



**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**

**Diplomado de profundización Cisco (Diseño e implementación de soluciones  
integradas LAN / WAN)**

**Trabajo Colaborativo 4**

**Autores:**

**Wilmer Saul Astudillo Fajardo Cod. 10294210**

**Magda Patricia León Cod. 52545456**

**Marly Angulo Mosquera Cod. 34674484**

**Angela Carolina Chacon Cod. 52918113**

**Diana Alejandra Hernandez**

**Grupo Colaborativo 34**

**Gerardo Granados Acuña**

**Tutor**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD).  
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA  
BOGOTÁ D.C.  
NOVIEMBRE 2017.  
INTRODUCCION**

En los siguientes capítulos a estudiar y en las siguientes actividades se podrán conocer de forma detallada algunos temas como el enrutamiento dinámico que es utilizado en organizaciones grandes con el fin de minimizar la carga de mantenimiento y operatividad especialmente cuando hay cambios en la red por daños por ejemplo, el enrutamiento dinámico proporciona escalabilidad en la red, podremos ver los protocolos utilizados para que esto sea posible por ejemplo.

Otro de los temas que se estudiarán por medio de las siguientes prácticas es el OSPF, el cual es un protocolo de estado de enlace que permite determinar la mejor ruta de los mensajes de una manera más eficiente comparada con el anterior (RIP), éste utiliza el concepto de áreas para realizar la escalabilidad.

También veremos las listas de control de acceso (ACL) para el tema de seguridad, es decir que por medio de estas un administrador de red puede permitir o restringir el uso del tráfico de su red en partes específicas.

Los DHCP permiten asignar de forma dinámica la dirección IP de los hosts en su red, esto minimiza razonablemente el mantenimiento de la misma, este es un protocolo muy útil en una organización donde los empleados están cambiando constantemente de ubicación.

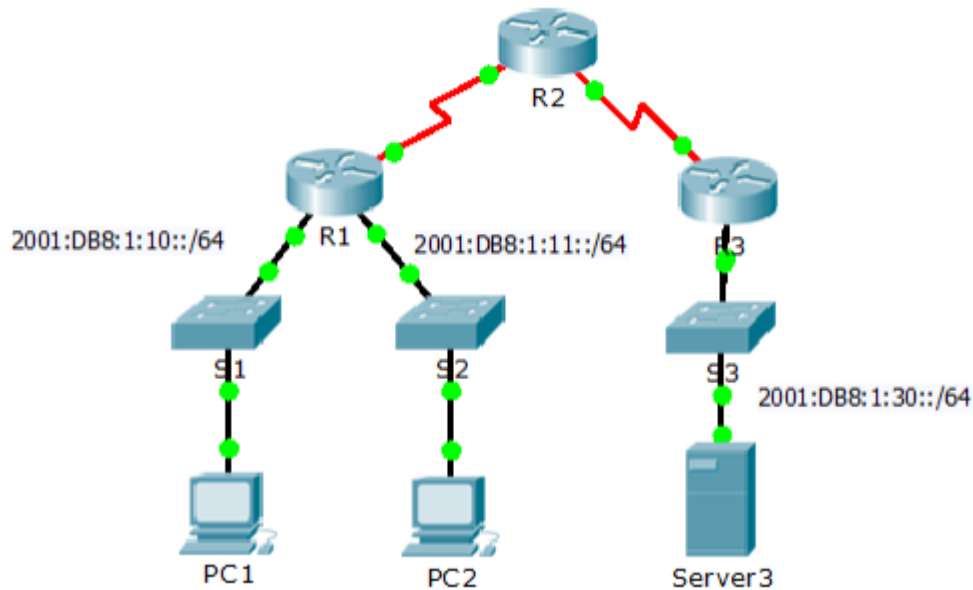
Este y otros temas como la traducción de direcciones IPv4 se podrán conocer más a fondo al realizar cada práctica propuesta a continuación.

## DESARROLLO ACTIVIDADES

### 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs Instructions IG

#### Packet Tracer - Configuring IPv6 ACLs

#### Topology



#### Addressing Table

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

#### Objectives

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

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

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

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

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

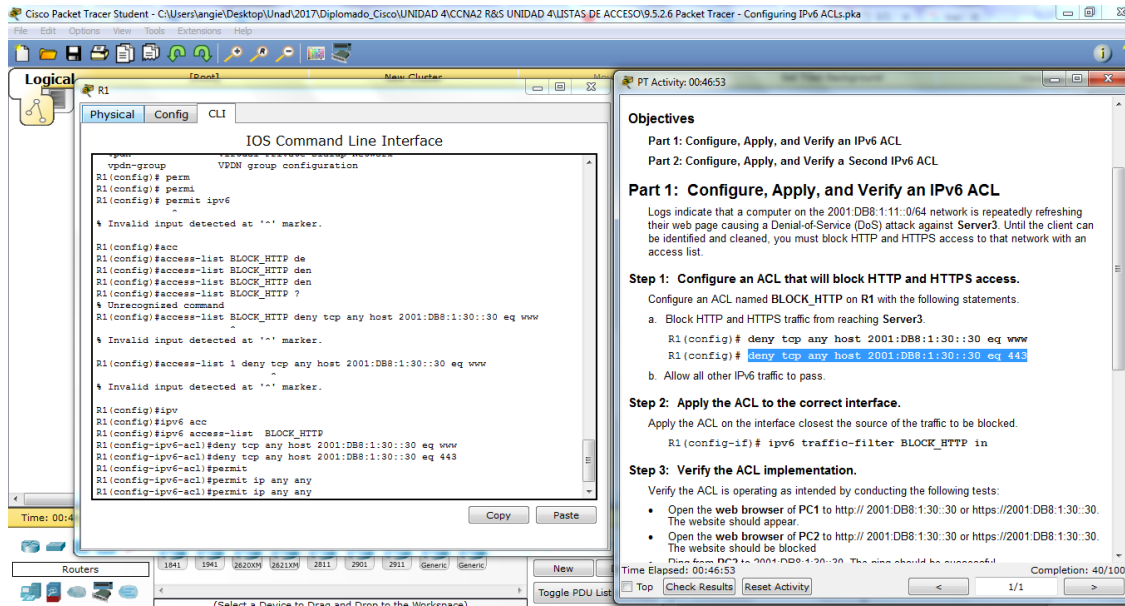
Configure an ACL named BLOCK\_HTTP on R1 with the following statements.

Block HTTP and HTTPS traffic from reaching Server3.

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

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

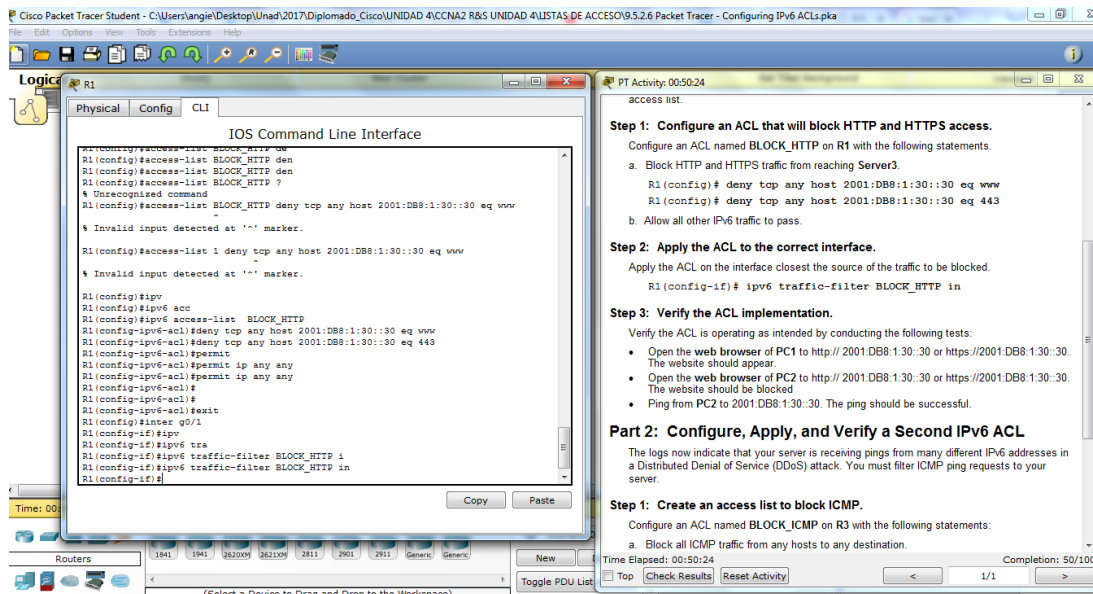
a. Allow all other IPv6 traffic to pass.



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

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

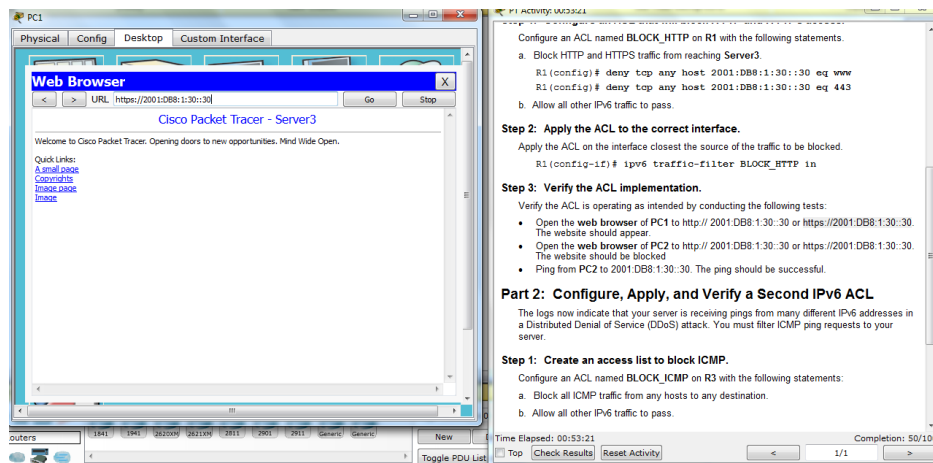
R1(config-if)# ipv6 traffic-filter BLOCK\_HTTP in



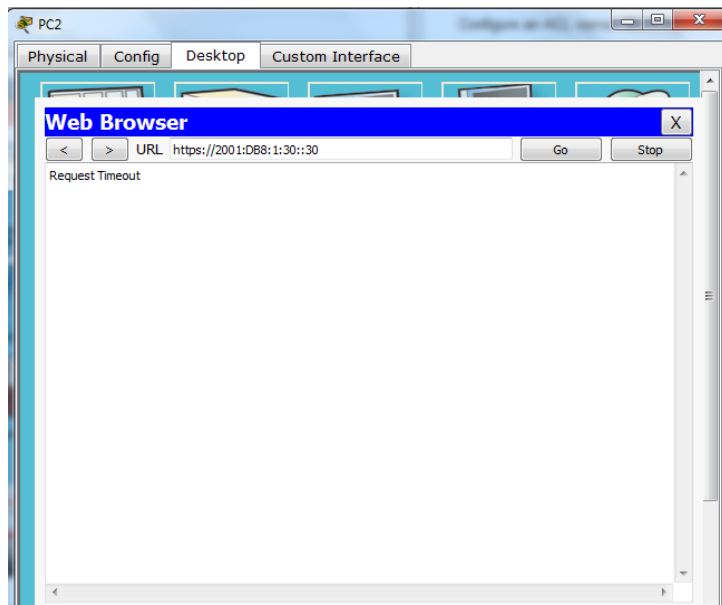
**Step 3: Verify the ACL implementation.**

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

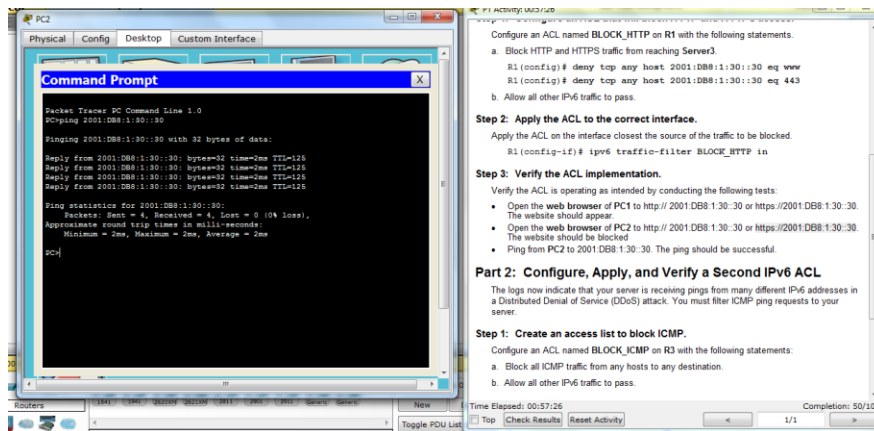
- Open the web browser of PC1 to <http://2001:DB8:1:30::30> or <https://2001:DB8:1:30::30>. The website should appear.



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



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



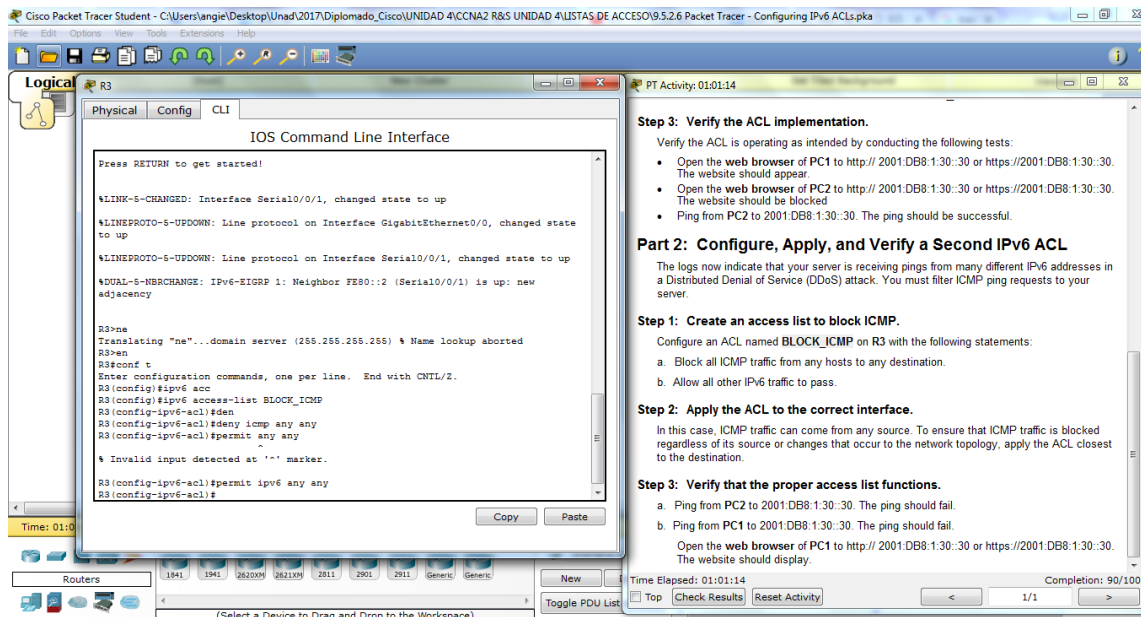
### Part 2: Configure, Apply, and Verify a Second IPv6 ACL

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

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

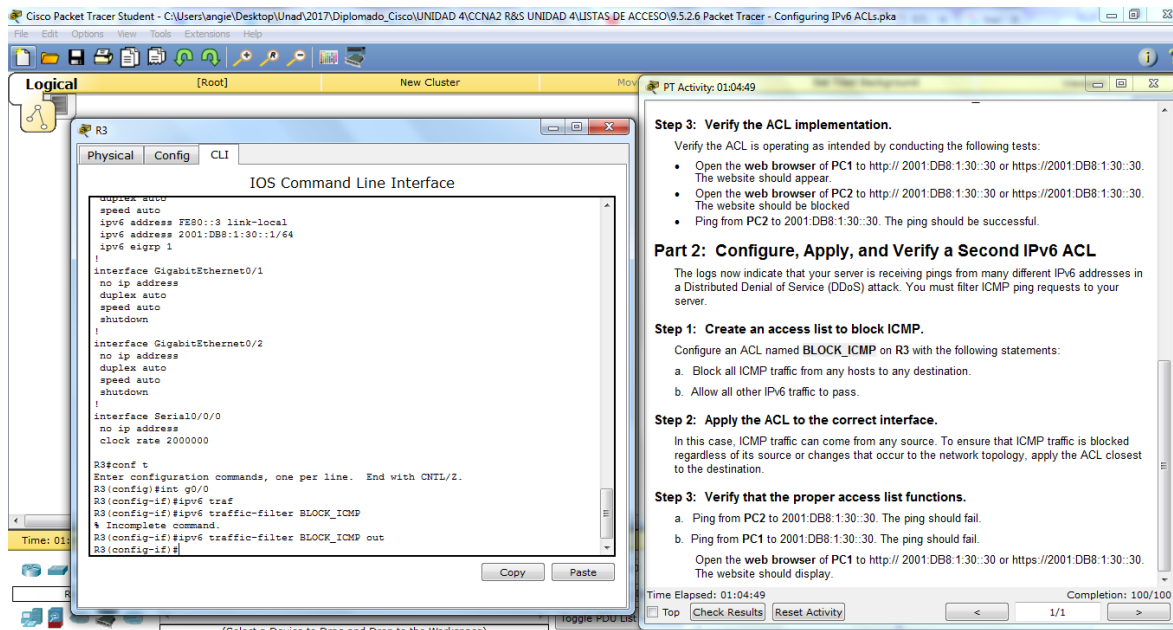
Configure an ACL named BLOCK\_ICMP on R3 with the following statements:

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



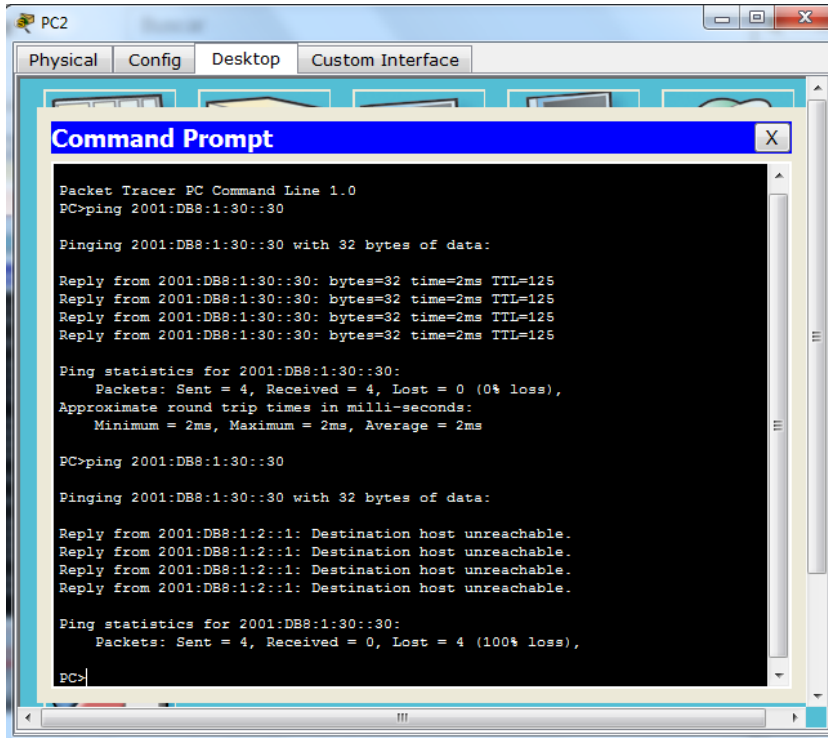
**Step 2: Apply the ACL to the correct interface.**

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



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

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



```
Packet Tracer PC Command Line 1.0
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>ping 2001:DB8:1:2::1

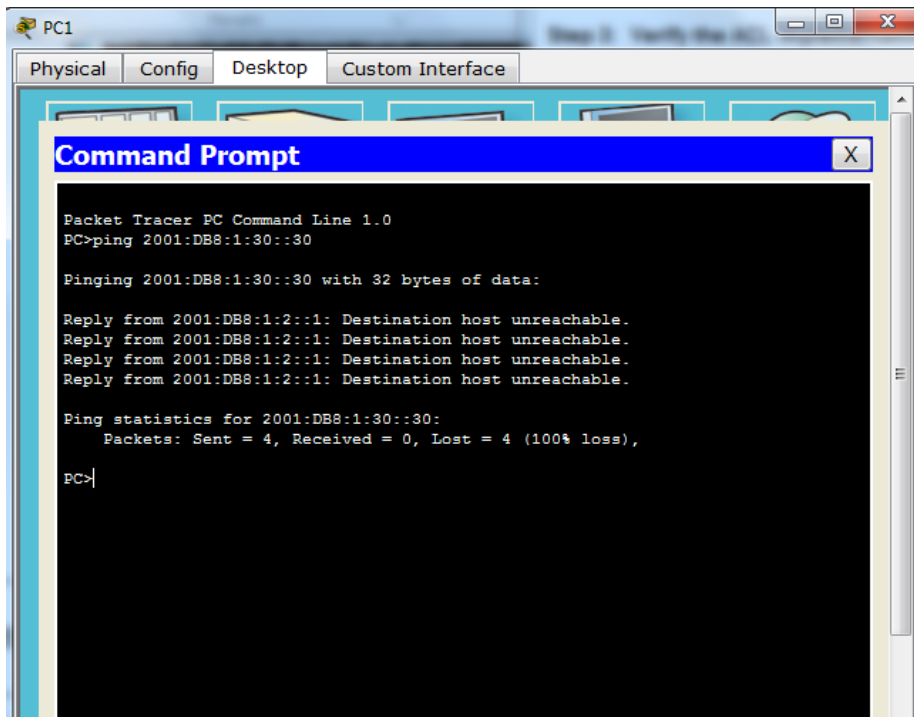
Pinging 2001:DB8:1:2::1 with 32 bytes of data:

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



```
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:1:30::30

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

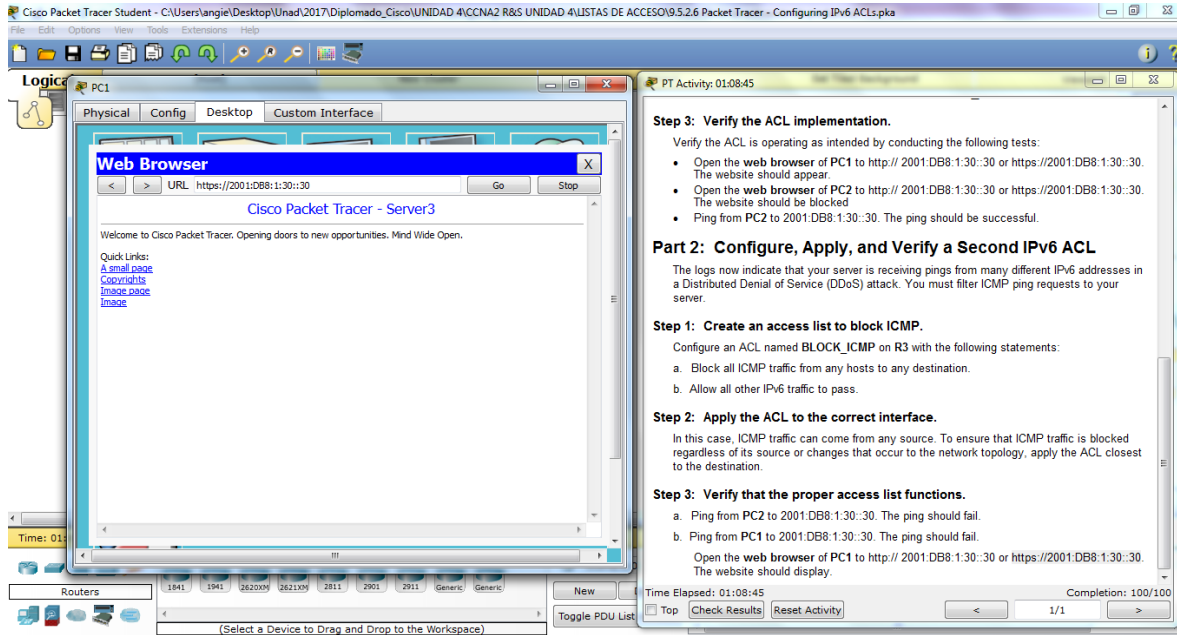
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

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

PC>
```



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



11.2.3.7 Lab - Configuring NAT Pool Overload and PAT

Topología

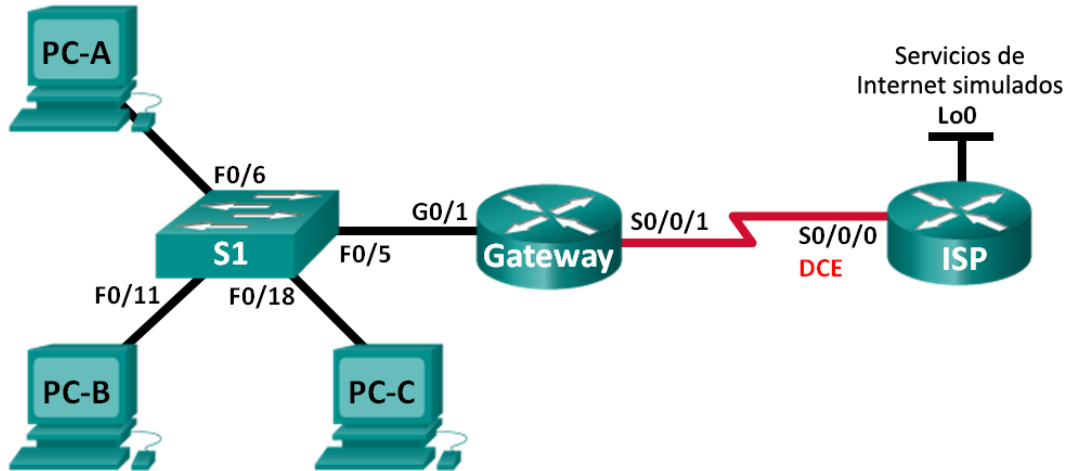


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar un conjunto de NAT con sobrecarga

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones

a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

En la parte 2, el ISP asignó una única dirección IP, 209.165.201.18, a su empresa para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Usará la traducción de la dirección del puerto (PAT) para convertir varias direcciones internas en la única dirección pública utilizable. Se probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

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

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

### **Recursos necesarios**

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

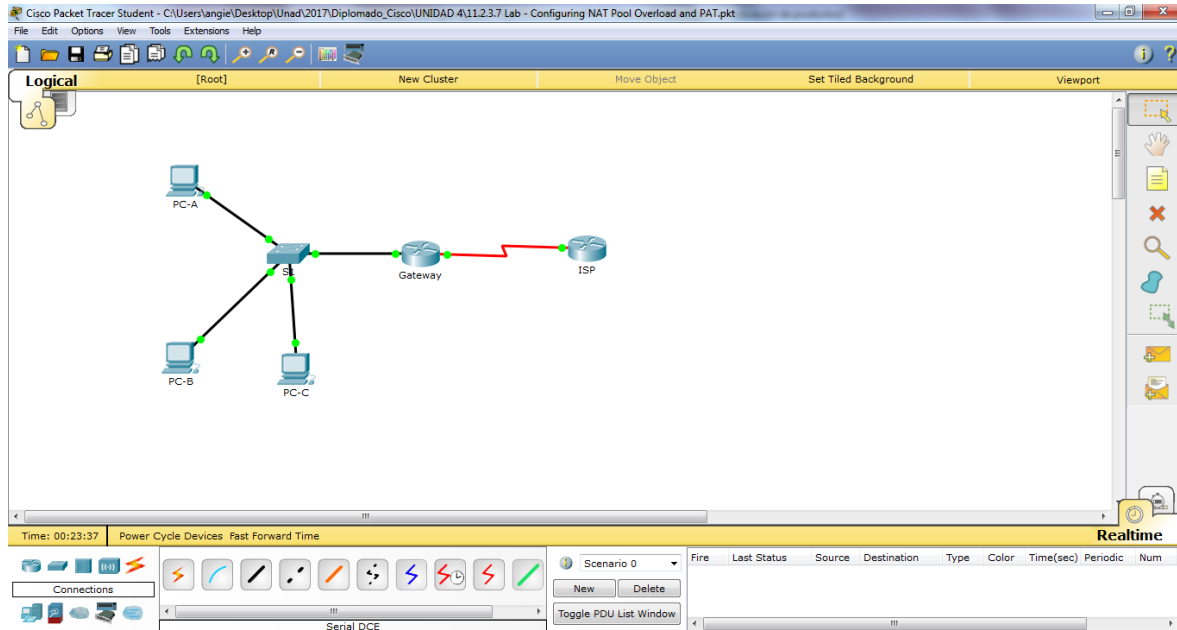
### **Parte 1: armar la red y verificar la conectividad**

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

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

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

**Paso 3:** inicializar y volver a cargar los routers y los switches.



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

- a. Desactive la búsqueda del DNS.
- b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- c. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.
- d. Configure el nombre del dispositivo como se muestra en la topología.
- e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

**Paso 5:** configurar el routing estático.

- a. Cree una ruta estática desde el router ISP hasta el router Gateway.

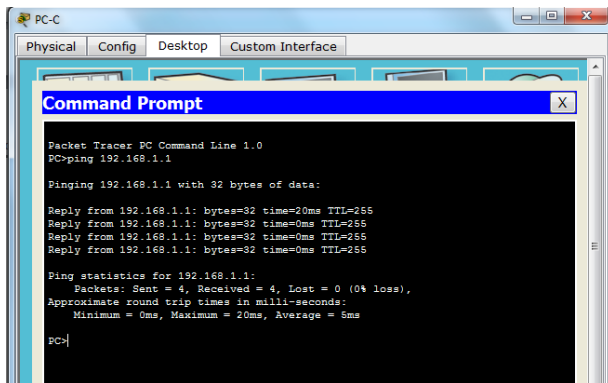
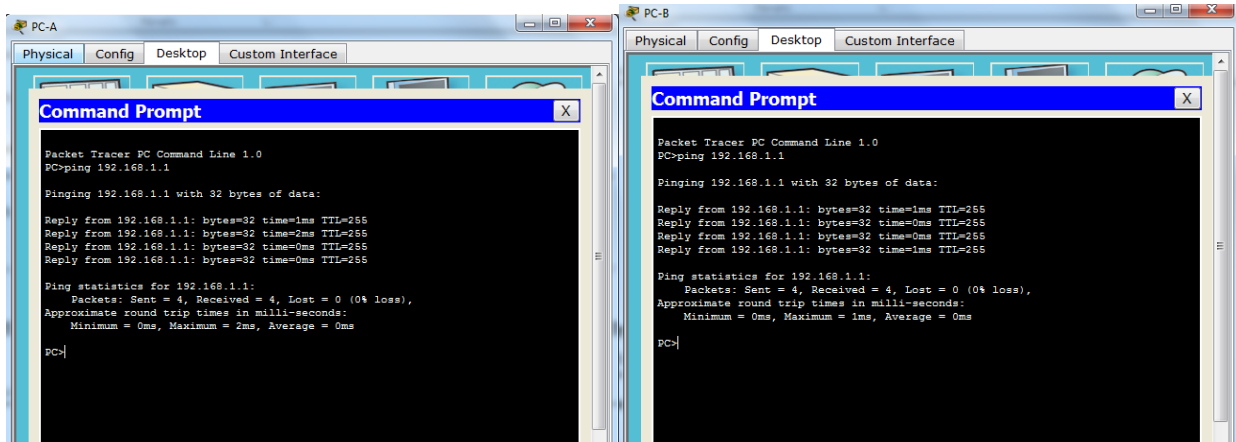
```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

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

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

**Paso 6: Verificar la conectividad de la red**

- a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.
- b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.



**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**

**Paso 2: definir el conjunto de direcciones IP públicas utilizables.**

Gateway(config)# **ip nat pool public\_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

**Paso 3:** definir la NAT desde la lista de origen interna hasta el conjunto externo.

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

**Paso 4:** Especifique las interfaces.

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

```
Gateway(config)# interface g0/1
```

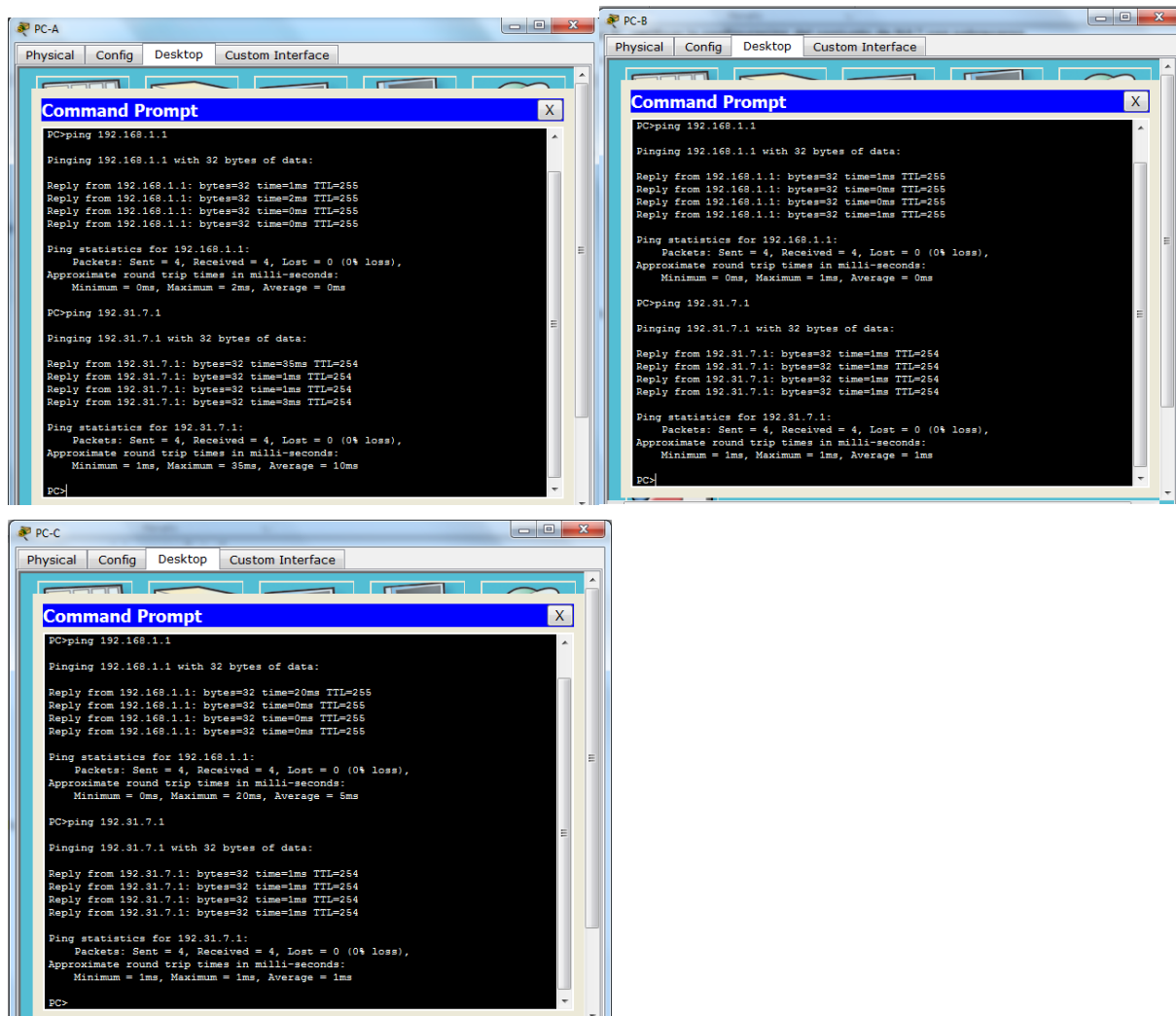
```
Gateway(config-if)# ip nat inside
```

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

```
Gateway(config-if)# ip nat outside
```

**Paso 5:** verificar la configuración del conjunto de NAT con sobrecarga.

a. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.



b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# show ip nat statistics

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:25 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public\_access refcount 3

pool public\_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

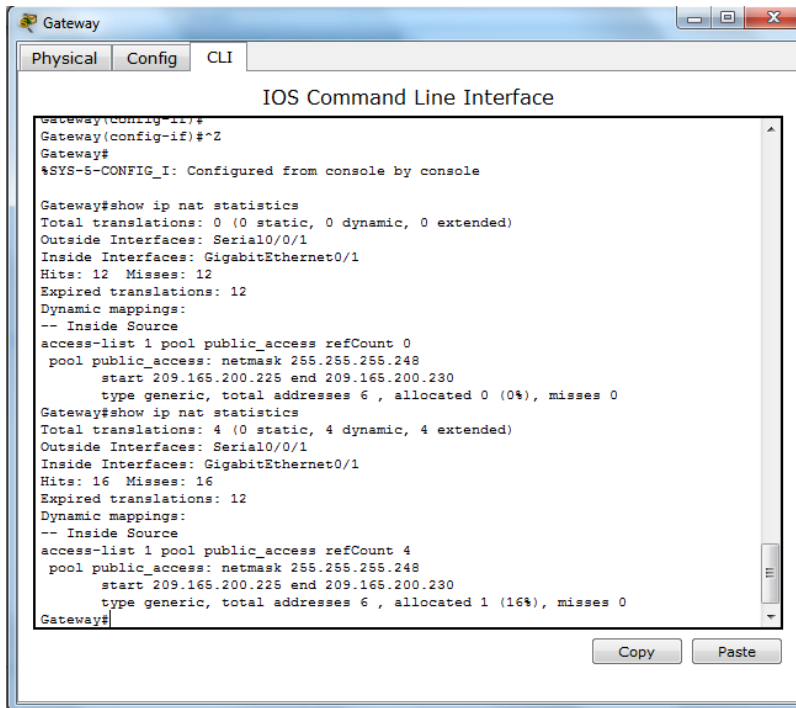
type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

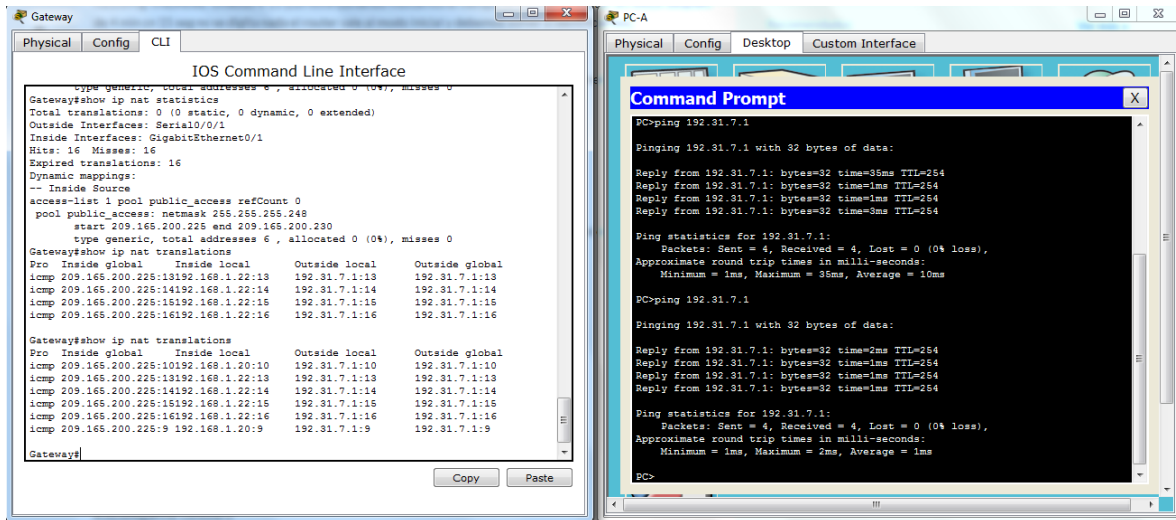
Queued Packets: 0



c. Muestre las NAT en el router Gateway.

Gateway# show ip nat translations

```
Pro Inside global   Inside local   Outside local   Outside global
icmp 209.165.200.225:0 192.168.1.20:1 192.31.7.1:1 192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1 192.31.7.1:1 192.31.7.1:2
```



**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?   6  

¿Cuántas direcciones IP globales internas se indican?   6  

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas?   1  

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

**No se tiene respuesta a ping ya que no se realizó configuración de ruta estática en el router 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.**

**Paso 2: verificar la configuración para NAT.**

- Verifique que se hayan borrado las estadísticas.
- Verifique que las interfaces externa e interna estén configuradas para NAT.
- Verifique que la ACL aún esté configurada para NAT.

¿Qué comando usó para confirmar los resultados de los pasos a al c?



Show ip nat translations, show ip nat statistics

**Paso 3:** eliminar el conjunto de direcciones IP públicas utilizables.

Gateway(config)# no ip nat pool public\_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248

**Paso 4:** eliminar la traducción NAT de la lista de origen interna al conjunto externo.

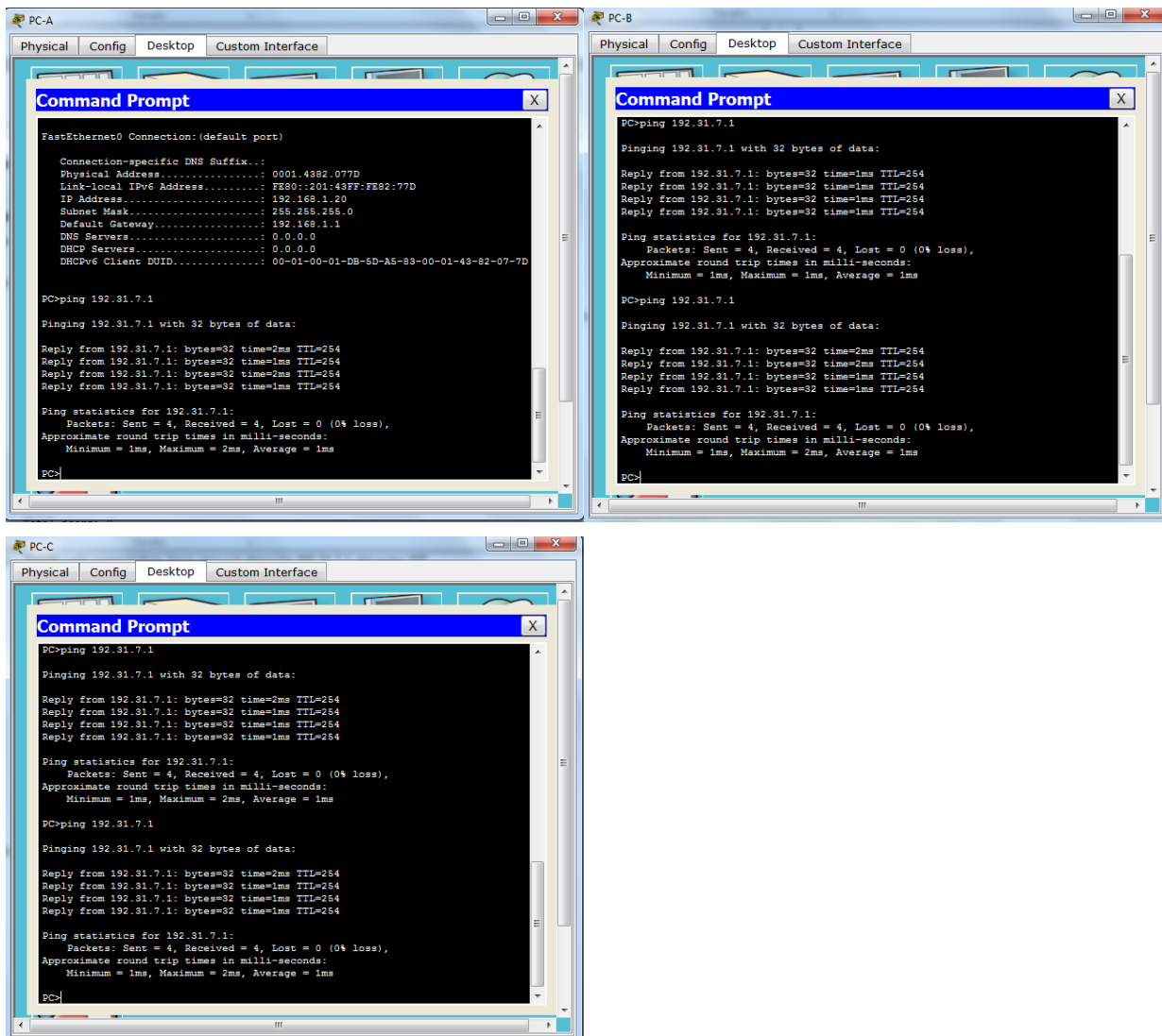
Gateway(config)# no ip nat inside source list 1 pool public\_access overload

**Paso 5:** asociar la lista de origen a la interfaz externa.

Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload

**Paso 6:** probar la configuración PAT.

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.



b. Muestre las estadísticas de NAT en el router Gateway.

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

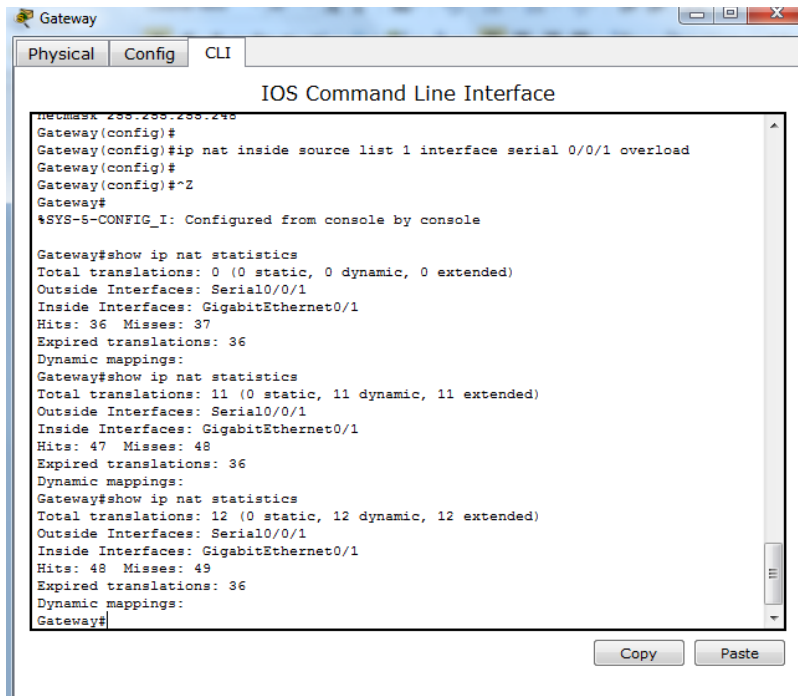
**[Id: 2] access-list 1 interface Serial0/0/1 refcount 3**

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0



```

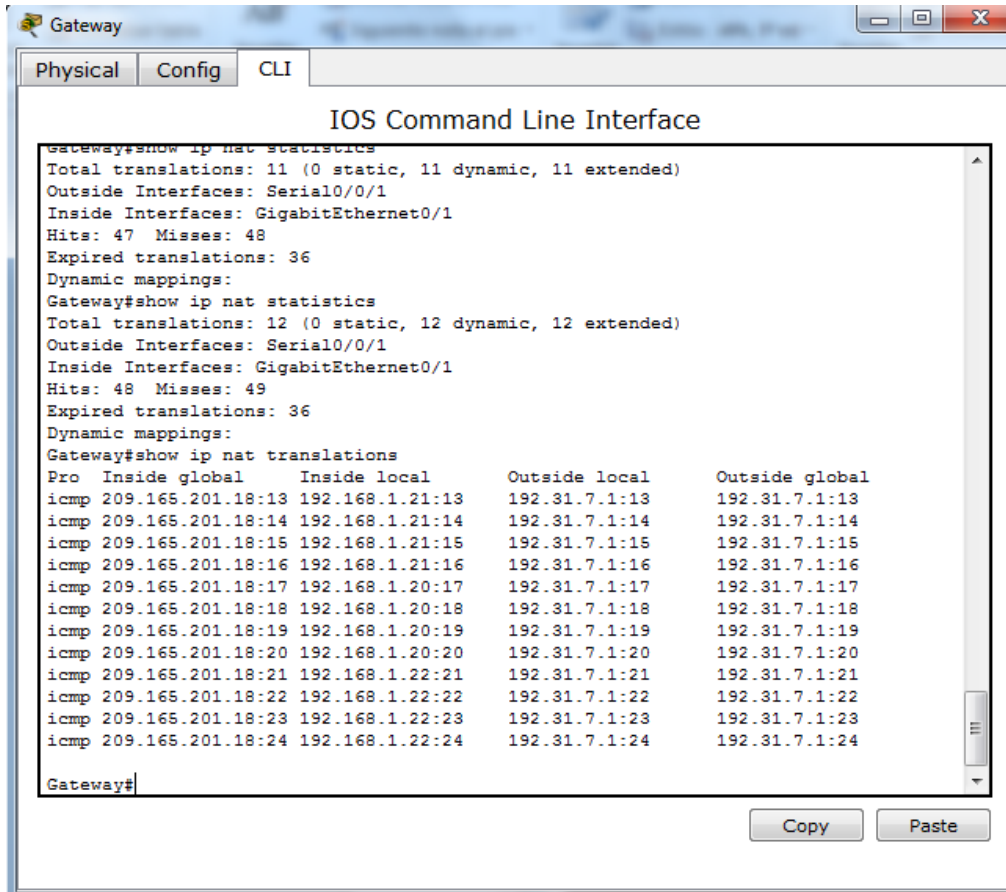
Gateway
Physical Config CLI
IOS Command Line Interface
RUCMASX 288.288.288.248
Gateway(config)#
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 overload
Gateway(config)#
Gateway(config)#^Z
Gateway#
#SYS-5-CONFIG_I: Configured from console by console

Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 36 Misses: 37
Expired translations: 36
Dynamic mappings:
Gateway#show ip nat statistics
Total translations: 11 (0 static, 11 dynamic, 11 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 47 Misses: 48
Expired translations: 36
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: 48 Misses: 49
Expired translations: 36
Dynamic mappings:
Gateway#
Copy Paste
  
```

c. Muestre las traducciones NAT en el Gateway.

Gateway# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.18:3	192.168.1.20:1	192.31.7.1:1	192.31.7.1:3
icmp	209.165.201.18:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.201.18:4	192.168.1.22:1	192.31.7.1:1	192.31.7.1:4



## Reflexión

¿Qué ventajas tiene la PAT?

Mapea varias direcciones IP privadas a una sola dirección IP pública, utiliza números únicos de puerto origen en la dirección IP global interna para distinguir entre las traducciones

10.2.3.5 configuración de DHCPv6 sin estado y con estado

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1	64	No aplicable
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

Objetivos

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

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Solo mediante configuración automática de dirección sin estado (SLAAC)
- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
- Mediante DHCPv6 con estado

Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

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

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

**Nota:** la plantilla **default bias** que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla **dual-ipv4-and-ipv6** o la plantilla **lanbase-routing** en SDM. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

#### S1# show sdm prefer

Siga estos pasos para asignar la plantilla **dual-ipv4-and-ipv6** como la plantilla de SDM predeterminada:

```
S1# config t
```

```
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
```

```
S1(config)# end
```

```
S1# reload
```

#### Recursos necesarios

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

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

#### Parte 4: armar la red y configurar los parámetros básicos de los dispositivos

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

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

**Paso 2:** inicializar y volver a cargar el router y el switch según sea necesario.

**Paso 3: Configurar R1**

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Guardar la configuración en ejecución en la configuración de inicio.

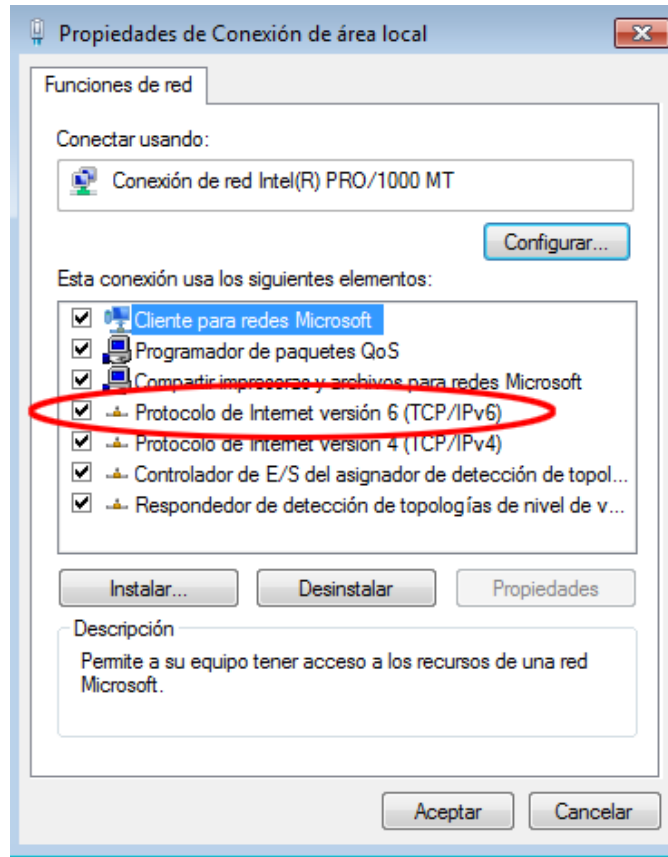
**Paso 4: configurar el S1.**

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Desactive administrativamente todas las interfaces inactivas.
- i. Guarde la configuración en ejecución en la configuración de inicio.

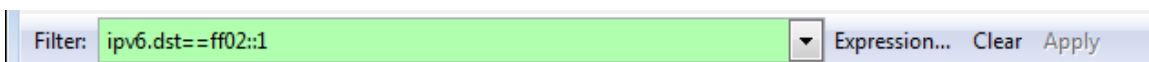
**Parte 5: configurar la red para SLAAC**

**Paso 1: preparar la PC-A.**

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

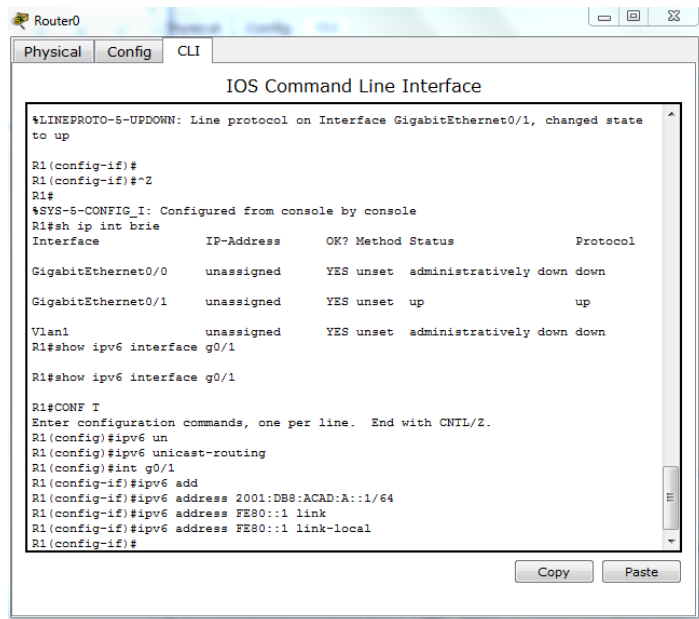


- b. Inicie una captura del tráfico en la NIC con Wireshark.
- c. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes. La entrada de filtro que se usa con Wireshark es **ipv6.dst==ff02::1**, como se muestra aquí.



### Paso 2: Configurar R1

- a. Habilite el routing de unidifusión IPv6.
- b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.
- c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.
- d. Active la interfaz G0/1.



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

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

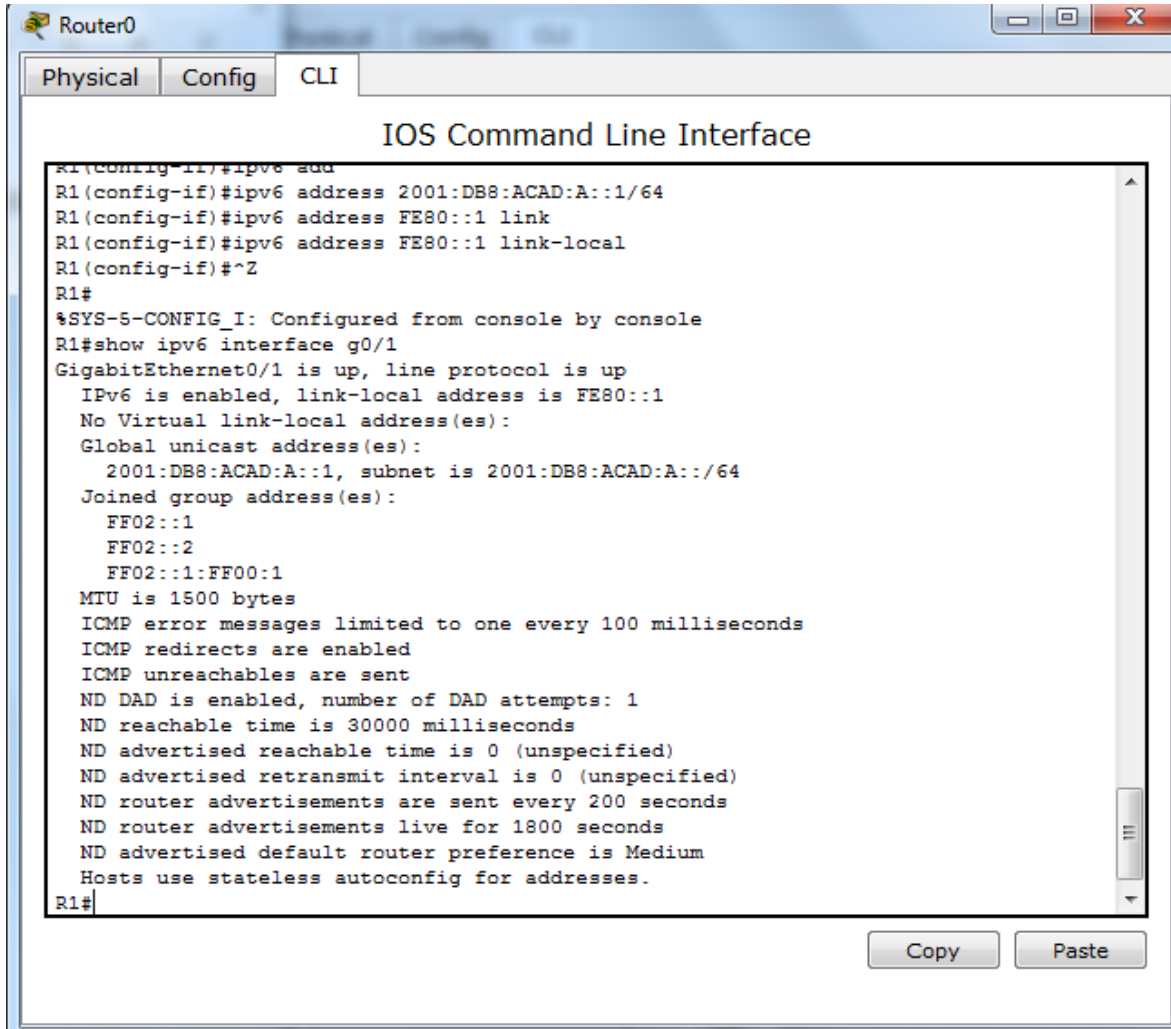
**R1# show ipv6 interface g0/1**

```

GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP 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.



**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

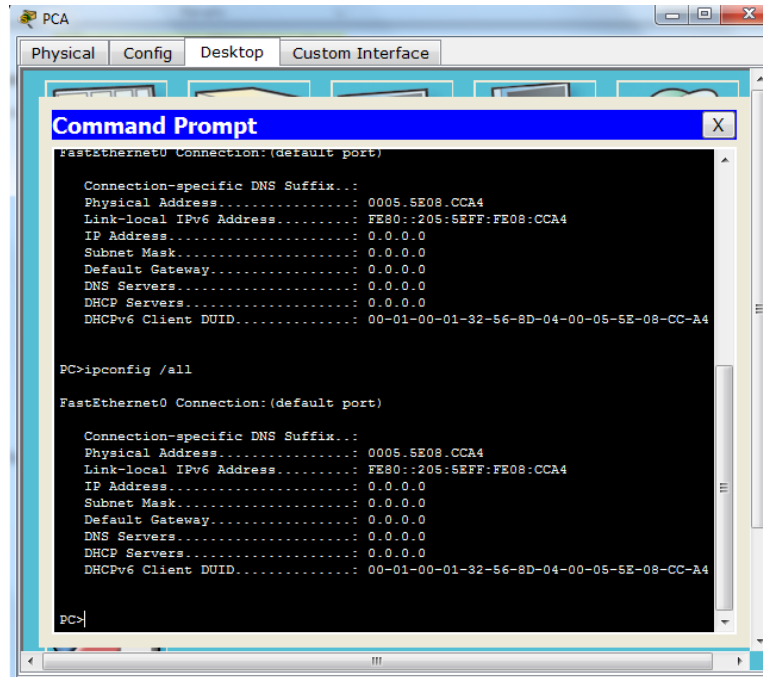
Default router is FE80::1 on Vlan1

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

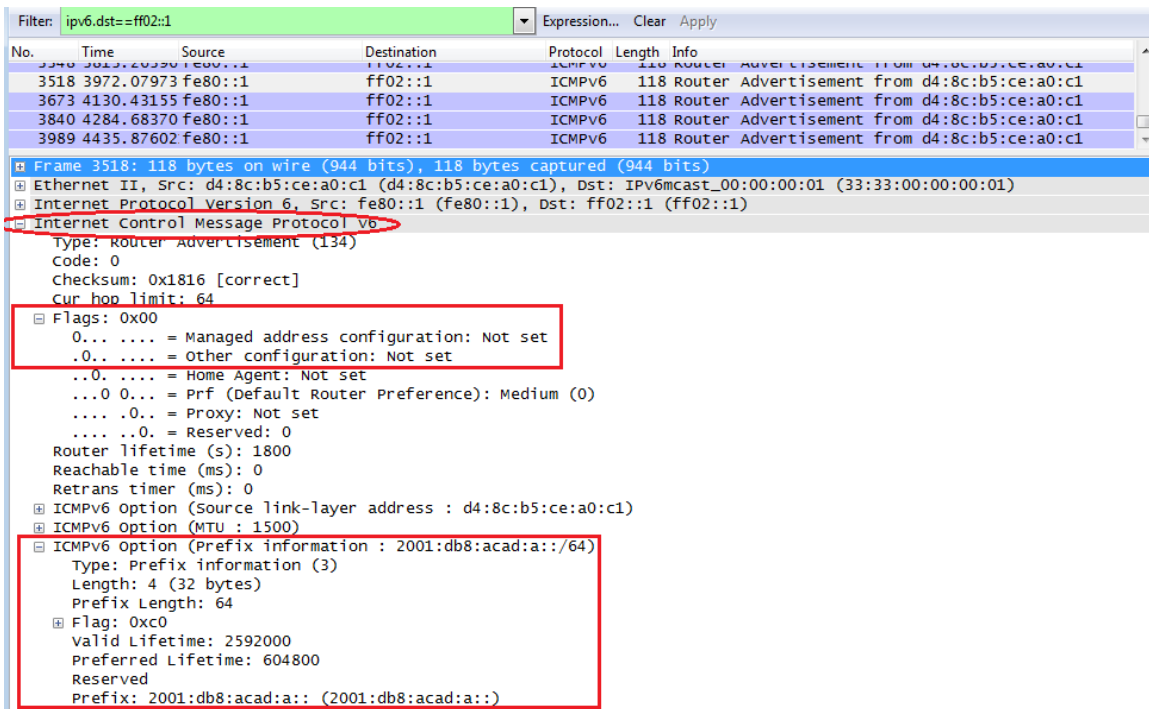
- a. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all**. Verifique que la PC-A muestre una dirección IPv6 con el prefijo 2001:db8:acad:a::/64. El gateway predeterminado debe tener la dirección FE80::1.

