0/0/1
R1(config-if)#bandwith
R1(config-if)#bandwith 128
                       ^
% Invalid input detected at '^' marker.

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

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, 00:05:11, Serial0/0/0
O     192.168.3.0 [110/782] via 192.168.13.2, 00:05:11, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/845] via 192.168.12.2, 00:05:11, Serial0/0/0
                      [110/845] via 192.168.13.2, 00:05:11, Serial0/0/1

R1#
```

nos muestra dos caminos

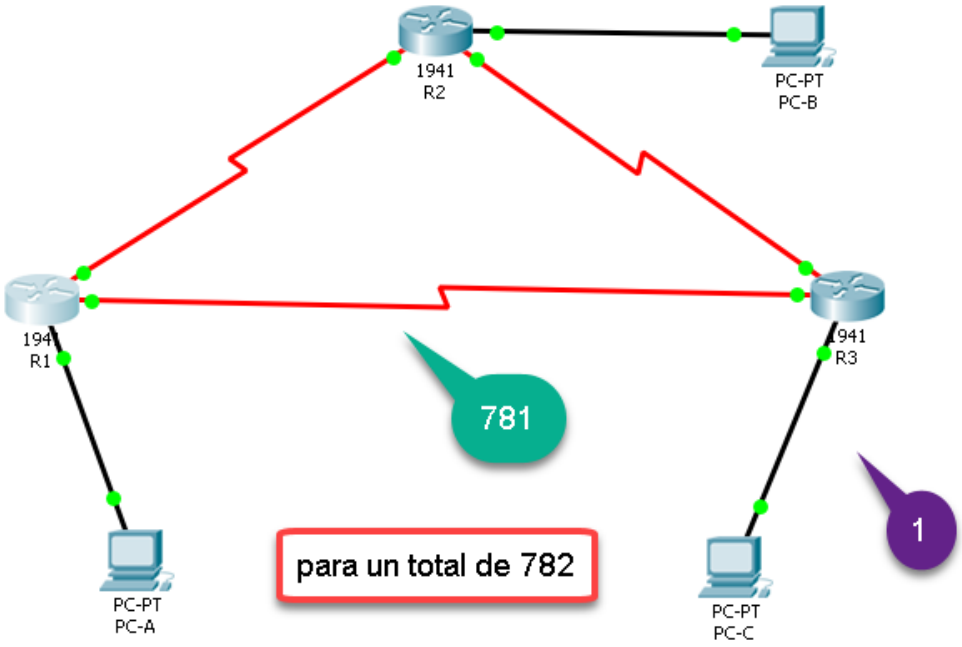
costo 845

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.

```
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: 781
```

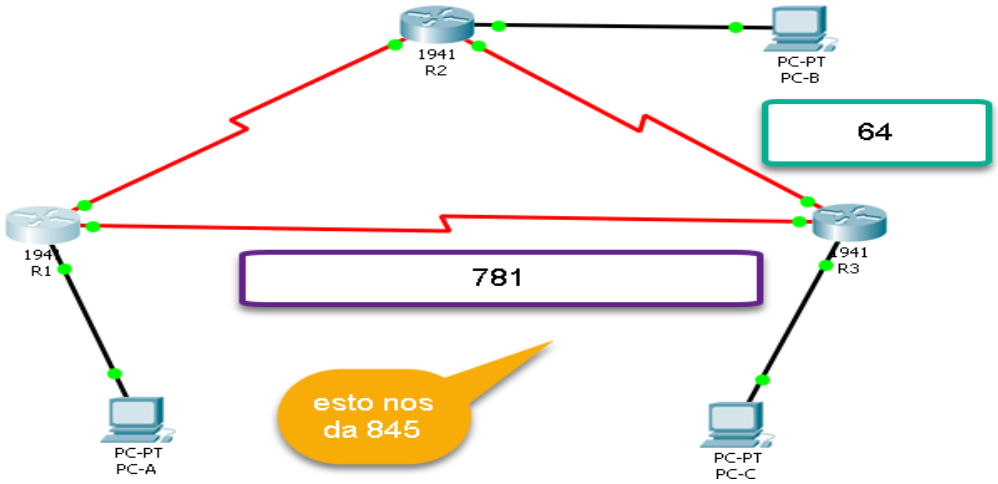
Para llegar a la red **192.168.3.0** donde el costo es 782

```
O    192.168.3.0 [110/782] via 192.168.13.2, 00:05:11, Serial0/0/1
```



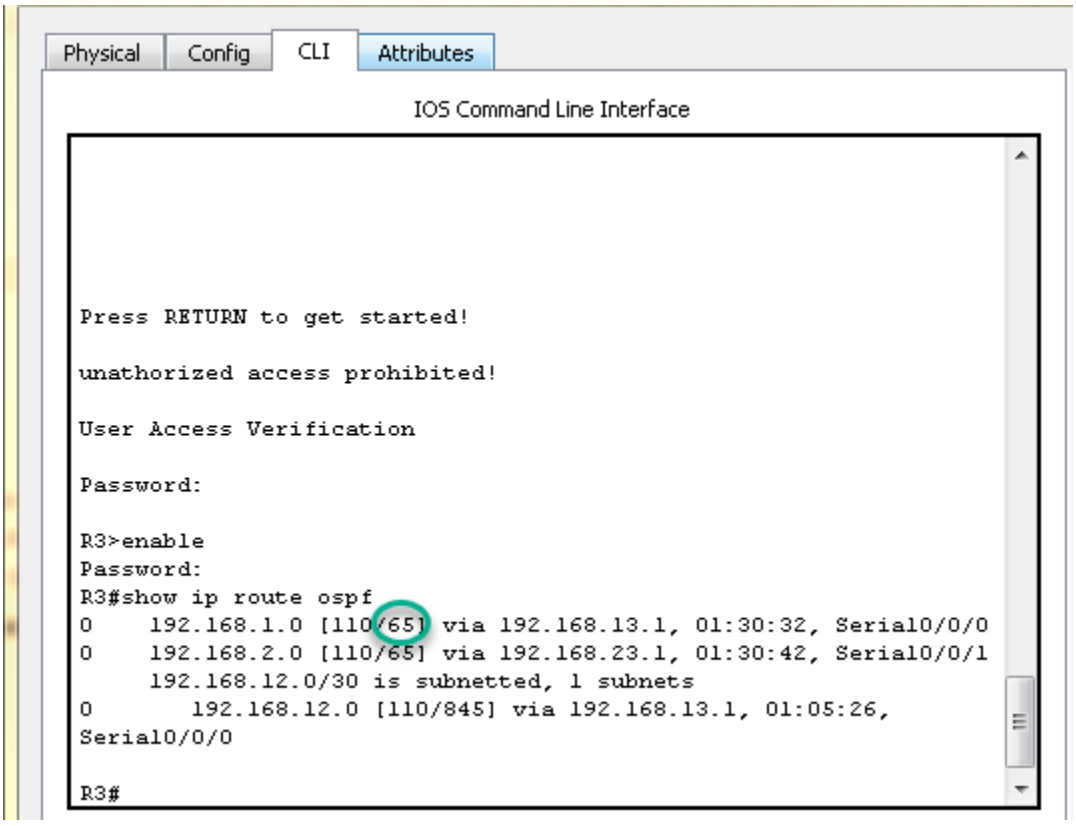

El costo para llegar a la 192.168.23.0 el costo es 845

```
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/845] via 192.168.12.2, 00:05:11, Serial0/0/0
                     [110/845] via 192.168.13.2, 00:05:11, Serial0/0/1
```

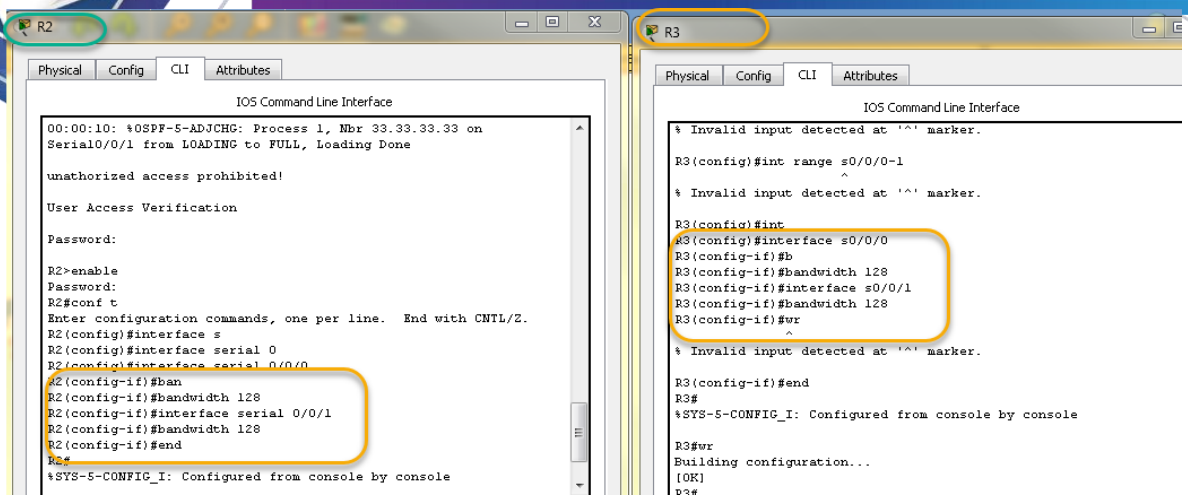



h. Emita el comando **show ip route ospf** en el R3. El costo acumulado de 192.168.1.0/24 todavía se muestra como 65. A diferencia del comando **clock rate**, el comando **bandwidth** se tiene que aplicar en ambos extremos de un enlace serial.

R3# **show ip route ospf**



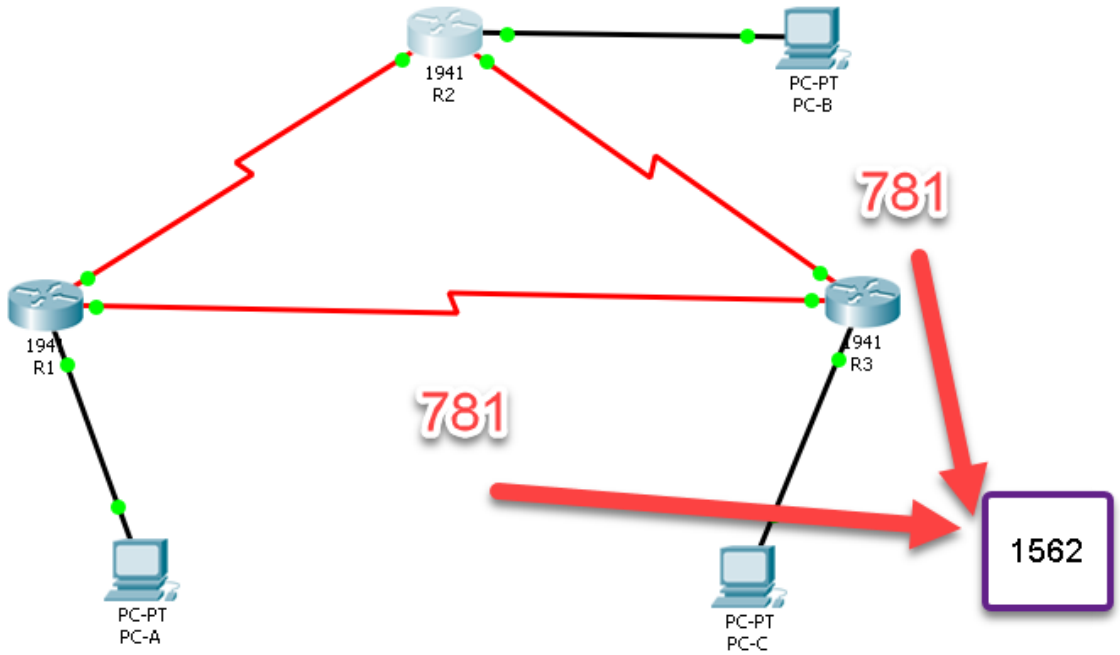

i.Emita el comando **bandwidth 128** en todas las interfaces seriales restantes de la topología.




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

```
R1#show ip route os
R1#show ip route ospf
O    192.168.2.0 [110/782] via 192.168.12.2, 00:46:47, Serial0/0/0
O    192.168.3.0 [110/782] via 192.168.13.2, 00:46:47, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:02:51, Serial0/0/0
                     [110/1562] via 192.168.13.2, 00:02:51, Serial0/0/1

R1#
```

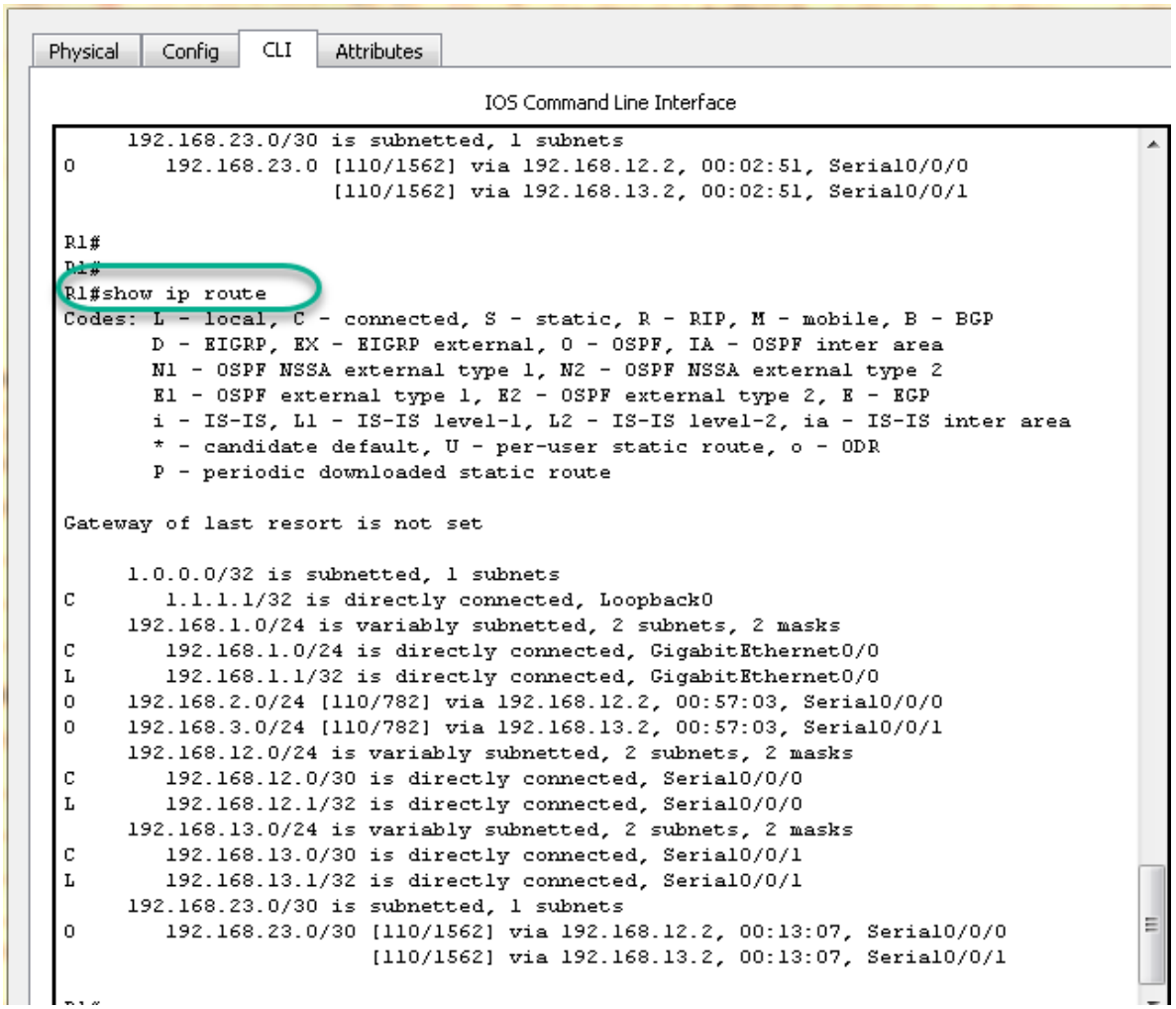
Para llegar a la red 192.168.23.0 se requiere



**Paso 3: cambiar el costo de la ruta.**

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

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




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

R1(config)# **int s0/0/1**

```
R1(config-if)# ip ospf cost 1565
```

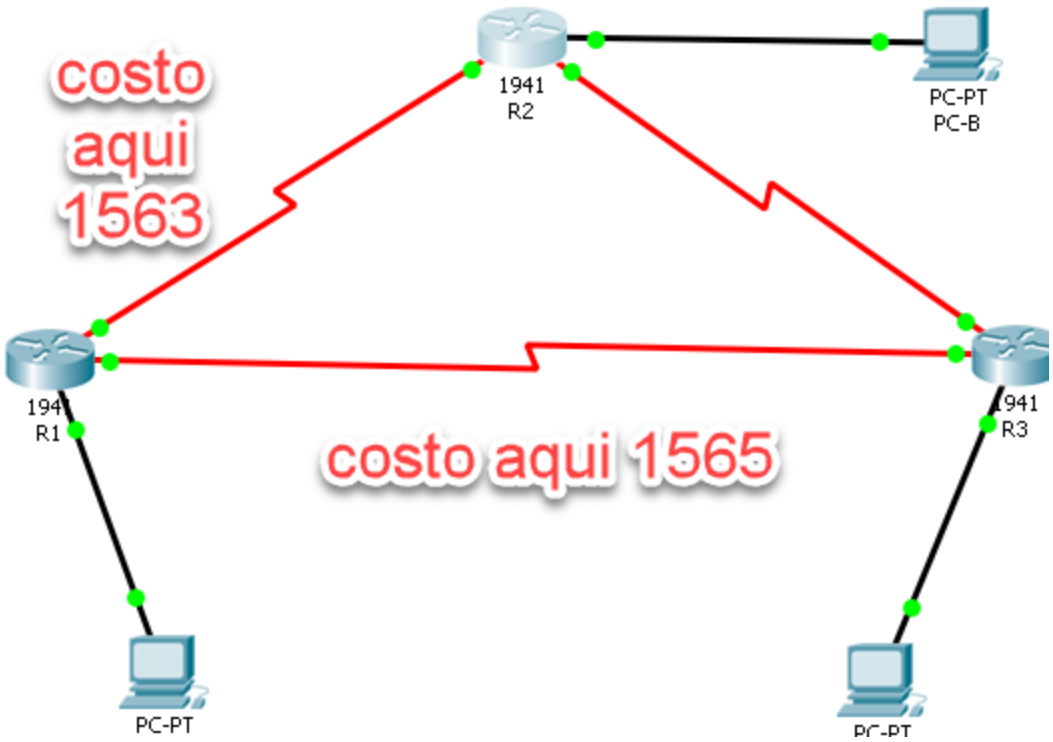
```
R1#conf t
Enter configuration commands, one per line.  End with CNTI
R1(config)#inter s0/0/1
R1(config-if)#ip os
R1(config-if)#ip ospf c
R1(config-if)#ip ospf cost 1565
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

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.

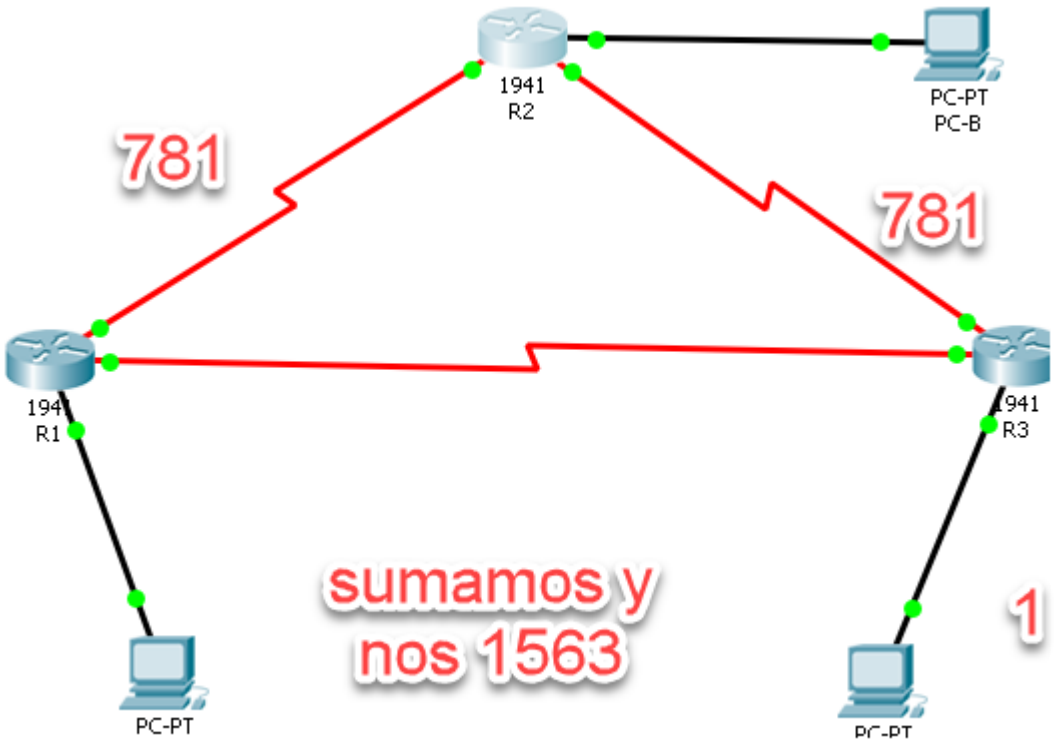
R1# **show ip route ospf**

```
R1#show ip route ospf
O    192.168.2.0 [110/782] via 192.168.12.2, 01:05:33, Serial0/0/0
O    192.168.3.0 [110/1563] via 192.168.12.2, 00:04:45, Serial0/0/0
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:04:45, Serial0/0/0

R1#
```

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


costo
aqui
1563
1941
R2
PC-PT
PC-B
1941
R1
1941
R3
costo aqui 1565
PC-PT

Entonces


781
781
1941
R2
PC-PT
PC-B
1941
R1
1941
R3
sumamos y
nos 1563
1
PC-PT

**REFLEXION**

**4. ¿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 múltiples si la ID del router está asociado a una interfaz activa.

**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 cuando se configura una interfaz LAN como pasiva elimina la información de routing OSPF innecesariamente en esa interfaz y a la vez se libera ancho de banda.

**8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3.**

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

**Topología**

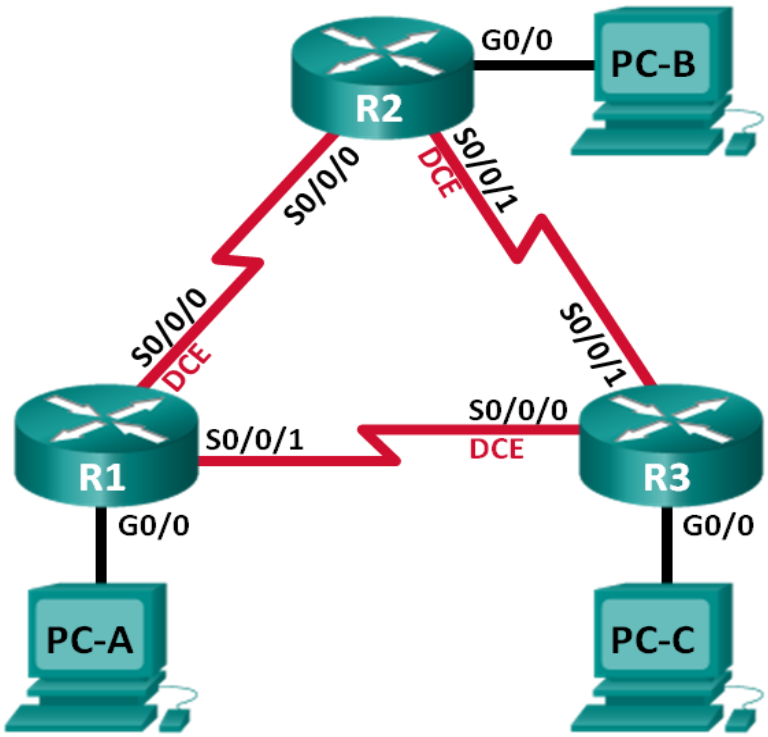
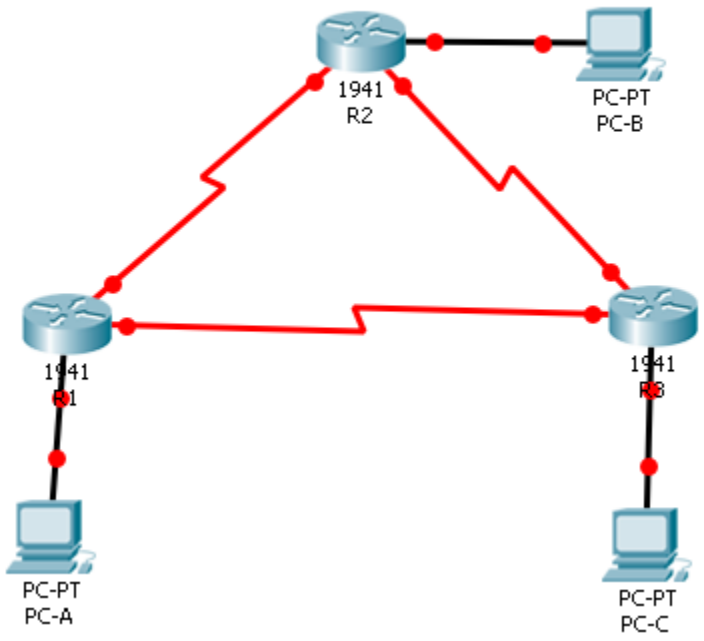



**Tabla de direccionamiento**

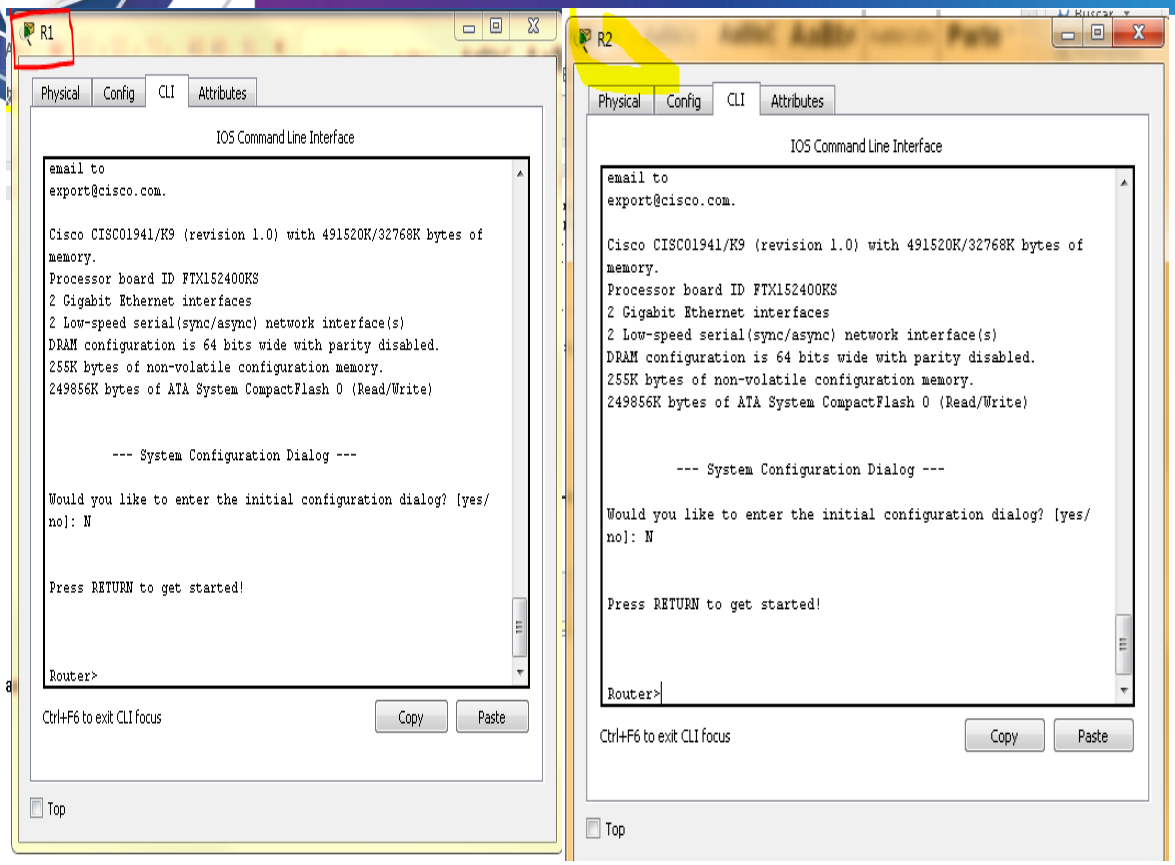
| Dispositivo | Interfaz | Dirección IPv6 | Gateway predeterminado |
|---|---|---|---|
| R1 | G0/0 | 2001:DB8:ACAD:A::1/64<br>FE80::1 link-local | No aplicable |
| | S0/0/0 (DCE) | 2001:DB8:ACAD:12::1/64<br>FE80::1 link-local | No aplicable |
| | S0/0/1 | 2001:DB8:ACAD:13::1/64<br>FE80::1 link-local | 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 |

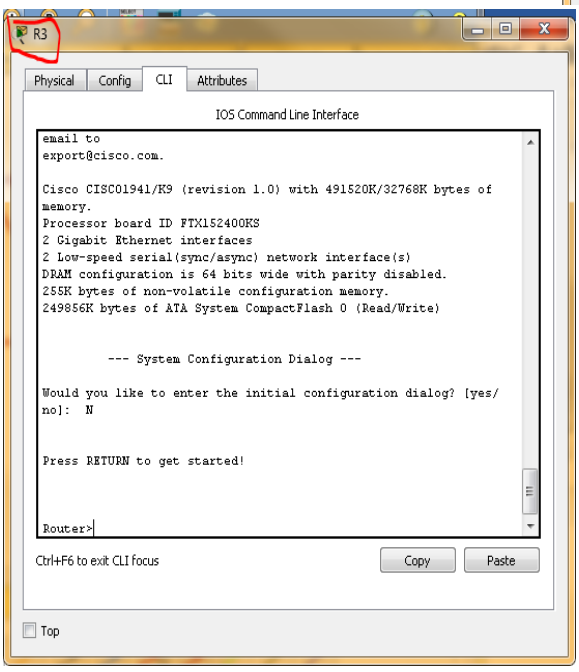
**Part 7:** **Armar la red y configurar los parámetros básicos de los dispositivos**

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



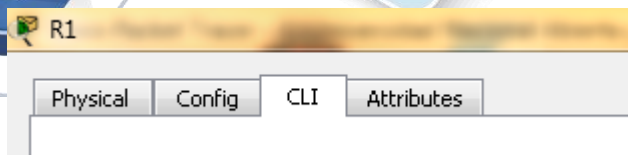

**Step 2:** **inicializar y volver a cargar los routers según sea necesario.**



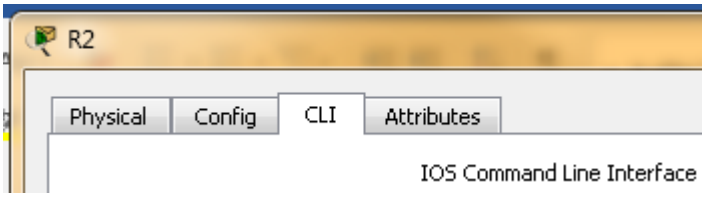




**Step 3: configurar los parámetros básicos para cada router.**

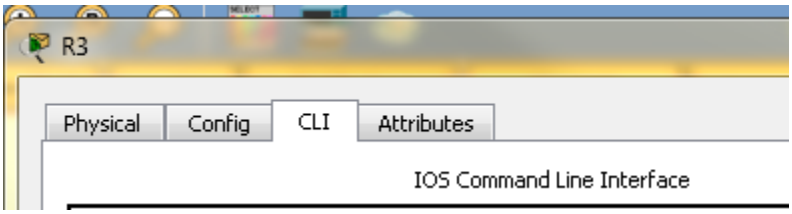
a. Desactive la búsqueda del DNS.




```
Router(config)#no ip domain-lookup
```

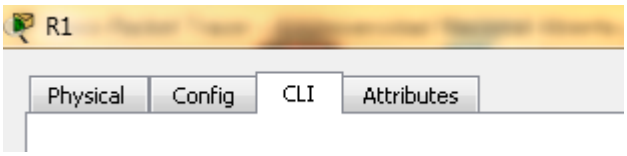



```
Router(config)#no ip domain-lookup
```

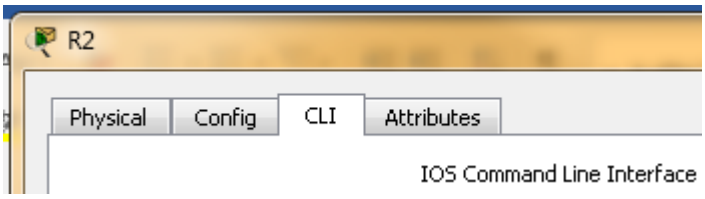



```
Router(config)#no ip domain-lookup
```

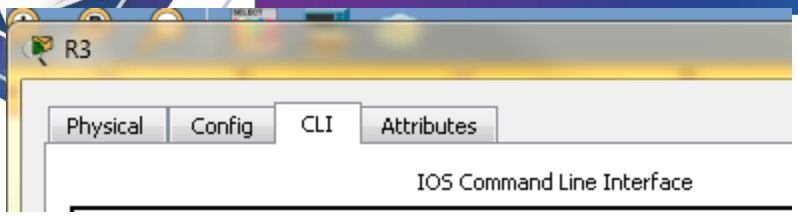
b. Configure el nombre del dispositivo como se muestra en la topología.




```
Router(config)#hostname R1
```

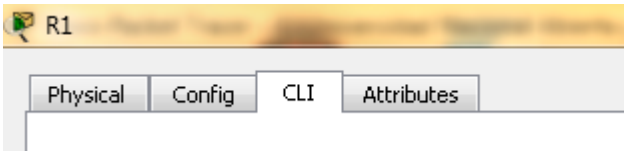



```
Router(config)#hostname R2
```

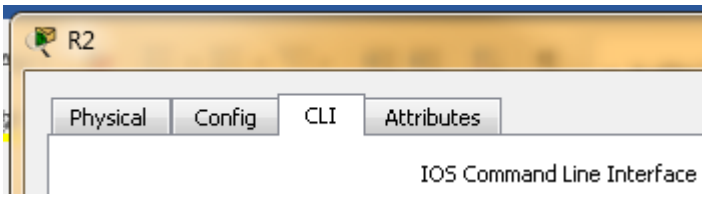



```
Router(config)#hostname R3
```

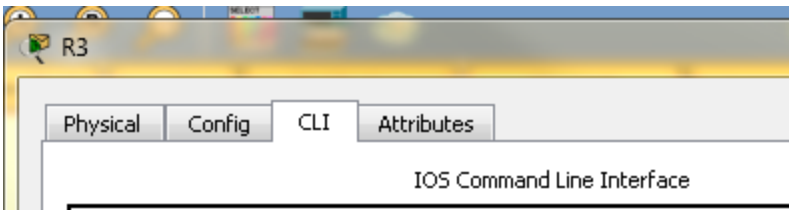
c. Asigne **class** como la contraseña del modo EXEC privilegiado.




```
R1(config)#enable secret class
```

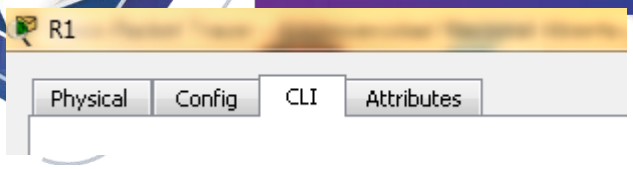



```
R2(config)#enable secret class
```

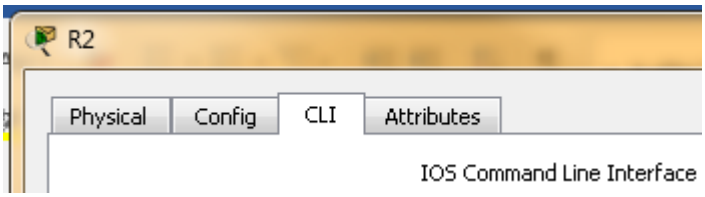



```
R3(config)#ENAble secret class
```

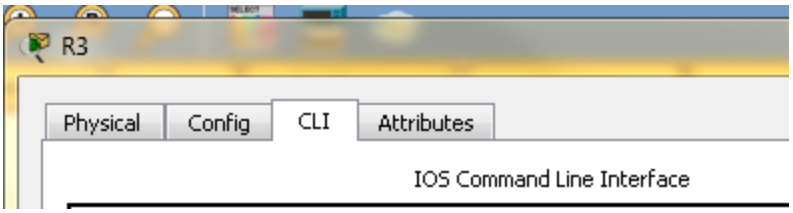
d. Asigne **cisco** como la contraseña de vty.




```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login

R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
```

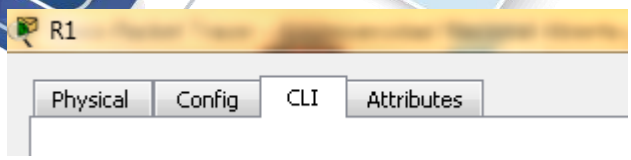



```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#end

R2(config)#line vty 0 15
R2(config-line)#passw
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#
```

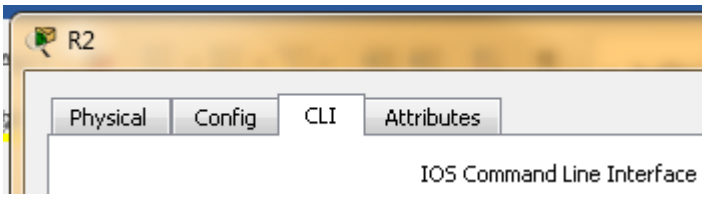



```
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#end

R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#
```

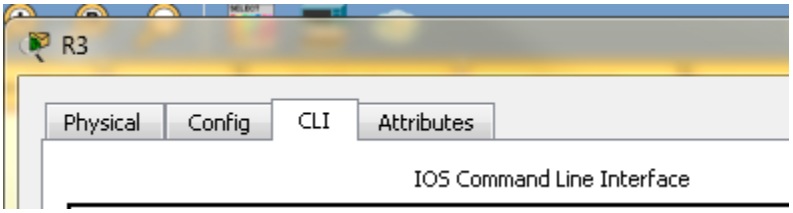
e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.




```
R1(config-line)#banner motd #Welcome authorized Users!#
```

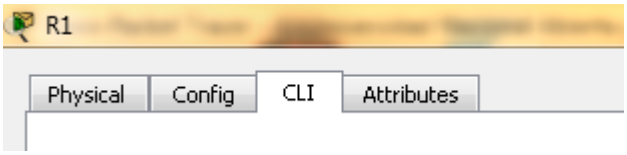



```
R2(config-line)#banner motd #Unauthorized access Prohibited!#
```

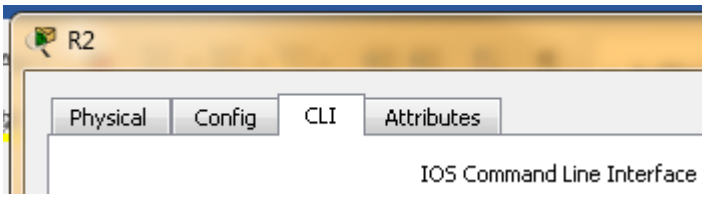



```
R3(config-line)#banner motd #Unauthorized access prohibited!#
```

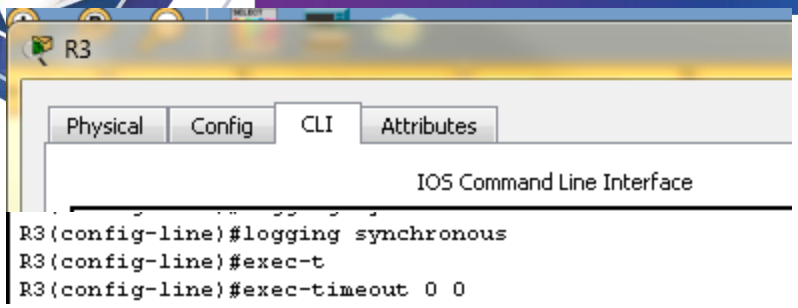
f. Configure **logging synchronous** para la línea de consola.



