



Trabajo colaborativo 4

Claudia Yoana Otalvaro Garces – 111198435  
Grupo 203092\_52

Tutor  
Nilson Albeiro Ferreira Manzanares

Universidad Nacional Abierta y a Distancia – UNAD  
Diplomado de Profundización CISCO (Diseño e Implementación de Soluciones Integradas LAN/WAN)  
Semestre B 2017

## Introducción

En la configuración básica de RIPv2 y RIPv6 se debe tener en cuenta los parámetros básicos de los dispositivos, al igual que se debe configurar y verificar el routing RIPv2, lo mismo sucede con la IPv6 en los dispositivos, cabe recalcar que el RIPv2 se utiliza para enrutar direcciones IPv4 en redes pequeñas, por otro lado la configuración de OSPFv2 básico de área única, en donde el protocolo OSPF es un protocolo de routing de estado de enlace para las redes IP, lo cual se definió OSPFv2 para redes IPv4 y OSPFv3 para redes IPv6, en estas se configura y verifica el routing OSPF al igual que se cambian las asignaciones de ID del router, las interfaces OSPF pasivas y se cambian las métricas.

Por otro lado la configuración de DHCPv4 básico en un router o configuración dinámica de host (DHCP), es un protocolo de red que permite a los administradores de red administrar y automatizar la asignación de direcciones IP, en este escenario lo que se realiza es la configuración de un servidor de DHCPv4 y un agente de retransmisión DHCP, de igual manera se trabaja en la configuración básica de DHCPv4 en un Switch, en el cual se cambiaría la preferencia de SDM, la configuración DHCPv4 y la misma configuración DHCP pero para varias VLAN, por último habilitar el routing IP, siendo el servidor de DHCPv4 de Cisco el que asigna y administra direcciones IPv4 de conjuntos de direcciones identificados que están asociados a VLAN específicas e interfaces virtuales de switch (SVI).

También hablamos de configuración de DHCPv6 sin estado y con estado, en las cuales se realizarán configuraciones de la red para SLAAC, DHCPv6 sin estado y DHCP con estado, recordando siempre las tres maneras de configuraciones en la asignación dinámica de direcciones IPv6 de unidifusión global, las cuales se mencionan a continuación:

- 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

Cuando se trabaja en la configuración de NAT dinámica y estática, se habla del proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada, también se trata la configuración de un conjunto de NAT con sobrecarga y PAT en ellos se configuraran y verificaran un conjunto de NAT con carga y finalmente se configura y verifica PAT.

La configuración estándar de ACLs implica la configuración, aplicación y verificación de una ACL estándar, igual planifica una implementación de ACL, se recuerda que las listas de control de acceso (ACL), estándar son secuencias de comandos de configuración de enrutadores que controlan si un enrutador permite o niega paquetes en función de la dirección de origen, también se trabaja la configuración de las ACL estándar nominales en donde se configura y aplica una ACL estándar designada y se verifica la implementación de ACL. Continuando con la configuración de ACL, estas se trabajan también en líneas VTY.

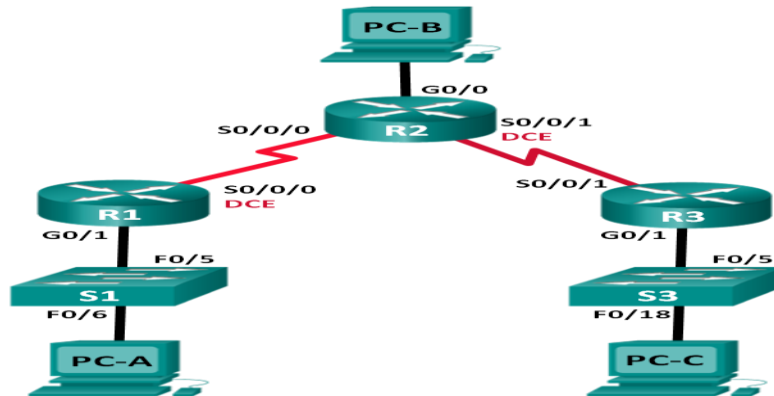


---

Por último se trabaja la configuración de las ACL de IPv6, en las cuales se configurara, aplicara y verificara una ACL de IPv6, lo mismo sucede con una segunda ACL de IPv6, cada una de las configuraciones serán realizadas y evidenciadas.

### 7.3.2.4 Lab – Configuring Basic RIPv2 and RIPv6

#### Topología



#### 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 RIPv6**

- Configurar y verificar que se esté ejecutando RIPv6 en los routers.
- Examinar las tablas de routing.
- Configurar una ruta predeterminada.
- Verificar la conectividad de extremo a extremo.

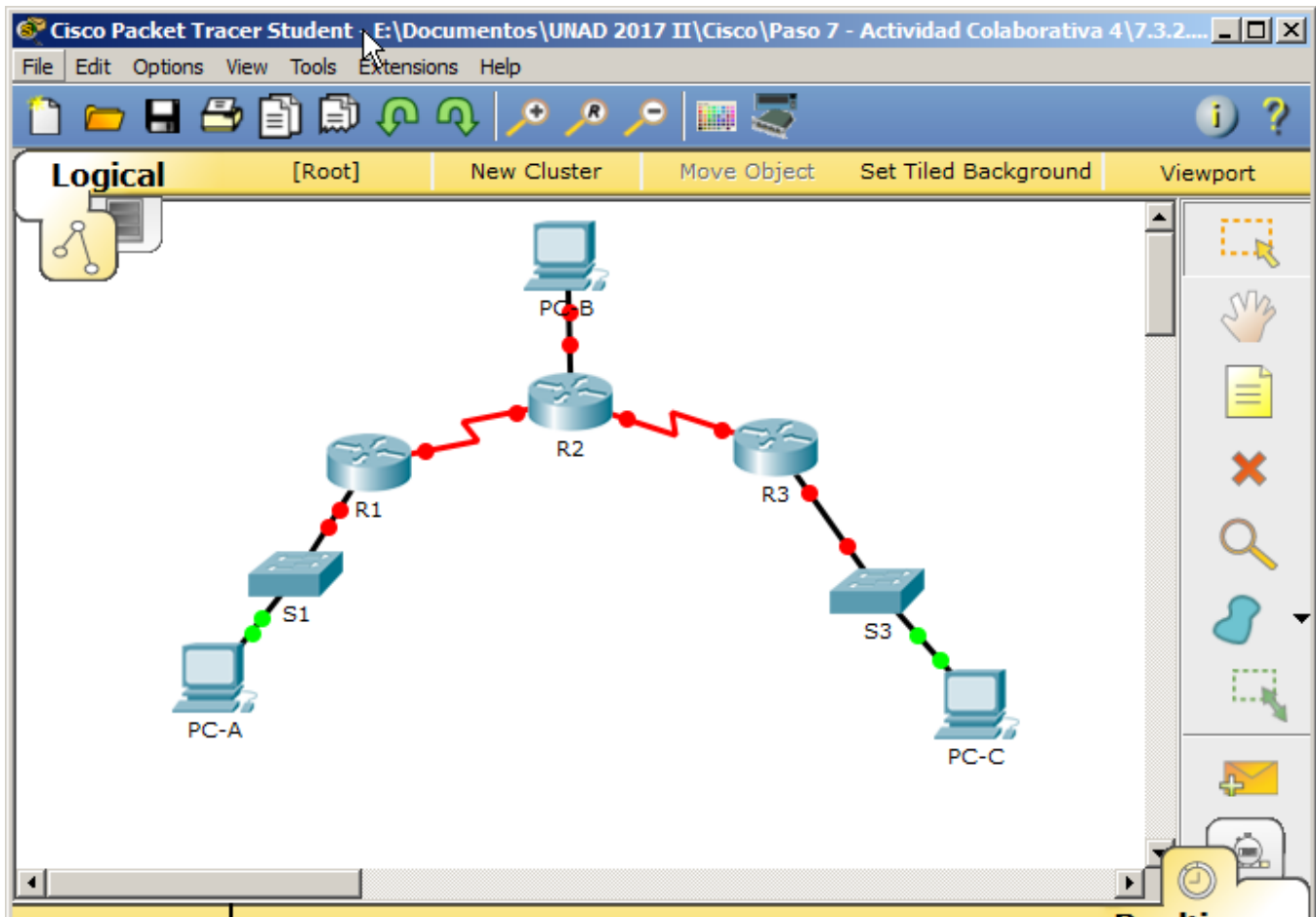
## Tabla de direccionamiento

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

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

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

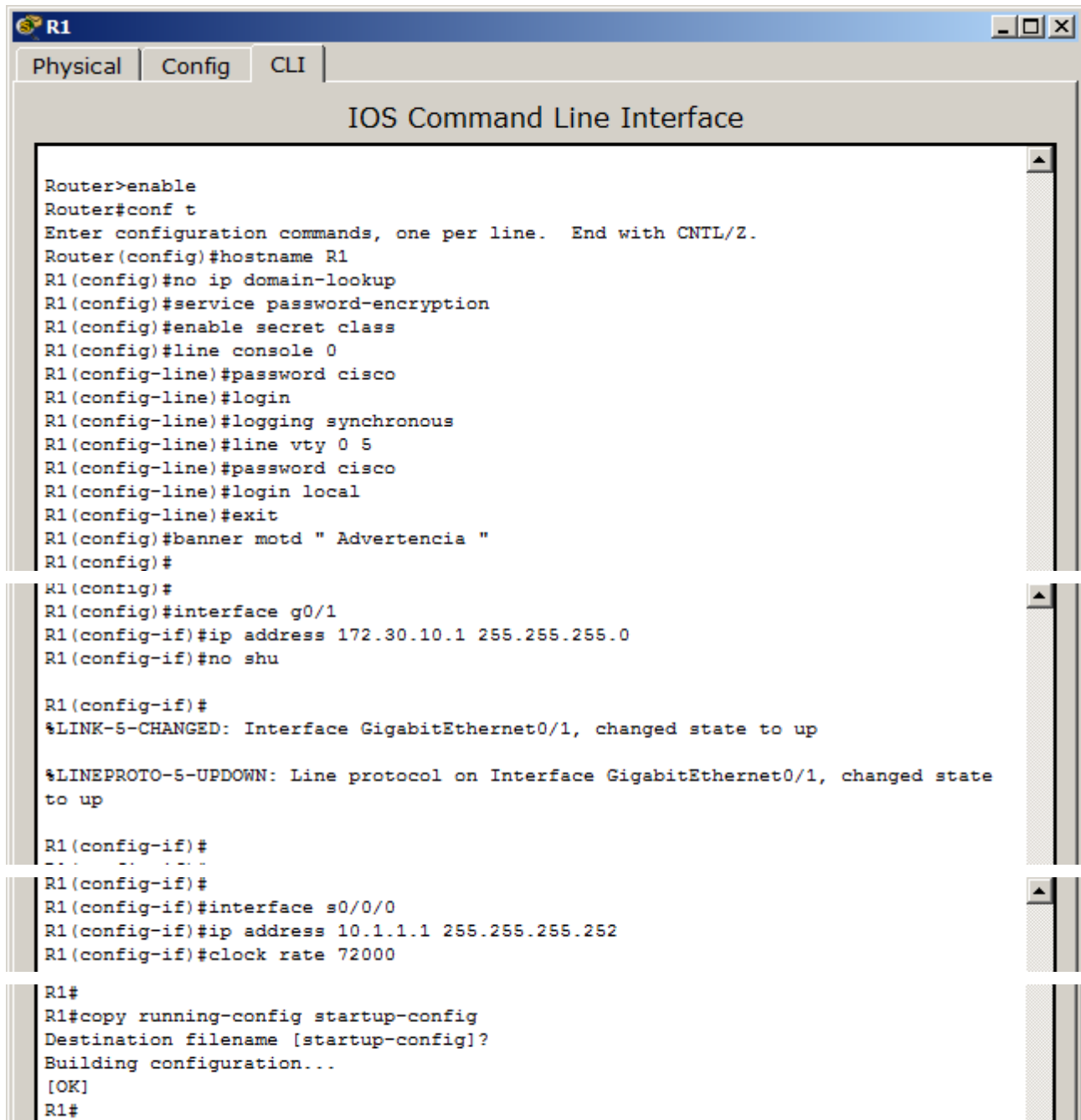
**Paso 1. realizar el cableado de red tal como se muestra en la topología.**



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

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

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



The screenshot shows the IOS Command Line Interface for router R1. The window title is 'R1' and it has tabs for 'Physical', 'Config', and 'CLI'. The CLI shows the following configuration steps:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#service password-encryption
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 5
R1(config-line)#password cisco
R1(config-line)#login local
R1(config-line)#exit
R1(config)#banner motd " Advertencia "
R1(config)#

R1(config)#
R1(config)#interface g0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#no shu

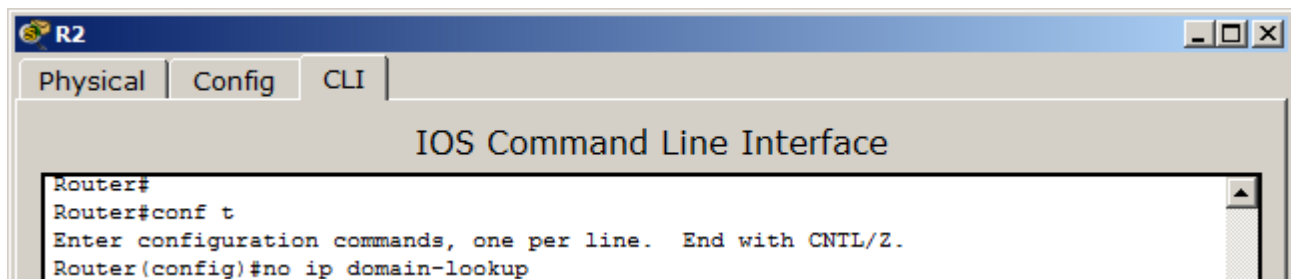
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R1(config-if)#

R1(config-if)#
R1(config-if)#interface s0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 72000

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



The screenshot shows the IOS Command Line Interface for router R2. The window title is 'R2' and it has tabs for 'Physical', 'Config', and 'CLI'. The CLI shows the following configuration steps:

```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
```

```

Router(config)#hostname R2
R2(config)#service password-encryption
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#line vty 0 5
R2(config-line)#password local
R2(config-line)#exit
R2(config)#banner motd " Advertencia "
R2(config)#interface g0/0
R2(config-if)#ip address 209.165.201.1 255.255.255.0
R2(config-if)#interface s0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#interface s0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shu

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

R2(config)#interface s0/0/1
R2(config-if)#clock rate 72000
This command applies only to DCE interfaces
R2(config-if)#no shu

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

```

```

R3
Physical | Config | CLI
IOS Command Line Interface

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3

R3(config)#
R3(config)#enable password class
R3(config)#service password-encryption
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 5
R3(config-line)#password local
R3(config-line)#logging synchronous
R3(config-line)#banner motd " Advertencia "
R3(config)#

```



```
R3(config)#
R3(config)#interface g0/1
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#no shu

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

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

R3(config-if)#interface s0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut

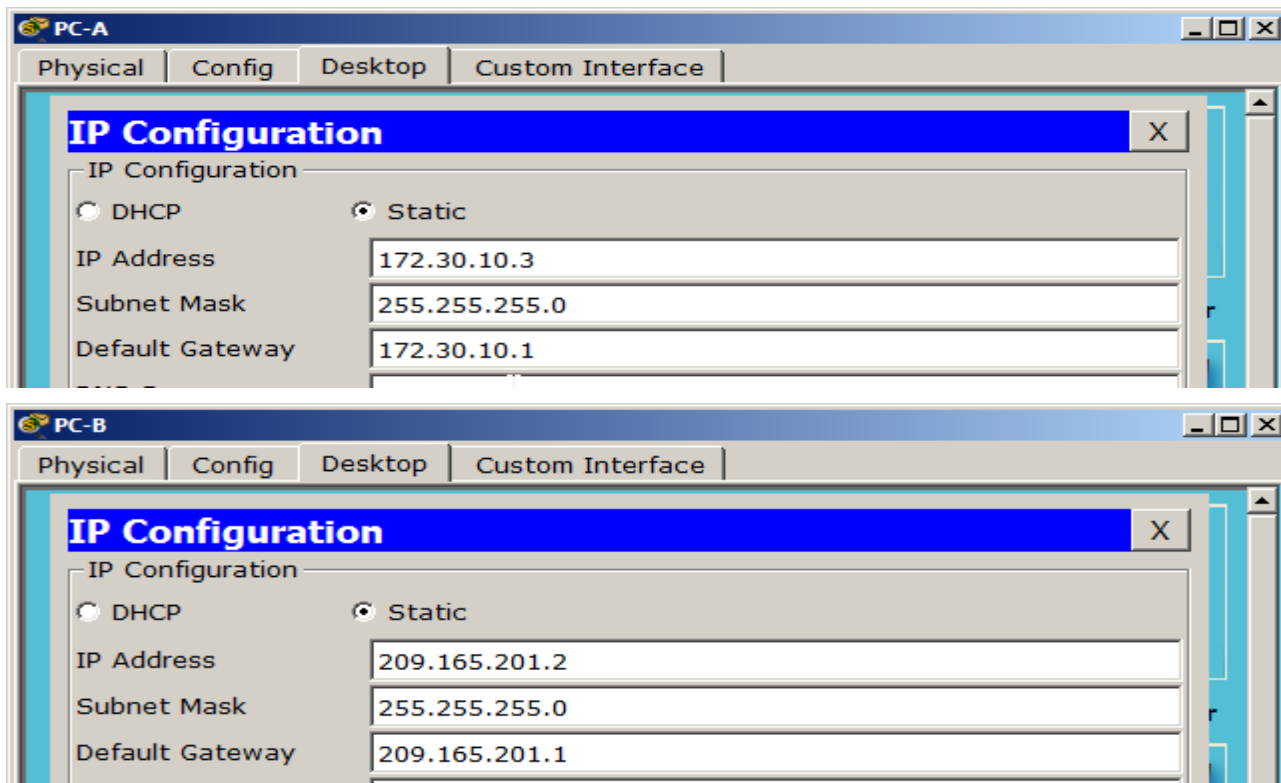
R3(config-if)#
%LINK-5-CHANGED: Interface Serial10/0/1, changed state to up

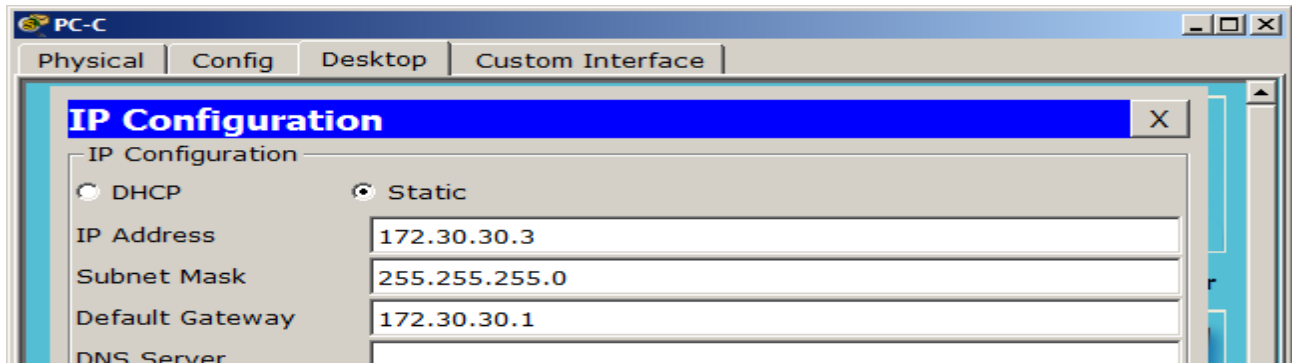
R3(config-if)#
R3(config-if)#
R3(config-if)#interface s0/0/1
R3(config-if)#clock rate 72000
R3(config-if)#no shu
R3(config-if)#

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

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

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

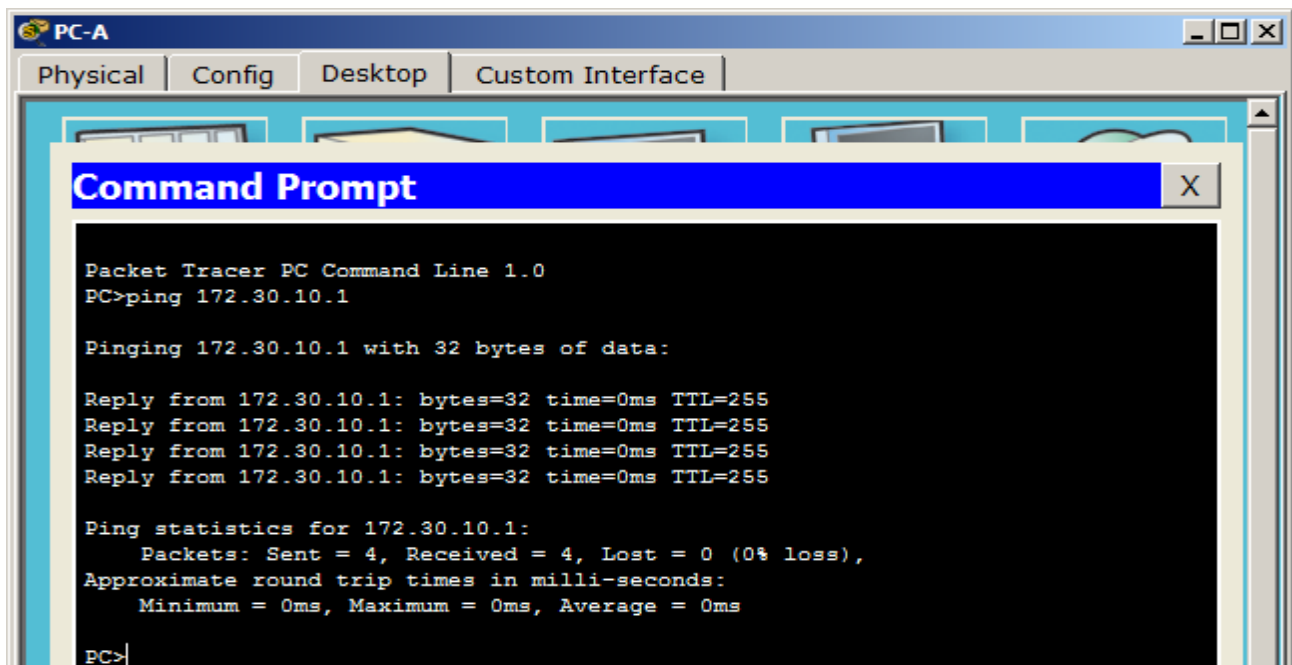


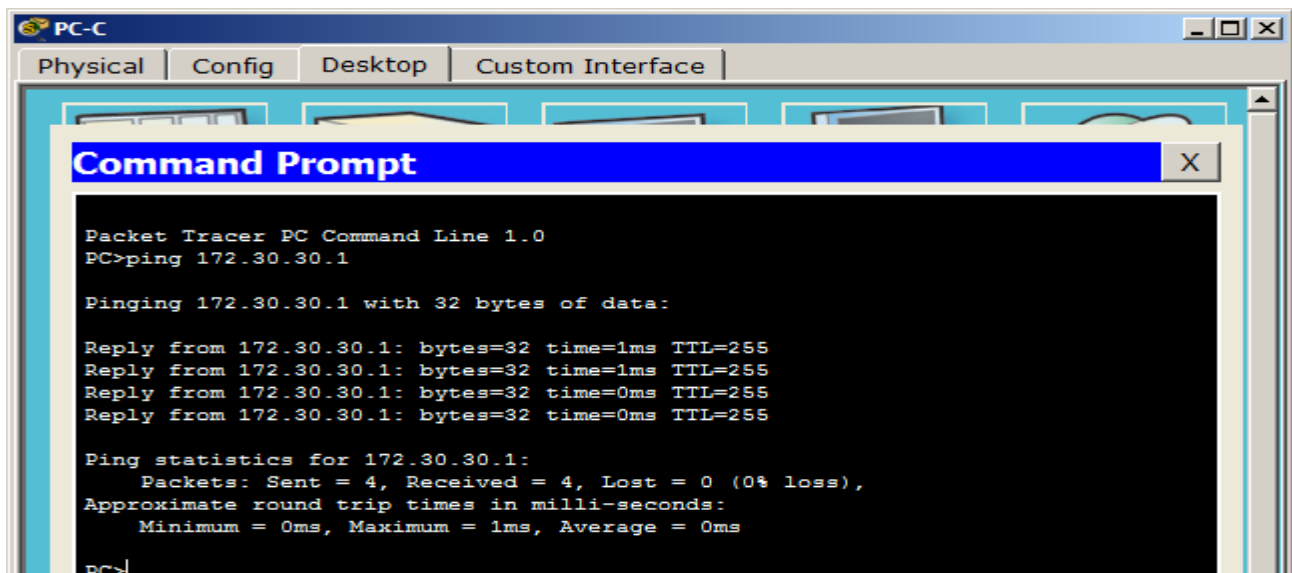
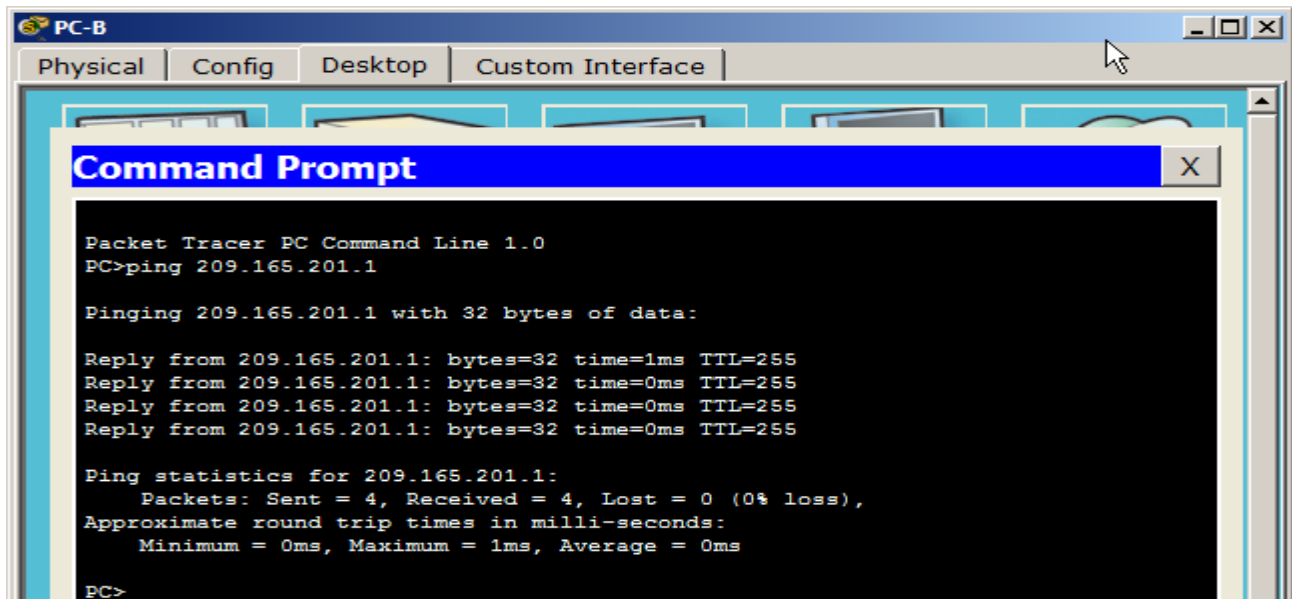


### Paso 5. Probar la conectividad.

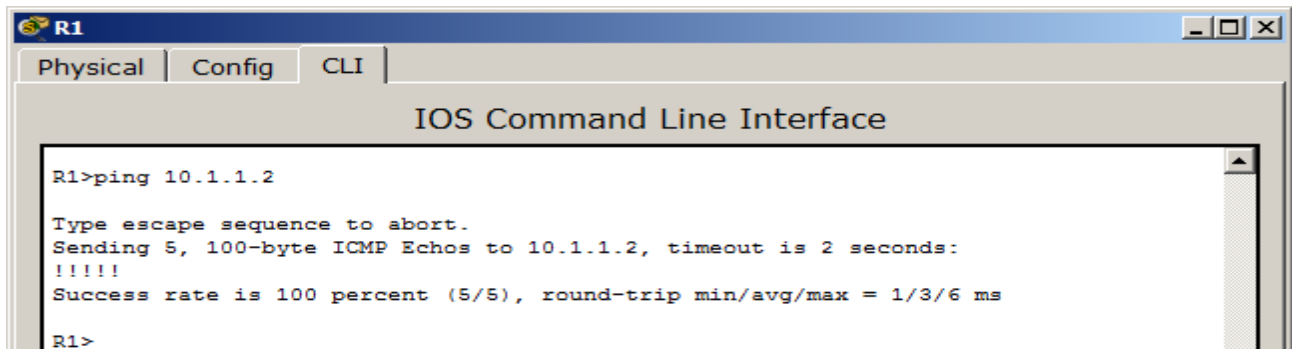
En este momento, las computadoras no pueden hacerse ping entre sí.

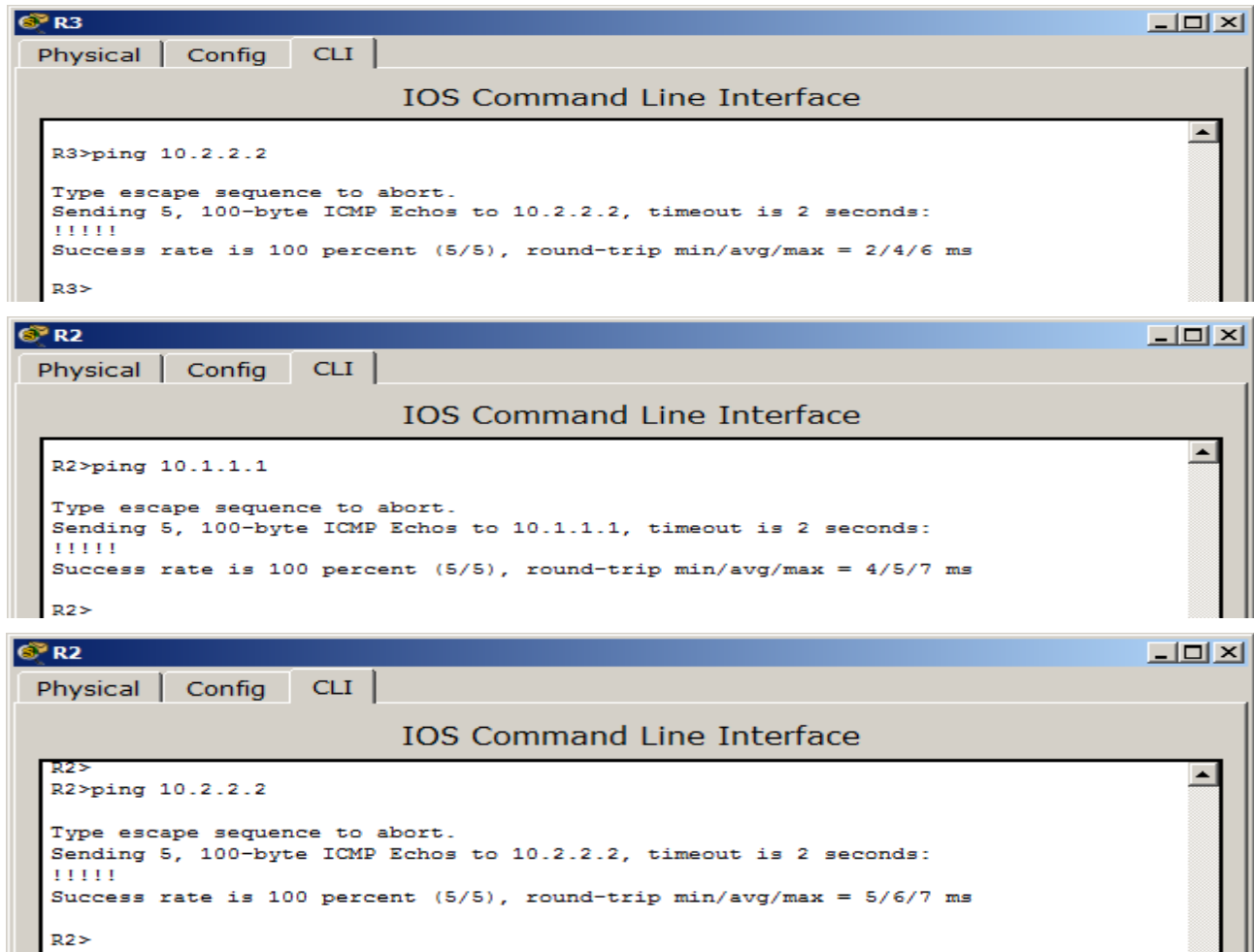
- a. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.





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





## 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.

- 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.

```

R1
Physical | Config | CLI |
IOS Command Line Interface

R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#passive-interface g0/1
R1(config-router)#network 172.30.0.0
R1(config-router)#network 10.0.0.0
R1(config-router)#

```

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

```

R3
Physical | Config | CLI |
IOS Command Line Interface

R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#passive-interface g0/1
R3(config-router)#network 172.30.0.0
R3(config-router)#network 10.0.0.0
R3(config-router)#

```

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

```

R2
Physical | Config | CLI |
IOS Command Line Interface

R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#passive-interface g0/0
R2(config-router)#network 10.0.0.0

```

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

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

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

R2# **show ip interface brief**

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

```
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0      209.165.201.1  YES manual  up          up
GigabitEthernet0/1      unassigned      YES unset   administratively down down
Serial10/0/0            10.1.1.2        YES manual  up          up
Serial10/0/1            10.2.2.2        YES manual  up          up
Vlan1                    unassigned      YES unset   administratively down down
R2#
```

b. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? No ¿Por qué? Porque no hay una ruta que llegue a PC-B

```
PC-A
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Request timed out.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.

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

¿Es posible hacer ping de la PC-A a la PC-C? No ¿Por qué? Porque R1 y R3 no tienen rutas hacia el router remoto.

```
PC-A
Physical Config Desktop Custom Interface

Command Prompt

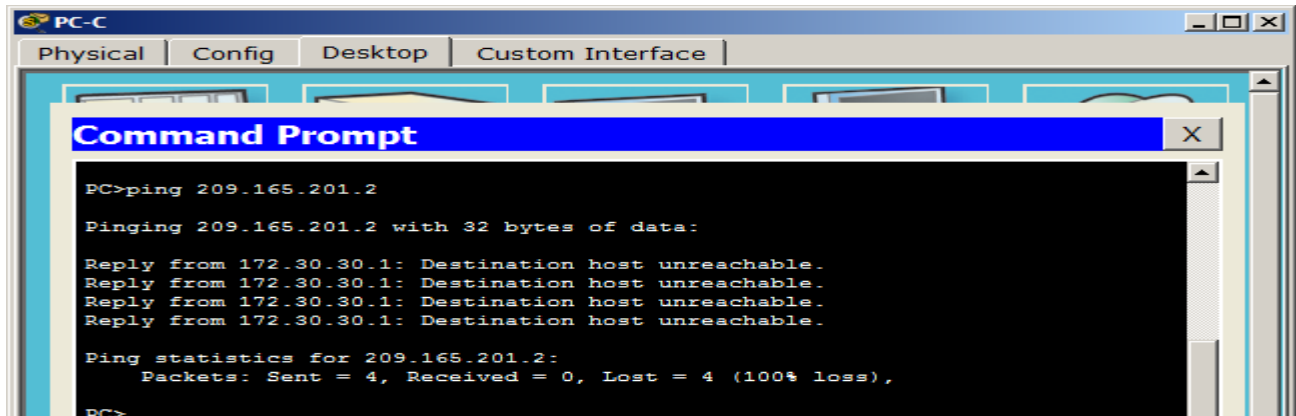
PC>ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:

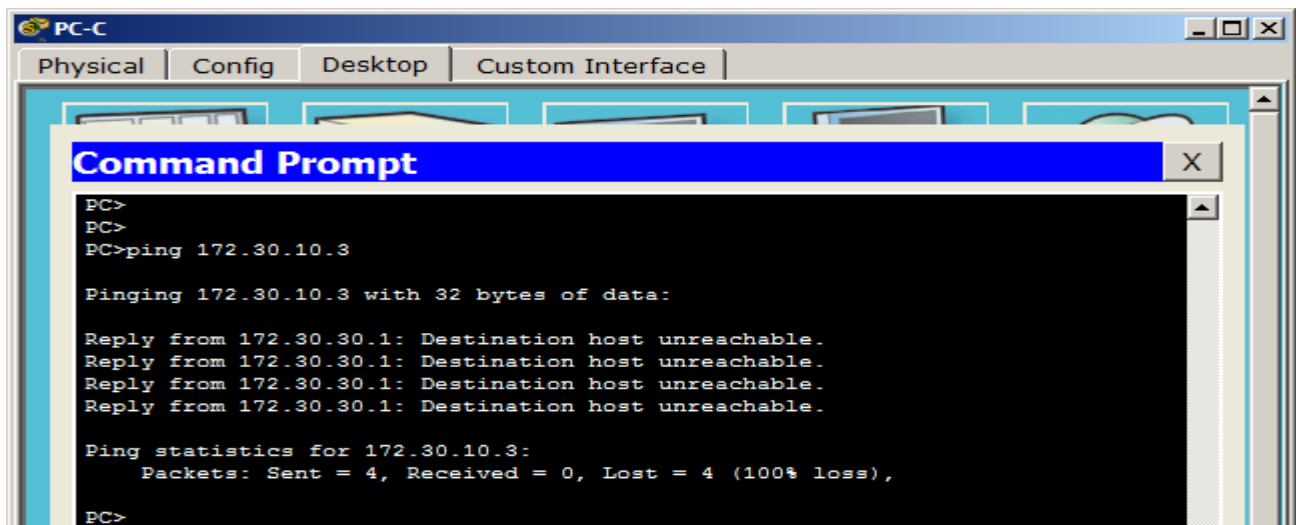
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>
```

¿Es posible hacer ping de la PC-C a la PC-B? No ¿Por qué? Porque PC-B no participa en RIP en la red LAN.



¿Es posible hacer ping de la PC-C a la PC-A? No ¿Por qué? Porque R1 y R3 no tienen rutas específicas remotas, no hay ruta a la subred.



c. Verifique que RIPv2 se ejecute en los routers.

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

R1# **show ip protocols**

Routing Protocol is "rip"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Sending updates every 30 seconds, next due in 7 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Redistributing: rip

Default version control: **send version 2, receive 2**

Interface            Send Recv Triggered RIP Key-chain

Serial0/0/0        2    2

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

10.0.0.0

172.30.0.0

Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

10.1.1.2	120	
----------	-----	--

Distance: (default is 120)

```
R1
Physical Config CLI
IOS Command Line Interface
Password:
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 19 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
Interface          send recv triggered rlp  Key-chain
Serial0/0/0        2         2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
    10.0.0.0
    172.30.0.0
Passive Interface(s):
    GigabitEthernet0/1
Routing Information Sources:
    Gateway         Distance    Last Update
    10.1.1.2        120        00:00:08
Distance: (default is 120)
R1#
```

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

```
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.0.0/16 via 0.0.0.0 in 1 hops

R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
    10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
    10.2.2.0/30 via 0.0.0.0, metric 1, tag 0

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

R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.0.0/16 via 0.0.0.0 in 1 hops
```

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



```
R2
Physical | Config | CLI |
IOS Command Line Interface
R2#undebug all
All possible debugging has been turned off
R2#
```

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

```
R3
Physical | Config | CLI |
IOS Command Line Interface
R3#
R3#show run
Building configuration...

Current configuration : 1083 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
```

```
R3
Physical | Config | CLI |
IOS Command Line Interface
ip address 10.2.2.1 255.255.255.252
clock rate 72000
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
passive-interface GigabitEthernet0/1
network 10.0.0.0
network 172.30.0.0
!
ip classless
!
ip flow-export version 9
```

d. Examinar el sumarización automática de las rutas.

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

R2# **show ip route**

<Output Omitted>

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

- C 10.1.1.0/30 is directly connected, Serial0/0/0
- L 10.1.1.2/32 is directly connected, Serial0/0/0
- C 10.2.2.0/30 is directly connected, Serial0/0/1
- L 10.2.2.2/32 is directly connected, Serial0/0/1

```

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

```

```

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

Gateway of last resort is not set

    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, 00:00:06, Serial0/0/1
        [120/1] via 10.1.1.1, 00:00:03, Serial0/0/0
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C     209.165.201.0/24 is directly connected, GigabitEthernet0/0
L     209.165.201.1/32 is directly connected, GigabitEthernet0/0
R2#

```

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

**R1# show ip route**

<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

```

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

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 3 subnets, 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, 00:00:07, Serial0/0/0
 172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R1#
```

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

**R3# show ip route**

<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
```

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

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R   10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:10, Serial0/0/1
C   10.2.2.0/30 is directly connected, Serial0/0/1
L   10.2.2.1/32 is directly connected, Serial0/0/1
172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C   172.30.30.0/24 is directly connected, GigabitEthernet0/1
L   172.30.30.1/32 is directly connected, GigabitEthernet0/1
R3#
```

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

En las siguientes redes ambas cuentan con una máscara de subred /16

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

```
R2
Physical Config CLI
IOS Command Line Interface
R2#
R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops

R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops

R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0

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

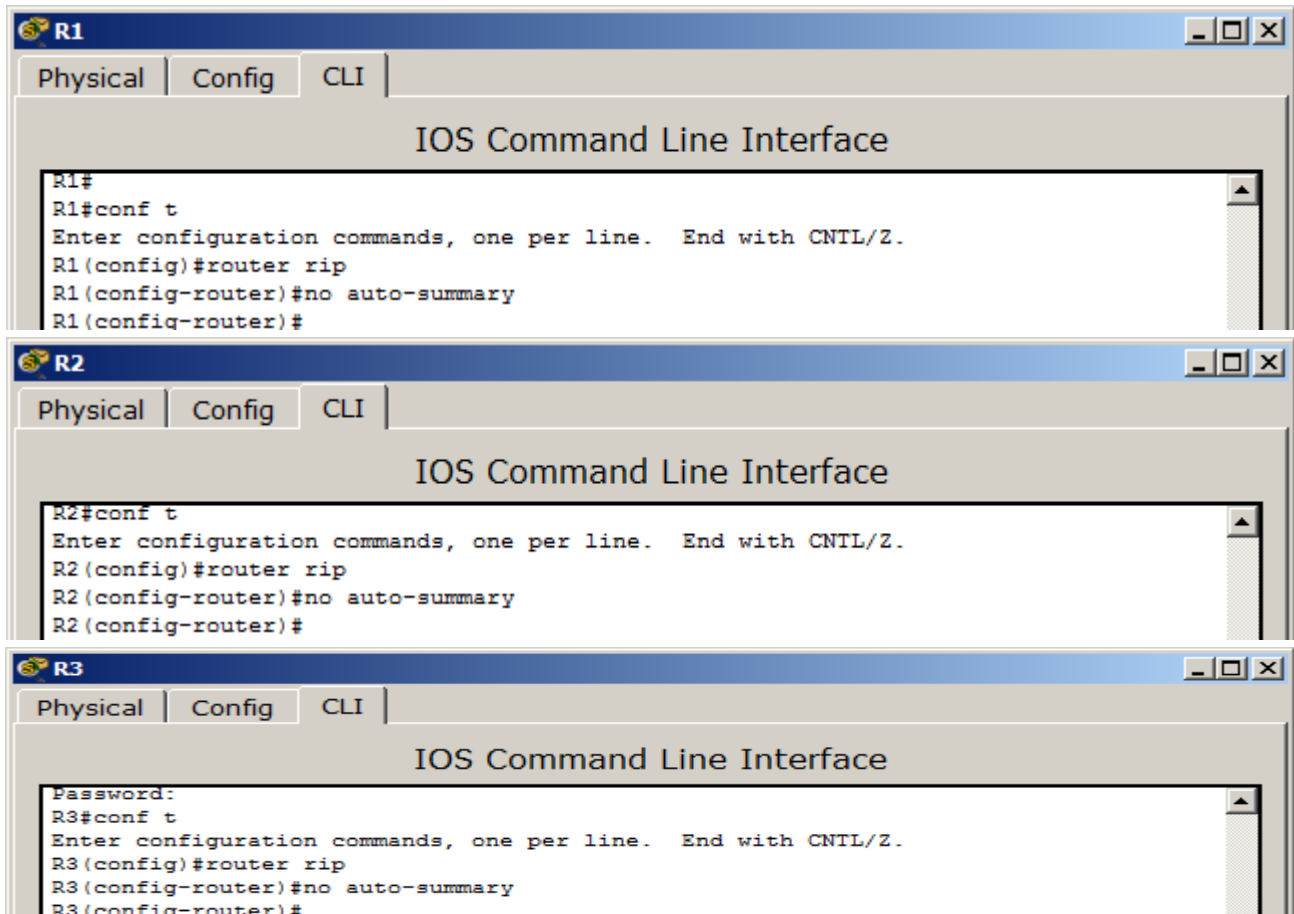
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops
```

### Paso 3. Desactivar la sumarización automática.

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

```
R1(config)# router rip
```

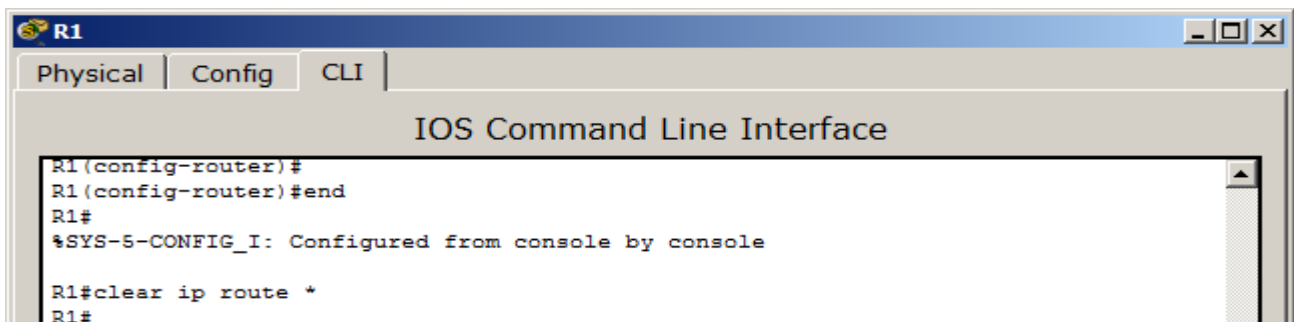
```
R1(config-router)# no auto-summary
```



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

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

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



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

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

R2# **show ip route**

<Output Omitted>

Gateway of last resort is not set

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

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

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

C 10.2.2.0/30 is directly connected, Serial0/0/1

L 10.2.2.2/32 is directly connected, Serial0/0/1

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

R 172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:01, Serial0/0/1

[120/1] via 10.1.1.1, 00:01:15, Serial0/0/0

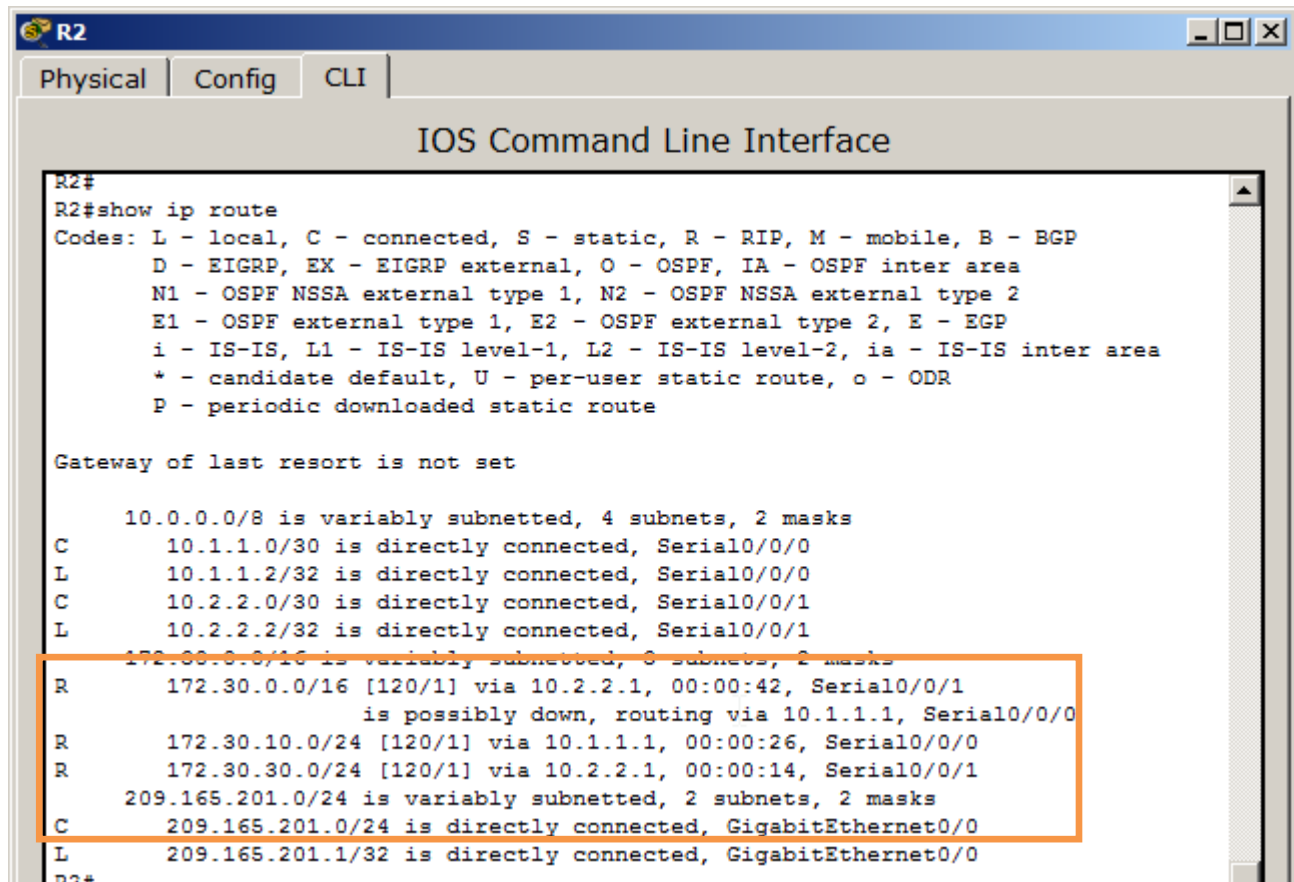
R 172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0

R 172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04, Serial0/0/1

209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.201.0/24 is directly connected, GigabitEthernet0/0

L 209.165.201.1/32 is directly connected, GigabitEthernet0/0



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

Gateway of last resort is not set

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 is variably subnetted, 3 subnets, 2 masks
R 172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:42, Serial0/0/1
is possibly down, routing via 10.1.1.1, Serial0/0/0
R 172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:26, Serial0/0/0
R 172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:14, Serial0/0/1
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.201.0/24 is directly connected, GigabitEthernet0/0
L 209.165.201.1/32 is directly connected, GigabitEthernet0/0
R2#
```

R1# **show ip route**

<Output Omitted>

Gateway of last resort is not set

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

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

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

R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, 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

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

Gateway of last resort is not set

 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, 4 subnets, 3 masks
R    172.30.0.0/16 [120/2] via 10.1.1.2, 00:00:19, Serial0/0/0
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R    172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:19, Serial0/0/0
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

R 172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1

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

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R 10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:24, Serial0/0/1
C 10.2.2.0/30 is directly connected, Serial0/0/1
D 10.2.2.1/32 is directly connected, Serial0/0/1
R 172.30.0.0/16 is variably subnetted, 4 subnets, 3 masks
R 172.30.0.0/16 is possibly down, routing via 10.2.2.2, Serial0/0/1
R 172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:24, Serial0/0/1
C 172.30.30.0/24 is directly connected, GigabitEthernet0/1
L 172.30.30.1/32 is directly connected, GigabitEthernet0/1
R3#
```

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

**R2# debug ip rip**

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

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

172.30.30.0/24

172.30.10.0/24

```
R2
Physical Config CLI
IOS Command Line Interface
R2#
R2#debug ip rip
RIP protocol debugging is on

R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
172.30.0.0/16 via 0.0.0.0, metric 16, tag 0
172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
```

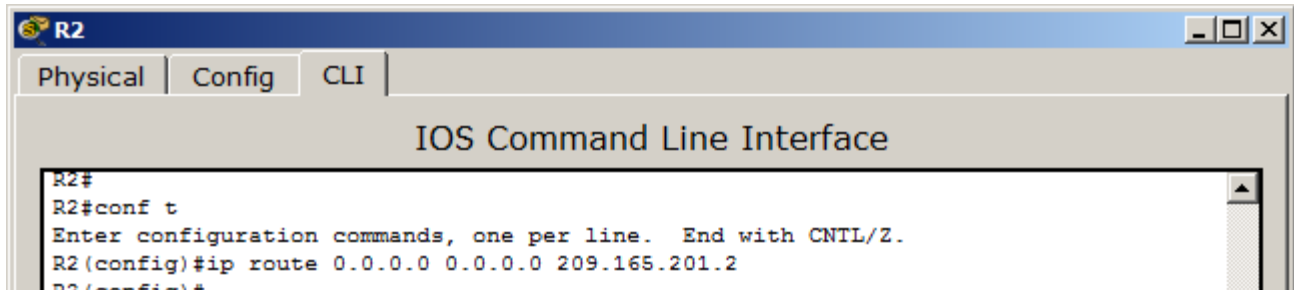
¿Se incluyen ahora las máscaras de las subredes en las actualizaciones de enrutamiento? Sí



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

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

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

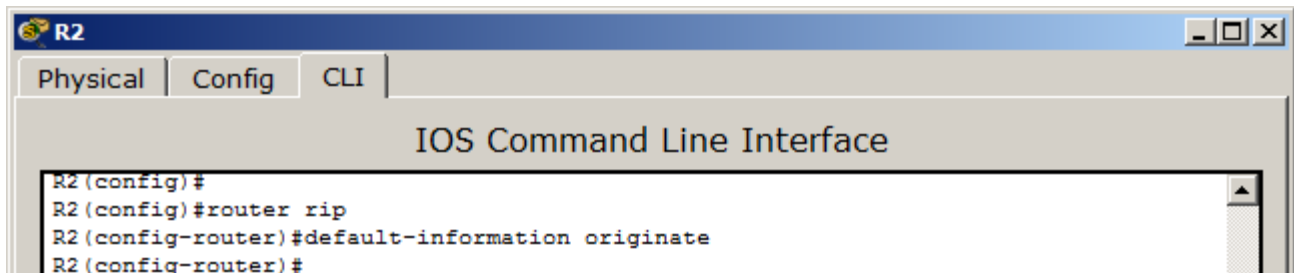


```
R2
Physical | Config | CLI
IOS Command Line Interface
R2#
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#
```

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

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

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



```
R2
Physical | Config | CLI
IOS Command Line Interface
R2(config)#
R2(config)#router rip
R2(config-router)#default-information originate
R2(config-router)#
```

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

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

```
R1# show ip route
```

```
<Output Omitted>
```

```
Gateway of last resort is 10.1.1.2 to network 0.0.0.0
```

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

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

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

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

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

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

```
C 172.30.10.0/24 is directly connected, GigabitEthernet0/1
```

```
L 172.30.10.1/32 is directly connected, GigabitEthernet0/1
```

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

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

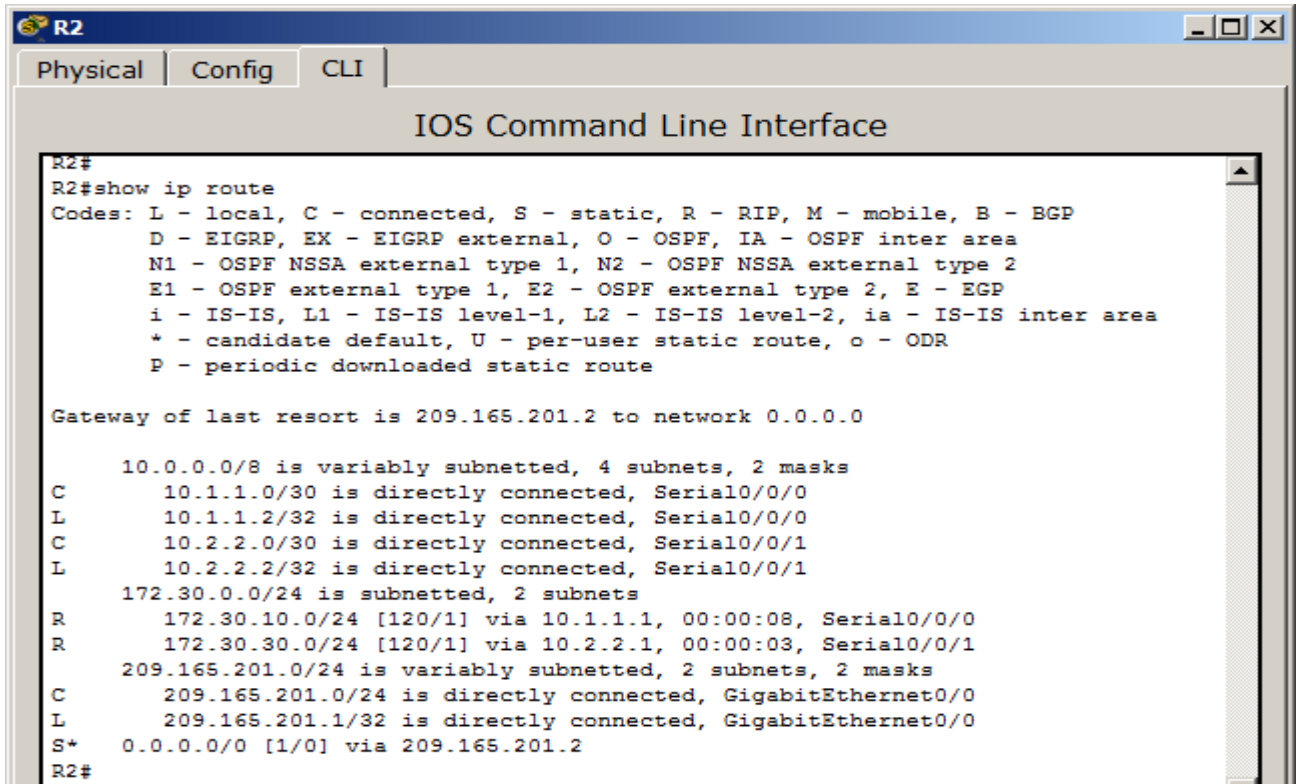
Gateway of last resort is 10.1.1.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, 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
R*     0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0
R1#
```

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

Hay un Gateway de último alcance o puerta de enlace que nos conecta a internet y la ruta por defecto esta vía RIP.

d. Consulte la tabla de routing en el R2.



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

Gateway of last resort is 209.165.201.2 to network 0.0.0.0

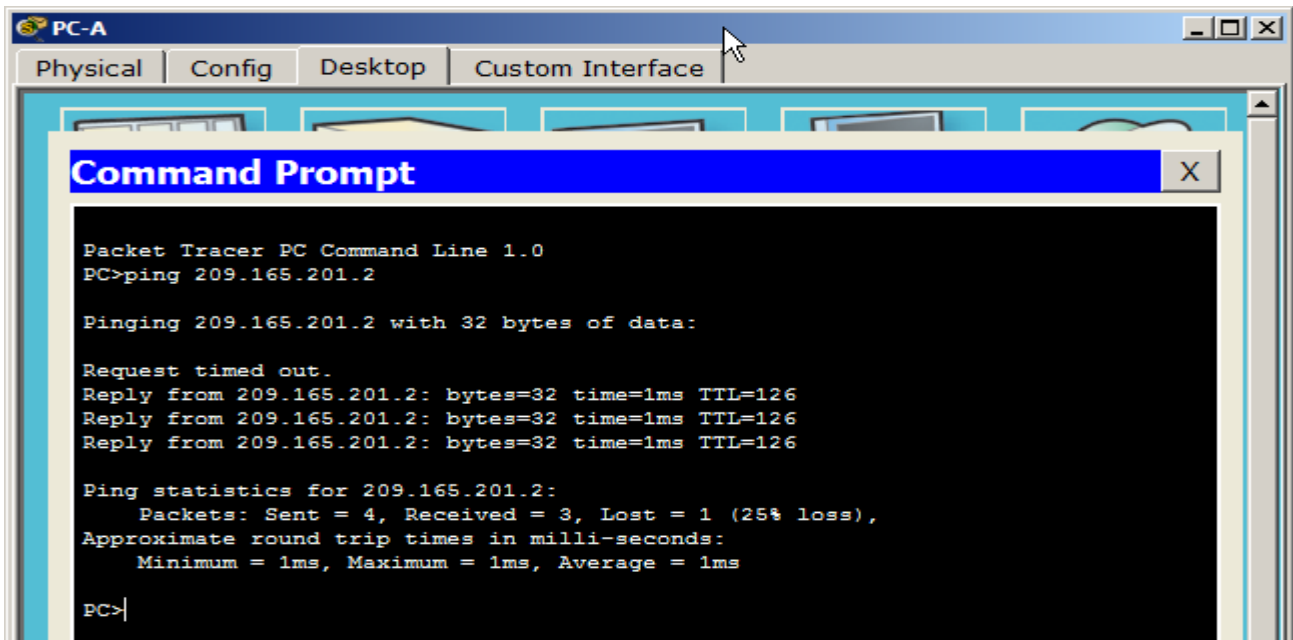
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
   C   10.1.1.0/30 is directly connected, Serial0/0/0
   L   10.1.1.2/32 is directly connected, Serial0/0/0
   C   10.2.2.0/30 is directly connected, Serial0/0/1
   L   10.2.2.2/32 is directly connected, Serial0/0/1
    172.30.0.0/24 is subnetted, 2 subnets
   R   172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:08, Serial0/0/0
   R   172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:03, Serial0/0/1
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
   C   209.165.201.0/24 is directly connected, GigabitEthernet0/0
   L   209.165.201.1/32 is directly connected, GigabitEthernet0/0
   S*  0.0.0.0/0 [1/0] via 209.165.201.2
R2#
```

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

R2 tiene una ruta estática por defecto la ruta 0209.165.201.2 que es conectada a la g0/0.

