

# **CCNA Routing & switching: Principios básicos de routing y switching**

Elaborado por:

Sandra Tatiana Mejía Flórez

Andrea Milena Perdomo

Luz Esthela Ballesteros

Juan Camilo Escobar

Juan pablo Mayorga

Entregado a:

Juan Carlos Vesga Ferreira

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Universidad Nacional Abierta y a Distancia

Ingeniería de Sistemas

Bogotá

2017

## Tabla de contenido

Introducción	3
Objetivos	4
Packet Tracer - Configure IP ACLs to Mitigate Attacks Instructor	5
Packet Tracer Configuring Standard ACLs Instructions IG Topología	24
Packet Tracer - Configuring Named Standard ACLs Instructions IG	32
Packet Tracer - Configuring an ACL on VTY Lines Instructions IG Topology	38
Packet Tracer - Configuring IPv6 ACLs Instructions IG	41
Lab - Configuring Basic RIPv2 and RIPv6	45
Lab - Configuring Basic Single-Area OSPFv2	68
Lab - Configuring Basic Single-Area OSPFv3	118
Lab - Configuring Basic DHCPv4 on a Router	131
Lab - Configuring Basic DHCPv4 on a Switch	157
Lab - Configuring Dynamic and Static NAT	172

## **Introducción**

En el presente trabajo se desarrollará todas las tareas (prácticas de laboratorio) correspondientes a las temáticas que forman parte de la unidad 4 del curso cisco. este busca identificar y solucionar problemas propios de enrutamiento mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces.

Cada una de las prácticas se desarrolla mediante el uso de la herramienta de simulación packet tracer el cual permite facilitar el aprendizaje en un entorno práctico.

## Objetivos

- Comprender y describir conceptos básicos de switching y el funcionamiento de los switches de Cisco.
- Comprender y describir las tecnologías de switching mejoradas.
- Comprender y describir los protocolos de routing dinámico, los protocolos de routing de vector de distancia y los protocolos de routing de estado de enlace.
- Configurar las operaciones básicas en una red de routing y switching pequeña y resolver los problemas relacionados.
- Llevar a cabo la configuración y la resolución de problemas de VLAN y del routing entre VLAN.
- Verificar la conectividad entre dispositivos antes de la configuración del firewall.
- Usar ACL para asegurar que el acceso remoto a los enrutadores esté disponible solo desde la estación de administración PC-C.

## Packet Tracer - Configure IP ACLs to Mitigate Attacks Instructor

### Topología

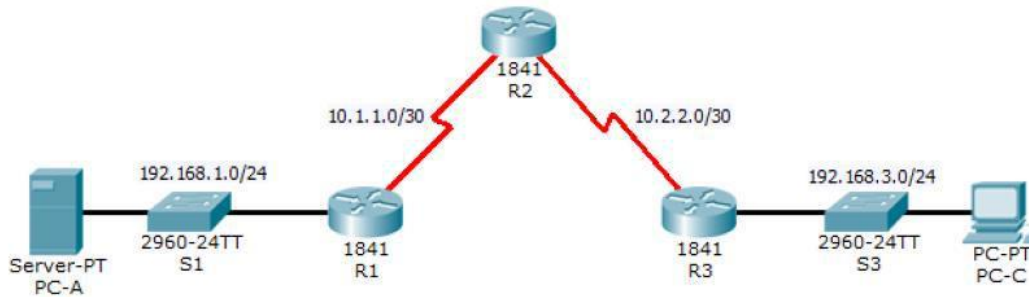


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	PUERTO DEL SWITCH
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

**Configure las ACL en R1 y R3 para mitigar los ataques.**

**Verificar la funcionalidad de ACL.**

Información básica/situación

El acceso a los enrutadores R1, R2 y R3 solo debe permitirse desde PC-C, la estación de administración. PC-C también se utiliza para realizar pruebas de conectividad a PC-A, un servidor que proporciona servicios DNS, SMTP, FTP y HTTPS.

El procedimiento operativo estándar es aplicar ACL en los enrutadores de borde para mitigar las amenazas comunes en función de la dirección IP de origen y / o de destino. En esta actividad, crea ACL en los enrutadores de borde R1 y R3 para lograr este objetivo. A continuación, verifica la funcionalidad de ACL de los hosts internos y externos.

Los enrutadores se han pre-configurado con lo siguiente:

Habilitar contraseña: **ciscoenpa55**

Contraseña para la consola: **ciscoconpa55**

Nombre de usuario para líneas VTY: **SSHadmin**

Contraseña para líneas VTY: **ciscosshpa55**

Direccionamiento IP

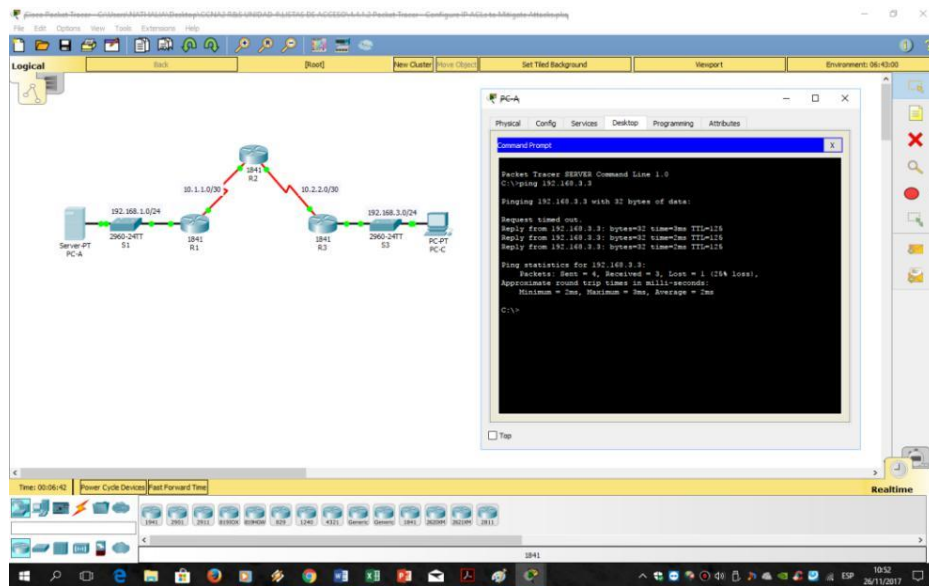
Enrutamiento estático

**Parte 1: verificar la conectividad de red básica**

Verifique la conectividad de la red antes de configurar las ACL de IP.

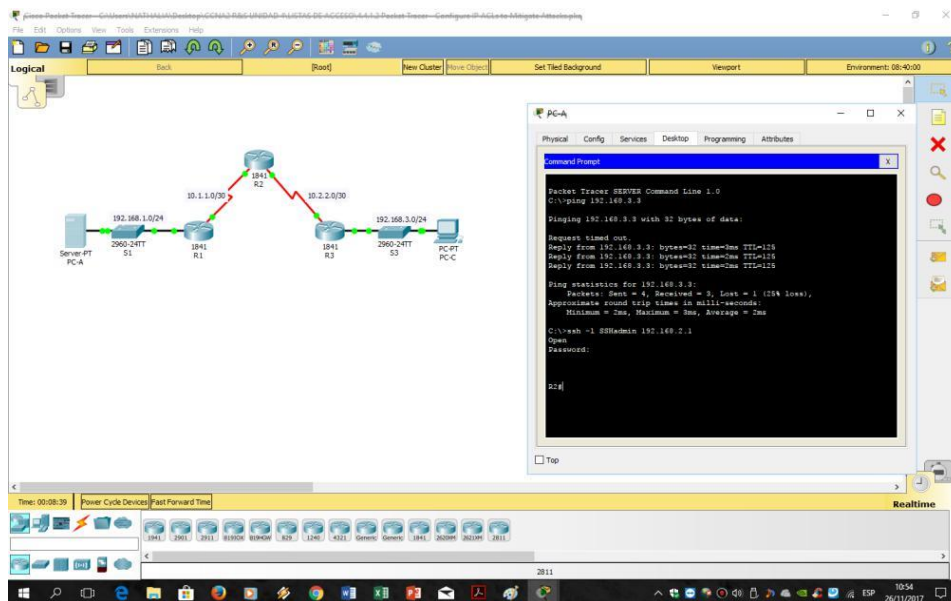
**Paso 1: desde la PC-A, verifique la conectividad con PC-C y R2.**

a. Desde el símbolo del sistema, haga ping a PC-C (192.168.3.3).



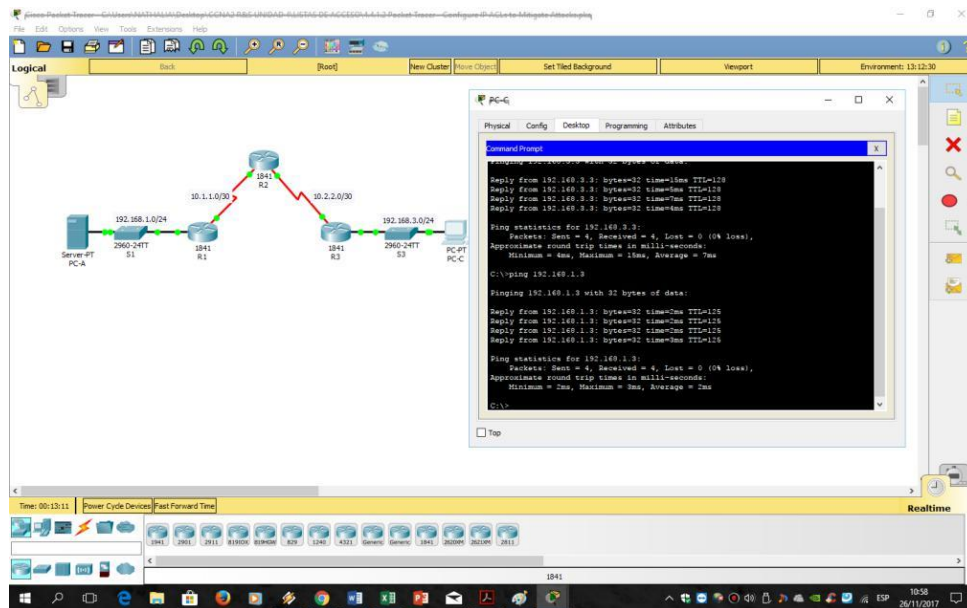
b. Desde el símbolo del sistema, establezca una sesión SSH a la interfaz R2 Lo0 (192.168.2.1) usando el nombre de usuario SSHadmin y la contraseña ciscosshpa55. Cuando termine, salga de la sesión SSH.

**PC> ssh -l SSHadmin 192.168.2.1**

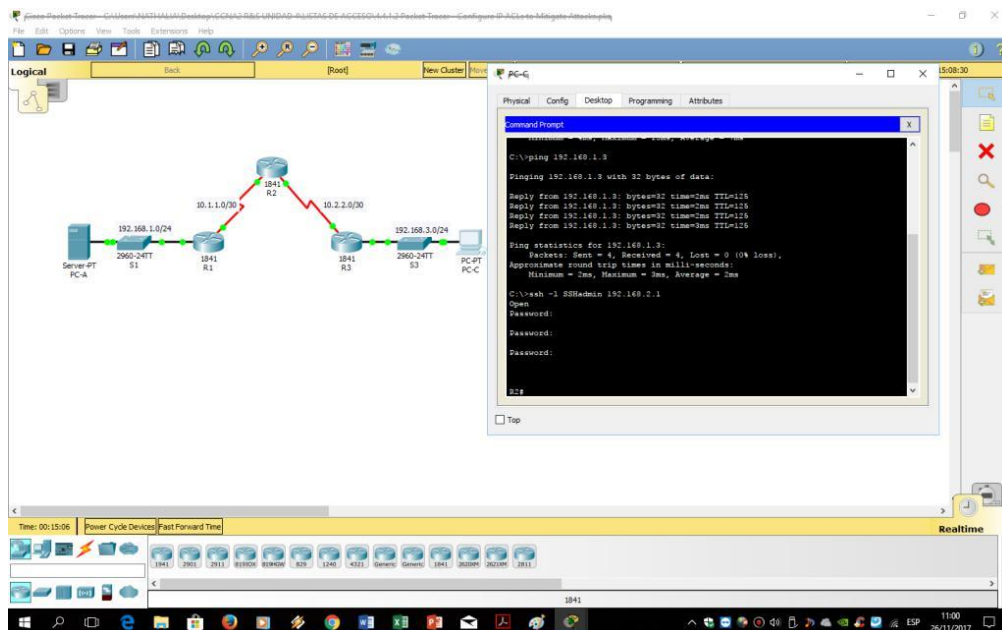


## Paso 2: desde PC-C, verifique la conectividad con PC-A y R2.

a. Desde el símbolo del sistema, haga ping a PC-A (192.168.1.3).

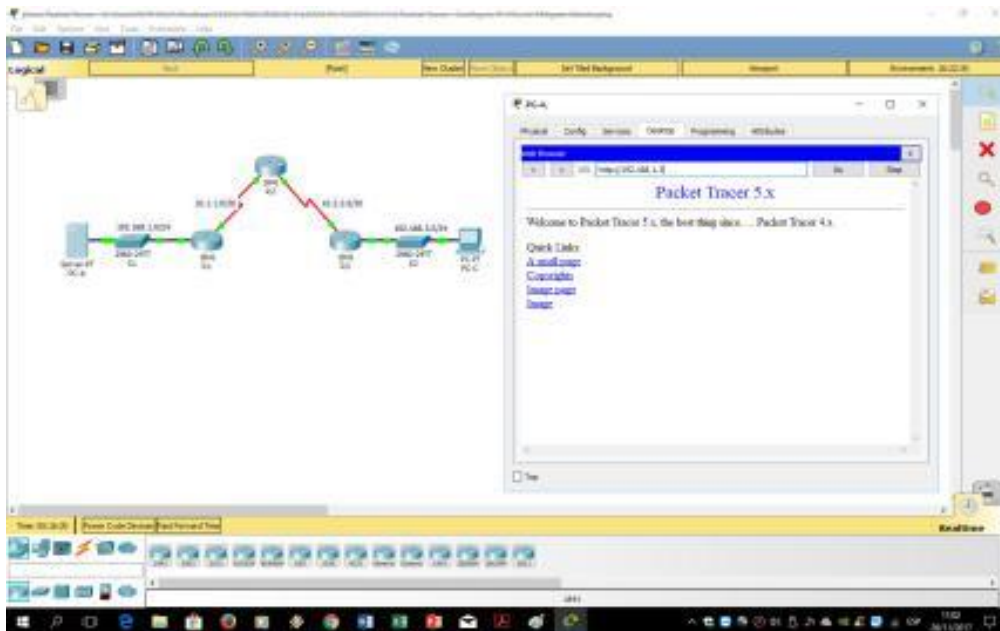


b. Desde el símbolo del sistema, establezca una sesión SSH a la interfaz R2 Lo0 (192.168.2.1) usando el nombre de usuario **SSHadmin** y la contraseña **ciscosshpa55**. Cierre la sesión SSH cuando haya terminado. PC> ssh -l SSHadmin 192.168.2.1





- c. Abra un navegador web en el servidor PC-A (192.168.1.3) para visualizar la página web.  
Cierre el navegador cuando termine



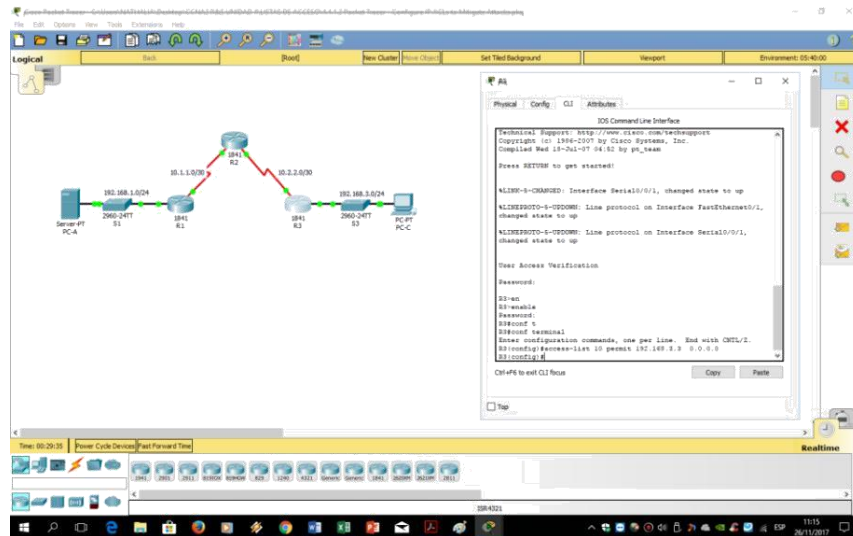
## Parte 2: Acceso seguro a enrutadores

**Paso 1: Configure la ACL 10 para bloquear todo el acceso remoto a los enrutadores, excepto desde PC-C.**

Use el comando `access-list` para crear una IP ACL numerada en R1, R2 y R3.