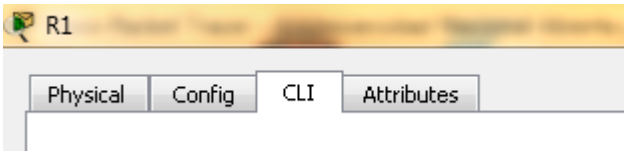

```
R1(config-line)#loggin synchronous
```

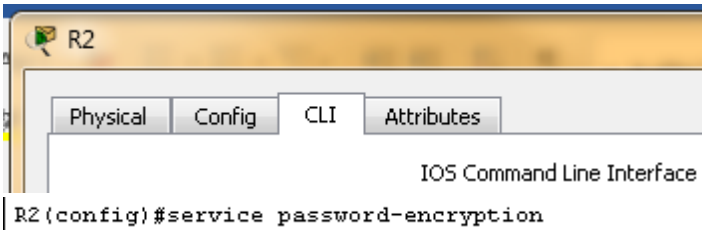


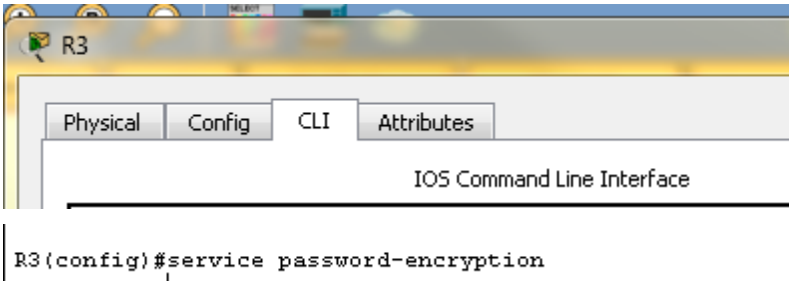

```
R2(config-line)#logging synchronous
R2(config-line)#exec
R2(config-line)#exec-timeout 0 0
```




g. Cifre las contraseñas de texto no cifrado.

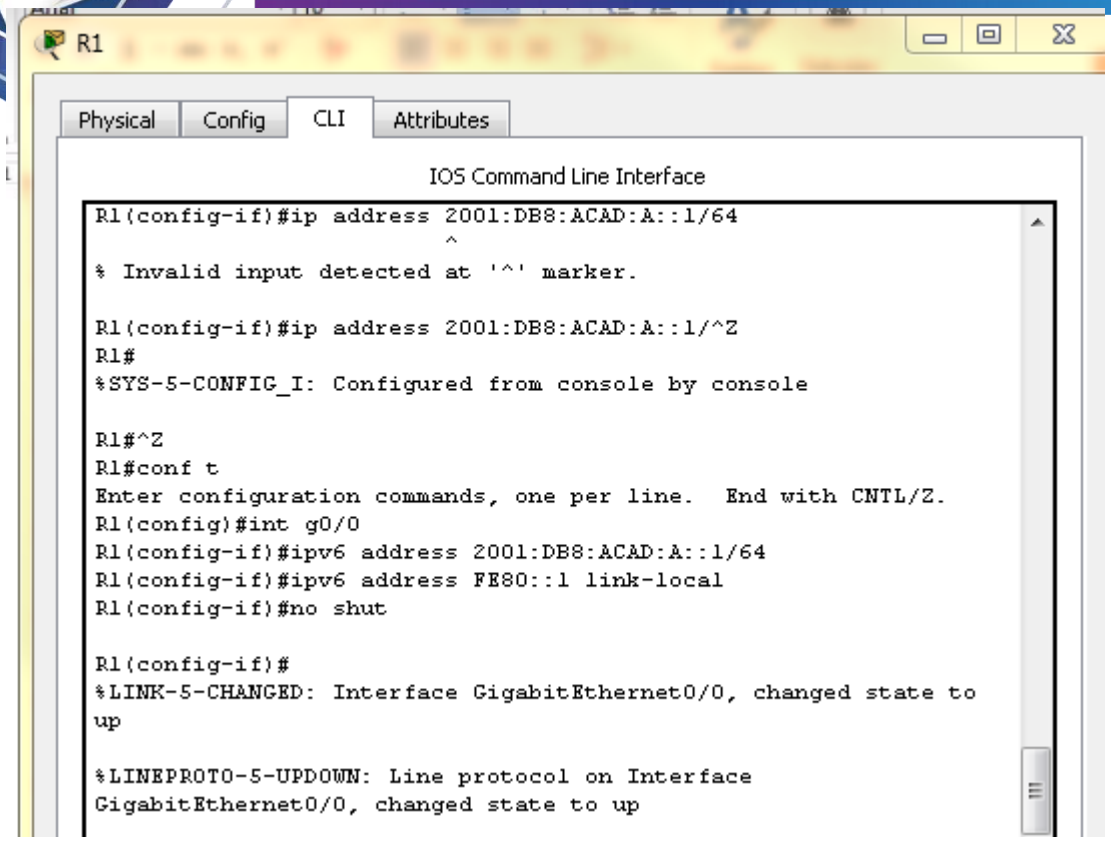


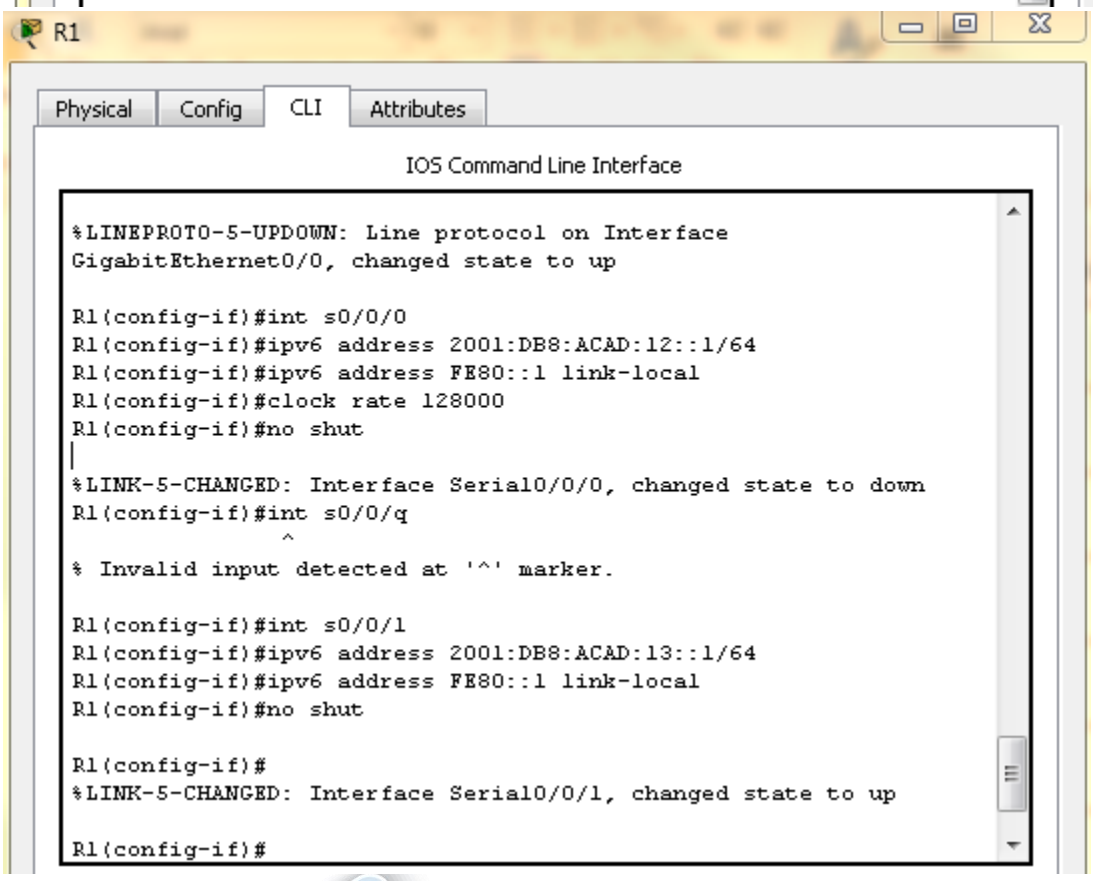



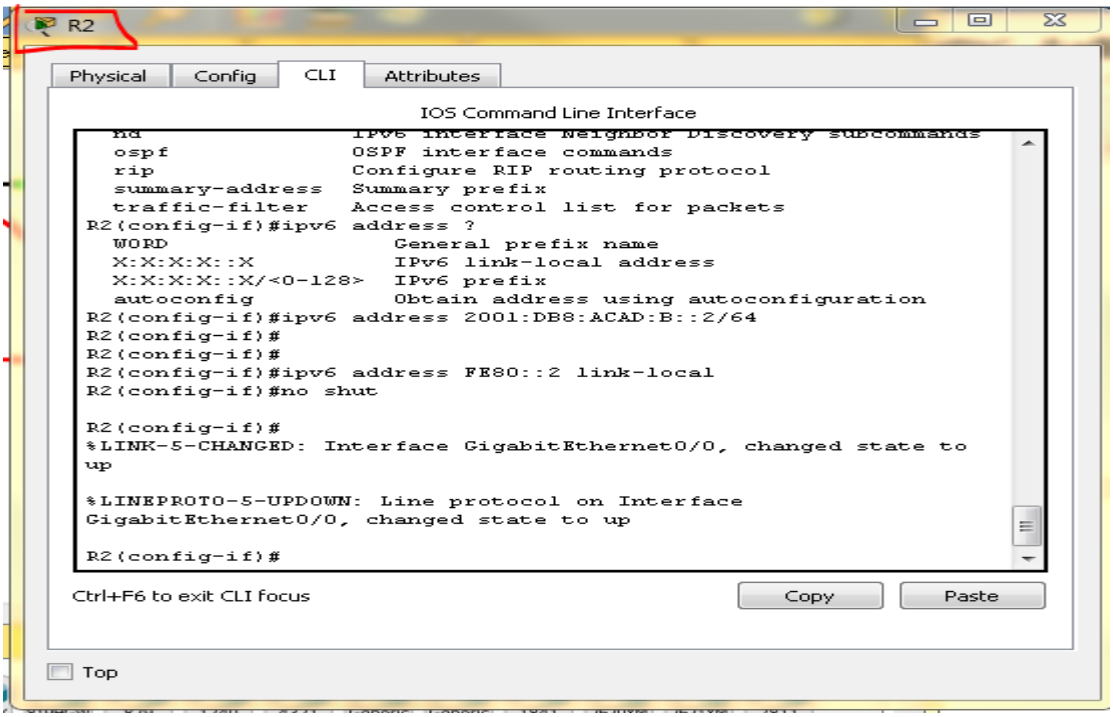

h. Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.

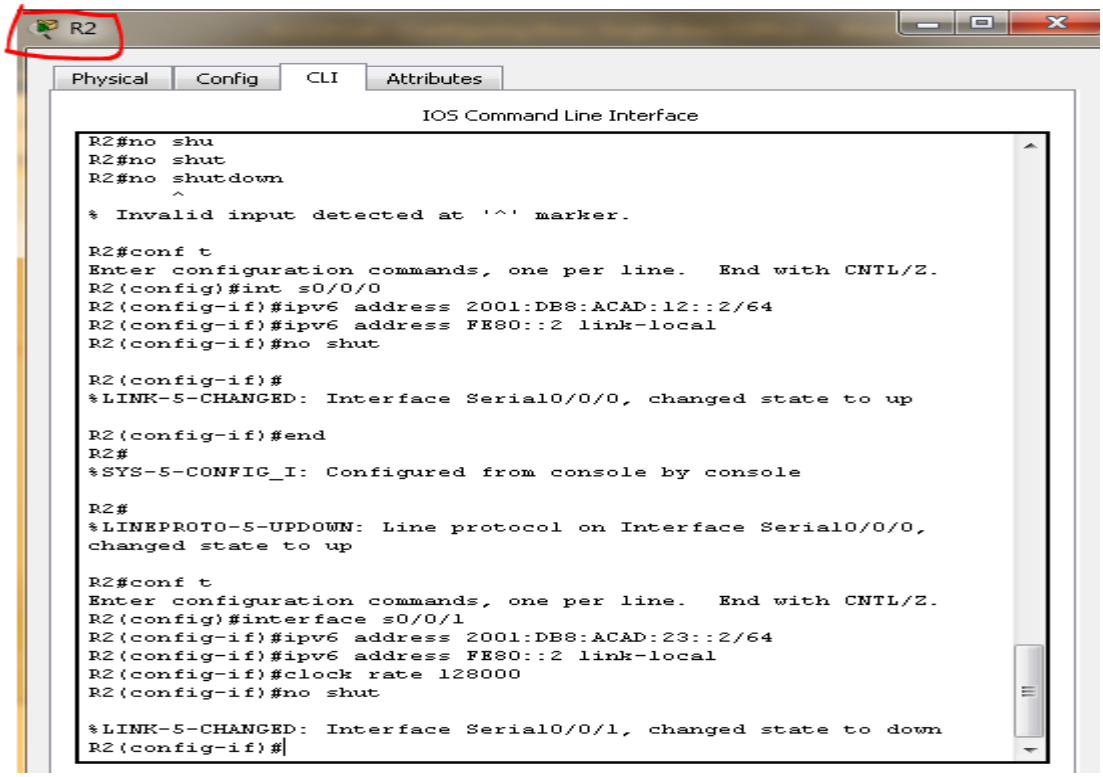
Router 1


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1(config-if)#ip address 2001:DB8:ACAD:A::1/64
^
% Invalid input detected at '^' marker.
R1(config-if)#ip address 2001:DB8:ACAD:A::1/^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#^Z
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut
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

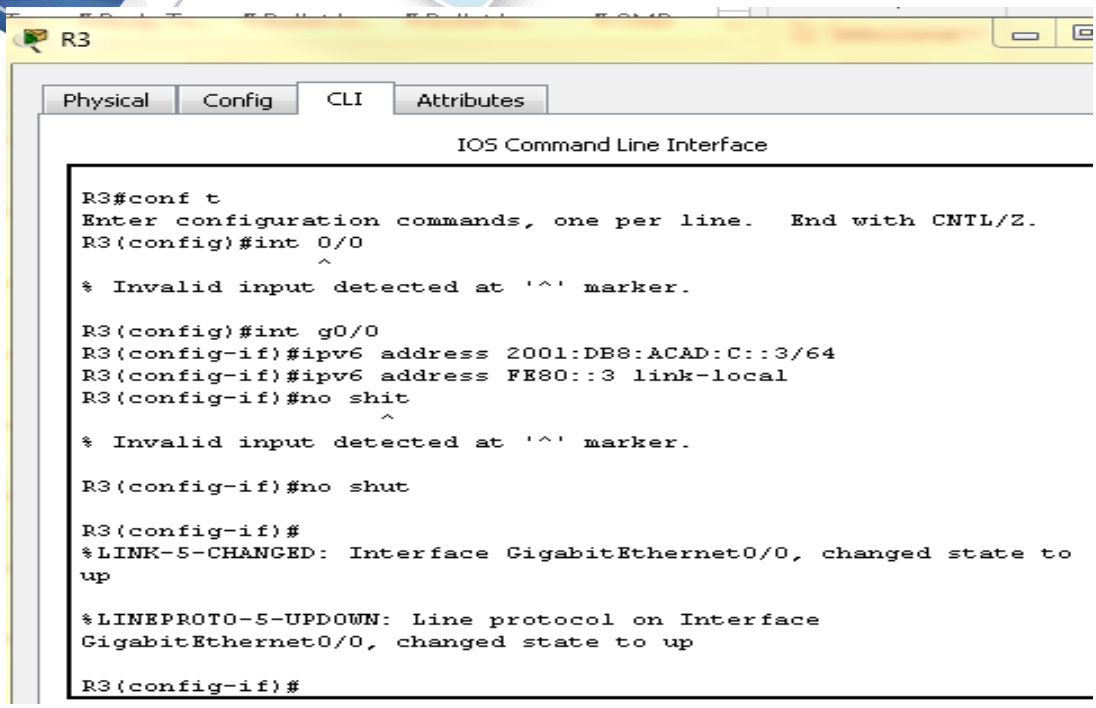

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R1(config-if)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#clock rate 128000
R1(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#int s0/0/q
^
% Invalid input detected at '^' marker.
R1(config-if)#int s0/0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:13::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
R1(config-if)#

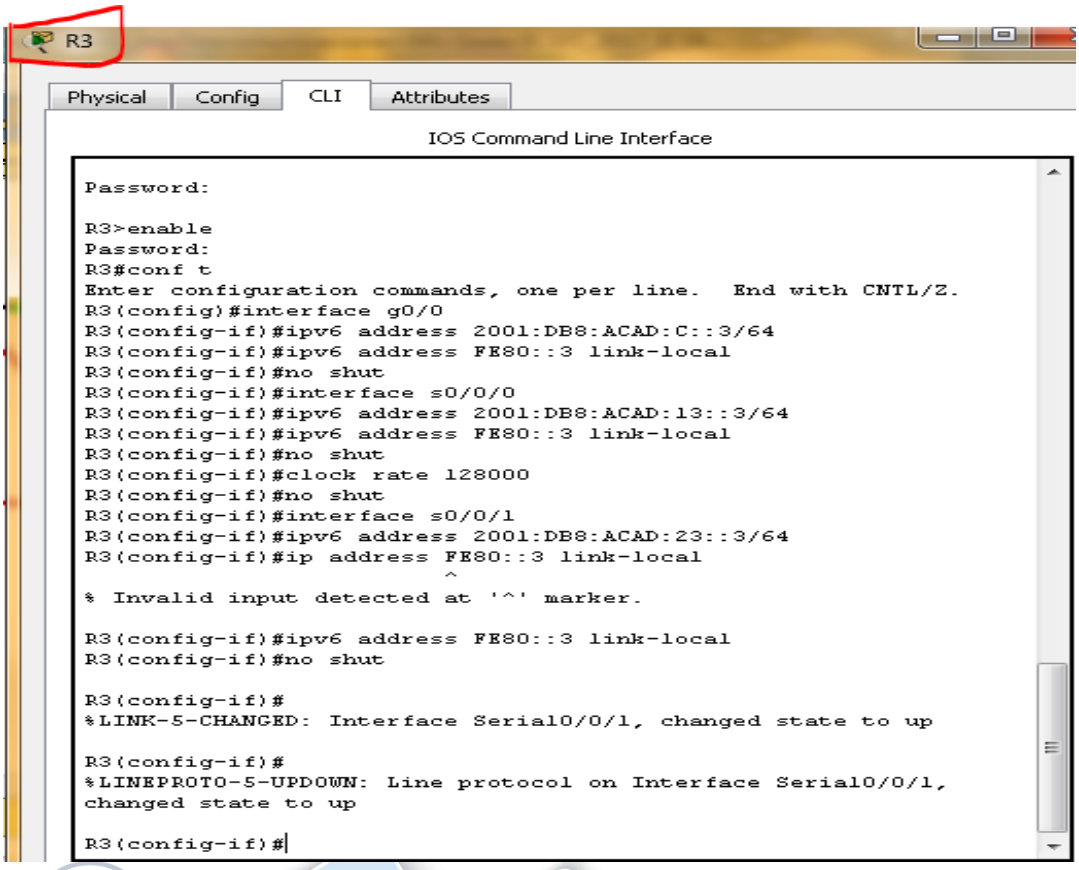
Router 2


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
nd IPv6 interface Neighbor Discovery subcommands
ospf OSPF interface commands
rip Configure RIP routing protocol
summary-address Summary prefix
traffic-filter Access control list for packets
R2(config-if)#ipv6 address ?
WORD General prefix name
X:X:X:X::X IPv6 link-local address
X:X:X:X::X/<0-128> IPv6 prefix
autoconfig Obtain address using autoconfiguration
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#
R2(config-if)#
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2#no shu
R2#no shut
R2#no shutdown
^
% Invalid input detected at '^' marker.
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface s0/0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#clock rate 128000
R2(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#

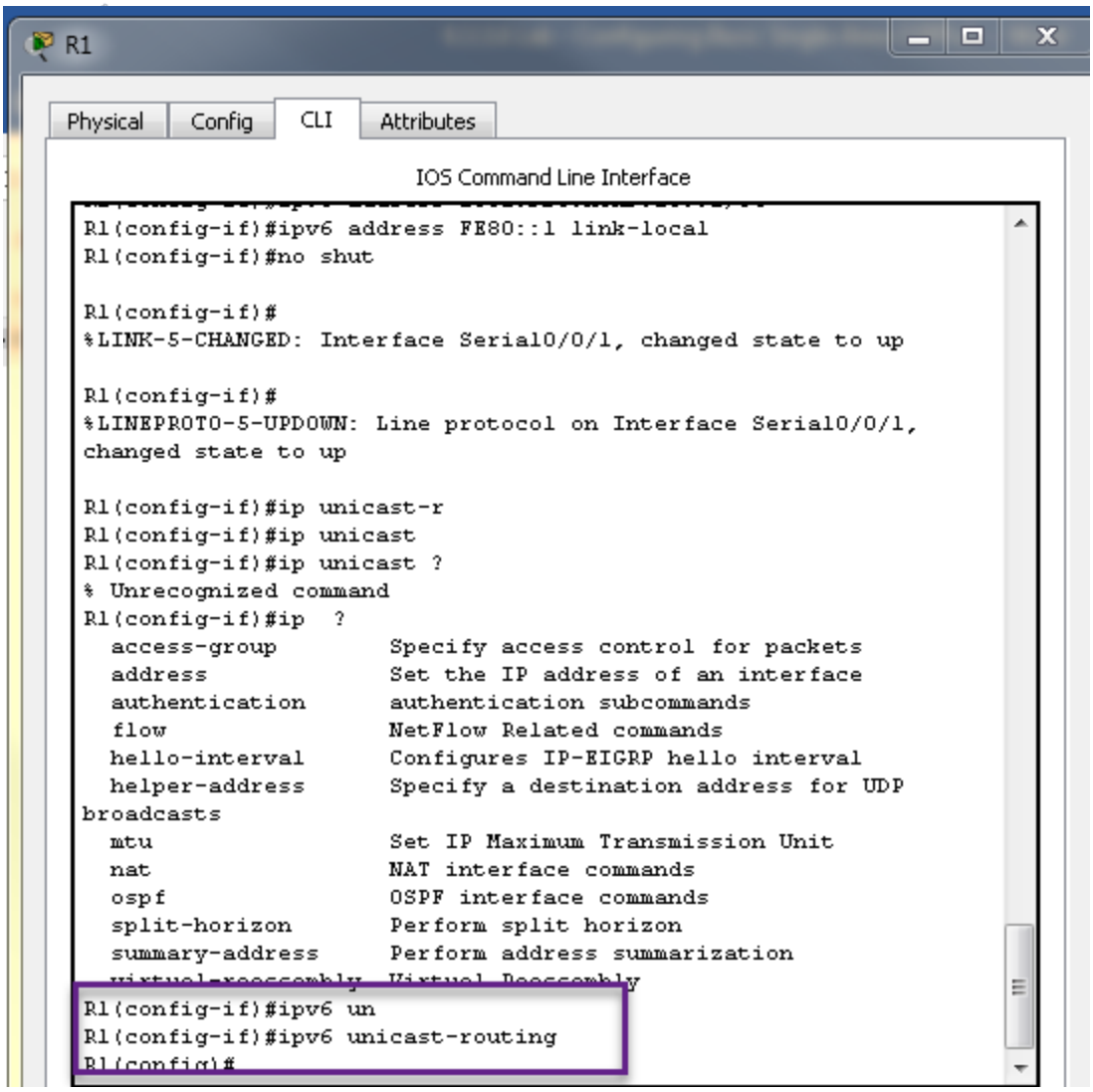
ROUTER R3


R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int 0/0
^
% Invalid input detected at '^' marker.
R3(config)#int g0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shit
^
% Invalid input detected at '^' marker.
R3(config-if)#no shut
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)#

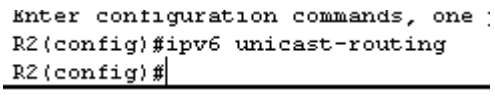

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface g0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shut
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:13::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shut
R3(config-if)#clock rate 128000
R3(config-if)#no shut
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ip address FE80::3 link-local
^
% Invalid input detected at '^' marker.
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shut
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
R3(config-if)#

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

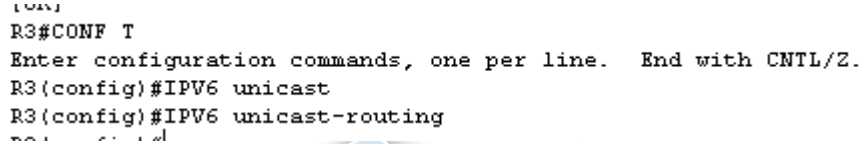
**ROUTER 1**




ROUTER 2




ROUTER 3

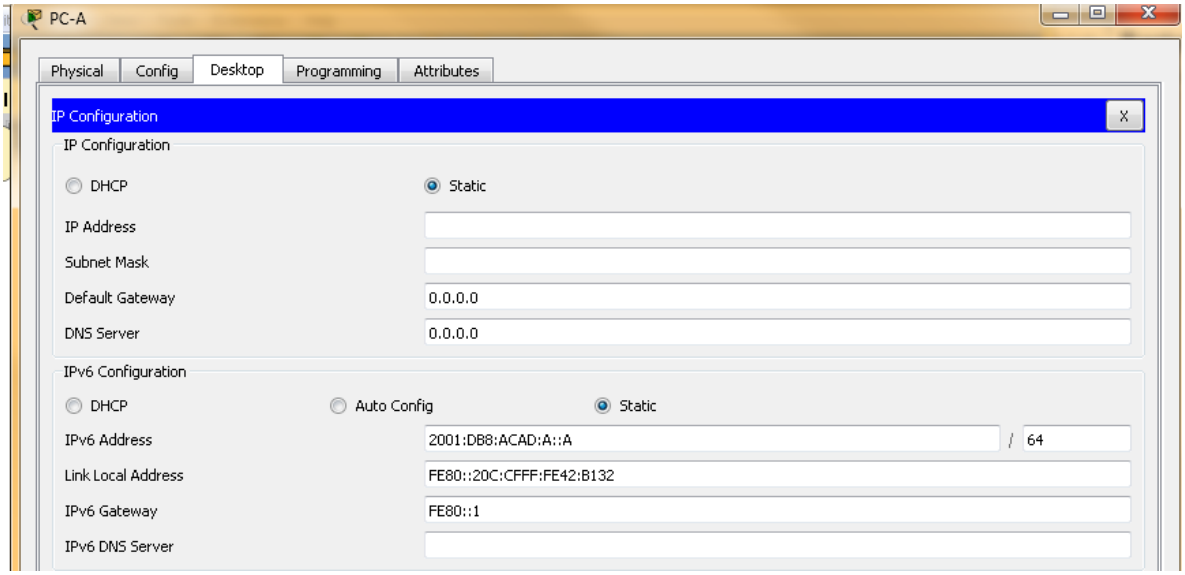


j. Copie la configuración en ejecución en la configuración de inicio

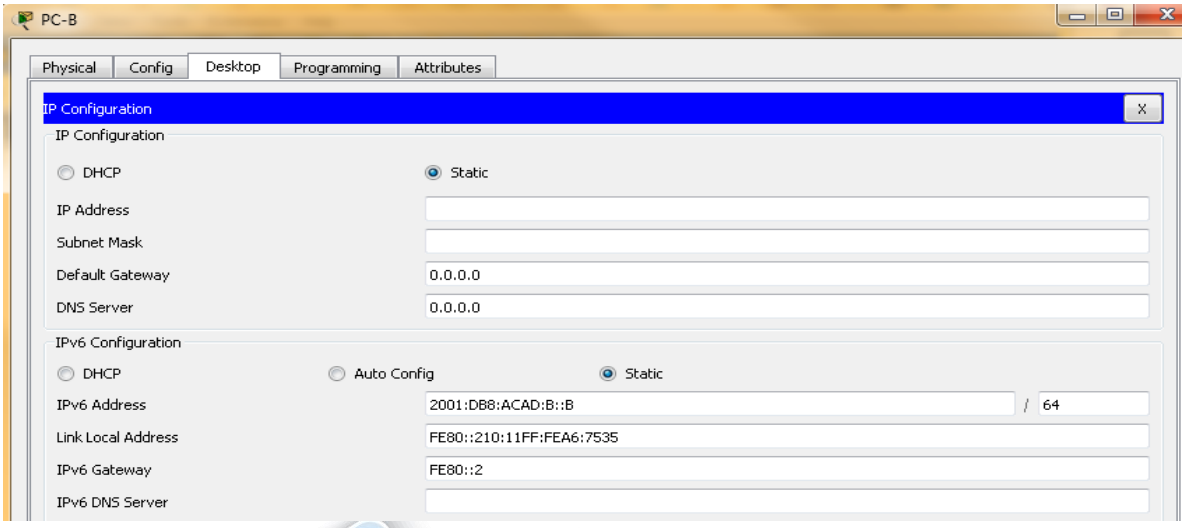
```
%SYS-5-CONFIG_I: Configured from

R2#WR
Building configuration...
[OK]
R2#
```

**Step 4: configurar los equipos host.**

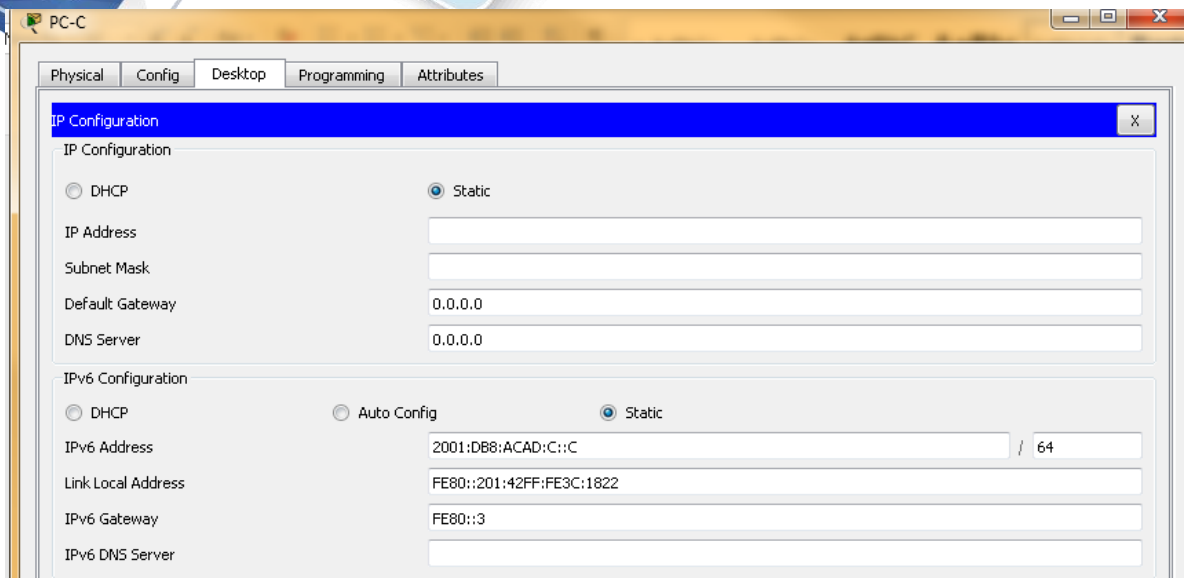
Configuración tarjeta PC-A




Configuracion tarjeta PC-B



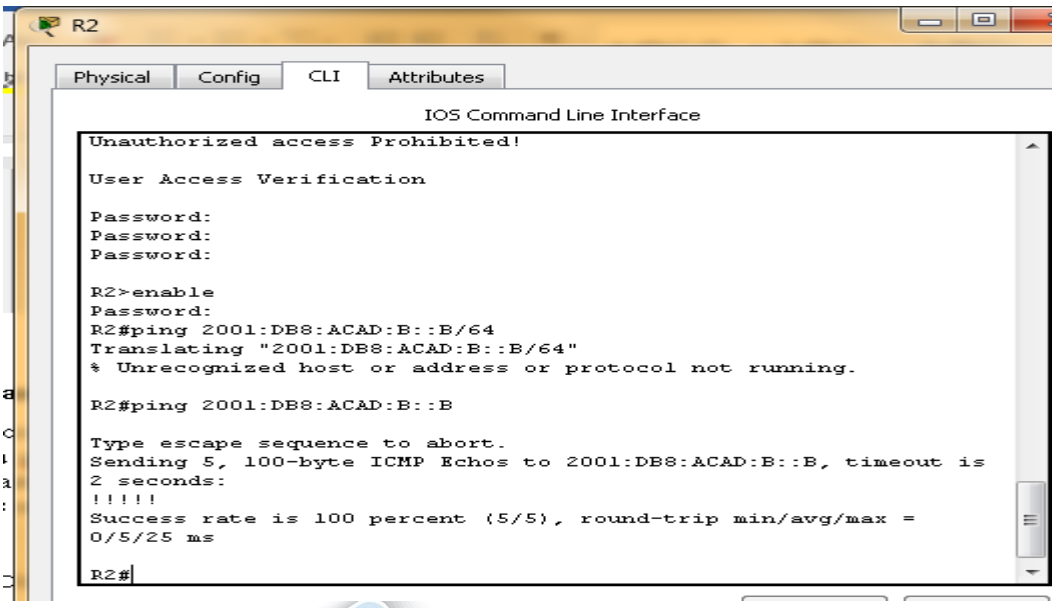
Configuración tarjeta PC-C




**Step 5: Probar la conectividad.**

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

**ROUTER 2 A PC-B**



**ROUTER 2 A SERIAL 0/0/0 DE R1**

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

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::1, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9
ms
```

**ROUTER 2 A SERIAL 0/0/1 DE R3**

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

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::3, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8
ms

R2#
```

**Part 8: configurar el routing OSPFv3**

**Step 1: asignar ID a los routers.**

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

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

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

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

**Router 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)#
```

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

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

```
Enter configuration commands, one pe
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1
id,please configure manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#
```

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

Router 2

```
R2#conf t
Enter configuration commands, one per line.  End with
R2(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a r
id,please configure manually
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#
```

Router 3

```
Password:
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-
id,please configure manually
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#
```

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

R2# **show ipv6 ospf**

Routing Process "ospfv3 1" with ID 2.2.2.2

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

Router is not originating router-LSAs with maximum metric

<Output Omitted>

**Router 2**

```
[OK]
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
```

**Router 3**

```
[OK]
R3#show ipv6 ospf
 Routing Process "ospfv3 1" with ID 3.3.3.3
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 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
```

**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.**

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

R1(config)# interface g0/0

R1(config-if)# ipv6 ospf 1 area 0

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

R1(config-if)# ipv6 ospf 1 area 0

R1(config-if)# interface s0/0/1

R1(config-if)# ipv6 ospf 1 area 0

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

**Router 1**

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

**Router 2**

```
R2(config)#interface 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)#
01:20:12: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

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

**Router 3**

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
01:30:09: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
01:30:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done

R3(config-if)#
```

b. ver mensajes de adyacencia de vecino.

R1#

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

R1#

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

**Router 1**

```
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#
01:20:12: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0
from LOADING to FULL, Loading Done

R1(config-if)#
01:30:09: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done
```

**Router 2**

```
R2(config-if)#
01:20:12: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

R2(config-if)#int s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
01:30:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done
```

**Router 3**

```
R3(config-if)#
01:30:09: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
01:30:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done
```

**Step 2: 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)

**Router 1**

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

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:32    3               Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:30    3               Serial0/0/1
R1#
```

**Router 2**

```
[OK]
R2#show ipv6 osp
R2#show ipv6 ospf ne
R2#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
1.1.1.1           0   FULL/  -        00:00:39    3               Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:39    4               Serial0/0/1
R2#
```