### Paso 6. Verifique la conectividad.

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



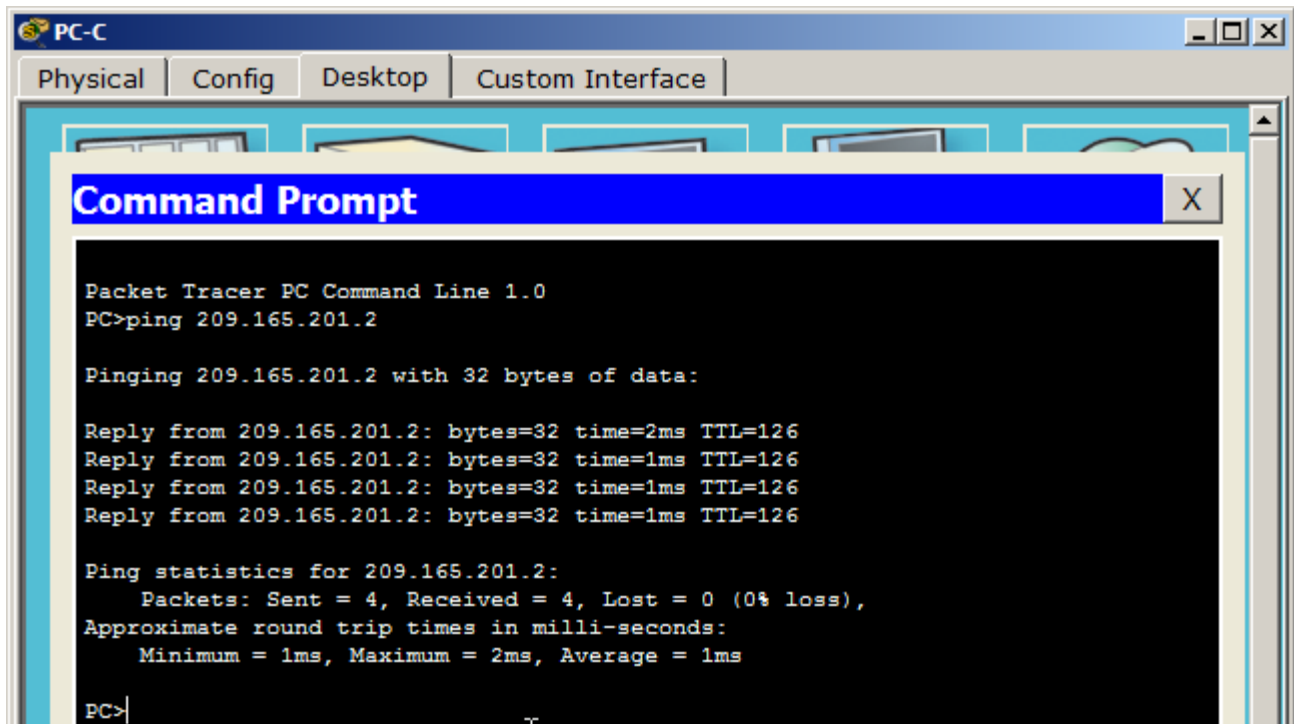
```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Request timed out.
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

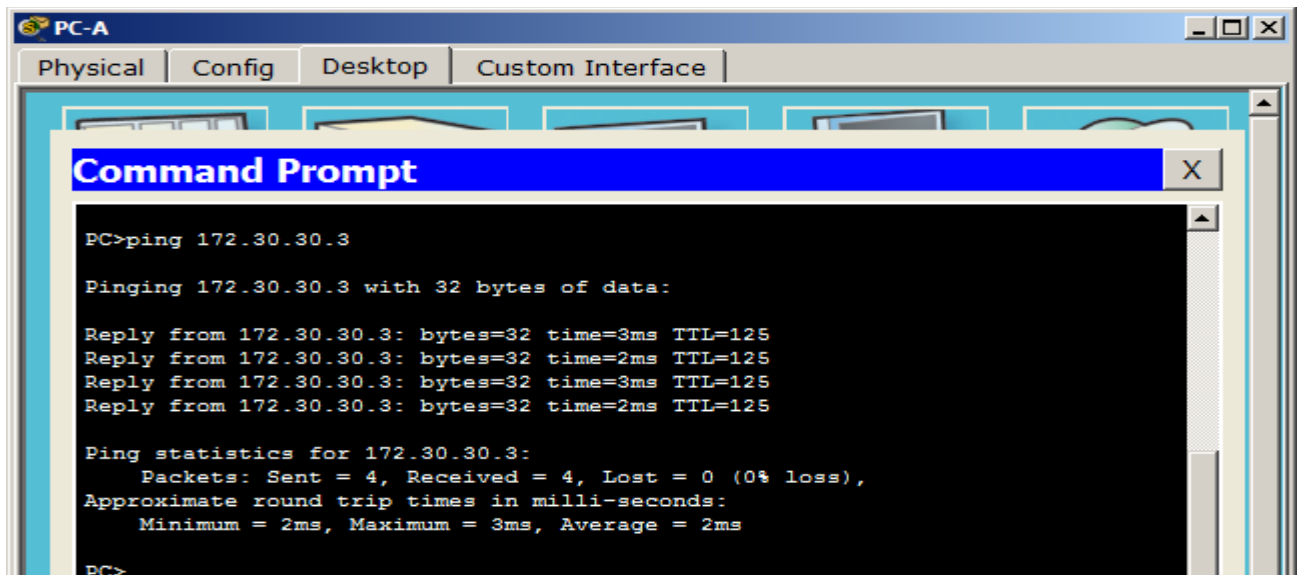
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

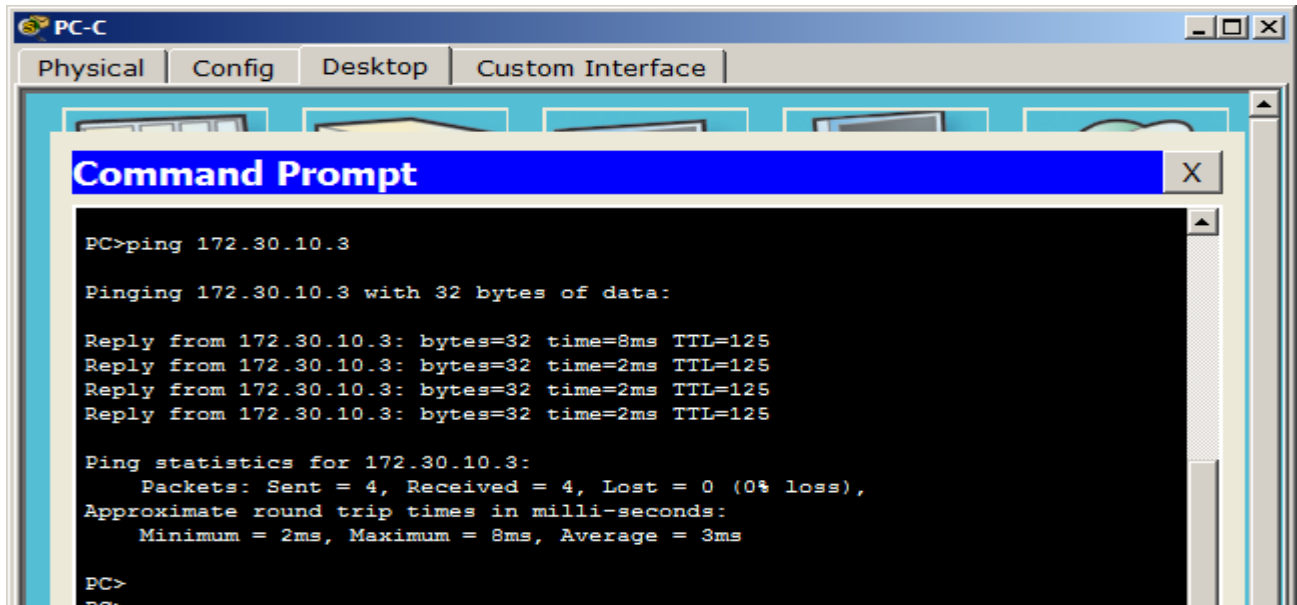
PC>
```



¿Tuvieron éxito los pings? Sí

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





The image shows a screenshot of a PC-C desktop environment. The desktop has tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. A 'Command Prompt' window is open, displaying the following text:

```
PC>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.10.3: bytes=32 time=8ms TTL=125
Reply from 172.30.10.3: bytes=32 time=2ms TTL=125
Reply from 172.30.10.3: bytes=32 time=2ms TTL=125
Reply from 172.30.10.3: bytes=32 time=2ms TTL=125

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 8ms, Average = 3ms

PC>
```

¿Tuvieron éxito los pings? Sí

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

### Parte 3: configurar IPv6 en los dispositivos

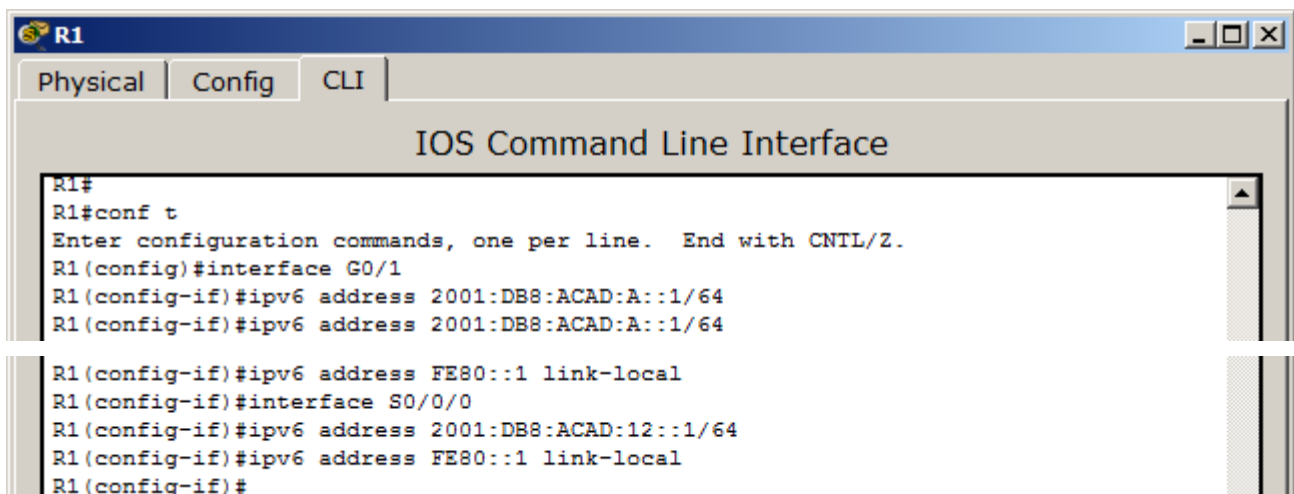
En la parte 3, configurará todas las interfaces con direcciones IPv6 y verificará la conectividad.

## Tabla de direccionamiento

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

### Paso 1. configurar los equipos host.

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



```

R1
Physical Config CLI
IOS Command Line Interface
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface G0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64

R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#interface S0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#
  
```

R2

Physical | Config | CLI

### IOS Command Line Interface

```
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface G0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#interface S0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#interface S0/0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link-local
```

R3

Physical | Config | CLI

### IOS Command Line Interface

```
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface G0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#interface S0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#
```

PC-A

### IPv6 Configuration

DHCP  Auto Config  Static

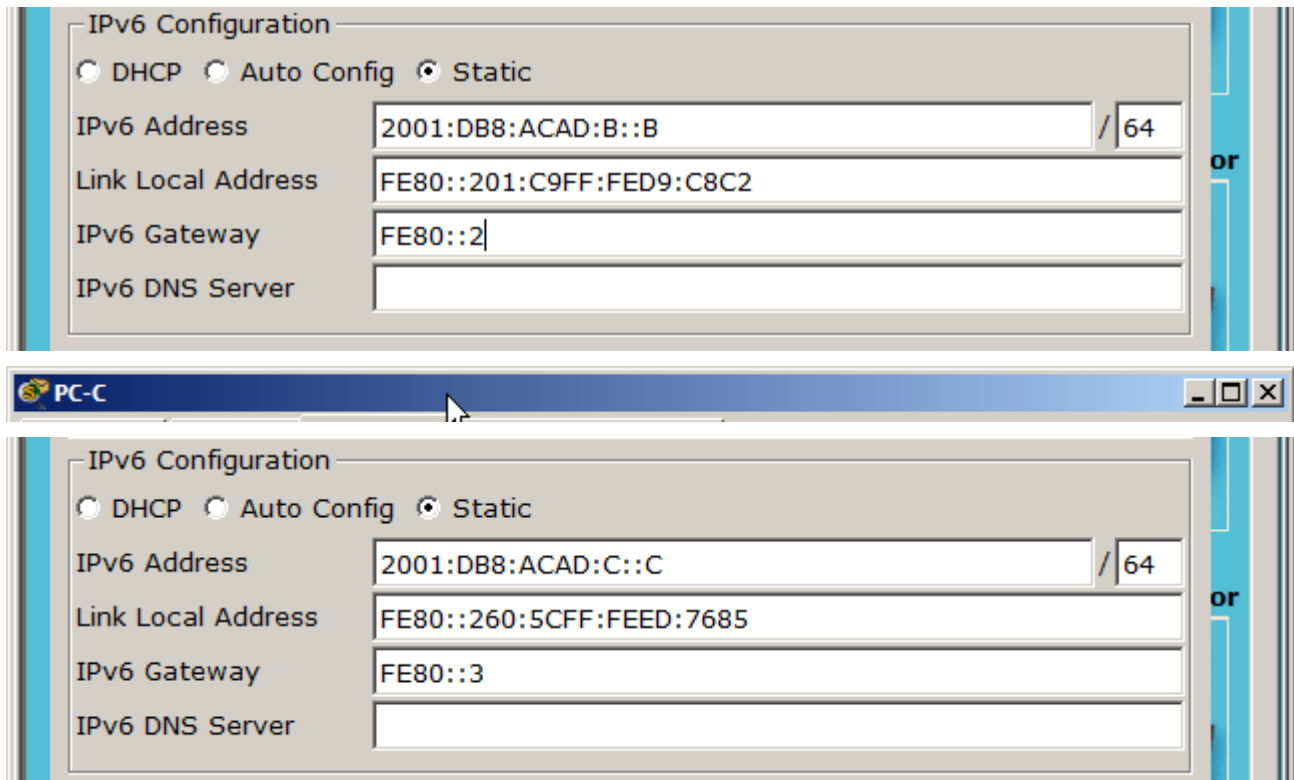
IPv6 Address: 2001:DB8:ACAD:A::A / 64

Link Local Address: FE80::202:4AFF:FE9D:E9B3

IPv6 Gateway: FE80::1

IPv6 DNS Server:

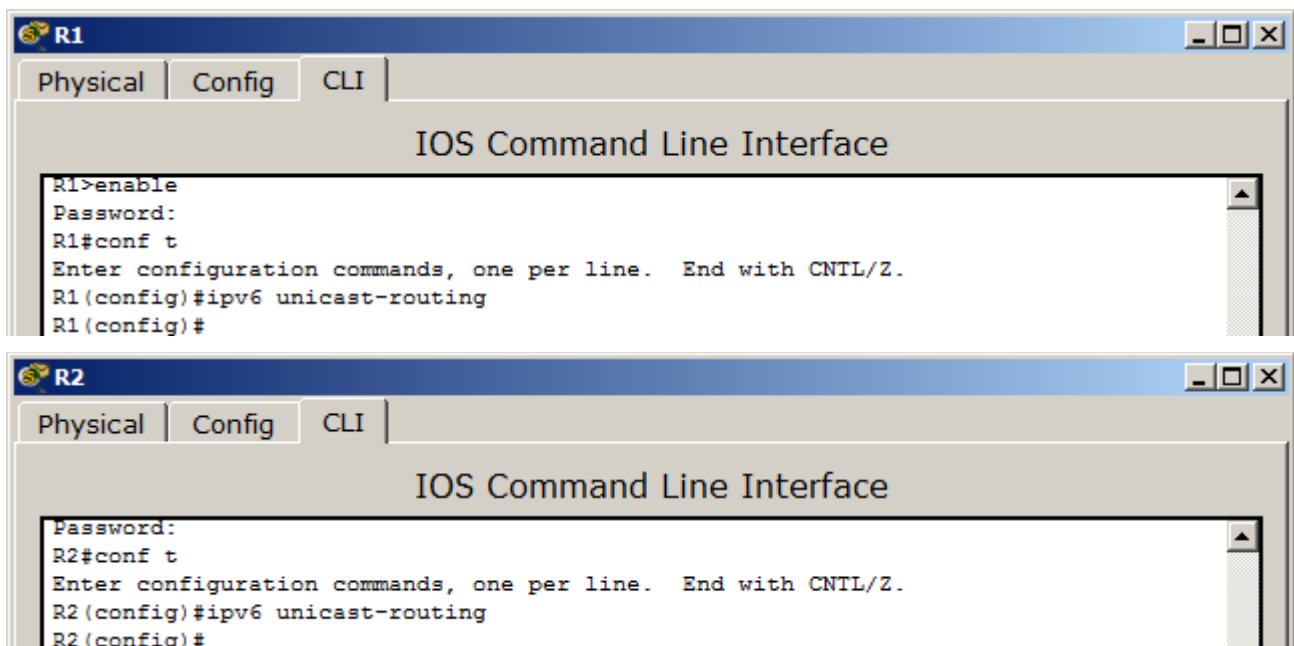
PC-B



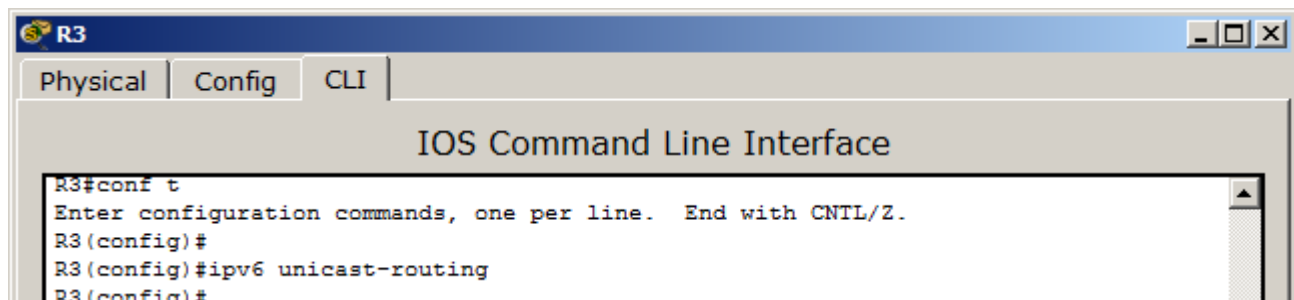
## Paso 2. configurar IPv6 en los routers.

**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.
- Habilite el routing IPv6 en cada router.



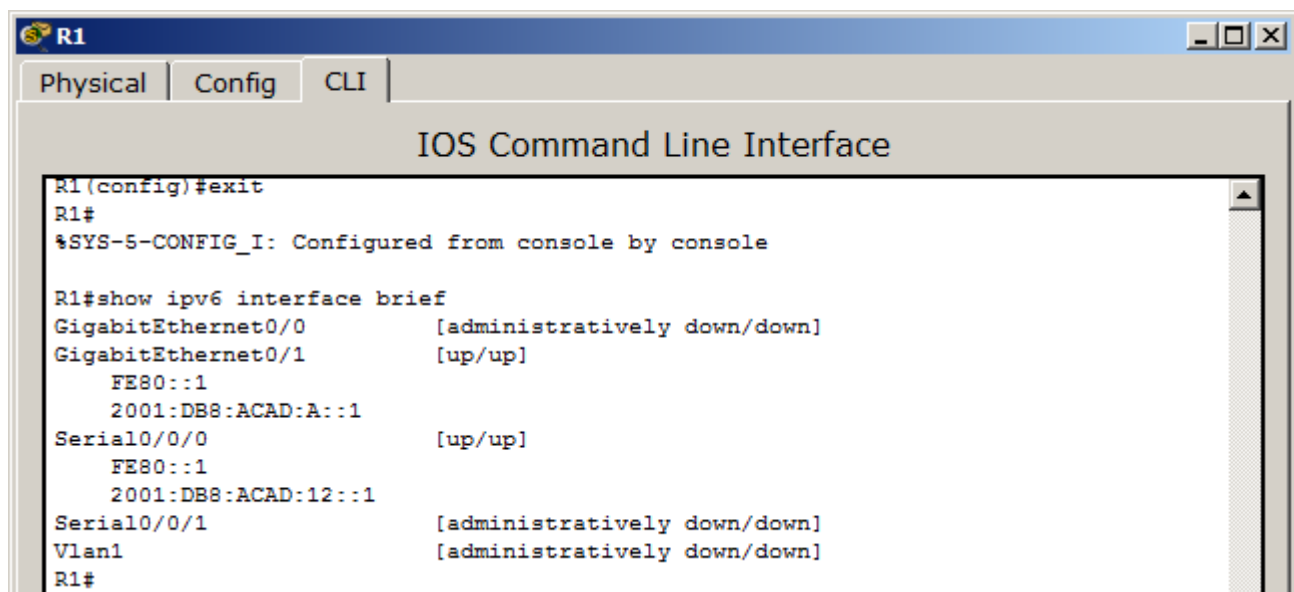




```
R3
Physical Config CLI
IOS Command Line Interface
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#ipv6 unicast-routing
R3(config)#
```

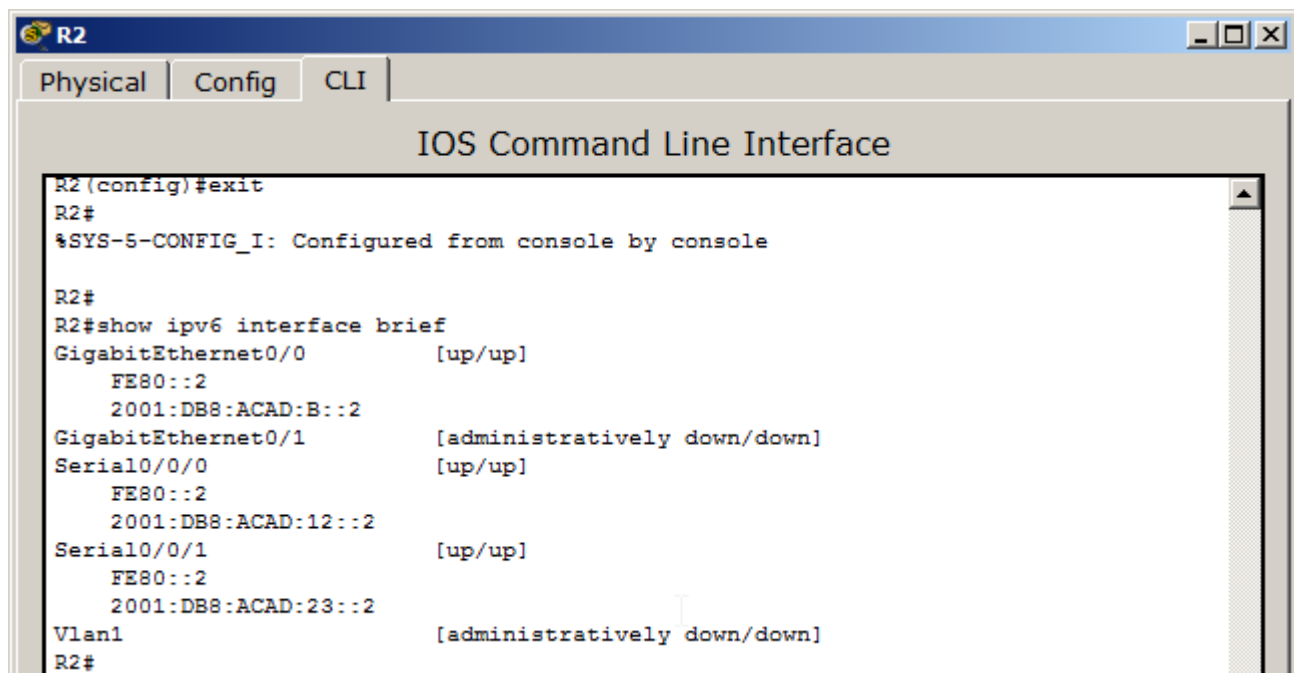
- c. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.

show ipv6 interface brief



```
R1
Physical Config CLI
IOS Command Line Interface
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 interface brief
GigabitEthernet0/0      [administratively down/down]
GigabitEthernet0/1      [up/up]
    FE80::1
    2001:DB8:ACAD:A::1
Serial10/0/0            [up/up]
    FE80::1
    2001:DB8:ACAD:12::1
Serial10/0/1            [administratively down/down]
Vlan1                   [administratively down/down]
R1#
```



```
R2
Physical Config CLI
IOS Command Line Interface
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
R2#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::2
    2001:DB8:ACAD:B::2
GigabitEthernet0/1      [administratively down/down]
Serial10/0/0            [up/up]
    FE80::2
    2001:DB8:ACAD:12::2
Serial10/0/1            [up/up]
    FE80::2
    2001:DB8:ACAD:23::2
Vlan1                   [administratively down/down]
R2#
```

The screenshot shows the CLI of a router named R3. The 'CLI' tab is selected. The command 'show ipv6 interface brief' has been executed, displaying the following output:

```
R3#
R3#show ipv6 interface brief
GigabitEthernet0/0      [administratively down/down]
GigabitEthernet0/1      [up/up]
    FE80::3
    2001:DB8:ACAD:C::3
Serial10/0/0            [administratively down/down]
Serial10/0/1            [up/up]
    FE80::3
    2001:DB8:ACAD:23::3
Vlan1                   [administratively down/down]
R3#
```

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

The screenshot shows the Command Prompt of PC-A. The user has entered the command 'ping 172.30.10.1'. The output shows four successful replies with 0ms round-trip times.

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:

Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

The screenshot shows the Command Prompt of PC-B. The user has entered the command 'ping 209.165.201.1'. The output shows four successful replies with 0ms round-trip times.

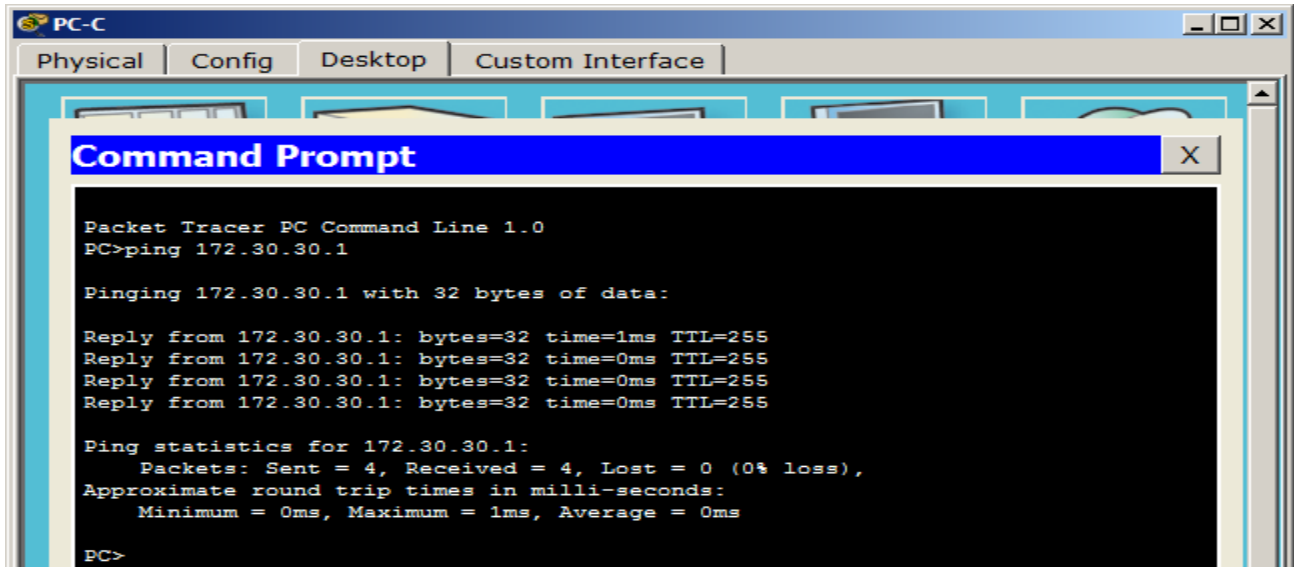
```
PC-B
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

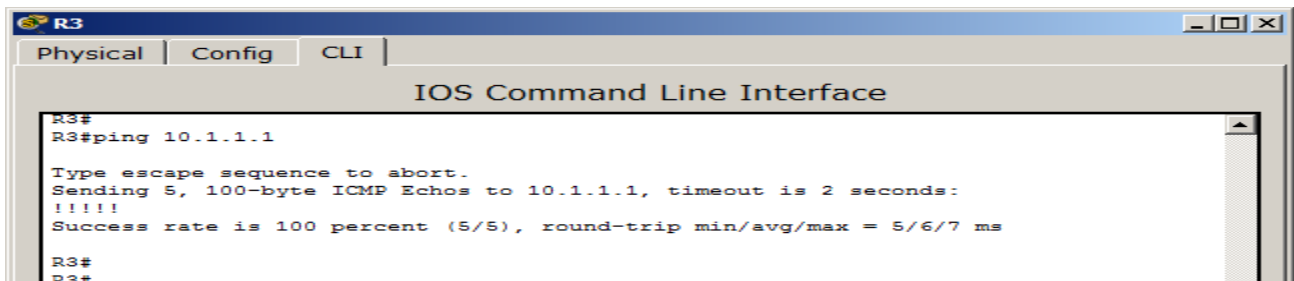
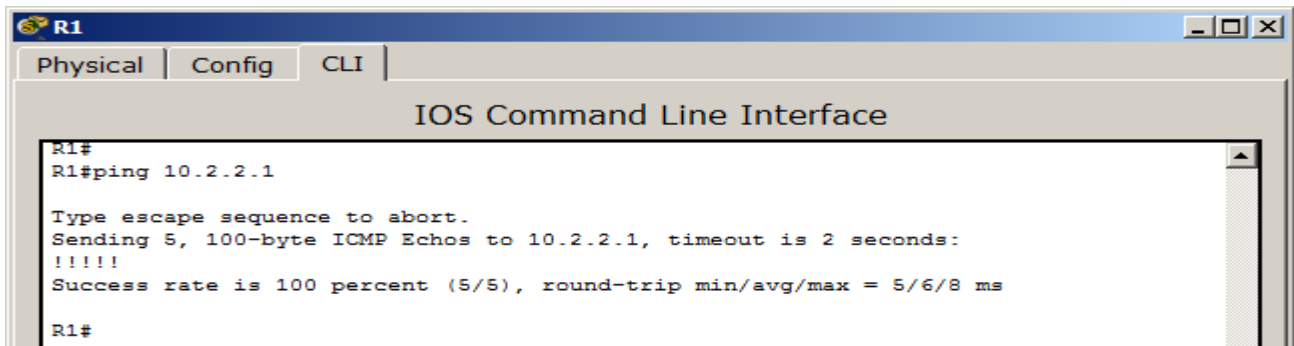
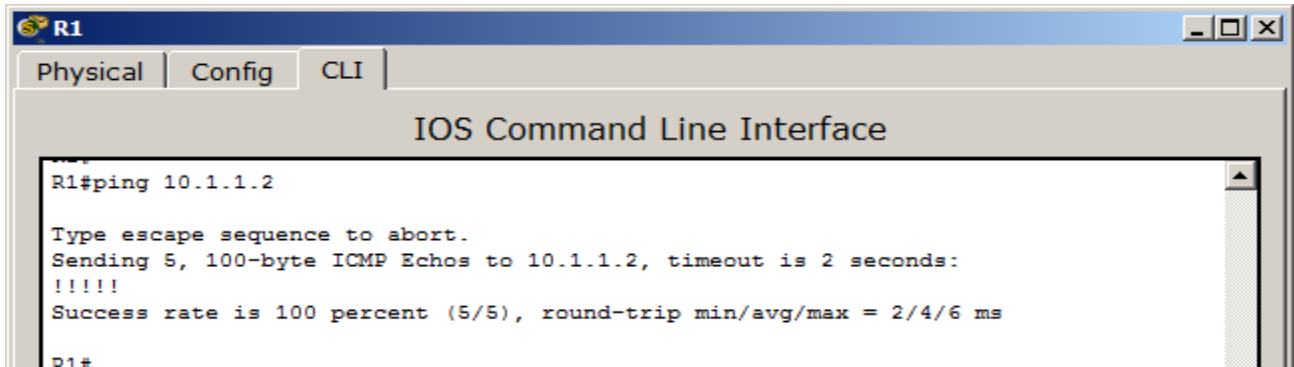
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255

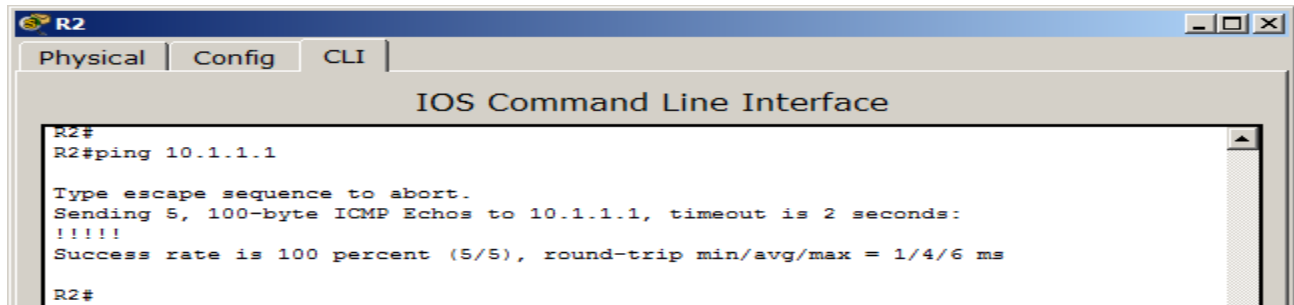
Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```



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





```
R2#
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/6 ms

R2#
```

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

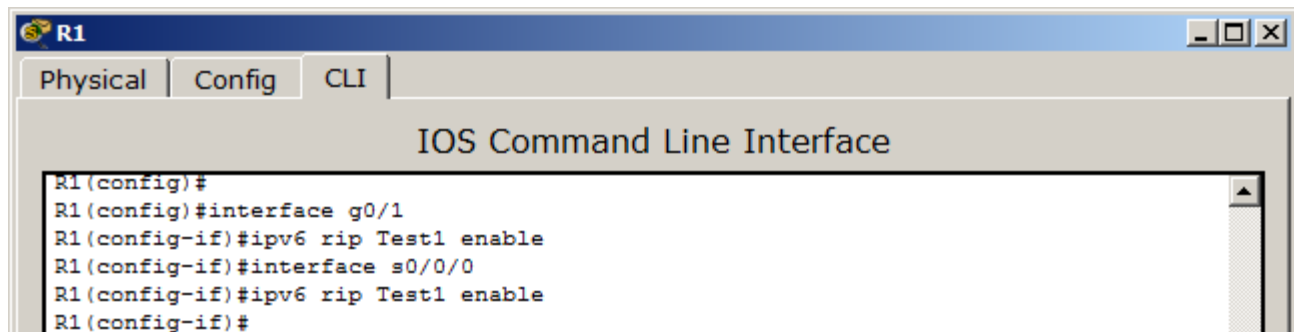
En la parte 4, configurará el routing RIPng en todos los routers, verificará que las tablas de routing estén correctamente actualizadas, configurará y distribuirá una ruta predeterminada, y verificará la conectividad de extremo a extremo.

#### Paso 1. configurar el routing RIPng.

Con IPv6, es común tener varias direcciones IPv6 configuradas en una interfaz. La instrucción `network` se eliminó en RIPng. En cambio, el routing RIPng se habilita en el nivel de la interfaz y se identifica por un nombre de proceso pertinente en el nivel local, ya que se pueden crear varios procesos con RIPng.

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

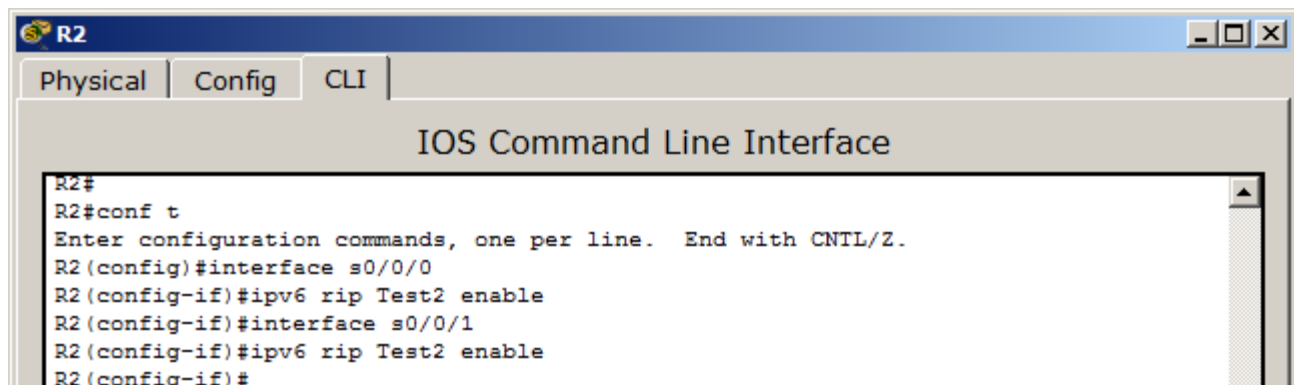
```
R1(config)# interface g0/1
R1(config)# ipv6 rip Test1 enable
R1(config)# interface s0/0/0
R1(config)# ipv6 rip Test1 enable
```



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

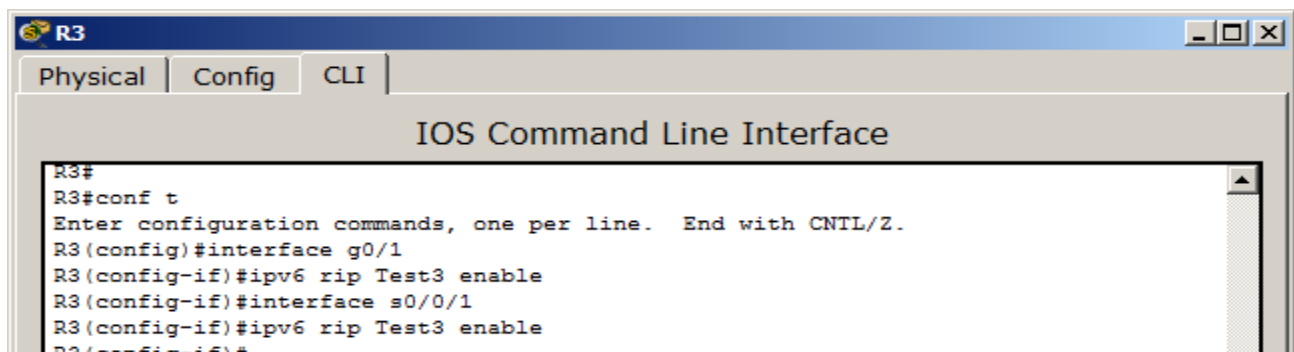
R1(config)#
R1(config)#interface g0/1
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#
```

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

A screenshot of the IOS Command Line Interface for router R2. The window title is 'R2' and it has tabs for 'Physical', 'Config', and 'CLI'. The CLI shows the following commands and prompts:

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

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

A screenshot of the IOS Command Line Interface for router R3. The window title is 'R3' and it has tabs for 'Physical', 'Config', and 'CLI'. The CLI shows the following commands and prompts:

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

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

```
R1
Physical | Config | CLI
IOS Command Line Interface
R1#
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test1"
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
  Redistribution:
    None
```

```
R2
Physical | Config | CLI
IOS Command Line Interface
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

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

R2#
```

```
R3
Physical | Config | CLI
IOS Command Line Interface
R3#
%SYS-5-CONFIG_I: Configured from console by console

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

¿En qué forma se indica RIPng en el resultado?

RIPng esta listado por el nombre del proceso.

- 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

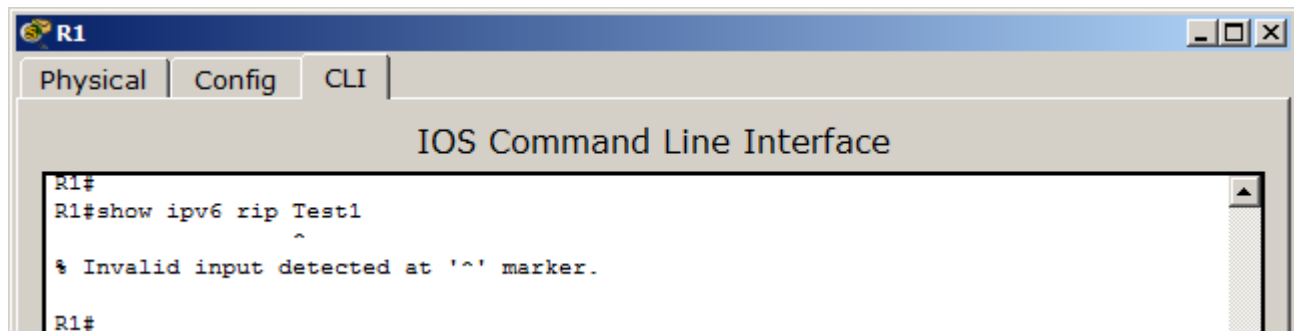
Interfaces:

GigabitEthernet0/1

Serial0/0/0

Redistribution:

None



```
R1#
R1#show ipv6 rip Test1
^
% Invalid input detected at '^' marker.
R1#
```

¿Cuáles son las similitudes entre RIPv2 y RIPv6?

Ambas tienen la distancia administrativa de 120, usan el conteo de saltos como la métrica y envían actualizaciones cada 30 segundos.

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

show ipv6 route

En el R1, ¿cuántas rutas se descubrieron mediante RIPv6? 2

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

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



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

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

The screenshot shows the CLI of router R3. The user has entered the command 'show ipv6 route'. The output displays the IPv6 routing table with 7 entries. The routes are: 2001:DB8:ACAD:A::/64 (RIP), 2001:DB8:ACAD:C::/64 (Connected), 2001:DB8:ACAD:C::3/128 (Local), 2001:DB8:ACAD:12::/64 (RIP), 2001:DB8:ACAD:23::/64 (Connected), 2001:DB8:ACAD:23::3/128 (Local), and FF00::/8 (Local). The legend indicates that R stands for RIP, C for Connected, L for Local, S for Static, and B for BGP.

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

- g. Verifique la conectividad entre las computadoras.  
¿Es posible hacer ping de la PC-A a la PC-B? No

The screenshot shows the Command Prompt on PC-A. The user has entered the command 'ping 2001:DB8:ACAD:B::B/64', which failed with the message 'Ping request could not find host 2001:DB8:ACAD:B::B/64. Please check the name and try again.' The user then entered 'ping 2001:DB8:ACAD:B::B', which also failed. The output shows 'Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:' followed by four 'Destination host unreachable' replies. The ping statistics show 'Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)'.

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>
PC>ping 2001:DB8:ACAD:B::B/64
Ping request could not find host 2001:DB8:ACAD:B::B/64. Please check the name
and try again.
PC>ping 2001:DB8:ACAD:B::B

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

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

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

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

The screenshot shows a Windows-style window titled "PC-A" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". A "Command Prompt" window is open, displaying the following text:

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

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

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

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

PC>
```

¿Es posible hacer ping de la PC-C a la PC-B? No

The screenshot shows a Windows-style window titled "PC-C" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". A "Command Prompt" window is open, displaying the following text:

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

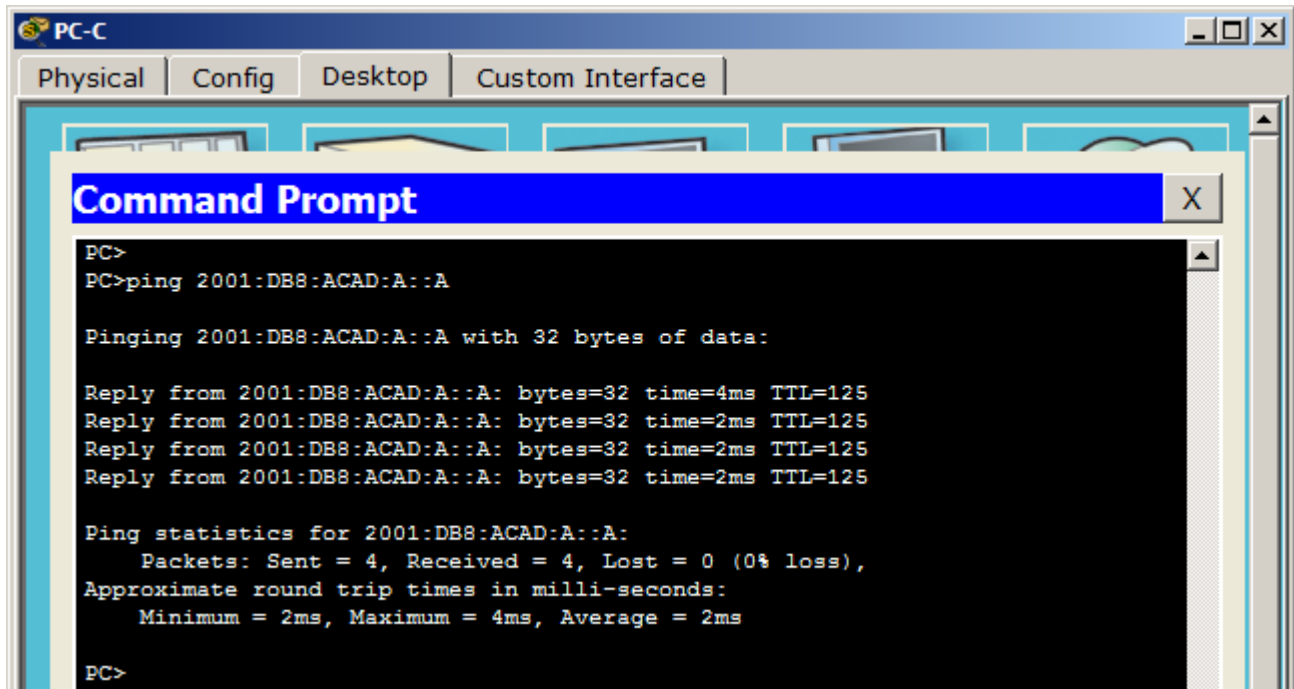
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

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

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

PC>
```

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



```
PC-C
Physical Config Desktop Custom Interface

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

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

Reply from 2001:DB8:ACAD:A::A: bytes=32 time=4ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125

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

PC>
```

¿Por qué algunos pings tuvieron éxito y otros no?

No hay una ruta que se especifique para la PC-B

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

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

ipv6 route ::/0 2001:DB8:ACAD:B::B

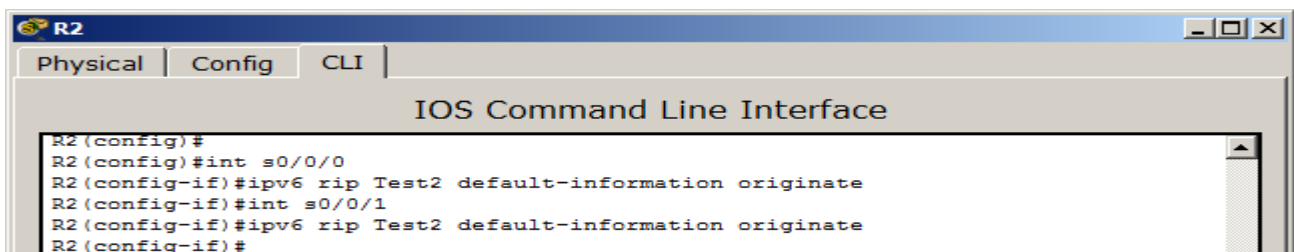
- Las rutas estáticas se pueden incluir en las actualizaciones RIPng mediante el comando **ipv6 rip nombre de proceso default-information originate** en el modo de configuración de interfaz. Configure los enlaces seriales en el R2 para enviar la ruta predeterminada en actualizaciones RIPng.

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

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

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

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



```
R2
Physical Config CLI

IOS Command Line Interface

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

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

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

```
R2# show ipv6 route
```

```
IPv6 Routing Table - 10 entries
```

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

```
U - Per-user Static route, M - MIPv6
```

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

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

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

```
D - EIGRP, EX - EIGRP external
```

```
S ::/64 [1/0]
```

```
via 2001:DB8:ACAD:B::B
```

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

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

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

```
via ::, GigabitEthernet0/1
```

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

```
via ::, GigabitEthernet0/1
```

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

```
via FE80::3, Serial0/0/1
```

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

```
via ::, Serial0/0/0
```

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

```
via ::, Serial0/0/0
```

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

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

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

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

```
L FF00::/8 [0/0]
```

```
via ::, Null0
```

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

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

Tiene una ruta por defecto estática que se muestra en R2.

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

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

La tabla de ruteo se muestra distribuida gracias a RIPng con una métrica de 2.

#### **Paso 4. Verifique la conectividad.**

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

```
PC-A
Physical Config Desktop Custom Interface

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

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

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

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

PC>
```

¿Tuvieron éxito los pings? Sí

## Reflexión

1. ¿Por qué desactivaría la sumarización automática para RIPv2?  
Seria para que los router no resuman las rutas hacia la clase mayor y así poder conectividad entre redes discontinuas.
2. En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3?  
Aprendieron de actualizaciones de RIP recibidas por el router R2 donde se configuro la ruta por defecto.
3. ¿En qué se diferencian la configuración de RIPv2 y la de RIPng?  
RIPng se configura en las interfaces y RIPv2 se configura notificando las redes.

Tabla de resumen de interfaces del router

### Resumen de interfaces del router

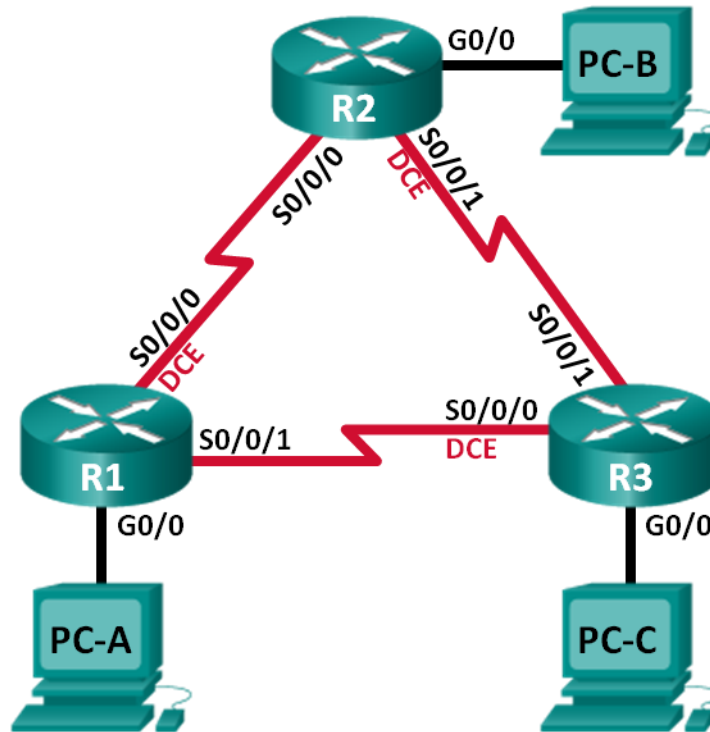
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)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

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



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

#### Topología



## Tabla de direccionamiento

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

## Objetivos

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

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

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

Paso 3: configurar los parámetros básicos para cada Router.

## Parte 2. armar la red y configurar los parámetros básicos de los dispositivos

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

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

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

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

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

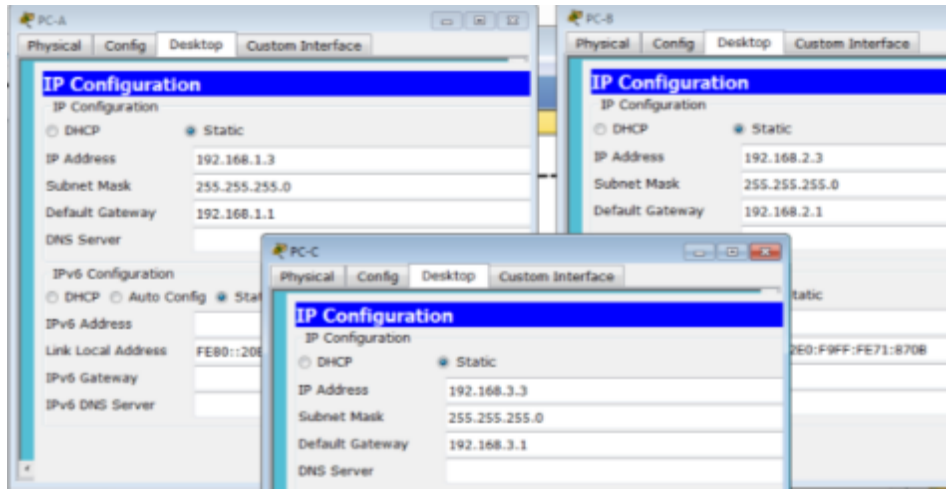
```
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#banner motd % Unauthorized access is strictly prohib:
R1(config)#int g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

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

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

Paso 4: configurar los equipos host.



Paso 5: Probar la conectividad.

```
R1#ping 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

R1#ping 192.168.13.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/22 ms
```

```
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Parte 2: Configurar y verificar el enrutamiento OSPF

Paso 1: Configure el protocolo OSPF en R1.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.3 area 0
R1(config-router)#network 192.168.13.0 0.0.0.3 area 0
R1(config-router)#
```

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

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

```
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, 00:04:09, Serial0/0/0
O   192.168.3.0/24 [110/65] via 192.168.13.2, 00:02:33, 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 192.168.12.1, 00:06:12, Serial0/0/0
```

```
Gateway of last resort is not set

O   192.168.1.0/24 [110/65] via 192.168.12.1, 00:06:12, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.2.0/24 is directly connected, GigabitEthernet0/0
L   192.168.2.1/32 is directly connected, GigabitEthernet0/0
O   192.168.3.0/24 [110/65] via 192.168.23.2, 00:04:20, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.12.0/30 is directly connected, Serial0/0/0
L   192.168.12.2/32 is directly connected, Serial0/0/0
192.168.13.0/30 is subnetted, 1 subnets
O   192.168.13.0/30 [110/128] via 192.168.12.1, 00:04:20, Serial0/0/0
    [110/128] via 192.168.23.2, 00:04:20, Serial0/0/1
192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
```

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

```
Gateway of last resort is not set

O   192.168.1.0/24 [110/65] via 192.168.13.1, 00:04:47, Serial0/0/0
O   192.168.2.0/24 [110/65] via 192.168.23.1, 00:04:26, Serial0/0/1
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.3.0/24 is directly connected, GigabitEthernet0/0
L   192.168.3.1/32 is directly connected, GigabitEthernet0/0
192.168.12.0/30 is subnetted, 1 subnets
O   192.168.12.0/30 [110/128] via 192.168.13.1, 00:04:26, Serial0/0/0
    [110/128] via 192.168.23.1, 00:04:26, Serial0/0/1
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
```

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

Paso 4: verificar la configuración del protocolo OSPF.

El comando show ipprotocols 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.

```
Routing for Networks:
 192.168.3.0 0.0.0.255 area 0
 192.168.13.0 0.0.0.3 area 0
 192.168.23.0 0.0.0.3 area 0
Routing Information Sources:
 Gateway          Distance      Last Update
 192.168.13.1     110          00:09:19
 192.168.23.1     110          00:09:03
 ... ..
```

Paso 5: verificar la información del proceso OSPF.

Use el comando show ipospf 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

```
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 stu
External flood list length 0
Area BACKBONE(0)
  Number of interfaces in this area is 3
  Area has no authentication
  SPF algorithm executed 4 times
  Area ranges are
  Number of LSA 3. Checksum Sum 0x00c59a
  Number of opaque link LSA 0. Checksum Sum 0x
  Number of DCbitless LSA 0
```

Paso 6: verificar la configuración de la interfaz OSPF.

El comando “show ipospf interface brief” no se puede implementar en PacketTracer. Se puede utilizar el comando “show ipospf interface”

Paso 7: Verificar la conectividad de extremo a extremo.