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

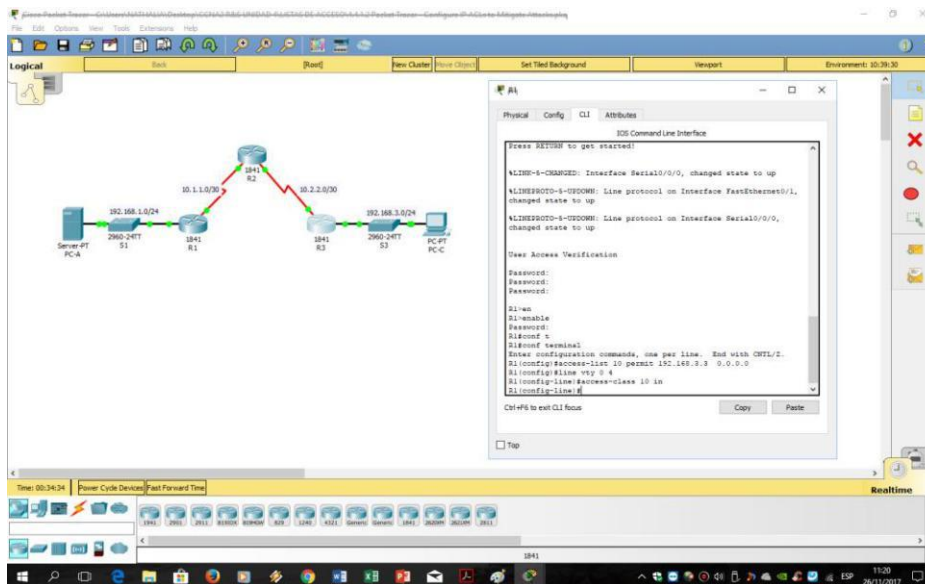




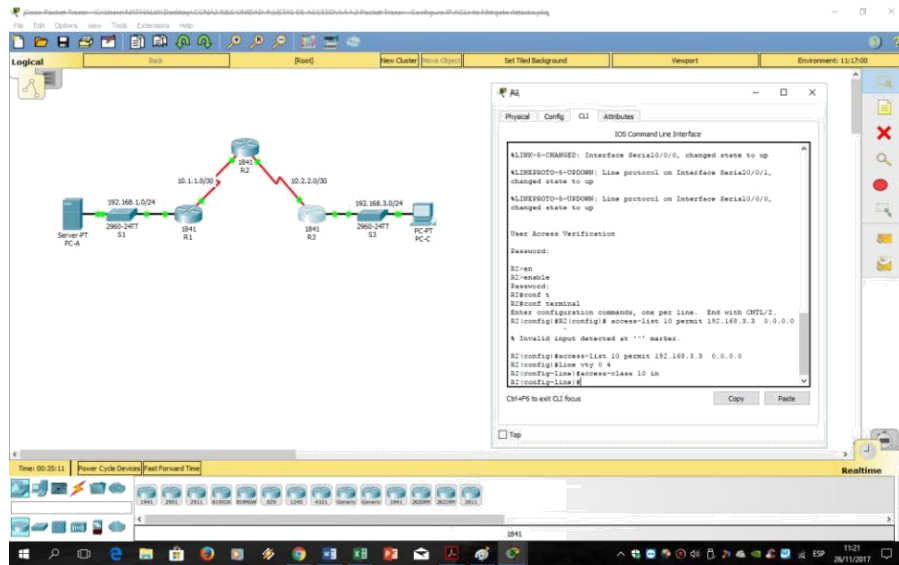
## Paso 2: aplique ACL 10 al tráfico de entrada en las líneas VTY.

Utilice el comando **access-class** para aplicar la lista de acceso al tráfico entrante en las líneas VTY.

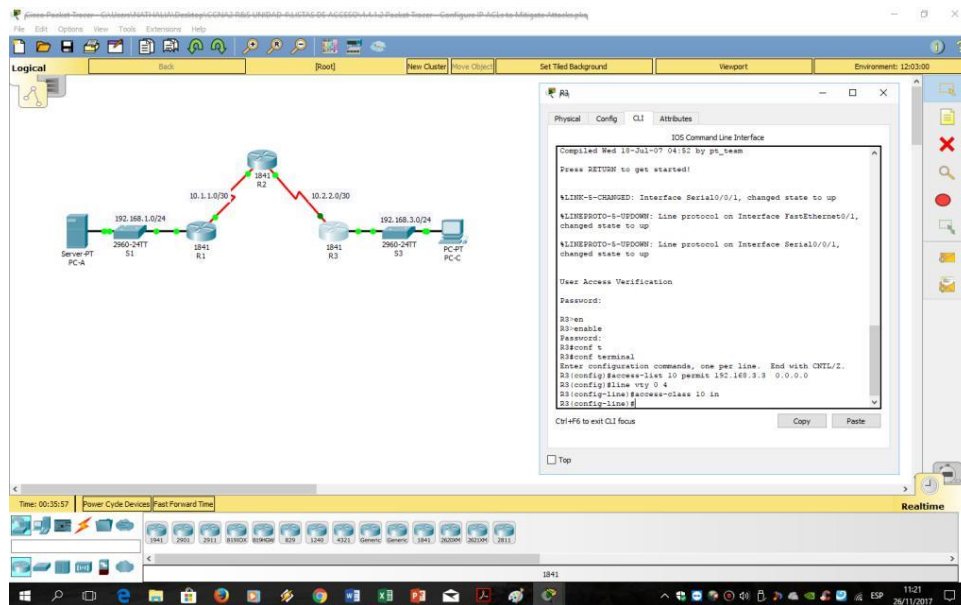
R1(config-line)# **access-class 10 in**



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



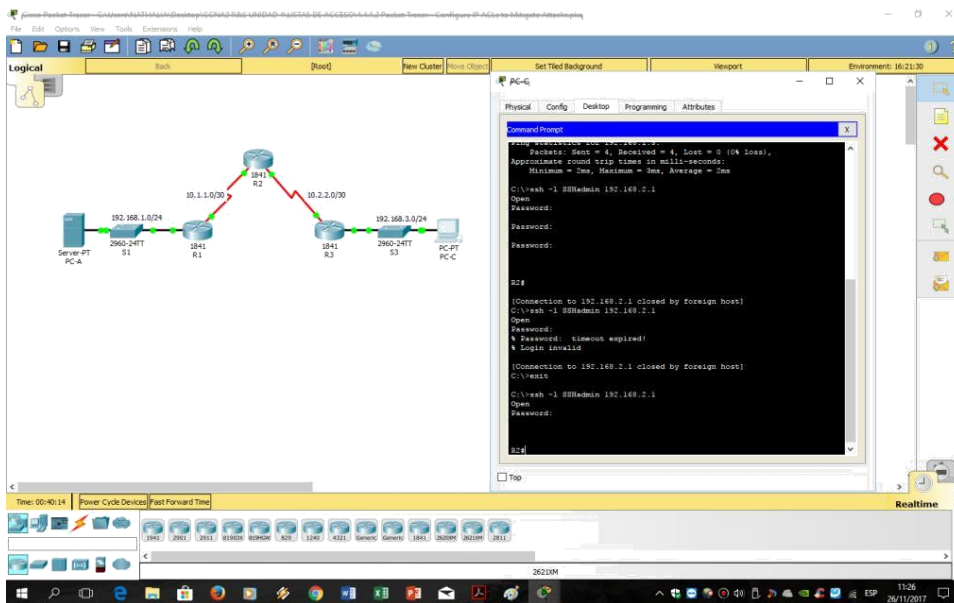
R3(config-line)# access-class 10 in



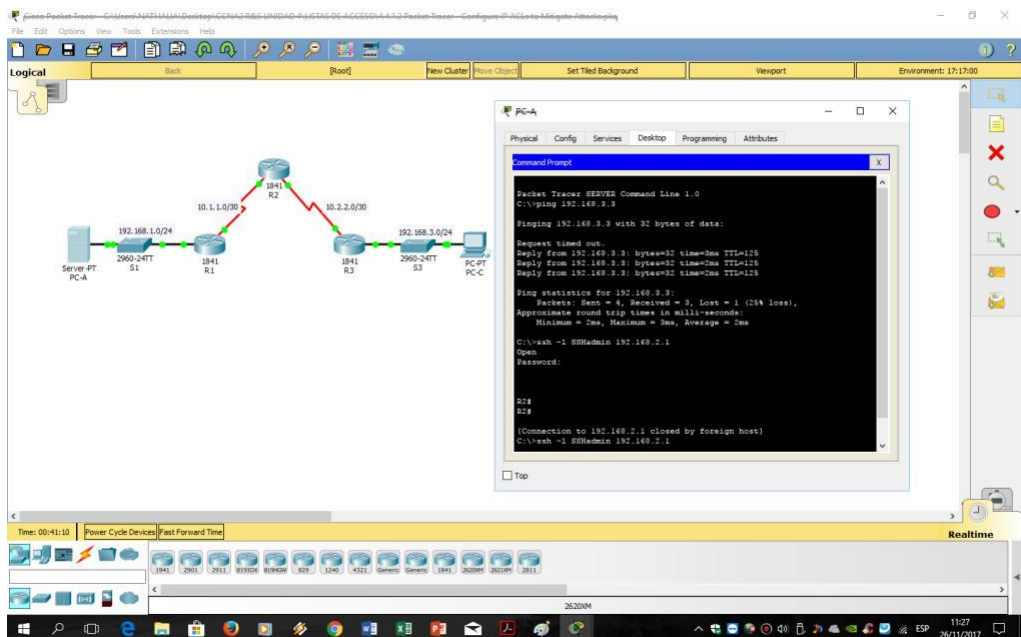
### Paso 3: Verifique el acceso exclusivo desde la estación de administración PC-C.

a. Establezca una sesión SSH en **192.168.2.1** desde PC-C (debería tener éxito).

PC> ssh -l SSHAdmin 192.168.2.1

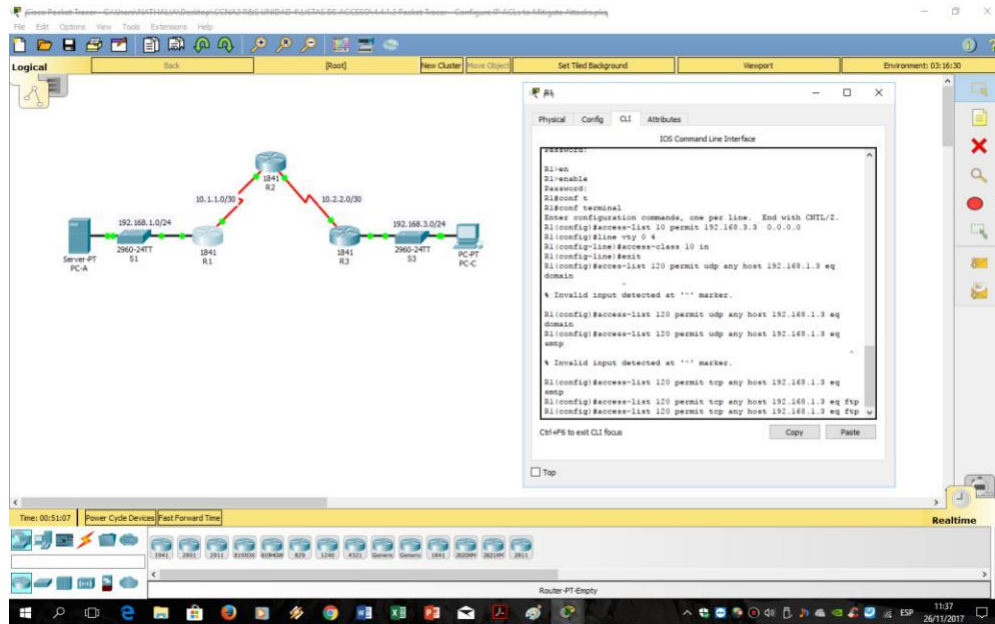


b. Establezca una sesión SSH a **192.168.2.1** desde PC-A (debería fallar).

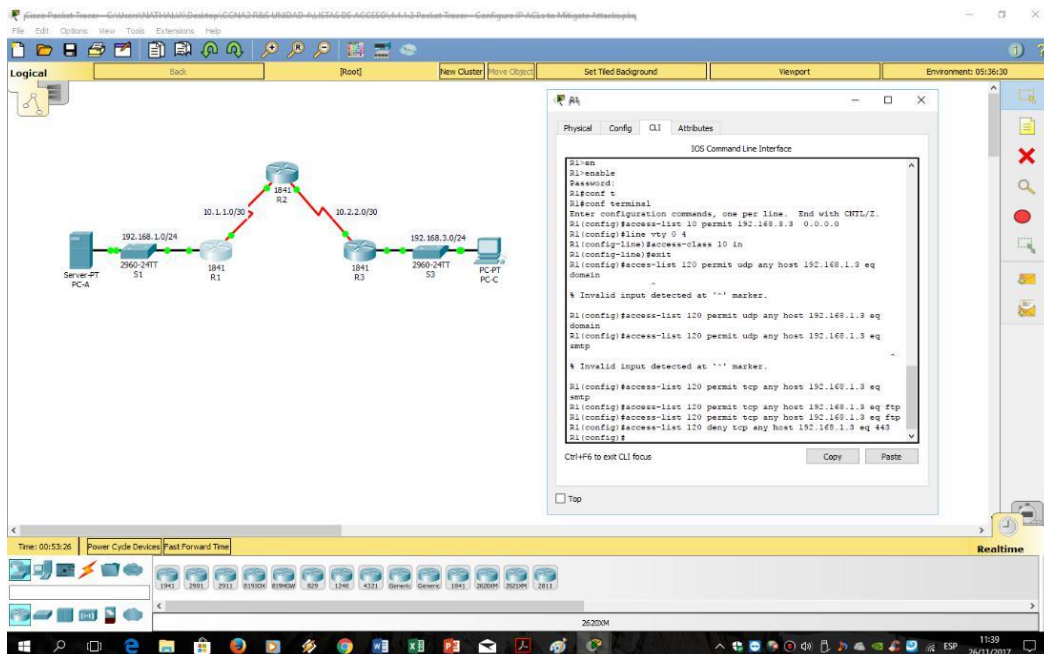


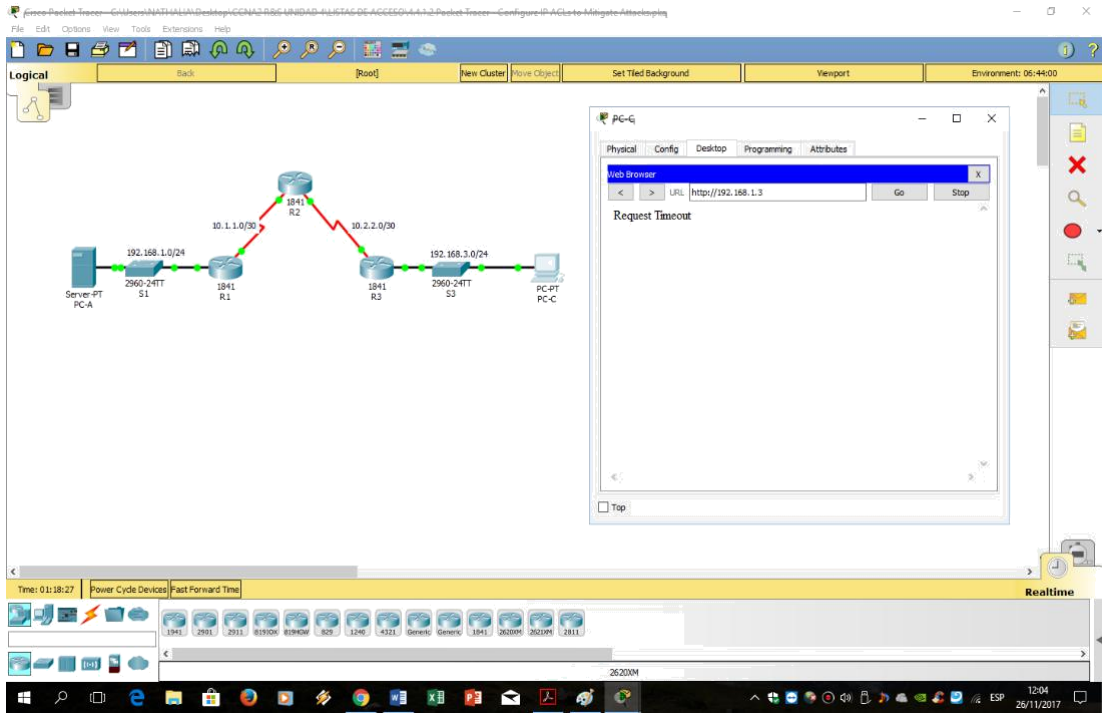
### Parte 3: Cree una ACL IP numerada 120 en R1

Permita que cualquier servidor externo acceda a los servicios DNS, SMTP y FTP en el servidor PC-A.

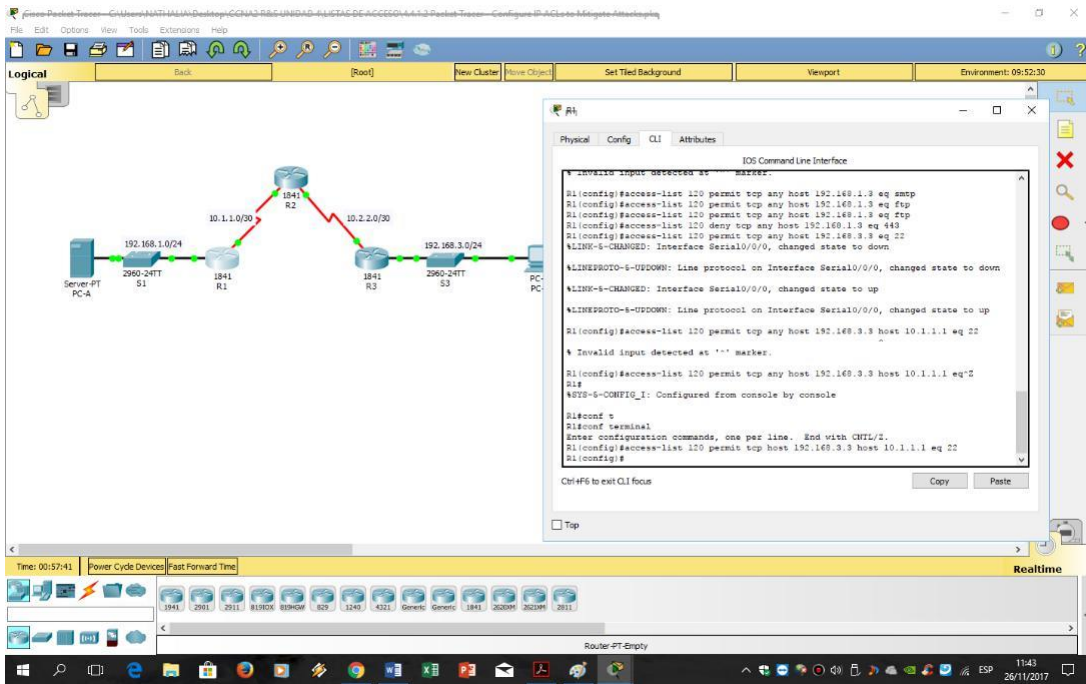


Niegue cualquier acceso de host externo a los servicios HTTPS en PC-A





Permita que PC-C tenga acceso a R1 a través de SSH.



**Paso 1: Verifique que PC-C pueda acceder a la PC-A a través de HTTPS usando el navegador web.**

Asegúrese de deshabilitar HTTP y habilitar HTTPS en el servidor PC-A.

