# Diplomado de Profundización Cisco

## (Diseño e Implementación de Soluciones Integradas LAN – WAN)

**Yenifer Maricela Tabi Tituaña**

**Universidad Nacional Abierta y a Distancia - UNAD**

**Escuela de Ciencias Básicas y Tecnologías de la Información- ECBTI**

**Diplomado en Cisco**

**Silvia 2018**

# Diplomado de Profundización Cisco

## (Diseño e Implementación de Soluciones Integradas LAN - WAN)

**Yenifer Maricela Tabi Tituaña**

**Código: 1.064.432.426**

Diplomado en Cisco presentado como requisito para optar al título profesional en Ingeniería de Sistemas

**PhD. Juan Carlos Vesga Ferreira**

**Asesor**

**Universidad Nacional Abierta y a Distancia - UNAD**

**Escuela de Ciencias Básicas y Tecnologías de la Información- ECBTI**

**Diplomado en Cisco**

**Silvia 2018**

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

## Dedicatoria

Primero que nada se lo dedico a mi Dios Todo Poderoso quien me dio la fuerza de poder trasnochar a pesar de terminar tan cansada después del trabajo, a mis padres quienes no solo me apoyaron monetariamente sino también alentándome cada día mejor dicho cada noche a no rendirme y seguir, a mis hermanos quienes con su ejemplo de no renunciar sin importar que tan duro sea me inspiraron a no desfallecer, a mi prometido que trasnocho muchas veces conmigo para colaborarme en lo que necesitara, a mi institución SENA el primero en abrirme las puertas para superarme y por último y n menos importante a la UNAD y a su cuerpo docente que siempre estuvo presente en el momento que lo necesite y que me enseñaron que conseguir las cosas cuesta y que nada es fácil en esta vida.

## Agradecimientos

Agradezco a Dios a quien siempre sentí a mi lado dándome fuerzas en aquellas madrugadas en las que trabajaba y me mantenía despierta y enfocada, ayudándome a entender y responder de manera excelente a la tutora asignada.

Agradezco también a mi familia quien siempre estuvo allí para mí en todo momento dándome fuerzas para que no me rinda.

Y por último agradezco a la ingeniera Nancy Amparo Guaca Girón por siempre estar pendiente de cada uno de nosotros recordándonos las fechas y verificando los trabajos.

# Tabla de contenido

# Lista de Tablas

# Lista de Ilustraciones

## Resumen

El documento fue desarrollado con diferentes prácticas diseñado redes y configurándolos en un programa llamado Packet Tracer, este producto tiene el propósito de ser usado como un producto educativo que brinda exposición a la interfaz comando línea de los dispositivos de Cisco para practicar y aprender por descubrimiento.

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla dando click en ellos se puede ingresar a sus consolas de configuración.
Allí están soportados todos los comandos del Cisco también se puede hacer simulaciones de conectividad todo ello desde las mismas consolas incluidas y haciendo ejercicios de una red u otra también para ir aprendiendo.

El documento cuenta con guía desarrolladas paso a paso lo hecho en los simuladores y soportado a través de pantallazos.



## Abstract

The document was developed with different practices designed networks and configured in a program called Packet Tracer, this product is intended to be used as an educational product that provides exposure to the command line interface of Cisco devices to practice and learn by discovery.

In this program the physical topology of the network is created by simply dragging the devices to the screen by clicking on them you can enter their configuration consoles.

There all Cisco commands are supported, you can also do connectivity simulations all from the same consoles included and doing exercises of a network or another also to learn.
The document has a step-by-step guide developed in the simulators and supported through screenshots.

## Introducción

Hoy en día, muchas empresas buscan personas de alta competitividad con sus certificaciones apropiadas, en especial certificaciones CCNA.

Aquellos que cuentan con estos certificados pueden asumir funciones como coordinación de recursos para incorporar los requisitos de red en la empresa y además prestar apoyo en la red.

Con este diplomado se puede llegar a desarrolla competencias importantes como la asistencia en la planificación, la ejecución, la prevención y el reconocimiento de los requisitos en la red del sistema

Hoy en día el ingeniero debe ser capaz de realizar funciones mas importantes en las tecnologías de la información y ue mejor que ganar experiencia a través de un simulador en sistemas e información, tecnología y poder integrar los sistemas

# Objetivos

## Objetivo General:

Identificar y solucionar problemas propios de enrutamiento mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces.

## Objetivos Específicos:

- ✓ Verificar la conectividad entre los dispositivos antes de la configuración del firewall.
- ✓ Utilice las ACL para garantizar el acceso remoto a los enrutadores solo está disponible desde la estación de administración PC-C.
- ✓ Configure las ACL en R1 y R3 para mitigar los ataques.
- ✓ Verificar la funcionalidad de ACL.
- ✓ Armar la red y configurar los parámetros básicos de los dispositivos.
- ✓ Configurar y verificar el routing OSPF.
- ✓ Configurar y aplicar una ACL estándar designada.
- ✓ Verificar la implementación de ACL.
- ✓ Configurar, aplicar y verificar una ACL de IPv6.
- ✓ Configurar, aplicar y verificar una segunda ACL de IPv6.
- ✓ Armar la red y configurar los parámetros básicos de los dispositivos.
- ✓ Configurar la red para SLAAC.
- ✓ Configurar la red para DHCPv6 sin estado.
- ✓ Configurar la red para DHCPv6 con estado.
- ✓ Armar la red y verificar la conectividad.
- ✓ Configurar y verificar la NAT estática.
- ✓ Configurar y verificar la NAT dinámica.
- ✓ Información básica/situación

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

### Topología

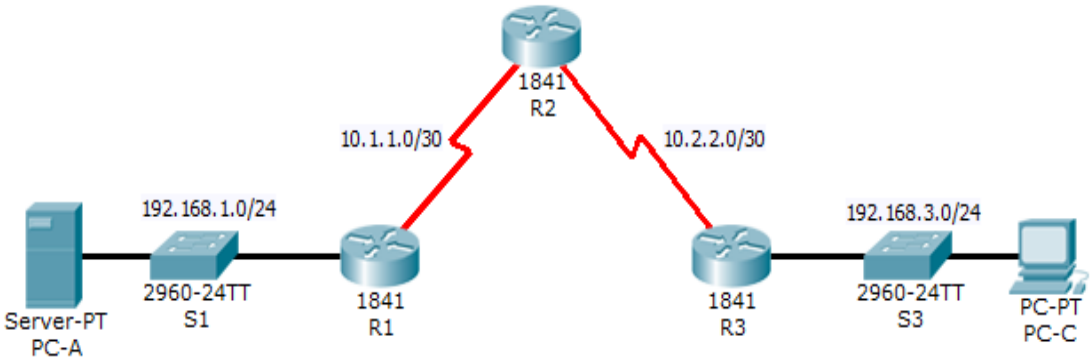


*Figure 1 Topología 4.4.1.2*

### Addressing Table

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

*Tabla 1 Configure IP ACLs to mitigate*

### Objetivos

- 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

## Parte 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

### Paso 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
```

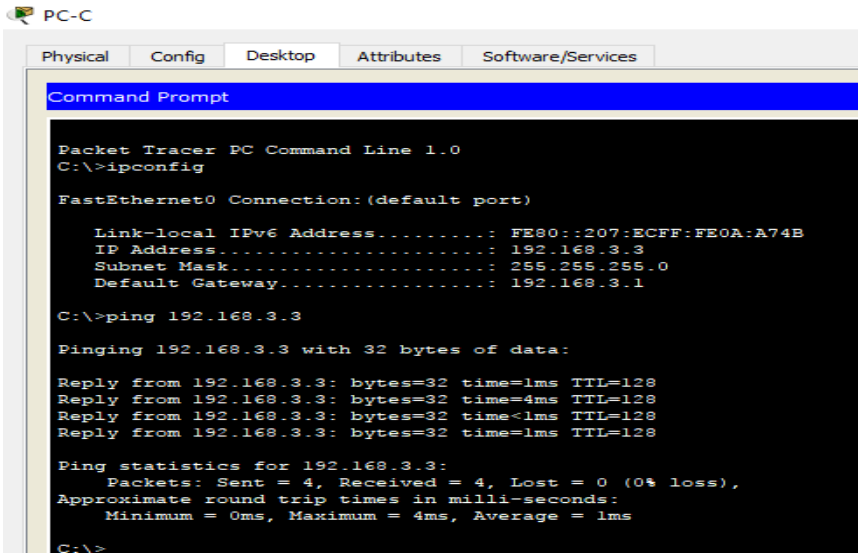


*Figure 2 Verificación de conectividad*

## Paso 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
```

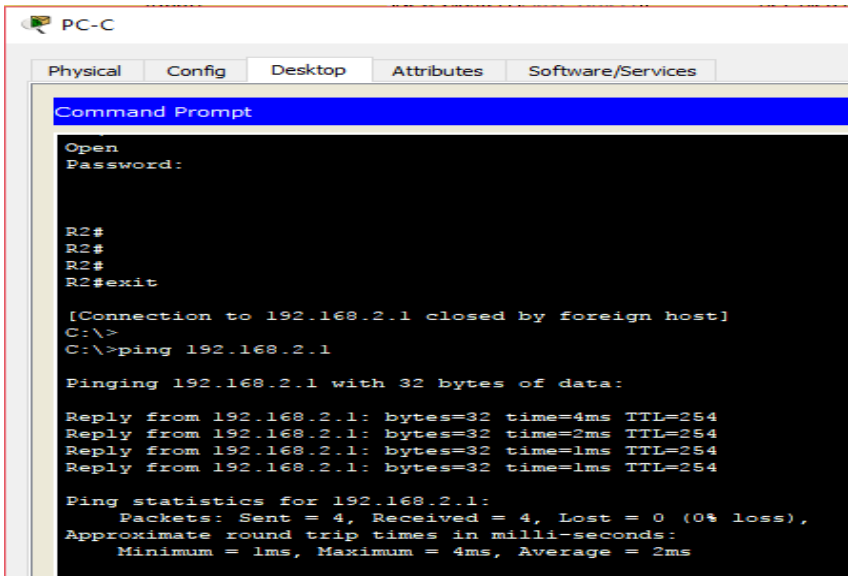


*Figure 3 Comando prompt*

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

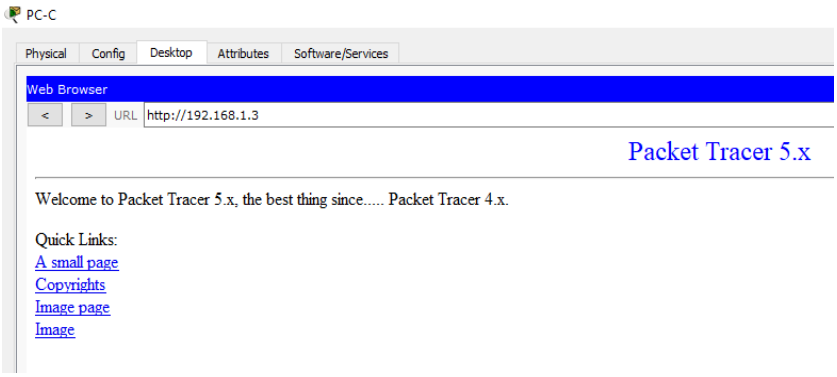


*Figure 4 Browser a Pc-A*

## Parte 2: Secure Access to Routers

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

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

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

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

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

```
R1(config-line)# access-class 10 in
R2(config-line)# access-class 10 in
R3(config-line)# access-class 10 in
```

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

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

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

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

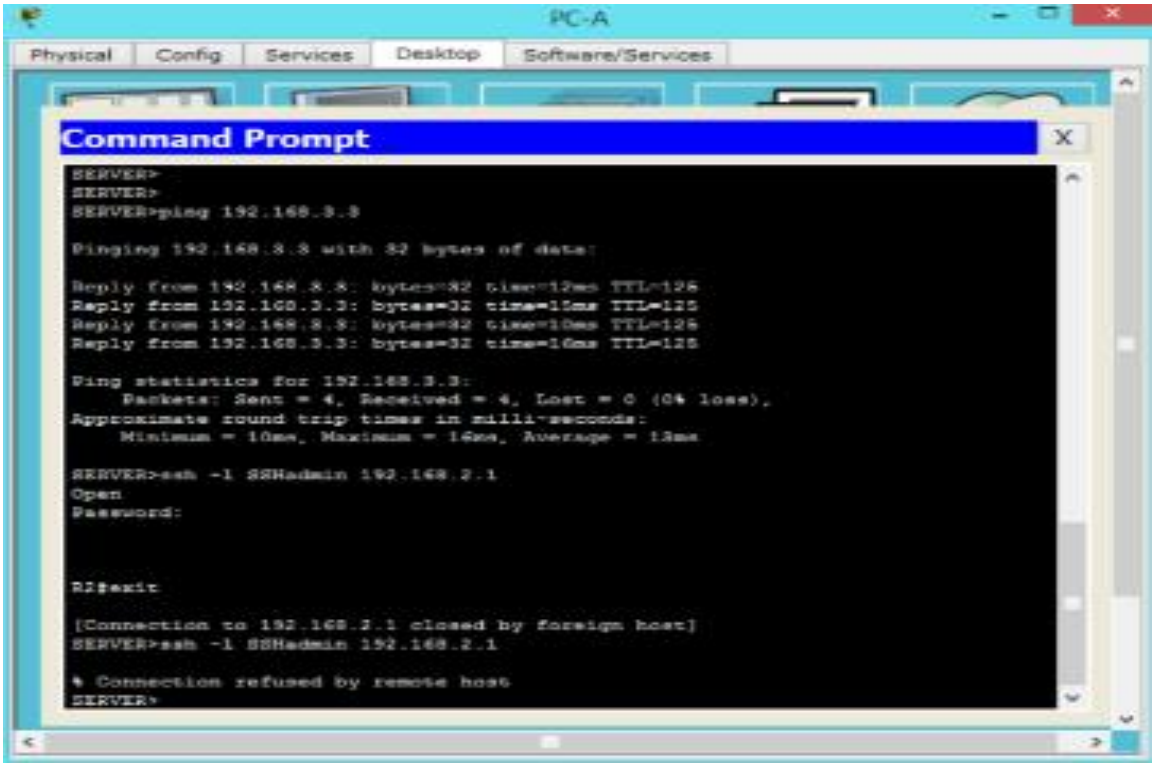


*Figure 5 Sesión SSH*

## Parte 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.

### Paso 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**.

### Paso 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
```

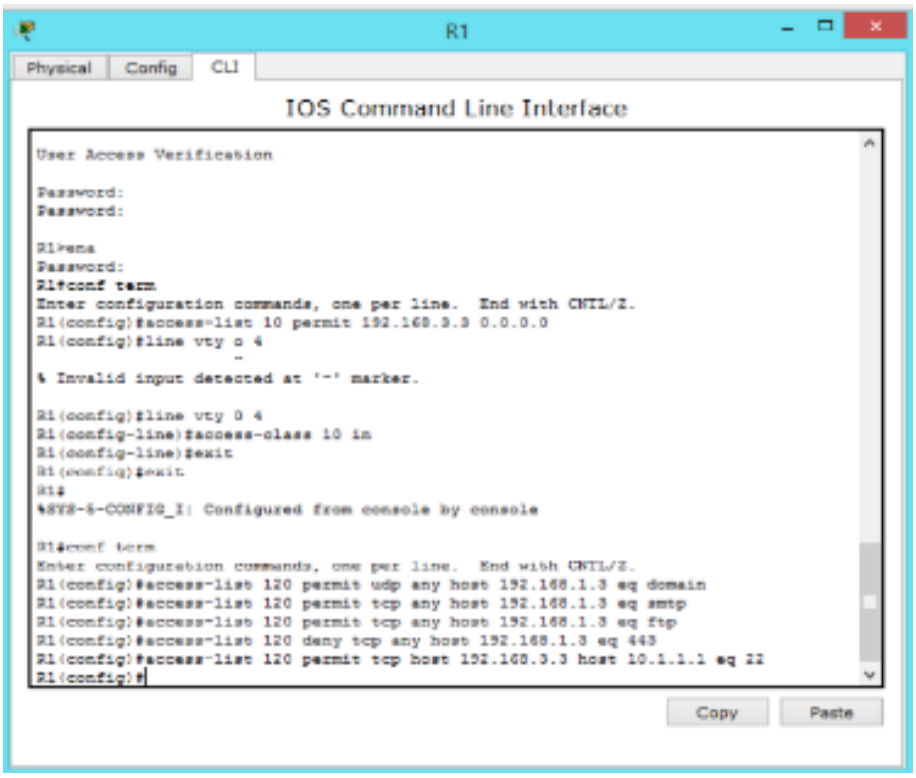


*Figure 6 Creación de un número IP-ACL*

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

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

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

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

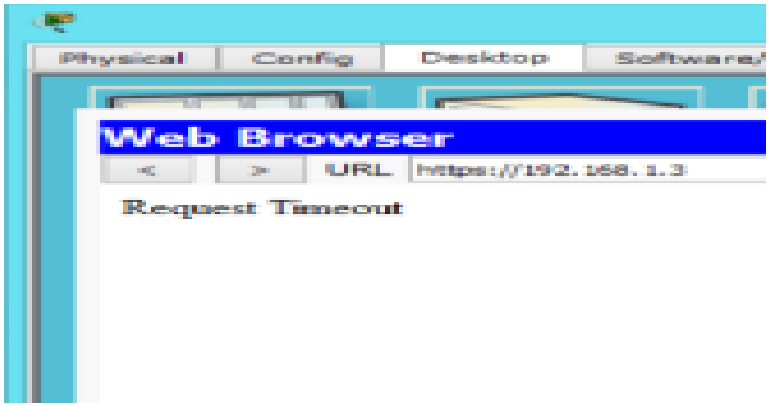


*Figure 7 Web browser*

## Parte 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.

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

### Paso 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
```

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

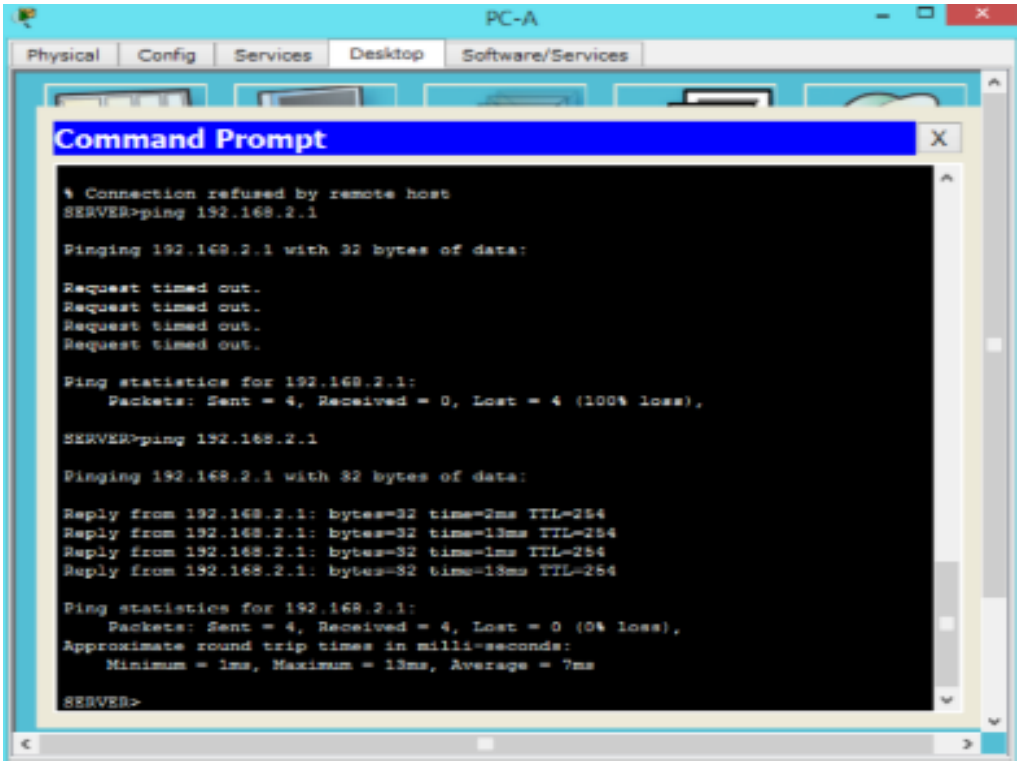


*Figure 8 Command prompt*

## Parte 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**.

### Paso 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
```

### Paso 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
```

## Parte 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.

### Paso 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
```

### Paso 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
```

### Paso 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.

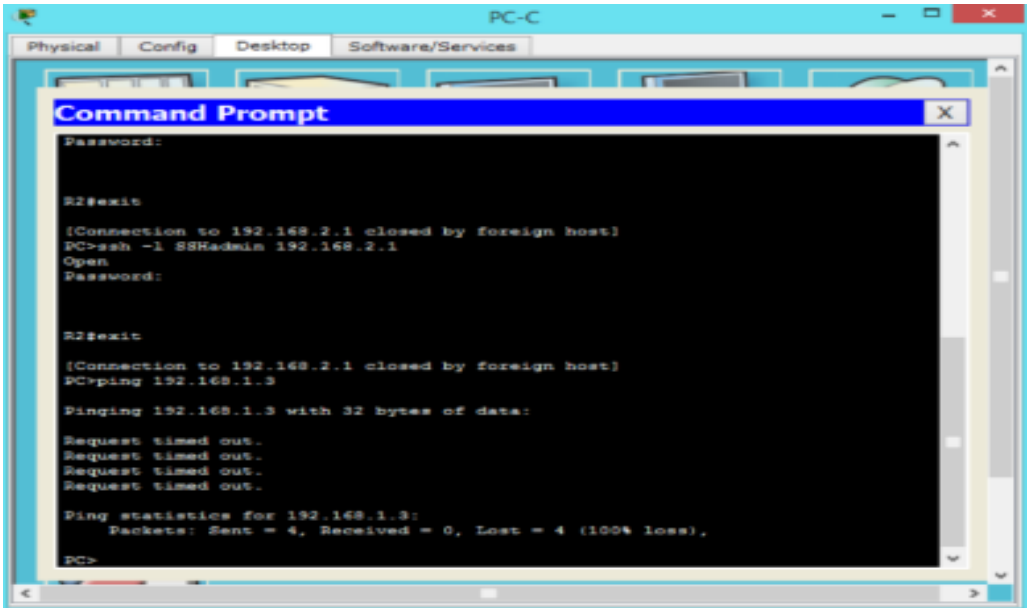


*Figure 9 Ping al servidor Pc-A*

**Paso 4: Check results.**

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

**!!!Script for R1**

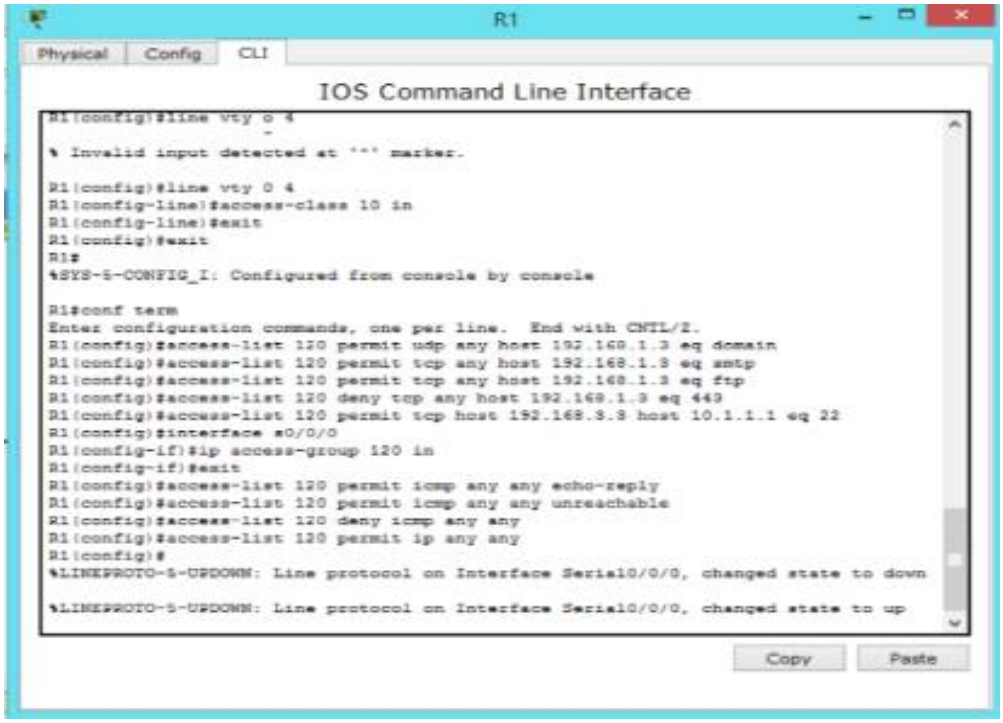


*Figure 10 Resultados script para R1*

## !!!Script for R2

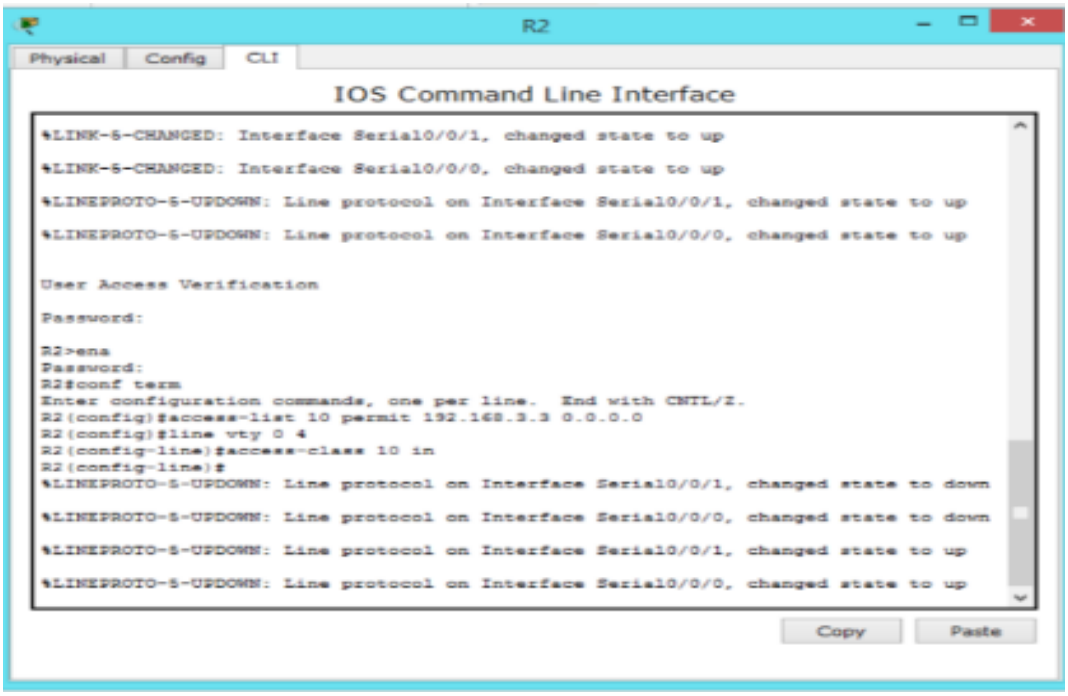


*Figure 11 Resultados script para R2*

## !!!Script for R3

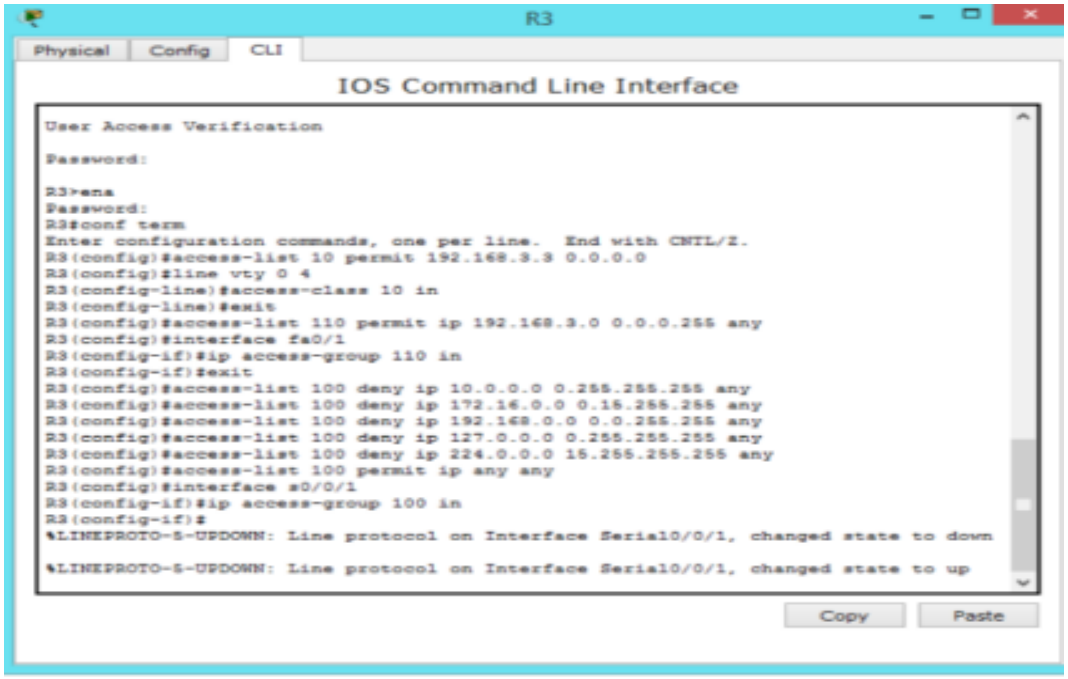


*Figure 12 Resultados script para R3*

## Práctica 7.3.2.4 Lab - Configuring Basic RIPv2 and RIPng

### Topología

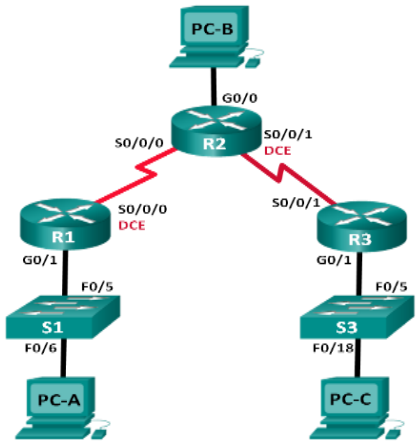


*Figure 13 Topología 7.3.2.4*

### 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 |

*Tabla 2 Configuring basic RIPv2 and RIPng*

**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.

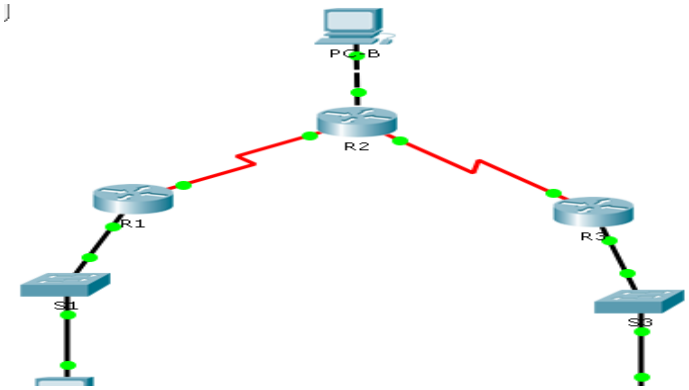


*Figure 14 Cableado de red*

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

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

Desactive la búsqueda del DNS.

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

Configurar la encriptación de contraseñas.

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

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

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

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

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

Configure una descripción para cada interfaz con una dirección IP.

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

Copie la configuración en ejecución en la configuración de inicio.

**Router 1:**

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd # this is secure system#
R1(config)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

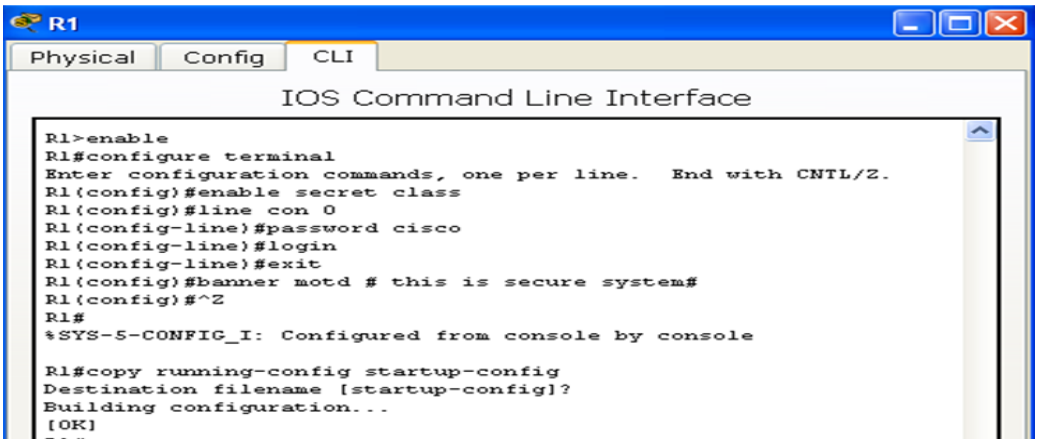


*Figure 15 Router 1*

*R1(config)#*

R1(config)#interface g 0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#no shutdown

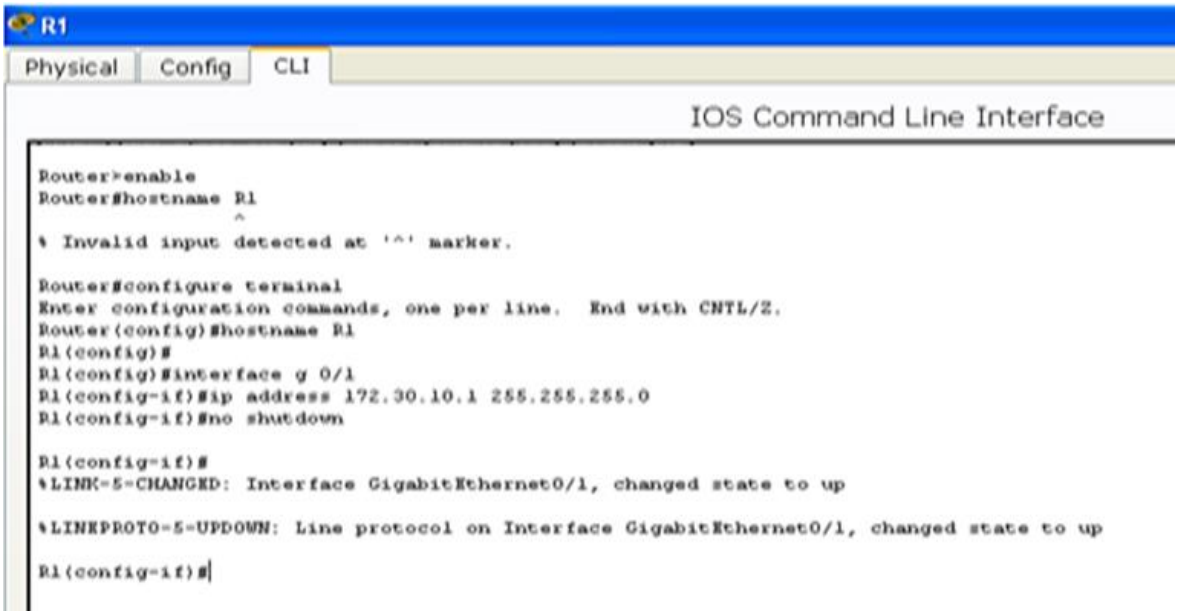


*Figure 16 Router 1*

R1(config)#interface Serial0/0/0
R1(config-if)#interface Serial 0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

R1(config-if)#

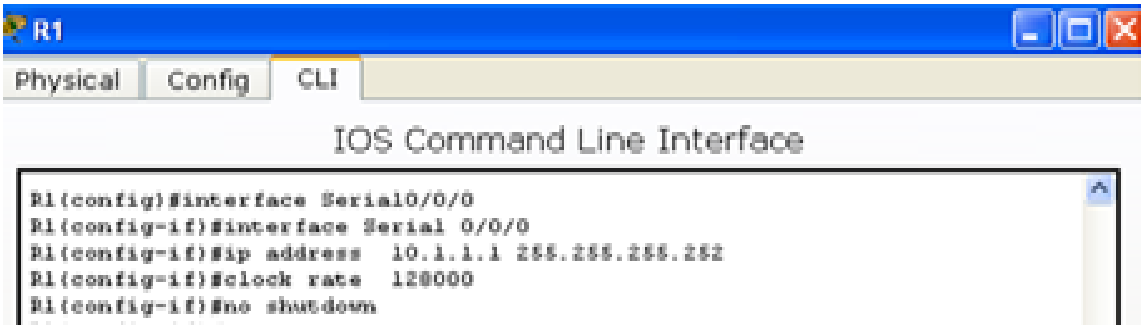


*Figure 17 Router 1*

## Router 2:

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret class
Router(config)#line 0
No physical hardware support for line 3
Router(config)#line con 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#banner motd # thi is a secure sytem#
Router(config)#banner motd # thi is a secure system#

Router(config)#^Z

Router(config)#hostname R2

R2(config)#

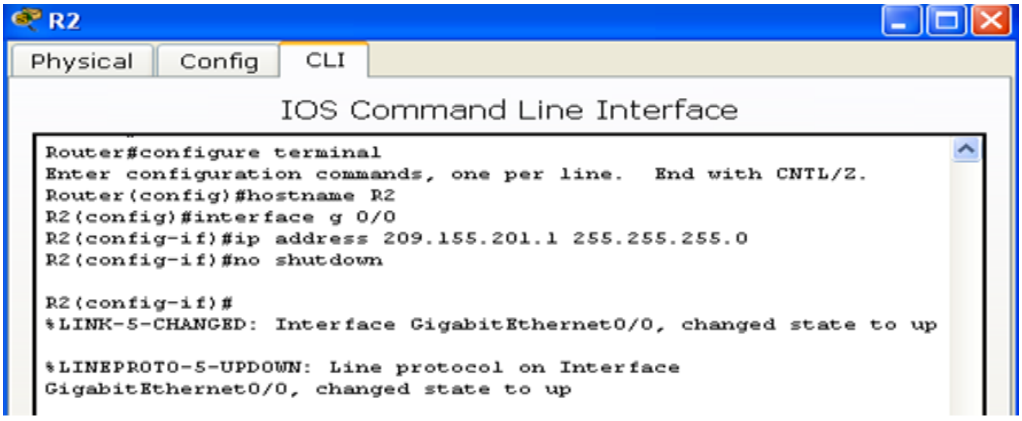


*Figure 18 Router 2*

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#interface g 0/0
R2(config-if)#ip address 209.155.201.1 255.255.255.0
R2(config-if)#no shutdown

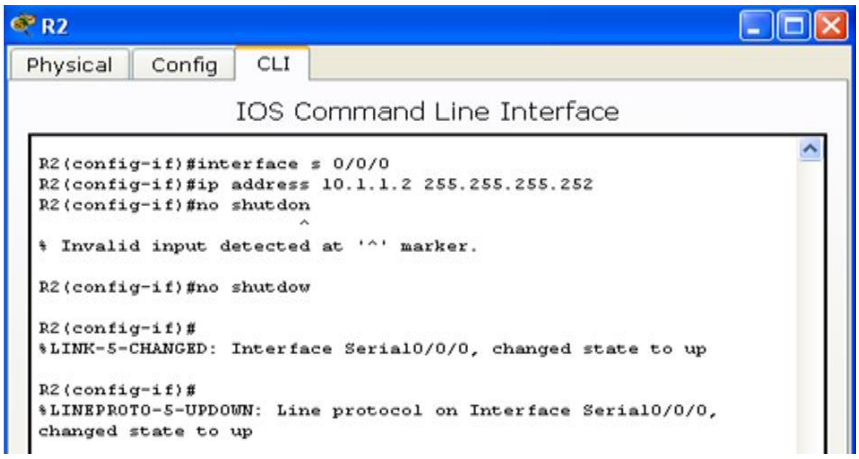


*Figure 19 Router 2*

R2(config-if)#interface s 0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252

R2(config-if)#no shutdown

R2(config-if)#interface s 0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

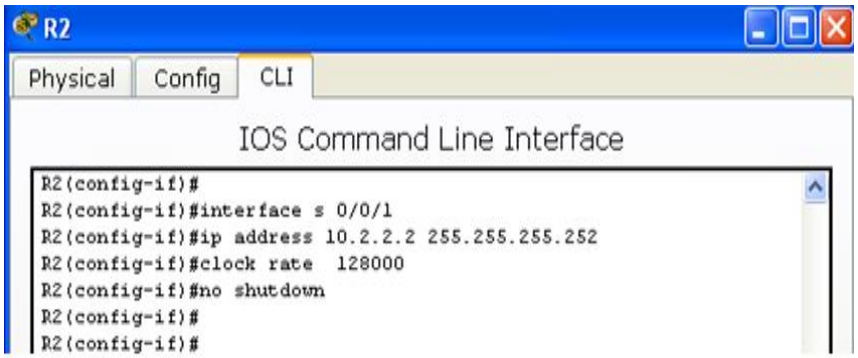


*Figure 20 Router 2*

**Router 3:**

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret class
Router(config)#line con 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#banner motd # this is secure system#
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Router#