**Router 3**

```
R3#show ipv6 os
R3#show ipv6 ospf ne
R3#show ipv6 ospf neighbor

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

**Step 3: verificar la configuración del protocolo OSPFv3.**

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

R1# **show ipv6 protocols**

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "ospf 1"

Router ID 1.1.1.1

Number of areas: 1 normal, 0 stub, 0 nssa

Interfaces (Area 0):

Serial0/0/1

Serial0/0/0

GigabitEthernet0/0

Redistribution:

None

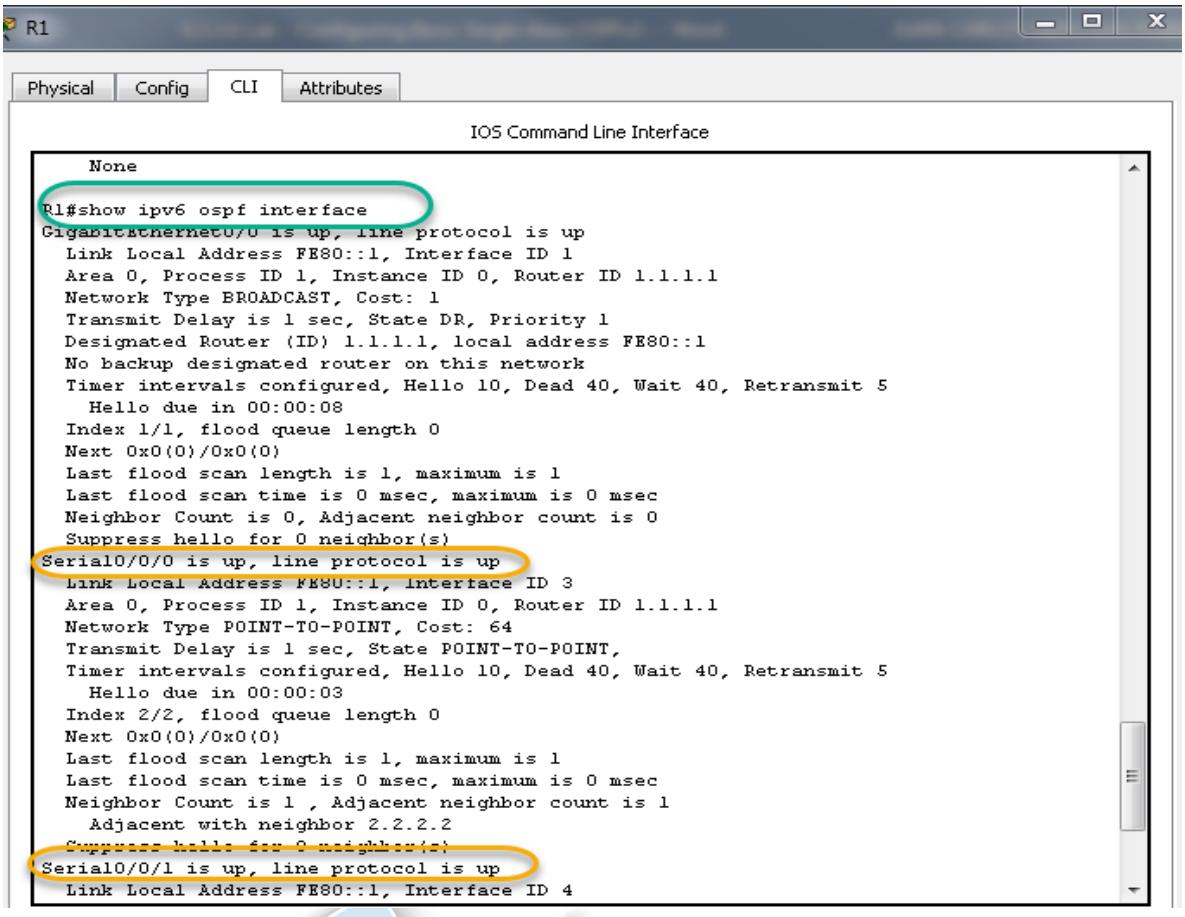
```
R1#show ipv6 prot
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
```

**Step 4: verificar las interfaces OSPFv3.**

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

R1# show ipv6 ospf interface
Serial0/0/1 is up, line protocol is up
Link Local Address FE80::1, Interface ID 7
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Graceful restart helper support enabled
Index 1/3/3, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 3.3.3.3
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 6
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00 Graceful restart helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1

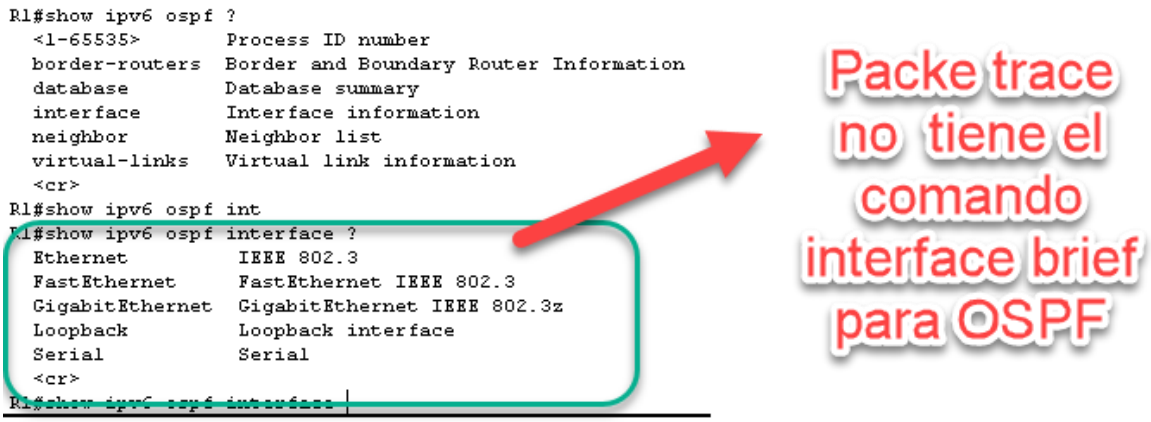
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)



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

R1# **show ipv6 ospf interface brief**

| Interface | PID | Area | Intf ID | Cost | State | Nbrs F/C |
|---|---|---|---|---|---|---|
| Se0/0/1 | 1 | 0 | 7 | 64 | P2P | 1/1 |
| Se0/0/0 | 1 | 0 | 6 | 64 | P2P | 1/1 |
| Gi0/0 | | | | | | |




**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 - default - 10 entries

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

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

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

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

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

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

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

via FE80::1, Serial0/0/0

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

via GigabitEthernet0/0, directly connected

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

via GigabitEthernet0/0, receive

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

via FE80::3, Serial0/0/1

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

via Serial0/0/0, directly connected

L 2001:DB8:ACAD:12::2/128 [0/0]

via Serial0/0/0, receive

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

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

C 2001:DB8:ACAD:23::/64 [0/0]

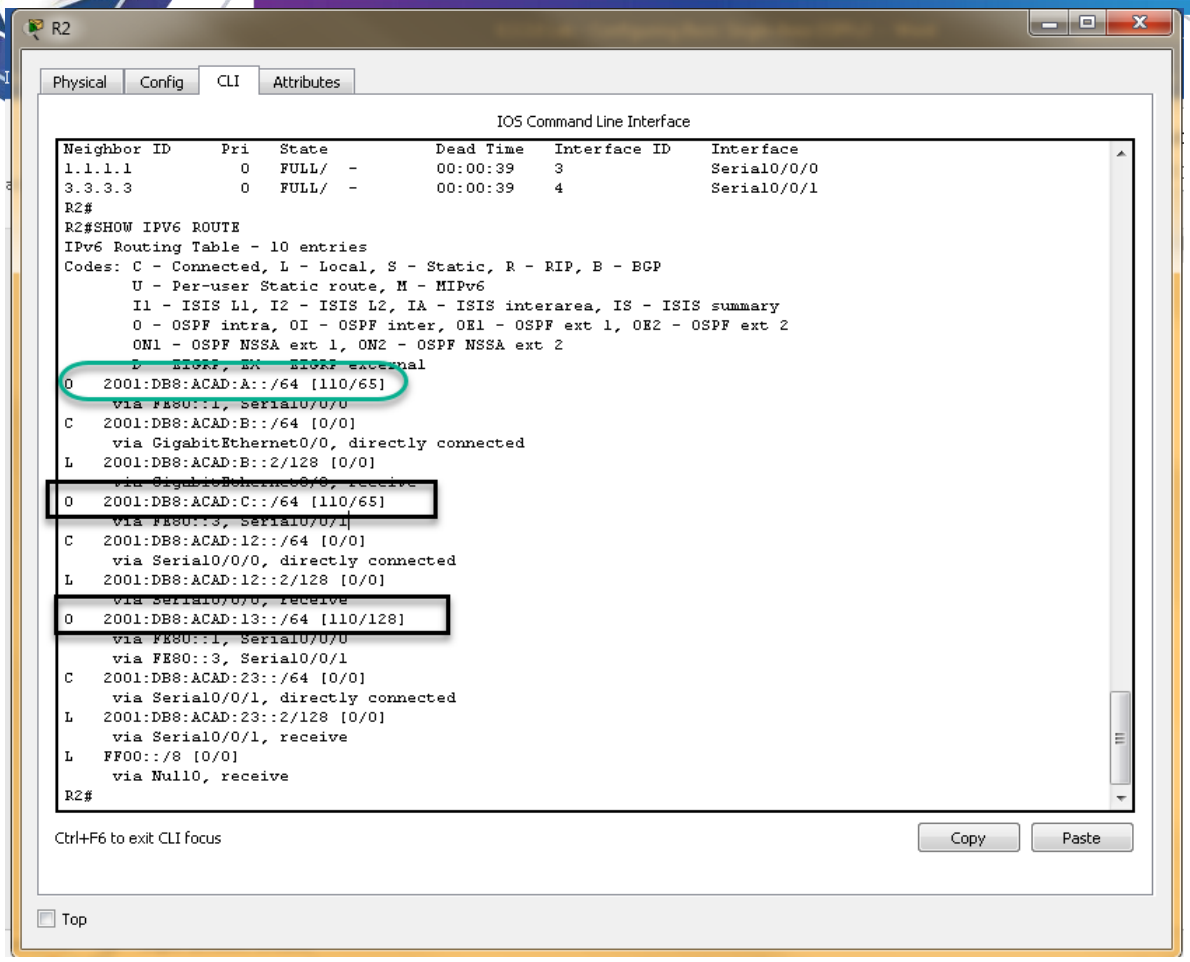
via Serial0/0/1, directly connected

L 2001:DB8:ACAD:23::2/128 [0/0]

via Serial0/0/1, receive

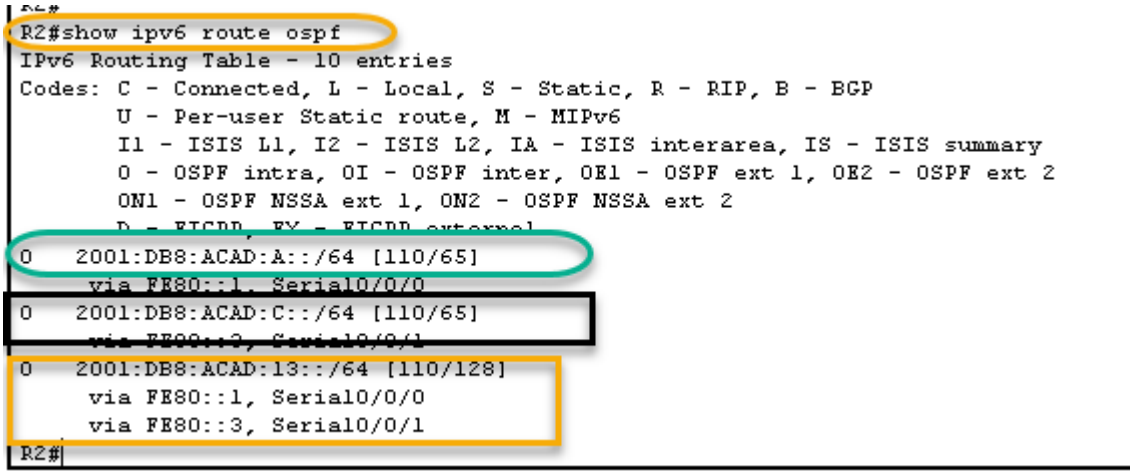
L FF00::/8 [0/0]

via Null0, receive




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

**Show ipv6 route ospf**



**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.

**PC-A a PC-B**

```
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:ACAD:B::B

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

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 4ms

C:\>
```

**PC-A PC-C**

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

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\>
```

**Parte 3: configurar las interfaces pasivas de OSPFv3**

El comando passive-interface evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. En la parte 3, utilizará el comando passive-interface para configurar una única interfaz como pasiva.

También configurará OSPFv3 para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas

**Paso 1: configurar una interfaz pasiva.**

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

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

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

```
R1#show ip ospf interface g0/0
%OSPF: OSPF not enabled on GigabitEthernet0/0
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

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

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

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

```
  Suppress hello for 0 neighbor(s)
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#
```

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

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

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

```
*Jan 3 3:10:16.1: %SYS-5-CONFIG_I: Configured from console by console

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

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

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

**Router 2**

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

**Router 3**

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

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

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

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

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
04:48:28: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Interface down or detached

04:48:28: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down:
Interface down or detached

R2(config-rtr)#
```

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

R1# **show ipv6 ospf neighbor**

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

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

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

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           0   FULL/  -        00:00:38    3               Serial0/0/1
R1#
```

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

R2# **show ipv6 ospf interface s0/0/0**
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2, Interface ID 6
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Graceful restart helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 3
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

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

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

```
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]
```

no se encuentra la red 2001:DB8:ACAD:B::/64

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

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

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

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

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
05:01:13: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
```

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

en R1

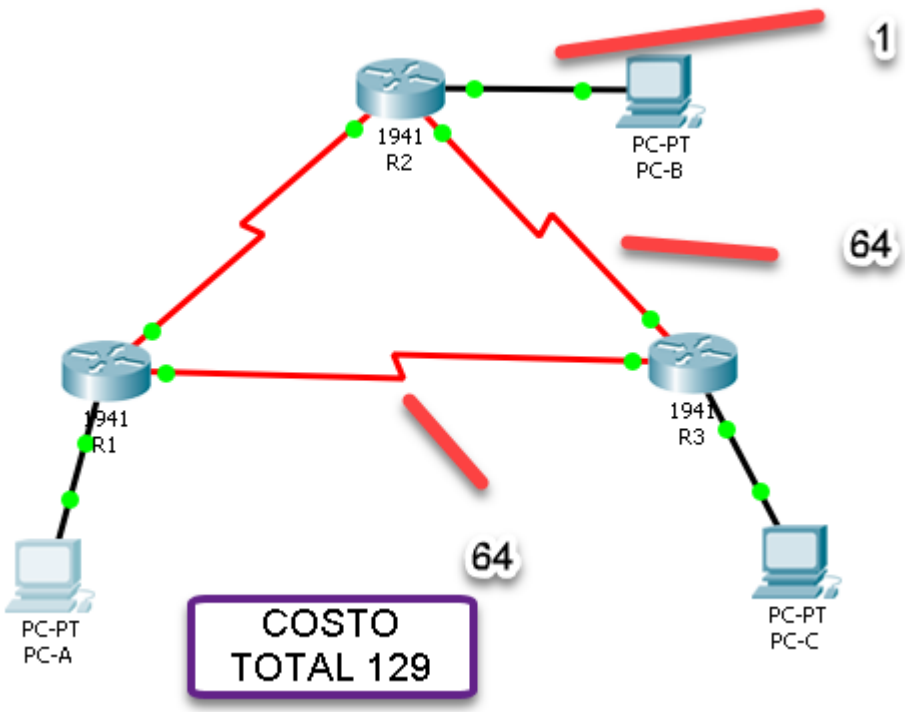
```
R1#show ipv6 route  ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O   2001:DB8:ACAD:B::/64 [110/129]
     via FE80::3, Serial0/0/1
O   2001:DB8:ACAD:C::/64 [110/65]
     via FE80::3, Serial0/0/1
O   2001:DB8:ACAD:23::/64 [110/128]
     via FE80::3, Serial0/0/1

R1#SHOW IPV6 OSPF NEighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           0   FULL/  -        00:00:33    3               Serial0/0/1
R1#
```

En R3

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

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
1.1.1.1           0   FULL/  -        00:00:32    4               Serial0/0/0
2.2.2.2           0   FULL/  -        00:00:32    4               Serial0/0/1
R3#
```

¿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? _EL COSTO ES 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

Todo el trafico de la red 2001:DB8:ACAD:B::/64 de r1 deberá ser enrutado a R3 por la interface serial s0/0/0 de r2 , esta se encuentra confgurada como una interface passiva de tal manera que OSPFV3 no manda información de routeo notificándose a través de esta interfaz, el costo acumulado 129 resulta del trafico de r3 2001:DB8:ACAD:B::/64 este trafico pasa por dos interfaces T1 (1544 MB/S) enlace serial con un costo de 64 cada uno y un interface gigabit 0/0 con un costo de 1

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

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#
05:30:43: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

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

EN ROUTE 2

```
R2#show ipv6 ospf ne
R2#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
1.1.1.1           0   FULL/  -        00:00:38    3               Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:30    4               Serial0/0/1
R2#
```

EN ROUTE 1

```
R1#show ipv6 os
R1#show ipv6 ospf ne
R1#show ipv6 ospf neighbor

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

**Reflexión**

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

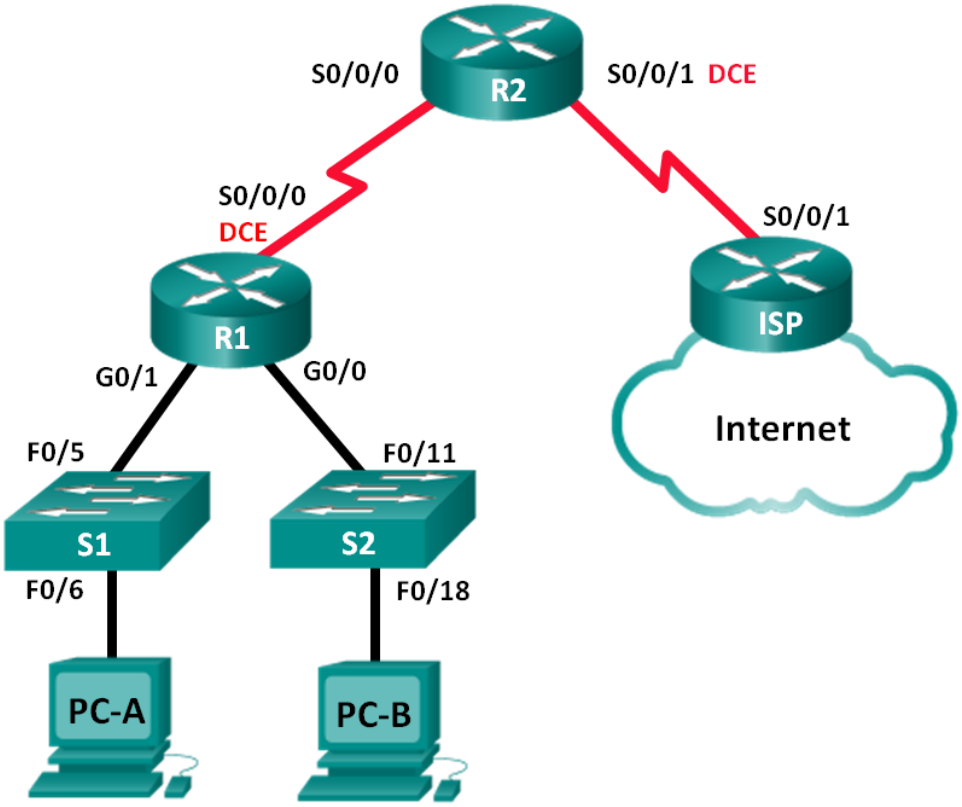
Sí, porque la ID del proceso OSPFv3 se usa solo localmente en el router, y no es necesario que este coincida con la ID del proceso que se usa en los otros routers en el área OSPFv3

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

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

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

### Topología



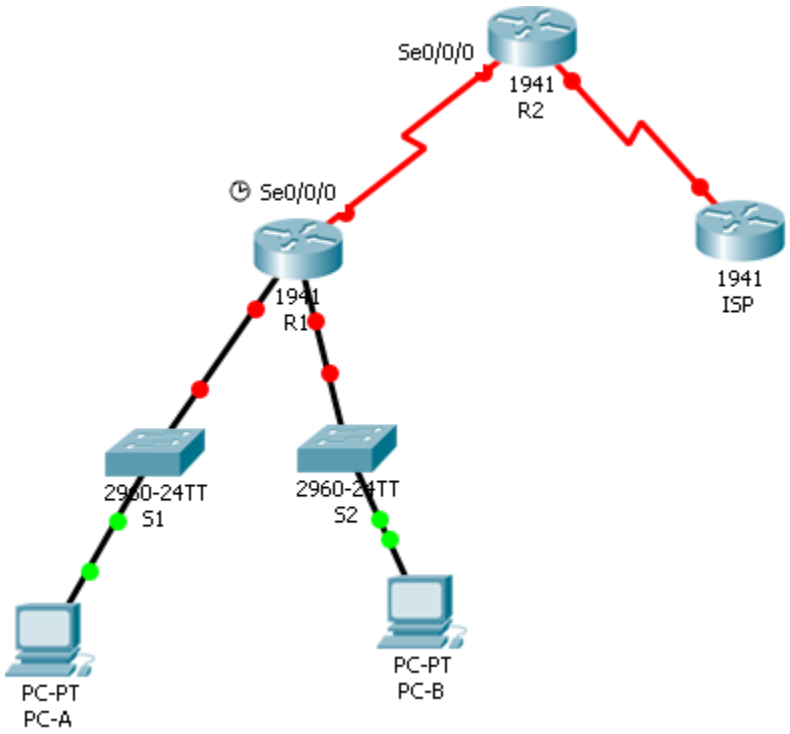

### Tabla de direccionamiento

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

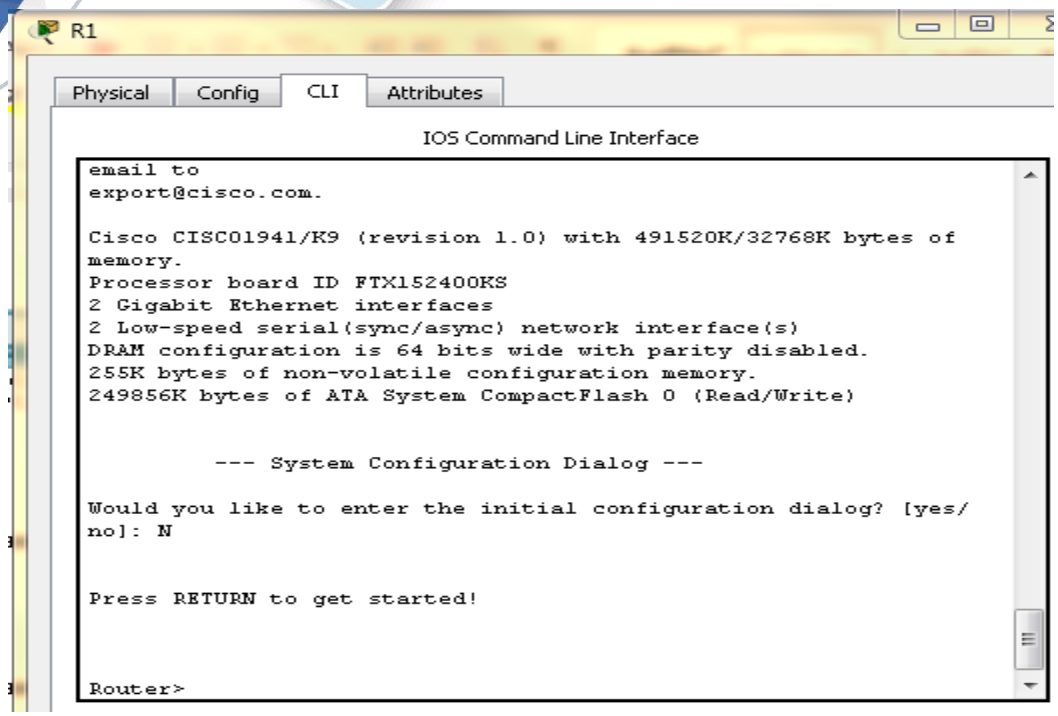
**Parte 1:Armar la red y configurar los parámetros básicos de los dispositivos**

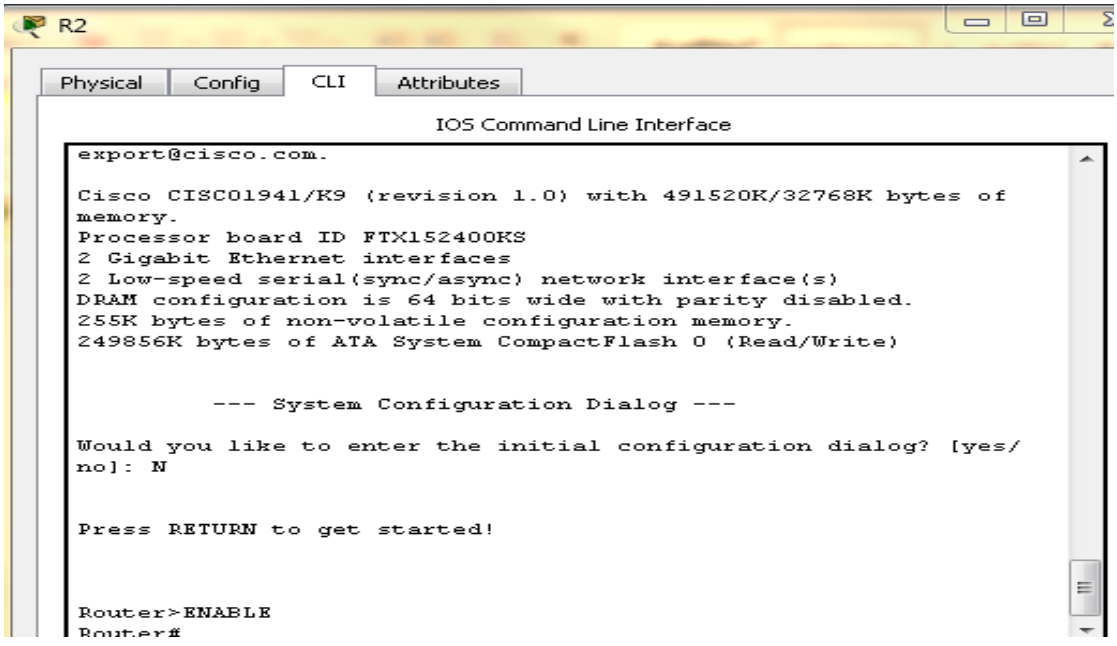
En la parte 1, establecerá la topología de la red y configurará los routers y switches con los parámetros básicos, como las contraseñas y las direcciones IP. Además, configurará los parámetros de IP de las computadoras en la topología.

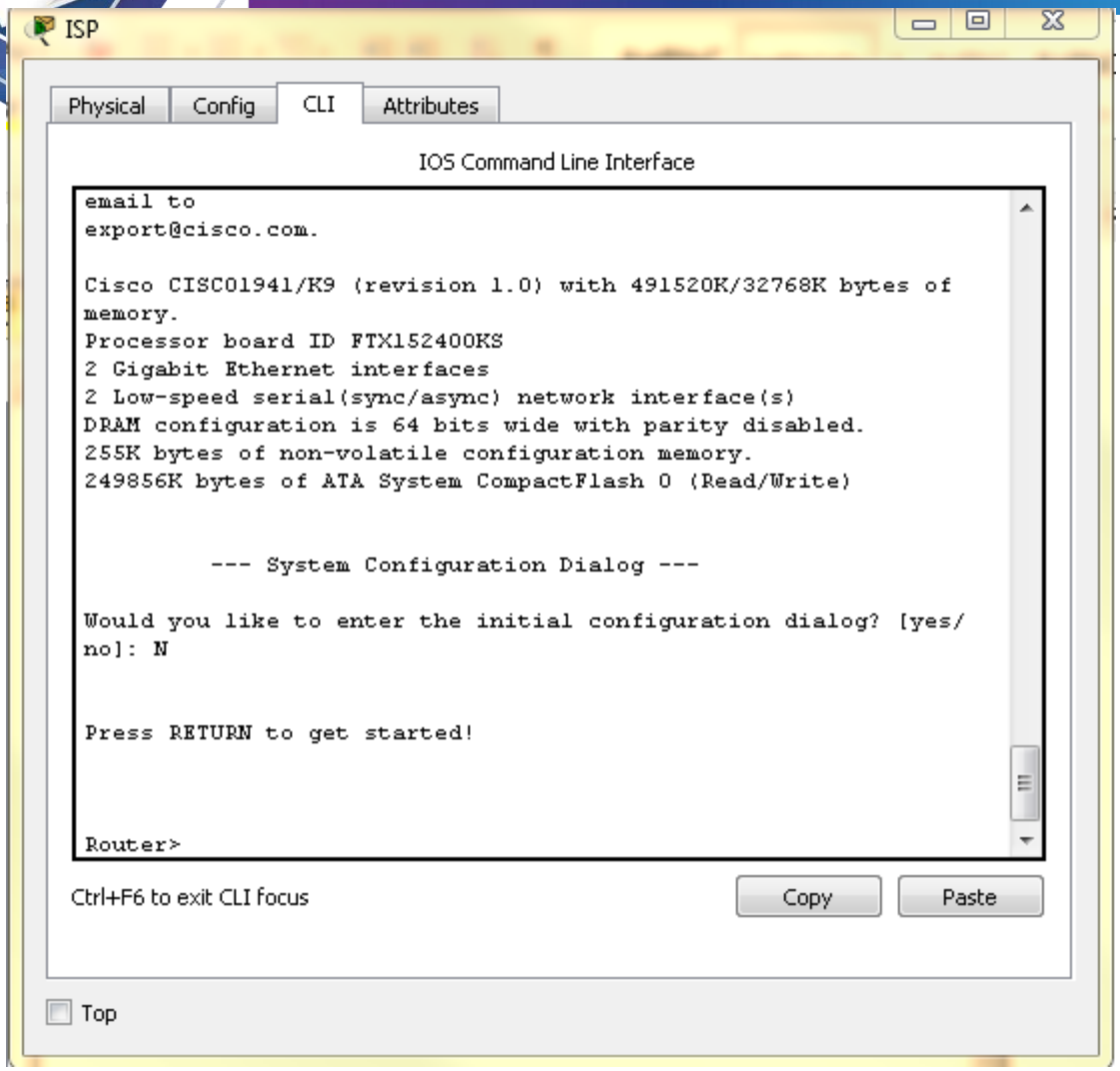
**Paso 1: realizar el cableado de red tal como se muestra en la topología.**




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

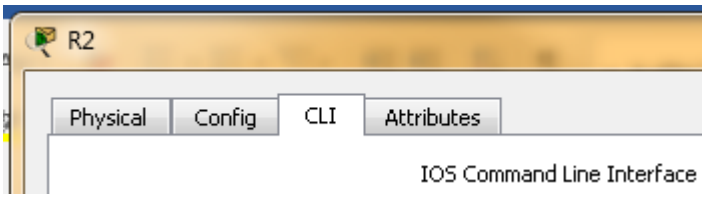

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of
memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/
no]: N
Press RETURN to get started!
Router>


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of
memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
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 ---
Would you like to enter the initial configuration dialog? [yes/
no]: N
Press RETURN to get started!
Router>ENABLE
Router#

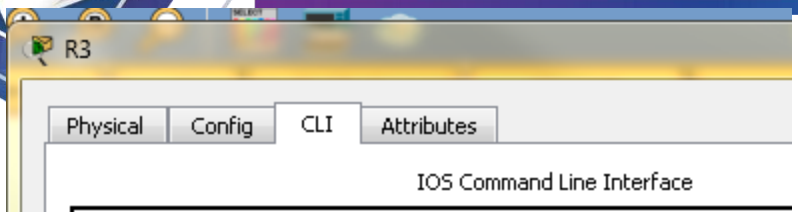



**Paso 3: configurar los parámetros básicos para cada router.**

a. Desactive la búsqueda DNS.


```
Router(config)#no ip domain-lookup
```




```
Router(config)#no ip domain-lookup
```

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

R1

```
Router(config)#hostname R1
R1(config)#WR
           ^
```

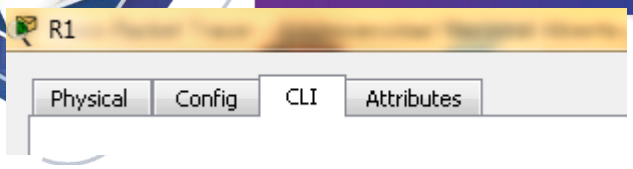
R2

```
Enter configuration commands,
Router(config)#HOSTNAME R2
R2(config)#
```

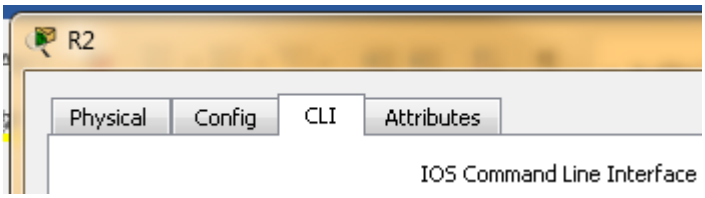
ISP

```
Router#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#HOSTNAME ISP
ISP(config)#
```

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



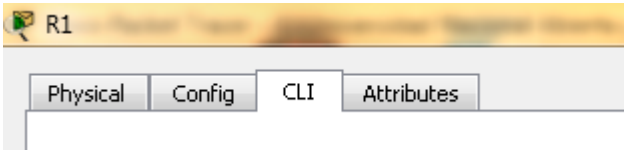

```
R1(config)#enable secret class
```



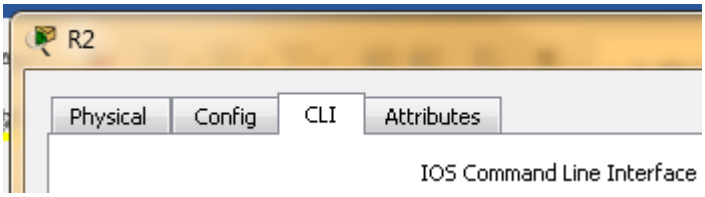

```
R2(config)#enable secret class
```


```
R3(config)#ENAble secret class
```

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




```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login

R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
```



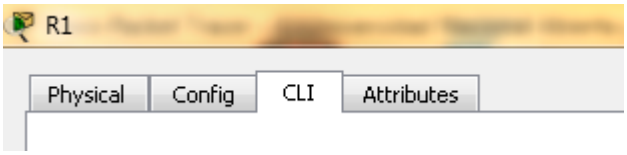
```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#end
```

```
R2(config)#line vty 0 15
R2(config-line)#passw
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#
```

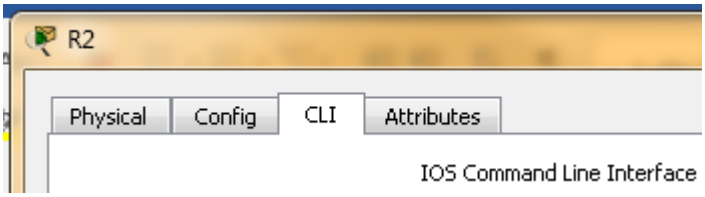

```
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#end
```

```
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#
```

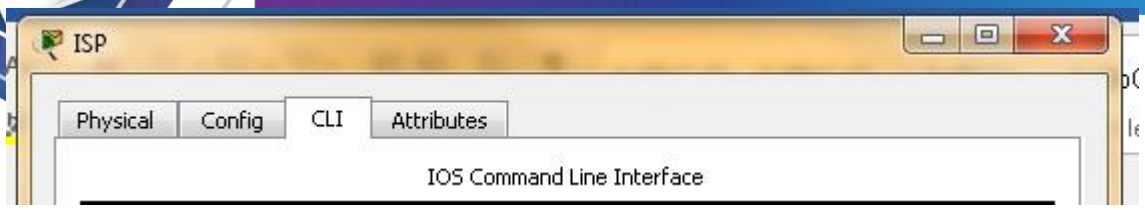
e. Configure logging synchronous para evitar que los mensajes de consola interrumpan la entrada de comandos.




```
R1(config-line)#loggin synchronous
```




```
R2(config-line)#logging synchronous
R2(config-line)#exec
R2(config-line)#exec-timeout 0 0
```



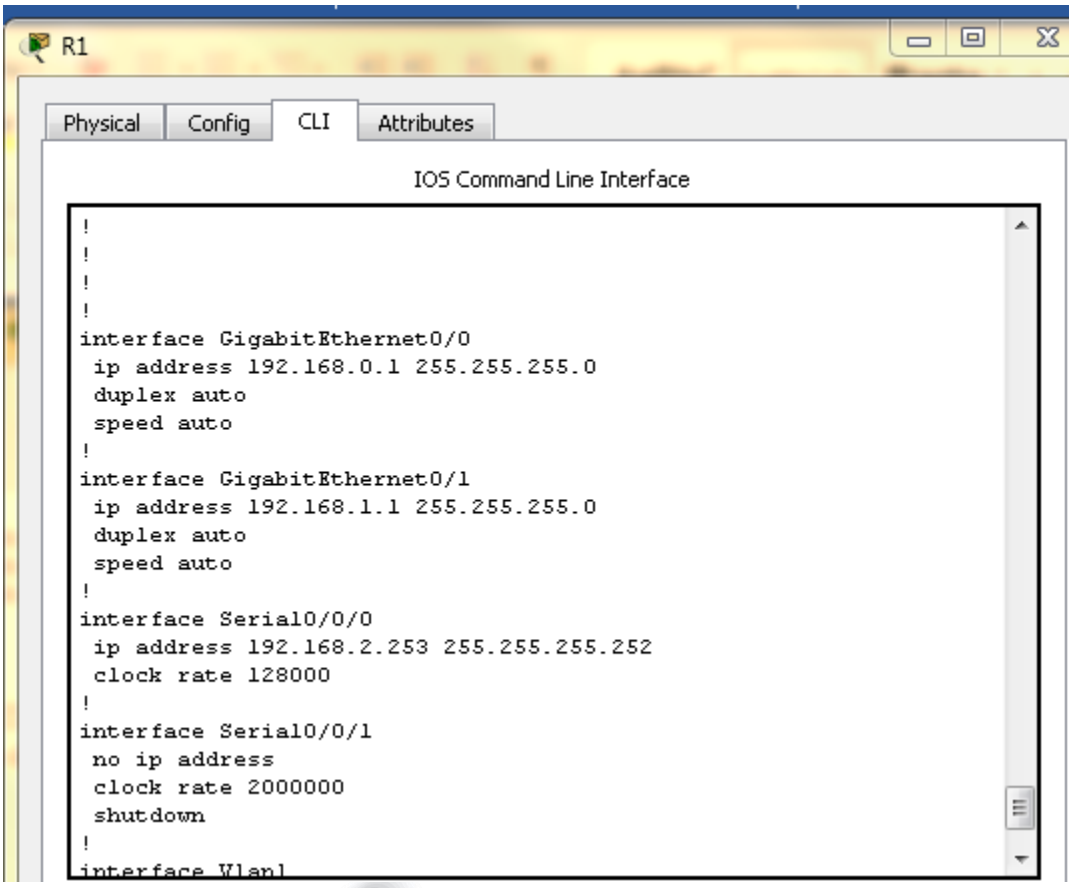

```
R3(config-line)#logging synchronous
R3(config-line)#exec-t
R3(config-line)#exec-timeout 0 0
```

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

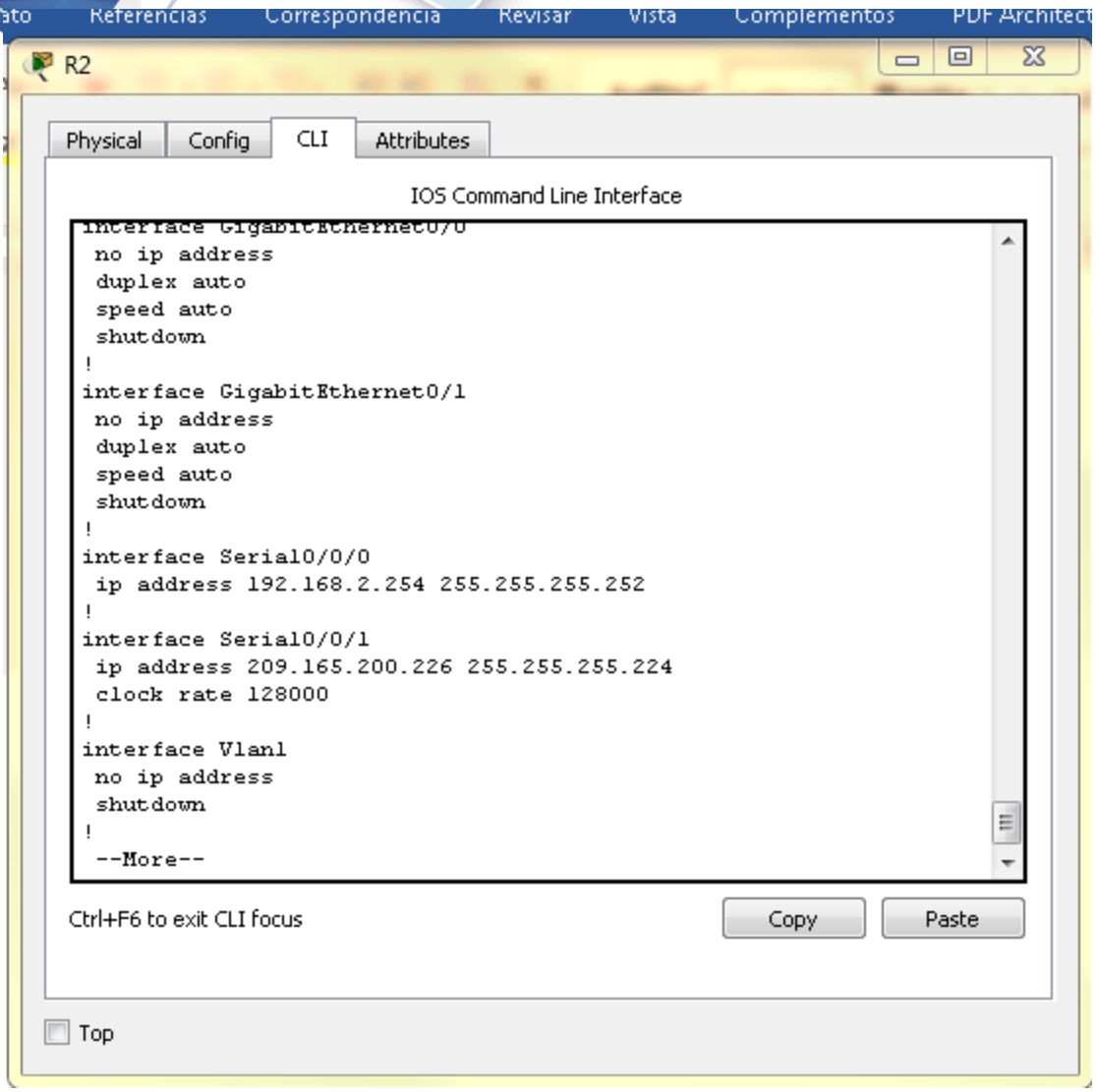
g.Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.

RESPUESTA FY G

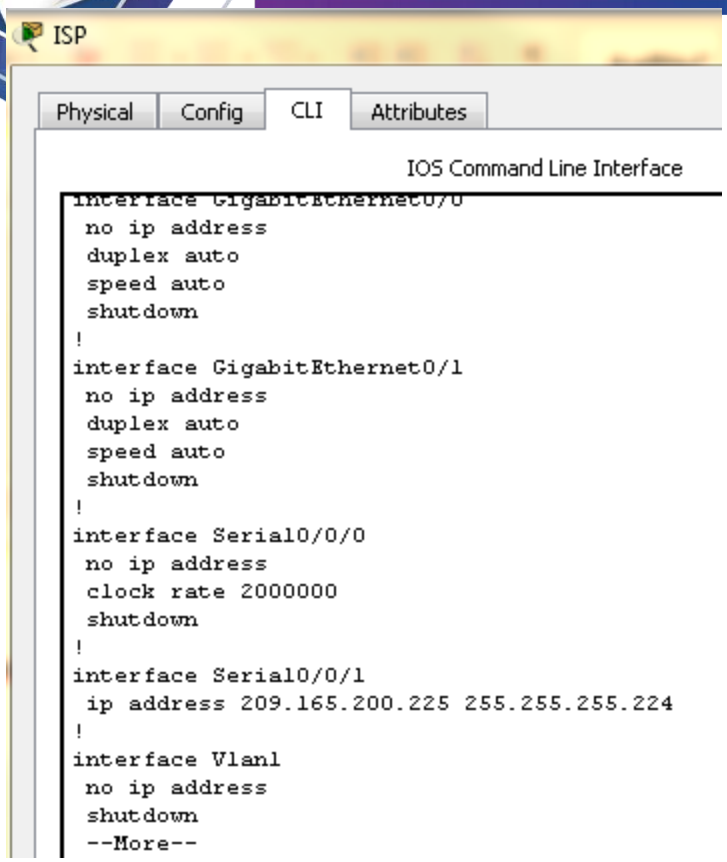
**Configuracion Router 1**



**Confguracion router 2**




**Configuracion router ISP**




**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

```
Enter configuration commands, one per line.  End with
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.168.0.1 0.0.0.255
R1(config-router)#network 192.168.2.252 0.0.0.3
R1(config-router)#no auto-suma
R1(config-router)#no auto-sumamary
                   ^
% Invalid input detected at '^' marker.