**Paso 2: configure la ACL 120 para permitir y denegar específicamente el tráfico especificado.**

Use el comando access-list para crear una ACL IP numerada.

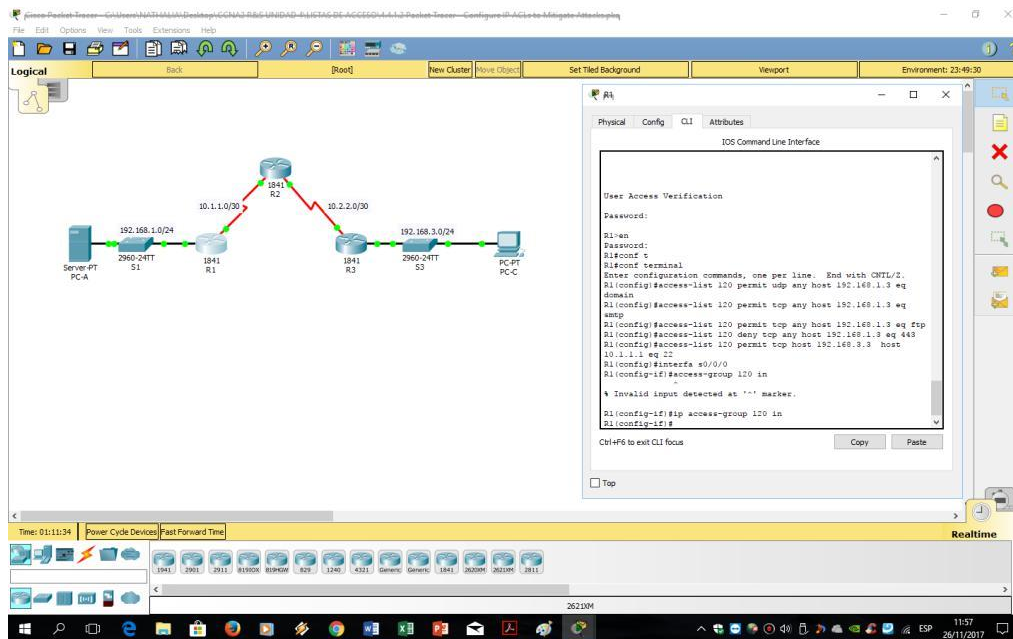
R1 (config) # access-list 120 permitir udp cualquier host 192.168.1.3 eq dominio

R1 (config) # access-list 120 permitir tcp cualquier host 192.168.1.3 eq smtp

R1 (config) # access-list 120 permitir tcp cualquier host 192.168.1.3 eq ftp

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

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



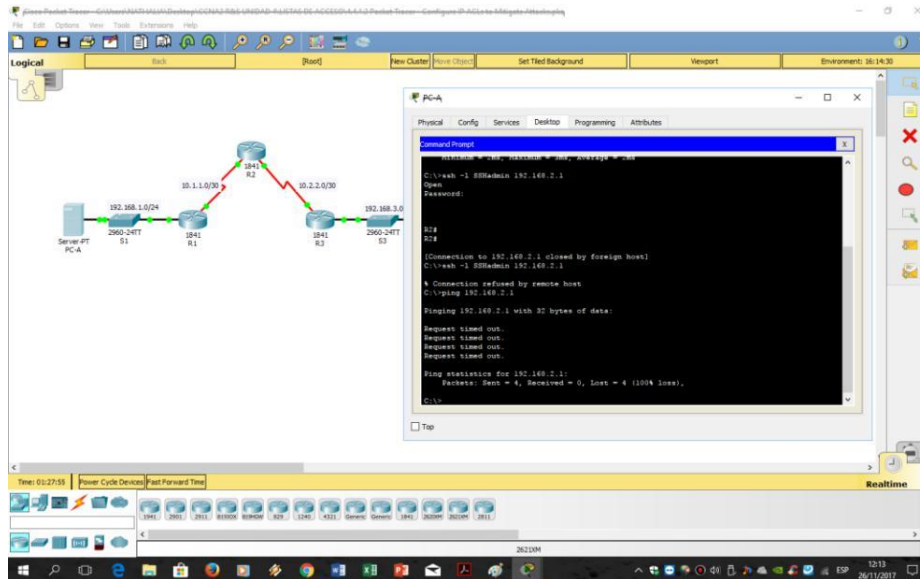




## Parte 4: Modificar una ACL existente en R1

Permitir respuestas de eco ICMP y mensajes inalcanzables de destino desde la red externa (en relación con R1); denegar todos los demás paquetes ICMP entrantes.

**Paso 1: Verifique que la PC-A no pueda hacer ping exitosamente en la interfaz loopback en R2.**



**Paso 2: Realice los cambios necesarios en la ACL 120 para permitir y denegar el tráfico especificado.**

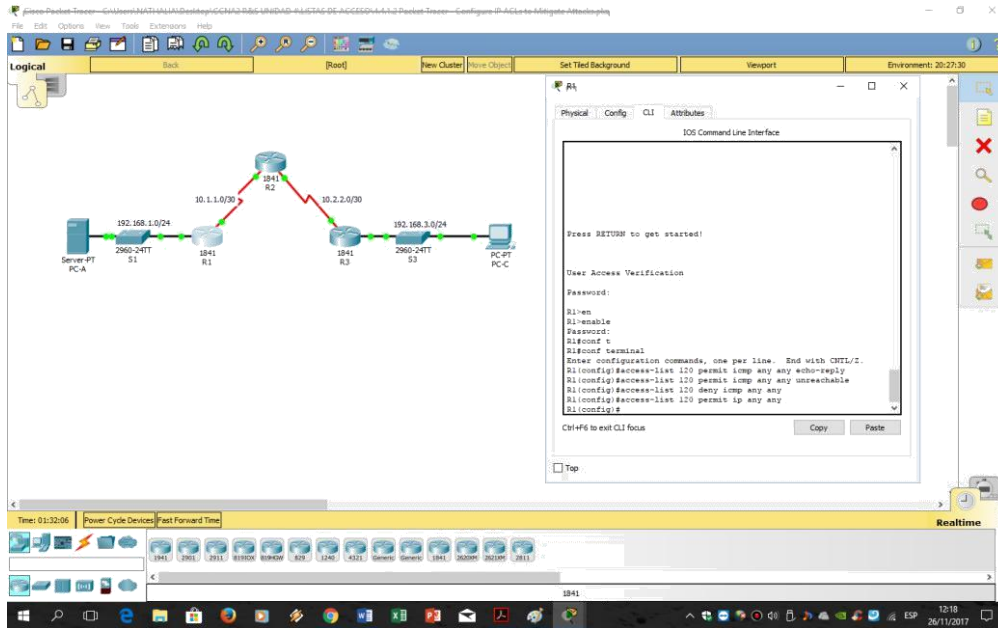
Use el comando access-list para crear una ACL IP numerada.

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

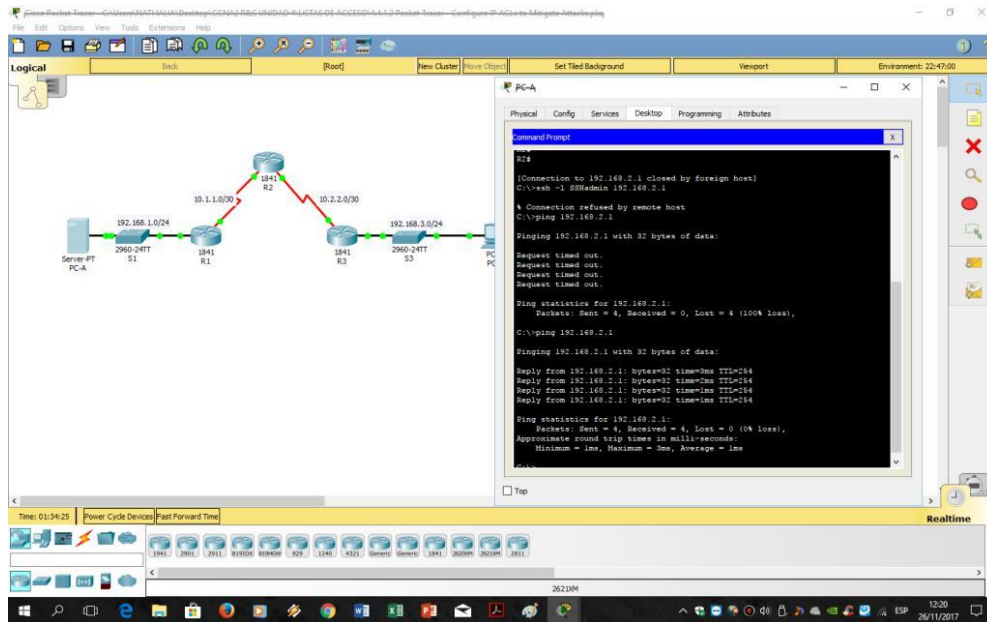
```
R1(config)# access-list 120 permit icmp any any unreachable
```

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

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



**Paso 3: Verifique que PC-A pueda hacer ping con éxito en la interfaz loopback en R2.**



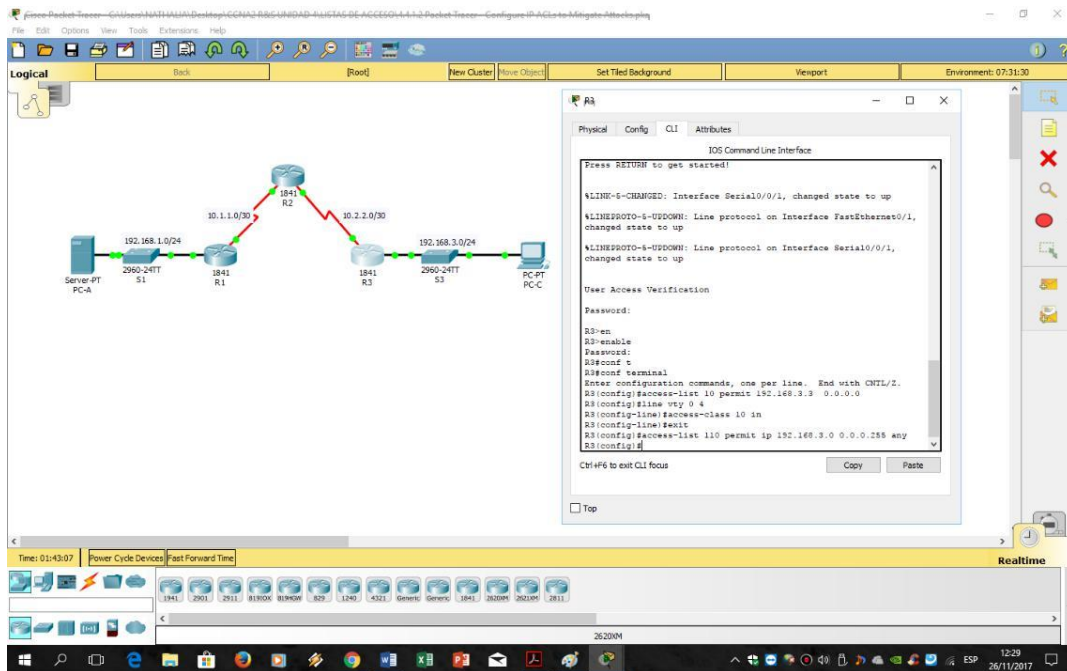
## Parte 5: Crear una ACL IP numerada 110 en R3

Denegar todos los paquetes salientes con la dirección de origen fuera del rango de direcciones IP internas en R3.

### Paso 1: configure la ACL 110 para permitir solo el tráfico desde la red interna.

Use el comando **access-list** para crear una ACL IP numerada.

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

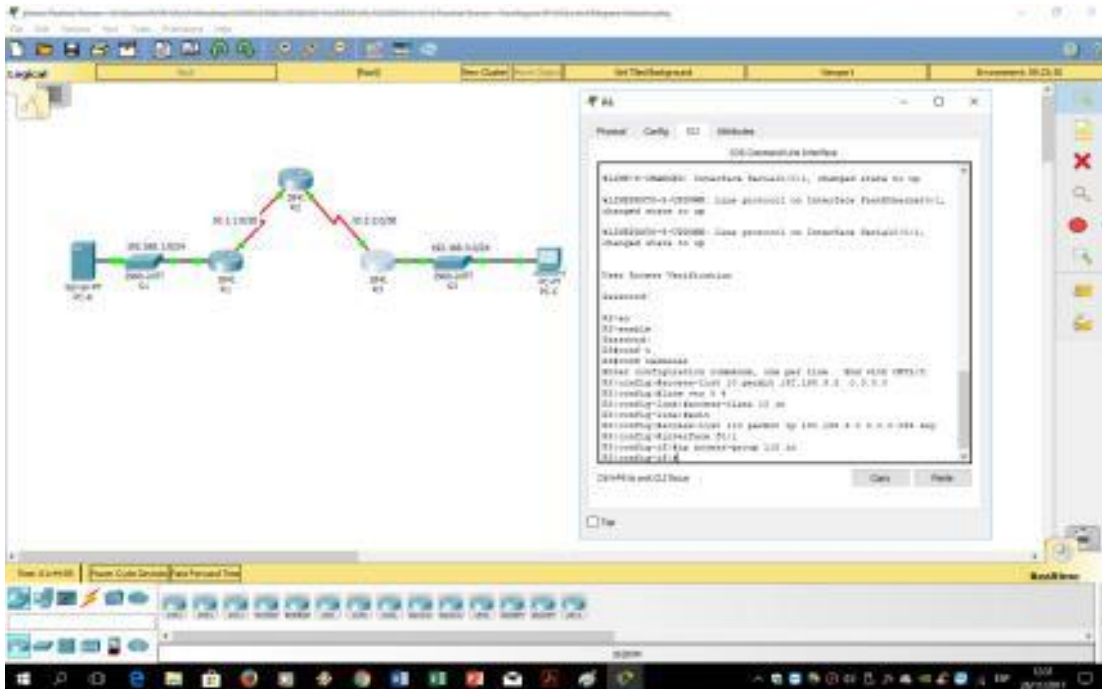


### Paso 2: aplique la ACL a la interfaz F0 / 1.

Use el comando **ip access-group** para aplicar la lista de acceso al tráfico entrante en la interfaz F0 / 1.

R3 (config) # interface fa0 / 1

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



## Parte 6: Crear una ACL 100 de IP numerada en R3

En R3, bloquee todos los paquetes que contengan la dirección IP de origen del siguiente grupo de direcciones: 127.0.0.0/8, cualquier dirección privada RFC 1918 y cualquier dirección de multidifusión IP.

**Paso 1: configure la ACL 100 para bloquear todo el tráfico especificado de la red externa.**

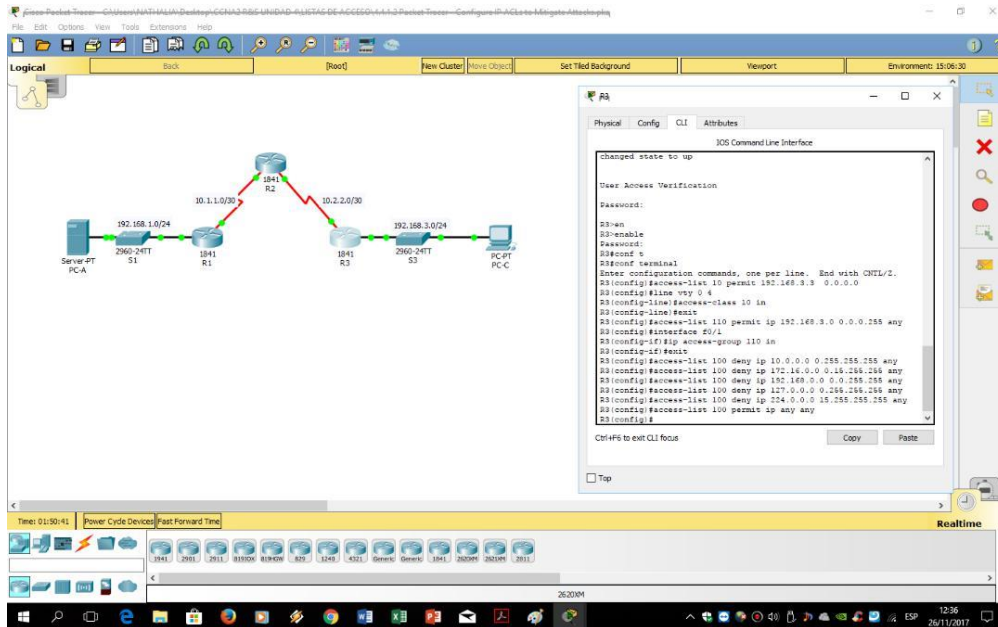
También debe bloquear el tráfico proveniente de su propio espacio de direcciones internas si no es una dirección RFC 1918 (en esta actividad, su espacio de direcciones internas es parte del espacio de direcciones privadas especificado en RFC 1918).

Use el comando access-list para crear una ACL IP numerada

```

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

```



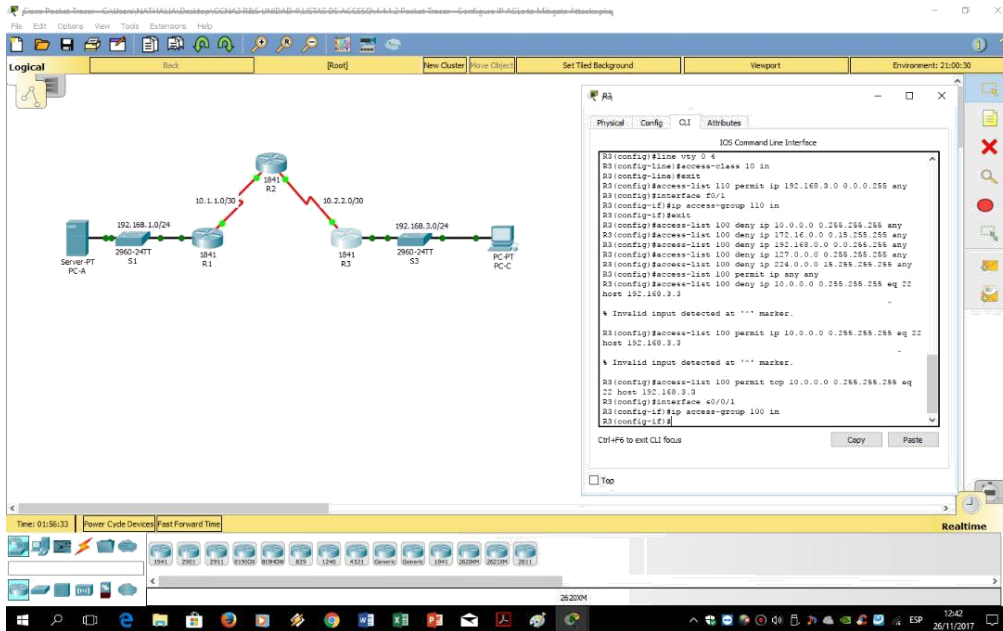
## Paso 2: aplique la ACL a la interfaz Serial 0/0/1.