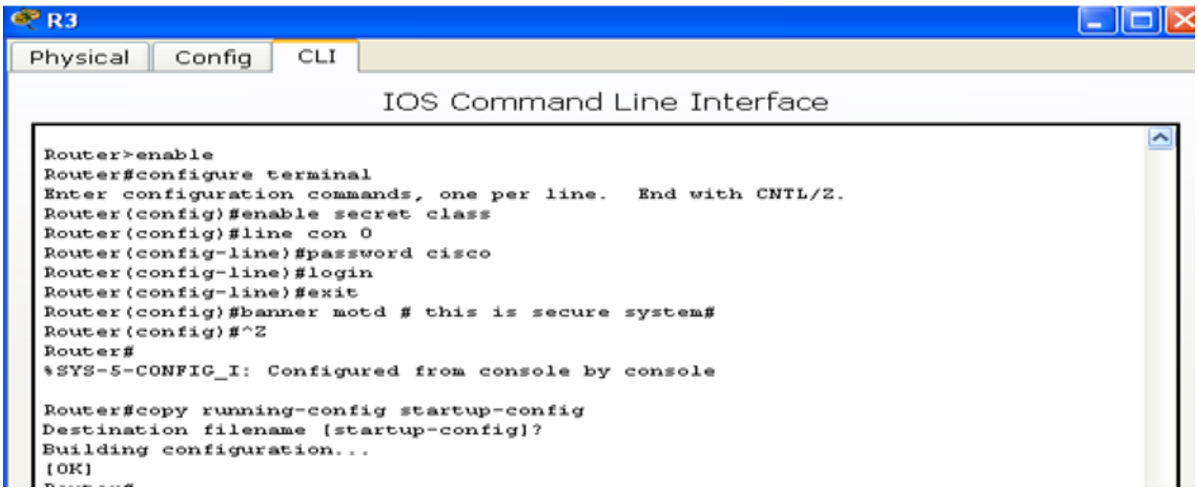


*Figure 21 Router 3*

R3(config)#interface g 0/1
R3(config-if)#
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface s 0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown

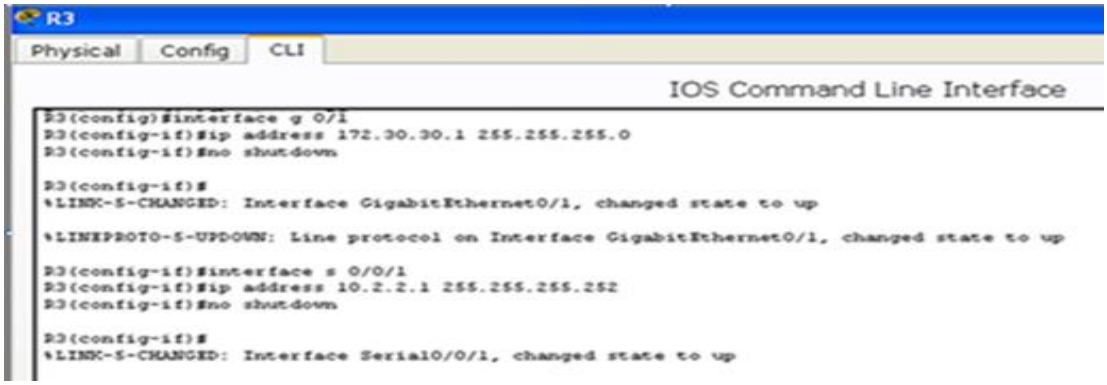


*Figure 22 Router 3*

## Paso 4. Configurar los equipos host.

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

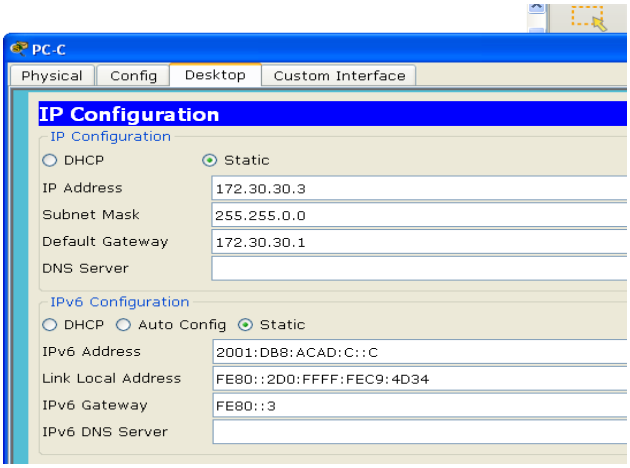


*Figure 23 Configuración equipo host Pc-C*

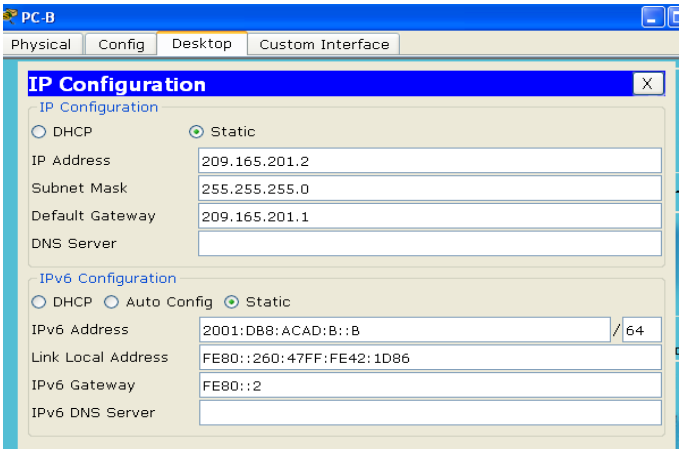


*Figure 24 Configuración equipo host Pc-B*

### Paso 5. Probar la conectividad.

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

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

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

## 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.

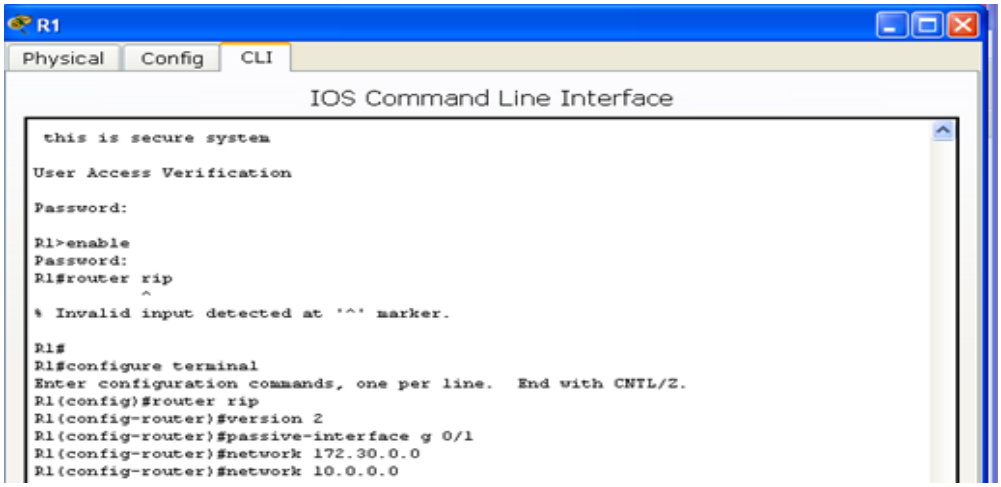


*Figure 25 Configurar enrutamiento RIPv2 en R1*

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

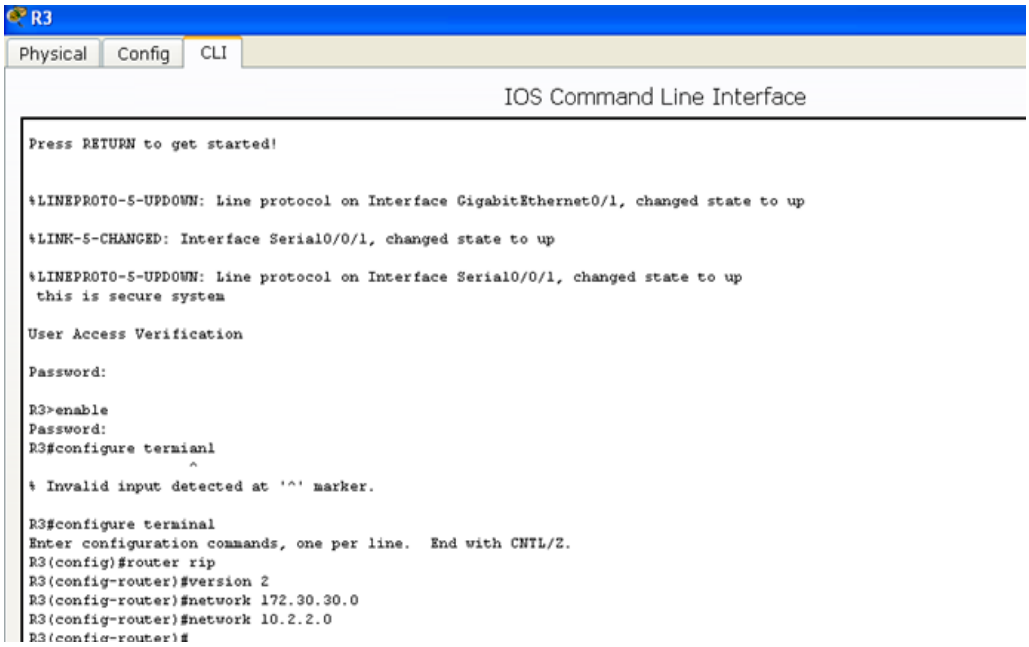


*Figure 26 Configurar enrutamiento RIPv2 en R3*

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.

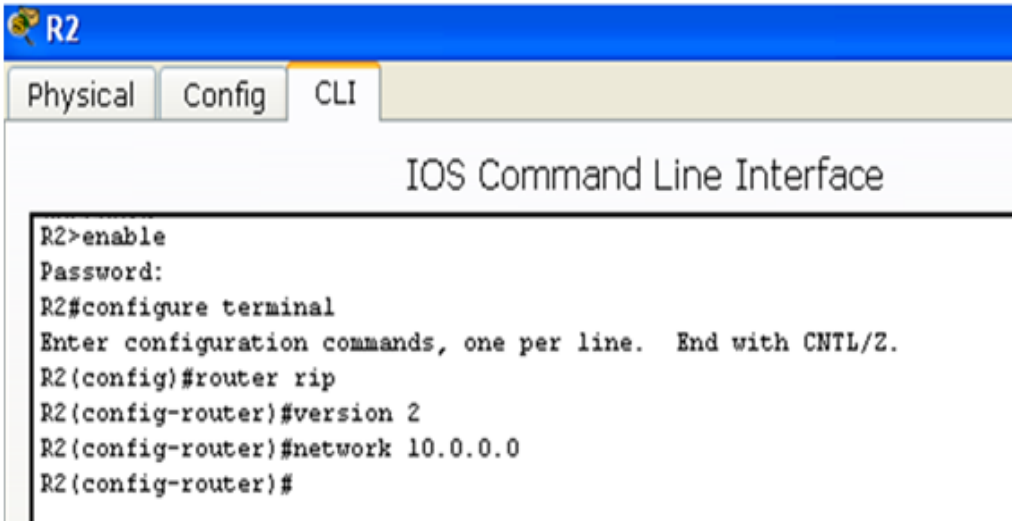


*Figure 27 Configurar enrutamiento RIPv2 en R2*

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

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
```

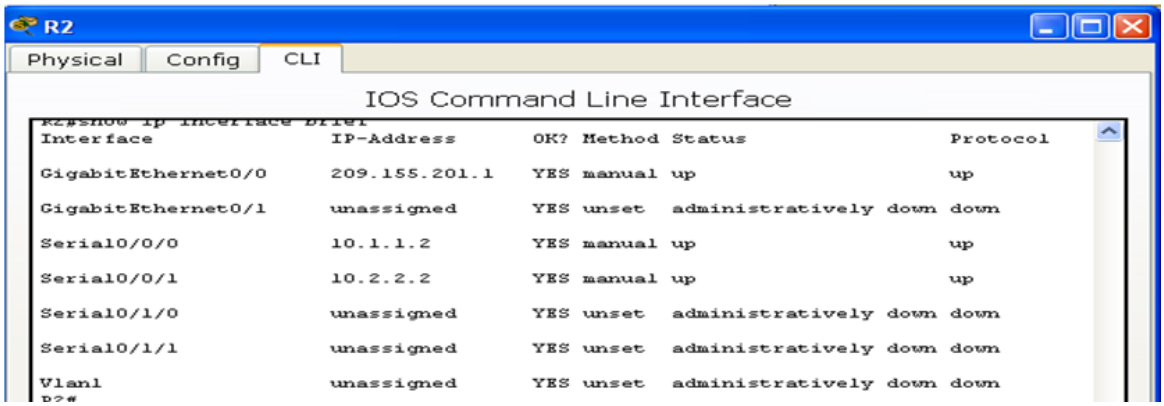


*Figure 28 Estado actual enlaces seriales en R2*

Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? __NO__ ¿Por qué?

Porque la red 209.165.200.0 no ha sido ingresada con el comando RIP v2 en el router2, Por lo cual los routers no están intercambiando información acerca de la red.

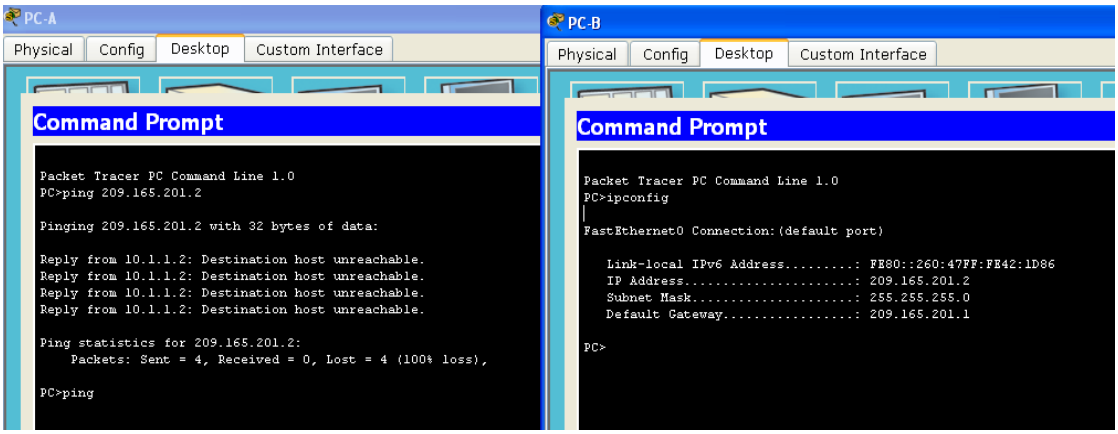


*Figure 29 Conectividad entre Pc*

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

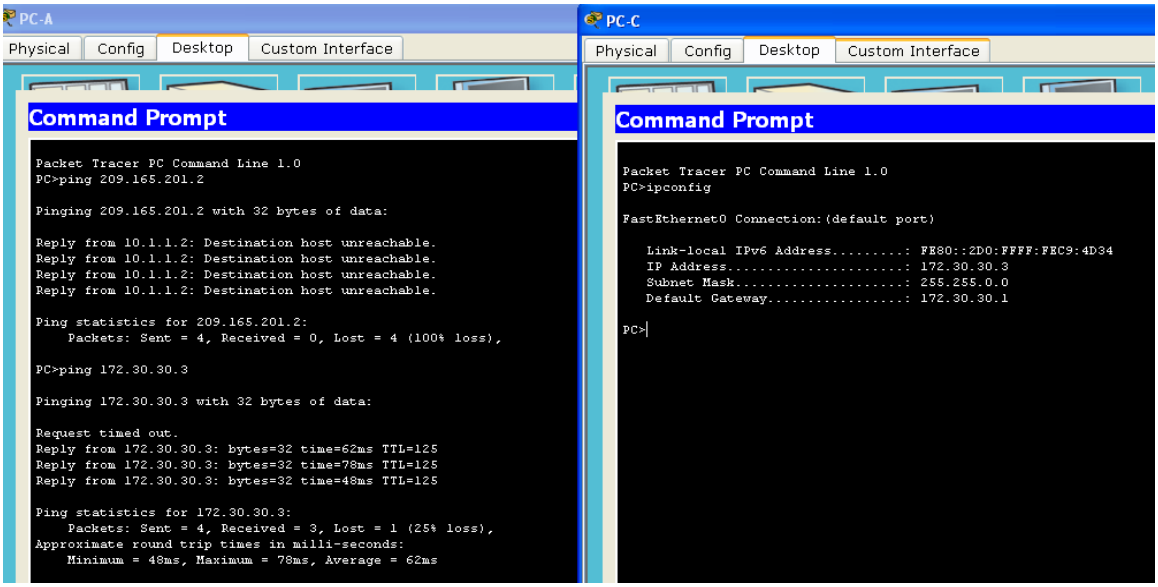


*Figure 30 Ping de Pc-A a Pc-C*

¿Es posible hacer ping de la PC-C a la PC-B? _NO_ ¿Por qué?

Porque la red 172.30.0.0 no ha sido ingresada con el comando RIP v2 en el router2,

Por lo cual los routers no están intercambiando información acerca de la red.

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

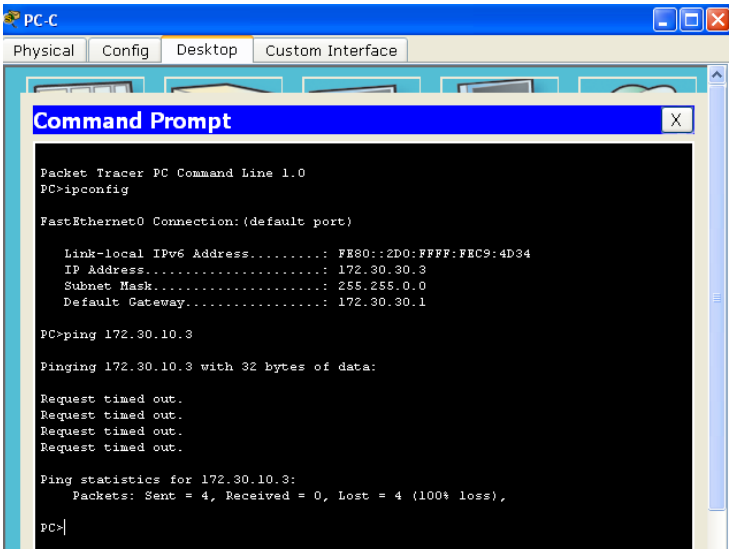


*Figure 31 Ping de Pc-C a Pc-A*

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)
```

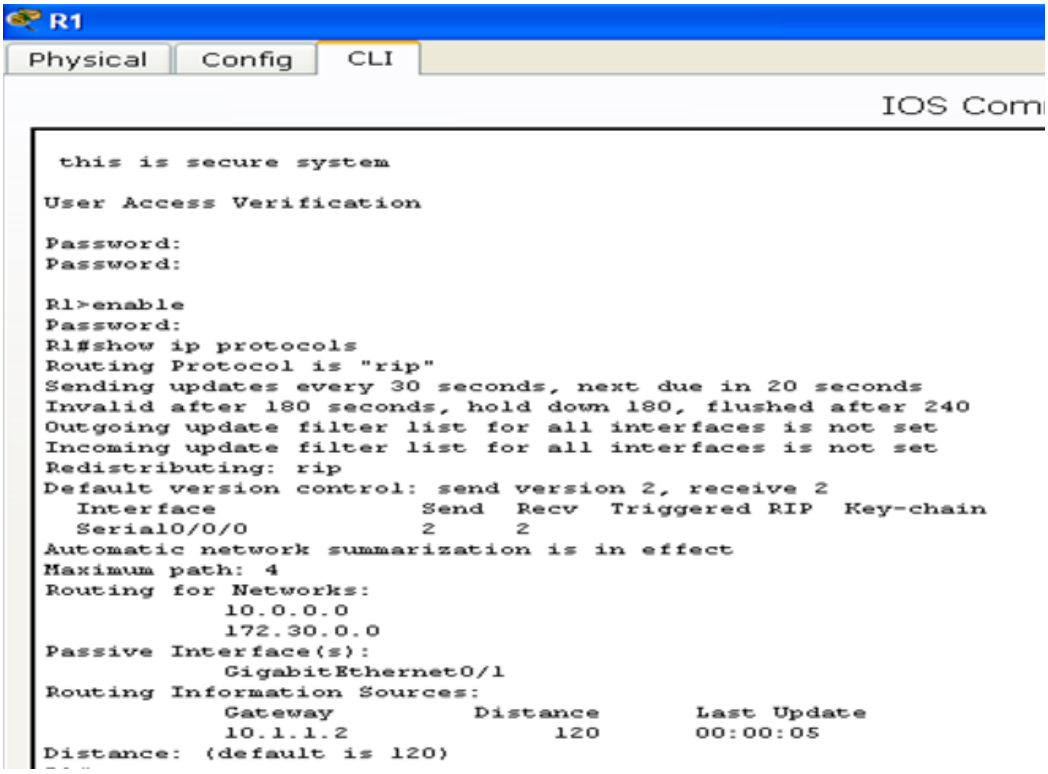


*Figure 32 Verificación RIPv2 en los routers*

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

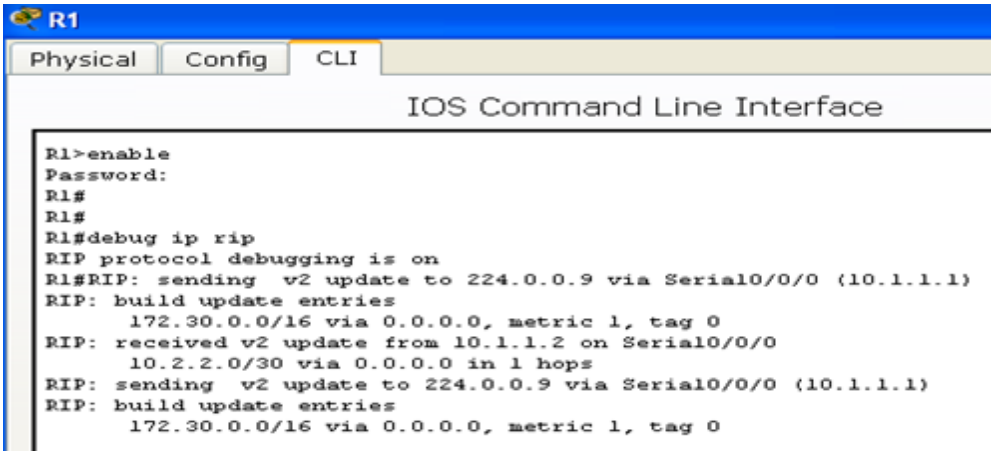


*Figure 33 Ejecución RIPv2*

Se visualizan las actualizaciones que se hacen, las actualizaciones se envían a través de la multicast 224.0.0.9 Esta es la dirección que usan para intercambiar actualizaciones. Por la serial 0/0/0 se está informando la red 10.1.1.2

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

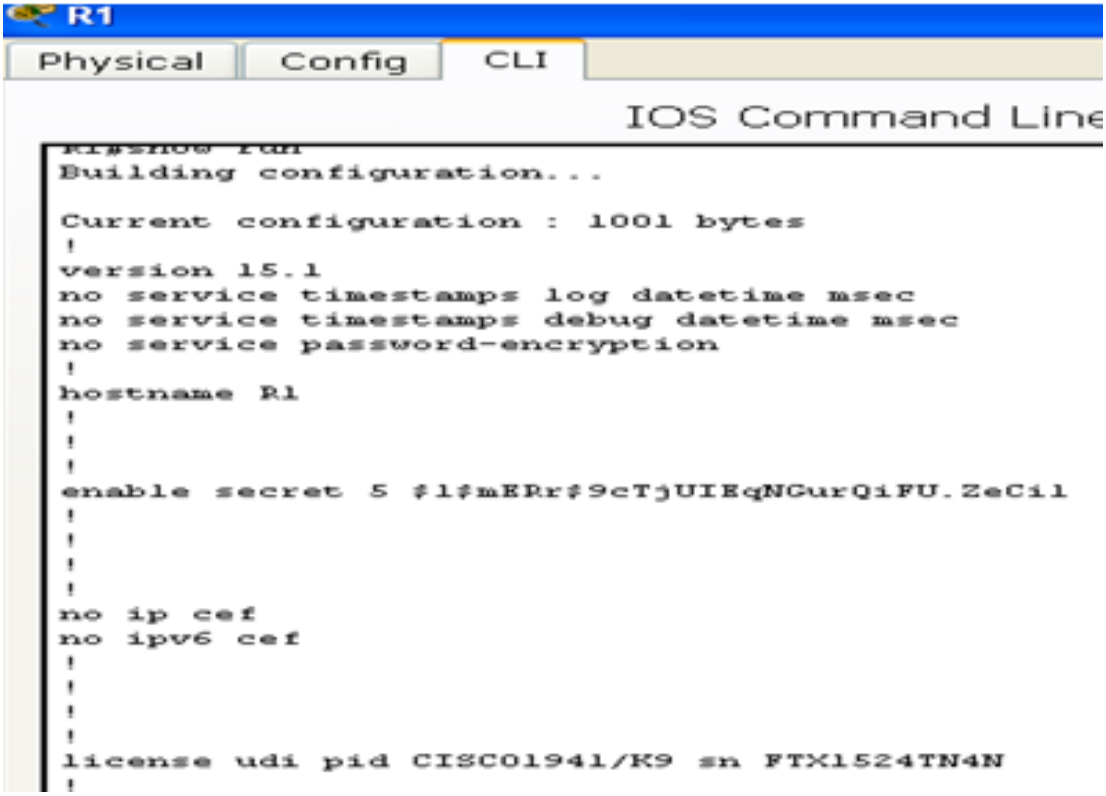


*Figure 34 Comando undebug all*

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

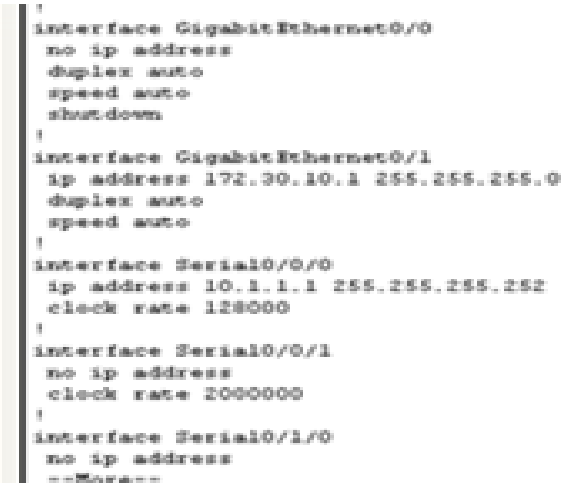


*Figure 35 Comando Show run en R3*

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
```

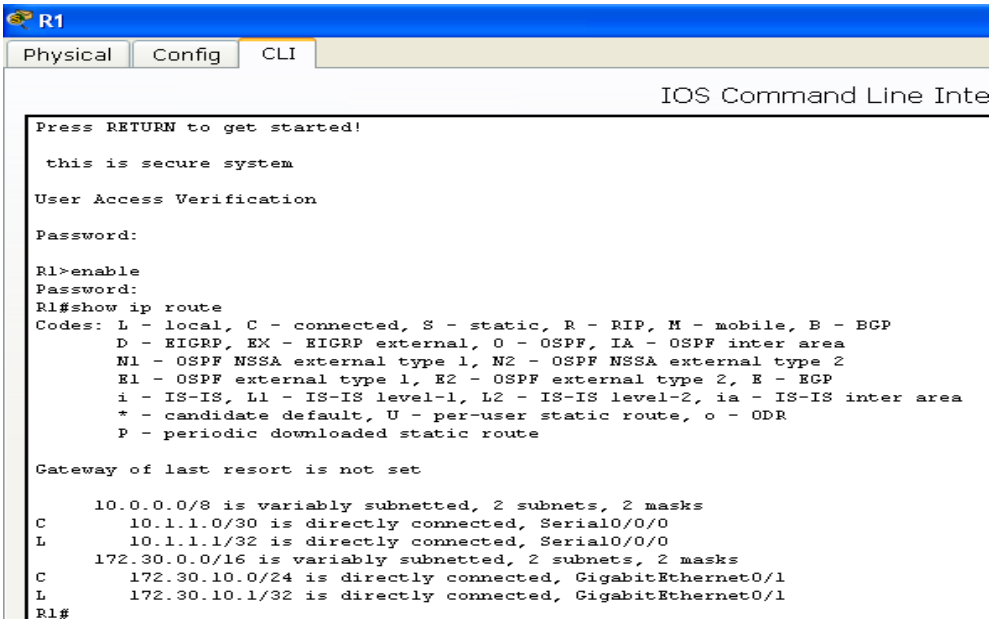


*Figure 36 Sumarización automática de las Rutas*

Utilice el comando **debug ip rip** en el R2 para determinar las rutas recibidas en las actualizaciones RIP del R3 e indíquelas a continuación, incluida la máscara de subred. Por lo tanto, las tablas de routing del R1 y el R2 no muestran las subredes 172.30.0.0 en el R3.

### Paso 3. Desactivar la sumarización automática.

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

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

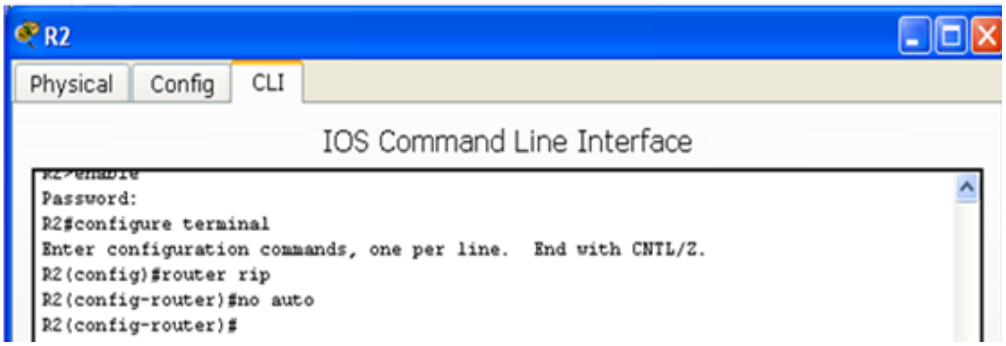


*Figure 37 Desactivar sumarización automática*

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

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


*Figure 38 Comando clear ip route*

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
```

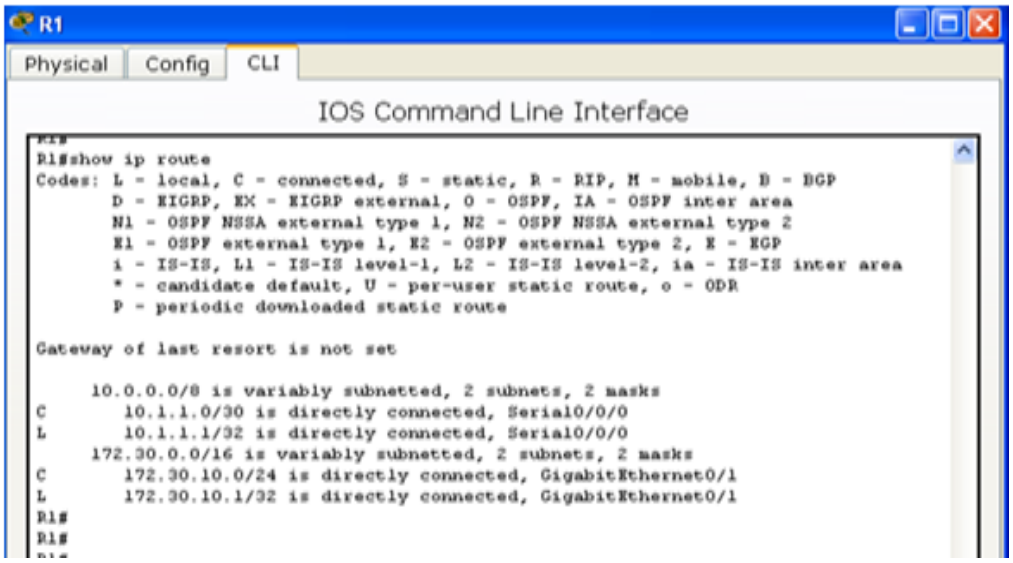


*Figure 39 Tablas de enrutamiento*

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

```
R2# debug ip rip
```

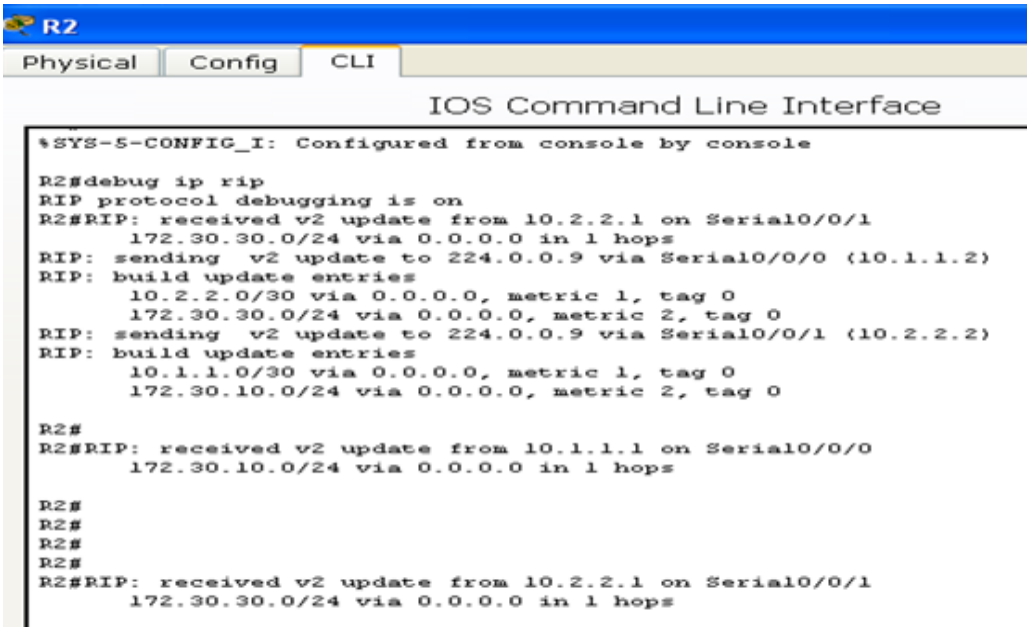


*Figure 40 Comando debug ip rip en R2*

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

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
```

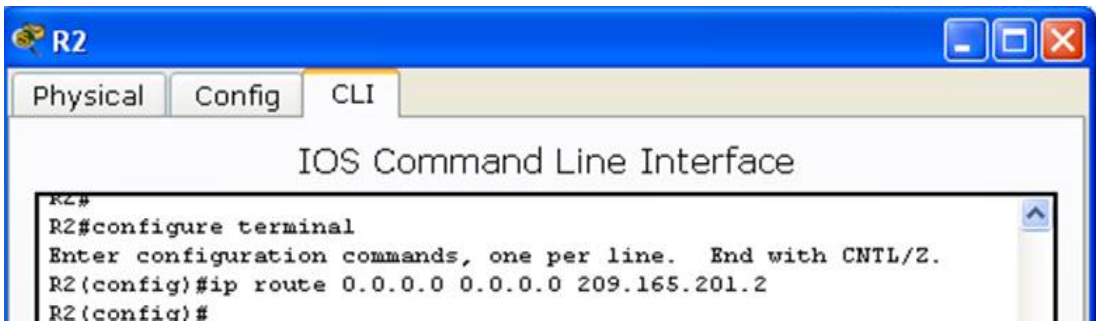


*Figure 41 Ruta estática*

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
```