```
Reply from 192.168.1.3: bytes=32 time=1ms TTL=
Reply from 192.168.1.3: bytes=32 time=2ms TTL=

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=
Reply from 192.168.3.3: bytes=32 time=4ms TTL=
Reply from 192.168.3.3: bytes=32 time=1ms TTL=
Reply from 192.168.3.3: bytes=32 time=1ms TTL=

Ping statistics for 192.168.3.3:
```

Parte 3: cambiar las asignaciones de ID del Router

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

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

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

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

Paso 1: Cambie las ID de Router con direcciones de loopback.

```

R2(config)#interface lo0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#end

R3(config)#interface lo0
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R3(config-if)#ip address 3.3.3.3 255.255.255.255
R3(config-if)#end

```

Guarde la configuración en ejecución en la configuración de inicio de todos los Routers.

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

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

```

number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 192.168.1.0 0.0.0.255 area 0
 192.168.12.0 0.0.0.3 area 0
 192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
 Gateway      Distance    Last Update
 1.1.1.1             110        00:01:03
 2.2.2.2             110        00:01:03
 3.3.3.3             110        00:01:03
 192.168.13.1       110        00:13:18

```

Emita el comando show ip ospf neighbor para mostrar los cambios de ID de Router de los Routers vecinos.

```

R1#show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address        Interface
3.3.3.3        0    FULL/ -         00:00:35   192.168.13.2  Serial0/0/1
2.2.2.2        0    FULL/ -         00:00:31   192.168.12.2  Serial0/0/0
R1#

```

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

```

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

```



```

ROUTER ID 11.11.11.11
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 192.168.1.0 0.0.0.255 area 0
 192.168.12.0 0.0.0.3 area 0
 192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
 Gateway      Distance    Last Update
 1.1.1.1      110         00:14:03
 2.2.2.2      110         00:14:03
 3.3.3.3      110         00:00:33
 11.11.11.11  110         00:00:25
 22.22.22.22  110         00:00:25
 33.33.33.33  110         00:00:25
 192.168.13.1 110         00:26:18

```

e. Emita el comando `show ipospfneighbor` en el R1 para verificar que se muestren las nuevas ID de los Routers R2 y R3.

```

R1#show ip ospf neighbor
Neighbor ID   Pri  State           Dead Time   Address      Interface
33.33.33.33   0    FULL/ -         00:00:33   192.168.13.2 Serial0/0/1
22.22.22.22   0    FULL/ -         00:00:39   192.168.12.2 Serial0/0/0
R1#

```

#### Parte 4: configurar las interfaces pasivas de OSPF

Paso 1: configurar una interfaz pasiva.

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

```

NO backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:00
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec

```

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

Vuelva a emitir el comando `show ipospf interface g0/0` para verificar que la interfaz G0/0 ahora sea pasiva

```
GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
```

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

```
1 - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

2.0.0.0/32 is subnetted, 1 subnets
C    2.2.2.2/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:10:19, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, GigabitEthernet0/0
L    192.168.2.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/65] via 192.168.23.2, 00:11:40, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.2/32 is directly connected, Serial0/0/0
192.168.13.0/30 is subnetted, 1 subnets
O    192.168.13.0/30 [110/128] via 192.168.12.1, 00:10:19, Serial0/0/0
110/128] via 192.168.23.2, 00:11:40, Serial0/0/1
```

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

Emita el comando show ipospfneighbor en el R1 para verificar que el R2 aparezca como un vecino OSPF.

```
R1#show ip ospf neighbor

Neighbor ID    Pri   State           Dead Time   Address        Interface
33.33.33.33    0    FULL/ -         00:00:35   192.168.13.2   Serial0/0/1
22.22.22.22    0    FULL/ -         00:00:30   192.168.12.2   Serial0/0/0
```

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

```
R2(config)#router ospf 1
R2(config-router)#passive-interface default
R2(config-router)#
00:33:04: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
00:33:04: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

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

```
R1#show ip ospf neighbor
Neighbor ID   Pri  State           Dead Time   Address      Interface
33.33.33.33   0    FULL/ -         00:00:39   192.168.13.2 Serial0/0/1
R1#
```

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

```
NO backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
```

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

```
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#
00:40:01: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

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

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

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

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

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

¿Qué indica esta información?

La interfaz S0/0/1 en el Router R2 se configuro como interfaz pasiva, por esta razón la información de routing OSPF no se anuncia en esa interfaz. Métrica de costo acumulado para la red 192.168.2.0/24 en el R3 es 129 debido a que el tráfico debe pasar a través de dos enlaces seriales con un costo de 64 cada uno, el enlace LAN Gigabit 0/0 del R2 tiene un costo de uno, lo que da el costo de uno.

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

```
R2#conf t
```

```
R2(config)#Routerospf 1
```

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

Vuelva a emitir el comando show iproute en el R3.

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

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

La métrica de costo acumulado para la red 192.168.2.0/24 en el R3 es 65, el enlace serial tiene un costo 64 y el enlace LAN tiene un costo de 1.

¿El R2 aparece como vecino OSPF del R3? Si

Parte 5: cambiar las métricas de OSPF

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

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

```
R1#show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Hardware is CN Gigabit Ethernet, address is 00e0.b02c.5d01 (bia 00e0.b02c.5d01)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
```

Emita el comando show iprouteospf en el R1 para determinar la ruta a la red 192.168.3.0/24.

```
R1#show ip route ospf
O 192.168.2.0 [110/65] via 192.168.12.2, 00:42:28, Serial0/0/0
O 192.168.3.0 [110/65] via 192.168.13.2, 01:08:08, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
O   192.168.23.0 [110/128] via 192.168.12.2, 00:42:28, Serial0/0/0
                               [110/128] via 192.168.13.2, 00:42:28, Serial0/0/1
R1#
```

Emita el comando show ipospf interface en el R3 para determinar el costo de routing para G0/0.

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
```

Emita el comando show ipospf interface s0/0/1 en el R1 para ver el costo de routing para S0/0/1.

```
no backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:02
Index 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
```

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

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

Vuelva a emitir el comando show ipospf interface para ver el nuevo costo de G0/0 en el R3 y de S0/0/1 en el R1

```
no backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0  Adjacent neighbor count is 0
```

Vuelva a emitir el comando show iprouteospf para ver el nuevo costo acumulado de la ruta 192.168.3.0/24 (10 + 6476 = 6486).

```
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:00
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 33.33.33.33
Suppress hello for 0 neighbor(s)
R1#show ip route ospf
O   192.168.2.0 [110/6576] via 192.168.12.2, 00:05:54, Serial0/0/0
O   192.168.3.0 [110/6576] via 192.168.13.2, 00:05:17, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
```

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

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

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

En la actualidad los equipos admiten cada vez más velocidades de enlaces más rápidas que 100Mb/s que es el valor predeterminado, por lo que para obtener un cálculo más preciso del costo de estos enlaces más rápidos, se necesita una configuración del ancho de banda de referencia predeterminado más alta.

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

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

```
R1#show interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 192.168.12.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output hang never
Type description of "Serial0/0/0" interface
Serial0/0/0
```

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

```
R1#show ip route ospf
O 192.168.2.0 [110/164] via 192.168.12.2, 00:09:46, Serial0/0/0
O 192.168.3.0 [110/164] via 192.168.13.2, 00:09:46, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O   192.168.23.0 [110/6540] via 192.168.12.2, 00:09:46, Serial0/0/0
   [110/6540] via 192.168.13.2, 00:09:46, Serial0/0/1
R1#
```

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

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

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

```
R1#show ip route ospf
O 192.168.2.0 [110/881] via 192.168.12.2, 00:01:30, Serial0/0/0
O 192.168.3.0 [110/164] via 192.168.13.2, 00:13:16, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O   192.168.23.0 [110/6540] via 192.168.13.2, 00:01:30, Serial0/0/1
R1#
```

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

```
R1(config)#interface s0/0/1
R1(config-if)#bandwidth 128
R1(config-if)#
```

Vuelva a emitir el comando show ip route ospf para ver el costo acumulado de ambas rutas a la red 192.168.23.0/24. Observe que otra vez hay dos rutas con el mismo costo (845) a la red 192.168.23.0/24: una a través de S0/0/0 y otra a través de S0/0/1.

```
R1#show ip route ospf
O 192.168.2.0 [110/881] via 192.168.12.2, 00:06:38, Serial0/0/0
O 192.168.3.0 [110/881] via 192.168.13.2, 00:01:20, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0 [110/7257] via 192.168.12.2, 00:01:20, Serial0/0/0
   [110/7257] via 192.168.13.2, 00:01:20, Serial0/0/1
```

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

Costos a la red 192.168.3.0/24: el enlace serial S0/0/1 de R1 tiene un costo de 781 más el costo de la interfaz gigabit de R3 que es de 1 lo que da un costo acumulado de 782.

Costo a la red 192.168.23.0/30: el enlace serial S0/0/1 de R1 tiene un costo de 781 y el enlace serial S0/0/1 de R 3 tiene un costo 64, lo que da un total de 845

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

```
R3#show ip route ospf
O 192.168.1.0 [110/6477] via 192.168.13.1, 00:27:04, Serial0/0/0
O 192.168.2.0 [110/6576] via 192.168.23.1, 00:35:37, Serial0/0/1
  192.168.12.0/30 is subnetted, 1 subnets
O    192.168.12.0 [110/7257] via 192.168.13.1, 00:15:18, Serial0/0/0
```

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

```
R1#show ip route ospf
O 192.168.2.0 [110/881] via 192.168.12.2, 00:26:17, Serial0/0/0
O 192.168.3.0 [110/881] via 192.168.13.2, 00:20:58, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0 [110/7257] via 192.168.12.2, 00:20:58, Serial0/0/0
   [110/7257] via 192.168.13.2, 00:20:58, Serial0/0/1
```

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

El nuevo costo es de 7257

Paso 3: cambiar el costo de la ruta.

Emita el comando show ip route ospf en el R1.

```

R1#show ip route ospf
O   192.168.2.0 [110/881] via 192.168.12.2, 00:29:54, Serial0/0/0
O   192.168.3.0 [110/881] via 192.168.13.2, 00:24:35, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O   192.168.23.0 [110/7257] via 192.168.12.2, 00:24:35, Serial0/0/0
    [110/7257] via 192.168.13.2, 00:24:35, Serial0/0/1
...

```

Aplique el comando `ipospfcost 1565` a la interfaz `S0/0/1` en el R1. Un costo de 1565 es mayor que el costo acumulado de la ruta a través del R2, que es 1562.

Vuelva a emitir el comando `show iprouteospf` en el R1 para mostrar el efecto que produjo este cambio en la tabla de routing. Todas las rutas OSPF para el R1 ahora se enrutan a través del R2.

```

R1#show ip route ospf
O   192.168.2.0 [110/881] via 192.168.12.2, 00:32:49, Serial0/0/0
O   192.168.3.0 [110/1665] via 192.168.13.2, 00:00:37, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets

```

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

El protocolo OSPF elige la ruta con menor costo, en este caso 1665 ya que el costo del enlace serial `S0/0/0` de R1 y el enlace serial `S0/0/1` de R2 tienen un costo de 881 cada uno y el enlace gigabit `G0/0` de R3 tiene un costo de 1.

Reflexión

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

Las asignaciones de ID de Router controlan el proceso de elección de Router designado (DR) y Router designado de respaldo (BDR) en una red de accesos múltiples. Si la ID del Router está asociada a una interfaz activa, puede cambiar si la interfaz deja de funcionar. Por esta razón, se debe establecer con la dirección IP de una interfaz loopback que siempre está activa, o con el comando `Router-id`.

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

Los enlaces seriales utilizados son enlaces punto a punto, así que no se realiza una elección de DR/BDR, ya que el proceso de elección de DR/BDR es solo un problema en una red de accesos múltiples, como Ethernet

¿Por qué querría configurar una interfaz OSPF como pasiva?

Se configuran interfaz como pasivas para no saturar la red con información innecesaria y liberar ancho de banda, los enlaces seriales si deben estar activas para que publiquen la red a sus vecinos.

## 1. CONCLUSIONES DEL EJERCICIO



Se configuro y verifico mediante el comando ping el correcto funcionamiento del protocolo de comunicación OSPF.

El protocolo OSPF elige la ruta con menor costo acumulado. Predeterminadamente OSPF calcula el costo de un enlace con la configuración del ancho de banda, se puede configurar el costo de un enlace con el comando “ipospfcost” y el costo que se le quiera dar al enlace, solo se puede configurar un enlace a la vez.

Se configuran interfaz como pasivas para no saturar la red con información innecesaria y liberar ancho de banda, los enlaces seriales si deben estar activas para que publiquen la red a sus vecinos.

Las asignaciones de ID de Router controlan el proceso de elección de Router designado (DR) y Router designado de respaldo (BDR) en una red de accesos múltiples. Si la ID del Router está asociada a una interfaz activa, puede cambiar si la interfaz deja de funcionar. Por esta razón, se debe establecer con la dirección IP de una interfaz loopback que siempre está activa, o con el comando Router-id.

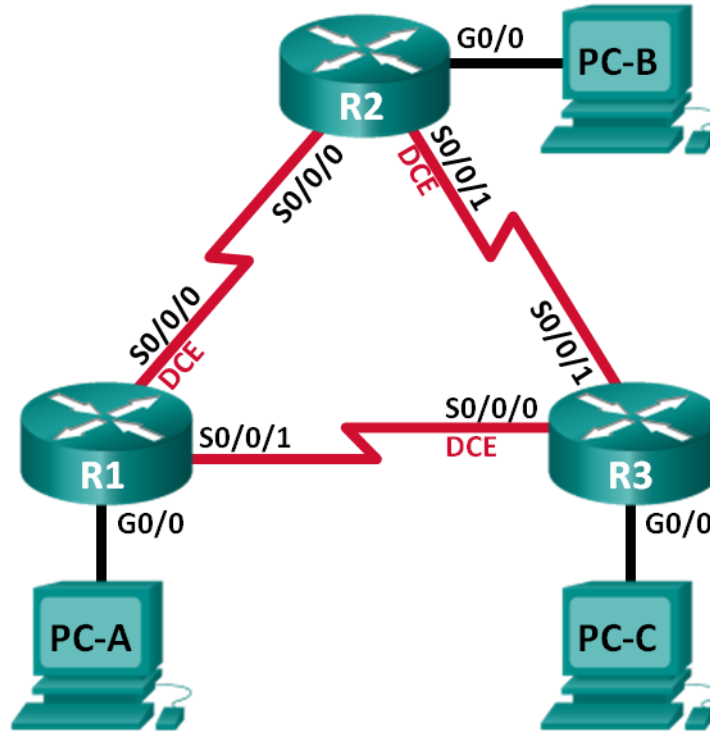
### Tabla de resumen de interfaces del router

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

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

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

#### Topología



## Tabla de direccionamiento

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

## Objetivos

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

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

**Parte 3: configurar interfaces pasivas OSPFv3**

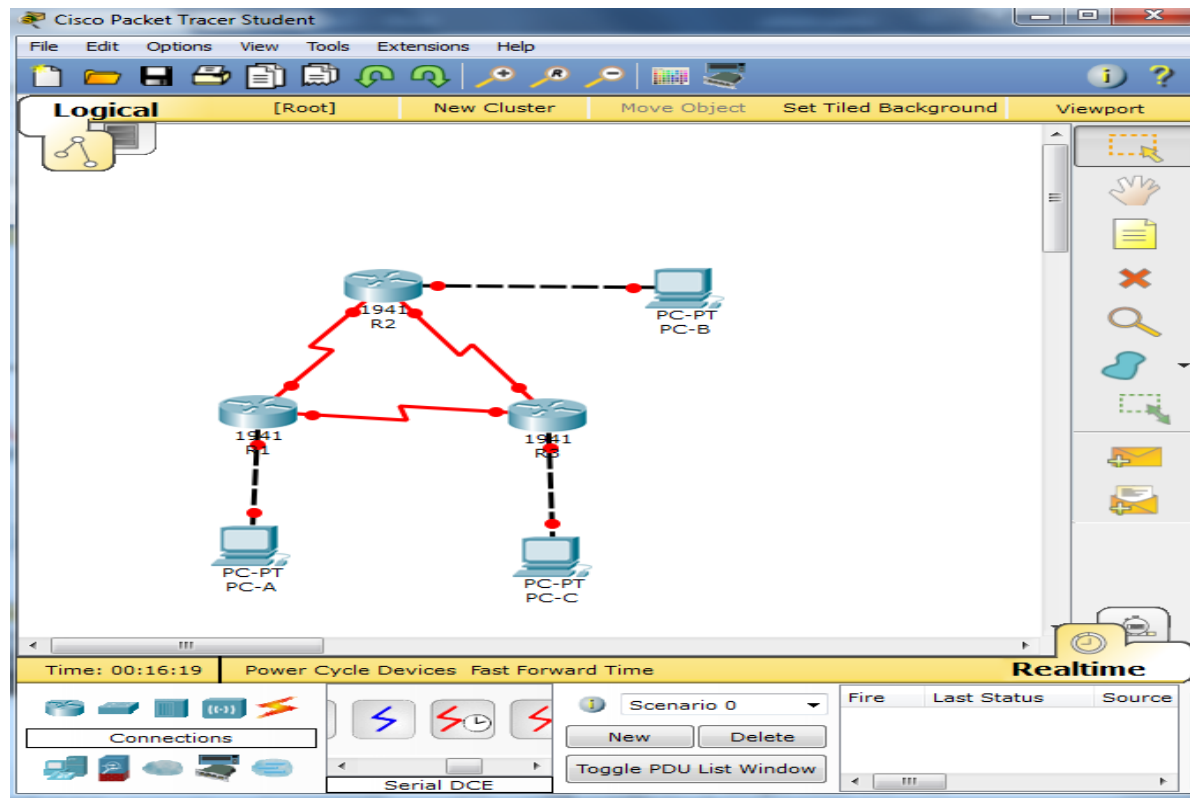
## Recursos necesarios

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

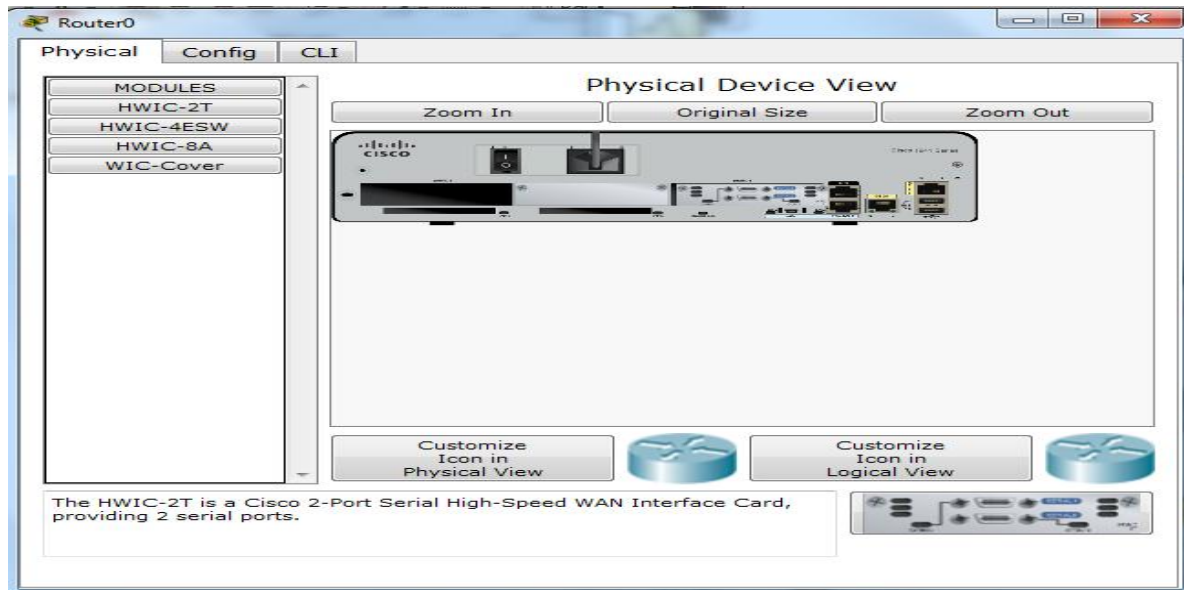
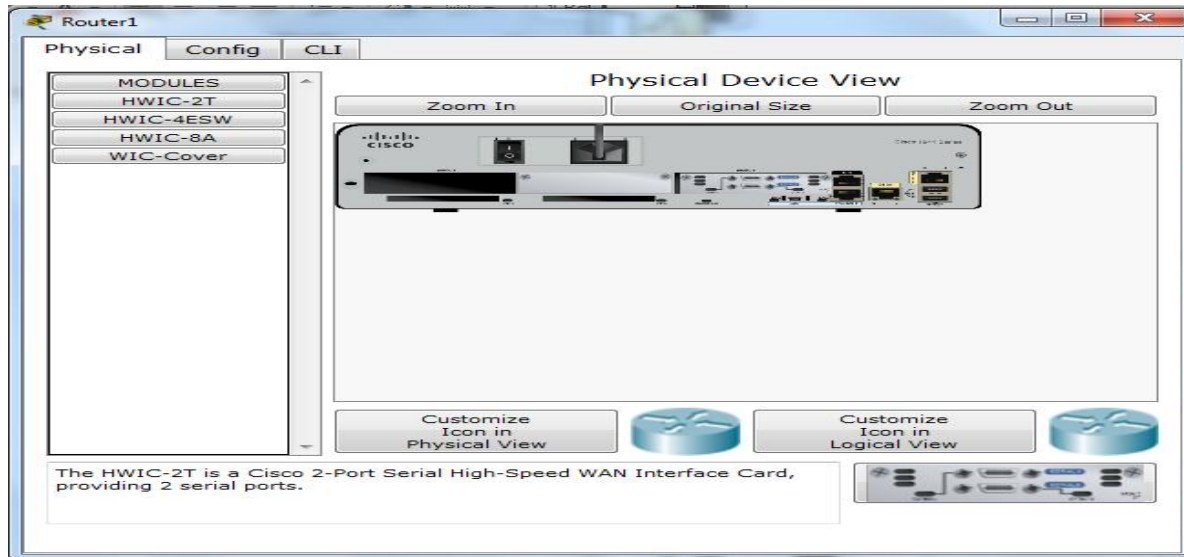
## Armar la red y configurar los parámetros básicos de los dispositivos

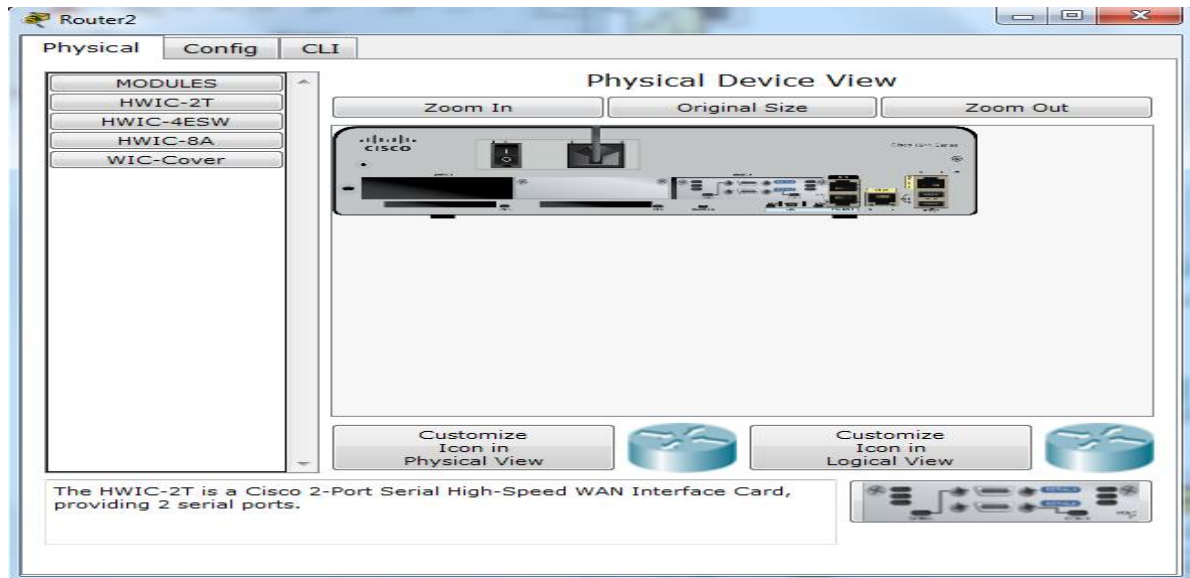
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

### Paso 4. realizar el cableado de red tal como se muestra en la topología.



### Paso 5. inicializar y volver a cargar los routers según sea necesario.





**Paso 6. configurar los parámetros básicos para cada router.**

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de vty.
- e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- f. Configure **logging synchronous** para la línea de consola.
- g. Cifre las contraseñas de texto no cifrado.
- h. Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.
- i. Habilite el routing de unidifusión IPv6 en cada router.
- j. Copie la configuración en ejecución en la configuración de inicio



```
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 5
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#banner motd "warning"
R2(config)#service password-encryption
R2(config)#ipv6 unicast-routing
R2(config)#
R2(config)#interface g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

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

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

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

R2(config-if)#
```

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

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

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

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

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

R2(config-if)#interface serial 0/0/1
R2(config-if)#interface serial 0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

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

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



```
R3
Physical Config CLI
IOS Command Line Interface

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 5
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#banner motd "warning"
R3(config)#service password-encryption
R3(config)#ip v6 unicast-routing
R3(config)#interface g0/0
R3(config-if)#ip v6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ip v6 address FE80::3 link-local
R3(config-if)#no shutdown

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

R3(config-if)#interface serial 0/0/0
R3(config-if)#ip v6 address 2001:DB8:ACAD:13::3/64
R3(config-if)#ip v6 address FE80::3 link-local
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown

R3(config-if)#
```

```
R3
Physical Config CLI
IOS Command Line Interface

R3(config-if)#ip v6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ip v6 address FE80::3 link-local
R3(config-if)#no shutdown

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

R3(config-if)#interface serial 0/0/0
R3(config-if)#ip v6 address 2001:DB8:ACAD:13::3/64
R3(config-if)#ip v6 address FE80::3 link-local
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown

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

R3(config-if)#interface serial 0/0/1
R3(config-if)#ip v6 address FE80::3 link-local
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R3(config-if)#ip v6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ip v6 address FE80::3 link-local
R3(config-if)#no shutdown

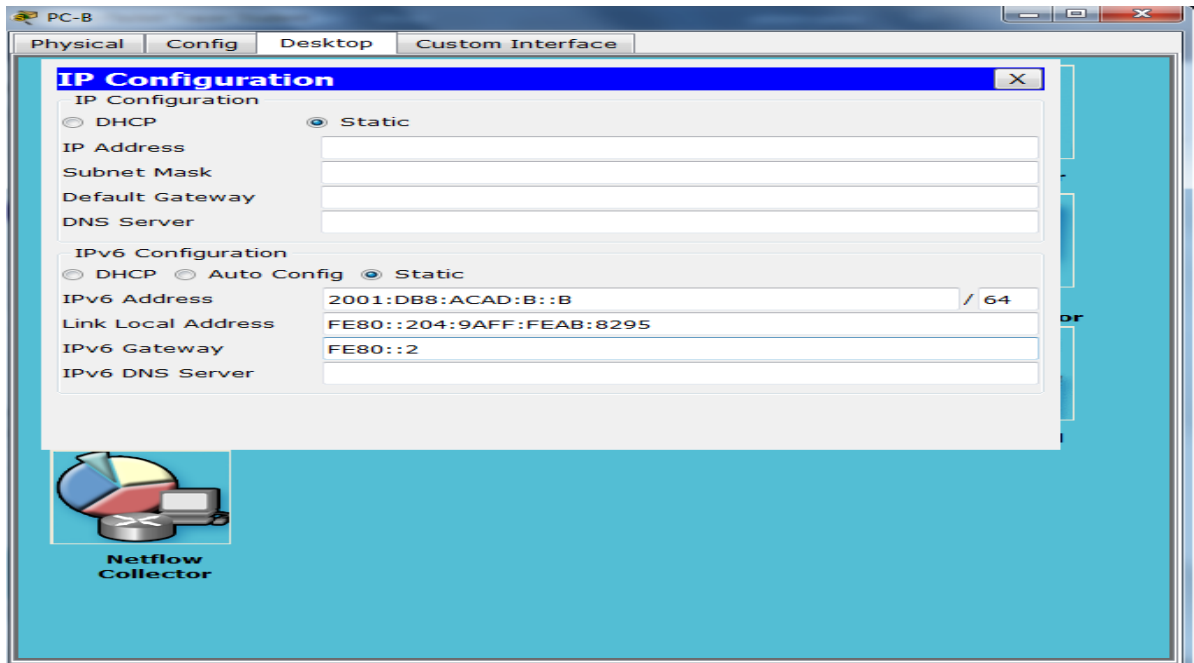
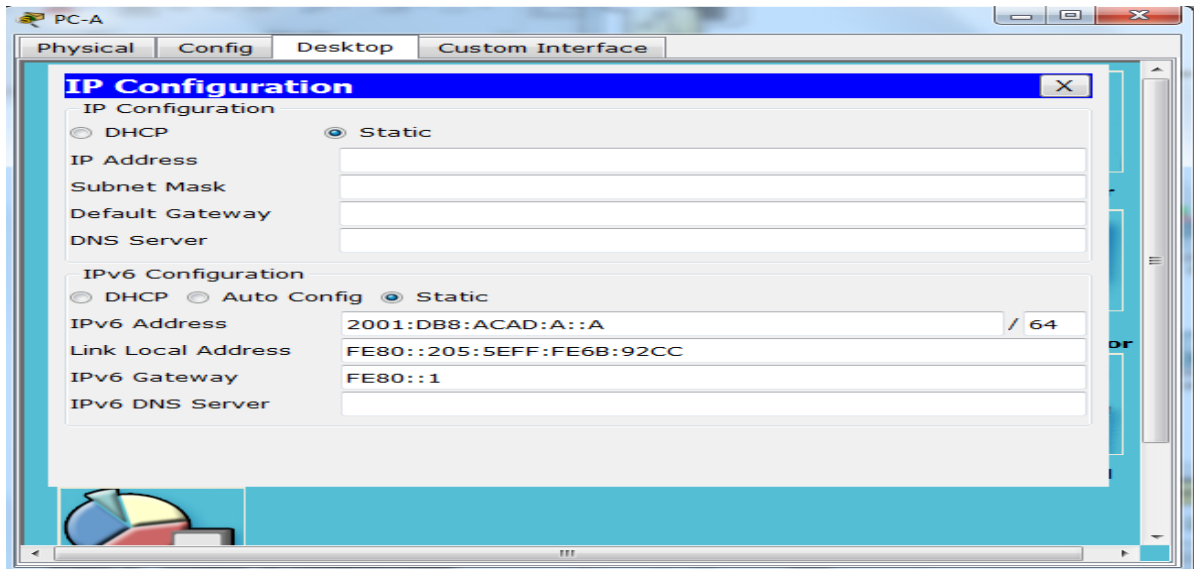
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

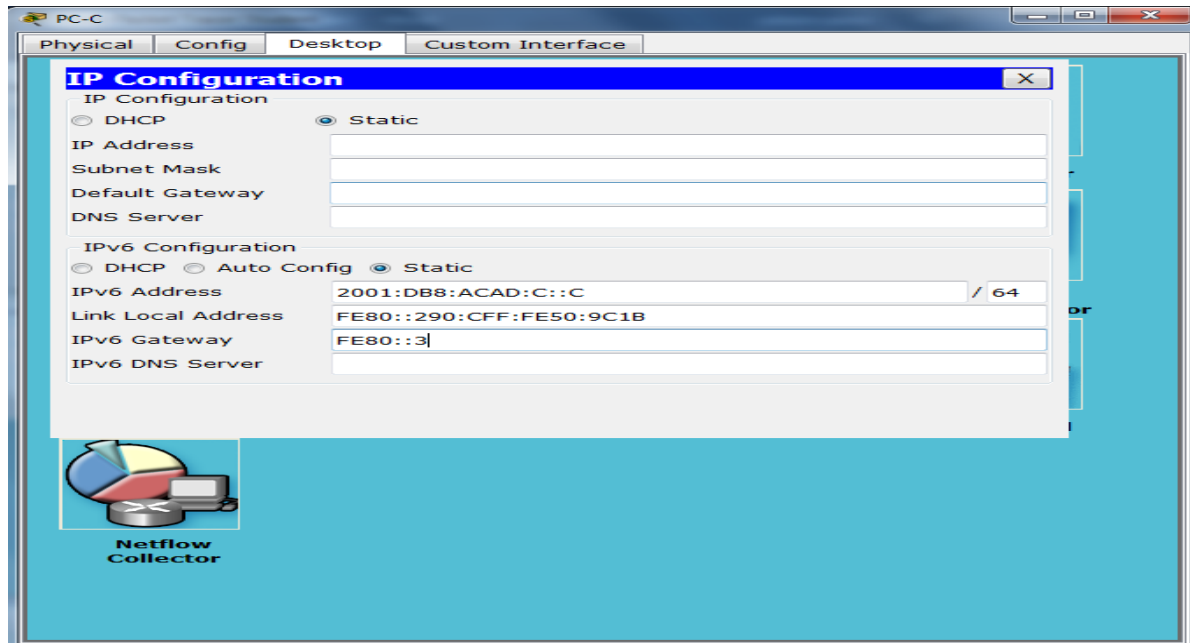
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

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

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

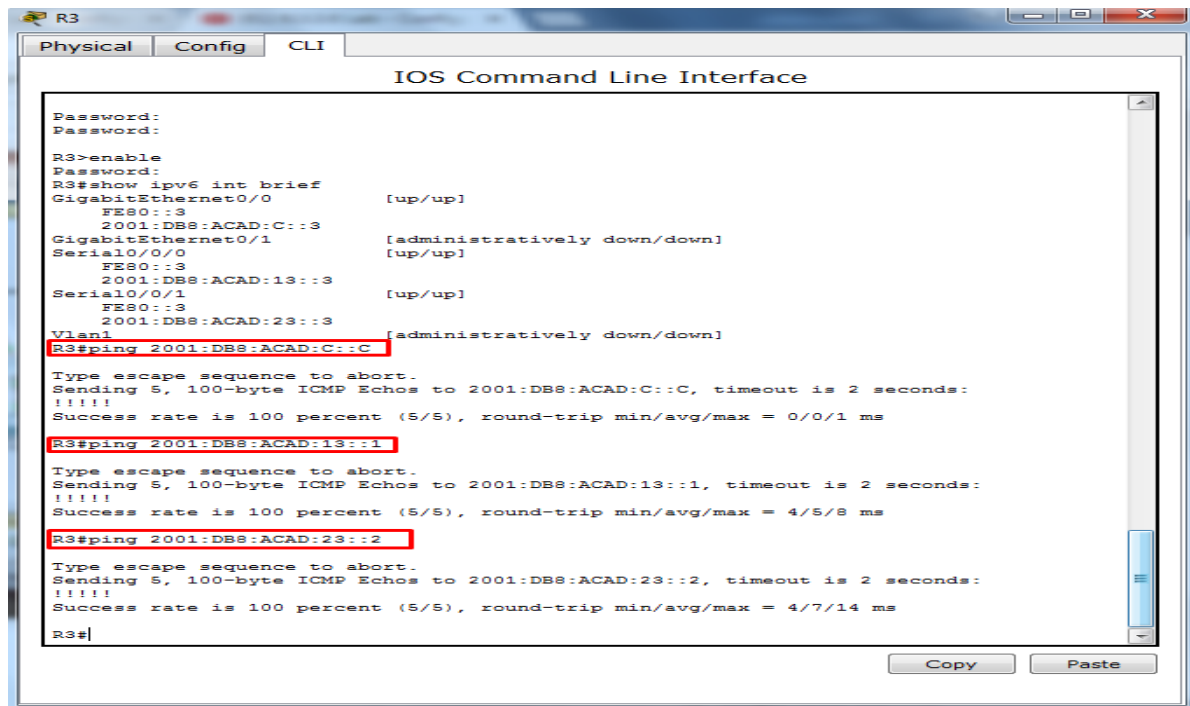
**Paso 7. configurar los equipos host.**

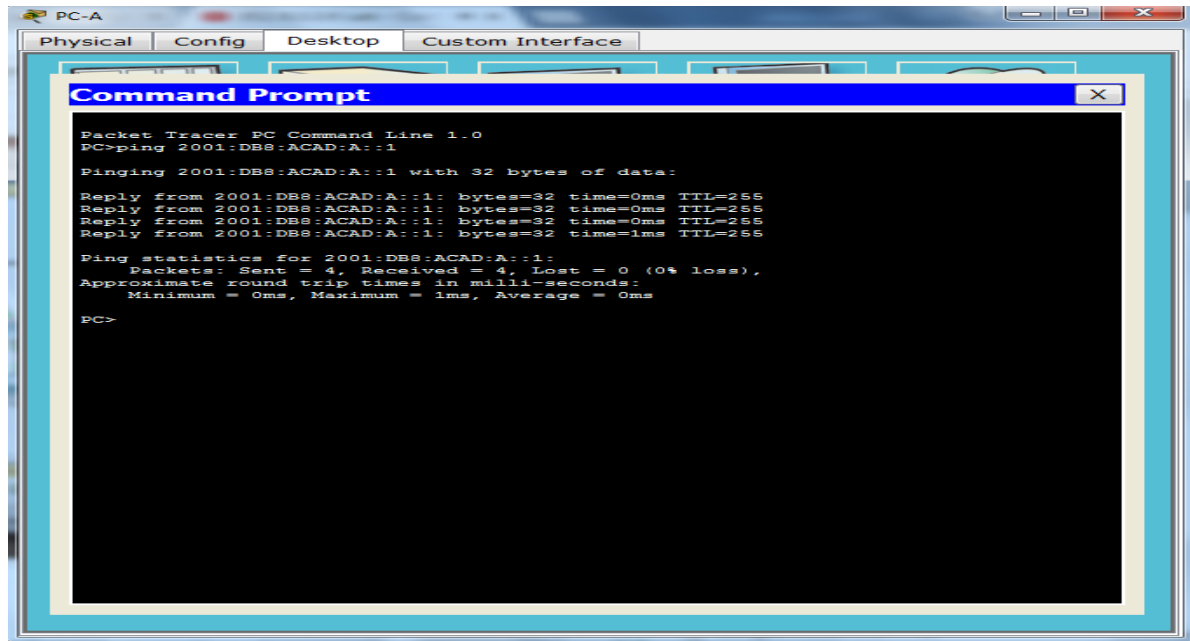




## Paso 8. Probar la conectividad.

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





### Parte 3. configurar el routing OSPFv3

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

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

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

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

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

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

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

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

```
R1
Physical Config CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
warning

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#unicast-routing
^
% Invalid input detected at '^' marker.

R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure
manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

R1#
```

- c. Inicie el proceso de routing de OSPFv3 y asigne la ID de router **2.2.2.2** al R2 y la ID de router **3.3.3.3** al R3.
- d. Emita el comando **show ipv6 ospf** para verificar las ID de router de todos los routers.

R2# **show ipv6 ospf**

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

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

Router is not originating router-LSAs with maximum metric

<Output Omitted>

```
R1
Physical Config CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
warning

User Access Verification

Password:
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#unicast-routing
~
% Invalid input detected at '^' marker.

R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure
manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

R1#
```

```
R2
Physical Config CLI
IOS Command Line Interface

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
warning

User Access Verification

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

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

R2#
```

```

R3
Physical Config CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
warning
User Access Verification
Password:
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 unicas-routing
% Invalid input detected at '^' marker.
R3(config)#ipv6 unicas-routing
% Invalid input detected at '^' marker.
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa

```

## Paso 2. configurar OSPFv6 en el R1.

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

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

```
R1(config)# interface g0/0
```

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

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

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

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

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

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

```
R1
Physical Config CLI
IOS Command Line Interface

Password:
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#unicast-routing
~
% Invalid input detected at '^' marker.

R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R1(config-rttr)#router-id 1.1.1.1
R1(config-rttr)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

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

```
R2
Physical Config CLI
IOS Command Line Interface

User Access Verification

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

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

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/
00:14:20: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
```

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

R1#



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

R1#

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

### Paso 3. verificar vecinos de OSPFv3.

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

R1# **show ipv6 ospf neighbor**

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

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:39	6	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:36	6	Serial0/0/0

```
R3
Physical Config CLI
IOS Command Line Interface
R3(config)#ipv6 unicast-routing
^
% Invalid input detected at '^' marker.
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
00:16:58: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R3(config-if)#
00:17:03: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
R3(config-if)#
```

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

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

R1# **show ipv6 protocols**

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "ospf 1"

Router ID 1.1.1.1

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

Interfaces (Area 0):

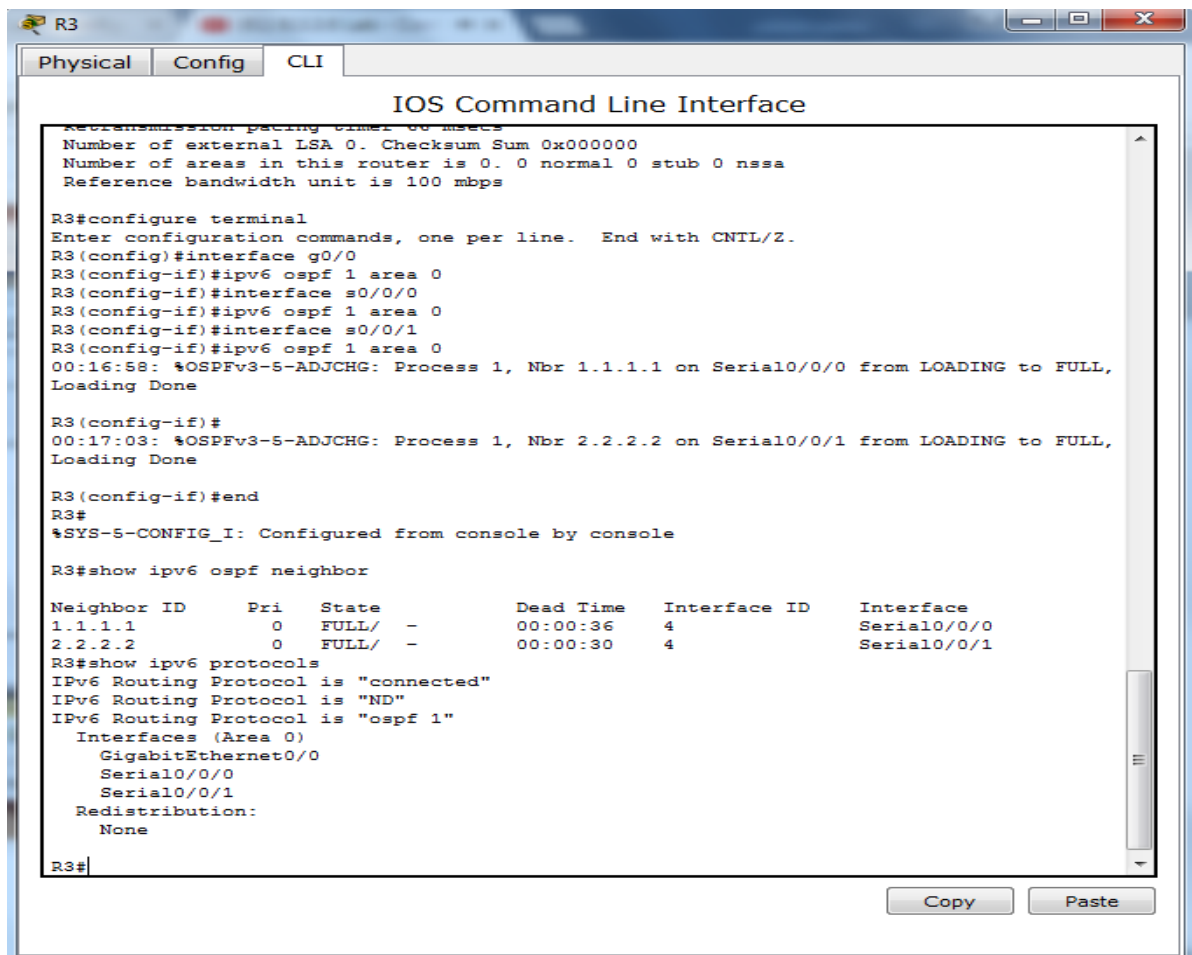
Serial0/0/1

Serial0/0/0

GigabitEthernet0/0

Redistribution:

None



```
R3
Physical Config CLI
IOS Command Line Interface
Retransmission pacing timer 60 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
00:16:58: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done

R3(config-if)#
00:17:03: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL,
Loading Done

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

R3#show ipv6 ospf neighbor

Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:00:36   4             Serial0/0/0
2.2.2.2          0    FULL/ -         00:00:30   4             Serial0/0/1

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

R3#
```

## Paso 5. verificar las interfaces OSPFv3.

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

R1# **show ipv6 ospf interface**

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

Link Local Address FE80::1, Interface ID 7

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

Network Type POINT\_TO\_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT\_TO\_POINT

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

Hello due in 00:00:05

Graceful restart helper support enabled

Index 1/3/3, flood queue length 0

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

Last flood scan length is 1, maximum is 1

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

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 3.3.3.3

Suppress hello for 0 neighbor(s)

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

Link Local Address FE80::1, Interface ID 6

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

Network Type POINT\_TO\_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT\_TO\_POINT

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

Hello due in 00:00:00

Graceful restart helper support enabled

Index 1/2/2, flood queue length 0

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

Last flood scan length is 1, maximum is 2

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

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 2.2.2.2

Suppress hello for 0 neighbor(s)

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

Link Local Address FE80::1, Interface ID 3

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

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

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

No backup designated router on this network

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

Hello due in 00:00:03

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

```
R3#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:00:36   4            Serial0/0/0
2.2.2.2          0    FULL/ -         00:00:30   4            Serial0/0/1
R3#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
R3#show ipv6 ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, local address FE80::3
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::3, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 3.3.3.3
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
--More--
```

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

R1# **show ipv6 ospf interface brief**

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
Se0/0/1	1	0	7	64	P2P	1/1	
Se0/0/0	1	0	6	64	P2P	1/1	
Gi0/0	1	0	3	1	DR	0/0	

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

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

**R2# show ipv6 route**

IPv6 Routing Table - default - 10 entries

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

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

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

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

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

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

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

via FE80::1, Serial0/0/0

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

via GigabitEthernet0/0, directly connected

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

via GigabitEthernet0/0, receive

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

via FE80::3, Serial0/0/1

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

via Serial0/0/0, directly connected

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

via Serial0/0/0, receive

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

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

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

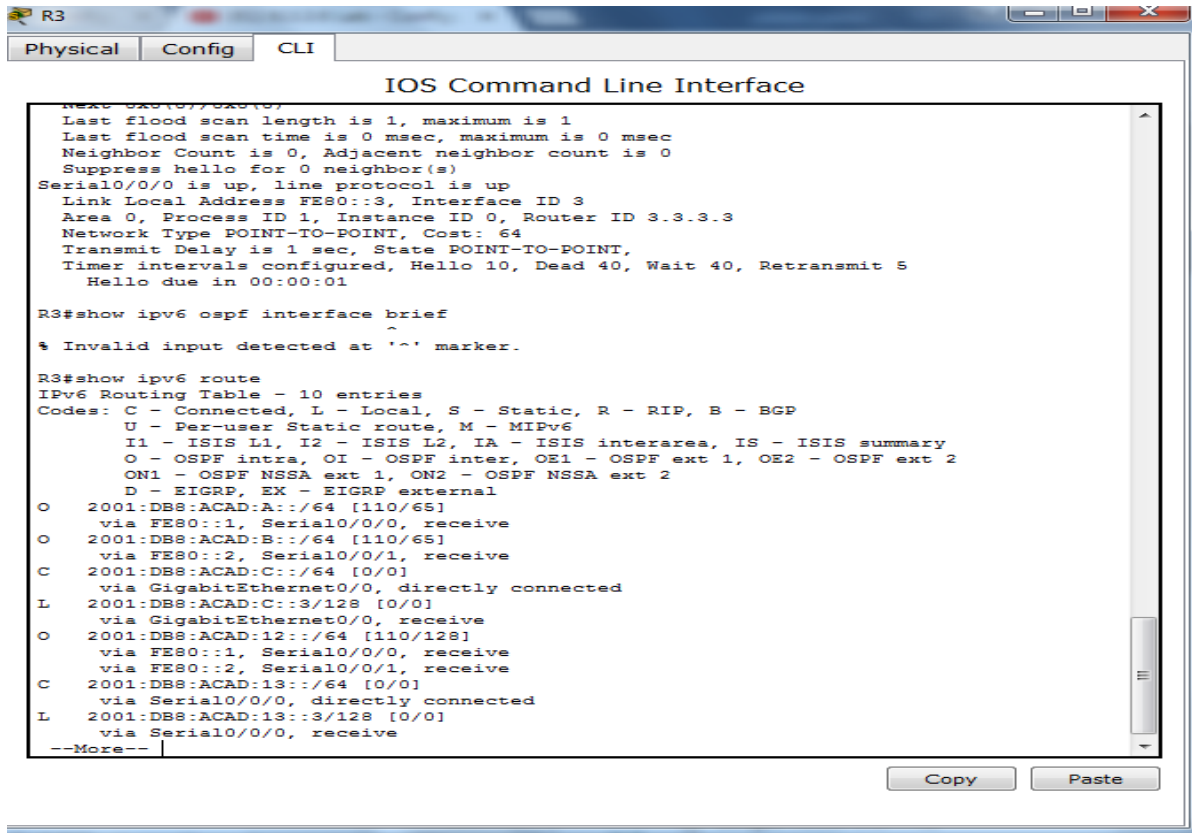
via Serial0/0/1, directly connected

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

via Serial0/0/1, receive

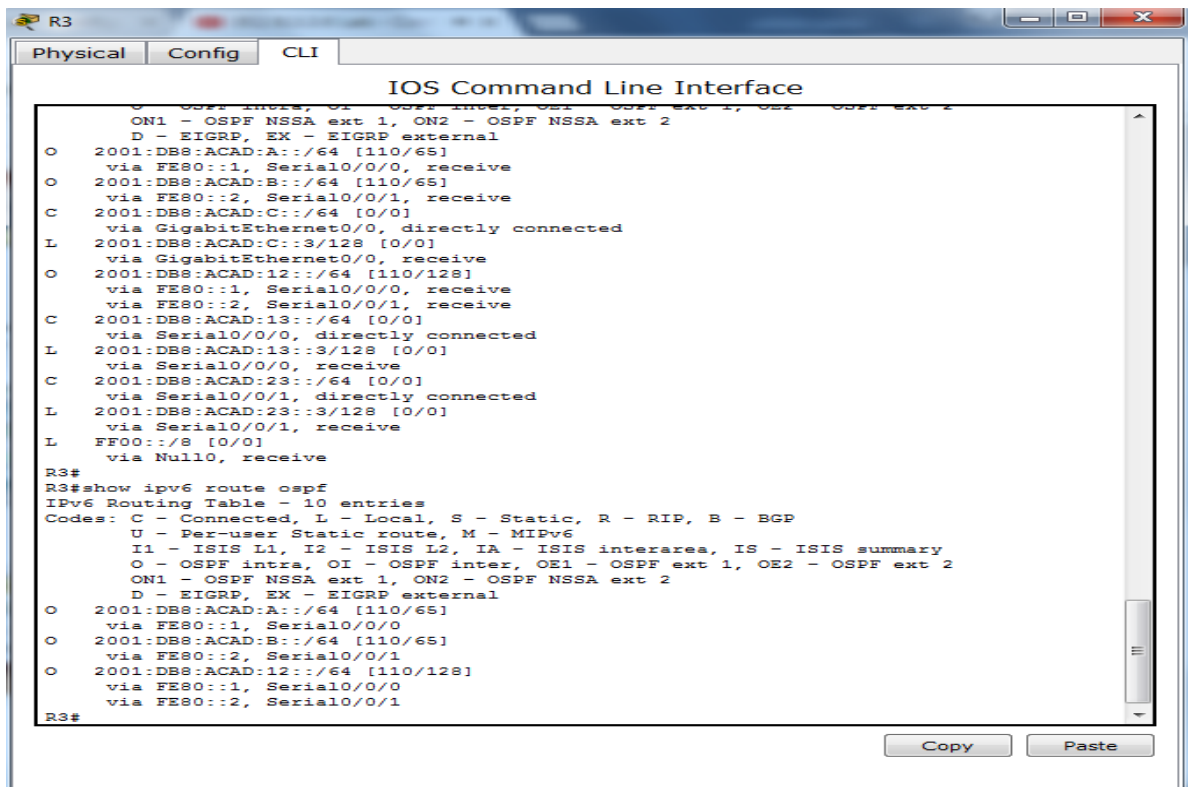
L FF00::/8 [0/0]

via Null0, receive



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

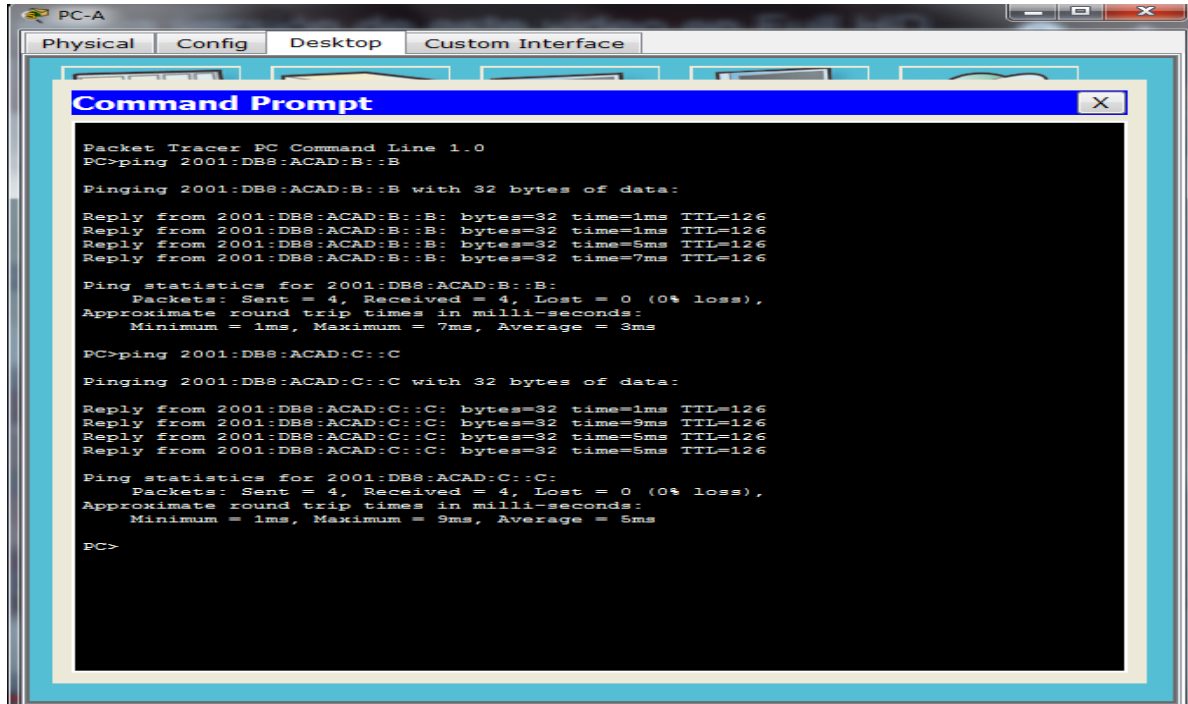
**Show ipv6 route ospf**



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

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

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



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=5ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=7ms TTL=126
Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 3ms
PC>ping 2001:DB8:ACAD:C::C
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=9ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=5ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=5ms TTL=126
Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 9ms, Average = 5ms
PC>
```

## Parte 4. configurar las interfaces pasivas de OSPFv3

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

### Paso 1. configurar una interfaz pasiva.

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

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

```
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
```

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

Hello due in 00:00:05

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

```
R1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started!

warning

User Access Verification

Password:

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

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

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

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



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

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

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

```

R1
Physical Config CLI
IOS Command Line Interface
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#enable
R1#configure termina
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#
Copy Paste

```

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

**R2# show ipv6 route ospf**

IPv6 Routing Table - default - 10 entries

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

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

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

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

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

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

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

via FE80::1, Serial0/0/0

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

via FE80::3, Serial0/0/1

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

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

```
R2
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

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

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

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

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

R2(config-rtr)# **passive-interface default**

```
R2
Physical Config CLI
IOS Command Line Interface

warning
User Access Verification
Password:
R2>enable
Password:
R2#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:13::/64 [110/128]
  via FE80::1, Serial0/0/0
  via FE80::3, Serial0/0/1
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ospf 1
-
% Invalid input detected at '^' marker.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
R2(config-rtr)#
```

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

R1# **show ipv6 ospf neighbor**

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

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

```

R2
Physical Config CLI
IOS Command Line Interface
Password:
R2>enable
Password:
R2#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O   2001:DB8:ACAD:A::/64 [110/65]
    via FE80::1, Serial0/0/0
O   2001:DB8:ACAD:C::/64 [110/65]
    via FE80::3, Serial0/0/1
O   2001:DB8:ACAD:13::/64 [110/128]
    via FE80::1, Serial0/0/0
    via FE80::3, Serial0/0/1
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ospf 1

% Invalid input detected at '^' marker.

R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached

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

R2#show ipv6 ospf neighbor
R2#
  
```

```

R1
Physical Config CLI
IOS Command Line Interface
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#enable
R1#configure termina
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtx)#passive-interface g0/0
R1(config-rtx)#end
R1#
*SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#
00:34:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Dead timer expired
00:34:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
3.3.3.3          0    FULL/-          00:00:31    3             Serial0/0/1
R1#
Copy Paste

```

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

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

```

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

```

```
R2
Physical Config CLI
IOS Command Line Interface
2001:DB8:ACAD:B::/64 (110/120)
  via FE80::1, Serial0/0/0
  via FE80::3, Serial0/0/1
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ospf 1
^
% Invalid input detected at '^' marker.

R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

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

R2#show ipv6 ospf neighbor
R2#show ipv6 ospf interface s0/0/0
^
% Invalid input detected at '^' marker.