```

Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . :
    Descripción . . . . . : Conexión de red Intel(R) PRO/1000
    MTU
    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 6: configurar la red para DHCPv6 sin estado**

**Paso 1: configurar un servidor de DHCP IPv6 en el R1.**

a. Cree un pool de DHCP IPv6.

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

b. Asigne un nombre de dominio al pool.

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

c. Asigne una dirección de servidor DNS.

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

```
R1(config-dhcpv6)# exit
```

d. Asigne el pool de DHCPv6 a la interfaz.

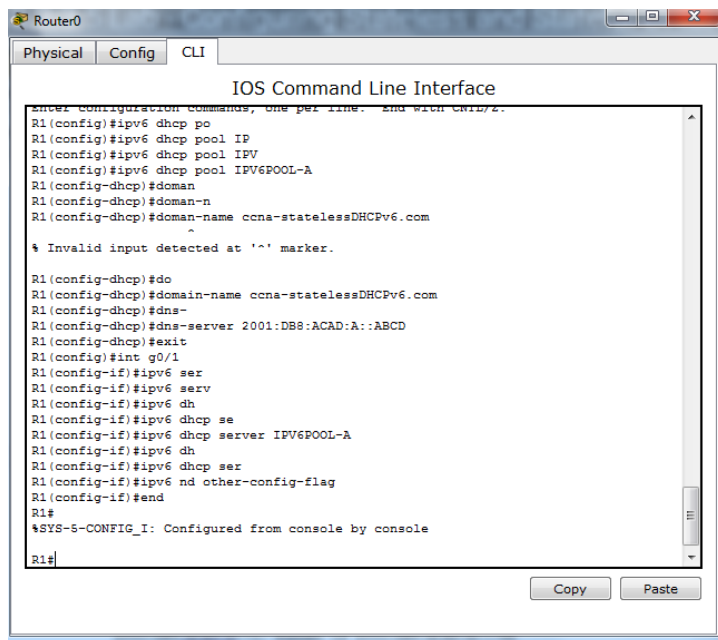
```
R1(config)# interface g0/1
```

```
R1(config-if)# ipv6 dhcp server IPV6POOL-A
```

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

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

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

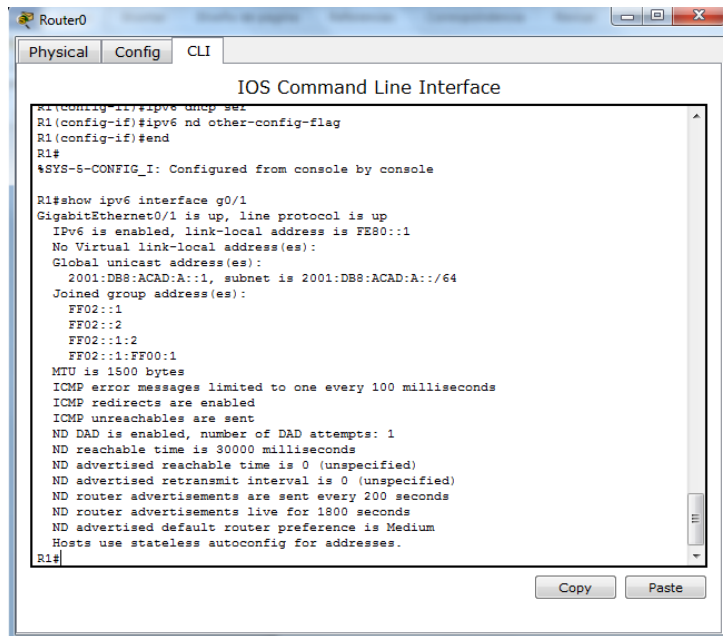


**Paso 2: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.**

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

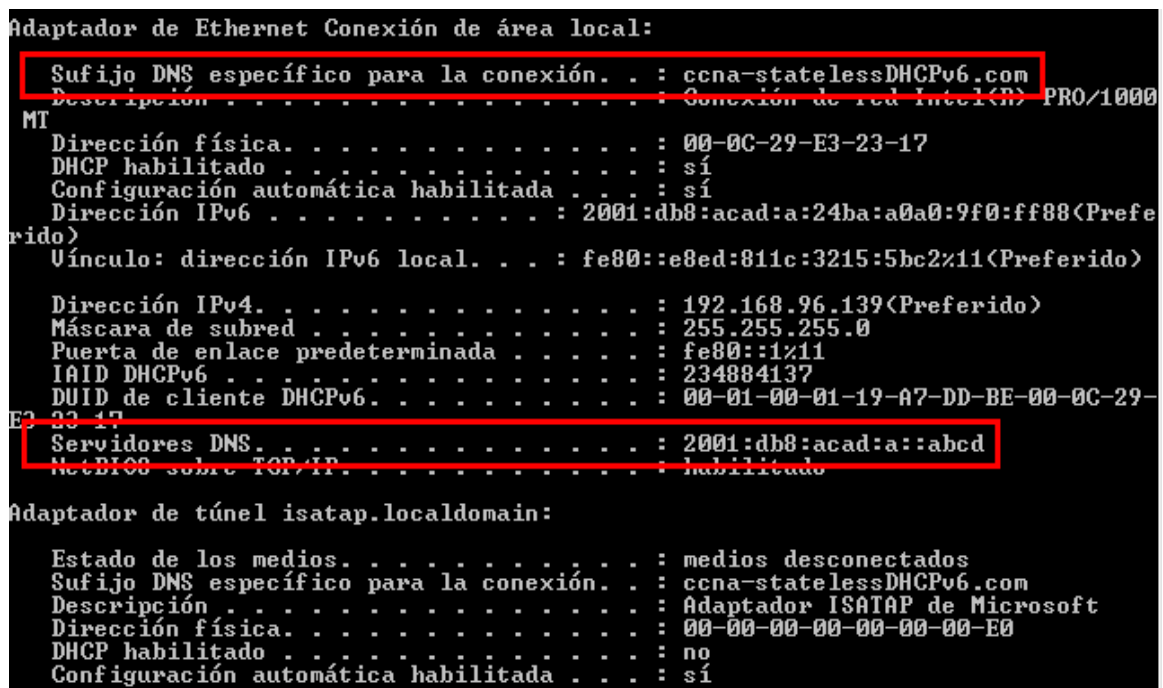
```
R1# show ipv6 interface g0/1
```

GigabitEthernet0/1 is up, line protocol is up  
IPv6 is enabled, link-local address is FE80::1  
No Virtual link-local address(es):  
Global unicast address(es):  
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64  
Joined group address(es):  
  FF02::1  
  FF02::2  
  FF02::1:2  
  FF02::1:FF00:1  
  FF05::1:3  
MTU is 1500 bytes  
ICMP error messages limited to one every 100 milliseconds  
ICMP redirects are enabled  
ICMP 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.



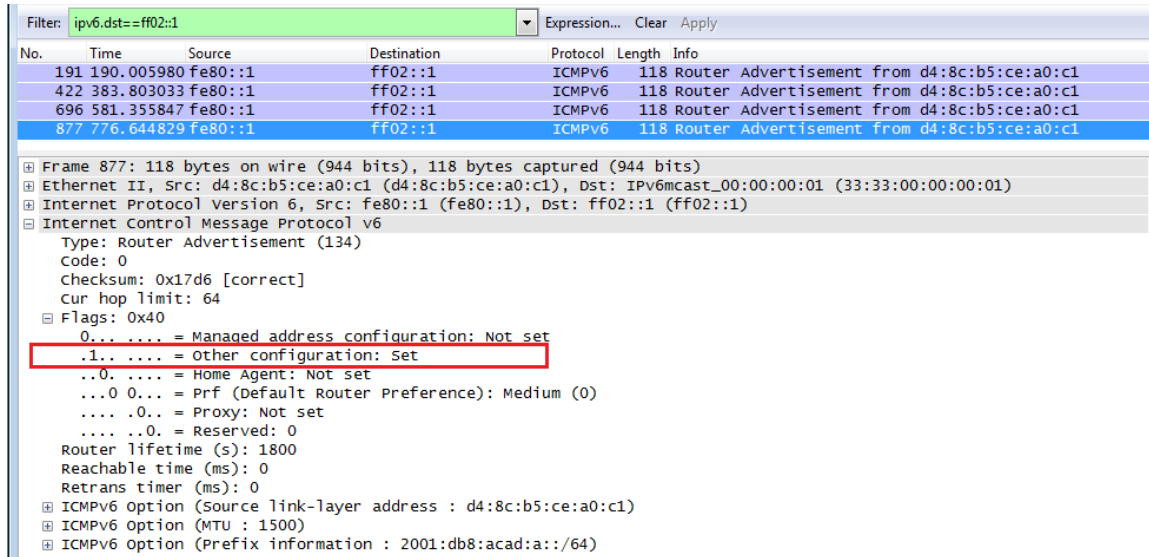
**Paso 3: ver los cambios realizados en la red en la PC-A.**

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.



**Paso 4: ver los mensajes RA en Wireshark.**

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



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

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

R1# `show ipv6 dhcp binding`

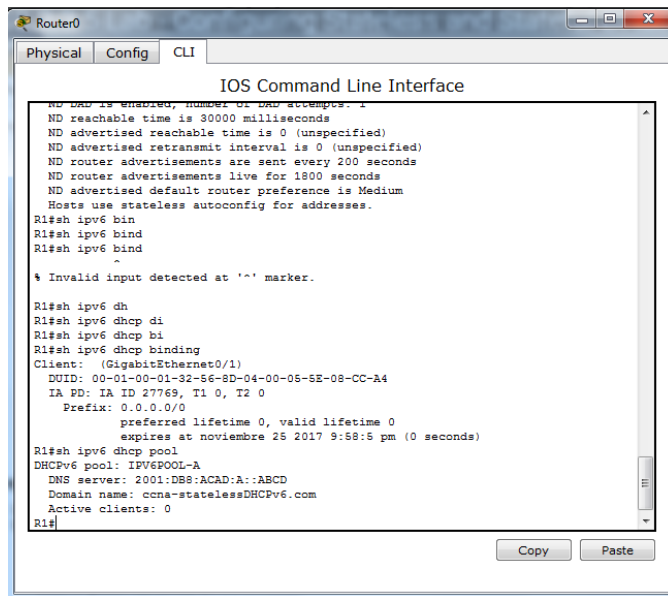
R1# `show ipv6 dhcp pool`

DHCPv6 pool: IPV6POOL-A

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-statelessDHCPv6.com

Active clients: 0



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

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

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

S1(config)# **interface f0/6**

S1(config-if)# **shutdown**

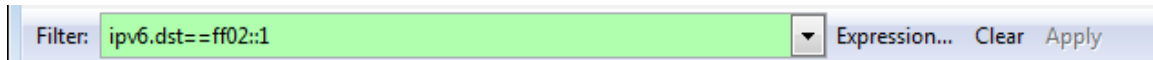
- b. Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.
- c. Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.
  - 1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.
  - 2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.



**Parte 7: configurar la red para DHCPv6 con estado**

**Paso 1: preparar la PC-A.**

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



**Paso 2: cambiar el pool de DHCPv6 en el R1.**

- a. Agregue el prefijo de red al pool.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```

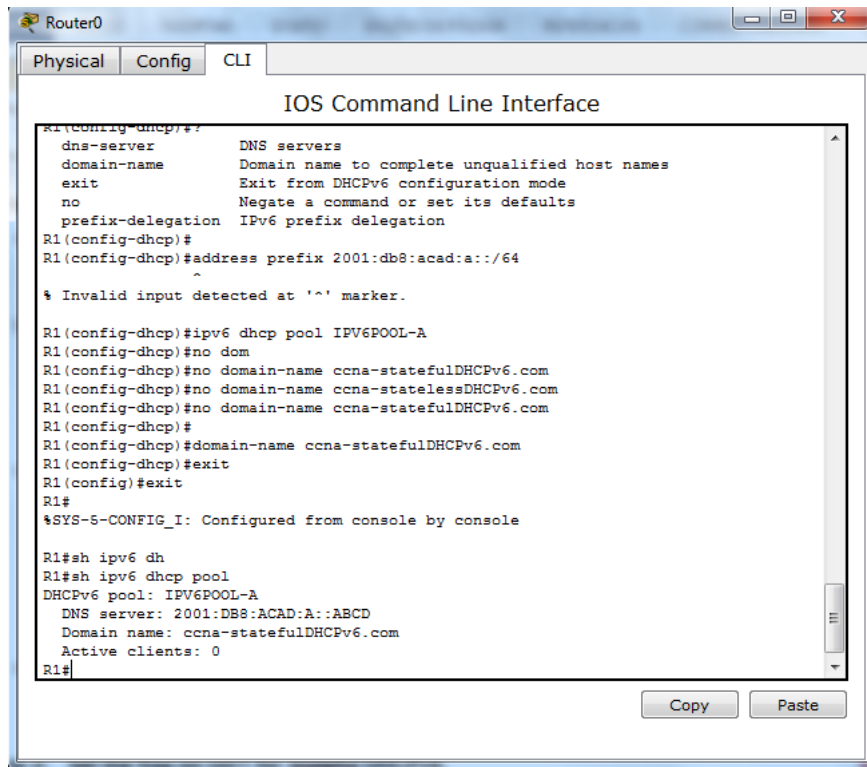
- b. Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.

**Nota:** debe eliminar el antiguo nombre de dominio. El comando **domain-name** no lo reemplaza.

```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)# end
```

- c. Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (0 in use, 0 conflicts)
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 0
```



```

Router0
Physical Config CLI
IOS Command Line Interface
R1(config-dhcp)#?
  dns-server          DNS servers
  domain-name        Domain name to complete unqualified host names
  exit               Exit from DHCPv6 configuration mode
  no                 Negate a command or set its defaults
  prefix-delegation  IPv6 prefix delegation
R1(config-dhcp)#
R1(config-dhcp)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.

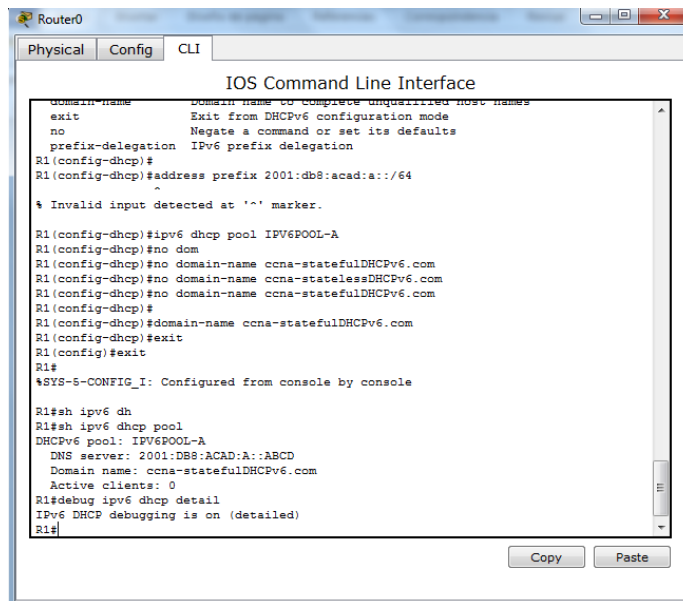
R1(config-dhcp)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#no dom
R1(config-dhcp)#no domain-name ccna-statefulDHCPv6.com
R1(config-dhcp)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#no domain-name ccna-statefulDHCPv6.com
R1(config-dhcp)#
R1(config-dhcp)#domain-name ccna-statefulDHCPv6.com
R1(config-dhcp)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#sh ipv6 dh
R1#sh 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)



```

Router0
Physical Config CLI
IOS Command Line Interface
  domain-name        Domain name to complete unqualified host names
  exit               Exit from DHCPv6 configuration mode
  no                 Negate a command or set its defaults
  prefix-delegation  IPv6 prefix delegation
R1(config-dhcp)#
R1(config-dhcp)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.

R1(config-dhcp)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#no dom
R1(config-dhcp)#no domain-name ccna-statefulDHCPv6.com
R1(config-dhcp)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#no domain-name ccna-statefulDHCPv6.com
R1(config-dhcp)#
R1(config-dhcp)#domain-name ccna-statefulDHCPv6.com
R1(config-dhcp)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#sh ipv6 dh
R1#sh 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
```

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 4: verificar la configuración de DHCPv6 con estado en el R1.**

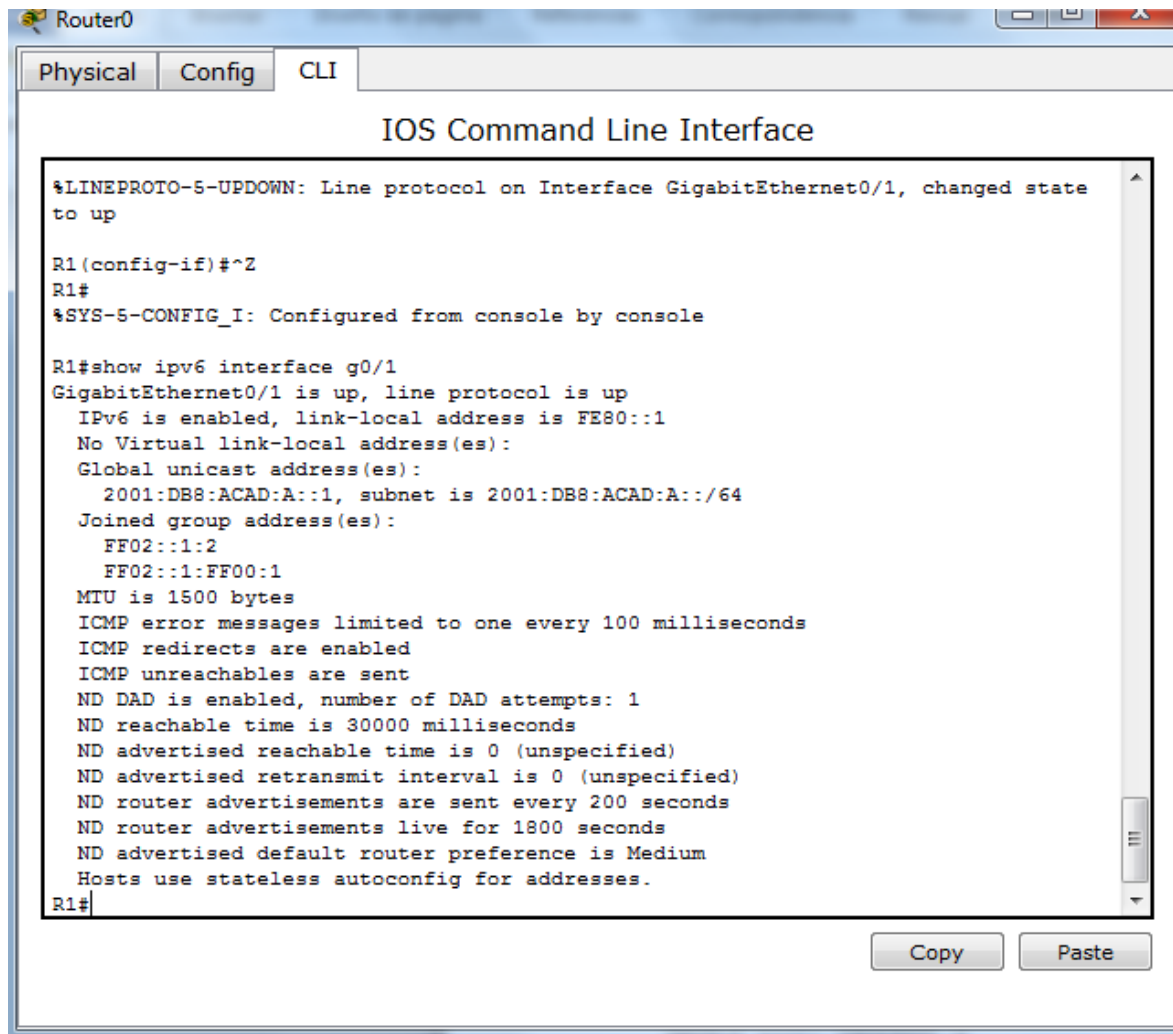
a. Emita el comando **show ipv6 interface g0/1** para verificar que la interfaz esté en el modo DHCPv6 con estado.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF02::1:FF00:1
  FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
```

ND advertised retransmit interval is 0 (unspecified)  
 ND router advertisements are sent every 200 seconds  
 ND router advertisements live for 1800 seconds  
 ND advertised default router preference is Medium

**Hosts use DHCP to obtain routable addresses.**

Hosts use DHCP to obtain other configuration.



b. En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.

c. Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

**R1# show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (1 in use, 0 conflicts)

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-StatefulDHCPv6.com

Active clients: 1

d. Emita el comando **show ipv6 dhcp binding** para verificar que la PC-A haya recibido su dirección IPv6 de unidifusión del pool de DHCP. Compare la dirección de cliente con la dirección IPv6 link-local en la PC-A mediante el comando **ipconfig /all**. Compare la dirección proporcionada por el comando **show** con la dirección IPv6 que se indica con el comando **ipconfig /all** en la PC-A.

R1# **show ipv6 dhcp binding**

**Client: FE80::D428:7DE2:997C:B05A**

DUID: 0001000117F6723D000C298D5444

Username : unassigned

IA NA: IA ID 0x0E000C29, T1 43200, T2 69120

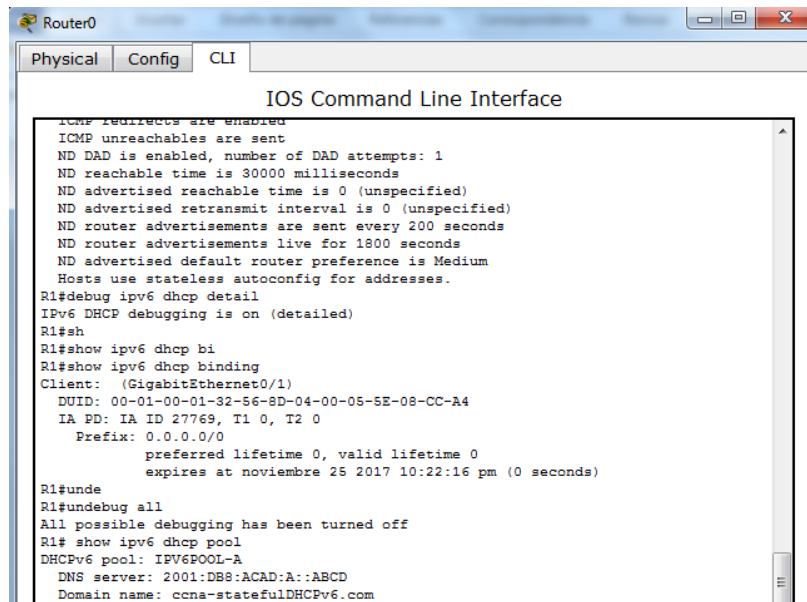
**Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE**

preferred lifetime 86400, valid lifetime 172800

expires at Mar 07 2013 04:09 PM (171595 seconds)

```

Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión. . . : ccna-StatefulDHCPv6.com
  Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
  Dirección física. . . . . : 00-0C-29-E3-23-17
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Dirección IPv6 . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce (Preferido)
  Concesión obtenida. . . . . : jueves, 05 de septiembre de 2013
16:07:59
  La concesión expira . . . . . : jueves, 05 de septiembre de 2013
16:38:03
  Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88 (Preferido)
  Vínculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a%11 (Preferido)
  Dirección IPv4. . . . . : 192.168.96.139 (Preferido)
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : fe80::1%11
  IAID DHCPv6 . . . . . : 234884137
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-
E3-23-17
  Servidores DNS. . . . . : 2001:db8:acad:a::abcd
  NetBIOS sobre TCP/IP. . . . . : habilitado
  
```



```

Router0
Physical Config CLI
IOS Command Line Interface
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R1#sh
R1#show ipv6 dhcp bi
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-32-56-8D-04-00-06-5E-08-CC-A4
IA PD: IA ID 27769, T1 0, T2 0
Prefix: 0.0.0.0/0
preferred lifetime 0, valid lifetime 0
expires at noviembre 25 2017 10:22:16 pm (0 seconds)
R1#unde
R1#undebug all
All possible debugging has been turned off
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statefulDHCPv6.com
  
```

e. Emita el comando **undebug all** en el R1 para detener la depuración de DHCPv6.

**Nota:** escribir **u all** es la forma más abreviada de este comando y sirve para saber si quiere evitar que los mensajes de depuración se desplacen hacia abajo constantemente en la pantalla de la sesión de terminal. Si hay varias depuraciones en proceso, el comando **undebug all** las detiene todas.

R1# **u all**

Se ha desactivado toda depuración posible

f. Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.

1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

\*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

\*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents

\*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

\*Mar 5 16:42:39.775: dst FF02::1:2

\*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238

\*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2

\*Mar 5 16:42:39.775: elapsed-time 6300

\*Mar 5 16:42:39.775: option CLIENTID(1), len 14

2) Examine el mensaje de respuesta enviado a la PC-A con la información de red DHCP.

\*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

\*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents

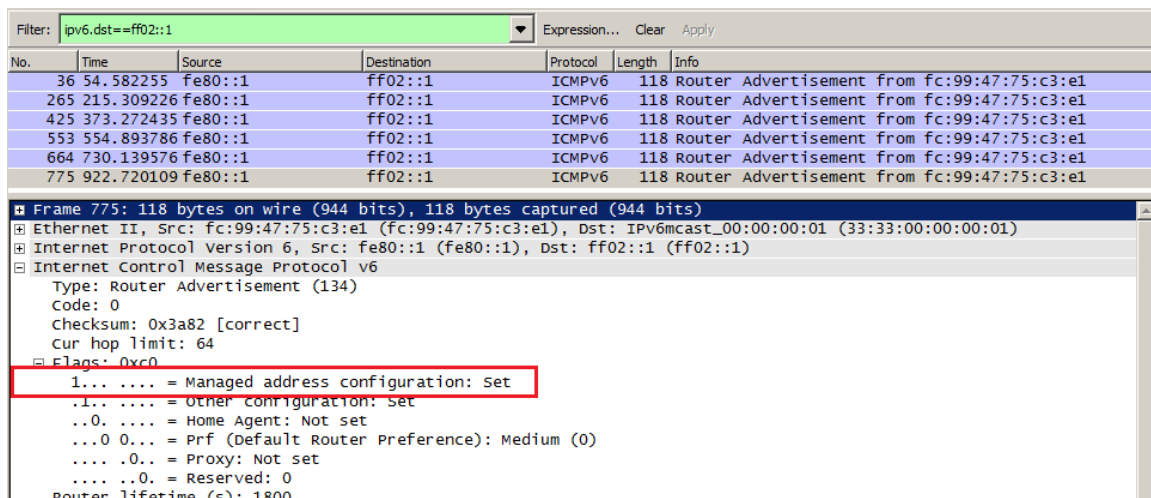
\*Mar 5 16:42:39.779: src FE80::1

\*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

```
*Mar 5 16:42:39.779: type REPLY(7), xid 1039238
*Mar 5 16:42:39.779: option SERVERID(2), len 10
*Mar 5 16:42:39.779: 00030001FC994775C3E0
*Mar 5 16:42:39.779: option CLIENTID(1), len 14
*Mar 5 16:42:39.779: 00010001
R1#17F6723D000C298D5444
*Mar 5 16:42:39.779: option IA-NA(3), len 40
*Mar 5 16:42:39.779: IAID 0xE000C29, T1 43200, T2 69120
*Mar 5 16:42:39.779: option IAADDR(5), len 24
*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar 5 16:42:39.779: preferred 86400, valid 172800
*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com
```

**Paso 5: verificar DHCPv6 con estado en la PC-A.**

- a. Detenga la captura de Wireshark en la PC-A.
- b. Expanda el mensaje RA más reciente que se indica en Wireshark. Verifique que se haya establecido el indicador **Managed address configuration** (Configuración de dirección administrada).



- c. Cambie el filtro en Wireshark para ver solo los paquetes **DHCPv6** escribiendo **dhcpv6** y, a continuación, haga clic en **Apply** (Aplicar). Resalte la última respuesta DHCPv6 de la lista y expanda la información de DHCPv6. Examine la información de red DHCPv6 incluida en este paquete.

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
<div style="border: 1px solid gray; padding: 5px;"> <div style="border: 1px solid gray; padding: 2px;">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)</div> <div style="border: 1px solid gray; padding: 2px;">Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)</div> <div style="border: 1px solid gray; padding: 2px;">User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)</div> <div style="border: 1px solid gray; padding: 2px;">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 style="border: 1px solid red; padding: 2px;">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 style="border: 1px solid red; padding: 2px;">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 style="border: 1px solid red; padding: 2px;">Domain: ccna-StatefulDHCPv6.com</li> </ul> </li> </ul> </li> </ul> </div> </div>						

### Reflexión

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

EL DHCPv6 utiliza más recursos de memoria. Los clientes con DHCPv6 sin estado no utilizan servidor DHCP para obtener información de dirección con esto no es necesario almacenar.

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

Cisco recomienda DHCPv6 sin estado para implementar redes IPv6.



**9.2.1.11 Packet Tracer - Configuring Named Standard ACLs**

**Addressing Table**

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

**Objectives**

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

**Part 2: Verify the ACL Implementation**

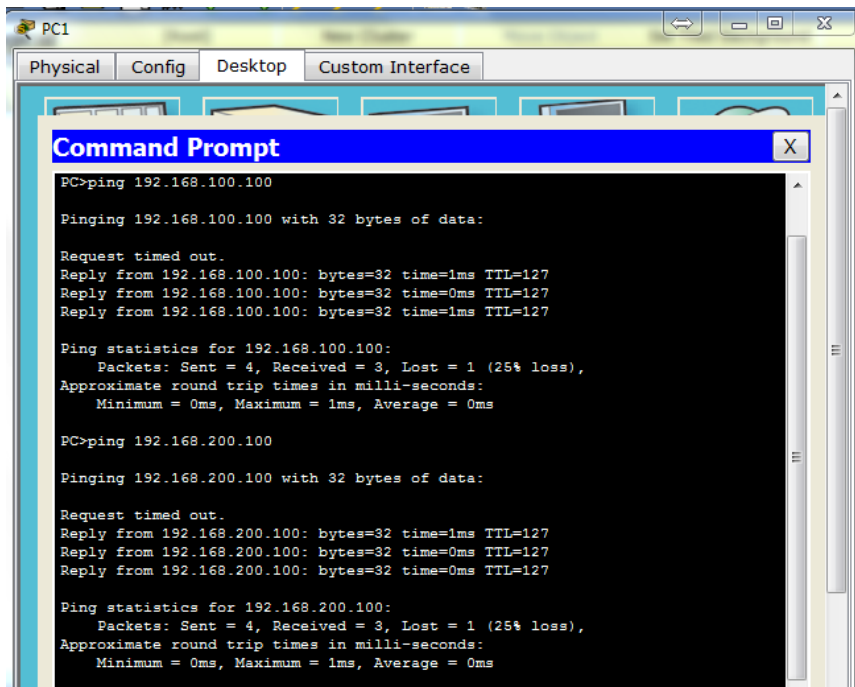
**Background / Scenario**

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

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

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

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



```
PC1
Physical Config Desktop Custom Interface
Command Prompt
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=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127

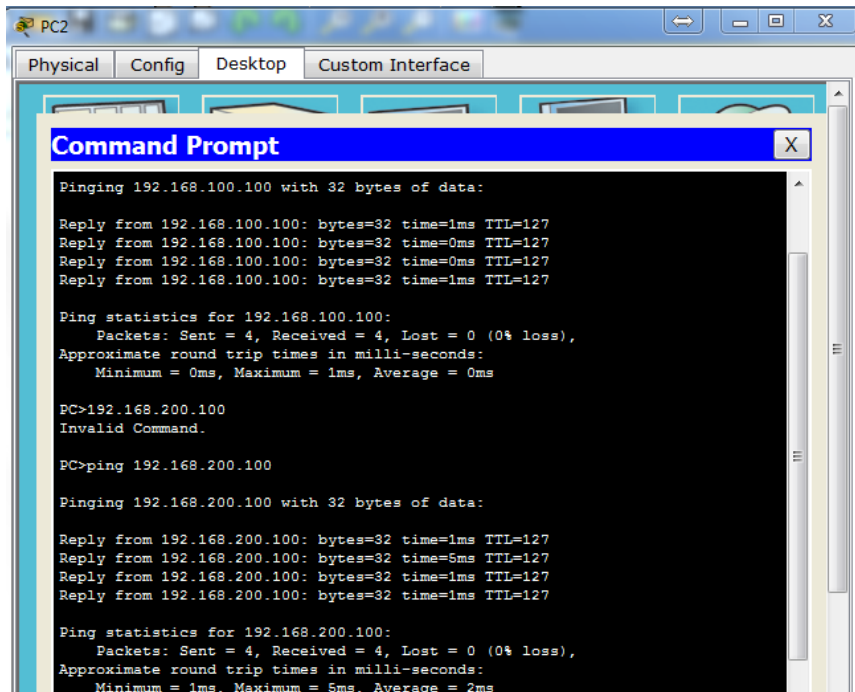
Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

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



```
PC2
Physical Config Desktop Custom Interface
Command Prompt

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127

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

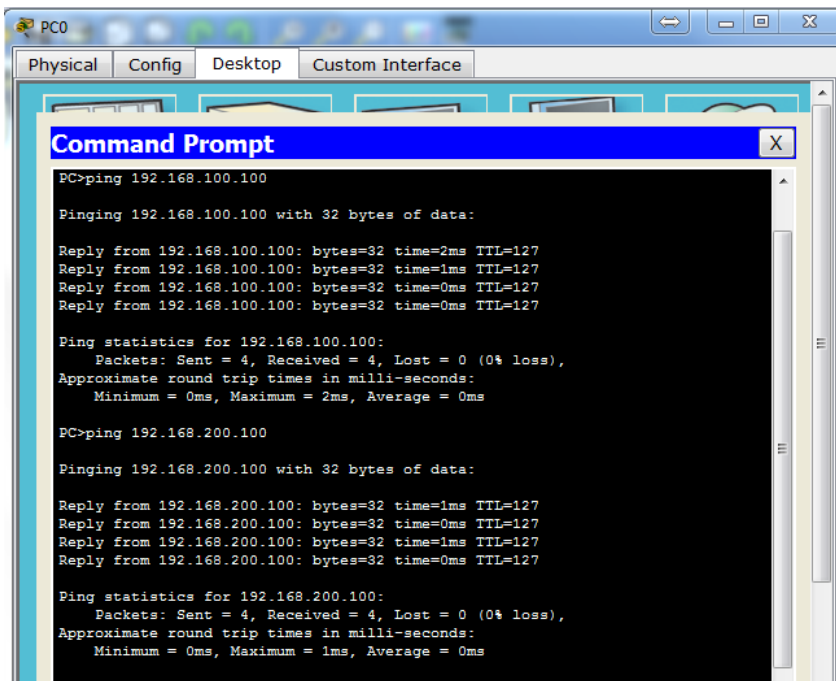
PC>192.168.200.100
Invalid Command.

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=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=5ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
```



```

PC0
Physical Config Desktop Custom Interface
Command Prompt
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=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms 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 = 2ms, Average = 0ms
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=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms 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 = 1ms, Average = 0ms
  
```

En este momento la hacer ping al servidor de archivos y al servidor web no existe conexión.

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

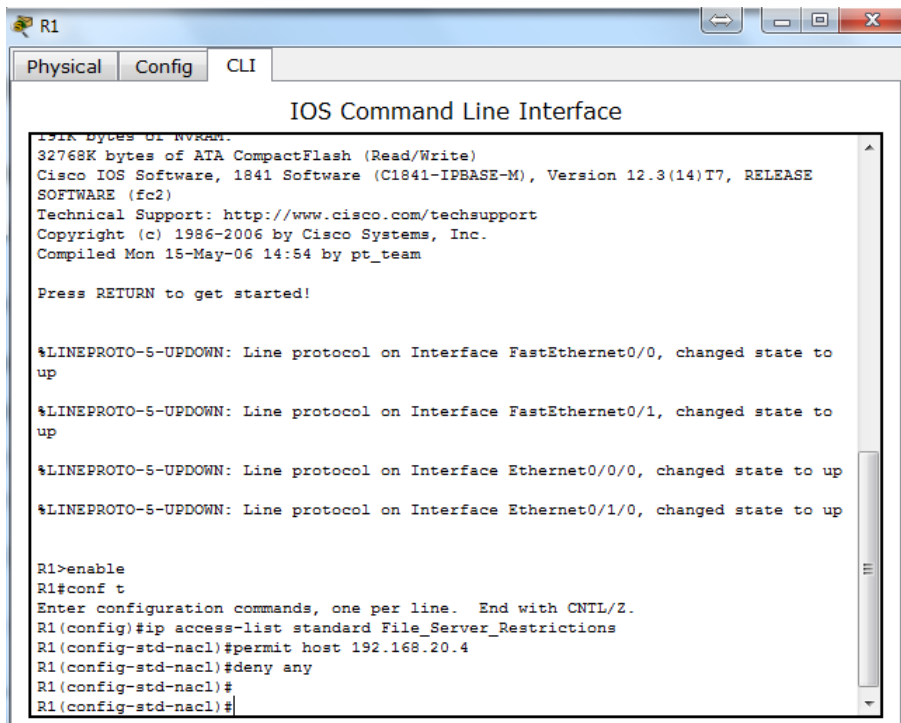
Configure the following named ACL on R1.

R1(config)# ip access-list standard File\_Server\_Restrictions

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

R1(config-std-nacl)# deny any

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



```

R1
Physical Config CLI
IOS Command Line Interface
32768K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1/0, changed state to up

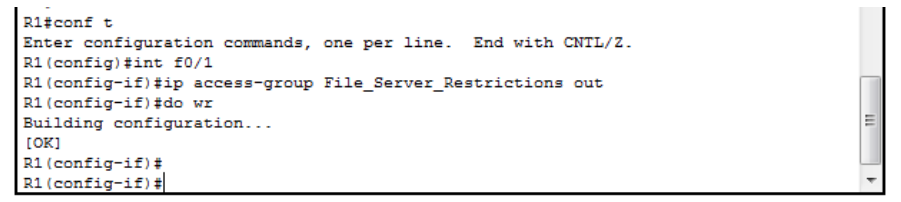
R1>enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#deny any
R1(config-std-nacl)#
R1(config-std-nacl)#
  
```

**Step 3: Apply the named ACL.**

- a. Apply the ACL outbound on the interface Fast Ethernet 0/1.

R1(config-if)# ip access-group File\_Server\_Restrictions out

- b. Save the configuration.



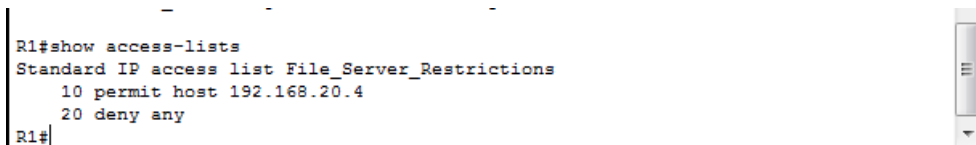
```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#do wr
Building configuration...
[OK]
R1(config-if)#
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#
  
```

Copy Paste

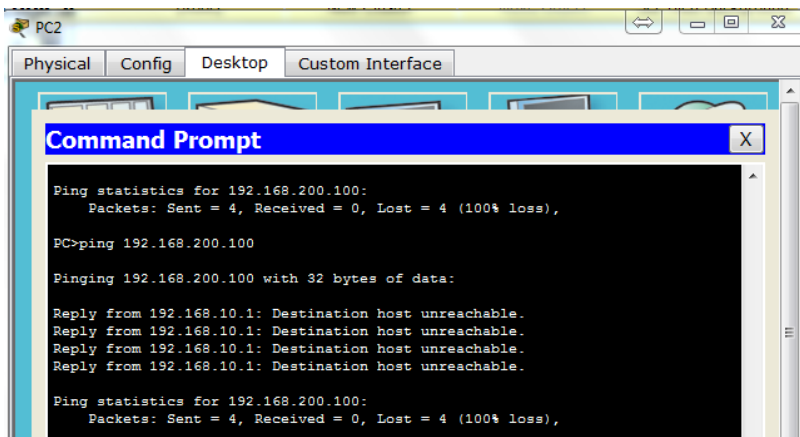
```
R1#show ip interface fastethernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
Internet address is 192.168.200.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing 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--
```

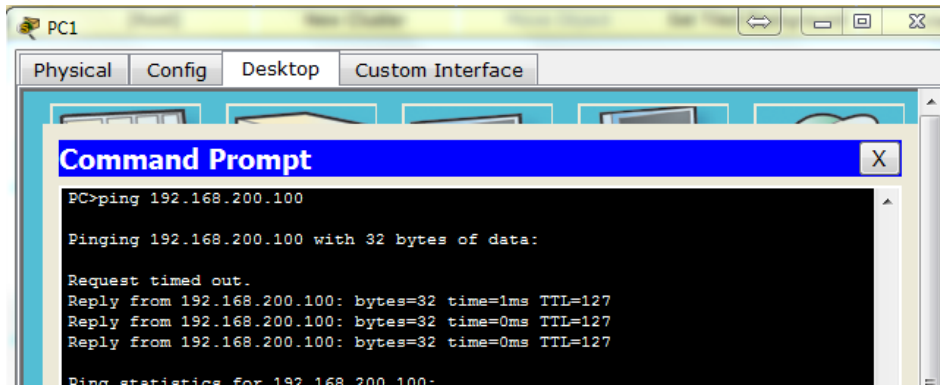
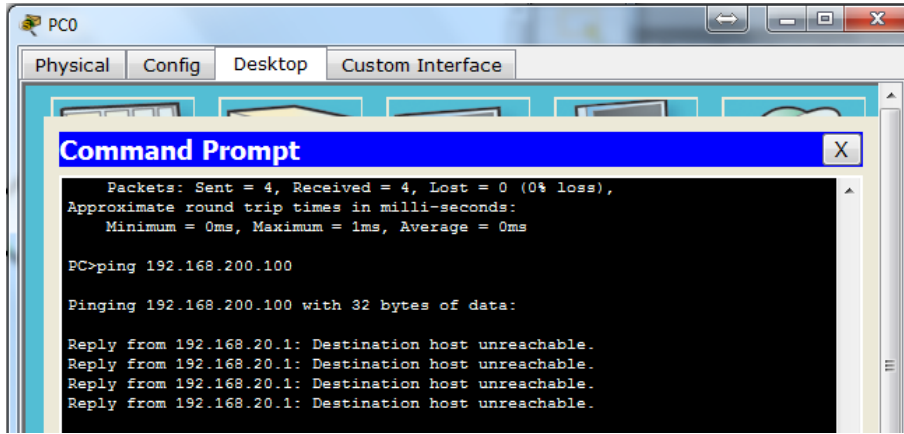
Copy Paste

```
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
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
```

**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**.





**Cumplimiento actividad**

## Activity Results

Time Elapsed: 01:41:59

Congratulations Guest! You completed the activity.

Overall Feedback    Assessment Items    Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Point
[-] Network		
[-] R1		
[-] ACL		0
[-] File_Server_Restric...	Correct	80
[-] Ports		0
[-] 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

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

Topología

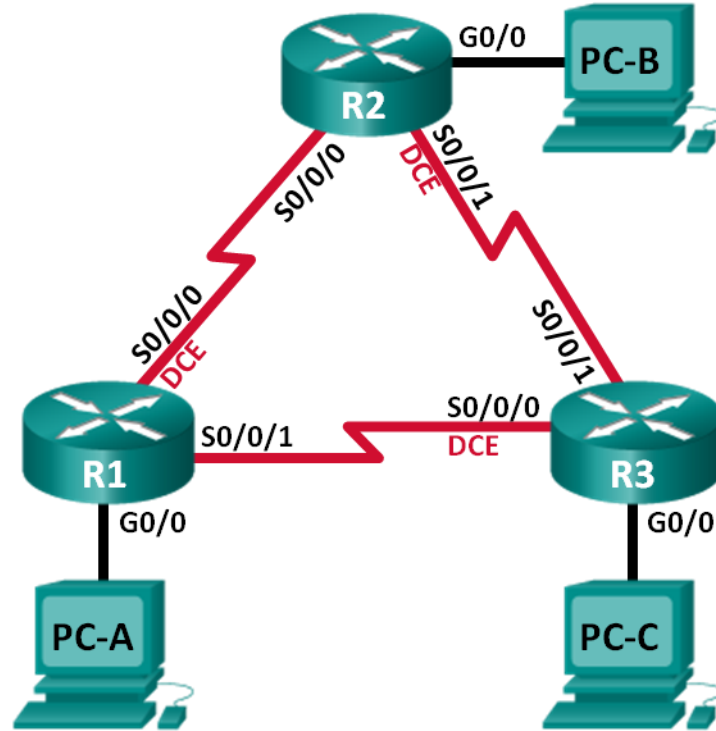


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Gateway predeterminado
R1	G0/0	2001:DB8:ACAD:A::1/64 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**

### Información básica/situación

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



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

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

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

### Recursos necesarios

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

### Parte 8: 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.

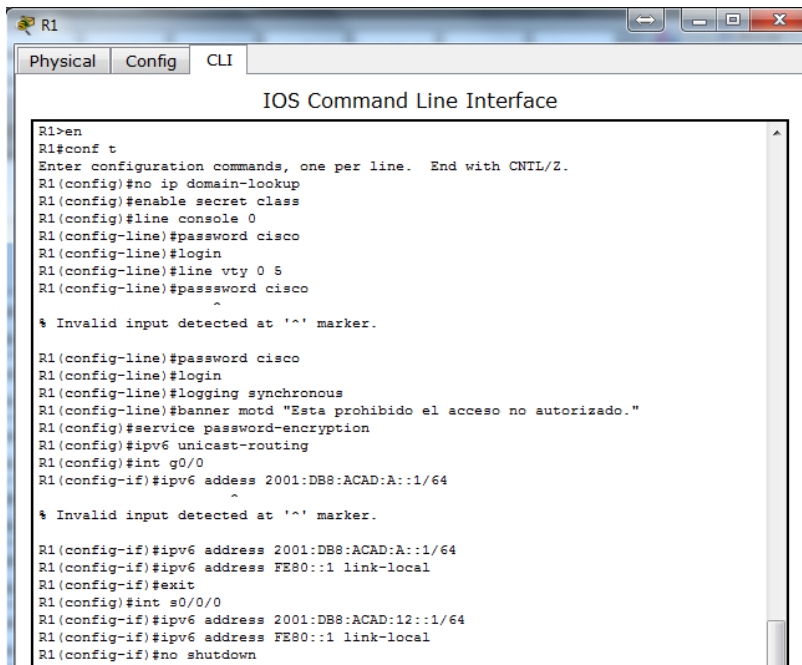
**Paso 1:** realizar el cableado de red tal como se muestra en la topología.

**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 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



```

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

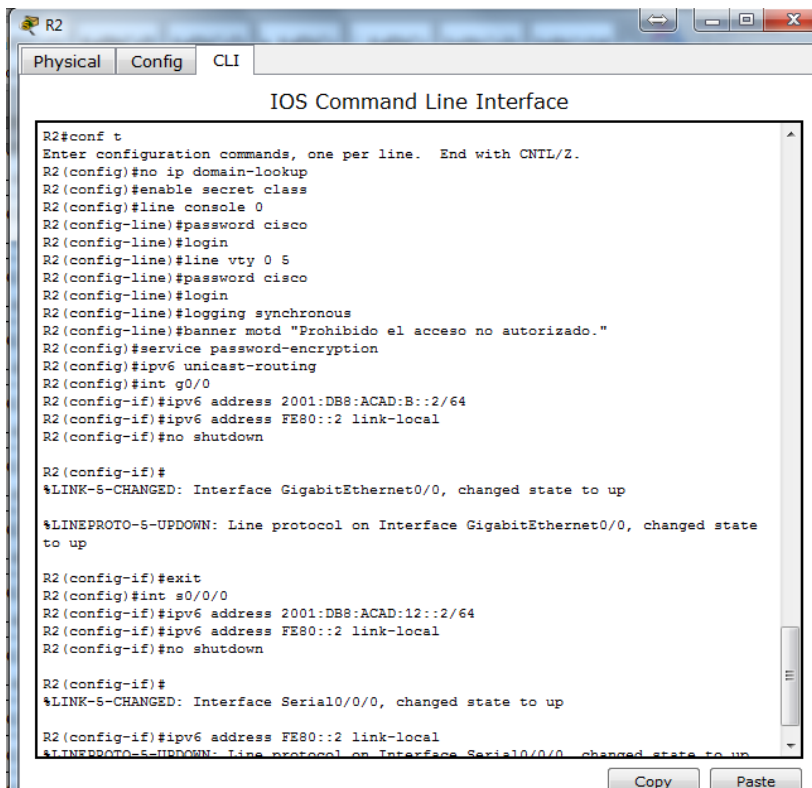
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 5
R1(config-line)#password cisco

% Invalid input detected at '^' marker.

R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#banner motd "Esta prohibido el acceso no autorizado."
R1(config)#service password-encryption
R1(config)#ipv6 unicast-routing
R1(config)#int g0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64

% Invalid input detected at '^' marker.

R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown
  
```



```

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

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

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

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

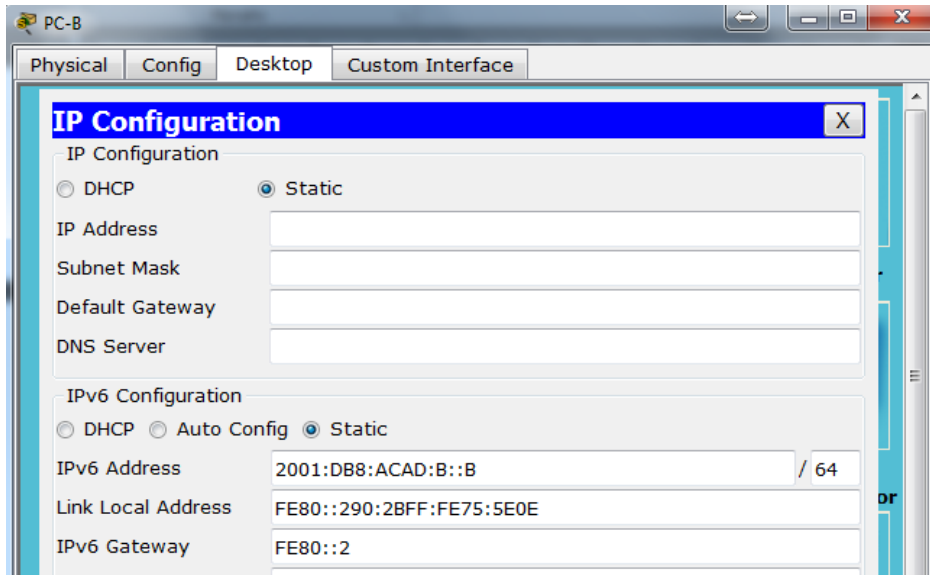
R2(config-if)#exit
R2(config)#int s0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

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

R2(config-if)#ipv6 address FE80::2 link-local
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
  
```

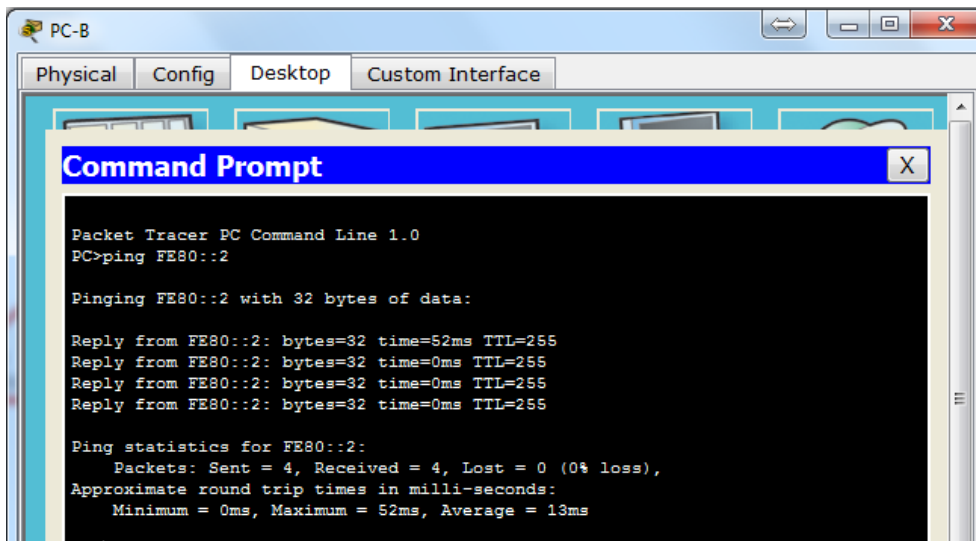
Copy Paste

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



**Paso 5: Probar la conectividad.**

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



**Parte 9: 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**.

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

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

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

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

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

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.

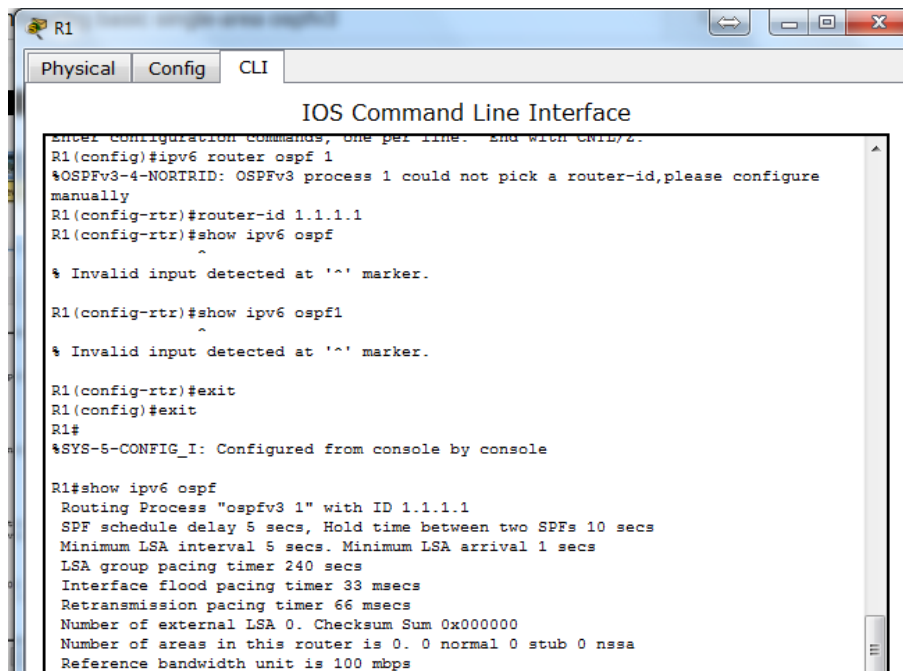
```
R2# show ipv6 ospf
```

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
-----
Enter configuration commands, one per line. End with Ctrl/Z.
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure
manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#show ipv6 ospf
^
% Invalid input detected at '^' marker.

R1(config-rtr)#show ipv6 ospf1
^
% Invalid input detected at '^' marker.

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

```

R2
Physical Config CLI
IOS Command Line Interface
R2>en
Password:
R2#ipv6 router ospf 1
^
% Invalid input detected at '^' marker.

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

```

R3
Physical Config CLI
IOS Command Line Interface
User Access Verification

Password:

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

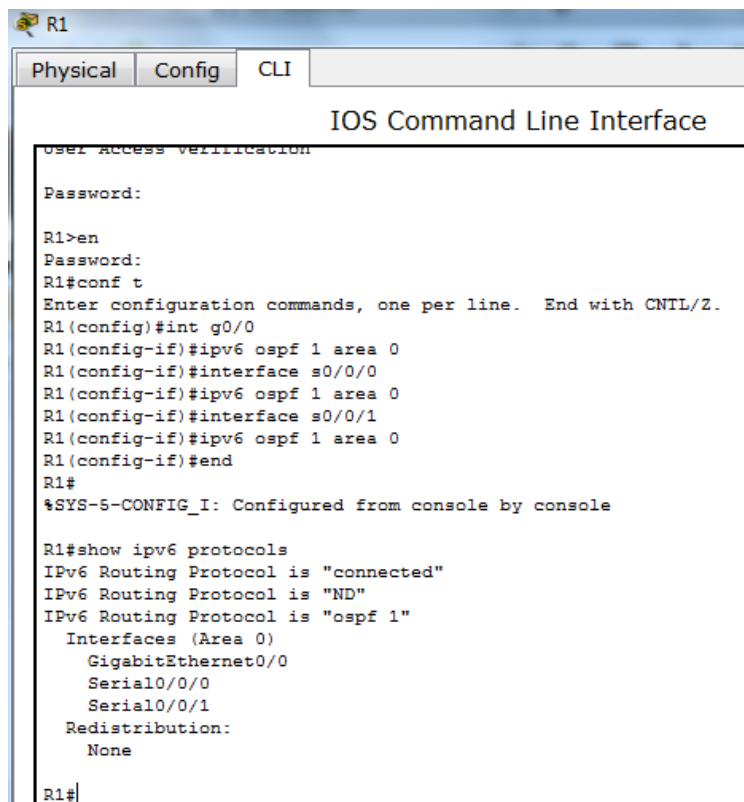
**Paso 2: configurar OSPFv6 en el R1.**

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

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

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

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



```
R1
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int 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)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

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

R1#

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

R1#

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

```

R2
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 ospf 1 area 0
^
% Invalid input detected at '^' marker.
R2(config-if)#ipv6 ospf 1 area 0
^
% Invalid input detected at '^' marker.
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)#
18:49:06: %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)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
18:51:34: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to
FULL, Loading Done
  
```

```

R3
Physical Config CLI
IOS Command Line Interface
Password:
R3>class
Translating "class"
% Unknown command or computer name, or unable to find computer address
R3>en
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/1
R3(config-if)#
18:51:13: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
18:51:26: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to
FULL, Loading Done
end
R3#
%SYS-5-CONFIG_I: Configured from console by console
  
```

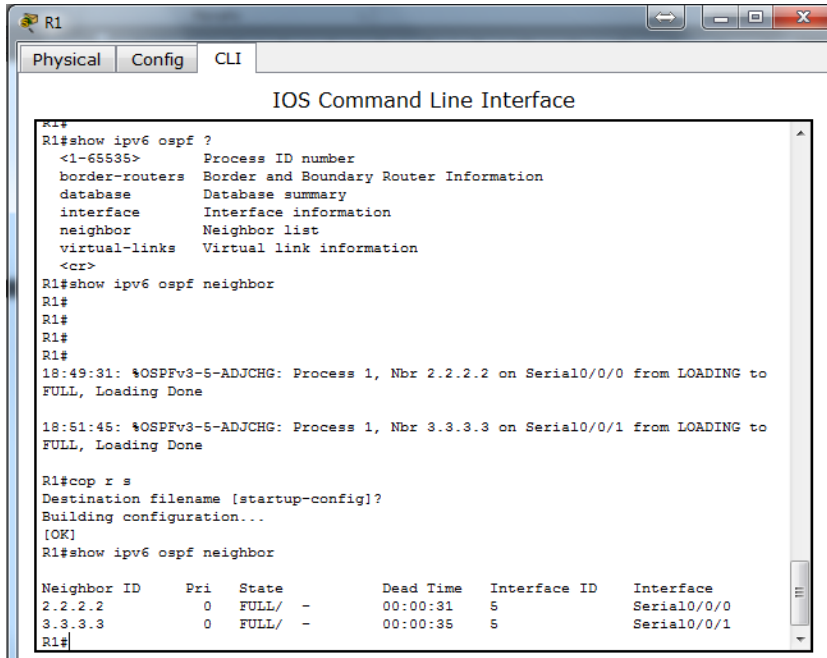
**Paso 3: verificar vecinos de OSPFv3.**

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



```

R1#show ipv6 ospf ?
<1-65535> Process ID number
border-routers Border and Boundary Router Information
database Database summary
interface Interface information
neighbor Neighbor list
virtual-links Virtual link information
<cr>
R1#show ipv6 ospf neighbor
R1#
R1#
R1#
R1#
18:49:31: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
18:51:45: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
R1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#show ipv6 ospf neighbor
Neighbor ID Pri State Dead Time Interface ID Interface
2.2.2.2 0 FULL/ - 00:00:31 5 Serial0/0/0
3.3.3.3 0 FULL/ - 00:00:35 5 Serial0/0/1
R1#
  
```

**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



```

R1
-----
Physical  Config  CLI
-----
IOS Comn

R1#
R1#
R1#
18:49:31: %OSPFv3-5-ADJCHG: Process 1
FULL, Loading Done

18:51:45: %OSPFv3-5-ADJCHG: Process 1
FULL, Loading Done

R1#cop r s
Destination filename [startup-config]
Building configuration...
[OK]
R1#show ipv6 ospf neighbor

Neighbor ID      Pri   State
2.2.2.2          0    FULL/  -
3.3.3.3          0    FULL/  -
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None

```

**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

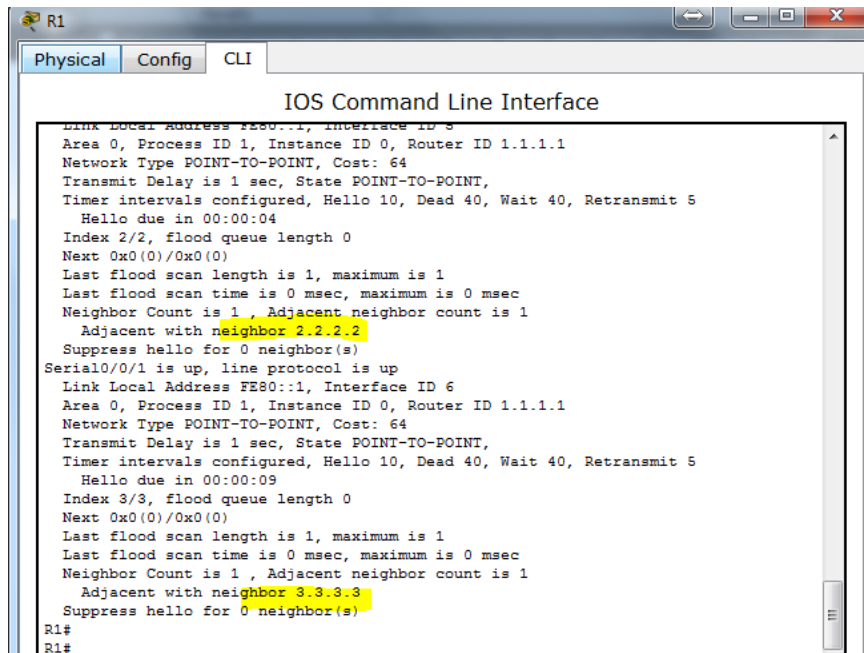
Next 0x0(0)/0x0(0)/0x0(0)

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)



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
  
```

% Invalid input detected at '^' marker.