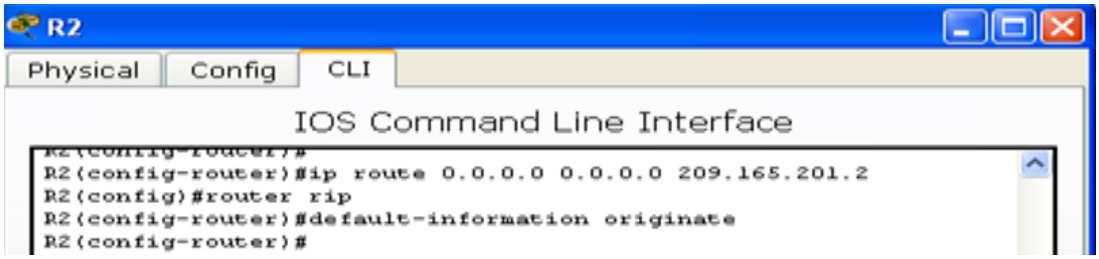


*Figure 42 Comando default information originale*

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

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
```

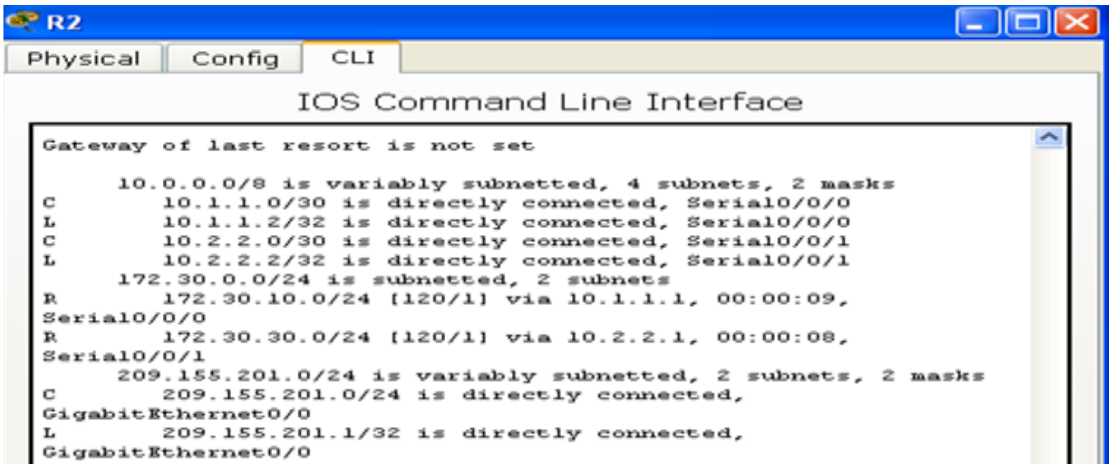


*Figure 43 Tabla routing en R1*

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

R2(config)# **router rip**

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

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?

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

## Paso 6. Verifique la conectividad.

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_

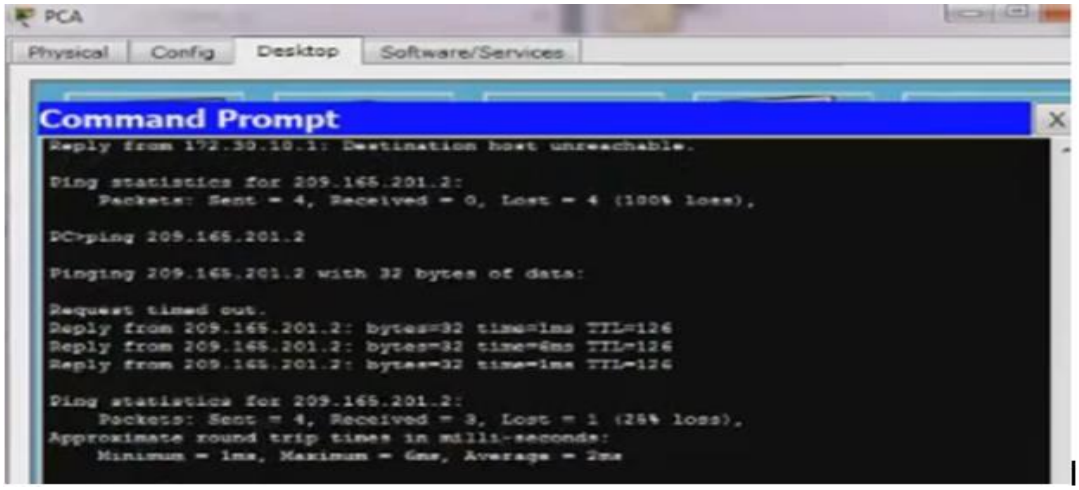


*Figure 44 Ping Pc-A a Pc-C*

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.

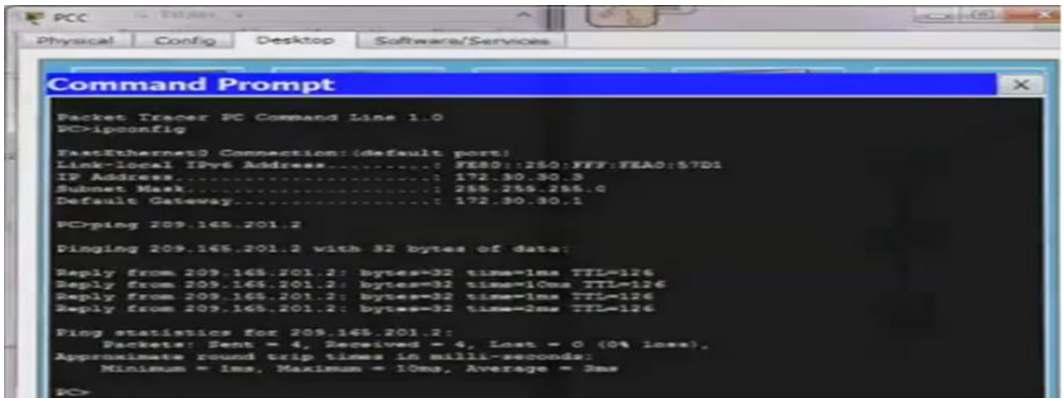


*Figure 45 Verificación hosts*

## 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 |

*Tabla 3 Configuración IPv6 en los dispositivos*

### 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.

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

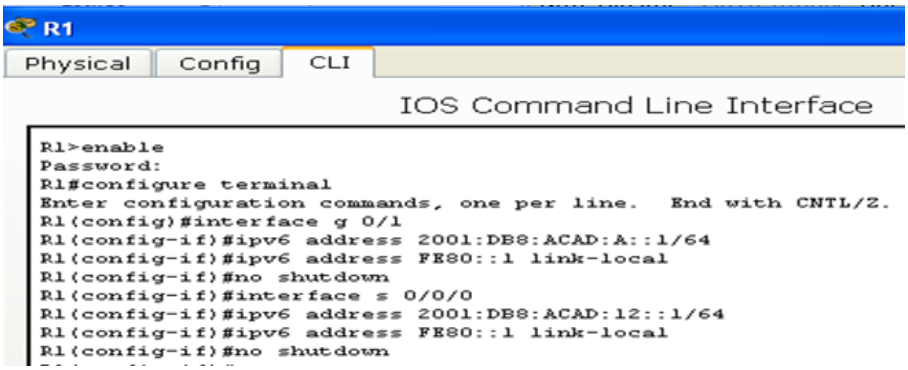


*Figure 46 Direccionamiento para cada interfaz del router R1*

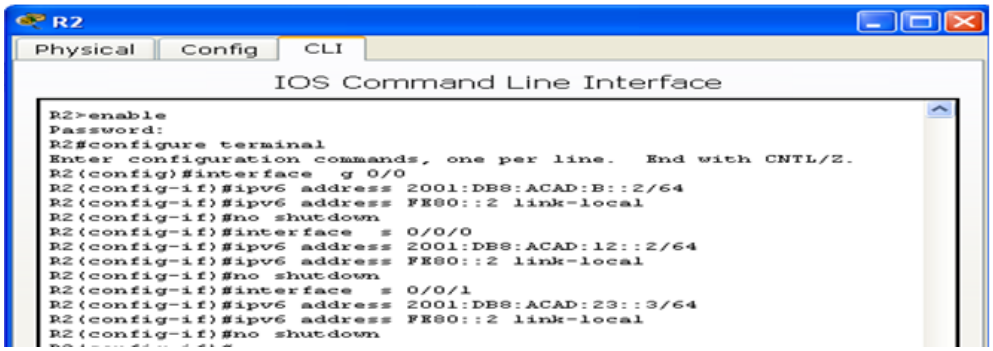


*Figure 47 Direccionamiento para cada interfaz del router R2*

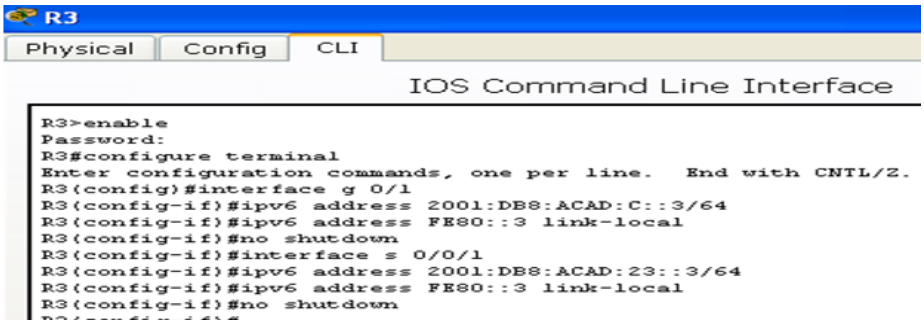


*Figure 48 Direccionamiento para cada interfaz del router R3*

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

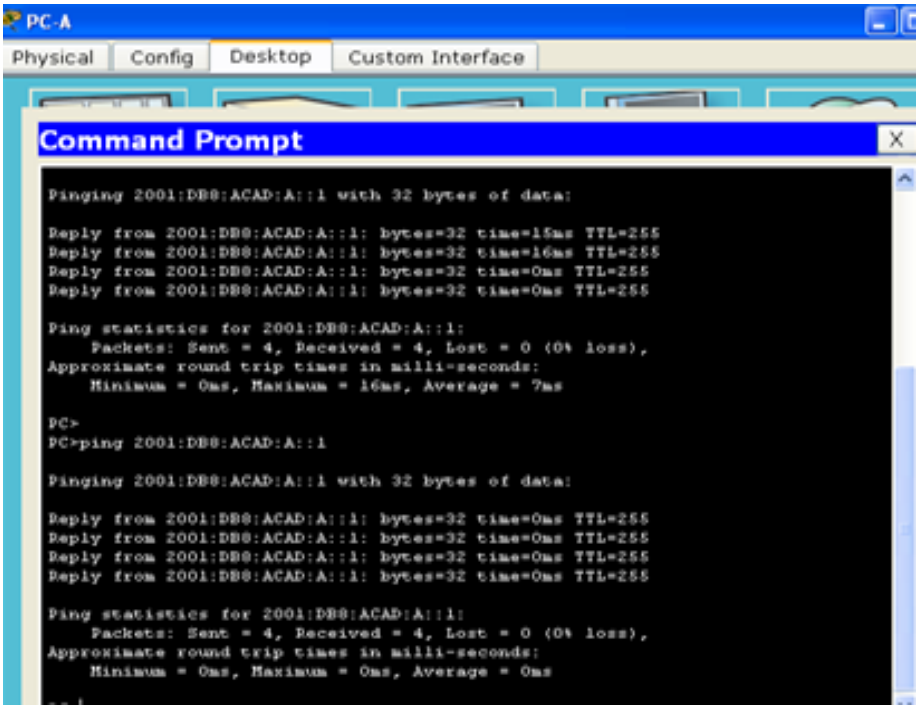


*Figure 49 Ping a router desde Pc-A*

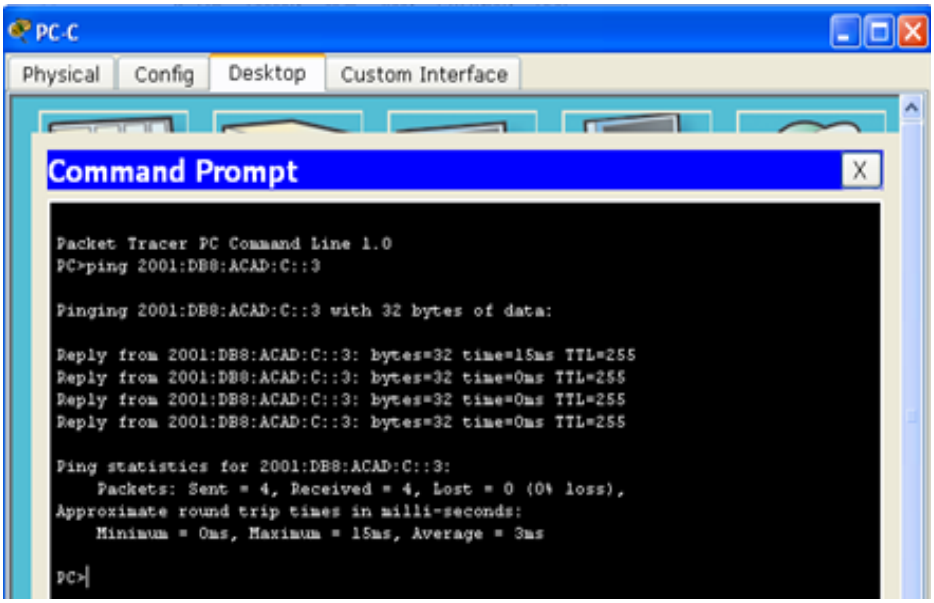


*Figure 50 Ping a router desde Pc-C*

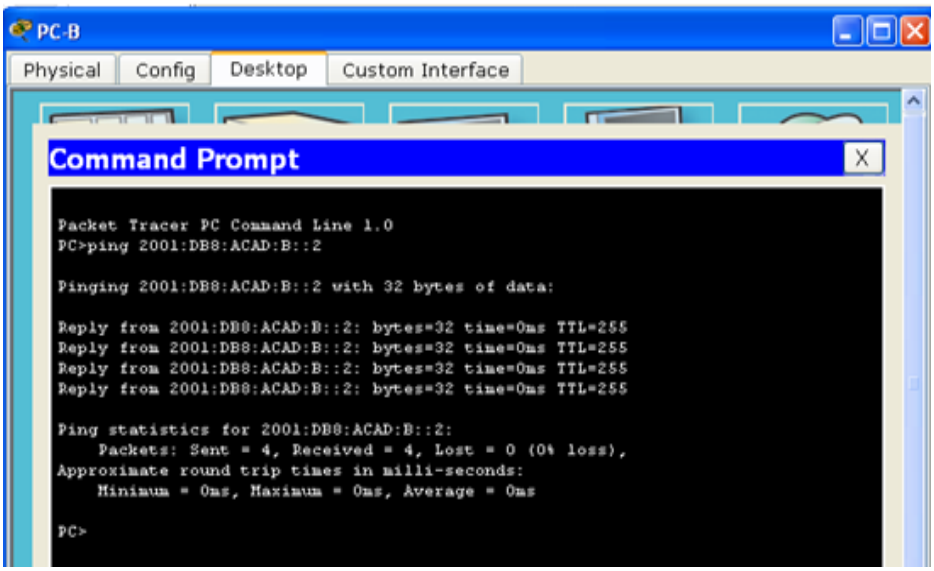


*Figure 51 Ping a router desde Pc-B*

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

Resuelto en las pantallas anteriores …

## 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
```

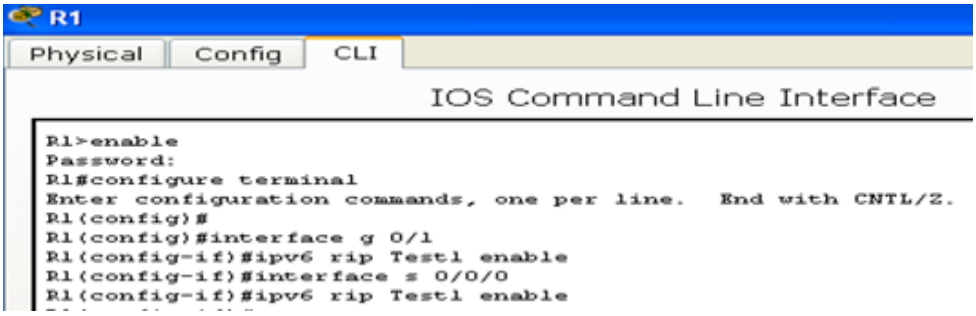


*Figure 52 Test 1*

**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

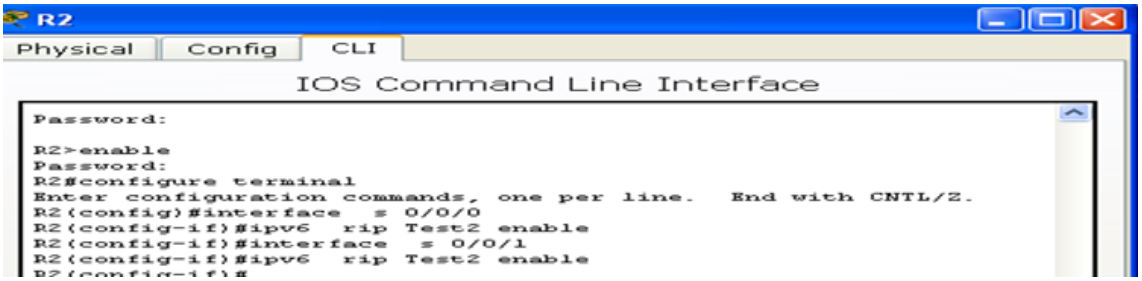


*Figure 53 Test 2*

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

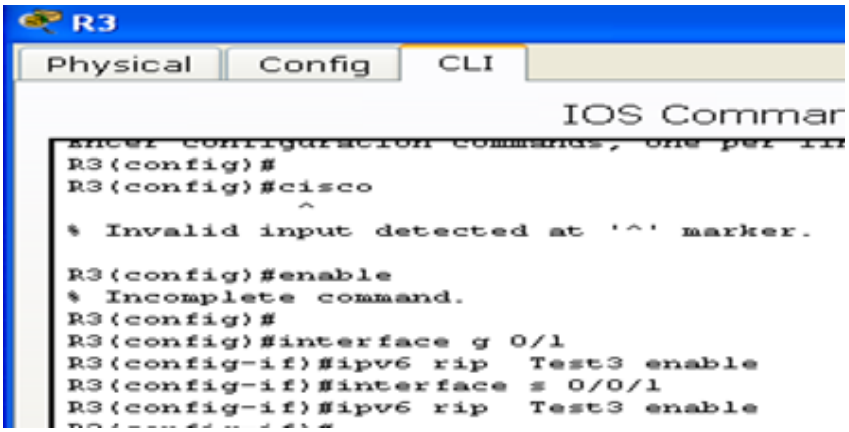


*Figure 54 Test 3*

**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
```

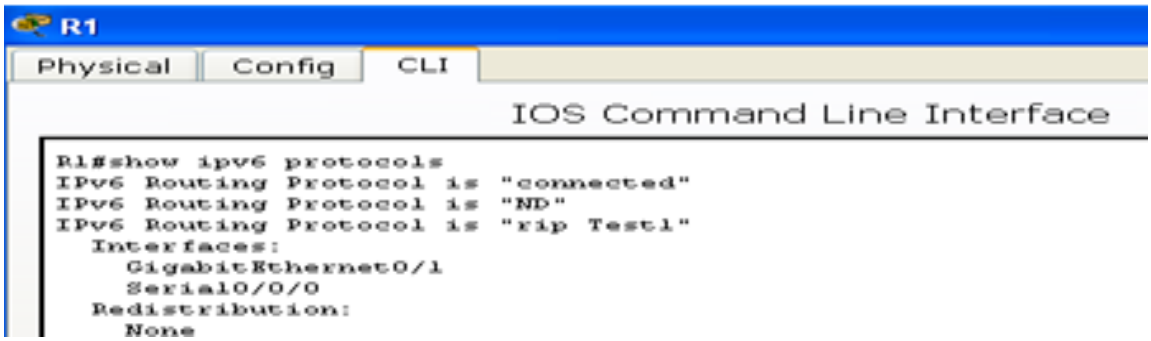


*Figure 55 Verificación RIPng*

¿En qué forma se indica RIPng en el resultado?

R1# show ipv6 protocols

**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
```


*Figure 56 Comando shoe ipv6 rip test 1*

**f.** ¿Cuáles son las similitudes entre RIPv2 y RIPng?

Las actualizaciones se envían cada 30 segundos y expiran en 180 segundos, estas actualizaciones se mantienen cada 0 segundos y se eliminan después de 120 segundos.

**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. | | | | |

*Tabla 4 Resumen de interfaces del router*

## Práctica 8.2.4.5 Packet Tracer Configuración de OSPFv2 Básico de Área Única

### Topología

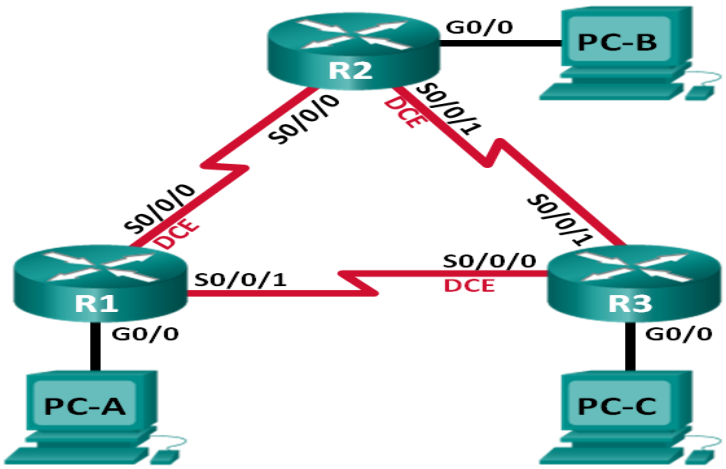


*Figure 57 Topología 8.2.4.5*

### 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 |

*Tabla 5 Configuración OSPFv2 básico de área única*

### Objetivos

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

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

### Información básica/situación

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

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

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

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

### Recursos necesarios

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

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

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

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

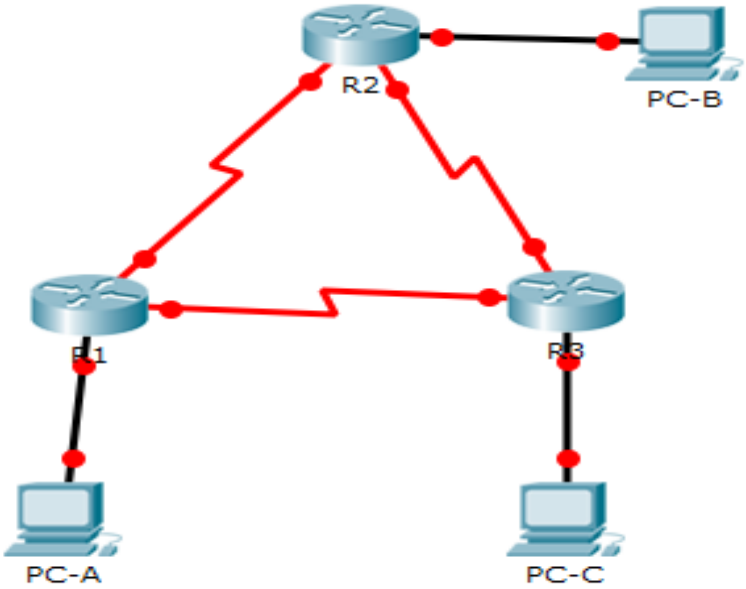


*Figure 58 Topología*

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

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

**a.** Desactive la búsqueda del DNS.

**b. C**onfigure 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.

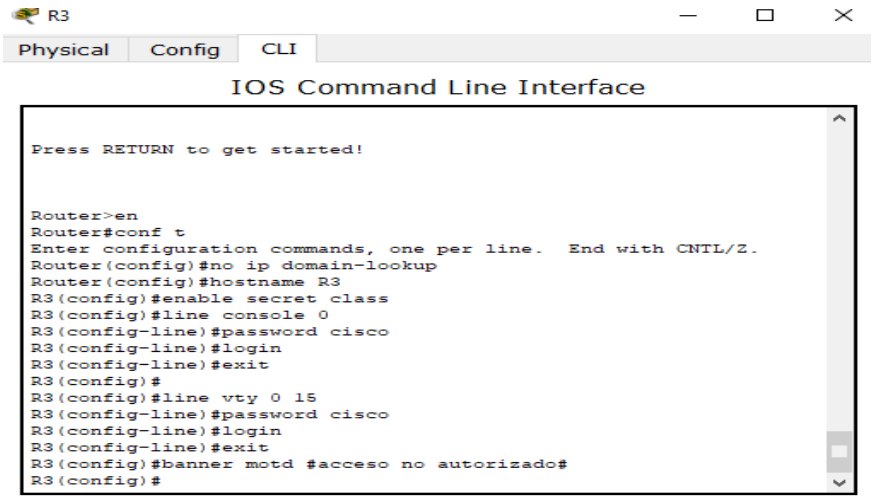


*Figure 59 Configuración de parámetros básicos*

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

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

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

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

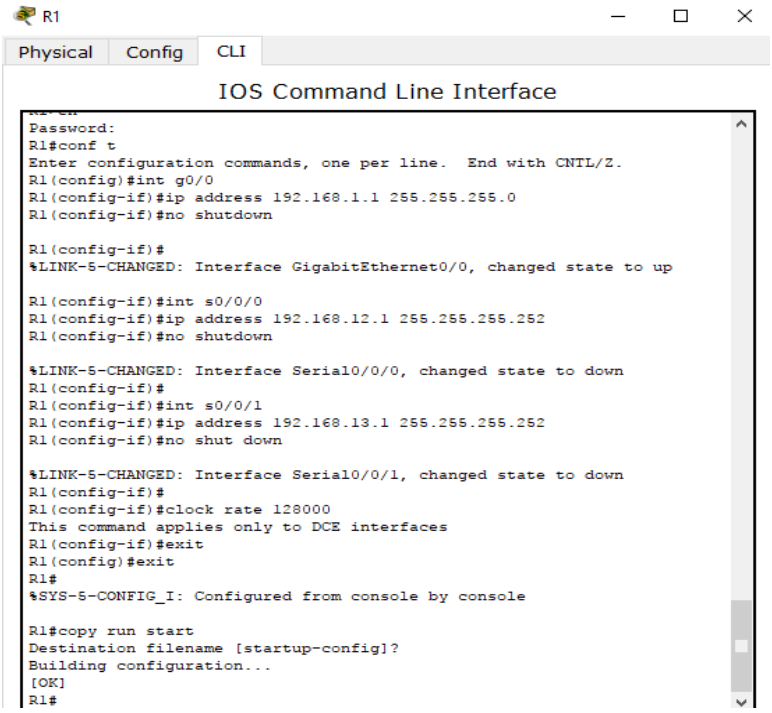


*Figure 60 Configuración de parámetros básicos.*

## Paso 4: Configurar los equipos host.

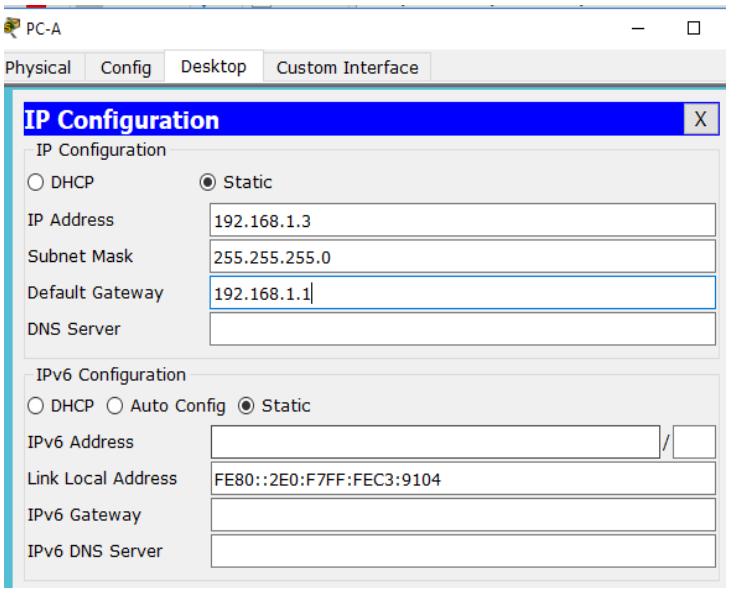


*Figure 61 Configuración Pc-A*

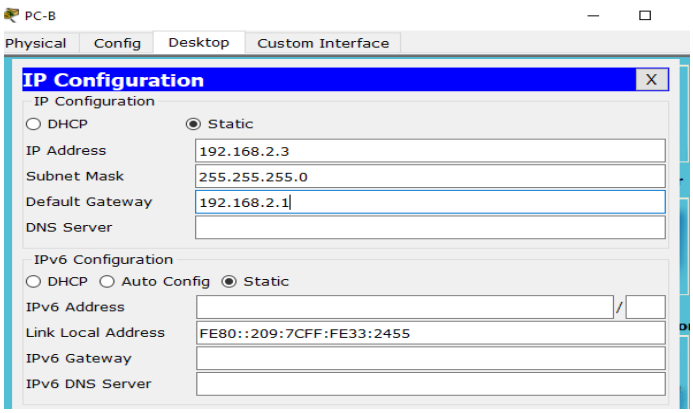


*Figure 62 Configuración Pc-B*

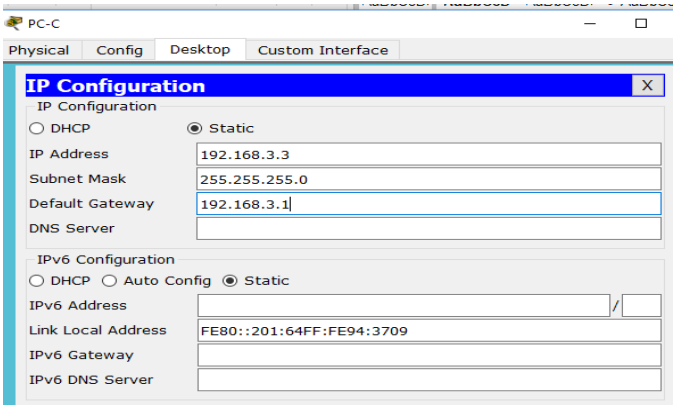


*Figure 63 Configuración Pc-C*

### 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.

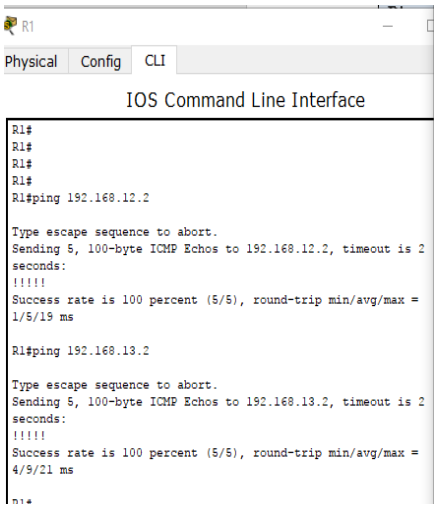


*Figure 64 Probando conectividad*

## Parte 2: Configurar y verificar el enrutamiento OSPF

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

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

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

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

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

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

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

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

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

```
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#
```

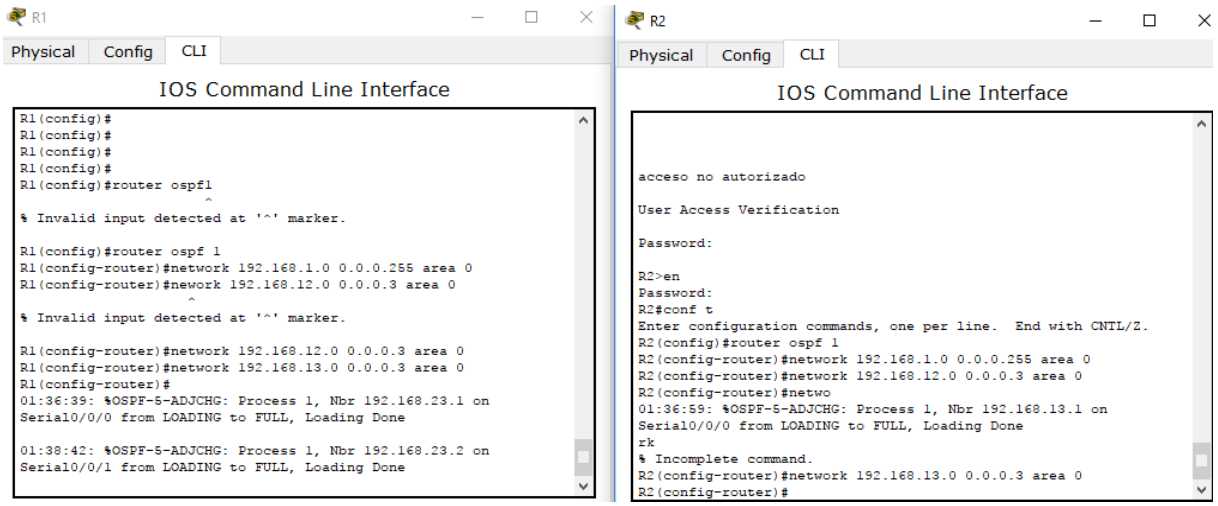


*Figure 65 Configuración OSPFen R1 y R2*

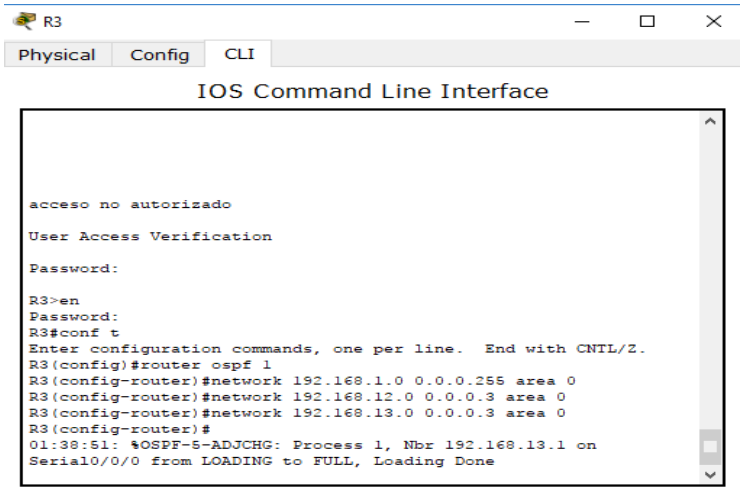


*Figure 66 Configuración OSPFen R3*

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

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

```
R1# show ip ospf neighbor

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

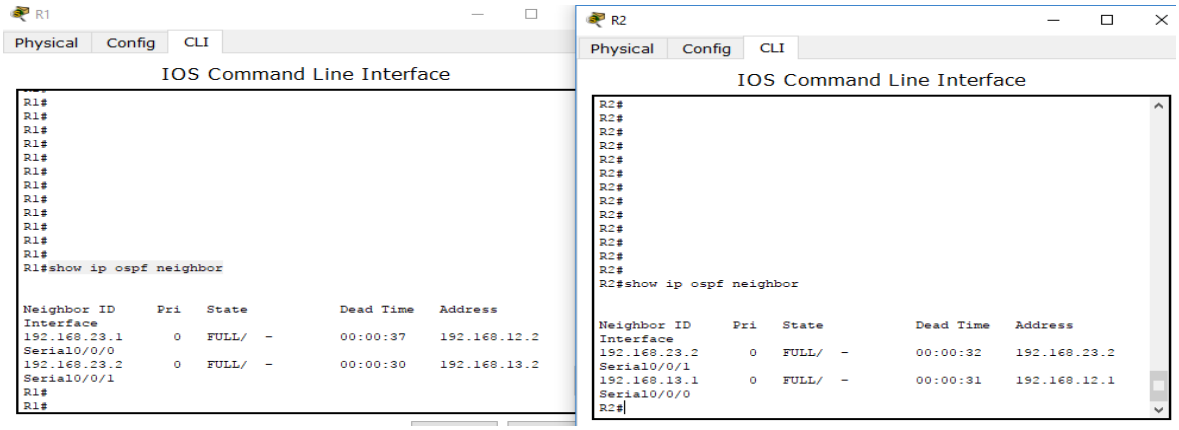


*Figure 67 Verificación de vecinos OSPF en R1 y R2*

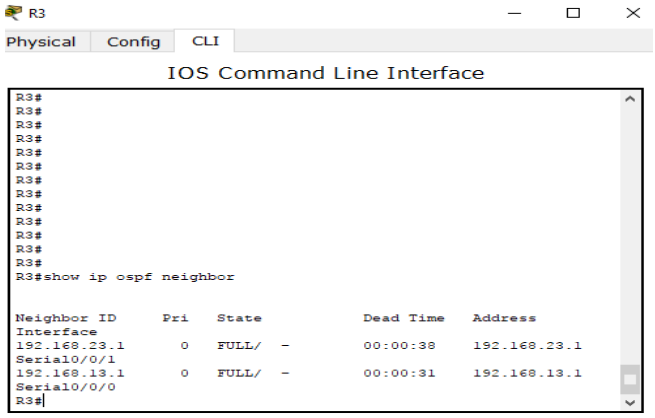


*Figure 68 Verificación de vecinos OSPF en R3*

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

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

Gateway of last resort is not set

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

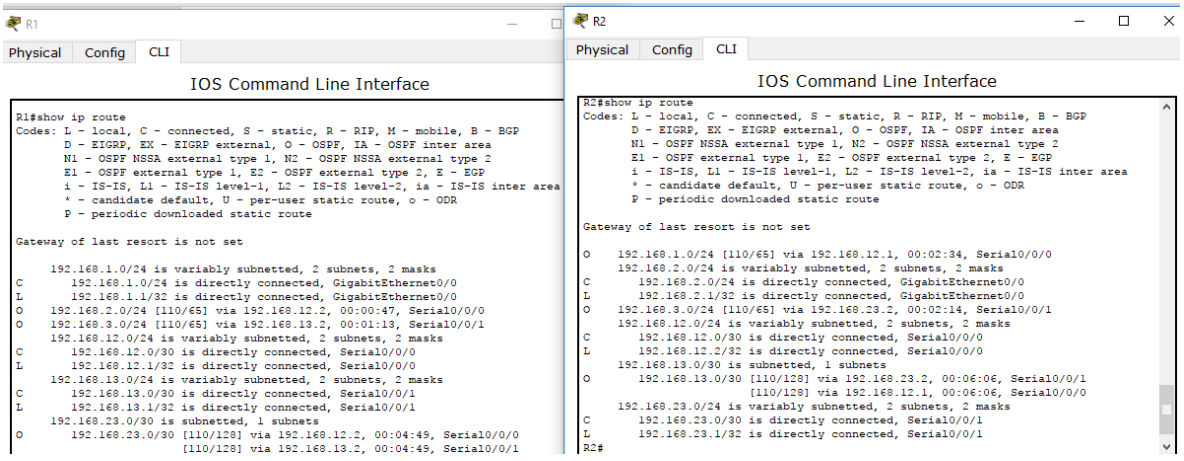


*Figure 69 Verificación de redes en R1 yR2*

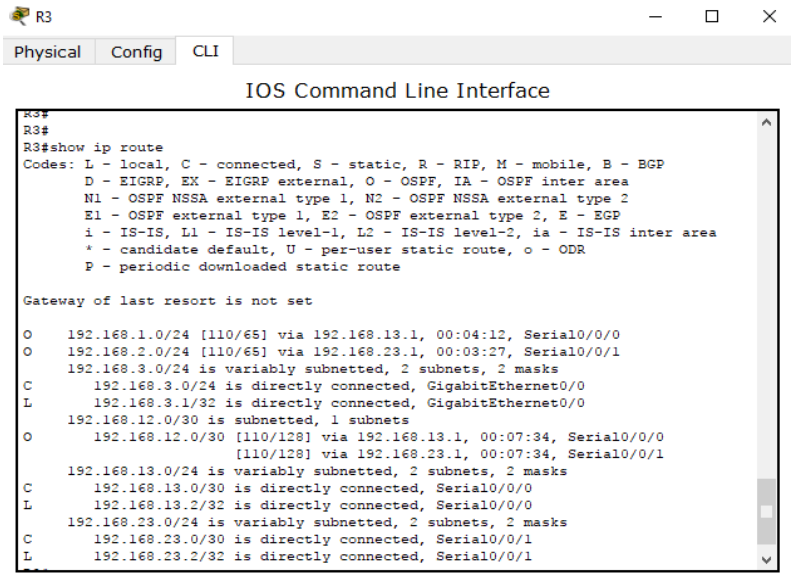


*Figure 70 Verificación de redes en R3*

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

**R=/ show ip route ospf**

## Paso 4: Verificar la configuración del protocolo OSPF.

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

```
R1# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.23.2         110      00:19:16
    192.168.23.1         110      00:20:03
```

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

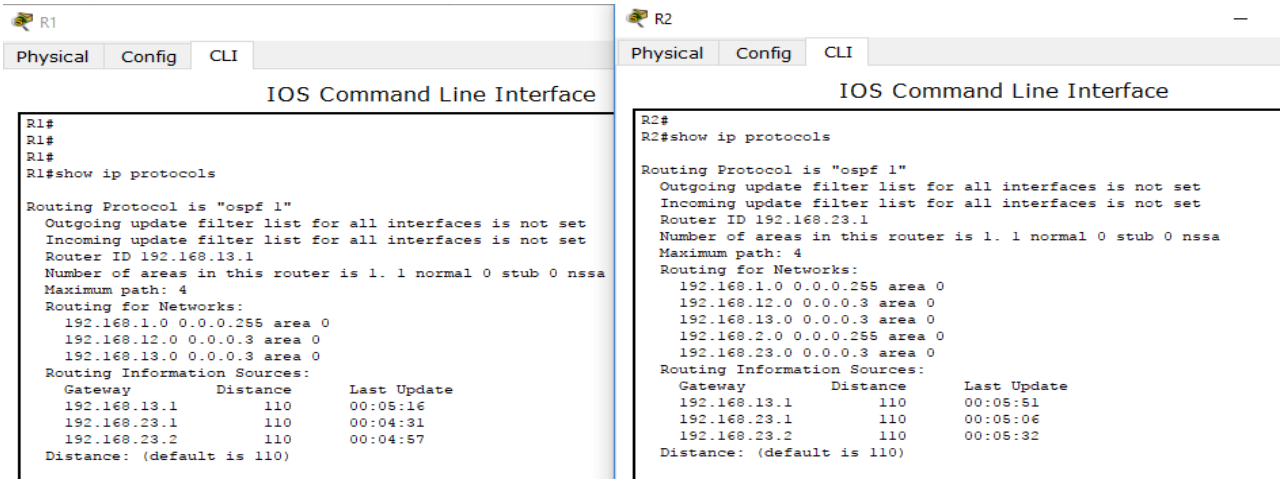


*Figure 71 Verificación de protocolo OSPF en R1 y R2*

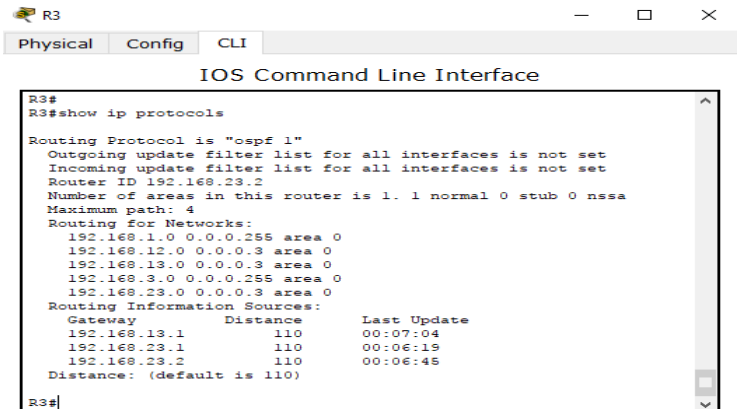


*Figure 72 Verificación de protocolo OSPF en R3*

## Paso 5: Verificar la información del proceso OSPF.

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

```
R1# show ip ospf
 Routing Process "ospf 1" with ID 192.168.13.1
 Start time: 00:20:23.260, Time elapsed: 00:25:08.296
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
```

```
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
   Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm last executed 00:22:53.756 ago
        SPF algorithm executed 7 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x019A61
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

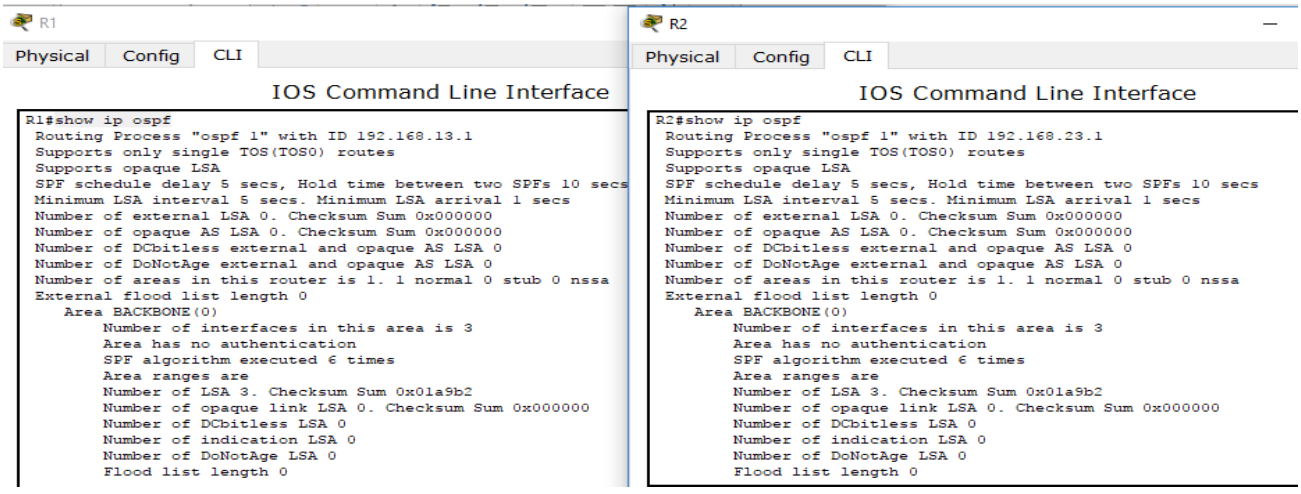


*Figure 73 Verificación de proceso OSPF en R1 y R2*

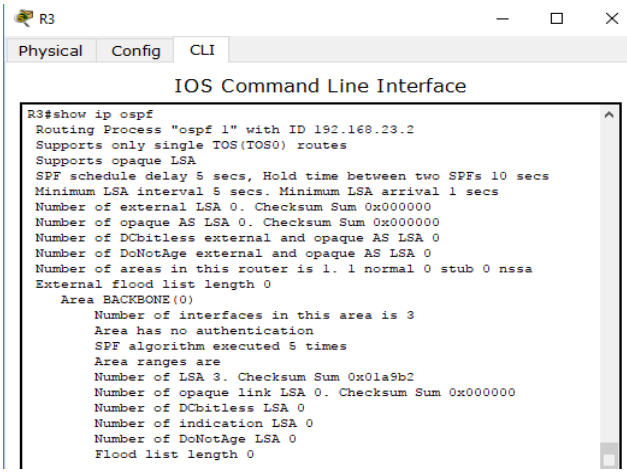


*Figure 74 Verificación de proceso OSPF en R3*

## Paso 6: Verificar la configuración de la interfaz OSPF.

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

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

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

```
R1# show ip ospf interface
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network
Statement
  Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT,
Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
```