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

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

```
R3 con0 is now available

Press RETURN to get started.

warning
User Access Verification
Password:
R3>enable
Password:
R3#show ipv6 route ospf
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:12::/64 [110/128]
  via FE80::1, Serial0/0/0
R3#
```

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

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

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

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

```
R2
Physical Config CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ospf 1
^
% Invalid input detected at '^' marker.

R2(config)#ipv6 router ospf 1
R2(config-rttr)#passive-interface default
R2(config-rttr)#
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

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

R2#show ipv6 ospf neighbor
R2#show ipv6 ospf interface s/0/0/0
^
% Invalid input detected at '^' marker.

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

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

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64? **La s0/0/1**

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

¿El R2 aparece como vecino OSPFv3 en el R1? **No**

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

¿Qué indica esta información?

**Que como se ha desactivado la interface como pasiva R1 y R2 no se comunican porque no hay camino**

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



```
R2(R2)
R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
00:34:02: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show ipv6 ospf neighbor
R2#show ipv6 ospf interface s0/0/0
^
% Invalid input detected at '^' marker.
R2#show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
00:41:04: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#
```

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

```

R1#show ipv6 ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1#
00:34:39: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Dead timer expired
00:34:39: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
3.3.3.3          0    FULL/ -         00:00:31    3             Serial0/0/1
R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
3.3.3.3          0    FULL/ -         00:00:31    3             Serial0/0/1
R1#
00:48:12: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL,
Loading Done
R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
2.2.2.2          0    FULL/ -         00:00:38    3             Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:34    3             Serial0/0/1
R1#

```

## Reflexión

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

**Si porque si se le coloca procesos a R1 como 1 a R2 como 2 y a R3 como 3 son localmente significativos no afectan a los demás routers y el área debe ser 0 en todas para que estén en la misma área de ruteo pero OSPF 1 puede variar**

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

**Removiendo la entrada network ayuda a prevenir los errores y las direcciones Ipv6 una interface puede tener múltiples direcciones asignadas a ella asignando una interface una área o ospf todas las redes multicas en esa interface van automáticamente asignadas al área o Ospf y también graban una ruta creada in la tabla de ruteo de ipv6**

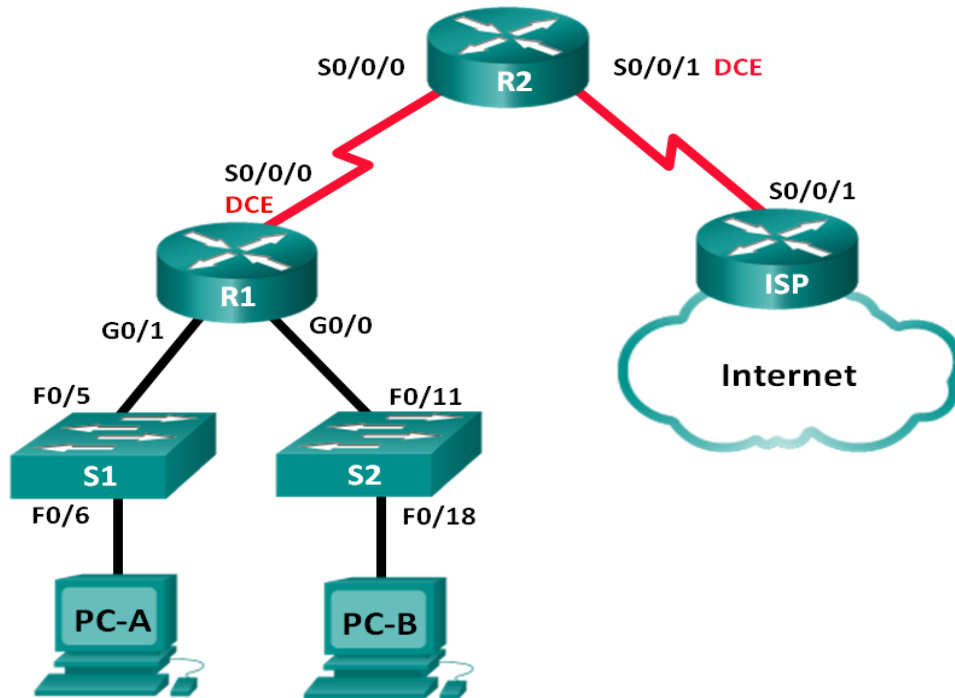
## Tabla de resumen de interfaces del router

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

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

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

#### Topología



#### Tabla de direccionamiento

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

## **Objetivos**

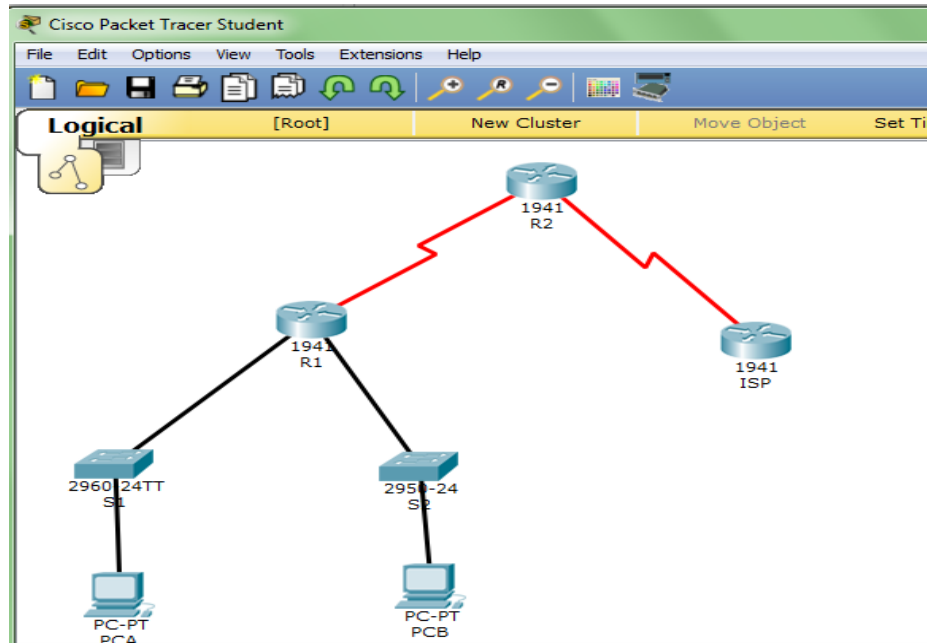
**Parte 1: armar la red y configurar los parámetros básicos de los dispositivos**

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

## Parte 5. armar la red y configurar los parámetros básicos de los dispositivos

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

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



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

R1

```
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

R2

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

ISP

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

S1

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

---

S2

```
Switch>
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

---

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

- a. Desactive la búsqueda DNS.

R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#
```

---

R2

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#no ip domain-lookup
```

IPS

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

---

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

R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#exit
```

R2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#exit
```

ISP

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#exit
ISP#
```

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

## R1

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

## R2

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

## ISP

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

## R1 contraseña consola

```
R1(config)#line con 0
R1(config-line)#password cisco
```

## R1 contraseña vty

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#loggin synchronous
^
% Invalid input detected at '^' marker.
R1(config-line)#logging synchronous
^
% Invalid input detected at '^' marker.
R1(config-line)#logging synchronous
R1(config-line)#
```

## R2 contraseña consola

```
Enter configuration commands, one per
R2(config)#line con 0
R2(config-line)#password cisco
```

## R2 contraseña vty

```
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
```

## ISP contraseña consola

```
ISP(config-line)#password cisco
ISP(config-line)#login
```

## ISP contraseña vty



```
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
```

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

**R1**

```
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#loggin synchronous
R1(config-line)#exit
R1(config)#
```

**R2**

```
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#loggin synchronous
```

**ISP**

```
ISP(config)#line con 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#loggin synchronous
ISP(config-line)#exit
```

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

**R1**

```
R1(config)#int g 0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

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

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

R1(config-if)#int g 0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

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

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

**R2**

```
R2(config)#int s 0/0/0
R2(config-if)#ip address 192.168.2.254 255.255.255.252
R2(config-if)#no shutdown
```

**ISP**

```
ISP(config)#int s 0/0/1
ISP(config-if)#ip address 209.165.200.225 255.255.255.224
ISP(config-if)#no shutdown
```

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

## R1

```
R1(config-if)#int s 0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#ip address 192.168.2.253 255.255.255.252
R1(config-if)#no shutdown
```

## R2

```
R2(config)#int s 0/0/1
R2(config-if)#clock rate 128000
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#no shutdown
```

- h. Configure EIGRP for R1.

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

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

- 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)#route eigrp 1
R2(config-router)#network 192.168.2.252 0.0.0.3
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is up: new
adjacency

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

```

```

R2
Physical Config CLI
IOS Command Line Interface
249556K Bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is u
adjacency

User Access Verification

Password:

R2>enable
Password:
R2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
R2(config)#
R2(config)#

```

- j. Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.  
**ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226**

```
R2
Physical Config CLI
IOS Command Line Interface
249836K Bytes of ATA System CompactFlash 0 (read/write)

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, cha
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, cha
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0
adjacency

User Access Verification

Password:
R2>enable
Password:
R2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
R2(config)#
```

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

#### **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**

```
ISP
Physical Config CLI
IOS Command Line Interface

User Access Verification
Password:
ISP>enable
Password:
ISP#ping 192.168.2.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/33/143 ms
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 = 12/46/184 ms
ISP#
```

R2

```
R2#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 = 9/155/736 ms
R2#ping 209.165.200.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/154/727 ms
---
```

R1

```
R1
Physical Config CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.254 (Serial0/0/0) is up: new adjacency

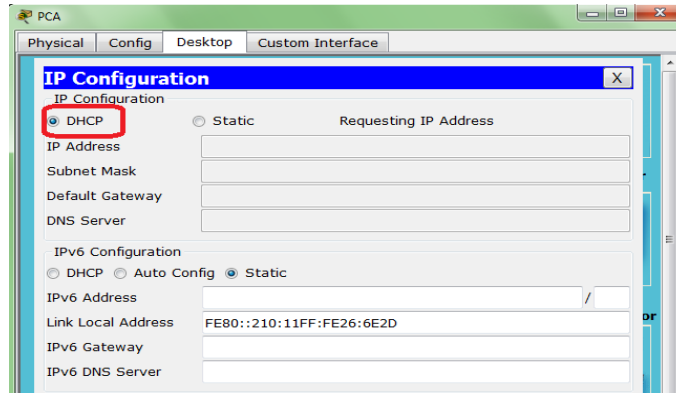
User Access Verification

Password:

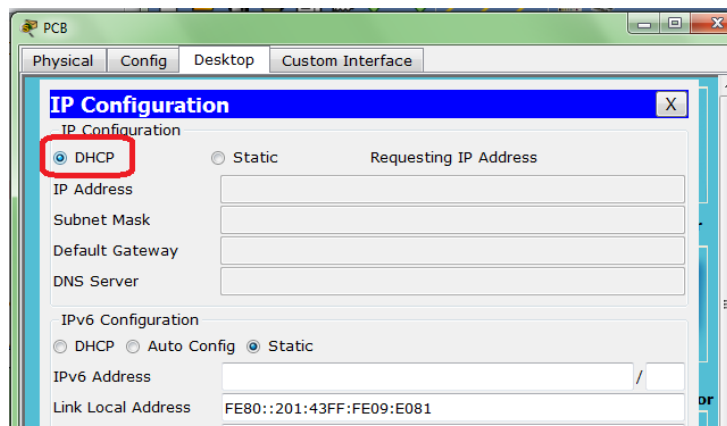
R1>enable
Password:
R1#ping 209.165.200.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225: timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/57/233 ms
R1#ping 192.168.2.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/45/180 ms
R1#
```

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

PCA



PCB



## Parte 6. configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

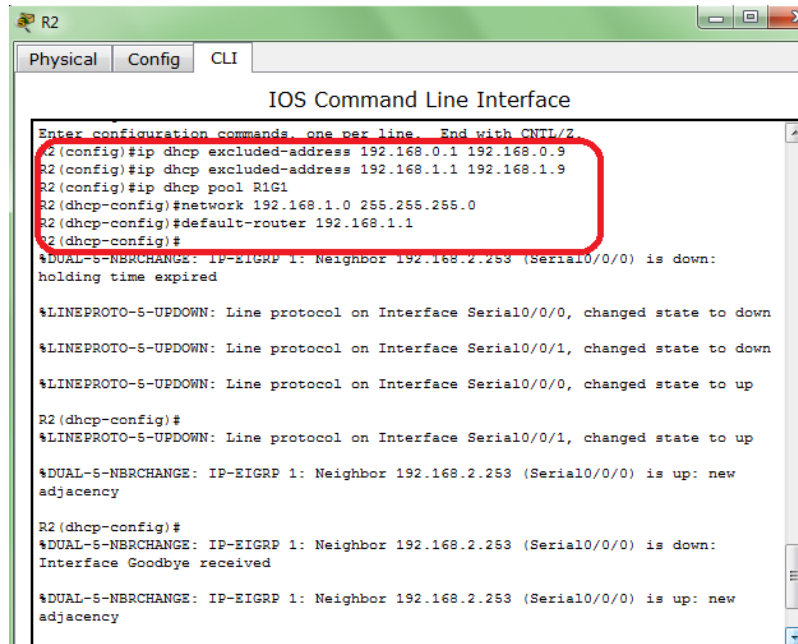
Para asignar automáticamente la información de dirección en la red, configure el R2 como servidor de DHCPv4 y el R1 como agente de retransmisión DHCP.

### 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.



```
R2
Physical Config CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is down:
holding time expired

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

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

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is up: new
adjacency

R2(dhcp-config)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is down:
Interface Goodbye received

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is up: new
adjacency
```

```
R2
Physical Config CLI
IOS Command Line Interface
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is down:
holding time expired
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(dhcp-config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is up: new
adjacency
R2(dhcp-config)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is down:
Interface Goodbye received
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is up: new
adjacency
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#exit
R2(Config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#
```

Nota: En packet tracer no se puede incluir un dominio ni un tiempo de arrendamiento ya que es un simulador esto se hace en un router real.

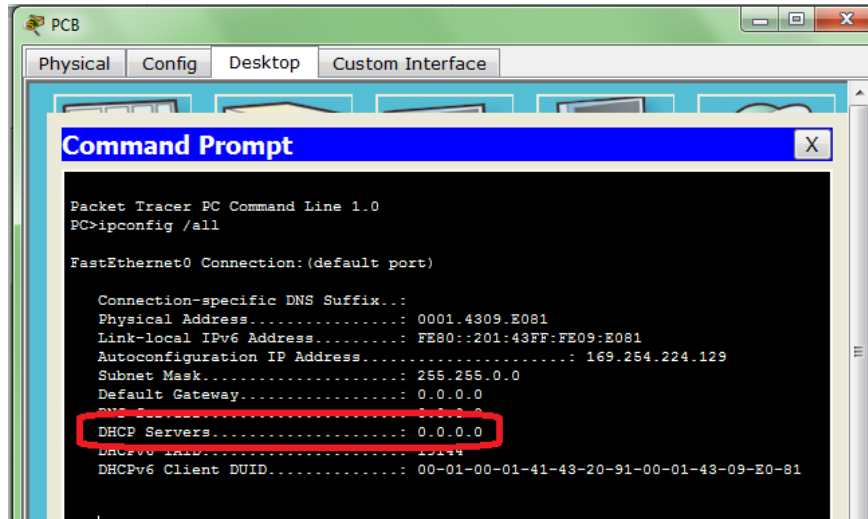
En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando **ipconfig /all**. ¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué?

### PCA

```
PCA
Physical Config Desktop Custom Interface
Command Prompt X
Packet Tracer PC Command Line 1.0
PC>ipconfig /oll
Invalid Command.
PC>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Physical Address...: 0010.1126.6E2D
Link-local IPv6 Address...: FE80::210:11FF:FE26:6E2D
Autoconfiguration IP Address...: 169.254.110.45
Subnet Mask...: 255.255.0.0
Default Gateway...: 0.0.0.0
DNS Servers...:
DHCP Servers...: 0.0.0.0
DHCPv6 Ind...:
DHCPv6 Client DUID...: 00-01-00-01-AD-97-14-88-00-10-11-26-6E-2D
```

### PCB



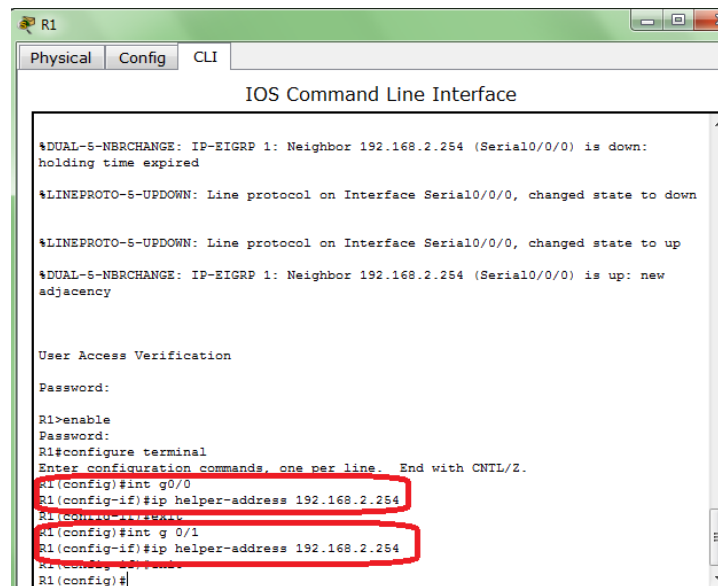


**RTA:** No recibió ninguna ip de R2 porque este se encuentra en otra red lejana.

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

Configure las direcciones IP de ayuda en el R1 para que reenvíe 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.



Registrar la configuración IP para la PC-A y la PC-B.

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

**PCA**

```

PCA
Physical Config Desktop Custom Interface

Command Prompt

Connection-specific DNS Suffix...:
Physical Address.....: 0010.1126.6E2D
Link-local IPv6 Address.....: FE80::210:11FF:FE26:6E2D
Autoconfiguration IP Address.....: 169.254.110.45
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....: 15188
DHCPv6 Client DUID.....: 00-01-00-01-AD-97-14-88-00-10-11-26-6E-2D

PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0010.1126.6E2D
Link-local IPv6 Address.....: FE80::210:11FF:FE26:6E2D
IP Address.....: 192.168.1.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 209.165.200.225
DHCP Servers.....: 192.168.2.254
DHCPv6 IAID.....: 15188
DHCPv6 Client DUID.....: 00-01-00-01-AD-97-14-88-00-10-11-26-6E-2D

PC>

```

PCB

```

PCB
Physical Config Desktop Custom Interface

Command Prompt

Connection-specific DNS Suffix...:
Physical Address.....: 0001.4309.E081
Link-local IPv6 Address.....: FE80::201:43FF:FE09:E081
Autoconfiguration IP Address.....: 169.254.224.129
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....: 19144
DHCPv6 Client DUID.....: 00-01-00-01-41-43-20-91-00-01-43-09-E0-81

PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0001.4309.E081
Link-local IPv6 Address.....: FE80::201:43FF:FE09:E081
IP Address.....: 192.168.0.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.0.1
DNS Servers.....: 209.165.200.225
DHCP Servers.....: 192.168.2.254
DHCPv6 IAID.....: 19144
DHCPv6 Client DUID.....: 00-01-00-01-41-43-20-91-00-01-43-09-E0-81

```

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?

**RTA:** Como se habían excluido de la 1 a la nueve la primera en usarcé es la 10

**PCA**

```
Link-Local IPv6 Address..... FE80::210:11FF:F
IP Address..... 192.168.1.10
Subnet Mask..... 255.255.255.0
```

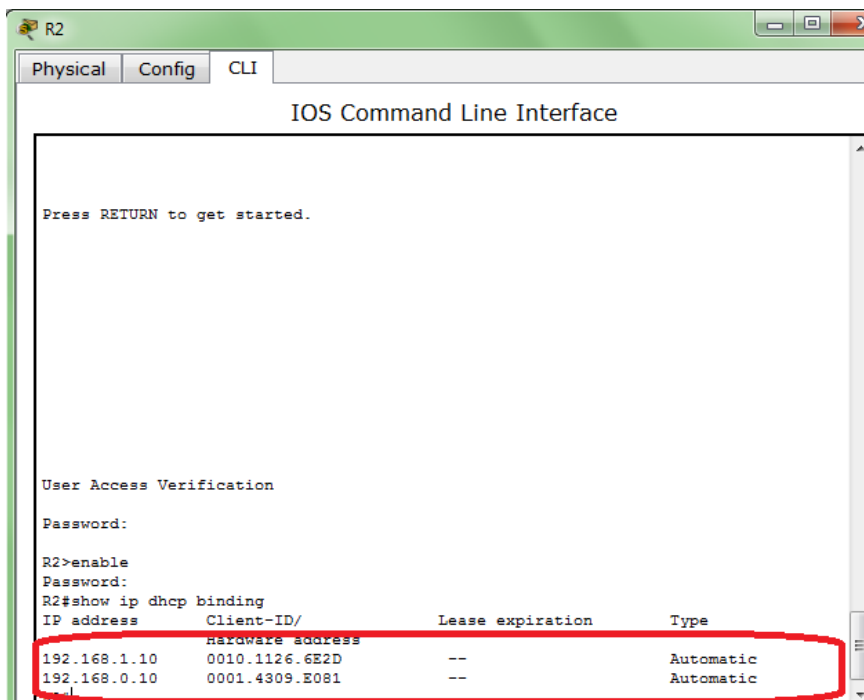
## PCB

```
IP Address..... 192.168.0.10
Subnet Mask..... 255.255.255.0
```

### Paso 3. verificar los servicios DHCP y los arrendamientos de direcciones en el R2.

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

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



```
R2
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started.
User Access Verification
Password:
R2>enable
Password:
R2#show ip dhcp binding
IP address      Client-ID/      Lease expiration  Type
                Hardware address
192.168.1.10    0010.1126.6E2D  --                Automatic
192.168.0.10    0001.4309.E081  --                Automatic
```

- En el R2, introduzca el comando **show ip dhcp server statistics** para ver la actividad de mensajes y las estadísticas del pool de DHCP.

¿Cuántos tipos de mensajes DHCP se indican en el resultado?

```
R2#show ip dhcp server statistic
^
% Invalid input detected at '^' marker.

R2#show ip dhcp server statistics
^
% Invalid input detected at '^' marker.
```

Nota: al parece este comando no es válido en packet tracer

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

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

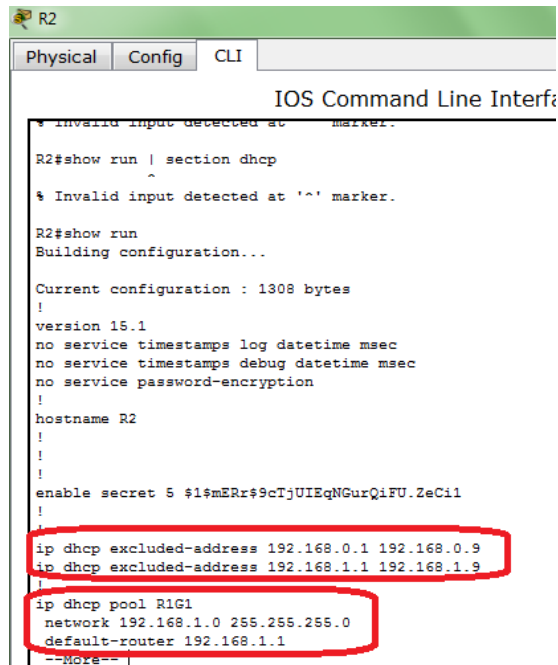
```
R2#show ip dhcp pool
      ^
% Invalid input detected at '^' marker.
R2#
```

Nota: de igual manera que con el comando anterior no es válido en el simulador packet tracer

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

```
R2#show run | section dhcp
      ^
% Invalid input detected at '^' marker.
```

**RTA:** al correr el comando completo no corre pero si solo ingresamos el comando show run este nos muestra la configuración que nos solicitan en este punto.



```
R2
Physical Config CLI
IOS Command Line Interface

% Invalid input detected at '^' marker.

R2#show run | section dhcp
      ^
% Invalid input detected at '^' marker.

R2#show run
Building configuration...

Current configuration : 1308 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
--More--
```

```
R2
Physical Config CLI
IOS Command Line Interface
Current configuration : 1308 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 209.165.200.225
ip dhcp pool R1G0
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 209.165.200.225
!
```

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

### G0/0

```
R1
Physical Config CLI
IOS Command Line Interface
R1#show ip int g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.0.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 192.168.2.254
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
```

### G0/1

```
R1
Physical Config CLI
IOS Command Line Interface
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
R1#show ip int g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 192.168.2.254
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
--More--
```

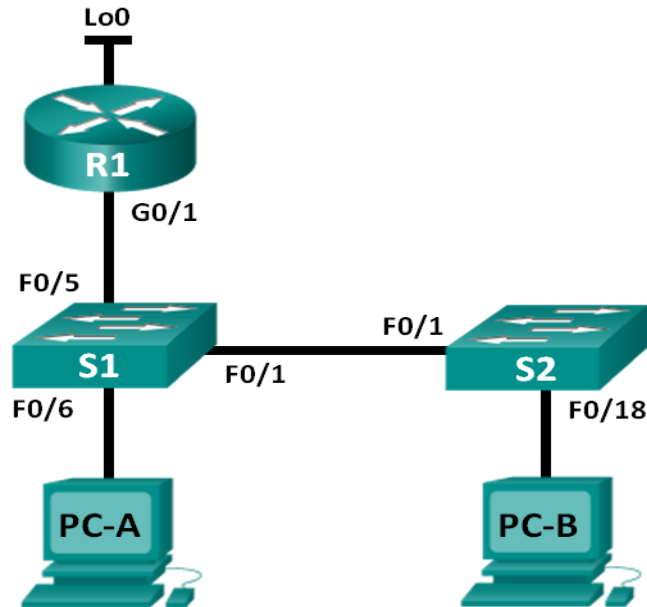
## Reflexión

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

**RTA:** este nos permite ahorrar recursos de hardware, si solo utilizamos DHCP en un solo router y no en varios nos será más fácil la administración de los mismos ya que no tendríamos que estar ingresando de uno en uno.

### 10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch

#### Topología



#### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.22 5	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

## Objetivos

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

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

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

### **Parte 3: configurar DHCPv4**

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

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

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

### **Parte 5: habilitar el routing IP**

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

## Recursos necesarios

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



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

**Paso 4:** realizar el cableado de red tal como se muestra en la topología.

**Paso 5:** inicializar y volver a cargar los routers y switches.

**Paso 6:** configurar los parámetros básicos en los dispositivos.

- a. Asigne los nombres de dispositivos como se muestra en la topología.
- b. Desactive la búsqueda del DNS.
- c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
- d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 5
R1(config-line)#password cisco
R1(config-line)#login local
R1(config-line)#exit
R1(config)#interface g0/1
R1(config-if)#ip address 192.168.1.10 255.255.255.0
R1(config-if)#no shutdown
```

```
R1(config-if)#interface lo0

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

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

R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#
```

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

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#vlan 2
S1(config-vlan)#exit
S1(config)#interface vlan 2
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

S1(config-if)#ip address 192.168.2.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#

```

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

## Parte 2: cambiar la preferencia de SDM

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

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

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

S1# **show sdm prefer**

The current template is "default" template.

The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

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

```
S1#show sdm prefer
^
% Invalid input detected at '^' marker.
S1#
```

Packet Tracer no soporta este comando

¿Cuál es la plantilla actual?

Las respuestas pueden variar pero estas pueden ser de “default” o de “dual-ipv4 y ipv6 default” o también podría ser “lanbase-routing”

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

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

```
S1(config)# sdm prefer lanbase-routing
```

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

¿Qué plantilla estará disponible después de la recarga? Lanbase-routing

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

```
S1# reload
```

System configuration has been modified. Save? [yes/no]: **no**

Proceed with reload? [confirm]

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

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

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

```
S1# show sdm prefer
```

The current template is "lanbase-routing" template.

The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

number of unicast mac addresses: 4K

number of IPv4 IGMP groups + multicast routes: 0.25K

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

## Parte 2: configurar DHCPv4

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

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

- i. Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.  
Ip dhcp excluded-address 192.168.1.1 192.168.1.10
- j. Cree un pool de DHCP con el nombre **DHCP1**. En el espacio proporcionado, escriba el comando que utilizó.  
Ip dhcp pool DHCP1
- k. Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.  
Network 192.168.1.0 255.255.255.0
- l. Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.  
Default-router 192.168.1.1
- m. Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.  
Dns-server 192.168.1.9

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

Lease 3

- o. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#ip dhcp pool DHCP1
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.1.1
S1(dhcp-config)#dns-server 192.168.1.9
S1(dhcp-config)#lease 3
^
% Invalid input detected at '^' marker.

S1(dhcp-config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

## Paso 2: verificar la conectividad y DHCP.

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

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.1.11

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.

Para la PC-B, incluya lo siguiente:

Dirección IP: 192.168.1.12

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1

```
PC-A
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0060.7095.01BA
Link-local IPv6 Address.....: FE80::260:70FF:FE95:1BA
IP Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 192.168.1.9
DHCP Servers.....: 192.168.1.1
DHCPv6 Client DUID.....: 00-01-00-01-E3-21-B5-3C-00-60-70-95-01-BA
```

```
PC-B
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0050.0F6E.5E57
Link-local IPv6 Address.....: FE80::250:FFF:FE6E:5E57
IP Address.....: 192.168.1.12
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 192.168.1.9
DHCP Servers.....: 192.168.1.1
DHCPv6 Client DUID.....: 00-01-00-01-12-20-E9-40-00-50-0F-6E-5E-57
```

- q. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.  
¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? Si  
¿Es posible hacer ping de la PC-A a la PC-B? Si  
¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1? Si  
Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.

### Paso 3: configurar DHCPv4 para varias VLAN

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

#### **Paso 4: asignar un puerto a la VLAN 2.**

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

Interface g0/6

Switchport mode access

Switchport access vlan 2

#### **Paso 5: configurar DHCPv4 para la VLAN 2.**

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

Ip dhcp excluded-address 192.168.2.1 192.168.2.10

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

Ip dhcp pool DHCP2

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

Network 192.168.2.0 255.255.255.0

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

Default-router 192.168.2.1

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

Dns-server 192.168.2.9

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

Lease 3

- x. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```

S1>enable
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

S1(config-if)#exit
S1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)#ip dhcp pool DHCP2
S1(dhcp-config)#network 192.168.2.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.2.1
S1(dhcp-config)#dns-server 192.168.2.9
S1(dhcp-config)#lease 3
^
% Invalid input detected at '^' marker.

S1(dhcp-config)#

```

#### Paso 6: verificar la conectividad y DHCPv4.

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

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.2.11

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.2.1

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

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

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

¿Los pings eran correctos? ¿Por qué?

No porque aún no pueden salir y porque aún no se aplica el ruteo

```

PC>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0060.7095.01BA
    Link-local IPv6 Address.....: FE80::260:70FF:FE95:1BA
    IP Address.....: 192.168.2.11
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 192.168.2.1
    DNS Servers.....: 192.168.2.9
    DHCP Servers.....: 192.168.2.1
    DHCPv6 Client DUID.....: 00-01-00-01-E3-21-B5-3C-00-60-70-95-01-BA

```



```

PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255

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

```

```

PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

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

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

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

¿Qué resultado arrojó este comando?

Que las 2 rutas están conectadas, lo que hace que si conozca las dos redes, pero nopuede hacer ruteo entre las dos, para ello ay que activarlas.

```

S1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Vlan1
C    192.168.2.0/24 is directly connected, Vlan2
S1#

```

### Parte 3: habilitar el routing IP

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

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

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

```
S1(config)# ip routing
```

- cc. Verificar la conectividad entre las VLAN.

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

¿Qué función realiza el switch?

Establece una conexión entre los PCs, pero no puede hacer ping al router

```
PC>ping 168.168.1.12

Pinging 168.168.1.12 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 168.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- dd. Vea la información de la tabla de routing para el S1.

¿Qué información de la ruta está incluida en el resultado de este comando?

Conoce sus dos Vlan pero no hace ping al router, para hacer ruteo necesita rutas estáticas

```
S1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C     192.168.1.0/24 is directly connected, Vlan1
C     192.168.2.0/24 is directly connected, Vlan2
S1#
```

- ee. Vea la información de la tabla de routing para el R1.

¿Qué información de la ruta está incluida en el resultado de este comando?

Las direcciones de las redes y el loopback

```

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

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.10/32 is directly connected, GigabitEthernet0/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
R1#

```

ff. ¿Es posible hacer ping de la PC-A al R1? No

¿Es posible hacer ping de la PC-A a la interfaz Lo0? No

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Se debe agregar una ruta estática

## Paso 2: asignar rutas estáticas.

Habilitar el routing IP permite que el switch enrute entre VLAN asignadas en el switch. Para que todas las VLAN se comuniquen con el router, es necesario agregar rutas estáticas a la tabla de routing del switch y del router.

gg. En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.

Ip route 0.0.0.0.0.0.0 192.168.1.10

```

S1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.10
S1(config)#

```

hh. En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

Ip route 192.168.2.0 255.255.255.0 g0/1

```

R1(config)#ip route 192.168.2.0 255.255.255.0 g0/1

```

ii. Vea la información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?

Esta red estática indica que sale a cualquier otra red a través de la Ip del router

```

S1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

C     192.168.1.0/24 is directly connected, Vlan1
C     192.168.2.0/24 is directly connected, Vlan2
S*   0.0.0.0/0 [1/0] via 192.168.1.10
S1#

```

jj. Ve a la información de la tabla de routing para el R1.

¿Cómo está representada la ruta estática?

Atraves de una ruta estática aprende que existe una red dos, la cual antes no la conocía por lo mismo el router antes no podía responder por su Lo0 ni por su propia interface

```

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

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.1.0/24 is directly connected, GigabitEthernet0/1
L     192.168.1.10/32 is directly connected, GigabitEthernet0/1
S     192.168.2.0/24 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C     209.165.200.224/27 is directly connected, Loopback0
L     209.165.200.225/32 is directly connected, Loopback0
R1#

```

kk. ¿Es posible hacer ping de la PC-A al R1? Si

¿Es posible hacer ping de la PC-A a la interfaz Lo0? Si

Ping R1

```
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=1ms TTL=254
Reply from 192.168.1.10: bytes=32 time=14ms TTL=254

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 4ms
```

## Ping Lo0

```
PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

## **Reflexión**

1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

Es necesario incluir direcciones porque si nosotros le vamos a dar a las computadoras las direcciones que ya hemos usado, en cualquiera de los dispositivos, ya sean los switch, route o las pcs, puede haber un posible conflicto de IP, por ello se excluiría las direcciones estáticas.

2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts

Como en los switch no se han creado dos DHCP, lo que se hace es asignar cierto puerto para vlan1 y cierto puerto para la vlan2, para que de este modo pueda el switch mandar por ay la información de DHCP.

3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?

Este realiza la función de capa 3 de route

### Tabla de resumen de interfaces del router

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

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

### Apéndice A: comandos de configuración

#### Configurar DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

#### Configurar DHCPv4 para varias VLAN

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
```

```
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)# ip dhcp pool DHCP2
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.2.1
S1(dhcp-config)# dns-server 192.168.2.9
S1(dhcp-config)# lease 3
```

### **Habilitar routing IP**

```
S1(config)# ip routing
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```



### 10.2.3.5 Lab – Configuring Stateless and Stateful DHCPv6

#### Topología



#### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1	64	No aplicable
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

#### Objetivos

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

**Parte 2:** configurar la red para SLAAC

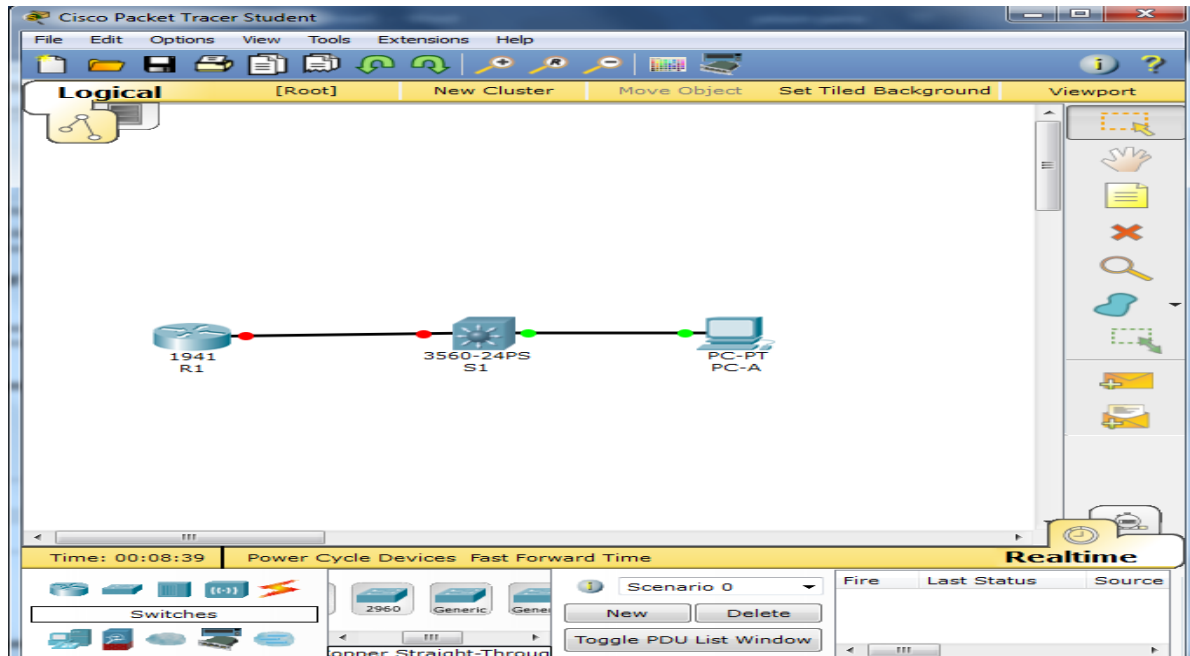
**Parte 3:** configurar la red para DHCPv6 sin estado

**Parte 4:** configurar la red para DHCPv6 con estado

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

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

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



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

### Paso 3. Configurar R1

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Guardar la configuración en ejecución en la configuración de inicio.

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

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 5
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#banner motd "warning"
R1(config)#service password-encryption
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

#### 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.

```
S1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

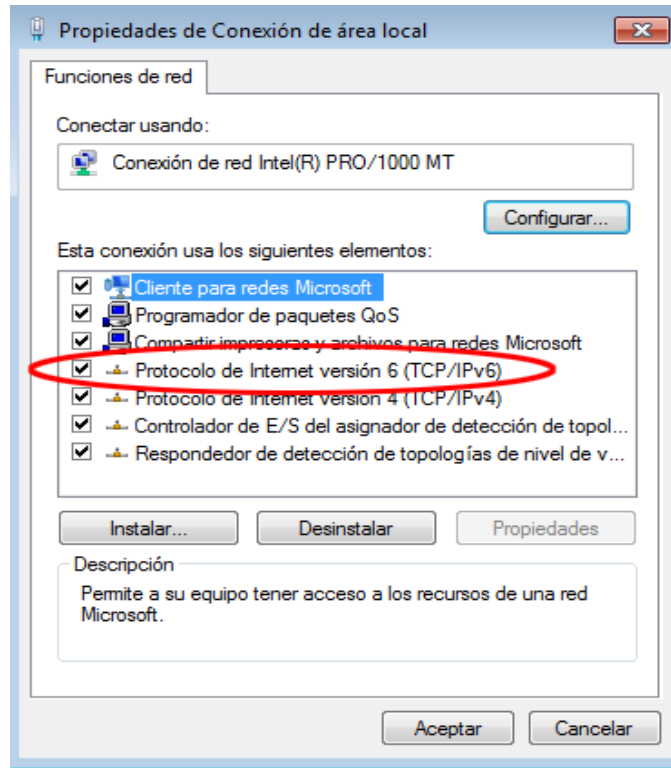
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 5
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#login synchronous
S1(config-line)#banner motd "warning"
S1(config)#service password-encryption
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

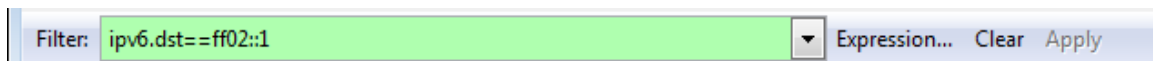
## Parte 2. configurar la red para SLAAC

### Paso 1. preparar la PC-A.

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



- b. Inicie una captura del tráfico en la NIC con Wireshark.
- c. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes. La entrada de filtro que se usa con Wireshark es **ipv6.dst==ff02::1**, como se muestra aquí.



## Paso 2. Configurar R1

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

```
R1
Physical Config CLI
IOS Command Line Interface

!
end

R1#
R1#
R1#
R1#
R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

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

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

R1(config-if)#
```

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

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

**R1# show ipv6 interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::1

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

**FF02::2**

FF02::1:FF00:1

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

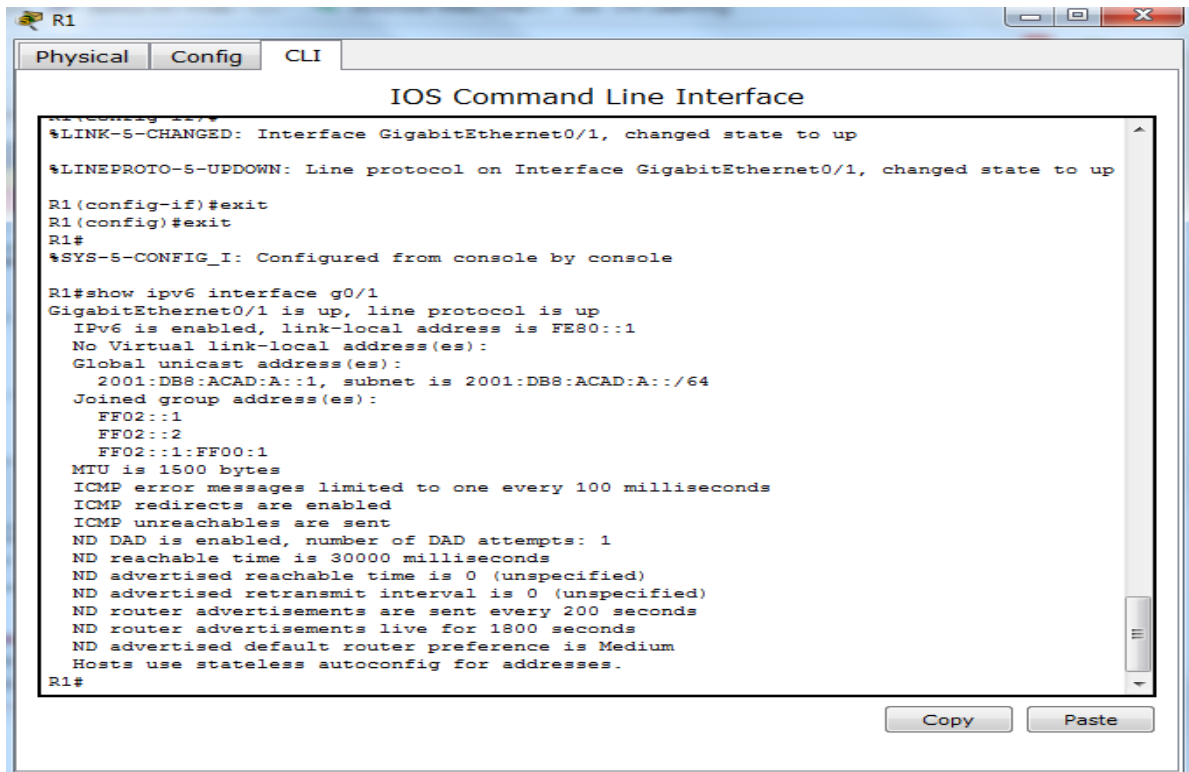
ICMP unreachable are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)  
ND router advertisements are sent every 200 seconds  
ND router advertisements live for 1800 seconds  
ND advertised default router preference is Medium  
Hosts use stateless autoconfig for addresses.

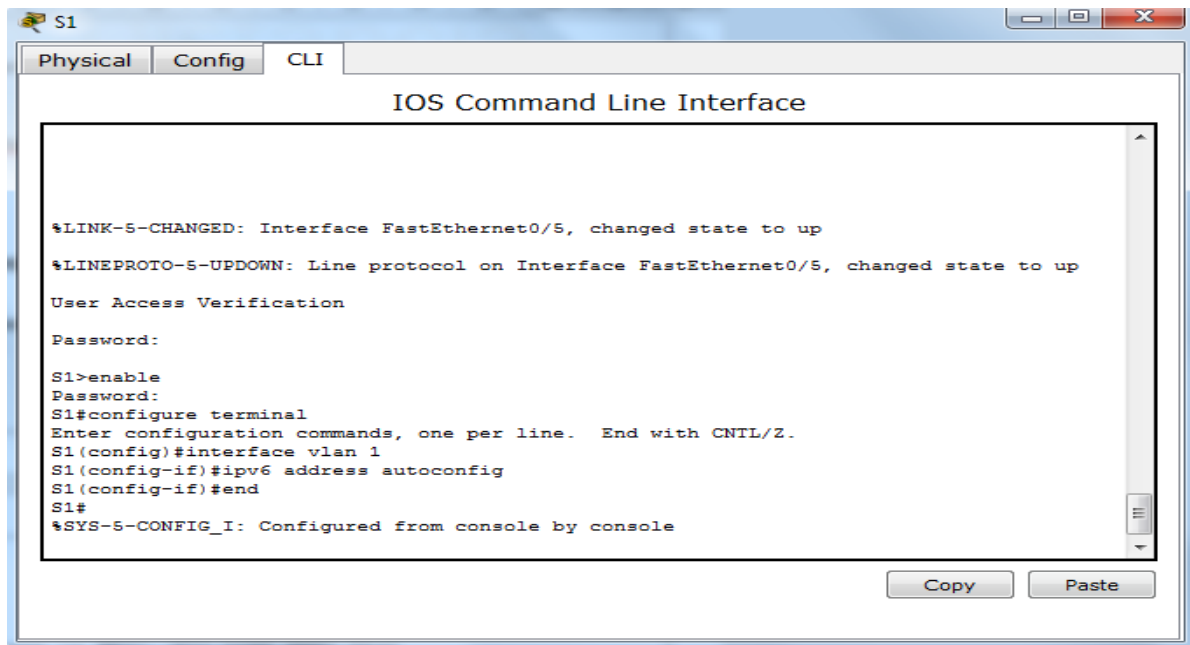


```
R1
Physical Config CLI
IOS Command Line Interface
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FE02::1
  FE02::2
  FE02::1:FE00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#
```

#### Paso 4. configurar el S1.

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

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



### Paso 5. verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

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

```
S1# show ipv6 interface
```

```
Vlan1 is up, line protocol is up
```

```
IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
```

```
No Virtual link-local address(es):
```

```
Stateless address autoconfig enabled
```

```
Global unicast address(es):
```

```
2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64
```

```
[EUI/CAL/PRE]
```

```
valid lifetime 2591988 preferred lifetime 604788
```

```
Joined group address(es):
```

```
FF02::1
```

```
FF02::1:FFE8:8A40
```

```
MTU is 1500 bytes
```

```
ICMP error messages limited to one every 100 milliseconds
```

```
ICMP redirects are enabled
```

```
ICMP unreachable are sent
```

```
Output features: Check hwidb
```

```
ND DAD is enabled, number of DAD attempts: 1
```

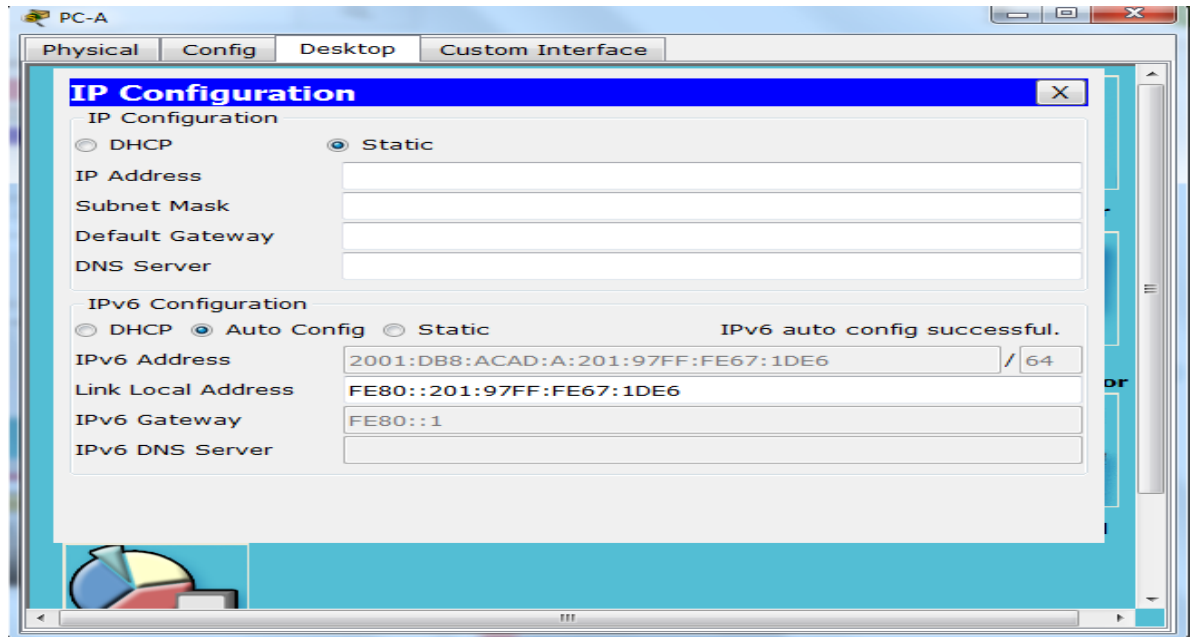
```
ND reachable time is 30000 milliseconds (using 30000)
```

```
ND NS retransmit interval is 1000 milliseconds
```

```
Default router is FE80::1 on Vlan1
```

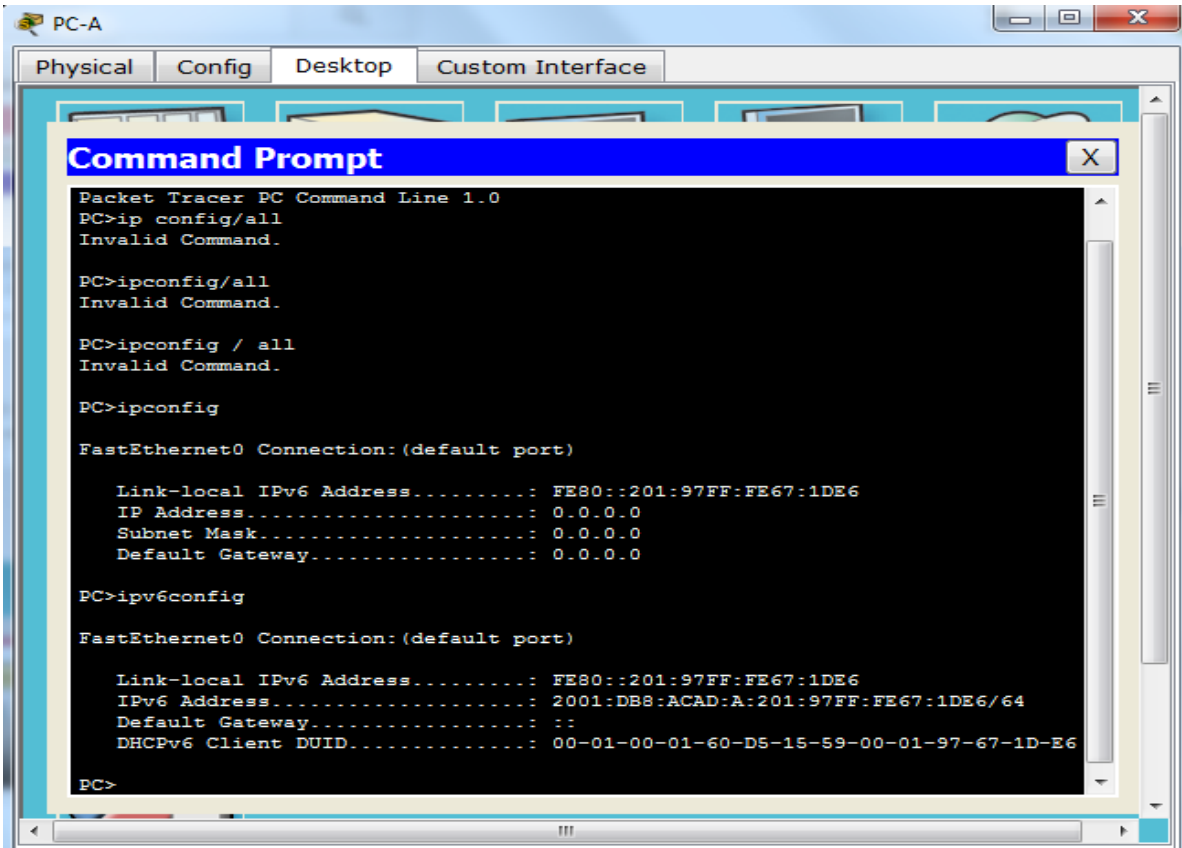


Paso 6. verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

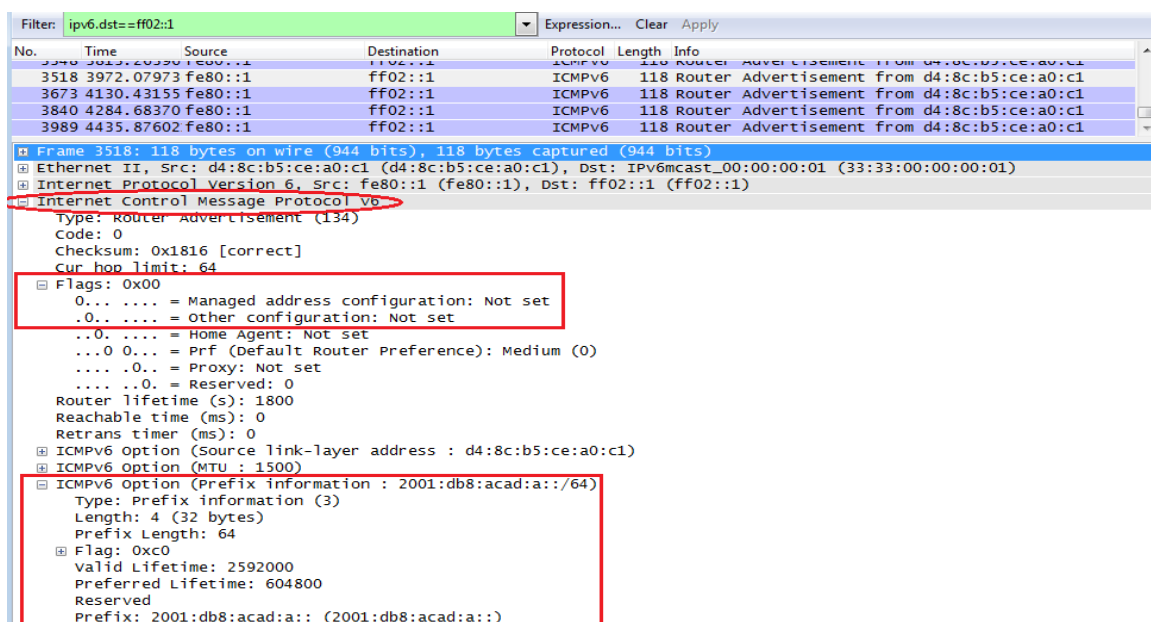


- a. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all**. Verifique que la PC-A muestre una dirección IPv6 con el prefijo 2001:db8:acad:a::/64. El gateway predeterminado debe tener la dirección FE80::1.

```
Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . : 
    Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
    Dirección física. . . . . : 00-0C-29-E3-23-17
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Preferido)
    Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11(Preferido)
    Dirección IPv4. . . . . : 192.168.96.139(Preferido)
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : fe80::1%11
    Servidores DNS . . . . . : fec0:0:0:ffff::1%1
                                   fec0:0:0:ffff::2%1
                                   fec0:0:0:ffff::3%1
    NetBIOS sobre TCP/IP. . . . . : habilitado
```



- b. En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.



### Parte 3. configurar la red para DHCPv6 sin estado

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

- a. Cree un pool de DHCP IPv6.

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

- 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.