### 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

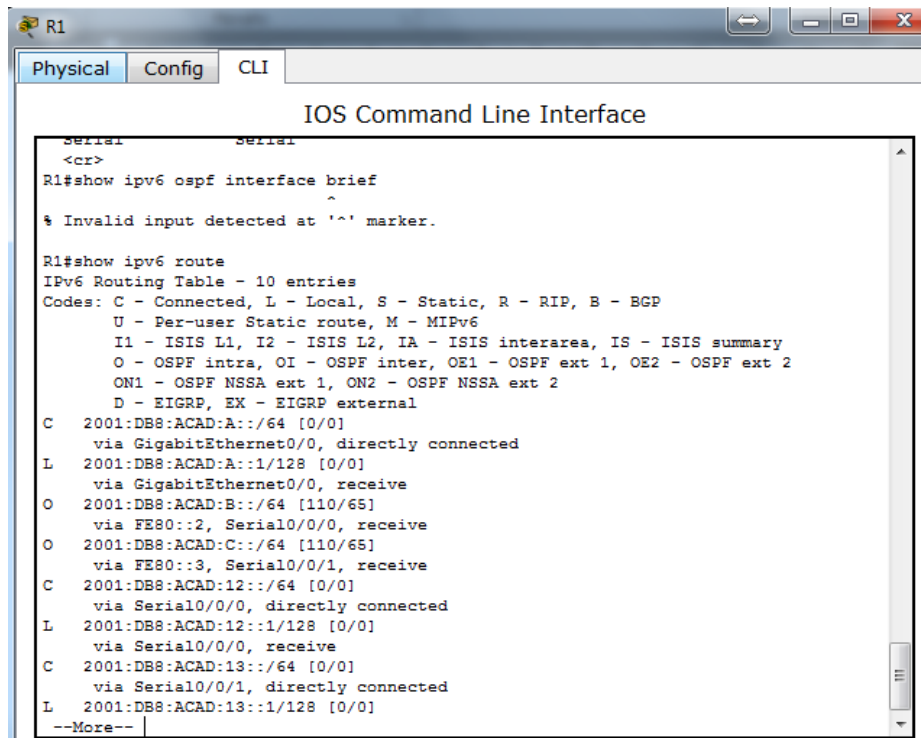
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

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



```

R1
Physical Config CLI
IOS Command Line Interface
Serial Serial
<cr>
R1#show ipv6 ospf interface brief
^
% Invalid input detected at '^' marker.

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

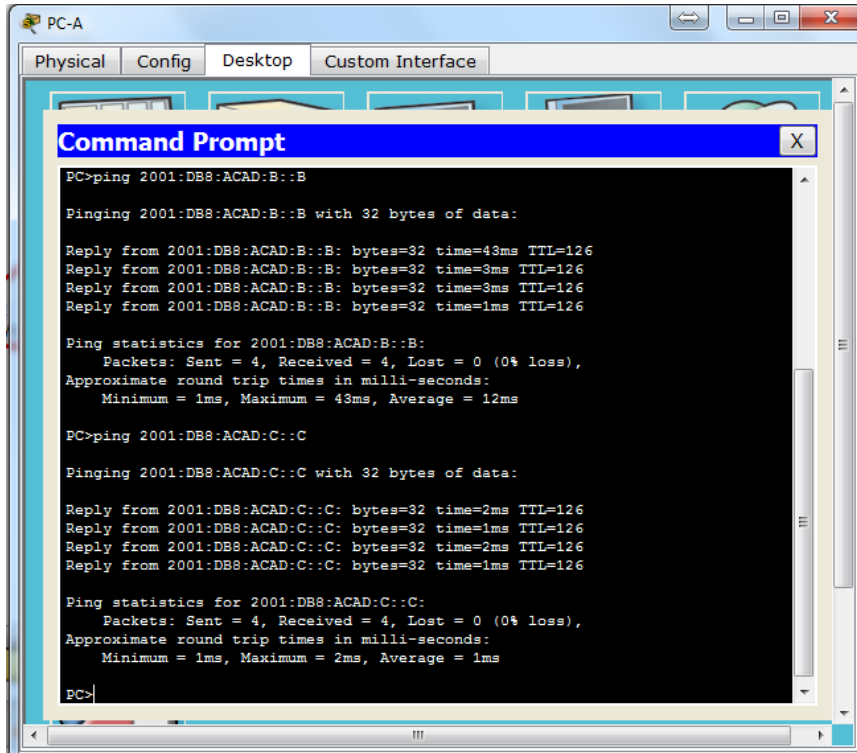
¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?

**show ip ospf neighbor**

**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
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=43ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=3ms 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 = 43ms, Average = 12ms

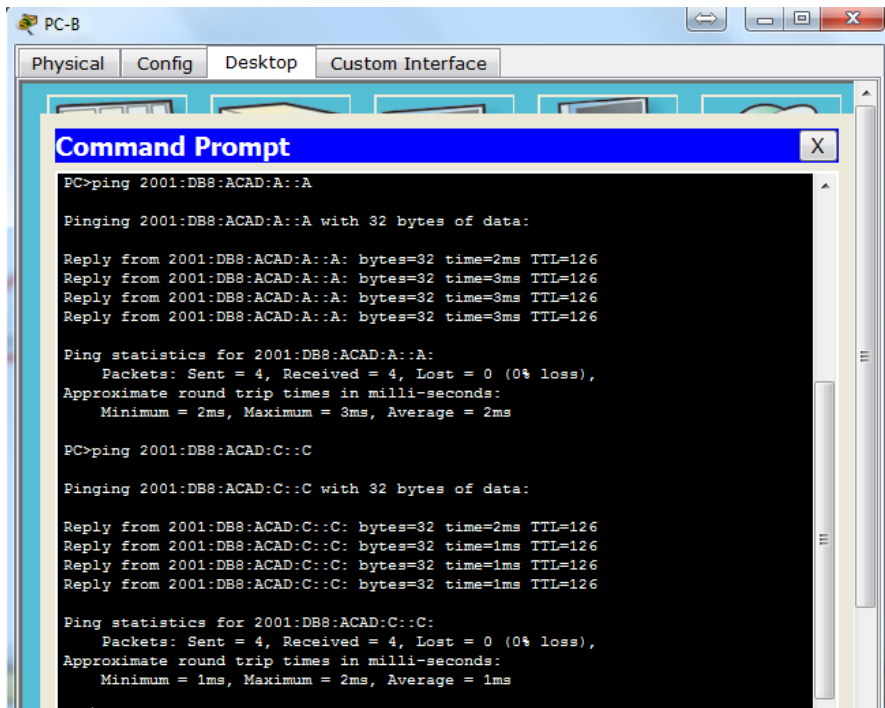
PC>ping 2001:DB8:ACAD:C::C

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

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>
  
```



```

PC-B
Physical Config Desktop Custom Interface
Command Prompt
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=2ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=3ms TTL=126

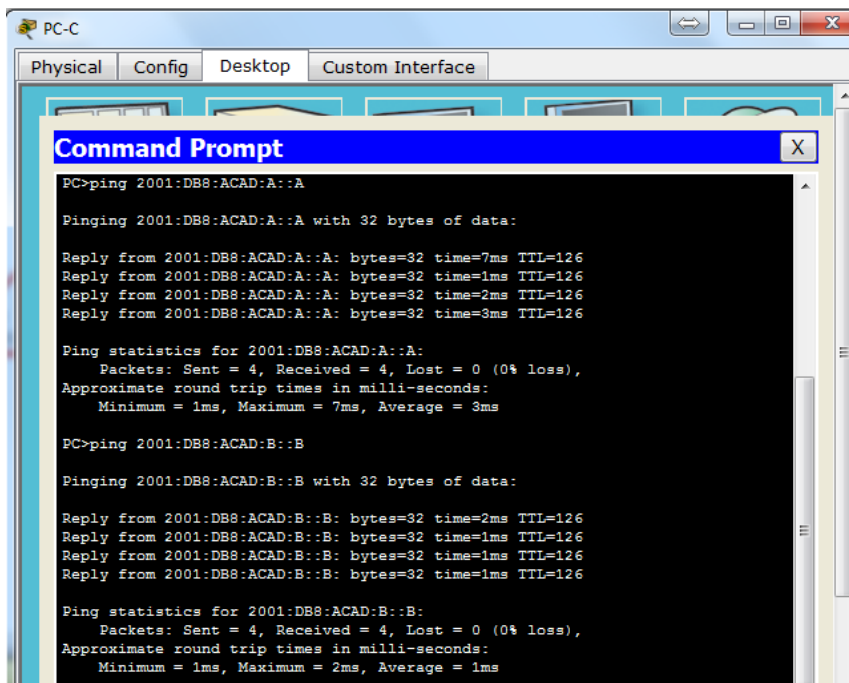
Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

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=2ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
  
```



```

PC-C
Physical Config Desktop Custom Interface
Command Prompt
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=7ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=3ms TTL=126

Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 3ms

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=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
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 = 2ms, Average = 1ms
  
```

### Parte 10: configurar las interfaces pasivas de OSPFv3

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

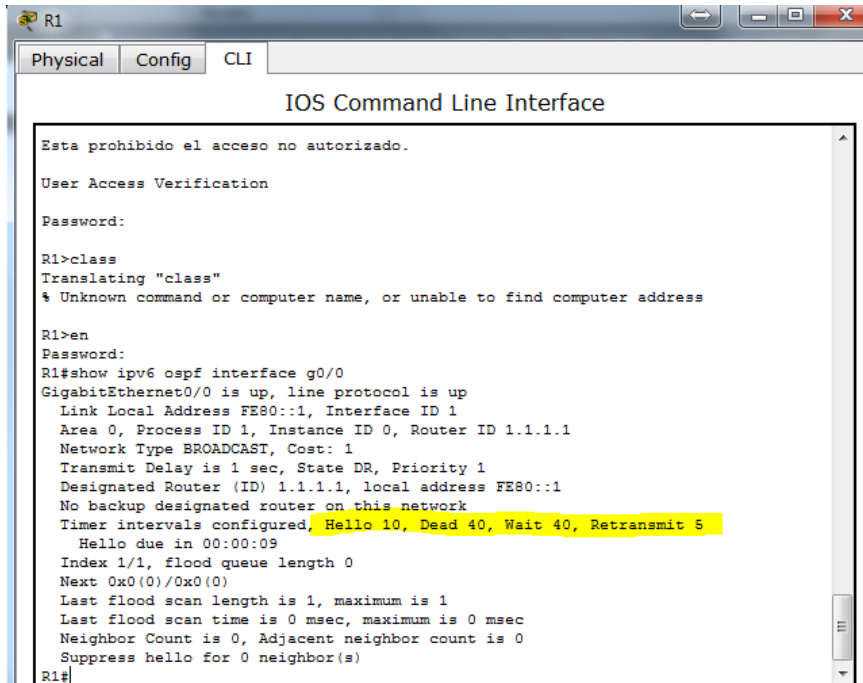
router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

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

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

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

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



```

R1
Physical Config CLI
IOS Command Line Interface
Esta prohibido el acceso no autorizado.
User Access Verification
Password:
R1>class
Translating "class"
% Unknown command or computer name, or unable to find computer address
R1>en
Password:
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:09
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#
  
```

- 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.

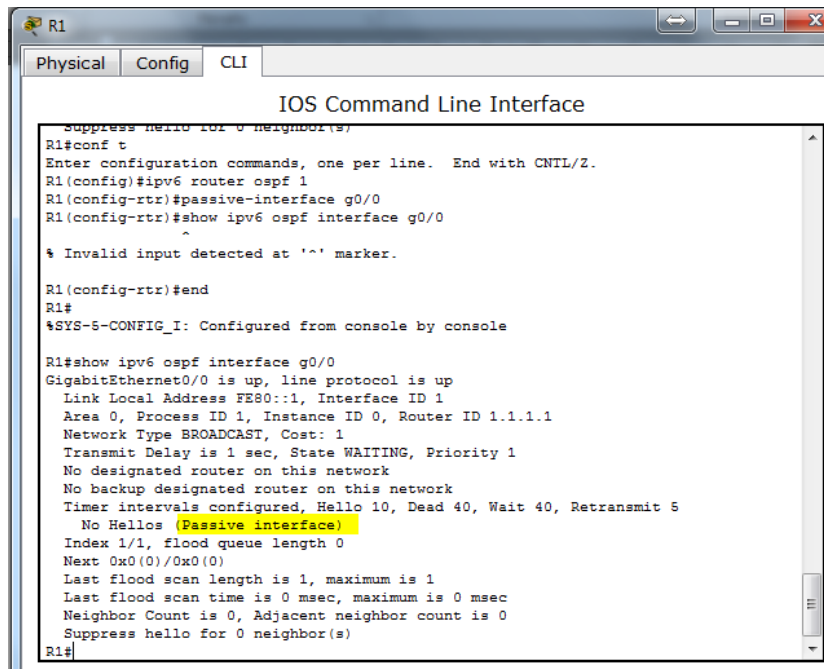
```
R1# show ipv6 ospf interface g0/0
```

```

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)



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
Prohibido el acceso no autorizado.
User Access Verification
Password:
R2>class
Translating "class"
% Unknown command or computer name, or unable to find computer address
R2>en
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**

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

R1# **show ipv6 ospf neighbor**

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

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

```

R1#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
3.3.3.3         0    FULL/ -         00:00:36   5             Serial0/0/1
R1#
  
```

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

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

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

Link Local Address FE80::2, Interface ID 6

Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2

Network Type POINT\_TO\_POINT, Cost: 64  
 Transmit Delay is 1 sec, State POINT\_TO\_POINT  
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
**No Hellos (Passive interface)**  
 Graceful restart helper support enabled  
 Index 1/2/2, flood queue length 0  
 Next 0x0(0)/0x0(0)/0x0(0)  
 Last flood scan length is 2, maximum is 3  
 Last flood scan time is 0 msec, maximum is 0 msec  
 Neighbor Count is 0, Adjacent neighbor count is 0  
 Suppress hello for 0 neighbor(s)

```
R2#show ipv6 ospf neighbor
R2#show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 5
  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)
```

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**.

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**

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? **Serial0/0/1**

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

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

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

¿Qué indica esta información?

Todo el tráfico de la red B desde R1 será ruteado a través de R3. La interface S0/0/0 en R2 esta aun configurada como pasiva de tal manera que OSPFv3 no manda información de ruteo notificándose a través de esta interfaz.

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.

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

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

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
1.1.1.1	0	FULL/ -	00:00:34	5	Serial10/0/0
3.3.3.3	0	FULL/ -	00:00:38	6	Serial10/0/1

```
R2#
```

### Reflexión

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

Si, porque el proceso OSPF es solamente utilizado y local en un router, no necesita coincidir el proceso usado en otros routers en la misma área.

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

Removiendo la entrada network ayuda a prevenir los errores en las direcciones IPV6.

### 10.3.1.1 IoE and DHCP Instructions

#### Objetivo

Configure DHCP para IPv4 o IPv6 en un router Cisco 1941.

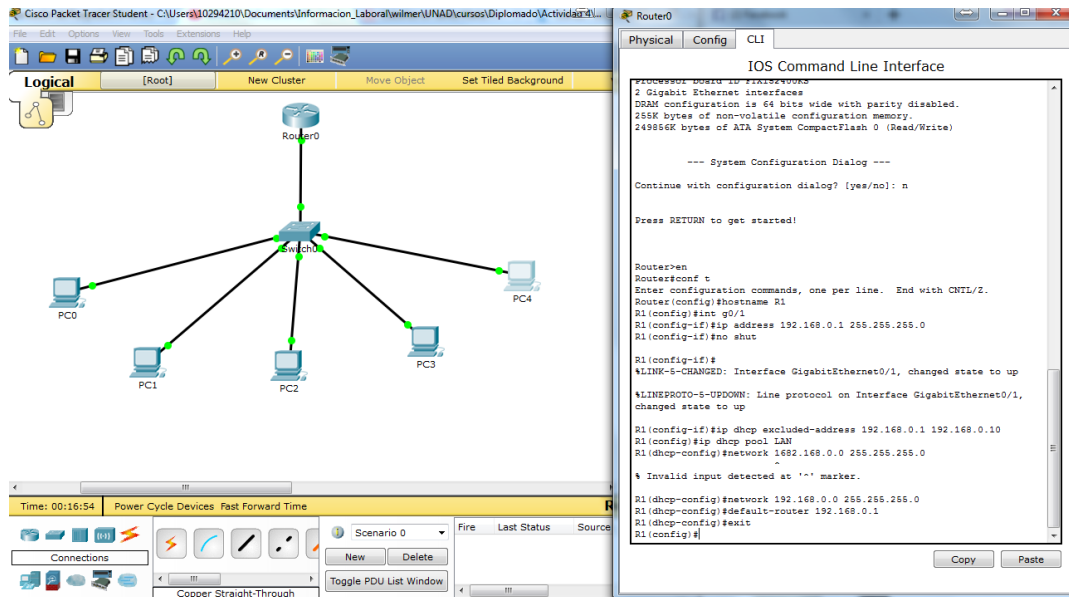
#### Situación

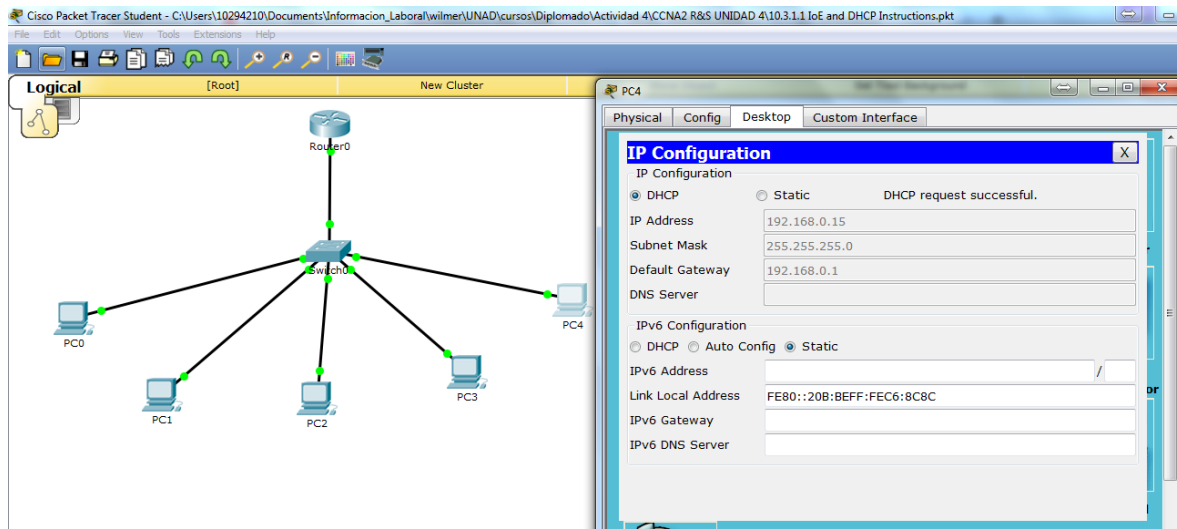
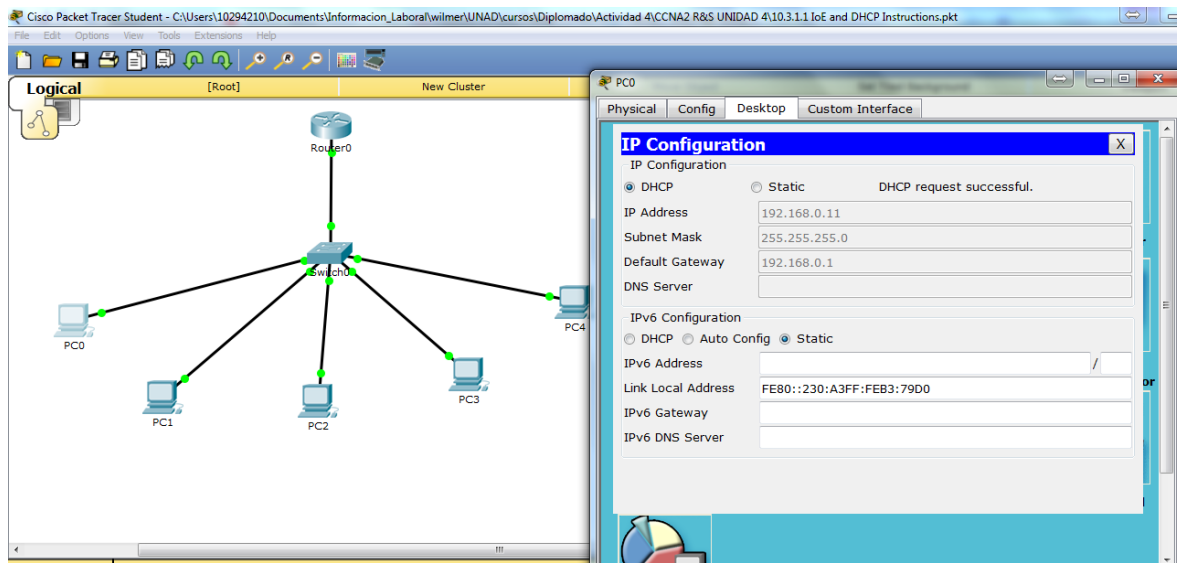
En este capítulo, se presenta el concepto del uso del proceso de DHCP en la red de una pequeña a mediana empresa; sin embargo, el protocolo DHCP también tiene otros usos.

Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.
- Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones DHCP del servidor de DHCP.
- Muestre los resultados que validen que cada terminal garantiza una dirección IP del servidor. Utilice un programa de captura de pantalla para guardar la información del resultado o emplee el comando de la tecla **ImprPant**.
- Presente sus conclusiones a un compañero de clase o a la clase.





## Recursos necesarios

Software de Packet Tracer

## Reflexión

1. ¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica? ¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?

El router Cisco 1941 permite disminuir la administración ya que automáticamente asigna de forma eficiente las Ip para cada host, dependiendo el número de host también se podría utilizar un ISR.

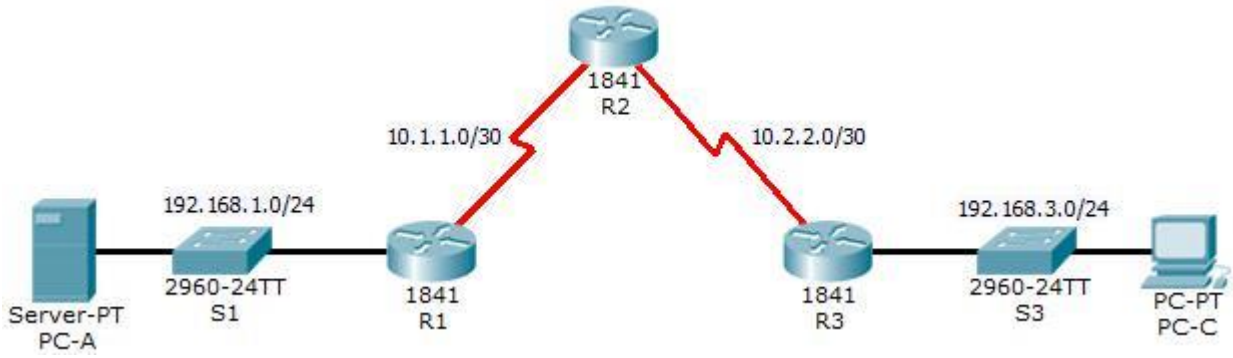
2. ¿Cómo cree que las pequeñas y medianas empresas pueden usar la asignación de direcciones IP de DHCP en el mundo de las redes IPv6 e IdT? Mediante la técnica de la lluvia de ideas, piense y registre cinco respuestas posibles.

- Asignando el rango correcto de acuerdo a su crecimiento.

- La cantidad de IP IPv6 aún son demasiadas para agotarse por lo que un servidor DHCP no tenía problemas al asignar direcciones.
- No tendría restricciones al ir creciendo la empresa, puede tener aumentar sus sedes y host exponencialmente.

Practica 4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks

Topology



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
	SO/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	SO/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	SO/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
	So0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

**Objectives**

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

**Background / Scenario**

Access to routers R1, R2, and R3 should only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, a server providing DNS, SMTP, FTP, and HTTPS services.

Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and/or destination IP address. In this activity, you create ACLs on edge routers R1 and R3 to achieve this goal. You then verify ACL functionality from internal and external hosts.

The routers have been pre-configured with the following:

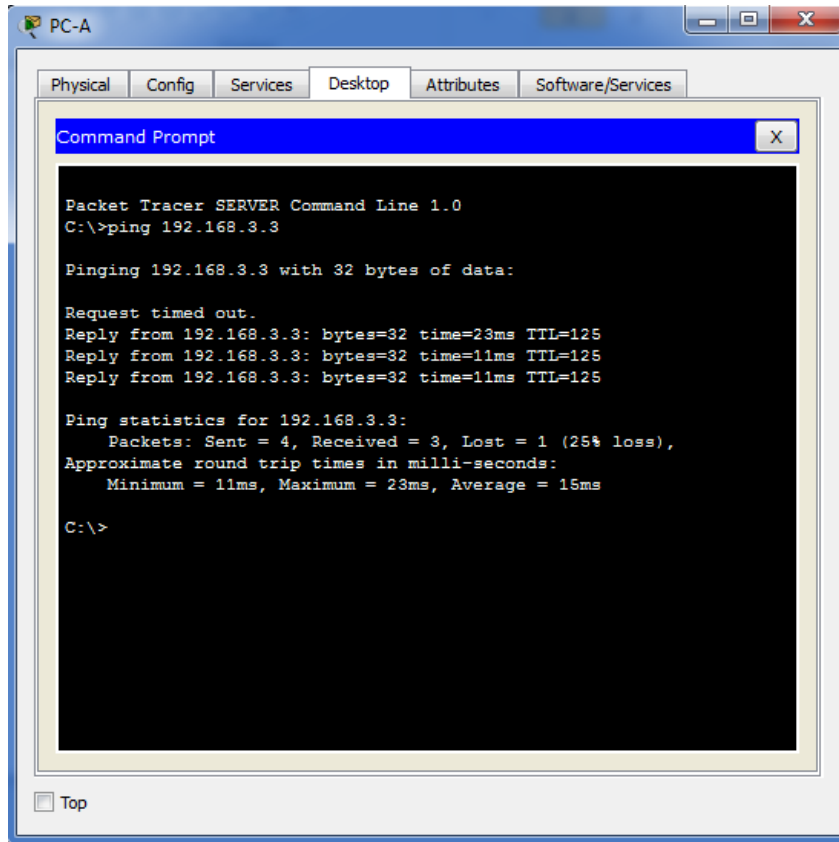
- o Enable password: **ciscoenpa55**
  
- o Password for console: **ciscoconpa55** o  
Username for VTY lines: **SSHadmin**
  
- o Password for VTY lines: **ciscosshpa55** o IP  
addressing
  
- o Static routing

**Part 1: Verify Basic Network Connectivity**

Verify network connectivity prior to configuring the IP ACLs.

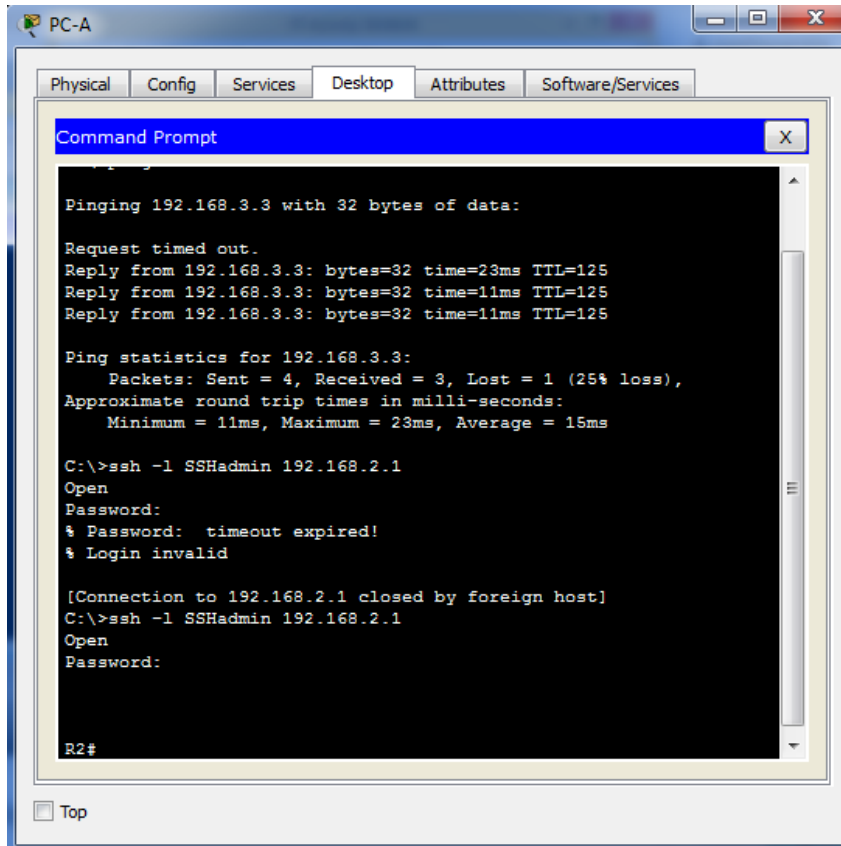
**Step 1: From PC-A, verify connectivity to PC-C and R2.**

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



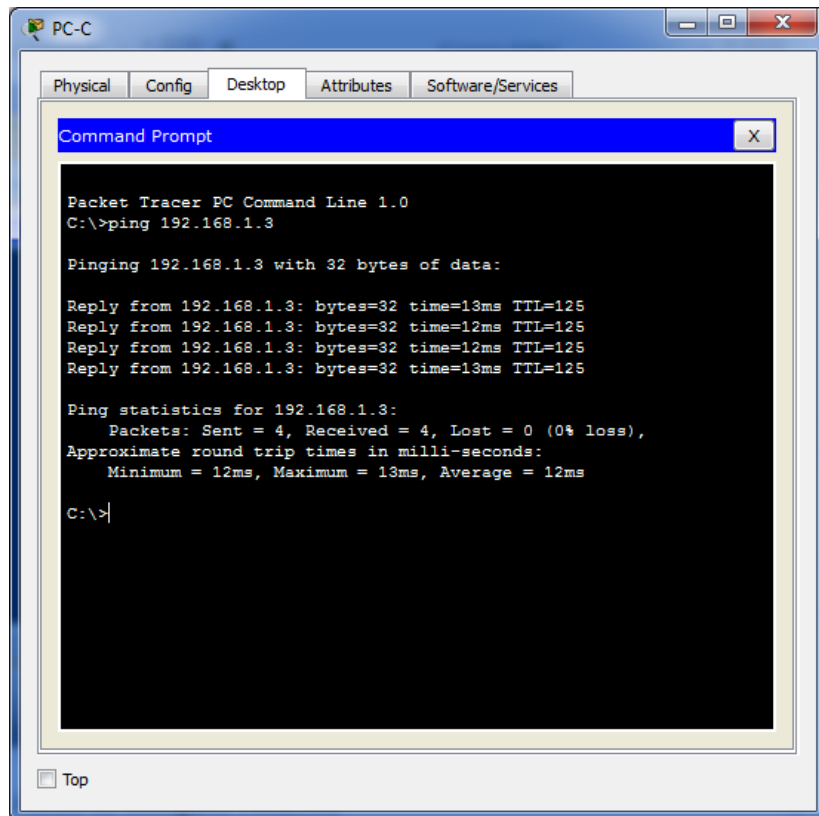
b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. When finished, exit the SSH session.

PC> ssh -l SSHadmin 192.168.2.1



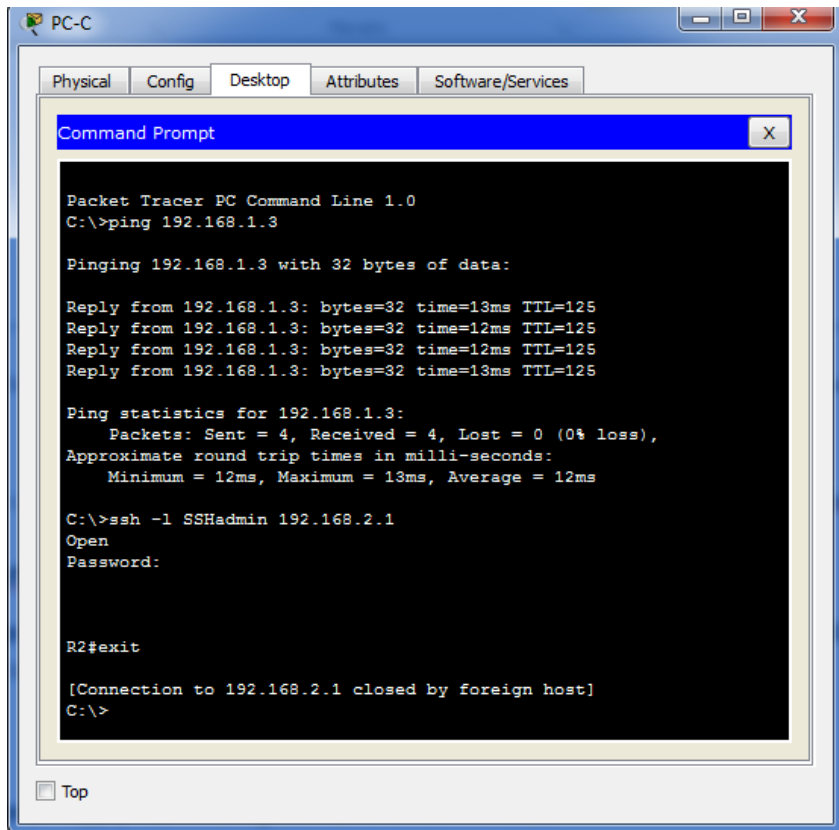
**Step 2: From PC-C, verify connectivity to PC-A and R2.**

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

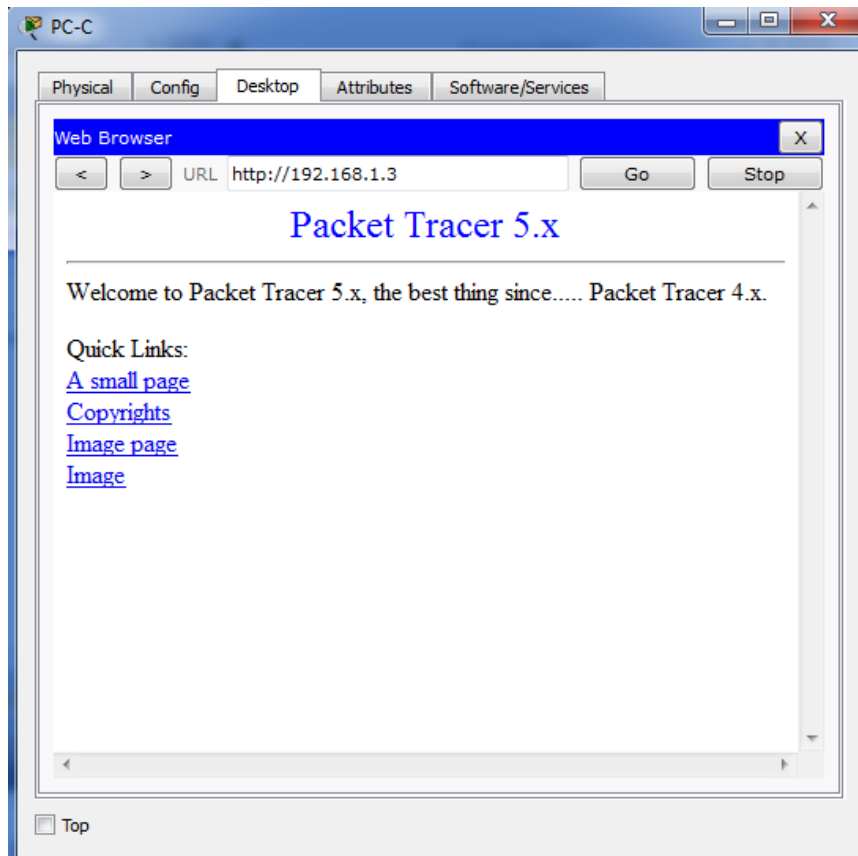


b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. Close the SSH session when finished.

**PC> ssh -l SSHadmin 192.168.2.1**



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



## Part 2: Secure Access to Routers

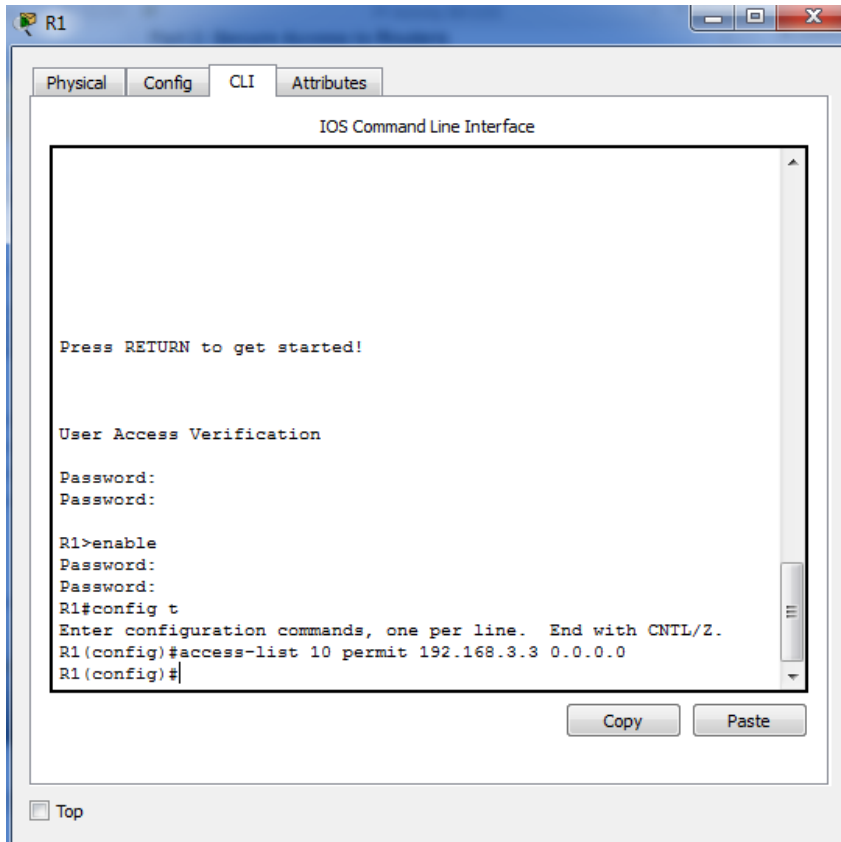
**Step 1:** Configure ACL 10 to block all remote access to the routers except from PC-C.

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

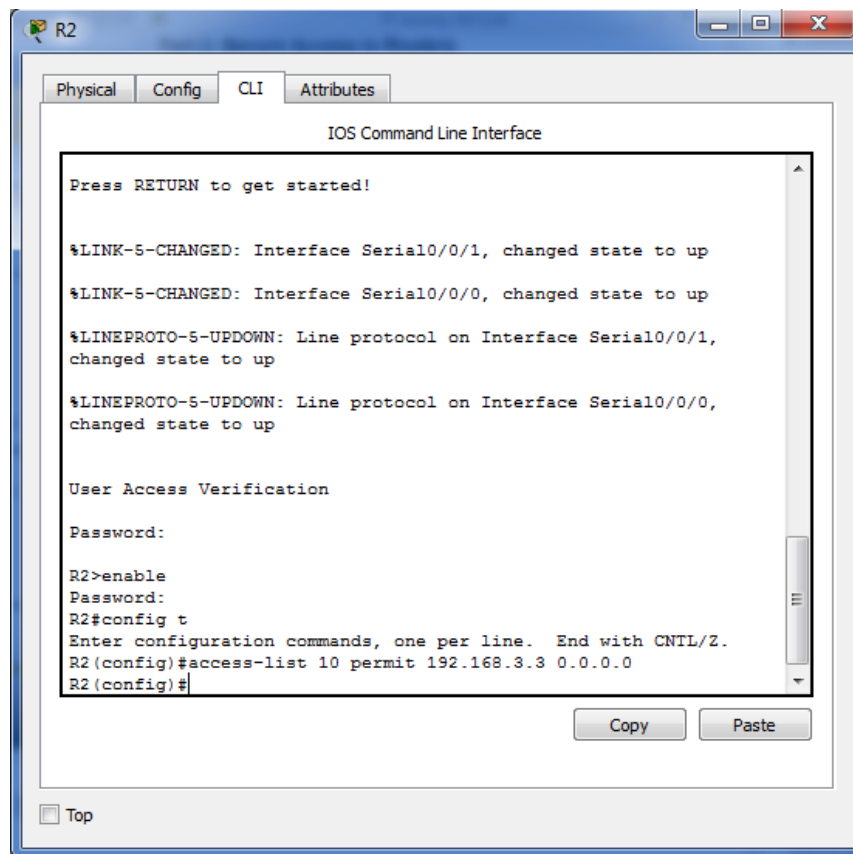
```
R1(config)# access-list 10 permit 192.168.3.3 0.0.0.0
```

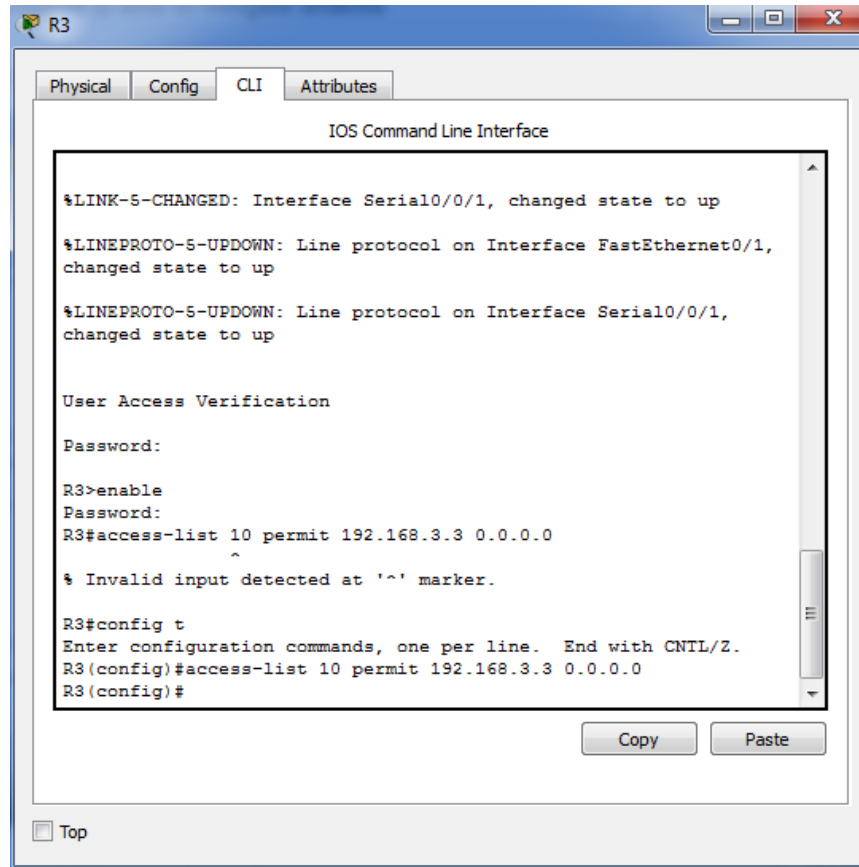
```
R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0
```

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









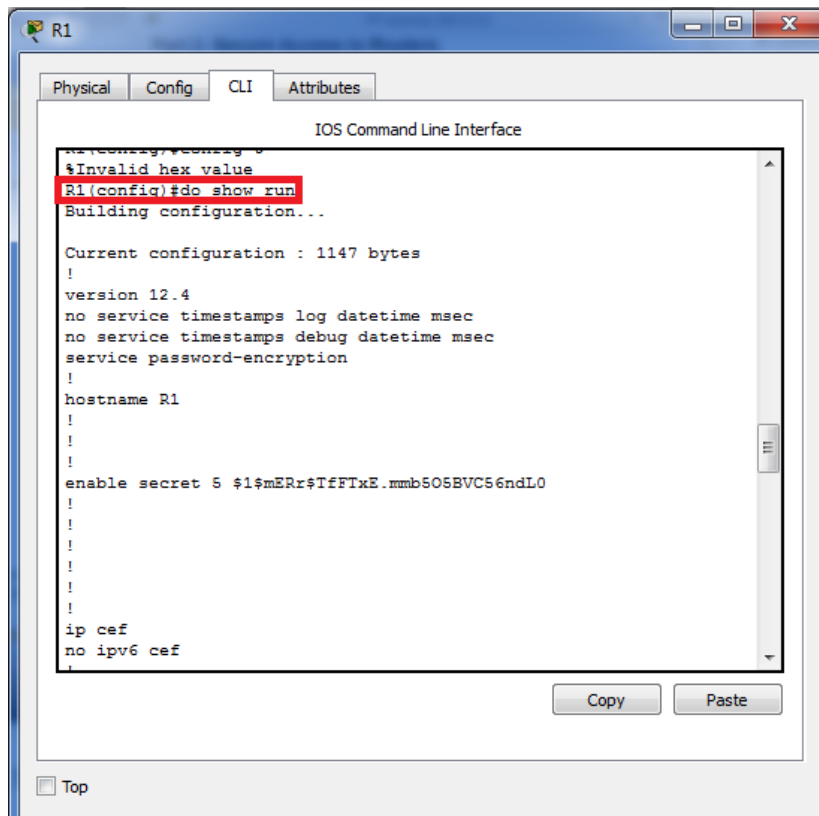
**Step 2: Apply ACL 10 to ingress traffic on the VTY lines.**

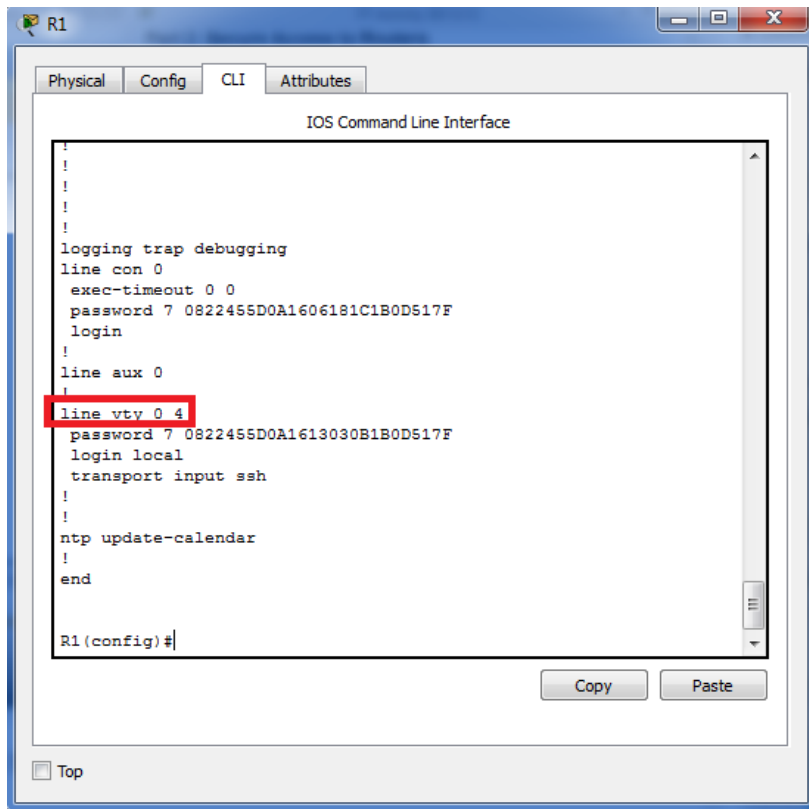
Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

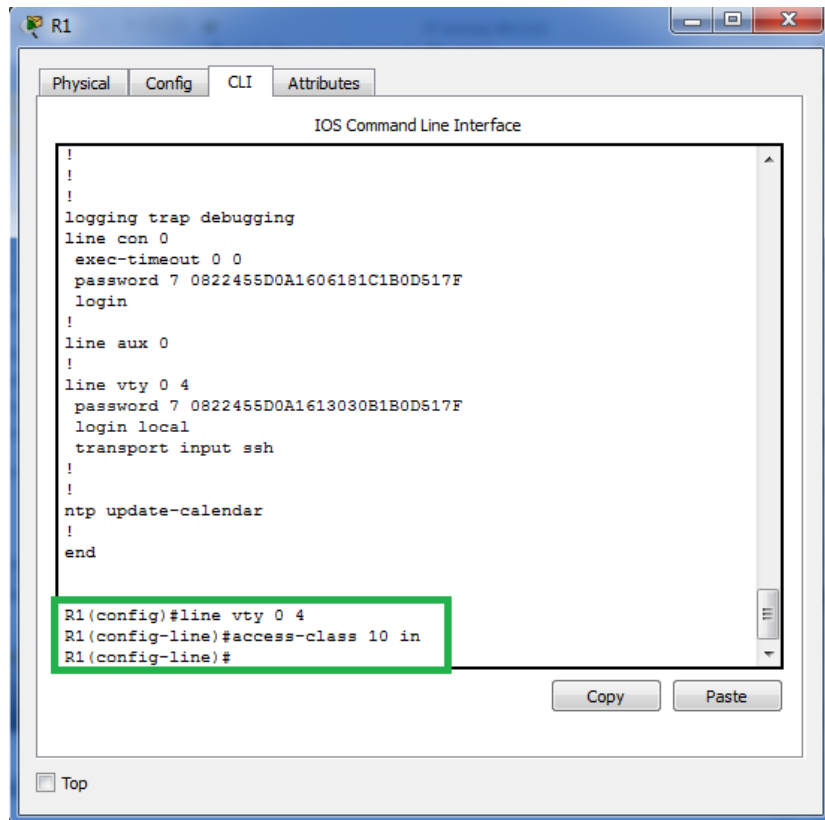
```
R1(config-line)# access-class 10 in
```

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

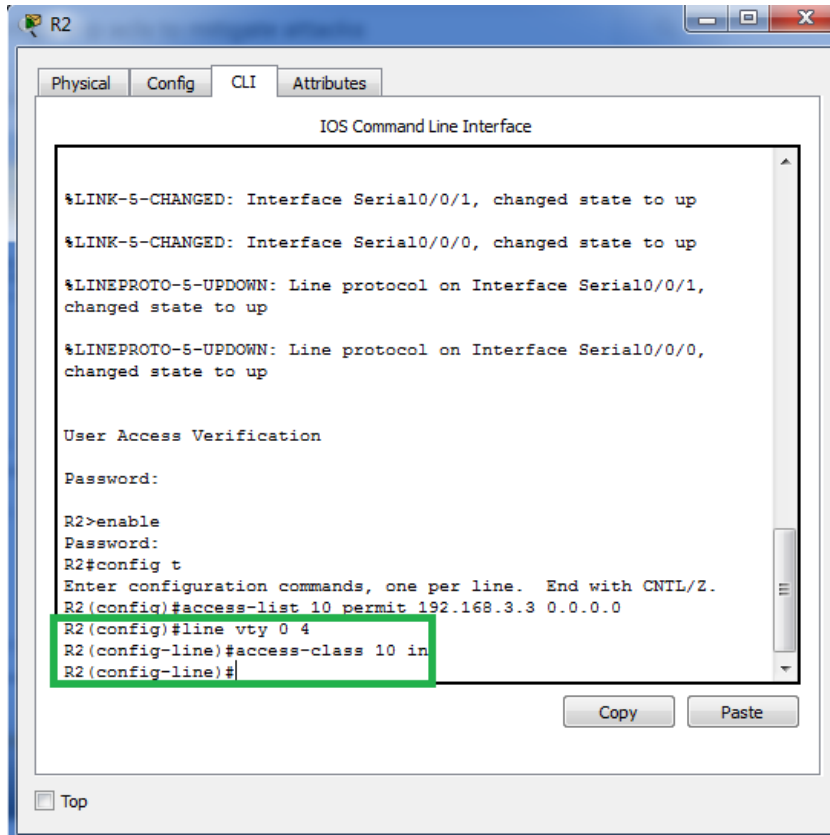
```
R3(config-line)# access-class 10 in
```



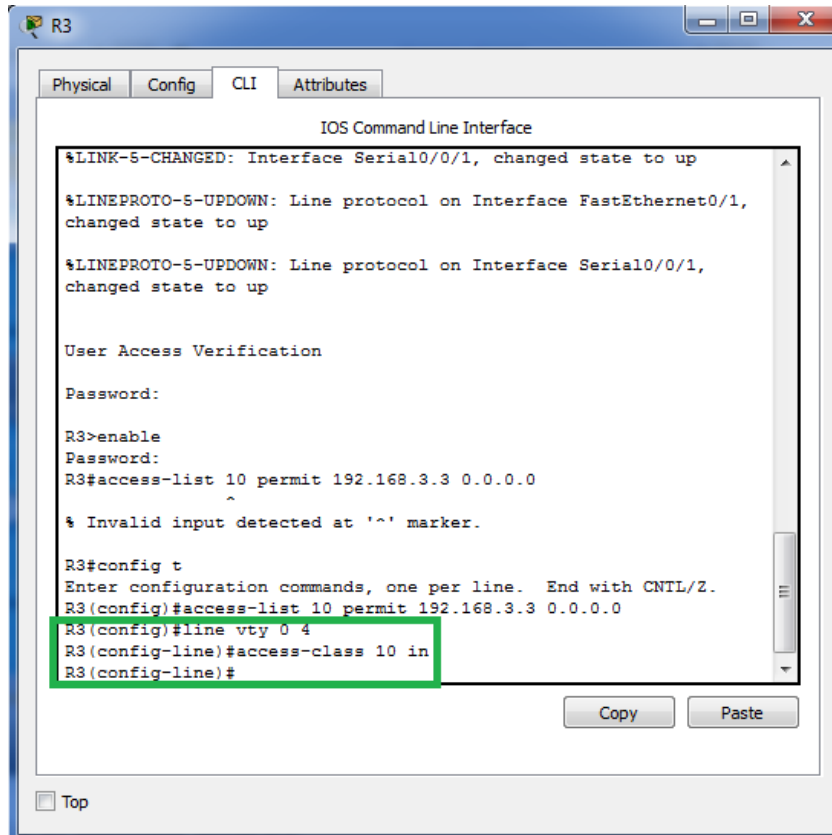




Ahora para el router 2



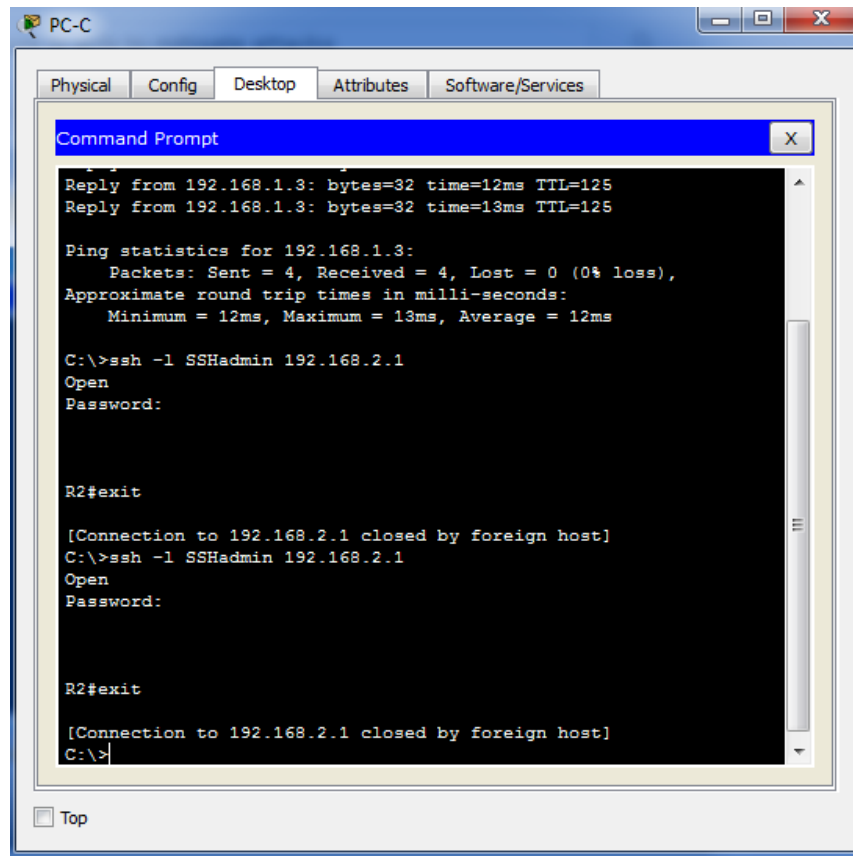
Ahora para el router 3



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

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

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



The screenshot shows a Windows desktop window titled "PC-C" with tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". A "Command Prompt" window is open, displaying the following text:

```
Reply from 192.168.1.3: bytes=32 time=12ms TTL=125
Reply from 192.168.1.3: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 13ms, Average = 12ms

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

R2#exit

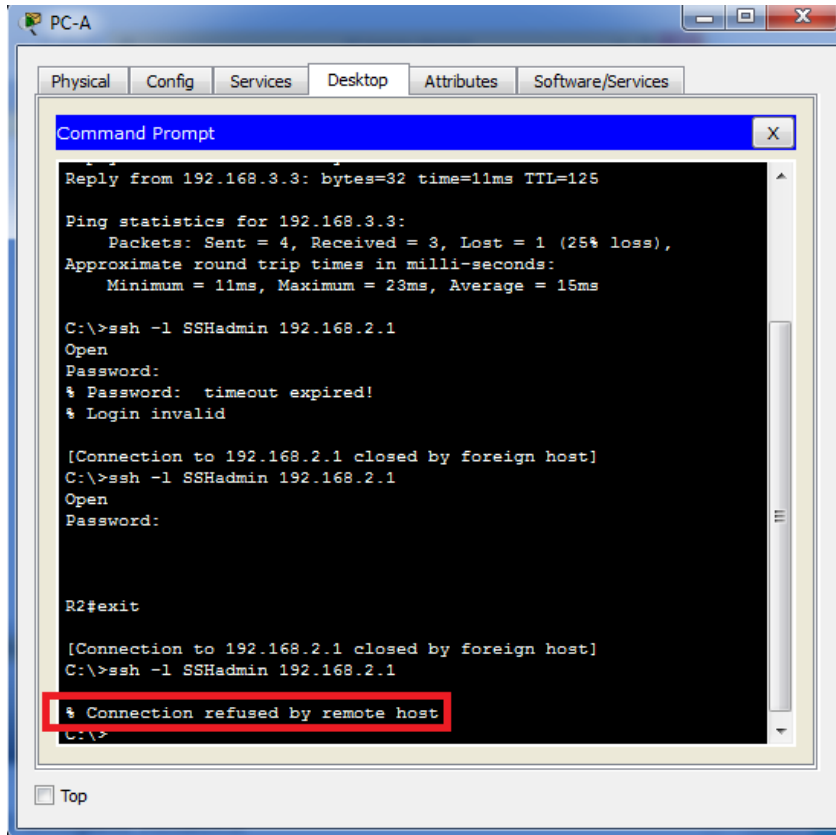
[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l SSHAdmin 192.168.2.1
Open
Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