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

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

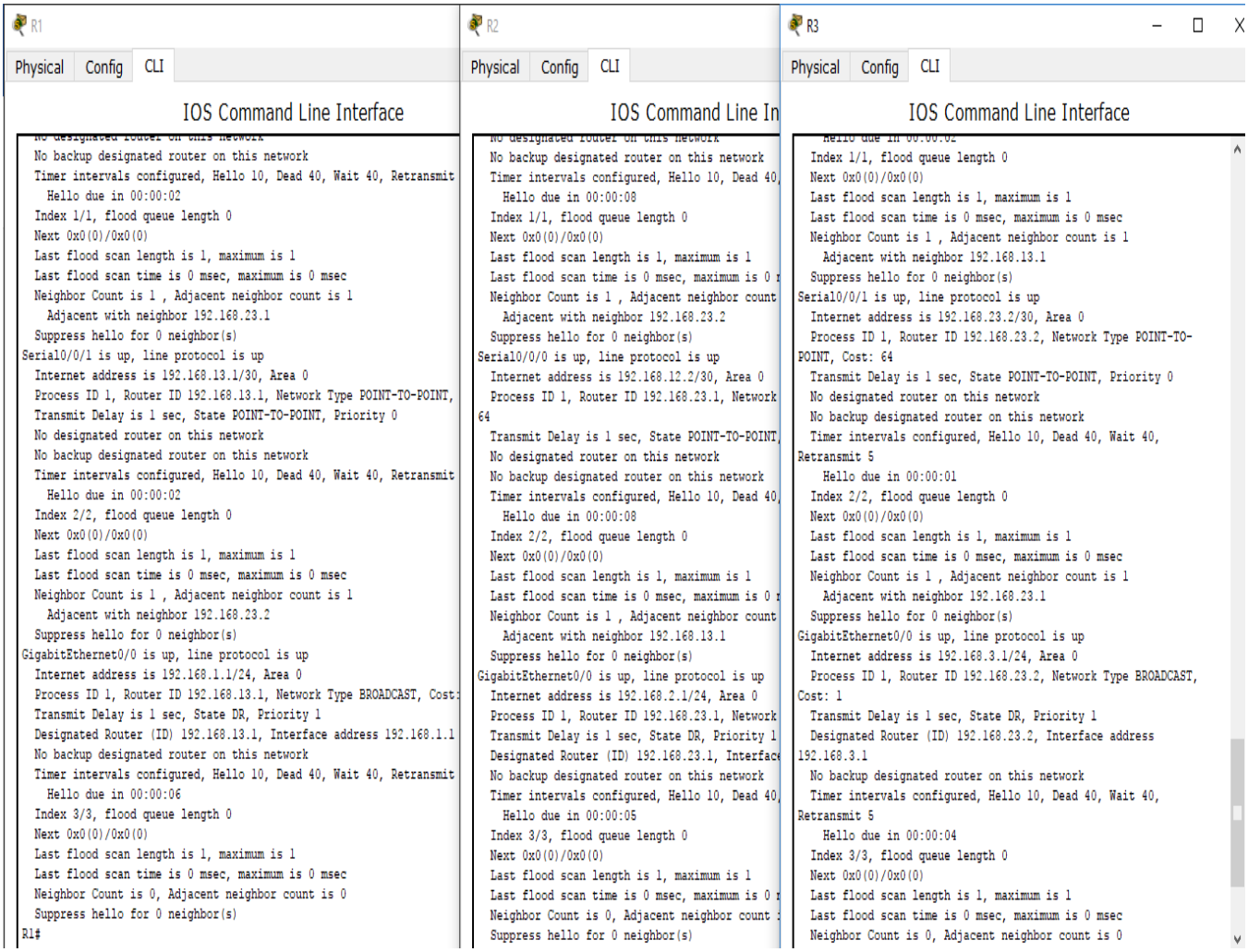


*Figure 75 Verificación interfaz OSPF*

## 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.

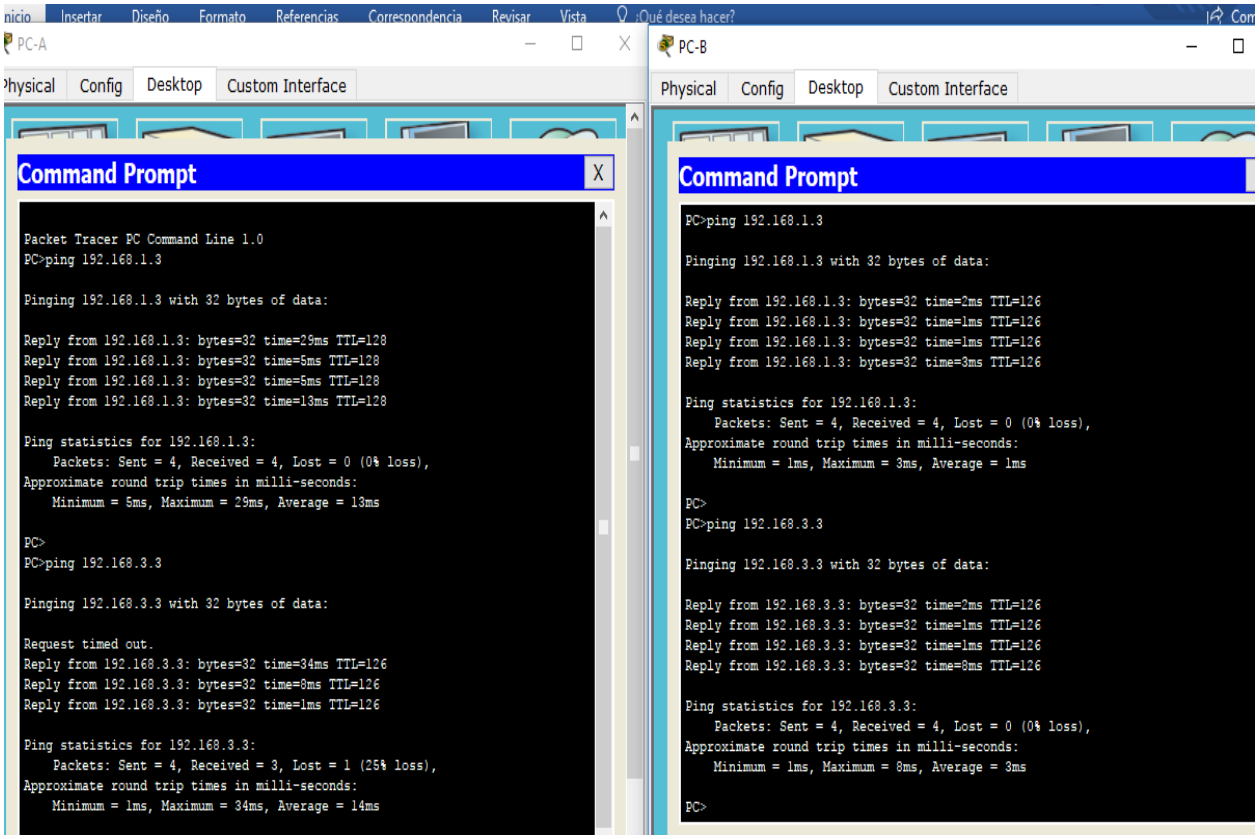


*Figure 76 Verificación de conectividad en Pc-A y Pc-B*

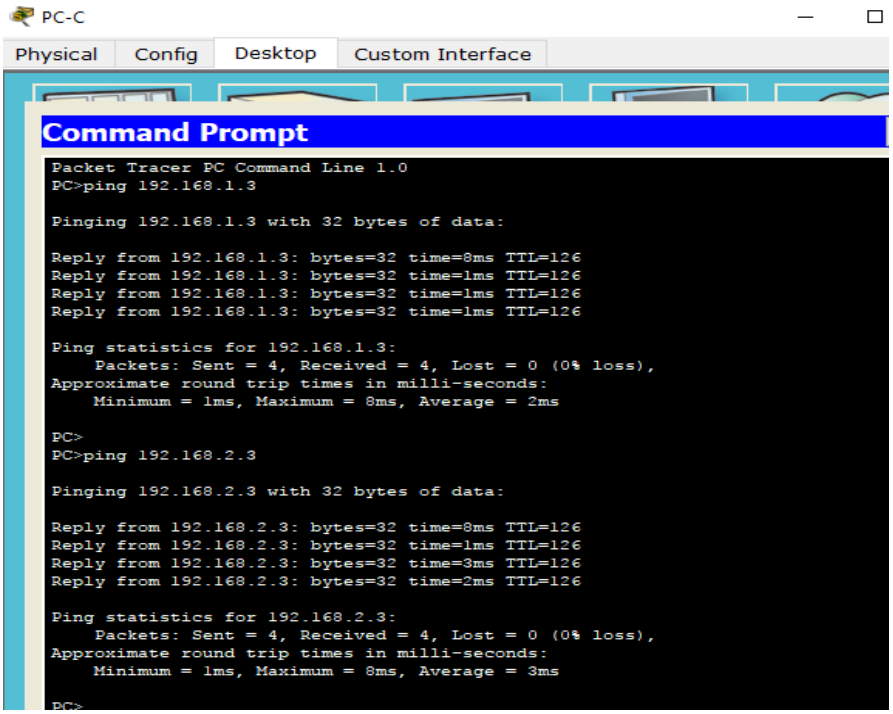


*Figure 77 Verificación de conectividad en Pc-B*

**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. | | | | |

*Tabla 6 Resumen de interfaces del router*

## Práctica - 9.2.1.10 Packet Tracer Configuring Standard ACLs Instructions IG

## Topología

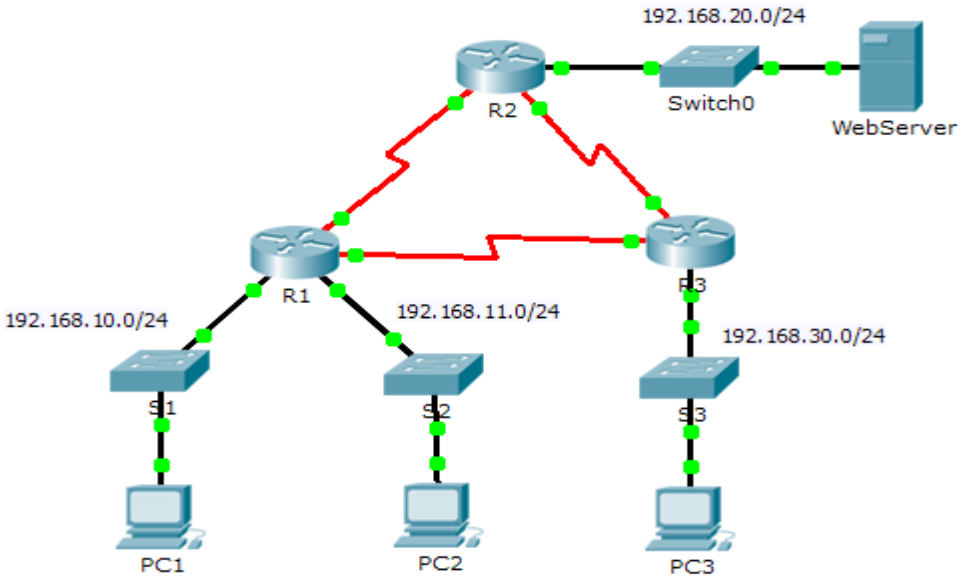


*Figure 78 Topología 9.2.1.10*

## Addressing Table

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

*Tabla 7 Configuring standar ACLs instructions IG*

**Objectivos**

**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.

## Parte 1: Plan an ACL Implementation

**Paso 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.

**Paso 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.

## Parte 2: Configure, Apply, and Verify a Standard ACL

### Paso 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
```

```
R3#show access-lists
Standard IP access list 1
    10 deny 192.168.10.0 0.0.0.255 (4 match(es))
    20 permit any

R3#
```

*Figure 79 ACL*

### Paso 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#show access-lists
Standard IP access list 1
    10 deny 192.168.10.0 0.0.0.255 (4 match(es))
    20 permit any

R3#
```

*Figure 80 ACL.*

**Paso 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.

**b.** With the two ACLs in place, network traffic is restricted according to the policies detailed in Part

Use the following tests to verify the ACL implementations:

- ✓ A ping from 192.168.10.10 to 192.168.11.10 succeeds.

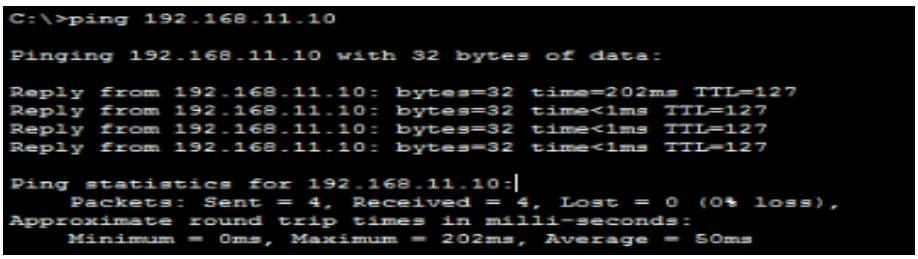


*Figure 81 Ping desde 192.168.10.10 a 192.168.11.10*

- ✓ A ping from 192.168.10.10 to 192.168.20.254 succeeds.

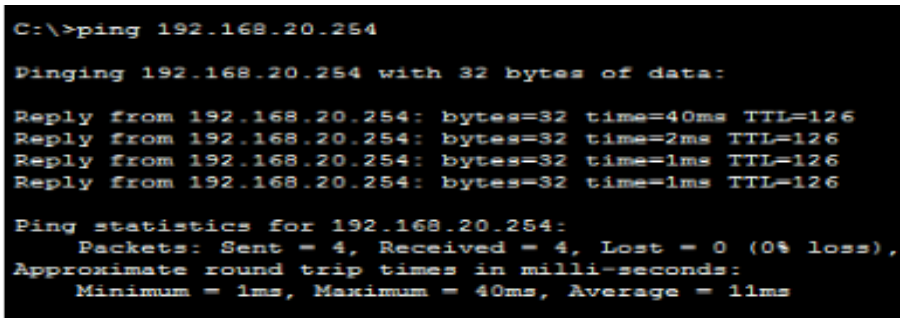


*Figure 82 Ping desde 192.168.10.10 a 192.168.20.254*

✓ A ping from 192.168.11.10 to 192.168.20.254 fails.

```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

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

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

*Figure 83 Ping desde 192.168.11.10 a 192.168.20.254*

✓ A ping from 192.168.10.10 to 192.168.30.10 fails.

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

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

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

*Figure 84 Ping desde 192.168.10.10 a 192.168.30.10*

✓ A ping from 192.168.11.10 to 192.168.30.10 succeeds.

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=2ms TTL=126
Reply from 192.168.30.10: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

*Figure 85 Ping desde 192.168.11.10 a 192.168.30.10*

✓ A ping from 192.168.30.10 to 192.168.20.254 succeeds.

```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=2ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=11ms TTL=126