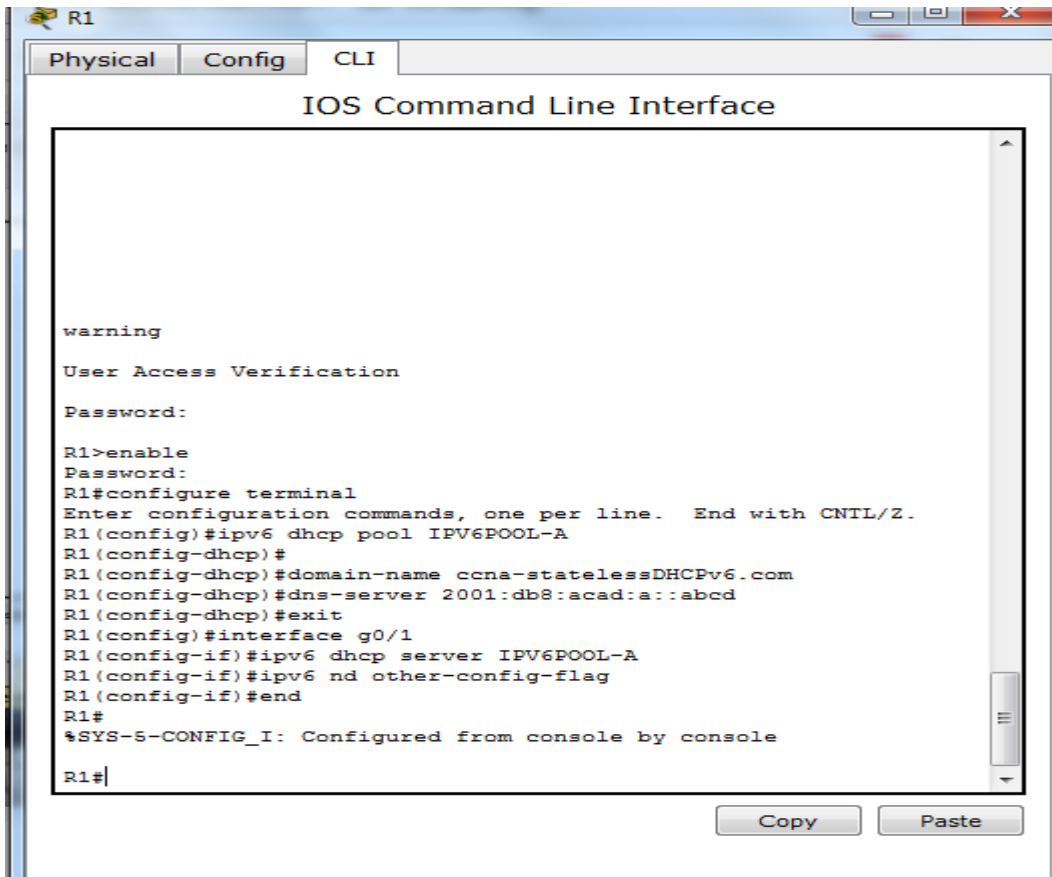
```
R1(config)# interface g0/1
```

```
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
```



```
R1
Physical Config CLI
IOS Command Line Interface

warning
User Access Verification
Password:
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#
R1(config-dhcp)#domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#dns-server 2001:db8:acad:a::abcd
R1(config-dhcp)#exit
R1(config)#interface g0/1
R1(config-if)#ipv6 dhcp server IPV6POOL-A
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

## 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 unreachable are sent
```

```
ND DAD is enabled, number of DAD attempts: 1
```

```
ND reachable time is 30000 milliseconds (using 30000)
```

```
ND advertised reachable time is 0 (unspecified)
```

```
ND advertised retransmit interval is 0 (unspecified)
```

```
ND router advertisements are sent every 200 seconds
```

```
ND router advertisements live for 1800 seconds
```

```
ND advertised default router preference is Medium
```

```
Hosts use stateless autoconfig for addresses.
```

```
Hosts use DHCP to obtain other configuration.
```

```
R1
Physical Config CLI
IOS Command Line Interface
R1(config-dhcp)#dns-server 2001:db8:acad:a::abcd
R1(config-dhcp)#exit
R1(config)#interface g0/1
R1(config-if)#ipv6 dhcp server IPV6POOL-A
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

**Paso 3. ver los cambios realizados en la red en la PC-A.**

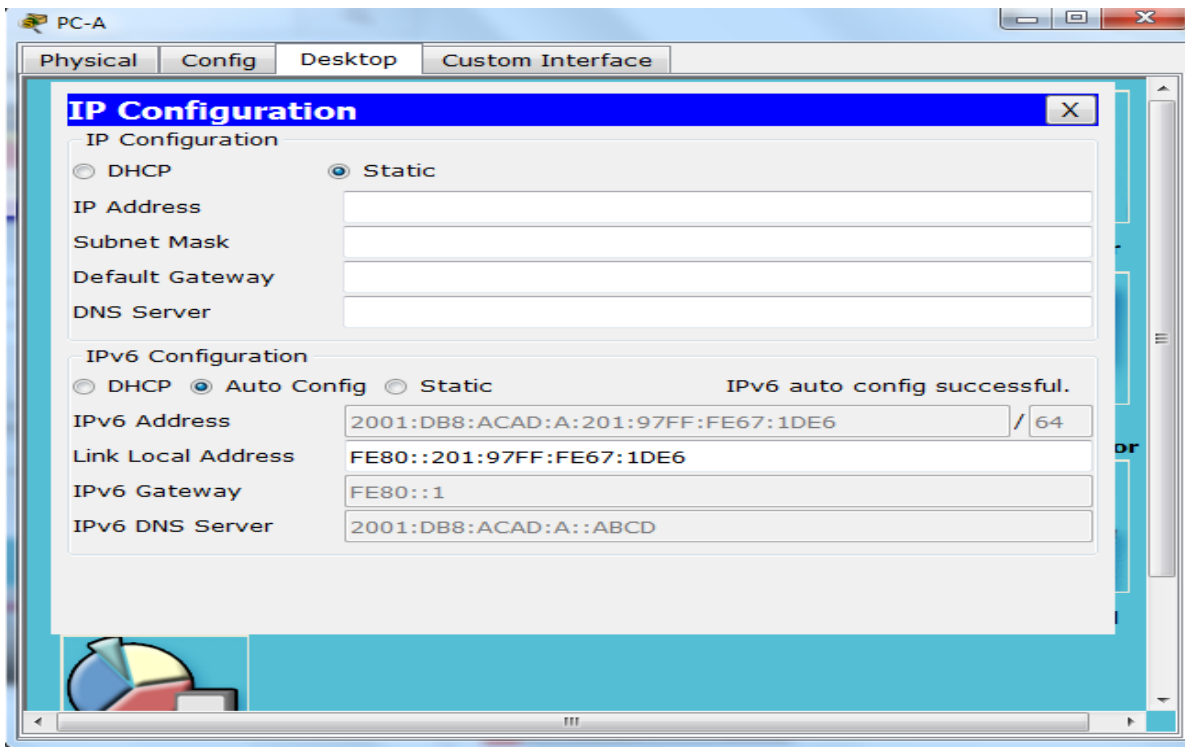
Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente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

```

Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
  Descripción . . . . . : Conexión de red Interic(8) PRO/1000
  MTU . . . . . : 1500
  Dirección física. . . . . : 00-0C-29-E3-23-17
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
  Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>
  Dirección IPv4. . . . . : 192.168.96.139<Preferido>
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . : fe80::1%11
  IAID DHCPv6 . . . . . : 234884137
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-E3-23-17
  Servidores DNS. . . . . : 2001:db8:acad:a::abcd
  NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de túnel isatap.localdomain:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
  Descripción . . . . . : Adaptador ISATAP de Microsoft
  Dirección física. . . . . : 00-00-00-00-00-00-00-E0
  DHCP habilitado . . . . . : no
  Configuración automática habilitada . . . : sí

```



```

PC-A
Physical Config Desktop Custom Interface

Command Prompt

PC>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address..... FE80::201:97FF:FE67:1DE6
IP Address..... 0.0.0.0
Subnet Mask..... 0.0.0.0
Default Gateway..... 0.0.0.0

PC>ipv6config

FastEthernet0 Connection:(default port)

Link-local IPv6 Address..... FE80::201:97FF:FE67:1DE6
IPv6 Address..... 2001:DB8:ACAD:A:201:97FF:FE67:1DE6/64
Default Gateway..... ::
DHCPv6 Client DUID..... 00-01-00-01-60-D5-15-59-00-01-97-67-1D-E6

PC>ipv6config

FastEthernet0 Connection:(default port)

Link-local IPv6 Address..... FE80::201:97FF:FE67:1DE6
IPv6 Address..... 2001:DB8:ACAD:A:201:97FF:FE67:1DE6/64
Default Gateway..... ::
DHCPv6 IAID..... 27990
DHCPv6 Client DUID..... 00-01-00-01-60-D5-15-59-00-01-97-67-1D-E6

PC>

```

**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.

No.	Time	Source	Destination	Protocol	Length	Info
191	190.005980	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
422	383.803033	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
696	581.355847	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
877	776.644829	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1

```

Frame 877: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0x17d6 [correct]
  Cur hop limit: 64
  Flags: 0x40
    0... .. = Managed address configuration: Not set
    .1.. .... = Other configuration: Set
    ..0. .... = Home Agent: Not set
    ...0 ... = Prf (Default Router Preference): Medium (0)
    ....0.. = Proxy: Not set
    ....0. = Reserved: 0
  Router lifetime (s): 1800
  Reachable time (ms): 0
  Retrans timer (ms): 0
  ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
  ICMPv6 Option (MTU : 1500)
  ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)

```

**Paso 5. verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.**

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

R1# show ipv6 dhcp binding

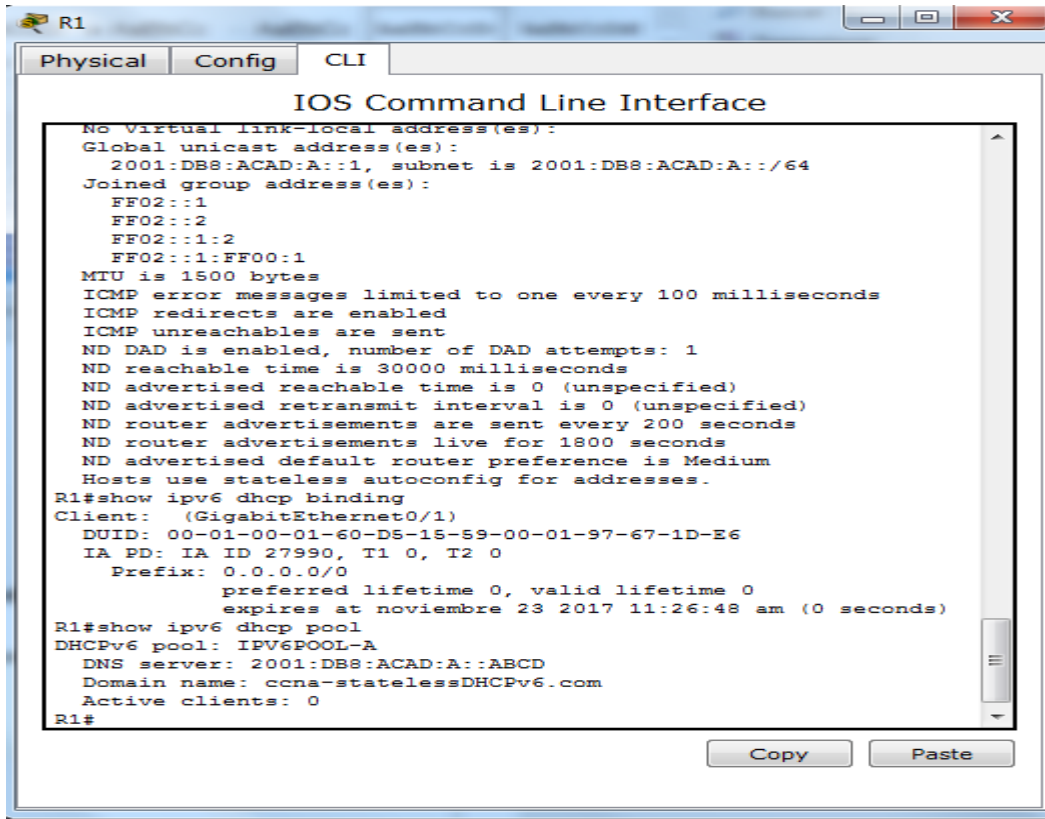
R1# show ipv6 dhcp pool

DHCPv6 pool: IPV6POOL-A

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-statelessDHCPv6.com

Active clients: 0



The screenshot shows the IOS Command Line Interface (CLI) for router R1. The interface is titled "IOS Command Line Interface" and has tabs for "Physical", "Config", and "CLI". The output of the command "show ipv6 dhcp binding" is displayed, showing details for a DHCPv6 pool named "IPV6POOL-A". The output includes the global unicast address (2001:DB8:ACAD:A::1), the subnet (2001:DB8:ACAD:A::/64), and the joined group address (FF02::1). It also shows the MTU (1500 bytes), ICMP error messages limited to one every 100 milliseconds, and ND DAD is enabled. The output of "show ipv6 dhcp pool" shows the DNS server (2001:DB8:ACAD:A::ABCD) and the domain name (ccna-statelessDHCPv6.com). The output of "show ipv6 dhcp binding" shows a client on GigabitEthernet0/1 with a DUID of 00-01-00-01-60-D5-15-S9-00-01-97-67-1D-E6 and an IA PD of 0.0.0.0/0. The output of "show ipv6 dhcp pool" shows the DNS server (2001:DB8:ACAD:A::ABCD) and the domain name (ccna-statelessDHCPv6.com). The output of "show ipv6 dhcp binding" shows 0 active clients.

```

No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-60-D5-15-S9-00-01-97-67-1D-E6
IA PD: IA ID 27990, T1 0, T2 0
  Prefix: 0.0.0.0/0
         preferred lifetime 0, valid lifetime 0
         expires at noviembre 23 2017 11:26:48 am (0 seconds)
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
R1#
```

## Paso 6. restablecer la configuración de red IPv6 de la PC-A.

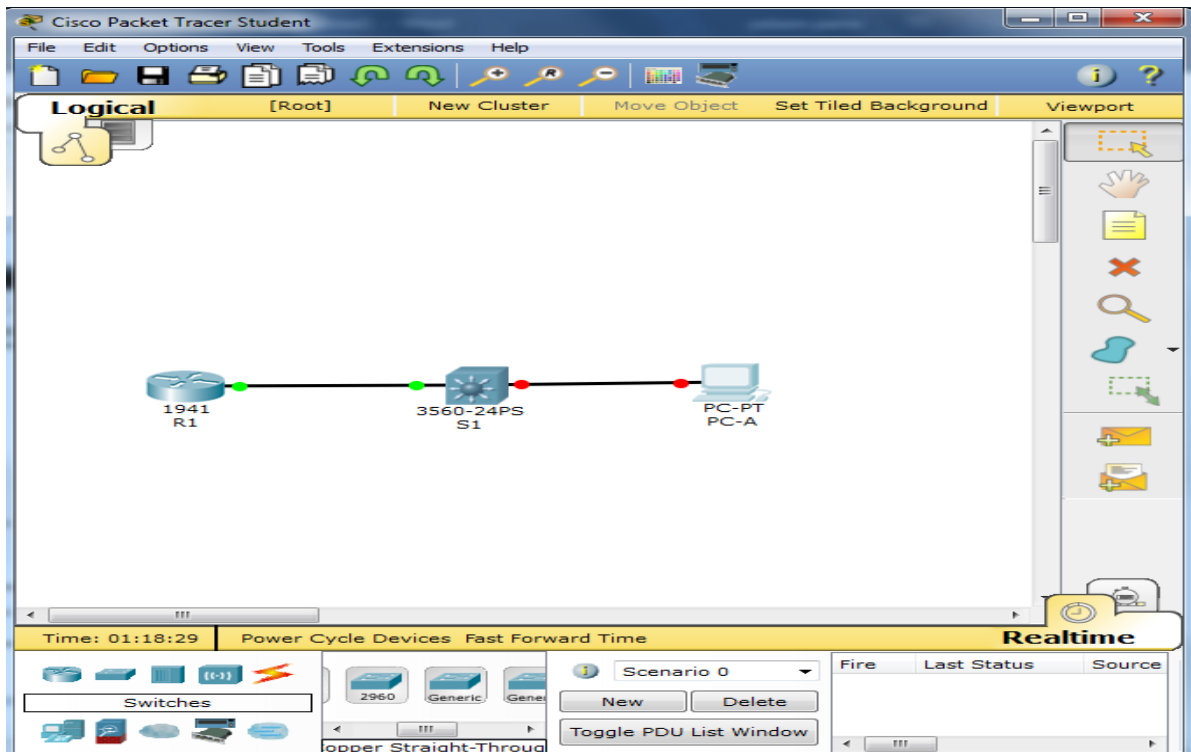
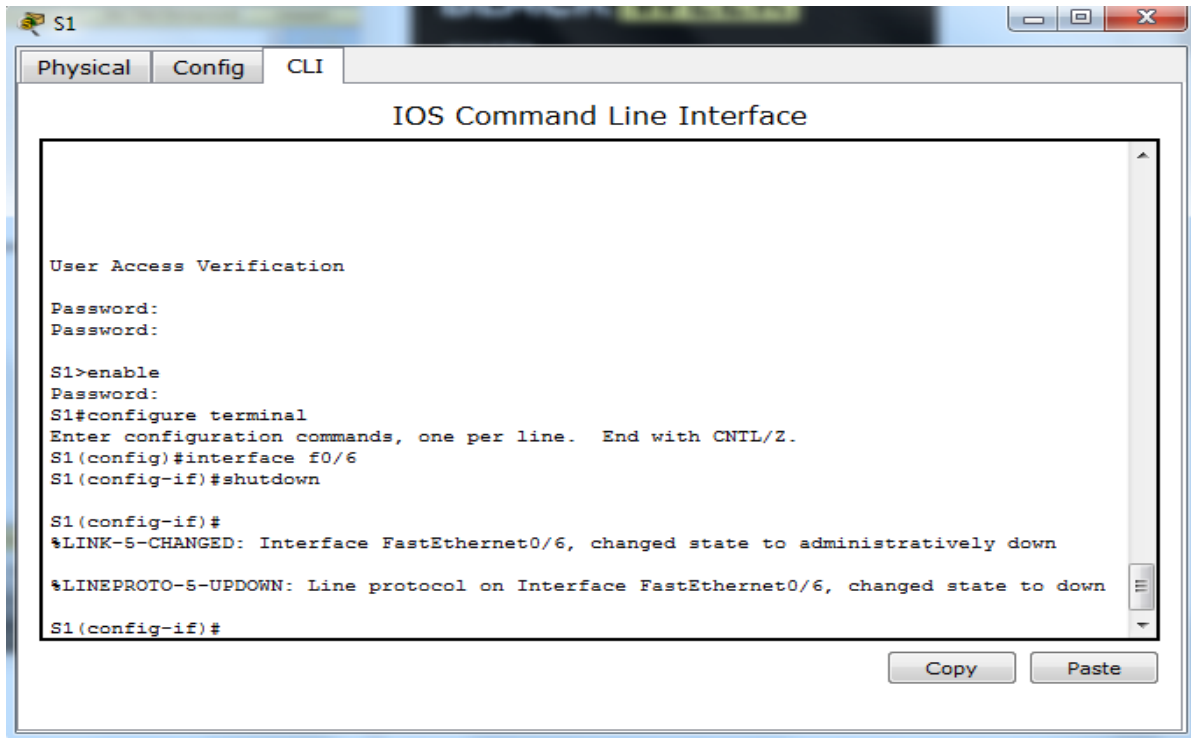
- Desactive la interfaz F0/6 del S1.

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

S1(config)# **interface f0/6**

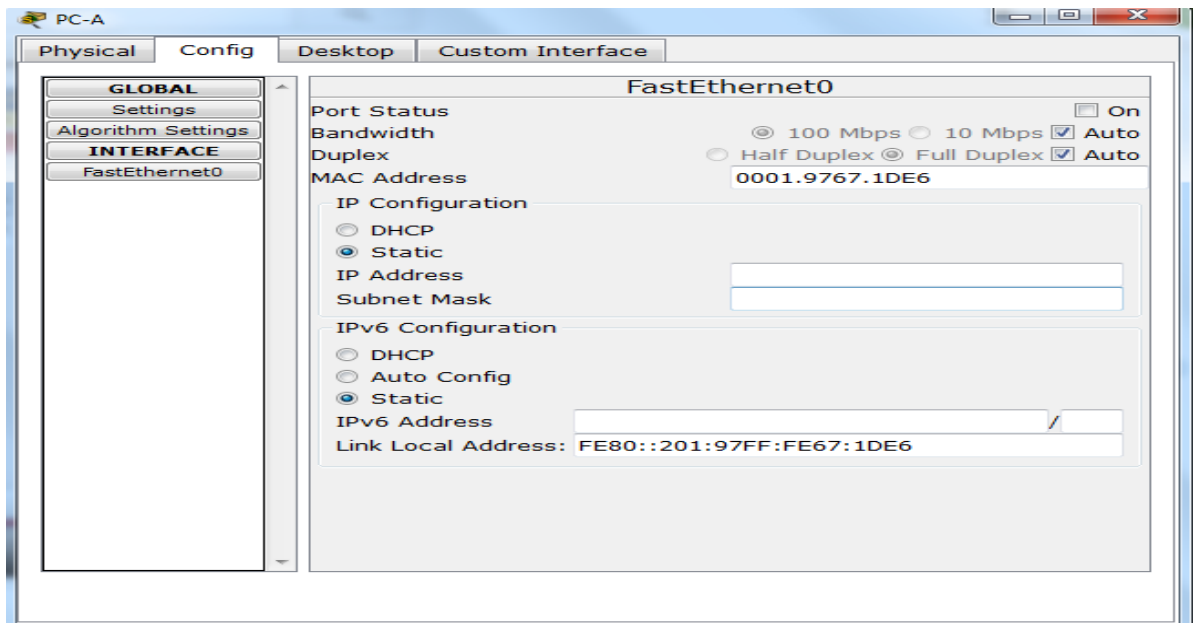
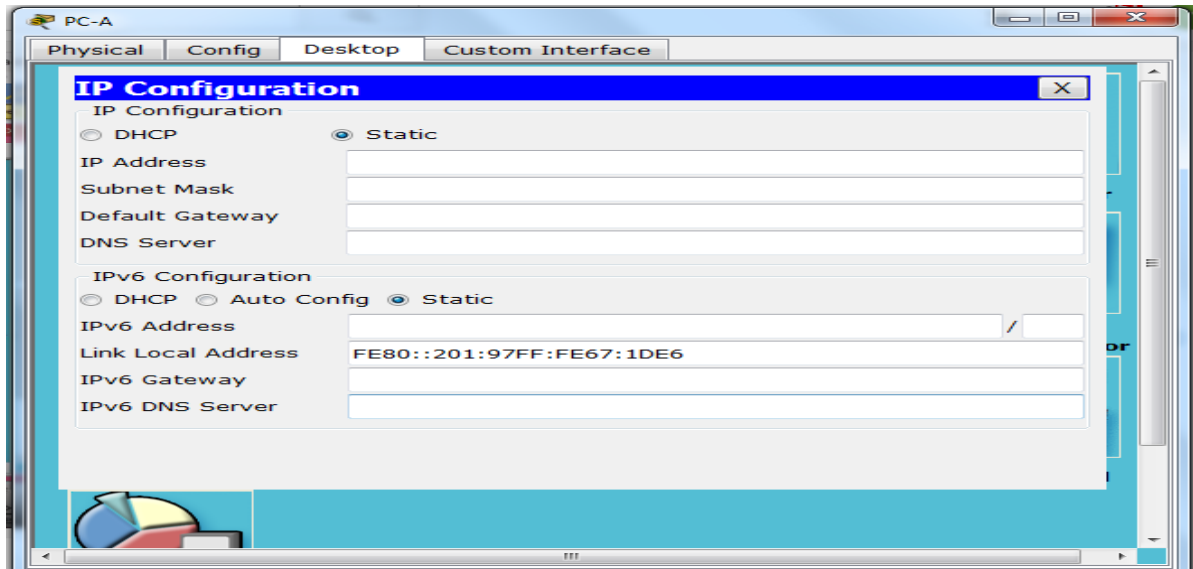
S1(config-if)# **shutdown**





- Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.
- Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.

- 1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.

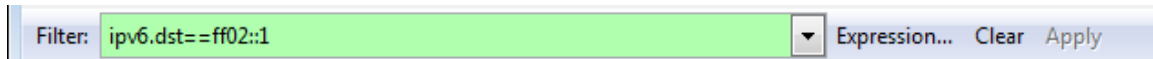


- 2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

#### Parte 4. configurar la red para DHCPv6 con estado

##### Paso 1. preparar la PC-A.

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

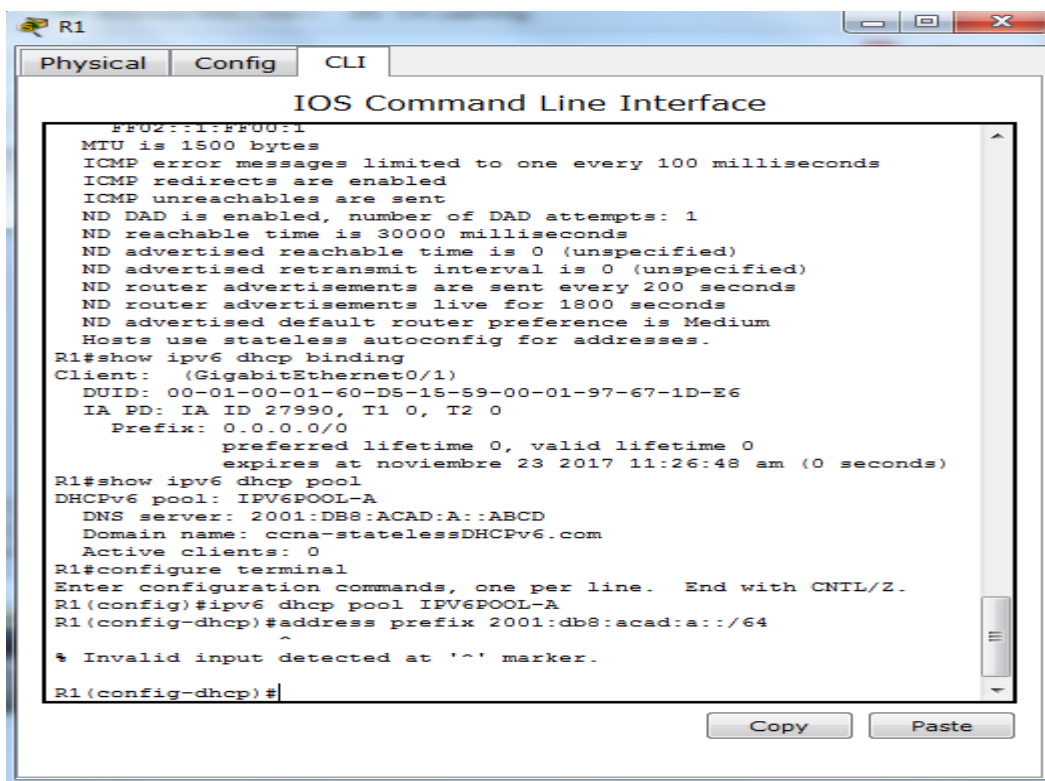


##### Paso 2. cambiar el pool de DHCPv6 en el R1.

- Agregue el prefijo de red al pool.

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

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



- Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.

**Nota:** debe eliminar el antiguo nombre de dominio. El comando **domain-name** no lo reemplaza.

```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com
```

```
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
```

```
R1(config-dhcpv6)# end
```

```
R1
Physical Config CLI
IOS Command Line Interface
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-60-D5-15-59-00-01-97-67-1D-E6
IA PD: IA ID 27990, T1 0, T2 0
Prefix: 0.0.0.0/0
        preferred lifetime 0, valid lifetime 0
        expires at noviembre 23 2017 11:26:48 am (0 seconds)
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.
R1(config-dhcp)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcp)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

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

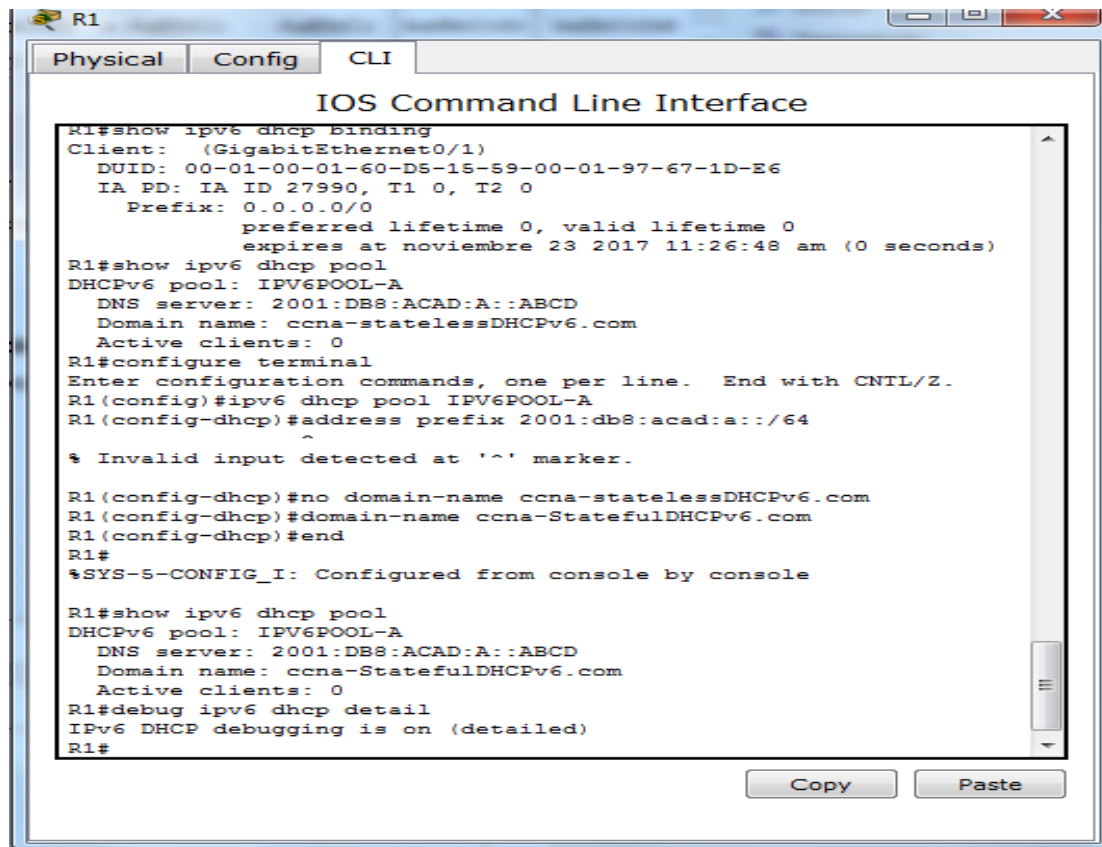
Active clients: 0

```
R1
Physical Config CLI
IOS Command Line Interface
ND advertised default Router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-60-DS-15-59-00-01-97-67-1D-E6
IA PD: IA ID 27990, T1 0, T2 0
Prefix: 0.0.0.0/0
        preferred lifetime 0, valid lifetime 0
        expires at noviembre 23 2017 11:26:48 am (0 seconds)
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.
R1(config-dhcp)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcp)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 0
R1#
```

d. Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

**R1# debug ipv6 dhcp detail**

IPv6 DHCP debugging is on (detailed)



The screenshot shows a terminal window titled "R1" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" where the following commands and outputs are shown:

```
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-60-D5-15-59-00-01-97-67-1D-E6
IA PD: IA ID 27990, T1 0, T2 0
Prefix: 0.0.0.0/0
        preferred lifetime 0, valid lifetime 0
        expires at noviembre 23 2017 11:26:48 am (0 seconds)

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

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.

R1(config-dhcp)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcp)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 0

R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R1#
```

**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
```

The screenshot shows a window titled "R1" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" terminal output. The output shows the configuration of a DHCPv6 pool named "IPV6POOL-A" with a DNS server at "2001:DB8:ACAD:A::ABCD" and a domain name of "ccna-StatefulDHCPv6.com". It then shows the configuration of interface "g0/1" being shut down and then brought back up. The terminal output is as follows:

```
R1#debug ipv6 dhcp detail
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 0
R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1
R1(config-if)#shutdown

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

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

R1(config-if)#ipv6 nd managed-config-flag
R1(config-if)#no 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)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

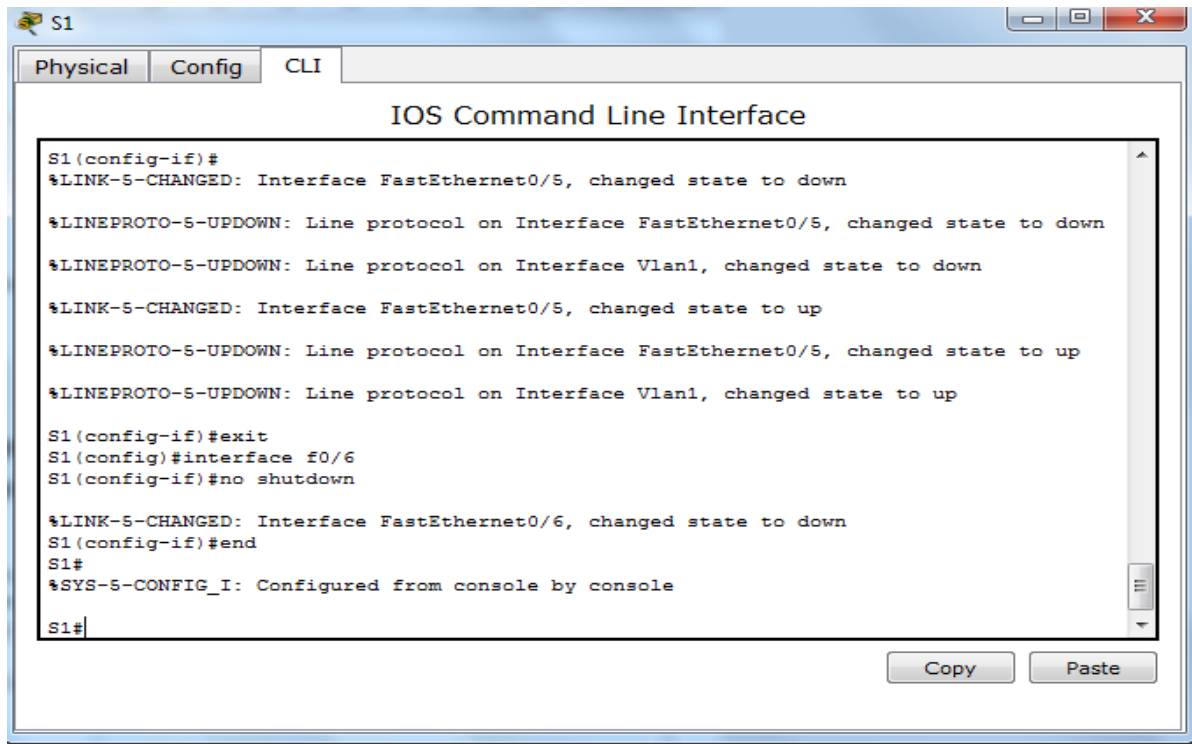
R1#
```

At the bottom of the window, there are "Copy" and "Paste" buttons.

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

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

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



#### Paso 5. verificar la configuración de DHCPv6 con estado en el R1.

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

```
R1# show ipv6 interface g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
```

```
IPv6 is enabled, link-local address is FE80::1
```

```
No Virtual link-local address(es):
```

```
Global unicast address(es):
```

```
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
```

```
Joined group address(es):
```

```
FF02::1
```

```
FF02::2
```

```
FF02::1:2
```

```
FF02::1:FF00:1
```



FF05::1:3

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

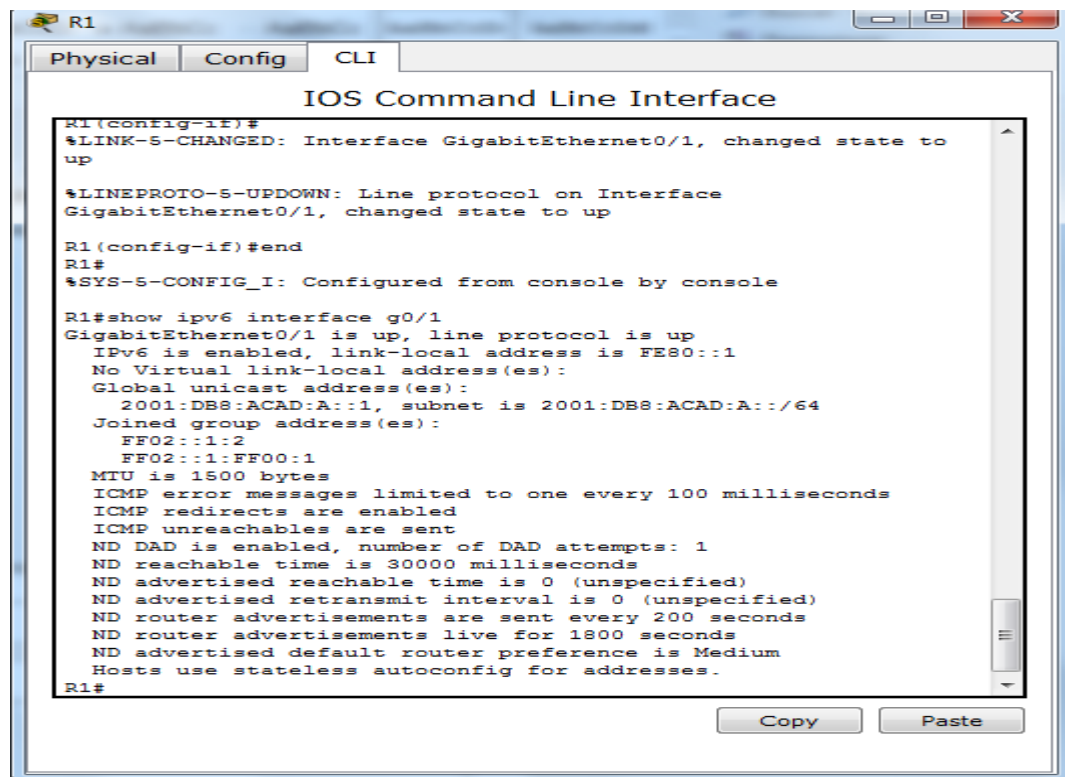
ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use DHCP to obtain routable addresses.

Hosts use DHCP to obtain other configuration.



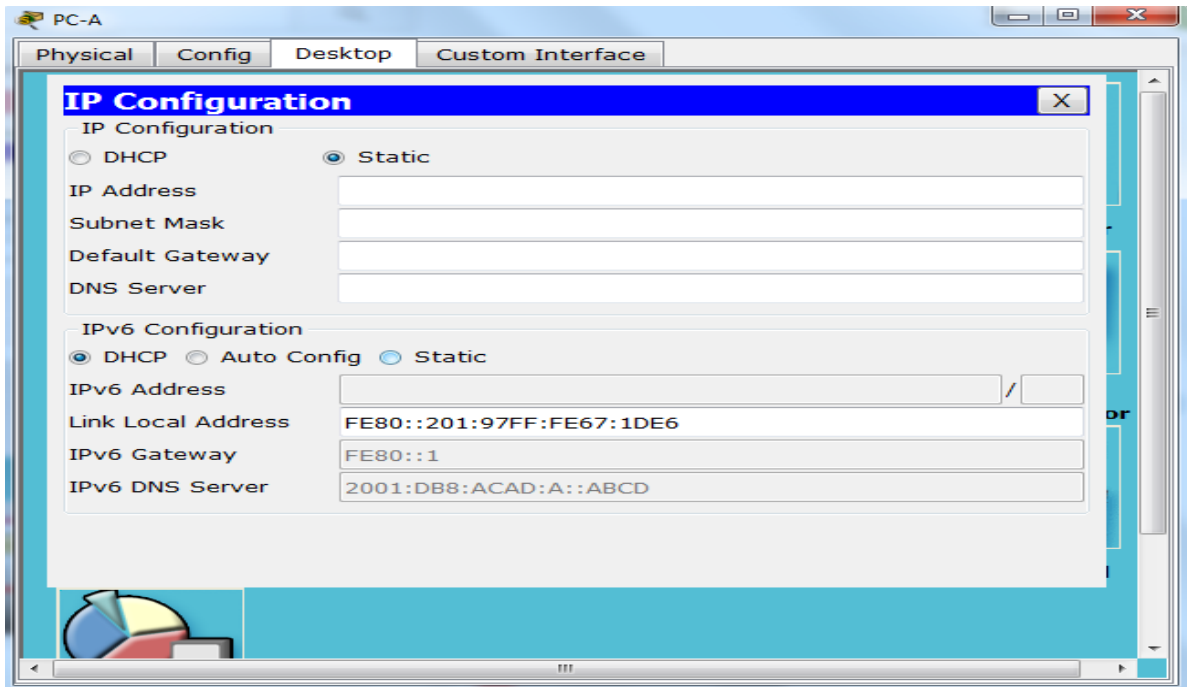
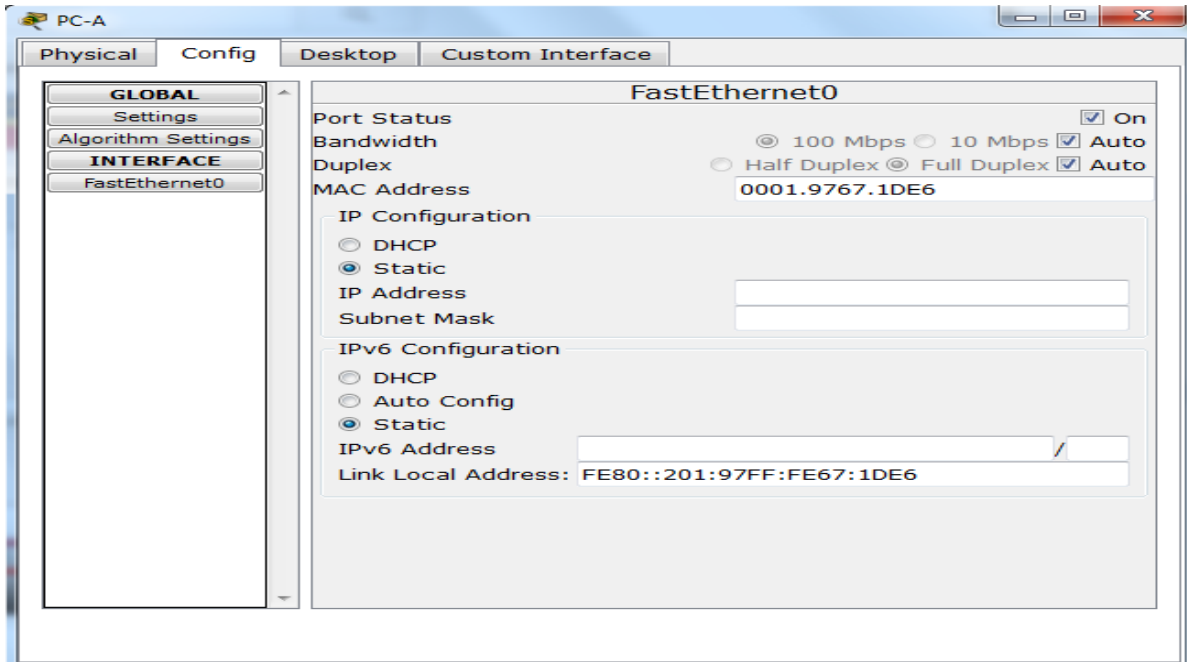
```
R1
Physical Config CLI
IOS Command Line Interface
R1(config-if)#
%LINK-S-CHANGED: Interface GigabitEthernet0/1, changed state to
up

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

R1(config-if)#end
R1#
%SYS-S-CONFIG_I: Configured from console by console

R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FE02::1:2
  FE02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#
```

- 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.

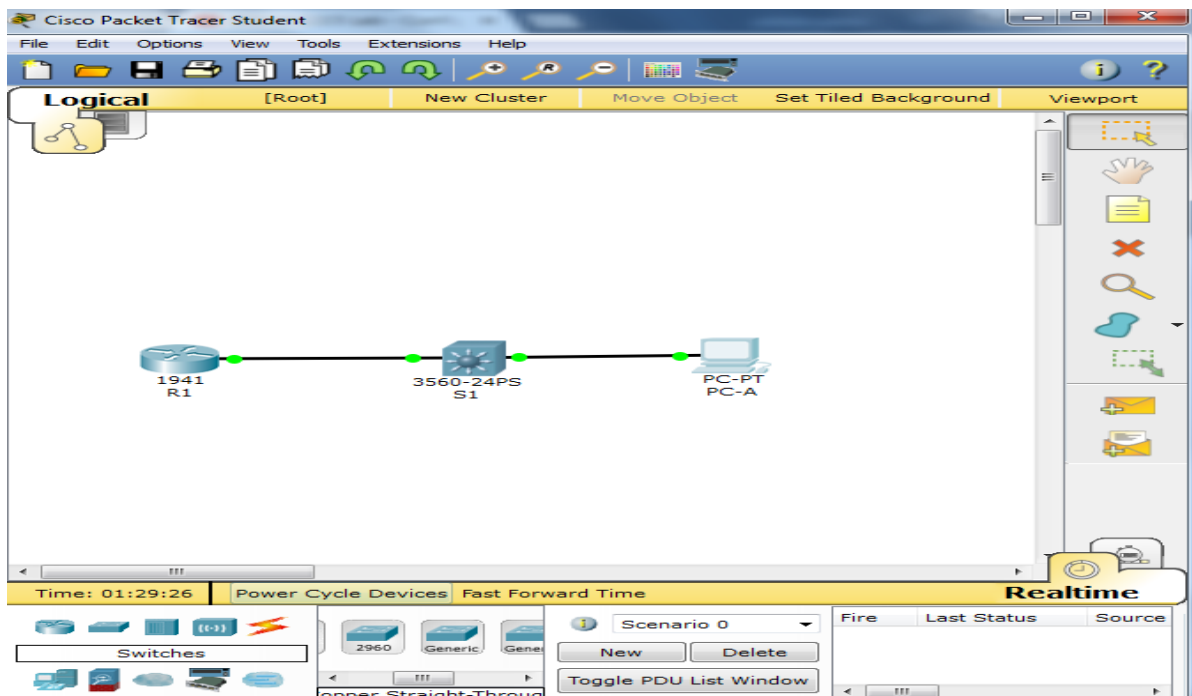




```
R1
Physical Config CLI
IOS Command Line Interface
*mar 1 01:27:13.726: option SERVERID(2), len 24
*mar 1 01:27:13.726: preferred 0, valid 0, prefix 0.0.0.0/0
*mar 1 01:27:13.726: IPv6 DHCP: Using interface pool IPV6POOL-A
*mar 1 01:27:13.726: IPv6 DHCP: Creating binding for
FE80::201:97FF:FE67:1DE6 in pool IPV6POOL-A
*mar 1 01:27:13.726: IPv6 DHCP: Allocating IA_PD 27990 in binding
for FE80::201:97FF:FE67:1DE6
*mar 1 01:27:13.726: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in
binding for FE80::201:97FF:FE67:1DE6, IAID 27990

*mar 1 01:27:13.726: IPv6 DHCP: Sending REPLY to
FE80::201:97FF:FE67:1DE6 on GigabitEthernet0/1
*mar 1 01:27:13.726: IPv6 DHCP: detailed packet contents
*mar 1 01:27:13.726:   src FE80::1 (GigabitEthernet0/1)
*mar 1 01:27:13.726:   dst FE80::201:97FF:FE67:1DE6
(GigabitEthernet0/1)
*mar 1 01:27:13.726:   type REPLY(7), xid 2
*mar 1 01:27:13.726:   option SERVERID(2), len 24
*mar 1 01:27:13.726:     0003000100400BCC801
*mar 1 01:27:13.726:   option CLIENTID(1), len 45
*mar 1 01:27:13.726:     00-01-00-01-60-D5-15-S9-00-01-97-67-1D-
E6
*mar 1 01:27:13.726:   option IA-PD(25), len 41
*mar 1 01:27:13.726:     IAID 0x27990, T1 0, T2 0
*mar 1 01:27:13.726:   option IAPREFIX(26), len 29
*mar 1 01:27:13.726:     preferred 0, valid 0, prefix 0.0.0.0/0
*mar 1 01:27:13.726:   option DNS-SERVERS(23), len 20
*mar 1 01:27:13.726:     2001:DB8:ACAD:A::ABCD
*mar 1 01:27:13.726:   option DOMAIN-LIST(24), len 5
*mar 1 01:27:13.726:     ccna-StatefulDHCPv6.com

R1#
R1#
```



c. Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

R1# **show ipv6 dhcp pool**

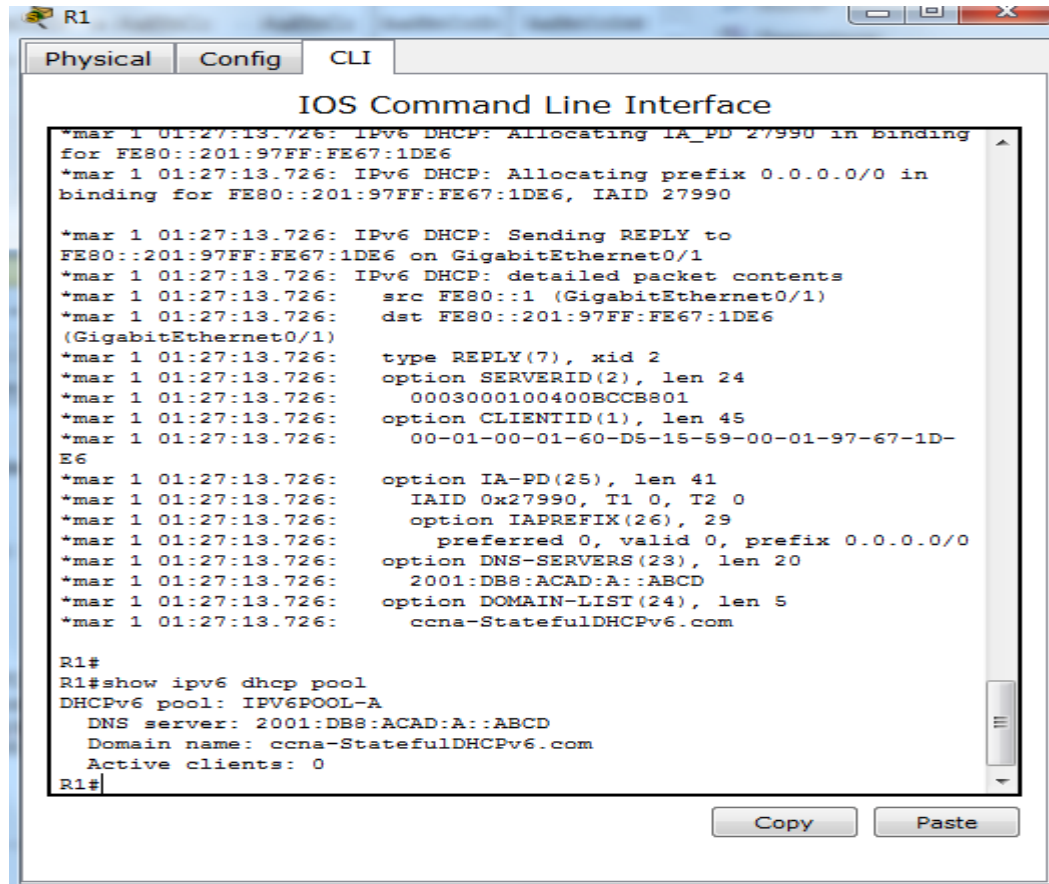
DHCPv6 pool: IPV6POOL-A

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



```
R1
Physical Config CLI
IOS Command Line Interface
*mar 1 01:27:13.726: IPv6 DHCP: Allocating IA_PD 27990 in binding
for FE80::201:97FF:FE67:1DE6
*mar 1 01:27:13.726: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in
binding for FE80::201:97FF:FE67:1DE6, IAID 27990
*mar 1 01:27:13.726: IPv6 DHCP: Sending REPLY to
FE80::201:97FF:FE67:1DE6 on GigabitEthernet0/1
*mar 1 01:27:13.726: IPv6 DHCP: detailed packet contents
*mar 1 01:27:13.726:   src FE80::1 (GigabitEthernet0/1)
*mar 1 01:27:13.726:   dst FE80::201:97FF:FE67:1DE6
(GigabitEthernet0/1)
*mar 1 01:27:13.726:   type REPLY(7), xid 2
*mar 1 01:27:13.726:   option SERVERID(2), len 24
0003000100400BCCB801
*mar 1 01:27:13.726:   option CLIENTID(1), len 45
00-01-00-01-60-D5-15-S9-00-01-97-67-1D-
E6
*mar 1 01:27:13.726:   option IA-PD(25), len 41
*mar 1 01:27:13.726:   IAID 0x27990, T1 0, T2 0
*mar 1 01:27:13.726:   option IAPREFIX(26), 29
preferred 0, valid 0, prefix 0.0.0.0/0
*mar 1 01:27:13.726:   option DNS-SERVERS(23), len 20
2001:DB8:ACAD:A::ABCD
*mar 1 01:27:13.726:   option DOMAIN-LIST(24), len 5
ccna-StatefulDHCPv6.com
R1#
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 0
R1#
```

- d. 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)

```

R1
Physical Config CLI
IOS Command Line Interface
*mar 1 01:27:13.726: IPv6 DHCP: detailed packet contents
*mar 1 01:27:13.726: src FE80::1 (GigabitEthernet0/1)
*mar 1 01:27:13.726: dst FE80::201:97FF:FE67:1DE6
(GigabitEthernet0/1)
*mar 1 01:27:13.726: type REPLY(7), xid 2
*mar 1 01:27:13.726: option SERVERID(2), len 24
*mar 1 01:27:13.726: 0003000100400BCCB801
*mar 1 01:27:13.726: option CLIENTID(1), len 45
*mar 1 01:27:13.726: 00-01-00-01-60-D5-15-S9-00-01-97-67-1D-
E6
*mar 1 01:27:13.726: option IA-PD(25), len 41
*mar 1 01:27:13.726: IAID 0x27990, T1 0, T2 0
*mar 1 01:27:13.726: option IAPREFIX(26), 29
*mar 1 01:27:13.726: preferred 0, valid 0, prefix 0.0.0.0/0
*mar 1 01:27:13.726: option DNS-SERVERS(23), len 20
*mar 1 01:27:13.726: 2001:DB8:ACAD:A::ABCD
*mar 1 01:27:13.726: option DOMAIN-LIST(24), len 5
*mar 1 01:27:13.726: ccna-StatefulDHCPv6.com

R1#
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 0
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-60-D5-15-S9-00-01-97-67-1D-E6
IA PD: IA ID 27990, T1 0, T2 0
Prefix: 0.0.0.0/0
preferred lifetime 0, valid lifetime 0
expires at noviembre 23 2017 11:43:11 am (0 seconds)
R1#
Copy Paste

```

```

Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . : ccna-StatefulDHCPv6.com
Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
Dirección física. . . . . : 00-0C-29-E3-23-17
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce<Preferido>
Concesión obtenida. . . . . : jueves, 05 de septiembre de 2013
16:07:59
La concesión expira . . . . . : jueves, 05 de septiembre de 2013
16:38:03
Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
16:38:03
Únculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a::11<Preferido>
Dirección IPv4. . . . . : 192.168.96.139<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::1%11
IAID DHCPv6 . . . . . : 234884137
DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-
E3-23-17
Servidores DNS . . . . . : 2001:db8:acad:a::abcd
NetBIOS sobre TCP/IP. . . . . : habilitado

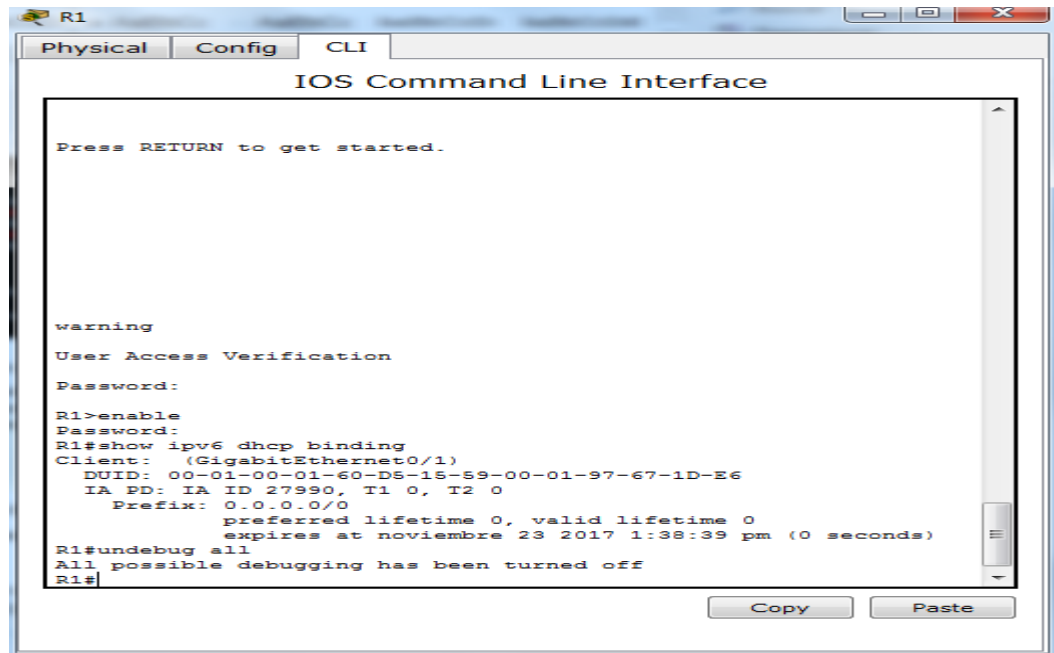
```

- e. Emita el comando **undebg 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 **undebg all** las detiene todas.

R1# **u all**

Se ha desactivado toda depuración posible



f. Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.

1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

\*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

\*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents

\*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

\*Mar 5 16:42:39.775: dst FF02::1:2

\*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238

\*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2

\*Mar 5 16:42:39.775: elapsed-time 6300

\*Mar 5 16:42:39.775: option CLIENTID(1), len 14

2) Examine el mensaje de respuesta enviado a la PC-A con la información de red DHCP.

\*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

\*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents

\*Mar 5 16:42:39.779: src FE80::1

\*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

\*Mar 5 16:42:39.779: type REPLY(7), xid 1039238

\*Mar 5 16:42:39.779: option SERVERID(2), len 10

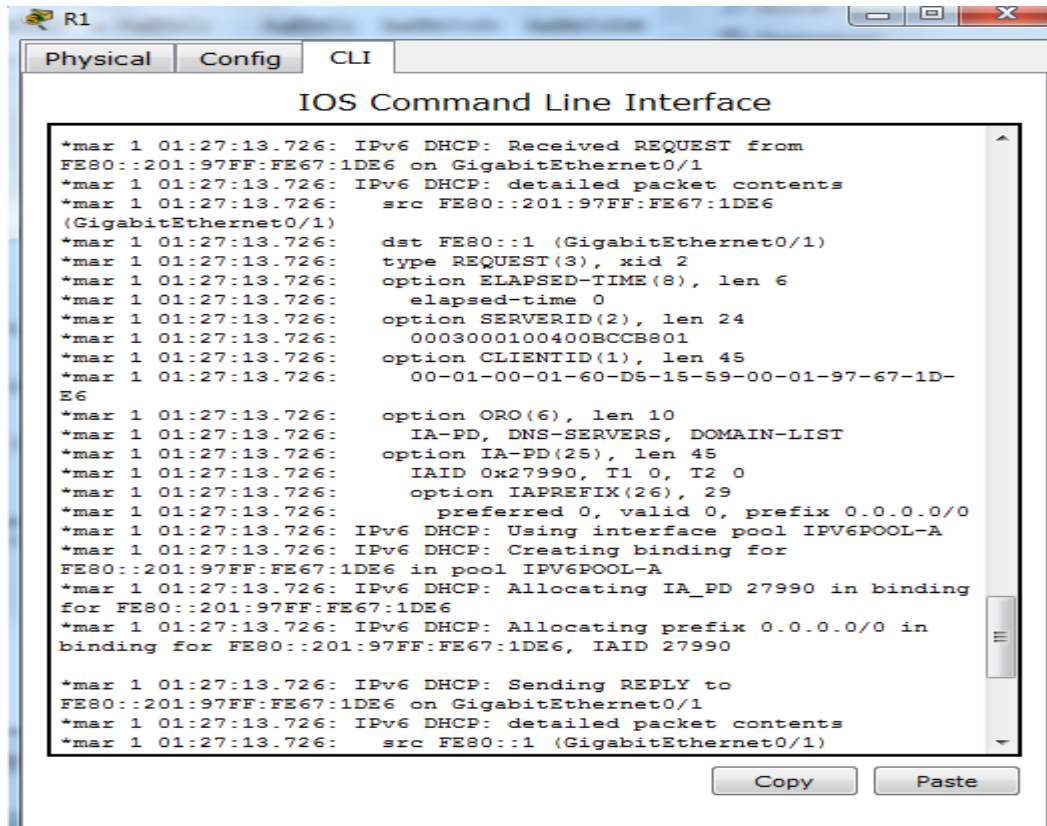
\*Mar 5 16:42:39.779: 00030001FC994775C3E0

\*Mar 5 16:42:39.779: option CLIENTID(1), len 14

\*Mar 5 16:42:39.779: 00010001

R1#17F6723D000C298D5444

- \*Mar 5 16:42:39.779: option IA-NA(3), len 40
- \*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120
- \*Mar 5 16:42:39.779: option IAADDR(5), len 24
- \*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE
- \*Mar 5 16:42:39.779: preferred 86400, valid 172800
- \*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
- \*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
- \*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
- \*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com





```

IOS Command Line Interface
*mar 1 01:27:13.726: option serverid(2), len 24
*mar 1 01:27:13.726: preferred 0, valid 0, prefix 0.0.0.0/0
*mar 1 01:27:13.726: IPv6 DHCP: Using interface pool IPV6POOL-A
*mar 1 01:27:13.726: IPv6 DHCP: Creating binding for
FE80::201:97FF:FE67:1DE6 in pool IPV6POOL-A
*mar 1 01:27:13.726: IPv6 DHCP: Allocating IA_PD 27990 in binding
for FE80::201:97FF:FE67:1DE6
*mar 1 01:27:13.726: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in
binding for FE80::201:97FF:FE67:1DE6, IAID 27990