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

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

R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.252 0.0.0.3
R2(config-router)# redistribute static

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

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

R2(config-router)#no auto-
R2(config-router)#no auto-summary
R2(config-router)#redistribute static
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
R2(config)#
```

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

ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226

```
ISP>enable
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#
```

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

```
R2>enable
R2#wr
Building configuration...
[OK]
R2#
```

**Paso 4: verificar la conectividad de red entre los routers.**

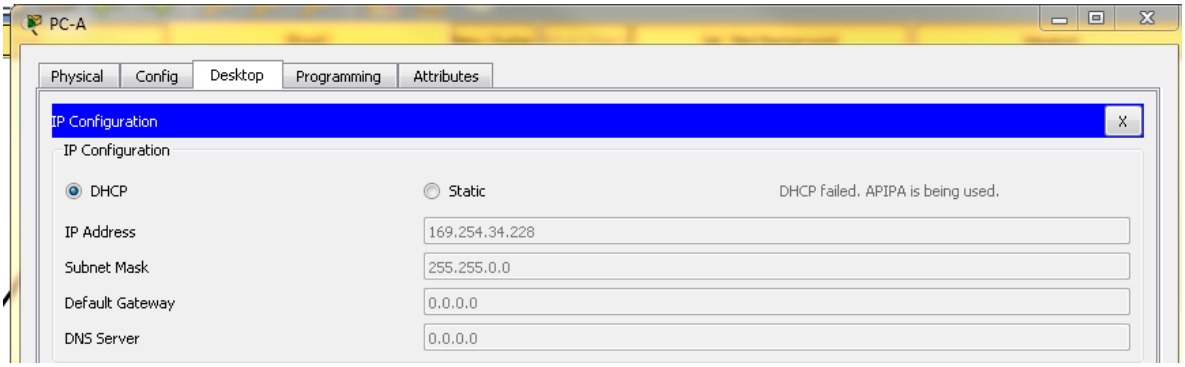
Si algún ping entre los routers falla, corrija los errores antes de continuar con el siguiente paso. Use los comandos show ip route y show ip interface brief para detectar posibles problemas.

**Desde ISP A ROUTER 1 192.168.2.253**

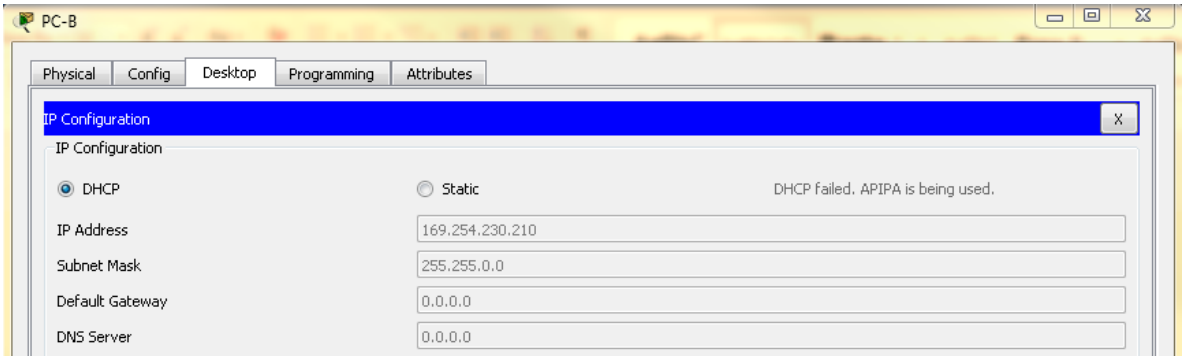
```
ISP#ping 192.168.2.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
2/4/11 ms

ISP#
```

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

**PC-A**




**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 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.

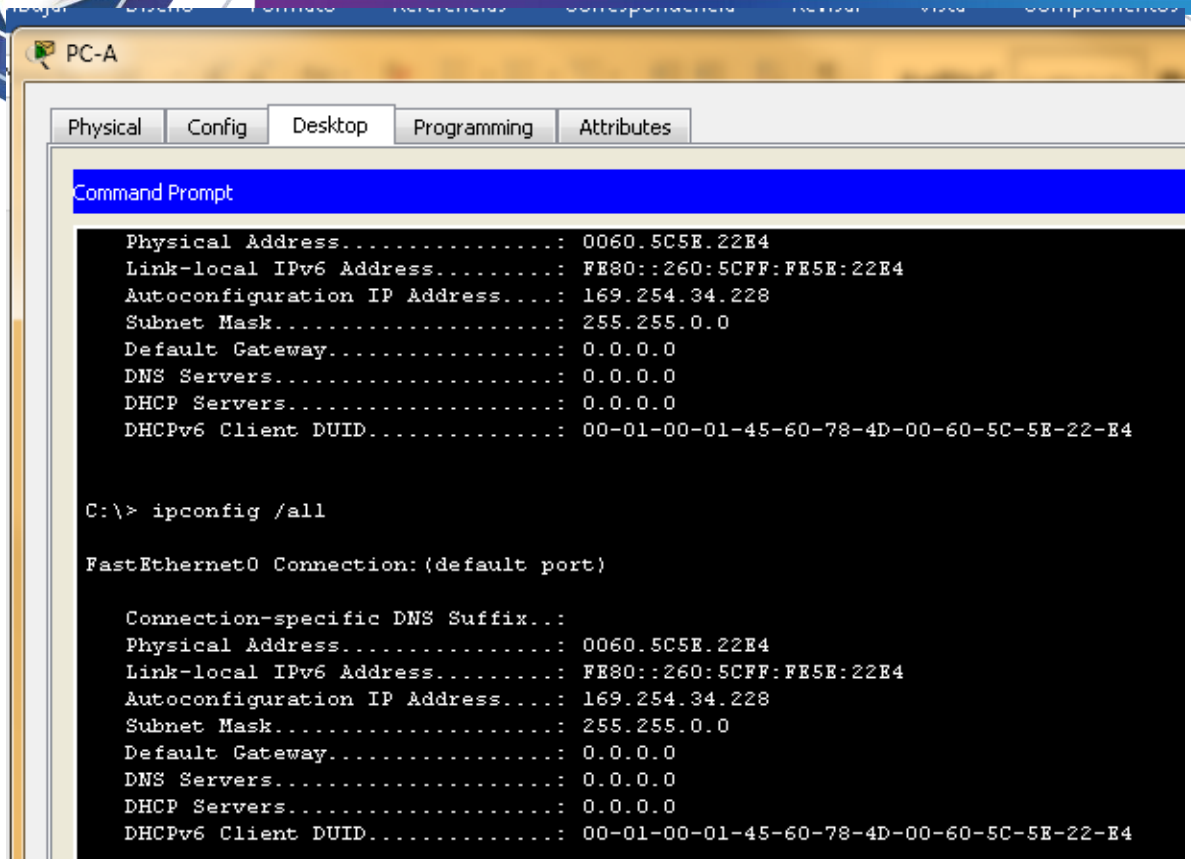
Excluya las primeras nueve direcciones en cada LAN del R1; empiece por .1. El resto de las direcciones deben estar disponibles en el conjunto de direcciones DHCP. Asegúrese de que cada conjunto de

```
R2>ENABLE
R2#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#Network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#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)#WR
                ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#wr
                ^
```

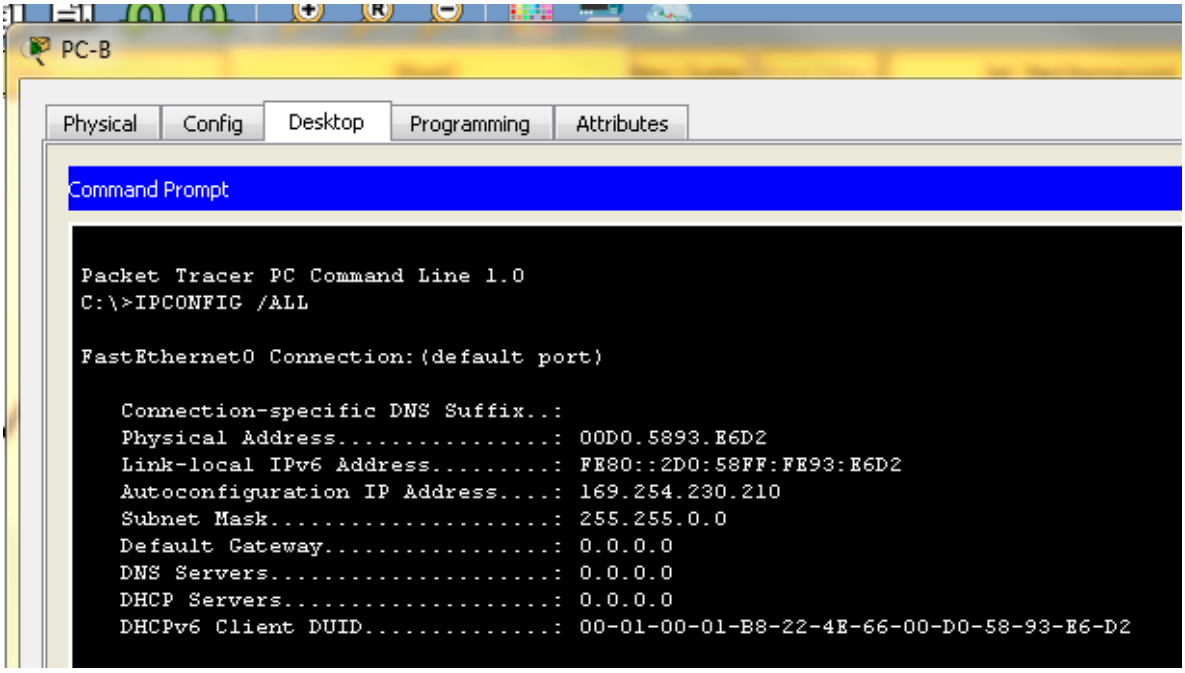
En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando **ipconfig /all.** ¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué?

No porque el router 2 se encuentra en otra red

PC-A




PC-B



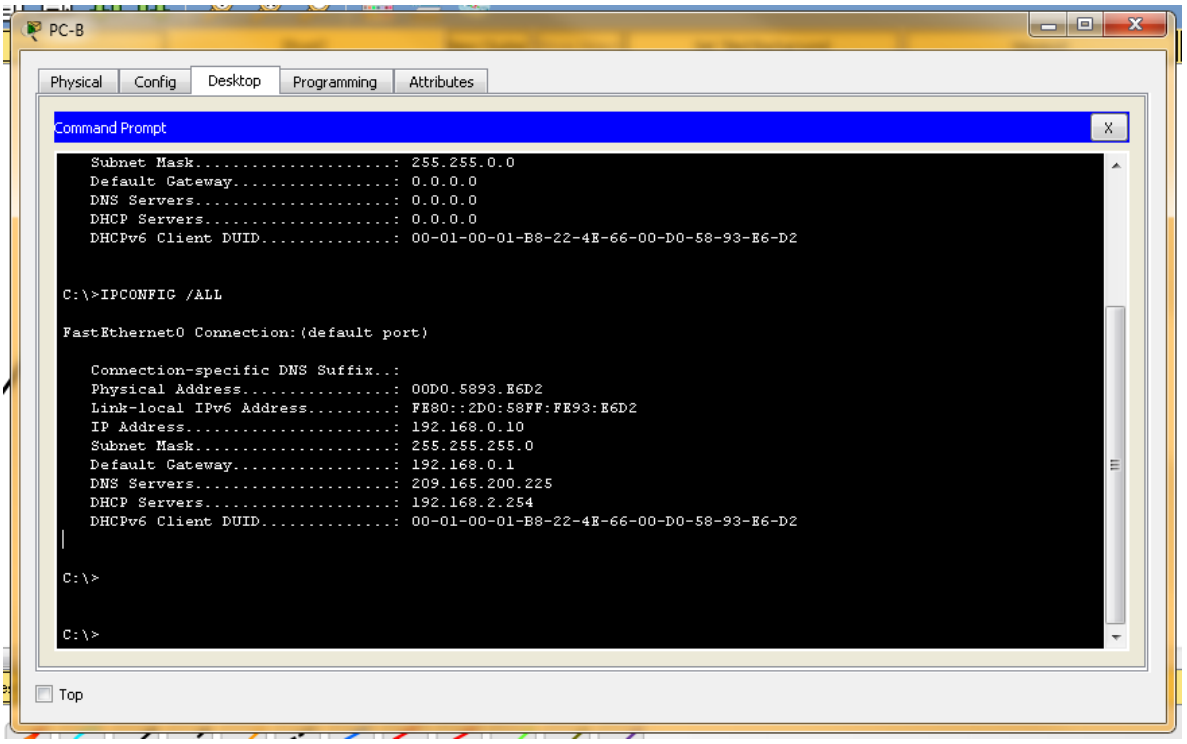

**Paso 3: Configurar el R1 como agente de retransmisión DHCP.**

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>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/0
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
R1(config)#interface g0/1
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#do wr
Building configuration...
[OK]
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

**Paso 4: 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.




**Paso 5: Verificar los servicios DHCP y los arrendamientos de direcciones en el R2.**

a. En el R2, introduzca el comando show ip dhcp binding para ver los arrendamientos de direcciones DHCP.
Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado?