Use el comando ip access-group para aplicar la lista de acceso al tráfico entrante en la interfaz Serial 0/0/1.

```

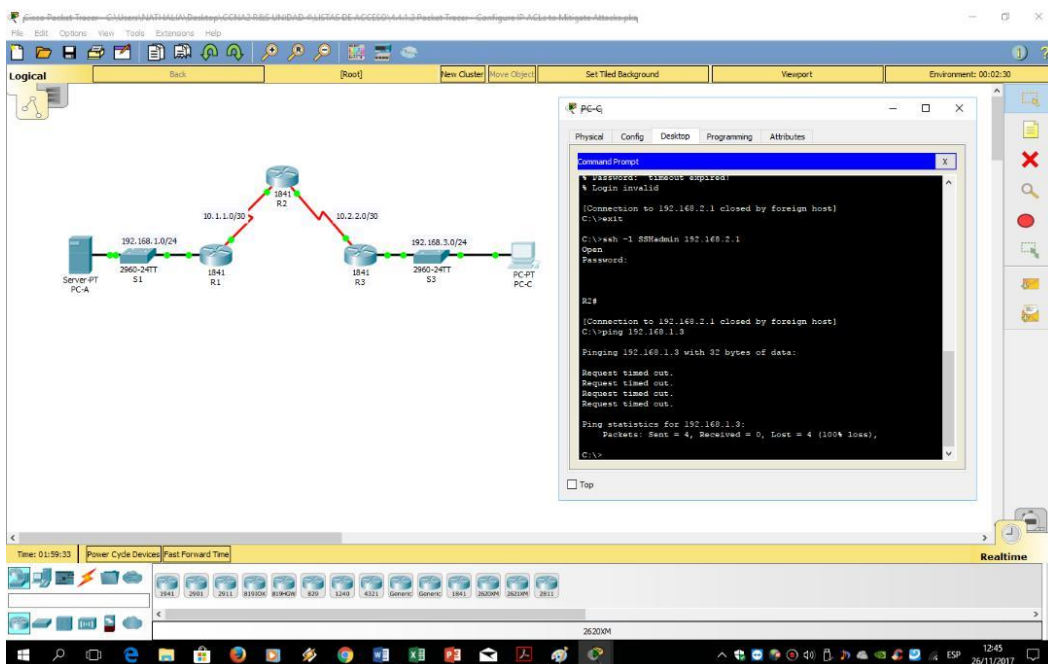
R3(config)# interface s0/0/1
R3(config-if)# ip access-group 100 in

```



**Paso 3: Confirme que la interfaz de entrada de tráfico especificada Serial 0/0/1 se elimine.**

Desde el indicador de comando de PC-C, haga ping al servidor PC-A. Las respuestas de eco ICMP están bloqueadas por la ACL ya que se obtienen del espacio de direcciones 192.168.0.0/16.



### 9.2.1.10 Packet Tracer Configuring Standard ACLs Instructions

#### IG Topología

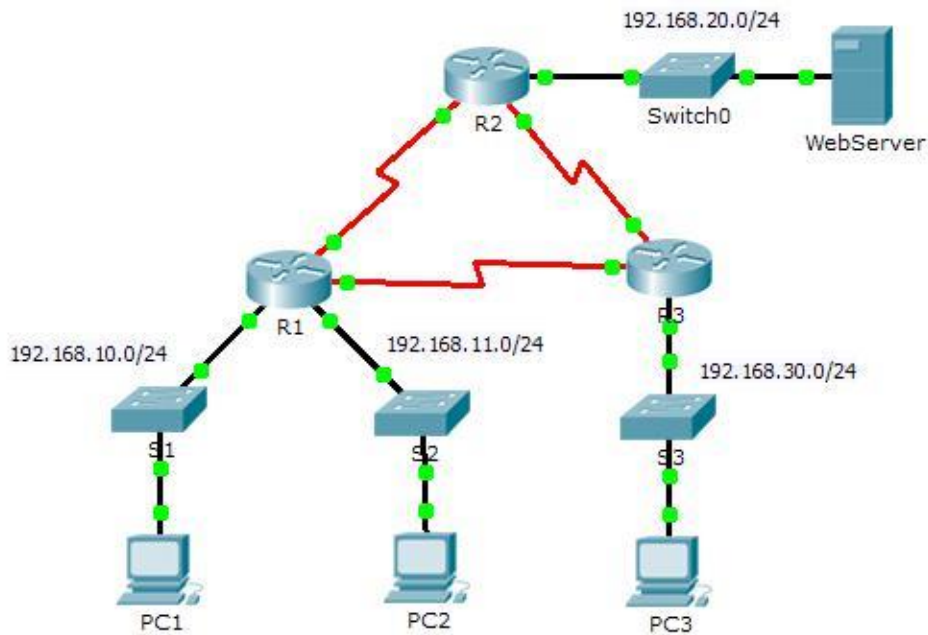


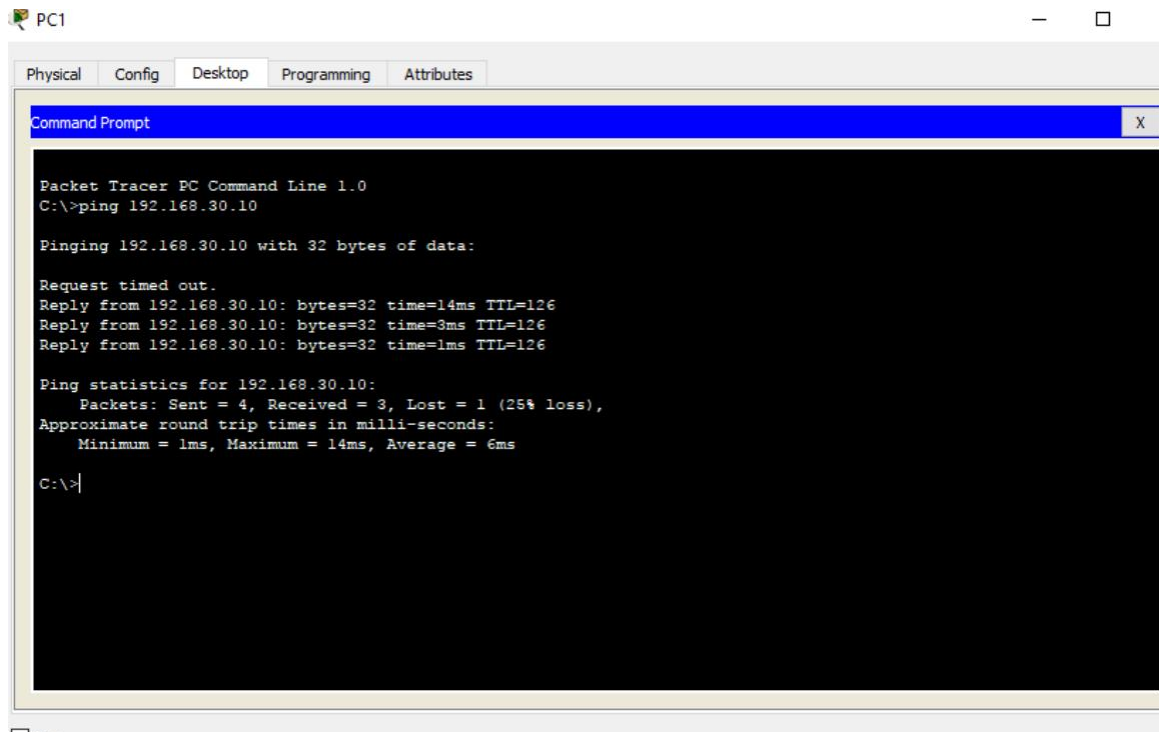
Tabla de direccionamiento

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



## Parte 1: planificar una implementación de ACL

**Paso 1:** investigue la configuración de red actual. Antes de aplicar cualquier ACL a una red, es importante confirmar que tiene conectividad completa. Verifique que la red tenga conectividad completa eligiendo una PC y haciendo ping a otros dispositivos en la red. Debería poder hacer ping con éxito en todos los dispositivos.



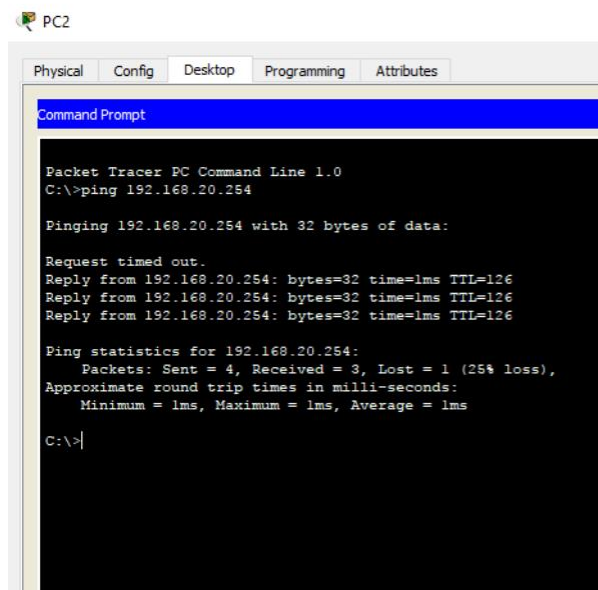
```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.10: bytes=32 time=14ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 6ms

C:\>|
```



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>|
```

**Paso 2:** Evalúa dos políticas de red y planifica implementaciones de ACL.

a. Las siguientes políticas de red están implementadas en R2:

La red 192.168.11.0/24 no tiene acceso permitido al servidor web en la red 192.168.20.0/24.

El resto del acceso está permitido.

Para restringir el acceso desde la red 192.168.11.0/24 al WebServer en 192.168.20.254 sin interferir con otro tráfico, debe crearse una ACL en R2. La lista de acceso debe colocarse en la interfaz de salida al servidor web. Se debe crear una segunda regla en R2 para permitir el resto del tráfico.

b. Las siguientes políticas de red se implementan en R3:

La red 192.168.10.0/24 no puede comunicarse con la red 192.168.30.0/24. Todos los demás accesos están permitidos.

Para restringir el acceso desde la red 192.168.10.0/24 a la red 192.168.30 / 24 sin interferir con otro tráfico, se deberá crear una lista de acceso en R3. La ACL debe colocarse en la interfaz de salida para PC3. Se debe crear una segunda regla en R3 para permitir todo el resto del tráfico.

## **Parte 2: configurar, aplicar y verificar una ACL estándar**

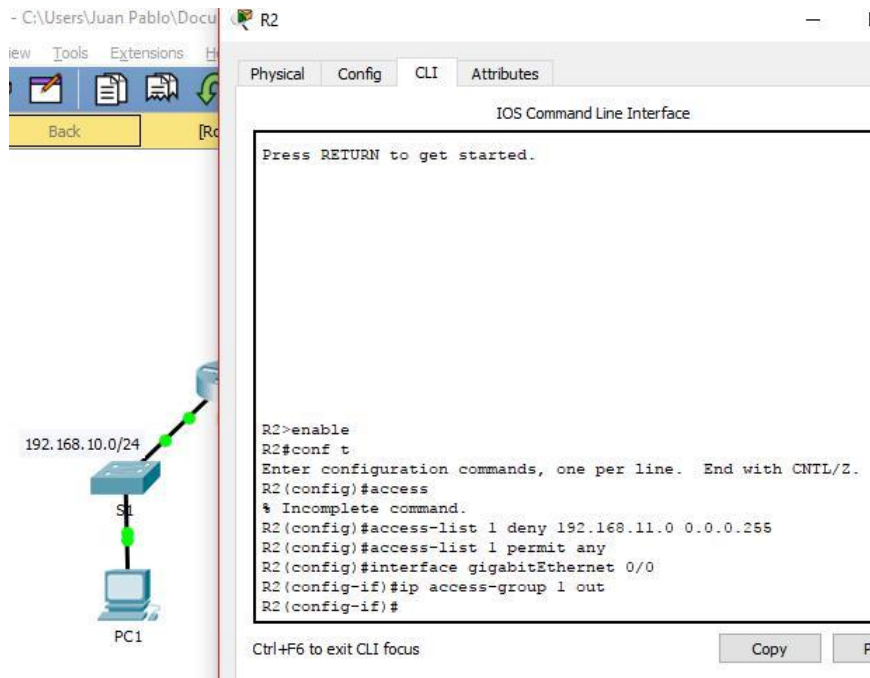
**Paso 1:** configurar y aplicar una ACL estándar numerada en R2.

a. Cree una ACL usando el número 1 en R2 con una declaración que niega el acceso a la red 192.168.20.0/24 desde la red 192.168.11.0/24.

b. De manera predeterminada, una lista de acceso niega todo el tráfico que no coincide con una regla. Para permitir todo el resto del tráfico, configure la siguiente declaración:

```
R2(config)# access-list 1 permit any
```

c. Para que la ACL realmente filtre el tráfico, se debe aplicar a alguna operación del enrutador. Aplicar la ACL colocándola para el tráfico saliente en la interfaz Gigabit Ethernet 0/0



**Paso 2:** configure y aplique una ACL estándar numerada en R3.

a. Cree una ACL usando el número 1 en R3 con una declaración que niega el acceso a la red 192.168.30.0/24 desde la red PC1 (192.168.10.0/24).

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

b. De forma predeterminada, una ACL deniega todo el tráfico que no coincide con una regla. Para permitir el resto del tráfico, cree una segunda regla para ACL 1.

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

c. Aplique la ACL colocándola para el tráfico saliente en la interfaz Gigabit Ethernet 0/0.

```
Interfaz R3 (config) # GigabitEthernet0 / 0
```

```
R3 (config-if) # ip access-group 1 out
```

```
R3>enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip access
% Incomplete command.
R3(config-if)#ip access-group 1 out
R3(config-if)#
```

**Paso 3:** Verificar la configuración y funcionalidad de ACL.

a. En R2 y R3, ingrese el comando show access-list para verificar las configuraciones de ACL. Ingrese el comando show run o show ip interface gigabitethernet 0/0 para verificar las ubicaciones de ACL.

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

Ctrl+F6 to exit CLI focus Copy

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

Ctrl+F6 to exit CLI focus Copy Paste

b. Con las dos ACL en su lugar, el tráfico de red está restringido según las políticas detalladas en la Parte 1. Use las siguientes pruebas para verificar las implementaciones de ACL:

- A ping from 192.168.10.10 to 192.168.11.10 tiene éxito
- A ping from 192.168.10.10 to 192.168.20.254 tiene éxito.
- A ping from 192.168.11.10 to 192.168.20.254 falla.

PC1

```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time<lms TTL=127
Reply from 192.168.11.10: bytes=32 time<lms TTL=127
Reply from 192.168.11.10: bytes=32 time<lms TTL=127
Reply from 192.168.11.10: bytes=32 time<lms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1

```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Link-local IPv6 Address . . . . . : FE80::201:96FF:FE06:A5AB
    IP Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

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=lms TTL=126
Reply from 192.168.20.254: bytes=32 time=lms TTL=126
Reply from 192.168.20.254: bytes=32 time=lms TTL=126
Reply from 192.168.20.254: bytes=32 time=lms 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 = lms, Maximum = lms, Average = lms
```

```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 192.168.20.254:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
  Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ipconfig

FastEthernet0 Connection: (default port)

  Link-local IPv6 Address . . . . . : FE80::20B:BEFF:FEE5:8C47
  IP Address . . . . . : 192.168.11.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.11.1

C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

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

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

C:\>
```

Un ping de 192.168.10.10 a 192.168.30.10 falla.  
Un ping de 192.168.11.10 a 192.168.30.10 tiene éxito.  
Un ping de 192.168.30.10 a 192.168.20.254 tiene éxito.