*mar 1 01:27:13.726: IPv6 DHCP: Sending REPLY to
FE80::201:97FF:FE67:1DE6 on GigabitEthernet0/1
*mar 1 01:27:13.726: IPv6 DHCP: detailed packet contents
*mar 1 01:27:13.726: src FE80::1 (GigabitEthernet0/1)
*mar 1 01:27:13.726: dst FE80::201:97FF:FE67:1DE6
(GigabitEthernet0/1)
*mar 1 01:27:13.726: type REPLY(7), xid 2
*mar 1 01:27:13.726: option SERVERID(2), len 24
*mar 1 01:27:13.726: 0003000100400BCCB801
*mar 1 01:27:13.726: option CLIENTID(1), len 45
*mar 1 01:27:13.726: 00-01-00-01-60-DS-15-S9-00-01-97-67-1D-
E6
*mar 1 01:27:13.726: option IA-PD(25), len 41
*mar 1 01:27:13.726: IAID 0x27990, T1 0, T2 0
*mar 1 01:27:13.726: option IAPREFIX(26), len 29
*mar 1 01:27:13.726: preferred 0, valid 0, prefix 0.0.0.0/0
*mar 1 01:27:13.726: option DNS-SERVERS(23), len 20
*mar 1 01:27:13.726: 2001:DB8:ACAD:A:ABCD
*mar 1 01:27:13.726: option DOMAIN-LIST(24), len 5
*mar 1 01:27:13.726: ccna-StatefulDHCPv6.com

R1#
R1#
Copy Paste

```

**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).

Filter: `ipv6.dst==ff02::1` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
36	54.582255	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
265	215.309226	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
425	373.272435	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
553	554.893786	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
664	730.139576	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
775	922.720109	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1

Frame 775: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: IPv6mcast\_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
  - Type: Router Advertisement (134)
  - Code: 0
  - Checksum: 0x3a82 [correct]
  - Cur hop limit: 64
  - Flags: 0xc0
    - 1... .. = Managed address configuration: Set
    - ..1.. .. = Other configuration: Set
    - ..0. .... = Home Agent: Not set
    - ...0 0... = Prf (Default Router Preference): Medium (0)
    - .... .0.. = Proxy: Not set
    - .... .0. = Reserved: 0
  - Router lifetime (s): 1800

- c. Cambie el filtro en Wireshark para ver solo los paquetes **DHCPv6** escribiendo `dhcpv6` y, a continuación, haga clic en **Apply** (Aplicar). Resalte la última respuesta DHCPv6 de la lista y

expanda la información de DHCPv6. Examine la información de red DHCPv6 incluida en este paquete.

No.	Time	Source	Destination	Protocol	Length	Info
250	443.078236	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
267	475.083284	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
425	656.281211	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0xc86c32 CID: 0001000117f6723d000c2
429	656.282249	fe80::1	fe80::d428:7de2:997ff02::1:2	DHCPv6	191	Advertise XID: 0xc86c32 CID: 0001000117f6723d000c2
460	657.292018	fe80::d428:7de2:997ff02::1:2		DHCPv6	188	Request XID: 0xc86c32 CID: 0001000117f6723d000c2
462	657.292638	fe80::1	fe80::d428:7de2:997ff02::1:2	DHCPv6	191	Reply XID: 0xc86c32 CID: 0001000117f6723d000c298

<ul style="list-style-type: none"> <li>⊟ Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: vmware_be:6c:89 (00:50:56:be:6c:89)</li> <li>⊟ Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)</li> <li>⊟ User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)</li> <li>⊟ DHCPv6 <ul style="list-style-type: none"> <li>Message type: Reply (7)</li> <li>Transaction ID: 0xc86c32</li> <li>⊟ Server Identifier: 00030001fc994775c3e0</li> <li>⊟ Client Identifier: 0001000117f6723d000c298d5444</li> <li>⊟ Identity Association for Non-temporary Address <ul style="list-style-type: none"> <li>Option: Identity Association for Non-temporary Address (3)</li> <li>Length: 40</li> <li>Value: 0e000c290000a8c000010e000005001820010db8acad000a...</li> <li>IAID: 0e000c29</li> <li>T1: 43200</li> <li>T2: 69120</li> <li>⊟ IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce</li> </ul> </li> <li>⊟ DNS recursive name server <ul style="list-style-type: none"> <li>Option: DNS recursive name server (23)</li> <li>Length: 16</li> <li>Value: 20010db8acad000a000000000000abcd</li> <li>DNS servers address: 2001:db8:acad:a:abcd</li> </ul> </li> <li>⊟ Domain Search List <ul style="list-style-type: none"> <li>Option: Domain Search List (24)</li> <li>Length: 25</li> <li>Value: 1363636e612d537461746566756c44484350763603636f6d...</li> <li>DNS Domain Search List <ul style="list-style-type: none"> <li>Domain: ccna-statefulDHCPv6.com</li> </ul> </li> </ul> </li> </ul> </li> </ul>
---

## Reflexión

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

**DHCPv6 con estado usa más recursos de memoria, pero DHCPv6 con estado requiere que el enrutador almacene información de estado dinámico sobre los clientes de DHCPv6 Los clientes.**

**DHCPv6 sin estado no usan el servidor DHCP para obtener información de dirección, por lo que esta información no necesita almacenarse**

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

**Cisco recomienda la DHCPv6 sin estado cuando implementan y desarrollan redes en IPv6 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.

### 10.3.1.1 IoE and DHCP Instructions

#### IdT y DHCP

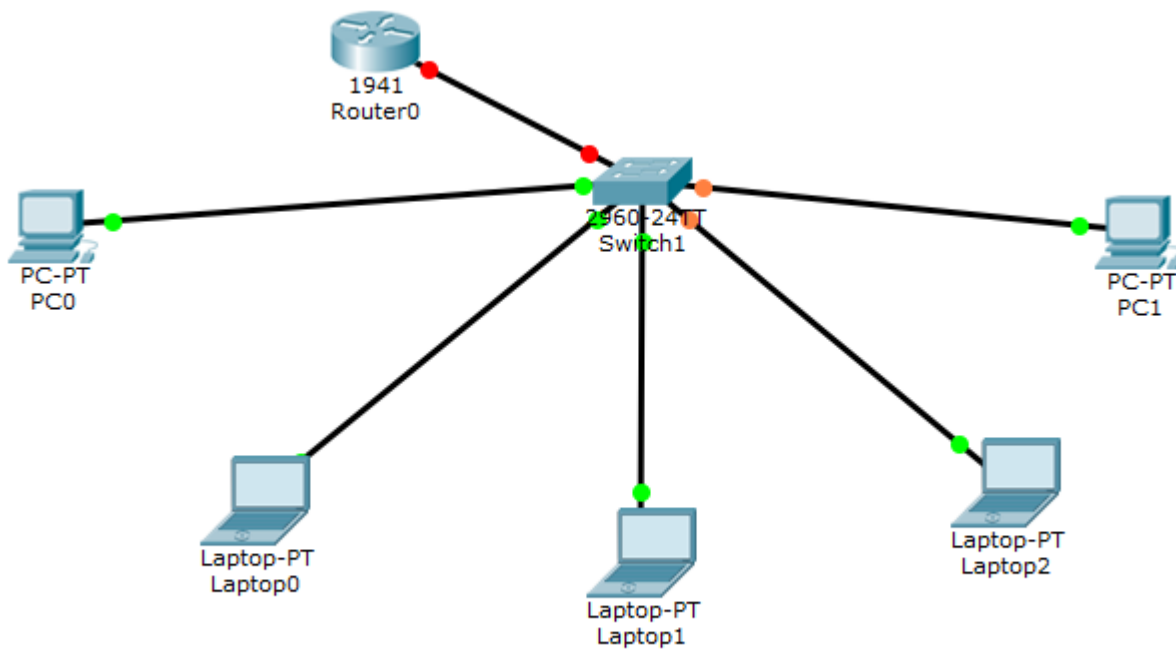
#### Objetivo

Configure DHCP para IPv4 o IPv6 en un router Cisco 1941.

#### Recursos necesarios

Software de Packet Tracer

#### SOLUCION



## Configuración inicial del Router =>

- Asignamos nombre e IP de la interface G0/1 al router:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#Hostname R1
R1(config)#int g0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no Sh

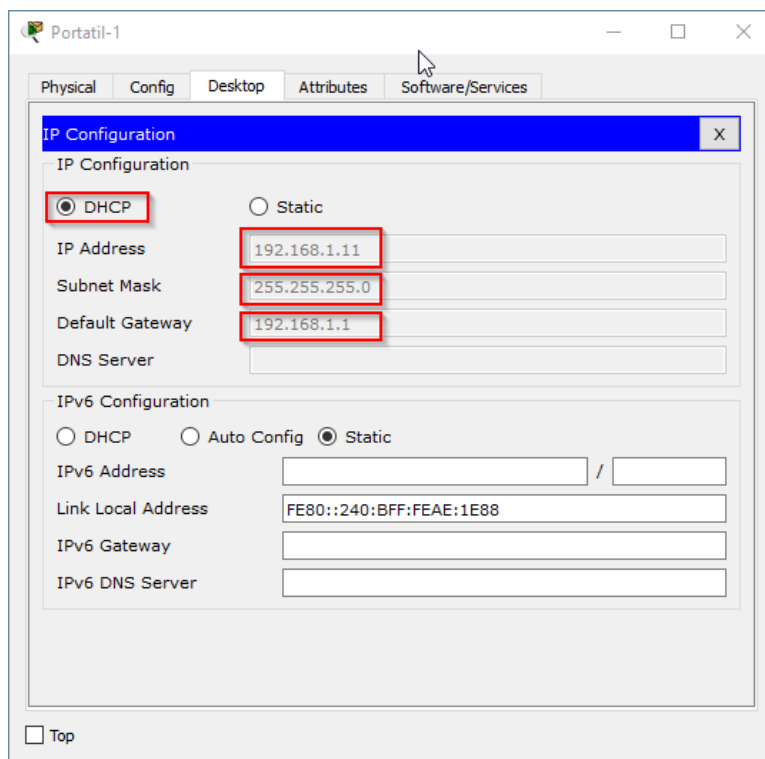
R1(config-if)#
%LINK-S-CHANGED: Interface GigabitEthernet0/1, changed state to
up
```

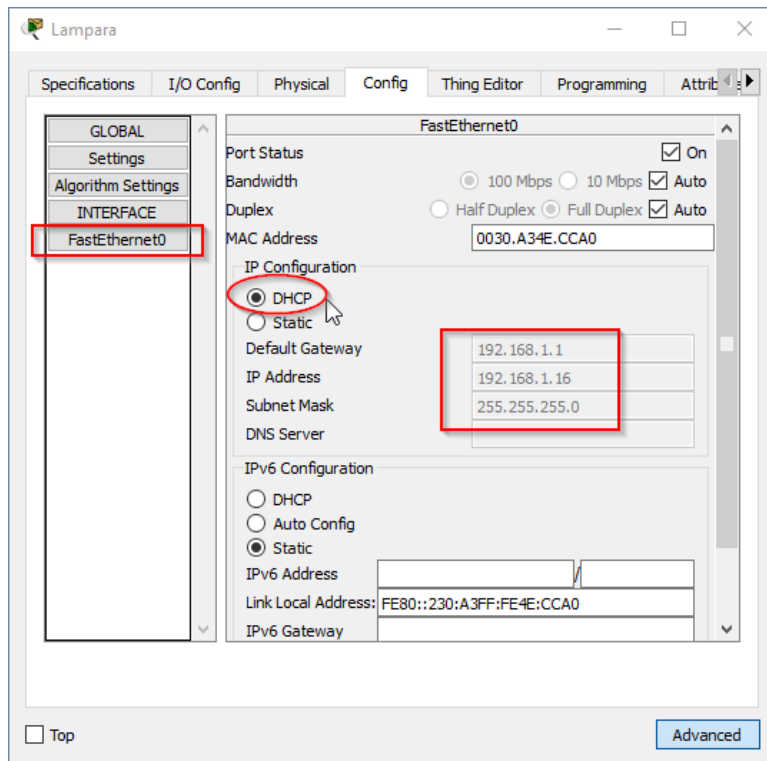
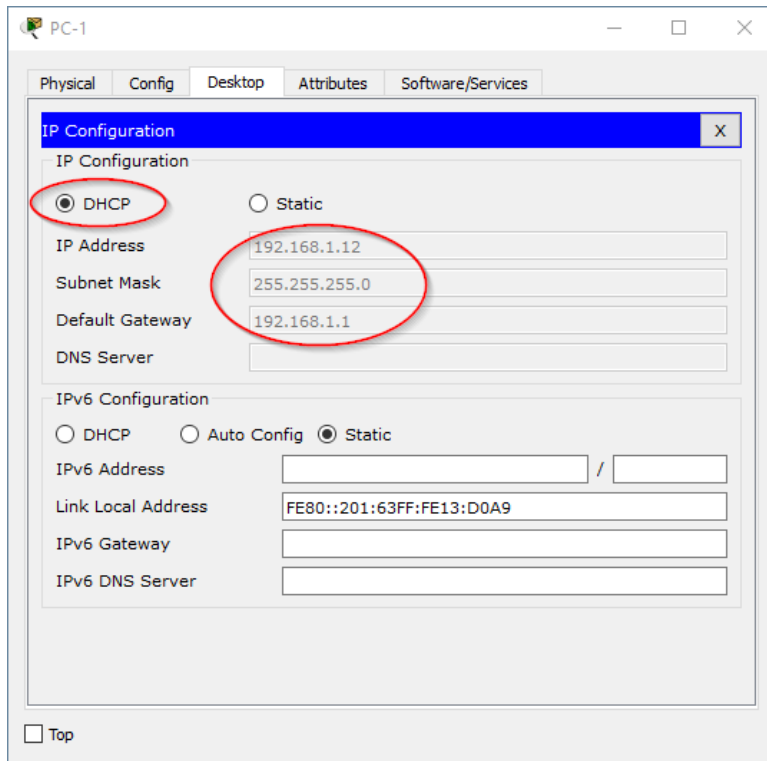
- Configuramos la parte del DHCP(que asigne ip's de la 192.168.1.11 en adelante):

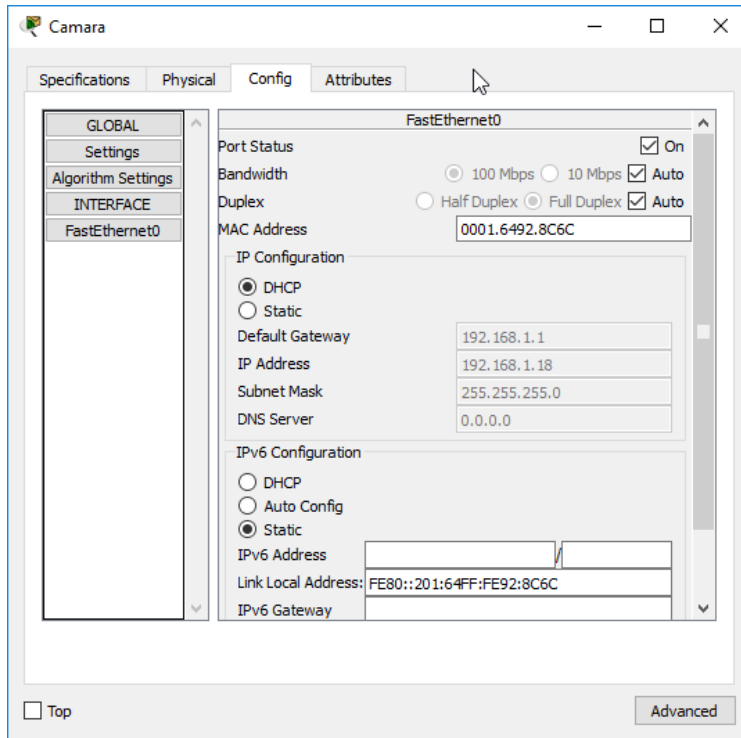
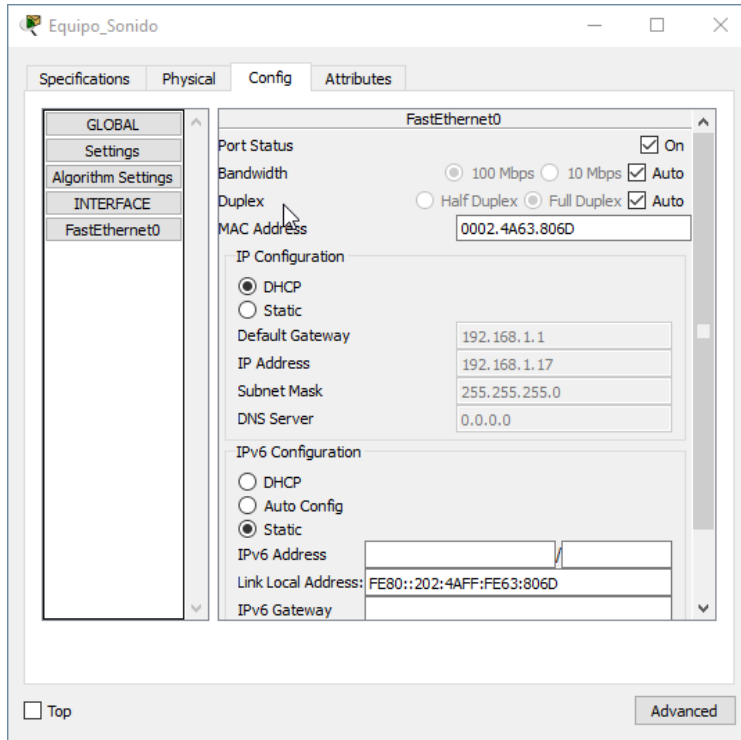
```
R1(config-if)#exit
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
R1(config)#ip dhcp pool LAN
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#exit
R1(config)#
```

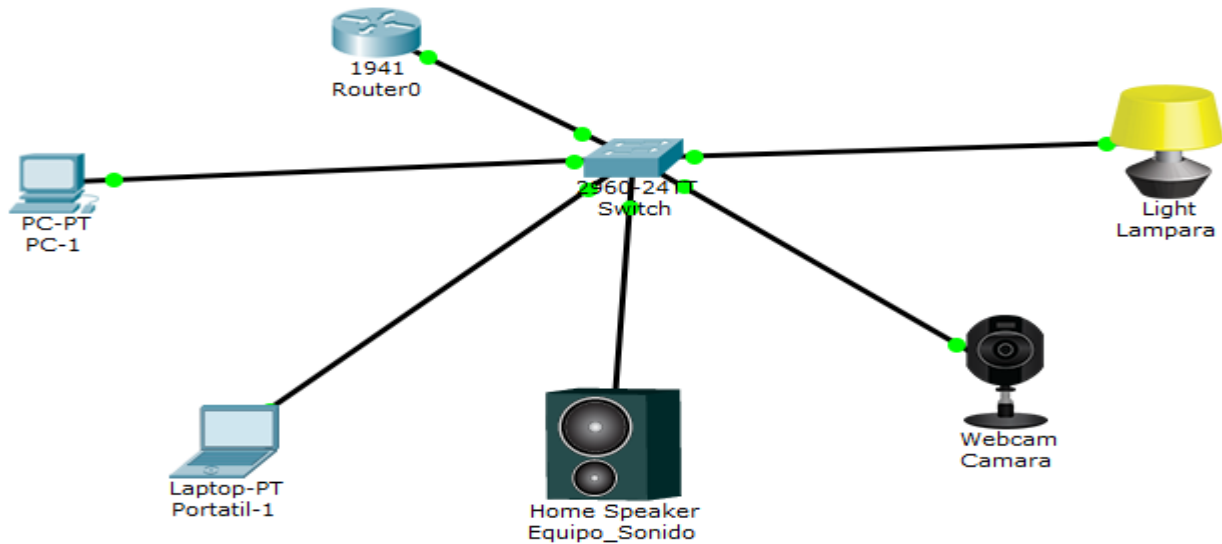
## Configuración de los dispositivos =>

- Creamos el direccionamiento automático en los diferentes dispositivos:

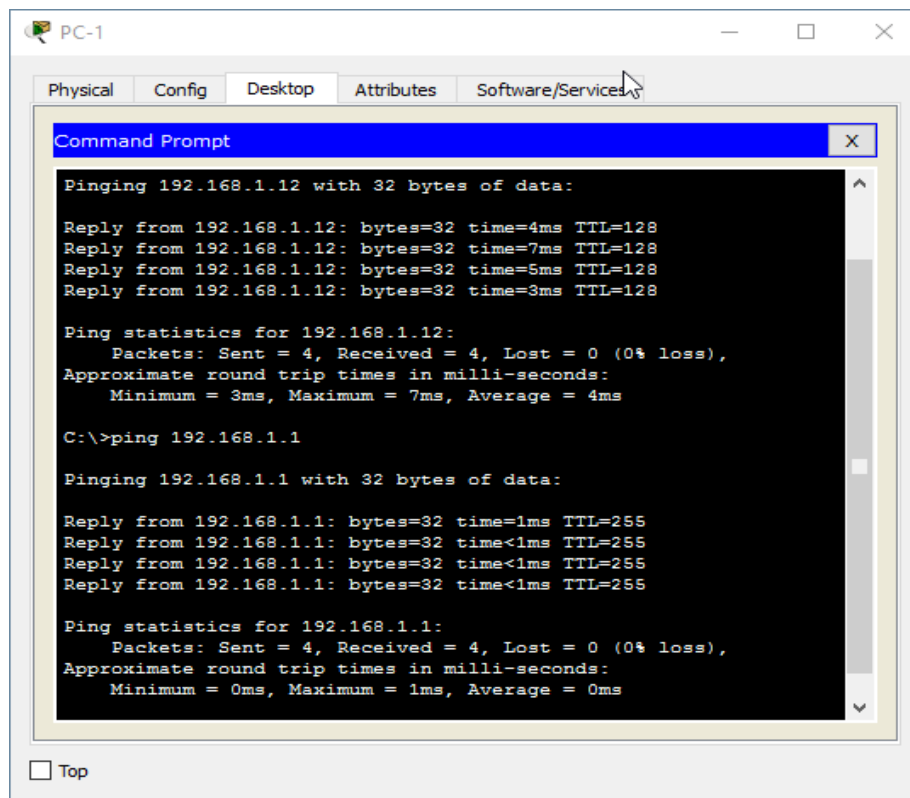








Probamos conectividad entre equipos y router =>



## Reflexión

1. ¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica?  
¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?

Porque el Router 1941 ofrece una amplia gama de servicios de seguridad en comparación con otros ISR por lo cual es más confiable si de prestaciones y seguridad se trata. Pero si se puede



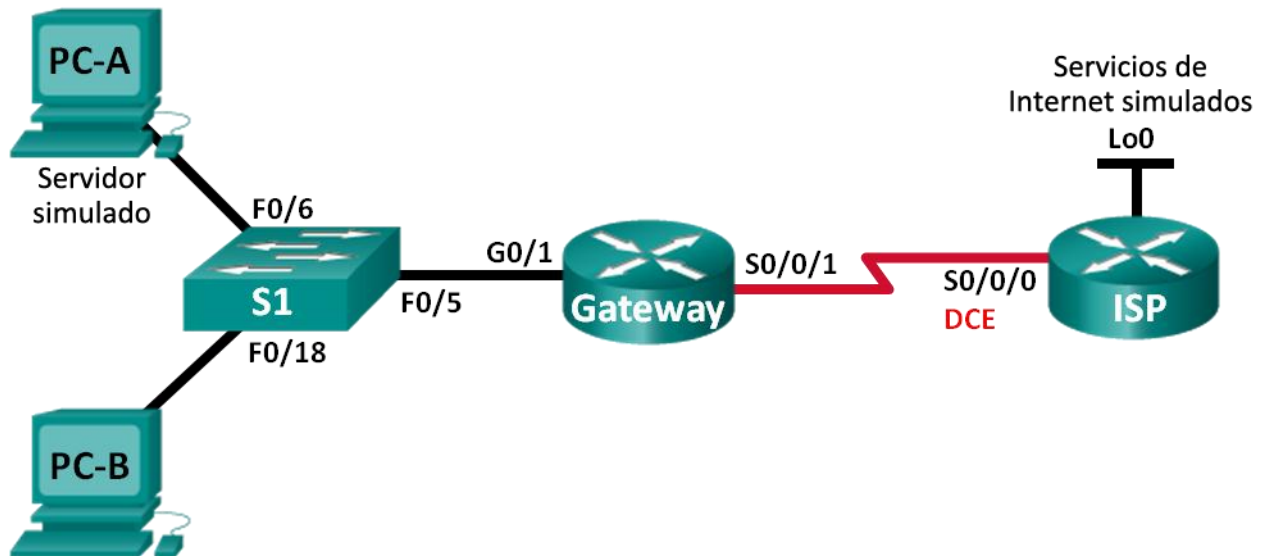
usar un ISR mas pequeño como servidor dhcp, pero el rendimiento es menor y puede ser vulnerable a ataques informáticos. \_\_

2. ¿Cómo cree que las pequeñas y medianas empresas pueden usar la asignación de direcciones IP de DHCP en el mundo de las redes IPv6 e IdT? Mediante la técnica de la lluvia de ideas, piense y registre cinco respuestas posibles.

- Control de Electrodomesticos (Domotica) en el hogar u oficina.
- Identificación de errores de dispositivos de Red para su correspondiente mantenimiento.
- Sistemas cerrados de televisión (Vigilancia).
- Control de Procesos de una empresa atraves de una red dhcp.
- Control y monitoreo de PLC's, IED's y cualquier elemento de una Red en cualquier Empresa

### 11.2.2.6 Lab – Configuring Dynamic and Static NAT

#### Topología



## Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.1 8	255.255.255.25 2	N/A
ISP	S0/0/0 (DCE)	209.165.201.1 7	255.255.255.25 2	N/A
	G0/0	192.31.7.1	255.255.255.0	N/A
Server ISP	NIC	192.31.7.2	255.255.255.0	192.31.7.1
PC-A (servidor simulado)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

## Objetivos

**Parte 1: armar la red y verificar la conectividad**

**Parte 2: configurar y verificar la NAT estática**

**Parte 3: configurar y verificar la NAT dinámica**

## 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 5. armar la red y verificar la conectividad**

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

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

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

### **Paso 2. configurar los equipos host.**

### **Paso 3. inicializar y volver a cargar los routers y los switches según sea necesario.**

### **Paso 4. configurar los parámetros básicos para cada router.**

- a. Desactive la búsqueda del DNS.
- b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- c. Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.
- d. Configure el nombre del dispositivo como se muestra en la topología.
- e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#username cisco pass
Gateway(config)#username cisco password cisco
Gateway(config)#line console 0
Gateway(config-line)#login local
Gateway(config-line)#logging syn
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#no ip domain-lo
Gateway(config)#no ip domain-lookup
Gateway(config)#enable secret class
Gateway(config)#line vty 0 4
Gateway(config-line)#login local
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit

```

### Paso 5. crear un servidor web simulado en el ISP.

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

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

- Habilite el servicio del servidor HTTP en el ISP.

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

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

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

**(EL PROGRAMA NO PERMITE HACER ESTA CONFIGURACIÓN, EN SU REEMPLAZO COLOCAMOS UN SERVIDOR WEB “SERVER ISP”)**

### Paso 6. configurar el routing estático.

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

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

- Cree una ruta predeterminada del router Gateway al router ISP.

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

**Paso 7. Guardar la configuración en ejecución en la configuración de inicio.**

**Paso 8. Verificar la conectividad de la red**

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

```
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=54ms TTL=255
Reply from 192.168.1.1: bytes=32 time=2ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=21ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 54ms, Average = 19ms
```

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=18ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 7ms
```

- b. Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.

```

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

```

```

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

```

```

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1
L      192.168.1.1/32 is directly connected, GigabitEthernet0/1
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.201.16/30 is directly connected, Serial0/0/1
L      209.165.201.18/32 is directly connected, Serial0/0/1
S*    0.0.0.0/0 [1/0] via 209.165.201.17

```

```

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

```

```

Gateway of last resort is not set

```

```

      192.31.7.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.31.7.0/24 is directly connected, GigabitEthernet0/0
L      192.31.7.1/32 is directly connected, GigabitEthernet0/0
      209.165.200.0/27 is subnetted, 1 subnets
S      209.165.200.224/27 [1/0] via 209.165.201.18
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.201.16/30 is directly connected, Serial0/0/0
L      209.165.201.17/32 is directly connected, Serial0/0/0

```

## Parte 6. 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.

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

```
Gateway# show ip nat translations
```

```
Pro Inside global   Inside local   Outside local   Outside global
```

```
--- 209.165.200.225 192.168.1.20   ---           ---
```

```
Gateway#show ip nat translations
```

```
Pro  Inside global   Inside local   Outside local
```

```
Outside global
```

```
--- 209.165.200.225 192.168.1.20   ---           ---
```

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = 209.165.200.225

¿Quién asigna la dirección global interna?

El router - el proveedor de internet

¿Quién asigna la dirección local interna?

Los administradores de red

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

```
SERVER>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=31ms TTL=254
Reply from 192.31.7.1: bytes=32 time=20ms TTL=254
Reply from 192.31.7.1: bytes=32 time=31ms TTL=254
Reply from 192.31.7.1: bytes=32 time=21ms TTL=254
Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 31ms, Average = 25ms
SERVER>ping 192.31.7.2
Pinging 192.31.7.2 with 32 bytes of data:
Reply from 192.31.7.2: bytes=32 time=38ms TTL=126
Reply from 192.31.7.2: bytes=32 time=16ms TTL=126
Reply from 192.31.7.2: bytes=32 time=39ms TTL=126
Reply from 192.31.7.2: bytes=32 time=36ms TTL=126
Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 39ms, Average = 32ms
```

Gateway# show ip nat translations

Pro Inside global    Inside local    Outside local    Outside global

icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1

--- 209.165.200.225 192.168.1.20 --- ---

```
Gateway#show ip nat translations
Pro Inside global    Inside local    Outside local    Outside
global
icmp 209.165.200.225:37192.168.1.20:37 192.31.7.2:37 192.31.7.2:37
icmp 209.165.200.225:38192.168.1.20:38 192.31.7.2:38 192.31.7.2:38
icmp 209.165.200.225:39192.168.1.20:39 192.31.7.2:39 192.31.7.2:39
icmp 209.165.200.225:40192.168.1.20:40 192.31.7.2:40 192.31.7.2:40
icmp 209.165.200.225:41192.168.1.20:41 192.31.7.1:41 192.31.7.1:41
icmp 209.165.200.225:42192.168.1.20:42 192.31.7.1:42 192.31.7.1:42
icmp 209.165.200.225:43192.168.1.20:43 192.31.7.1:43 192.31.7.1:43
icmp 209.165.200.225:44192.168.1.20:44 192.31.7.1:44 192.31.7.1:44
icmp 209.165.200.225:45192.168.1.20:45 192.31.7.2:45 192.31.7.2:45
icmp 209.165.200.225:46192.168.1.20:46 192.31.7.2:46 192.31.7.2:46
icmp 209.165.200.225:47192.168.1.20:47 192.31.7.2:47 192.31.7.2:47
icmp 209.165.200.225:48192.168.1.20:48 192.31.7.2:48 192.31.7.2:48
--- 209.165.200.225 192.168.1.20 --- ---
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? 41



**Nota:** puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

- c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

```
Pro Inside global    Inside local    Outside local    Outside global
icmp 209.165.200.225:1  192.168.1.20:1  192.31.7.1:1    192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23   192.31.7.1:23
--- 209.165.200.225    192.168.1.20    ---             ---
```

```
Gateway#show ip nat translations
Pro Inside global    Inside local    Outside local    Outside
global
--- 209.165.200.225  192.168.1.20    ---             ---
tcp 209.165.200.225:1025 192.168.1.20:1025 192.31.7.2:80
192.31.7.2:80
```

**Nota:** es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

¿Qué protocolo se usó para esta traducción? Web

¿Cuáles son los números de puerto que se usaron?

Global/local interno: 1025

Global/local externo: 80

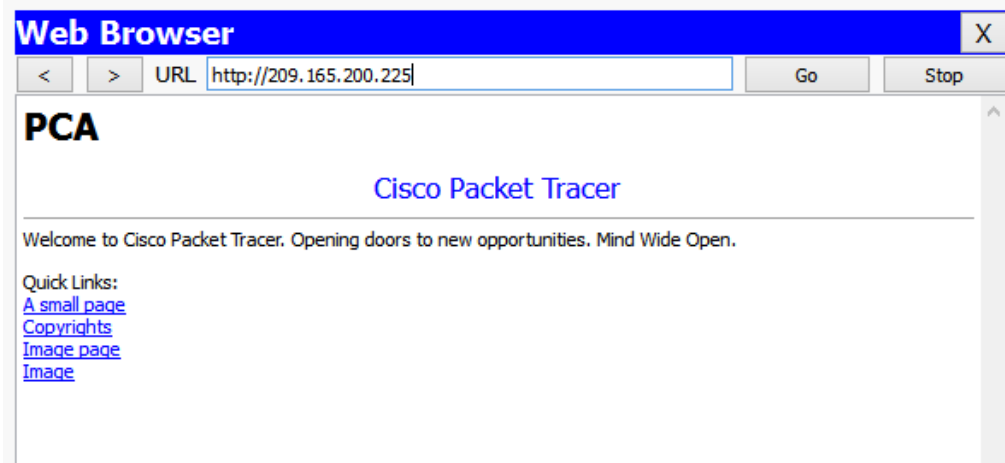
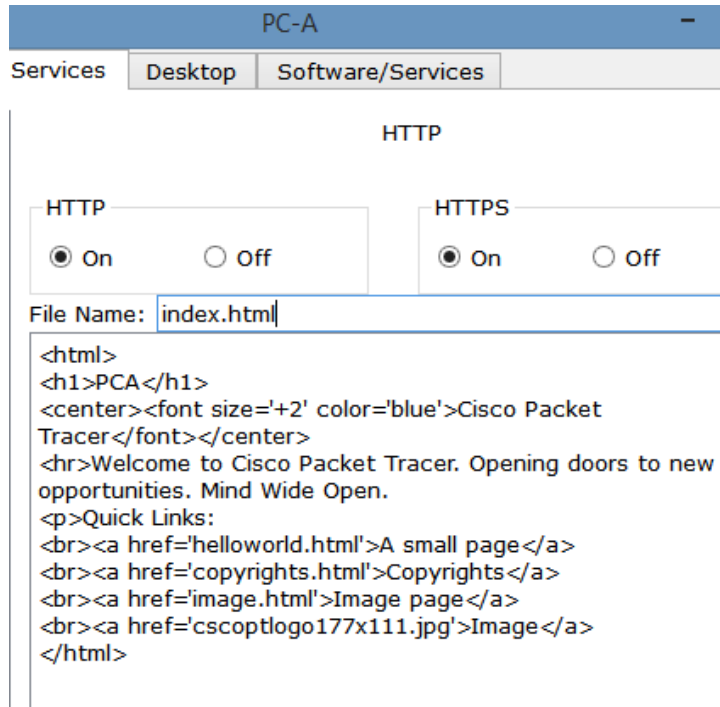
- d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.

```
Packet Tracer SERVER Command Line 1.0
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=3ms TTL=126
Reply from 209.165.200.225: bytes=32 time=16ms TTL=126
Reply from 209.165.200.225: bytes=32 time=13ms TTL=126
Reply from 209.165.200.225: bytes=32 time=12ms TTL=126

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 16ms, Average = 11ms
```



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

Gateway# **show ip nat translations**

Pro Inside global    Inside local    Outside local    Outside global

**icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12**

--- 209.165.200.225    192.168.1.20    ---    ---

Gateway#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.225:1025	192.168.1.20:1025	192.31.7.2:80	192.31.7.2:80
tcp	209.165.200.225:80	192.168.1.20:80	192.31.7.2:1025	192.31.7.2:1025
tcp	209.165.200.225:80	192.168.1.20:80	192.31.7.2:1026	192.31.7.2:1026

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

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

Gateway# **show ip nat statics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 00:02:12 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

```
Gateway#show ip nat statistics
Total translations: 4 (1 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 56 Misses: 51
Expired translations: 48
Dynamic mappings:
```

**Nota:** este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

## Parte 7. configurar y verificar la NAT dinámica

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

### Paso 1. borrar las NAT.

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

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

```
Gateway# clear ip nat statistics
```

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

### 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.

```
Gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial10/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 56 Misses: 51
Expired translations: 48
Dynamic mappings:
```

### Paso 4. definir el conjunto de direcciones IP públicas utilizables.

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

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

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

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

**Paso 6. probar la configuración.**

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

```
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=21ms TTL=254
Reply from 192.31.7.1: bytes=32 time=32ms TTL=254
Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=32ms TTL=254
Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 32ms, Average = 24ms
```

```
Gateway# show ip nat translations
```

```
Pro Inside global   Inside local   Outside local   Outside global
--- 209.165.200.225  192.168.1.20   ---            ---
icmp 209.165.200.242:1 192.168.1.21:1 192.31.7.1:1  192.31.7.1:1
--- 209.165.200.242  192.168.1.21   ---            ---
```

```
Gateway#show ip nat translations
Pro  Inside global   Inside local   Outside local   Outside global
icmp 209.165.200.242:33 192.168.1.21:33 192.31.7.1:33 192.31.7.1:33
icmp 209.165.200.242:34 192.168.1.21:34 192.31.7.1:34 192.31.7.1:34
icmp 209.165.200.242:35 192.168.1.21:35 192.31.7.1:35 192.31.7.1:35
icmp 209.165.200.242:36 192.168.1.21:36 192.31.7.1:36 192.31.7.1:36
--- 209.165.200.225   192.168.1.20   ---            ---
```

¿Cuál es la traducción de la dirección host local interna de la PC-B?

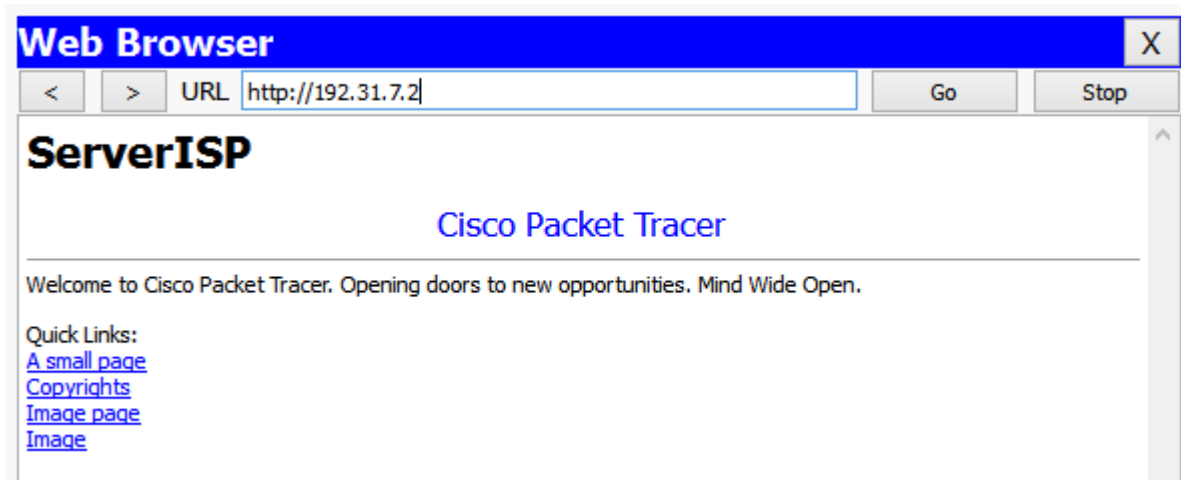
192.168.1.21 = 209.165.200.242

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

¿Qué número de puerto se usó en este intercambio ICMP? **33**

- 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**.

Para nuestro caso ingresamos por el 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 --- ---
```

```
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.242:1025 192.168.1.21:1025 192.31.7.2:80 192.31.7.2:80
```

¿Qué protocolo se usó en esta traducción? Http

¿Qué números de puerto se usaron?

Interno: 1025

Externo: 80

¿Qué número de puerto bien conocido y qué servicio se usaron? el http usó el 80

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

```
Gateway# show ip nat statistics
```

```
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
```

```
Peak translations: 17, occurred 00:06:40 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```

```
GigabitEthernet0/1
```

```
Hits: 345 Misses: 0
```

```
CEF Translated packets: 345, CEF Punted packets: 0
```

```
Expired translations: 20
```

```
Dynamic mappings:
```

-- Inside Source

```
[Id: 1] access-list 1 pool public_access refcount 2
```

```
pool public_access: netmask 255.255.255.224
```

```
start 209.165.200.242 end 209.165.200.254
```

```
type generic, total addresses 13, allocated 1 (7%), misses 0
```

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

```
Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 71 Misses: 84
Expired translations: 56
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13 , allocated 1 (7%), misses 0
```

**Nota:** este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

### 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.

- Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225
```

Static entry in use, do you want to delete child entries? [no]: **yes**

- Borre las NAT y las estadísticas.
- Haga ping al ISP (192.31.7.1) desde ambos hosts.



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 --- ---

```
Gateway#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 71 Misses: 84
Expired translations: 56
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 1 (7%), misses 0
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 209.165.200.242:1025192.168.1.21:1025 192.31.7.2:80      192.31.7.2:80
```

**Nota:** este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

## Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

Debido a que las ipv4 se estaban acabando se implementó utilizar para un grupo de red privadas el uso de una sola red pública, de esta manera se realiza un ahorro de Ip porque varias pc pueden ingresar a internet con la misma Ip pública (Aumenta la flexibilidad de las conexiones con la red pública). Adicional a esto aumenta el nivel de seguridad, un usuario no aparece en internet con su Ip privada, sino con la Ip pública asignada.

2. ¿Cuáles son las limitaciones de NAT?

Entre su desventajas esta que algunas aplicaciones que utilizan el direccionamiento IP dejan de funcionar, porque esconde las direcciones IP de extremo a extremo, no todas las aplicaciones y protocolos son compatibles con NAT; también aumenta el retardo y necesita mayor potencia de computación.

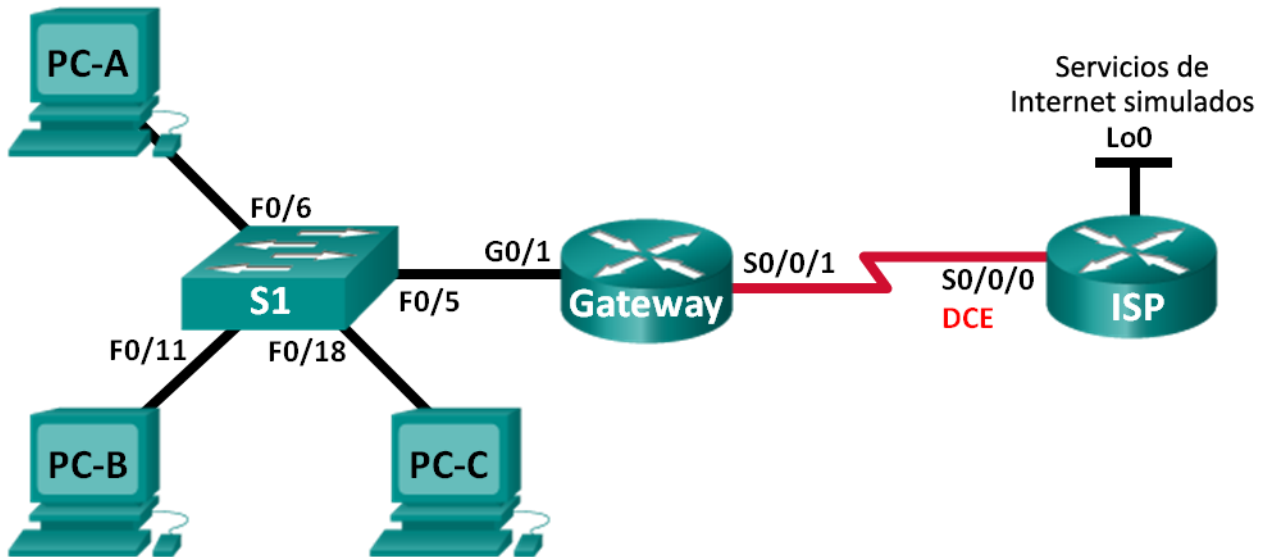
**Tabla de resumen de interfaces del router**

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

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

### 11.2.3.7 Lab – Configuring NAT Pool Overload and PAT

#### Topología



#### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

#### Objetivos

**Parte 1: armar la red y verificar la conectividad**

## Parte 2: configurar y verificar un conjunto de NAT con sobrecarga

## Parte 3: configurar y verificar PAT

### Recursos necesarios

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

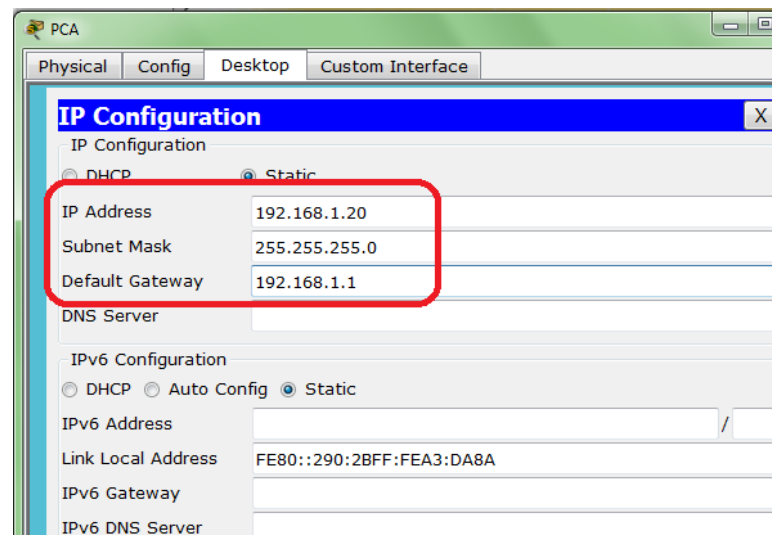
### Parte 1: armar la red y verificar la conectividad

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

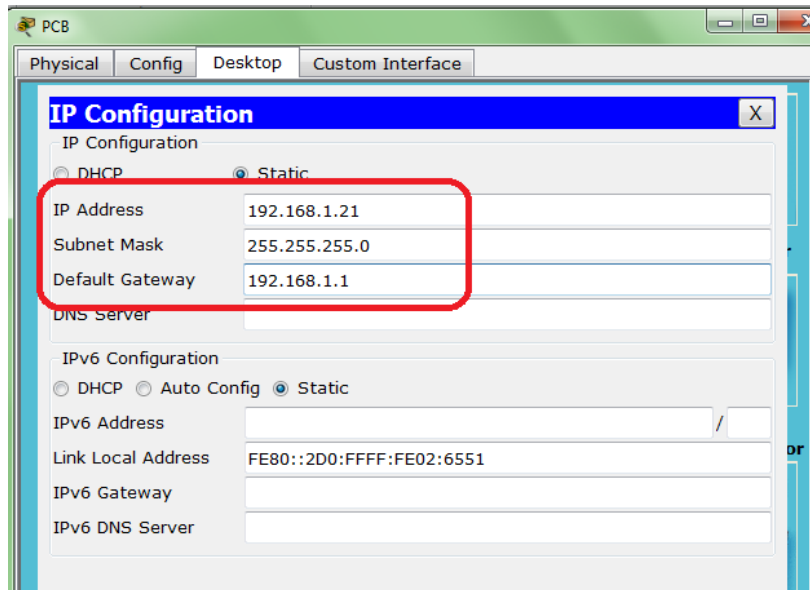
#### Paso 1: realizar el cableado de red tal como se muestra en la topología.

#### Paso 2: configurar los equipos host.

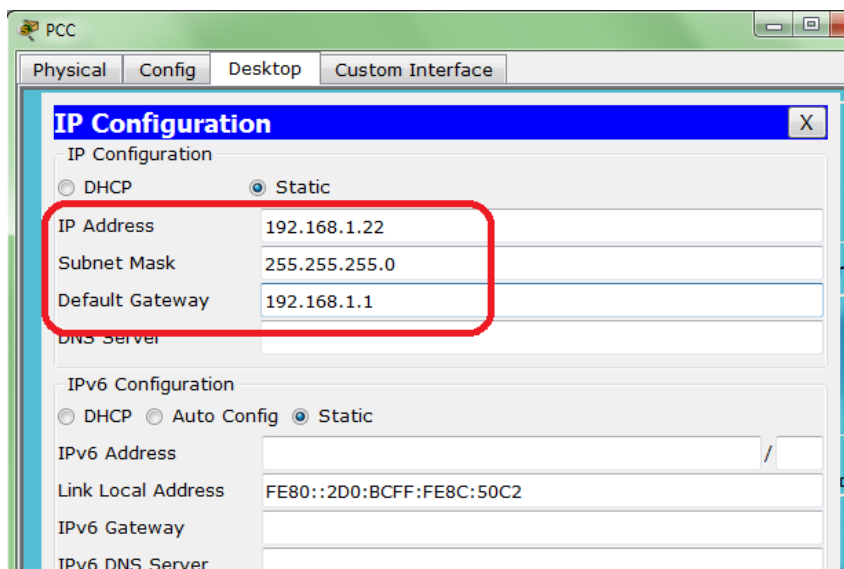
##### PCA



##### PCB



PCC



**Paso 3: inicializar y volver a cargar los routers y los switches.**

**Gateway**

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

**ISP**

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

S1

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

#### Paso 4: configurar los parámetros básicos para cada router.

- e. Desactive la búsqueda del DNS.

##### Gateway

```
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#
```

##### ISP

```
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#
```

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

##### Gateway

```
Gateway(config)#enable secret class
Gateway(config)#int g0/1
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config-if)#no shutdown

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

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

Gateway(config-if)#exit
Gateway(config)#int s 0/0/1
Gateway(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway(config-if)#no shutdown

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

##### ISP

```

ISP
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
ISP>enable
Password:
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int lo 0
ISP(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP(config-if)#ip address 192.31.7.1 255.255.255.255
ISP(config-if)#exit
ISP(config)#int s 0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
ISP(config-if)#

```

g. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

```

ISP
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
ISP>enable
Password:
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int lo 0
ISP(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP(config-if)#ip address 192.31.7.1 255.255.255.255
ISP(config-if)#exit
ISP(config)#int s 0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
ISP(config-if)#

```

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

### Gateway

```

Router(config)#no ip domain-lookup
Router(config)#hostname Gateway
Gateway(config)#

```

### ISP

```

Gateway(config)#hostname ISP
ISP(config)#

```

### S1

```

Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#

```

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

Gateway contraseña consola



```
Gateway(config)#line con 0
Gateway(config-line)#password cisco
```

### Gateway contraseña vty

```
Gateway(config)#line vty 0 4
Gateway(config-line)#password cisco
```

### ISP contraseña consola

```
ISP(config)#line con 0
ISP(config-line)#password cisco
```

### ISP contraseña vty

```
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
```

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

### Gateway

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

### ISP

```
-----
ISP(config)#enable secret class
ISP(config)#
```

- k. Configure **logging synchronous** para evitar que los mensajes de consola interrumpen la entrada del comando.

### Gateway

```
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#loggin synchronous
Gateway(config-line)#exit
```

### ISP

```
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#loggin synchronous
```

## Paso 5: configurar el routing estático.

1. Cree una ruta estática desde el router ISP hasta el router Gateway.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

```
ISP
Physical Config CLI
IOS Command Line Interface
Password:
ISP>enable
Password:
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int lo 0

ISP(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
ISP(config-if)#ip address 192.31.7.1 255.255.255.255
ISP(config-if)#exit
ISP(config)#int s 0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

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

ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
ISP(config-if)#exit
ISP(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
ISP(config)#
```

m. Cree una ruta predeterminada del router Gateway al router ISP.

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

```
| Gateway(config)#ip route 0.0.0.0.0.0.0.0 209.165.201.17
| ^
```

### Paso 6: Verificar la conectividad de la red

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

PCA

```
PCA
Physical Config Desktop Custom Interface
Command Prompt
C:\>ping 192.168.1.1
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

PCB

```
PCB
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PCC

```
PCC
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>
```

- o. Verifique que las rutas estáticas estén bien configuradas en ambos routers.

```

PCA
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

**RTA:** Al hacer ping desde PCA a la ruta 192.31.7.1 del ISP, se va a mostrar fallida ya que la ruta estática que tiene el ISP no tiene como destino 192.168.1.0 sino la red publica 209.165.200.224.

## Parte 2: configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

### Paso 1: definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

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

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

```

Enter configuration commands, one per line. End with END.
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#

```

### Paso 3: definir el conjunto de direcciones IP públicas utilizables.

Gateway(config)# **ip nat pool public\_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

```

Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#ip nat pool public_access 209.165.200.225 209.165.200.230 netmask
255.255.255.248
Gateway(config)#

```

### Paso 4: definir la NAT desde la lista de origen interna hasta el conjunto externo.

Gateway(config)# **ip nat inside source list 1 pool public\_access overload**

```

255.255.255.248
Gateway(config)#ip nat inside source list 1 pool public_access overload
Gateway(config)#

```

## Paso 5: Especifique las interfaces.

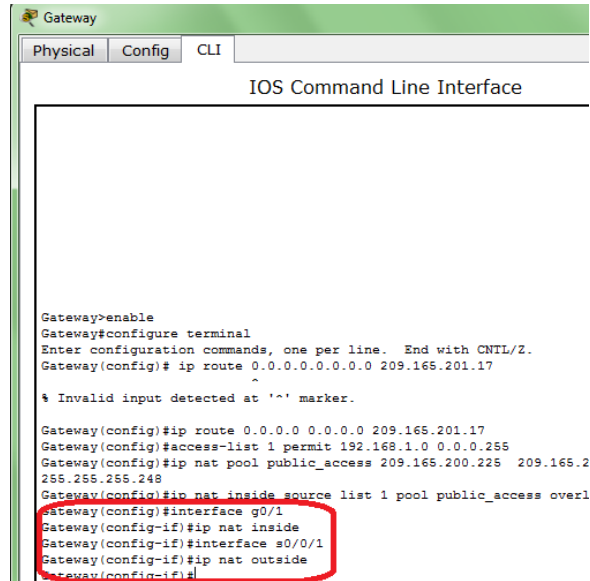
Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
```

```
Gateway(config-if)# ip nat inside
```

```
Gateway(config-if)# interface s0/0/1
```

```
Gateway(config-if)# ip nat outside
```



```
Gateway
Physical Config CLI
IOS Command Line Interface

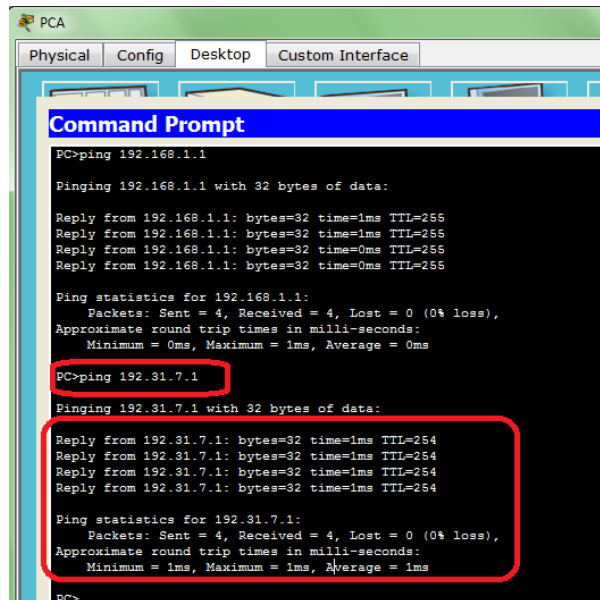
Gateway>enable
Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
^
% Invalid input detected at '^' marker.

Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#ip nat pool public_access 209.165.200.225 209.165.2
255.255.255.248
Gateway(config)#ip nat inside source list 1 pool public_access overloa
Gateway(config)#interface g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface s0/0/1
Gateway(config-if)#ip nat outside
Gateway(config-if)#
```

## Paso 6: verificar la configuración del conjunto de NAT con sobrecarga.

p. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.

PCA



```
PCA
Physical Config Desktop Custom Interface
Command Prompt

PCA>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PCA>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

PCA>
```

PCB

```
PCB
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

PCC

```
PCC
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
PC>
```

q. Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:25 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public\_access refcount 3

pool public\_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

```
Gateway>enable
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12 Misses: 12
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 24 Misses: 24
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 12
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6 , allocated 1 (16%), misses 0
```

r. Muestre las NAT en el router Gateway.

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:0	192.168.1.20:1	192.31.7.1:1	192.31.7.1:0
icmp	209.165.200.225:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.200.225:2	192.168.1.22:1	192.31.7.1:1	192.31.7.1:2

**Nota:** es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior?

RTA: 3

```

-----
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:1024 192.168.1.21:13  192.31.7.1:13     192.31.7.1:1024
icmp 209.165.200.225:1025 192.168.1.21:14  192.31.7.1:14     192.31.7.1:1025
icmp 209.165.200.225:1026 192.168.1.21:15  192.31.7.1:15     192.31.7.1:1026
icmp 209.165.200.225:1027 192.168.1.21:16  192.31.7.1:16     192.31.7.1:1027
icmp 209.165.200.225:1028 192.168.1.22:13  192.31.7.1:13     192.31.7.1:1028
icmp 209.165.200.225:1029 192.168.1.22:14  192.31.7.1:14     192.31.7.1:1029
icmp 209.165.200.225:1030 192.168.1.22:15  192.31.7.1:15     192.31.7.1:1030
icmp 209.165.200.225:1031 192.168.1.22:16  192.31.7.1:16     192.31.7.1:1031
icmp 209.165.200.225:13  192.168.1.20:13  192.31.7.1:13     192.31.7.1:13
icmp 209.165.200.225:14  192.168.1.20:14  192.31.7.1:14     192.31.7.1:14
icmp 209.165.200.225:15  192.168.1.20:15  192.31.7.1:15     192.31.7.1:15
icmp 209.165.200.225:16  192.168.1.20:16  192.31.7.1:16     192.31.7.1:16

```

¿Cuántas direcciones IP globales internas se indican?

RTA: 1 dirección del pool de direcciones

```

-----
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:1024 192.168.1.21:13  192.31.7.1:13     192.31.7.1:1024
icmp 209.165.200.225:1025 192.168.1.21:14  192.31.7.1:14     192.31.7.1:1025
icmp 209.165.200.225:1026 192.168.1.21:15  192.31.7.1:15     192.31.7.1:1026
icmp 209.165.200.225:1027 192.168.1.21:16  192.31.7.1:16     192.31.7.1:1027
icmp 209.165.200.225:1028 192.168.1.22:13  192.31.7.1:13     192.31.7.1:1028
icmp 209.165.200.225:1029 192.168.1.22:14  192.31.7.1:14     192.31.7.1:1029
icmp 209.165.200.225:1030 192.168.1.22:15  192.31.7.1:15     192.31.7.1:1030
icmp 209.165.200.225:1031 192.168.1.22:16  192.31.7.1:16     192.31.7.1:1031
icmp 209.165.200.225:13  192.168.1.20:13  192.31.7.1:13     192.31.7.1:13
icmp 209.165.200.225:14  192.168.1.20:14  192.31.7.1:14     192.31.7.1:14
icmp 209.165.200.225:15  192.168.1.20:15  192.31.7.1:15     192.31.7.1:15
icmp 209.165.200.225:16  192.168.1.20:16  192.31.7.1:16     192.31.7.1:16
Gateway#

```

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas?