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

*Figure 86 Ping desde 192.168.30.10 a 192.168.20.254*

## Práctica - 9.2.1.11 Packet Tracer Configuring Named Standard ACLs

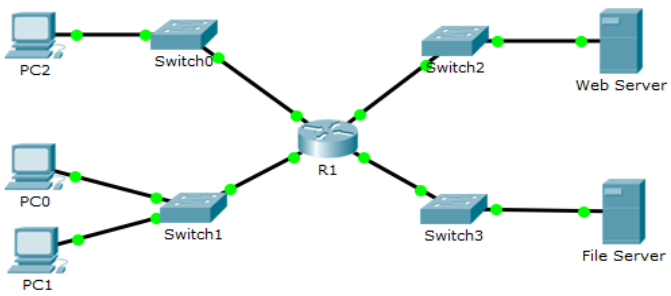


*Figure 87 Topología 9.2.1.11*

### Addressing Table

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

*Tabla 8 Configuring named standard ACLs*

### Objetivos:

**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.

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

### Paso 1: Verify connectivity before the ACL is configured and applied.

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

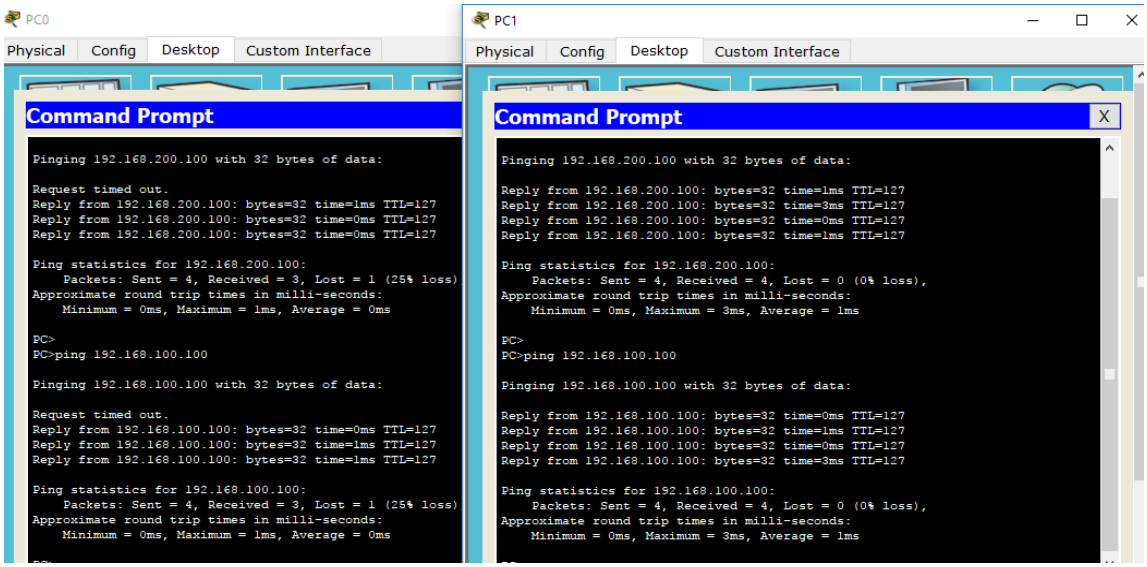


*Figure 88 Verificación de conectividad en Pc0 y Pc1*

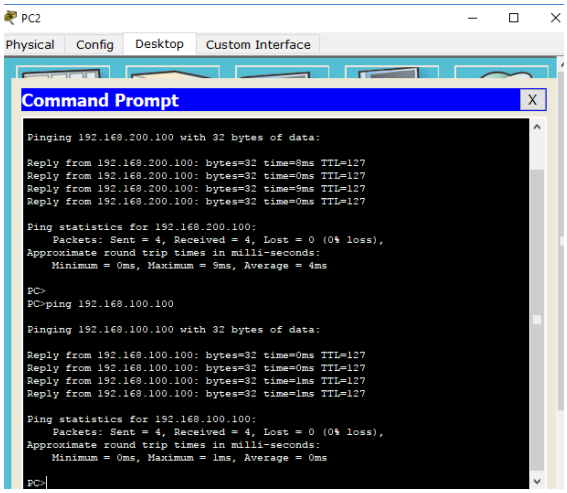


*Figure 89 Verificación de conectividad en Pc2*

### Paso 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.

### Paso 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.

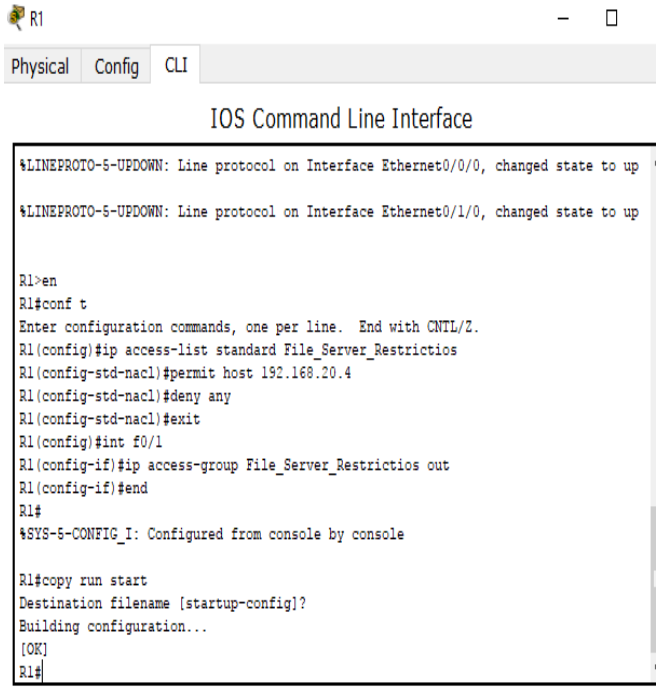


*Figure 90 Guardando configuración*

## Parte 2: Verify the ACL Implementation.

### Paso 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.

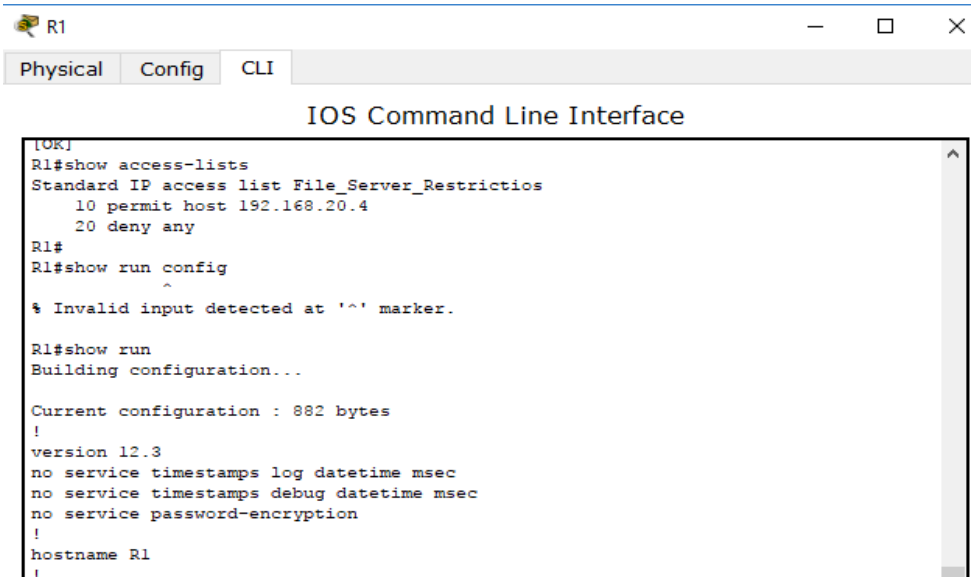


*Figure 91 Verificación configuración*

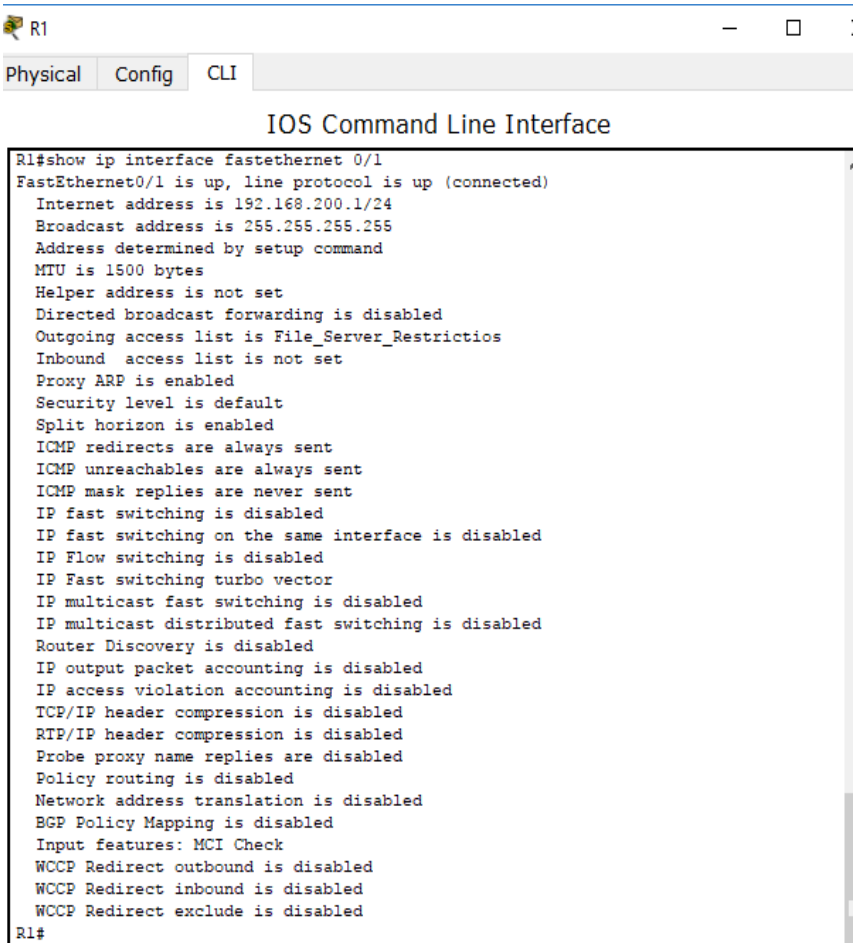


*Figure 92 Continuación de la verificación de configuración*

## Paso 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**.

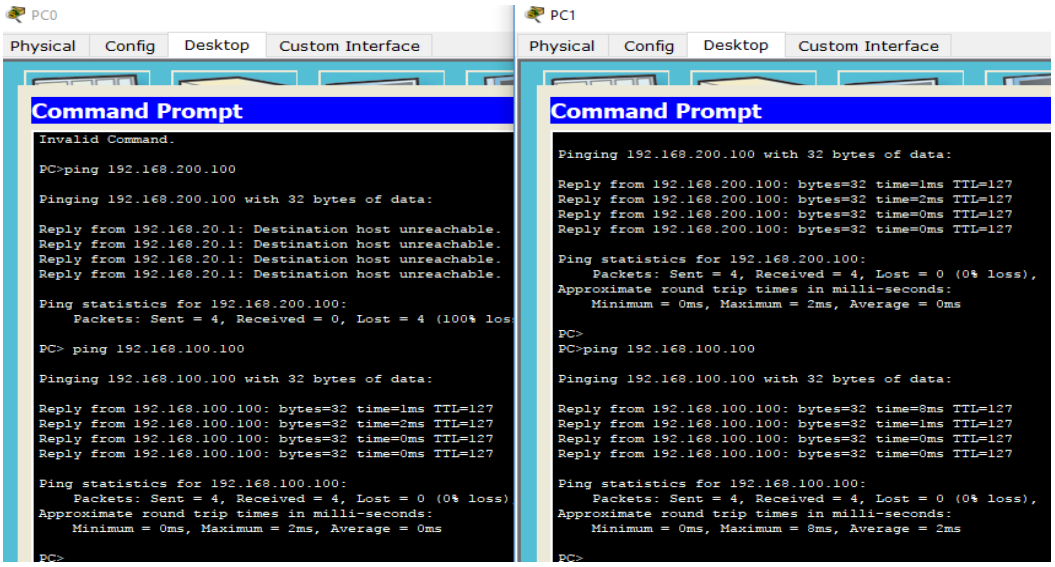


*Figure 93 Ping webserver en Pc0 y Pc1*

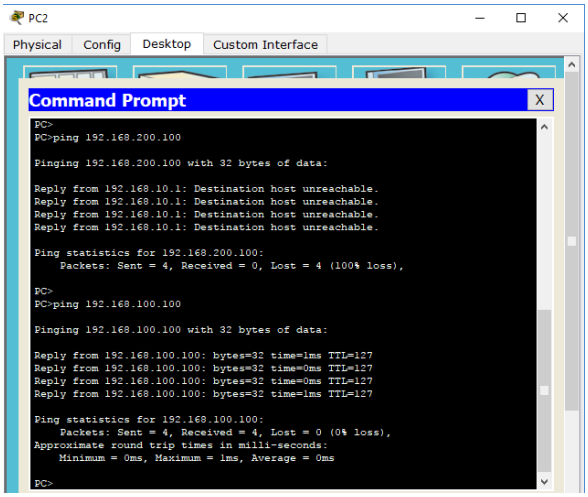


*Figure 94 Ping webserver en Pc2*

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

### Topología

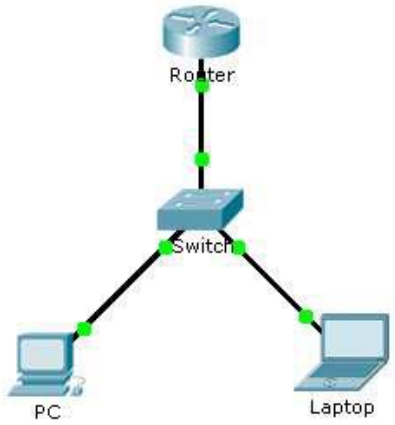


*Figure 95 Topología 9.2.3.3*

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

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

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

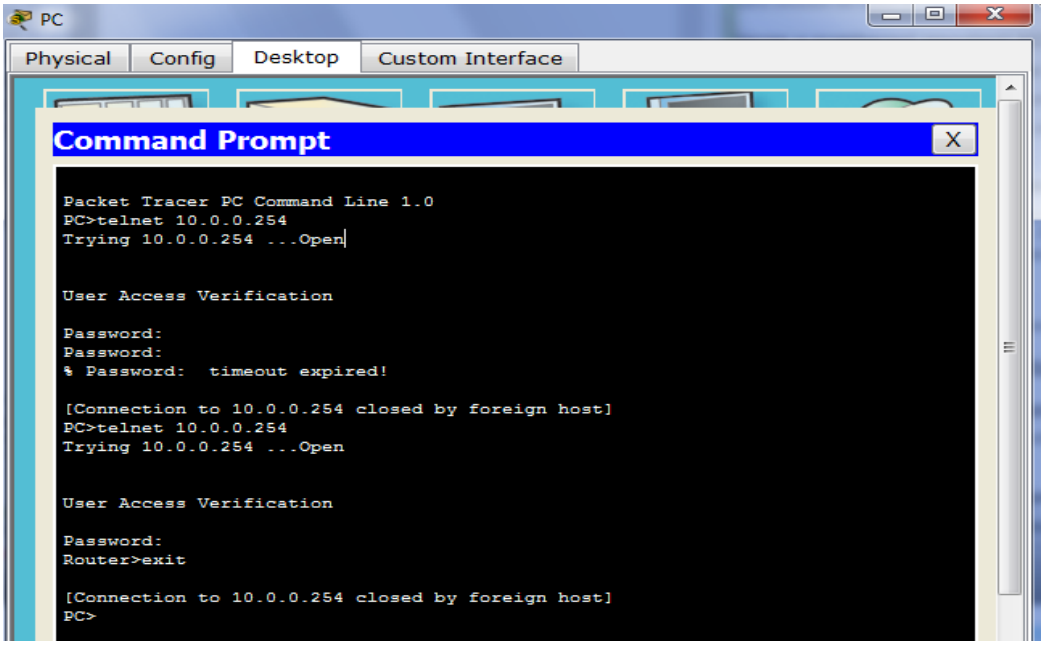


*Figure 96 verificación de acceso telnet en Pc*

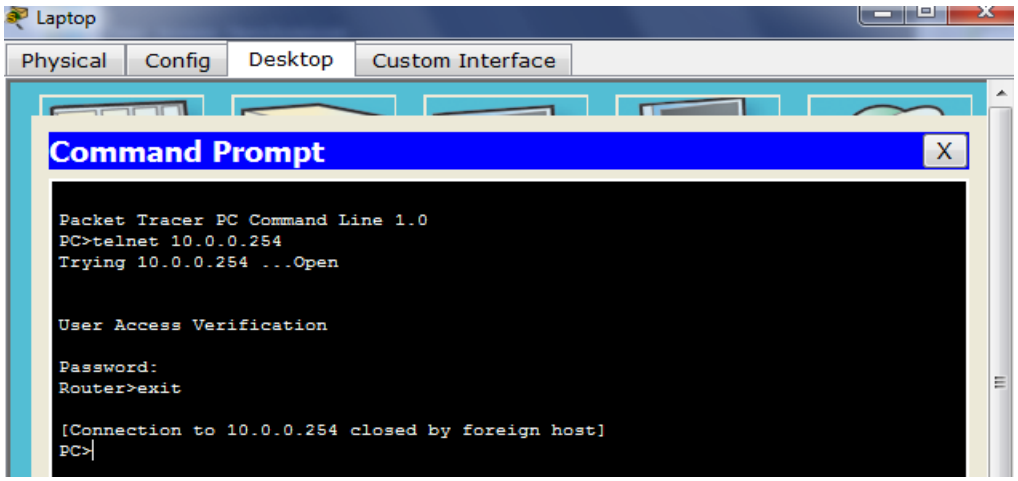


*Figure 97 verificación de acceso telnet en Laptop*

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

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

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

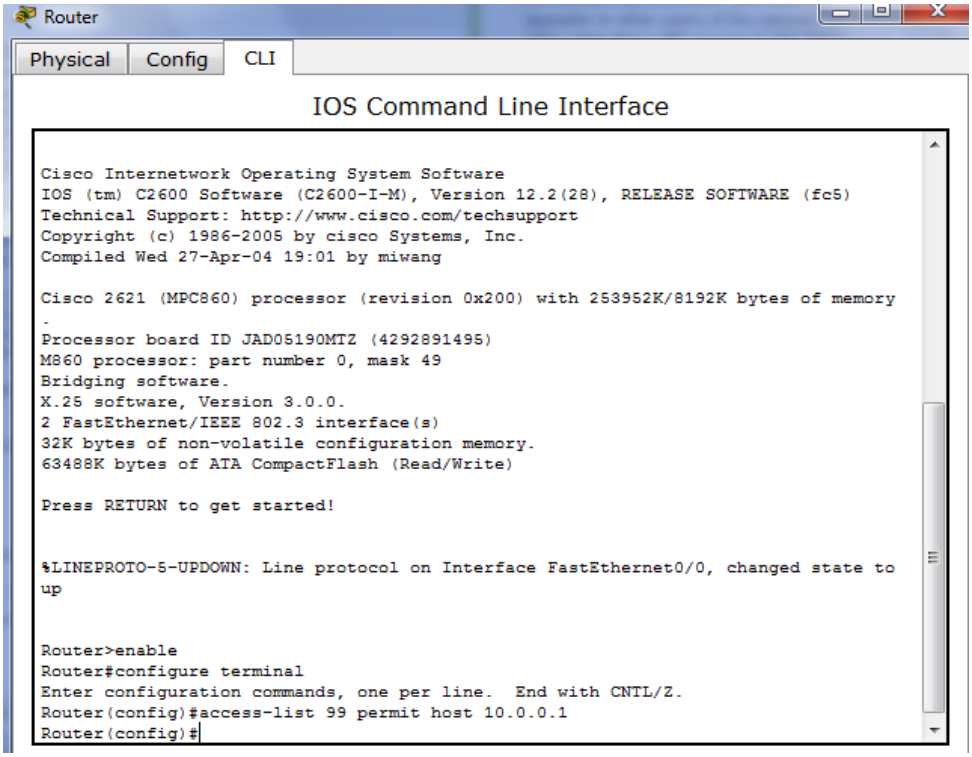


*Figure 98 Configuración número estándar ACL*

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

**Al final de la lista de acceso hay una denegación implícita que niega todas las conexiones**

### Paso 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
```

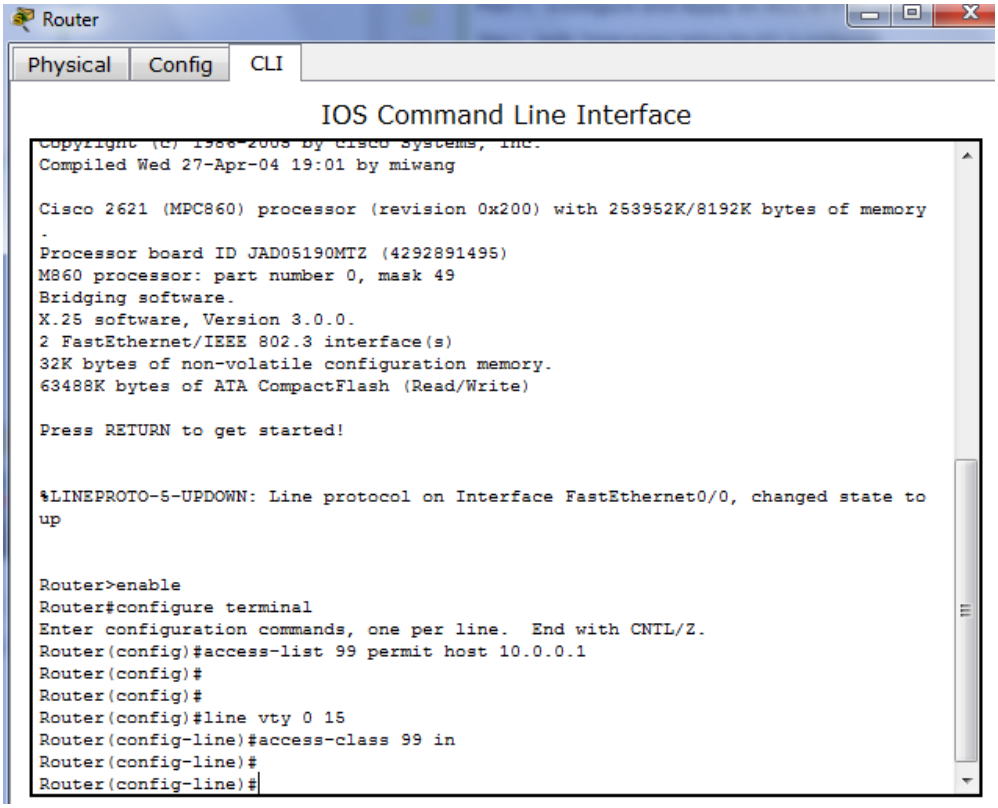


*Figure 99 Estandar ACL*

## Parte 2: Verify the ACL Implementation

### Paso 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.

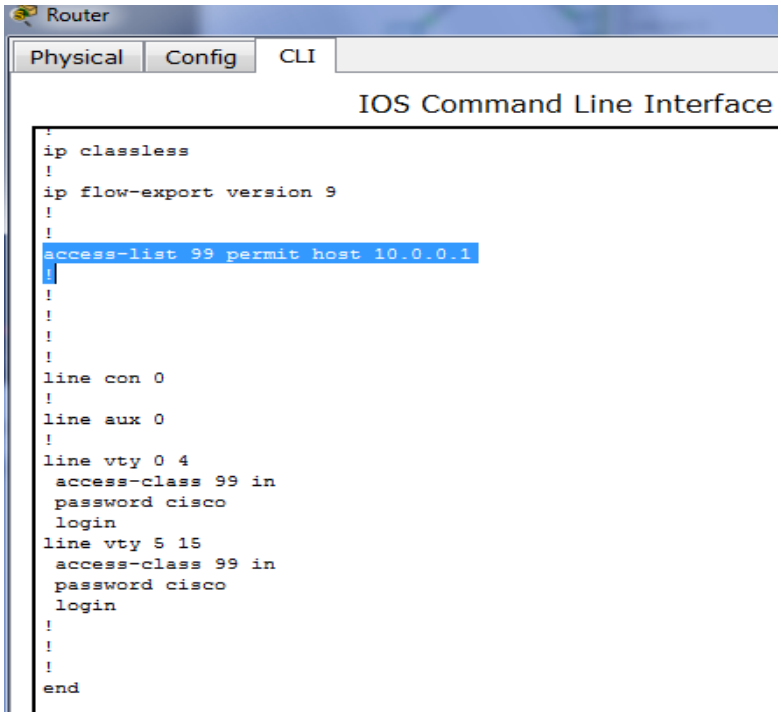


*Figure 100 Configuración VTY lines*

**Paso 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.

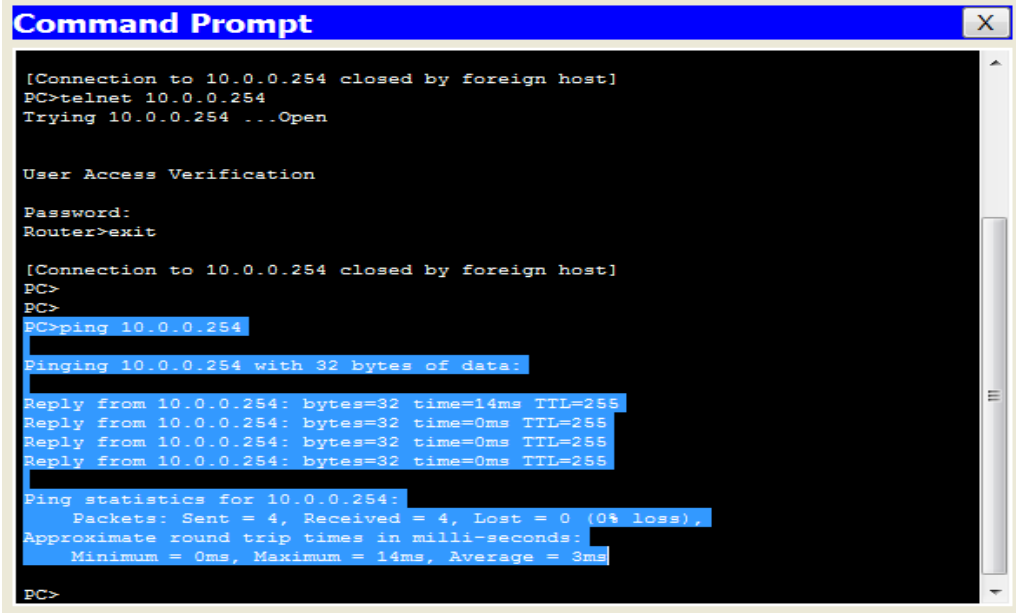


*Figure 101 Ping Laptop a Router*

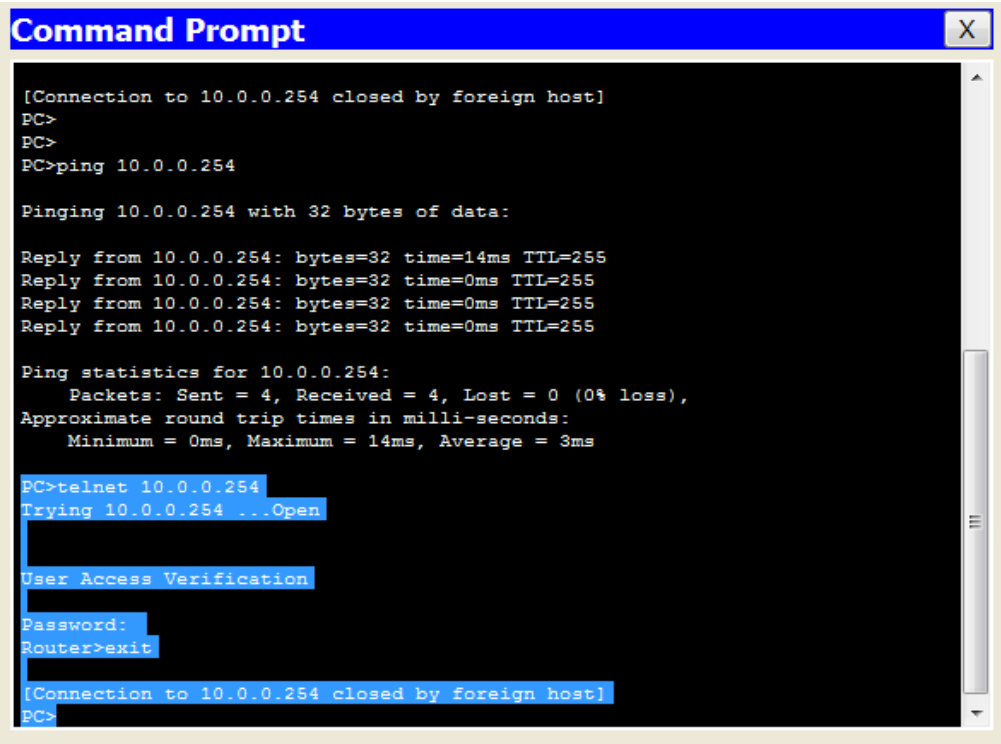


*Figure 102 Ping Pc a Telnet*

## Práctica 9.5.2.6 Packet Tracer Configuring IPv6 ACLs Instructions IG

### Topología

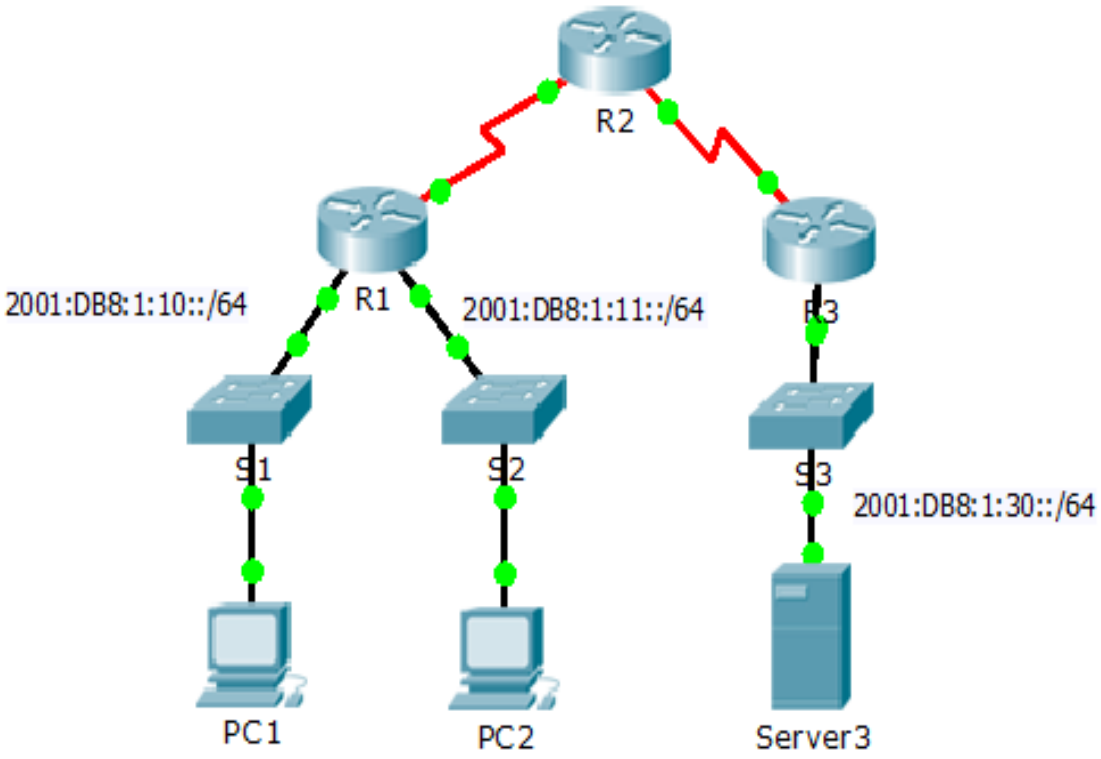


*Figure 103 Topología 9.5.2.6*

### Addressing Table

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

*Tabla 9 Configuring IPv6 ACLs instruction IG*

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

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

## Parte 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.

Los registros expresan que un ordenador hace a la red 11 estar repetidamente refrescando su página, esto causa un ataque de denegación de servicio en contra el servidor 3.

Para que el cliente pueda ser identificado y borrado se debe bloquear el acceso al HTTP y al HTTPS hacia la red por medio de una lista de acceso.

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

Configure una lista de control de acceso ACL named BLOCK_HTTP on R1 with the following statements. a. Block HTTP and HTTPS traffic from reaching Server3.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
Denegamos el paso del tcp desde cualquier origen  hacia el host servidor3,
equivalente a www.
Bloquear  el trafico HTTP y HTTPS hacia el servidor3.
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

Aquí denegamos el paso tcp del servidor origen hacia el servidor3 a través del puerto 443.

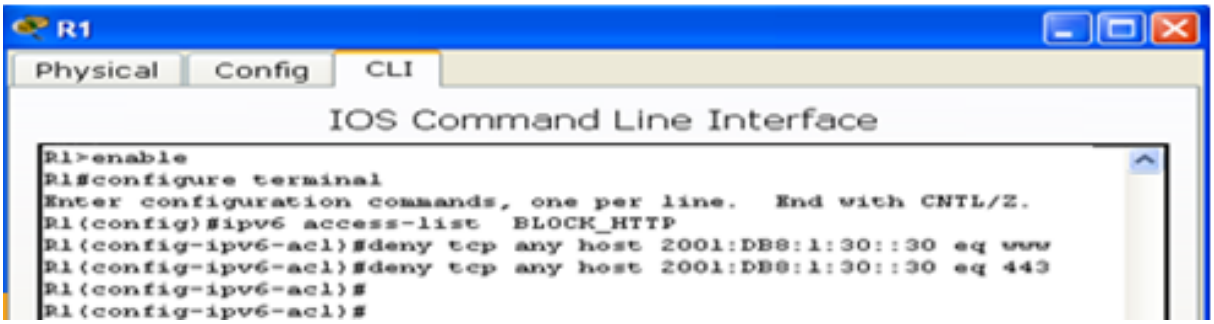


*Figure 104 Configuración ACL*

Allow all other IPv6 traffic to pass.

R1(config)# permit ipv6 any any

Se permite todo el tráfico ipv6 en la red

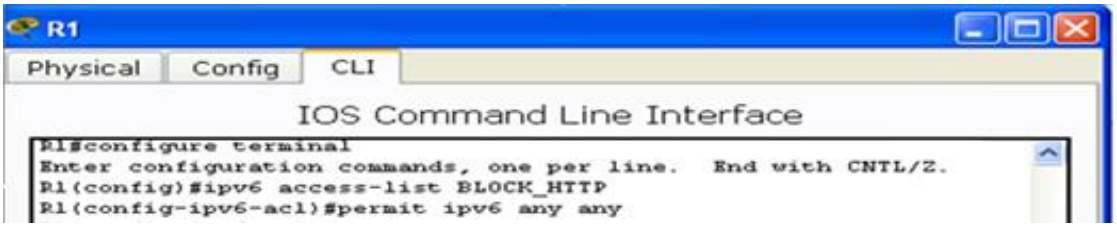


*Figure 105 Permiso todo tipode tráfico*

## Paso 2: Apply the ACL to the correct interface. (Aplicar las ACL correctamente)

Aplique la lista de acceso a la interface más cercana del origen del tráfico para que pueda ser bloqueado.
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
```


*Figure 106 Aplicar ACL*

## Paso 3: Verify the ACL implementation.

Verify the ACL is operating as intended by conducting the following tests:
Verifique la implementación de las líneas de control de acceso ACL
Open the **web browser** of **PC1** to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.

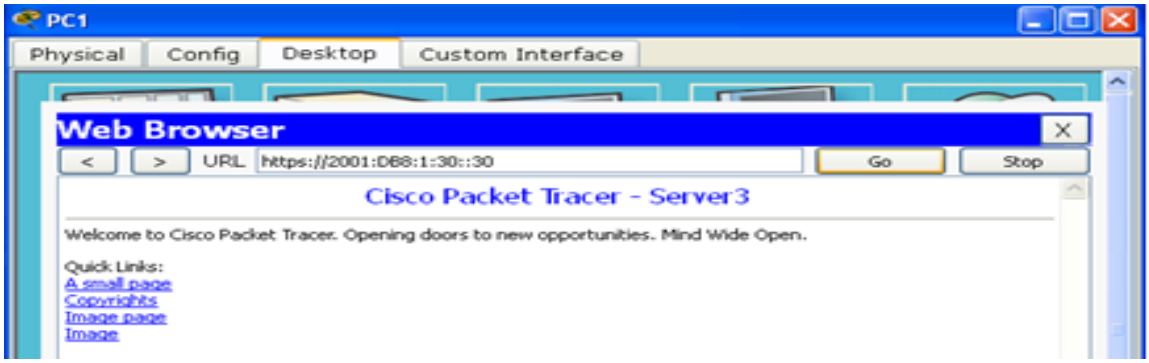


*Figure 107 web browser desde Pc1*

Es satisfactorio.

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

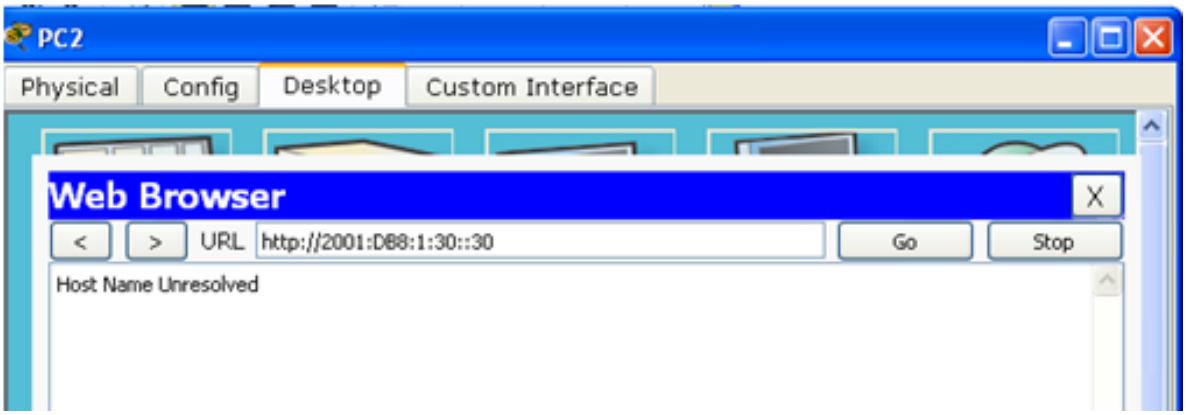


*Figure 108 Web browser desde Pc2*

El sitio está bloqueado

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

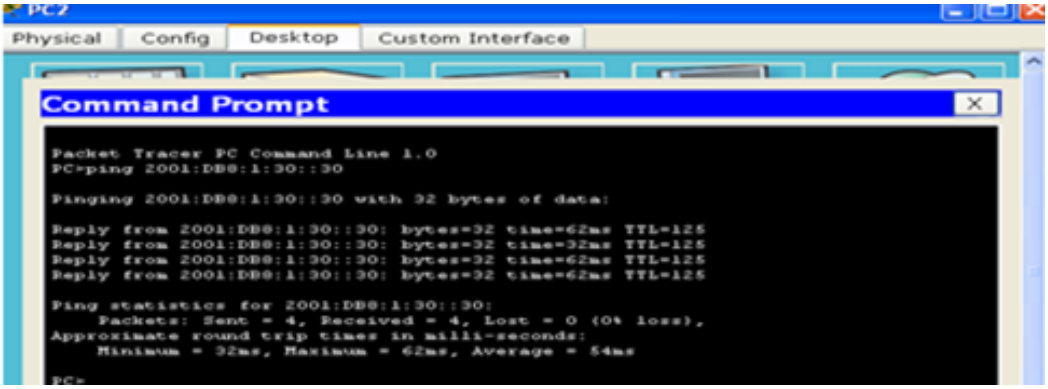


*Figure 109 Ping desde Pc2*

Es correcto. La comunicación es satisfactoria.

## Parte 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.

Configure, aplique y verifique una ACL un segunda IPv6 ACL

Los registros ahora expresan que nuestro servidor está recibiendo ping de muchas

direcciones IPv6 en un ataque denegación de servicio distribuido. Se debe filtrar las solicitudes ICMP en su servidor.

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

Crear una lista de acceso BLOCK_ICMP en su servidor.

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

**a.** Block all ICMP traffic from any hosts to any destination.
Bloquear el trafico ICMP desde cualquier origen hacia cualquier destino.

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

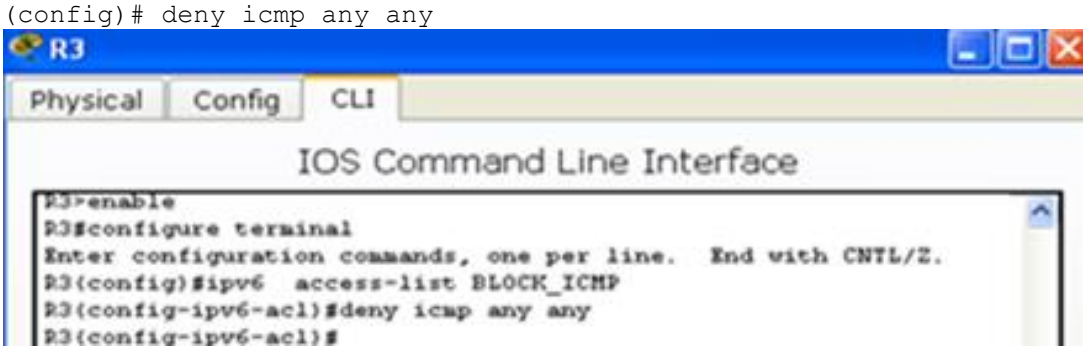


*Figure 110 Comando Block_ICMP*

**b.** Allow all other IPv6 traffic to pass.
Permitir todo el tráfico en IPv6 desde cualquier origen hacia cualquier destino.

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

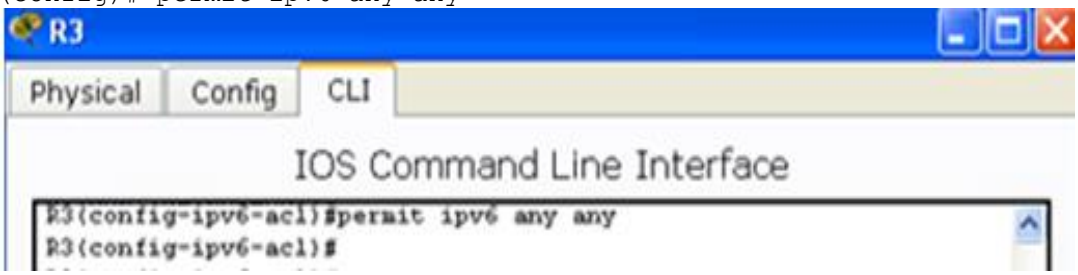


*Figure 111 Permite el tráfico ipv6*

**Paso 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
```

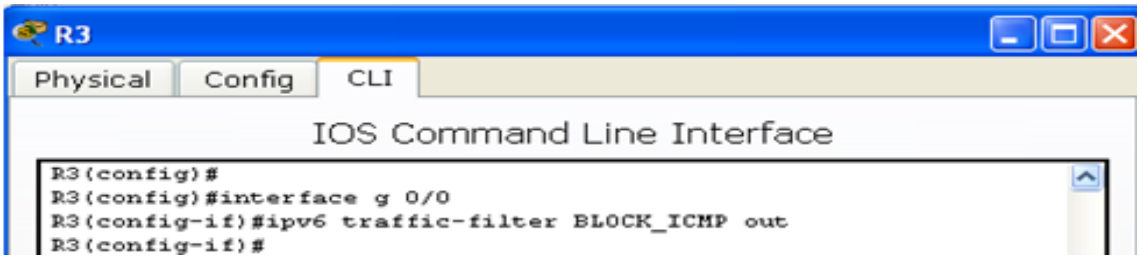


*Figure 112 Bloqueo de ICMP*

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

**a**. Ping from **PC2** to 2001:DB8:1:30::30.

The ping should fail.

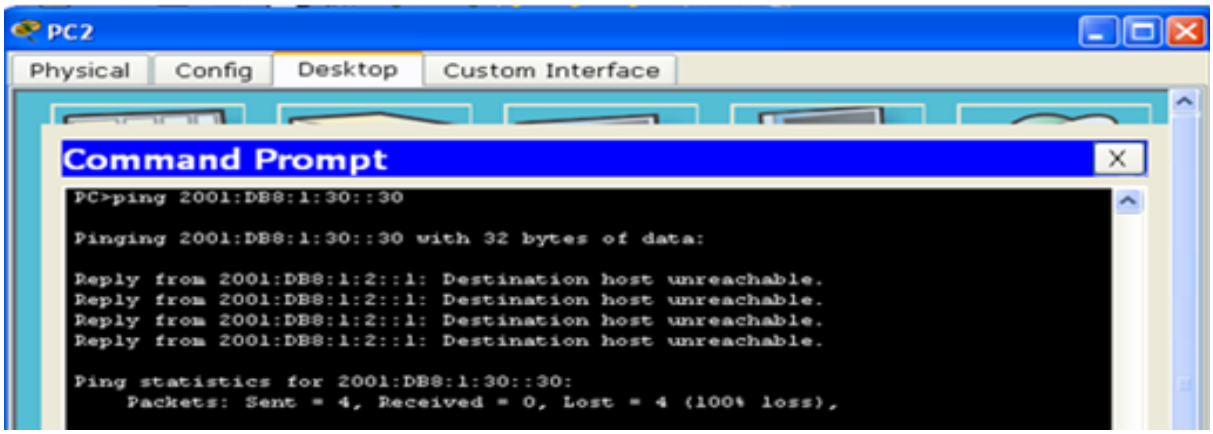


*Figure 113 Ping desde Pc2*

No reconoce la comunicación.

**c.** 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.


*Figure 114 Web browser de Pc1*

## Práctica 10.1.2.4 - Laboratorio: configuración de DHCPv4 básico en un router

### Topología

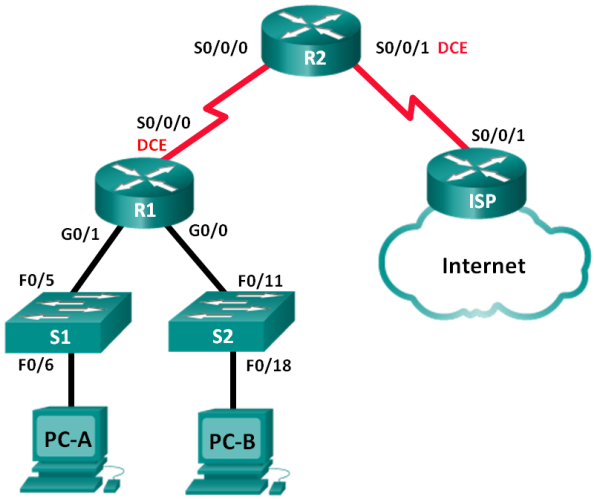


*Figure 115 Topología 10.1.2.4*

### 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 |

*Tabla 10 Configuración DHCPv4 básico en un router*

.

**Recursos necesarios**

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

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

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

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

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

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

**a.** Desactive la búsqueda DNS.

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

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

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

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

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

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

Physical | Config | CLI

IOS Command Line Interface

```
R1(config)#interface g0/0
R1(config-if)#ip add 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

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

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

R1(config-if)#interface g0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

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

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

R1(config-if)#int s0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#ip address 192.168.2.253 25.255.255.252
Bad mask 0x19FFFFFC for address 192.168.2.253
R1(config-if)#no shutdown

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

*Figure 116 Configuración parámetros básicos en R1*

Physical | Config | CLI

IOS Command Line Interface

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int s0/0/0
R2(config-if)#ip address 192.168.2.254 255.255.255.252
R2(config-if)#no shutdown

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

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

R2(config-if)#int s0/0/1
R2(config-if)#clock rate 128
                         ^
% Invalid input detected at '^' marker.

R2(config-if)#clock rate 128
                         ^
% Invalid input detected at '^' marker.

R2(config-if)#clock rate 128000
R2(config-if)#ip address 209.165.200.226
% Incomplete command.
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#no shutdown

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

*Figure 117 Configuración parámetros básicos en R2*

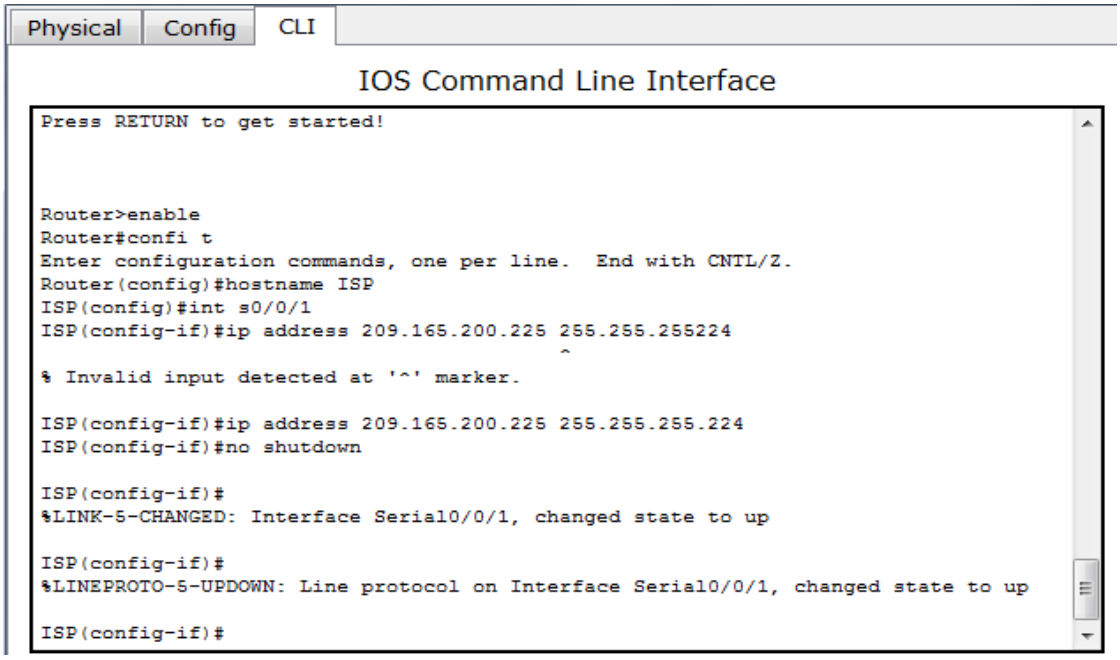


*Figure 118 Configuración parámetros básicos en R3*

**h.** Configure EIGRP for R1.

```
R1(config)# router eigrp 1
R1(config-router)# network 192.168.0.0 0.0.0.255
R1(config-router)# network 192.168.1.0 0.0.0.255
R1(config-router)# network 192.168.2.252 0.0.0.3
R1(config-router)# no auto-summary
```

```
R1(config-if)#int s0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#ip address 192.168.2.253 25.255.255.252
Bad mask 0x19FFFFFC for address 192.168.2.253
R1(config-if)#ip address 192.168.2.253 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 192.168.2.252 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#
```

*Figure 119 configuración EIGRP en R1*

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

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

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

*Figure 120 Configuración EIGRP y Ruta predeterminada ISP en R2*

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

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

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

```
ISP#enable
ISP#confit
Translating "confit"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

ISP#configure terminal
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)#
```

*Figure 121 Copia configuración en ejecución*

## 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.

```
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 = 2/6/20 ms

ISP#
```

*Figure 122 Conectividad entre routers*

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

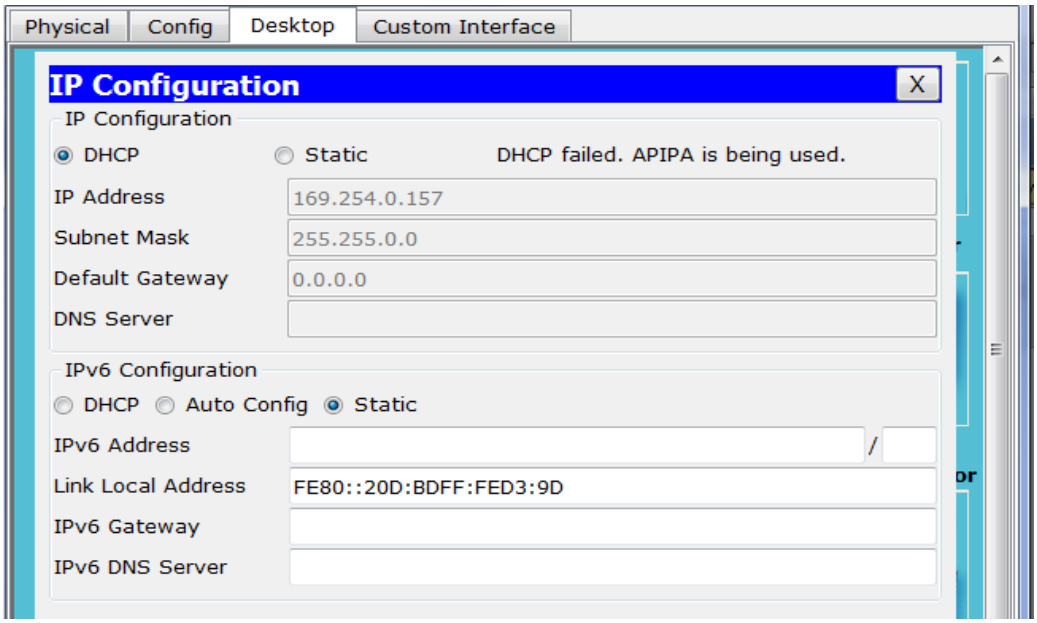


*Figure 123 Configuración DHCP en Pc-A*

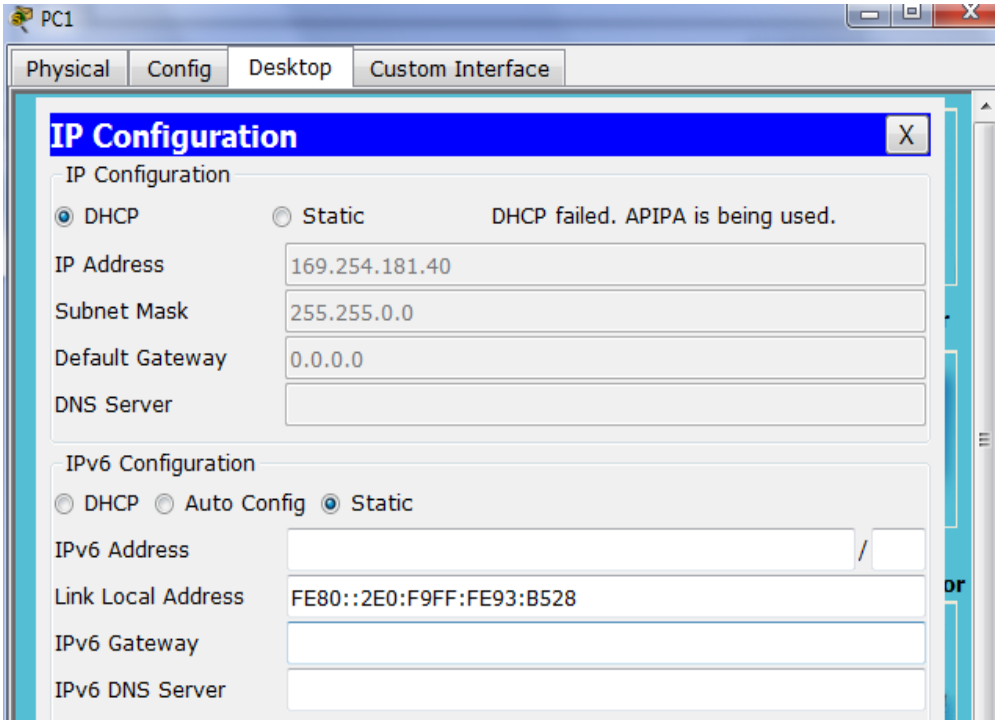


*Figure 124 Configuración DHCP en Pc-B*

## Parte 2: Configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

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

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

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

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

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

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

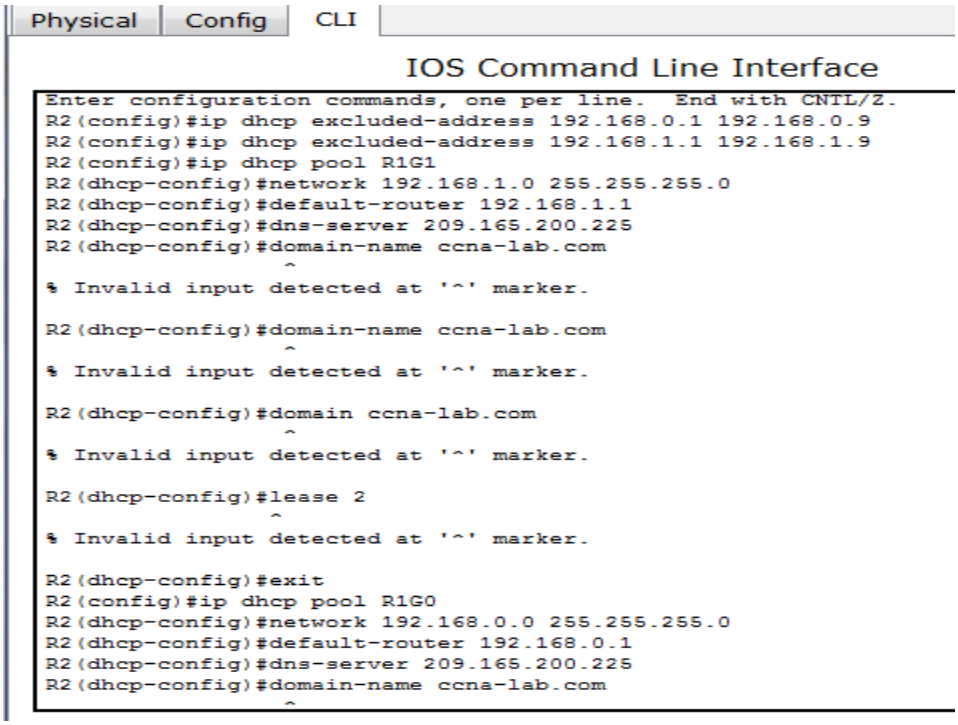


*Figure 125 Configuración parámetros servidor DHCPv4 en R2*

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 han recibido la dirección ip en r2 porque R1 se a configurado como agente relay de dhcp**

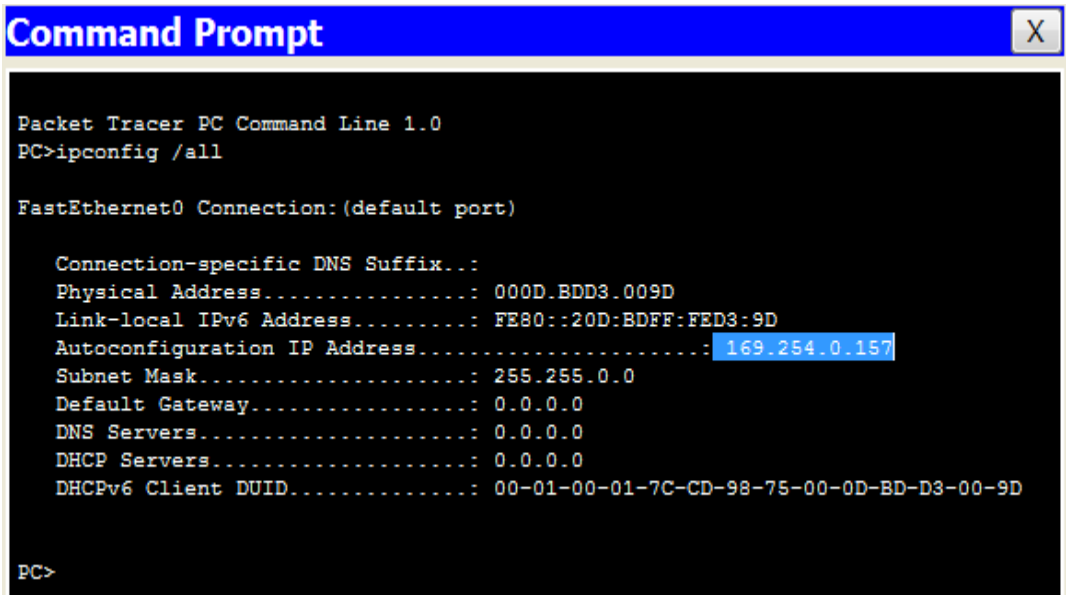


*Figure 126 Comando ipconfig/all*

## Paso 2: Configurar el R1 como agente de retransmisión DHCP.

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

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

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

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

**a.** 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.

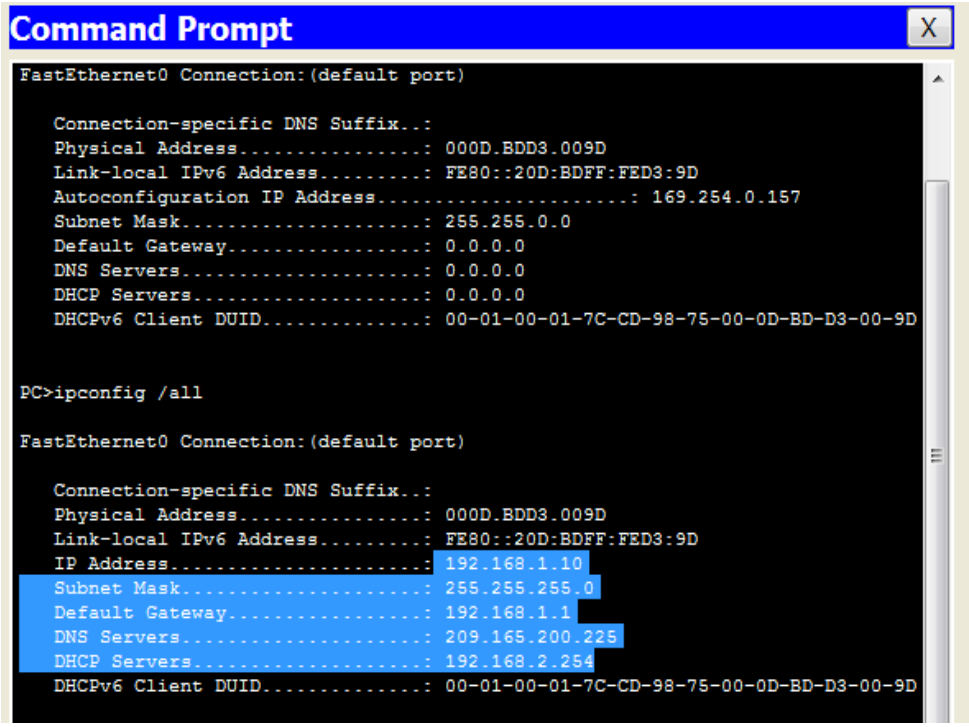


*Figure 127 Registrar configuración IP en Pc-A*

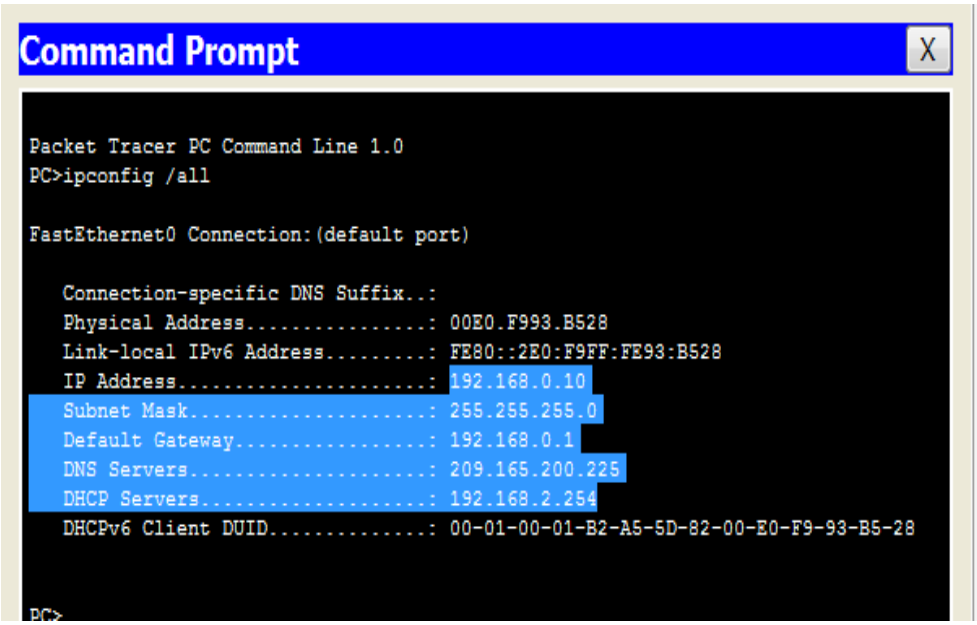


*Figure 128 Registrar configuración IP en Pc-B*

Según el pool de DHCP que se configuró en el R2, ¿cuáles son las primeras direcciones IP disponibles que la PC-A y la PC-B pueden arrendar?