```
R2>ENABLE
R2#show ip dhcp b
R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.0.10     00D0.5893.E6D2    |      --                     Automatic
R2#
```

Muestra el Tipo y la mac del equipo

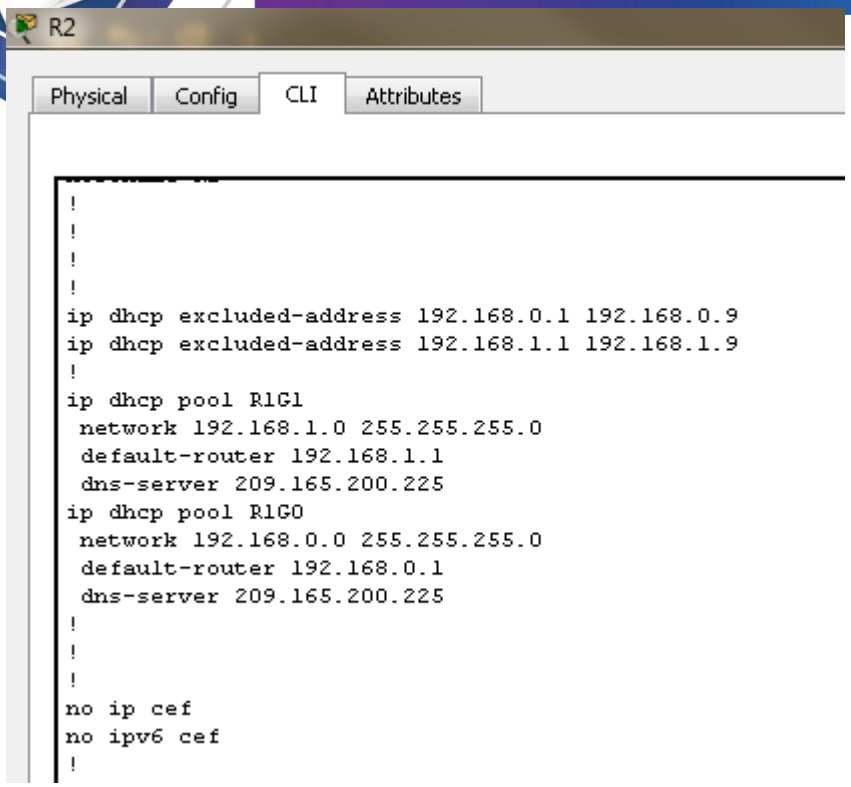
b. En el R2, introduzca el comando show ip dhcp server statistics para ver la actividad de mensajes y las estadísticas del pool de DHCP.
¿Cuántos tipos de mensajes DHCP se indican en el resultado?

El comando DHCP statics no esta implementado en Packet Tracer

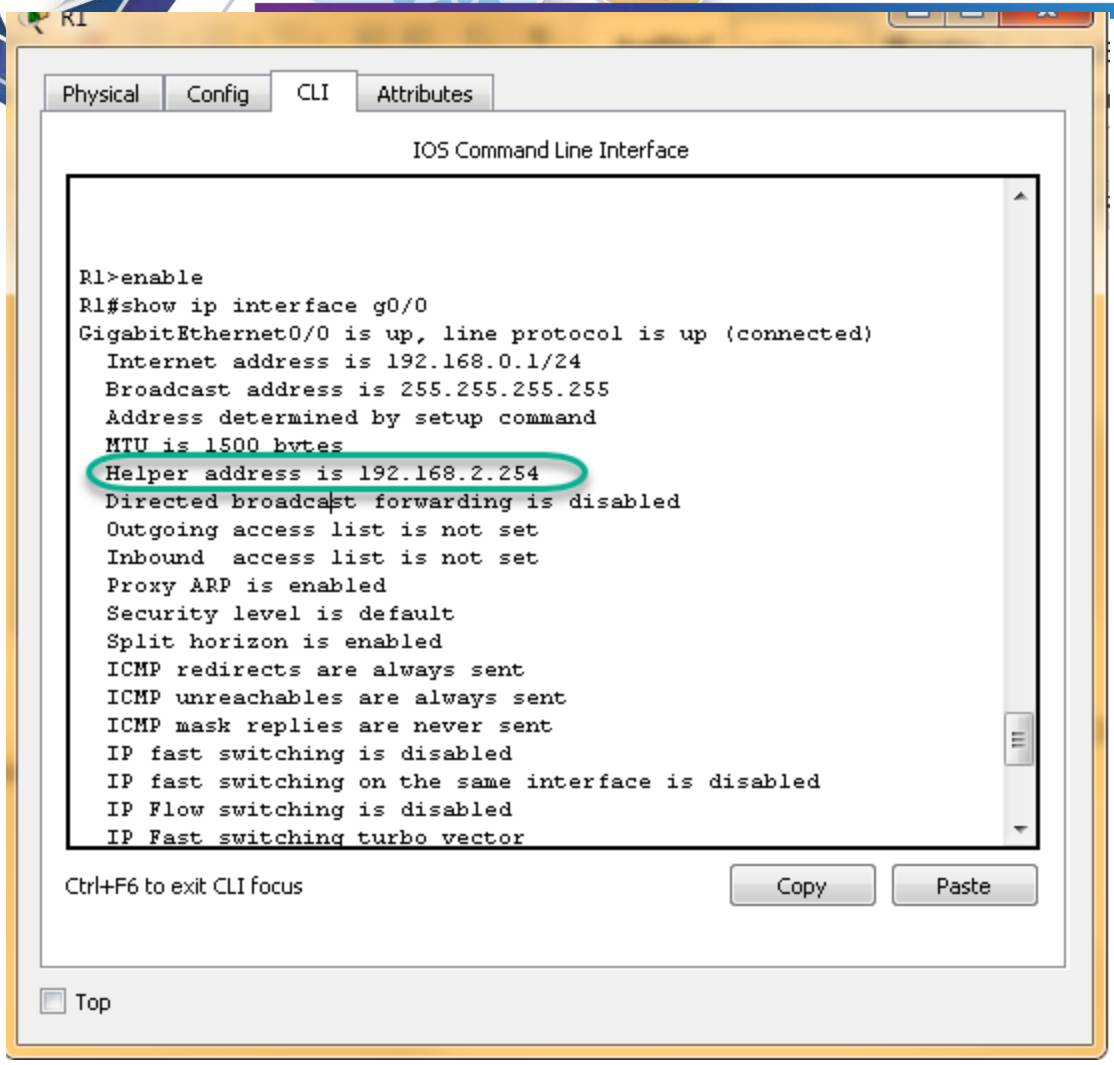
c. En el R2, introduzca el comando show ip dhcp pool para ver la configuración del pool de DHCP.
En el resultado del comando show ip dhcp pool, ¿a qué hace referencia el índice actual (Current index)?

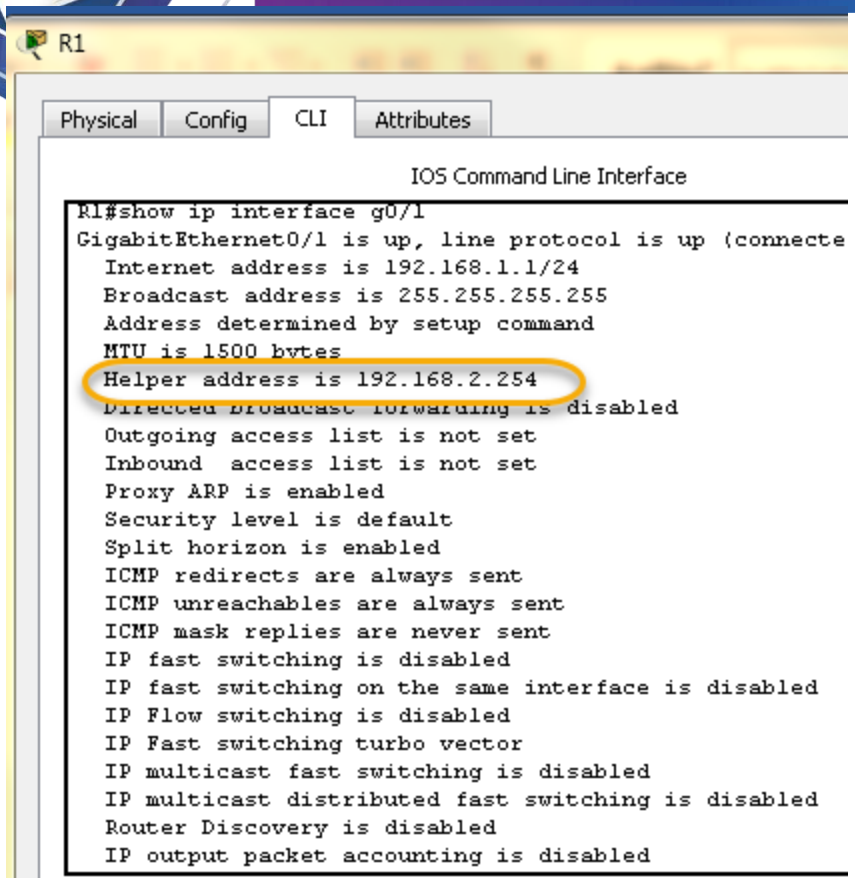
El comando SHOW IP DHCP POOL no esta implementado en Packet tracer

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




e. En el R2, introduzca el comando show run interface para las interfaces G0/0 y G0/1 para ver la configuración de retransmisión DHCP en la configuración en ejecución.


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1>enable
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
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
Ctrl+F6 to exit CLI focus
Copy
Paste
Top




**Reflexion**

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

Es que tener un servidor de DHCP del router independiente para cada subred agregaría más complejidad y disminuir la administración centralizada de la red.

**10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch.**

**Topología**

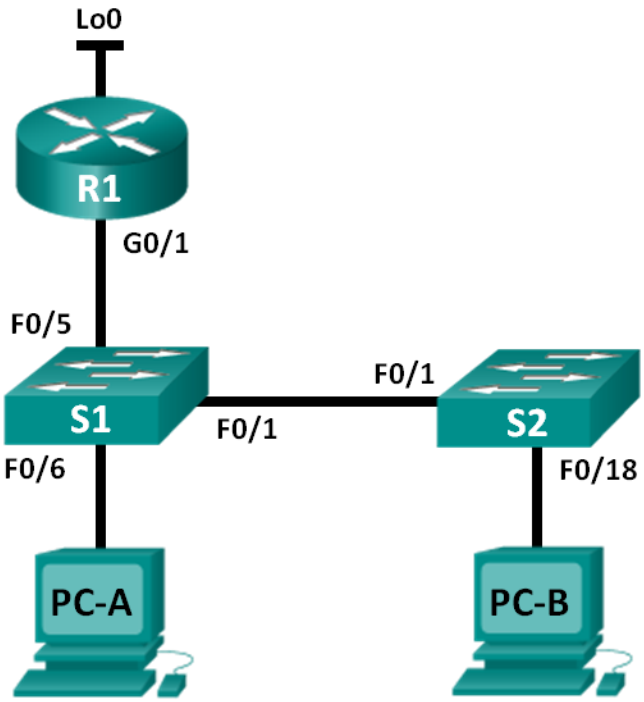



**Tabla de direccionamiento**

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

**Objetivos**

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

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

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

**Parte 3: configurar DHCPv4**

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

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

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

**Parte 5: habilitar el routing IP**

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

## Información básica/situación

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

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

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

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

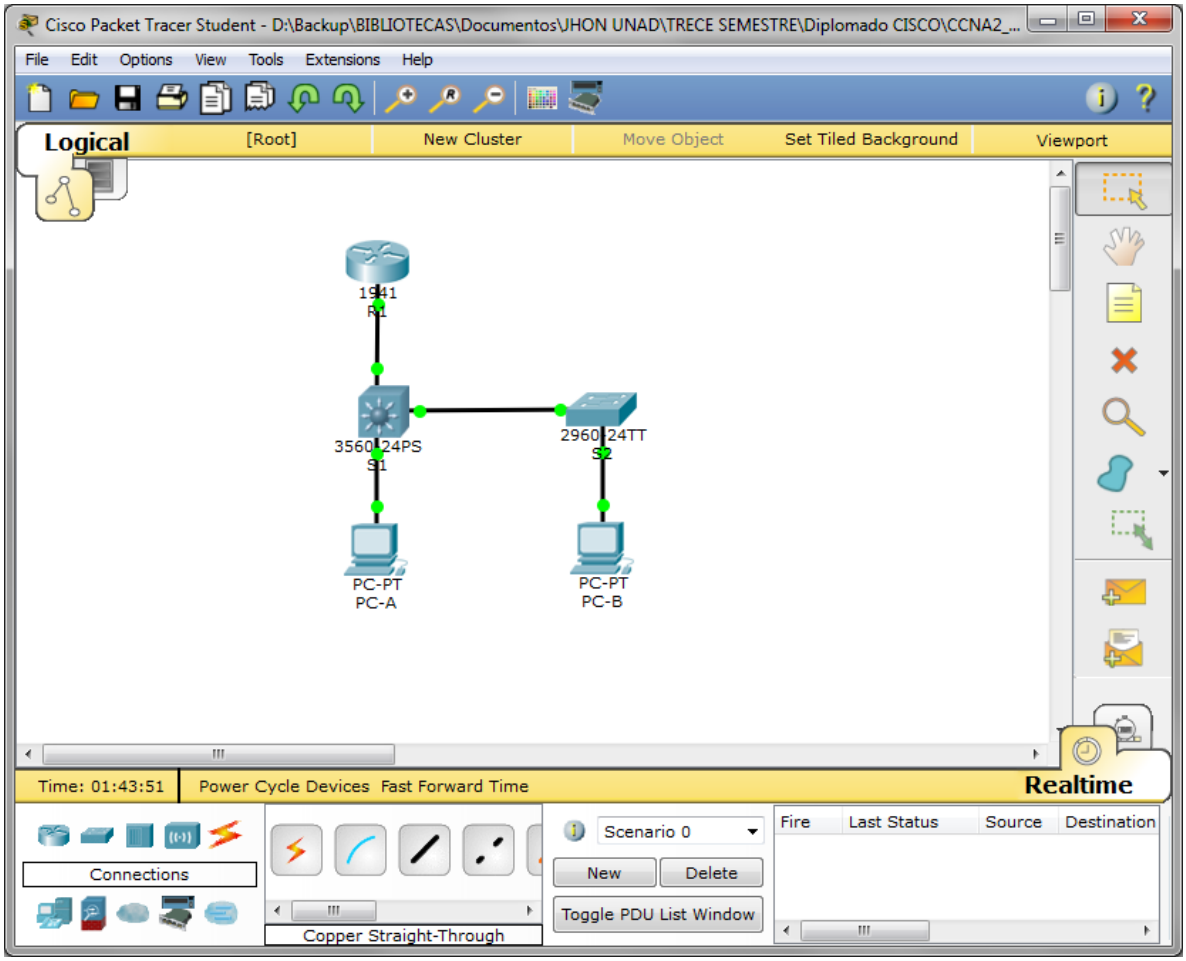
## Recursos necesarios

- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

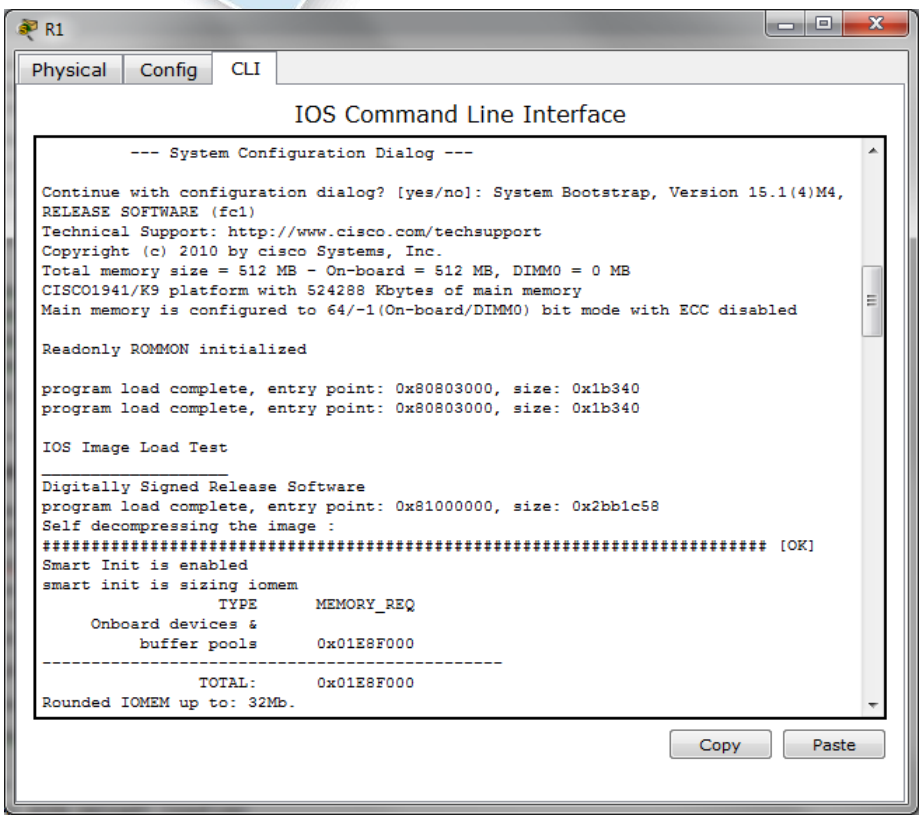
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

## Parte 9: 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.

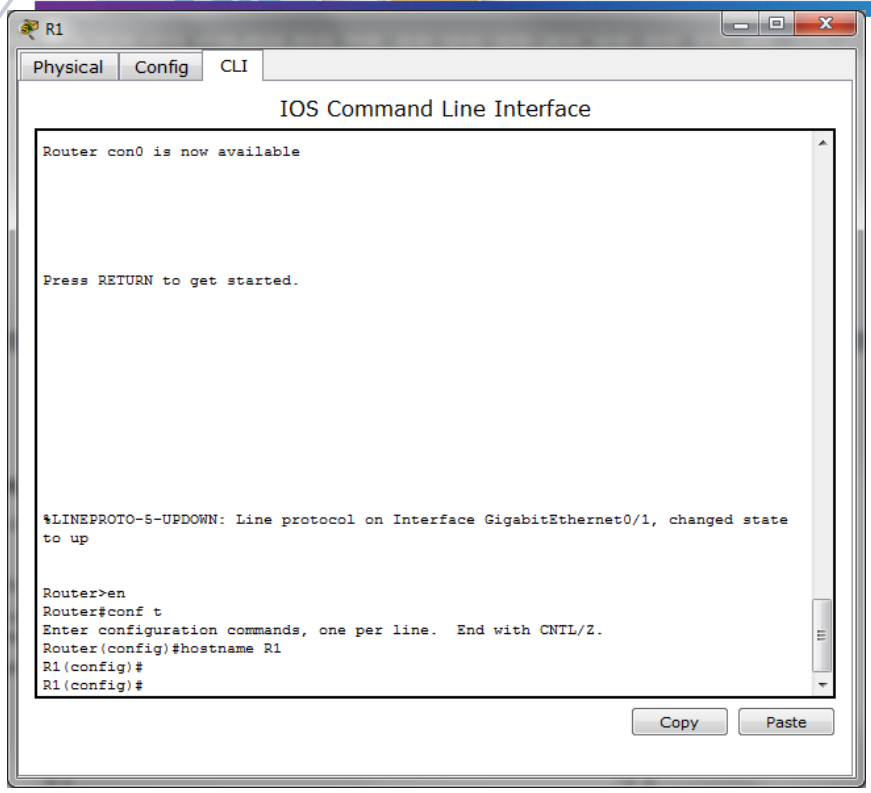


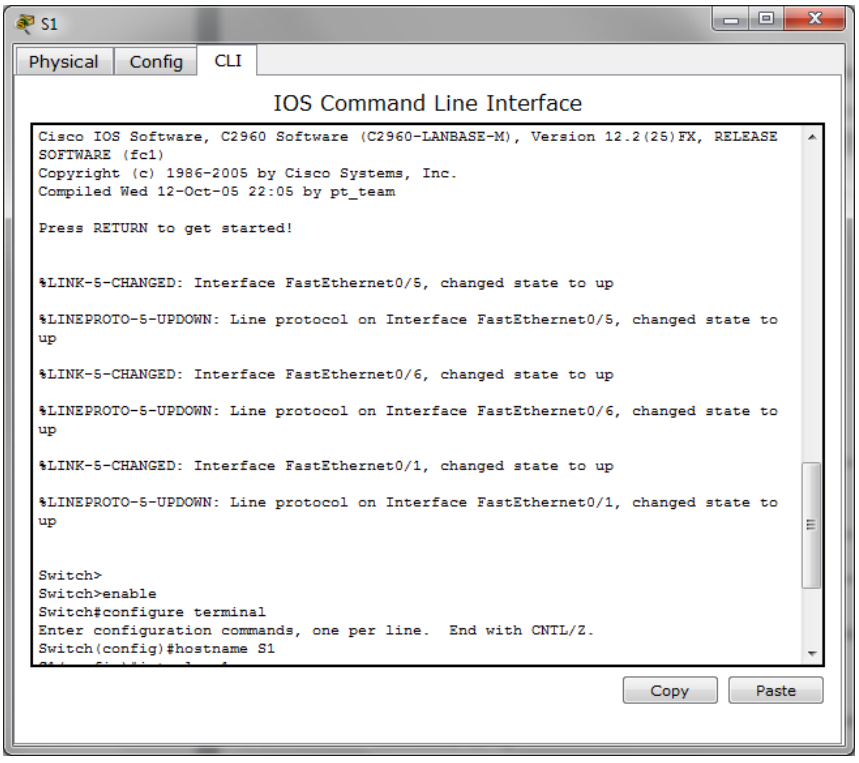
**Paso 2: inicializar y volver a cargar los routers y switches.**

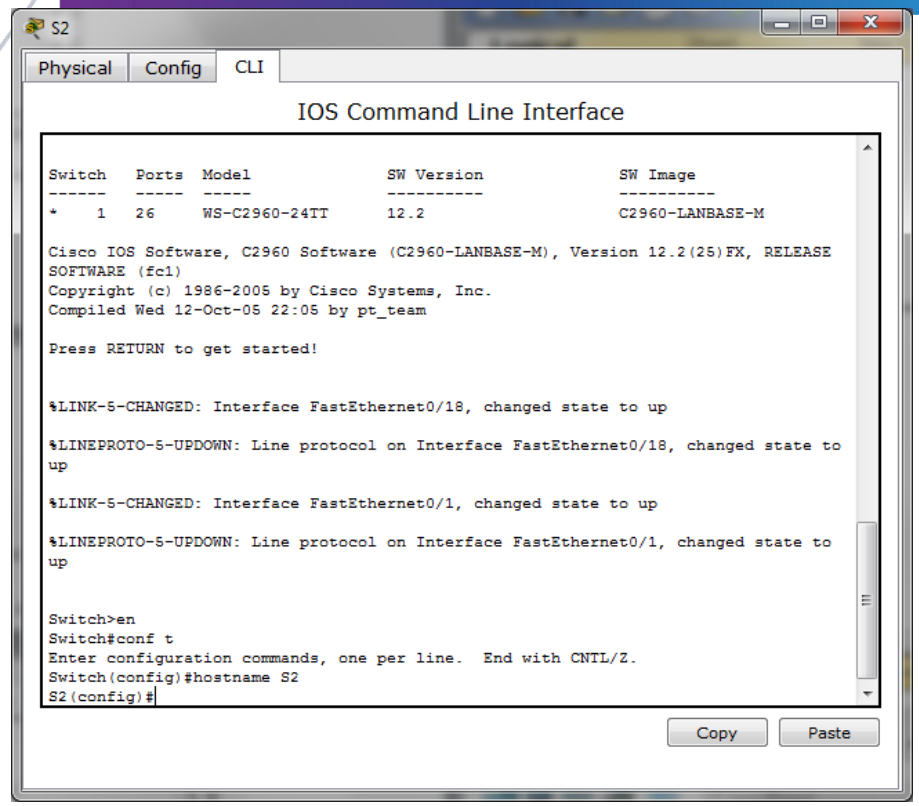



**Paso 3: configurar los parámetros básicos en los dispositivos.**

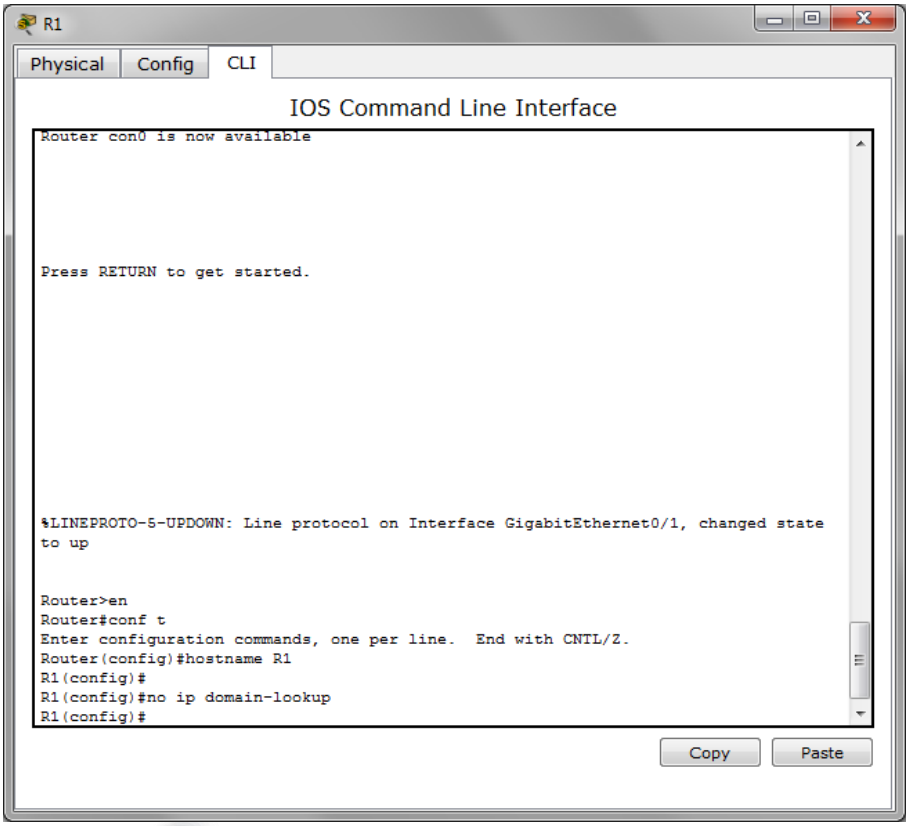
a. Asigne los nombres de dispositivos como se muestra en la topología.


R1
Physical
Config
CLI
IOS Command Line Interface
Router con0 is now available
Press RETURN to get started.
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#
Copy
Paste

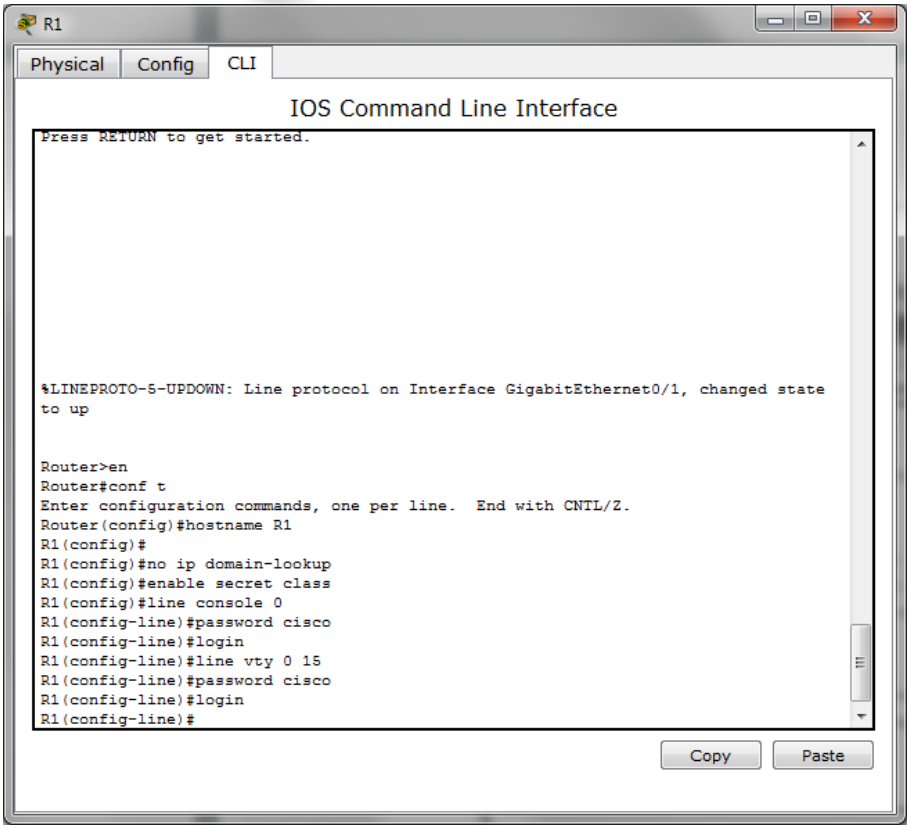

S1
Physical
Config
CLI
IOS Command Line Interface
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, 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
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
Copy
Paste



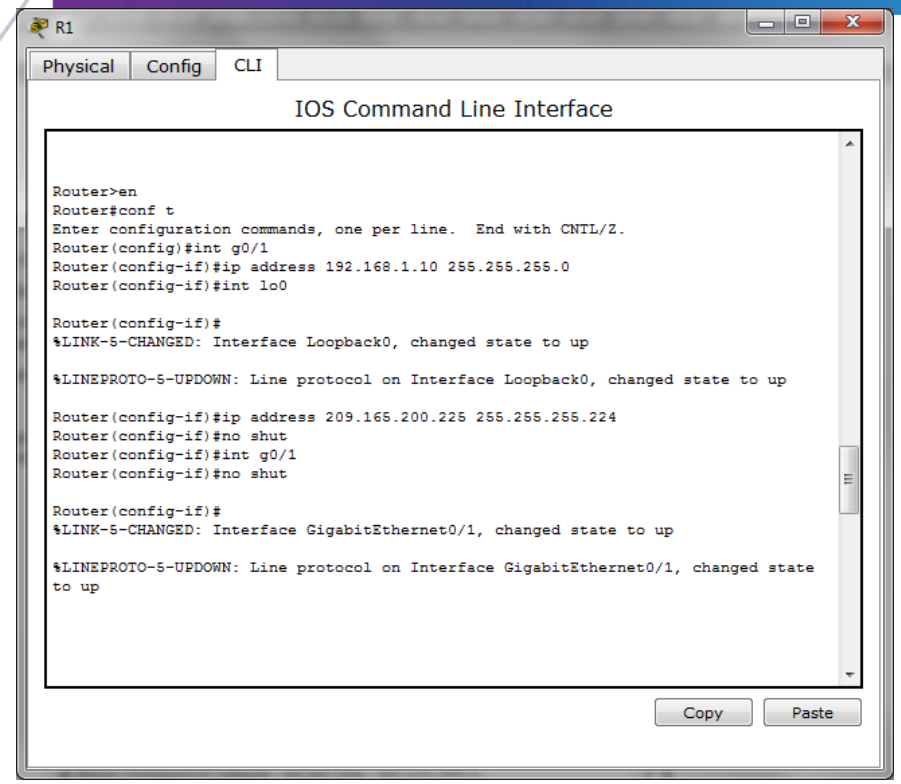

b. Desactive la búsqueda del DNS.



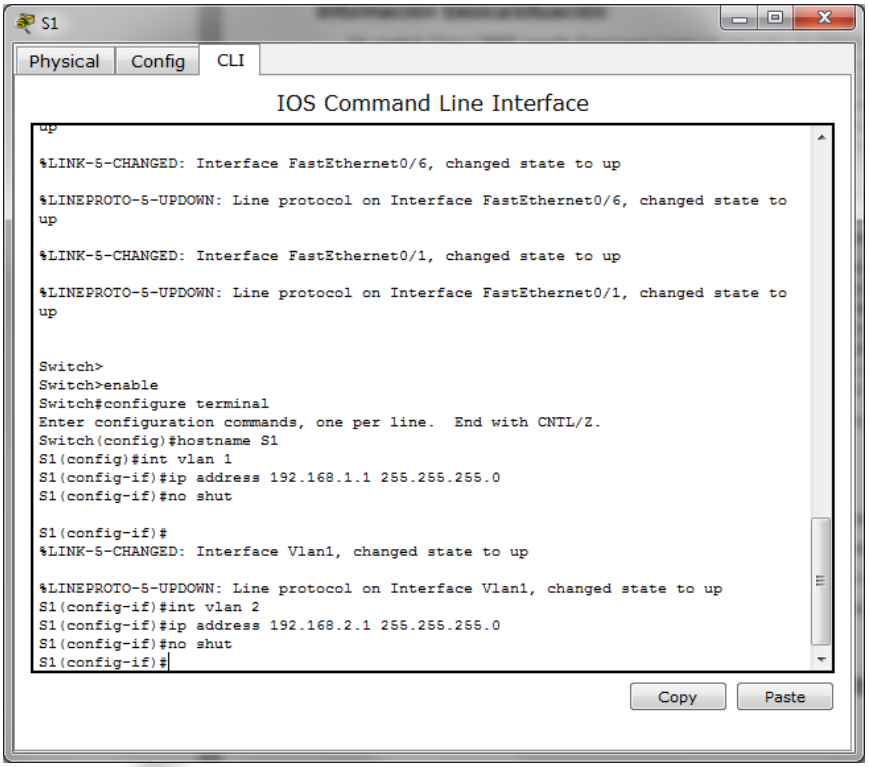
c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.



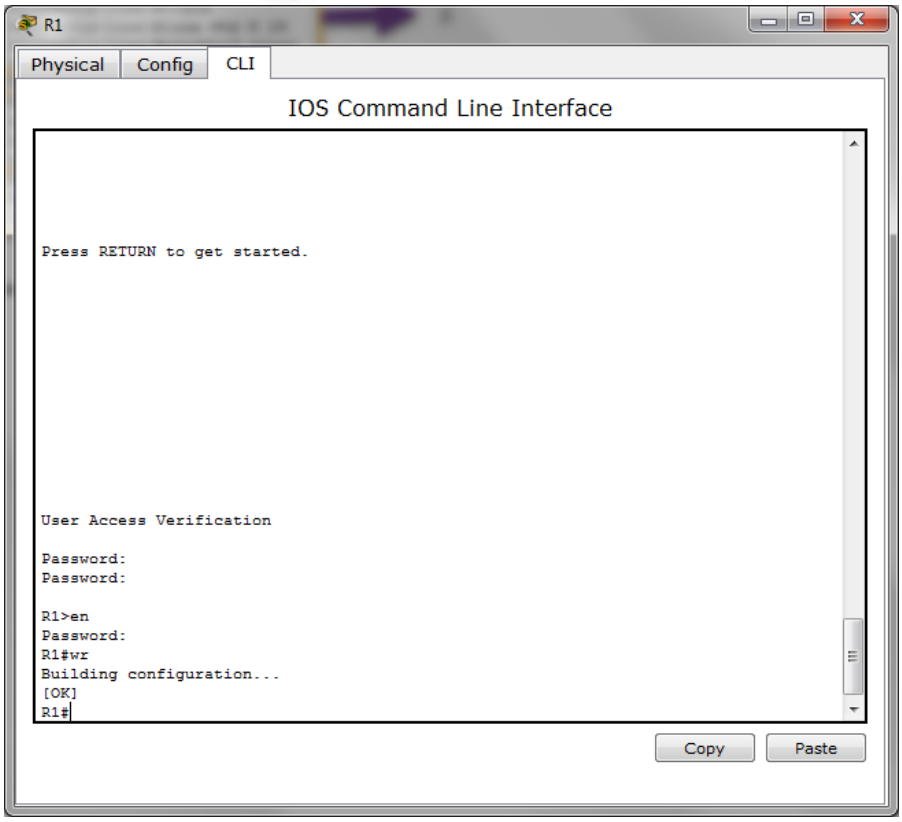

d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.




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



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




## Parte 10: 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? **lanbase-routing**

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

S1# **reload**

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

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

**Paso 3: verificar que la plantilla lanbase-routing esté cargada.**

Emita el comando **show sdm prefer** para verificar si la plantilla lanbase-routing se cargó en el S1.

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

number of unicast mac addresses: 4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes: 0.75K

number of directly-connected IPv4 hosts: 0.75K
number of indirect IPv4 routes: 16
number of IPv6 multicast groups: 0.375k
number of directly-connected IPv6 addresses: 0.75K
number of indirect IPv6 unicast routes: 16
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.125k
number of IPv4/MAC security aces: 0.375k
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 0.375k
number of IPv6 security aces: 127

## Parte 11: 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.

**ip dhcp excluded-address 192.168.1.1 192.168.1.10**

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

**ip dhcp pool DHCP1**

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

**network 192.168.1.0 255.255.255.0**

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

**default-router 192.168.1.1**

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

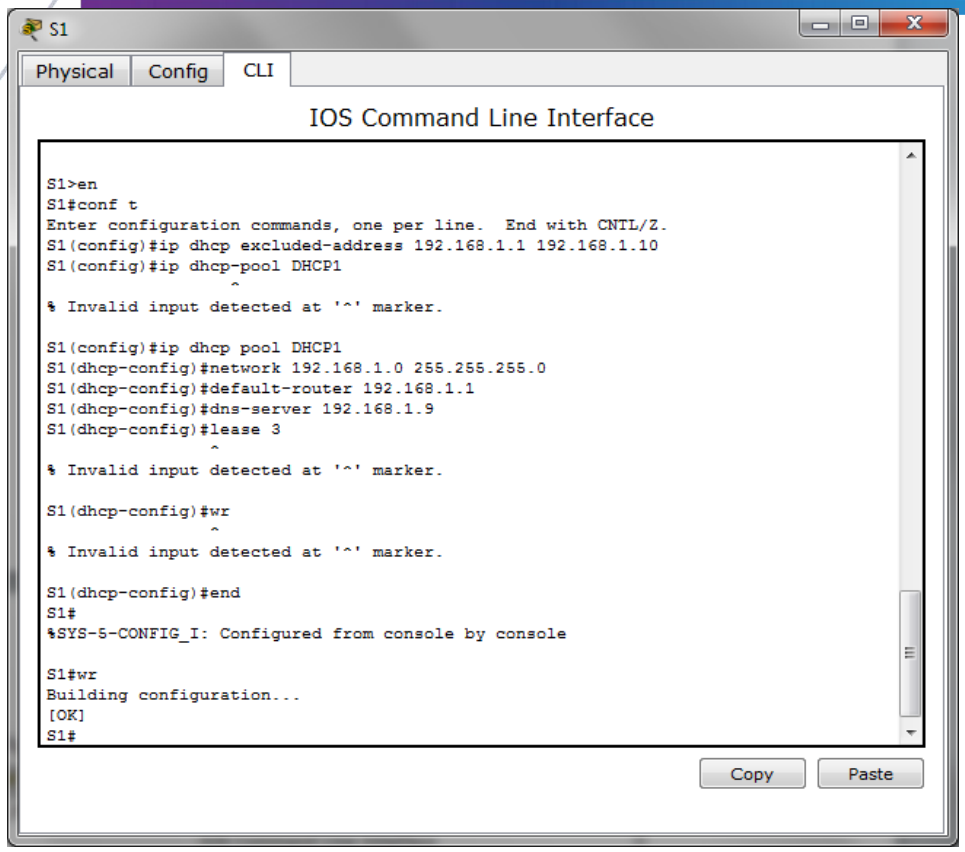
**dns-server 192.168.1.9**

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

**lease 3**

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

**wr**




**Paso 2: verificar la conectividad y DHCP.**

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

Para la PC-A, incluya lo siguiente:

Dirección IP: **192.168.1.11**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.1.1**

Para la PC-B, incluya lo siguiente:

Dirección IP: **192.168.1.12**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.1.1**

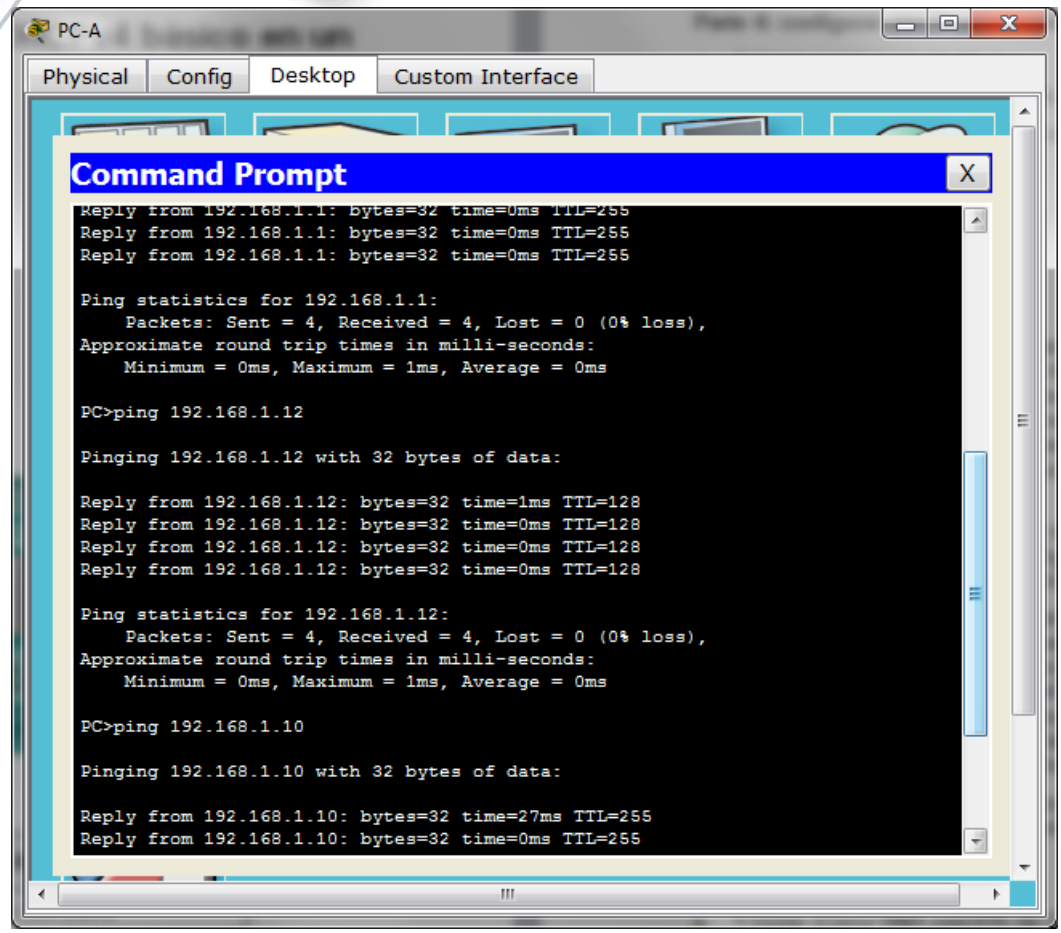
b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? **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 12: 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.

**int fa0/6**

**switchport mode access**

**switchport access vlan 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.

**ip dhcp excluded-address 192.168.2.1 192.168.2.10**

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

**ip dhcp pool DHCP2**

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

**network 192.168.2.0 255.255.255.0**

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

**default-router 192.168.2.1**

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

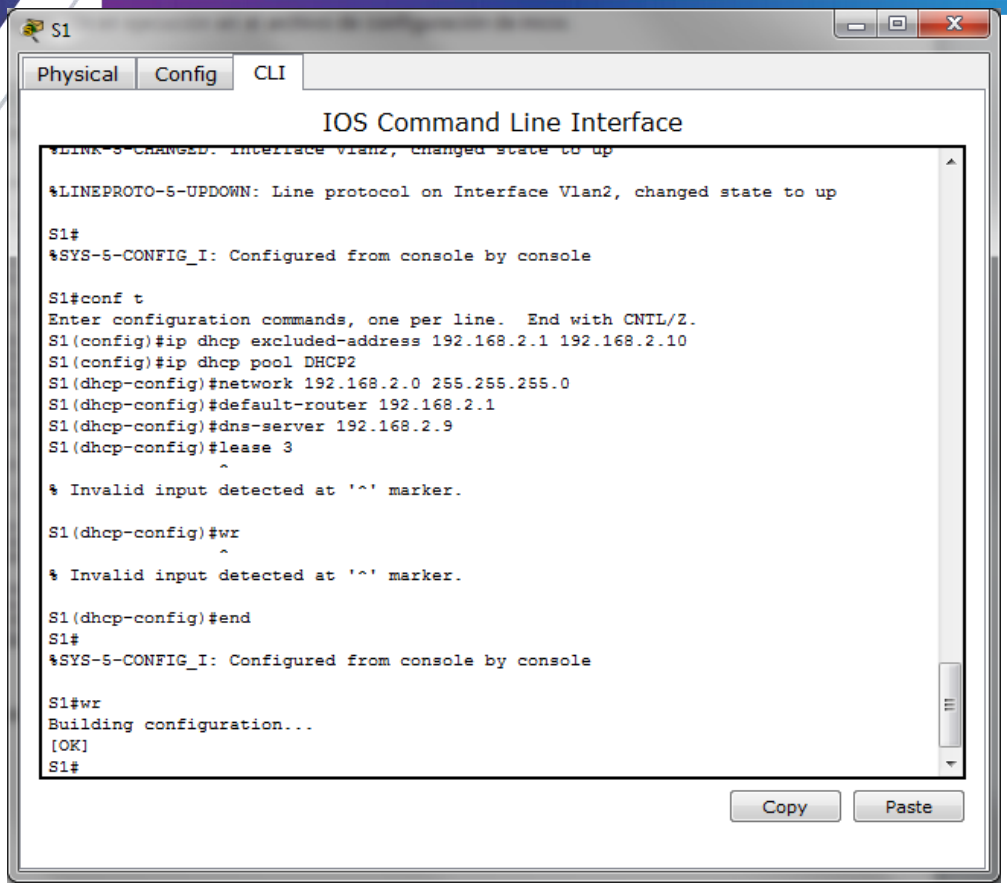
**dns-server 192.168.2.9**

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

**lease 3**

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

**wr**




**Paso 2: verificar la conectividad y DHCPv4.**

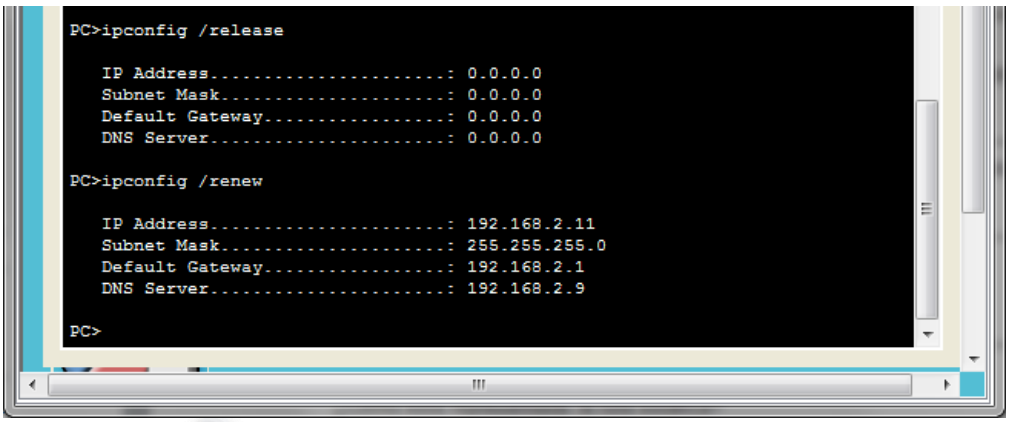
a. En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: **192.168.2.11**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.2.1**



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

¿Es posible hacer ping de la PC-A al gateway predeterminado? **SI**

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

¿Los pings eran correctos? ¿Por qué?

**El ping realizado a la puerta de enlace si fue satisfactorio, pero el realizado al PC-B no funcionó debido a que el PC-B estaba configurado en una red diferente.**

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

¿Qué resultado arrojó este comando?

**Que no está definido un default router**

## Parte 13: habilitar el routing IP

En la parte 5, habilitará el routing IP en el switch, que permitirá la comunicación entre VLAN. Para que todas las redes se comuniquen, se deben implementar rutas estáticas en el S1 y el R1.

### Paso 1: habilitar el routing IP en el S1.

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

S1(config)# **ip routing**

b. Verificar la conectividad entre las VLAN.

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

¿Qué función realiza el switch?

**El switch está haciendo la function de switch capa 3**

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?

**C 192.168.1.0/24 is directly connected vlan1**

**C 192.168.2.0/24 is directly connected vlan2**

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?

**Gateway of last resort is not set**

**192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks**
**C 192.168.1.0/24 is directly connected, GigabitEthernet0/1**
**L 192.168.1.10/32 is directly connected, GigabitEthernet0/1**

**209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks**
**C 209.165.200.224/27 is directly connected, Loopback0**
**L 209.165.200.225/32 is directly connected, Loopback0**

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 al switch 1 y otra al router 1, utilizando el comando ip route**

**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.

**ip route 0.0.0.0 0.0.0.0 192.168.1.10**

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

**ip route 192.168.2.0 255.255.255.0 g0/1**

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

¿Cómo está representada la ruta estática predeterminada?

**C 192.168.1.0/24 is directly connected, Vlan1**
**C 192.168.2.0/24 is directly connected, Vlan2**
**S* 0.0.0.0/0 [1/0] via 192.168.1.10**

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

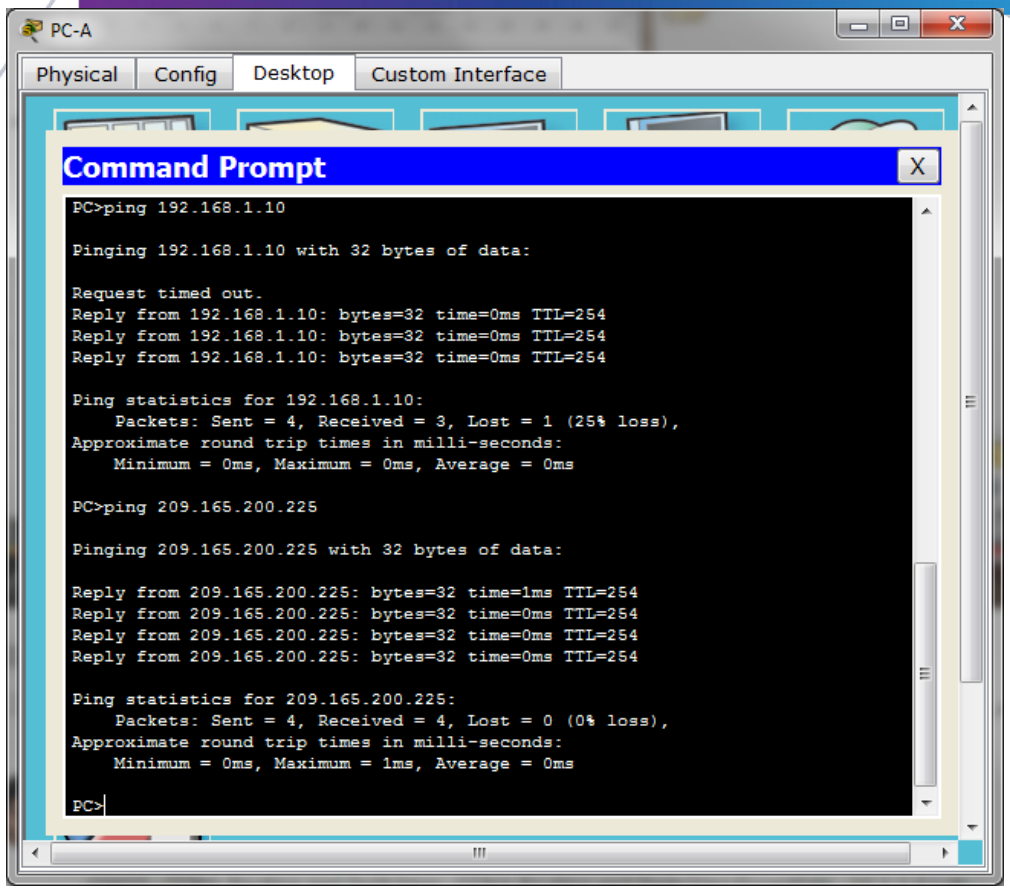
¿Cómo está representada la ruta estática?

Gateway of last resort is not set

**192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks**
**C 192.168.1.0/24 is directly connected, GigabitEthernet0/1**
**L 192.168.1.10/32 is directly connected, GigabitEthernet0/1**
**S 192.168.2.0/24 is directly connected, GigabitEthernet0/1**
**209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks**
**C 209.165.200.224/27 is directly connected, Loopback0**
**L 209.165.200.225/32 is directly connected, Loopback0**

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

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


PC-A
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Ping statistics for 209.165.200.225:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>

**Reflexión**

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

   **Para que no se presentara conflicto de IP al momento de asignar direcciones por dhcp con otras direcciones estáticas que tenemos configuradas.**

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

   **Se asigna un puerto para la vlan 1 y otro para la vlan 2**

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

   Es un switch de capa 3 utilizando el comando ip routing

**10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6.**

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

**Topología**


**Tabla de direccionamiento**

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

**Objetivos**

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

**Parte 2: configurar la red para SLAAC**

**Parte 3: configurar la red para DHCPv6 sin estado**

**Parte 4: configurar la red para DHCPv6 con estado**

**Información básica/situación**

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

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

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

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

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

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

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

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

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