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
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 = 1ms, Average = 1ms

C:\>ipconfig

FastEthernet0 Connection: (default port)

  Link-local IPv6 Address . . . . . : FE80::201:96FF:FE06:A5AB
  IP Address . . . . . : 192.168.10.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.10.1

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

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

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

C:\>
```

PC2

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

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

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Link-local IPv6 Address . . . . . : FE80::20B:BEFF:FEE5:8C47
    IP Address. . . . . : 192.168.11.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.11.1

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=6ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms 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 = 6ms, Average = 2ms
```

PC3

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.30.1

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Link-local IPv6 Address . . . . . : FE80::209:7CFF:FE4C:972B
    IP Address. . . . . : 192.168.30.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.30.1

C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

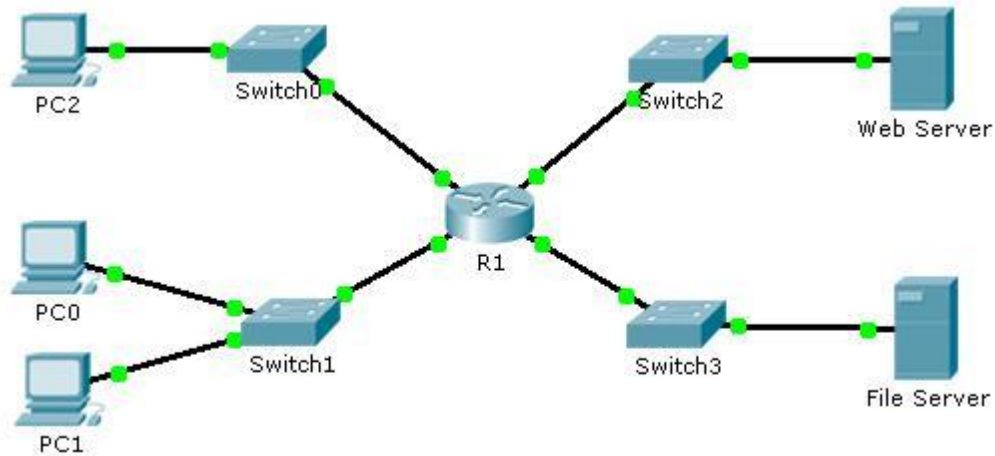
Reply from 192.168.20.254: bytes=32 time=4ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

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 = 4ms, Average = 1ms

C:\>
```

## 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs Instructions IG

### Topología



### Tabla de direccionamiento

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

### Parte 1: configurar y aplicar una ACL estándar designada

**Paso 1:** Verifique la conectividad antes de configurar y aplicar la ACL.

Las tres estaciones de trabajo deberían poder hacer ping al servidor web y al servidor de archivos.



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt X
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::20A:F3FF:FEEC:7D73
IP Address.....: 192.168.10.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1

C:\>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=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms 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 = 2ms, Average = 0ms

C:\>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=2ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\>
```

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt X
FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::260:3EFF:FE94:7DAA
IP Address.....: 192.168.20.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.20.1

C:\>ping 192.168.100.100

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=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\>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=2ms 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 = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Link-local IPv6 Address . . . . . : FE80::204:9AFF:FE44:2267
    IP Address . . . . . : 192.168.20.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.1

C:\>ping 192.168.100.100

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

C:\>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=1ms 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 = 0ms, Maximum = 1ms, Average = 0ms
```

**Paso 2:** configure una ACL estándar nombrada.

Configure la siguiente ACL nombrada en R1.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# deny any
```

```
R1>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)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

**Paso 3:** aplique la ACL nombrada.

a. Aplicar la ACL saliente en la interfaz Fast Ethernet 0/1.

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

```
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)#exit
R1(config)#interface fa0/1
R1(config-if)#int fa0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#
```

b. Guarde la configuración

## Parte 2: Verificar la implementación de ACL

**Paso 1:** Verifique la configuración de ACL y la aplicación a la interfaz.

Use el comando `show access-lists` para verificar la configuración de ACL. Utilice el comando `show run` o `show ip interface fastethernet 0/1` para verificar que la ACL se aplique correctamente a la interfaz.

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

R1#
```

Physical Config CLI Attributes

IOS Command Line Interface

```
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--
```

Paso 2: Verifique que la ACL esté funcionando correctamente.

Las tres estaciones de trabajo deberían poder hacer ping al servidor web, pero solo la PC1 debería poder hacer ping al servidor de archivos.

PC2

```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.100.100
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=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=3ms 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 = 3ms, Average = 1ms
```

PC0

```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=3ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=4ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127
Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

PC1

```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 192.168.100.100
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<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms 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 = 2ms, Average = 1ms
```

PC2

```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC0

```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC1

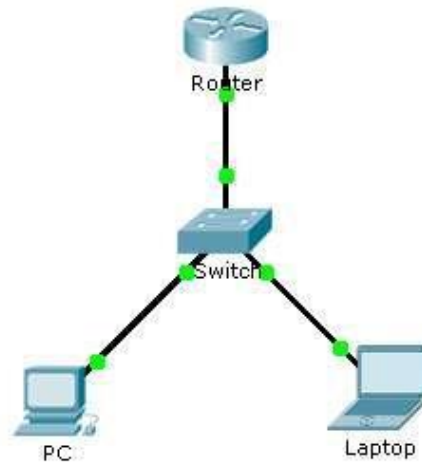
```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 192.168.200.100

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<1ms 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 = 0ms, Maximum = 1ms, Average = 0ms
```

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



#### Addressing Table

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

#### Objectives

##### Part 1: Configure and Apply an

##### ACL to VTY Lines Part 2: Verify

##### the ACL Implementation

#### Background

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

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

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

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

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

Configure the following numbered ACL on Router.

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

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

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

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

```
Router(config)# line vty 0 15
```

```
Router(config-line)# access-
```

```
class 99 in
```

**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.

**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.

Cisco Packet Tracer - D:\Google Drive\Documentos\Unad\Diplomado Cisco\Trabajo Colaborativo 4\CCNA2 R&S UNIDAD 4\LISTAS DE ACCESO\9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines.pka

File Edit Options View Tools Extensions Help

## Activity Results

Time Elapsed: 00:42:35

Congratulations Juan Camilo Escobar! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Congratulations! You successfully completed the Packet Tracer - Configuring an ACL on VTY Lines activity.

Close

Cisco Packet Tracer - D:\Google Drive\Documentos\Unad\Diplomado Cisco\Trabajo Colaborativo 4\CCNA2 R&S UNIDAD 4\LISTAS DE ACCESO\9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines.pka

File Edit Options View Tools Extensions Help

## Activity Results

Time Elapsed: 00:42:55

Congratulations Juan Camilo Escobar! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
Router				
ACL 99	Correct	70	ACL IPv4 Standard...	
VTY Lines				
VTY Line 0		0	Physical	
Access Contro...	Correct	6	IPv4 Standard...	
VTY Line 1		0	Physical	
Access Contro...	Correct	6	IPv4 Standard...	
VTY Line 2		0	Physical	
Access Contro...	Correct	6	IPv4 Standard...	
VTY Line 3		0	Physical	
Access Contro...	Correct	6	IPv4 Standard...	
VTY Line 4		0	Physical	
Access Contro...	Correct	6	IPv4 Standard...	

Score : 100/100  
Item Count : 6/6

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

Close



## 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs Instructions IG

### Packet Tracer - Configuring IPv6 ACLs

#### Addressing Table

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

#### Objectives

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

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

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

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

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

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

a. Block HTTP and HTTPS traffic from reaching **Server3**.

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

b. Allow all other IPv6 traffic to pass.

```
R1>EN  
R1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#ipv6 acc  
R1(config)#ipv6 access-list BLOCK_HTTP  
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www  
^  
% Invalid input detected at '^' marker.  
  
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www  
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443  
R1(config-ipv6-acl)#per  
R1(config-ipv6-acl)#permit ipv  
R1(config-ipv6-acl)#permit ipv6 any any
```

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

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

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

```
R1(config-if)#interface g0/1
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#ipv6
R1(config-if)#ipv6 tra
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP
% Incomplete command.
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

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

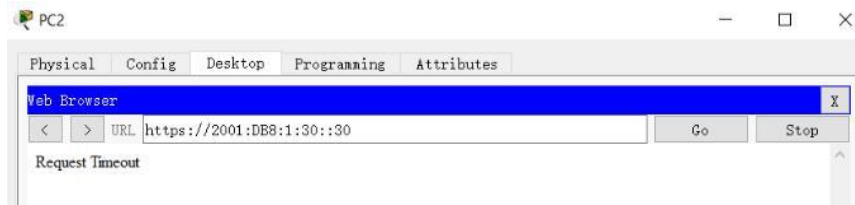
Verify the ACL is operating as intended by conducting the following tests:

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

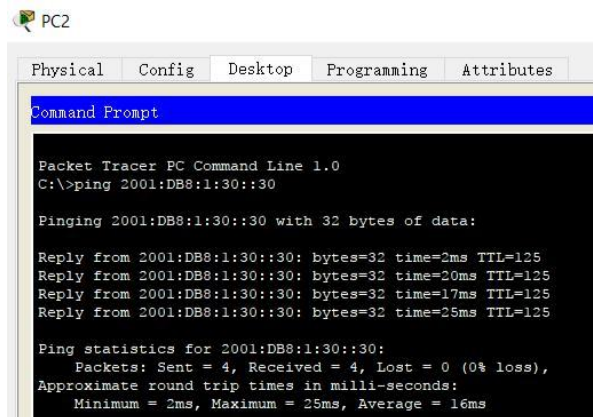


Open the **web browser** of **PC2** to `http:// 2001:DB8:1:30::30` or

`https://2001:DB8:1:30::30`. The website should be blocked



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



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

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

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

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

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

```
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#
R3(config-ipv6-acl)#
```

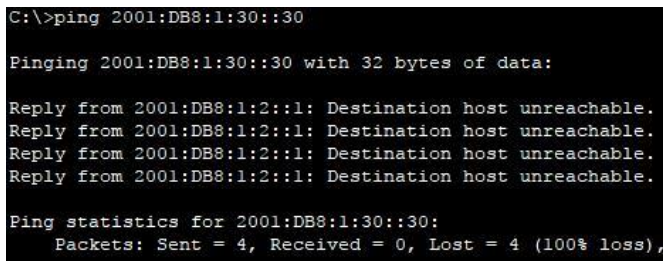
**Step 2: Apply the ACL to the correct interface.**

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

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

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

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



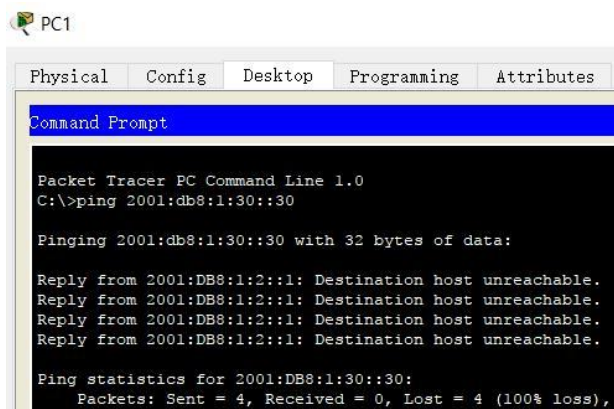
```
C:\>ping 2001:DB8:1:30::30

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),
```

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



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>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),
```

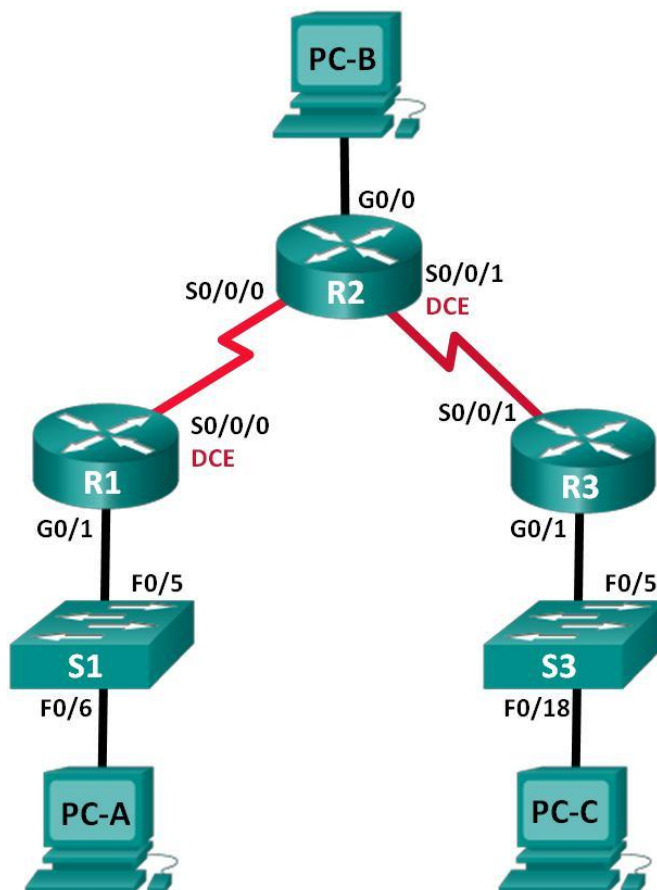
Open the **web browser** of **PC1** to `http:// 2001:DB8:1:30::30` or `https://2001:DB8:1:30::30`. The website should display.



### 7.3.2.4 Lab - Configuring Basic RIPv2 and RIPv6

**Práctica de laboratorio: configuración básica de RIPv2 y RIPv6**

**Topología**



## Tabla de direccionamiento

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

## Objetivos

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

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

Configurar y verificar que se esté ejecutando RIPv2 en los routers.

Configurar una interfaz pasiva.

Examinar las tablas de routing.

Desactivar la sumarización automática.

Configurar una ruta predeterminada.

Verificar la conectividad de extremo a extremo.

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

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

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

Configurar una ruta predeterminada.

Verificar la conectividad de extremo a extremo.

### **Información básica/situación**

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

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

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

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

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

### **Recursos necesarios**

3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet y seriales, como se muestra en la topología

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

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

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

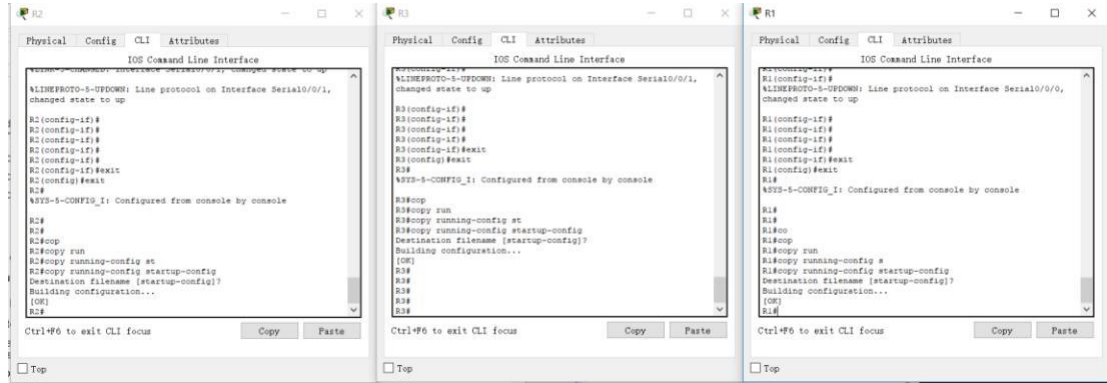
**Paso 2. inicializar y volver a cargar el router y el switch.**

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

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



- j. Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.
- k. Copie la configuración en ejecución en la configuración de inicio.



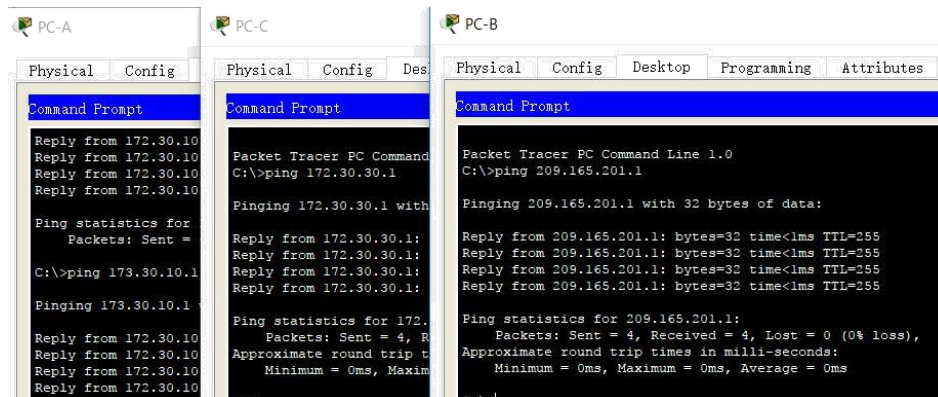
#### Paso 4. configurar los equipos host.

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

#### Paso 5. Probar la conectividad.

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

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



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

The screenshot shows three terminal windows side-by-side. The left window (R2) shows a successful ping to 10.1.1.2 with a success rate of 100% and a round-trip time of 1/4/16 ms. The middle window (R3) shows a successful ping to 10.2.2.2 with a success rate of 100% and a round-trip time of 1/4/15 ms. The right window (R1) shows a successful ping to 10.1.1.2 with a success rate of 100% and a round-trip time of 1/4/18 ms. All windows show the standard Cisco CLI output for a ping command, including the number of bytes sent, the success rate, and the round-trip time.

## 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.

- c. 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.

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

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

- e. 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.