**R=/ PC-B: 192.168.0.10 y en la PC-A: 192.168.1.10 verificar los servicios DHCP y los arrendamientos de direcciones en el R2.**

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

```
R2>ENABLE
R2#SHOW IP DHCP BINDING
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.10     000D.BDD3.009D           --                     Automatic
192.168.0.10     00E0.F993.B528           --                     Automatic
R2#
```

*Figure 129 Arrendamientos direcciones DHCP*

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

**Muestra las direcciones específicas de las computadoras añadidas a la red en el R2, introduzca el comando show ip dhcp server statistics para ver la actividad de mensajes y las estadísticas del pool de DHCP.**

## Práctica 10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6

### Topología

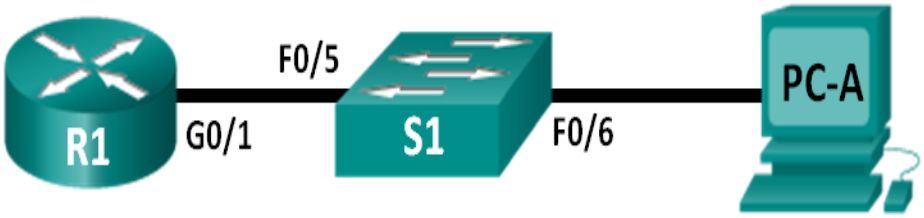


*Figure 130 Topología 10.2.3.5*

### 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 |

*Tabla 11 Configuring stateless and stateful DHCPv6*

### 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
```


*Figure 131 Asignación de plantilla*

Packet tracer no soporta los comandos anteriores.

**Recursos necesarios**

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

**Nota:** los servicios de cliente DHCPv6 están deshabilitados en Windows XP. Se recomienda usar un host con Windows 7 para esta práctica de laboratorio.

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

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

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


*Figure 132 Cableado*

### Paso 2: Inicializar y volver a cargar el router y el switch según sea necesario.

### Paso 3: Configurar R1

**f.** Desactive la búsqueda del DNS.

**g.** Configure el nombre del dispositivo.

**h.** Cifre las contraseñas de texto no cifrado.

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

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

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

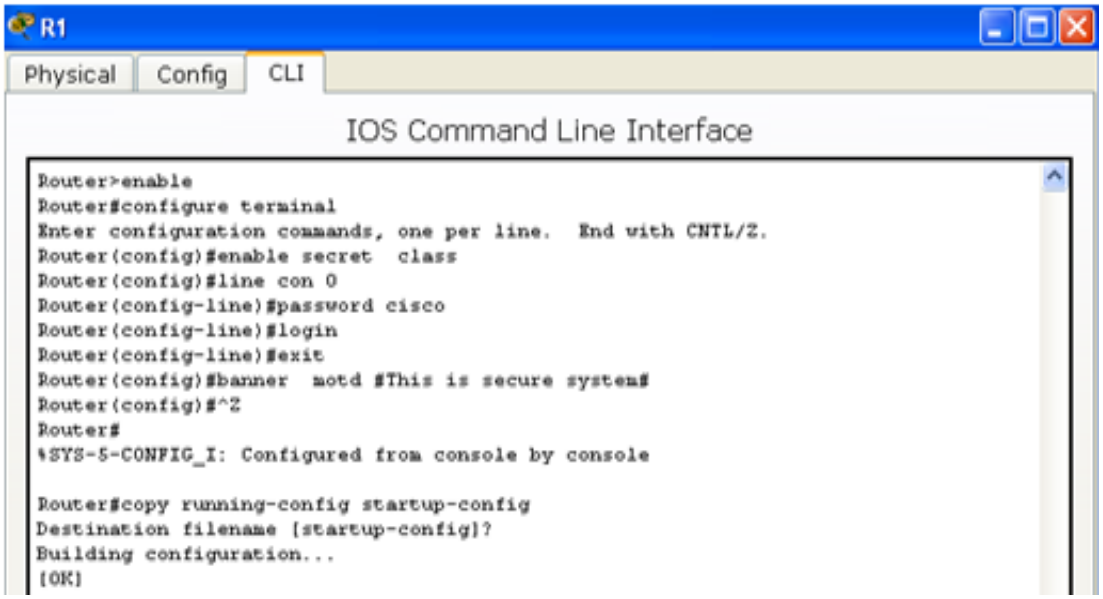


*Figure 133 Configuración R1*

**l.** Establezca el inicio de sesión de consola en modo sincrónico.

**m.** Guardar la configuración en ejecución en la configuración de inicio.

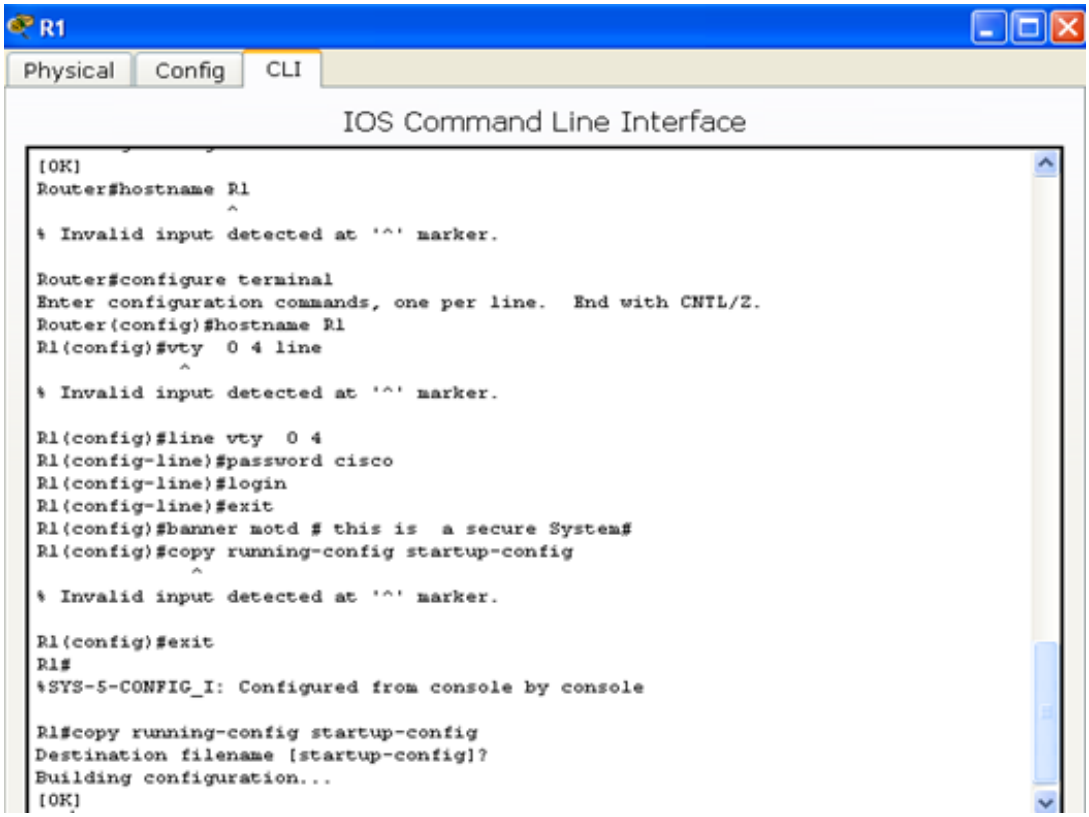


*Figure 134 Configuración R1.*

**Paso 4: configurar el S1.**

**a.** Desactive la búsqueda del DNS.

**b.** Configure el nombre del dispositivo.

**c.** Cifre las contraseñas de texto no cifrado.

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

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

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

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

**h.** Desactive administrativamente todas las interfaces inactivas.

**i.** Guarde la configuración en ejecución en la configuración de inicio.

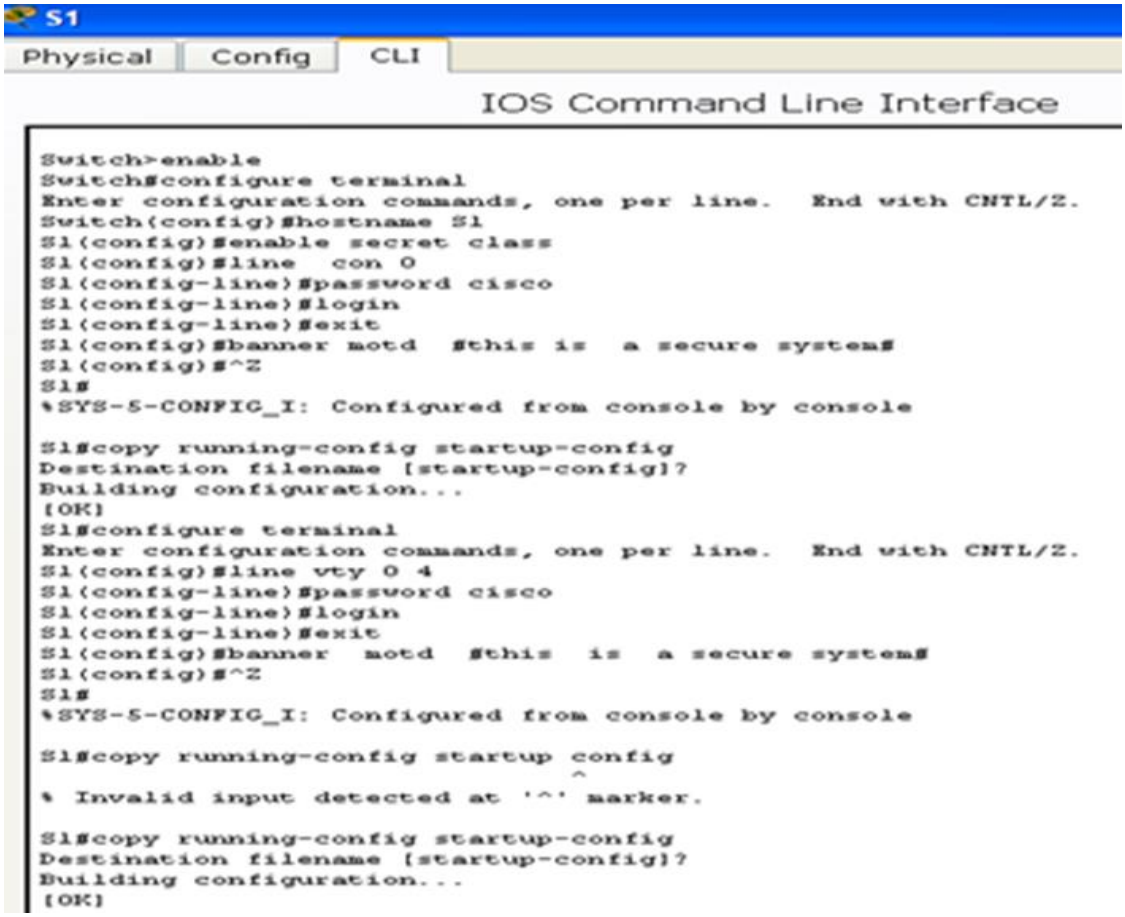


*Figure 135 Configuración Switch 1*

## Parte 2: Configurar la red para SLAAC

Configuración automática sin estado para SLAAC. Autoconfiguración de direcciones sin estado.

### Paso 1: Preparar la PC-A.

**a.** verifique que se haya habilitado el protocolo IPv6 en la ventana Propiedades de conexión de área local. Si la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) no está marcada, haga clic para activarla.

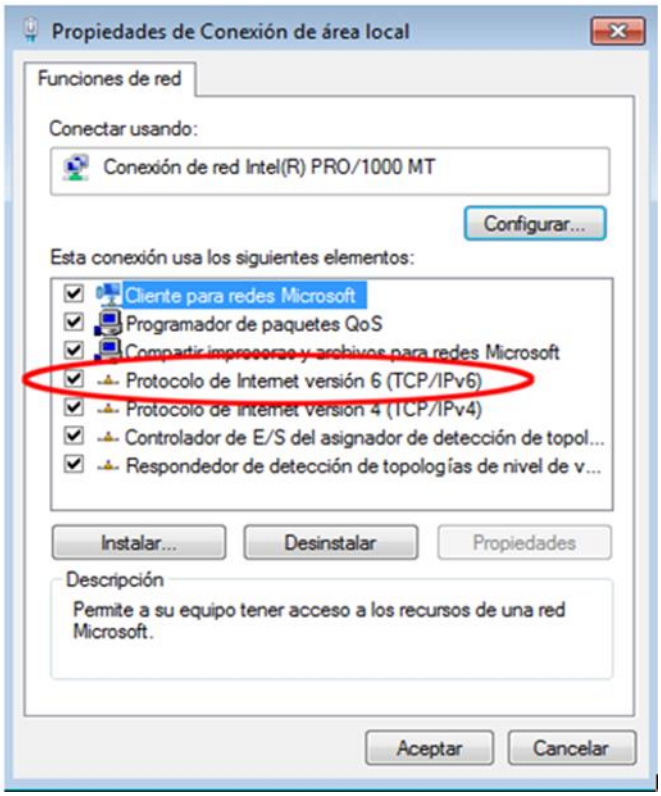


*Figure 136 Propiedades conexión área local*

**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.

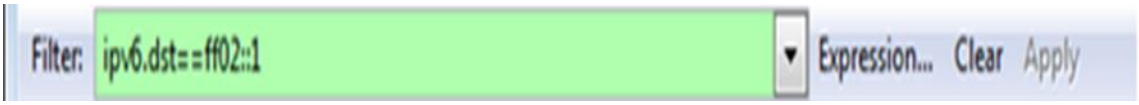


*Figure 137 Entrada Wireshark*

**Paso 2: Configurar R1**

**a. Habilite el routing de unidifusión IPv6.**

**b.** Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.

**c.** Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1

**d.** Active la interfaz G0/1.

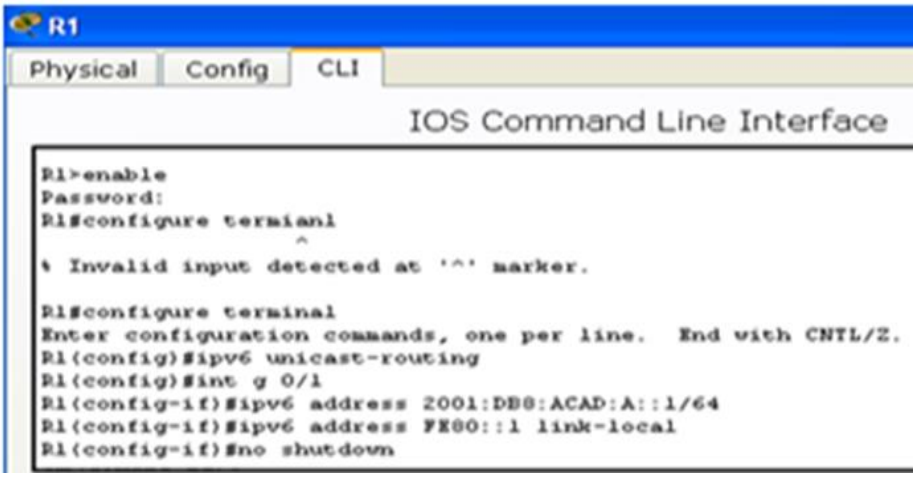


*Figure 138 Configuración R1*

**Paso 3: Verificar que el R1 forme parte del grupo de multidifusión de todos los routers.**

Use el comando **show ipv6 interface g0/1** para verificar que G0/1 forme parte del grupo de multidifusión de todos los routers (FF02::2). Los mensajes RA no se envían por G0/1 sin esa asignación de grupo.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
```

```
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

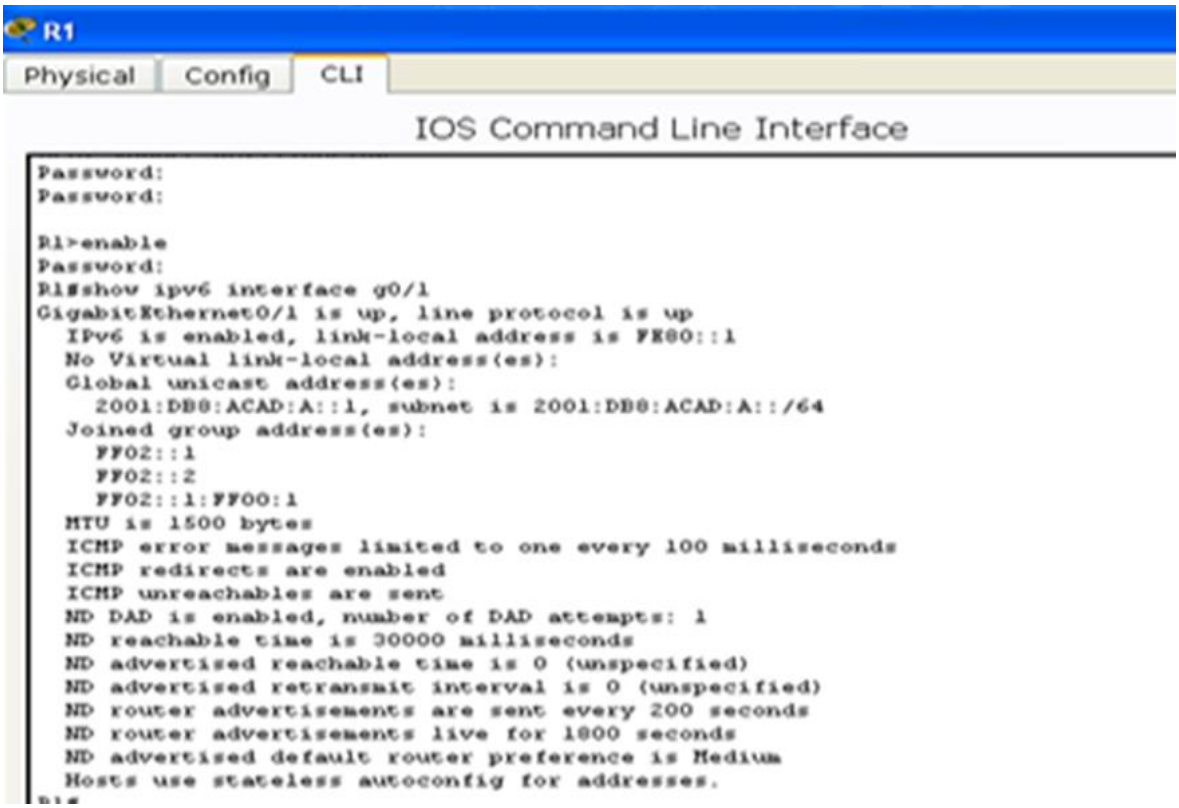


*Figure 139 Verificación de R1 en grupo de multidifusión*

## Paso 4: Configurar el S1.

Use el comando **ipv6 address autoconfig** en la VLAN 1 para obtener una dirección IPv6 a través de SLAAC.

```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
S1(config-if)# end
```

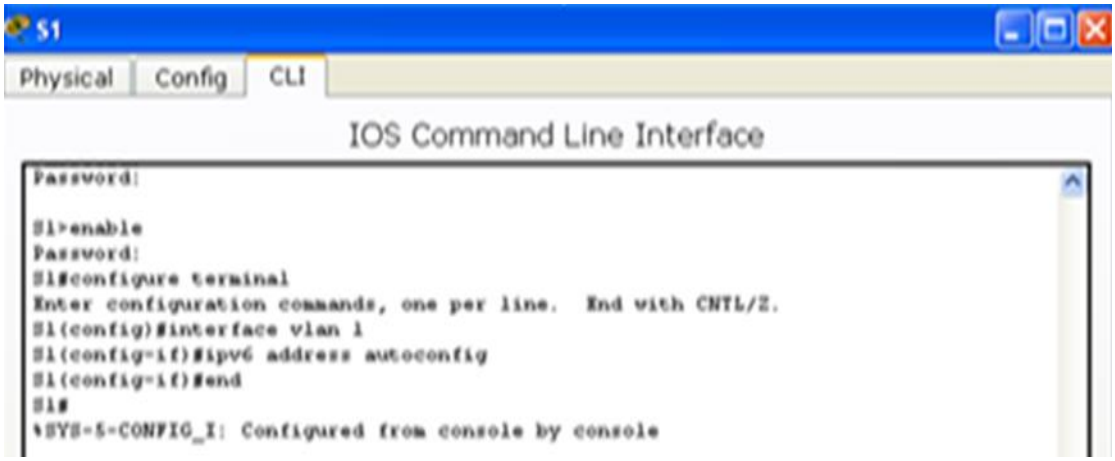


*Figure 140 Configuración Switch1*

**Paso 5: Verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.**

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

S1# **show ipv6 interface**

**(packet tracer no soporta esta característica o uso de este comando…)**

```
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
```

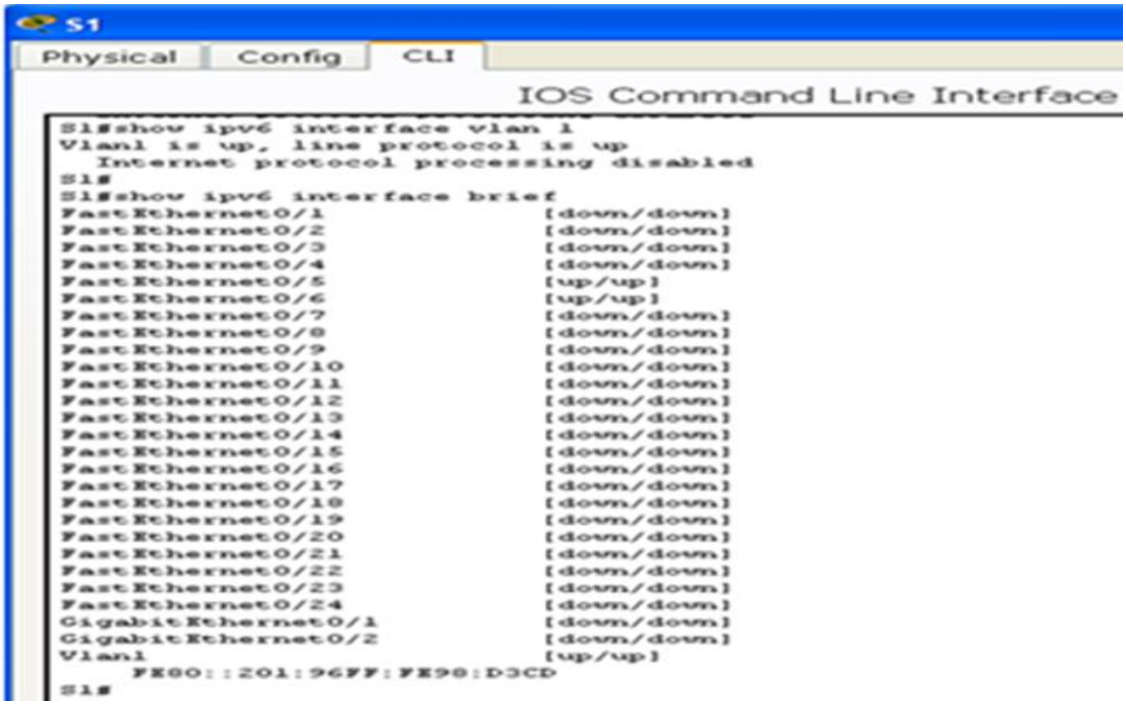


*Figure 141 VErificación de dirección unidifusión al switch 1*

**Paso 6: Verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.**

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

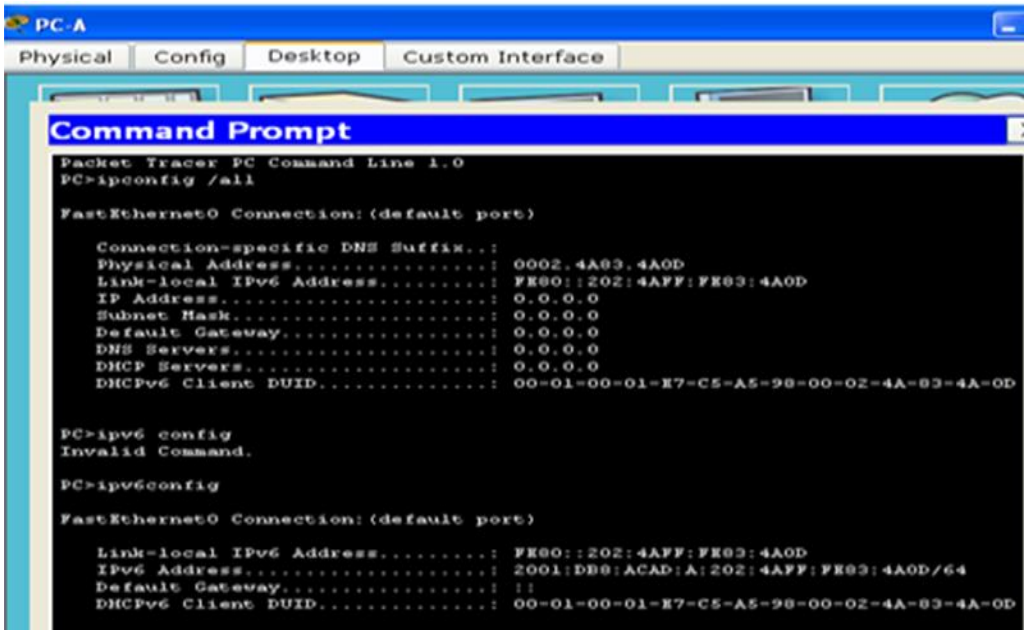


*Figure 142 Dirección ipv6*

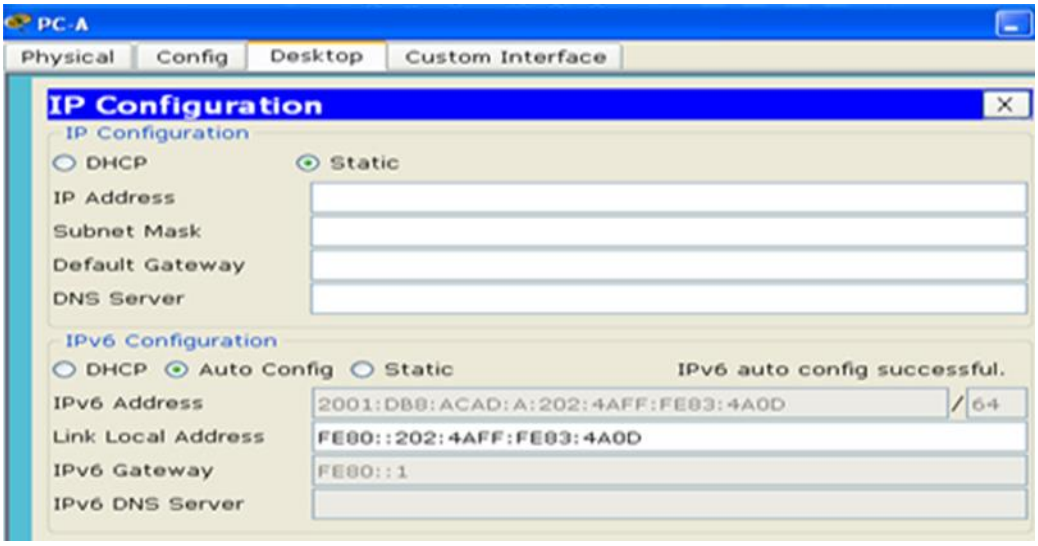


*Figure 143 Verificación dirección ipv6*

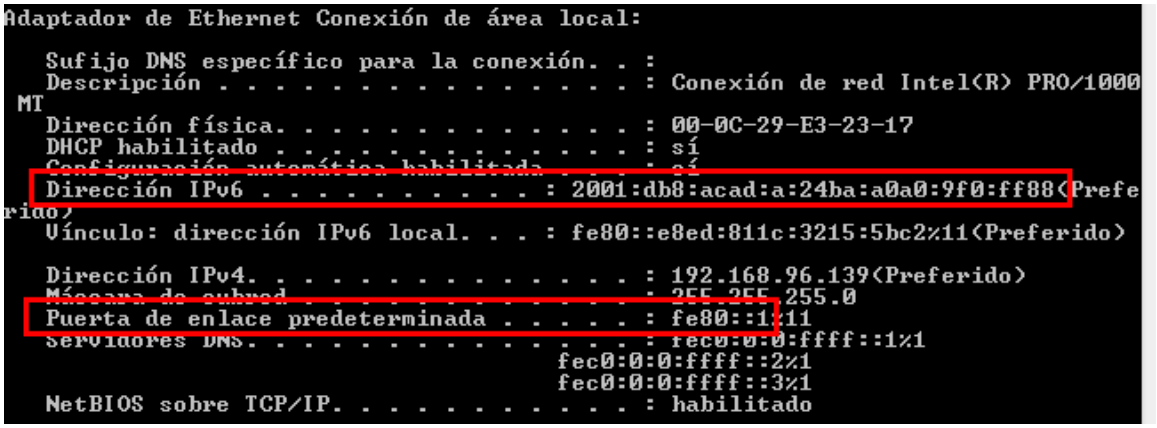


*Figure 144 Comprobando dirección ipv6*

**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.

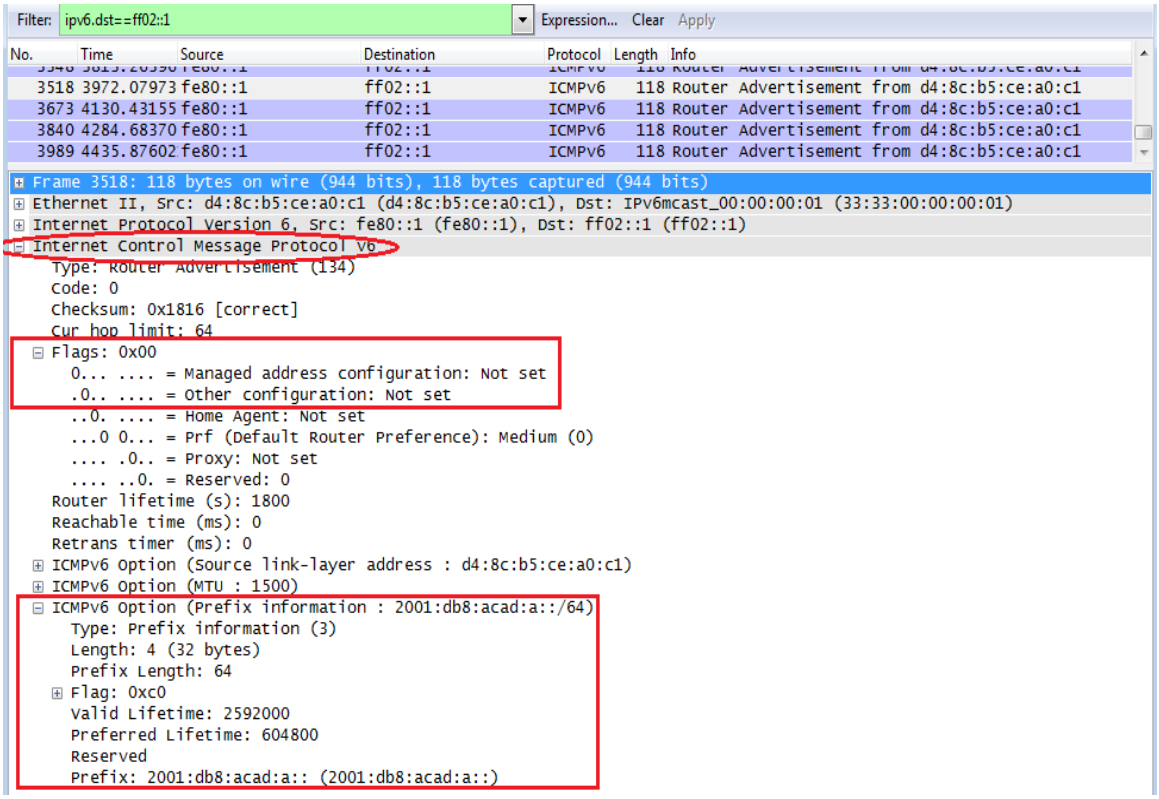


*Figure 145 Wireshark*

## Parte 3: Configurar la red para DHCPv6 sin estado

Configure la red para DHCP versión 6 sin estado.

### Paso 1: Configurar un servidor de DHCP IPv6 en el R1.

**a.** Cree un pool de DHCP IPv6.

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

**b.** Asigne un nombre de dominio al pool.

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

**c.** Asigne una dirección de servidor DNS.

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

**d.** Asigne el pool de DHCPv6 a la interfaz.

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

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

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


*Figure 146 Configuración del servidor DHCP ipv6 en R1*

**Paso 2: Verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.**

Use el comando **show ipv6 interface g0/1** para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando **show** verifica que se haya establecido other-config-flag.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:2
    FF02::1:FF00:1
    FF05::1:3
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
```

```
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
Hosts use DHCP to obtain other configuration.
```

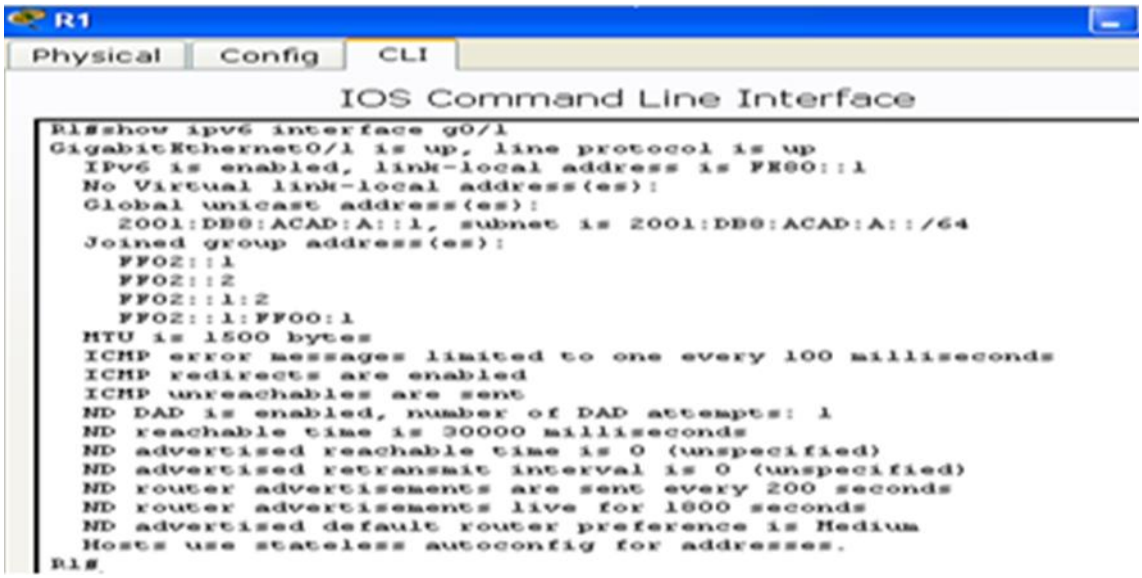


*Figure 147 Verificación de configuración DHCP*

### Paso 3: Ver los cambios realizados en la red en la PC-A.

Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente mediante SLAAC.

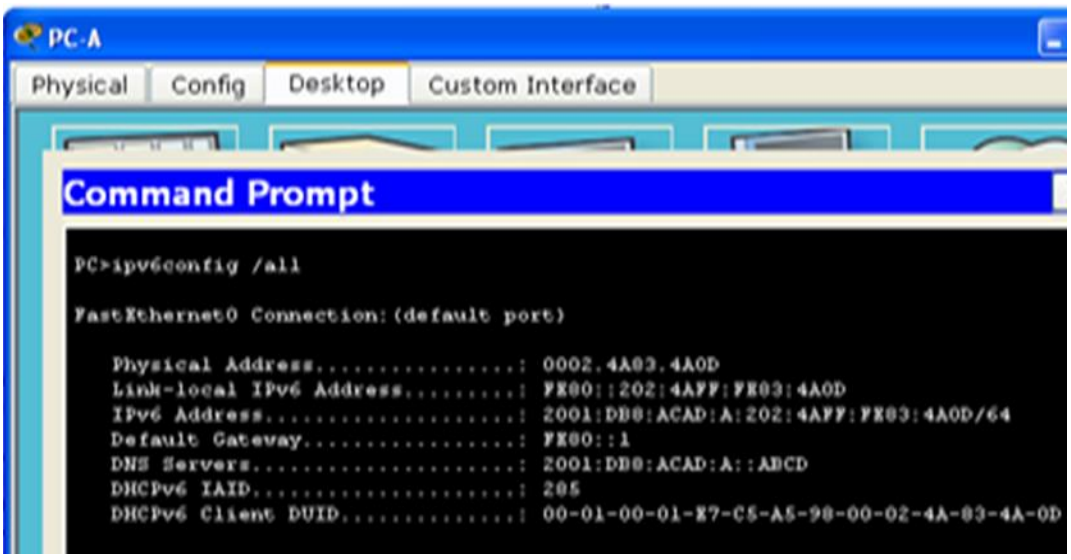


*Figure 148 Comando ipconfig/all*

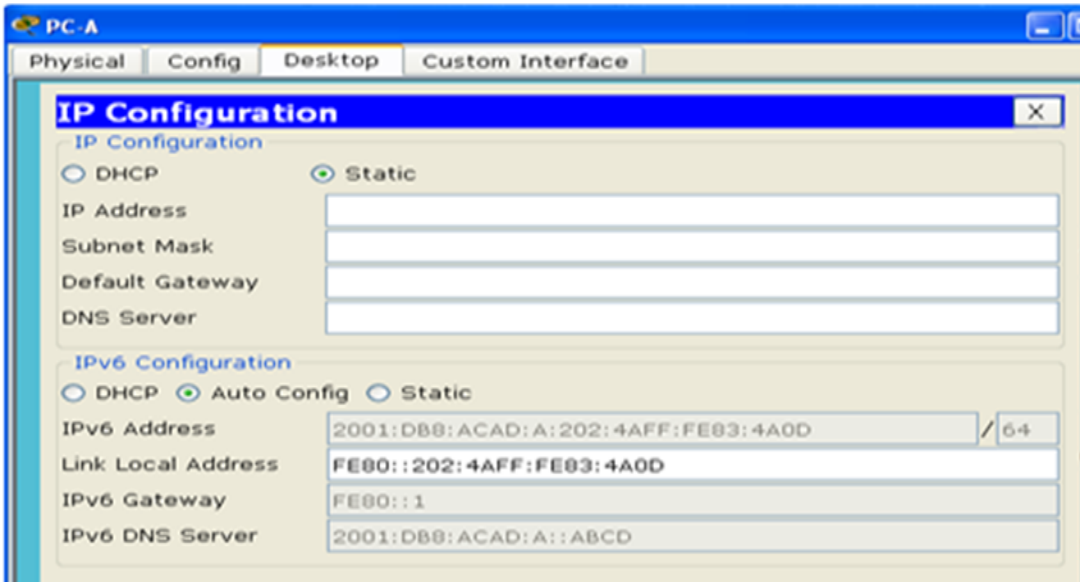


*Figure 149 Verificación en Pc-A*

```
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
```

*Figure 150 Comrobando datos*

## Paso 4: Ver los mensajes RA en Wireshark.

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

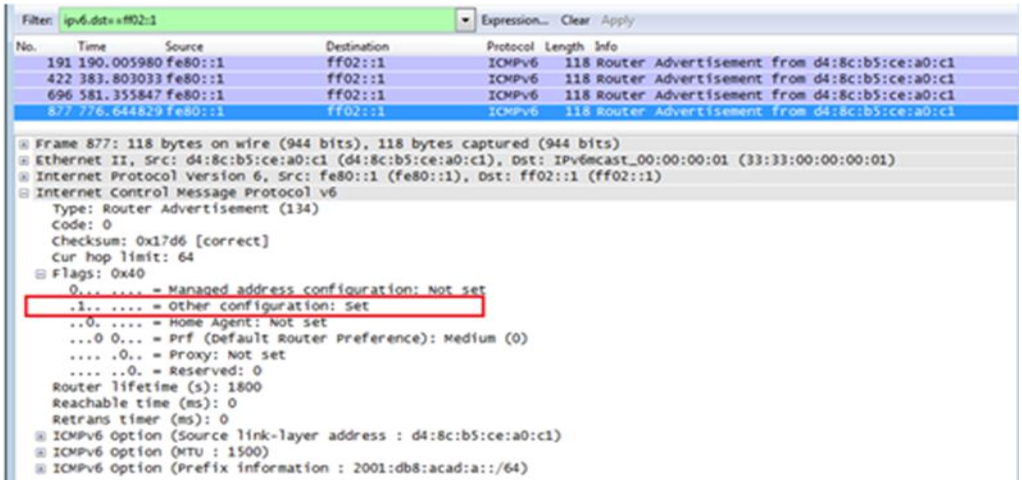


*Figure 151 Wireshark*

## Paso 5: Verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.

Use los comandos **show ipv6 dhcp binding** y **show ipv6 dhcp pool** para verificar que la PC-A no haya obtenido una dirección IPv6 del pool de DHCPv6.

```
R1# show ipv6 dhcp binding
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-statelessDHCPv6.com
Active clients:0
```


*Figure 152 Verificación de Pc-A*

**Paso 6: Restablecer la configuración de red IPv6 de la PC-A.**

**a.** Desactive la interfaz F0/6 del S1

**Nota:** la desactivación de la interfaz F0/6 evita que la PC-A reciba una nueva dirección IPv6 antes de que usted vuelva a configurar el R1 para DHCPv6 con estado en la parte 4.