```
S1# show sdm prefer
```

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

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

**Recursos necesarios**

- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

**Nota:** los servicios de cliente DHCPv6 están deshabilitados en Windows XP. Se recomienda usar un host con Windows 7 para esta práctica de laboratorio.

**Part 14: armar la red y configurar los parámetros básicos de los dispositivos**

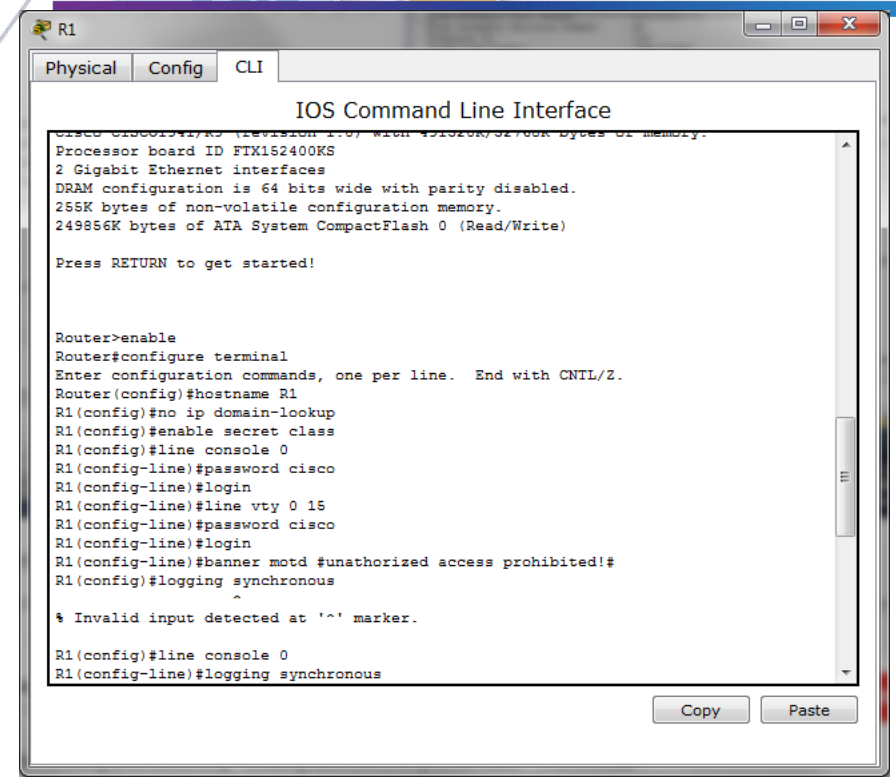
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos de configuración, como los nombres de dispositivos, las contraseñas y las direcciones IP de interfaz.

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

**Step 2: inicializar y volver a cargar el router y el switch según sea necesario.**

**Step 3: Configurar R1**

a. Desactive la búsqueda del DNS.
b. Configure el nombre del dispositivo.
c. Cifre las contraseñas de texto no cifrado.
d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
g. Establezca el inicio de sesión de consola en modo sincrónico.
h. Guardar la configuración en ejecución en la configuración de inicio.




**Step 4: configurar el S1.**

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo.

c. Cifre las contraseñas de texto no cifrado.

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

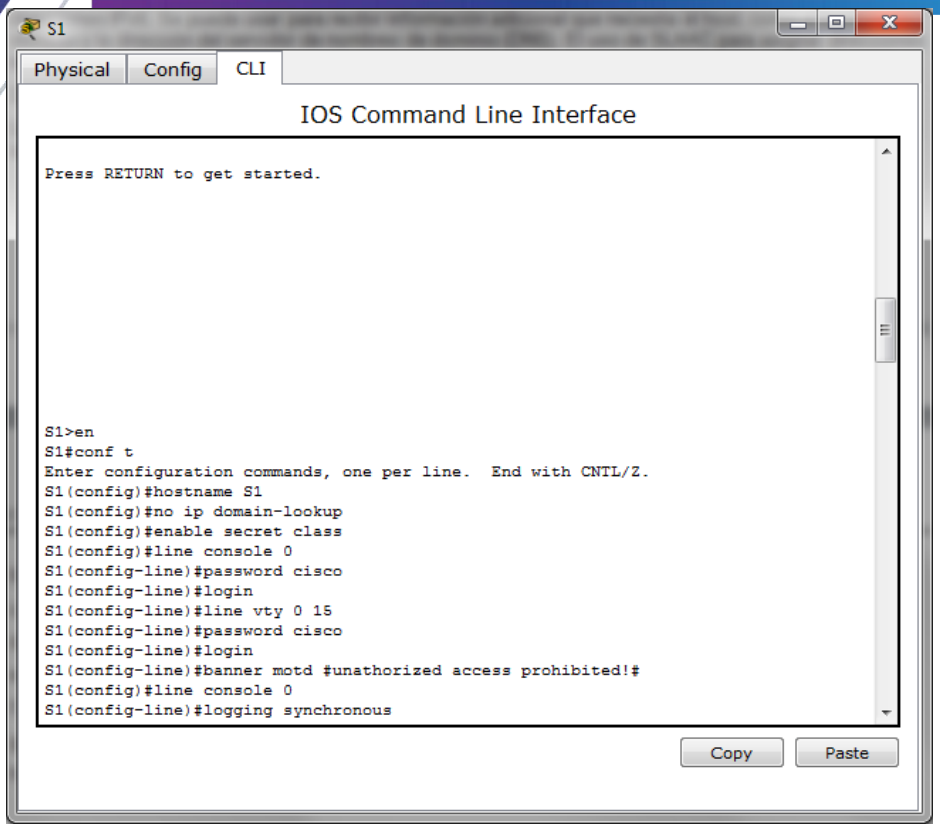
e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

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

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

h. Desactive administrativamente todas las interfaces inactivas.

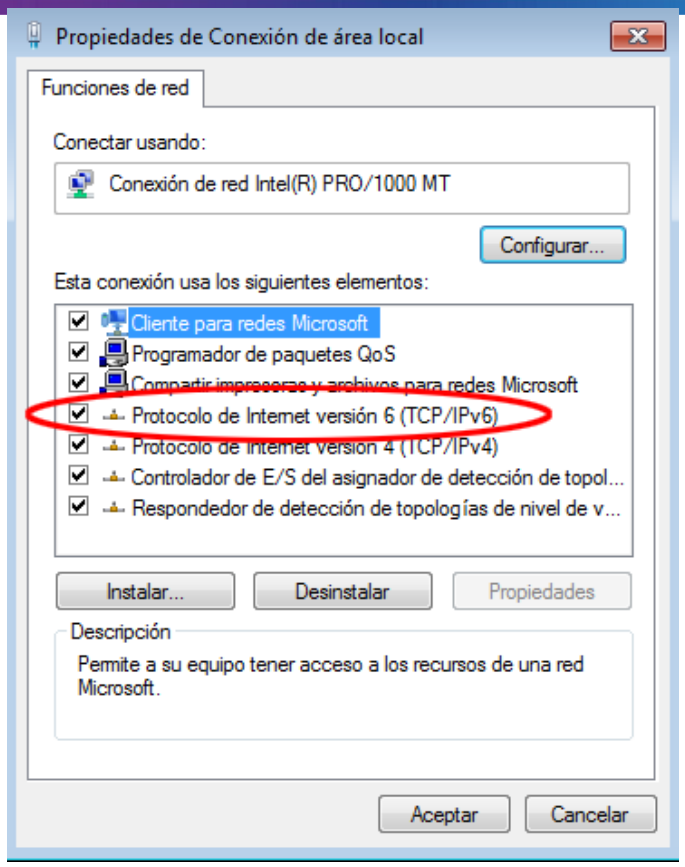
i. Guarde la configuración en ejecución en la configuración de inicio.




**Part 15: configurar la red para SLAAC**

**Step 1: preparar la PC-A.**

a. Verifique que se haya habilitado el protocolo IPv6 en la ventana Propiedades de conexión de área local. Si la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) no está marcada, haga clic para activarla.




b. Inicie una captura del tráfico en la NIC con Wireshark.

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

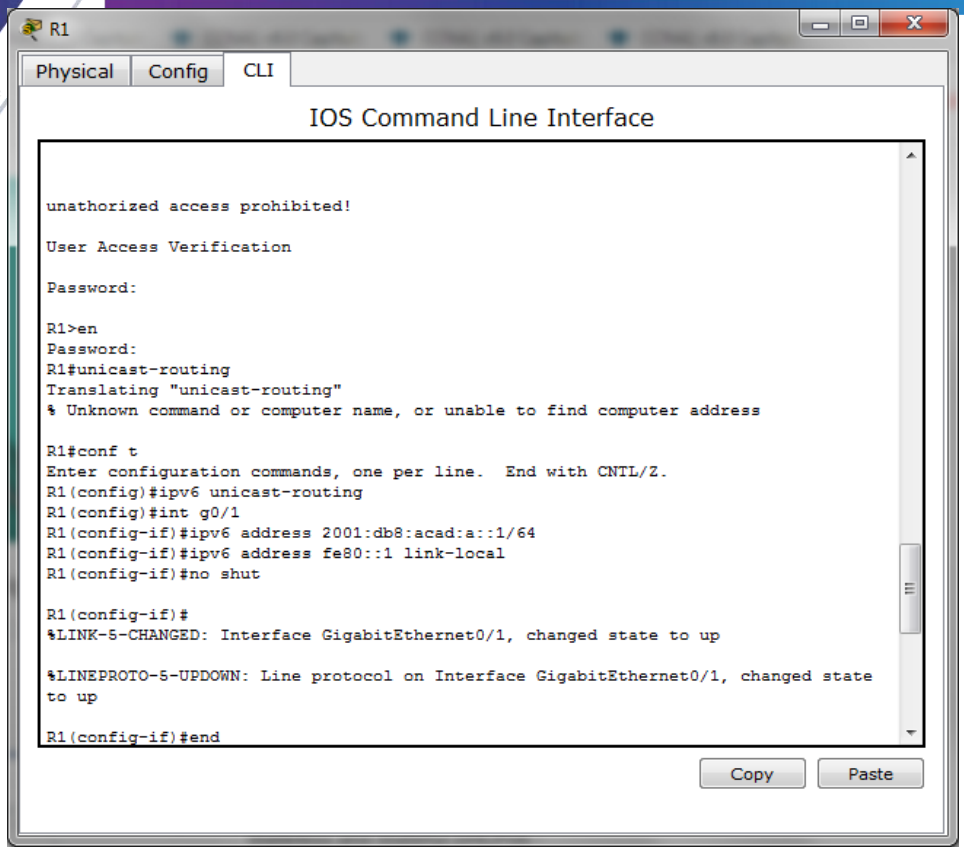

**Step 2: Configurar R1**

a. Habilite el routing de unidifusión IPv6.

b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.

c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.

d. Active la interfaz G0/1.

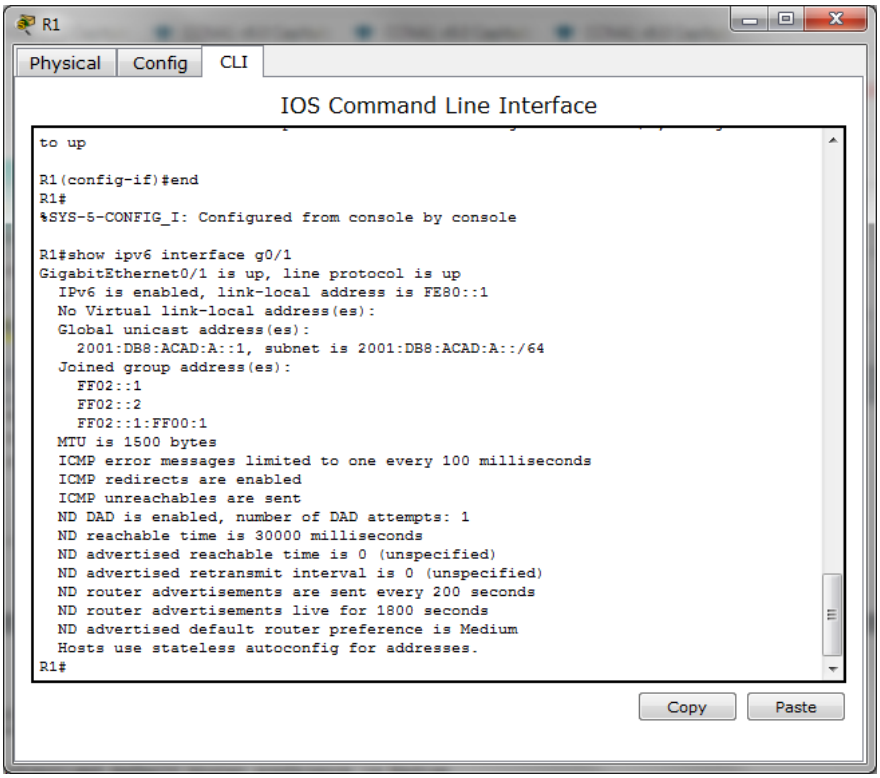



**Step 3: verificar que el R1 forme parte del grupo de multidifusión de todos los routers.**

Use el comando **show ipv6 interface g0/1** para verificar que G0/1 forme parte del grupo de multidifusión de todos los routers (FF02::2). Los mensajes RA no se envían por G0/1 sin esa asignación de grupo.

R1# **show ipv6 interface g0/1**
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.




**Step 4: configurar el S1.**

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

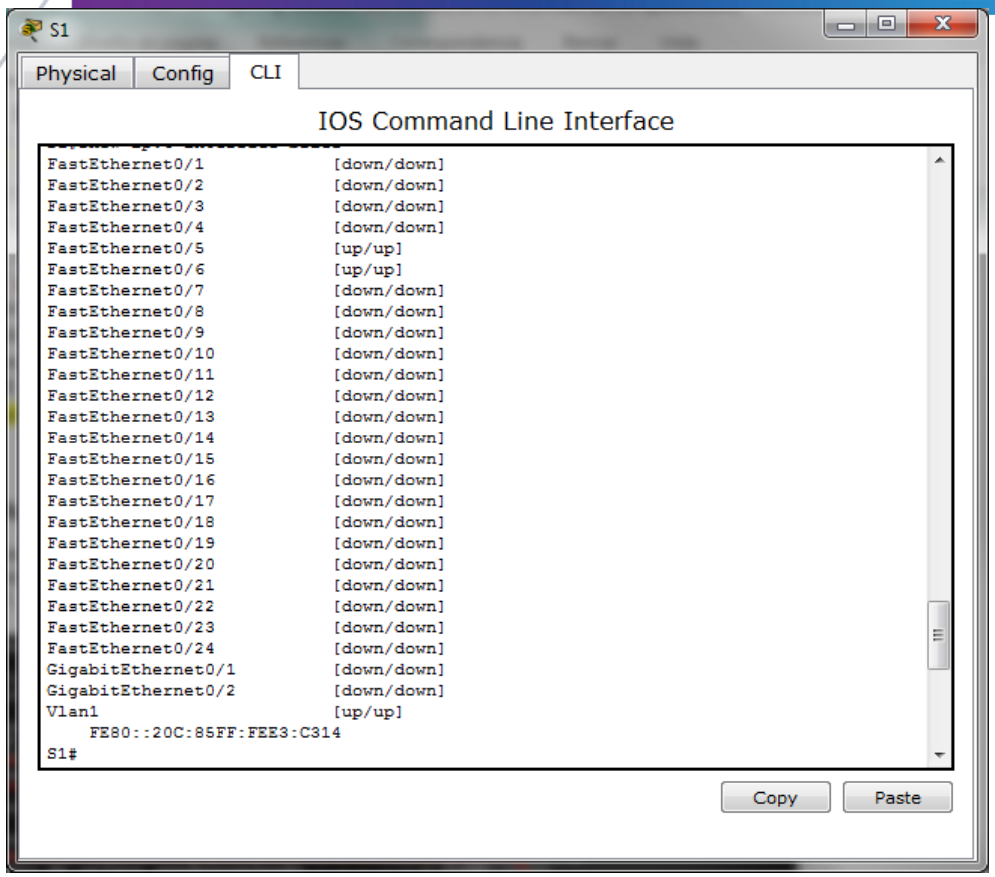
S1(config)# **interface vlan 1**
S1(config-if)# **ipv6 address autoconfig**
S1(config-if)# **end**

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

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

S1# **show ipv6 interface**
Vlan1 is up, line protocol is up

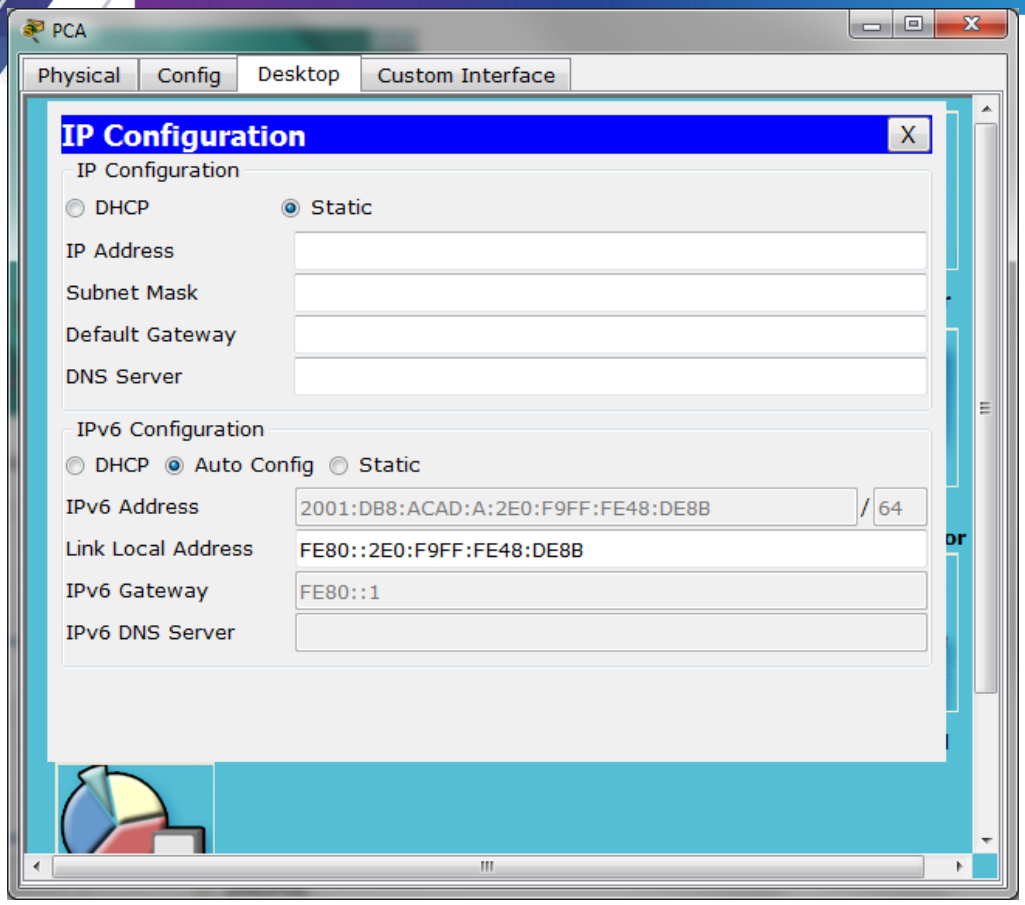
IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
No Virtual link-local address(es):
Stateless address autoconfig enabled
Global unicast address(es):
2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]
valid lifetime 2591988 preferred lifetime 604788
Joined group address(es):
FF02::1
FF02::1:FFE8:8A40
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
Output features: Check hwidb
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
Default router is FE80::1 on Vlan1



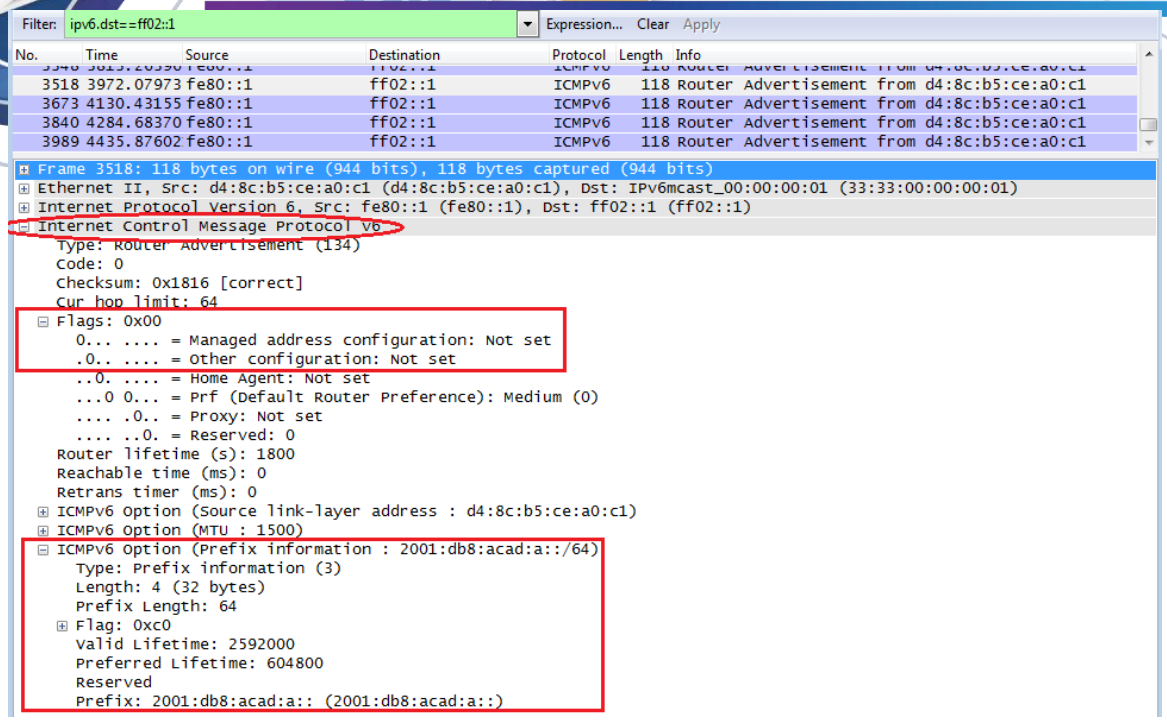

**Step 6: verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.**

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

```
Adaptador de Ethernet Conexión de área local:

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

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




b. En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.




## Part 16: configurar la red para DHCPv6 sin estado

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

a. Cree un pool de DHCP IPv6.

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

b. Asigne un nombre de dominio al pool.

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

c. Asigne una dirección de servidor DNS.

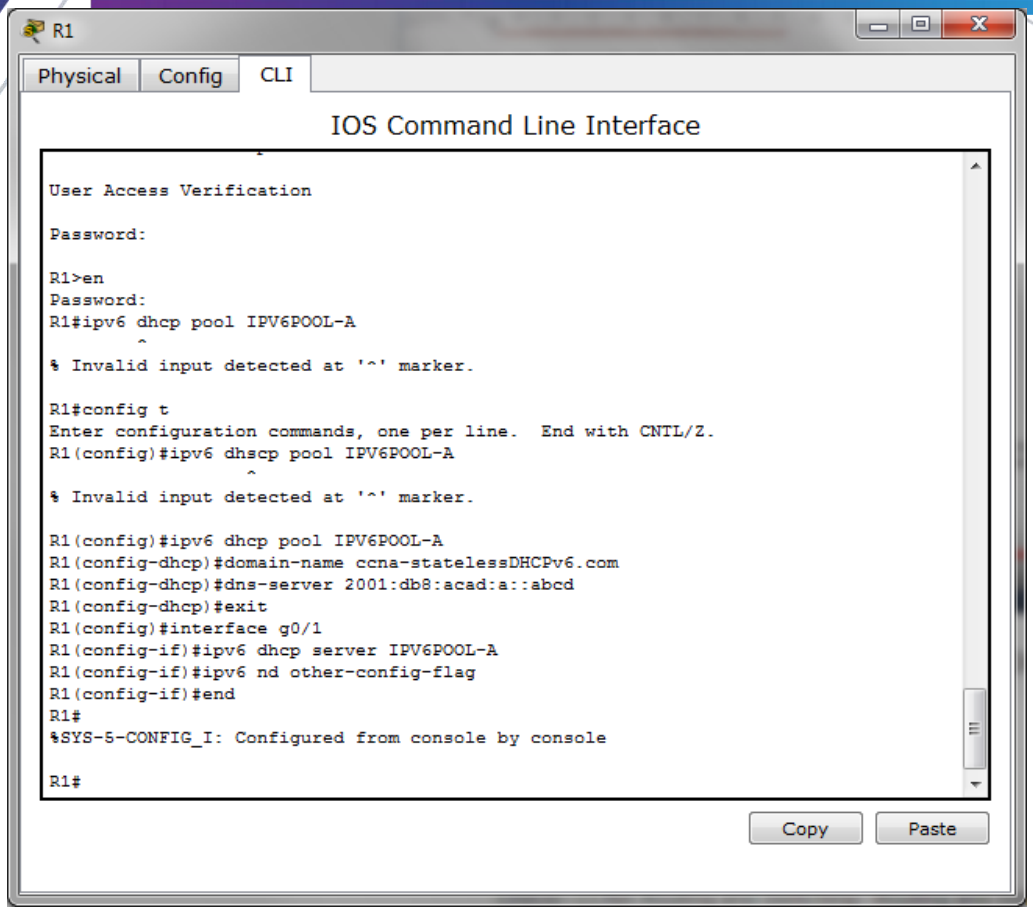
R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**
R1(config-dhcpv6)# **exit**

d. Asigne el pool de DHCPv6 a la interfaz.

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

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

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

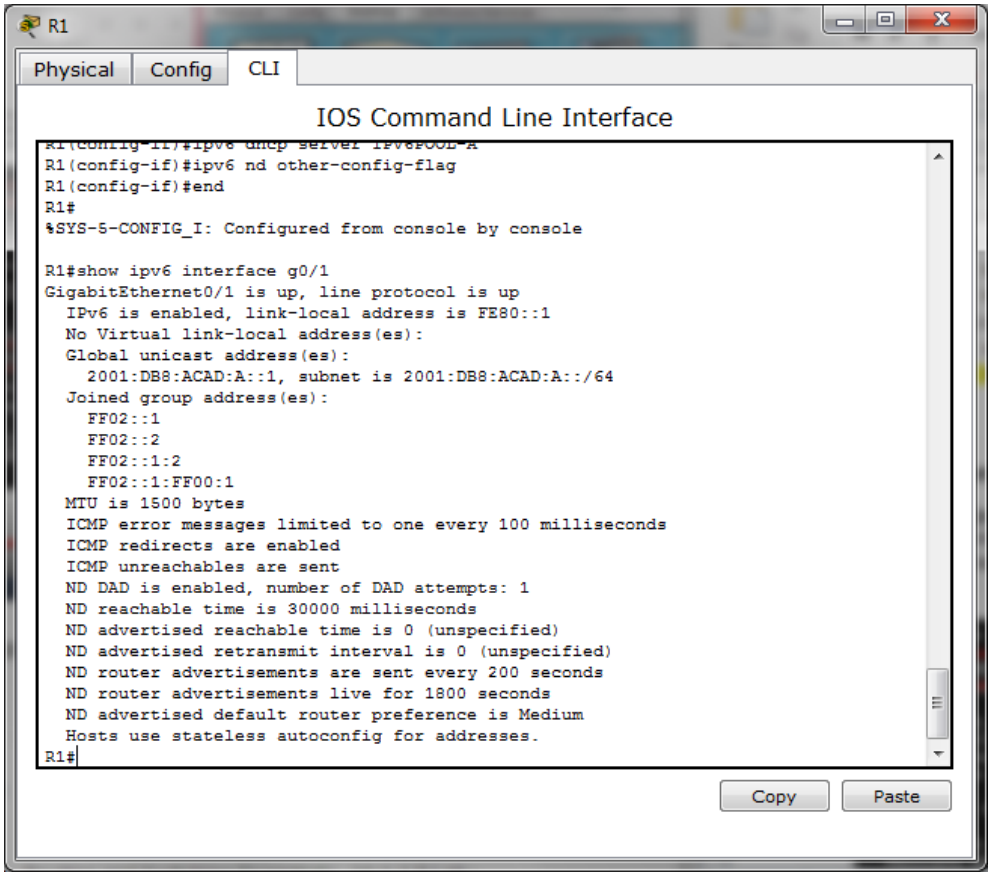



**Step 2: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.**

Use el comando **show ipv6 interface g0/1** para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando **show** verifica que se haya establecido other-config-flag.

R1# **show ipv6 interface g0/1**
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:2
FF02::1:FF00:1
FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds

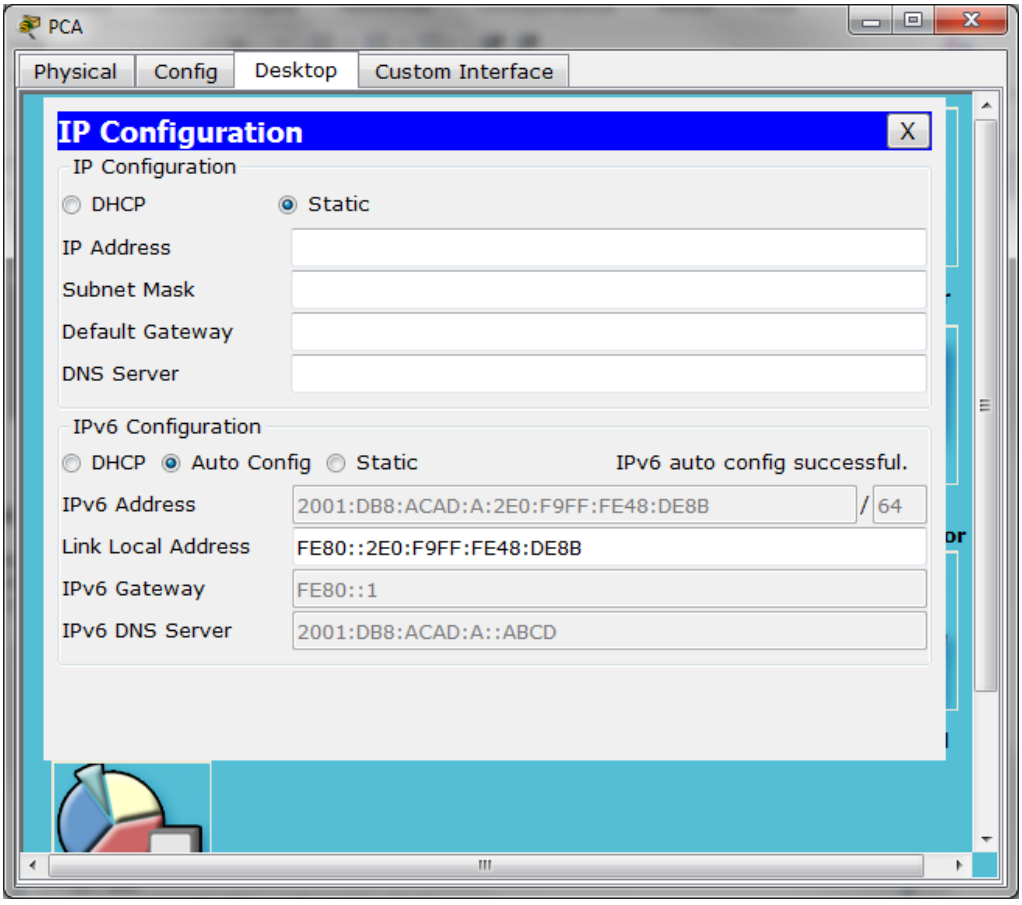
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds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




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

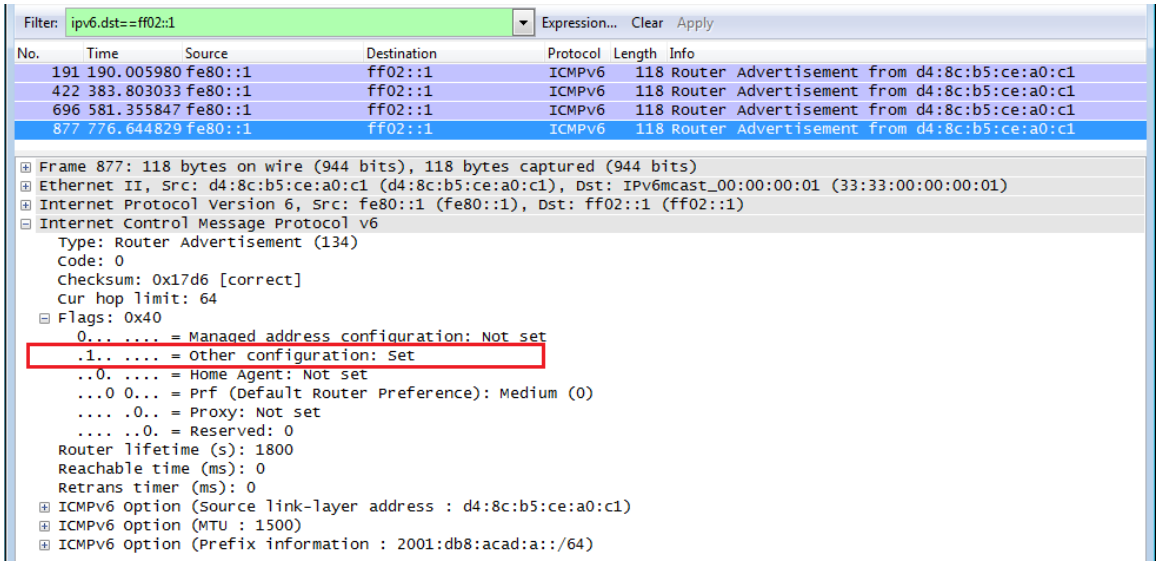
Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente mediante SLAAC.

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : ccna-statelessDHCPv6.com
   Descripción . . . . . . . . . . . . . . . : Conexión de red Intel(R) PRO/1000
MT
   Dirección física. . . . . . . . . . . . . : 00-0C-29-E3-23-17
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11(Preferido)

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

Adaptador de túnel isatap.localdomain:

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



**Step 4: ver los mensajes RA en Wireshark.**

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




**Step 5: verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.**

Use los comandos **show ipv6 dhcp binding** y **show ipv6 dhcp pool** para verificar que la PC-A no haya obtenido una dirección IPv6 del pool de DHCPv6.

R1# **show ipv6 dhcp binding**

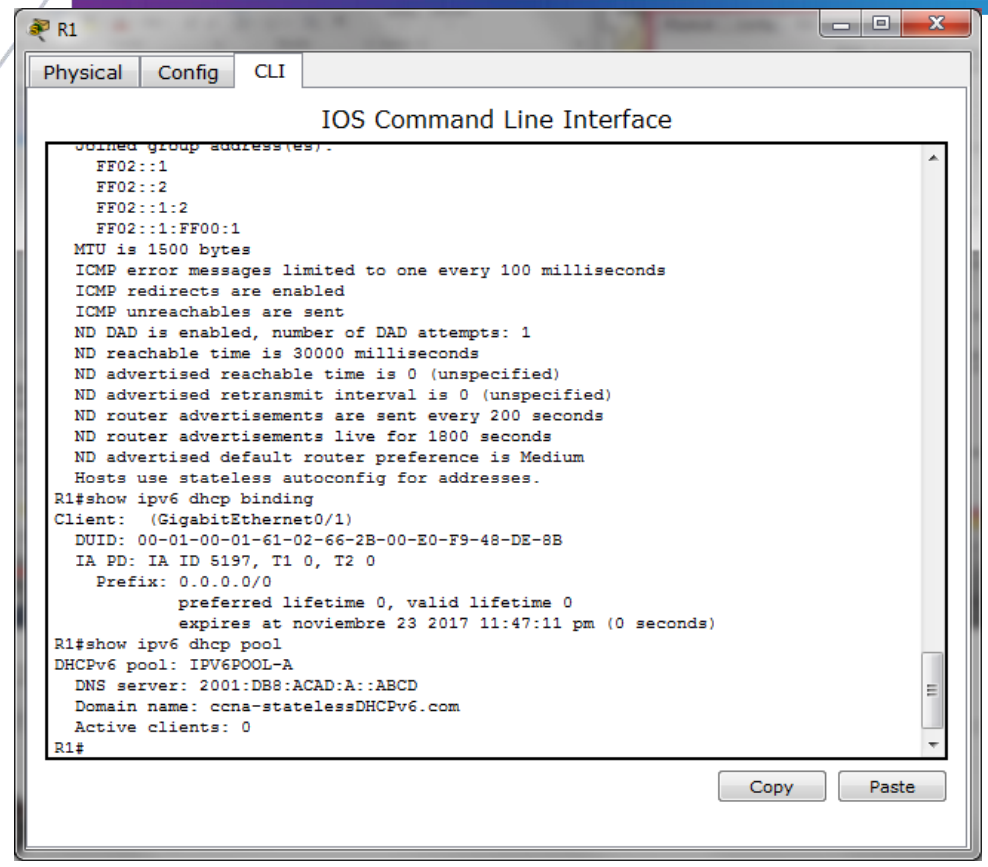
R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-statelessDHCPv6.com

Active clients: 0




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

a. Desactive la interfaz F0/6 del S1.

**Nota:** la desactivación de la interfaz F0/6 evita que la PC-A reciba una nueva dirección IPv6 antes de que usted vuelva a configurar el R1 para DHCPv6 con estado en la parte 4.

S1(config)# **interface f0/6**

S1(config-if)# **shutdown**

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

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

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

2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

## Part 17: configurar la red para DHCPv6 con estado

### Step 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.


### Step 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.

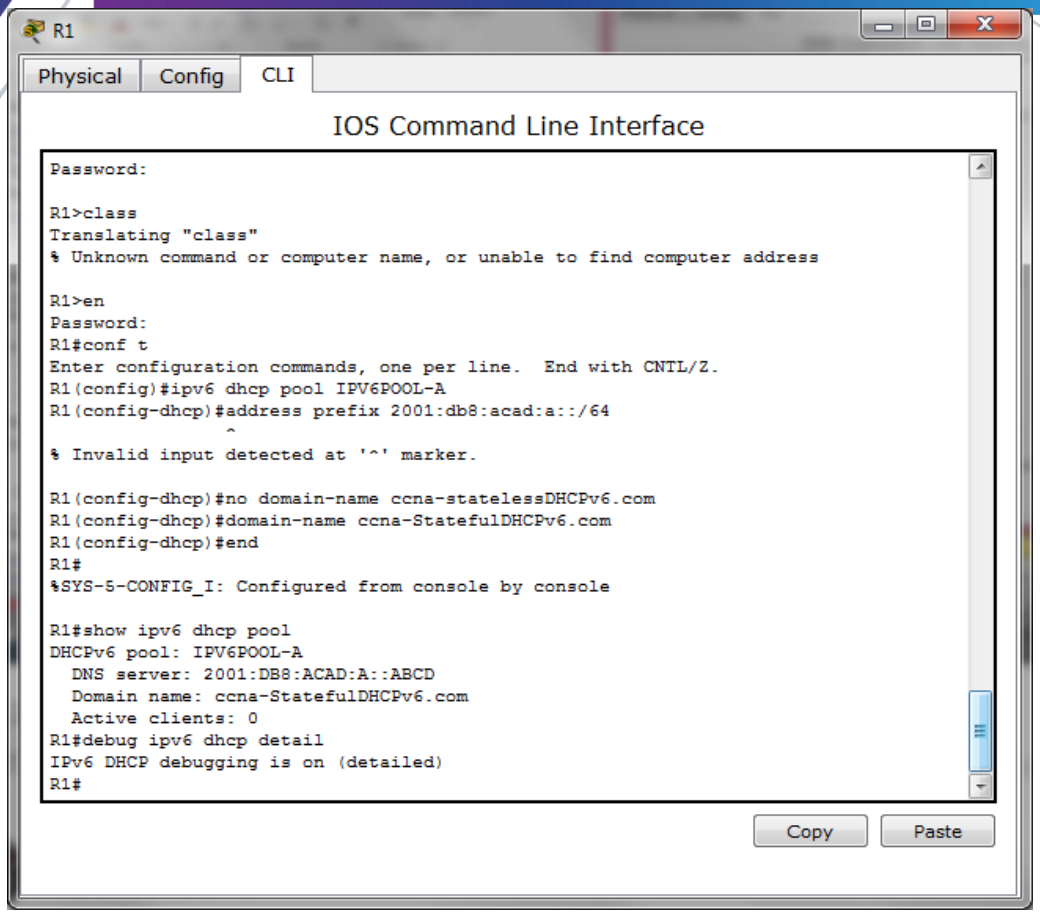
R1(config-dhcpv6)# **no domain-name ccna-statelessDHCPv6.com**
R1(config-dhcpv6)# **domain-name ccna-StatefulDHCPv6.com**
R1(config-dhcpv6)# **end**

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)




**Step 3: establecer el indicador en G0/1 para DHCPv6 con estado.**

**Nota:** la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.

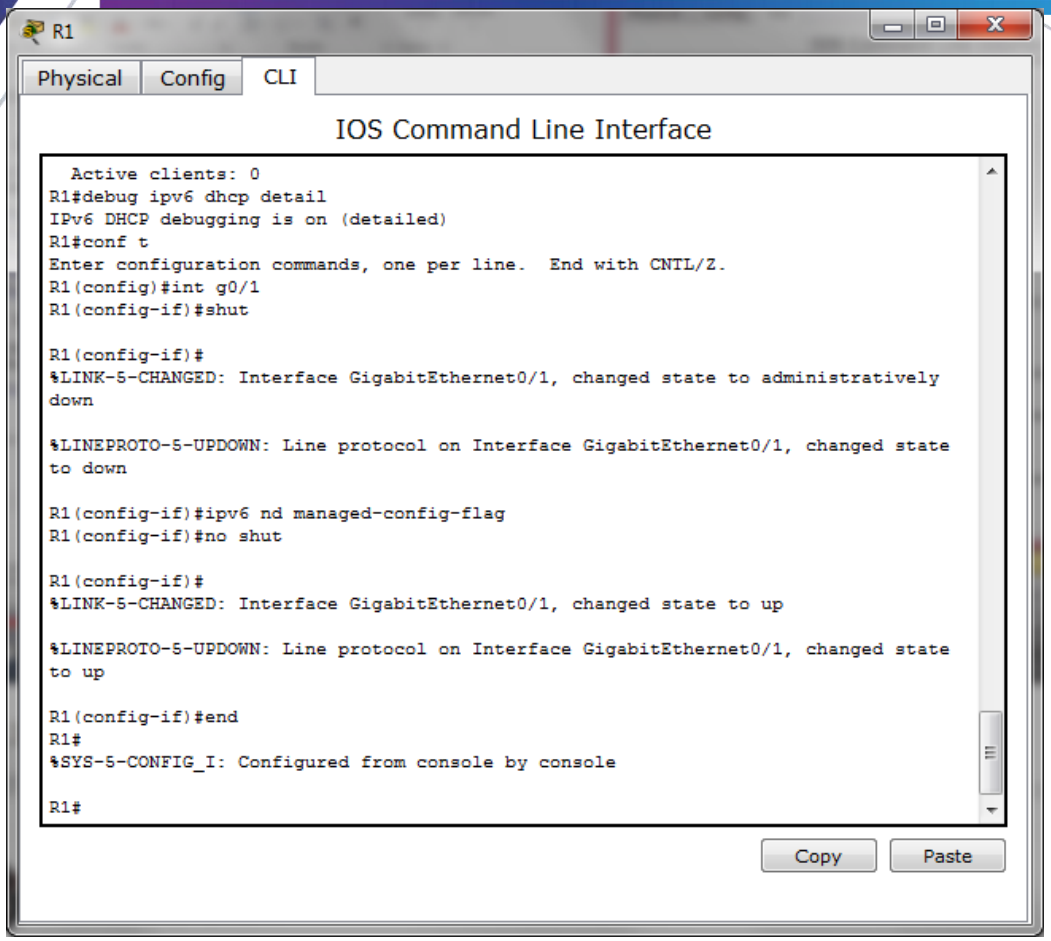
R1(config)# **interface g0/1**

R1(config-if)# **shutdown**

R1(config-if)# **ipv6 nd managed-config-flag**

R1(config-if)# **no shutdown**

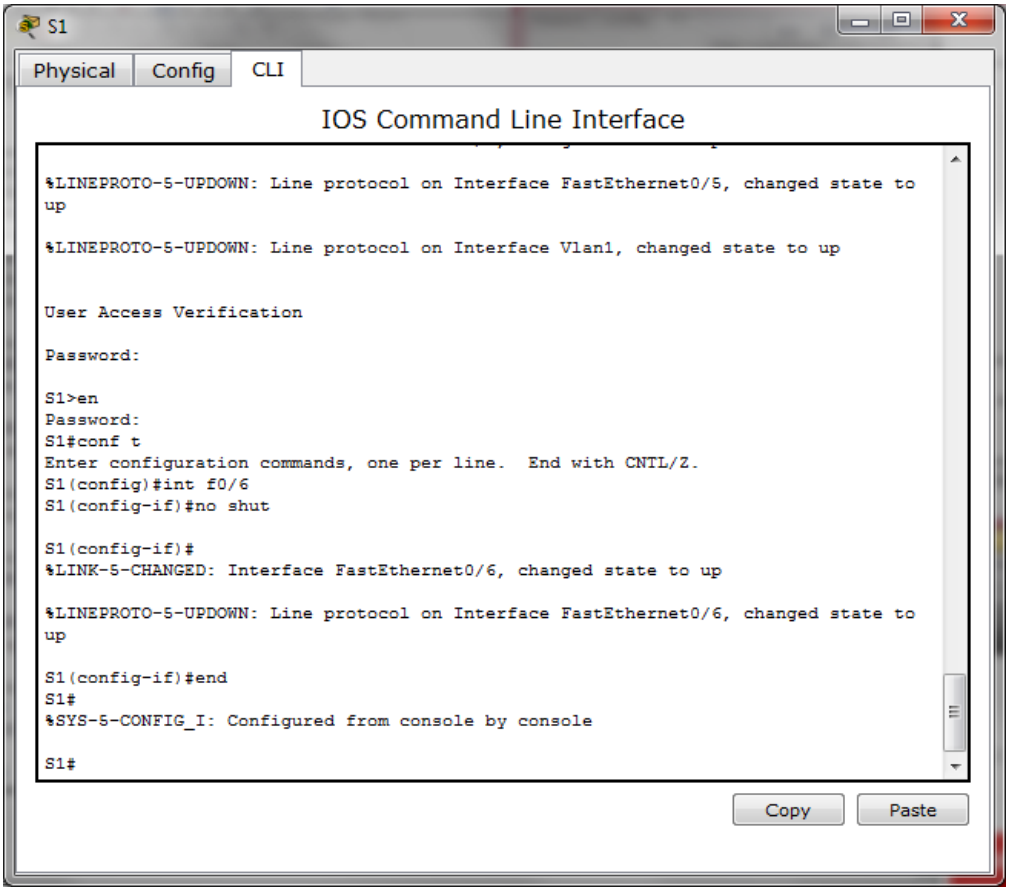
R1(config-if)# **end**


R1
Physical
Config
CLI
IOS Command Line Interface
Active clients: 0
R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#shut
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
R1(config-if)#ipv6 nd managed-config-flag
R1(config-if)#no shut
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
Copy
Paste

**Step 4: habilitar la interfaz F0/6 en el S1.**

Ahora que configuró el R1 para DHCPv6 con estado, puede volver a conectar la PC-A a la red activando la interfaz F0/6 en el S1.