RTA: 12 puertos diferentes para 12 paquetes diferentes

```

-----
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:1024 192.168.1.21:13  192.31.7.1:13     192.31.7.1:1024
icmp 209.165.200.225:1025 192.168.1.21:14  192.31.7.1:14     192.31.7.1:1025
icmp 209.165.200.225:1026 192.168.1.21:15  192.31.7.1:15     192.31.7.1:1026
icmp 209.165.200.225:1027 192.168.1.21:16  192.31.7.1:16     192.31.7.1:1027
icmp 209.165.200.225:1028 192.168.1.22:13  192.31.7.1:13     192.31.7.1:1028
icmp 209.165.200.225:1029 192.168.1.22:14  192.31.7.1:14     192.31.7.1:1029
icmp 209.165.200.225:1030 192.168.1.22:15  192.31.7.1:15     192.31.7.1:1030
icmp 209.165.200.225:1031 192.168.1.22:16  192.31.7.1:16     192.31.7.1:1031
icmp 209.165.200.225:13  192.168.1.20:13  192.31.7.1:13     192.31.7.1:13
icmp 209.165.200.225:14  192.168.1.20:14  192.31.7.1:14     192.31.7.1:14
icmp 209.165.200.225:15  192.168.1.20:15  192.31.7.1:15     192.31.7.1:15
icmp 209.165.200.225:16  192.168.1.20:16  192.31.7.1:16     192.31.7.1:16

```

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

RTA: sería fallido, ya que al hacer nat solo está tomando la ip del Gateway y los host no están mostrando sus ip.



```
ISP
Physical Config CLI
IOS Command Line Interface
ISP con0 is now available
Press RETURN to get started.
ISP>ping 192.168.1.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ISP>
```

### Parte 3: configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

#### Paso 1: borrar las NAT y las estadísticas en el router Gateway.

```
Gateway
Physical Config CLI
IOS Command Line Interface
% Invalid input detected at '^' marker.
Gateway>enable
Gateway#clear ip nat translation *
% Invalid input detected at '^' marker.
Gateway#clear ip nat translation *
% Invalid input detected at '^' marker.
Gateway#show ip translation
% Invalid input detected at '^' marker.
Gateway#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1025192.168.1.21:22 192.31.7.1:22 192.31.7.1:1025
icmp 209.165.200.225:1026192.168.1.21:23 192.31.7.1:23 192.31.7.1:1026
icmp 209.165.200.225:1027192.168.1.21:24 192.31.7.1:24 192.31.7.1:1027
icmp 209.165.200.225:1028192.168.1.22:21 192.31.7.1:21 192.31.7.1:1028
icmp 209.165.200.225:1029192.168.1.22:22 192.31.7.1:22 192.31.7.1:1029
icmp 209.165.200.225:1030192.168.1.22:23 192.31.7.1:23 192.31.7.1:1030
icmp 209.165.200.225:1031192.168.1.22:24 192.31.7.1:24 192.31.7.1:1031
Gateway#clear ip nat translation *
Gateway#show ip nat translation
```

#### Paso 2: verificar la configuración para NAT.

- s. Verifique que se hayan borrado las estadísticas.

```

Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 60 Misses: 60
Expired translations: 60
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
   start 209.165.200.225 end 209.165.200.230
   type generic, total addresses 6 , allocated 0 (0%), misses 0

```

- t. Verifique que las interfaces externa e interna estén configuradas para NAT.
- u. Verifique que la ACL aún esté configurada para NAT.

```

Gateway#clear ip nat translation *
Gateway#show ip translation
^
% Invalid input detected at '^' marker.

Gateway#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:1025192.168.1.21:22  192.31.7.1:22     192.31.7.1:22     192.31.7.1:22
icmp 209.165.200.225:1026192.168.1.21:23  192.31.7.1:23     192.31.7.1:23     192.31.7.1:23
icmp 209.165.200.225:1027192.168.1.21:24  192.31.7.1:24     192.31.7.1:24     192.31.7.1:24
icmp 209.165.200.225:1028192.168.1.22:21  192.31.7.1:21     192.31.7.1:21     192.31.7.1:21
icmp 209.165.200.225:1029192.168.1.22:22  192.31.7.1:22     192.31.7.1:22     192.31.7.1:22
icmp 209.165.200.225:1030192.168.1.22:23  192.31.7.1:23     192.31.7.1:23     192.31.7.1:23
icmp 209.165.200.225:1031192.168.1.22:24  192.31.7.1:24     192.31.7.1:24     192.31.7.1:24

Gateway#clear ip nat translation *
Gateway#show ip nat translation
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 60 Misses: 60
Expired translations: 60
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
   start 209.165.200.225 end 209.165.200.230
   type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#

```

¿Qué comando usó para confirmar los resultados de los pasos a al c)?

```
| Gateway#show ip nat statistics
```

### Paso 3: eliminar el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
```

```

Gateway
Physical Config CLI
IOS Command Line Interface
icmp 209.165.200.225:1029192.168.1.22:21 192.31.7.1:22 192.31.7.1:1029
icmp 209.165.200.225:1029192.168.1.22:22 192.31.7.1:22 192.31.7.1:1029
icmp 209.165.200.225:1030192.168.1.22:23 192.31.7.1:23 192.31.7.1:1030
icmp 209.165.200.225:1031192.168.1.22:24 192.31.7.1:24 192.31.7.1:1031

Gateway#clear ip nat translation *
Gateway#show ip nat translation
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 60 Misses: 60
Expired translations: 60
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask
255.255.255.248
^
% Invalid input detected at '^' marker.

Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
^
%Pool public_access in use, cannot destroy
Gateway(config)#

```

**Paso 4: eliminar la traducción NAT de la lista de origen interna al conjunto externo.**

Gateway(config)# no ip nat inside source list 1 pool public\_access overload

```

Gateway
Physical Config CLI
IOS Command Line Interface
icmp 209.165.200.225:1029192.168.1.22:22 192.31.7.1:22 192.31.7.1:1029
icmp 209.165.200.225:1030192.168.1.22:23 192.31.7.1:23 192.31.7.1:1030
icmp 209.165.200.225:1031192.168.1.22:24 192.31.7.1:24 192.31.7.1:1031

Gateway#clear ip nat translation *
Gateway#show ip nat translation
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 60 Misses: 60
Expired translations: 60
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask
255.255.255.248
^
% Invalid input detected at '^' marker.

Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
^
% Invalid input detected at '^' marker.
Gateway(config)#no ip nat inside source list 1 pool public_access overload
Gateway(config)#

```

**Paso 5: asociar la lista de origen a la interfaz externa.**

Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload

```
Gateway
Physical Config CLI
IOS Command Line Interface
Expired translations: 60
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6, allocated 0 (0%), misses 0
Gateway#no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask
255.255.255.248
^
% Invalid input detected at '^' marker.

Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
%Pool public_access in use, cannot destroy
Gateway(config)#no ip nat inside source list 1 pool public_access overload
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 overload
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

### Paso 6: probar la configuración PAT.

- v. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.

PCA

```
PCA
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.31.7.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.31.7.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>
```

PCB

```
PCB
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=12ms TTL=254
Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 6ms
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=16ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 4ms
PC>
```

PCC

```
PCC
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=3ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
PC>
```

w. Muestre las estadísticas de NAT en el router Gateway.

Gateway# show ip nat statistics

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:19 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

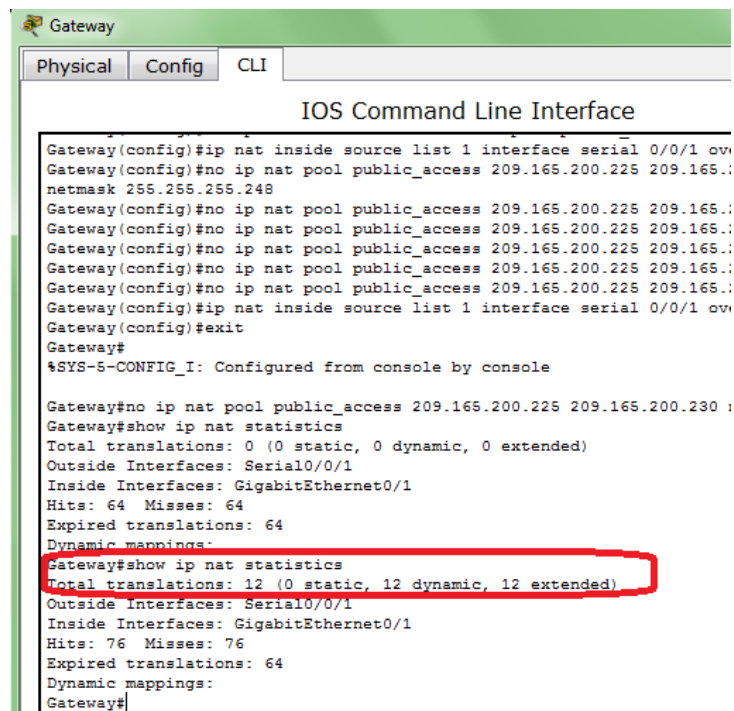
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0



```
Gateway
Physical Config CLI
IOS Command Line Interface
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 ov
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.
netmask 255.255.255.248
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 ov
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console

Gateway#no ip nat pool public_access 209.165.200.225 209.165.200.230 :
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 64 Misses: 64
Expired translations: 64
Dynamic mappings:
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 76 Misses: 76
Expired translations: 64
Dynamic mappings:
Gateway#
```

x. Muestre las traducciones NAT en el Gateway.

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.18:3	192.168.1.20:1	192.31.7.1:1	192.31.7.1:3
icmp	209.165.201.18:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.201.18:4	192.168.1.22:1	192.31.7.1:1	192.31.7.1:4

```
Gateway
Physical Config CLI
IOS Command Line Interface
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 76 Misses: 76
Expired translations: 64
Dynamic mappings:
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 76 Misses: 76
Expired translations: 76
Dynamic mappings:
Gateway#show ip nat translations
Pro inside global      inside local      Outside local      Outside global
icmp 209.165.201.18:1024192.168.1.22:29 192.31.7.1:29 192.31.7.1:1024
icmp 209.165.201.18:1025192.168.1.22:30 192.31.7.1:30 192.31.7.1:1025
icmp 209.165.201.18:1026192.168.1.22:31 192.31.7.1:31 192.31.7.1:1026
icmp 209.165.201.18:1027192.168.1.22:32 192.31.7.1:32 192.31.7.1:1027
icmp 209.165.201.18:29 192.168.1.21:29 192.31.7.1:29 192.31.7.1:29
icmp 209.165.201.18:30 192.168.1.21:30 192.31.7.1:30 192.31.7.1:30
icmp 209.165.201.18:31 192.168.1.21:31 192.31.7.1:31 192.31.7.1:31
icmp 209.165.201.18:32 192.168.1.21:32 192.31.7.1:32 192.31.7.1:32
icmp 209.165.201.18:33 192.168.1.20:33 192.31.7.1:33 192.31.7.1:33
icmp 209.165.201.18:34 192.168.1.20:34 192.31.7.1:34 192.31.7.1:34
icmp 209.165.201.18:35 192.168.1.20:35 192.31.7.1:35 192.31.7.1:35
icmp 209.165.201.18:36 192.168.1.20:36 192.31.7.1:36 192.31.7.1:36
Gateway#
```

## Reflexión

¿Qué ventajas tiene la PAT?

**RTA:** Que utiliza solo la interfaz de salida en este caso la ip 209.165.201.18 pero por diferentes puertos.

## Tabla de resumen de interfaces del router

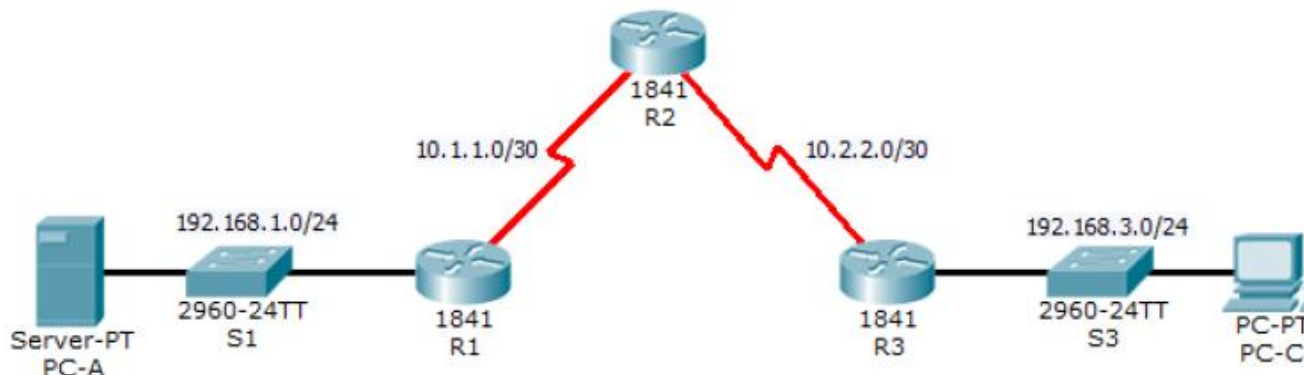
Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial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



### 4.4.1.2 Configure IP ACLs to Mitigate Attacks

## Configure IP ACLs to Mitigate Attacks



### 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

### Objectives

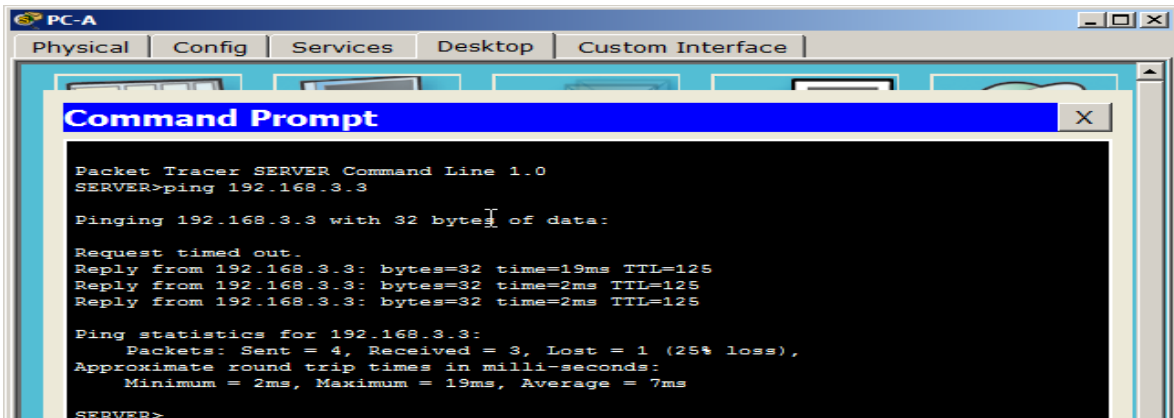
- Verify connectivity among devices before firewall configuration.
- Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- Configure ACLs on R1 and R3 to mitigate attacks.
- Verify ACL functionality.

## Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

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

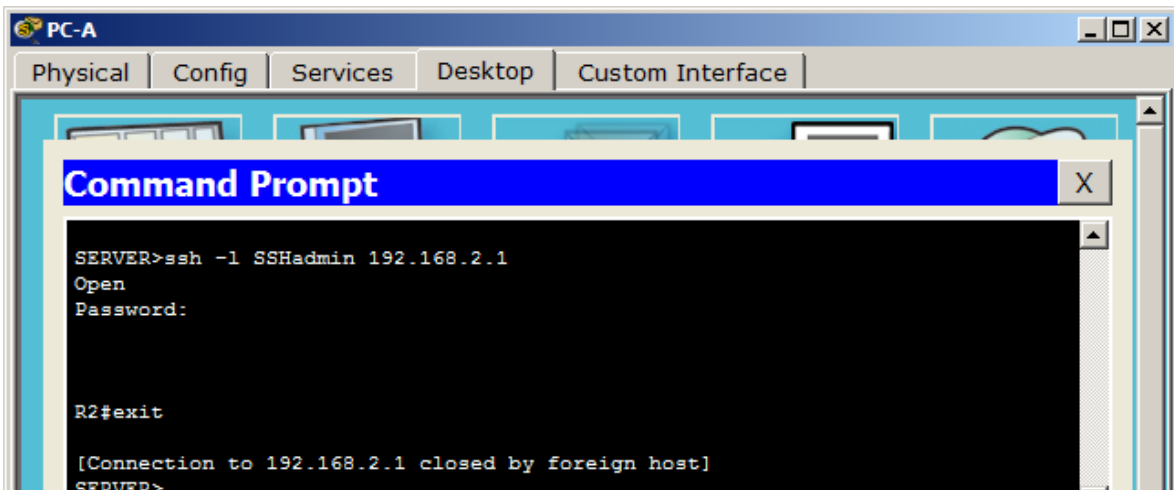
- a. From the command prompt, ping PC-C (192.168.3.3).



```
PC-A
Physical | Config | Services | Desktop | Custom Interface |
Command Prompt
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.3: bytes=32 time=19ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 19ms, Average = 7ms
SERVER>
```

- 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.

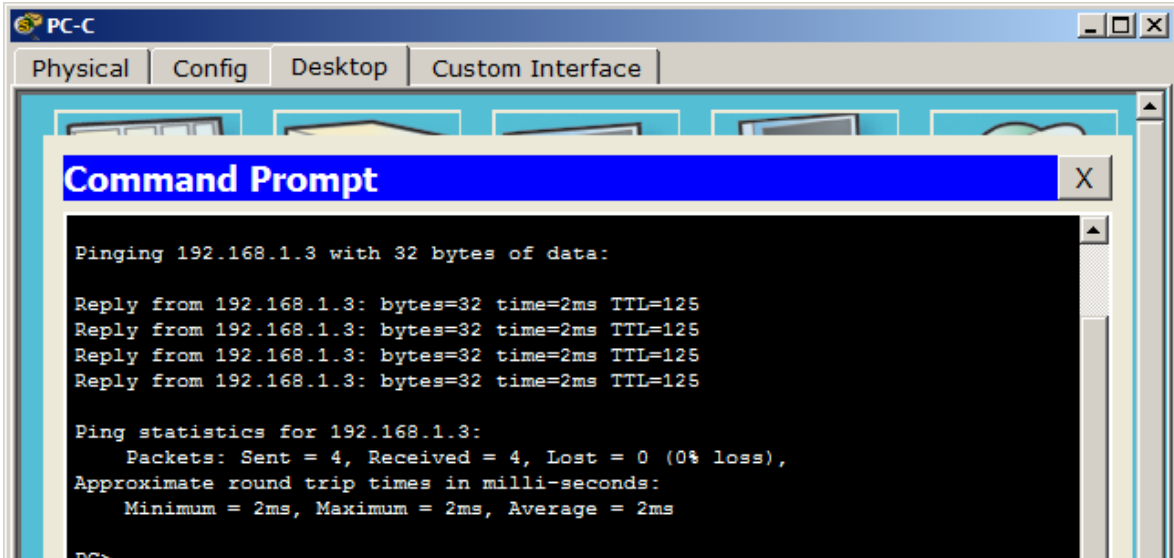
PC> ssh -l SSHadmin 192.168.2.1



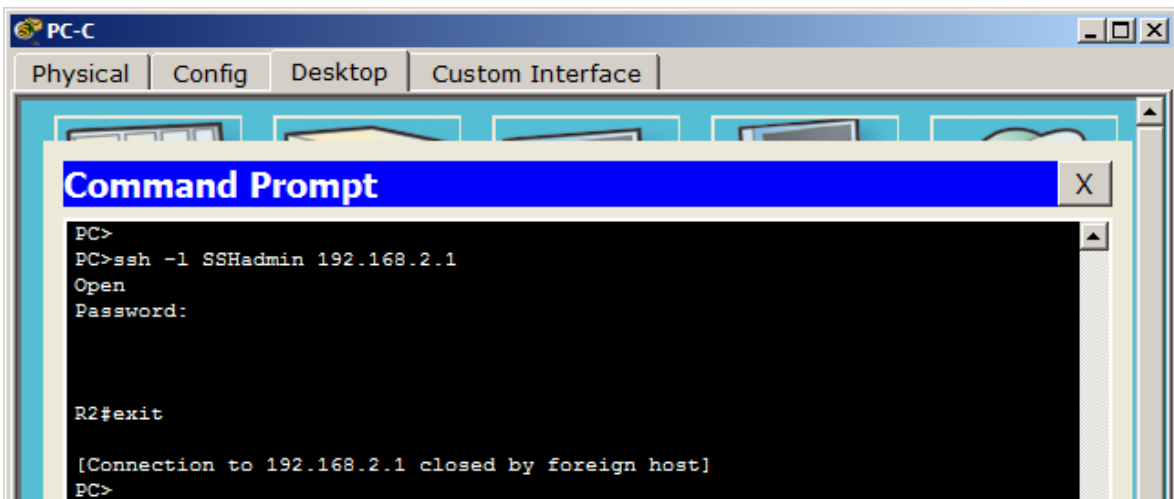
```
PC-A
Physical | Config | Services | Desktop | Custom Interface |
Command Prompt
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:
R2#exit
[Connection to 192.168.2.1 closed by foreign host]
SERVER>
```

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

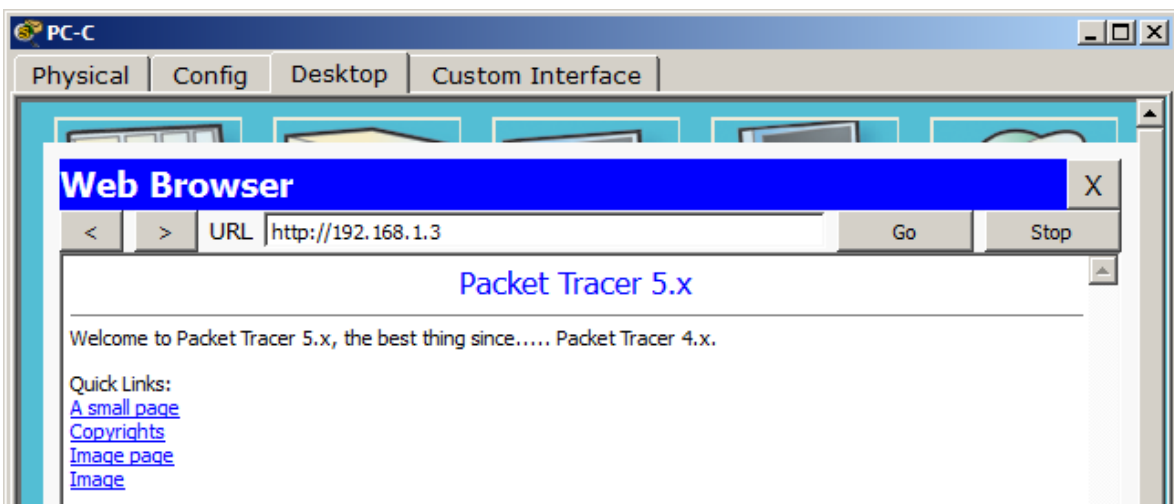
- a. From the command prompt, ping PC-A (192.168.1.3).



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



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



## Part 2: Secure Access to Routers

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

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

The image displays three screenshots of the Cisco IOS Command Line Interface (CLI) for routers R1, R2, and R3. Each screenshot shows the process of entering configuration mode and creating a numbered IP ACL (ACL 10) that permits traffic from the IP address 192.168.3.3. The CLI windows are titled 'R1', 'R2', and 'R3' respectively, and each has tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is selected in all three. The text in each window is as follows:

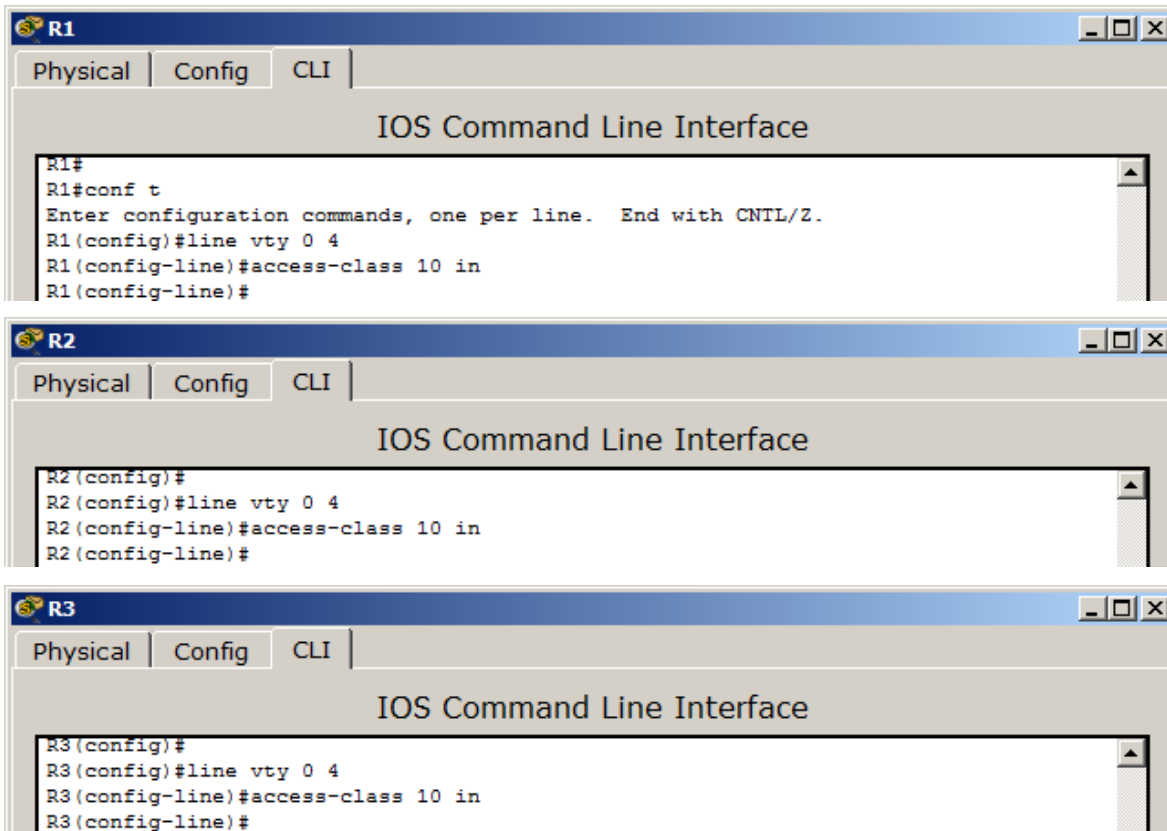
```
R1
Physical | Config | CLI
IOS Command Line Interface
User Access Verification
Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3
R1(config)#

R2
Physical | Config | CLI
IOS Command Line Interface
User Access Verification
Password:
Password:
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3
R2(config)#

R3
Physical | Config | CLI
IOS Command Line Interface
User Access Verification
Password:
R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#
```

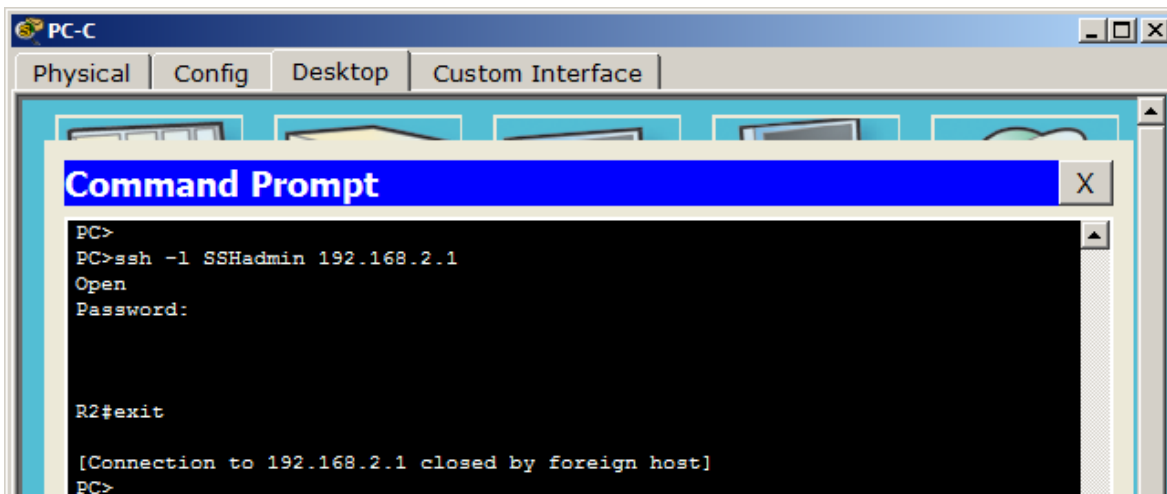
### Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

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

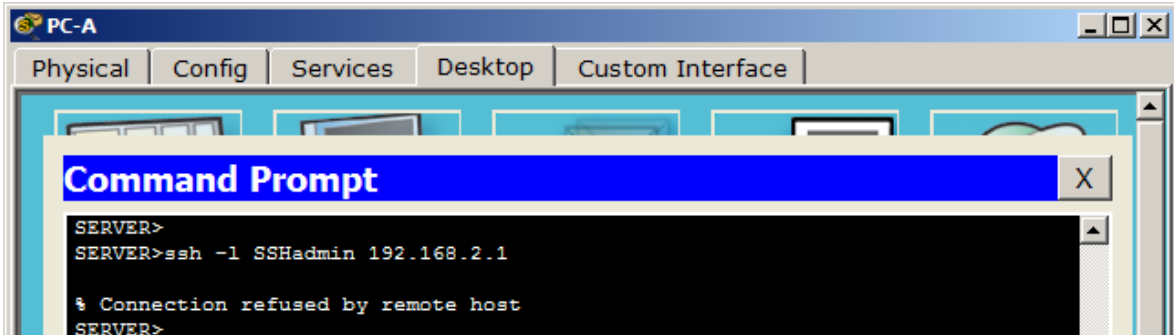


**Step 3: Verify exclusive access from management station PC-C.**

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



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

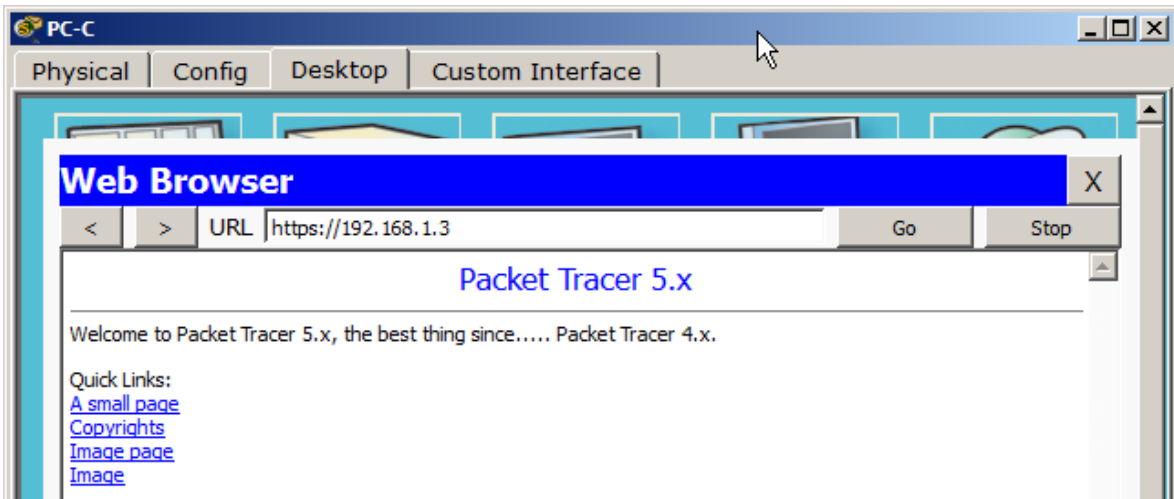


### Part 3: Create a Numbered IP ACL 120 on R1

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

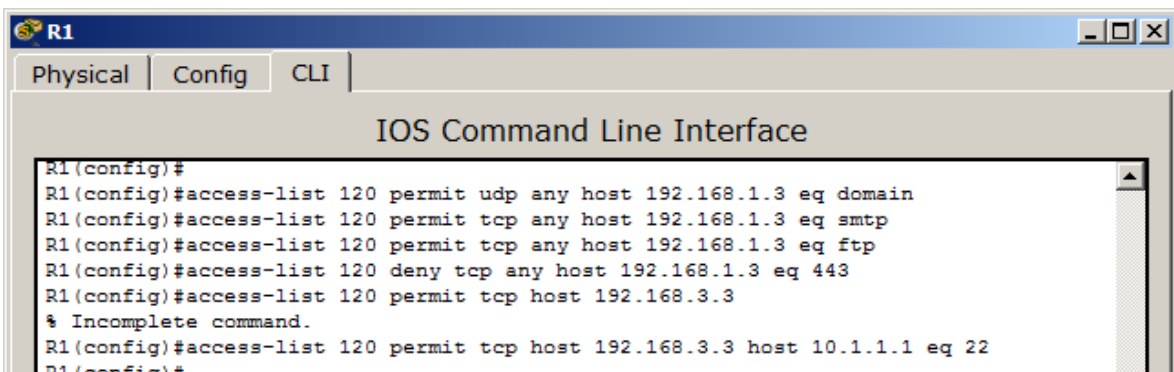
#### Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

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



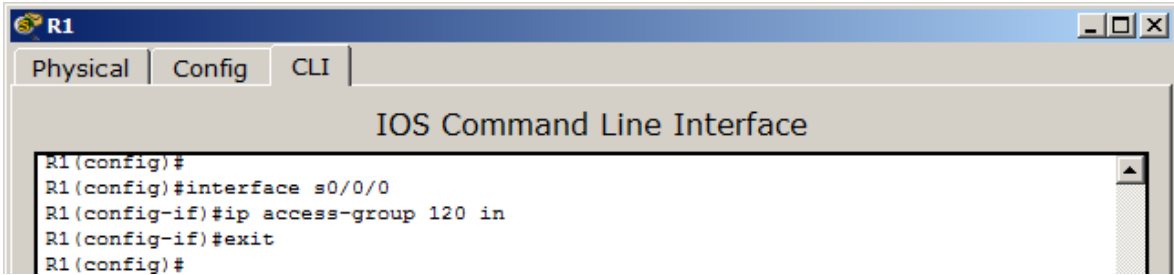
#### Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

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

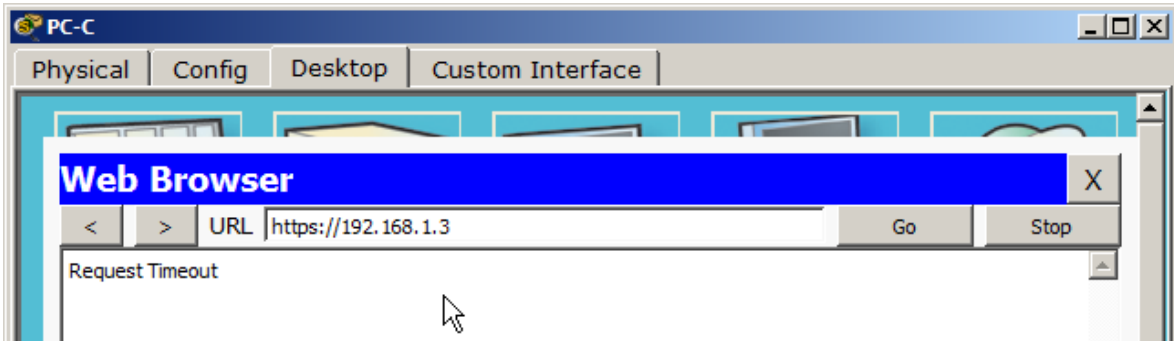


#### Step 3: Apply the ACL to interface S0/0/0.

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



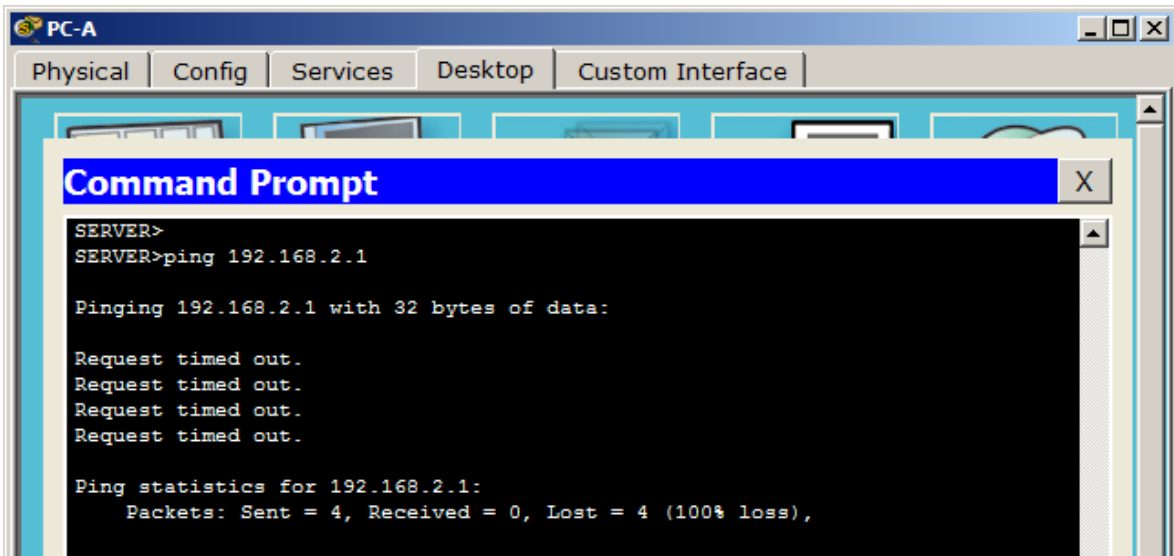
**Step 4:** Verify that PC-C cannot access PC-A via HTTPS using the web browser.



#### Part 4: Modify An Existing ACL on R1

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

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



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

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

```
R1
Physical Config CLI
IOS Command Line Interface
R1(config)#
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 permit deny icmp any any
^
% Invalid input detected at '^' marker.
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#
```

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

```
PC-A
Physical Config Services Desktop Custom Interface
Command Prompt
SERVER>
SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

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

SERVER>
```

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

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

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

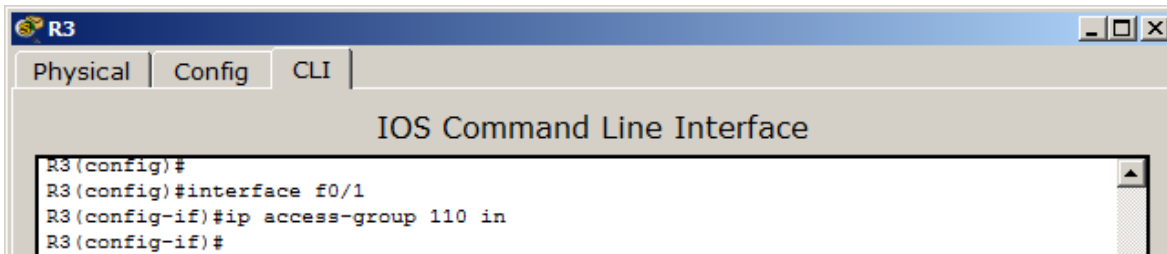
Use the **access-list** command to create a numbered IP ACL.

```
R3
Physical Config CLI
IOS Command Line Interface
R3(config)#
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#
```

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

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





```
R3
Physical Config CLI
IOS Command Line Interface
R3(config)#
R3(config)#interface f0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#
```

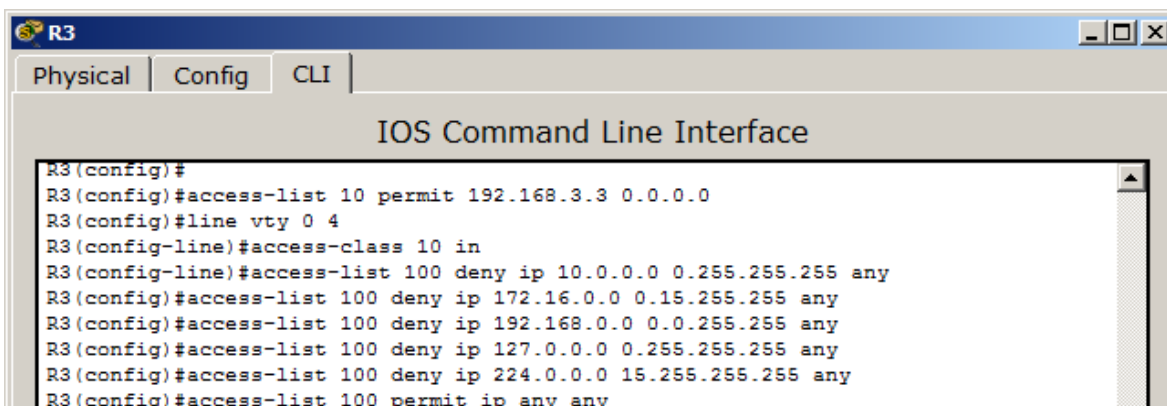
### Part 6: Create a Numbered IP ACL 100 on R3

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

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

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

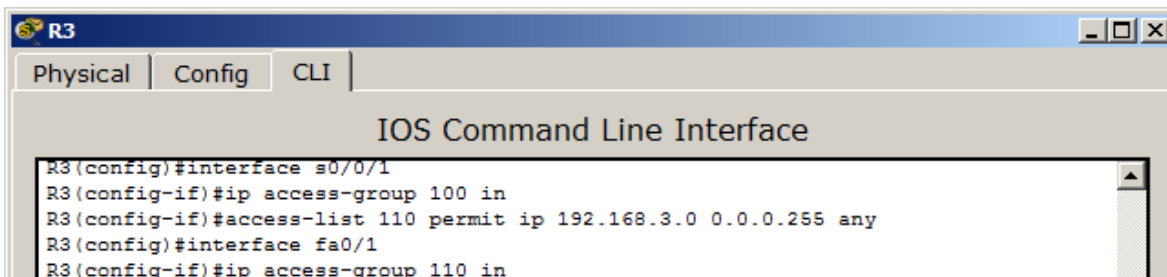
Use the **access-list** command to create a numbered IP ACL.



```
R3
Physical Config CLI
IOS Command Line Interface
R3(config)#
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
```

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

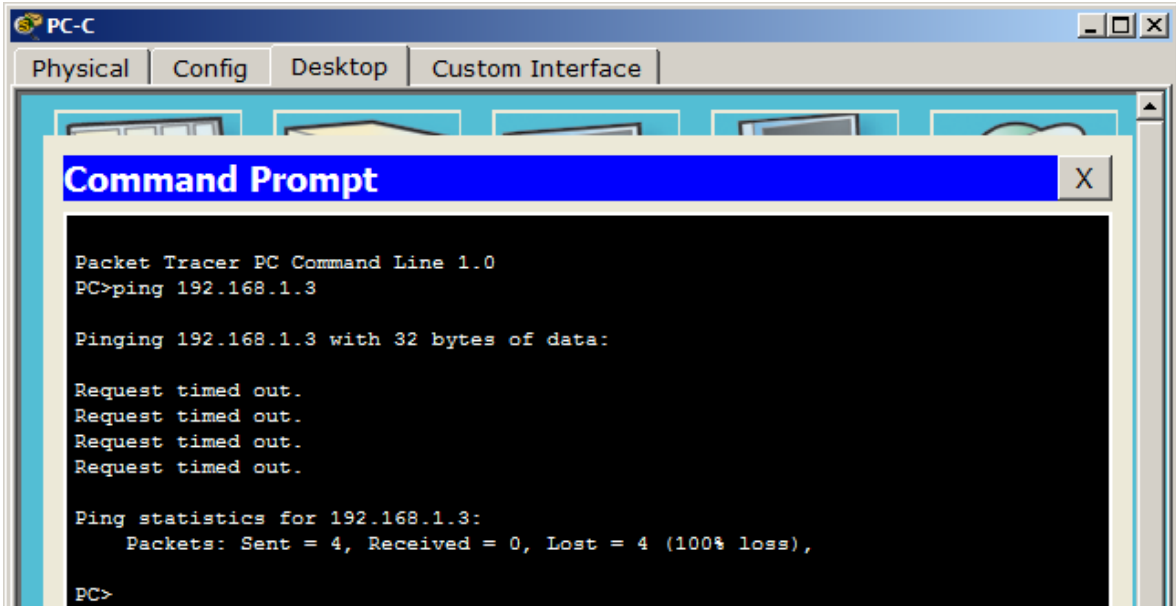
Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.



```
R3
Physical Config CLI
IOS Command Line Interface
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
```

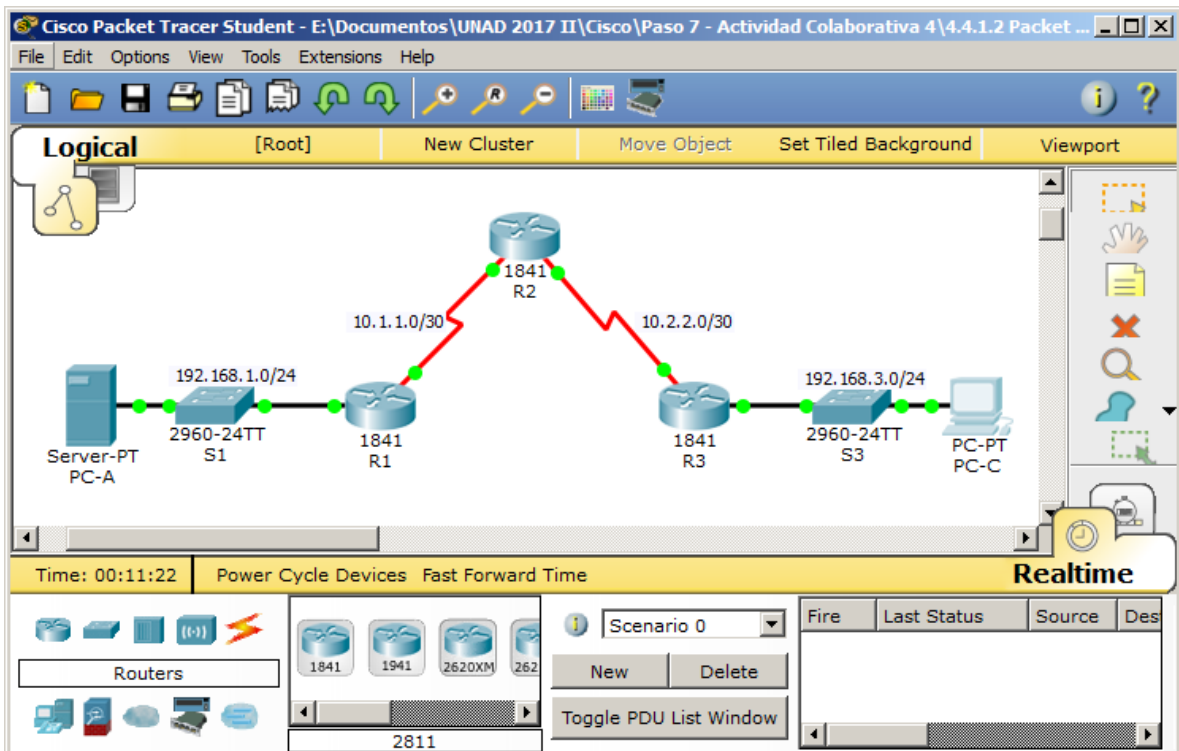
#### Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

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



**Step 4: Check results.**

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



Cisco Packet Tracer Student - E:\Documentos\UNAD 2017 II\Cisco\Paso 7 - Actividad Colaborativa 4\4.4.1.2 Packet Tracer - Confi... | File Edit Options View Tools Extensions Help

## Activity Results

Time Elapsed: 00:58:36

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

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

Score : 23/23

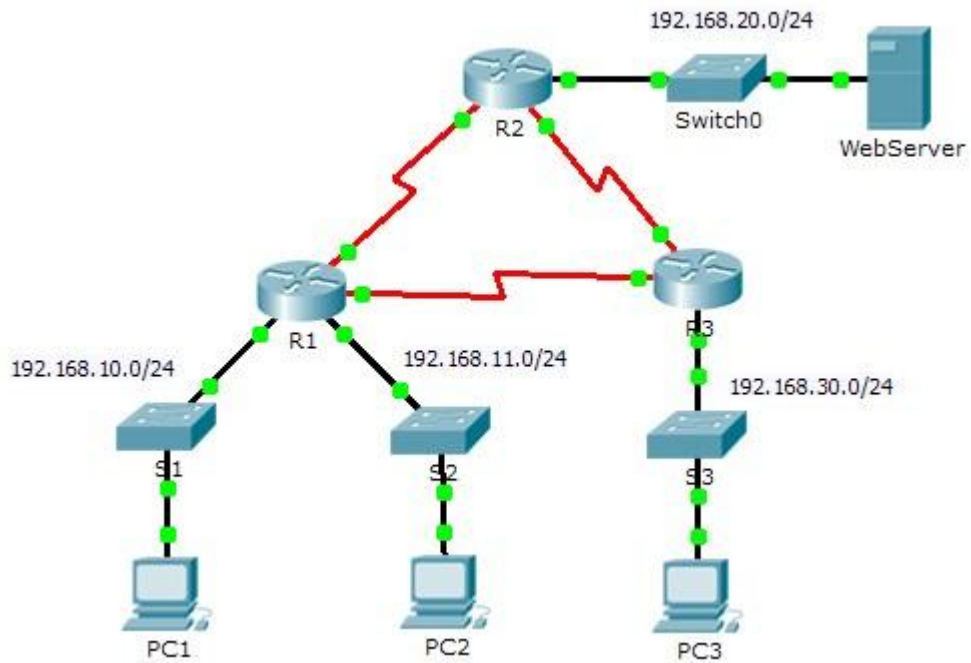
Item Count : 23/23

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

Close

### 9.2.1.10 Configuring Standard ACLs

#### Topology



## 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

## Objectives

### Part 1: Plan an ACL Implementation

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

#### Part 1: Plan an ACL Implementation

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

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

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

- a. The following network policies are implemented on **R2**:
  - The 192.168.11.0/24 network is not allowed access to the **WebServer** on the 192.168.20.0/24 network.
  - All other access is permitted.

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

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

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

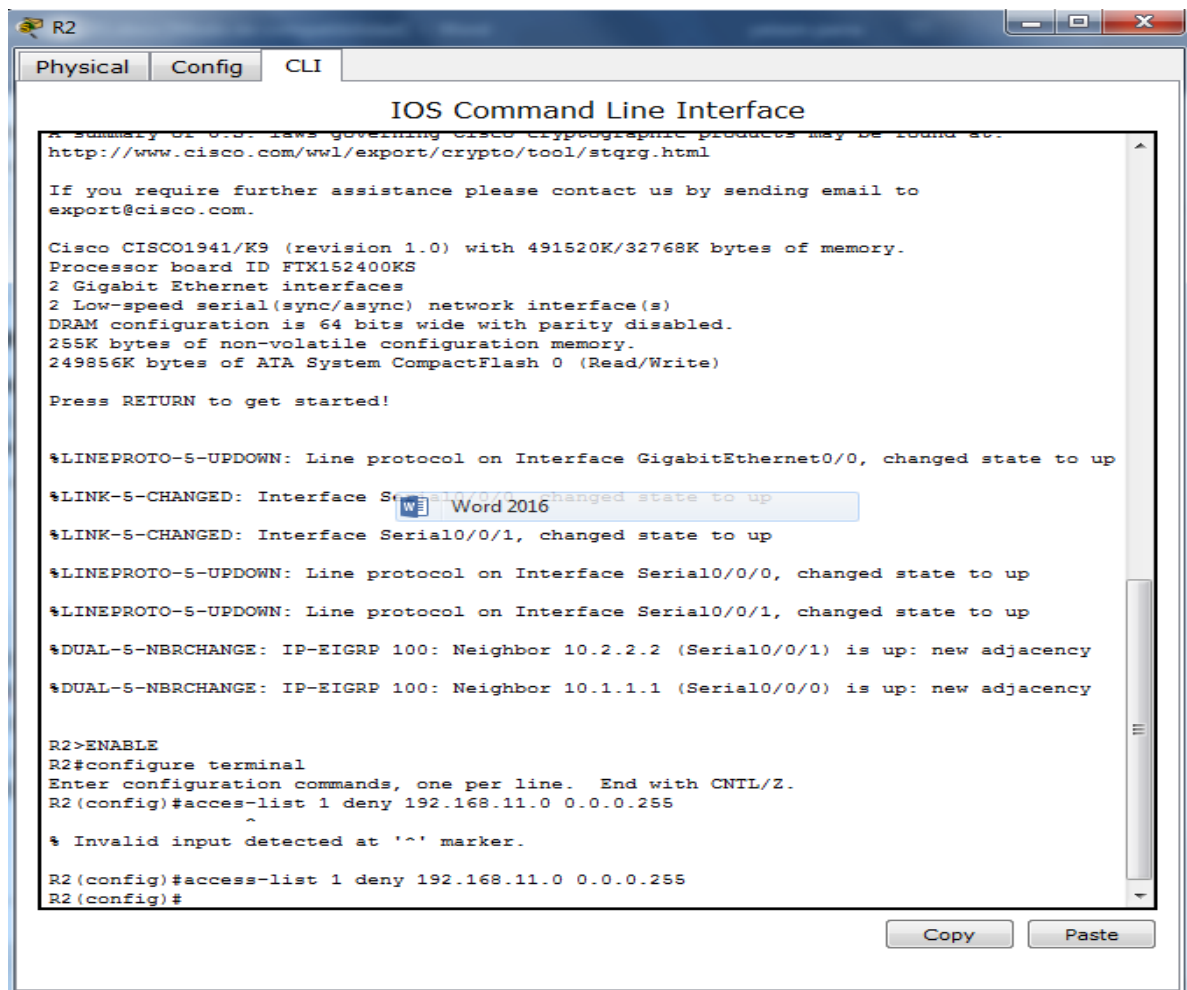
To restrict access from the 192.168.10.0/24 network to the 192.168.30.0/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must be placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

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

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

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

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



```
R2
Physical Config CLI
IOS Command Line Interface
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

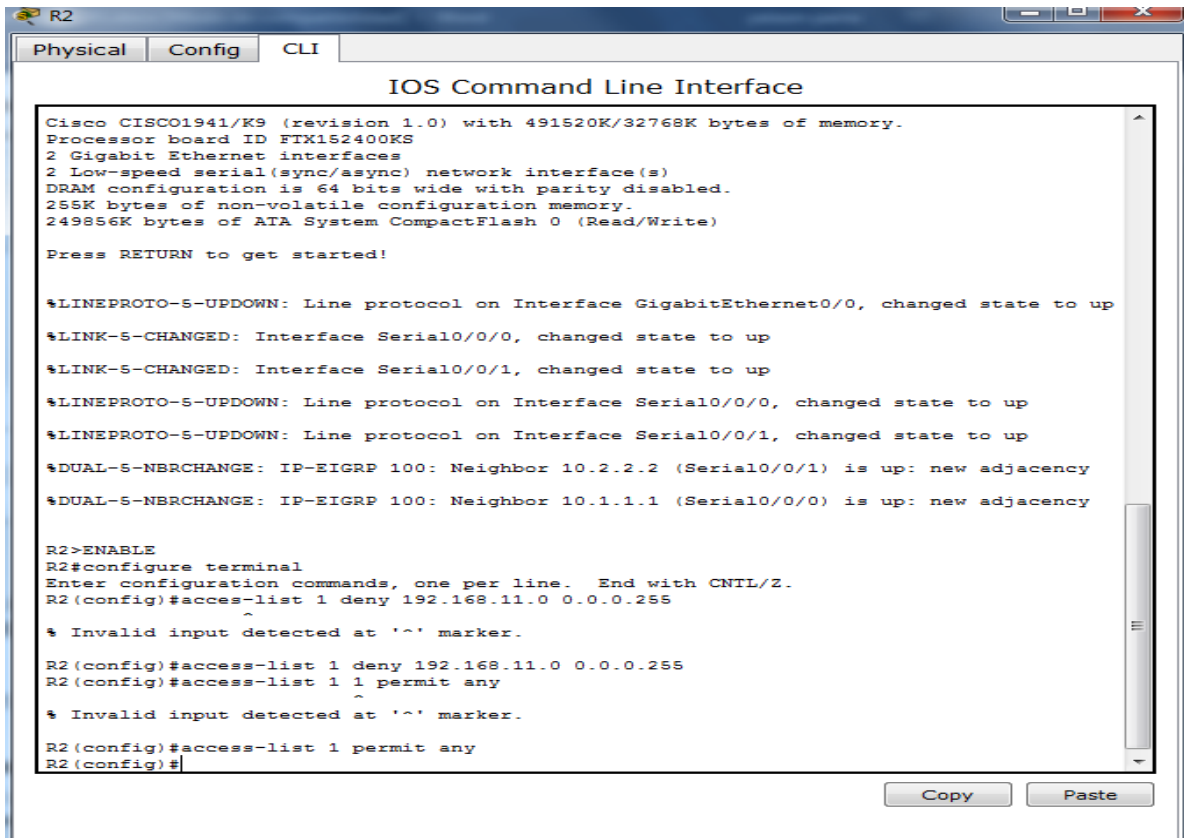
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.2 (Serial0/0/1) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency

R2>ENABLE
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
^
% Invalid input detected at '^' marker.

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

- 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
```



The screenshot shows a Cisco IOS Command Line Interface window for router R2. The window title is "R2" and it has tabs for "Physical", "Config", and "CLI". The main content area displays the following text:

```
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.2 (Serial0/0/1) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency

R2>ENABLE
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
^
% Invalid input detected at '^' marker.

R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 1 permit any
^
% Invalid input detected at '^' marker.

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

At the bottom of the window, there are "Copy" and "Paste" buttons.

- 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
```