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


*Figure 153 Restablecimiento de red ipv6*

**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.

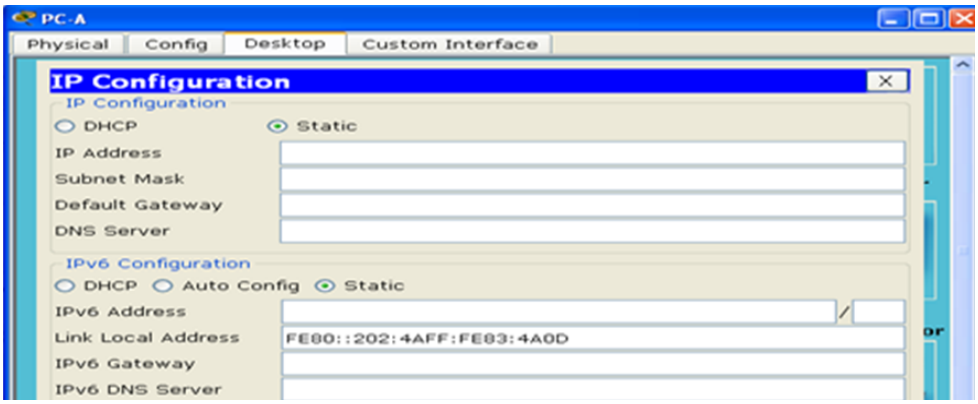


*Figure 154 Propiedades de conexión*

**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.

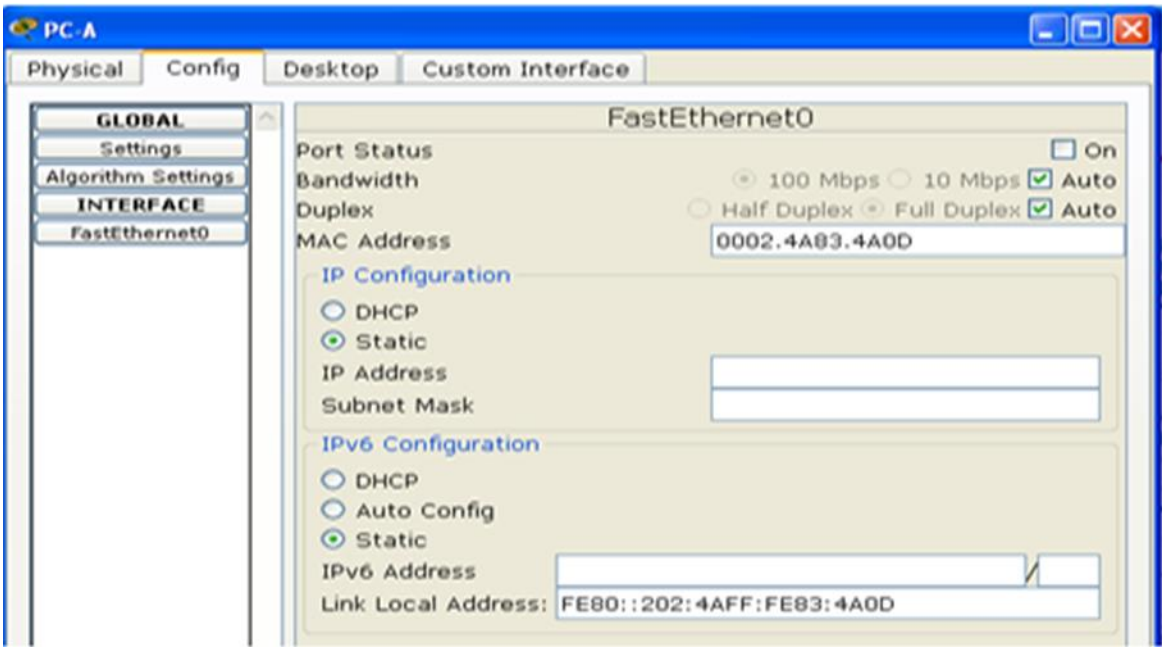


*Figure 155 Propiedades de conexión de área local*

## Parte 4: Configurar la red para DHCPv6 con estado

### Paso 1: Preparar la PC-A.

**a.** Inicie una captura del tráfico en la NIC con Wireshark.

**b.** Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes.

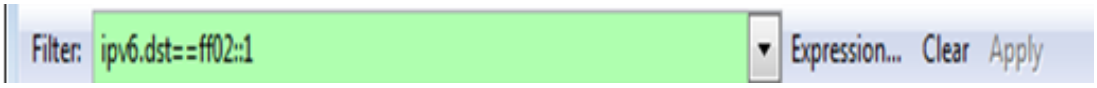


*Figure 156 Mensajes RA*

### Paso 2: Cambiar el pool de DHCPv6 en el R1.

**a.** Agregue el prefijo de red al pool.

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

```
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```

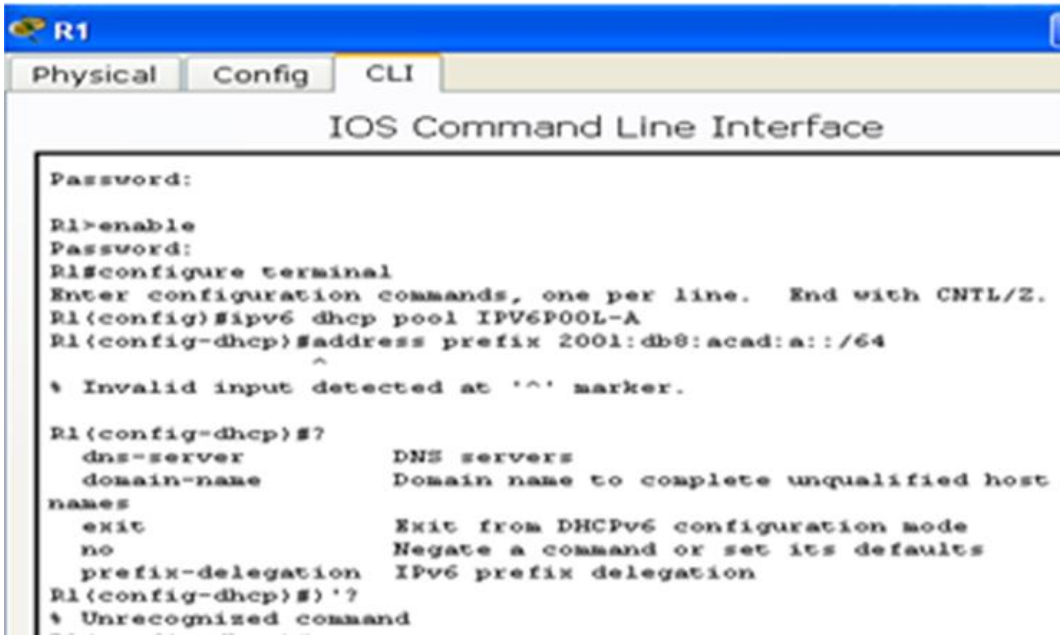


*Figure 157 Pool de DHCP en R1*

Packet tracert no soporta este commando.

**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
```


*Figure 158 Cambio de nombre de dominio*

**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
```


*Figure 159 Configuración del pool de DHCPv6*

**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)
```

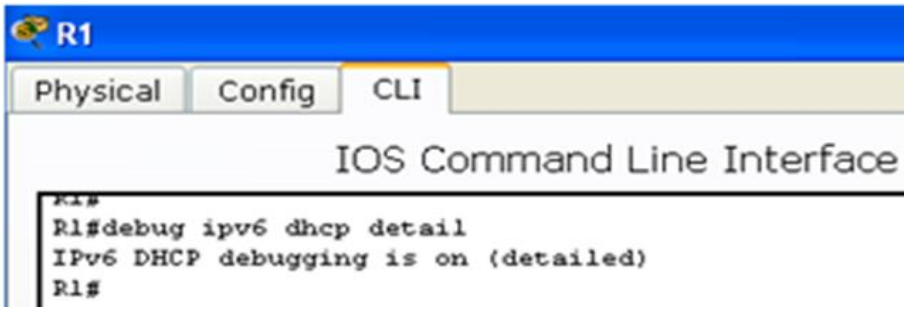


*Figure 160 Verificación de asignaciones de direcciones*

## Paso 3: Establecer el indicador en G0/1 para DHCPv6 con estado.

**Nota:** la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.

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

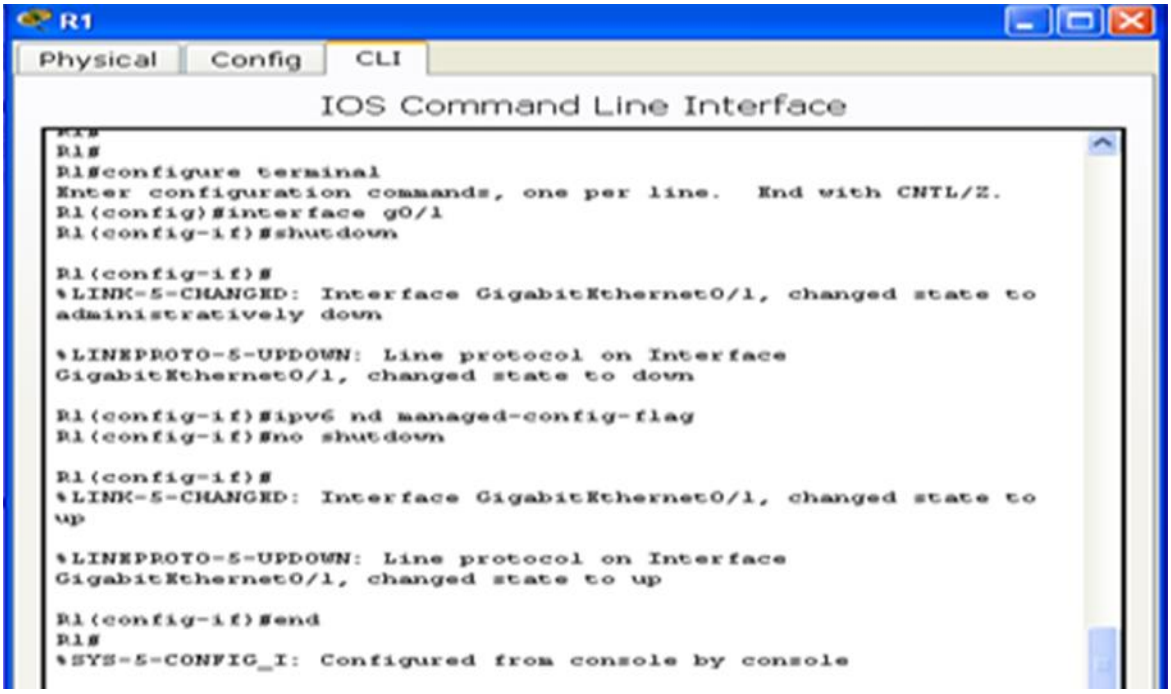


*Figure 161 Establece indicador*

## Paso 4: Habilitar la interfaz F0/6 en el S1.

Ahora que configuró el R1 para DHCPv6 con estado, puede volver a conectar la PC-A a la red activando la interfaz F0/6 en el S1.

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

S1(config-if)# end
```


*Figure 162 Habilitación interfaz F0/6*

**Paso 5: Verificar la configuración de DHCPv6 con estado en el R1.**

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

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

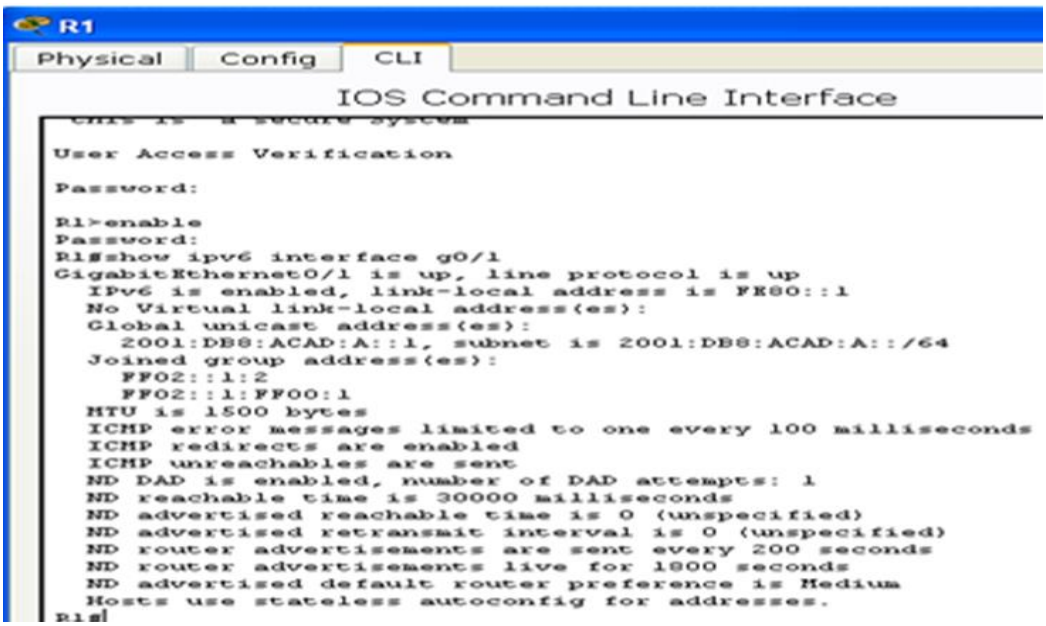


*Figure 163 Verificación de interfaz*

**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.


*Figure 164 Liberación de la dirección IPV6*

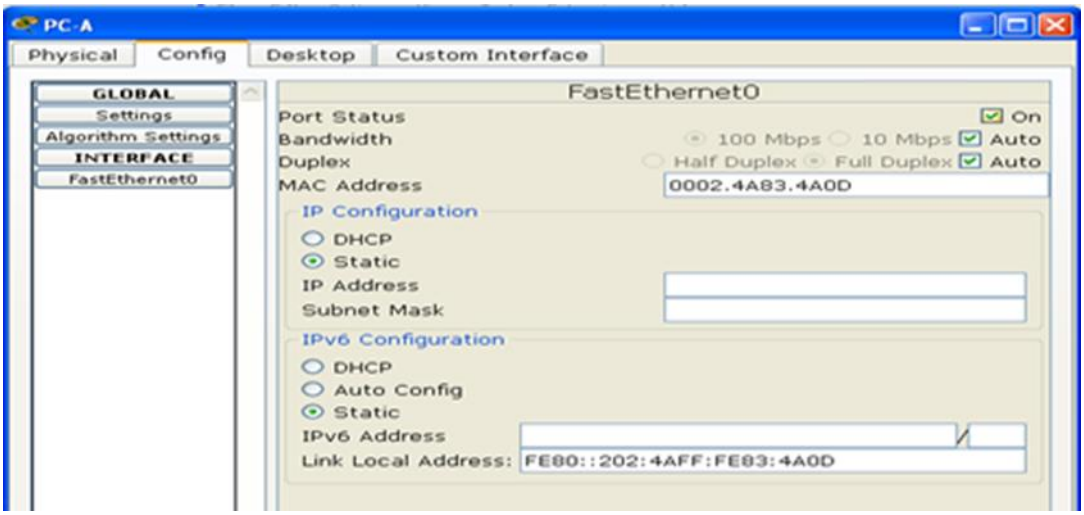


*Figure 165 Liberación de la dirección IPv6.*

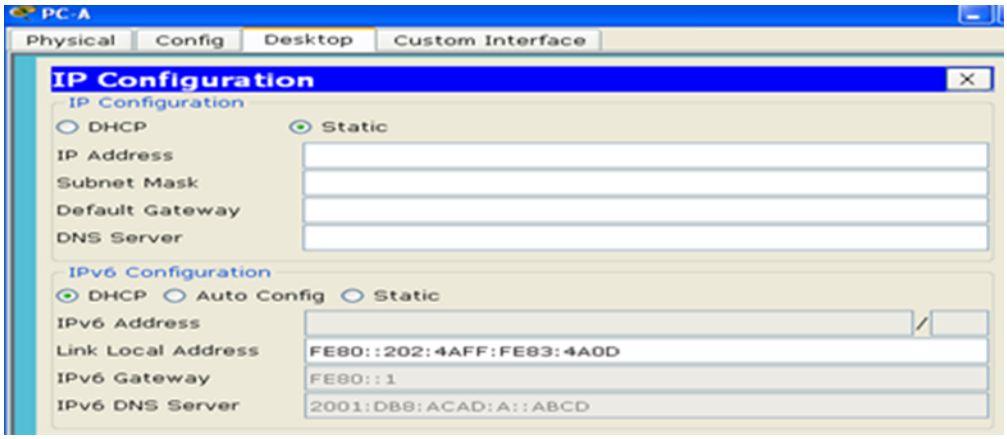


*Figure 166 Verificación de liberación de la dirección IPv6*

**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
```


*Figure 167 Verificación número de clientes activos*

**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)
```

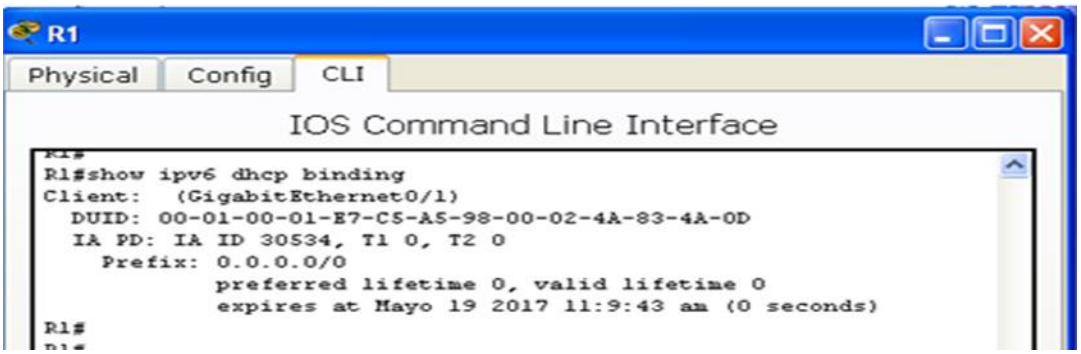


*Figure 168 Comparación de direcciones en R1*

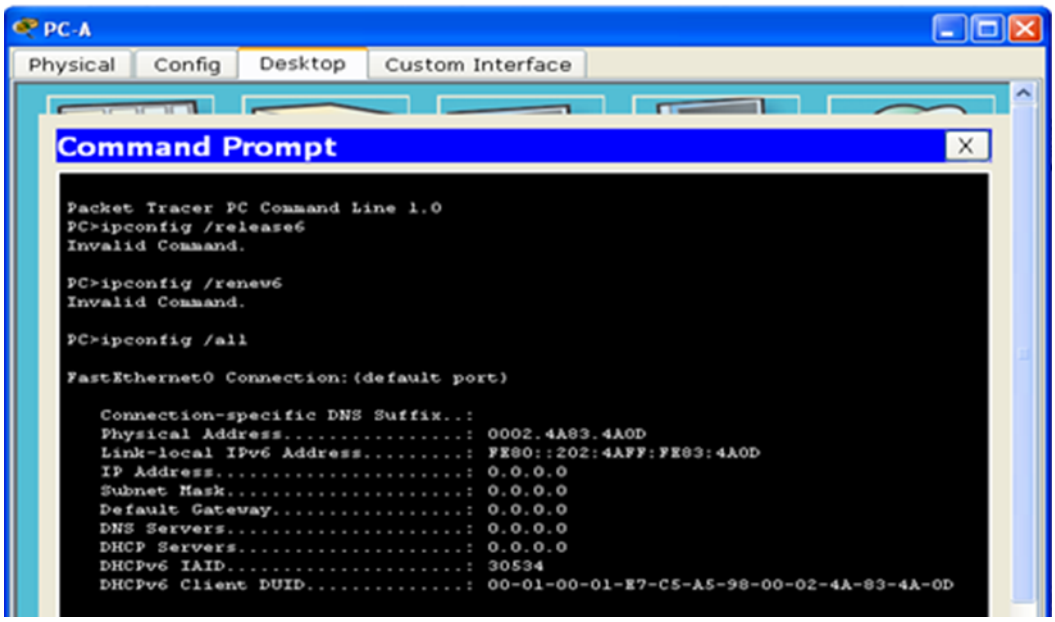


*Figure 169 Comandos para verificar direcciones*

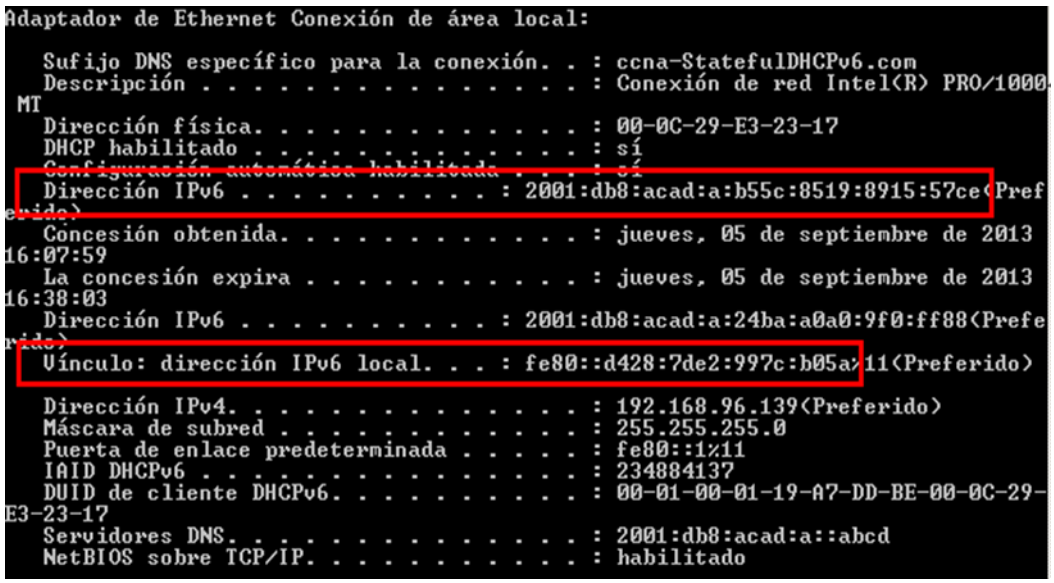


*Figure 170 Comparación de direcciones*

**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
```


*Figure 171 Detener depuración*

**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
```

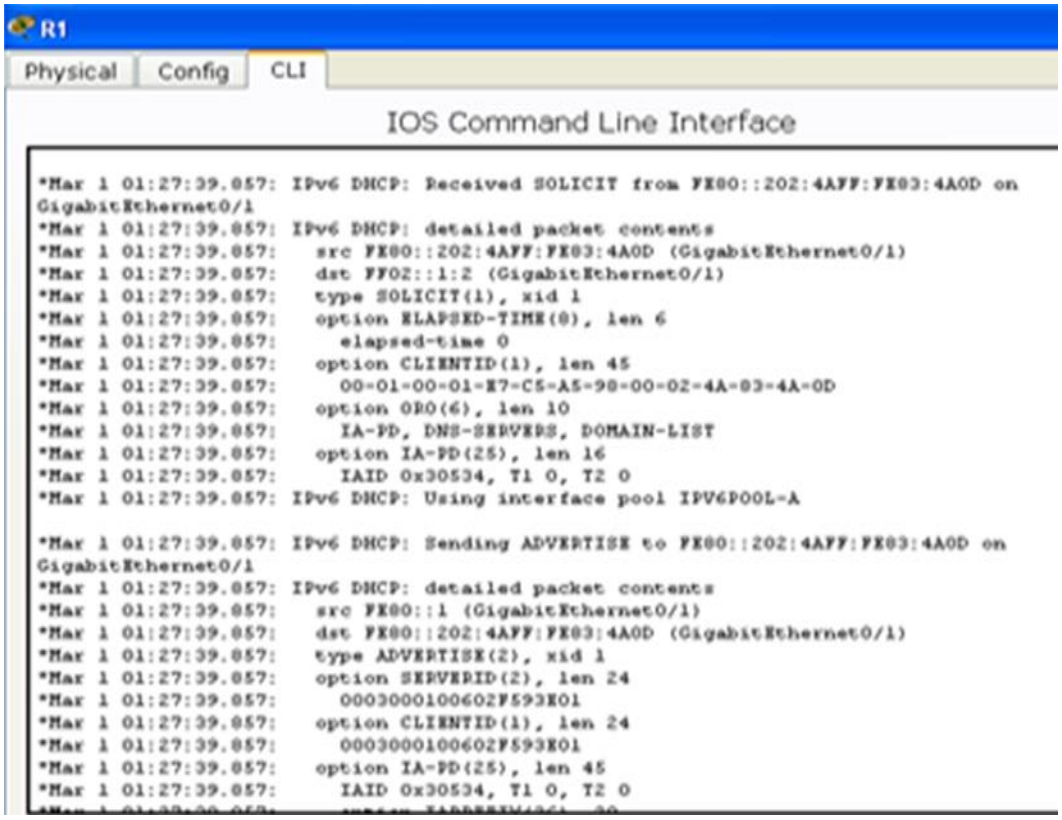


*Figure 172 Información de red*

**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
```

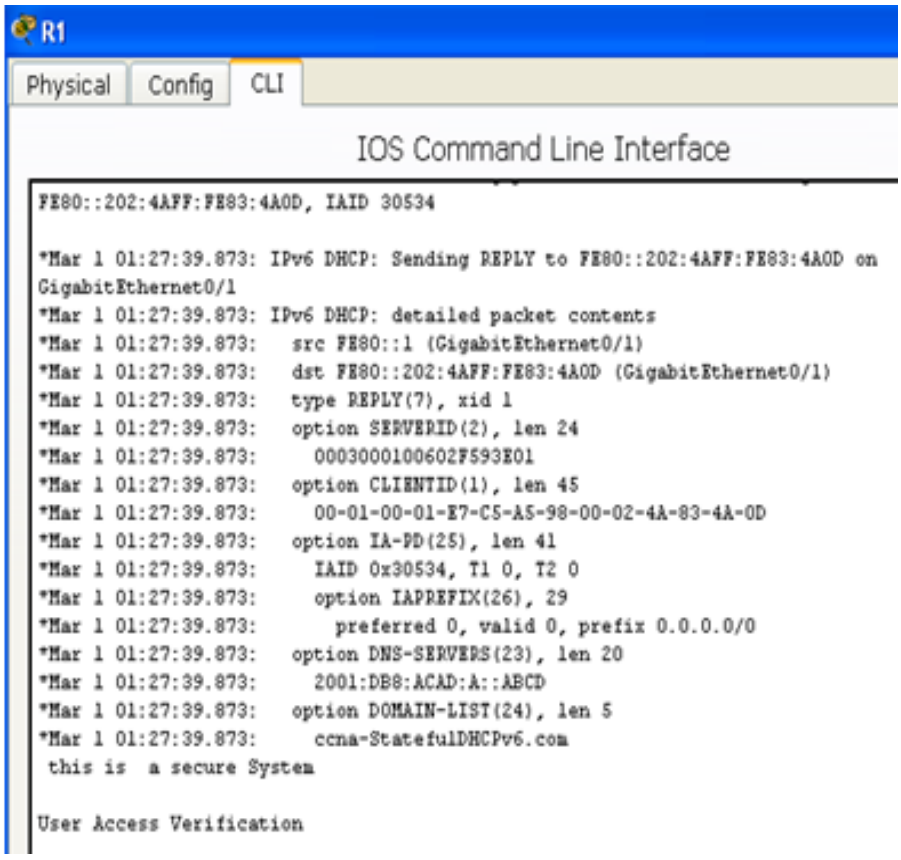


*Figure 173 Respuesta con información DHCP*

**Paso 6: Verificar DHCPv6 con estado en la PC-A.**

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

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

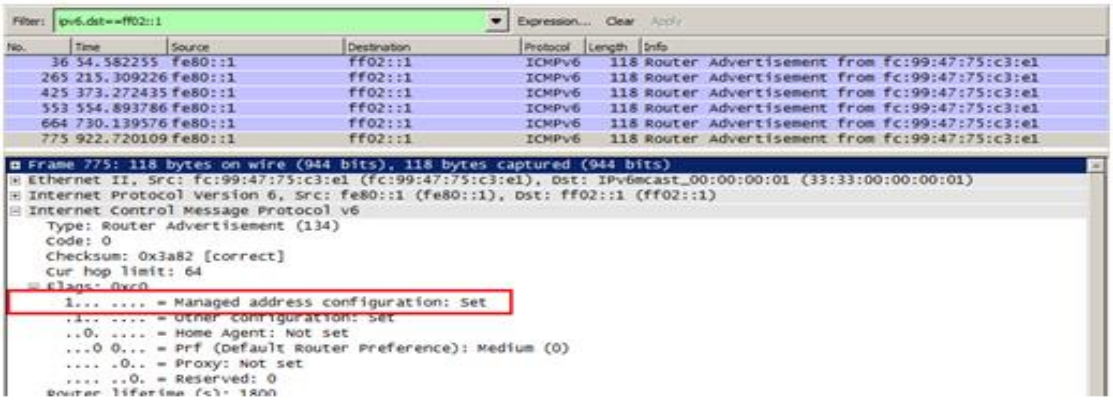


*Figure 174 Wireshark*

**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.

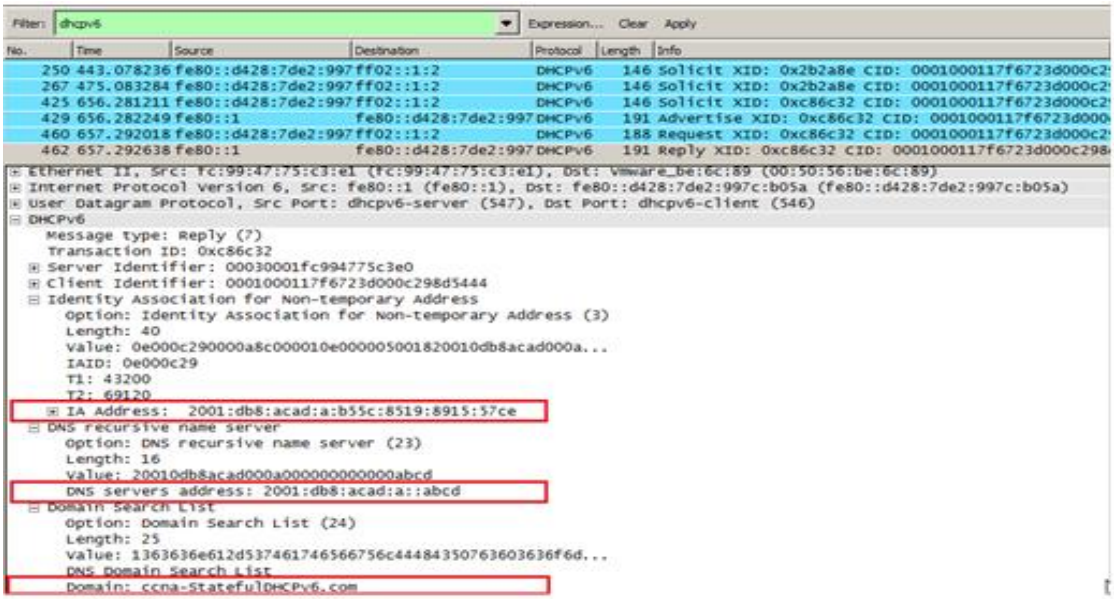


*Figure 175 Cambio del fitro en wireshark*

## Reflexión

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

   El método de direccionamiento DHCPv6 con estado porque este usa más recursos de memoria, el DHCPv6 con estado requiere que el router guarde dinámicamente el estado de información acerca de los clientes de HCPv6. El DHCPv6 sin estado para los clientesno utiliza el servidor DHCP para la obtención de las direcciones IPv6.

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

   De acuerdo a los estudios en CISCO, se recomienda la asignación dinámica de direcciones DHCPv6 sin estado cuando se desarrolla redes con IPv6 y sin un registro de red CISCO CNR.