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





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

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

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

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



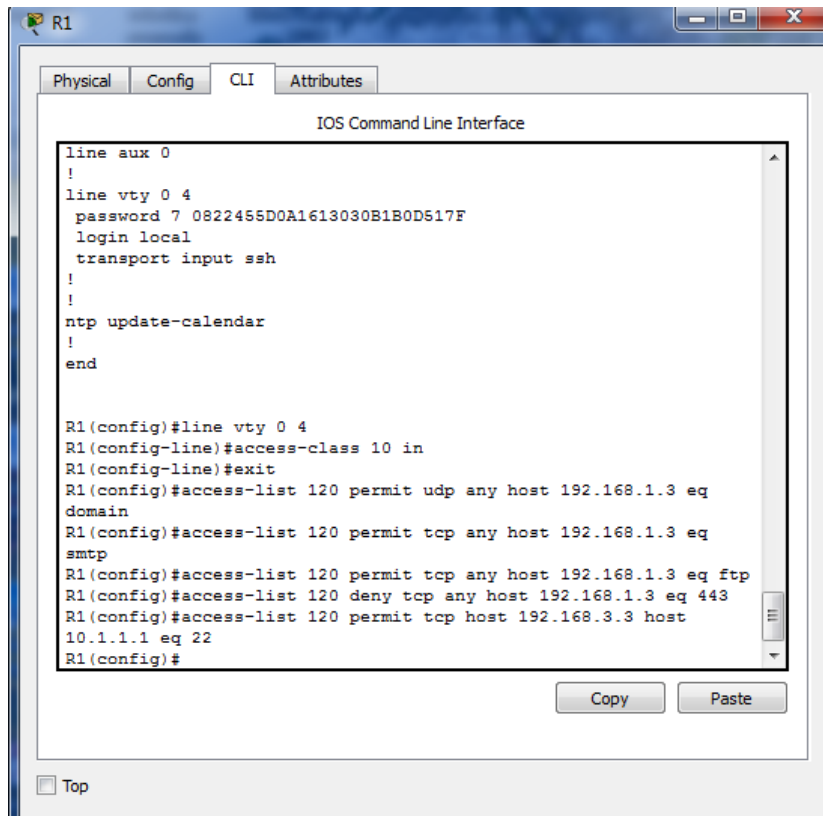
**Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.**

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

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

```
R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443
```

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



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
line aux 0
!
line vty 0 4
password 7 0822455D0A1613030B1B0D517F
login local
transport input ssh
!
!
ntp update-calendar
!
end

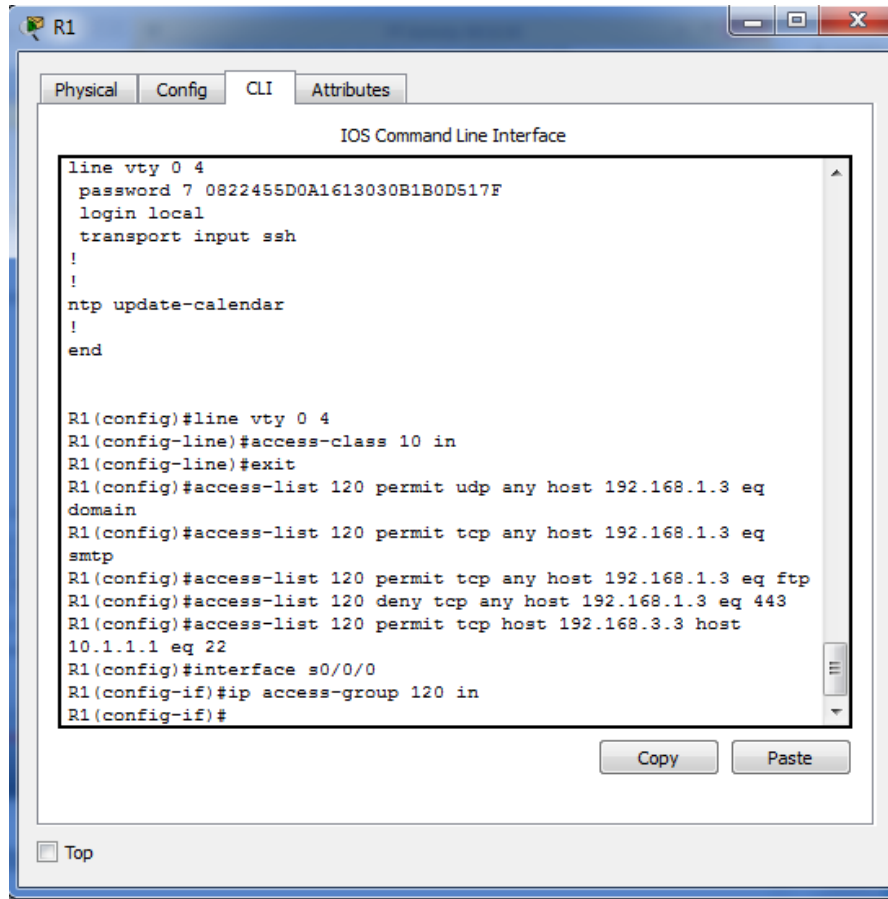
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#exit
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq
domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq
smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host
10.1.1.1 eq 22
R1(config)#
Copy Paste
Top
  
```

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

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

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

```
R1(config-if)# ip access-group 120 in
```

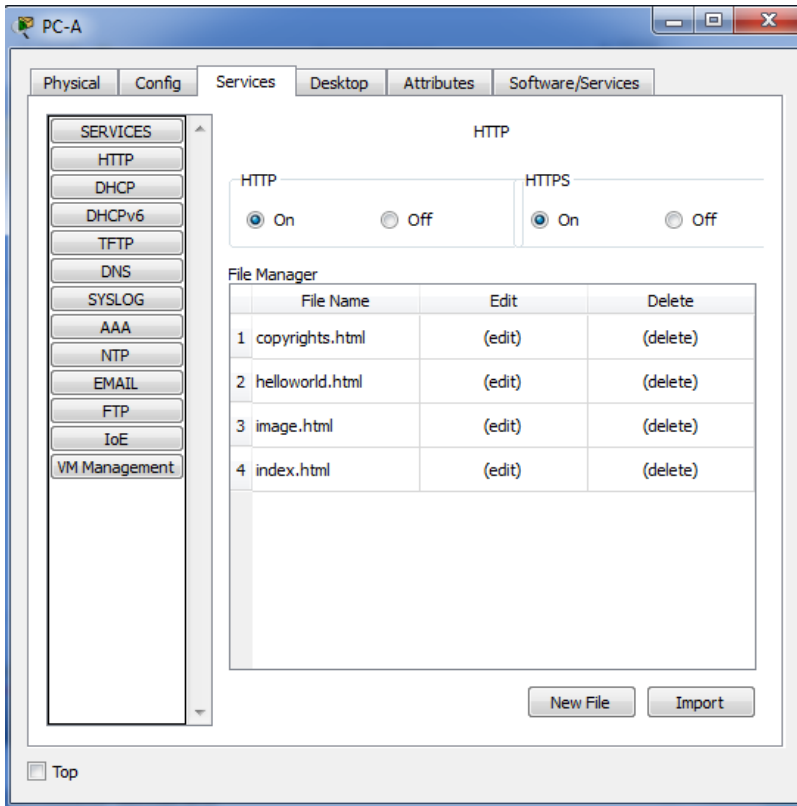
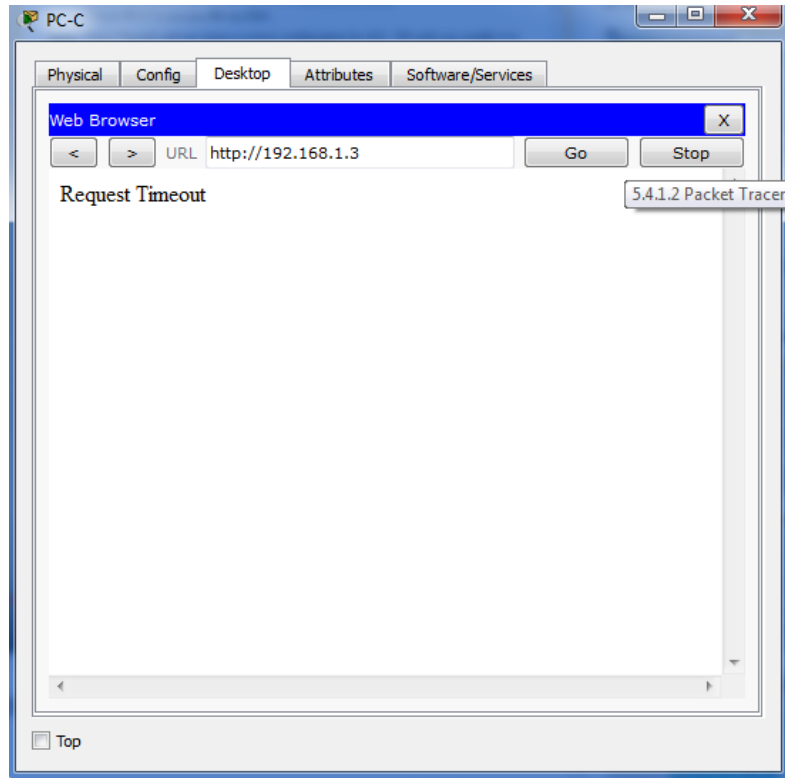


```

R1
Physical Config CLI Attributes
IOS Command Line Interface
line vty 0 4
password 7 0822455D0A1613030B1B0D517F
login local
transport input ssh
!
!
ntp update-calendar
!
end

R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#exit
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq
domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq
smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host
10.1.1.1 eq 22
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 120 in
R1(config-if)#
Copy Paste
Top
  
```

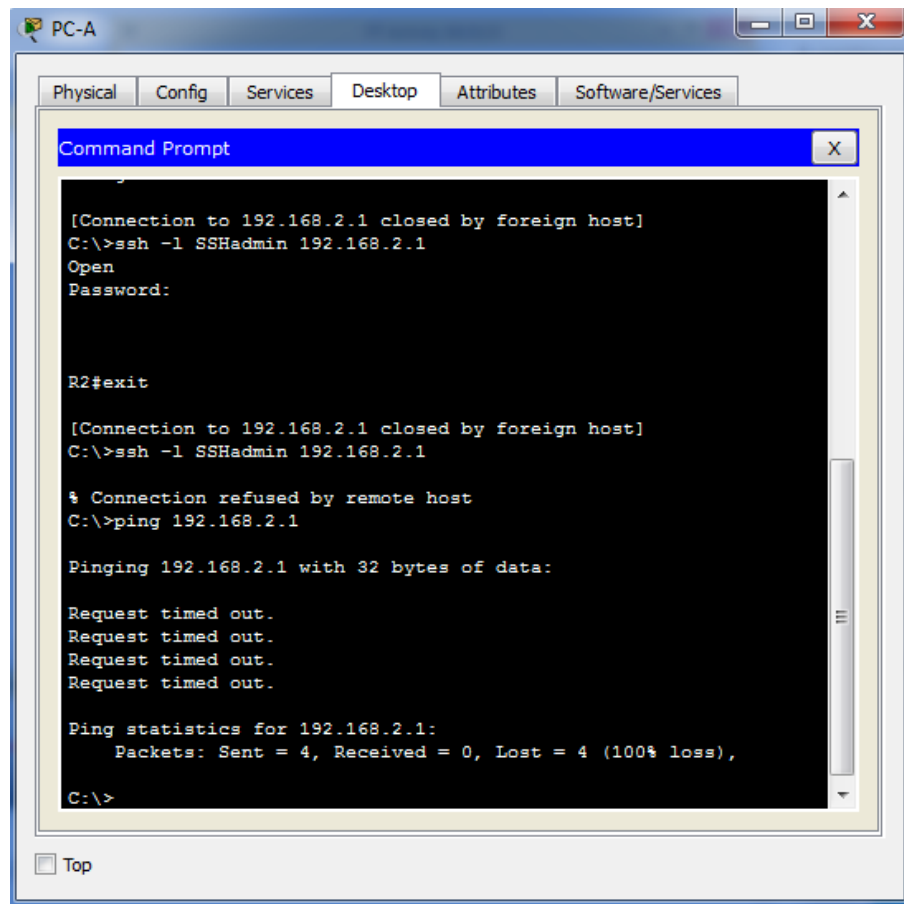
**Step 4:** Verify that PC-C cannot access PC-A via HTTPS using the web browser.



#### 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.



```
PC-A
Physical Config Services Desktop Attributes Software/Services
Command Prompt
[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l SSHAdmin 192.168.2.1
Open
Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l SSHAdmin 192.168.2.1

% Connection refused by remote host
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

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

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

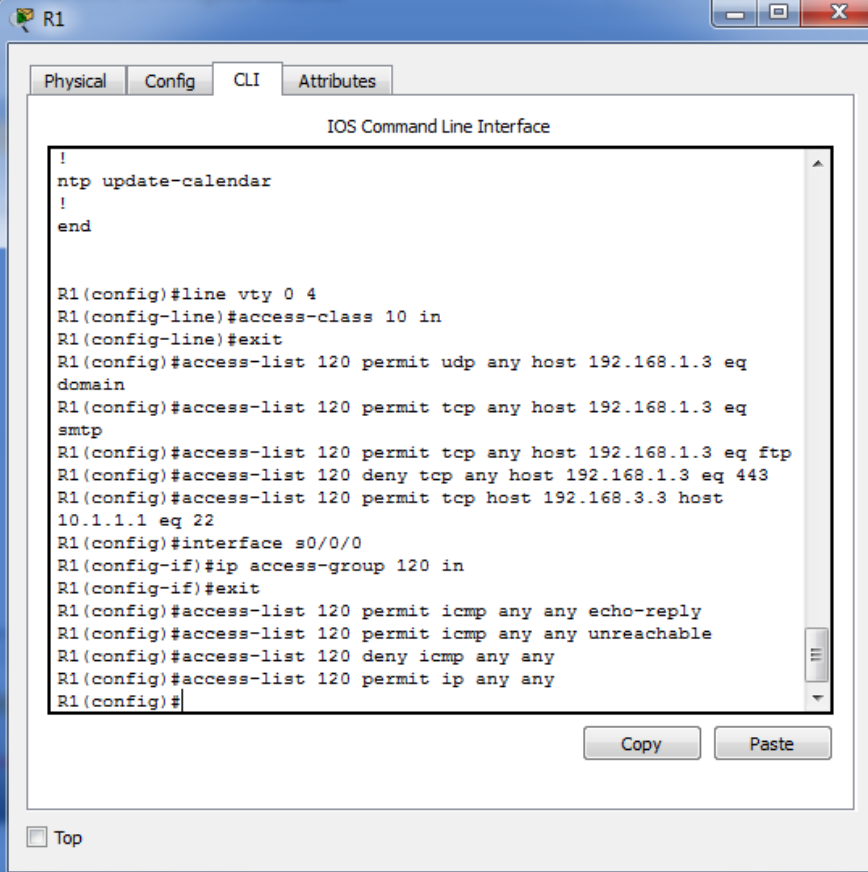
Use the `access-list` command to create a numbered IP ACL.

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

```
R1(config)# access-list 120 permit icmp any any unreachable
```

```
R1(config)# access-list 120 deny icmp any any
```

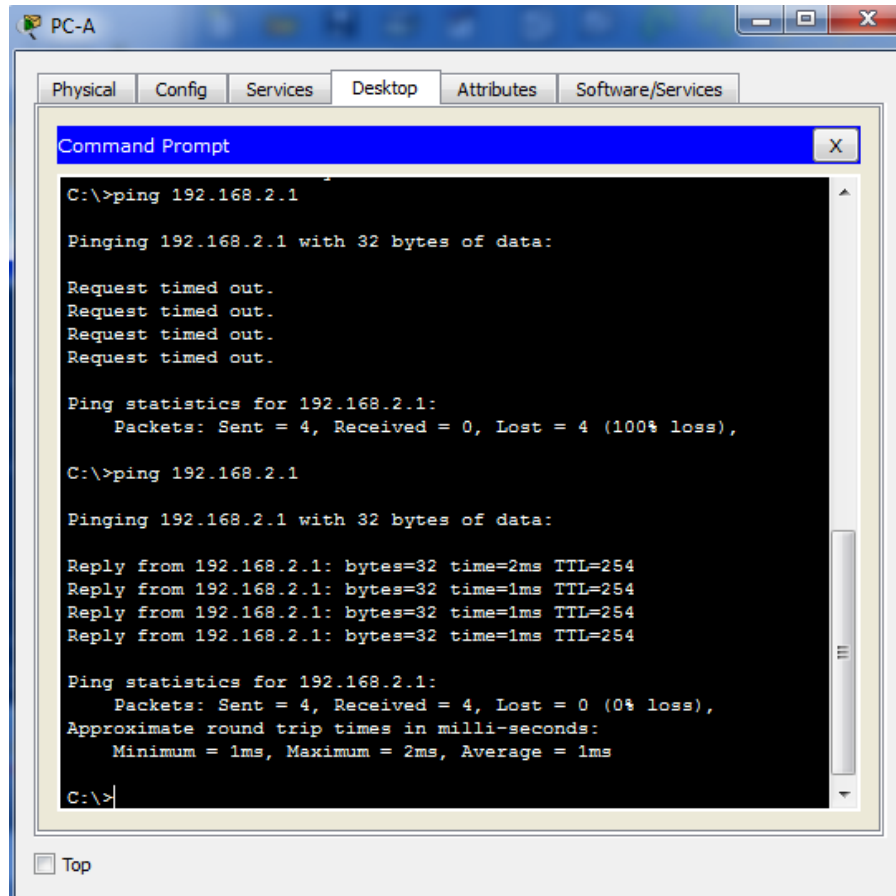
```
R1(config)# access-list 120 permit ip any any
```



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
!
ntp update-calendar
!
end

R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#exit
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq
domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq
smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host
10.1.1.1 eq 22
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 120 in
R1(config-if)#exit
R1(config)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#
```

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



```

PC-A
Physical Config Services Desktop Attributes Software/Services
Command Prompt
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

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

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

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

C:\>
  
```

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

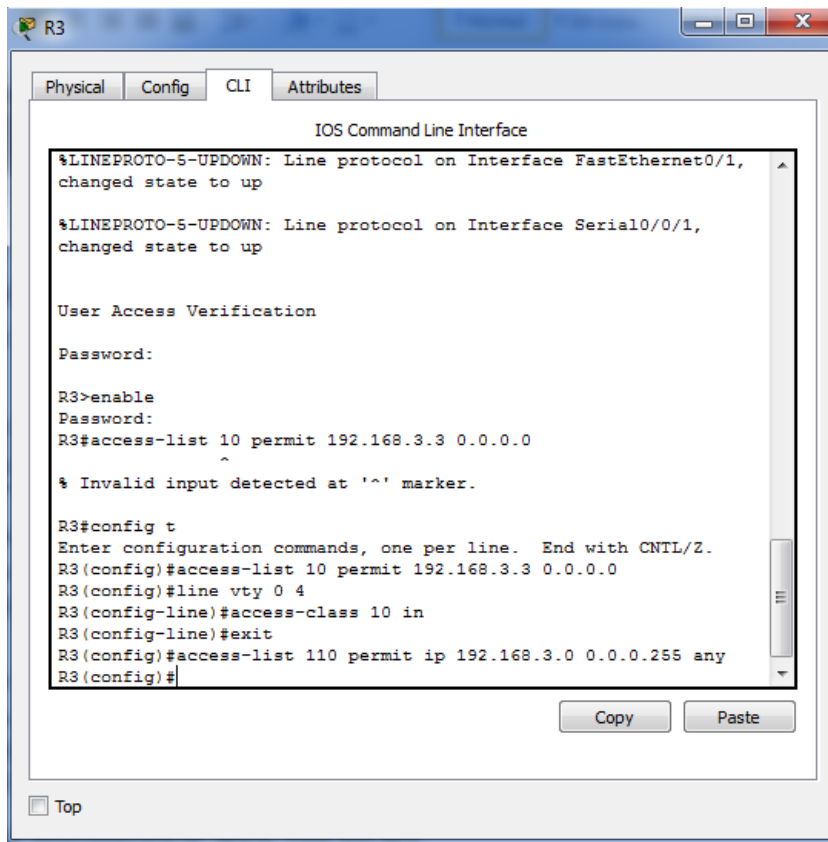
Deny all outbound packets with source address outside the range of internal IP addresses on **R3**.

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

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

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



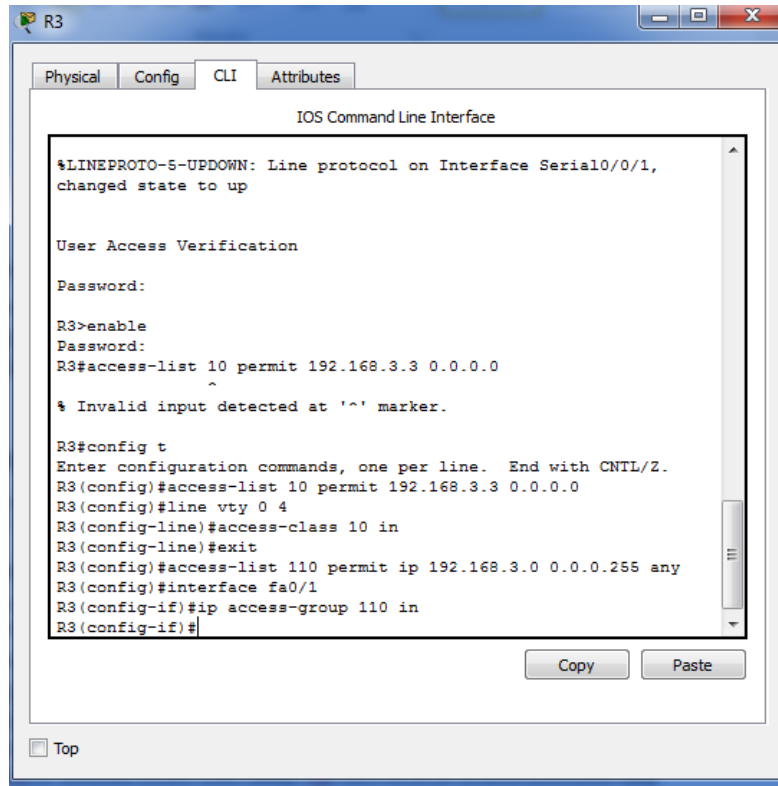


**Step 2: Apply the ACL to interface F0/1.**

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

```
R3(config)# interface fa0/1
```

```
R3(config-if)# ip access-group 110 in
```



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

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

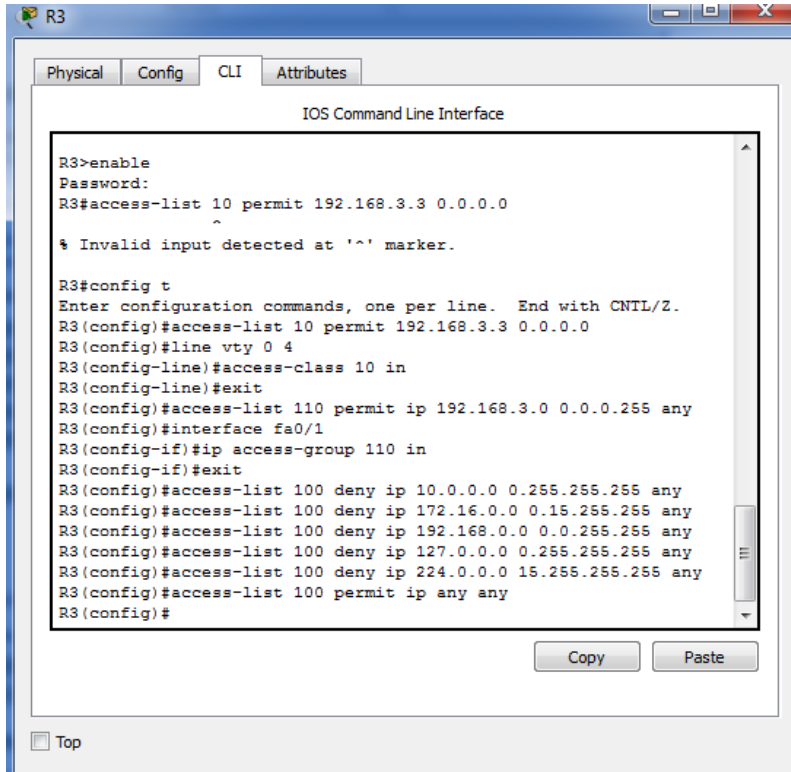
**Step 1: Configure ACL 100 to block all specified traffic from the outside network.**

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

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

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

R3(config)# **access-list 100 permit ip any any**



```

R3>enable
Password:
R3#access-list 10 permit 192.168.3.3 0.0.0.0
^
% Invalid input detected at '^' marker.

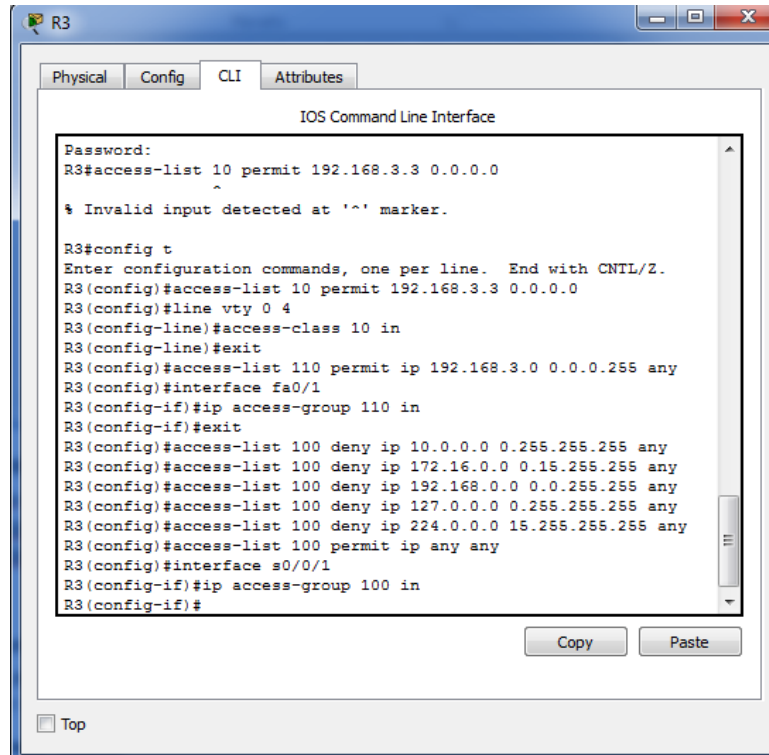
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#exit
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#
  
```

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

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

R3(config)# **interface s0/0/1**

R3(config-if)# **ip access-group 100 in**

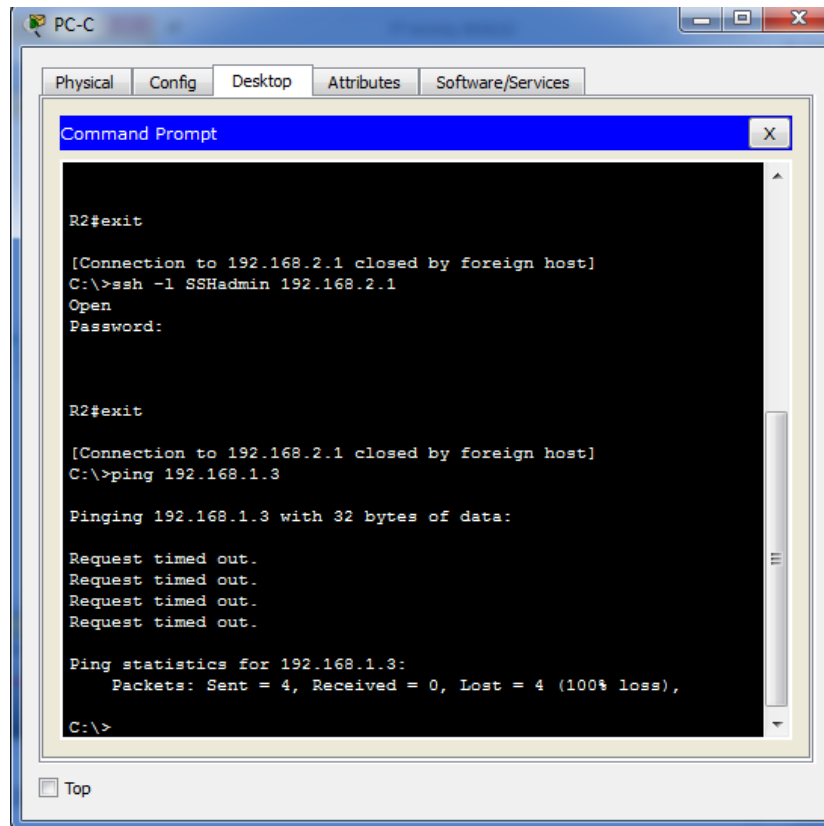


```

R3
Physical Config CLI Attributes
IOS Command Line Interface
Password:
R3#access-list 10 permit 192.168.3.3 0.0.0.0
^
Invalid input detected at '^' marker.
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#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
R3(config-if)#exit
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#
Copy Paste
Top
  
```

**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.

**!!!Script for R1**

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

```
access-class 10 in
```

```
access-list 120 permit udp any host 192.168.1.3 eq domain access-list 120
permit tcp any host 192.168.1.3 eq smtp access-list 120 permit tcp any
```



```
host 192.168.1.3 eq ftp access-list 120 deny tcp any host 192.168.1.3 eq
```

```
443
```



## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

```
access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22 interface s0/0/0
```

```
ip access-group 120 in
```

```
access-list 120 permit icmp any any echo-reply access-list 120 permit icmp any any unreachable access-list 120 deny icmp any any
```

```
access-list 120 permit ip any any
```

### !!!Script for R2

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

```
access-class 10 in
```

### !!!Script for R3

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

```
access-class 10 in
```

```
access-list 100 deny ip 10.0.0.0 0.255.255.255 any access-list 100 deny ip 172.16.0.0 0.15.255.255 any access-list 100 deny ip 192.168.0.0 0.0.255.255 any access-list 100 deny ip 127.0.0.0 0.255.255.255 any access-list 100 deny ip 224.0.0.0 15.255.255.255 any access-list 100 permit ip any any
```

```
interface s0/0/1
```

```
ip access-group 100 in
```

```
access-list 110 permit ip 192.168.3.0 0.0.0.255 any interface fa0/1
```

```
ip access-group 110 in
```



# UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

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		0	Other
Serial0/0/0		0	Other
Access-grou...	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
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

Score : 23/23  
Item Count : 23/23

Component	Items/Total	Score
ACL	23/23	23/23

Close

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)
R3			
ACL			
10	Correct	1	ACL
100	Correct	1	ACL
110	Correct	1	ACL
Ports		0	Other
FastEthernet0/1		0	Other
Access-grou...	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
VTY Line 3		0	Physical
Access Cont...	Correct	1	ACL
VTY Line 4		0	Physical
Access Cont...	Correct	1	ACL

Score : 23/23  
Item Count : 23/23

Component	Items/Total	Score
ACL	23/23	23/23

Close



Topología

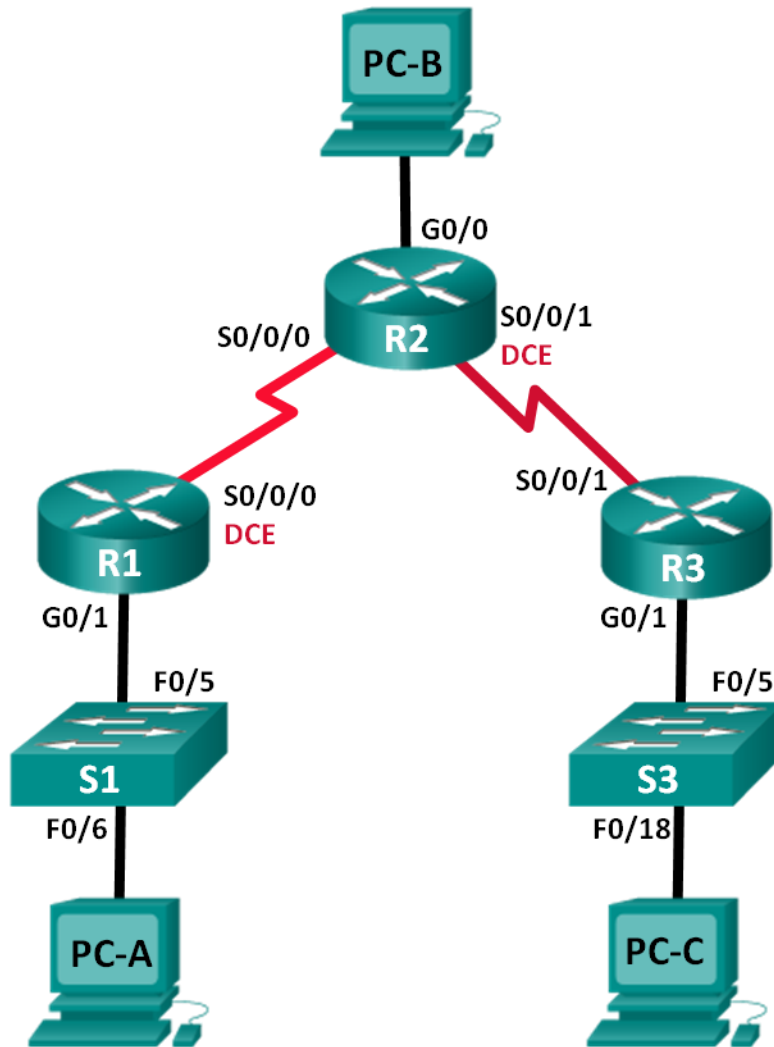


Tabla de direccionamiento

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

### Objetivos

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

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

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

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

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



## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

### Información básica/situación

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

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

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

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

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

### Recursos necesarios

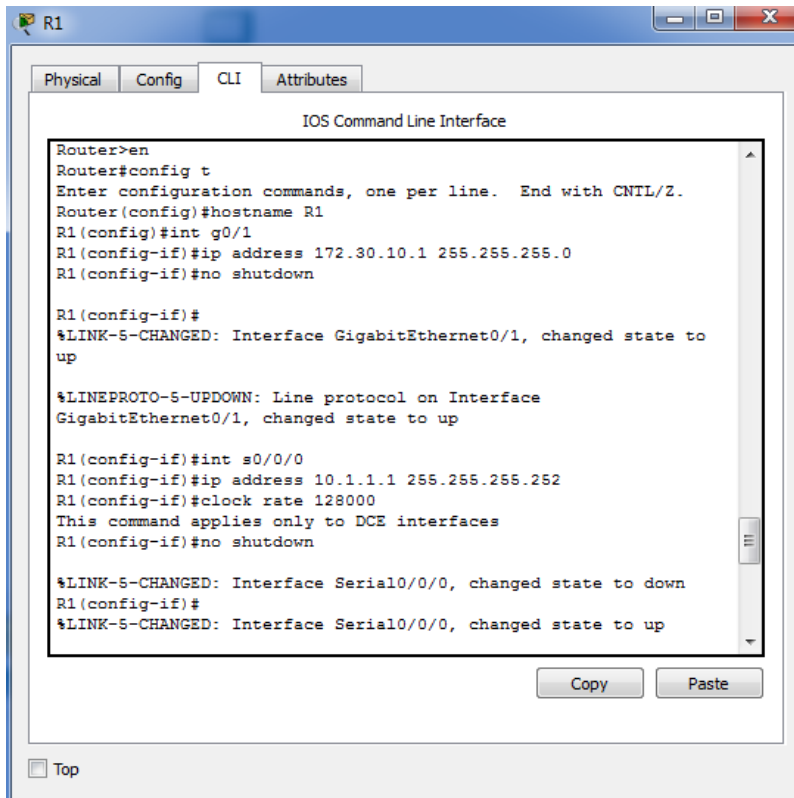
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

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

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



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



```
Router>en
Router#config 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 172.30.10.1 255.255.255.0
R1(config-if)#no shutdown

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

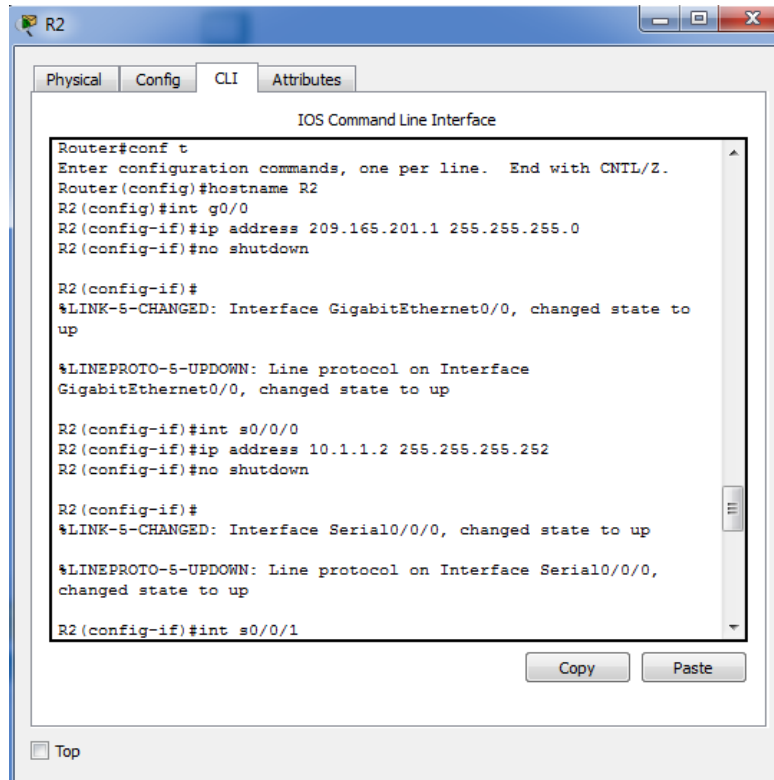
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R1(config-if)#int s0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#no shutdown

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

Copy Paste

Top



R2

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int g0/0
R2(config-if)#ip address 209.165.201.1 255.255.255.0
R2(config-if)#no shutdown

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

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

R2(config-if)#int s0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown

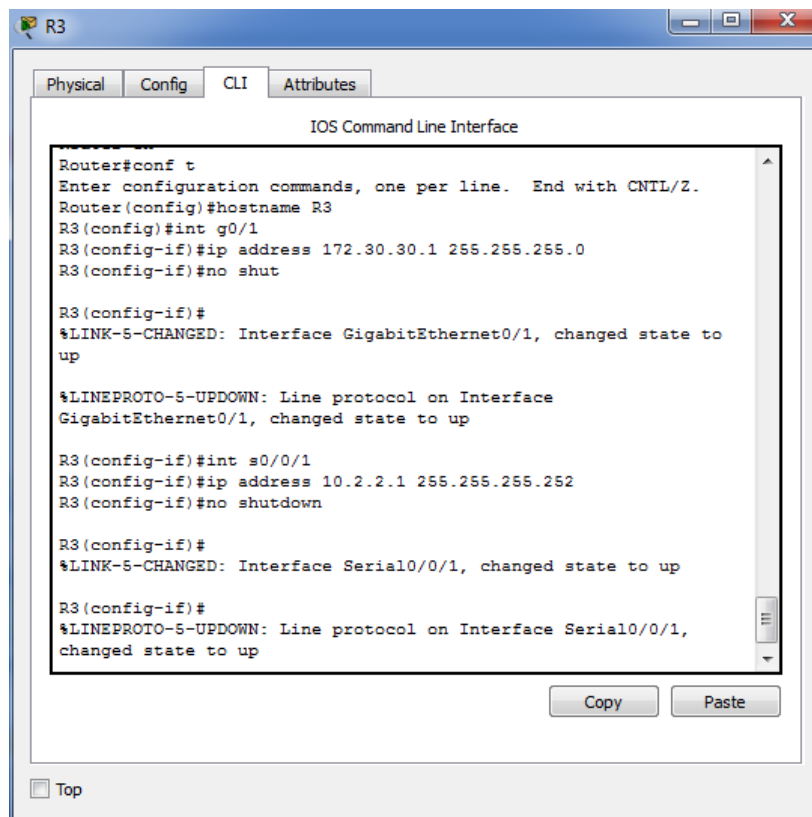
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

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

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

Copy Paste

Top



R3

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#int g0/1
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#no shut

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

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

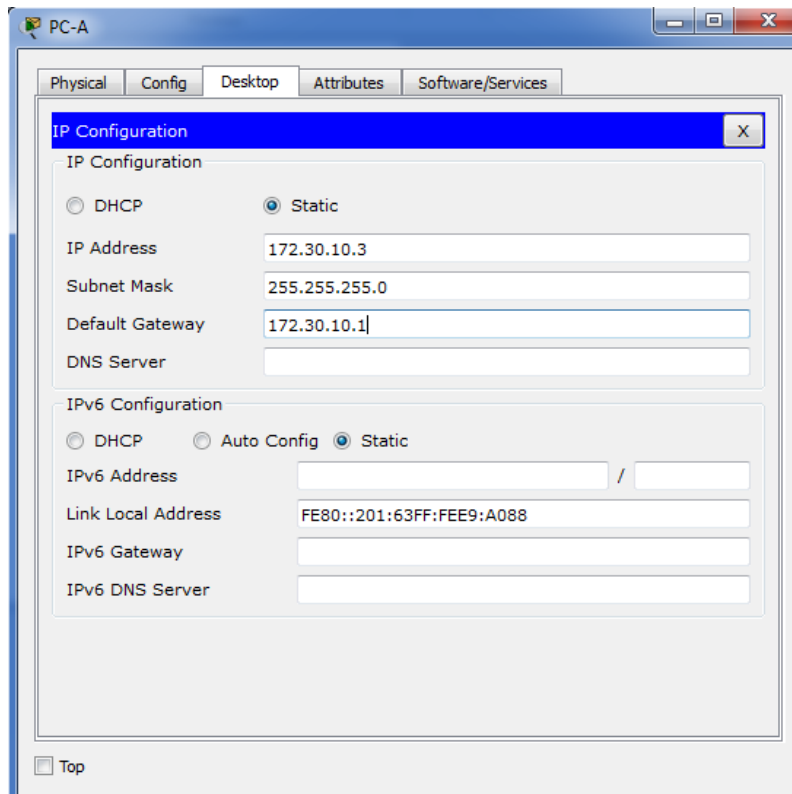
R3(config-if)#int s0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown

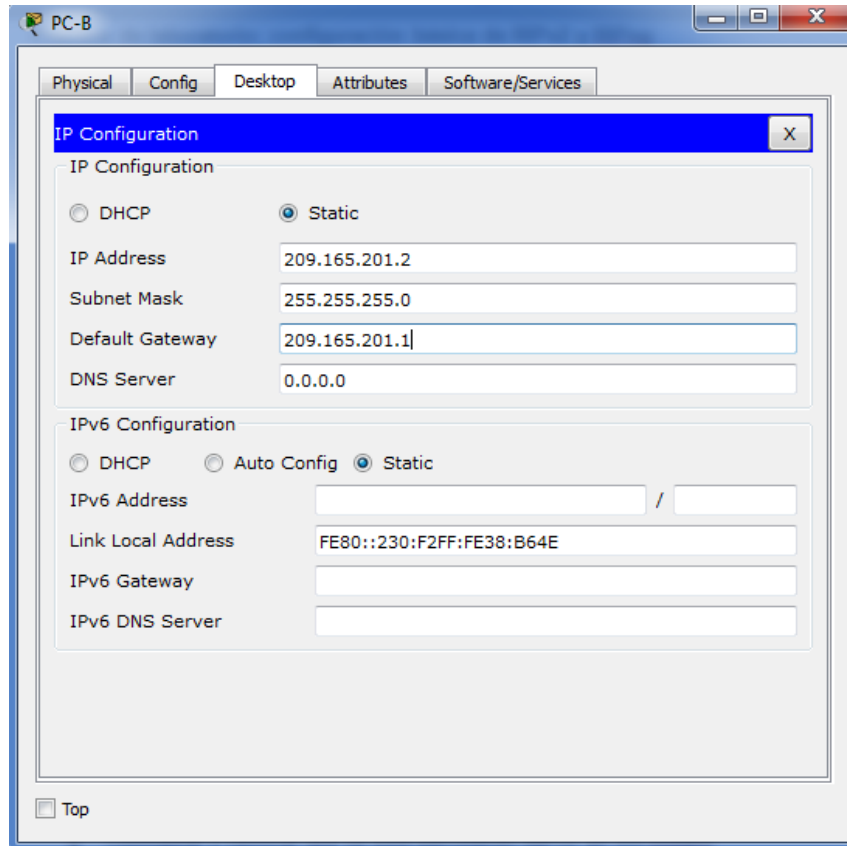
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

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

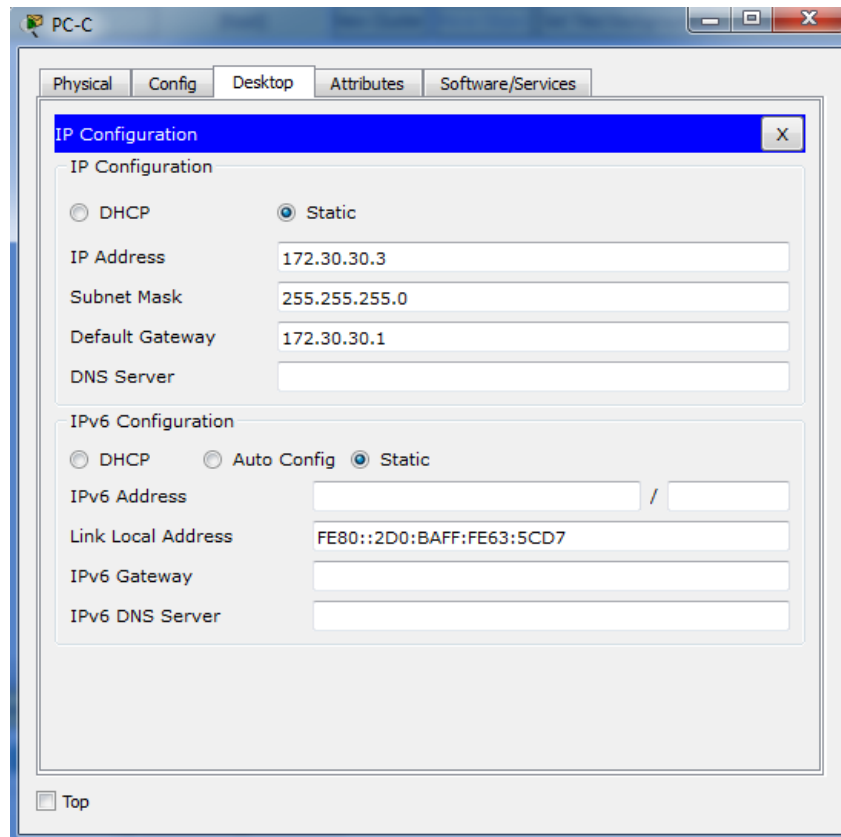
Copy Paste

Top



A screenshot of a Windows Network Configuration window titled 'PC-B'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Attributes', and 'Software/Services'. The 'Config' tab is active, showing 'IP Configuration' settings. The 'IP Configuration' section has a title bar with a close button. It contains two main sections: 'IP Configuration' and 'IPv6 Configuration'. In the 'IP Configuration' section, the 'Static' radio button is selected. The fields are: IP Address (209.165.201.2), Subnet Mask (255.255.255.0), Default Gateway (209.165.201.1), and DNS Server (0.0.0.0). In the 'IPv6 Configuration' section, the 'Static' radio button is selected. The fields are: IPv6 Address (empty), Link Local Address (FE80::230:F2FF:FE38:B64E), IPv6 Gateway (empty), and IPv6 DNS Server (empty). A 'Top' button is located at the bottom left of the window.





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

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

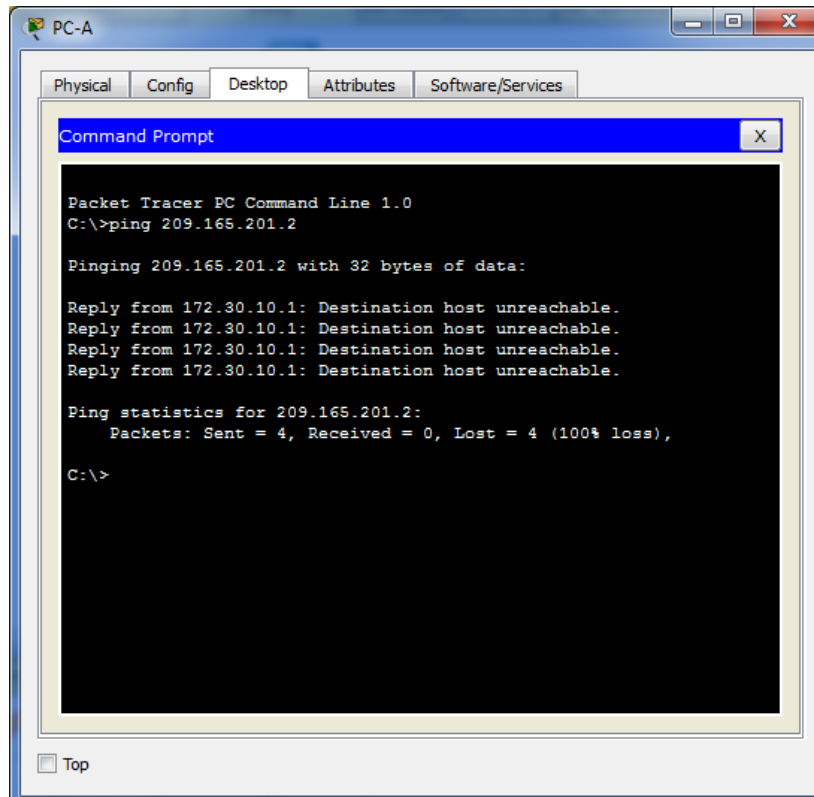
**Paso 4. configurar los equipos host.**

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.

- **Ping entre PC-A y PCB, no puede hacerse**



```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

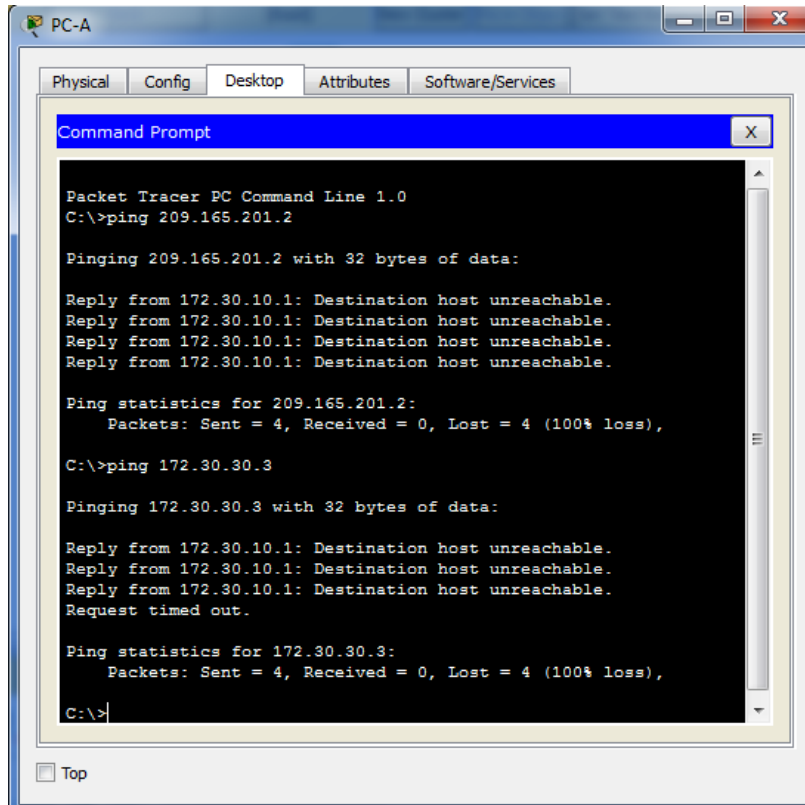
Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
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),

C:\>
```

- **Ping entre PC-A y PC-C, no puede hacerse**



```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
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),

C:\>ping 172.30.30.3

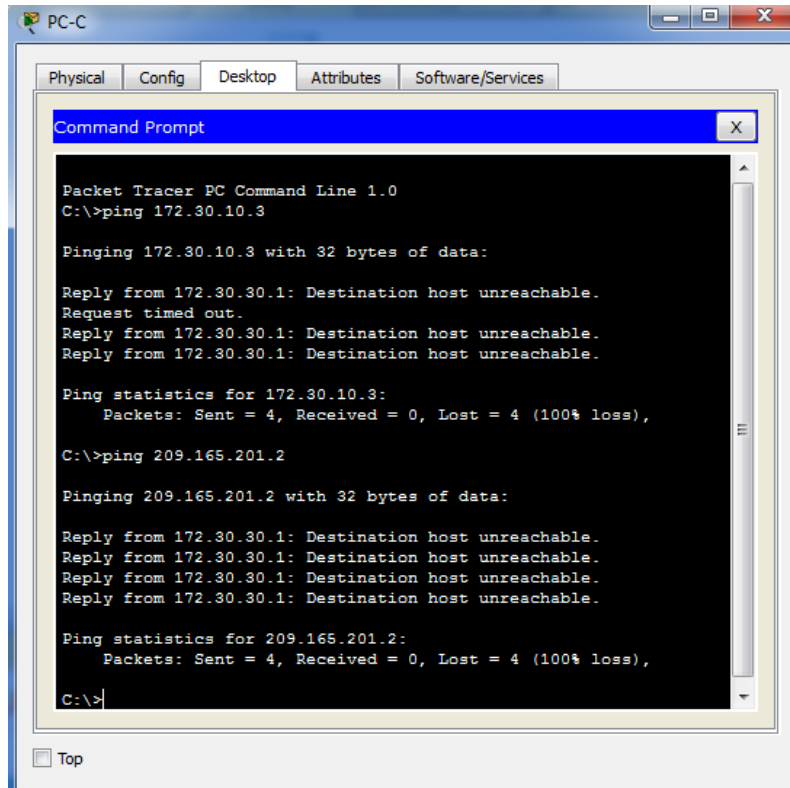
Pinging 172.30.30.3 with 32 bytes of data:

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

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

- Ping entre PC-C y PC-A y PC-B



```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Request timed out.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.201.2

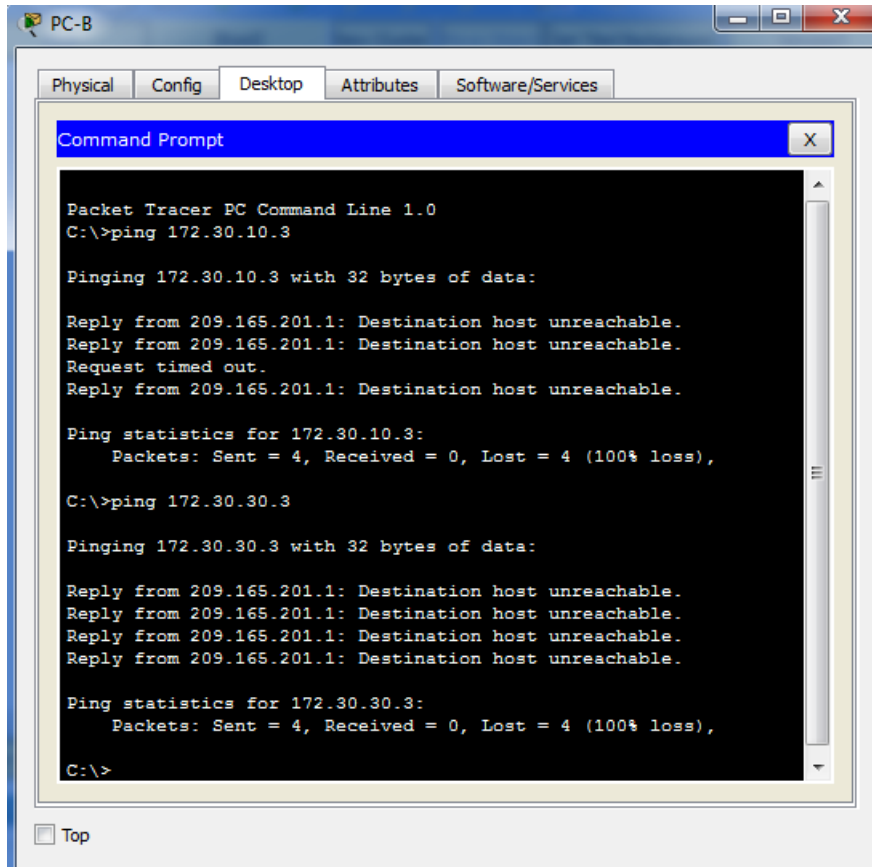
Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

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

C:\>
```

- Ping entre PC-B y PC-A y PC-C



```

PC-B
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 209.165.201.1: Destination host unreachable.
Reply from 209.165.201.1: Destination host unreachable.
Request timed out.
Reply from 209.165.201.1: Destination host unreachable.

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

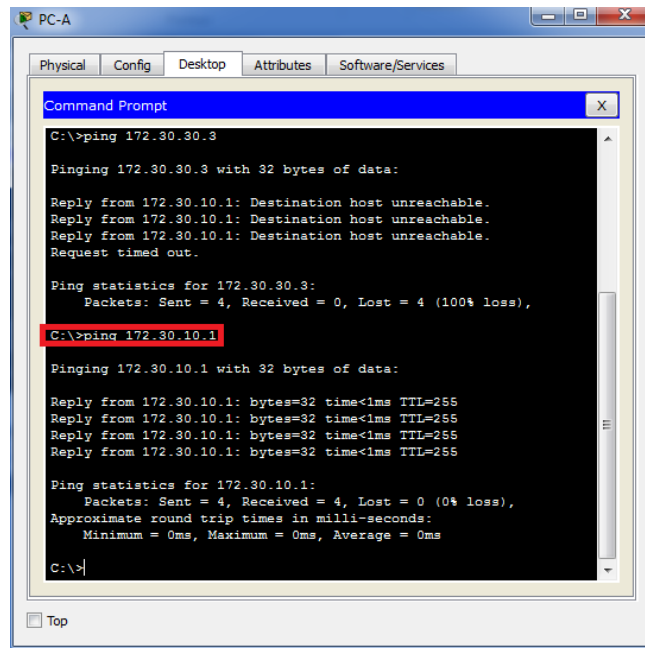
Reply from 209.165.201.1: Destination host unreachable.
Reply from 209.165.201.1: Destination host unreachable.
Reply from 209.165.201.1: Destination host unreachable.
Reply from 209.165.201.1: Destination host unreachable.

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
  
```

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

- Ping de PC-A a router 1



```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Request timed out.

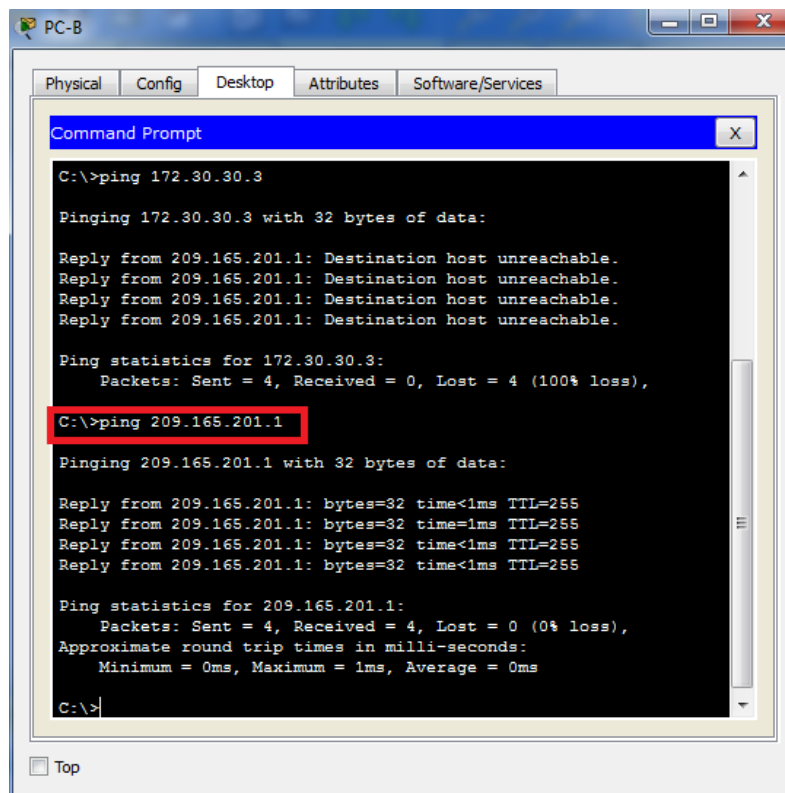
Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.30.10.1
Pinging 172.30.10.1 with 32 bytes of data:
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms 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

C:\>
```

- Ping de PC-B a router 2



```
PC-B
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 209.165.201.1: Destination host unreachable.
Reply from 209.165.201.1: Destination host unreachable.
Reply from 209.165.201.1: Destination host unreachable.
Reply from 209.165.201.1: Destination host unreachable.