```
R2(config)#router ri
R2(config)#router rip
R2(config-router)#ver
R2(config-router)#version 2
R2(config-router)#net
R2(config-router)#network 10.0.0.0
R2(config-router)#
```

## 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
Embedded-Service-Engine0/0 administratively down	unassigned	YES	unset	unset
GigabitEthernet0/0 up	209.165.201.1	YES	manual	up
GigabitEthernet0/1 administratively down	unassigned	YES	unset	unset
Serial0/0/0 up	10.1.1.2	YE S	manual	up
Serial0/0/1 up	10.2.2.2	YE S	manual	up

```

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

```

b. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? **\_NO\_** ¿Por qué? **La red del PC-B no fue anunciada por tal motivo no es accesible.**

¿Es posible hacer ping de la PC-A a la PC-C? **\_SI\_** ¿Por qué? **La red del PC-C fue anunciada de forma correcta.**

¿Es posible hacer ping de la PC-C a la PC-B? **\_NO\_** ¿Por qué? **La red del PC-B no fue anunciada por tal motivo no es accesible.**

¿Es posible hacer ping de la PC-C a la PC-A? **\_SI\_** ¿Por qué? **La red del PC-A fue anunciada de forma correcta.**

b. Verifique que RIPv2 se ejecute en los routers.

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

```

R1# show ip protocols Routing Protocol is
"rip"

```

```

Outgoing update filter list for all interfaces is not set Incoming update filter list for all
interfaces is not set Sending updates every 30 seconds, next due in 7 seconds Invalid after
180 seconds, hold down 180, flushed after 240 Redistributing: rip

```

```

Default version control: send version 2, receive 2

```

Interface	Send	Recv	Triggered RIP	Key-chain
Serial0/0/0	2	2		

```

Automatic network summarization is in effect

```

Maximum path: 4

Routing for Networks:

10.0.0.0

172.30.0.0

Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

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

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

Distance: (default is 120)

```
R1>show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 23 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
Serial0/0/0          2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway           Distance      Last Update
  10.1.1.2          120           00:00:02
Distance: (default is 120)
--
```

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

```
RIP protocol debugging is on
R2#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
```

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

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

```
router rip
version 2
```

```
passive-interface GigabitEthernet0/1
network 10.0.0.0
network 172.30.0.0
```

d.Examinar el sumarización automática de las rutas.

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

```
R2# show ip route
```

```
<Output Omitted>
```

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

```
C10.1.1.0/30 is directly connected, Serial0/0/0
```

```
L10.1.1.2/32 is directly connected, Serial0/0/0
```

```
C10.2.2.0/30 is directly connected, Serial0/0/1
```

```
L10.2.2.2/32 is directly connected, Serial0/0/1
```

```
R172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
```

```
Serial0/0/0 [120/1] via 10.1.1.1, 00:00:09,
```

```
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
```



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

```
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
```

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.

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

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

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

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

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

- g. Examine 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



C10.1.1.0/30 is directly connected, Serial0/0/0

L10.1.1.2/32 is directly connected, Serial0/0/0

C10.2.2.0/30 is directly connected, Serial0/0/1

L10.2.2.2/32 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

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

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

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

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

C 209.165.201.0/24 is directly connected,  
GigabitEthernet0/0

L 209.165.201.1/32 is directly connected,  
GigabitEthernet0/0

R1# **show ip route**

<Output Omitted>

Gateway of last resort is not set

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

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

L10.1.1.1/32 is directly connected, Serial0/0/0

R10.2.2.0/30 [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

L10.2.2.1/32 is directly connected, Serial0/0/1

R10.1.1.0/30 [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

R172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1

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

**R2# debug ip rip**

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

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

## 10.2.2.2

### 172.30.30.0

```
172.30.30.0/24 via 0.0.0.0, metric 2, 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
172.30.10.0/24 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 Serial0/0/0 (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: 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: 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 Serial0/0/0 (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: 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: 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 Serial0/0/0 (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: 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: 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
no debug ip rip
```

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

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

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

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

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

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

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

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

- k. 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

L10.1.1.1/32 is directly connected, Serial0/0/0

R10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0 172.30.0.0/16 is variably  
subnetted, 3 subnets, 2 masks

C 172.30.10.0/24 is directly connected,  
GigabitEthernet0/1

L 172.30.10.1/32 is directly connected,  
GigabitEthernet0/1

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

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

Porque la ruta estática predeterminada aparece publicada en los router R1 y R3, por medio de RIP.

- l. Consulte la tabla de routing en el R2.

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

Publicando en los demás routers la ruta estática predeterminada

### **Paso 6. Verifique la conectividad.**

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

¿Tuvieron éxito los pings? **\_SI\_**

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

¿Tuvieron éxito los pings? \_SI\_

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

### Parte 3: configurar IPv6 en los dispositivos

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

**Tabla de direccionamiento**

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

PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

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

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

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

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

- c. Para cada interfaz del router, asigne la dirección global y la dirección link local de la tabla de direccionamiento.
- d. Habilite el routing IPv6 en cada router.
- e. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.

**show ipv6 interface brief**

- f. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.
- g. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

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

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

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

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

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

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

- i. Configure RIPng para las interfaces seriales en el R2, con Test2 como el nombre de proceso. No lo configure para la interfaz G0/0
- j. Configure RIPng para cada interfaz en el R3, con **Test3** como el nombre de proceso.
- k. Verifique que RIPng se esté ejecutando en los routers.

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

```
R1# show ipv6 protocols
```

```
IPv6 Routing Protocol is "connected" IPv6 Routing
Protocol is "ND"
```

```
IPv6 Routing Protocol is "rip Test1" Interfaces:
```

```
Serial0/0/0
```

```
GigabitEthernet0/1
```

```
Redistribution: None
```

¿En qué forma se indica RIPng en el resultado?

```
IPv6 Routing Protocol is "rip Test1"
```

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

```
R1# show ipv6 rip Test1
```

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

```
Administrative distance is 120. Maximum paths is 16
```

```
Updates every 30 seconds, expire after 180
```

```
Holddown lasts 0 seconds, garbage collect after 120
```

```
Split horizon is on; poison reverse is off
```

Default routes are not generated Periodic updates 1, trigger updates 0  
Full Advertisement 0, Delayed Events 0

Interfaces:

GigabitEthernet0/1

Serial0/0/0

Redistribution:

None

¿Cuáles son las similitudes entre RIPv2 y RIPng?

El proceso de propagación de rutas es igual en los dos o mejor dicho son similares.

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

### **Show IPv6 Route\_**

En el R1, ¿cuántas rutas se descubrieron mediante RIPng? **2** En el R2, ¿cuántas rutas se descubrieron mediante RIPng? **2** En el R3, ¿cuántas rutas se descubrieron mediante RIPng? **2**

- n. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? **NO** ¿Es posible hacer ping de la PC-A a la PC-C? **SI** ¿Es posible hacer ping de la PC-C a la PC-B? **NO** ¿Es posible hacer ping de la PC-C a la PC-A? **SI** ¿Por qué algunos pings tuvieron éxito y otros no?

Esto sucede porque en la configuración del protocolo no se agregó la interface conectada al PC-B.

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



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

```
ipv6 route ::0/64 gigabitEthernet 0/0
```

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

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

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

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

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

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

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

```
R2# show ipv6 route
```

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

```
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP U - Per-user Static route, M - MIPv6
```

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

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

```
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 D - EIGRP, EX - EIGRP external
```

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

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

R            2001:DB8:ACAD:A::/64 [120/2] via  
FE80::1, Serial0/0/0

C            2001:DB8:ACAD:B::/64 [0/0] via ::,  
GigabitEthernet0/1

L            2001:DB8:ACAD:B::2/128 [0/0]  
via ::, GigabitEthernet0/1

R            2001:DB8:ACAD:C::/64 [120/2]  
via FE80::3, Serial0/0/1

C            2001:DB8:ACAD:12::/64 [0/0]  
via ::, Serial0/0/0

L            2001:DB8:ACAD:12::2/128 [0/0]  
via ::, Serial0/0/0

C            2001:DB8:ACAD:23::/64 [0/0] via  
::, Serial0/0/1

L            2001:DB8:ACAD:23::2/128 [0/0]  
via ::, Serial0/0/1

L            FF00::/8 [0/0] via  
::, Null0

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

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

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

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

**R ::/0 [120/1] por medio de RIP**

**Paso 4. Verifique la conectividad.**

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

¿Tuvieron éxito los pings? **SI**

### Reflexión

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

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

Porque en versión 2 para la sumarización necesita clases completas para que detecte las redes. Para que identifique y analice con las rutas directamente conectadas.

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

Por medio de rutas estáticas, que a su vez por medio del protocolo RIP los equipos de la red logran conocer.

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

RIPng se habilita en una interfaz, no en la configuración del router,

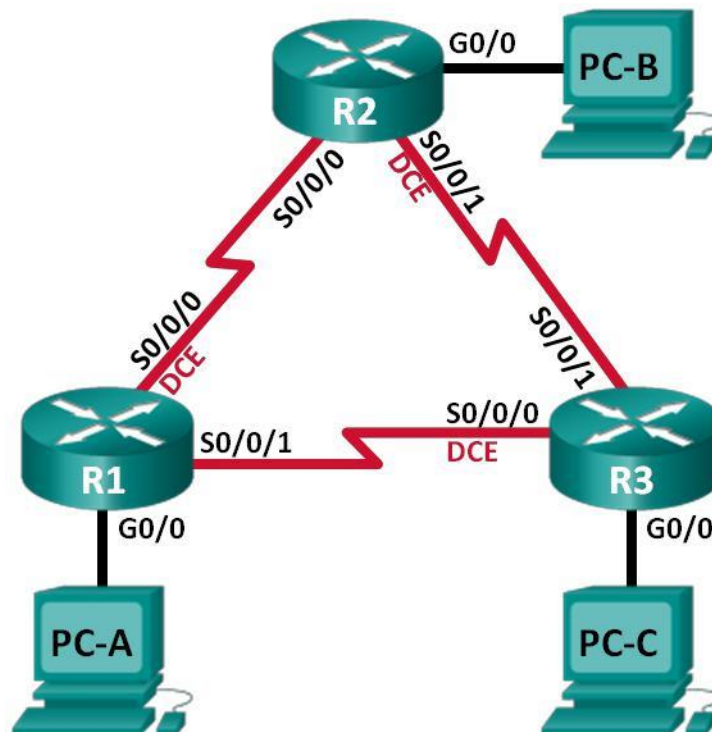
**Tabla de resumen de interfaces del router**

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

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

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

##### Topología



## Tabla de direccionamiento

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

### Objetivos

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

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

### **Parte 3: cambiar las asignaciones de ID del router**

### **Parte 4: configurar interfaces OSPF pasivas**

### **Parte 5: cambiar las métricas de OSPF**

#### **Información básica/situación**

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

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

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

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

#### **Recursos necesarios**

3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet y seriales, como se muestra en la topología

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

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

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

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

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

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

```

Router>enable
Router#conf
Router#configure ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ho
Router(config)#hostname R1
R1(config)#int
R1(config)#interface g0/0
R1(config-if)#ip add
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#no shutdown

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

R1(config-if)#exi
R1(config-if)#exit
R1(config)#inter ser
R1(config)#inter serial 0/0/0
R1(config-if)#ip addre
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#clo
R1(config-if)#clock r
R1(config-if)#clock rate 128000
R1(config-if)#inter serial 0/0/1
R1(config-if)#ip add
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no sh
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#inter serial 0/0/0
R1(config-if)#no sh
R1(config-if)#no shutdown
% 192.168.13.0 overlaps with Serial0/0/1
Serial0/0/0: incorrect IP address assignment
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#no sh
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

```



```

Router>enable
Router#con
Router#conf
Router#configure ter
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ho
Router(config)#hostname R2
R2(config)#inter
R2(config)#interface g0/0
R2(config-if)#ip add
R2(config-if)#ip address 192.168.12.2 255.255.255.252
R2(config-if)#no sh
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)#inter
R2(config)#interface s0/0/0
R2(config-if)#ip add
R2(config-if)#interface g0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#
R2(config-if)#
R2(config-if)#
R2(config-if)#interface s0/0/0
R2(config-if)#ip address 192.168.12.2 255.255.255.252
R2(config-if)#no sh
R2(config-if)#no shutdown

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

R2(config-if)#exit
R2(config)#ip address 192.168.12.2 255.255.255.252
%LINEPROTO-5-UPDOWN: Line protocol on Inteinterface s0/0/1
R2(config-if)#ip ad
R2(config-if)#ip address 192.168.23.1 255.255.255.252
R2(config-if)#cl
R2(config-if)#clock ra
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#no sh
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1. changed state to down

```

```

Router>enable
Router#conf
Router#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ho
Router(config)#hostname R3
R3(config)#inter
R3(config)#interface g0/0
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#no shutdown

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

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

R3(config-if)#
R3(config-if)#interface s0/0/0
R3(config-if)#ip add 192.168.13.2 255.255.255.252
R3(config-if)#clo
R3(config-if)#clock ra
R3(config-if)#clock rate 128000
R3(config-if)#no sh
R3(config-if)#no shutdown

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

R3(config-if)#
R3(config-if)#
R3(config-if)#
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
interface s0/0/1
R3(config-if)#ip add
R3(config-if)#ip address 192.168.23.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#no shutdown

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

```

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

**Paso 5. Probar la conectividad.**

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

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

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

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=3ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms 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 = 3ms, Average = 0ms
```

### Parte 3. Configurar y verificar el enrutamiento OSPF

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

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

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

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

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

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

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

```
R1(config)#router ospf 1  
R1(config-router)#net  
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0  
R1(config-router)#network 192.168.12.0 0.0.0.3 area 0  
R1(config-router)#network 192.168.23.0 0.0.0.3 area 0  
R1(config-router)#no network 192.168.23.0 0.0.0.3 area 0  
R1(config-router)#network 192.168.13.0 0.0.0.3 area 0  
R1(config-router)#  
01:18:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

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

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

R1#

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

R1#

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

R1#

```
R2(config)#router ospf 1  
R2(config-router)#netw  
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0  
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0  
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0  
01:19:32: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on Serial0/0/0 network 192.168.23.0 0.0.0.3 area 0  
--  
R3(config)#router ospf 1  
R3(config-router)#net  
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0  
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0  
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0  
01:30:37: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on Serial0/0/0 network 192.168.23.0 0.0.0.3 area 0
```

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

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

```
R1# show ip ospf neighbor
```

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

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

**R1# show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external  
type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E  
- EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o -  
ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L192.168.1.1/32 is directly connected, GigabitEthernet0/0

O 192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

C192.168.12.0/30 is directly connected, Serial0/0/0

L192.168.12.1/32 is directly connected, Serial0/0/0 192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks

C192.168.13.0/30 is directly connected, Serial0/0/1

L192.168.13.1/32 is directly connected, Serial0/0/1 192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0/30 [110/128] vía 192.168.12.2, 00:31:38, Serial0/0/0

[110/128] vía 192.168.13.2, 00:31:38,  
Serial0/0/1

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

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

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

**R1# show ip protocols**

\*\*\* IP Routing is NSF aware \*\*\*

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 192.168.13.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

```

192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
  Gateway           Distance      Last Update
  192.168.23.2      110          00:19:16
  192.168.23.1      110          00:20:03

```

Distance: (default is 110)

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

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

R1# **show ip ospf**

Routing Process "ospf 1" with ID 192.168.13.1

Start time: 00:20:23.260, Time elapsed: 00:25:08.296 Supports only single TOS(TOS0) routes Supports opaque LSA

Supports Link-local Signaling (LLS) Supports area transit capability Supports NSSA (compatible with RFC 3101) Event-log enabled, Maximum number of events: 1000, Mode: cyclic

Router is not originating router-LSAs with maximum metric Initial SPF schedule delay 5000 msec

Minimum hold time between two consecutive SPF's 10000 msec

Maximum wait time between two consecutive SPF's 10000 msec

Incremental-SPF disabled

Minimum LSA interval 5 secs

Minimum LSA arrival 1000 msec

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 opaque AS LSA 0. Checksum Sum 0x000000

Number of DCbitless external and opaque AS LSA 0  
Number of DoNotAge external and opaque AS LSA 0  
Number of areas in this router is 1. 1 normal 0 stub 0 nssa  
Number of areas transit capable is 0  
External flood list length 0  
IETF NSF helper support enabled  
Cisco NSF helper support enabled  
Reference bandwidth unit is 100 mbps  
Area BACKBONE(0)  
Number of interfaces in this area is 3  
Area has no authentication  
SPF algorithm last executed 00:22:53.756 ago  
SPF algorithm executed 7 times  
Area ranges are  
Number of LSA 3. Checksum Sum 0x019A61  
Number of opaque link LSA 0. Checksum Sum 0x000000  
Number of DCbitless LSA 0  
Number of indication LSA 0  
Number of DoNotAge LSA 0  
Flood list length 0

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

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



```

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

```

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

```

R1# show ip ospf interface

```

```

Serial0/0/1 is up, line protocol is up
Internet          Address 192.168.13.1/30, Area 0, Attached via
Network Statement

```

```

Process          ID 1, Router ID 192.168.13.1, Network Type
POINT_TO_POINT, Cost: 64

```

```

Topology-MTID          Cost   Disabled   Shutdown   Topology
Name
0                      64      no         no         Base

```

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

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

oob-resync timeout 40

Hello due in 00:00:01

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

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

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1,  
Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2 Suppress hello for 0  
neighbor(s)

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

Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 192.168.13.1, Network Type POINT\_TO\_POINT, Cost: 64

Topology-MTID Cost Disabled Shutdown Topology Name

0 64 no no Base Transmit Delay is 1 sec, State POINT\_TO\_POINT

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

oob-resync timeout 40

Hello due in 00:00:03

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 2/2, flood queue length 0

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

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1,  
Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.1 Suppress hello for 0  
neighbor(s)

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1

Topology-MTID Name	Cost	Disabled	Shutdown	Topology
0	1	no	no	Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated 192.168.1.1	Router (ID)	192.168.13.1,	Interface	address
---------------------------	-------------	---------------	-----------	---------

No backup designated router on this network

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

oob-resync timeout 40

Hello due in 00:00:01

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

**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 Programming Attributes
Command Prompt

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 = 3ms, Average = 0ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=3ms TTL=126
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126
Reply from 192.168.2.3: bytes=32 time=21ms TTL=126
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 21ms, Average = 7ms

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=5ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

PC-B

```
Physical Config Desktop Programming Attributes
Command Prompt

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

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=16ms TTL=126
Reply from 192.168.3.3: bytes=32 time=5ms TTL=126

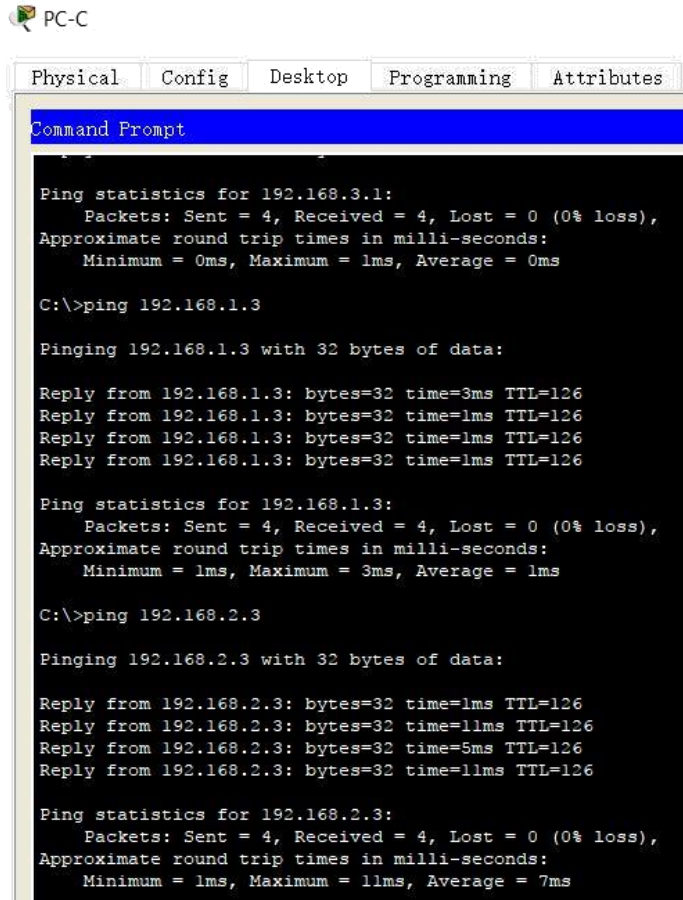
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 5ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=13ms TTL=126
Reply from 192.168.1.3: bytes=32 time=12ms TTL=126
Reply from 192.168.1.3: bytes=32 time=8ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 8ms
```



The screenshot shows a Windows desktop environment with a taskbar at the top containing icons for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The main window is a 'Command Prompt' with a black background and white text. It displays the results of two ping commands. The first command is 'ping 192.168.3.1', which shows four successful replies with 0% loss and an average round trip time of 0ms. The second command is 'ping 192.168.2.3', which also shows four successful replies with 0% loss and an average round trip time of 7ms.