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




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

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.

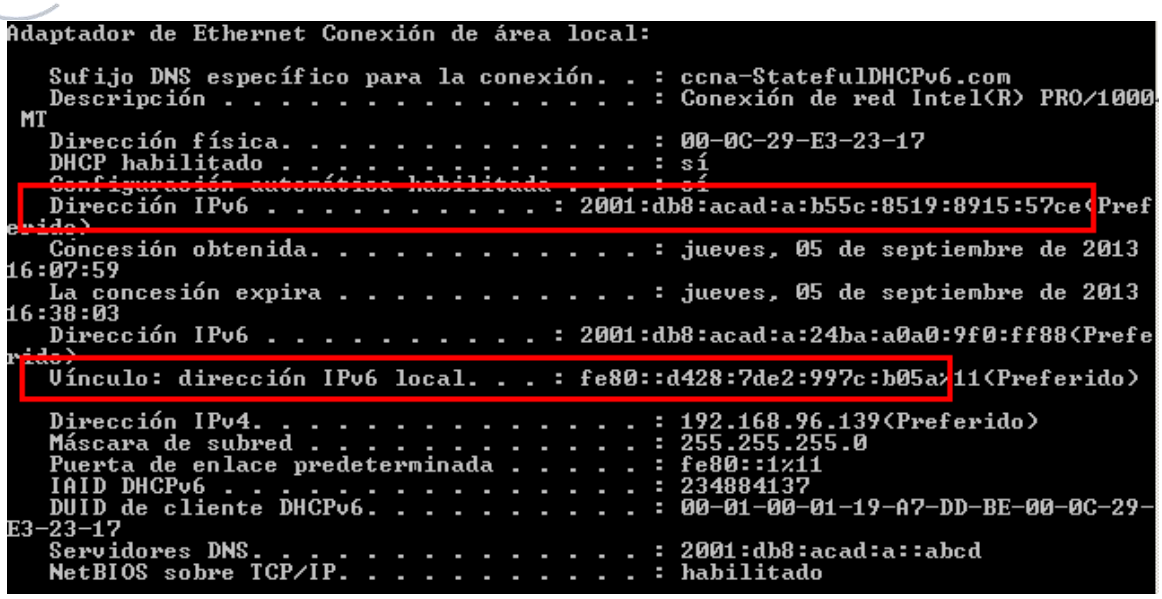
c. Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

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)




e. Emita el comando **undebug all** en el R1 para detener la depuración de DHCPv6.

**Nota:** escribir **u all** es la forma más abreviada de este comando y sirve para saber si quiere evitar que los mensajes de depuración se desplacen hacia abajo constantemente en la pantalla de la sesión de terminal. Si hay varias depuraciones en proceso, el comando **undebug all** las detiene todas.

R1# **u all**

Se ha desactivado toda depuración posible

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

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

*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents

*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

*Mar 5 16:42:39.775: dst FF02::1:2

*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238

*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2

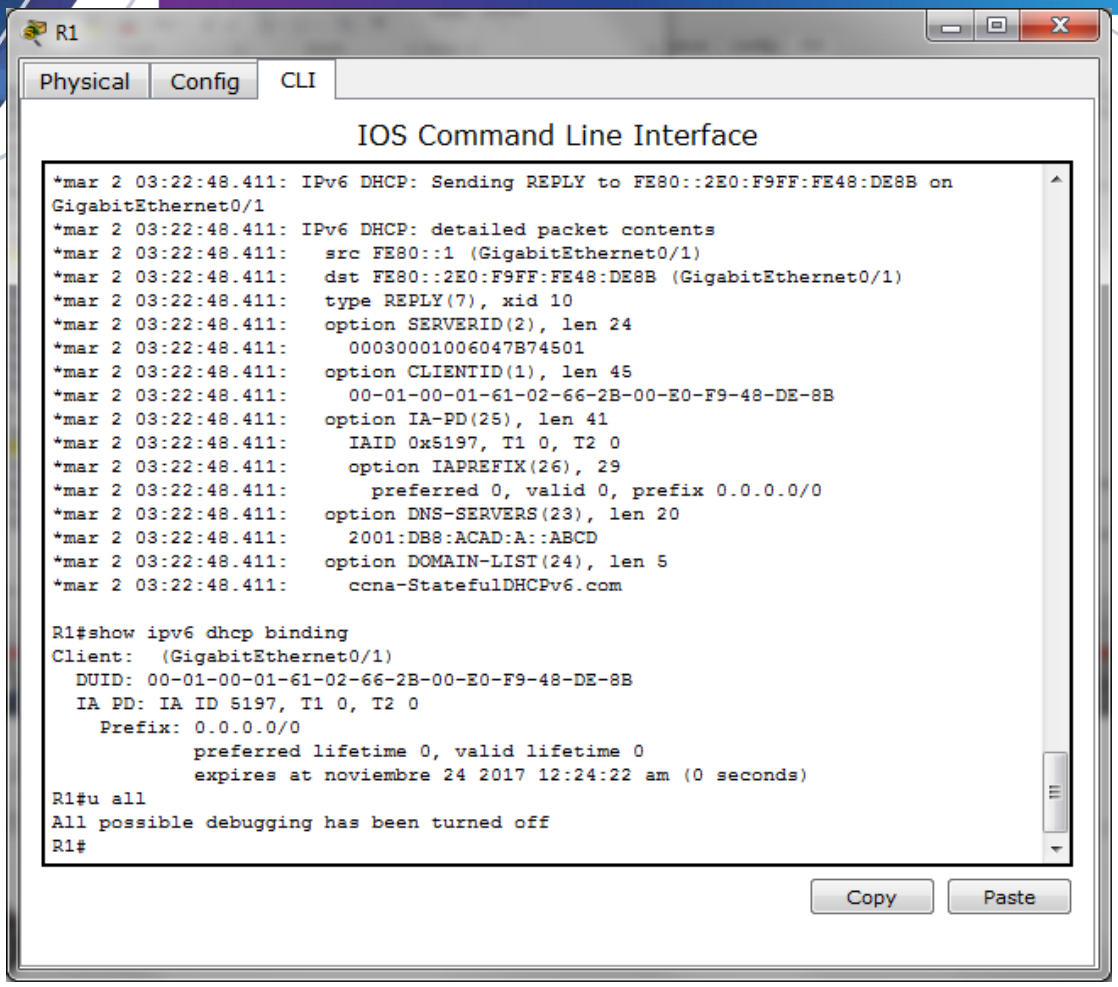
*Mar 5 16:42:39.775: elapsed-time 6300

*Mar 5 16:42:39.775: option CLIENTID(1), len 14

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

*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

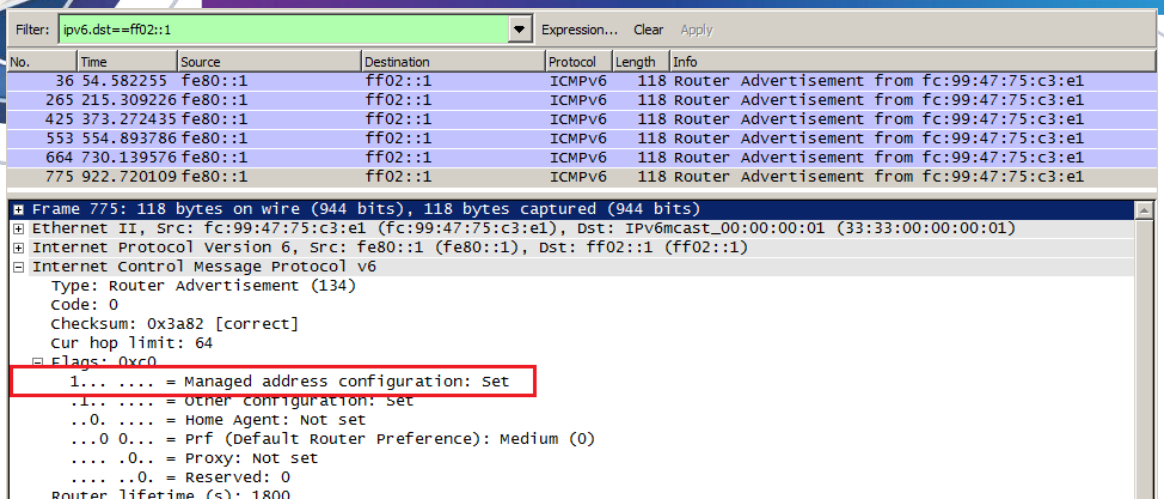
```
*Mar  5 16:42:39.779: IPv6 DHCP: detailed packet contents
*Mar  5 16:42:39.779:   src FE80::1
*Mar  5 16:42:39.779:   dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar  5 16:42:39.779:   type REPLY(7), xid 1039238
*Mar  5 16:42:39.779:   option SERVERID(2), len 10
*Mar  5 16:42:39.779:     00030001FC994775C3E0
*Mar  5 16:42:39.779:   option CLIENTID(1), len 14
*Mar  5 16:42:39.779:     00010001
R1#17F6723D000C298D5444
*Mar  5 16:42:39.779:   option IA-NA(3), len 40
*Mar  5 16:42:39.779:     IAID 0x0E000C29, T1 43200, T2 69120
*Mar  5 16:42:39.779:     option IAADDR(5), len 24
*Mar  5 16:42:39.779:       IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar  5 16:42:39.779:       preferred 86400, valid 172800
*Mar  5 16:42:39.779:   option DNS-SERVERS(23), len 16
*Mar  5 16:42:39.779:     2001:DB8:ACAD:A::ABCD
*Mar  5 16:42:39.779:   option DOMAIN-LIST(24), len 26
*Mar  5 16:42:39.779:     ccna-StatefulDHCPv6.com
```



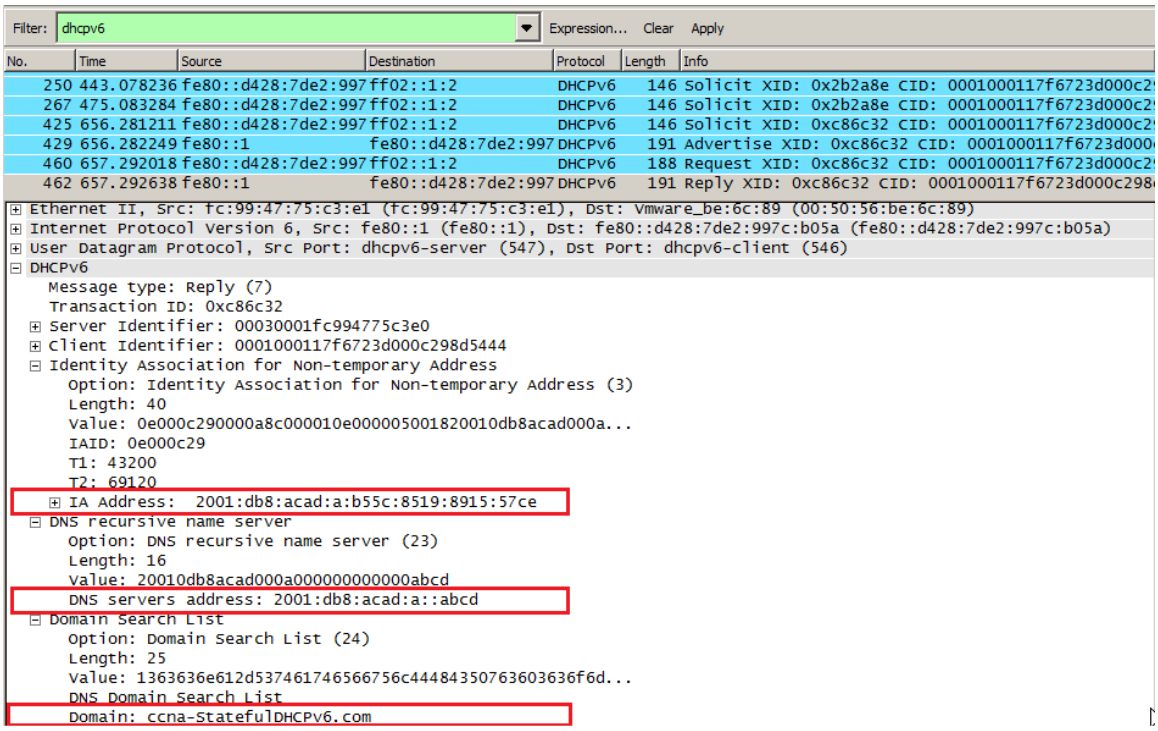

**Step 6: verificar DHCPv6 con estado en la PC-A.**

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?

**dhcp v6 con estado usa más recursos de memoria y requiere que el router guarde dinámicamente el estado de información acerca de los clientes dhcp6, sin estado no necesita guardar las direcciones porque no utiliza el servidor dhcp**

2. ¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado? **Cisco recomienda dhcpv6 sin estado**

### 10.3.1.1 IoE and DHCP Instructions

**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.

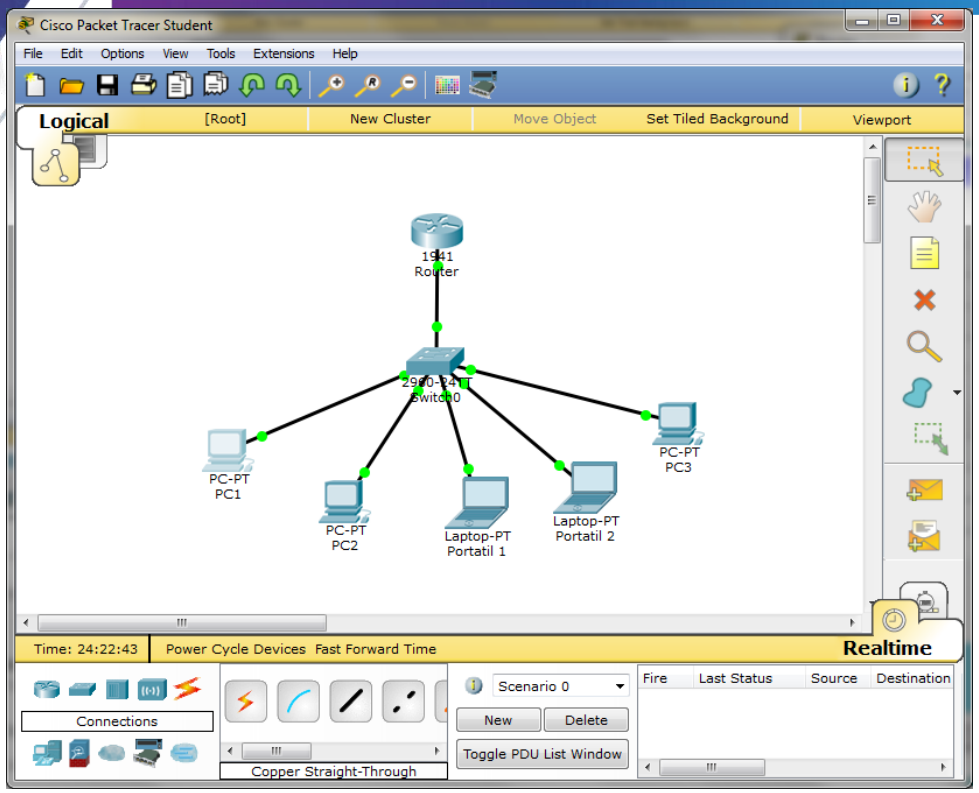
Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

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

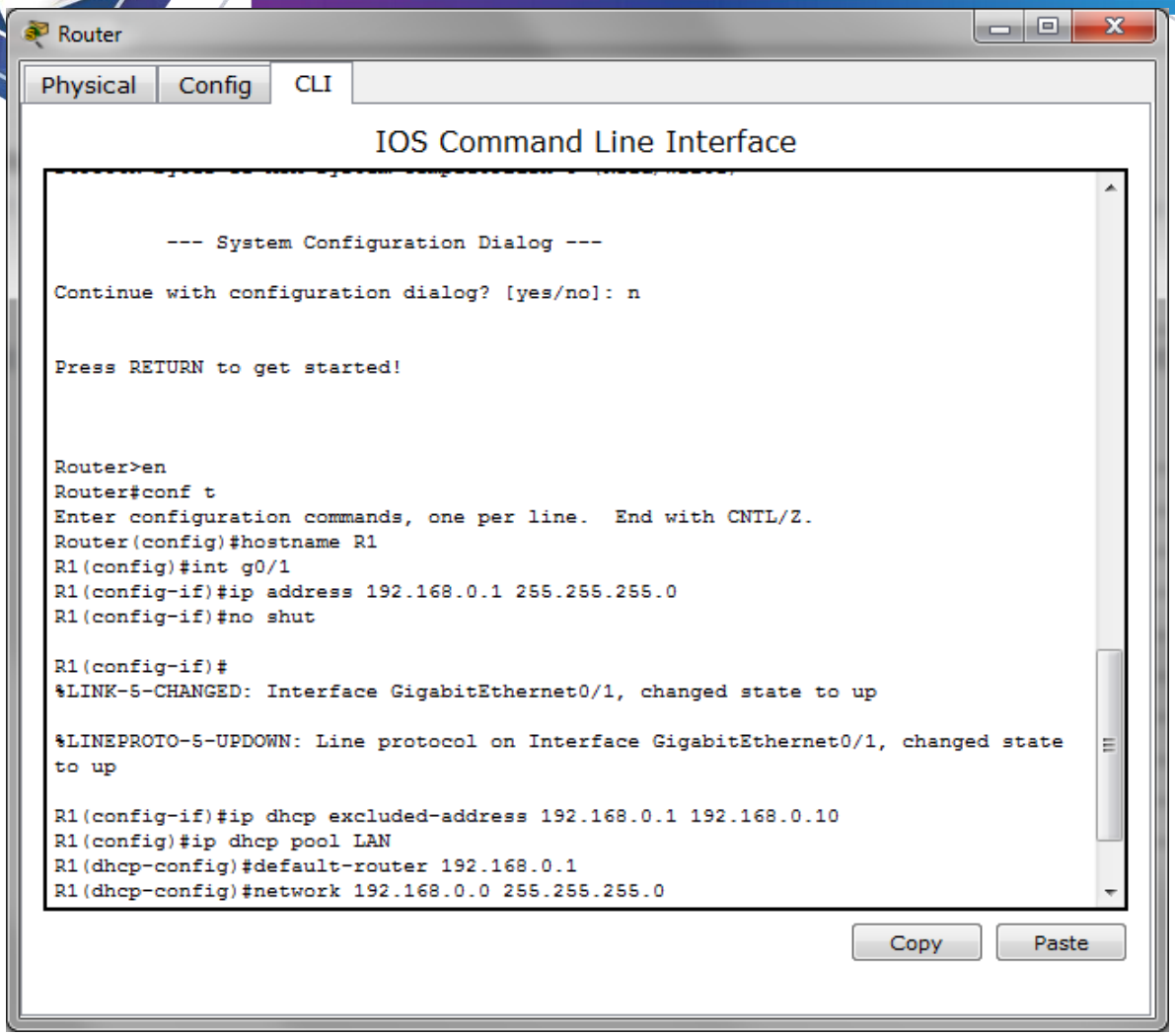
- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.
- Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones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

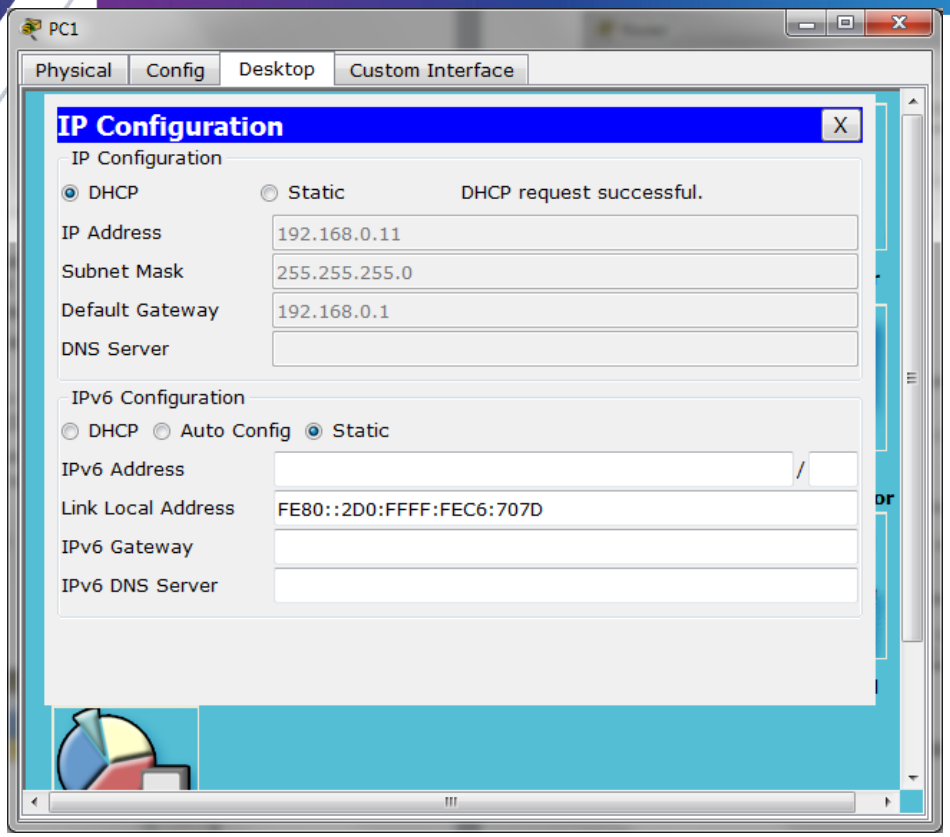
**Recursos necesarios**

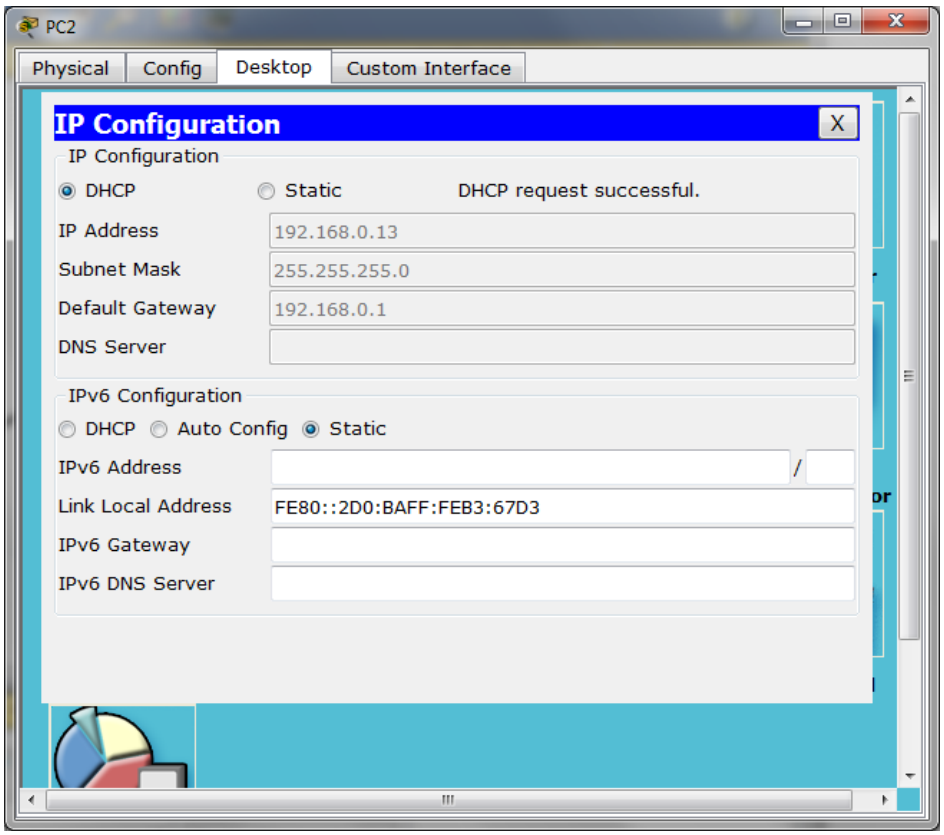
Software de Packet Tracer

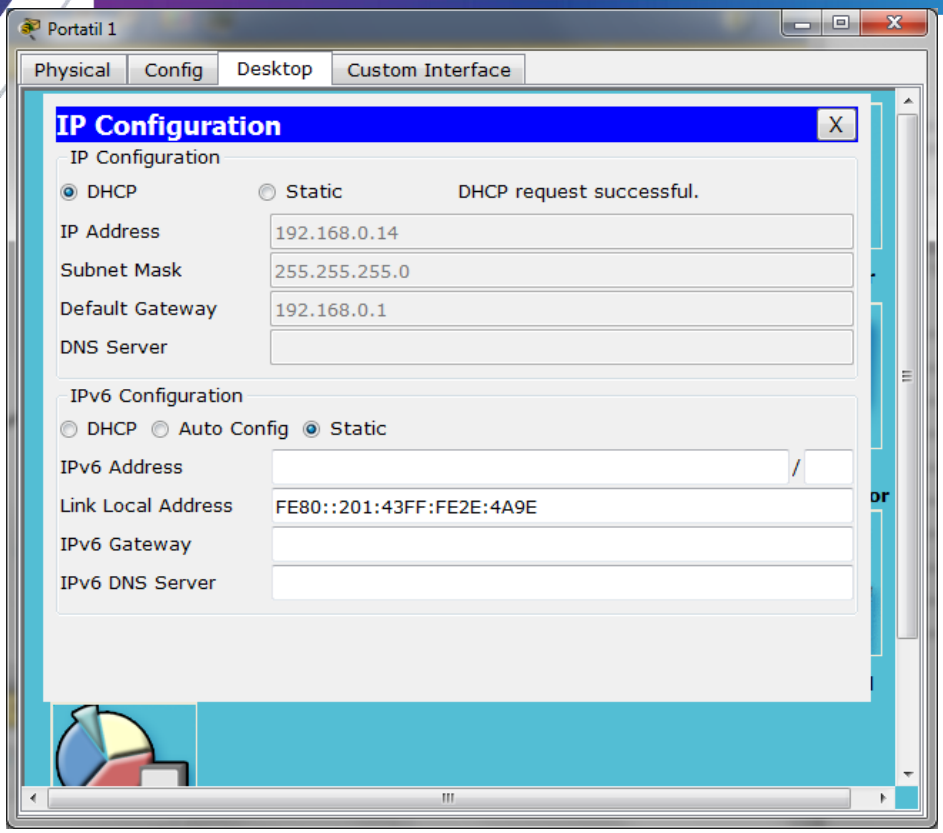


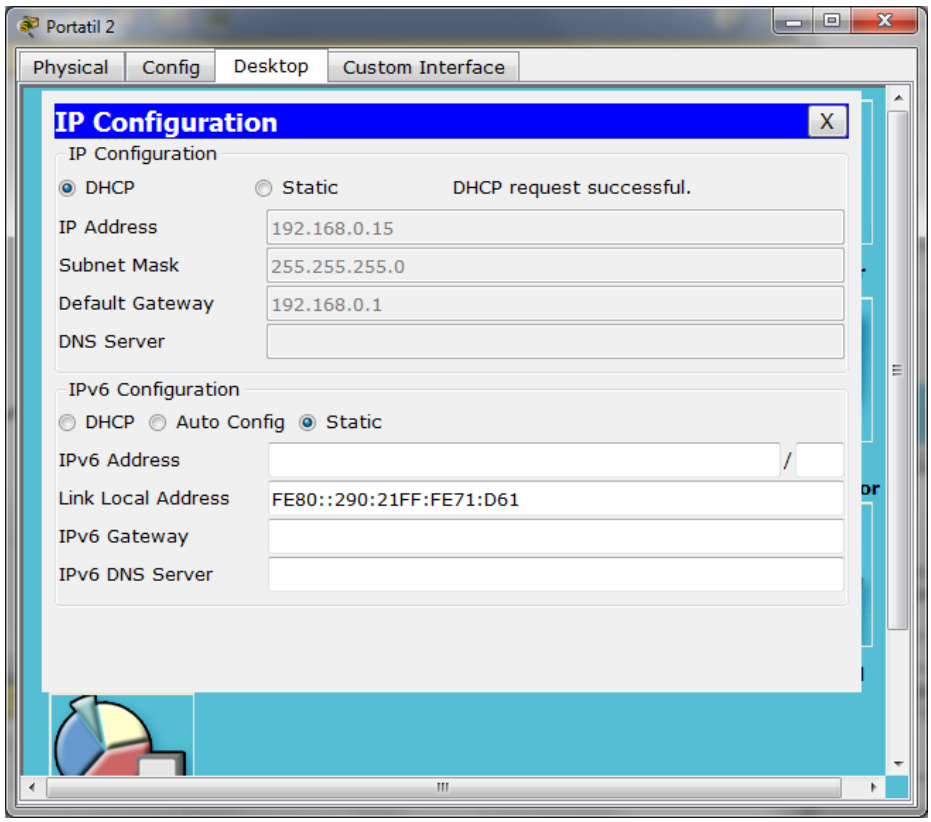

**Configuración del router para que funcione con dhcp**

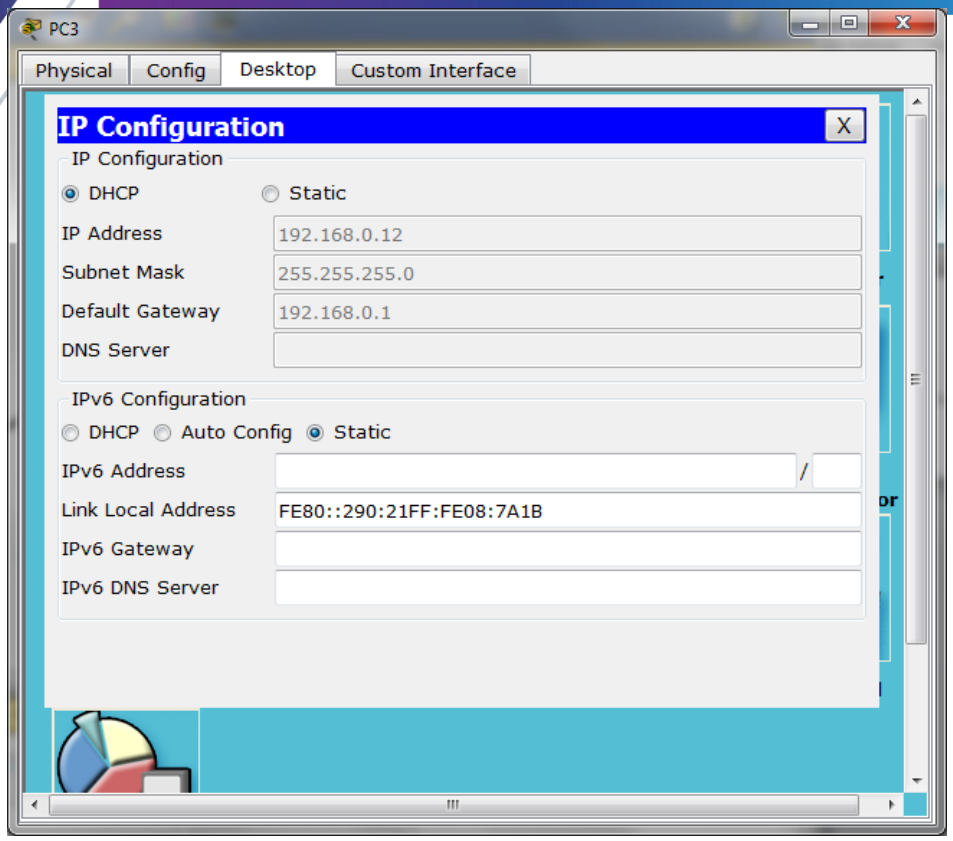

Router
Physical
Config
CLI
IOS Command Line Interface
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/1
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)#ip dhcp excluded-address 192.168.0.1 192.168.0.10
R1(config)#ip dhcp pool LAN
R1(dhcp-config)#default-router 192.168.0.1
R1(dhcp-config)#network 192.168.0.0 255.255.255.0
Copy
Paste


PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.0.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:FFFF:FEC6:707D
IPv6 Gateway
IPv6 DNS Server


PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.0.13
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:BAFF:FEB3:67D3
IPv6 Gateway
IPv6 DNS Server


Portatil 1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.0.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:43FF:FE2E:4A9E
IPv6 Gateway
IPv6 DNS Server


Portatil 2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.0.15
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::290:21FF:FE71:D61
IPv6 Gateway
IPv6 DNS Server




**Reflexión**

1. ¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica? ¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?

   **El router 1941 ofrece una amplia gama de servicios de seguridad en comparación con otros ISR más pequeños, lo cual lo convierte en un router muy confiable en cuanto a la seguridad y demás prestaciones. Igualmente se podría implementar un ISR más pequeño como servidor DHCP, solamente que tendría un menor rendimiento y sería muy vulnerable en cuanto 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.

   - ✓ **Se puede controlar y monitorear el estado y funcionamiento de un PCL mediante el direccionamiento IP de un servidor DHCP en una fábrica de procesos productivos.**
   - ✓ **En una empresa que tenga instalado un circuito cerrado de televisión con cámaras IP para asignar las direcciones con el servidor DHCP del router cisco.**
   - ✓ **Para controlar los diferentes electrodomésticos que trabajan con direcciones IP para que se conecten automáticamente sin preocuparnos por escribirlas manualmente.**

- **Para agilizar la asignación de direcciones IP en una empresa que tenga más de 20 equipos, evitándonos procesos manuales que podrían ocasionar duplicados en el direccionamiento IP.**

## 11.2.2.6 Lab - Configuring Dynamic and Static NAT

### Práctica de laboratorio: configuración de NAT dinámica y estática

### Topología

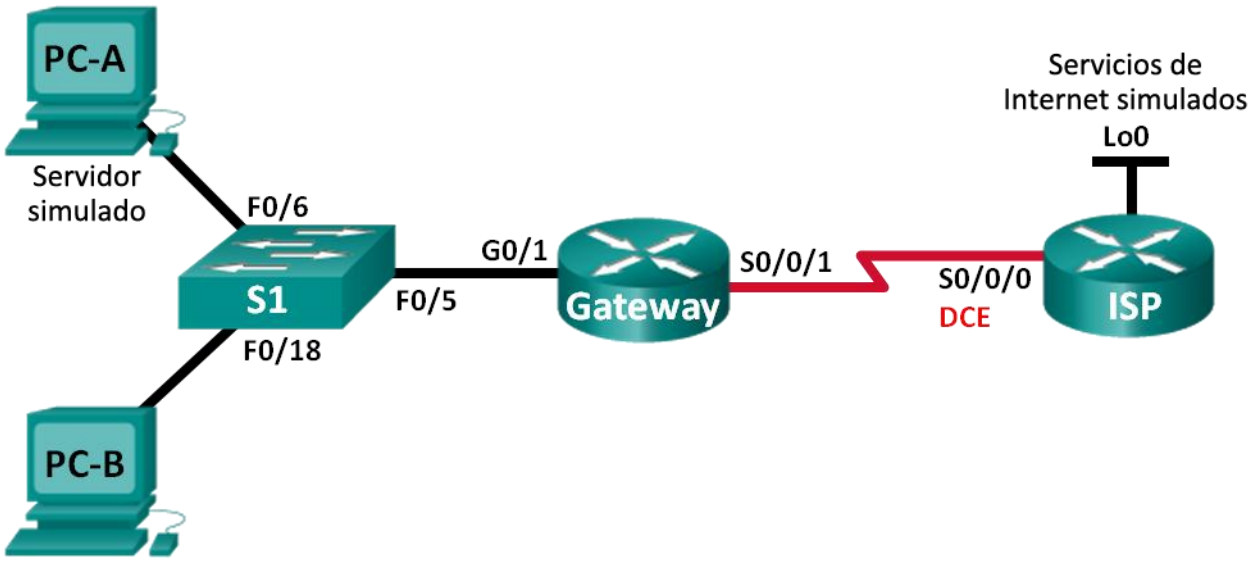


**Tabla de direccionamiento**

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

## Objetivos

**Parte 1: armar la red y verificar la conectividad**

**Parte 2: configurar y verificar la NAT estática**

**Parte 3: configurar y verificar la NAT dinámica**

## Información básica/situación

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

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

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

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

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

**Recursos necesarios**

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

**Part 18: armar la red y verificar la conectividad**

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

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

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

**Step 2: configurar los equipos host.**

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

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

a. Desactive la búsqueda del DNS.

b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

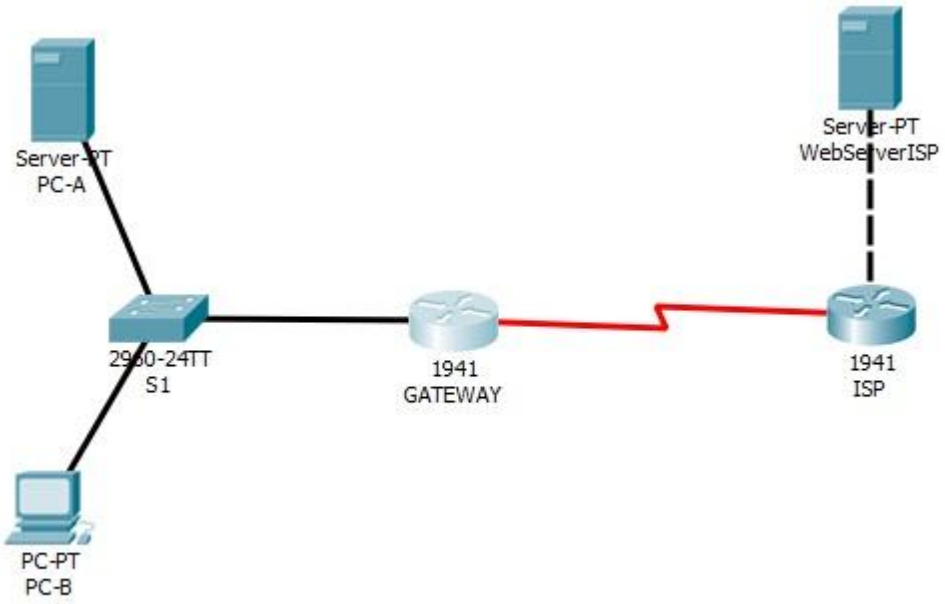
c. Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.