## Tabla de resumen de interfaces del router

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

*Tabla 12 Resumen de interfaces del router*

## Práctica 11.2.2.6 - Laboratorio: Configuración de Nat Dinámica y Estática

### Topología

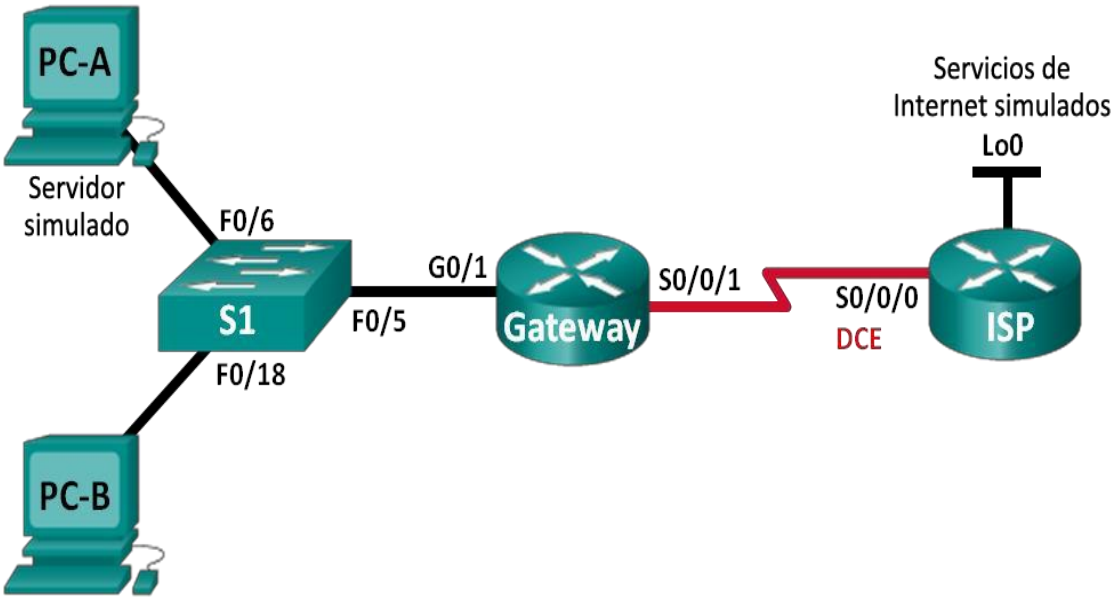


*Figure 176 Topología 11.2.2.6*

### 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 |

*Tabla 13 Configuración de NAT dinámica y estática*

**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**

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

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

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

**Recursos necesarios**

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

## Parte 1: Armar la red y verificar la conectividad

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

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

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

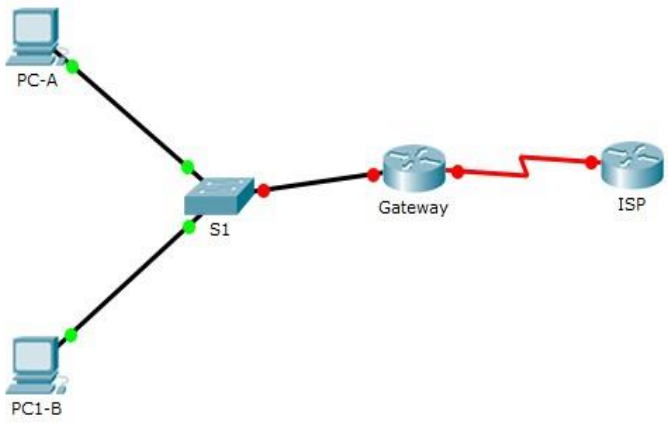


*Figure 177 Cableado*

**Paso 2: Configurar los equipos host.**

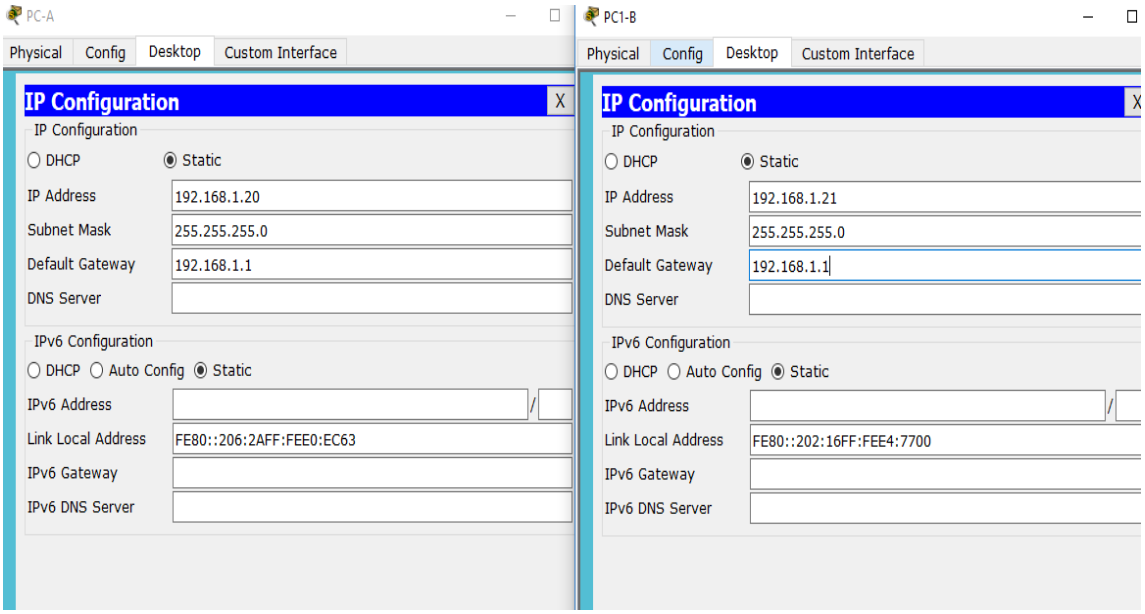


*Figure 178 Configuración de los equipos host en Pc-A y PC-B*

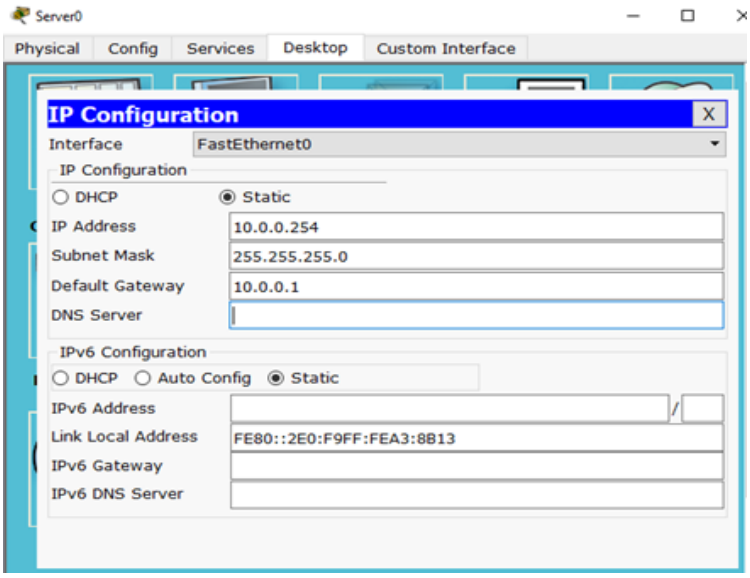


*Figure 179 Configuración de los equipos host en server0*

**Paso 3: Inicializar y volver a cargar los routers y los switches según sea necesario.**

**Paso 4: Configurar los parámetros básicos para cada router.**

**a.** Desactive la búsqueda del DNS.

**b.** Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

**c.** Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.

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

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

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

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

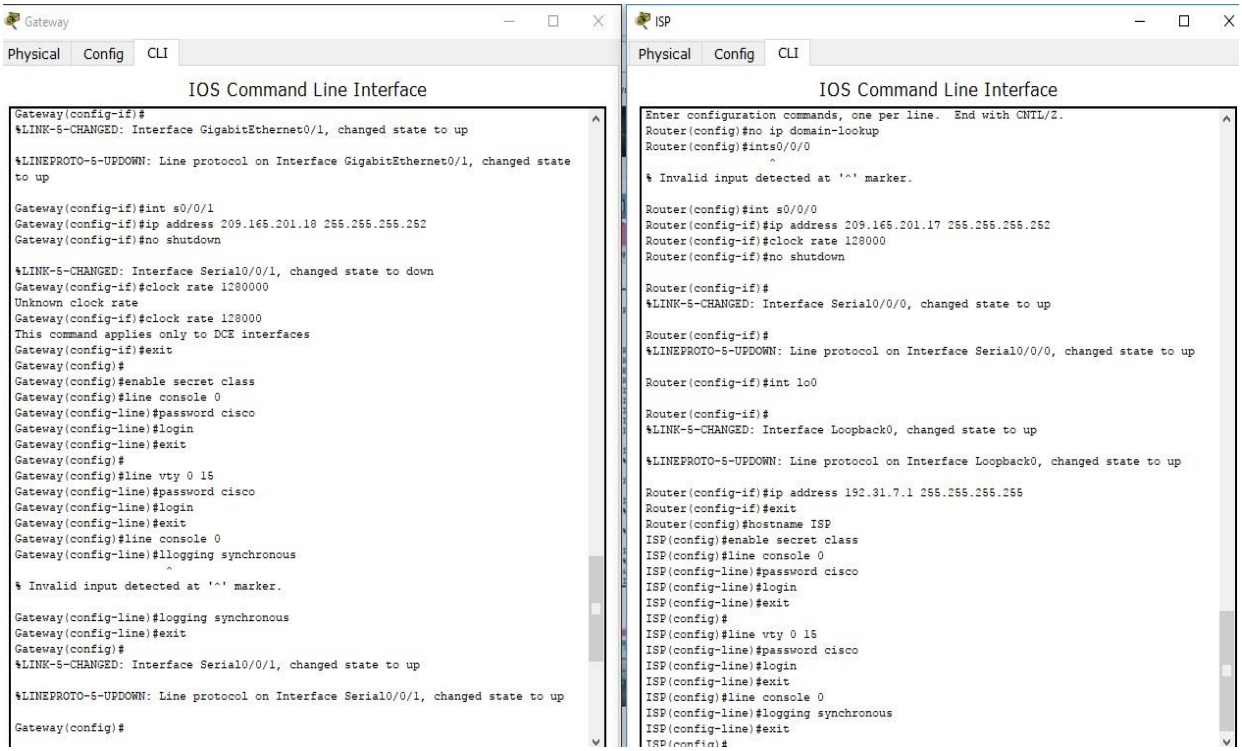


*Figure 180 Configuración de parámetros básicos Gateway y ISP*

## Paso 5: Crear un servidor web simulado en el ISP.

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

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

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

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

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

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

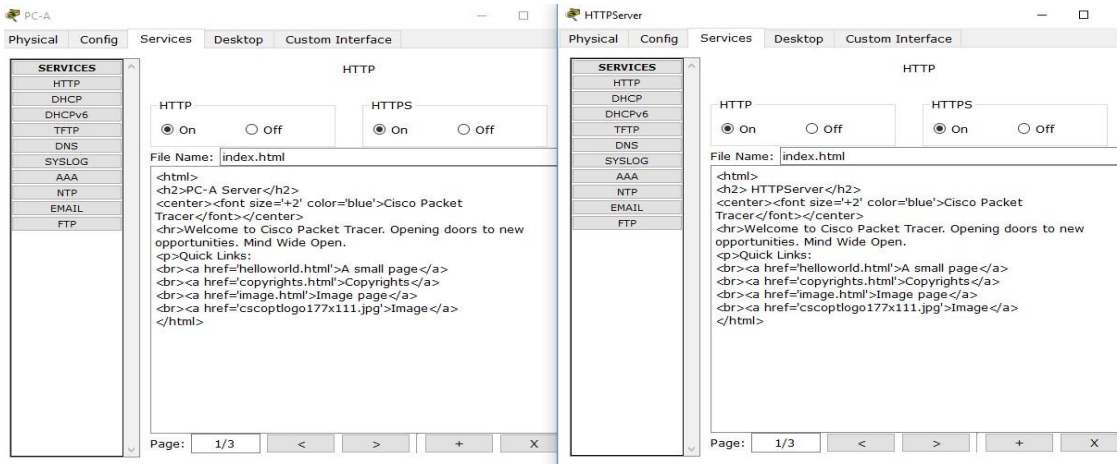


*Figure 181 Servidor web simulado*

## Paso 6: Configurar el routing estático.

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

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

**b.** Cree una ruta predeterminada del router Gateway al router ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

## Paso 7: Guardar la configuración en ejecución en la configuración de inicio.

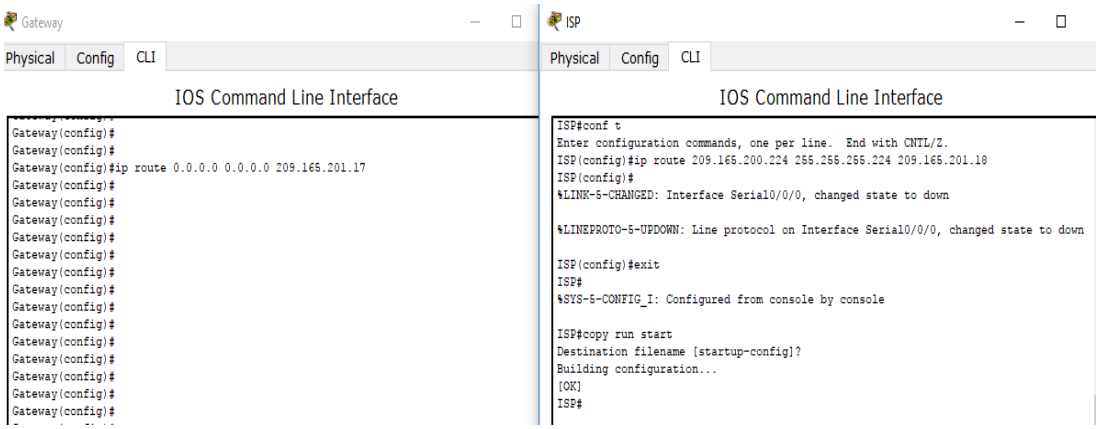


*Figure 182 Configuración guardada*

## Paso 8: Verificar la conectividad de la red

**a.** Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

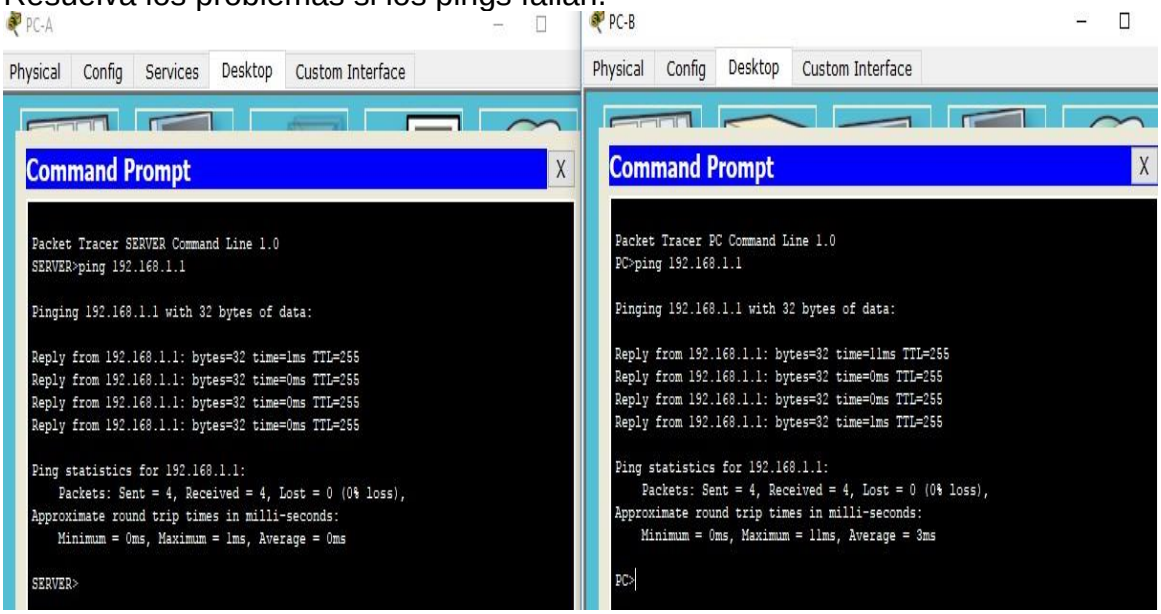


*Figure 183 Verificación conectividad de la red*

**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.

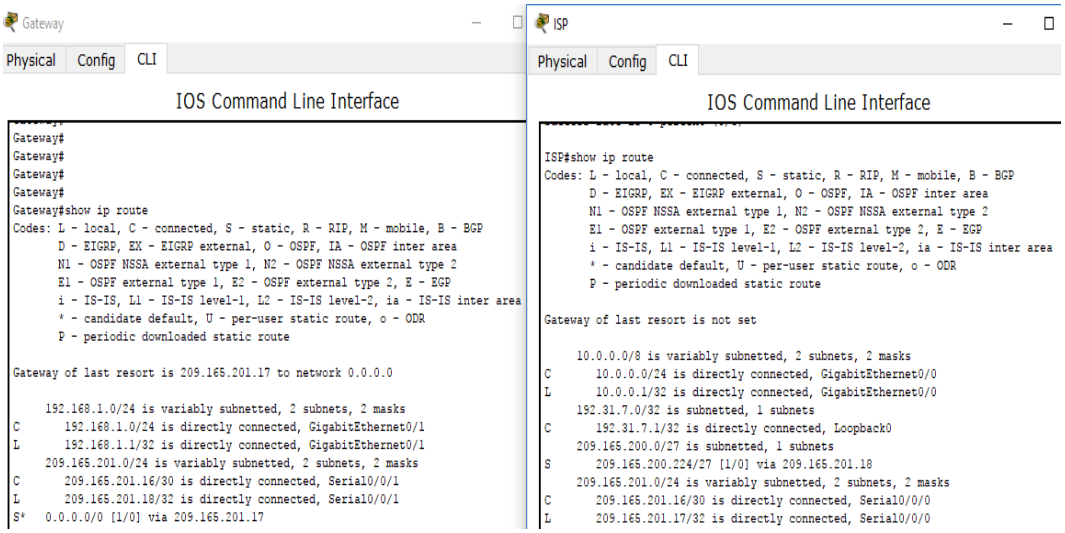


*Figure 184 Muestra de las tablas de routing*

## Parte 2: configurar y verificar la NAT estática.

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

### Paso 1: configurar una asignación estática.

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

Gateway(config)# **ip nat inside source static 192.168.1.20 209.165.200.225**

### Paso 2: Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

### Paso 3: Probar la configuración.

**a.** Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations.**

```
Gateway# show ip nat translations
Pro Inside global            Inside local  Outside local    Outside
global
--- 209.165.200.225    192.168.1.20        ---   ---
```

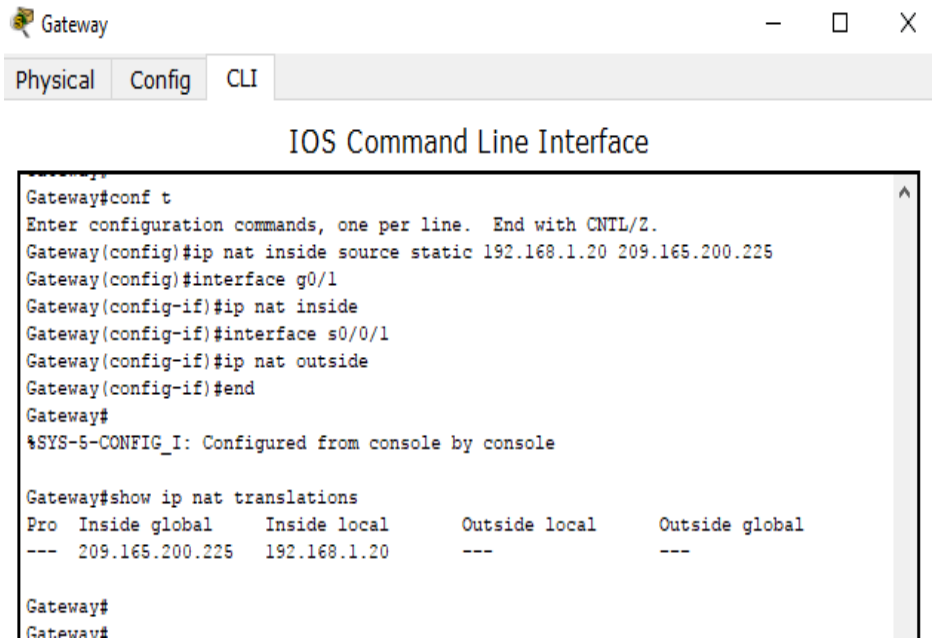


*Figure 185 Tabla de NAT estática*

¿Cuál es la traducción de la dirección host local interna?
192.168.1.20 = **209.165.200.225**

¿Quién asigna la dirección global interna?
**R=/ El router del pool de la NAT.**

¿Quién asigna la dirección local interna?
**R=/ El administrador de la estación de trabajo.**

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

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

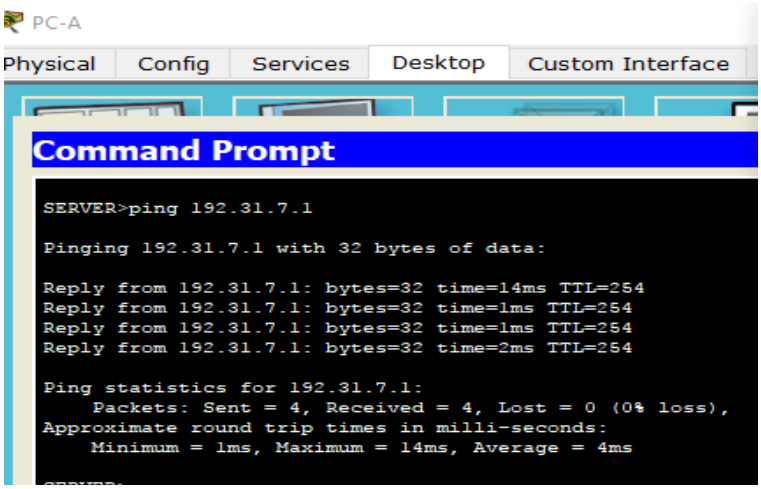


*Figure 186 Png a la interfaz Lo0*

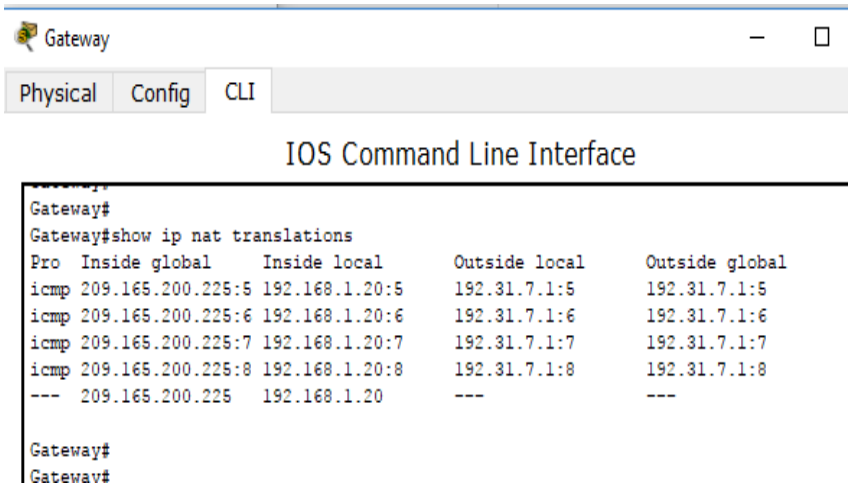


*Figure 187 Tabla de NAT*

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?
**R=/ El número de puertos varia.**

**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      ---    ---
```

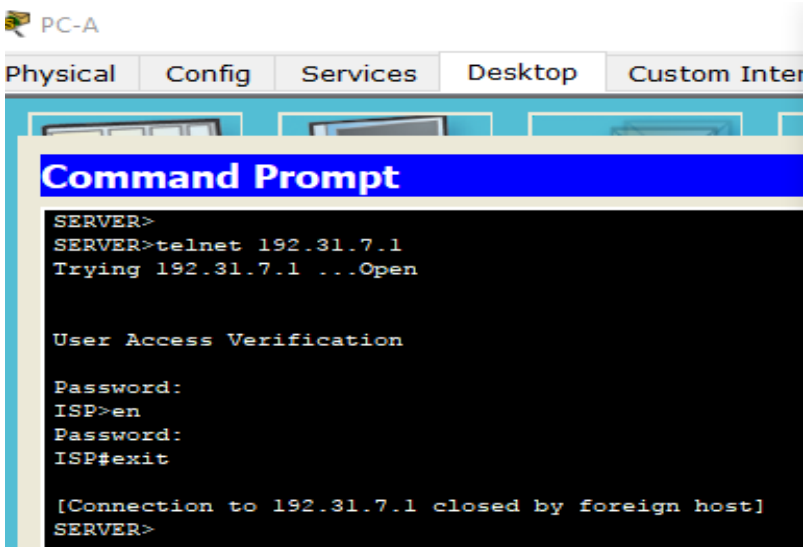


*Figure 188 Interfaz Lo0 en Pc-A*

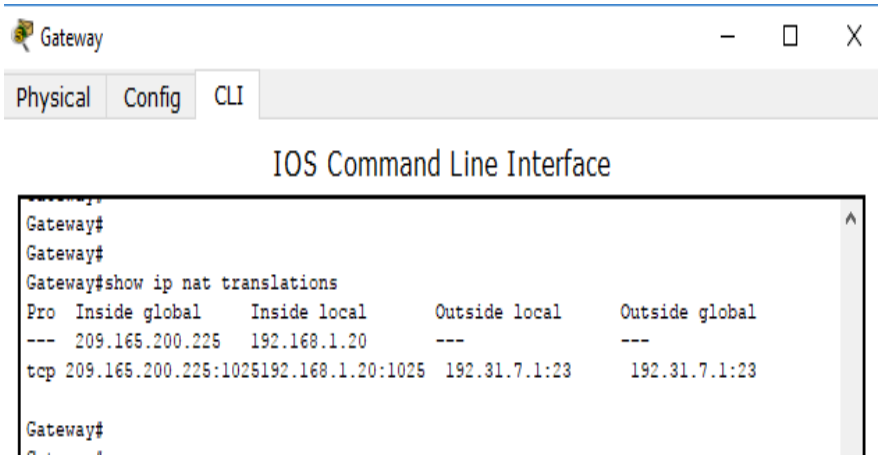


*Figure 189 Tabla NAT*

**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?
**R=/ Tcp**

¿Cuáles son los números de puerto que se usaron?
**R=/ Global/local interno: 1025**
**Globla/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.

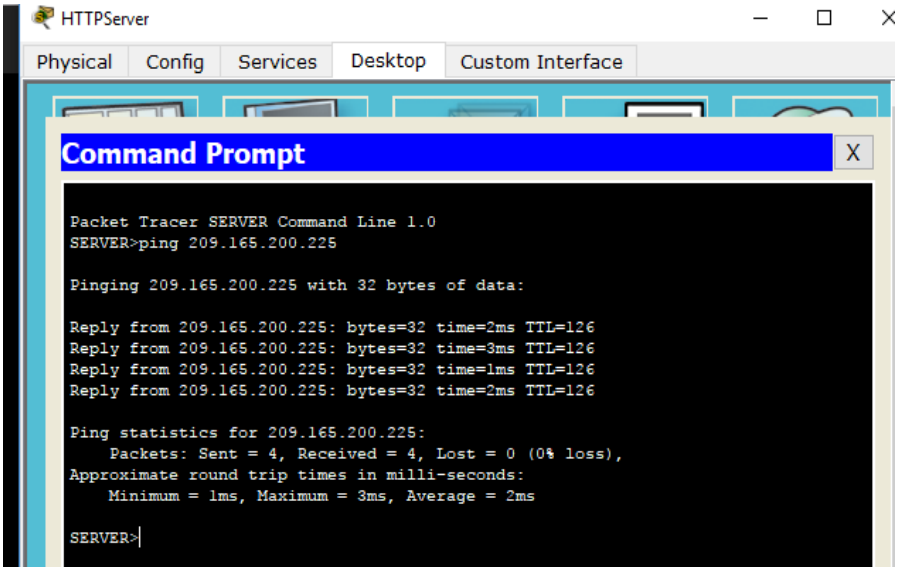


*Figure 190 Ping del ISP*

**e.** En el router Gateway, muestre la tabla de NAT para verificar la traducción.

```
Gateway# show ip nat translations
Pro Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:12
--- 209.165.200.225           192.168.1.20       ---                ---
```

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

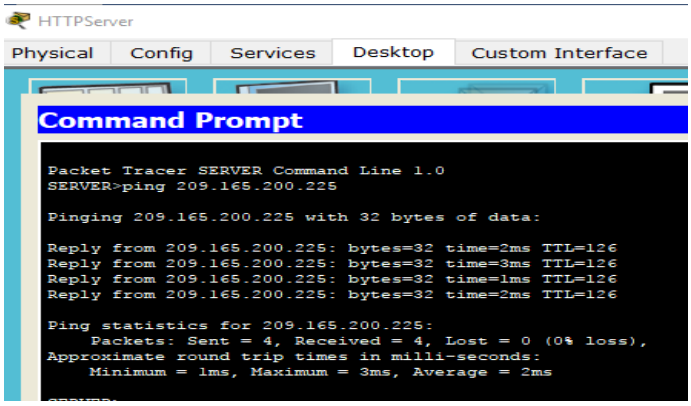


*Figure 191 Ping del ISP*

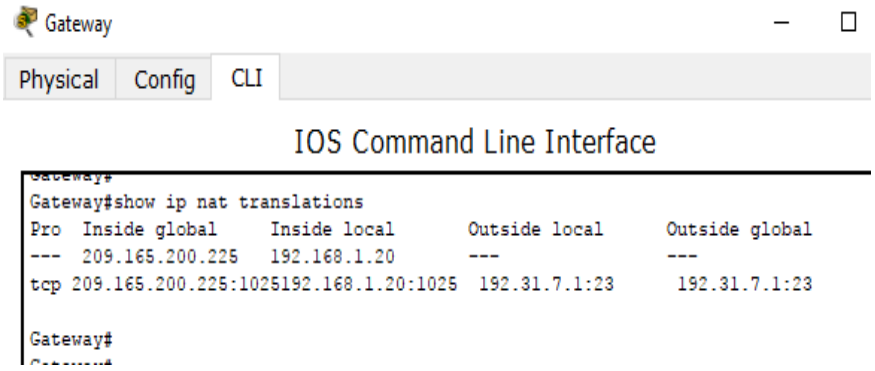


*Figure 192 Verificación de traducción*

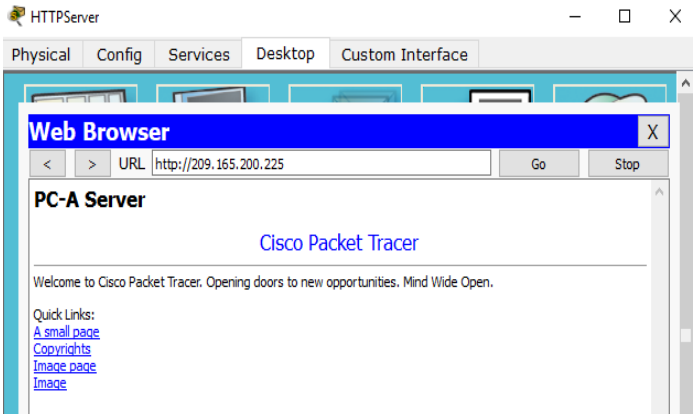


*Figure 193 Web browser*

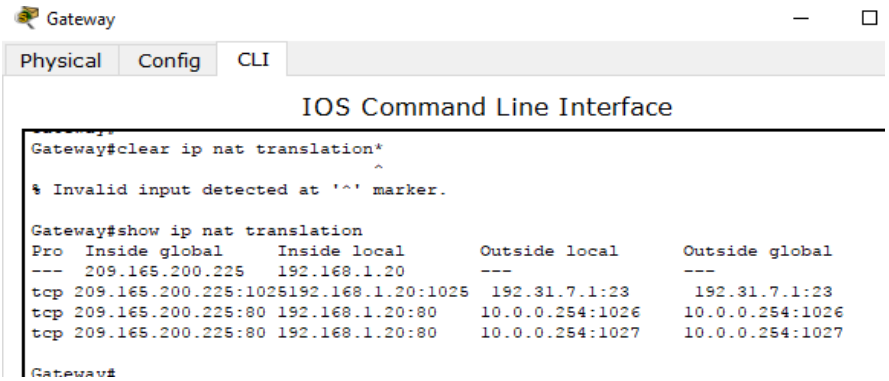


*Figure 194 NAT traducción*

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

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1
dynamic; 1 extended) Peak translations: 2,
occurred 00:02:12 ago
Outside interfaces:
    Serial0/0
```

```
    /1
Inside
 interfaces:
 GigabitEthernet
 0/1
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.

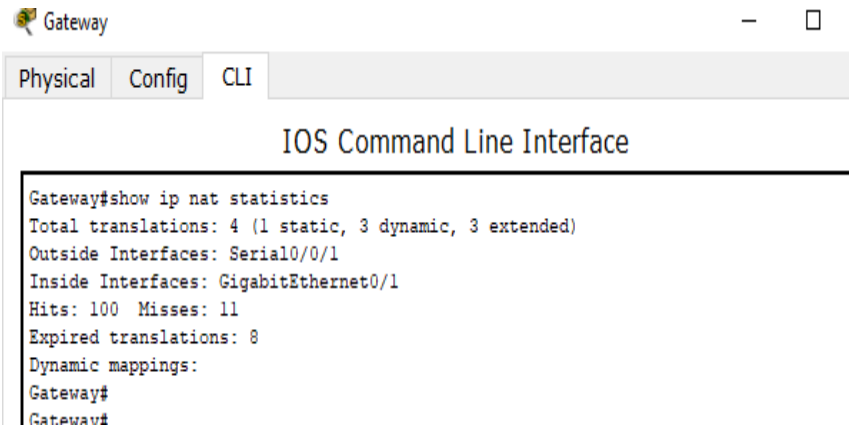


*Figure 195 Estáticas de NAT*

## Parte 3: Configurar yverificar la NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

### Paso 1: Borrar las NAT

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

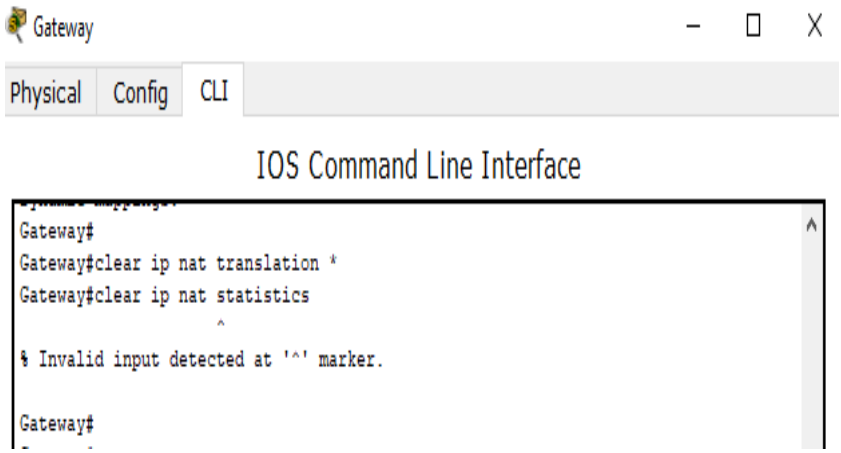


*Figure 196 Borrar las NAT*

**Paso 2: Definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.**

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

**Paso 3: Verificar que la configuración de interfaces NAT siga siendo válida.**

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

**Paso 4: Definir el conjunto de direcciones IP públicas utilizables.**

```
Gateway(config)# ip nat pool public_access 209.165.200.242
209.165.200.254 netmask
255.255.255.224
```

**Paso 5: Definir la NAT desde la lista de origen interna hasta el conjunto externo.**

**Nota:** recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

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

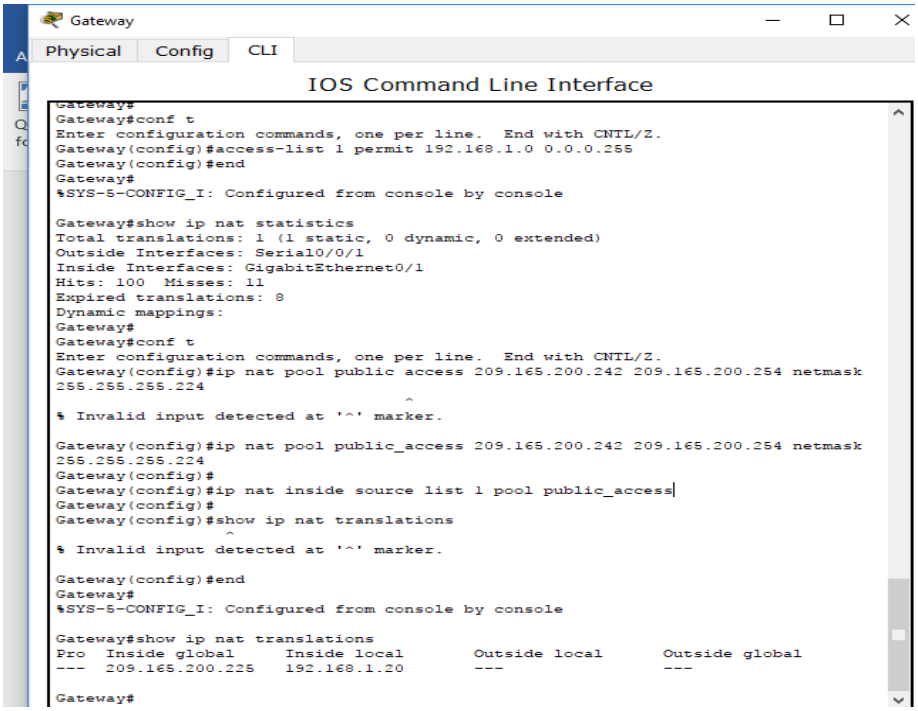


*Figure 197 Definir NAT*

## Paso 6: Probar la configuración.

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

```
Gateway# show ip nat translations
Pro Inside global            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    ---    ---
```

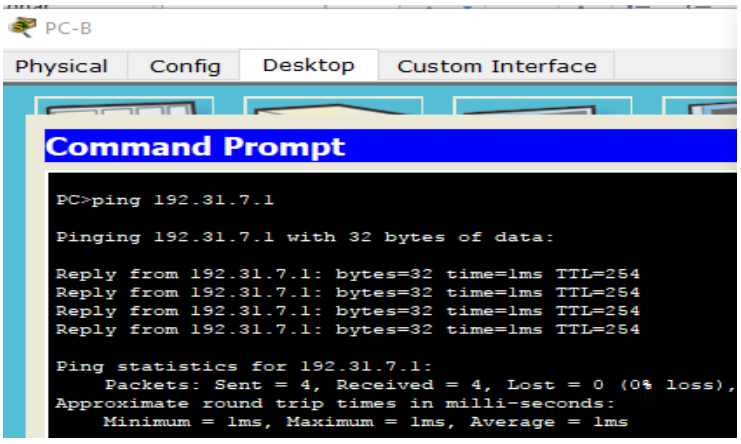


*Figure 198 Ping a la interfaz Lo0*

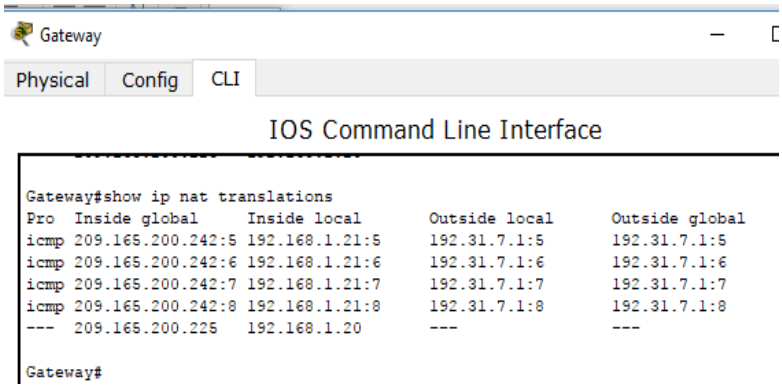


*Figure 199 Tabla de NAT en gateway*

¿Cuál es la traducción de la dirección host local interna de la PC-B?
192.168.1.21 = **209.165.200.242**

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

¿Qué número de puerto se usó en este intercambio ICMP?
**R=/ 1, 2, 3 y 4**

**b.** En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.

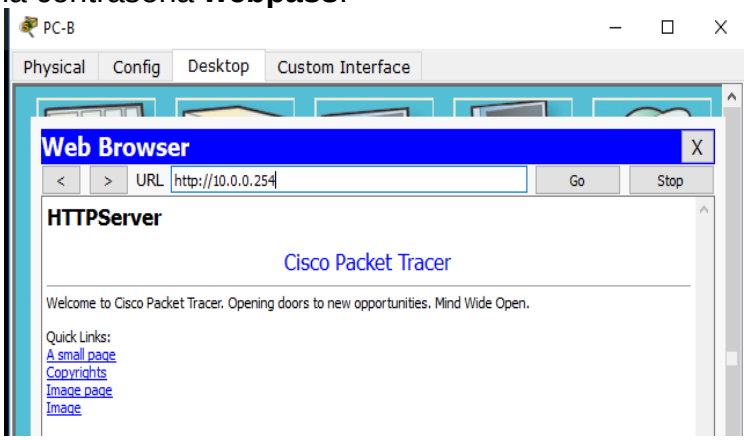


*Figure 200 Web browser*

**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       ---             ---
```

¿Qué protocolo se usó en esta traducción?
**R=/ tcp**

¿Qué números de puerto se usaron?

Interno: **1025**

Externo: **80**

¿Qué número de puerto bien conocido y qué servicio se usaron?
**R=/ Puerto 80 , http**

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

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)

  Peak translations: 17, occurred 00:06:40 ago
  Outside
   interfaces:
   Serial0/0/1
  Inside
   interfaces:
   GigabitEthernet0
   /1
  Hits: 345  Misses: 0
  CEF Translated packets: 345, CEF Punted packets: 0
  Expired translations: 20
```

```
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13, allocated 1 (7%), misses 0
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.

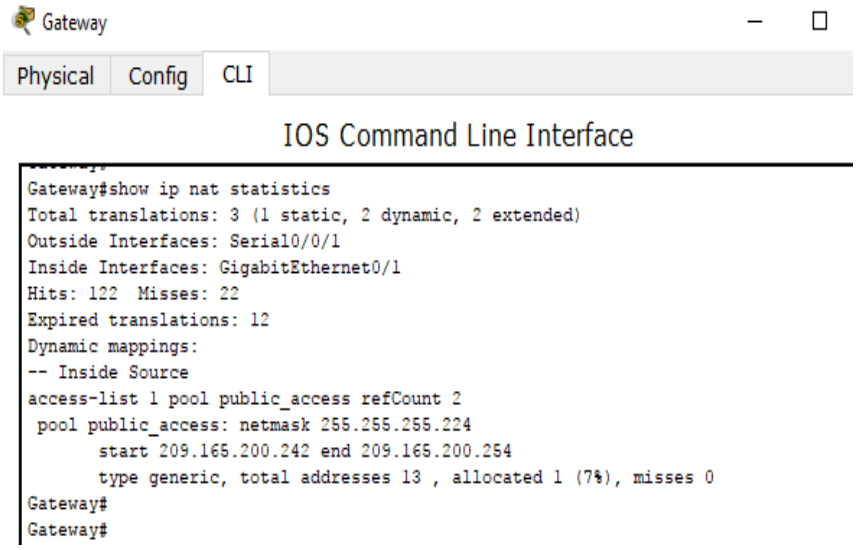


*Figure 201 Verificación de estadísticas NAT*

## Paso 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.

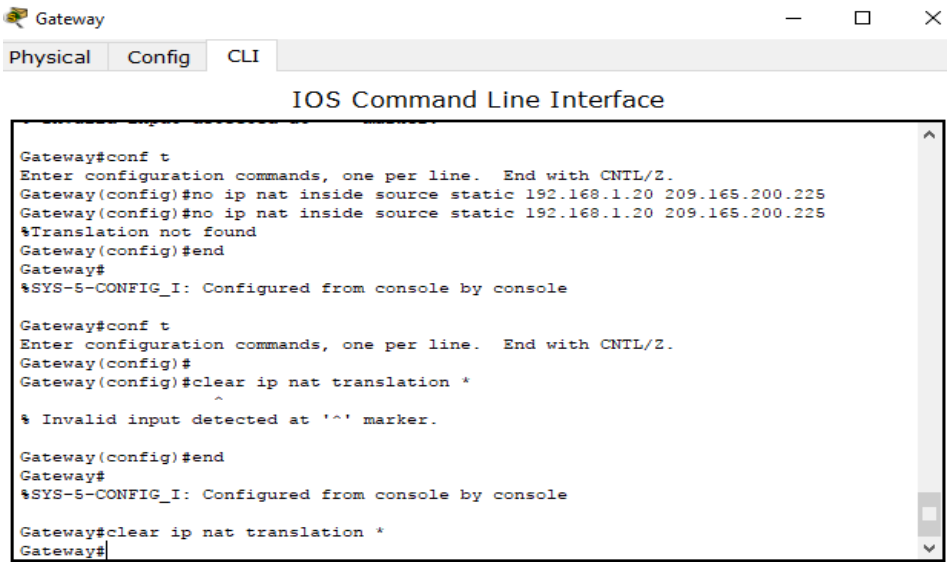


*Figure 202 Borrar las NAT y estadísticas*

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

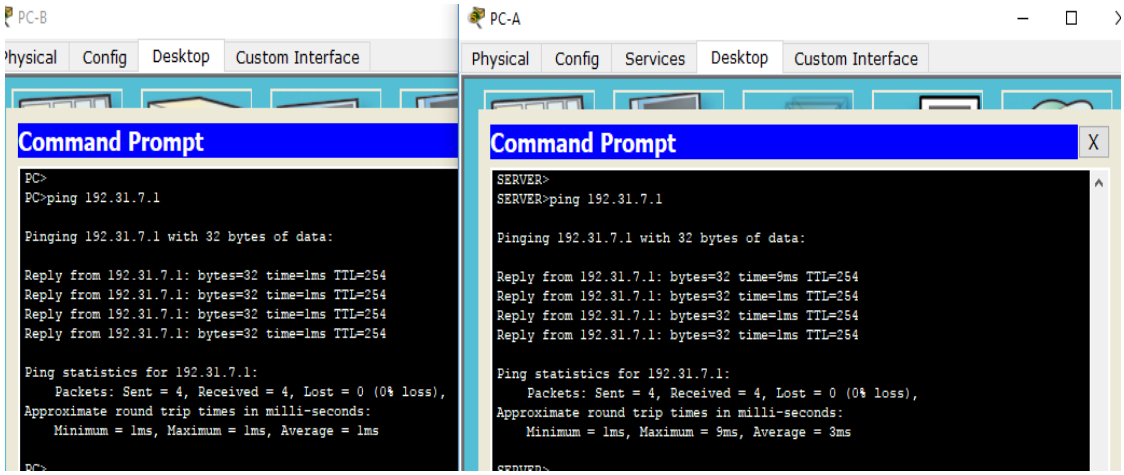


*Figure 203 Pinga la ISP*

**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.

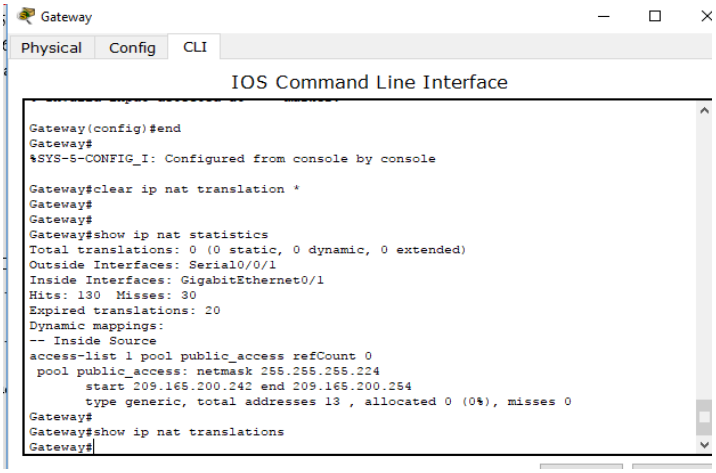


*Figure 204 Tabla y estadísticas de NAT*

## Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?
   **R=/ Las respuestas varían, pero deberían incluir: siempre que no haya suficientes direcciones IP públicas y para evitar el costo de adquisición de direcciones públicas de un ISP. NAT también puede proporcionar una medida**

**de seguridad al ocultar las direcciones internas de las redes externas.**

2. ¿Cuáles son las limitaciones de NAT?

   **R=/ NAT necesita la información de IP o de números de puerto en el encabezado IP y el encabezado TCP de los paquetes para la traducción. Esta es una lista parcial de los protocolos que no se pueden utilizar con NAT: SNMP, LDAP, Kerberos versión. 5.**

**Tabla de resumen de interfaces del router**

| Resumen de interfaces del router | | | | |
|---|---|---|---|---|
| **Modelo de router** | **Interfaz Ethernet #** | **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.**

*Tabla 14 Resumen de interfaces del router*

## Conclusiones

A través de este trabajo podemos ver la importancia de las ACL que son las listas de control de acceso y que pueden ser aplicadas en un router para poder controlar el tráfico de información dentro de una red de un lugar a otro (permitir, denegar o bloquear un servicio) de acuerdo con los requerimientos del sistema.

Se observa un ataque de denegación de servicio en donde se puede bloquear el acceso HTTP y HTTPS hacia la red por medio de las ACLs. Se puede denegar el tráfico TCP de un servidor a otro servidor a través del puerto 443, como también el permitir el tráfico IPV6 en la red. Esto nos permite aplicar las ACLs en la interface correcta. Podemos crear las ACLs y verificar su implementación.

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.

DHCP es un protocolo que configure dinámicamente los hots, el servidor DHCPv4 tiene la facultad de asignar y administrar direcciones IPv4 vinculadas a VLAN específicas. Esto se puede trabajar con el switch 2960 el cual funciona como dispositivo de capa 3 permitiendo trabajar el routing y rutas estáticas de igual forma únicas y múltiples esta última para permitir una comunicación constante entre los hosts de la red a trabajar.

Para su configuración para las VLAN se utilizan una serie de configuraciones y comando de acuerdo a los requerimientos, por ejemplo se deben excluir las 10 primeras direcciones de host válidas de la red para evitar que estas dinámicamente sean dadas a otros hosts el comando es ip dhcp excluded-address + las direcciones a excluir, con el comando ip dhcp pool se da el nombre al pool de DHCP de direccionamiento, de igual forma se debe asignar la red, el Gateway predeterminado, el servidor DNS, y DHCPv4 maneja un tiempo de arrendamiento que se debe determinar en días lo que el cliente debe estar pendiente de estar actualizando periódicamente.

## Referencias Bibliográficas


Durán, E. *Guía Carga trabajos de grado por autores repositorio UNAD.* Tomado de: https://drive.google.com/file/d/0B6RUvrqhqCRdNzB6TGV6WGFYa1E/view

Patiño, C. Guía para la redacción en el estilo APA.(6ta edición)

Cisco Networking Academy. Tomado de: http://ecovi.uagro.mx/ccna1/index.html

Introducción a Cisco Packet Tracer. Tomado de: http://simulacionderedeslan.blogspot.com.co/2013/06/introduccion-cisco-packet-tracer.html

Comandos Router Cisco. Pdf generate by  e$cRi

Comandos de Configuración de Dispositivos Cisco. Documento pdf.