```
Command Prompt

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=3ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=11ms TTL=126
Reply from 192.168.2.3: bytes=32 time=5ms TTL=126
Reply from 192.168.2.3: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 7ms
```

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

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

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

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

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

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

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

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

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

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

```
R1(config)#interface loopback 0

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

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

R1(config-if)#ip add
R1(config-if)#ip address 1.1.1.1 255.255.255.255
```

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

```
R2(config)#interface loopback 0

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

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

R2(config-if)#ip add
R2(config-if)#ip address 2.2.2.2 255.255.255.255

R3(config)#interface loopback 0

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

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

R3(config-if)#ip add
R3(config-if)#ip address 3.3.3.3 255.255.255.255
```

- c. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.
- d. Debe volver a cargar los routers para restablecer la ID del router a la dirección de loopback. Emita el comando **reload** en los tres routers. Presione Enter para confirmar la recarga.
- e. Una vez que se haya completado el proceso de recarga del router, emita el comando **show ip protocols** para ver la nueva ID del router.

R1# **show ip protocols**

\*\*\* IP Routing is NSF aware \*\*\*

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0 Last Update

Routing Information Sources:

Gateway	Distance	
1.3.3.3	110	00:01:00
1.2.2.2	110	00:01:14



Distance: (default is 110)

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

R1# **show ip ospf neighbor**

Neighbor ID Interface	Pri	State		Dead Time	Address
3.3.3.3 Serial0/0/1	0	FULL/	-	00:00:35	192.168.13.2
2.2.2.2 Serial0/0/0	0	FULL/	-	00:00:32	192.168.12.2

R1#

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

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

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

```
R1(config)# router ospf 1 R1(config-router)# router-id  
11.11.11.11
```

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

```
R1(config)# end
```

- b. Recibirá un mensaje informativo en el que se le indique que debe volver a cargar el router o usar el comando **clear ip ospf process** para que se aplique el cambio. Emita el comando **clear ip ospf process** en los tres routers. Escriba **yes** (sí) como respuesta al mensaje de verificación de restablecimiento y presione Enter.
- c. Establezca la ID del router R2 **22.22.22.22** y la ID del router R3 **33.33.33.33**. Luego, use el comando **clear ip ospf process** para restablecer el proceso de routing de OSPF.
- d. Emita el comando **show ip protocols** para verificar que la ID del router R1 haya cambiado.

```
R1# show ip protocols
```

```
*** IP Routing is NSF aware ***
```

Routing Protocol is "ospf 1"  
Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 11.11.11.11

Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

Gateway	Distance	Last Update
33.33.33.33	110	00:00:19
22.22.22.22	110	00:00:31
3.3.3.3	110	00:00:41
2.2.2.2	110	00:00:41

Distance: (default is 110)

```
show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 :
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1         110          00:05:32
    2.2.2.2         110          00:01:51
    3.3.3.3         110          00:00:22
    11.11.11.11    110          00:00:03
    22.22.22.22    110          00:00:12
    33.33.33.33    110          00:00:03
  Distance: (default is 110)
```

R1#

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

R1# **show ip ospf neighbor**

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

```
22.22.22.22          0 FULL/ -          00:00:32          192.168.12.2
Serial0/0/0
```

```
R1#show ip ospf neighbor
```

```
Neighbor ID      Pri   State           Dead Time   Address      Interface
33.33.33.33      0     FULL/ -         00:00:39   192.168.13.2 Serial0/0/1
22.22.22.22      0     FULL/ -         00:00:39   192.168.12.2 Serial0/0/0
R1#
```

## Parte 5. configurar las interfaces pasivas de OSPF

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

### Paso 1. configurar una interfaz pasiva.

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

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

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

```
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
```

```
Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
```

Topology-MTID Name	Cost	Disabled	Shutdown	Topology
0	1	no	no	Base

```
Transmit Delay is 1 sec, State DR, Priority 1
```

```
Designated Router (ID) 11.11.11.11, Interface address
```

192.168.1.1

No backup designated router on this network

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

oob-resync timeout 40

Hello due in 00:00:02

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

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

```
R1(config)# router ospf 1 R1(config-router)# passive-interface  
g0/0
```

```
R1(config)#router ospf 1  
R1 (config-router) #pas  
R1 (config-router) #passive-interface g0/0  
R1 (config-router) #
```

---

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

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

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1

Topology-MTID Name	Cost	Disabled	Shutdown	Topology
0	1	no	no	Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 11.11.11.11, Interface address

192.168.1.1

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
1#
```

No backup designated router on this network

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

oob-resync timeout 40

No Hellos (Passive interface)

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

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

**R2# 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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

+ - replicated route, % - next hop override Gateway of last resort is not set

2.0.0.0/32 is subnetted, 1 subnets

C 2.2.2.2 is directly connected, Loopback0

O 192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.2.0/24 is directly connected,  
GigabitEthernet0/0

L 192.168.2.1/32 is directly connected,  
GigabitEthernet0/0

O 192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.12.0/30 is directly connected, Serial0/0/0

L192.168.12.2/32 is directly connected, Serial0/0/0

192.168.13.0/30 is subnetted, 1 subnets

O 192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1

[110/128] via 192.168.12.1, 00:58:32,  
Serial0/0/0

192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.23.0/30 is directly connected, Serial0/0/1

L192.168.23.1/32 is directly connected, Serial0/0/1

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

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

```
R1# show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time      Address
Interface
33.33.33.33      0    FULL/ -         00:00:31      192.168.13.2
Serial0/0/1

22.22.22.22     0    FULL/ -         00:00:32      192.168.12.2
Serial0/0/0
```

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

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

```
R2(config-router)#
```

```
*Apr          3  00:03:00.979:      %OSPF-5-ADJCHG: Process 1, Nbr
```

```
11.11.11.11 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Interface down or detached
```

```
*Apr          3  00:03:00.979:      %OSPF-5-ADJCHG: Process 1, Nbr
33.33.33.33 on Serial0/0/1 from FULL to DOWN, Neighbor Down:
Interface down or detached
```

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

```
R1# show ip ospf neighbor
```

```
Neighbor ID      Pri   State           Dead Time      Address
Interface
33.33.33.33      0    FULL/ -         00:00:34      192.168.13.2
Serial0/0/1
```

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

```
Neighbor ID      Pri   State           Dead Time      Address      Interface
33.33.33.33      0    FULL/ -         00:00:37      192.168.13.2  Serial0/0/1
R1#
***
```



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

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

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

```
Internet          Address 192.168.12.2/30,      Area 0, Attached via
Network Statement

Process          ID 1, Router      ID 22.22.22.22,      Network Type
POINT_TO_POINT,      Cost: 64

Topology-MTID          Cost Disabled Shutdown      Topology
Name

      0                64      no      no          Base
```

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

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

oob-resync timeout 40

No Hellos (Passive interface)

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 2/2, flood queue length 0

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

Last flood scan length is 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)

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

```

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

Gateway of last resort is not set

 3.0.0.0/32 is subnetted, 1 subnets
C    3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:07:16, Serial0/0/0
O    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, GigabitEthernet0/0
L    192.168.3.1/32 is directly connected, GigabitEthernet0/0
O    192.168.12.0/30 is subnetted, 1 subnets
O    192.168.12.0/30 [110/128] via 192.168.13.1, 00:01:17, Serial0/0/0
O    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/0
L    192.168.13.2/32 is directly connected, Serial0/0/0
O    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.23.0/30 is directly connected, Serial0/0/1
L    192.168.23.2/32 is directly connected, Serial0/0/1

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

Gateway of last resort is not set

 1.0.0.0/32 is subnetted, 1 subnets
C    1.1.1.1/32 is directly connected, Loopback0
O    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:09:05, Serial0/0/1
O    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.1/32 is directly connected, Serial0/0/0
O    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/1
L    192.168.13.1/32 is directly connected, Serial0/0/1
O    192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0/30 [110/128] via 192.168.13.2, 00:03:44, Serial0/0/1

```

- f. En el R2, emita el comando **no passive-interface** para que el router envíe y reciba actualizaciones de routing OSPF. Después de introducir este comando, verá un

mensaje informativo que explica que se estableció una adyacencia de vecino con el R1.

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

```
*Apr          3 00:18:03.463:    %OSPF-5-ADJCHG: Process 1, Nbr  
11.11.11.11 on Serial0/0/0 from LOADING to FULL, Loading Done
```

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

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

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3?  
**[110/129]**

¿El R2 aparece como vecino OSPF en el R1? **SI** ¿El R2 aparece como vecino OSPF en el R3? **SI** ¿Qué indica esta información?

Que la configuración es correcta y se logra comunicación entre todos los puntos.

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

```
R2(config-router)#  
R2(config-router)#no passive-interface s0/0/1  
R2(config-router)#  
R2(config-router)#  
R2(config-router)#  
R2(config-router)#  
R2(config-router)#  
R2(config-router)#  
R2(config-router)#  
R2(config-router)#  
R2(config-router)#  
30:27:11: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from LOADING to FULL, Loading Done
```

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

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

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

**[110/65]**

¿El R2 aparece como vecino OSPF del R3? **SI**

## **Parte 6. cambiar las métricas de OSPF**

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

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

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

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

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

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

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

```
Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
```

```
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec, reliability  
255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set Keepalive set  
(10 sec)
```

```
Full Duplex, 100Mbps, media type is RJ45
```

```
output flow-control is unsupported, input flow-control is unsupported
```

```
ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input never, output 00:17:31, output hang never Last clearing of "show  
interface" counters never
```

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output  
drops: 0
```

```
Queueing strategy: fifo
```

```
Output queue: 0/40 (size/max)
```

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer Received 0  
broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

0 watchdog, 0 multicast, 0 pause input

279 packets output, 89865 bytes, 0 underruns

0 output errors, 0 collisions, 1 interface resets

0 unknown protocol drops

0 babbles, 0 late collision, 0 deferred

1 lost carrier, 0 no carrier, 0 pause output

0 output buffer failures, 0 output buffers swapped out

**Nota:** si la interfaz del equipo host solo admite velocidad Fast Ethernet, la configuración de ancho de banda de G0/0 puede diferir de la que se muestra arriba. Si la interfaz del equipo host no admite velocidad de gigabit, es probable que el ancho de banda se muestre como 100 000 Kbit/s.

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

**R1# show ip route ospf**

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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

+ - replicated route, % - next hop override Gateway of last resort is not set

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1

[110/128] via 192.168.12.2, 00:01:08,

Serial0/0/0

**Nota:** el costo acumulado del R1 a la red 192.168.3.0/24 es 65.

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

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

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST,

Cost: 1

Topology-MTID Name	Cost	Disabled	Shutdown	Topology
0	1	no	no	Base
Transmit Delay is 1 sec, State DR, Priority 1				
Designated Router 192.168.3.1	(ID)	192.168.23.2,	Interface	address

No backup designated router on this network

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

oob-resync timeout 40

Hello due in 00:00:05

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

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

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

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

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 1.1.1.1, Network Type POINT\_TO\_POINT, Cost: 64

Topology-MTID Name	Cost	Disabled	Shutdown	Topology
0	64	no	no	Base



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

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

oob-resync timeout 40

Hello due in 00:00:04

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

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

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1,  
Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2 Suppress hello for 0  
neighbor(s)

La suma de los costos de estas dos interfaces es el costo acumulado de la ruta a la red 192.168.3.0/24 en el R3 ( $1 + 64 = 65$ ), como puede observarse en el resultado del comando **show ip route**.

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

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

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

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

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

```
R3(config-router)#auto-cost re
R3(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R2(config-router)#
R2(config-router)#auto-cost re
R2(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R2(config-router)#
```

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

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

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST,

Cost: 10

Topology-MTID Name	Cost	Disabled	Shutdown	Topology
0	10	no	no	Base

Transmit Delay is 1 sec, State DR, Priority 1  
Designated Router (ID) 192.168.23.2, Interface address  
192.168.3.1

No backup designated router on this network

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

oob-resync timeout 40

Hello due in 00:00:02

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

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

GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.3.1/24, Area 0
 Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 100
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:02
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
.
```

**Nota:** si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo será diferente del que se muestra en el resultado. Por ejemplo, el costo será de 100 para la velocidad Fast Ethernet (100 Mb/s).

R1# **show ip ospf interface s0/0/1** Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 1.1.1.1, Network Type POINT\_TO\_POINT, Cost: 6476

Topology-MTID Name	Cost	Disabled	Shutdown	Topology
0	6476	no	no	Base

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

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
oob-resync timeout 40

Hello due in 00:00:05

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

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

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1,  
Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2 Suppress hello for 0  
neighbor(s)

- h. Vuelva a emitir el comando **show ip route ospf** para ver el nuevo costo acumulado de la ruta 192.168.3.0/24 ( $10 + 6476 = 6486$ ).

**Nota:** si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo total será diferente del que se muestra en el resultado. Por ejemplo, el costo acumulado será 6576 si G0/0 está funcionando con velocidad Fast Ethernet (100 Mb/s).

R1# **show ip route ospf**

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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

+ - replicated route, % - next hop override Gateway of last resort is not set

O 192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0

O 192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1

[110/12952] via 192.168.12.2, 00:05:17,  
Serial0/0/

**Nota:** cambiar el ancho de banda de referencia en los routers de 100 a 10 000 cambió los costos acumulados de todas las rutas en un factor de 100, pero el costo de cada enlace y ruta de interfaz ahora se refleja con mayor precisión.

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

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

```
R1(config-router)# auto-cost reference-bandwidth 100
```

```
% OSPF: Reference bandwidth is changed.
```

Please ensure reference bandwidth is consistent across all routers.

¿Por qué querría cambiar el ancho de banda de referencia OSPF predeterminado? **Para usar el valor de referencia de cada interface de forma correcta**

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

En la mayoría de los enlaces seriales, la métrica del ancho de banda será 1544 Kbits de manera predeterminada (la de un T1). Si esta no es la velocidad real del enlace serial, se deberá cambiar la configuración del ancho de banda para que coincida con la

velocidad real, a fin de permitir que el costo de la ruta se calcule correctamente en OSPF. Use el comando **bandwidth** para ajusta la configuración del ancho de banda de una interfaz.

**Nota:** un concepto erróneo habitual es suponer que con el comando **bandwidth** se cambia el ancho de banda físico, o la velocidad, del enlace. El comando modifica la métrica de ancho de banda que utiliza OSPF para calcular los costos de routing, pero no modifica el ancho de banda real (la velocidad) del enlace.

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

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

```
Serial0/0/0 is up, line protocol is up Hardware is WIC MBRD
Serial Internet address is 192.168.12.1/30
```

```
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec, reliability 255/255,
txload 1/255, rxload 1/255
```

```
Encapsulation HDLC, loopback not set Keepalive set (10
sec)
```

<Output Omitted>

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

**R1# show ip route ospf**

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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

+ - replicated route, % - next hop override Gateway of last resort is not set

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1

[110/128] via 192.168.12.2, 00:00:42,  
Serial0/0/0

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

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

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

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

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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

+ - replicated route, % - next hop override Gateway of last resort is not set

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1

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

R1# **show ip ospf interface brief**

Interface State Nbrs F/C	PID	Area	IP Address/Mask		Cost
Se0/0/1 1/1	1	0	192.168.13.1/30	64	P2P
Se0/0/0 1/1	1	0	192.168.12.1/30	781	P2P



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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, I - LISP

+ - replicated route, % - next hop override Gateway of  
last resort is not set

O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1

[110/845] via 192.168.12.2, 00:00:09,

Serial0/0/0

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

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

R3# **show ip route ospf**

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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

+ - replicated route, % - next hop override Gateway of last resort is  
not set

O 192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0

192.168.12.0/30 is subnetted, 1 subnets

O 192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1

[110/128] via 192.168.13.1, 00:30:58,  
Serial0/0/0

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

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

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

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

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

R1# show ip route ospf

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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

+ - replicated route, % - next hop override Gateway of last resort is not set

O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0

O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1

[110/1562] via 192.168.12.2, 00:02:40,  
Serial0/0/0

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

```
R1(config)# int s0/0/1 R1(config-if)# ip ospf cost  
1565
```

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

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

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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0

O 192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0

**Nota:** la manipulación de costos de enlace mediante el comando **ip ospf cost** es el método de preferencia y el más fácil para cambiar los costos de las rutas OSPF. Además de cambiar el costo basado en el ancho de banda, un administrador de red puede tener otros motivos para cambiar el costo de una ruta, como la preferencia por un proveedor de servicios específico o el costo monetario real de un enlace o de una ruta.