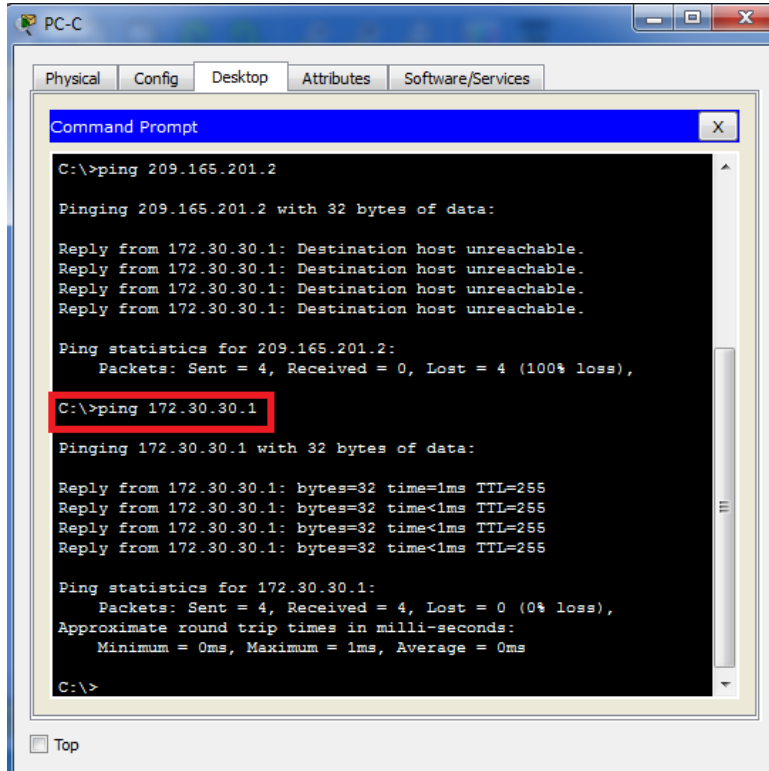
Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>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<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms 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

C:\>
```

- Ping de PC-C a router 3



```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

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

C:\>ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

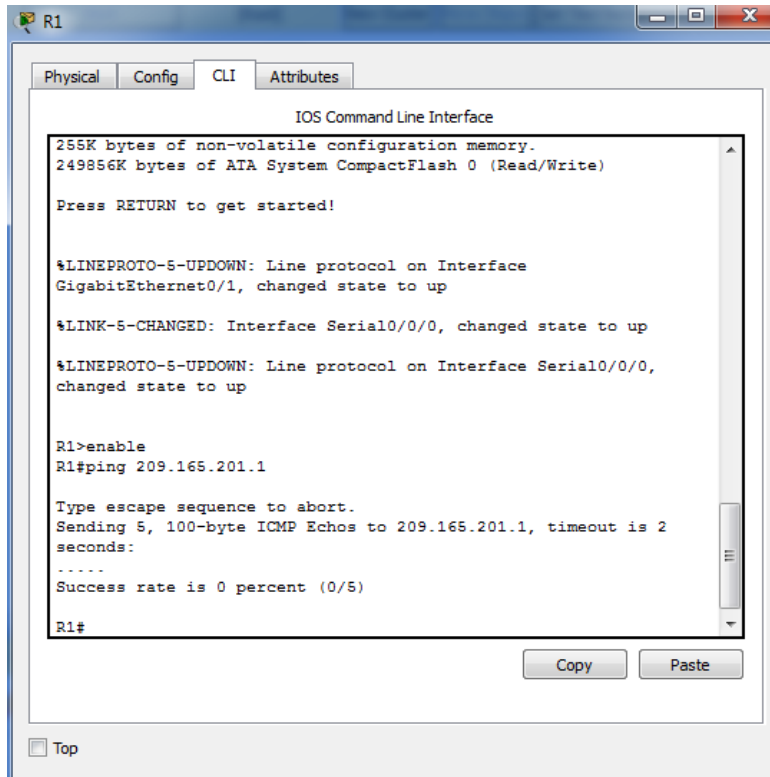
Reply from 172.30.30.1: bytes=32 time=1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

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

- Entre R1 y R2



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
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
GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

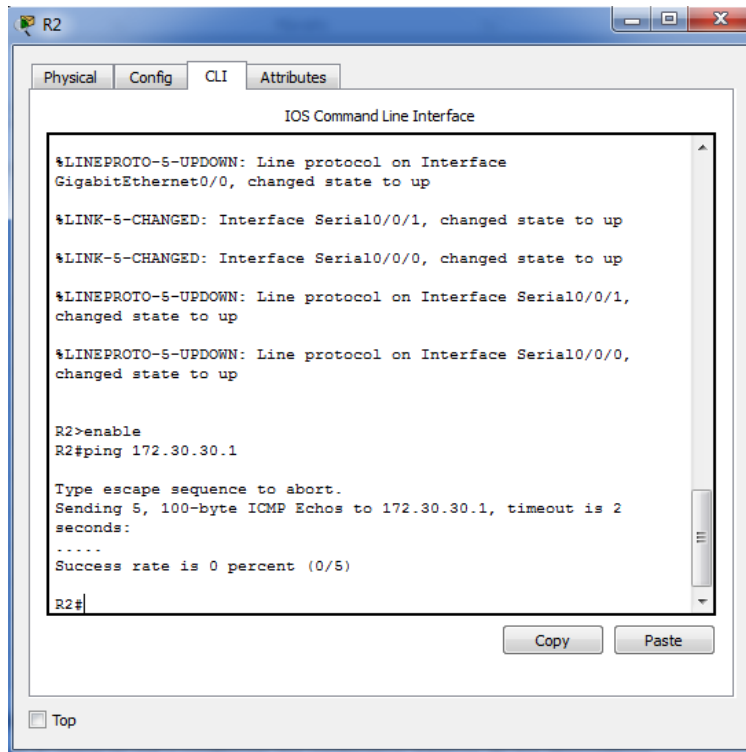
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

R1>enable
R1#ping 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

R1#
Copy Paste
Top
  
```

- Entre R2 y R3



```

R2
Physical Config CLI Attributes
IOS Command Line Interface

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

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/0, 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

R2>enable
R2#ping 172.30.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

R2#
Copy Paste
Top
  
```





## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

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

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

#### Paso 1. Configurar el enrutamiento RIPv2.

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

```
R1# config t
```

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

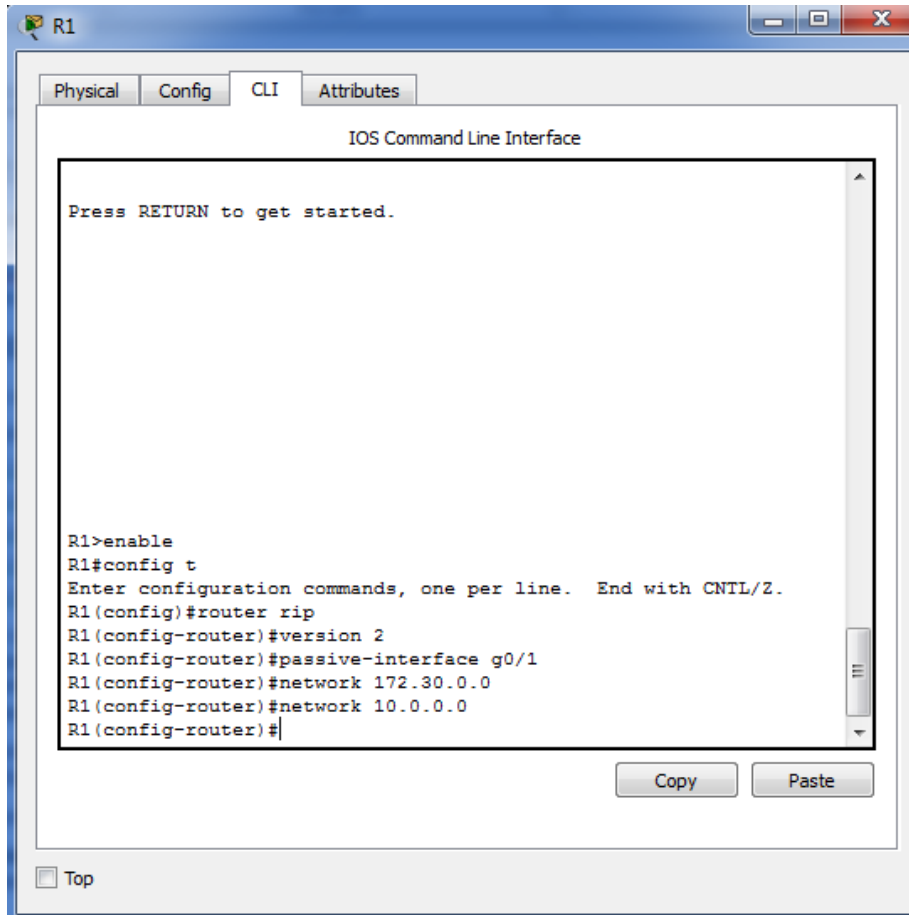
```
R1(config-router)# version 2
```

```
R1(config-router)# passive-interface g0/1
```

```
R1(config-router)# network 172.30.0.0
```

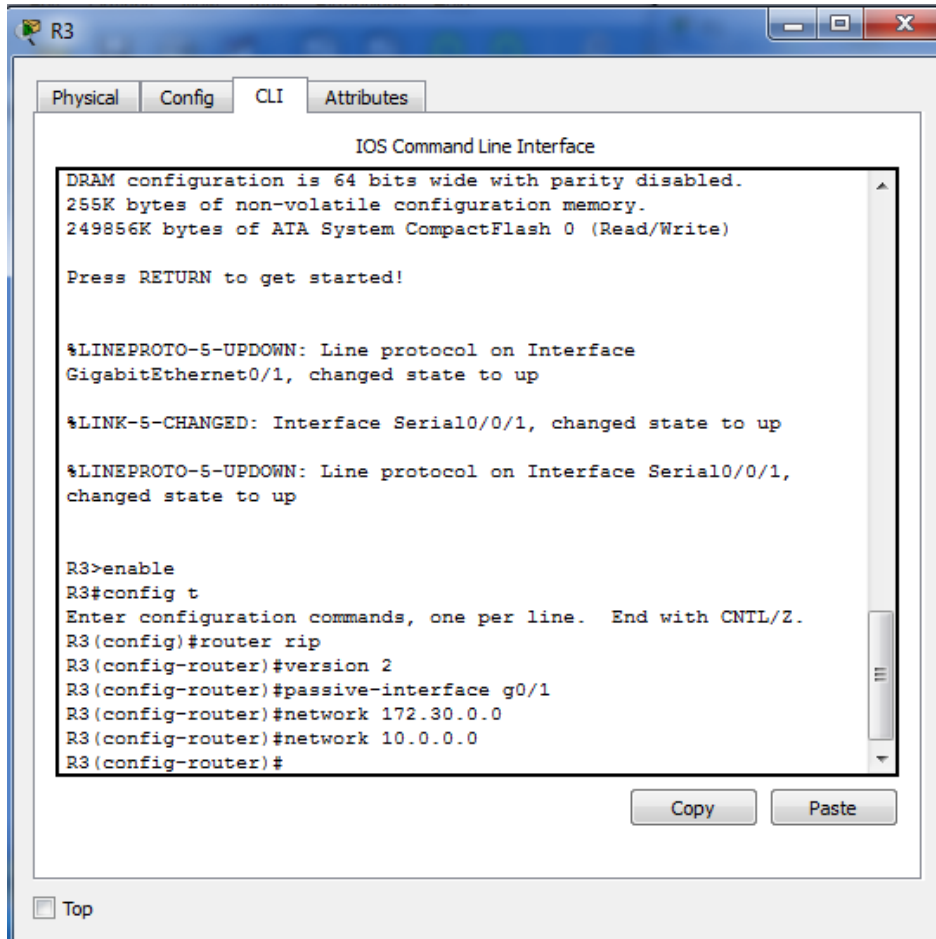
```
R1(config-router)# network 10.0.0.0
```

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



```
R1>enable
R1#config 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 Attributes
IOS Command Line Interface
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
GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

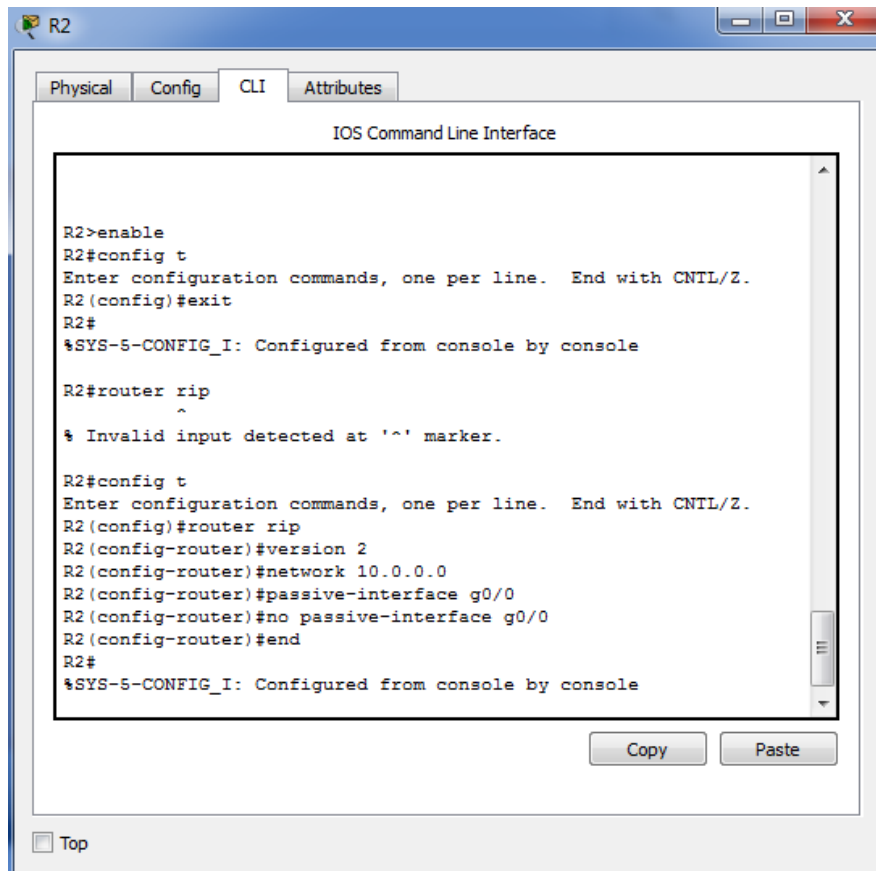
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

R3>enable
R3#config 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)#

Copy Paste
 Top
  
```

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

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

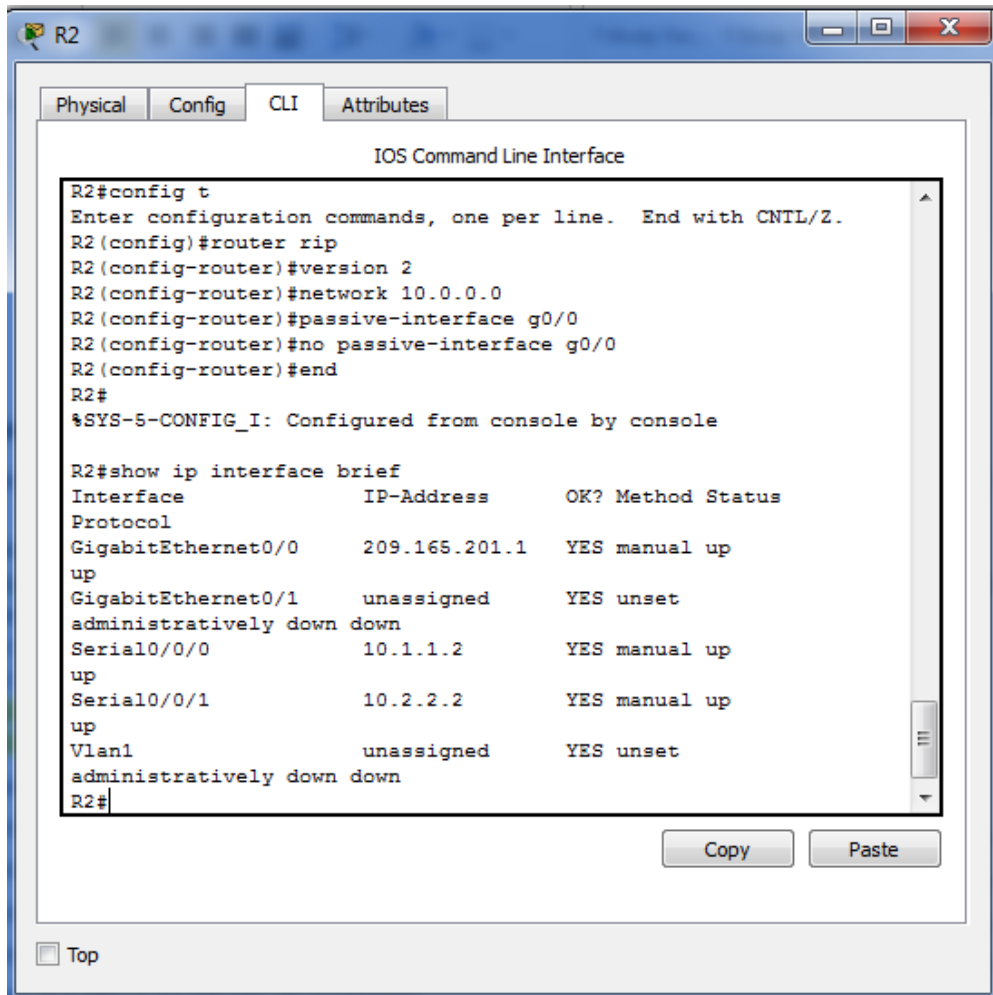


**Paso 2. examinar el estado actual de la red.**

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

R2# **show ip interface brief**

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



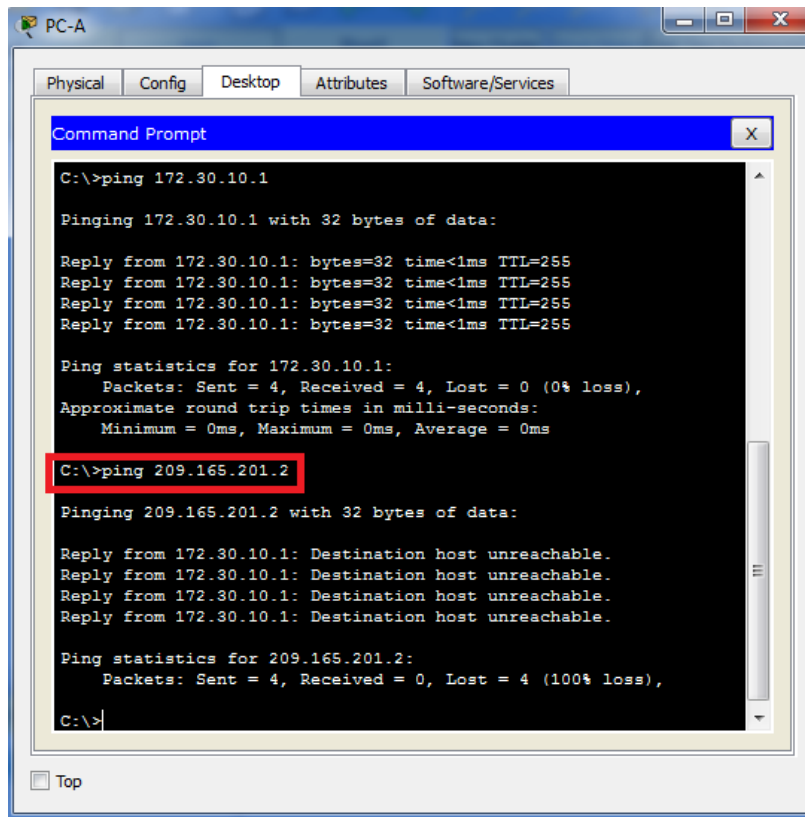
```

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#router rip
R2 (config-router)#version 2
R2 (config-router)#network 10.0.0.0
R2 (config-router)#passive-interface g0/0
R2 (config-router)#no passive-interface g0/0
R2 (config-router)#end
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? De R2 **no hay una ruta que llegue a PC-B o no está anunciando la ruta a PC-B, esta red no está participando en RIP**



```

PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:

Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms 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

C:\>ping 209.165.201.2

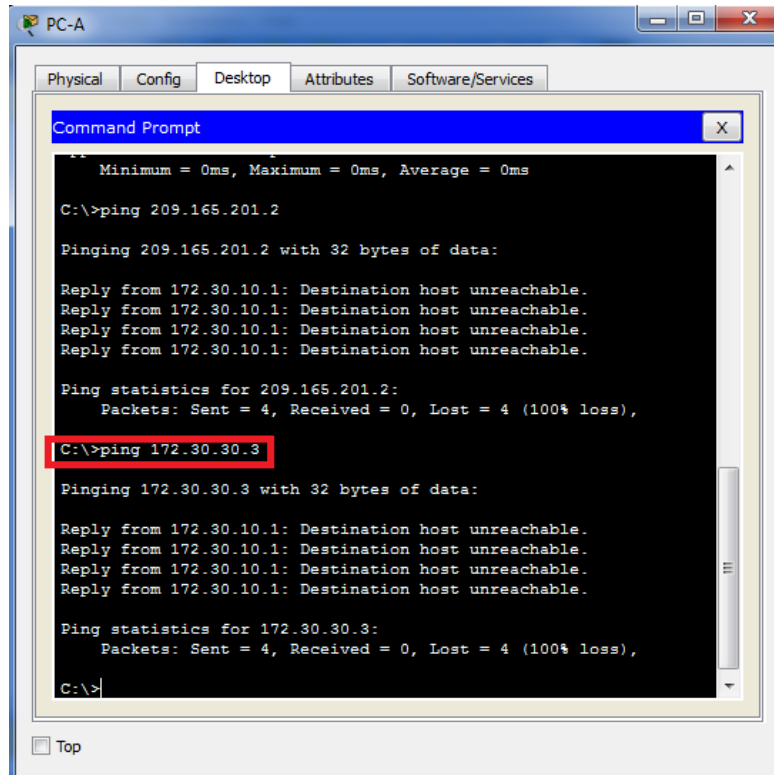
Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
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),

C:\>
  
```

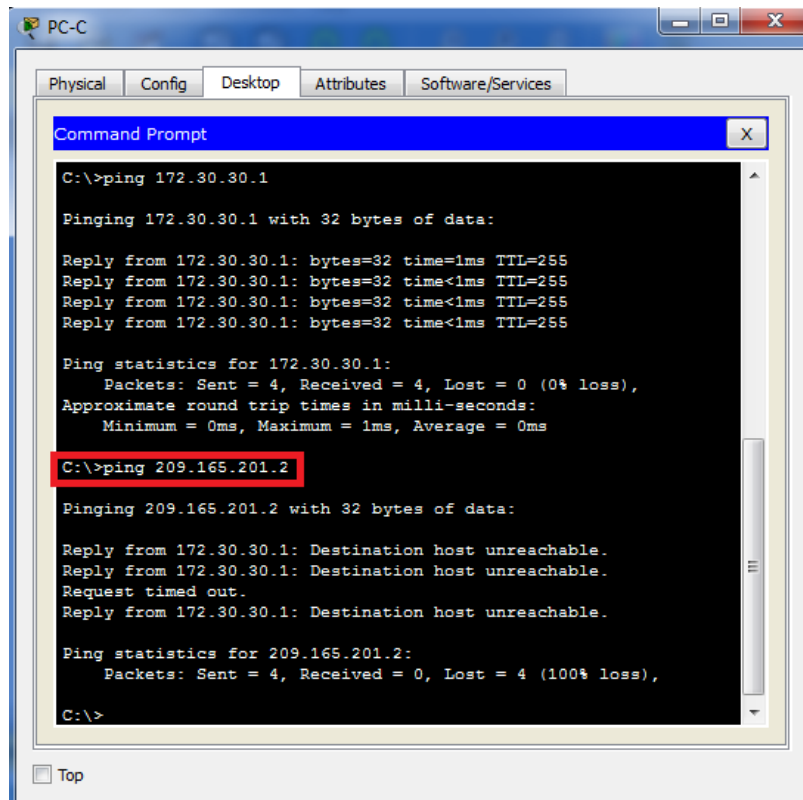
¿Es posible hacer ping de la PC-A a la PC-C? **No** ¿Por qué? **R1 y R3 no tienen rutas hacia la subred específica en el router remoto.**



```

PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
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),
C:\>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
  
```

¿Es posible hacer ping de la PC-C a la PC-B? **No** ¿Por qué? **no hay una ruta que llegue a PC-B o no está anunciando la ruta a PC-B, esta red no está participando en RIP**

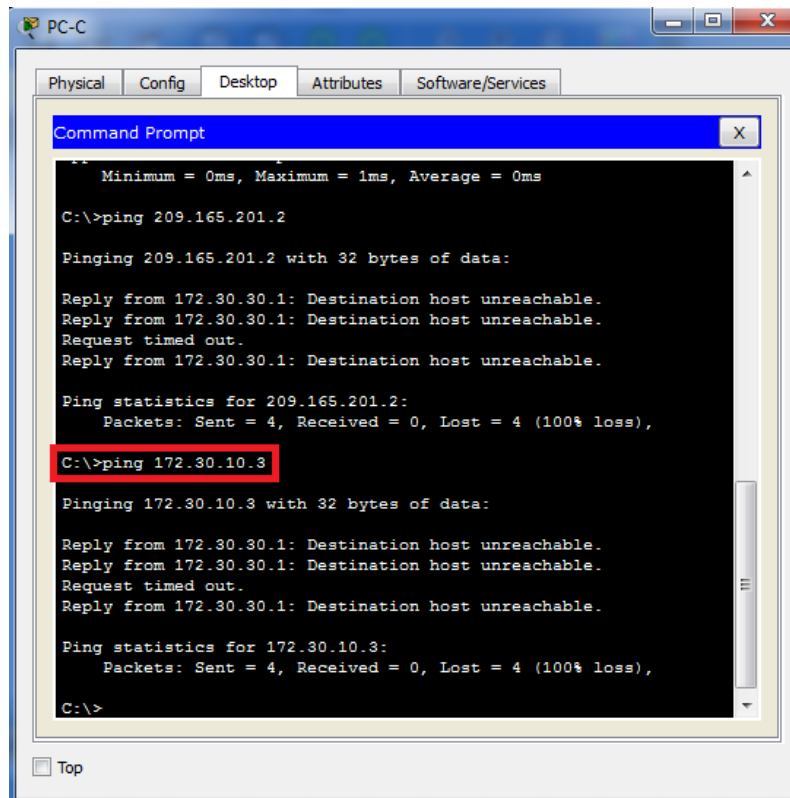


```

PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.1
Pinging 172.30.30.1 with 32 bytes of data:
Reply from 172.30.30.1: bytes=32 time=1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Request timed out.
Reply from 172.30.30.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
  
```

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





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			

Serial0/0/0 2 2

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

10.0.0.0

172.30.0.0

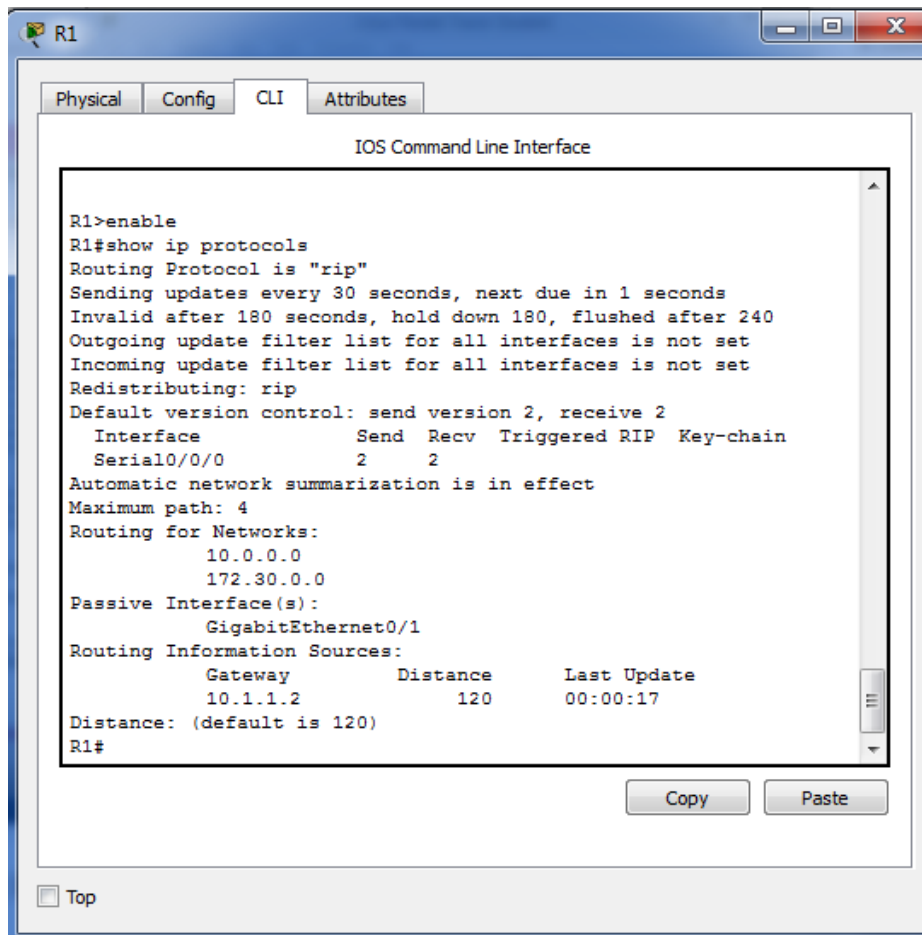
Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

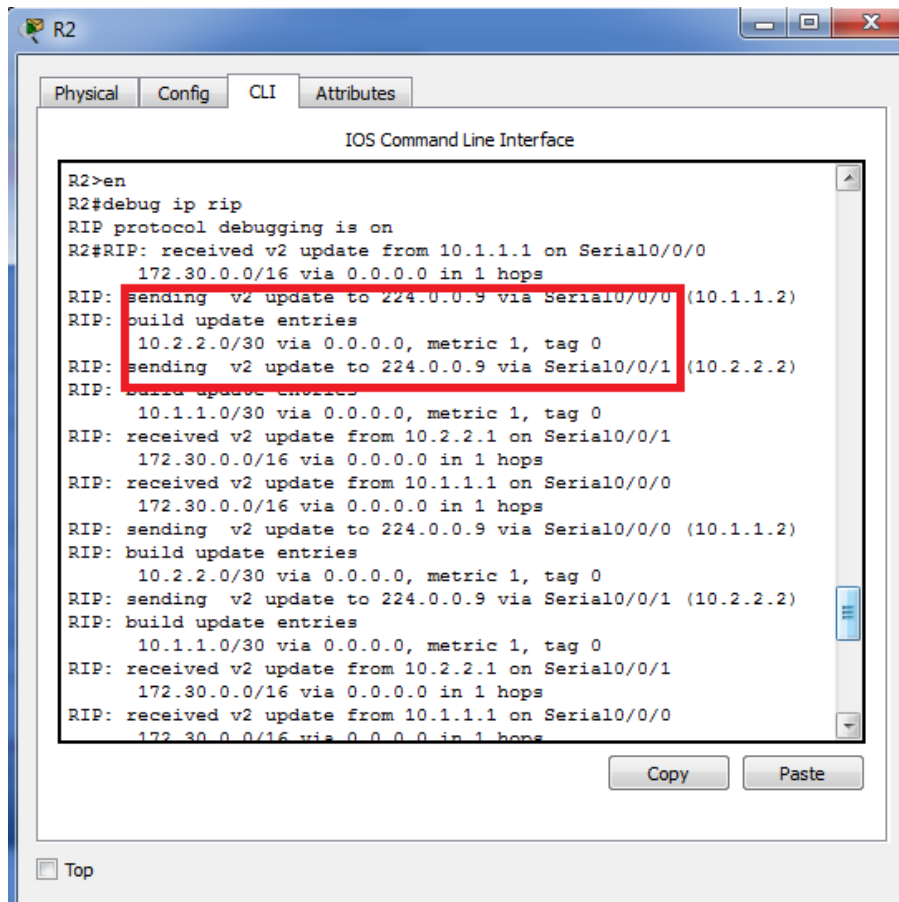
Gateway	Distance	Last Update
10.1.1.2	120	

Distance: (default is 120)



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

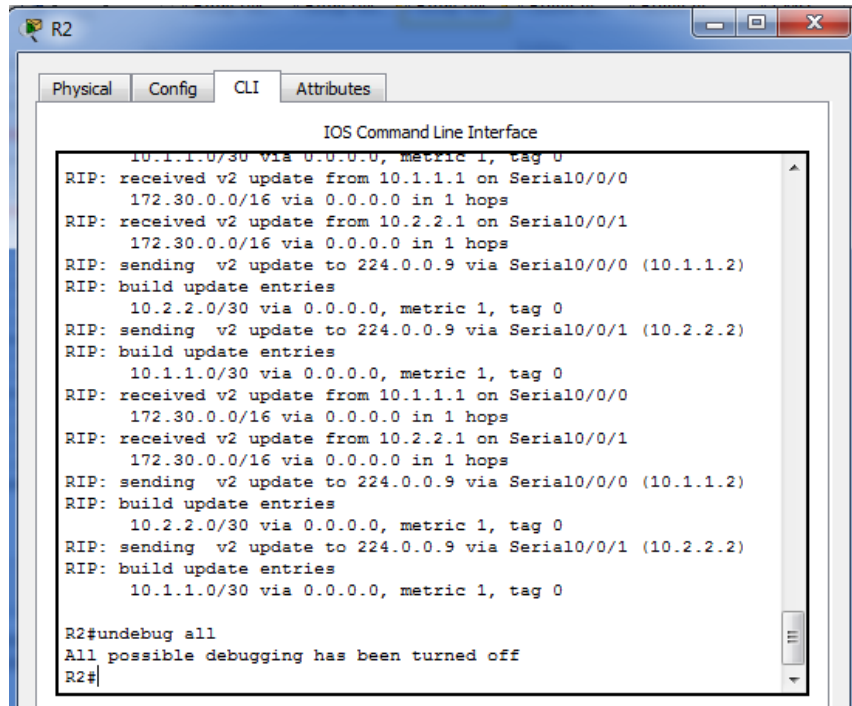
**Nos envía versión 2 por la dirección multicast 224.0.0.9 via serial 0/0/0 y via serial 0/0/1**



```

R2>en
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
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
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
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
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
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.



```

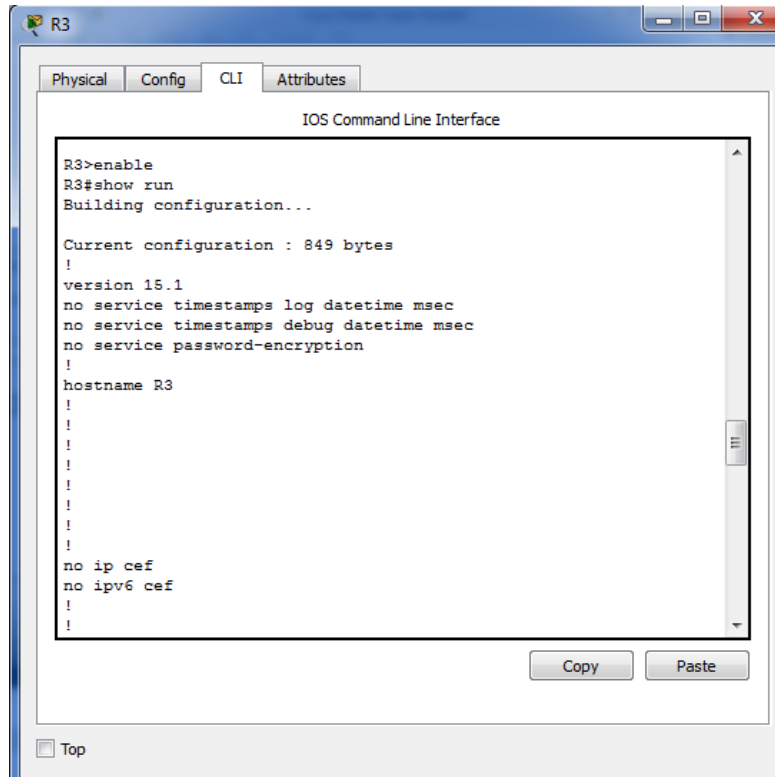
R2
Physical Config CLI Attributes
IOS Command Line Interface
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
    172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
    10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
    10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
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
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
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
    10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
    10.1.1.0/30 via 0.0.0.0, metric 1, tag 0

R2#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?

**Router rip**

**Versión 2**



R3

Physical Config CLI Attributes

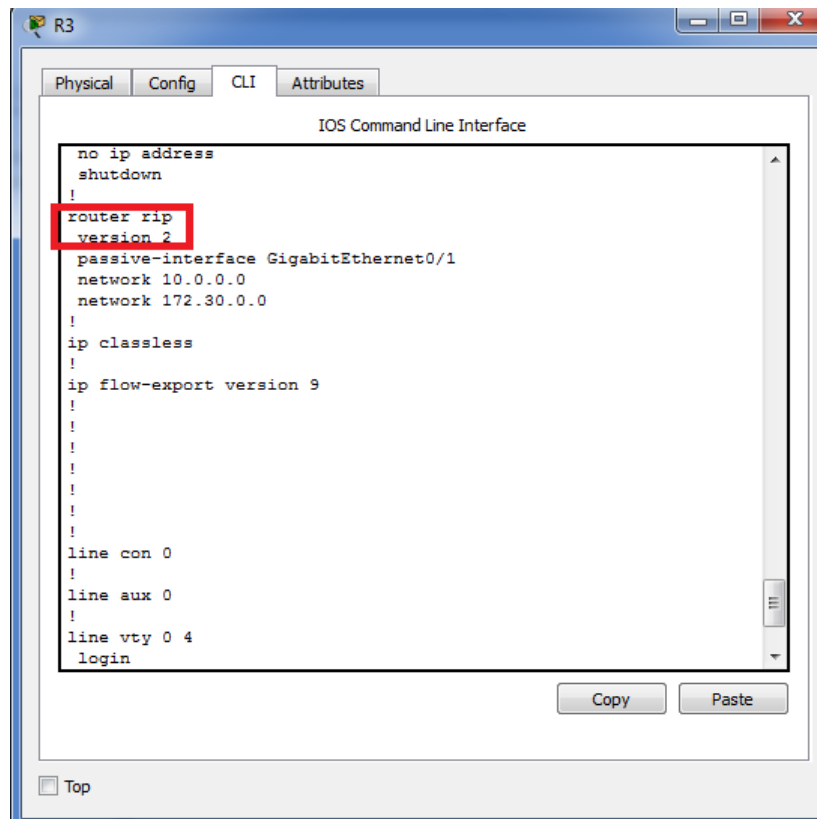
IOS Command Line Interface

```
R3>enable
R3#show run
Building configuration...

Current configuration : 849 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
```

Copy Paste

Top



R3

Physical Config CLI Attributes

IOS Command Line Interface

```
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
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
```

Copy Paste

Top

d. Examinar el sumarización automática de las rutas.

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

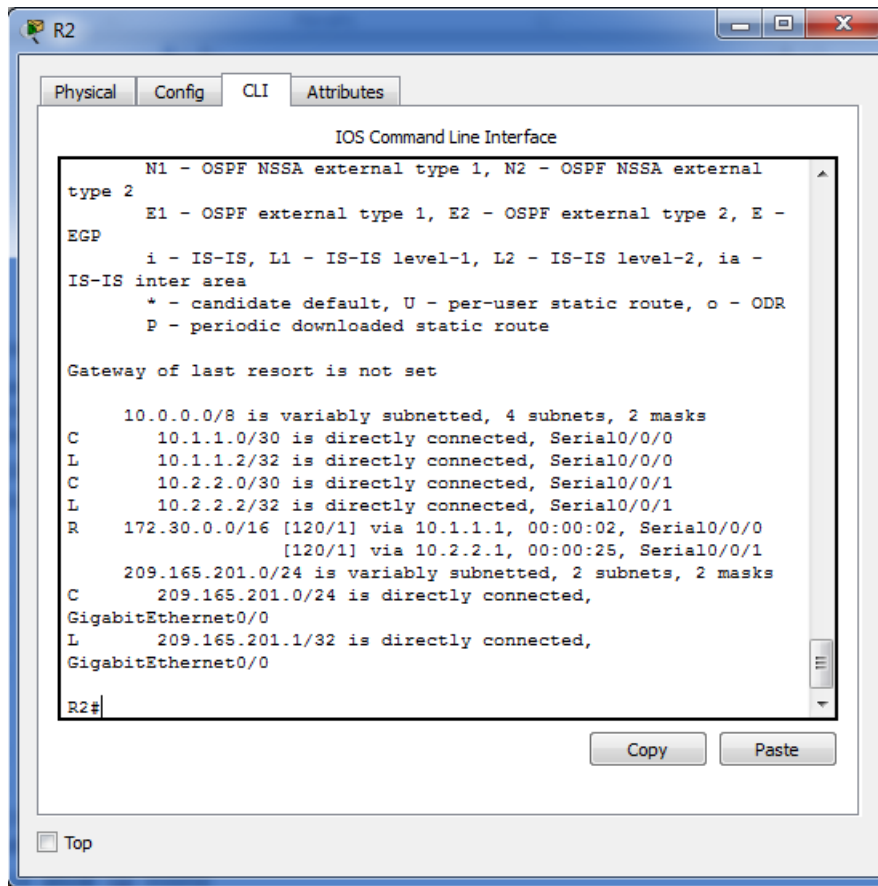
R2# show ip route

<Output Omitted>

- ```

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

```



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

R1# **show ip route**

<Output Omitted>

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

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

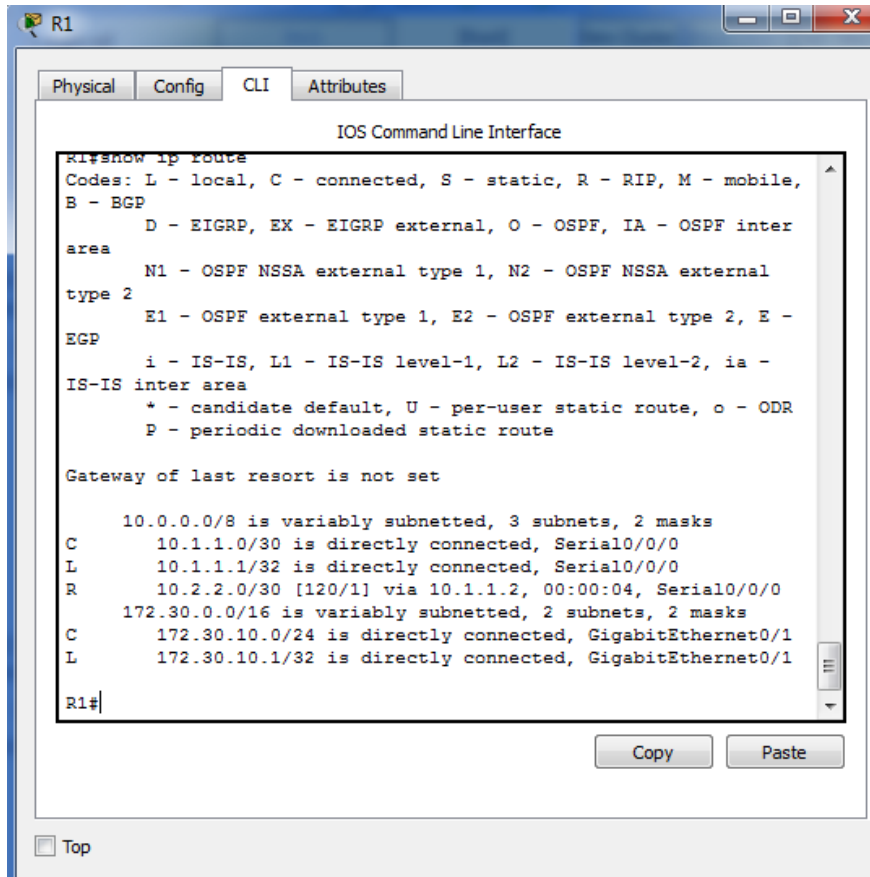
L 10.1.1.1/32 is directly connected, Serial0/0/0

R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0

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

C 172.30.10.0/24 is directly connected, GigabitEthernet0/1

L 172.30.10.1/32 is directly connected, GigabitEthernet0/1



```

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, 00:00:04, 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#
  
```

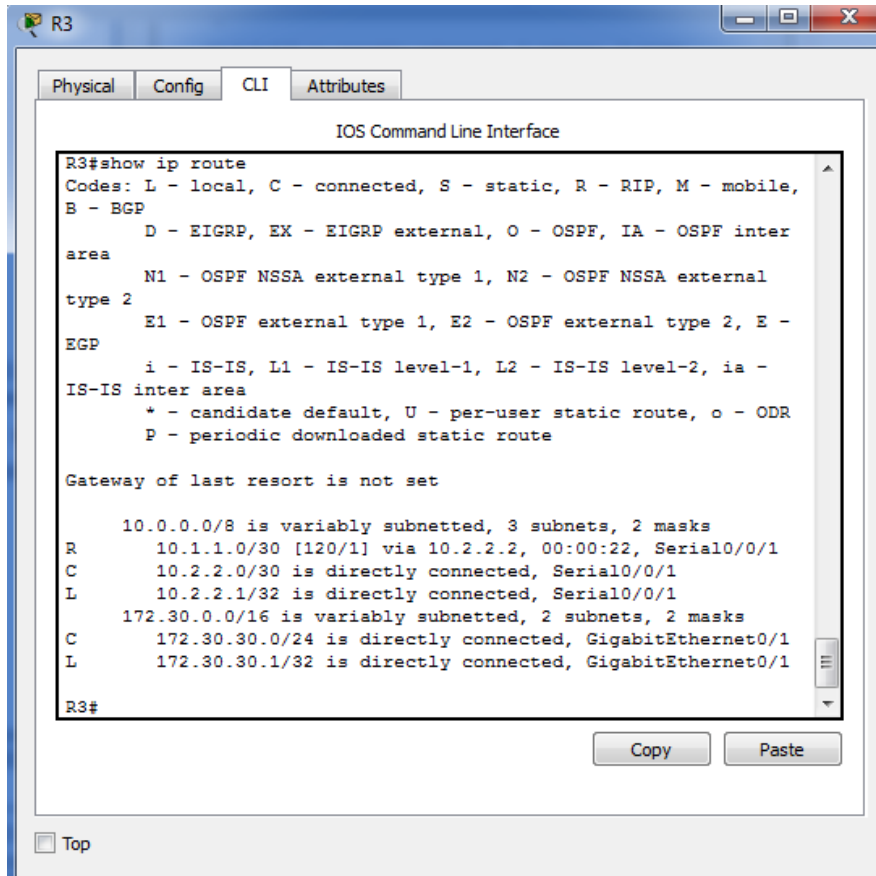
El R3 solo muestra sus propias subredes para la red 172.30.0.0. El R3 no tiene ninguna ruta para las subredes 172.30.0.0 en el R1.

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#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

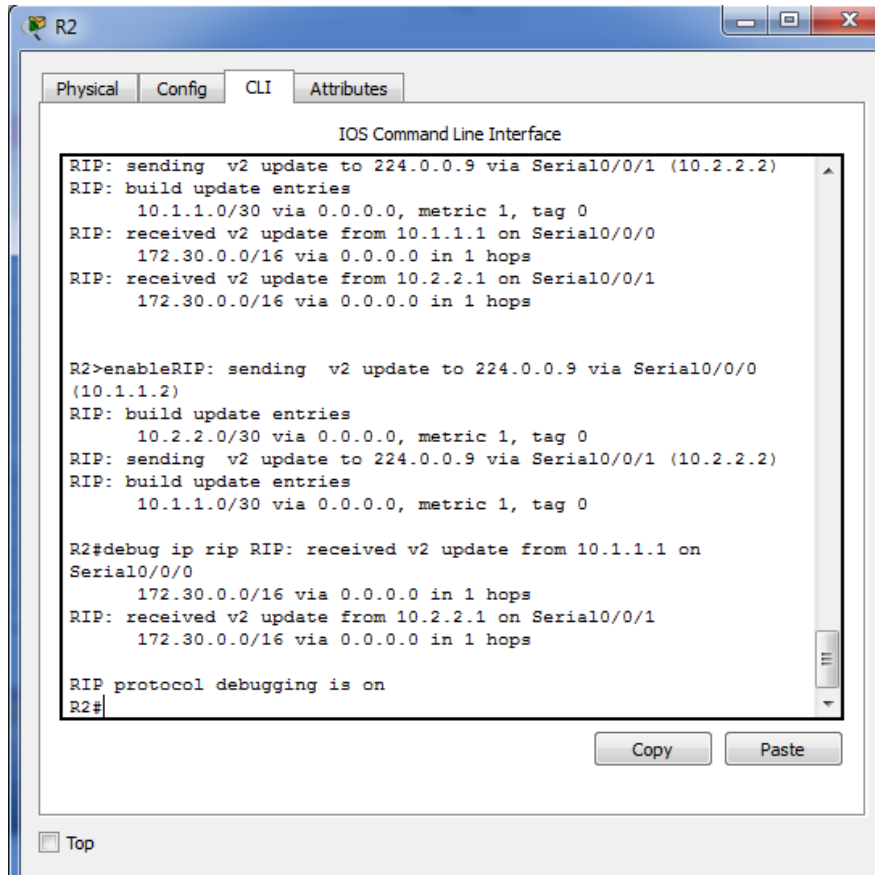
Gateway of last resort is not set

    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, 00:00:22, 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.

**172.30.0.0/16 via 0.0.0.0 in 1 hops**





```

R2
Physical Config CLI Attributes
IOS Command Line Interface
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: 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
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>enableRIP: sending v2 update to 224.0.0.9 via Serial0/0/0
(10.1.1.2)
RIP: build update entries
  10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
  10.1.1.0/30 via 0.0.0.0, metric 1, tag 0

R2#debug ip rip 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
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

RIP protocol debugging is on
R2#
  
```

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.

**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.

```

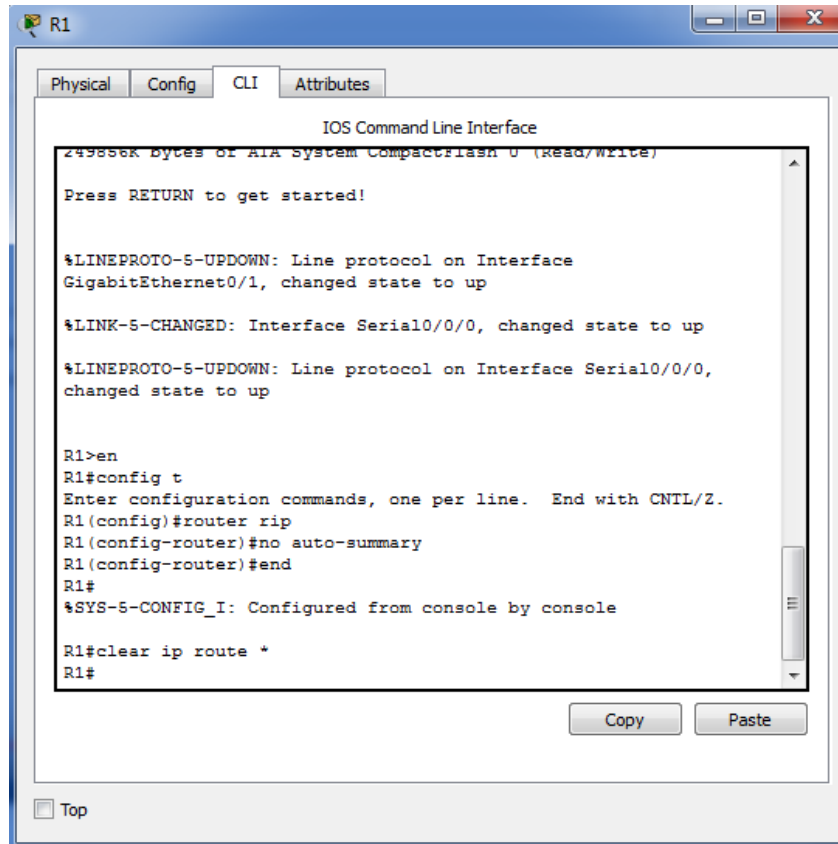
R1(config)# router rip
R1(config-router)# no auto-summary
  
```

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

```

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

**Para R1 tendremos:**



```
IOS Command Line Interface
249886K bytes of ATA System CompactFlash 0 (read/write)

Press RETURN to get started!

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

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

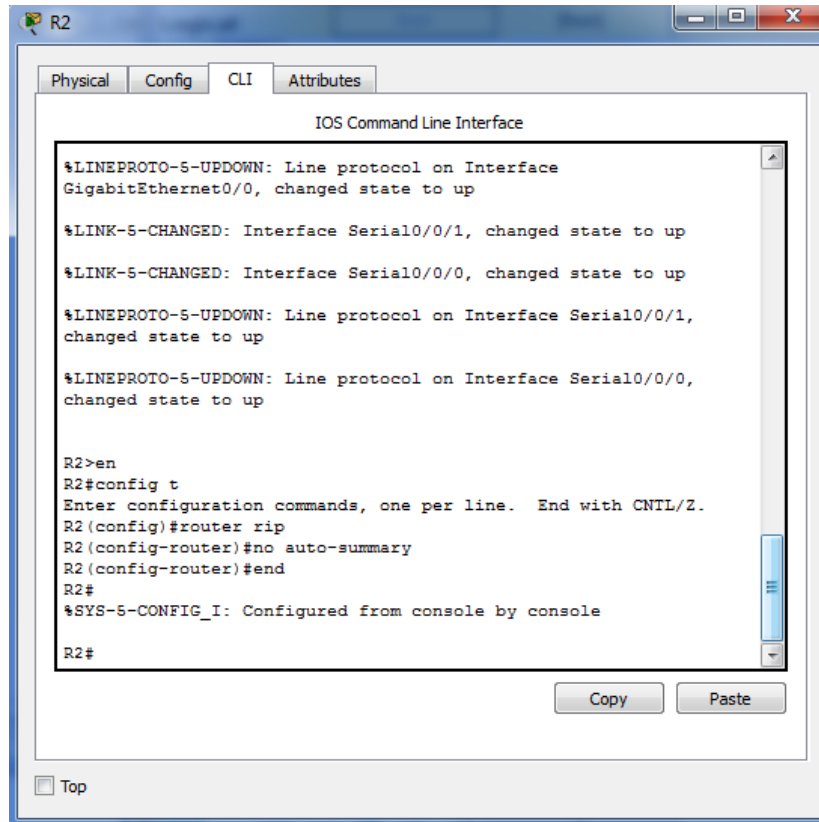
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

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

R1#clear ip route *
R1#
```

Copy Paste

Top

A screenshot of a network simulator window titled 'R2'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The main area is titled 'IOS Command Line Interface' and contains a text area with the following text:

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

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

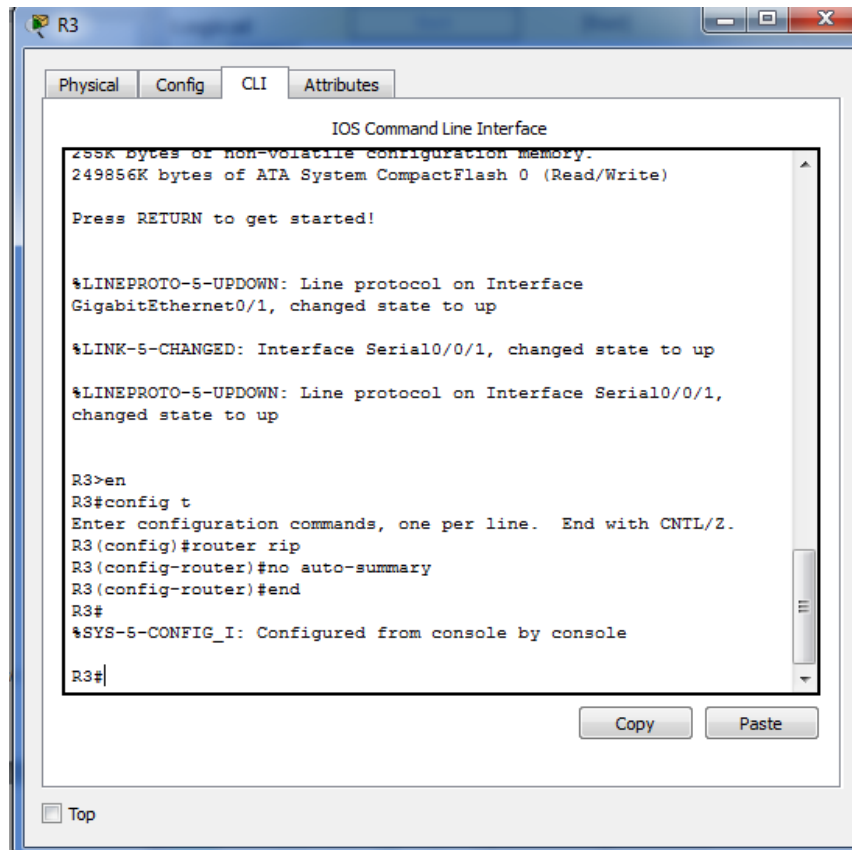
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%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

R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Below the text area are 'Copy' and 'Paste' buttons. At the bottom left of the window is a 'Top' button.