The screenshot shows the R2 IOS Command Line Interface. The window title is 'R2' and it has tabs for 'Physical', 'Config', and 'CLI'. The main content area displays the following text:

```
Processor board ID F11102700K
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.2 (Serial0/0/1) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency

R2>ENABLE
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
      ^
% Invalid input detected at '^' marker.

R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 1 permit any
      ^
% Invalid input detected at '^' marker.

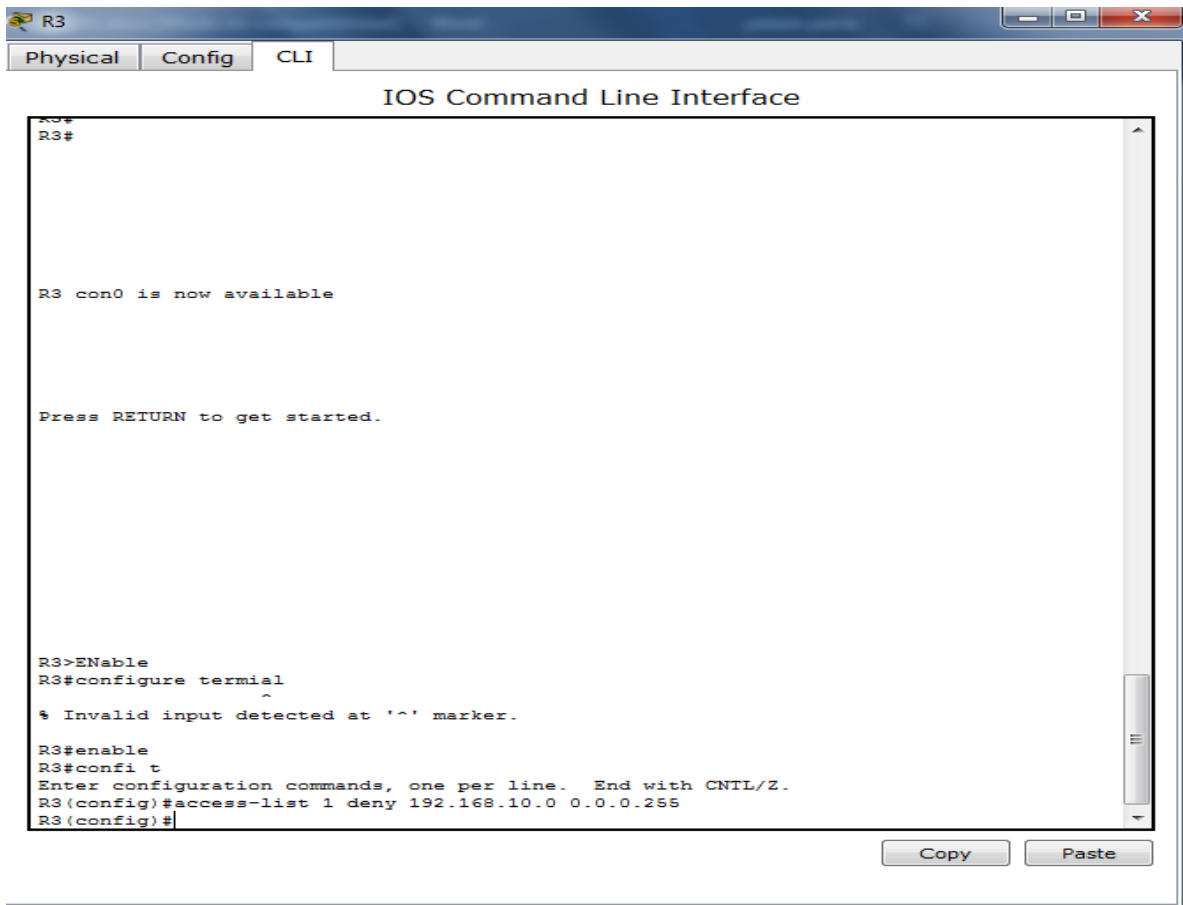
R2(config)#access-list 1 permit any
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

At the bottom right of the terminal window, there are 'Copy' and 'Paste' buttons.

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

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

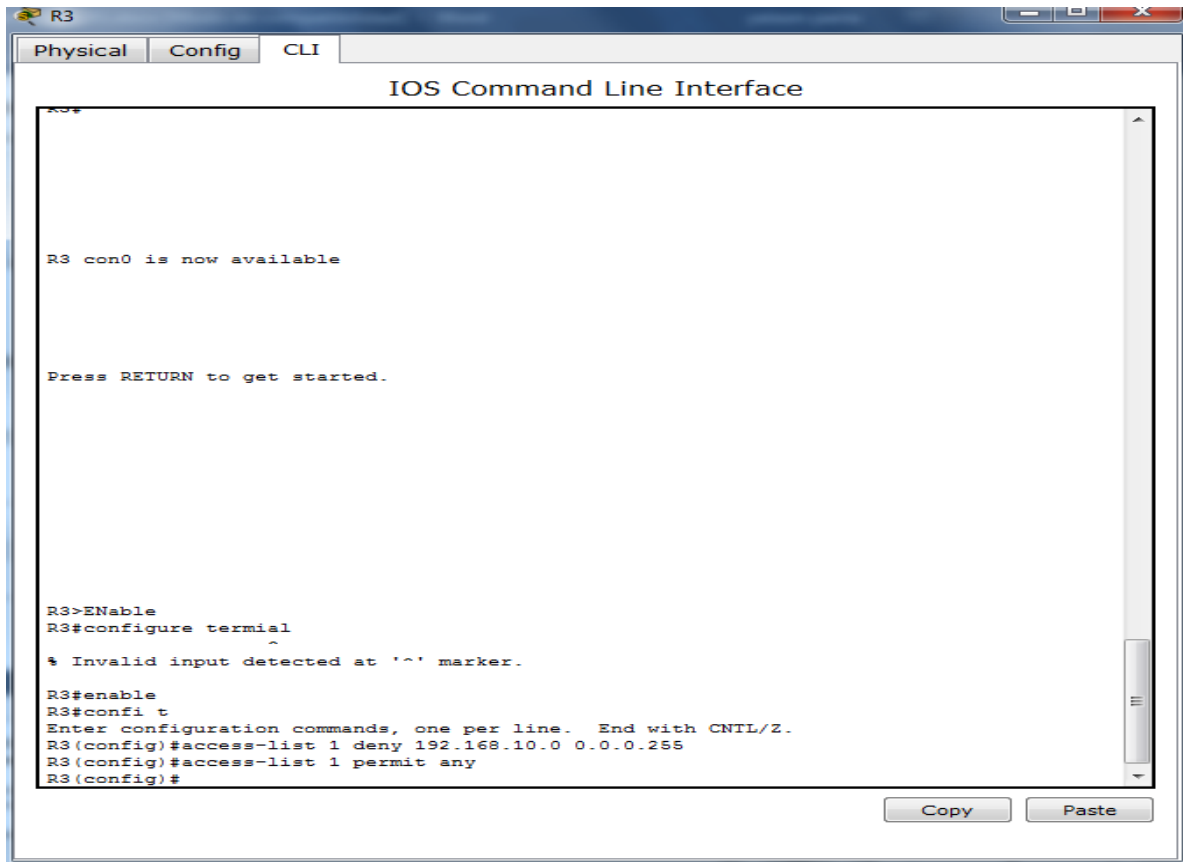
**R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255**



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

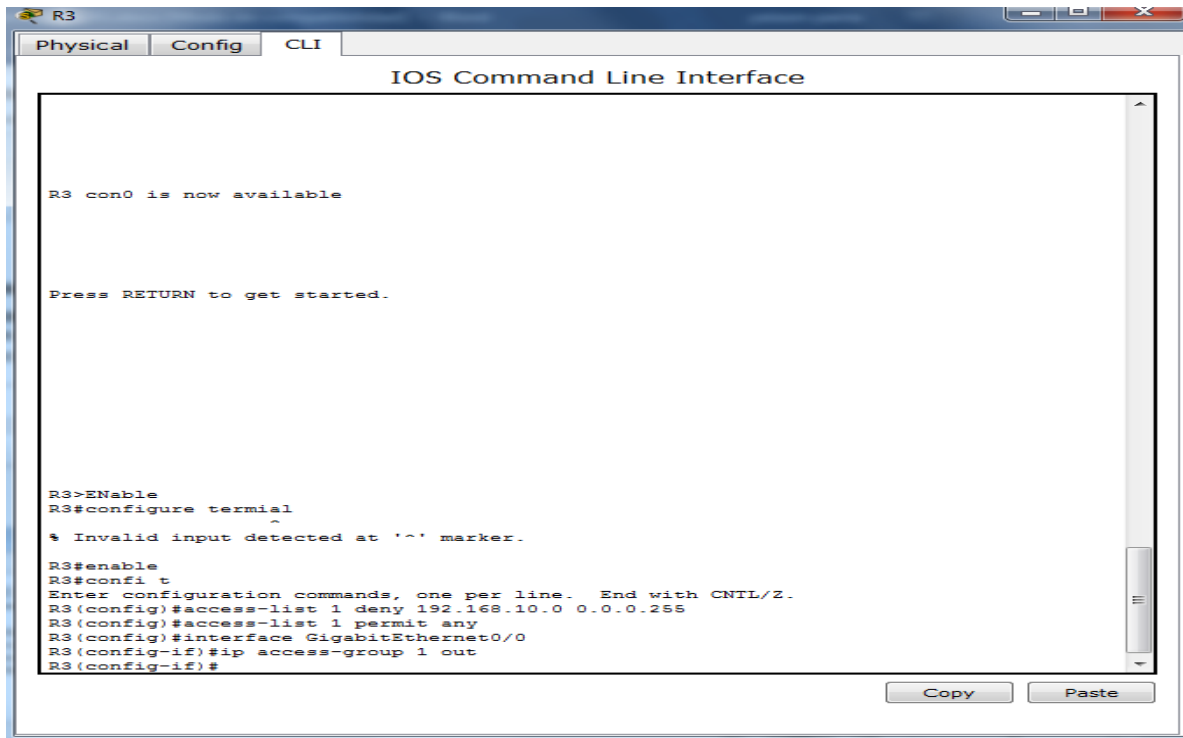
**R3(config)# access-list 1 permit any**





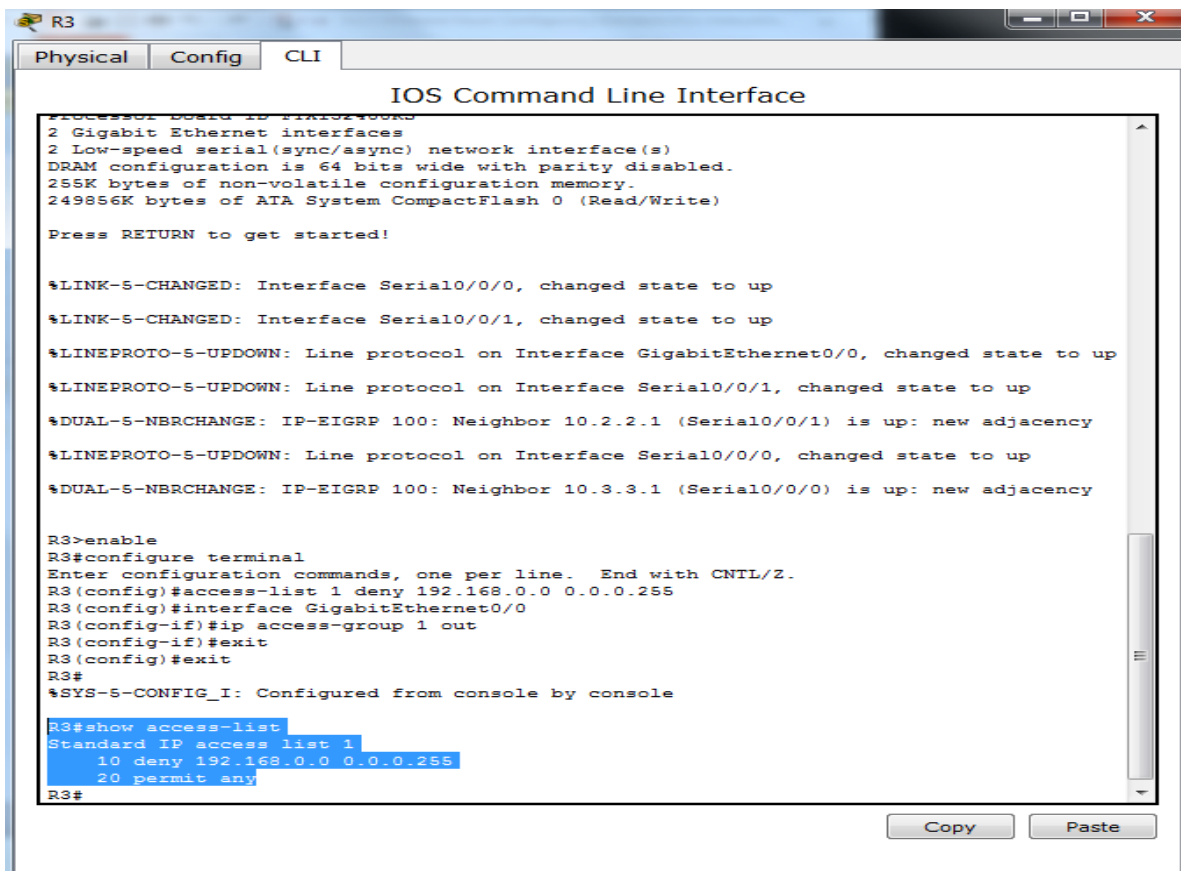
- c. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

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



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

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





R2

Physical Config CLI

### IOS Command Line Interface

```
interface GigabitEthernet0/0
ip address 192.168.20.1 255.255.255.0
ip access-group 1 out
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
description Link to R1
ip address 10.1.1.2 255.255.255.252
clock rate 2000000
!
interface Serial0/0/1
description Link to R3
ip address 10.2.2.1 255.255.255.252
clock rate 4000000
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
passive-interface GigabitEthernet0/0
network 192.168.20.0
network 10.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
access-list 1 deny 192.168.11.0 0.0.0.255
access-list 1 permit any
!
```

Copy Paste

R2

Physical Config CLI

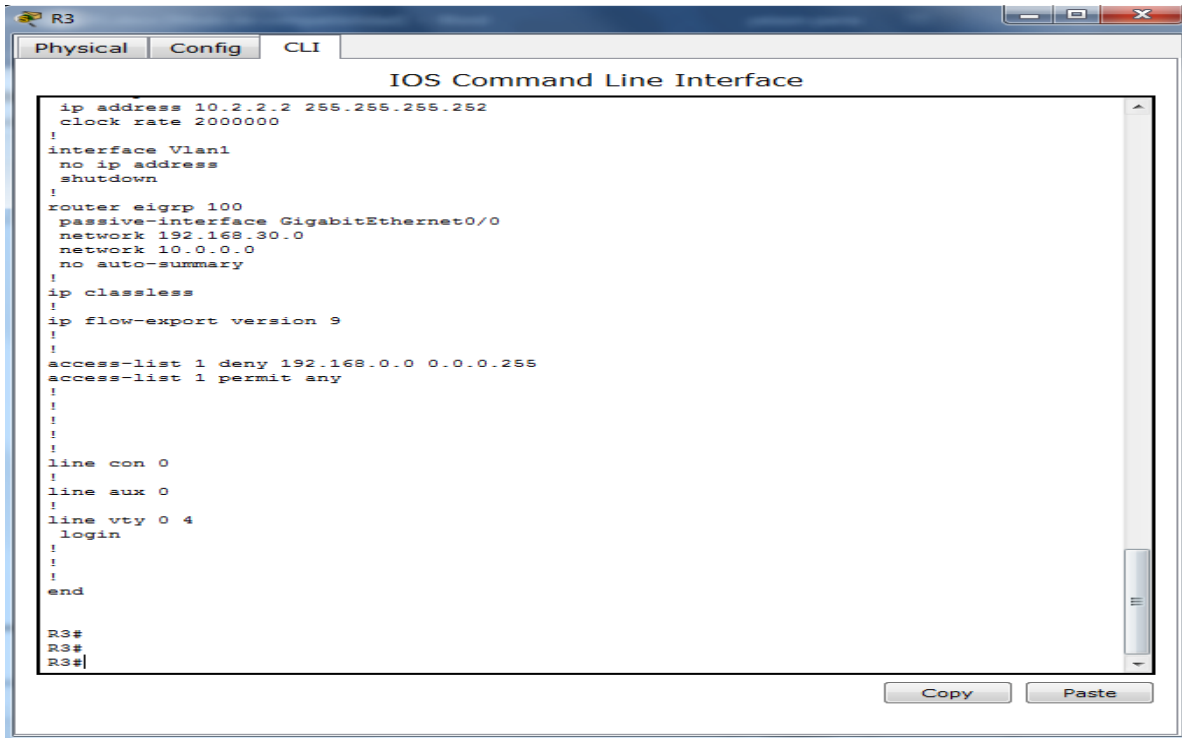
### IOS Command Line Interface

```
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
passive-interface GigabitEthernet0/0
network 192.168.20.0
network 10.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
access-list 1 deny 192.168.11.0 0.0.0.255
access-list 1 permit any
!
!
!
!
line con 0
login
!
line aux 0
!
line vty 0 4
login
!
!
!
end

R2#
R2#
R2#
R2#
```

Copy Paste





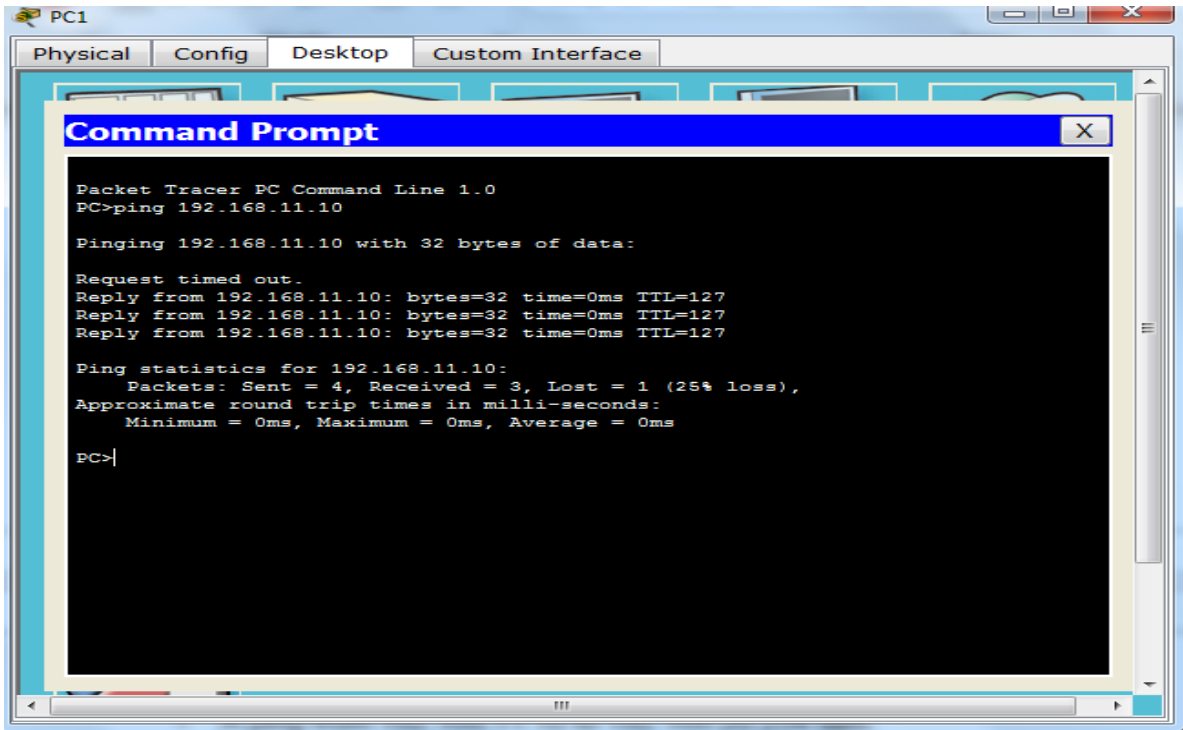
The screenshot shows a Cisco IOS CLI window for router R3. The window title is "R3" and it has tabs for "Physical", "Config", and "CLI". The main content area is titled "IOS Command Line Interface" and displays the following configuration commands:

```
ip address 10.2.2.2 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
passive-interface GigabitEthernet0/0
network 192.168.30.0
network 10.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
access-list 1 deny 192.168.0.0 0.0.0.255
access-list 1 permit any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
!
login
!
!
!
end

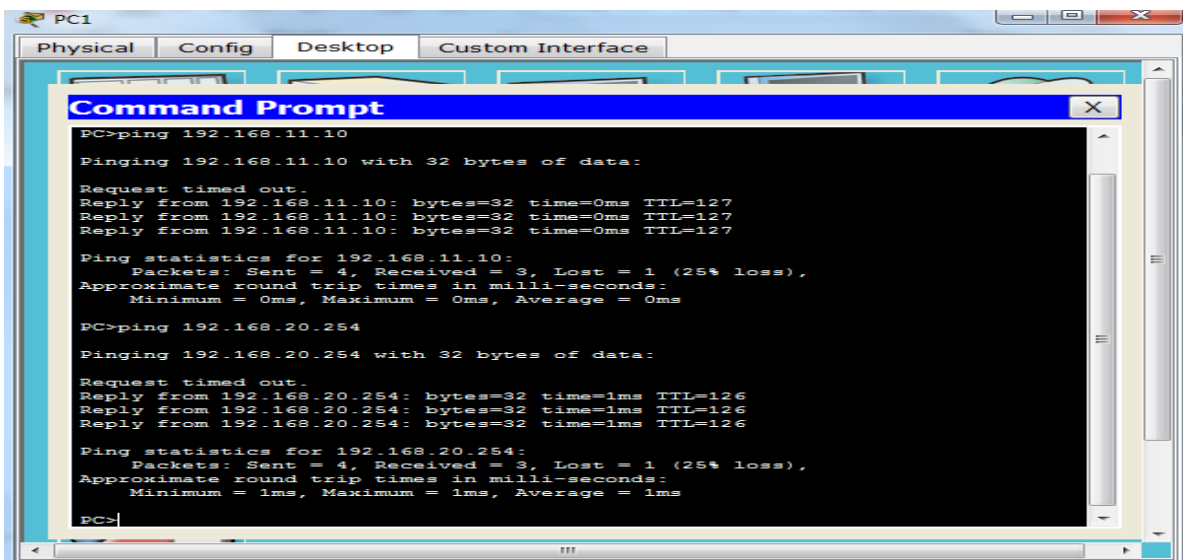
R3#
R3#
R3#
```

At the bottom right of the window, there are "Copy" and "Paste" buttons.

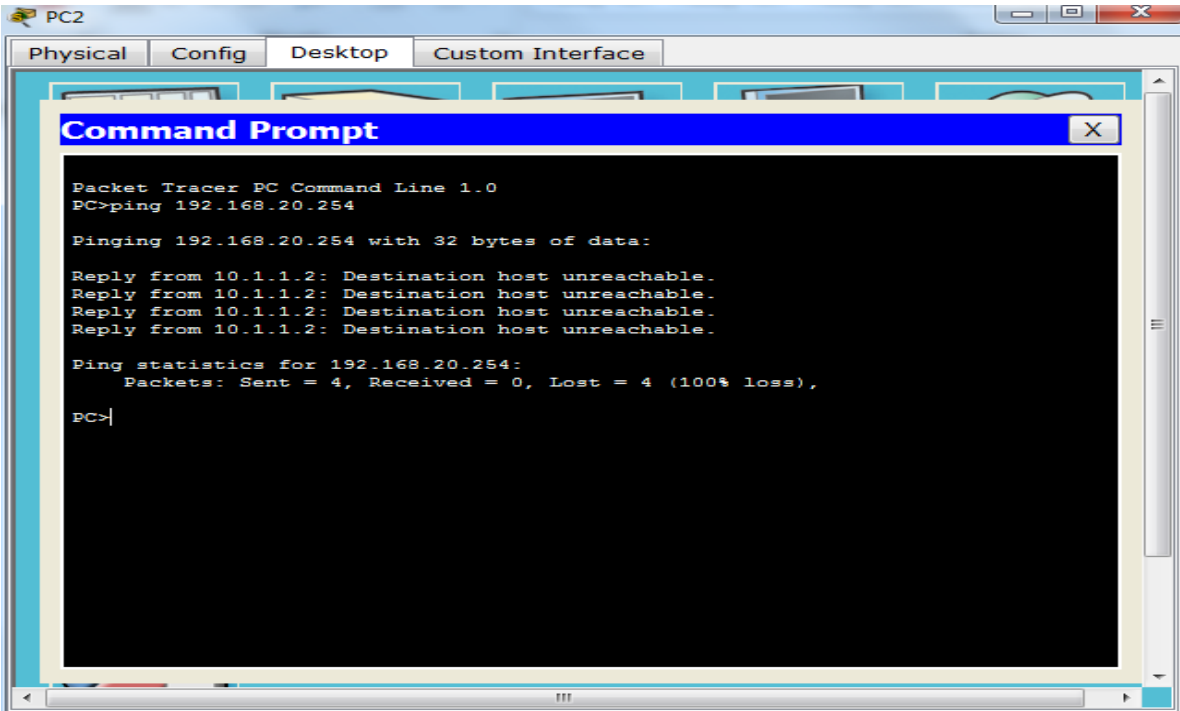
- b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:
- A ping from 192.168.10.10 to 192.168.11.10 succeeds.



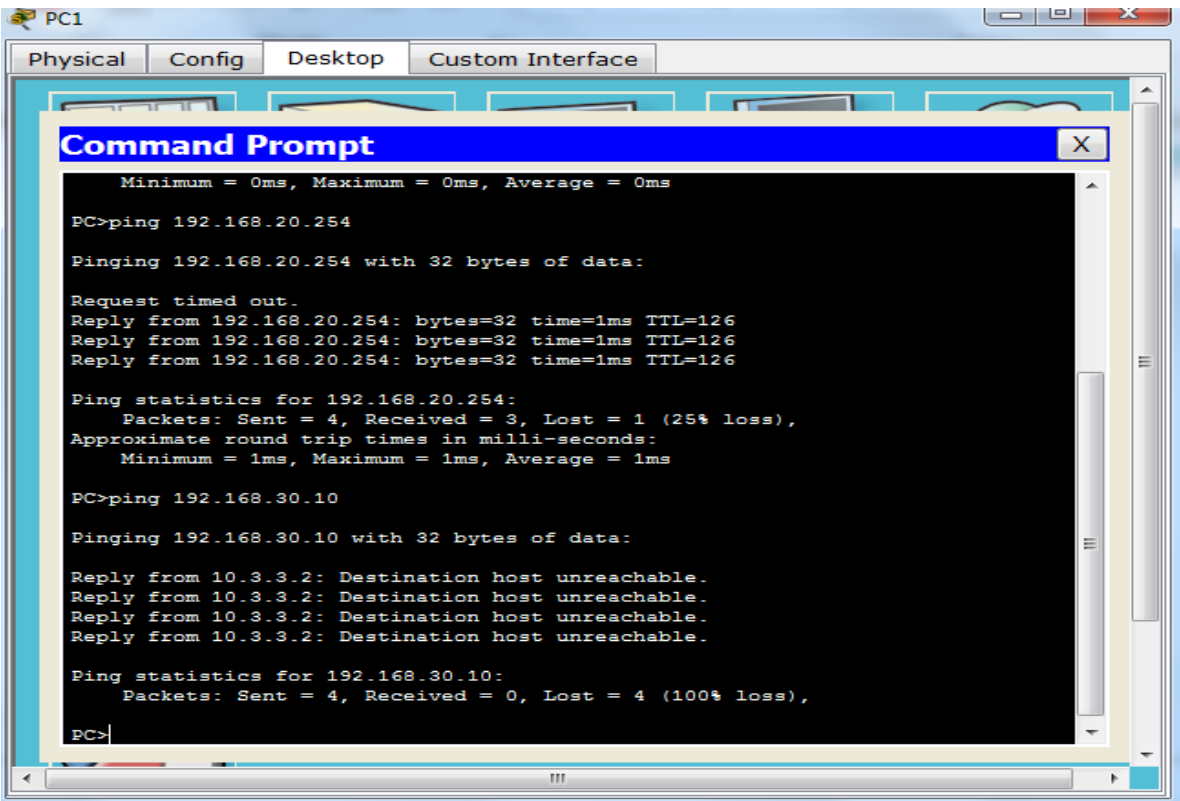
- A ping from 192.168.10.10 to 192.168.20.254 succeeds.



- A ping from 192.168.11.10 to 192.168.20.254 fails.

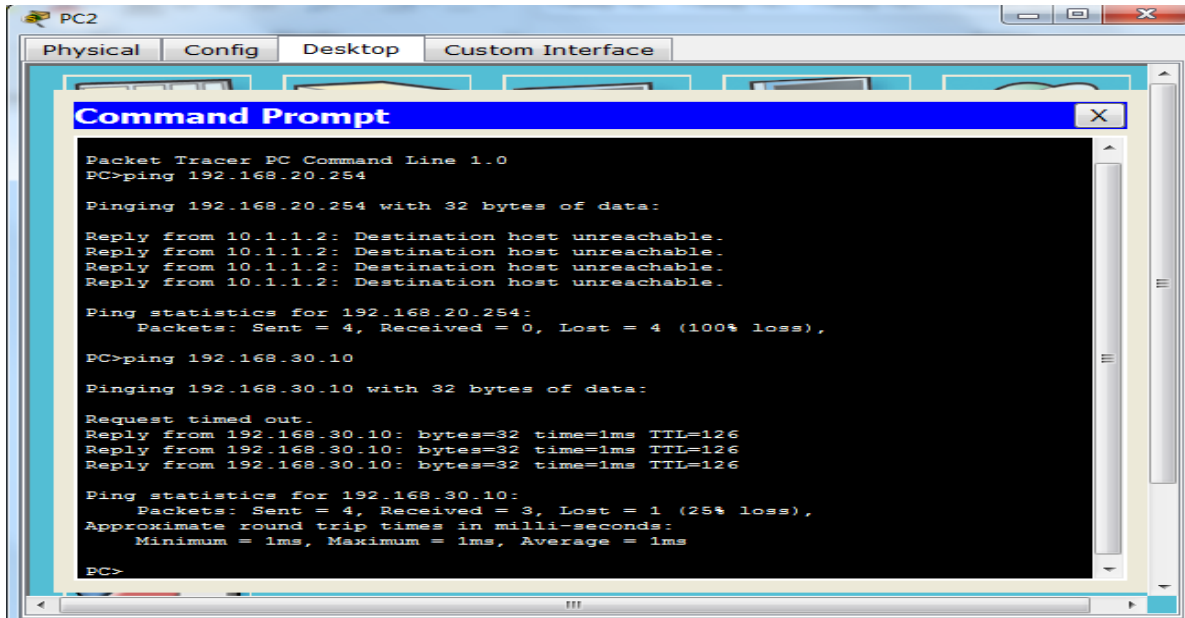


- A ping from 192.168.10.10 to 192.168.30.10 fails.

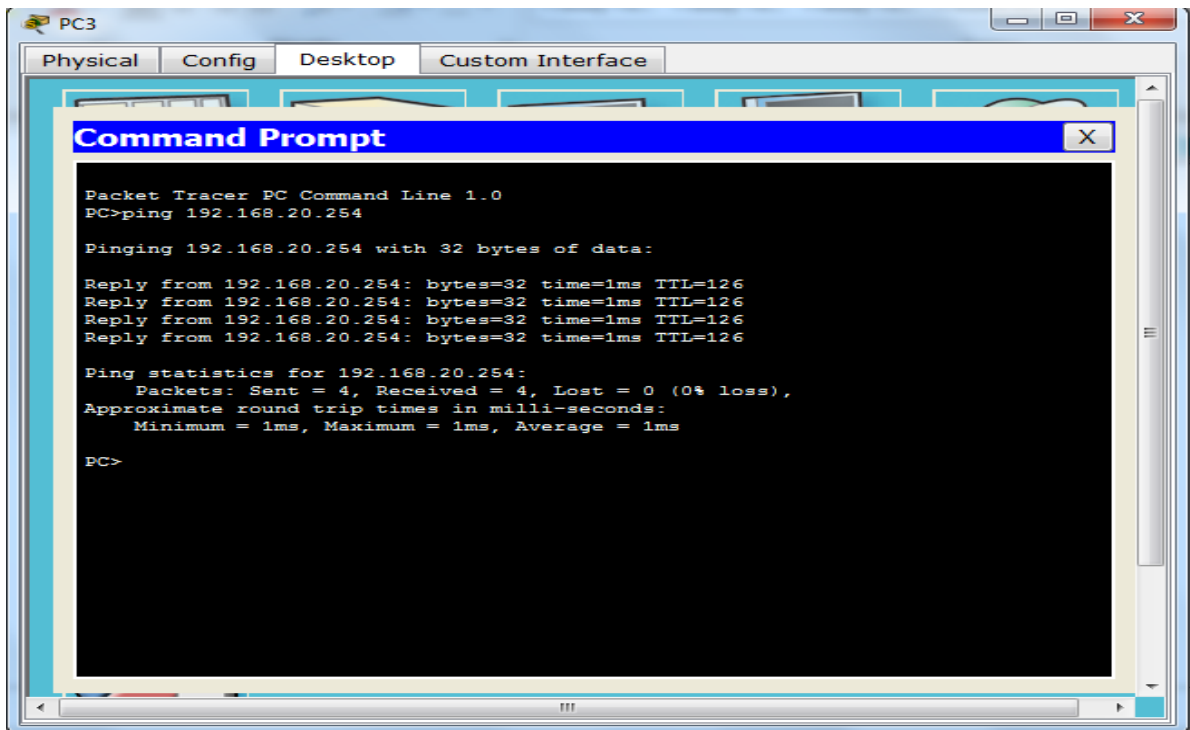




- A ping from 192.168.11.10 to 192.168.30.10 succeeds.



- A ping from 192.168.30.10 to 192.168.20.254 succeeds.



# Activity Results

Time Elapsed: 00:15:36

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items

- Network
  - R2
    - ACL 1 ✓
    - Ports
      - GigabitEthernet0/0
        - Access-group ...
  - R3
    - ACL 1 ✓
    - Ports
      - GigabitEthernet0/0
        - Access-group ...

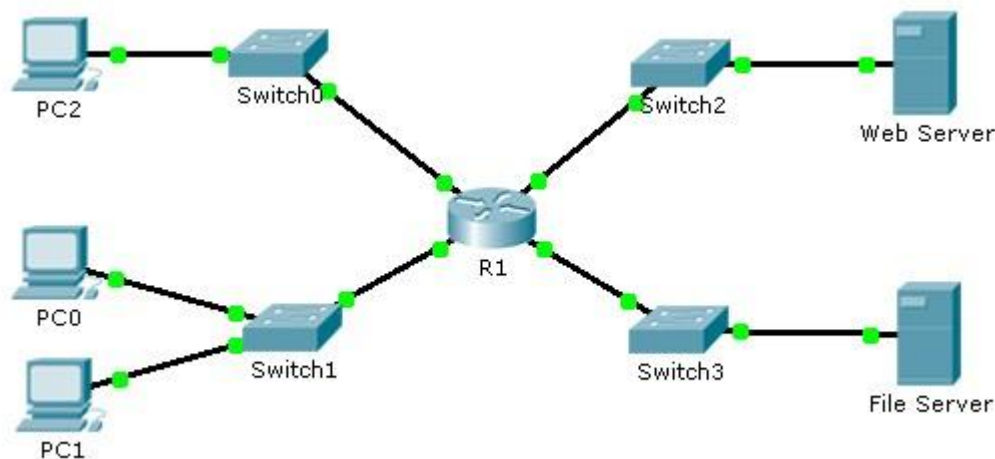
Score : 100/100  
Item Count : 4/4

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

Close

### 9.2.1.11 Configuring Named Standard ACLs

#### Topology



#### Addressing Table

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

#### Objectives

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

**ACL Part 2: Verify the ACL Implementation**

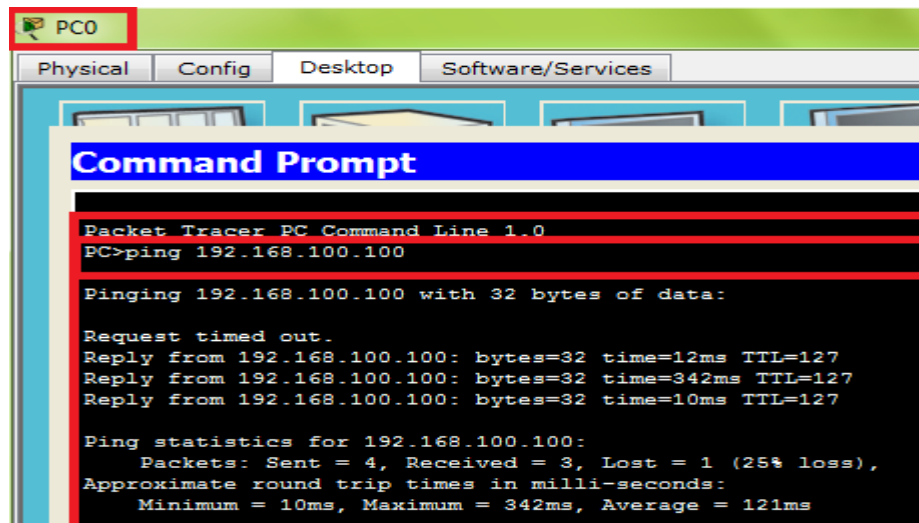
#### Background / Scenario

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

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

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

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



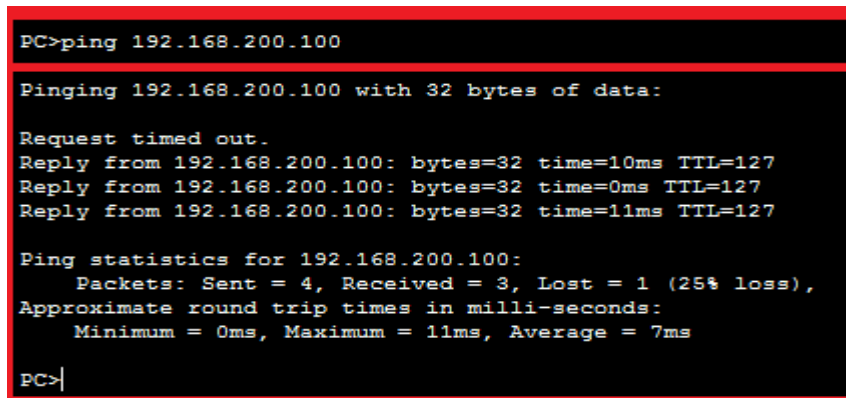
The screenshot shows a Packet Tracer PC interface with a Command Prompt window open. The window title is "Command Prompt" and the text inside reads:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=342ms TTL=127
Reply from 192.168.100.100: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 342ms, Average = 121ms
```



The screenshot shows a Packet Tracer PC interface with a Command Prompt window open. The window title is "Command Prompt" and the text inside reads:

```
PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time=10ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 7ms

PC>|
```

```
PC2
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=13ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=10ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 6ms
```

```
PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=11ms TTL=127
Reply from 192.168.200.100: bytes=32 time=10ms TTL=127
Reply from 192.168.200.100: bytes=32 time=3ms TTL=127
Reply from 192.168.200.100: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 11ms, Average = 8ms

PC>
```

## Step 2: Configure a named standard ACL.

Configure the following named ACL on **R1**.

```
R1(config)# ip access-list standard File_Server_Restrictions
```

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

```
R1(config-std-nacl)# deny any
```

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

## Step 3: Apply the named ACL.

- Apply the ACL outbound on the interface Fast Ethernet 0/1.

R1(config-if)# **ip access-group File\_Server\_Restrictions out**

- b. Save the configuration.

```
R1(config)#interface f0/1
R1(config-if)#ip access-group file_server_restrictions out
R1(config-if)#
```

## Part 2: Verify the ACL Implementation

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

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

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

```
R1#show run
Building configuration...

Current configuration : 888 bytes
!
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
```

```
R1#show ip interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
 Internet address is 192.168.200.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is file server restrictions
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
--More--
```

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

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

PC-0

```
PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

PC-1

```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=14ms TTL=127
Reply from 192.168.200.100: bytes=32 time=15ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 7ms

PC>

```

PC-2

```

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>

```

Evidencia de la actividad resuelta

**Activity Results** Time Elapsed: 00:47:36

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points
Network		
R1		
ACL		
File_Server_Restic...	Correct	0
Ports		
FastEthernet0/1		0
Access-group Out	Correct	20

**Score** : 100/100

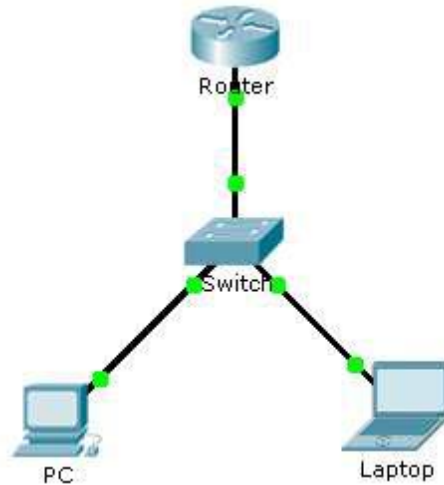
**Item Count** : 2/2

Component	Items/Total	Score
IPv4 Standard ACL Implementation	2/2	100/100



### 9.2.3.3 Configuring an ACL on VTY Lines

#### Topología



#### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Laptop	NIC	10.0.0.2	255.0.0.0	10.0.0.254

#### Objectives

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

**Part 2: Verify the ACL Implementation**

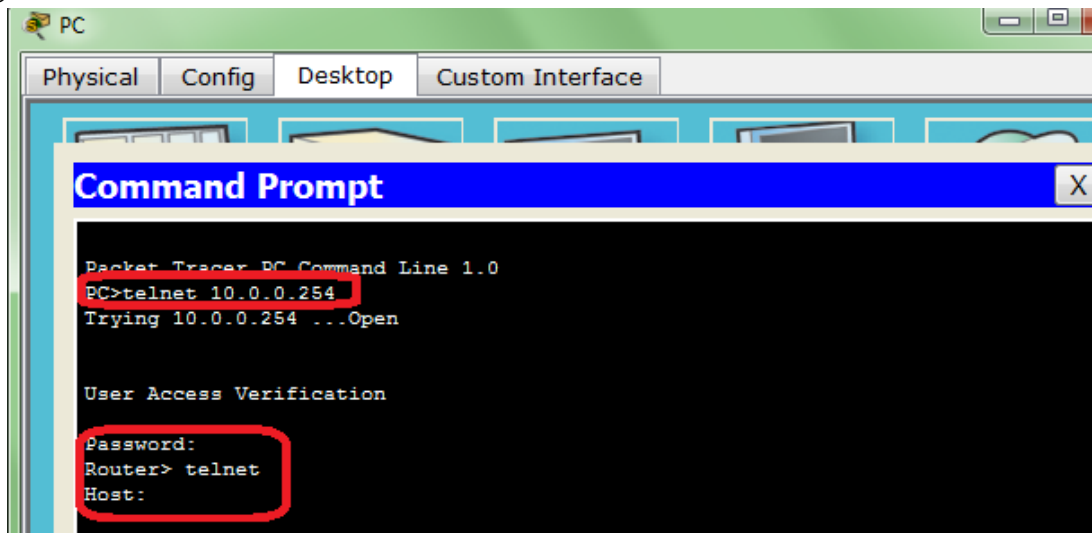
## Parte 1: configurar y aplicar ACL a líneas VTY

### Paso 1: Verifique el acceso de Telnet antes de que se configure la ACL.

- Ambas computadoras deberían acceder por Telnet al router. La contraseña es Cisco.

RTA: como se puede ver al ejecutar telnet con la dirección 10.0.0.254 correspondiente al router ya sea, desde PC o Laptop ambas nos permiten el acceso al router sin ninguna dificultad.

#### PC

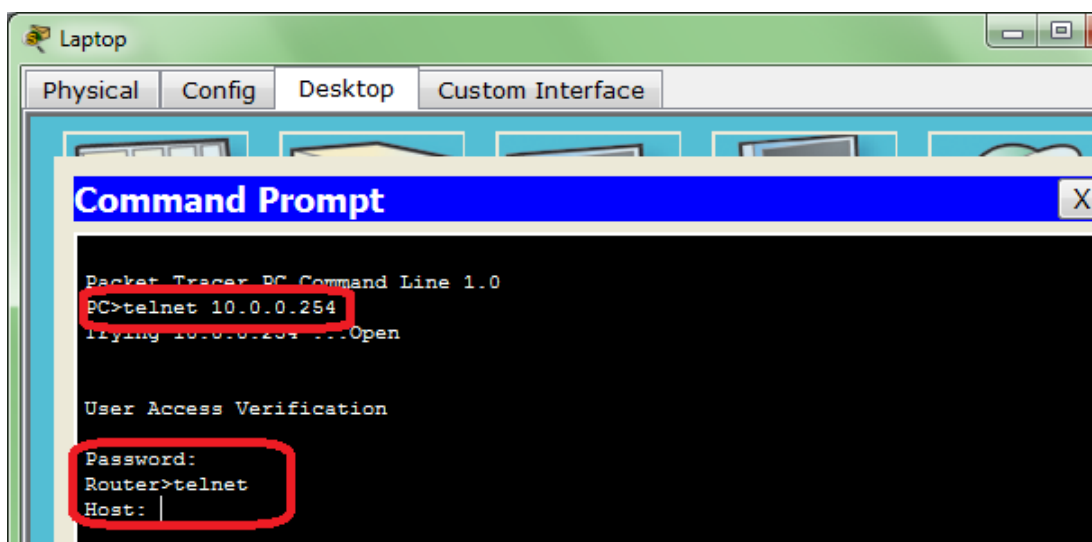


```
Packet Tracer PC Command Line 1.0
PC>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>telnet
Host:
```

#### Laptop



```
Packet Tracer PC Command Line 1.0
Laptop>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>telnet
Host:
```

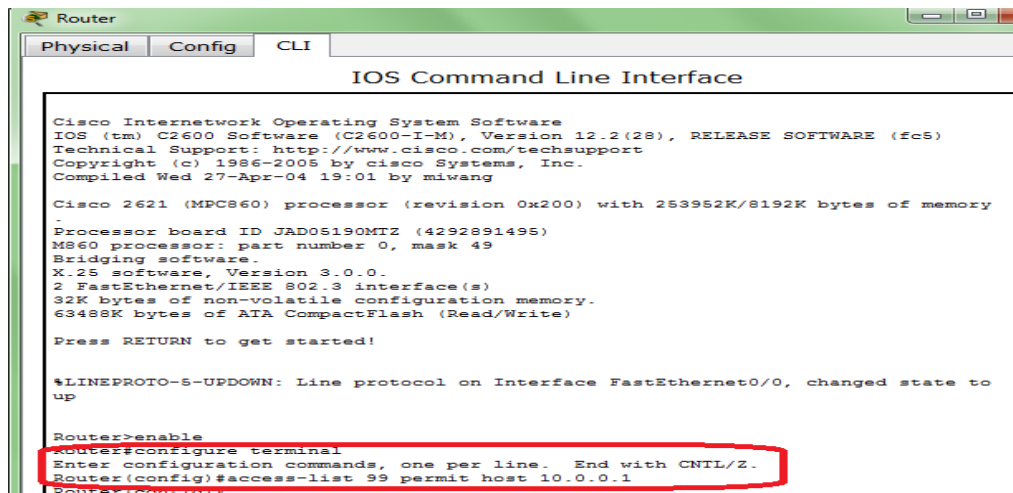
### Paso 2: configurar una ACL numerada estándar.

- Configure la siguiente ACL numerada en el router.

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

Como no queremos permitir el acceso a otras computadoras, la denegación implícita lista satisface nuestros requisitos.

RTA: creamos una lista donde estamos solamente dándole acceso al host 10.0.0.1 correspondiente a la dirección ip de la PC.



```
Router
Physical Config CLI
IOS Command Line Interface

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

Cisco 2621 (MPC860) processor (revision 0x200) with 253952K/8192K bytes of memory
-
Processor board ID JAD0S190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

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

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

### Paso 3: Coloque una ACL estándar nombrada en el router.

Se debe permitir el acceso a las interfaces del **router**, mientras que el acceso a Telnet debe estar restringido. Por lo tanto, debemos colocar la ACL en las líneas Telnet 0 a 4. Desde el indicador de configuración de **Router**, ingrese la configuración de línea modo para las líneas 0 - 4 y use el comando **access-class** para la ACL a todas las líneas VTY:

```
Router(config)# line vty 0 15
```

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

```
Router
Physical Config CLI
IOS Command Line Interface
Copyright (C) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Cisco 2621 (MPC860) processor (revision 0x200) with 253952K/8192K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

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

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#do wr
Building configuration...
[OK]
Router(config-line)#
```

## Parte 2: Verificar la implementación de ACL

### Paso 1: verifique la configuración de ACL y aplique a las líneas VTY.

- Use **show access-lists** para verificar la configuración de ACL. Use la ejecución del espectáculo para verificar que la ACL aplicado a las líneas VTY.

RTA: al ejecutar el comando para observar las listas de acceso nos muestra efectivamente la que acabamos de generar.

```
Router
Physical Config CLI
IOS Command Line Interface
X.25 software, version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

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

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#do wr
Building configuration...
[OK]
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

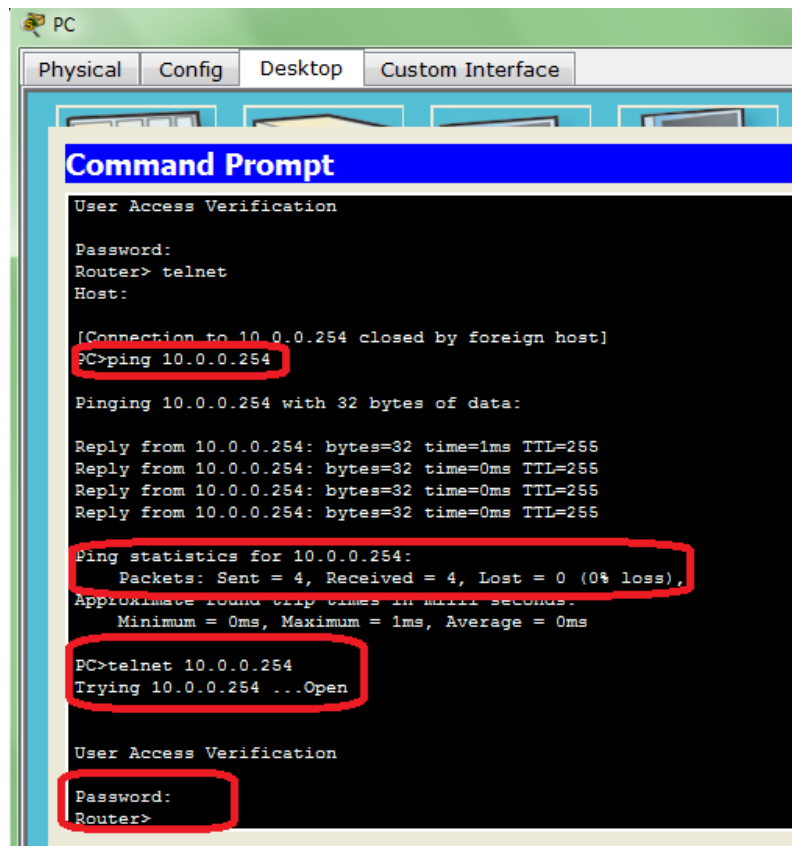
Router#show access-list
Standard IP access list 99
 10 permit host 10.0.0.1
Router#
```

### Paso 2: Verifique que la ACL esté funcionando correctamente.

Ambas computadoras deberían poder hacer ping al Enrutador, pero solo las PC deberían poder usar Telnet.

RTA: se puede observar que si ejecutamos el ping en las 2 computadoras este nos muestra que está correcto, pero al ejecutar el telnet en el **Laptop** automáticamente nos muestra un mensaje de conexión rechazada.

**PC**



The screenshot shows a Windows PC window titled 'PC' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. A 'Command Prompt' window is open, displaying the following text:

```
User Access Verification
Password:
Router> telnet
Host:

[Connection to 10.0.0.254 closed by foreign host]
PC>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=1ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255

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

PC>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification
Password:
Router>
```

Red boxes highlight the following elements in the screenshot:

- The command `PC>ping 10.0.0.254`
- The ping statistics for 10.0.0.254, showing 4 packets sent and received with 0% loss.
- The command `PC>telnet 10.0.0.254` and the response `Trying 10.0.0.254 ...Open`
- The password prompt `Password:` and the `Router>` prompt.

**Laptop**

```
Laptop
Physical | Config | Desktop | Custom Interface
Command Prompt
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>telnet
Host:

[Connection to 10.0.0.254 closed by foreign host]
PC>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

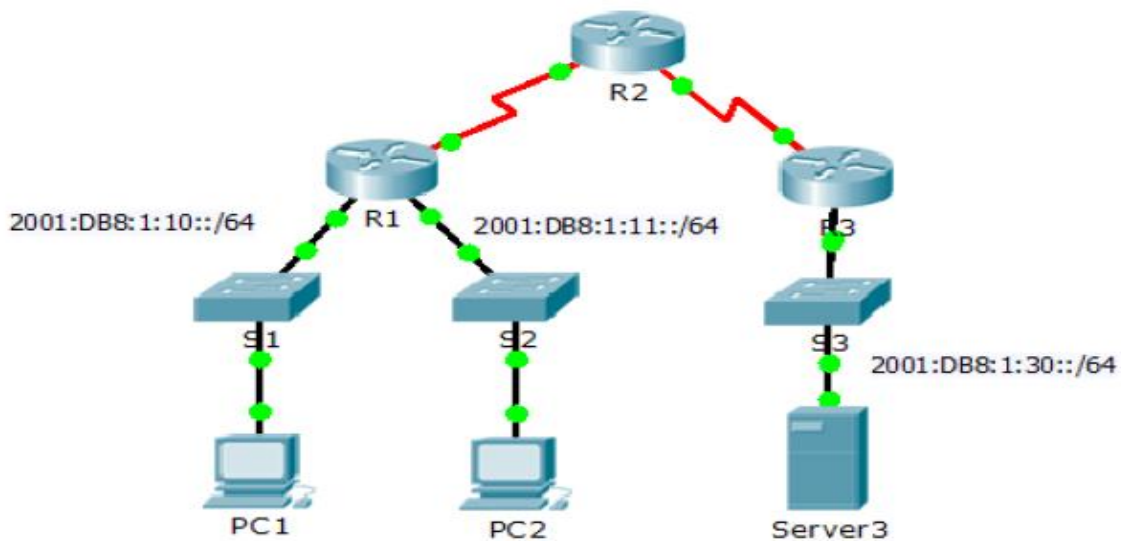
Reply from 10.0.0.254: bytes=32 time=2ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=9ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 9ms, Average = 2ms

PC>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
PC>
```

### 9.5.2.6 Configuring IPv6 ACLs

#### Topología



#### Tabla de direcciones

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

#### Objetivos

Parte 1: Configure, aplique y verifique una ACL IPv6

Parte 2: Configurar, aplicar y verificar una segunda ACL de IPv6

## Parte 1: Configure, aplique y verifique una ACL IPv6

Los registros indican que una computadora en la red 2001: DB8: 1: 11 :: 0/64 está actualizando repetidamente su página web causando un ataque de denegación de servicio (DoS) contra **Server3**. Hasta que el cliente pueda ser identificado y limpiado, debe bloquear el acceso HTTP y HTTPS a esa red con una lista de acceso.

### PASO 1: CONFIGURE UNA ACL QUE BLOQUEARÁ EL ACCESO HTTP Y HTTPS.

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

- a. Bloquear el tráfico HTTP y HTTPS de llegar a Server3.

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

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

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

- b. Permitir que todo el tráfico IPv6 pase

```
R1(config-ipv6-acl)#deny tcp any host
R1(config-ipv6-acl)#permit ip any any
R1(config-ipv6-acl)#
```

### Paso 2: Aplique la ACL a la interfaz correcta.

Aplique la ACL en la interfaz más cercana al origen del tráfico que se va a bloquear.

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

```
R1(config)#int g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

### Paso 3: Verificar la implementación de ACL

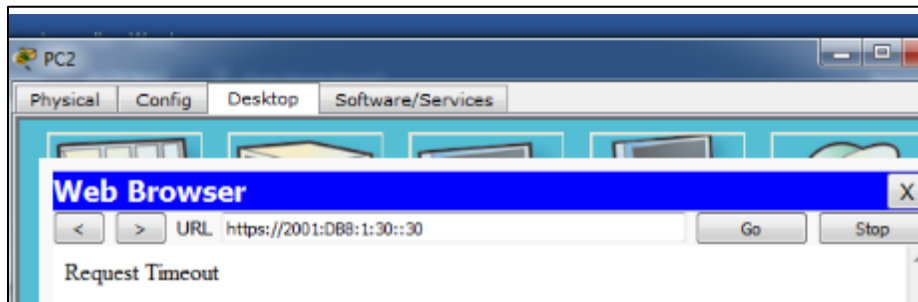
Verifique que la ACL esté funcionando según lo previsto realizando las siguientes pruebas:



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



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



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

```
PC>PING 2001:DB8:1:30::30

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

Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

PC>
```

## Parte 2: Configurar, aplicar y verificar una segunda ACL de IPv6

Los registros ahora indican que su servidor está recibiendo pings de muchas direcciones IPv6 diferentes en un ataque de denegación de servicio distribuido (DDoS). Debe filtrar peticiones de ping ICMP a su servidor

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

Configure una ACL denominada BLOCK\_ICMP en R3 con las siguientes sentencias:

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

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

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

- b. Allow all other IPv6 traffic to pass.

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

### Paso 2: Aplique la ACL a la interfaz correcta.

En este caso, el tráfico ICMP puede provenir de cualquier fuente. Para asegurarse de que el tráfico ICMP se bloquea independientemente de su origen o de los cambios que se produzcan en la topología de red, aplique la ACL más cercana al destino.

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g0/0
R3(config-if)#ipv6 traffic-filterer BLOCK_ICMP out
^
% Invalid input detected at '^' marker.
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

### Paso 3: Verifique que funcione la lista de acceso adecuado.

- a. Ping de PC2 a 2001:DB8:1:30::30. El ping debe fallar. segundo.

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

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

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

PC>
```

- b. Ping de PC1 a 2001:DB8:1:30::30. El ping debe fallar.

```
PC>PING 2001:db8:1:30::30

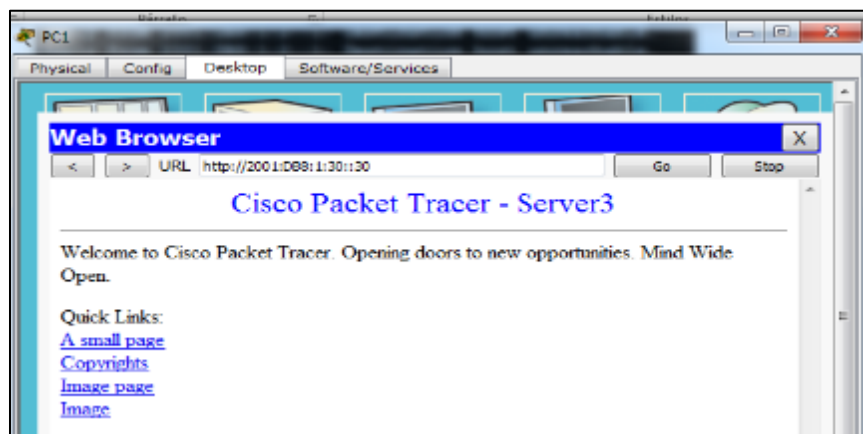
Pinging 2001:db8:1:30::30 with 32 bytes of data:

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

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

PC>
```

Abra el explorador Web de PC1 a <http://2001:DB8:1:30::30> o <https://2001:DB8:1:30::30>. El sitio web debe mostrar



## Conclusiones

El trabajo realizado por cada uno en el programa de Packet Tracer, pudo reflejar los conocimientos adquiridos por los estudiantes y en conclusión se puede decir lo siguiente:

- Con la realización de cada uno de los ejercicios se pudo lograr una configuración básica de RIPv2 y RIPv6
- Se definió OSPFv2 para redes IPv4 y OSPFv3 para redes IPv6
- Se trabaja la configuración de DHCPv4 básico en un router o configuración dinámica de host (DHCP)
- En el proceso de aprendizaje se trabaja la configuración de NAT dinámica y estática, logrando la asignación de una dirección pública a los dispositivos host dentro de una red privada
- Por último se manejó la configuración estándar de ACL

## Bibliografía

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e00xww&AN=440032&lang=es&site=ehost-live>

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de: <http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>