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

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

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

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




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

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**

**Packet Tracert no soporta estos comandos para ello se va a utilizar un servidor web del ISP**

**Step 6: configurar el routing estático.**

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

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

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

b. Cree una ruta predeterminada del router Gateway al router ISP.

Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

```
GATEWAY(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

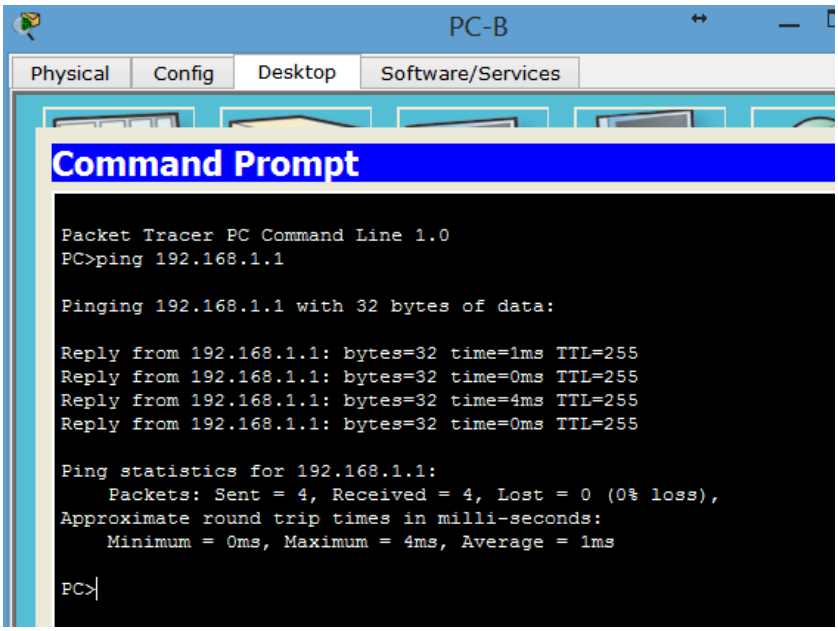
**Step 7: Guardar la configuración en ejecución en la configuración de inicio.**

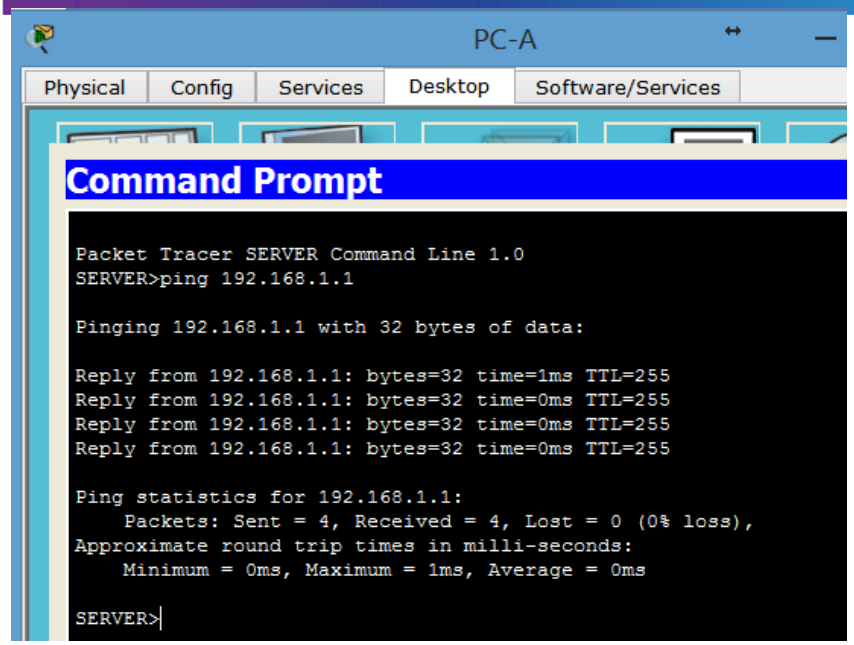
```
ISP#copy running-config star
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

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

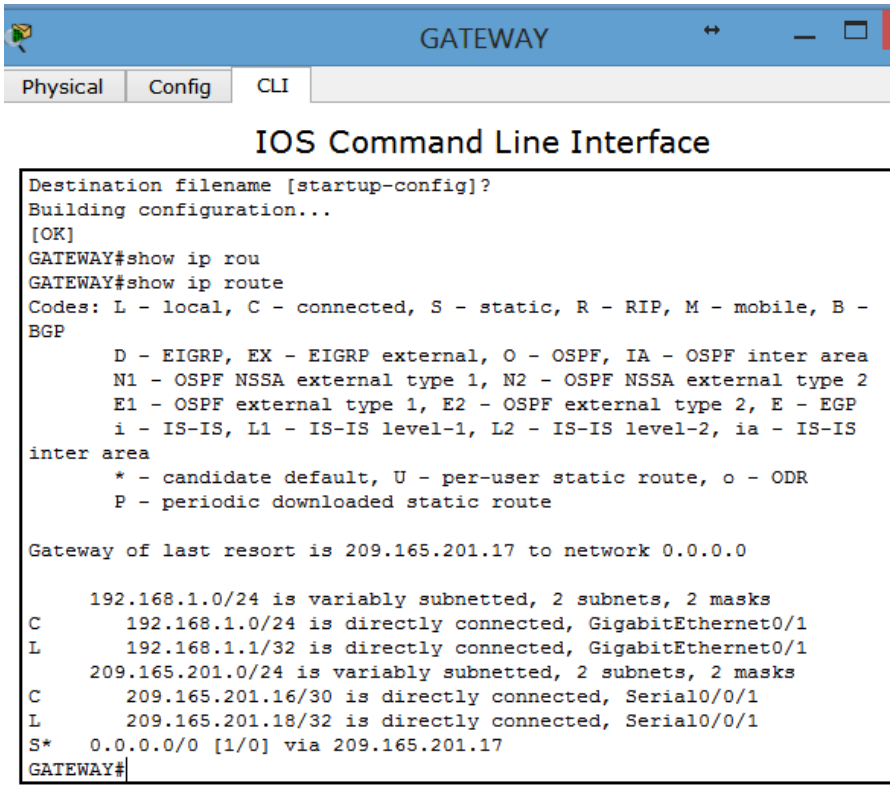
**Step 8: Verificar la conectividad de la red**

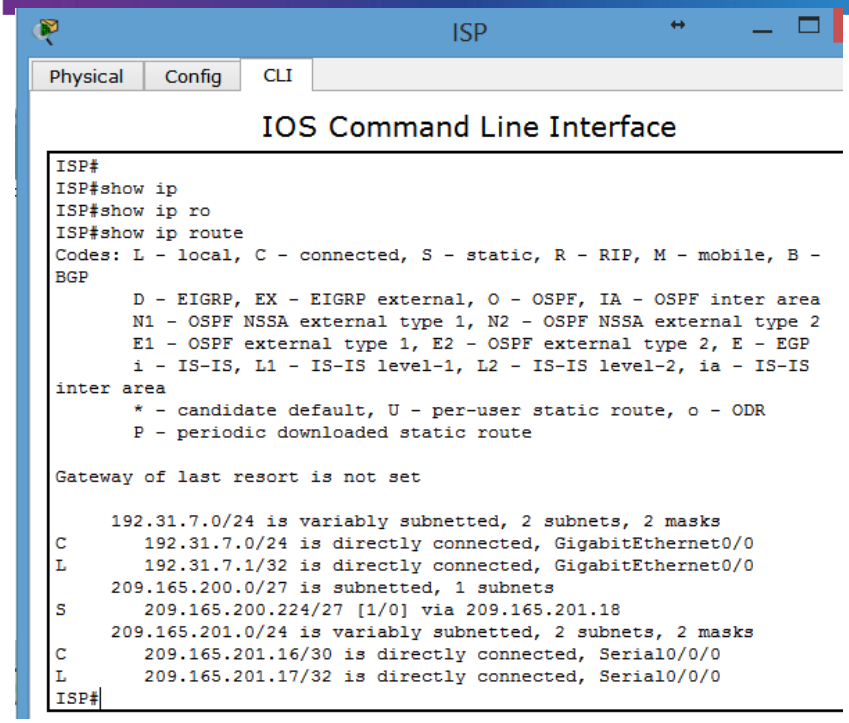
a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.






b. Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.






**Part 19: configurar y verificar la NAT estática.**

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

**Step 1: configurar una asignación estática.**

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

Gateway(config)# **ip nat inside source static 192.168.1.20 209.165.200.225**

```
GATEWAY(config)#ip nat inside source static 192.168.1.20 209.165.200.225
GATEWAY(config)#
```

**Step 2: Especifique las interfaces.**

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

Gateway(config)# **interface g0/1**
Gateway(config-if)# **ip nat inside**
Gateway(config-if)# **interface s0/0/1**
Gateway(config-if)# **ip nat outside**

```
GATEWAY(config)#interface g0/1
GATEWAY(config-if)#ip nat inside
GATEWAY(config-if)#exit
GATEWAY(config)#inter
GATEWAY(config)#interface s0/0/1
GATEWAY(config-if)#ip nat ou
GATEWAY(config-if)#ip nat outside
GATEWAY(config-if)#
```

**Step 3: probar la configuración.**

a. Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.225 192.168.1.20 --- ---

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside
global
---  209.165.200.225   192.168.1.20       ---                ---

GATEWAY#
```

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

192.168.1.20 = **Es la dirección IP publica 209.165.200.225**

¿Quién asigna la dirección global interna?

**Es asignada por el router desde el Pool de NAT.**

¿Quién asigna la dirección local interna?

**El administrador de red**

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

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=14ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 4ms
```

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 209.165.200.225:10192.168.1.20:10    192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.225:11192.168.1.20:11    192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.225:12192.168.1.20:12    192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.225:9 192.168.1.20:9     192.31.7.1:9       192.31.7.1:9
---  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? **Puertos 9, 10, 11 y 12**

**Nota:** puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23
--- 209.165.200.225 192.168.1.20 --- ---

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

GATEWAY#
```

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

¿Qué protocolo se usó para esta traducción? **Se usó el protocolo TCP**

¿Cuáles son los números de puerto que se usaron?

Global/local interno**: 1025**

Global/local externo: **23**

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

```
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=11ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126
Reply from 209.165.200.225: bytes=32 time=13ms TTL=126
Reply from 209.165.200.225: bytes=32 time=13ms TTL=126

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 9ms
```

e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12

--- 209.165.200.225 192.168.1.20 --- ---

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.254:1     192.31.7.254:1
icmp 209.165.200.225:2 192.168.1.20:2     192.31.7.254:2     192.31.7.254:2
icmp 209.165.200.225:3 192.168.1.20:3     192.31.7.254:3     192.31.7.254:3
icmp 209.165.200.225:4 192.168.1.20:4     192.31.7.254:4     192.31.7.254:4
---  209.165.200.225   192.168.1.20       ---                ---
tcp 209.165.200.225:1025192.168.1.20:1025  192.31.7.1:23      192.31.7.1:23
```

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

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

Gateway# **show ip nat statics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 00:02:12 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

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

```
GATEWAY#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 49  Misses: 13
Expired translations: 12
Dynamic mappings:
GATEWAY#
```

## Part 20: configurar y verificar la NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

### Step 1: borrar las NAT.

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

Gateway# **clear ip nat translation ***

Gateway# **clear ip nat statistics**

### Step 2: definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

Gateway(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

```
GATEWAY(config)#access-list 1 permit 192.168.1.0 0.0.0.255
GATEWAY(config)#
```

### Step 3: verificar que la configuración de interfaces NAT siga siendo válida.

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

```
GATEWAY#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 49  Misses: 13
Expired translations: 12
Dynamic mappings:
GATEWAY#
```

**Step 4: definir el conjunto de direcciones IP públicas utilizables.**

Gateway(config)# **ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224**

```
GATEWAY(config)#ip nat pool public_access 209.165.200.242
209.165.200.254 netmask 255.255.255.224
GATEWAY(config)#
```

**Step 5: definir la NAT desde la lista de origen interna hasta el conjunto externo.**

**Nota:** recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

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

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

**Step 6: probar la configuración.**

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=2ms 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=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 7ms
```

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 = **es la dirección IP 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? **Puertos 5,6,7 y 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  192.31.7.254:80    192.31.7.254:80
tcp 209.165.200.242:1026192.168.1.21:1026  192.31.7.254:80    192.31.7.254:80
```

¿Qué protocolo se usó en esta traducción? **Protocolo TCP**

¿Qué números de puerto se usaron?

Interno: **1025 Y 1026**

Externo: **Puerto 80**

¿Qué número de puerto bien conocido y qué servicio se usaron? **Puerto 80 y es utilizado para servicios de páginas Web.**

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

Gateway# **show ip nat statistics**

Total active translations: 3 (1 static, 2 dynamic; 1 extended)

Peak translations: 17, occurred 00:06:40 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 345 Misses: 0

CEF Translated packets: 345, CEF Punted packets: 0

Expired translations: 20

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 2

pool public_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

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

```
GATEWAY#show ip nat statistics
Total translations: 3 (1 static, 2 dynamic, 2 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 67  Misses: 19
Expired translations: 16
Dynamic mappings:
-- Inside Source
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
GATEWAY#
```

**Step 7: eliminar la entrada de NAT estática.**

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

Gateway(config)# **no ip nat inside source static 192.168.1.20 209.165.200.225**

Static entry in use, do you want to delete child entries? [no]: **yes**

b. Borre las NAT y las estadísticas.

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

d. Muestre la tabla y las estadísticas de NAT.

Gateway# **show ip nat statistics**

Total active translations: 4 (0 static, 4 dynamic; 2 extended)

Peak translations: 15, occurred 00:00:43 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 16  Misses: 0

CEF Translated packets: 285, CEF Punted packets: 0

Expired translations: 11

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 4

pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13, allocated 2 (15%), misses 0

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

Gateway# **show ip nat translation**

| Pro | Inside global | Inside local | Outside local | Outside global |
|---|---|---|---|---|
| icmp | 209.165.200.243:512 | 192.168.1.20:512 | 192.31.7.1:512 | 192.31.7.1:512 |
| --- | 209.165.200.243 | 192.168.1.20 | --- | --- |
| icmp | 209.165.200.242:512 | 192.168.1.21:512 | 192.31.7.1:512 | 192.31.7.1:512 |
| --- | 209.165.200.242 | 192.168.1.21 | --- | --- |

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

**PC-B a 192.31.7.1**

```
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=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=14ms 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 = 1ms, Maximum = 14ms, Average = 10ms
```

**Tabla de Traducción PC-B a 192.31.7.1**

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.242:10192.168.1.21:10    192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.242:11192.168.1.21:11    192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.242:12192.168.1.21:12    192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.242:9 192.168.1.21:9     192.31.7.1:9       192.31.7.1:9
```

## Tabla de Estadísticas del PC-B a 192.31.7.1

```
GATEWAY#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 71  Misses: 23
Expired translations: 20
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13 , allocated 0 (0%), misses 0
GATEWAY#
```

## Ping desde PC-A a 192.31.7.1

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=13ms TTL=254
Reply from 192.31.7.1: bytes=32 time=14ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 7ms
```

## Tabla de Traducción desde PC-A a 192.31.7.1

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.242:13192.168.1.20:13    192.31.7.1:13      192.31.7.1:13
icmp 209.165.200.242:14192.168.1.20:14    192.31.7.1:14      192.31.7.1:14
icmp 209.165.200.242:15192.168.1.20:15    192.31.7.1:15      192.31.7.1:15
icmp 209.165.200.242:16192.168.1.20:16    192.31.7.1:16      192.31.7.1:16
tcp 209.165.200.242:1026192.168.1.20:1026  192.31.7.1:23      192.31.7.1:23
```

## Tabla de estadísticas desde el PC-A a 192.31.7.1

```
GATEWAY#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 127  Misses: 32
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
 pool public_access: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13 , allocated 1 (7%), misses 0
```

**Reflexión**

1. ¿Por qué debe utilizarse la NAT en una red?

**No hay suficientes direcciones IP públicas, además para evitar o reducir costos en la adquisición de direcciones IP públicas desde un ISP. NAT se utiliza porque proporciona medidas de seguridad a las direcciones IP internas hacia las redes externas.**

2. ¿Cuáles son las limitaciones de NAT?

**NAT utiliza la información IP o el número de puerto en la cabecera IP y TCP para la translación de paquetes. Necesita también una lista parcial de protocolos que no pueden ser usados por NAT, esto aumenta un poco la latencia.**

- **Se deteriora el rendimiento.**
- **Se deteriora la funcionalidad de extremo a extremo.**
- **Se reduce el seguimiento IP de extremo a extremo.**
- **El tunneling se torna más complicado.**
- **El inicio de las conexiones TCP puede interrumpirse.**

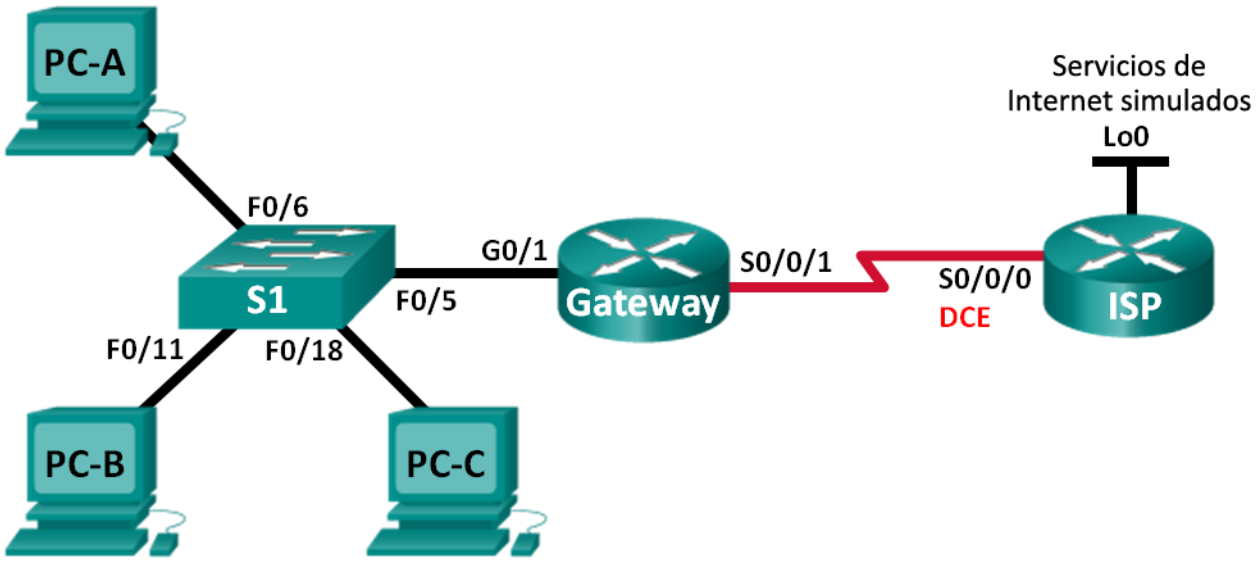
**Tabla de resumen de interfaces del router**

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

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

## 11.2.3.7 Lab - Configuring NAT Pool Overload and PAT

### Topología




### 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.

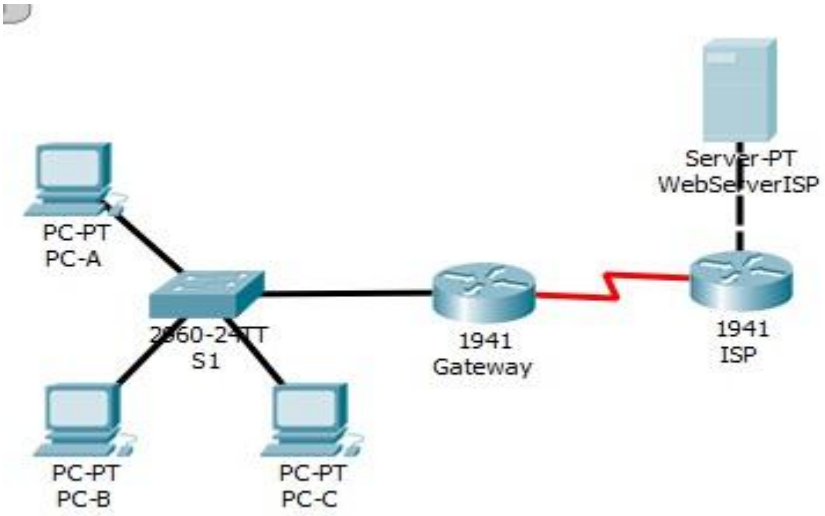
**Recursos necesarios**

- 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

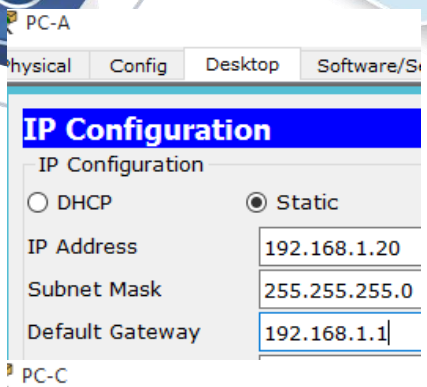
**Parte 1: armar la red y verificar la conectividad**

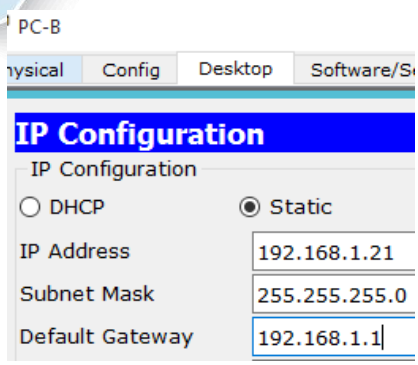
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

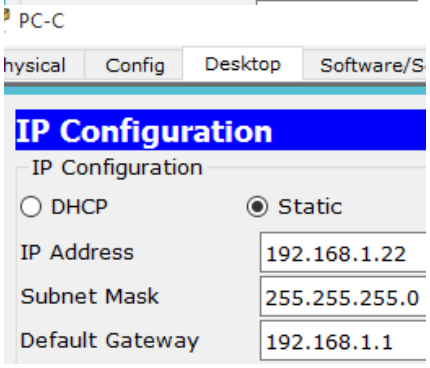
**Step 8: realizar el cableado de red tal como se muestra en la topología.**

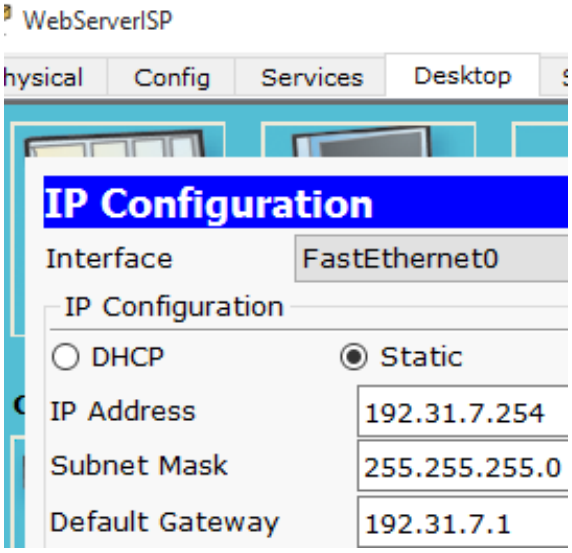


**Step 9: configurar los equipos host.**




la IP del servidor web debe estar dentro de la red .7.1

**Step 10: inicializar y volver a cargar los routers y los switches.**

**Step 11: 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.

**Gateway**

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#int g0/1
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config-if)#no shut

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

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

Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Gateway(config-if)#no shut
Gateway(config-if)#shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to administratively down
Gateway(config-if)#no shut

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

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#int g0/1
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config-if)#no shut

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

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

Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Gateway(config-if)#no shut
Gateway(config-if)#shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to
administratively down
Gateway(config-if)#no shut

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

**ISP**

*Router>en*
*Router#conf t*
*Enter configuration commands, one per line. End with CNTL/Z.*
*Router(config)#hostname ISP*
*ISP(config)#int s0/0/0*
*ISP(config-if)#ip address 209.165.201.17 255.255.255.252*
*ISP(config-if)#clock rate 128000*
*ISP(config-if)#no shut*

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

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

*ISP(config-if)#int g0/0*
*ISP(config-if)#ip address 192.31.7.1 255.255.255.0*
*ISP(config-if)#no shut*

*ISP(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*

*ISP(config-if)#exit*

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shut

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

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

ISP(config-if)#int g0/0
ISP(config-if)#ip address 192.31.7.1 255.255.255.0
ISP(config-if)#no shut

ISP(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

ISP(config-if)#
```

**Step 12: configurar el routing estático.**

a. Cree una ruta estática desde el router ISP hasta el router Gateway.

ISP(config)# **ip route 209.165.200.224 255.255.255.248 209.165.201.18**

```
ISP(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
ISP(config)#
```

b. Cree una ruta predeterminada del router Gateway al router ISP.

Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

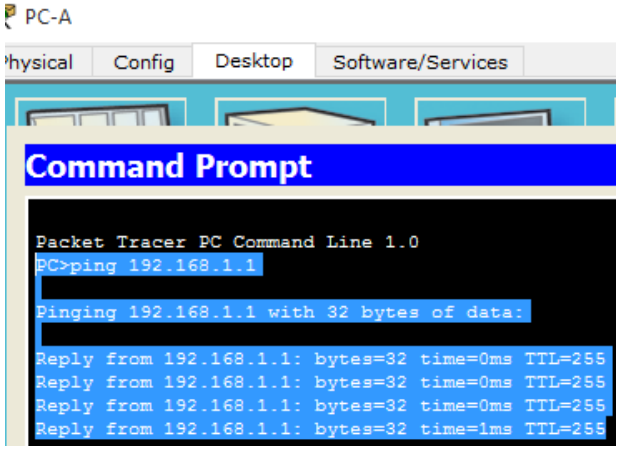
```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

**Step 13: Verificar la conectividad de la red**

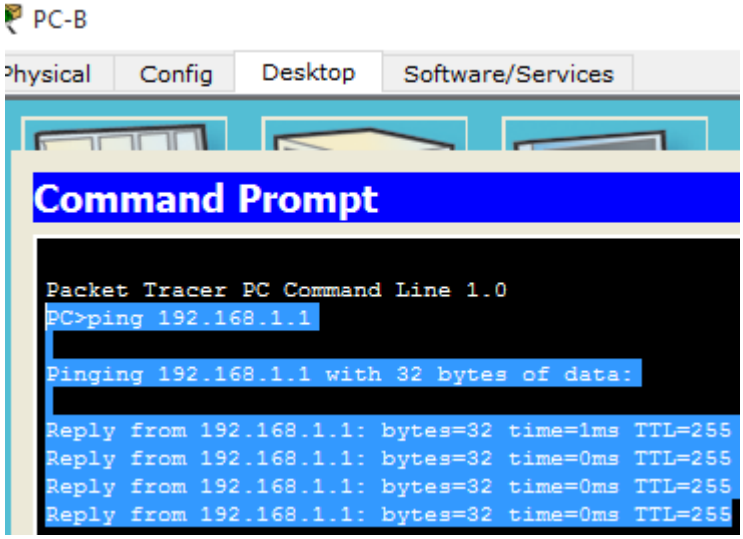
a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

PC-A

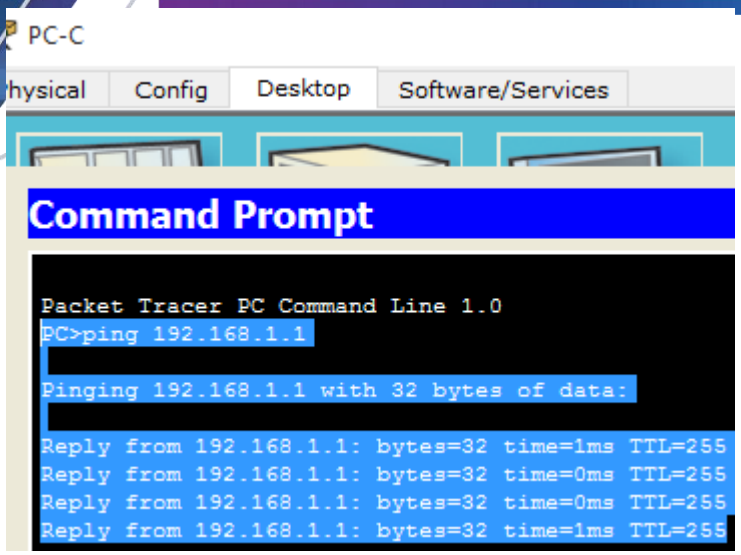
*PC>ping 192.168.1.1*
*Pinging 192.168.1.1 with 32 bytes of data:*
*Reply from 192.168.1.1: bytes=32 time=1ms TTL=255*
*Reply from 192.168.1.1: bytes=32 time=0ms TTL=255*
*Reply from 192.168.1.1: bytes=32 time=0ms TTL=255*
*Reply from 192.168.1.1: bytes=32 time=1ms TTL=255*




PC-B




PC-C




b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.

**Parte2: configurar y verificar el conjunto de NAT con sobrecarga**

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

**Step 14: 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**

```
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

**Step 15: 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**

```
Gateway(config)#ip nat pool public_access 209.165.200.225  209.165.200.230 netmask 255.255.255.248
```

**Step 16: 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**

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

**Step 17: 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)#int g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip nat outside
Gateway(config-if)#
```

**Step 18: 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.

PC-A

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

PC-B

```
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=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

PC-C

```
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=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1

Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6, allocated 1 (16%), misses 0

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

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12  Misses: 12
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.230
       type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#
```

c. Muestre las NAT en el router Gateway.

Gateway# **show ip nat translations**

| Pro | Inside global | Inside local | Outside local | Outside global |
|---|---|---|---|---|
| icmp | 209.165.200.225:0 | 192.168.1.20:1 | 192.31.7.1:1 | 192.31.7.1:0 |
| icmp | 209.165.200.225:1 | 192.168.1.21:1 | 192.31.7.1:1 | 192.31.7.1:1 |
| icmp | 209.165.200.225:2 | 192.168.1.22:1 | 192.31.7.1:1 | 192.31.7.1:2 |

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:1024192.168.1.21:1   192.31.7.1:1       192.31.7.1:1024
icmp 209.165.200.225:1025192.168.1.21:2   192.31.7.1:2       192.31.7.1:1025
icmp 209.165.200.225:1026192.168.1.21:3   192.31.7.1:3       192.31.7.1:1026
icmp 209.165.200.225:1027192.168.1.21:4   192.31.7.1:4       192.31.7.1:1027
icmp 209.165.200.225:1028192.168.1.22:1   192.31.7.1:1       192.31.7.1:1028
icmp 209.165.200.225:1029192.168.1.22:2   192.31.7.1:2       192.31.7.1:1029
icmp 209.165.200.225:1030192.168.1.22:3   192.31.7.1:3       192.31.7.1:1030
icmp 209.165.200.225:1031192.168.1.22:4   192.31.7.1:4       192.31.7.1:1031
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.20:2     192.31.7.1:2       192.31.7.1:2
icmp 209.165.200.225:3 192.168.1.20:3     192.31.7.1:3       192.31.7.1:3
icmp 209.165.200.225:4 192.168.1.20:4     192.31.7.1:4       192.31.7.1:4
```

**Nota:** es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? **3**

¿Cuántas direcciones IP globales internas se indican? **1**

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? **12**

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

**El ping no funciona porque el router solo conoce la ubicación de las direcciones internas globales en su tabla de enrutamiento, pero las direcciones internas locales no están notificadas.**

### Parte 3: configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

### Step 19: borrar las NAT y las estadísticas en el router Gateway.

```
Gateway#clear ip nat translation *
Gateway#clear ip nat statistics
^
% Invalid input detected at '^' marker
```

**PACKET TRACERT NO SOPORTA EL ULTIMO COMANDO**

### Step 20: 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?

**show ip nat statistics**

*Gateway#**show ip nat statistics***
*Total translations: 0 (0 static, 0 dynamic, 0 extended)*
*Outside Interfaces: Serial0/0/1*
*Inside Interfaces: GigabitEthernet0/1*
*Hits: 12 Misses: 12*
*Expired translations: 12*
*Dynamic mappings:*
*-- Inside Source*
*access-list 1 pool public_access refCount 0*
*pool public_access: netmask 255.255.255.248*
*start 209.165.200.225 end 209.165.200.230*
*type generic, total addresses 6 , allocated 0 (0%), misses 0*

**Step 21: 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**

Gateway(config)#**no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**
**%Pool public_access in use, cannot destroy**
Gateway(config)#

**Step 22: eliminar la traducción NAT de la lista de origen interna al conjunto externo.**

Gateway(config)# **no ip nat inside source list 1 pool public_access overload**

Gateway(config)#**no ip nat inside source list 1 pool public_access overload**
Gateway(config)#

**Step 23: asociar la lista de origen a la interfaz externa.**

Gateway(config)# **ip nat inside source list 1 interface serial 0/0/1 overload**

Gateway(config)#**ip nat inside source list 1 interface serial 0/0/1 overload**
Gateway(config)#

**Step 24: probar la configuración PAT.**

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.

PC-A

```
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=12ms TTL=254
Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=13ms TTL=254
```

PC-B

```
Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=15ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

PC-C

```
Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=13ms TTL=25
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0
Appl doors: 0
Normal doors: 0

Queued Packets: 0

Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 24 Misses: 24
Expired translations: 24
Dynamic mappings:
Gateway#show ip nat translations
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 36 Misses: 36
Expired translations: 24
Dynamic mappings:

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 24  Misses: 24
Expired translations: 24
Dynamic mappings:
Gateway#show ip nat translations
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 36  Misses: 36
Expired translations: 24
Dynamic mappings:
```

c. Muestre las traducciones NAT en el Gateway.

Gateway# **show ip nat translations**

| Pro | Inside global | Inside local | Outside local | Outside global |
|---|---|---|---|---|
| icmp | 209.165.201.18:3 | 192.168.1.20:1 | 192.31.7.1:1 | 192.31.7.1:3 |
| icmp | 209.165.201.18:1 | 192.168.1.21:1 | 192.31.7.1:1 | 192.31.7.1:1 |
| icmp | 209.165.201.18:4 | 192.168.1.22:1 | 192.31.7.1:1 | 192.31.7.1:4 |

Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.201.18:1024192.168.1.21:9 192.31.7.1:9 192.31.7.1:1024
icmp 209.165.201.18:1025192.168.1.21:10 192.31.7.1:10 192.31.7.1:1025
icmp 209.165.201.18:1026192.168.1.21:11 192.31.7.1:11 192.31.7.1:1026
icmp 209.165.201.18:1027192.168.1.21:12 192.31.7.1:12 192.31.7.1:1027
icmp 209.165.201.18:1028192.168.1.22:9 192.31.7.1:9 192.31.7.1:1028

icmp 209.165.201.18:1029192.168.1.22:10 192.31.7.1:10 192.31.7.1:1029
icmp 209.165.201.18:1030192.168.1.22:11 192.31.7.1:11 192.31.7.1:1030
icmp 209.165.201.18:1031192.168.1.22:12 192.31.7.1:12 192.31.7.1:1031
icmp 209.165.201.18:10 192.168.1.20:10 192.31.7.1:10 192.31.7.1:10
icmp 209.165.201.18:11 192.168.1.20:11 192.31.7.1:11 192.31.7.1:11
icmp 209.165.201.18:12 192.168.1.20:12 192.31.7.1:12 192.31.7.1:12
icmp 209.165.201.18:9 192.168.1.20:9 192.31.7.1:9 192.31.7.1:9

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.201.18:1024192.168.1.21:9     192.31.7.1:9       192.31.7.1:1024
icmp 209.165.201.18:1025192.168.1.21:10    192.31.7.1:10      192.31.7.1:1025
icmp 209.165.201.18:1026192.168.1.21:11    192.31.7.1:11      192.31.7.1:1026
icmp 209.165.201.18:1027192.168.1.21:12    192.31.7.1:12      192.31.7.1:1027
icmp 209.165.201.18:1028192.168.1.22:9     192.31.7.1:9       192.31.7.1:1028
icmp 209.165.201.18:1029192.168.1.22:10    192.31.7.1:10      192.31.7.1:1029
icmp 209.165.201.18:1030192.168.1.22:11    192.31.7.1:11      192.31.7.1:1030
icmp 209.165.201.18:1031192.168.1.22:12    192.31.7.1:12      192.31.7.1:1031
icmp 209.165.201.18:10 192.168.1.20:10     192.31.7.1:10      192.31.7.1:10
icmp 209.165.201.18:11 192.168.1.20:11     192.31.7.1:11      192.31.7.1:11
icmp 209.165.201.18:12 192.168.1.20:12     192.31.7.1:12      192.31.7.1:12
icmp 209.165.201.18:9  192.168.1.20:9      192.31.7.1:9       192.31.7.1:9
```

**Reflexión**

¿Qué ventajas tiene la PAT?

El PAT minimiza el uso del número de direcciones públicas necesarias para acceder a internet, PAT al igual que NAT, sirve para esconder las direcciones privadas de la red externa

Múltiples hosts internos pueden compartir una sola dirección IP para comunicación, conservando así direcciones IP.

Los hosts en la red privada no tienen que exponer sus direcciones IP privadas a la red pública.

**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.

## Conclusiones

- Se aprende a clasificar los protocolos de routing, y nos enseñan a mantener información de red más precisa, cuando se produce un cambio en la topología los protocolos de routing propagan esa información, por todo el dominio de routing.
- Se aprende a configurar el protocolo OSPF en los routers y realizar esquemas de red con dicho protocolo, así mismo como los comandos necesarios para verificar las interfaces de OSPF
- Se configuro DHCP en los ejercicios propuestos en Packet Tracer, en donde se incluyeron tres mecanismos diferentes de asignación de direcciones para proporcionar flexibilidad al asignar las direcciones desde una asignación manual, hasta una dinámica
- Se aprende a realizar diagnósticos en la resolución de problemas con DHCPV4 Y DHCPV6 desde resolver conflictos de dirección, hasta probar el funcionamiento en la misma subred.
- Se comprende la importancia de utilizar NAT en un entorno de red, tal es el caso que nos permite conservar las direcciones públicas y reduce la sobrecarga administrativa de forma considerable.
- Durante el desarrollo del trabajo se puedo realizar las configuraciones básicas e iniciales sobre los dispositivos CISCO como router y switch, donde se configuran cada Puerto para que las terminales tengan comunicación tanto con otros equipos de redes LAN diferentes como acceso a internet.
- Se realiza de manera adecuada todos los ejercicios y laboratorios utilizando el Software Packet Tracer, siguiendo los pasos de las guías y aplicando los conocimientos adquiridos durante el curso de Cisco

## Bibliografía


CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

Amberg, E. (2014). CCNA 1 Powertraining : ICND1/CCENT (100-101). Heidleberg: MITP. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=979032&lang=es&site=ehost-live

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de: http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de: http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de: http://gonda.nic.in/swangonda/pdf/ccna1.pdf