```

R3
  Physical  Config  CLI  Attributes
  IOS Command Line Interface
  258K 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
  GigabitEthernet0/1, changed state to up

  %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

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

  R3>en
  R3#config t
  Enter configuration commands, one per line.  End with CNTL/Z.
  R3(config)#router rip
  R3(config-router)#no auto-summary
  R3(config-router)#end
  R3#
  %SYS-5-CONFIG_I: Configured from console by console

  R3#
  
```

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



## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

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 Attributes

%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

R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#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 is possibly down, routing via 10.2.2.1, Serial0/0/1
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, 00:00:23, Serial0/0/1
C   209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.201.0/24 is directly connected, GigabitEthernet0/0
L   209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

R1# show ip route

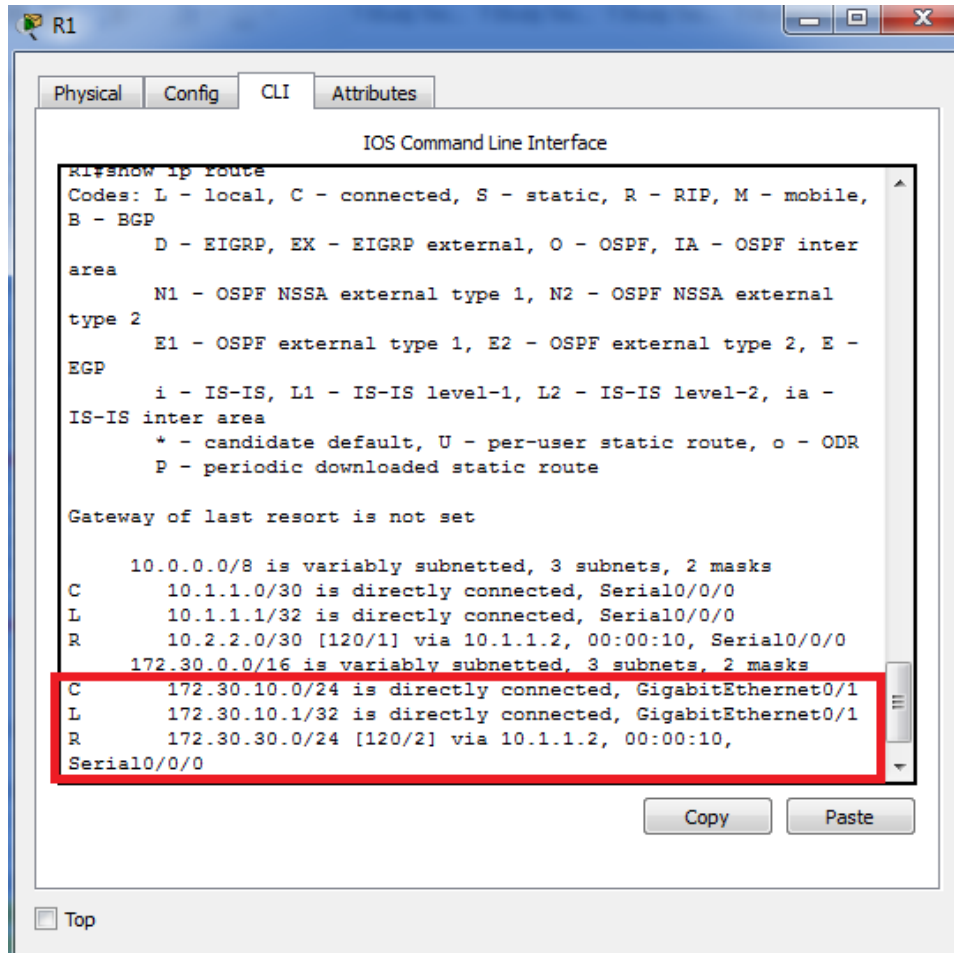
<Output Omitted>

Gateway of last resort is not set

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

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

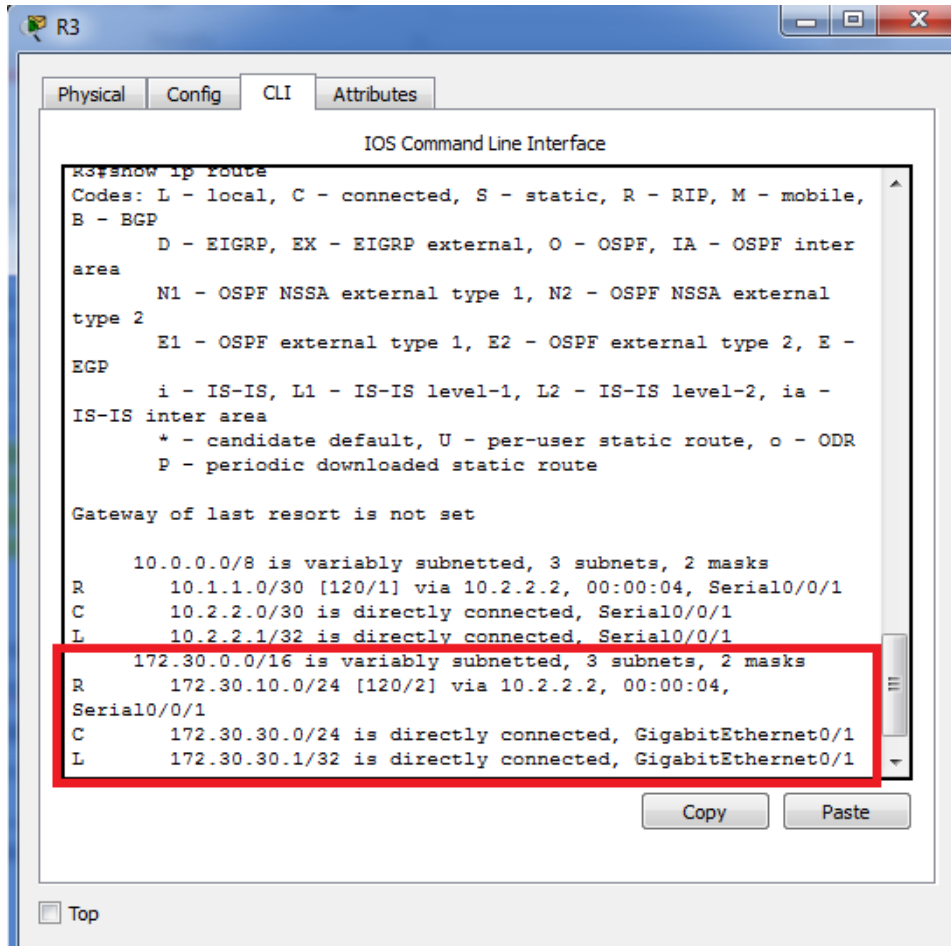
- C 172.30.10.0/24 is directly connected, GigabitEthernet0/1
- L 172.30.10.1/32 is directly connected, GigabitEthernet0/1
- R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0



R3# show ip route

<Output Omitted>

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



```

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, 00:00:04, 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
R    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R    172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:04,
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
  
```

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

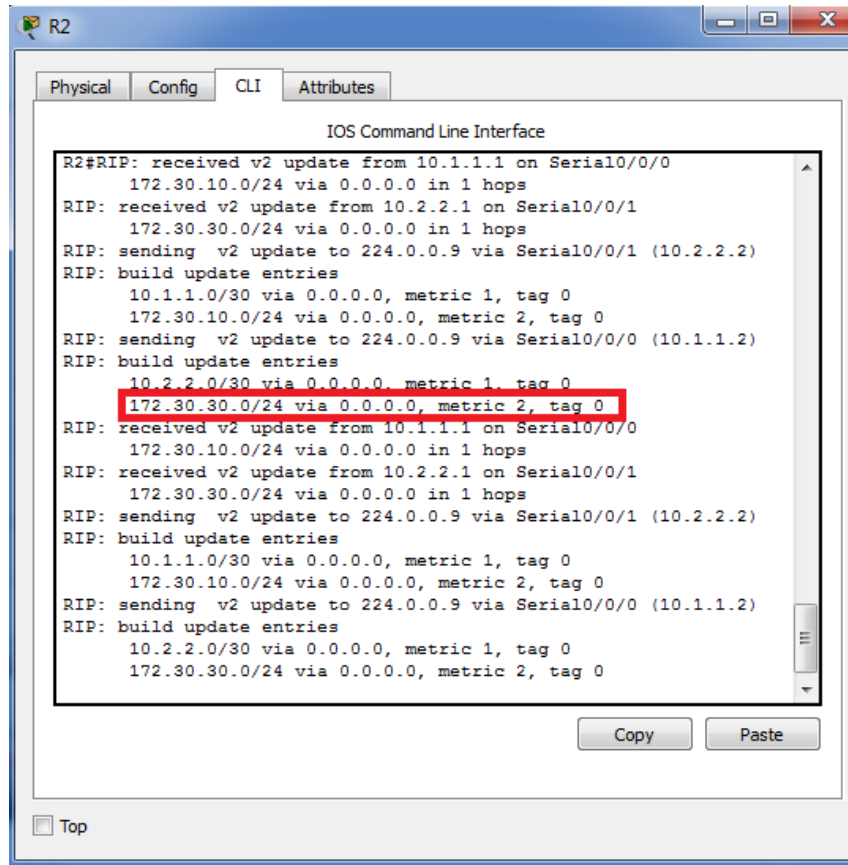
**R2# debug ip rip**

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 via 0.0.0.0, metric 2, tag 0**

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

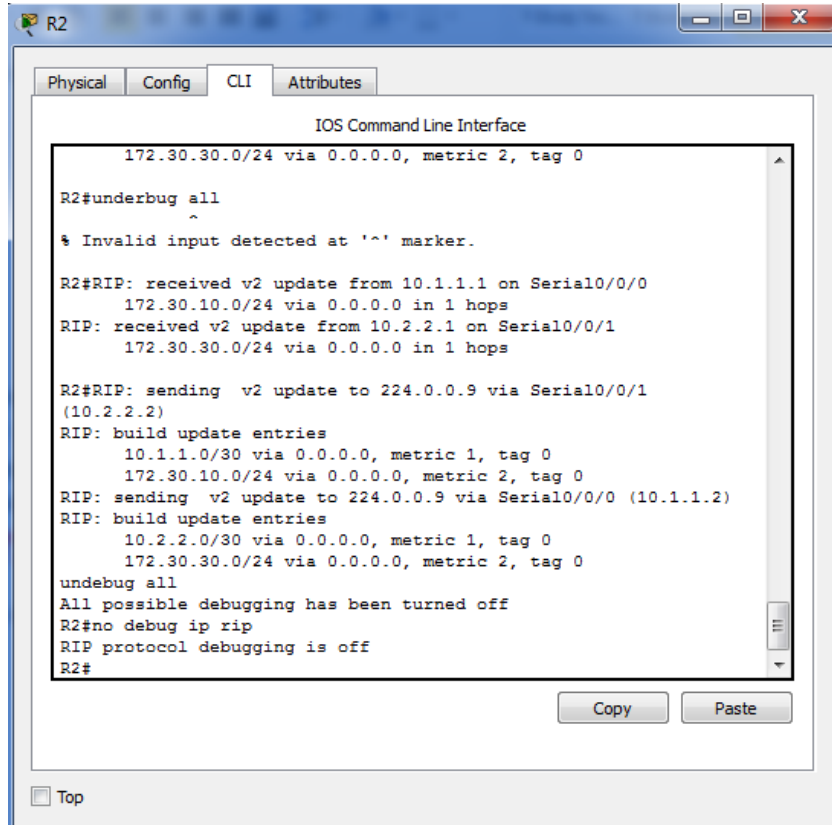


The screenshot shows a terminal window titled "R2" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows a sequence of RIP update messages. A red box highlights the following line: "172.30.30.0/24 via 0.0.0.0, metric 2, tag 0".

```
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
    172.30.30.0/24 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
    10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
    172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
    10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
    172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
    172.30.30.0/24 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
    10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
    172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
    10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
    172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
```

Buttons for "Copy" and "Paste" are visible at the bottom of the terminal window. A "Top" button is located at the bottom left of the window frame.





```

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

172.30.30.0/24 via 0.0.0.0, metric 2, tag 0

R2#underbug all
^
% Invalid input detected at '^' marker.

R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.30.0/24 via 0.0.0.0 in 1 hops

R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/1
(10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
undebug all
All possible debugging has been turned off
R2#no debug ip rip
RIP protocol debugging is off
R2#
  
```

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

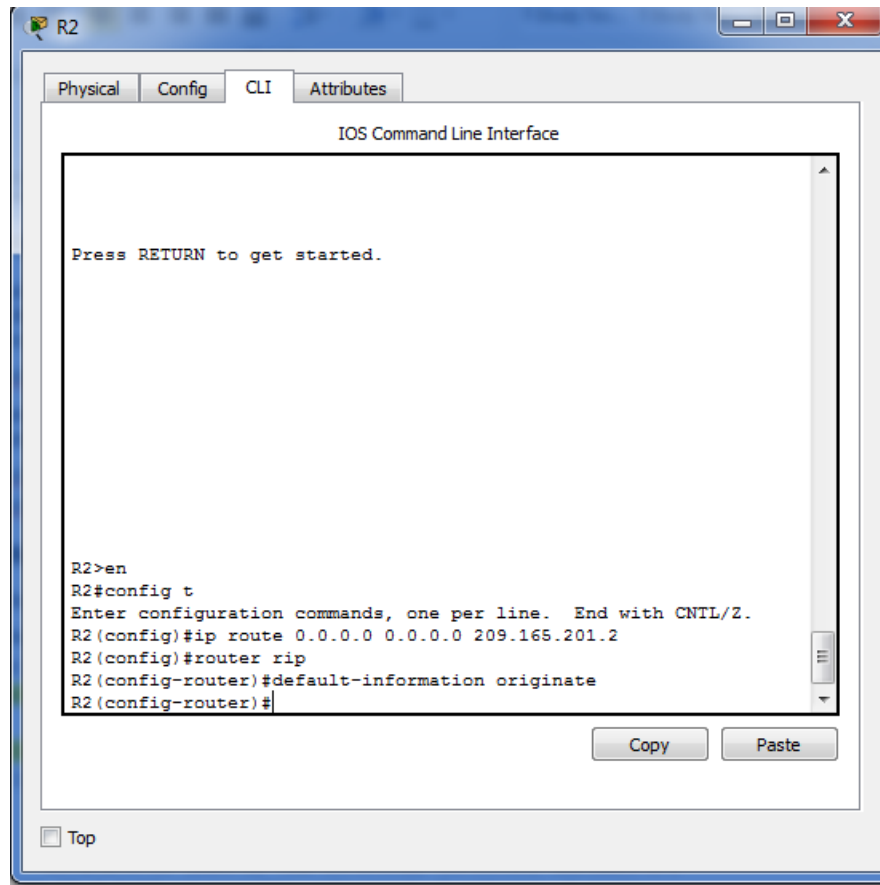
a. Desde el R2, cree una ruta estática a la red 0.0.0.0 0.0.0.0, con el comando **ip route**. Esto envía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet al establecer un gateway de último recurso en el router R2.

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

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

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

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



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

c. Consulte la tabla de routing en el R1.

R1# **show ip route**

<Output Omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

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

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

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

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

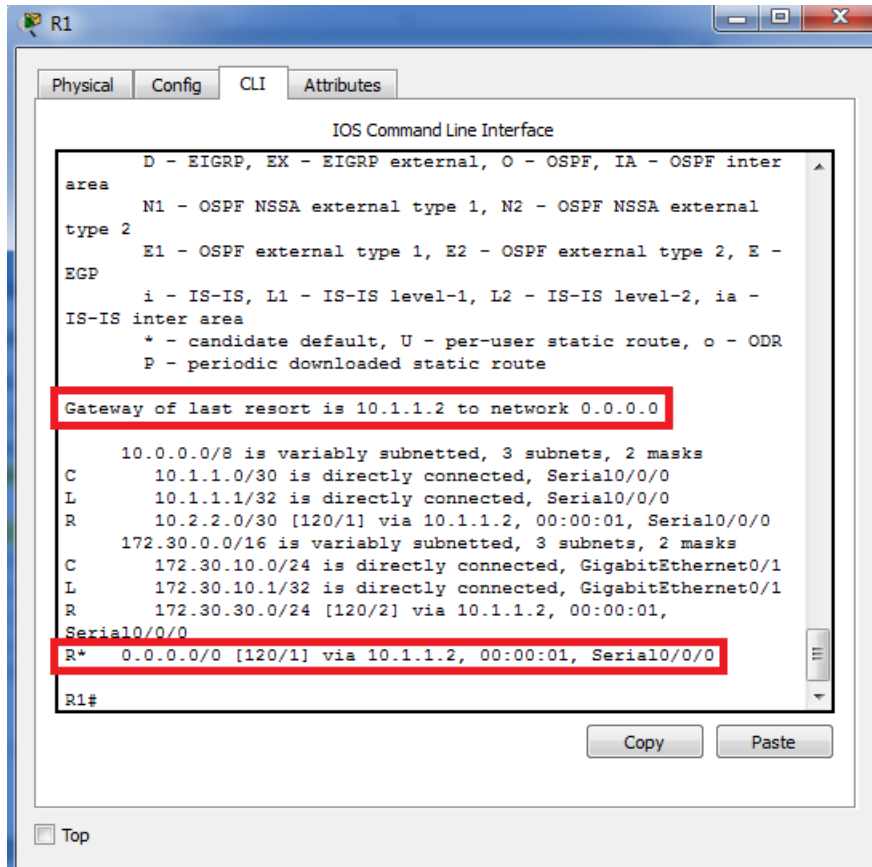
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0

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

C 172.30.10.0/24 is directly connected, GigabitEthernet0/1

L 172.30.10.1/32 is directly connected, GigabitEthernet0/1

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



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
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, Serial10/0/0
L 10.1.1.1/32 is directly connected, Serial10/0/0
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:01, Serial10/0/0
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, 00:00:01,
Serial10/0/0
R* 0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:01, Serial10/0/0
R1#
Copy Paste
Top
  
```

¿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, es decir, una puerta de enlace y la ruta predeterminada o por defecto aparece o nos muestra en la tabla de ruteo que esta prendida a través de RIP

d. Consulte la tabla de routing en el R2.

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

**R2 tiene una ruta estática por defecto a través de 0.0.0.0/0 [1/0] via 209.165.201.2 la cual es directamente conectada a G0/0**

```

R2
-----
Physical  Config  CLI  Attributes

R2>en
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

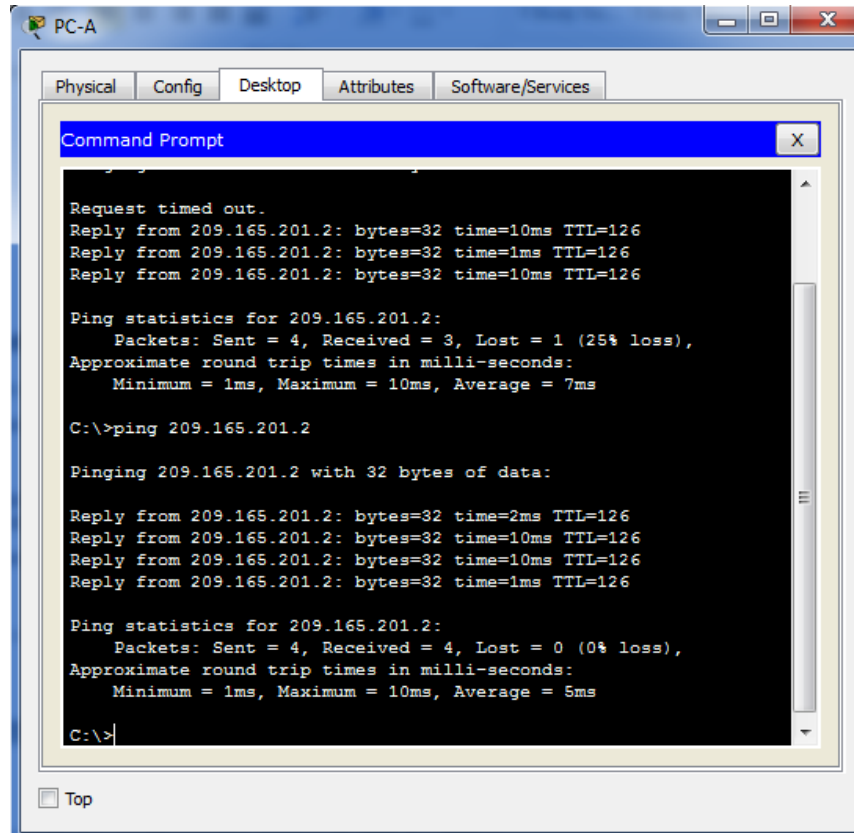
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
    172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:26, Serial0/0/1
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
S*     0.0.0.0/0 [1/0] via 209.165.201.2
R2#
  
```

**Paso 6. Verifique la conectividad.**

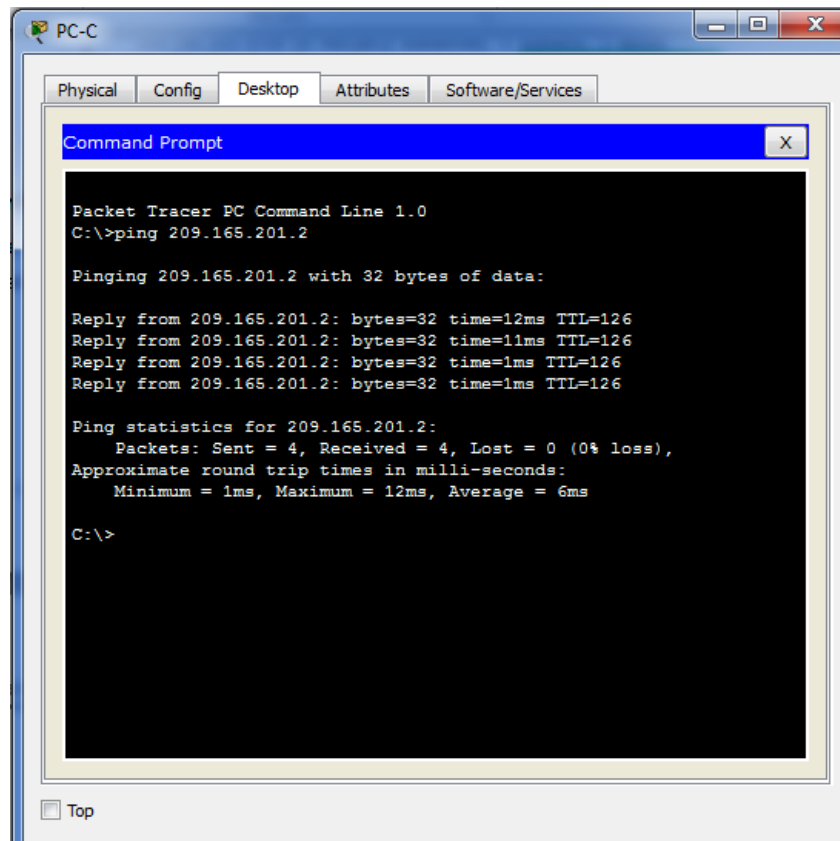
a. Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 209.165.201.2.

¿Tuvieron éxito los pings?

**SI**

A screenshot of a Windows Command Prompt window titled 'PC-A'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Attributes', and 'Software/Services'. The Command Prompt shows the output of a ping command to the IP address 209.165.201.2. The output is as follows:

```
Request timed out.  
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126  
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126  
Reply from 209.165.201.2: bytes=32 time=10ms 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 = 10ms, Average = 7ms  
  
C:\>ping 209.165.201.2  
  
Pinging 209.165.201.2 with 32 bytes of data:  
  
Reply from 209.165.201.2: bytes=32 time=2ms TTL=126  
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126  
Reply from 209.165.201.2: bytes=32 time=10ms 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 = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 10ms, Average = 5ms  
  
C:\>
```



```

Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=12ms TTL=126
Reply from 209.165.201.2: bytes=32 time=11ms 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 = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms

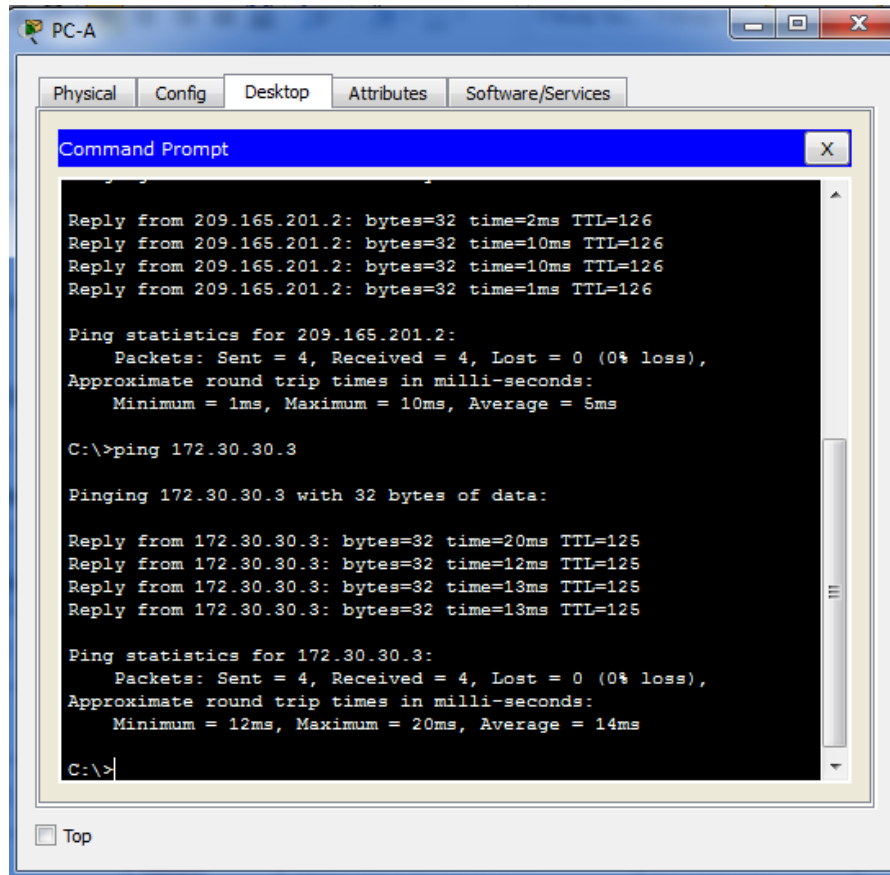
C:\>
  
```

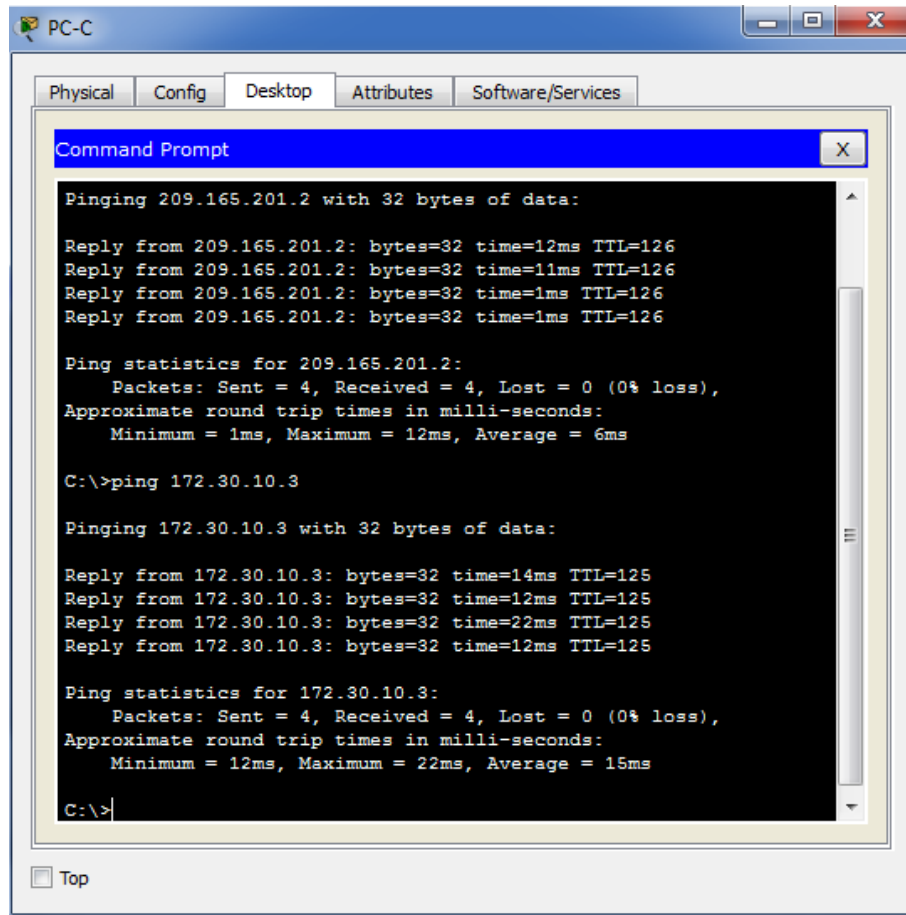
b. Verifique que los hosts dentro de la red dividida en subredes tengan posibilidad de conexión entre sí haciendo ping entre la PC-A y la PC-C.

¿Tuvieron éxito los pings?

**Si**

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





```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=12ms TTL=126
Reply from 209.165.201.2: bytes=32 time=11ms 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 = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.10.3: bytes=32 time=14ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Reply from 172.30.10.3: bytes=32 time=22ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms 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 = 12ms, Maximum = 22ms, Average = 15ms

C:\>
```

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

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



Tabla de direccionamiento

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

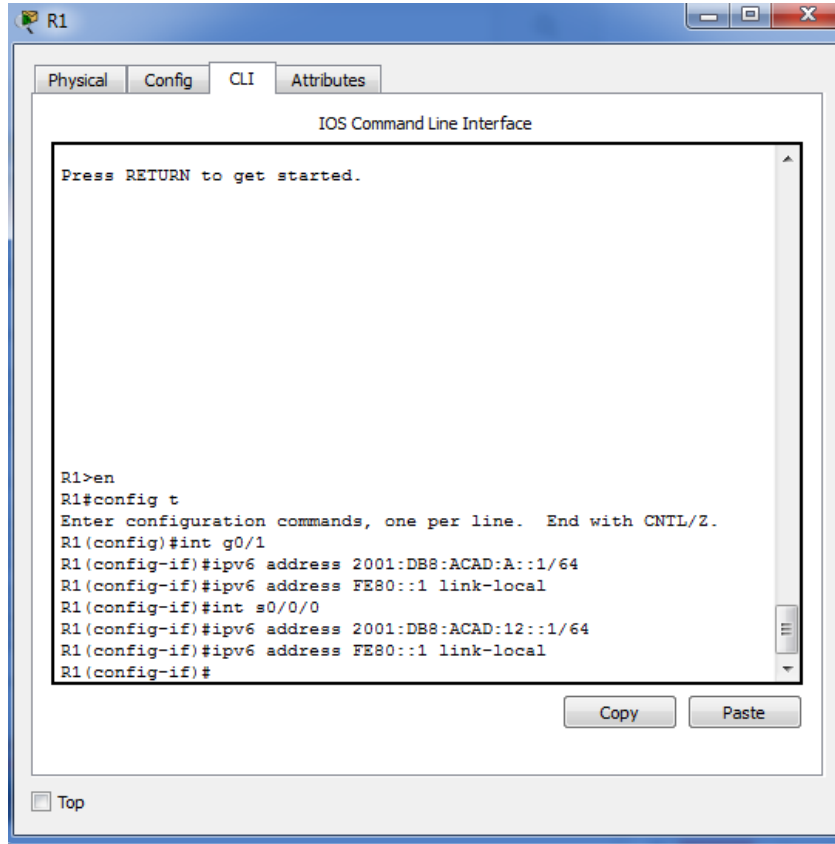
**Paso 1. configurar los equipos host.**

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

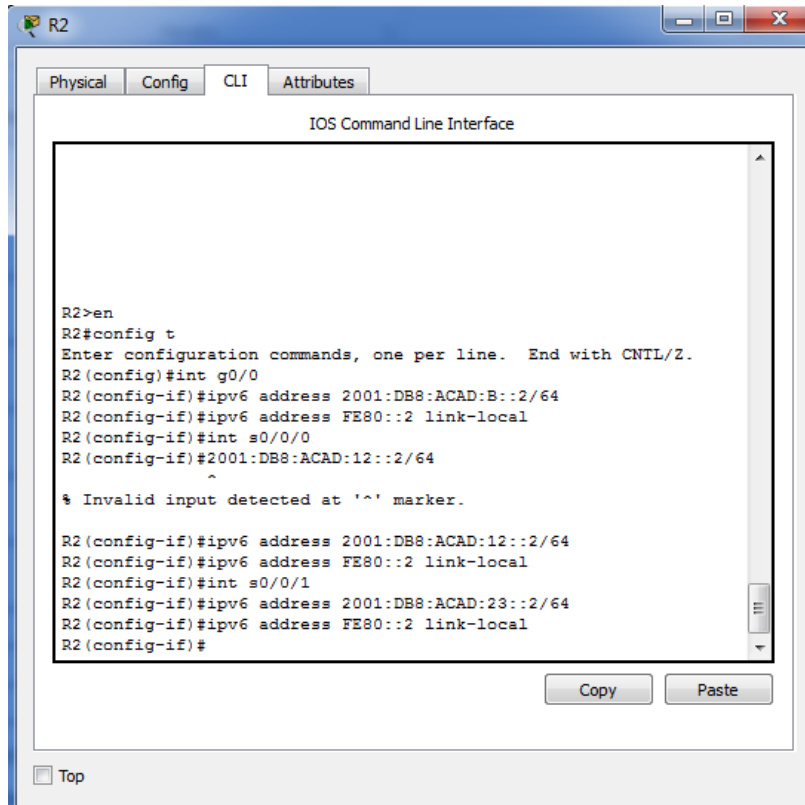
**Paso 2. configurar IPv6 en los routers.**

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

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



```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#
```

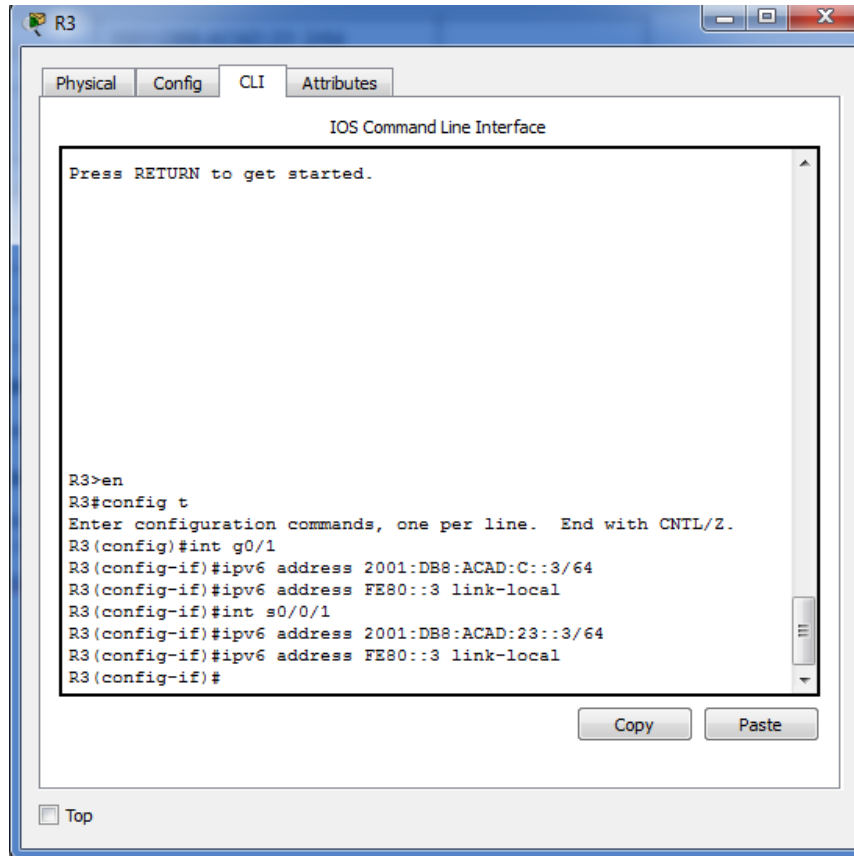


The screenshot shows a network simulator window titled 'R2'. It has four tabs: 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal text is as follows:

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#int s0/0/0
R2(config-if)#2001:DB8:ACAD:12::2/64
^
% Invalid input detected at '^' marker.

R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' button in the bottom-left corner.

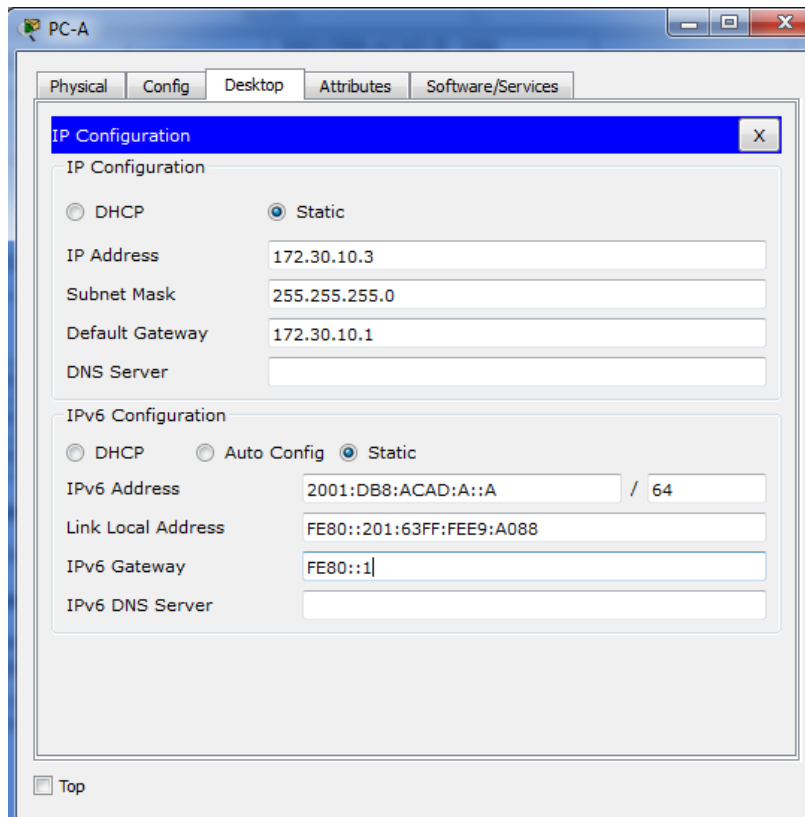


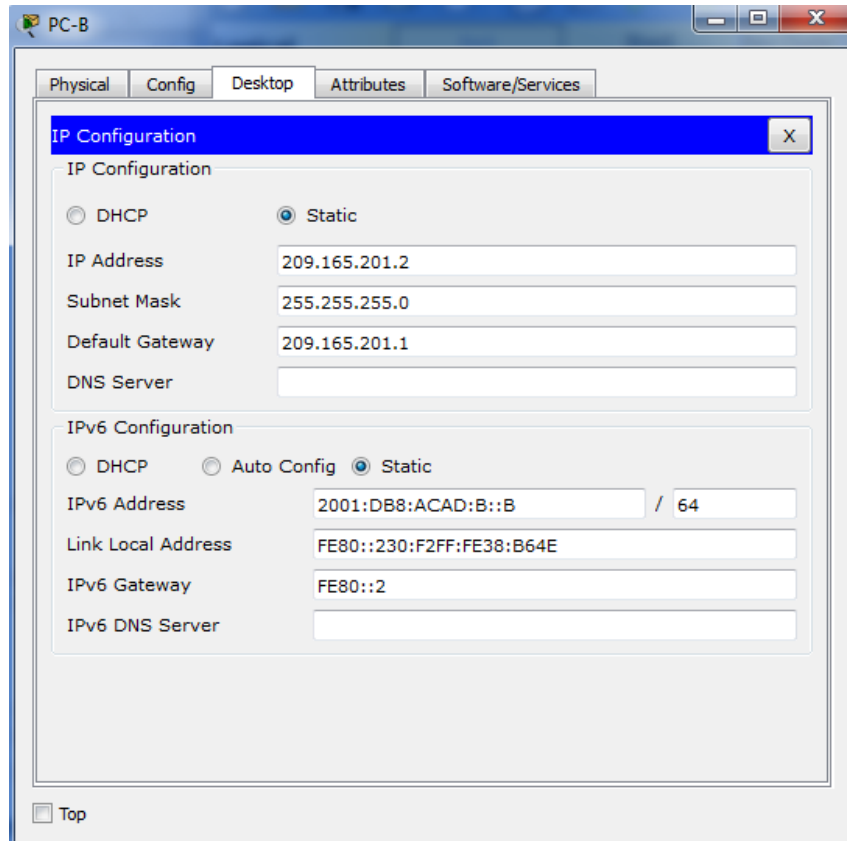
```
R3
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int 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)#int s0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#
```

Copy Paste

Top

A screenshot of a Windows Network Connections configuration window for a device named 'PC-A'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Attributes', and 'Software/Services'. The 'Config' tab is active, showing the 'IP Configuration' properties. The 'IP Configuration' section has a title bar with a close button. It contains two main sections: 'IP Configuration' and 'IPv6 Configuration'. In the 'IP Configuration' section, the 'Static' radio button is selected. The fields are: IP Address (172.30.10.3), Subnet Mask (255.255.255.0), Default Gateway (172.30.10.1), and DNS Server (empty). In the 'IPv6 Configuration' section, the 'Static' radio button is selected. The fields are: IPv6 Address (2001:DB8:ACAD:A::A / 64), Link Local Address (FE80::201:63FF:FEE9:A088), IPv6 Gateway (FE80::1), and IPv6 DNS Server (empty). A 'Top' button is located at the bottom left of the window.

A screenshot of a Windows Network Configuration window titled 'PC-B'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Attributes', and 'Software/Services'. The 'Config' tab is active, showing 'IP Configuration' and 'IPv6 Configuration' sections. The 'IP Configuration' section has 'Static' selected, with fields for IP Address (209.165.201.2), Subnet Mask (255.255.255.0), Default Gateway (209.165.201.1), and DNS Server. The 'IPv6 Configuration' section has 'Static' selected, with fields for IPv6 Address (2001:DB8:ACAD:B::B / 64), Link Local Address (FE80::230:F2FF:FE38:B64E), IPv6 Gateway (FE80::2), and IPv6 DNS Server. A 'Top' button is at the bottom left.

PC-B

Physical Config Desktop Attributes Software/Services

IP Configuration X

IP Configuration

DHCP  Static

IP Address 209.165.201.2

Subnet Mask 255.255.255.0

Default Gateway 209.165.201.1

DNS Server

IPv6 Configuration

DHCP  Auto Config  Static

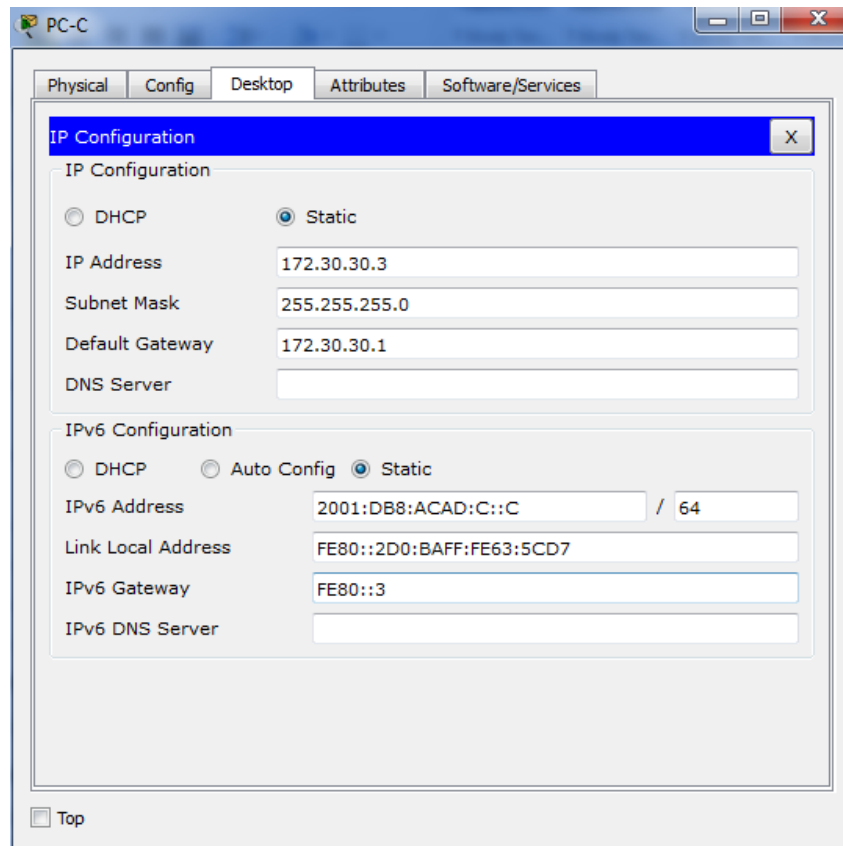
IPv6 Address 2001:DB8:ACAD:B::B / 64

Link Local Address FE80::230:F2FF:FE38:B64E

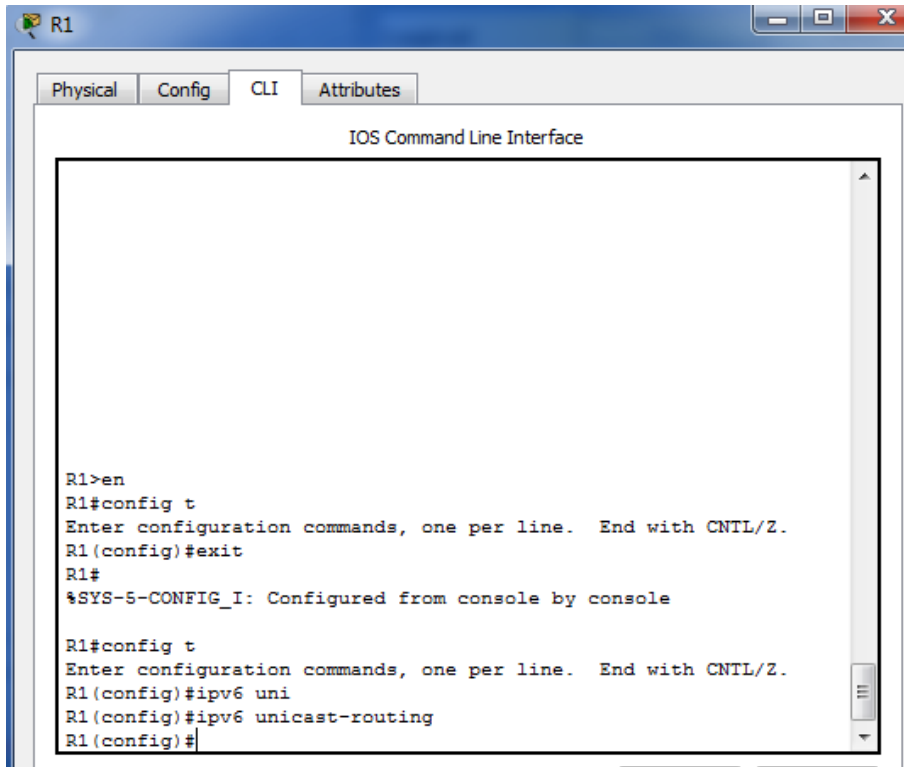
IPv6 Gateway FE80::2

IPv6 DNS Server

Top



- b. Habilite el routing IPv6 en cada router.



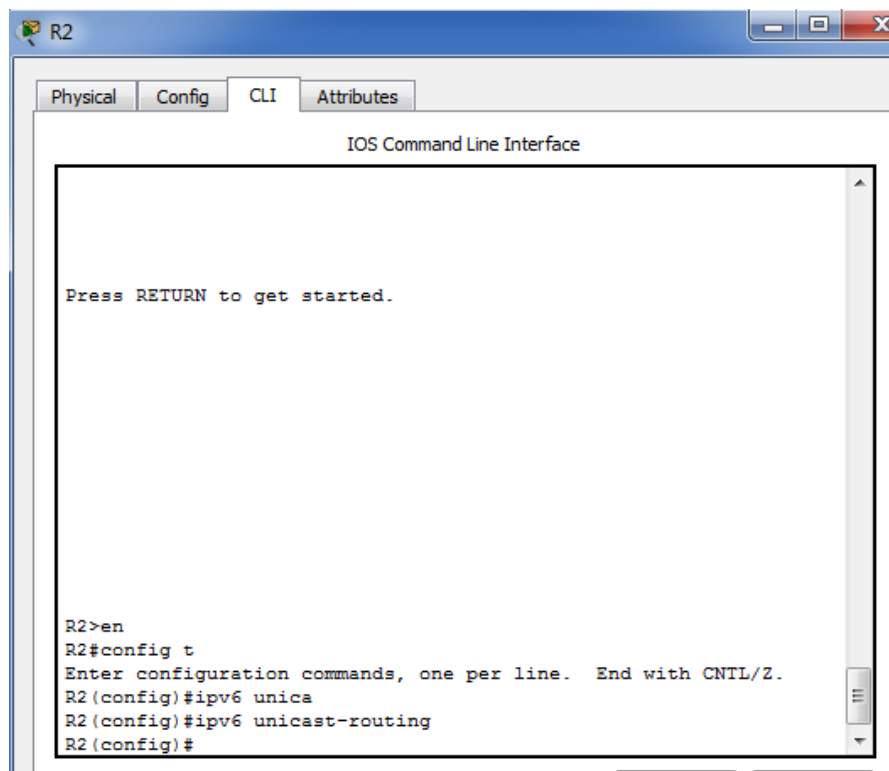
R1

Physical Config CLI Attributes

IOS Command Line Interface

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

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 uni
R1(config)#ipv6 unicast-routing
R1(config)#
```



R2

Physical Config CLI Attributes

IOS Command Line Interface

```
Press RETURN to get started.

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

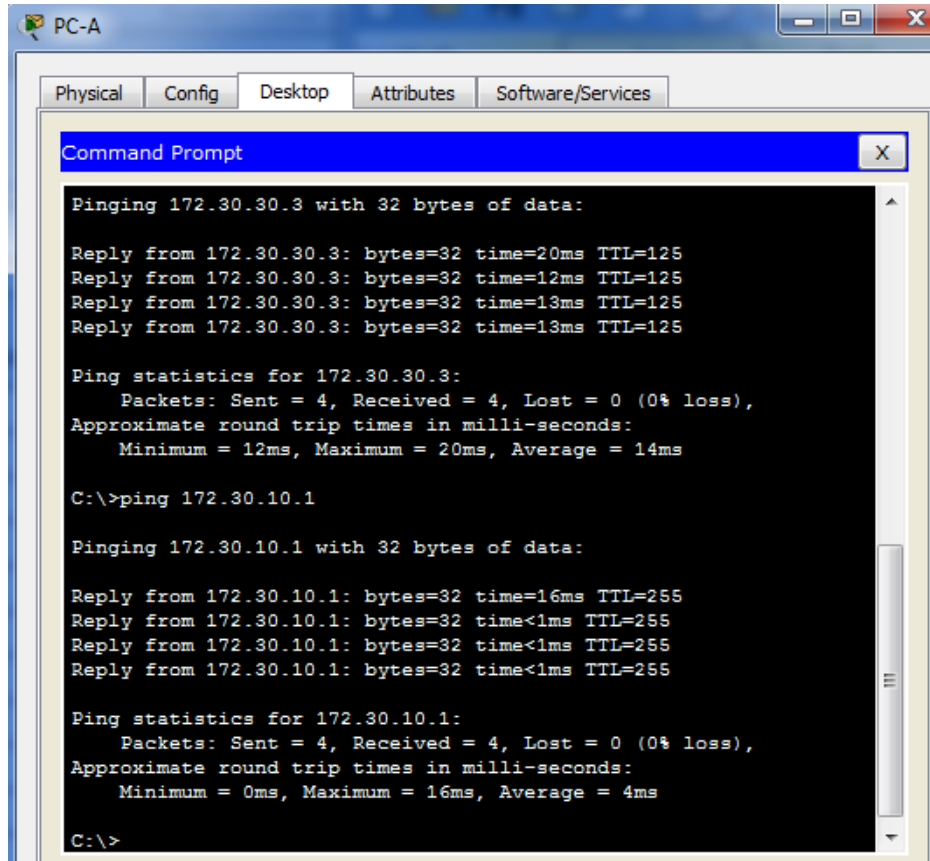






d. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.

- **Ping de PC-A a R1**



```

PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.30.3: bytes=32 time=20ms TTL=125
Reply from 172.30.30.3: bytes=32 time=12ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 20ms, Average = 14ms

C:\>ping 172.30.10.1

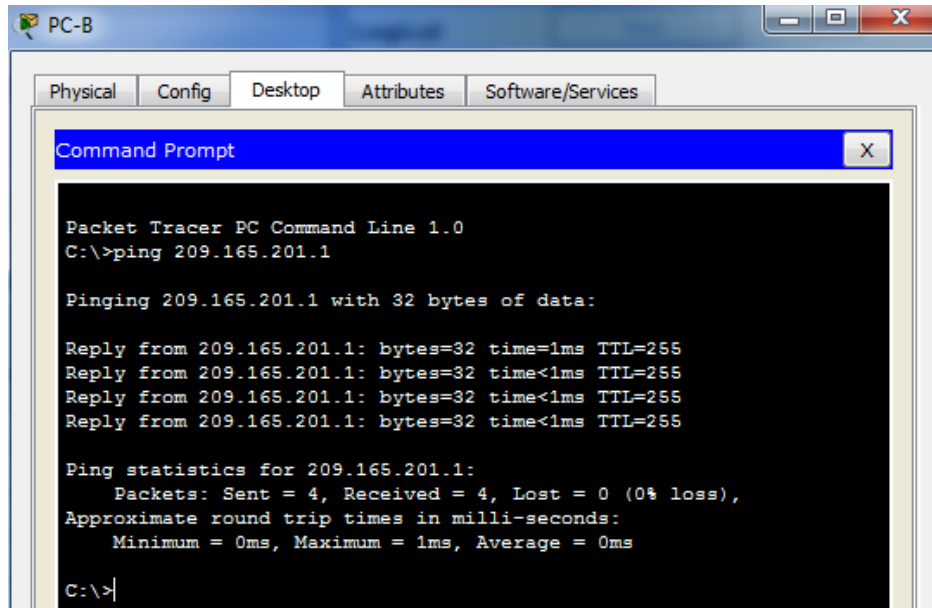
Pinging 172.30.10.1 with 32 bytes of data:

Reply from 172.30.10.1: bytes=32 time=16ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms 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 = 16ms, Average = 4ms

C:\>
  
```

- **Ping de PC-B a R2**



```

PC-B
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.1

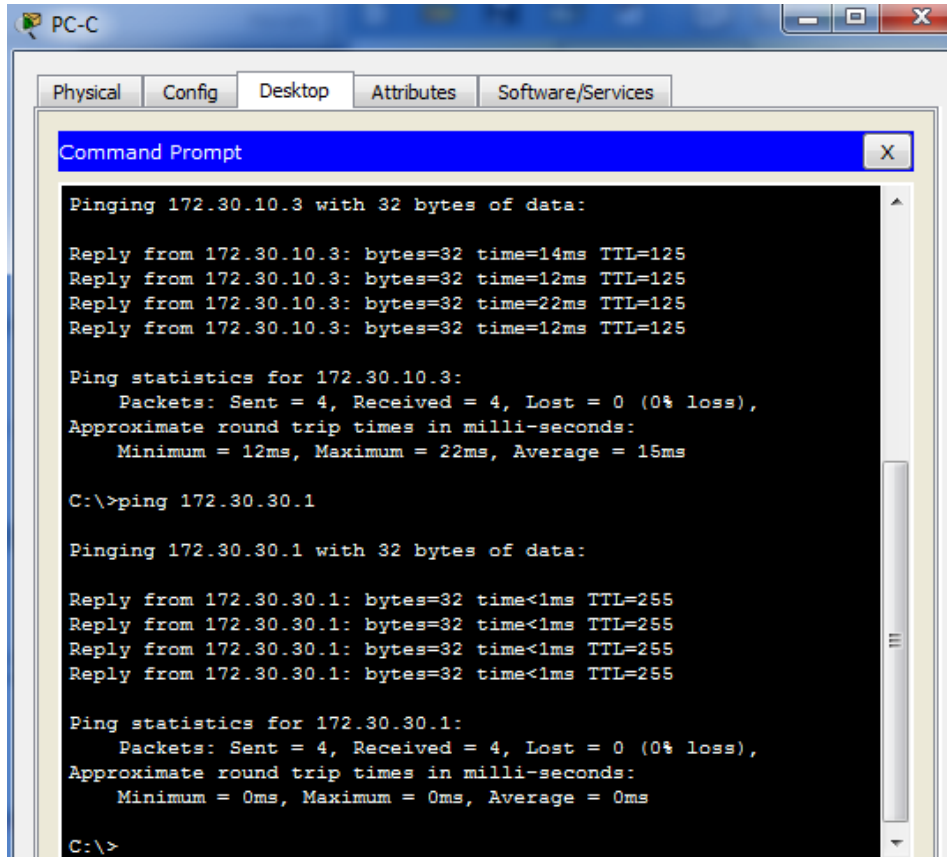
Pinging 209.165.201.1 with 32 bytes of data:

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

C:\>
  
```

- Ping de PC-C a R3



```

PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.10.3: bytes=32 time=14ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Reply from 172.30.10.3: bytes=32 time=22ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms 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 = 12ms, Maximum = 22ms, Average = 15ms

C:\>ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

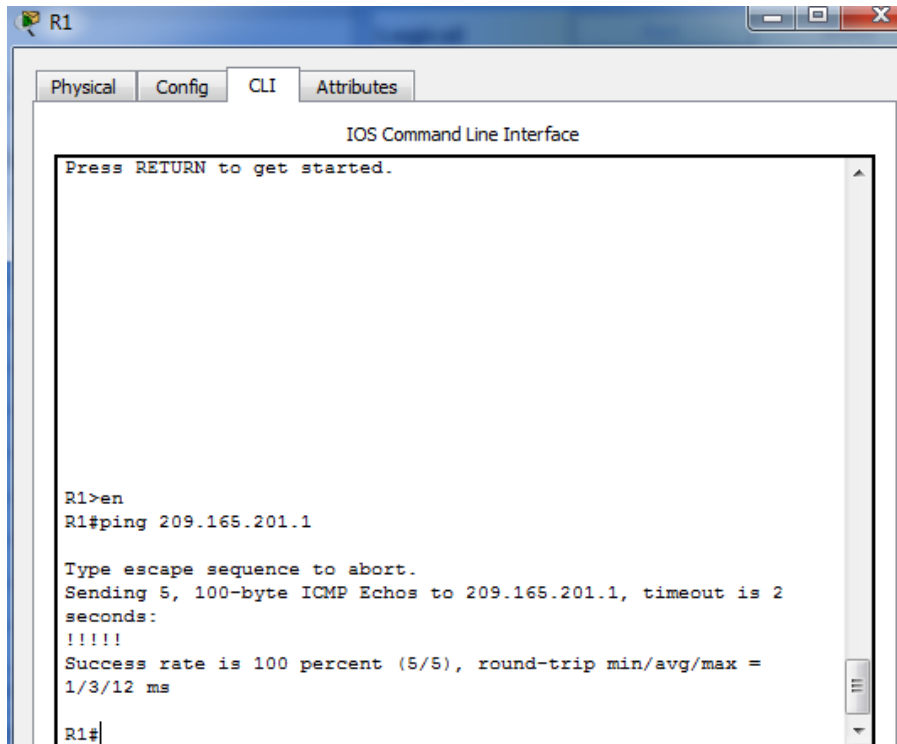
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
  
```

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

- Ping entre R1 y R2

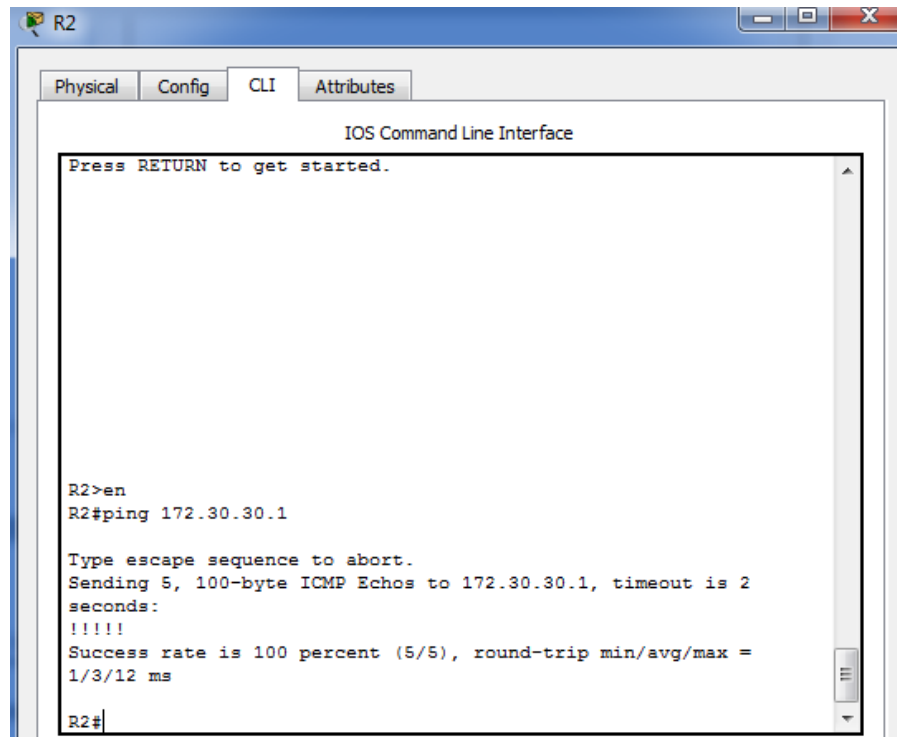


```
R1
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

R1>en
R1#ping 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms
R1#
```

- Ping entre R2 y R3

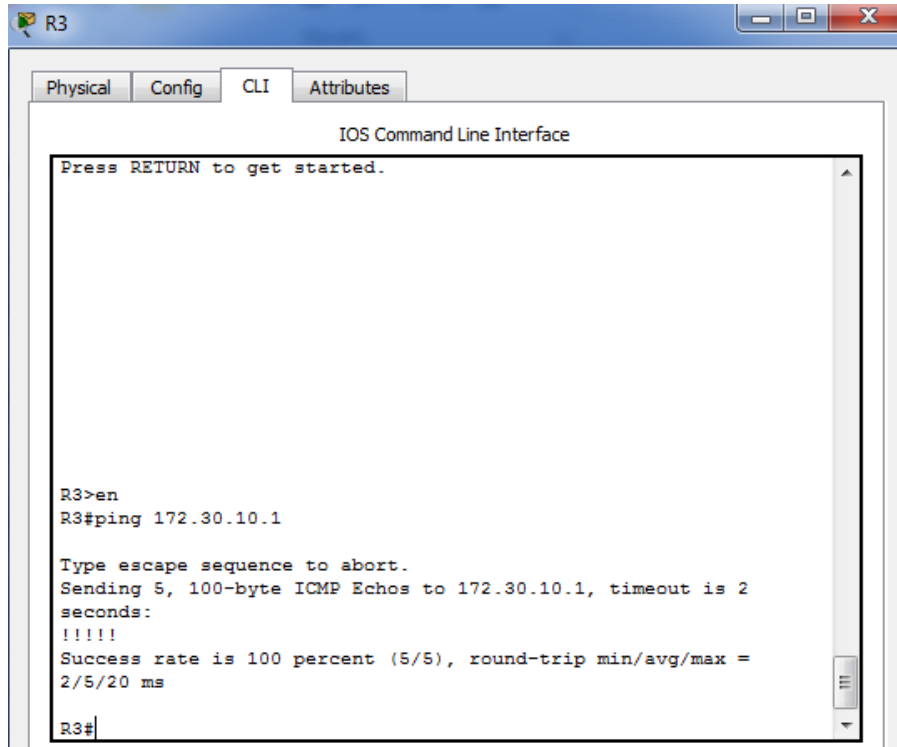


```
R2
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

R2>en
R2#ping 172.30.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms
R2#
```

- Ping entre R3 y R1



```

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

Press RETURN to get started.

R3>en
R3#ping 172.30.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.10.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
2/5/20 ms
R3#
  
```

#### 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.

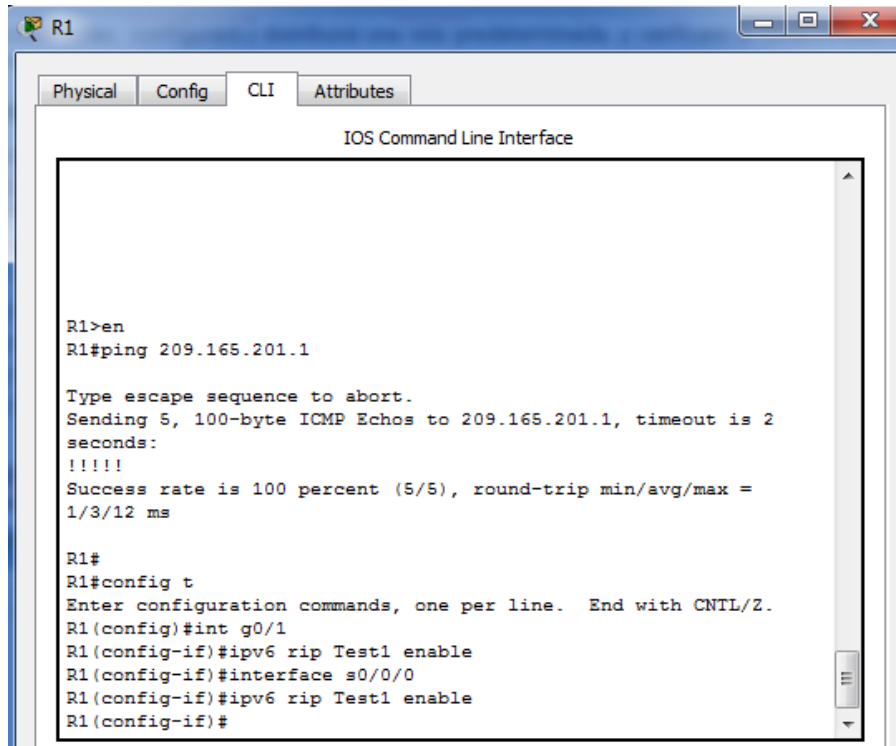
- Emita el comando **ipv6 rip Test1 enable** para cada interfaz en el R1 que participará en el routing RIPng, donde **Test1** es el nombre de proceso pertinente en el nivel local.

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

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

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

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



```

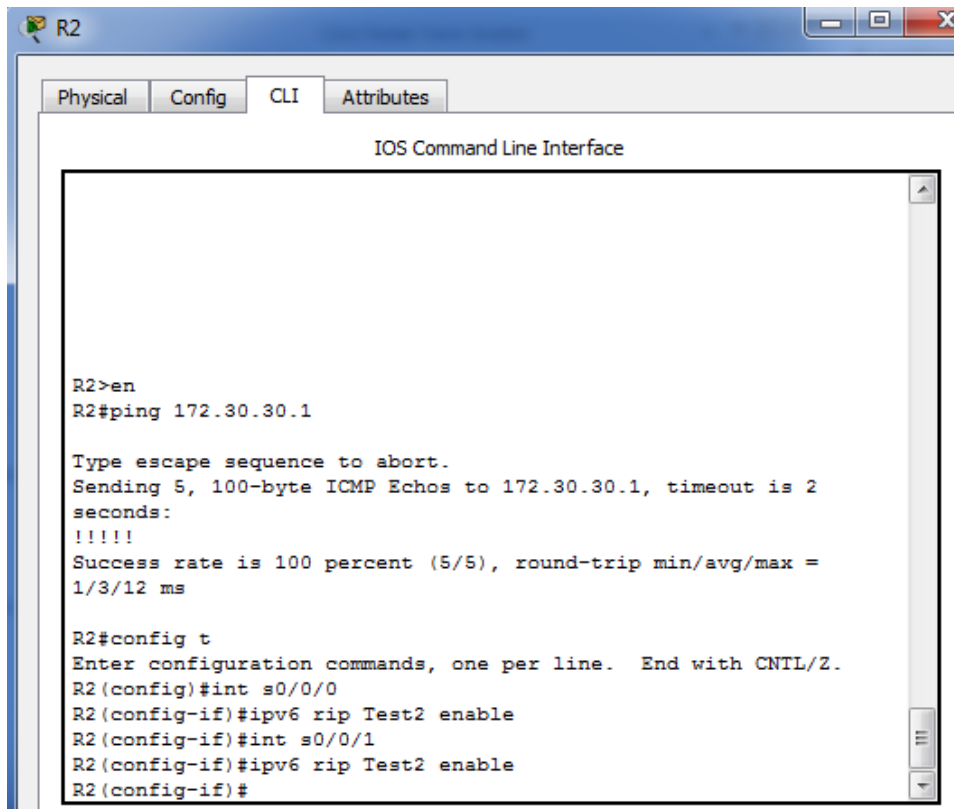
R1
-----
Physical Config CLI Attributes
IOS Command Line Interface

R1>en
R1#ping 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms

R1#
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int 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)#
  
```

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



```

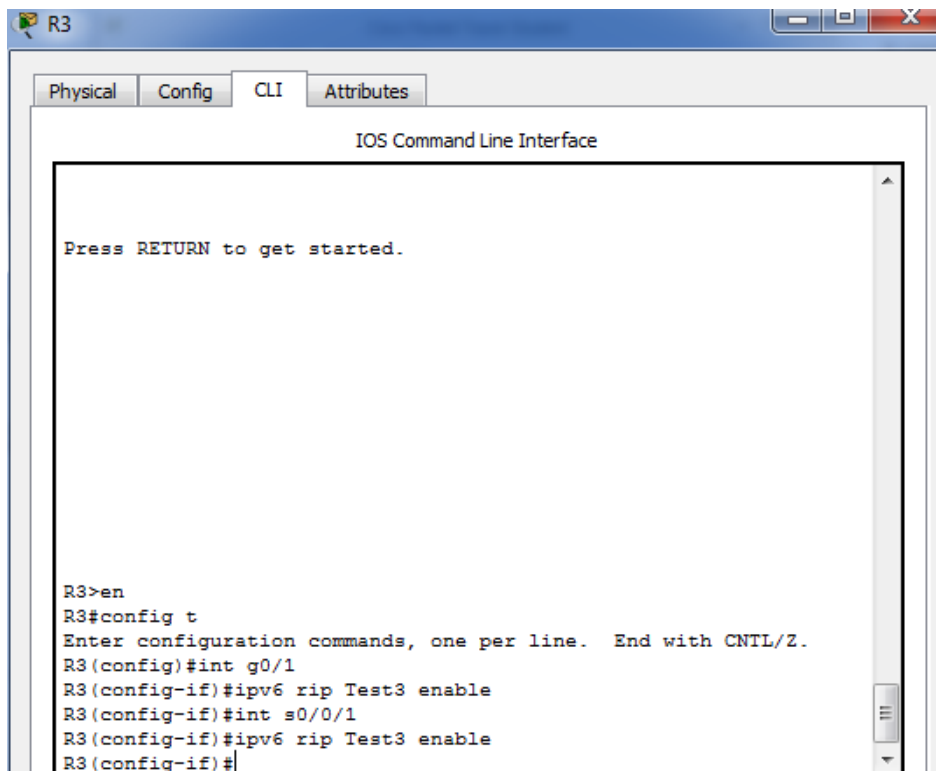
R2
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

R2>en
R2#ping 172.30.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/12 ms

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

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



```

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

Press RETURN to get started.

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



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"

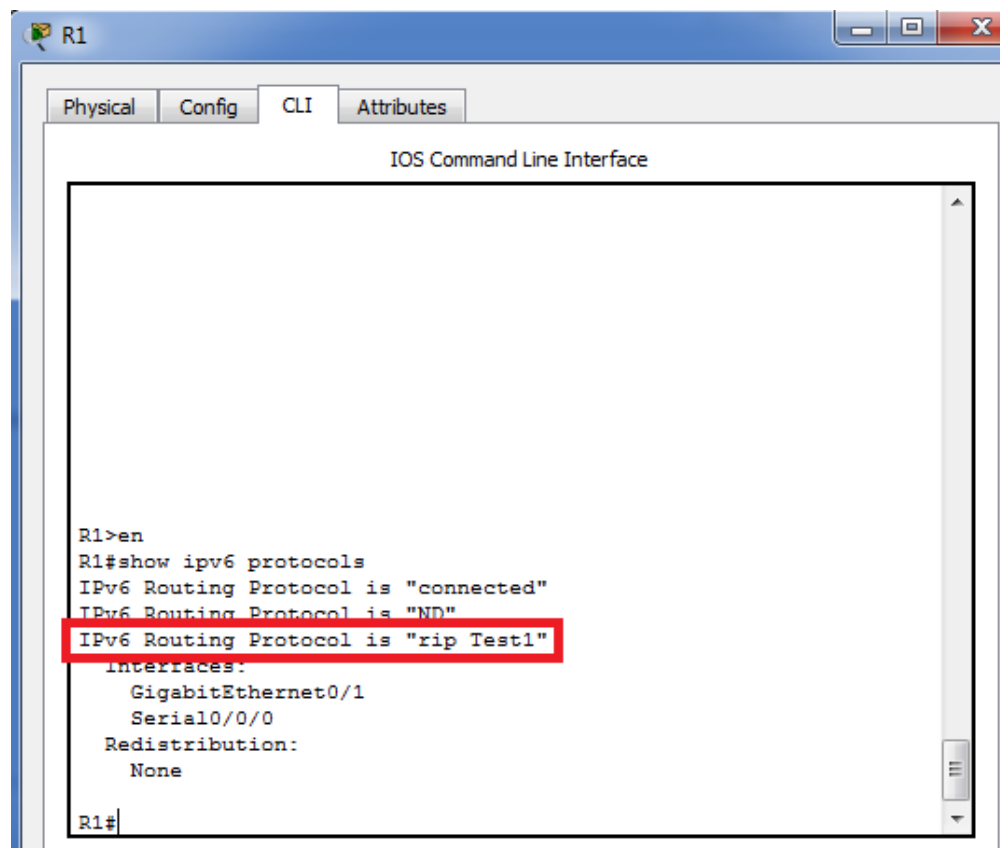
Interfaces:

Serial0/0/0

GigabitEthernet0/1

Redistribution:

None



```

R1>en
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
R1#
  
```

¿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

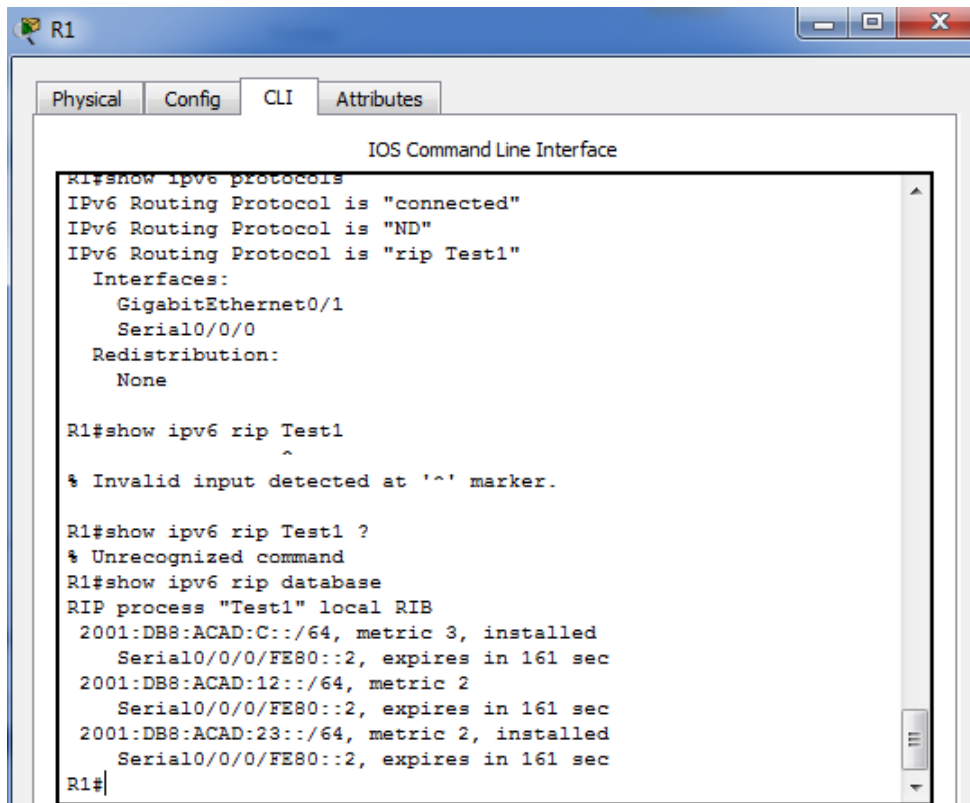
Interfaces:

GigabitEthernet0/1

Serial0/0/0

Redistribution:

None



```

R1#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

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

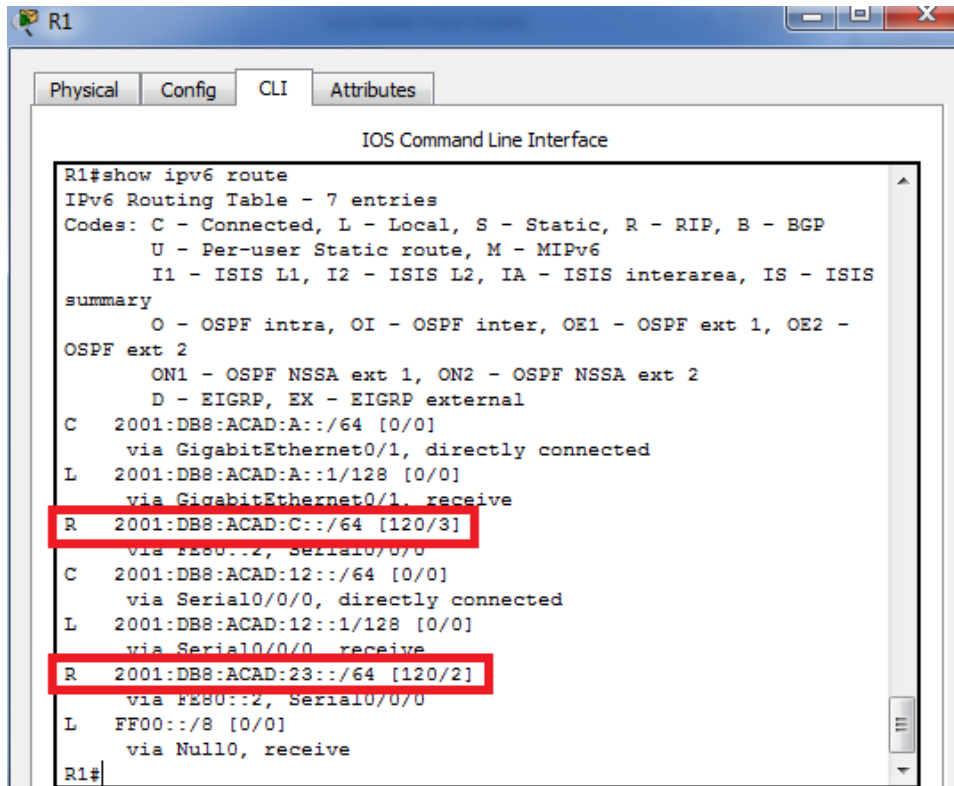
R1#show ipv6 rip Test1 ?
% Unrecognized command
R1#show ipv6 rip database
RIP process "Test1" local RIB
  2001:DB8:ACAD:C::/64, metric 3, installed
    Serial0/0/0/FE80::2, expires in 161 sec
  2001:DB8:ACAD:12::/64, metric 2
    Serial0/0/0/FE80::2, expires in 161 sec
  2001:DB8:ACAD:23::/64, metric 2, installed
    Serial0/0/0/FE80::2, expires in 161 sec
R1#
  
```

¿Cuáles son las similitudes entre RIPv2 y RIPng?

RIPv2 y RIPv6 tienen la distancia administrativa de 120 y usan el conteo de saltos como la métrica y envían actualizaciones cada 30 segundos

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

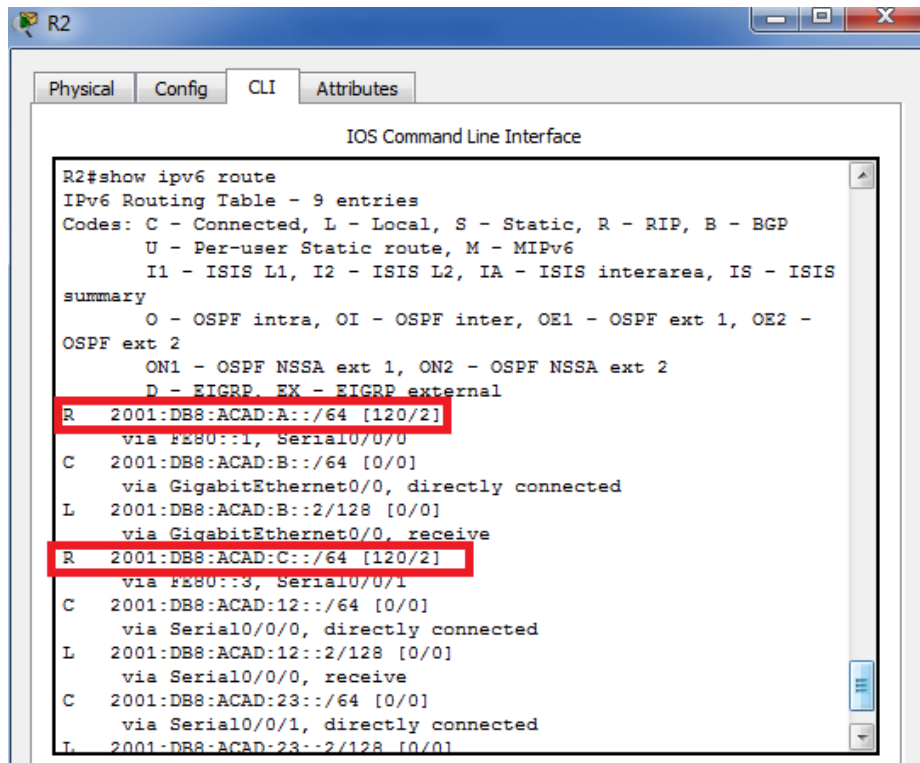
**Show ipv6 route**



```

R1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
  via GigabitEthernet0/1, receive
R 2001:DB8:ACAD:C::/64 [120/3]
  via FE80::2, Serial0/0/0
C 2001:DB8:ACAD:12::/64 [0/0]
  via Serial10/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
  via Serial10/0/0, receive
R 2001:DB8:ACAD:23::/64 [120/2]
  via FE80::2, Serial0/0/0
L FF00::/8 [0/0]
  via Null0, receive
R1#
  
```

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

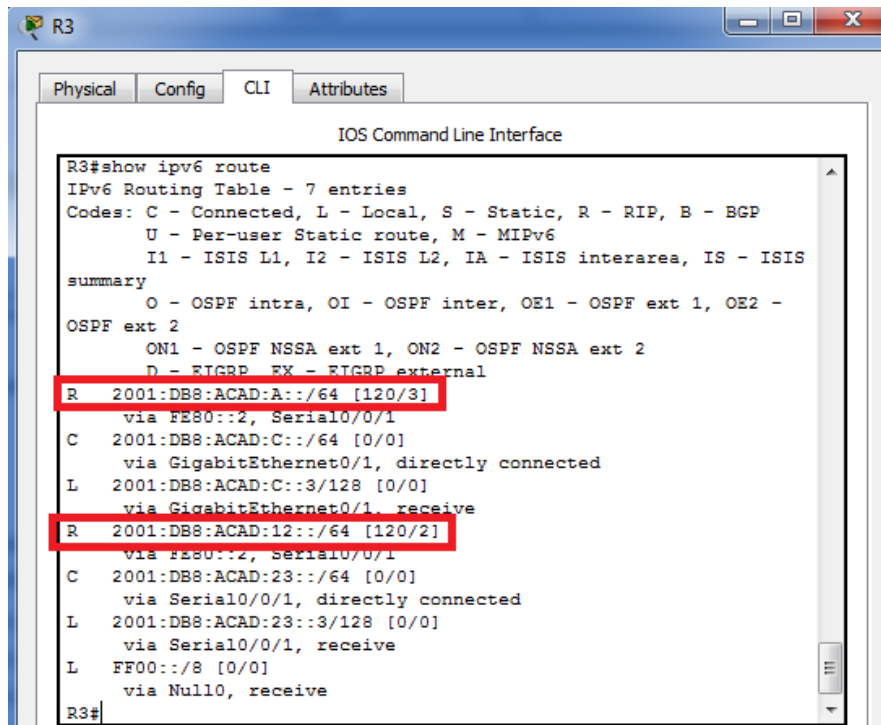


```

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

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

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



```

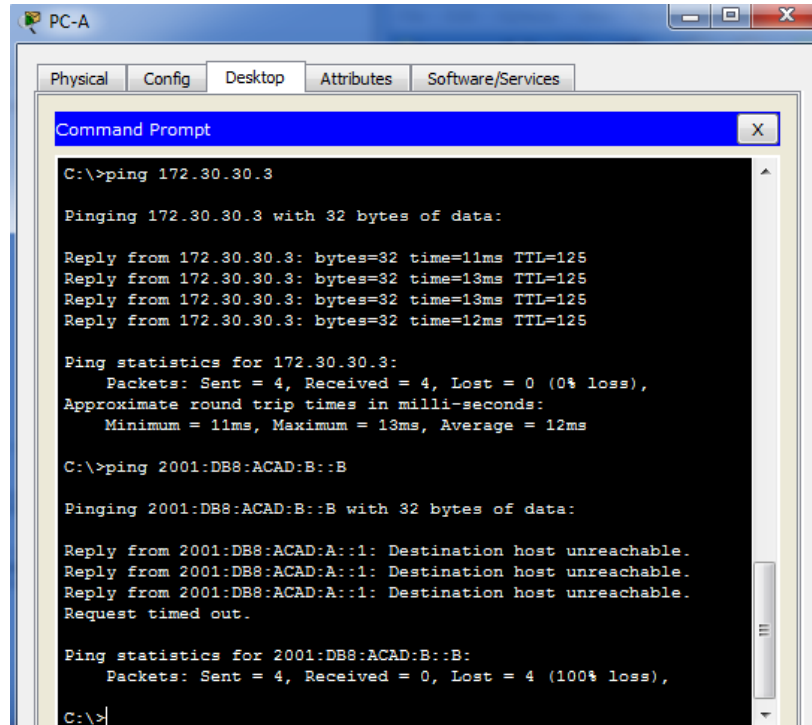
R3
-----
Physical Config CLI Attributes
-----
IOS Command Line Interface

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

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

Verifique la conectividad entre las computadoras.

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



```
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=11ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125
Reply from 172.30.30.3: bytes=32 time=12ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 12ms

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

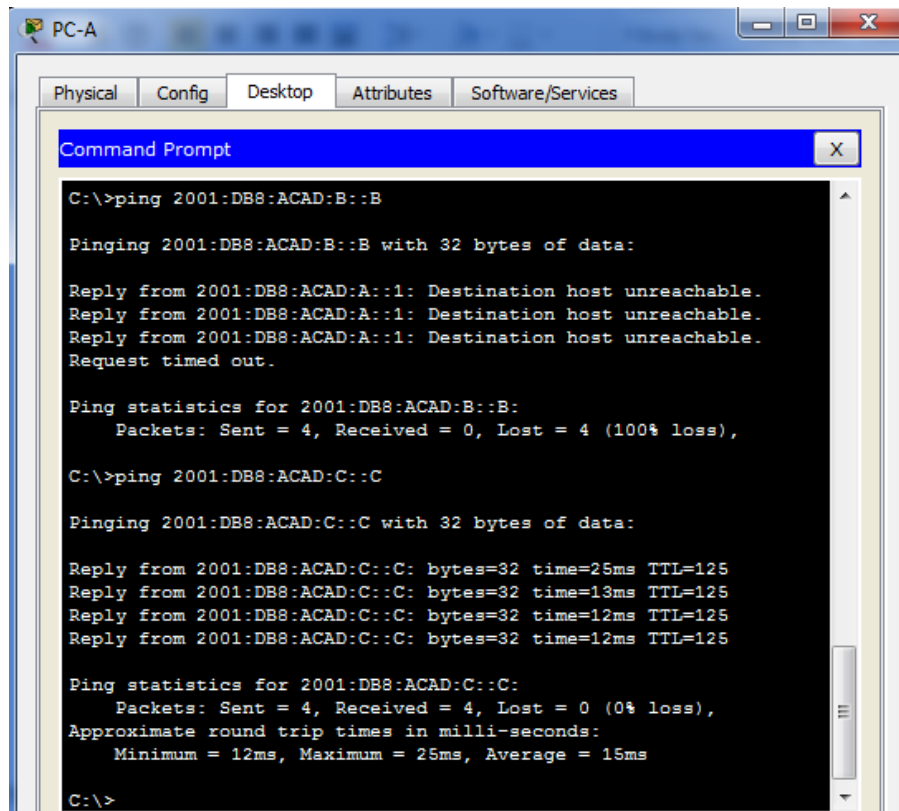
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

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

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

C:\>
```

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



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

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

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

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

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

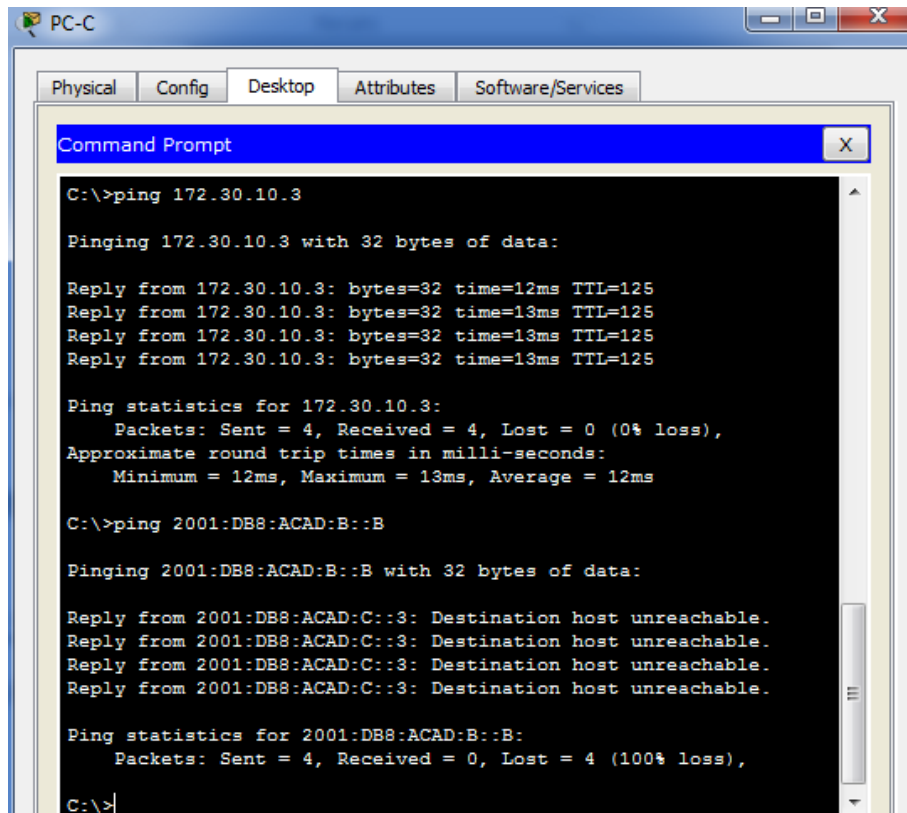
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=25ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms 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 = 12ms, Maximum = 25ms, Average = 15ms

C:\>
```

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



```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Reply from 172.30.10.3: bytes=32 time=13ms TTL=125
Reply from 172.30.10.3: bytes=32 time=13ms TTL=125
Reply from 172.30.10.3: bytes=32 time=13ms 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 = 12ms, Maximum = 13ms, Average = 12ms

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

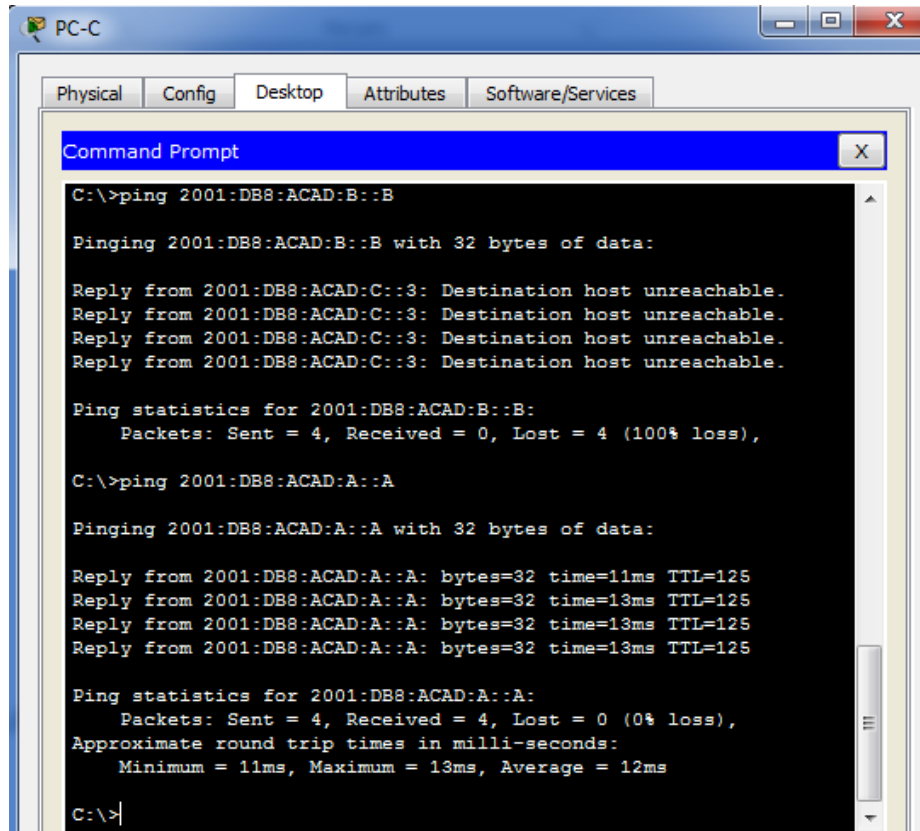
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
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),

C:\>
```

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



```

PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>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.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
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),

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

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

Reply from 2001:DB8:ACAD:A::A: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms 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 = 11ms, Maximum = 13ms, Average = 12ms

C:\>
  
```

¿Por qué algunos pings tuvieron éxito y otros no?


**No hay una ruta que se notifique para PC-B para la red 2001:DB8:ACAD:B::/64 NETWORK**

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

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

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





```

R2
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

R2>EN
R2#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#

```

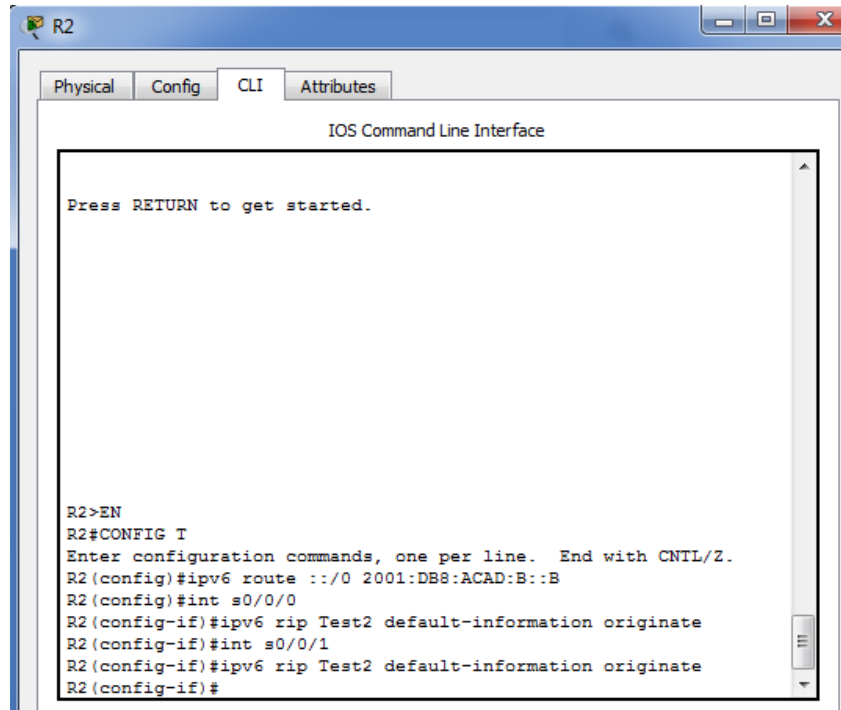
b. Las rutas estáticas se pueden incluir en las actualizaciones RIPng mediante el comando **ipv6 rip nombre de proceso default-information originate** en el modo de configuración de interfaz. Configure los enlaces seriales en el R2 para enviar la ruta predeterminada en actualizaciones RIPng.

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

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

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

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



```

R2>EN
R2#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2 (config)#int s0/0/0
R2 (config-if)#ipv6 rip Test2 default-information originate
R2 (config-if)#int s0/0/1
R2 (config-if)#ipv6 rip Test2 default-information originate
R2 (config-if)#
  
```

**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



## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

- 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

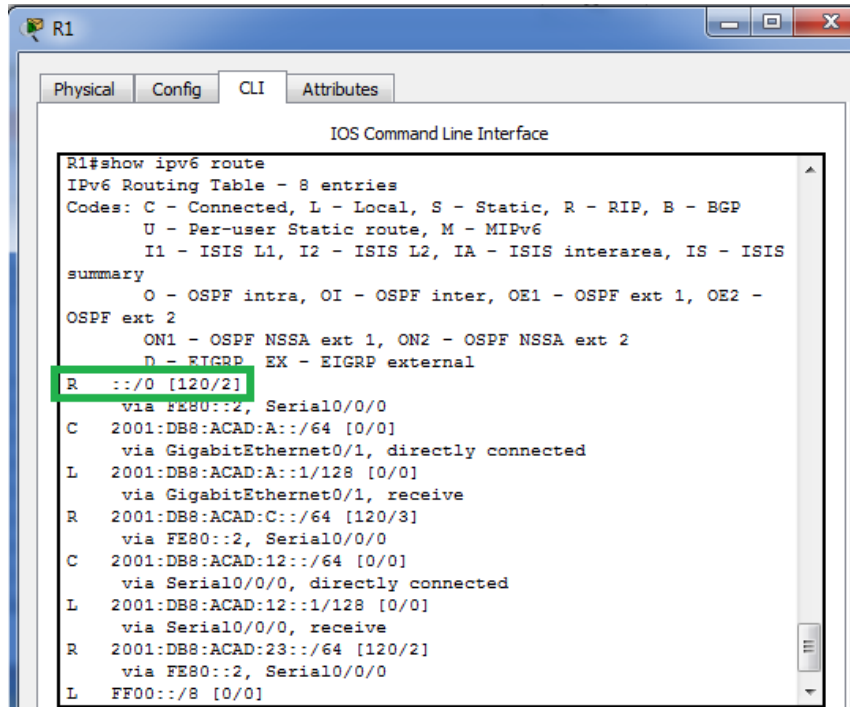
```
R2
Physical Config CLI Attributes
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

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

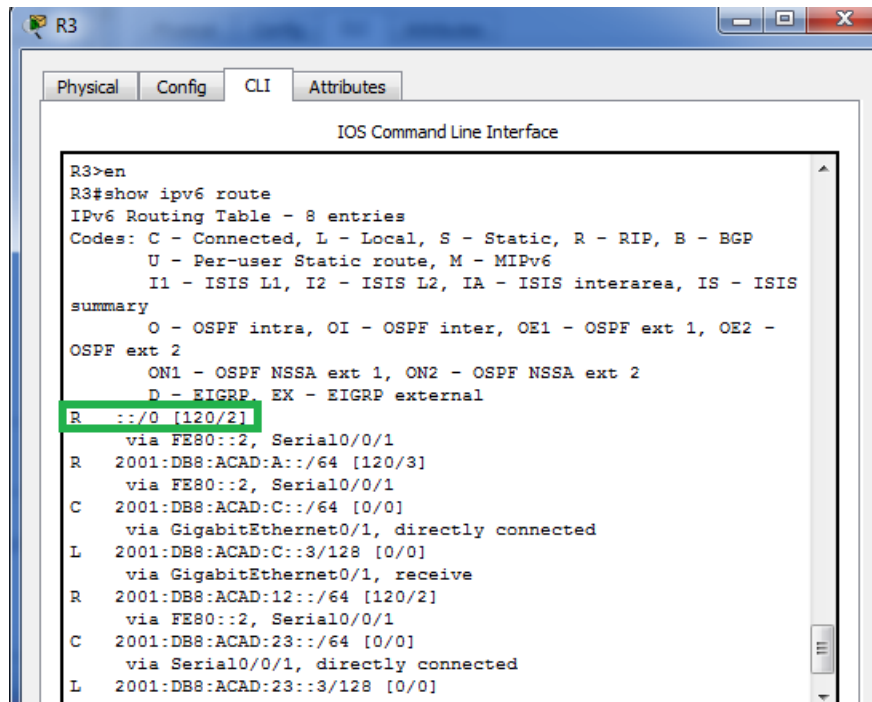
¿Cómo se puede saber, a partir de la tabla de routing, que el R2 tiene una ruta para el tráfico de Internet?

**Tiene una ruta estática por defecto que se muestra en R la señalada en verde arriba**

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



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



```

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

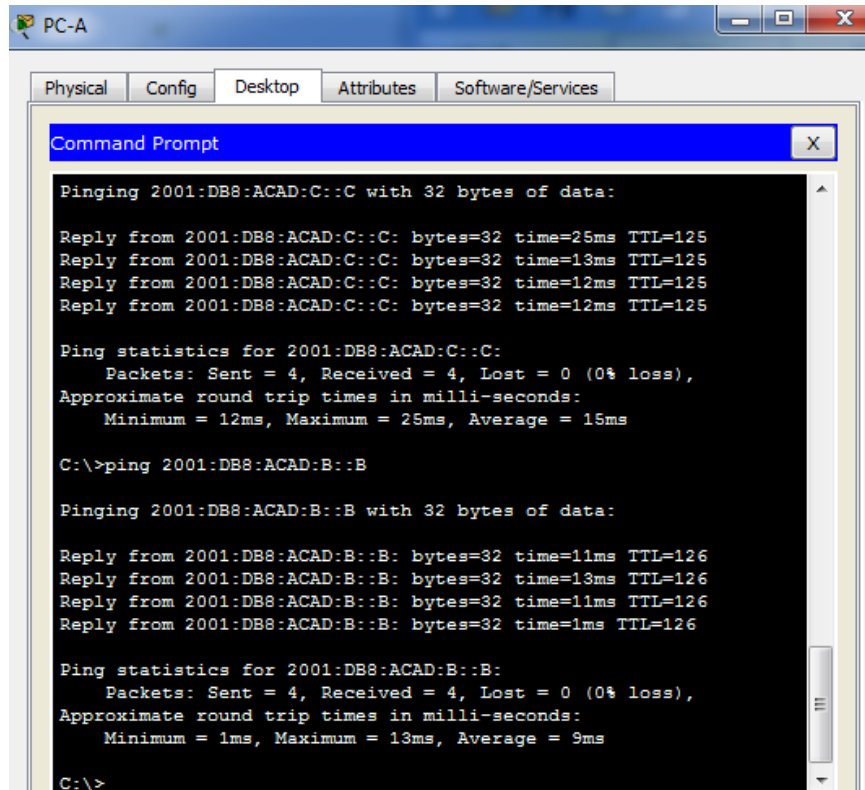
```

¿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 Attributes Software/Services
Command Prompt
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=25ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125

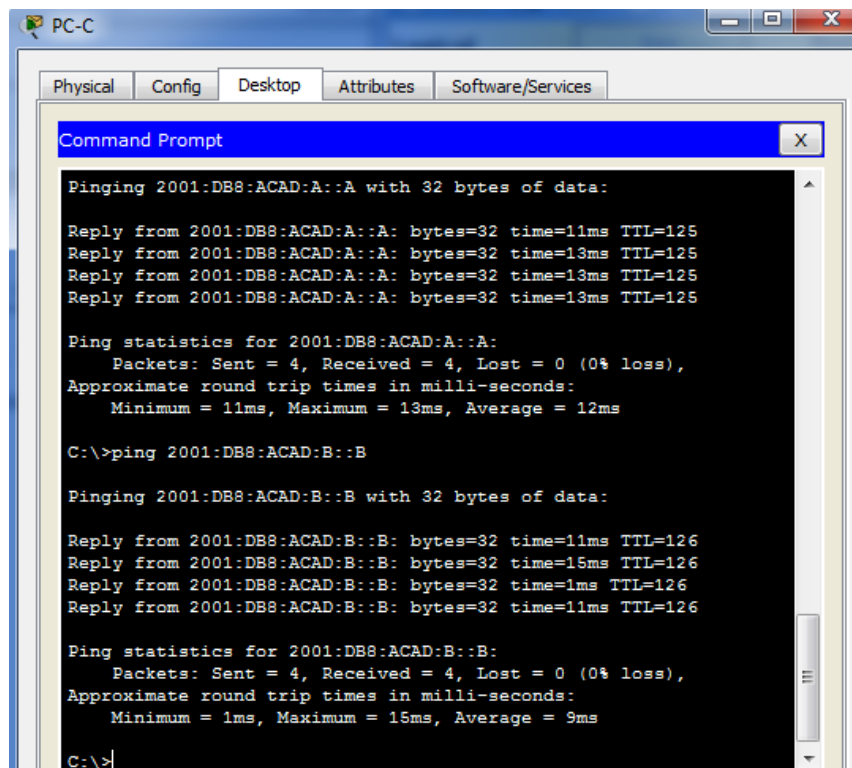
Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 25ms, Average = 15ms

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

Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=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 = 13ms, Average = 9ms

C:\>
```



```
PC-C
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms 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 = 11ms, Maximum = 13ms, Average = 12ms

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

Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=15ms 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=11ms 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 = 15ms, Average = 9ms

C:\>
```



## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

¿Tuvieron éxito los pings? SI

### Reflexión

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

**Sería bueno para que todos los routers no sumaricen las rutas hacia la clase mayor y así pueda haber continuidad entre redes discontinuas**

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

**Aprendieron de las actualizaciones de RIP recibidas desde el router 2 donde fue configurada la ruta por defecto en este caso R2**

3. ¿En qué se diferencian la configuración de RIPv2 y la de RIPv6?

**RIPv2 se configura como notificando las redes y RIPv6 se configura en las interfaces**

11.2.2.6 configuración de NAT dinámica y estática

Topología

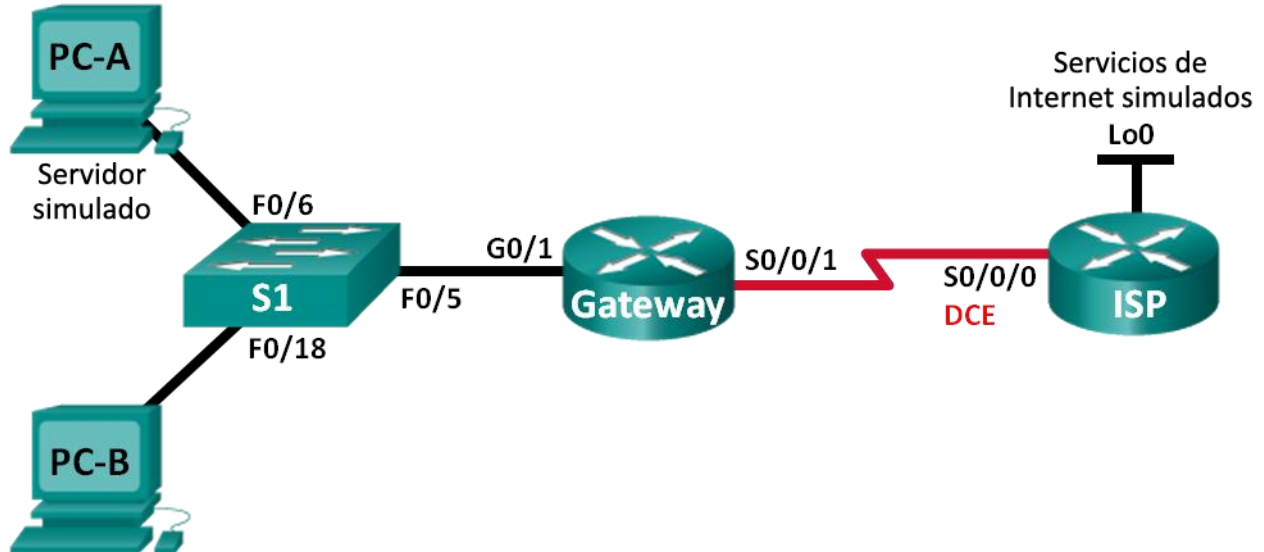


Tabla de direccionamiento

| Dispositivo              | Interfaz     | Dirección IP   | Máscara de subred | Gateway predeterminado |
|--------------------------|--------------|----------------|-------------------|------------------------|
| Gateway                  | G0/1         | 192.168.1.1    | 255.255.255.0     | N/A                    |
|                          | S0/0/1       | 209.165.201.18 | 255.255.255.252   | N/A                    |
| ISP                      | S0/0/0 (DCE) | 209.165.201.17 | 255.255.255.252   | N/A                    |
|                          | G0/0         | 192.31.7.1     | 255.255.255.0     | N/A                    |
| ServerISP                | 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





## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

### Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

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

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

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

### Recursos necesarios

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

### Parte 11: 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.

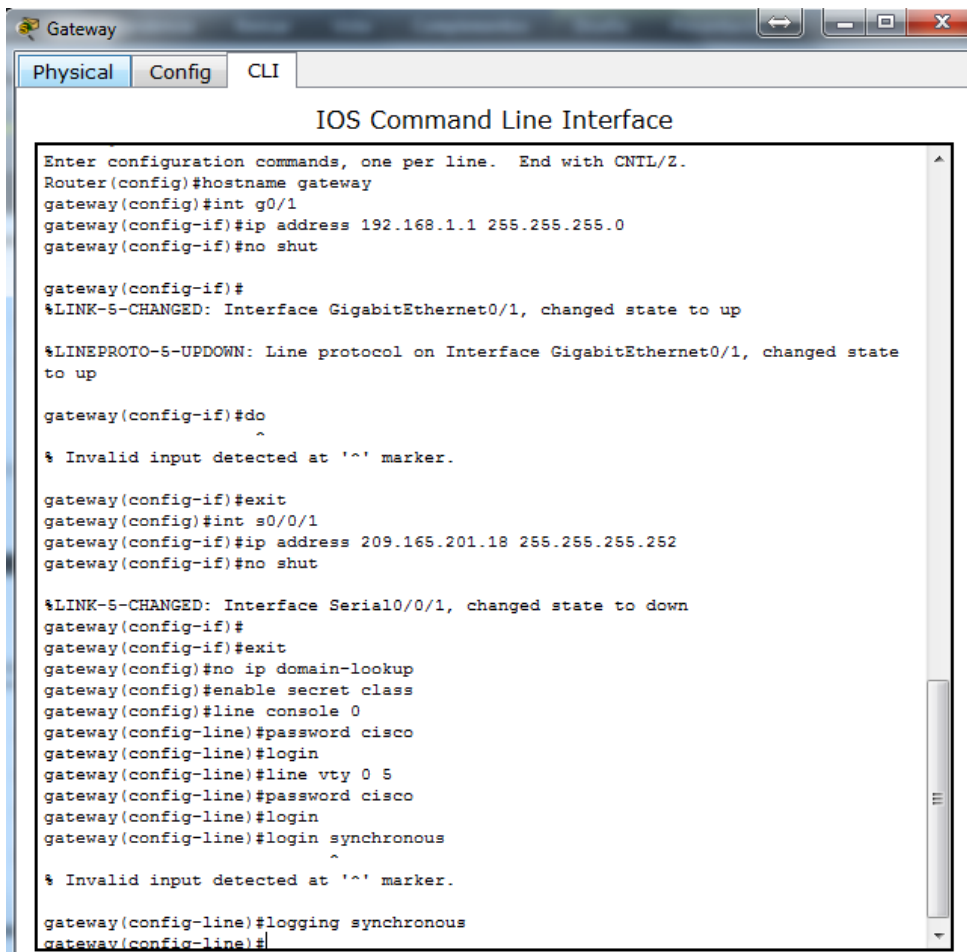
Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

**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.



```

Gateway
Physical Config CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname gateway
gateway(config)#int g0/1
gateway(config-if)#ip address 192.168.1.1 255.255.255.0
gateway(config-if)#no shut

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

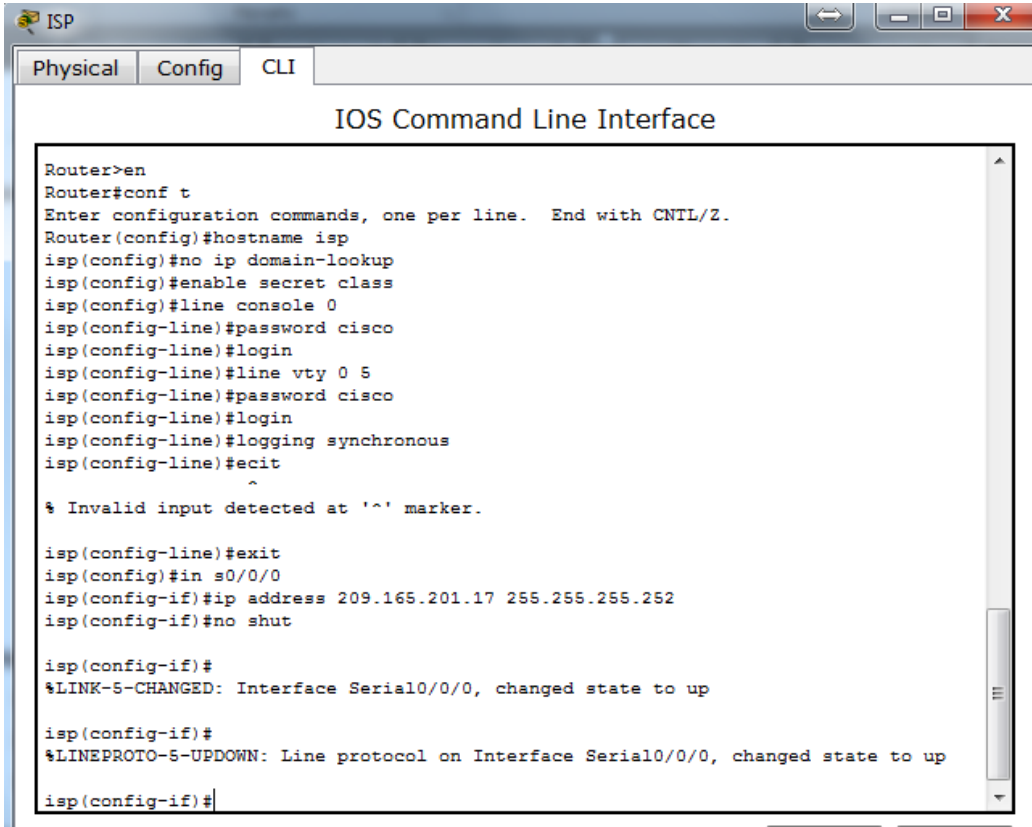
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

gateway(config-if)#do
^
% Invalid input detected at '^' marker.

gateway(config-if)#exit
gateway(config)#int s0/0/1
gateway(config-if)#ip address 209.165.201.18 255.255.255.252
gateway(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
gateway(config-if)#
gateway(config-if)#exit
gateway(config)#no ip domain-lookup
gateway(config)#enable secret class
gateway(config)#line console 0
gateway(config-line)#password cisco
gateway(config-line)#login
gateway(config-line)#line vty 0 5
gateway(config-line)#password cisco
gateway(config-line)#login
gateway(config-line)#login synchronous
^
% Invalid input detected at '^' marker.

gateway(config-line)#logging synchronous
gateway(config-line)#
  
```



```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname isp
isp(config)#no ip domain-lookup
isp(config)#enable secret class
isp(config)#line console 0
isp(config-line)#password cisco
isp(config-line)#login
isp(config-line)#line vty 0 5
isp(config-line)#password cisco
isp(config-line)#login
isp(config-line)#logging synchronous
isp(config-line)#exit
^
% Invalid input detected at '^' marker.

isp(config-line)#exit
isp(config)#in s0/0/0
isp(config-if)#ip address 209.165.201.17 255.255.255.252
isp(config-if)#no shut

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

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

isp(config-if)#
  
```

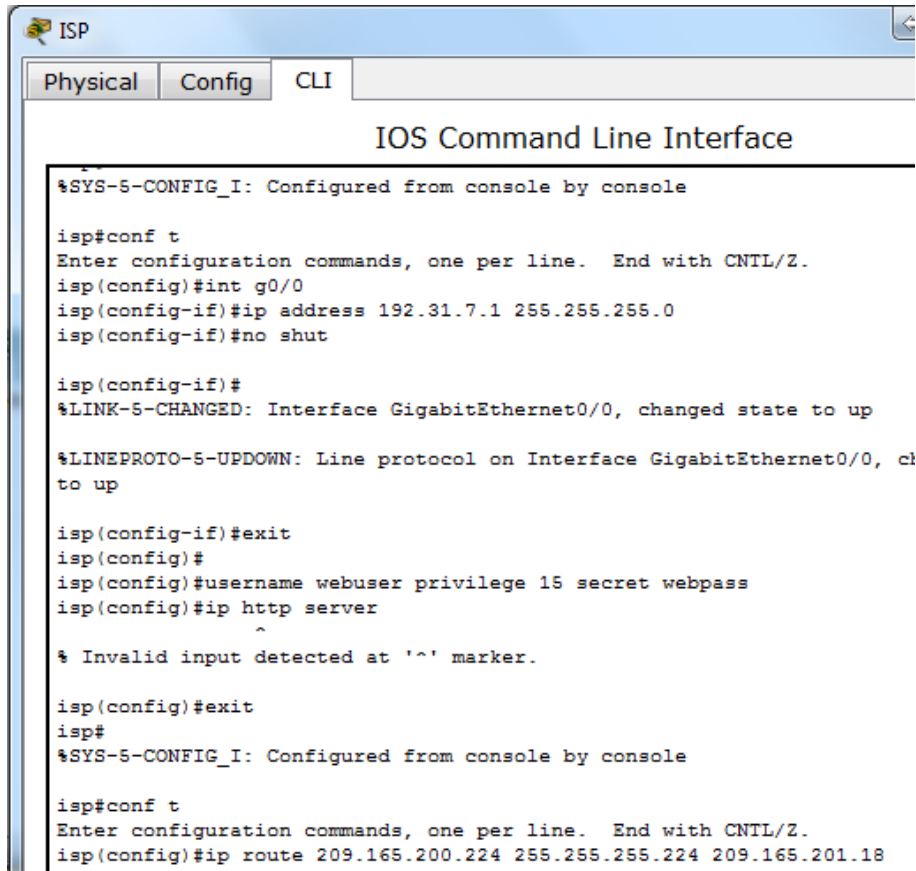
**Paso 5: crear un servidor web simulado en el ISP.**

- a. Cree un usuario local denominado **webuser** con la contraseña cifrada **webpass**.  
ISP(config)# **username webuser privilege 15 secret webpass**
- b. Habilite el servicio del servidor HTTP en el ISP.  
ISP(config)# **ip http server**
- c. Configure el servicio HTTP para utilizar la base de datos local.  
ISP(config)# **ip http authentication local**

No se puede realizar esto en packet tracer por ello se coloco un servidor WebServerISP

**Paso 6: configurar el routing estático.**

- a. Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.200.224/27.  
ISP(config)# **ip route 209.165.200.224 255.255.255.224 209.165.201.18**



```

ISP
Physical Config CLI
IOS Command Line Interface

%SYS-5-CONFIG_I: Configured from console by console

isp#conf t
Enter configuration commands, one per line. End with CNTL/Z.
isp(config)#int g0/0
isp(config-if)#ip address 192.31.7.1 255.255.255.0
isp(config-if)#no shut

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

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

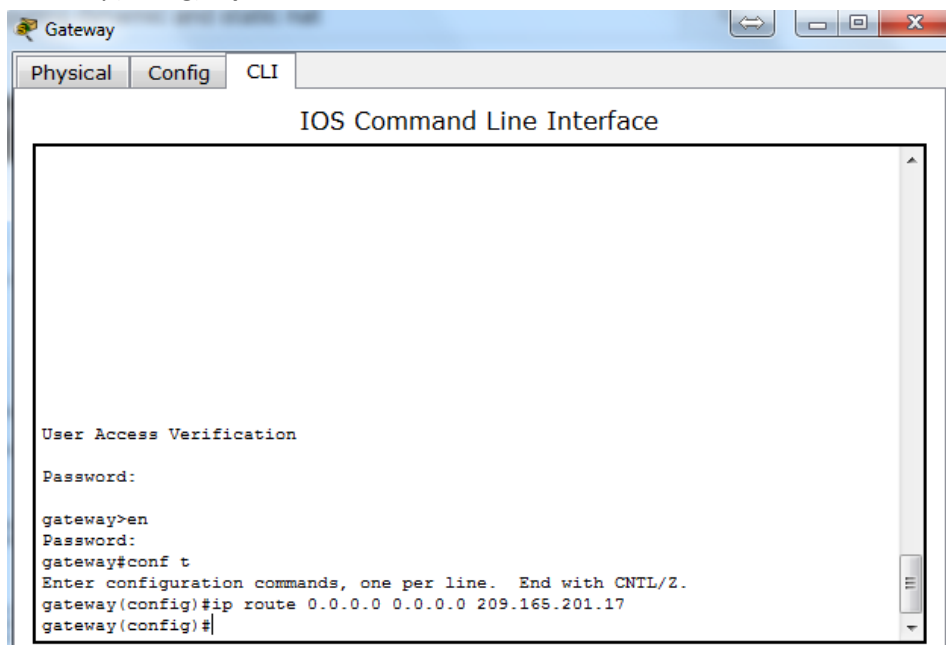
isp(config-if)#exit
isp(config)#
isp(config)#username webuser privilege 15 secret webpass
isp(config)#ip http server
^
% Invalid input detected at '^' marker.

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

isp#conf t
Enter configuration commands, one per line. End with CNTL/Z.
isp(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.18
  
```

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

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



```

Gateway
Physical Config CLI
IOS Command Line Interface

User Access Verification

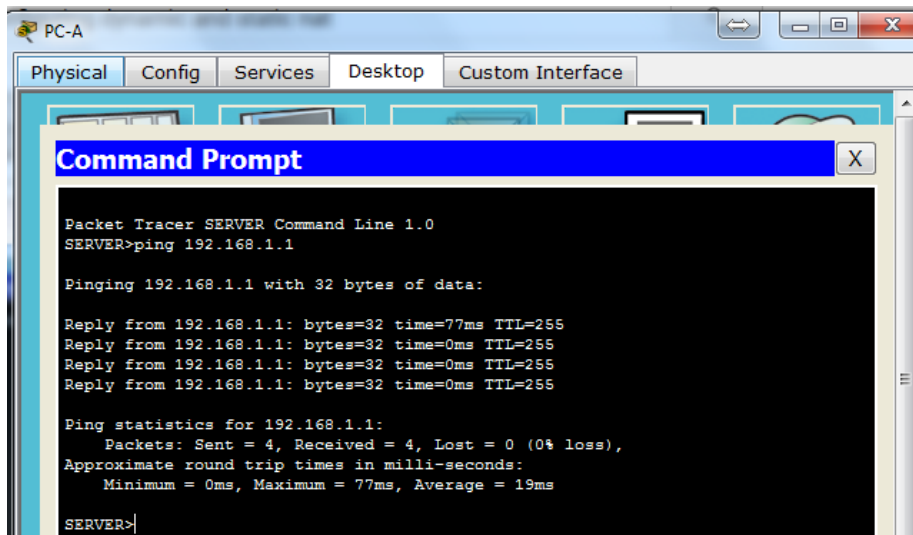
Password:

gateway>en
Password:
gateway#conf t
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
gateway(config)#
  
```

**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.



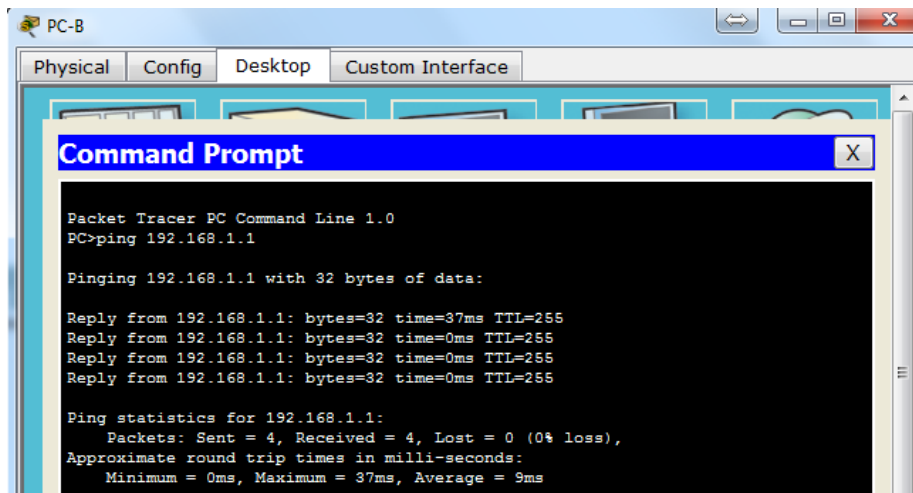
```

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=77ms 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 = 77ms, Average = 19ms
SERVER>
    
```



```

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=37ms 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 = 37ms, Average = 9ms
    
```

- 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.



# UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

```
Gateway
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
gateway>en
Password:
gateway#show ip router
^
% Invalid input detected at '^' marker.

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

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, GigabitEthernet0/1
L   192.168.1.1/32 is directly connected, GigabitEthernet0/1
  209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.201.16/30 is directly connected, Serial0/0/1
L   209.165.201.18/32 is directly connected, Serial0/0/1
S+  0.0.0.0/0 [1/0] via 209.165.201.17
gateway#
```

```
ISP
Physical Config CLI
IOS Command Line Interface
Password:
isp>en
Password:
isp#do show ip route
^
% Invalid input detected at '^' marker.

isp#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
isp(config)#
```

**Parte 12: 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**

```

gateway(config)#
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)#ip nat inside source static 192.168.1.20 209.165.200.225
gateway(config)#
  
```

**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**

```

gateway(config)#in g0/1
gateway(config-if)#ip nat inside
gateway(config-if)#int s0/0/1
gateway(config-if)#ip nat outside
gateway(config-if)#
  
```

Copy Pas

**Paso 3: probar la configuración.**

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

```

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

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

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = 209.165.200.225

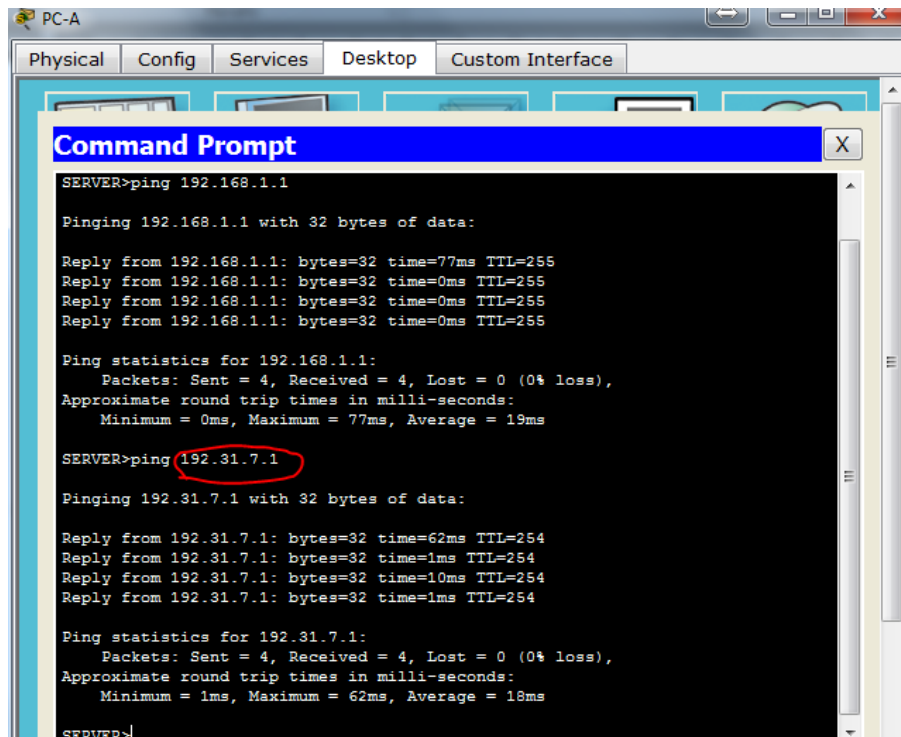
¿Quién asigna la dirección global interna?

Esta asignada por el router

¿Quién asigna la dirección local interna?

El administrador de red

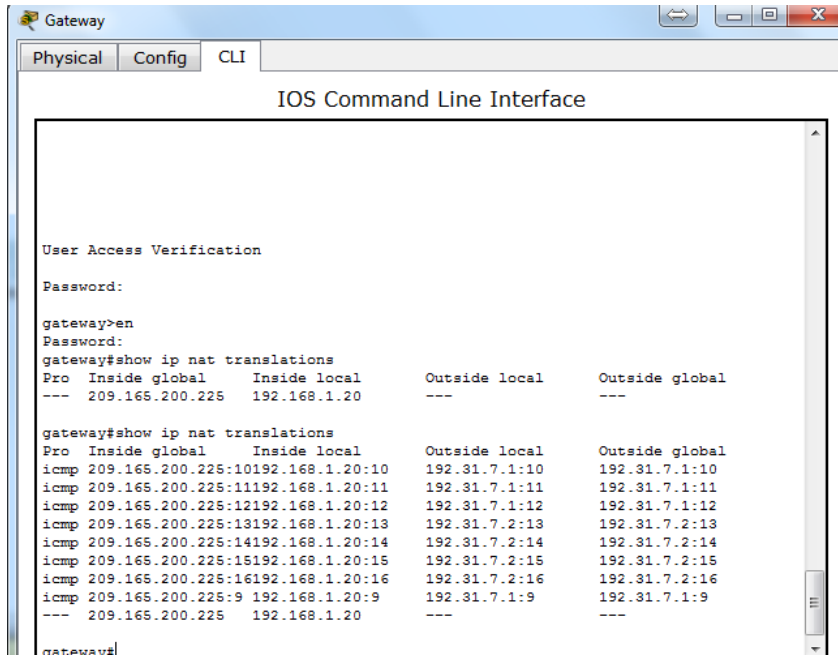
- b. En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.



Gateway# show ip nat translations

```
Pro  Inside global      Inside local      Outside local      Outside global
---  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   ---                ---
```





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.

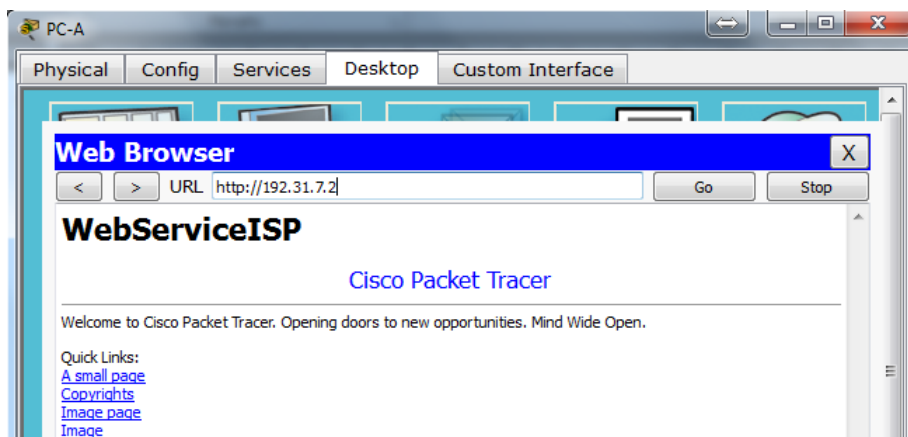
¿Qué número de puerto se usó en este intercambio ICMP? 10

**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
gateway#
```

**Nota:** es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

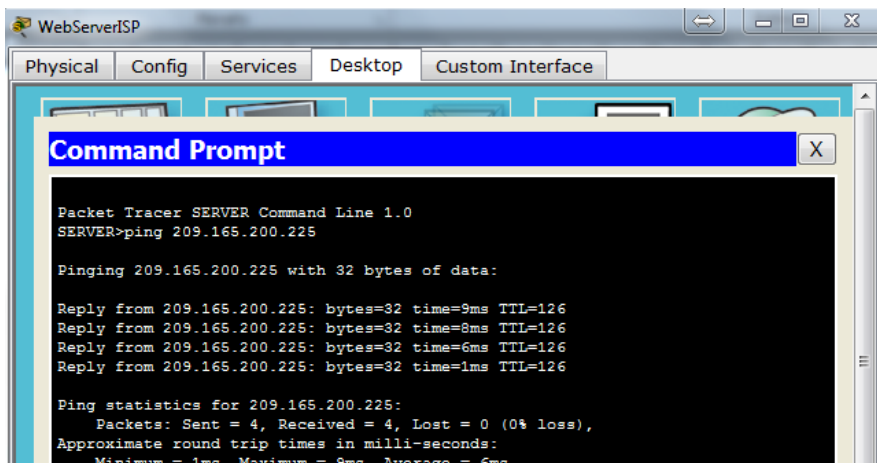
¿Qué protocolo se usó para esta traducción? **WEB**

¿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.



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

Gateway# **show ip nat translations**

```
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12  209.165.201.17:12 209.165.201.17:12
--- 209.165.200.225    192.168.1.20      ---                ---
```

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

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

Gateway# **show ip nat statistics**

```
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
```

Peak translations: 2, occurred 00:02:12 ago  
 Outside interfaces:  
   Serial0/0/1  
 Inside interfaces:  
   GigabitEthernet0/1  
 Hits: 39 Misses: 0  
 CEF Translated packets: 39, CEF Punted packets: 0  
 Expired translations: 3  
 Dynamic mappings:

Total doors: 0  
 Appl doors: 0  
 Normal doors: 0  
 Queued Packets: 0

**Nota:** este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

```
gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 22 Misses: 17
Expired translations: 16
Dynamic mappings:
gateway#
```

Copy Paste

**Parte 13: 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
```

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

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

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

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

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

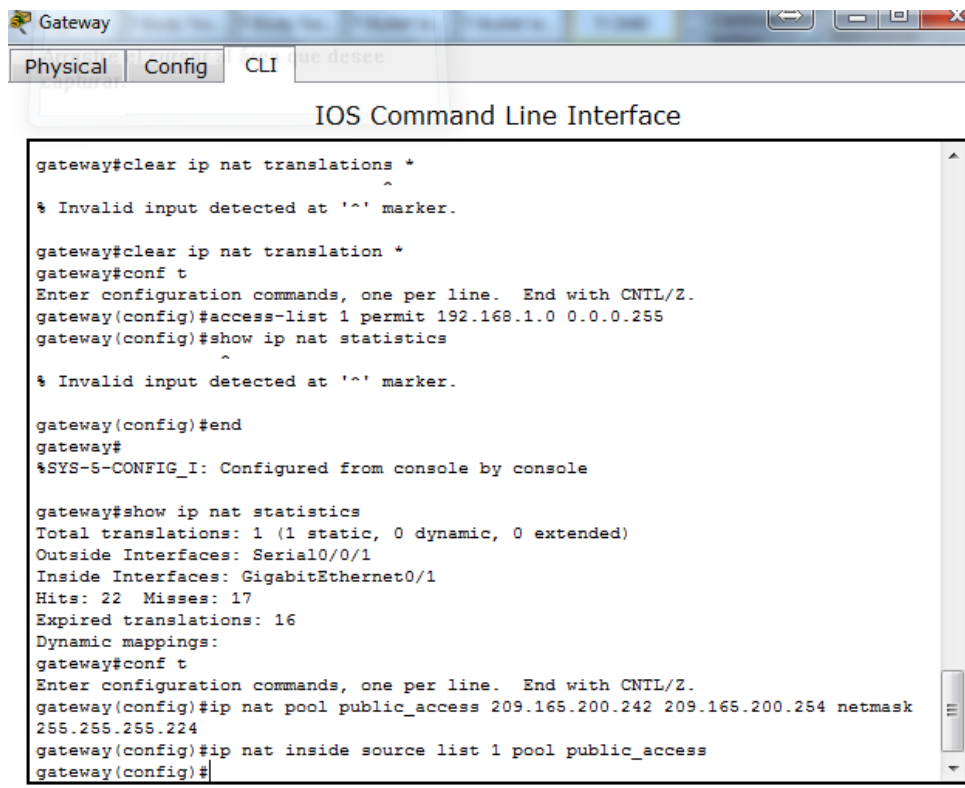
**Paso 4: definir el conjunto de direcciones IP públicas utilizables.**

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

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

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

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



```

Gateway
Physical Config CLI
IOS Command Line Interface

gateway#clear ip nat translations *
^
% Invalid input detected at '^' marker.

gateway#clear ip nat translation *
gateway#conf t
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
gateway(config)#show ip nat statistics
^
% Invalid input detected at '^' marker.

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

gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 22 Misses: 17
Expired translations: 16
Dynamic mappings:
gateway#conf t
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)#ip nat pool public_access 209.165.200.242 209.165.200.254 netmask
255.255.255.224
gateway(config)#ip nat inside source list 1 pool public_access
gateway(config)#
  
```

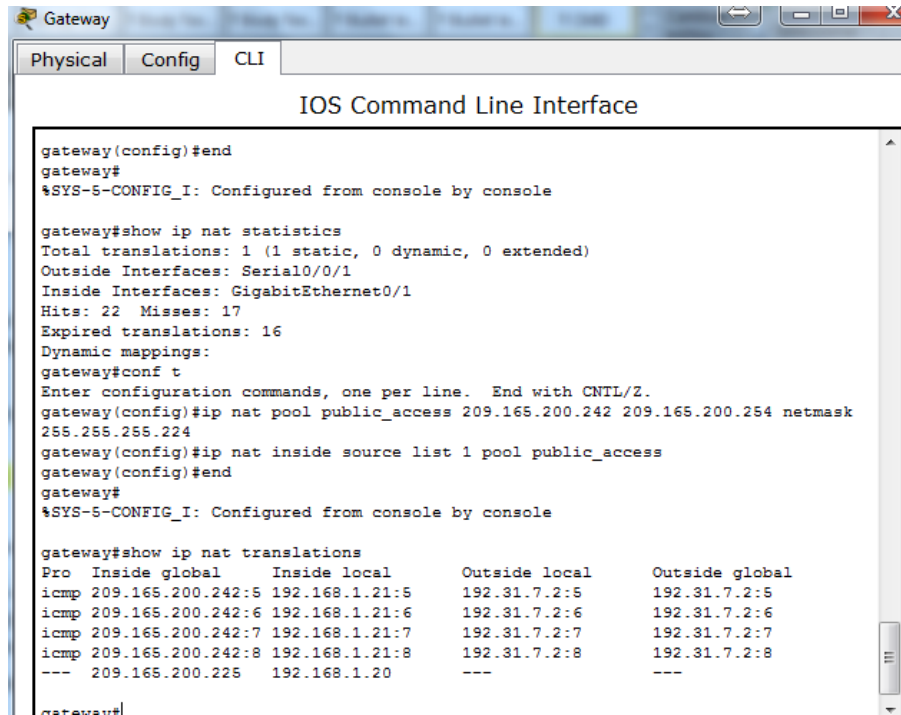
**Paso 6: probar la configuración.**

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

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

icmp 209.165.200.242:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1

--- 209.165.200.242 192.168.1.21 --- ---



```

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

gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 22 Misses: 17
Expired translations: 16
Dynamic mappings:
gateway#conf t
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)#ip nat pool public_access 209.165.200.242 209.165.200.254 netmask
255.255.255.224
gateway(config)#ip nat inside source list 1 pool public_access
gateway(config)#end
gateway#
%SYS-5-CONFIG_I: Configured from console by console

gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.242:5 192.168.1.21:5    192.31.7.2:5       192.31.7.2:5
icmp 209.165.200.242:6 192.168.1.21:6    192.31.7.2:6       192.31.7.2:6
icmp 209.165.200.242:7 192.168.1.21:7    192.31.7.2:7       192.31.7.2:7
icmp 209.165.200.242:8 192.168.1.21:8    192.31.7.2:8       192.31.7.2:8
--- 209.165.200.225    192.168.1.20      ---                 ---
  
```

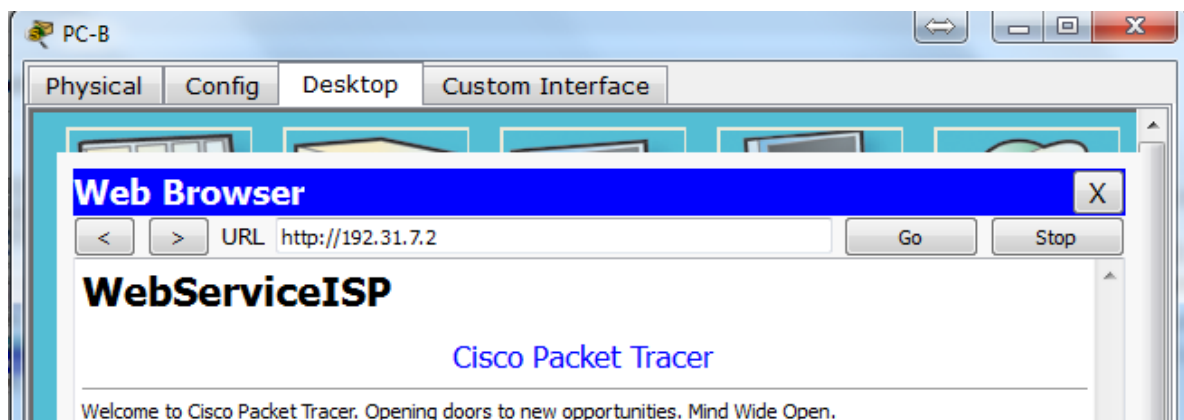
¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = 192.168.1.21:5 – 209.165.200.242

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

¿Qué número de puerto se usó en este intercambio ICMP? 5, 6 7, 8

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



- c. Muestre la tabla de NAT.



## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

```
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 172.31.7.2:80  172.31.7.2:80
tcp  209.165.200.242:1026 192.168.1.21:1026 192.31.7.2:80  192.31.7.2:80
gateway#
```

¿Qué protocolo se usó en esta traducción? `http`

¿Qué números de puerto se usaron?

Interno: 1025

Externo: 80

¿Qué número de puerto bien conocido y qué servicio se usaron? 80

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

```
Gateway# show ip nat statistics
```

```
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
```

```
Peak translations: 17, occurred 00:06:40 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```

GigabitEthernet0/1

Hits: 345 Misses: 0

CEF Translated packets: 345, CEF Punted packets: 0

Expired translations: 20

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public\_access refcount 2

pool public\_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

**Nota:** este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

```

gateway#show ip nat statistics
Total translations: 3 (1 static, 2 dynamic, 2 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 44 Misses: 29
Expired translations: 20
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 2
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 1 (7%), misses 0
gateway#

```

**Paso 7: eliminar la entrada de NAT estática.**

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

- a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

Gateway(config)# **no ip nat inside source static 192.168.1.20 209.165.200.225**

Static entry in use, do you want to delete child entries? [no]: **yes**

- b. Borre las NAT y las estadísticas.
- c. Haga ping al ISP (192.31.7.1) desde ambos hosts.
- d. Muestre la tabla y las estadísticas de NAT.



## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

Gateway# **show ip nat statistics**

Total active translations: 4 (0 static, 4 dynamic; 2 extended)

Peak translations: 15, occurred 00:00:43 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 16 Misses: 0

CEF Translated packets: 285, CEF Punted packets: 0

Expired translations: 11

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public\_access refcount 4

pool public\_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

```
gateway#show ip nat statistics
Total translations: 2 (0 static, 2 dynamic, 2 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 52 Misses: 37
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 2
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 1 (7%), misses 0
gateway#
```

Gateway# **show ip nat translation**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512 192.31.7.1:512

--- 209.165.200.243 192.168.1.20 --- ---

icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512 192.31.7.1:512

--- 209.165.200.242 192.168.1.21 --- ---

**Nota:** este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.





**Reflexión**

1. ¿Por qué debe utilizarse la NAT en una red?

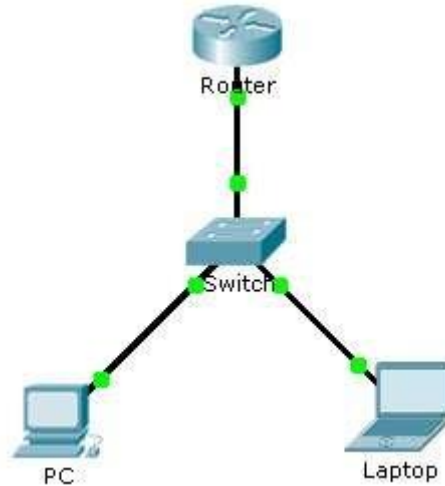
Existen para que no se acabaran las IP en IPv4, se ahorran IP, ayudan para la privacidad porque no muestran la IP.

2. ¿Cuáles son las limitaciones de NAT?

Es un poco demorada su configuración y algunos servicios no pueden funcionar

9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines

Topology



Addressing Table

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

Objectives

Part 1: Configure and Apply an ACL

to VTY Lines Part 2: Verify the ACL

Implementation

Background

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

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



## UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

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

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

---

**Packet Tracer - Configuring an ACL on VTY Lines****Step 2: Configure a numbered standard ACL.**

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

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

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

**IOS Command Line Interface**

```
63406K Bytes Of RAM CompiledFlash (read/write)
Press RETURN to get started!

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

Router>
Router>configure terminal
      ^
% Invalid input detected at '^' marker.

Router>
Router>config t
      ^
% Invalid input detected at '^' marker.

Router>enable
Router#cisco
Translating "cisco"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

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)#
Router(config)#
```

Copy

Paste

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

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

Router(config)# line vty 0 15

Router(config-line)# access-class 99 in

IOS Command Line Interface

```

Translating cisco...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

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)#
Router(config)#line vty
% Incomplete command.
Router(config)#line vty 0 15
Router(config-line)#access class 99 in
^
% Invalid input detected at '^' marker.

Router(config-line)#access-class 99 in
^
% Invalid input detected at '^' marker.

Router(config-line)# access?
access-class
Router(config-line)#
Router(config-line)#access?
access-class
Router(config-line)#access?
access-class
Router(config-line)#access
% Incomplete command.
Router(config-line)#access-class 99 in
Router(config-line)#
  
```

## Part 2: Verify the ACL Implementation

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

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

```

% Invalid input detected at '^' marker.

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#
Router#
Router#
  
```

```

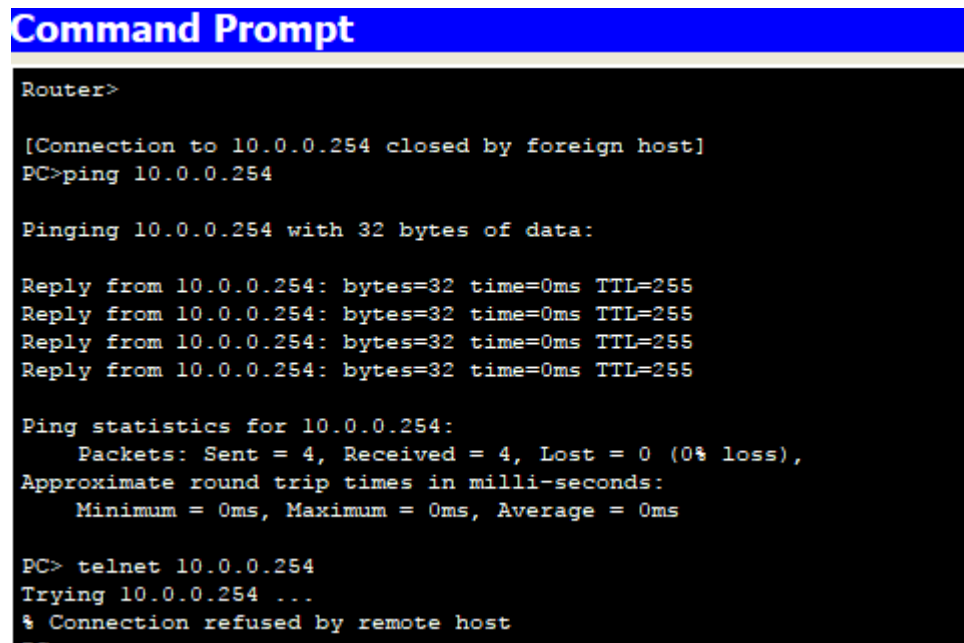
.
line vty 0 4
  access-class 99 in
  password cisco
  login
line vty 5 15
  access-class 99 in
  password cisco
  login
!
!
!
end

```

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

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

Laptop con acceso denegado



The screenshot shows a Windows Command Prompt window with a blue title bar that reads "Command Prompt". The text inside the window is as follows:

```

Router>

[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=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
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 milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC> telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host

```

PC con IP 10.0.0.1 con acceso permitido.

```
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=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
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 milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>
```

10.1.2.4 configuración de DHCPv4 básico en un router

Topología

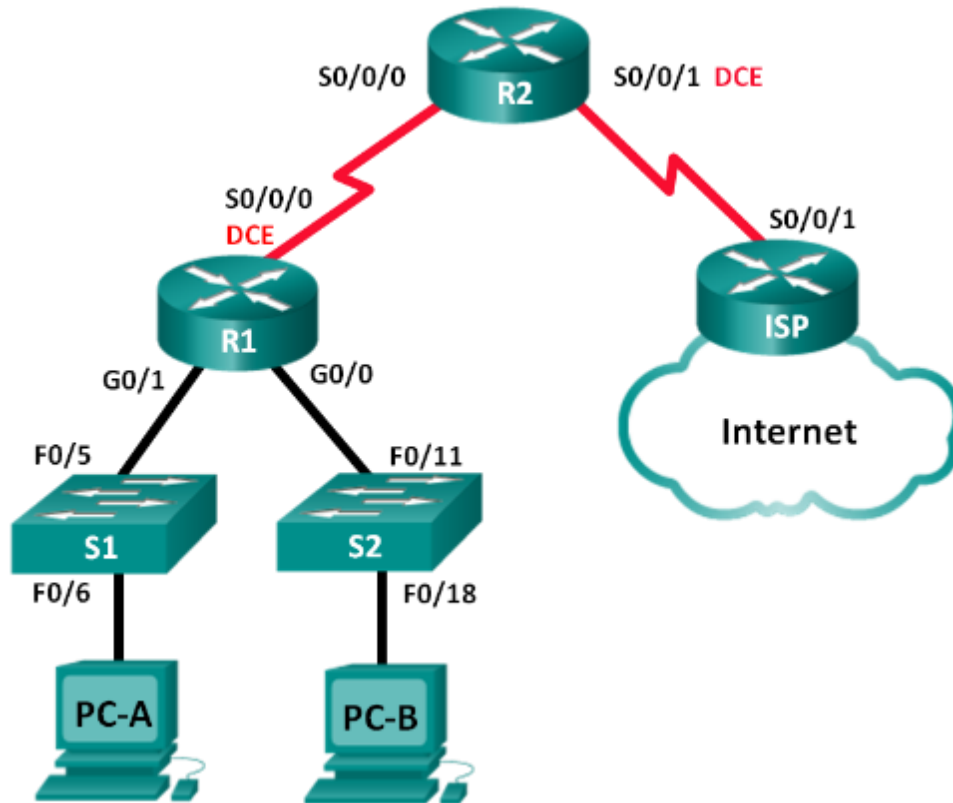


Tabla de direccionamiento

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



## Objetivos

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

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

## Información básica/situación

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

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

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

**Nota:** los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universal9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbase9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

## Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbase9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

**Parte 14: armar la red y configurar los parámetros básicos de los dispositivos**

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

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

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

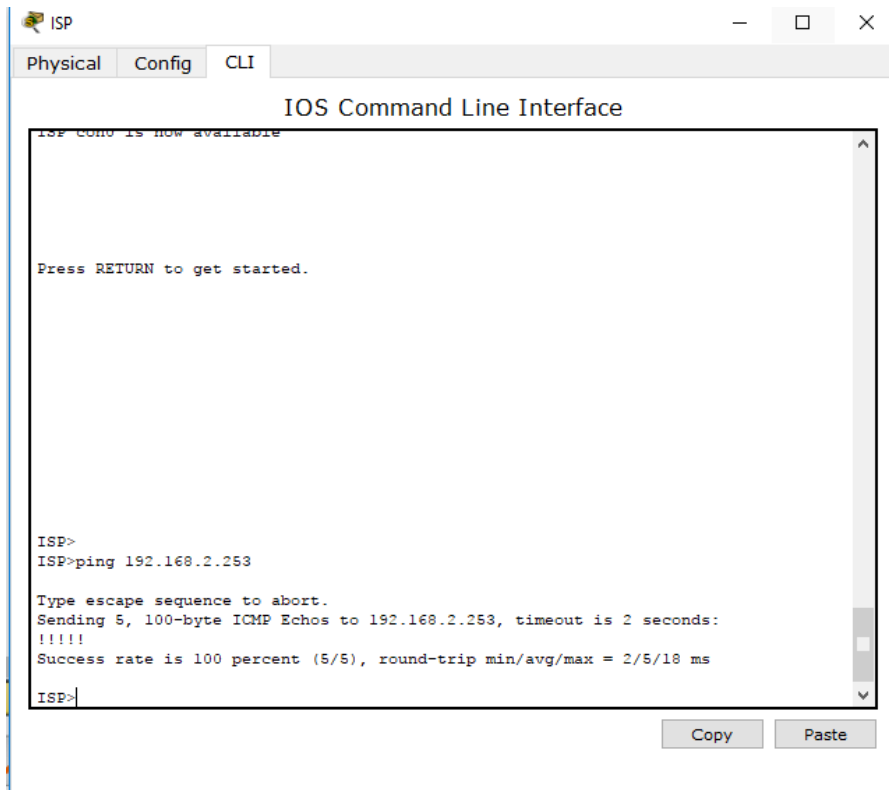
**Paso 3: configurar los parámetros básicos para cada router.**

- a. Desactive la búsqueda DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- e. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.
- f. Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.
- g. Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.
- h. Configure EIGRP for R1.  
R1(config)# **router eigrp 1**  
R1(config-router)# **network 192.168.0.0 0.0.0.255**  
R1(config-router)# **network 192.168.1.0 0.0.0.255**  
R1(config-router)# **network 192.168.2.252 0.0.0.3**  
R1(config-router)# **no auto-summary**
- i. Configure EIGRP y una ruta predeterminada al ISP en el R2.  
R2(config)# **router eigrp 1**  
R2(config-router)# **network 192.168.2.252 0.0.0.3**  
R2(config-router)# **redistribute static**  
R2(config-router)# **exit**  
R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.200.225**
- j. Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.  
ISP(config)# **ip route 192.168.0.0 255.255.252.0 209.165.200.226**
- k. Copie la configuración en ejecución en la configuración de inicio

**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.

Comprobacion de conectividad entre ISP hasta R1 exitoso.



```

ISP
Physical Config CLI
IOS Command Line Interface
ISP CONO is now available

Press RETURN to get started.

ISP>
ISP>ping 192.168.2.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/18 ms

ISP>
    
```

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

**Parte 15: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP**

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

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

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

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

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

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

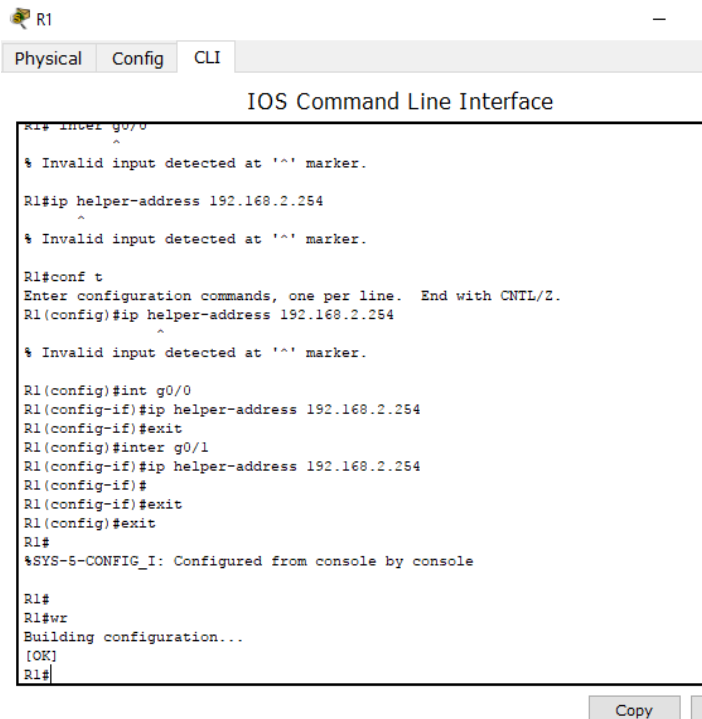
En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando **ipconfig /all**. ¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué?

No han recibido IP, y la razón es porque el servidor DHCP se encuentra en el R2 y aún no ha sido configurado en R1 para trasladar.

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

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

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



```

R1
-----
Physical Config CLI
IOS Command Line Interface
R1# int e0/0
^
% Invalid input detected at '^' marker.

R1# ip helper-address 192.168.2.254
^
% Invalid input detected at '^' marker.

R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip helper-address 192.168.2.254
^
% Invalid input detected at '^' marker.

R1(config)# int g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config)# int g0/1
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)#
R1(config-if)# exit
R1(config)# exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#wr
Building configuration...
[OK]
R1#
  
```

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

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

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0010.1100.8D15
Link-local IPv6 Address.....: FE80::210:11FF:FE00:8D15
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 Client DUID.....: 00-01-00-01-D5-B3-A4-2D-00-10-11-00-8D-15
```

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0030.F2E7.3CA2
Link-local IPv6 Address.....: FE80::230:F2FF:FEE7:3CA2
IP Address.....: 192.168.0.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.0.1
DNS Servers.....: 209.165.200.225
DHCP Servers.....: 192.168.2.254
DHCPv6 Client DUID.....: 00-01-00-01-A0-56-74-DA-00-30-F2-E7-3C-A2
```

---

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?

[192.168.0.10 y 192.168.1.10](#)

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

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

```

R2#
R2#show ip dhcp binding
IP address      Client-ID/      Lease expiration  Type
                Hardware address
192.168.1.10    0010.1100.8D15  --                Automatic
192.168.0.10    0030.F2E7.3CA2  --                Automatic
R2#
R2#
R2#

```

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

Mac Address, Tiempo de expiración, y tipo de asignación

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

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

En packet trace no es posible visualizar estadísticas.

- 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)?

Packet trace no permite ver información de estos comandos por no tratarse de un dhcp real.

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

Resultado de Show Run.

```

!
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
!

```

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

**R1**

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
```

G0/1

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

## Reflexión

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

Se ahorra la configuración de dhcp en los routers y así se aprovecha el rendimiento de estos y que solo uno haga el trabajo de DHCP. Administración más sencilla y centralizada.

10.1.2.5 configuración de DHCPv4 básico en un switch

Topología

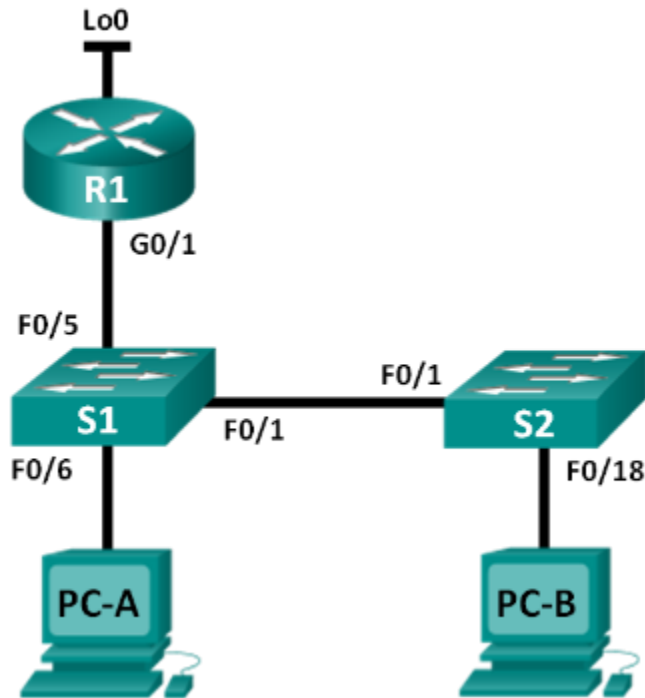


Tabla de direccionamiento

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

Objetivos

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

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

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

**Parte 3: configurar DHCPv4**

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



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

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

**Parte 5: habilitar el routing IP**

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

**Información básica/situación**

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

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

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

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

**Recursos necesarios**

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

## Parte 16: armar la red y configurar los parámetros básicos de los dispositivos

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

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

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

- a. Asigne los nombres de dispositivos como se muestra en la topología.
- b. Desactive la búsqueda del DNS.
- c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
- d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.
- e. Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.
- f. Guarde la configuración en ejecución en el archivo de configuración de inicio.

## Parte 17: cambiar la preferencia de SDM

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

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

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

```
S1# show sdm prefer
```

```
The current template is "default" template.
```

```
The selected template optimizes the resources in  
the switch to support this level of features for  
0 routed interfaces and 255 VLANs.
```

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

¿Cuál es la plantilla actual?

---

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

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

```
S1(config)# sdm prefer lanbase-routing
```

```
Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.
```

```
Use 'show sdm prefer' to see what SDM preference is currently active.
```

```
¿Qué plantilla estará disponible después de la recarga?
```

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

```
S1# reload
```

```
System configuration has been modified. Save? [yes/no]: no
```

```
Proceed with reload? [confirm]
```

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

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

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

```
S1# show sdm prefer
```

```
The current template is "lanbase-routing" template.
```

```
The selected template optimizes the resources in the switch to support this level of features for
```

```
0 routed interfaces and 255 VLANs.
```

```
number of unicast mac addresses:      4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes:        0.75K
  number of directly-connected IPv4 hosts: 0.75K
  number of indirect IPv4 routes:      16
number of IPv6 multicast groups:      0.375k
number of directly-connected IPv6 addresses: 0.75K
  number of indirect IPv6 unicast routes: 16
```



number of IPv4 policy based routing aces: 0  
number of IPv4/MAC qos aces: 0.125k  
number of IPv4/MAC security aces: 0.375k  
number of IPv6 policy based routing aces: 0  
number of IPv6 qos aces: 0.375k  
number of IPv6 security aces: 127

**Parte 18: configurar DHCPv4**

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

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

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

---

---

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

---

---

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

---

---

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

---

---

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

---

---

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

---

```

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)#
  
```

Copy

Paste

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

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

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

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.1.1 \_\_\_\_\_

Máscara de subred: 255.255.255.0 \_\_\_\_\_

Gateway predeterminado: 192.168.1.1 \_\_\_\_\_

```

Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0060.7007.337A
Link-local IPv6 Address.....: FE80::260:70FF:FE07:337A
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-A7-6E-62-43-00-60-70-07-33-7A

PC>
  
```

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 \_\_\_\_\_

```

Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0007.ECC7.E07E
Link-local IPv6 Address.....: FE80::207:ECFF:FEC7:E07E
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.....: 00-01-00-01-52-17-54-B1-00-07-EC-C7-E0-7E

PC>

```

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

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

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

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

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

```

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=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
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 = 0ms, Average = 0ms

```

```

PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=1ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255

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 = 1ms, Average = 0ms

```

## Parte 19: configurar DHCPv4 para varias VLAN

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

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

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

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

- a. Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.  
 \_\_ip dhcp exclude-address 192.168.2.1 192.168.2.10
- b. Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó.  
 \_\_ip dhcp pool DHCP2

- c. Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.  
 \_\_\_network 192.168.2.0 255.255.255.0 \_\_\_\_\_
- d. Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.  
 \_\_\_default-router 192.168.2.1 \_\_\_\_\_
- e. Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.  
 \_\_\_dns-server 192.168.2.9 \_\_\_\_\_
- f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.  
 \_\_\_lease 3 \_\_\_\_\_
- g. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```

S1(config)#ip dhcp
% Incomplete command.
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)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
S1#

```

**Paso 3: verificar la conectividad y DHCPv4.**

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

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.2.11

Mascara de subred: 255.255.255.0 \_\_\_\_\_

Gateway predeterminado: 192.168.2.1 \_\_\_\_\_



```

PC>ipconfig /release

IP Address . . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . : 0.0.0.0
DNS Server . . . . . : 0.0.0.0

PC>
PC>ipconfig /renew

IP Address . . . . . : 192.168.2.11
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
DNS Server . . . . . : 192.168.2.9
  
```

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

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

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

¿Los pings eran correctos? ¿Por qué?

No puede alcanzar la red 192.168.1.0 por que el router aun no hace routing

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

¿Qué resultado arrojó este comando?

```

-
C 192.168.1.0/24 is directly connected, Vlan1
C 192.168.2.0/24 is directly connected, Vlan2
  
```

## Parte 20: habilitar el routing IP

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

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

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

S1(config)# **ip routing**

- b. Verificar la conectividad entre las VLAN.

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

¿Qué función realiza el switch?

Cumple funciones de routing ahora

- c. Vea la información de la tabla de routing para el S1.

¿Qué información de la ruta está incluida en el resultado de este comando?

```
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#
```

Información de la tabla de routing para el R1.

¿Qué información de la ruta está incluida en el resultado de este comando?

```
Gateway of last resort is not set

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

- d. ¿Es posible hacer ping de la PC-A al R1? \_\_\_SI\_\_\_\_\_

¿Es posible hacer ping de la PC-A a la interfaz Lo0? \_\_\_SI\_\_\_\_\_

```

PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

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

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=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms 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 = 0ms, Average = 0ms

```

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

---

**Paso 2: asignar rutas estáticas.**

Habilitar el routing IP permite que el switch enrute entre VLAN asignadas en el switch. Para que todas las VLAN se comuniquen con el router, es necesario agregar rutas estáticas a la tabla de routing del switch y del router.

- a. En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.

\_\_ip route 0.0.0.0 0.0.0.0 192.168.1.10 \_\_\_\_\_

- b. En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

\_\_ip route 192.168.2.0 255.255.255.0 g0/1 \_\_\_\_\_

- c. Vea la información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?

```
Gateway of last resort is 192.168.1.10 to network
```

```
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
R1#
```

- d. Vea la información de la tabla de routing para el R1.

¿Cómo está representada la ruta estática?

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

```
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.10/32 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 is directly connected, GigabitEthernet0/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.224/27 is directly connected, Loopback0
L    209.165.200.225/32 is directly connected, Loopback0
R1#
```

- e. ¿Es posible hacer ping de la PC-A al R1? \_\_\_SI\_\_\_\_\_

¿Es posible hacer ping de la PC-A a la interfaz Lo0? \_\_\_SI\_\_\_\_\_



**Reflexión**

1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

Por que las direcciones asignadas a los equipos como router, switches o servidores deben ser fijas para evitar indisponibilidad de los servicios y problemas con los equipos de comunicación.

---

2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

\_Asignando cada pool a un puerto de switch diferente\_\_\_\_\_

3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?

Esta cumpliendo funciones de capa 3 - routing\_\_\_\_\_

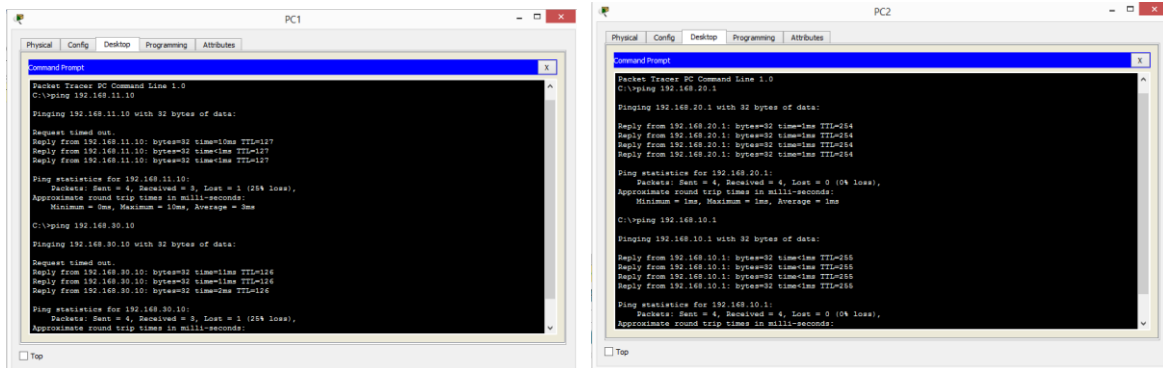
**168.2.0 255.255.255.0 g0/1**

**Tarea 9.2.1.10 PACKET TRACER – CONFIGURING STANDARD ACLS**

**Parte 1. Plan an ACL Implementation**

**Paso 1.** Investigate the current network configuration.

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



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

- a. The following network policies are implemented on **R2**:
  - The 192.168.11.0/24 network is not allowed access to the **WebServer** on the 192.168.20.0/24 network..
  - All other access is permitted.

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

- b. The following network policies are implemented on **R3**:
  - The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
  - All other access is permitted.

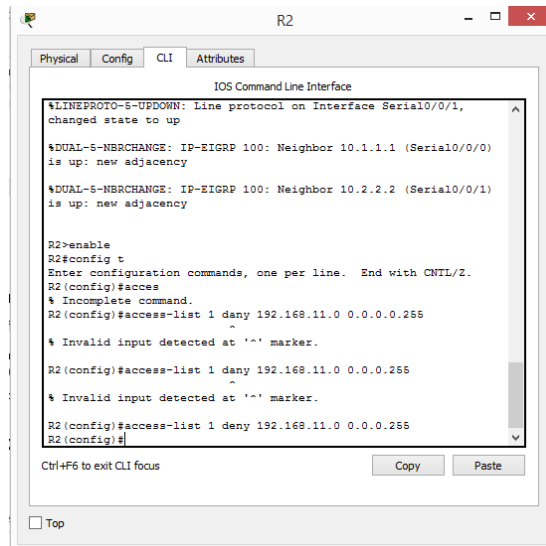
To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

**Parte 2. Configure, Apply, and Verify a Standard ACL**

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

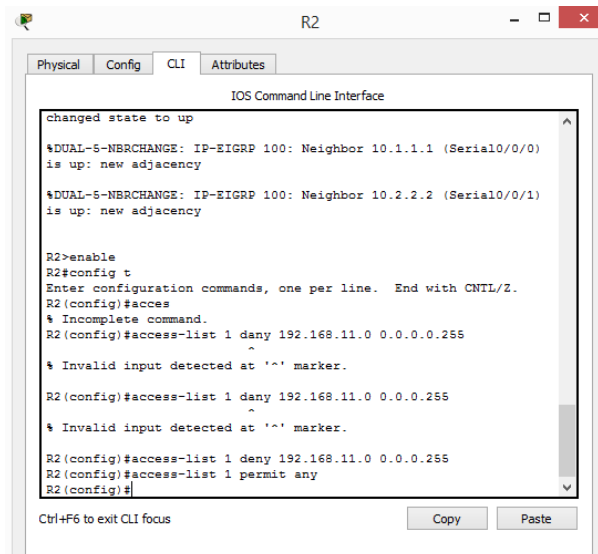
a. Create an ACL using the number 1 on **R2** with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.

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



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

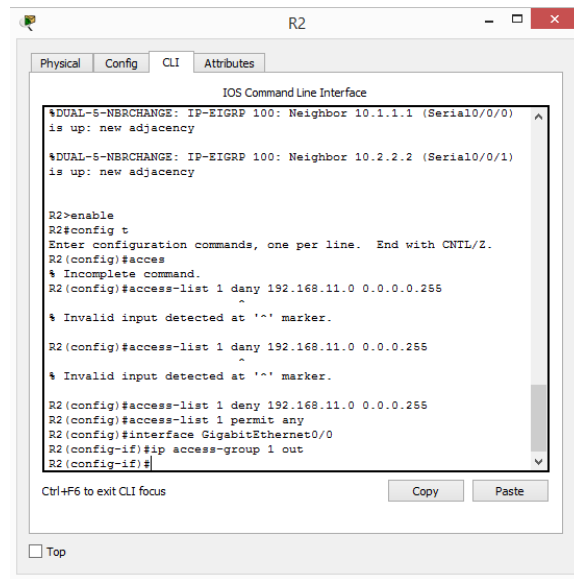
R2(config)# **access-list 1 permit any**



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

R2(config)# **interface GigabitEthernet0/0**

R2(config-if)# **ip access-group 1 out**

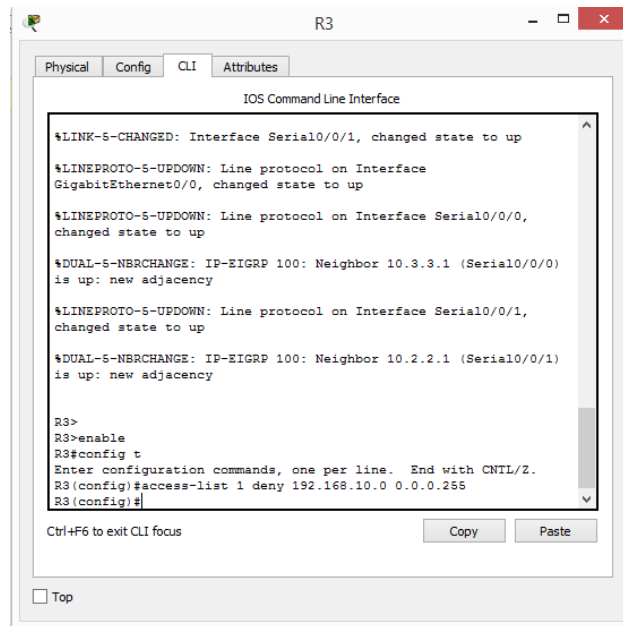


**Paso 2.** Configure and apply a numbered standard ACL on R3.

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

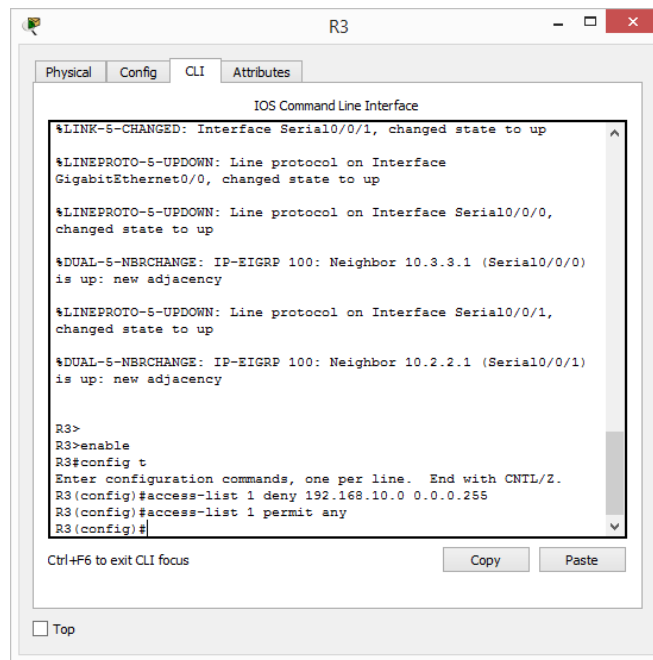
R3(config)# **access-list 1 deny 192.168.10.0 0.0.0.255**





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

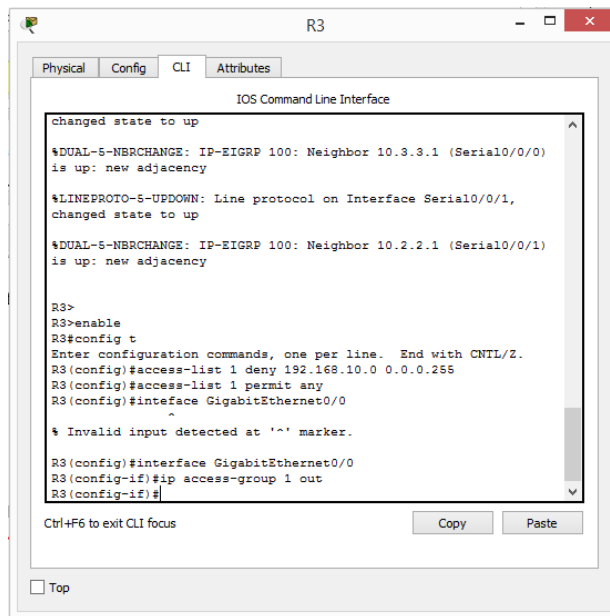
R3(config)# **access-list 1 permit any**



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

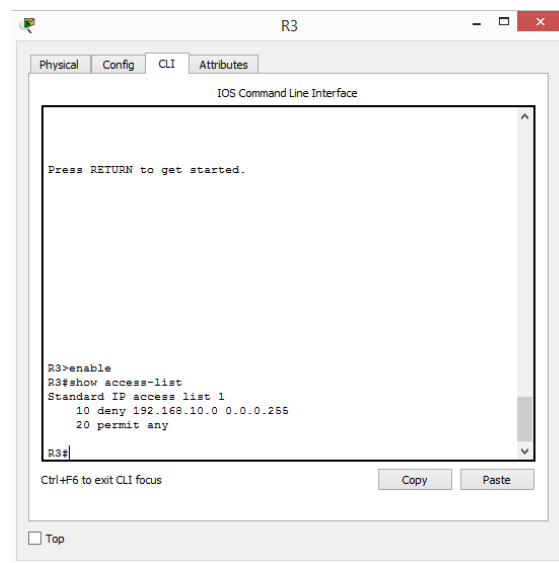
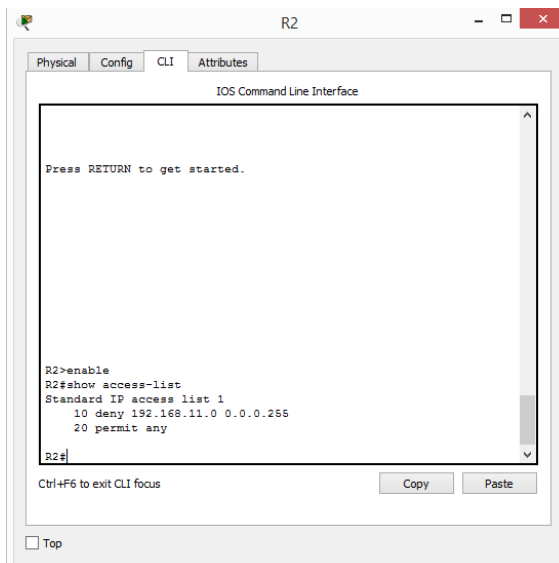
R3(config)# **interface GigabitEthernet0/0**

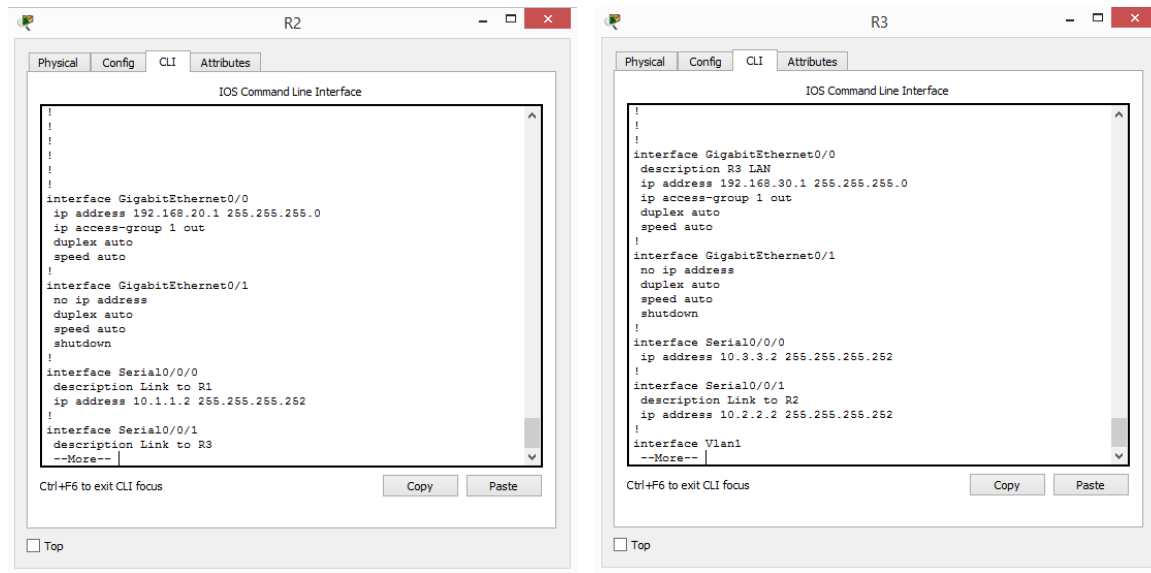
R3(config-if)# ip access-group 1 out



**Paso 3.** Verify ACL configuration and functionality.

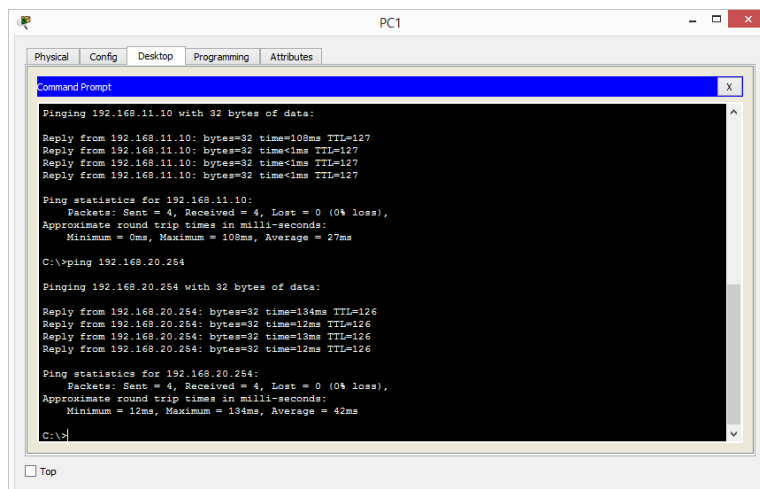
a. On **R2** and **R3**, enter the **show access-list** command to verify the ACL configurations. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.



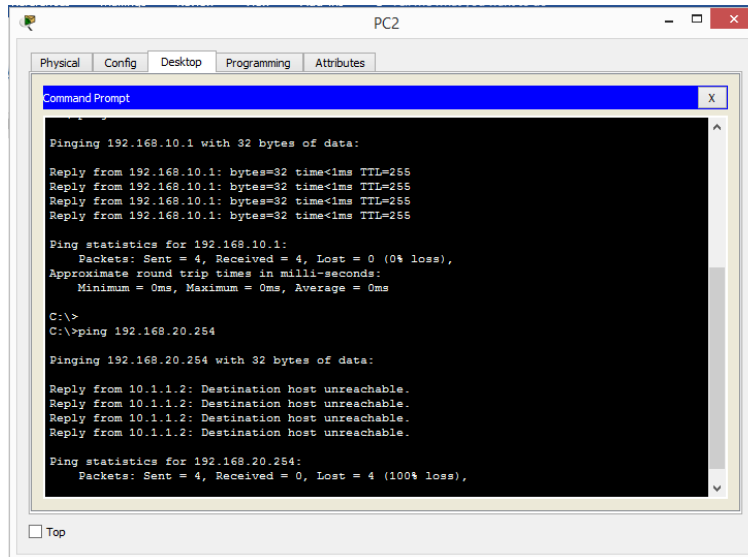


b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:

- ☐ 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.



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

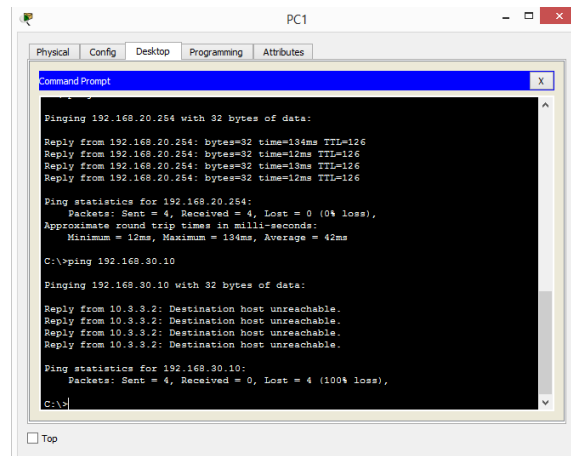
Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

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

❓ A ping from 192.168.10.10 to 192.168.30.10 fails.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.20.254 with 32 bytes of data:
Reply from 192.168.20.254: bytes=32 time=134ms TTL=126
Reply from 192.168.20.254: bytes=32 time=12ms TTL=126
Reply from 192.168.20.254: bytes=32 time=13ms TTL=126
Reply from 192.168.20.254: bytes=32 time=12ms TTL=126

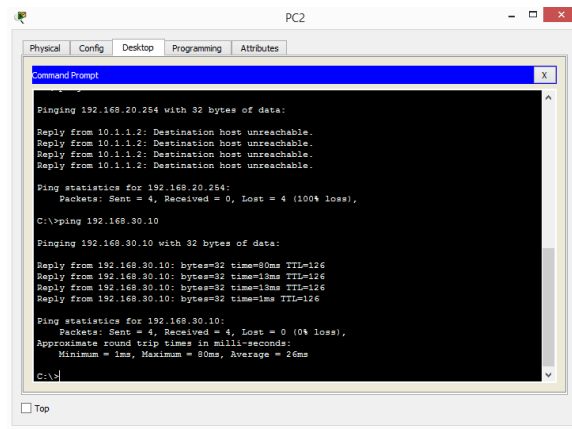
Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 134ms, Average = 42ms

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.

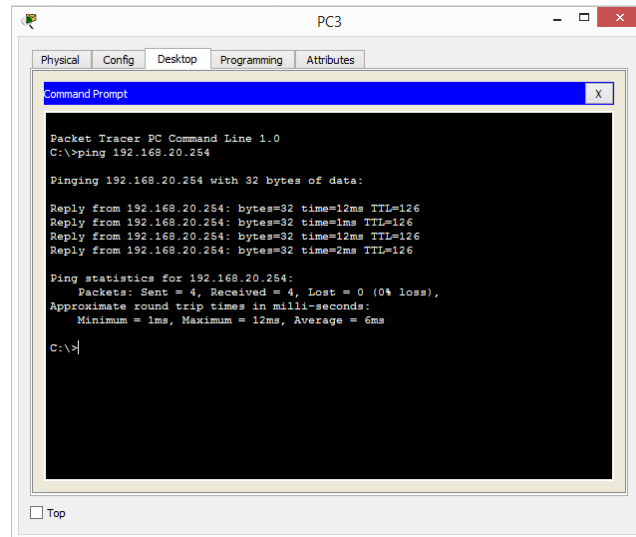
Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

❓ A ping from 192.168.11.10 to 192.168.30.10 succeeds.



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.20.254 with 32 bytes of data:
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.10
Pinging 192.168.30.10 with 32 bytes of data:
Reply from 192.168.30.10: bytes=32 time=50ms TTL=126
Reply from 192.168.30.10: bytes=32 time=3ms TTL=126
Reply from 192.168.30.10: bytes=32 time=3ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 50ms, Average = 26ms
C:\>
```

☐ A ping from 192.168.30.10 to 192.168.20.254 succeeds.



```
PC3
Physical Config Desktop Programming Attributes
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254
Pinging 192.168.20.254 with 32 bytes of data:
Reply from 192.168.20.254: bytes=32 time=12ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=12ms TTL=126
Reply from 192.168.20.254: bytes=32 time=2ms TTL=126
Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms
C:\>
```

### CONCLUSIONES

- El enrutamiento dinámico resulta demasiado útil en empresas donde existen miles de terminales o host ya que permiten una administración menos pesada, sobre todo cuando existen cambios en la red.
- El tema del mejor direccionamiento de ruta es fundamental en grandes cantidades de tráfico, esto permite minimizar los tiempos de envío y recepción y finalmente la fiabilidad de la red.
- El uso de las listas de control de acceso nos permiten restringir el tráfico en la red para que esta no se vea afectada, esto permite tener un control más eficiente y se evitan problemas futuros.
- Una de las mejores funcionalidades es el uso de las NAT en redes IPv4 debido a que el uso de esta configuración permite ampliar el número de IP y evitar que estas finalmente se acaben, adicional a esto permite que las IP no sean mostradas en los servidores permitiendo un grado mayor de seguridad.

**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). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de: [https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi\\_Tm](https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi_Tm)

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>