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

### Reflexión

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

Para lograr mantener un orden y tener una marca que me permita realizar troubleshooting

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

Se está trabajando en el protocolo ospf el cual realiza sus procesos de métrica de forma diferente

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

Para obligar al equipo a comprender la ruta por otra interface diferente a la usada

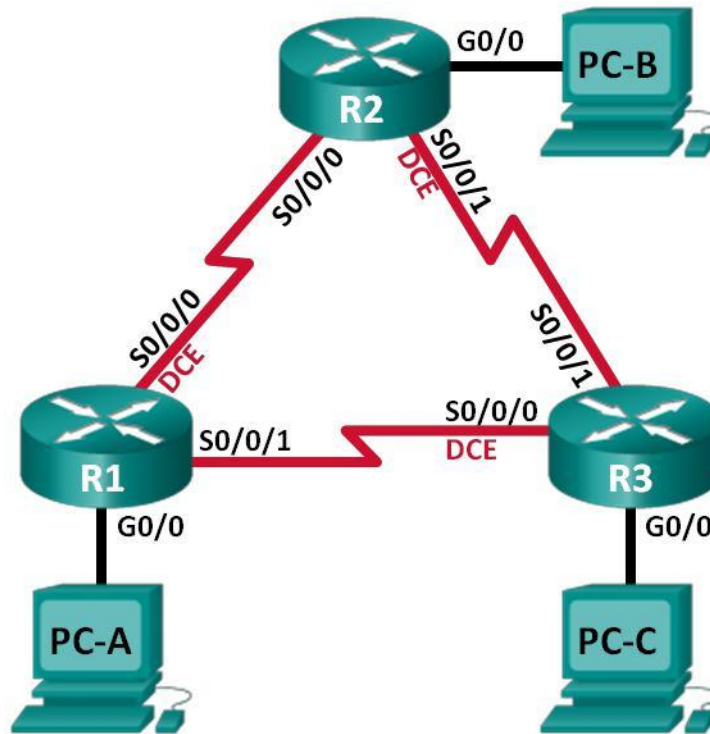
**Tabla de resumen de interfaces del router**

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

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

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

#### Topología



#### Tabla de direccionamiento

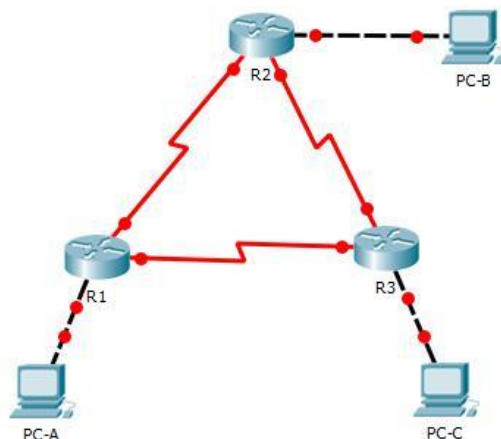
Dispositivo	Interfaz	Dirección IPv6	Gateway predeterminado
R1	G0/0	2001:DB8:ACAD:A::1/64 FE80::1 link-local	No aplicable
	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:13::1/64 FE80::1 link-local	No aplicable
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local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

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

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

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

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



**Paso 4:** 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 Attributes
IOS Command Line Interface
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 5
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#banner motd "Warning"
R1(config)#service password-encryption
R1(config)#in
% Incomplete command.
R1(config)#interface
% Incomplete command.
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#FE80::1 link-local
^
% Invalid input detected at '^' marker.
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#interface serial 0/0/0
```

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#clock rate 128000
R1(config-if)#interface serial 0/0/1
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#interface serial 0/0/0
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#interface serial 0/0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:13::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#interface serial 0/0/0
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#interface g0/0
R1(config-if)#no shutdown

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

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

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

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



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

Press RETURN to get started!

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 5
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#banner motd "Warning 2"
R2(config)#logging synchronous
R2(config)#logging synchronous
^
% Invalid input detected at '^' marker.

R2(config)#line vty 0 5
R2(config-line)#logging synchronous
R2(config-line)#service password-encryption
R2(config)#ipv6 unicast-routing
R2(config)#interface g0/0
R2(config-if)#ipv6 address |
```

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

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

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

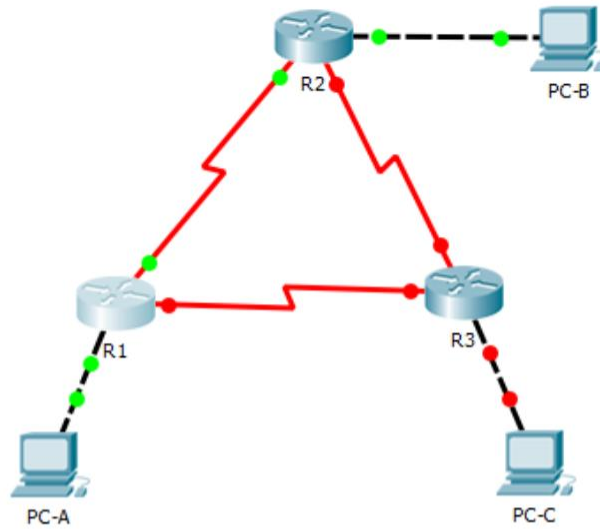
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#ip
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
v
% Incomplete command.
R2(config-if)#interface 0/0/1
^
% Invalid input detected at '^' marker.

R2(config-if)#interface serial 0/0/1
R2(config-if)#
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

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

R2#copy running-config
% Incomplete command.
R2#copy running-config startup-config
Destination filename [startup-config]:
```



R3

Physical Config CLI Attributes

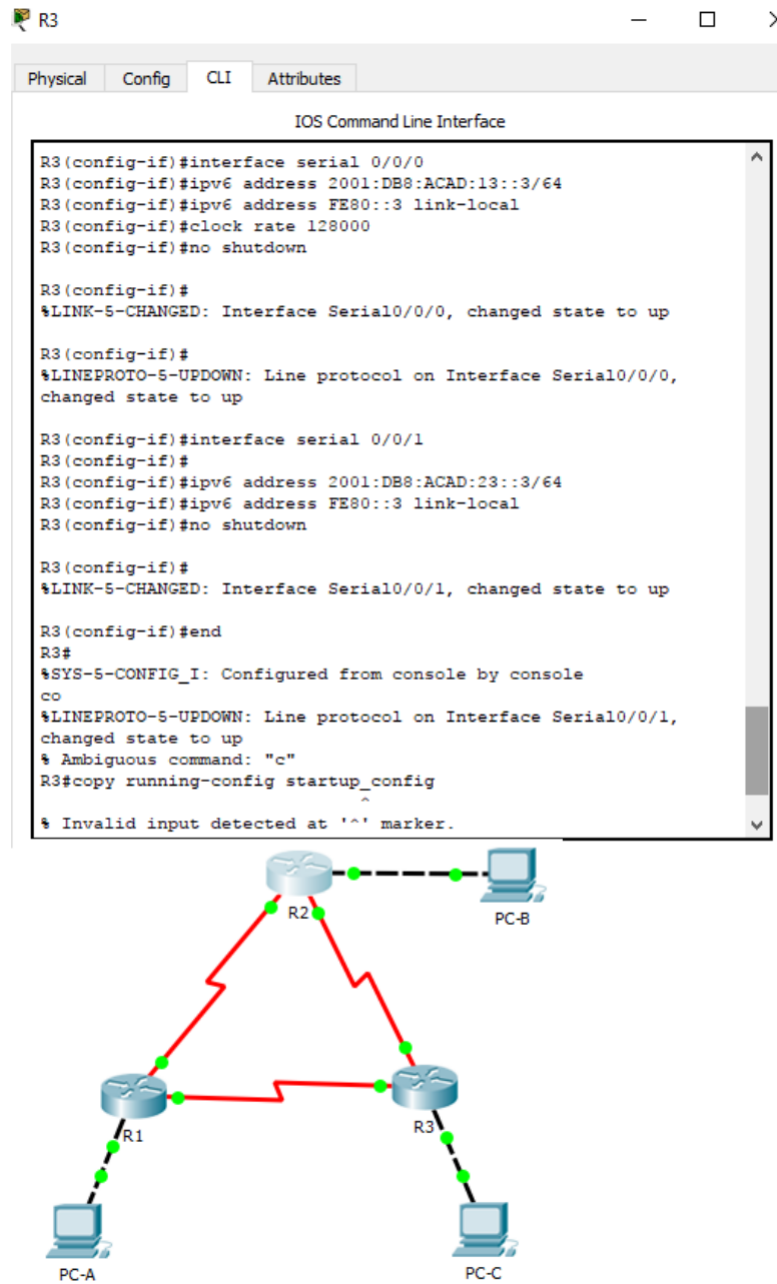
IOS Command Line Interface

```

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 5
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#service password-encryption
R3(config)#ipv6 unicast-routing
R3(config)#interface g0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown

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

CLI (55 to exit CLI) [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 2: Configurar el routing OSPFv3

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

### Paso 1: Asignar ID a los Routers.

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

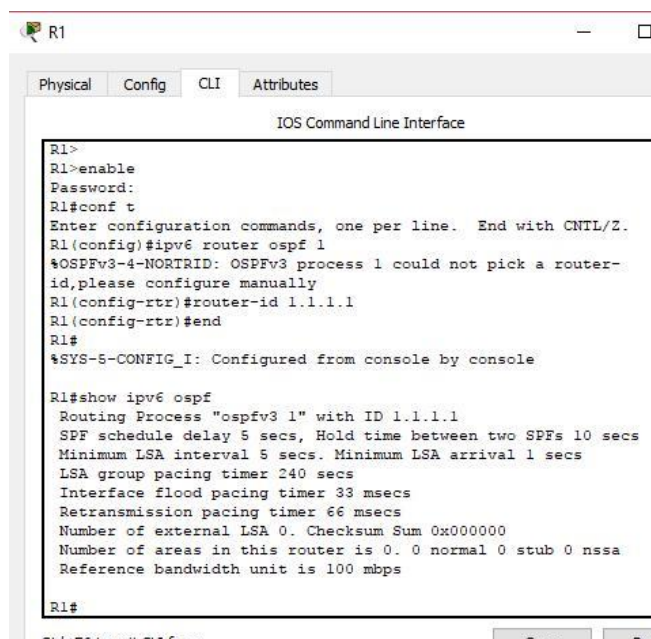
a. Emita el comando `ipv6 router ospf` para iniciar un proceso OSPFv3 en el router.

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

```
R1>
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-
id,please configure manually
```

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

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



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1>
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/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)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

R1#
```

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

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

```
R2# show ipv6 ospf
```

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

```
Event-log enabled, Maximum number of events: 1000, Mode: cyclic  
Router is not originating router-LSAs with maximum metric <Output  
Omitted>
```

```
R2
Physical Config CLI Attributes
IOS Command Line Interface
%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
Warning 2
User Access Verification
Password:
Password:
R2>enable
Password:
R2#config 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)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#

R3
Physical Config CLI Attributes
IOS Command Line Interface
R3#
R3#
R3#
R3#config 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)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
R3#
```

**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
```

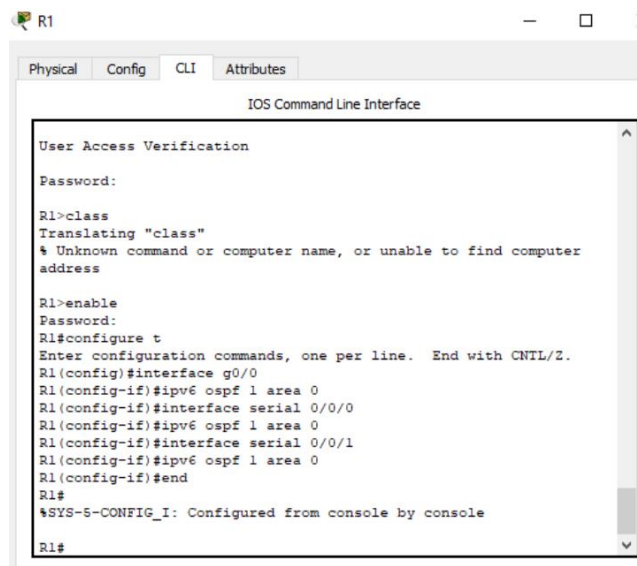
```
R1(config-if)# ipv6 ospf 1 area 0
```

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

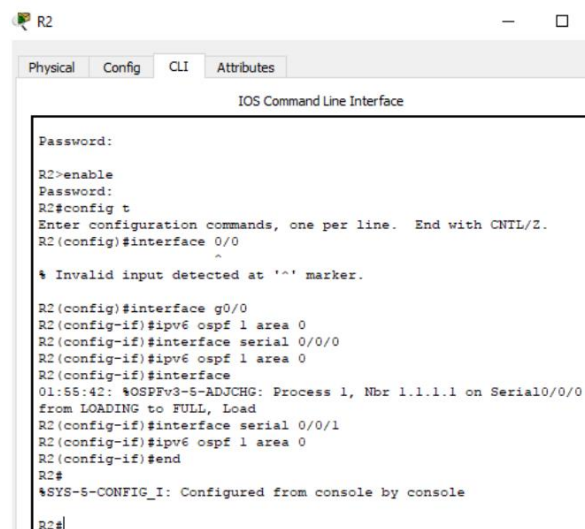
```
R1(config-if)# ipv6 ospf 1 area 0
```

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

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



The screenshot shows the CLI of router R1. The user has entered the following commands: `class`, `enable`, `configure t`, `interface g0/0`, `ipv6 ospf 1 area 0`, `interface serial 0/0/0`, `ipv6 ospf 1 area 0`, `interface serial 0/0/1`, `ipv6 ospf 1 area 0`, and `end`. The output shows the configuration is successful, with a message: `%SYS-5-CONFIG_I: Configured from console by console`.



The screenshot shows the CLI of router R2. The user has entered the following commands: `enable`, `configure t`, `interface 0/0`, `interface g0/0`, `ipv6 ospf 1 area 0`, `interface serial 0/0/0`, `ipv6 ospf 1 area 0`, `interface`, `interface serial 0/0/1`, `ipv6 ospf 1 area 0`, and `end`. The output shows the configuration is successful, with a message: `%SYS-5-CONFIG_I: Configured from console by console`.

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

R1#

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

R1#

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

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

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

R1# show ipv6 ospf neighbor

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

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

```
R1>enable
Password:
R1#show
% Incomplete command.
R1#show ipv6 ospf neighbor

Neighbor ID    Pri   State           Dead Time   Interface ID
Interface
2.2.2.2        0    FULL/ -         00:00:39   3
Serial0/0/0
3.3.3.3        0    FULL/ -         00:00:39   3
Serial0/0/1
R1#
```

```
R2>enable
Password:
R2#show ipv6 ospf neighbor

Neighbor ID    Pri   State           Dead Time   Interface ID
Interface
1.1.1.1        0    FULL/ -         00:00:35   3
Serial0/0/0
3.3.3.3        0    FULL/ -         00:00:31   4
Serial0/0/1
R2#
```

```

R3>enable
Password:
R3#show ipv6 ospf neighbors
^
% Invalid input detected at '^' marker.

R3#show ipv6 ospf neighbor

Neighbor ID      Pri   State           Dead Time   Interface ID
Interface
2.2.2.2          0    FULL/ -         00:00:30   4
Serial0/0/1
1.1.1.1          0    FULL/ -         00:00:36   4
Serial0/0/0
R3#

```

**Paso 4:** Verificar la configuración del protocolo OSPFv3.

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

```
R1# show ipv6 protocols
```

```
IPv6 Routing Protocol is "connected"
```

```
IPv6 Routing Protocol is "ND"
```

```
IPv6 Routing Protocol is "ospf 1"
```

```
Router ID 1.1.1.1
```

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

```
Interfaces (Area 0):
```

```
Serial0/0/1
```

```
Serial0/0/0
```

```
GigabitEthernet0/0
```

```
Redistribution:
```

```
None
```



```

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

R1#show ipv6 ospf interface
GigabitEthernet0/0 is up, line protocol is up

```

Ctrl+F6 to exit CLI focus

Copy

Paste

### 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.

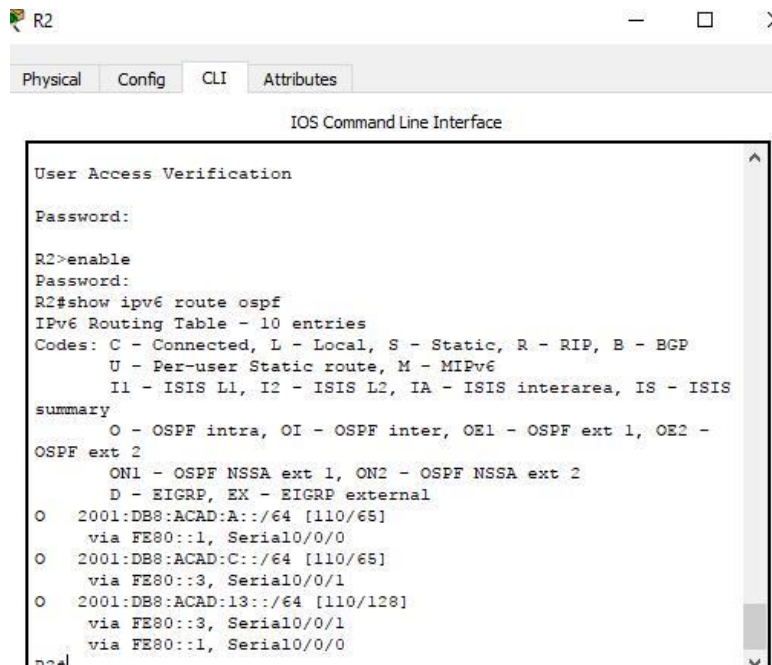
```

R1#show ipv6 ospf interface
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 00:00:01
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 4
  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 00:00:08
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 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 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1

```

### Parte 3: Configurar las interfaces pasivas de OSPFv3

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
Physical Config CLI Attributes
IOS Command Line Interface

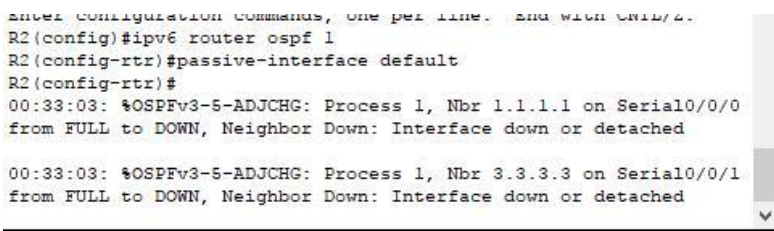
User Access Verification

Password:

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

**Paso 2:** Establecer la interfaz pasiva como la interfaz predeterminada en el Router.

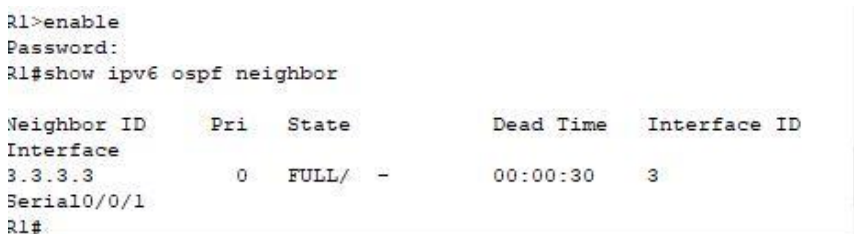
a. Emita el comando `passive-interface default` en el R2 para establecer todas las interfaces OSPFv3 como pasivas de manera predeterminada



```
Enter configuration commands, one per line. End with CNTRL-Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
00:33:03: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached

00:33:03: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
R2#
```

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>enable
Password:
R1#show ipv6 ospf neighbor

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

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

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

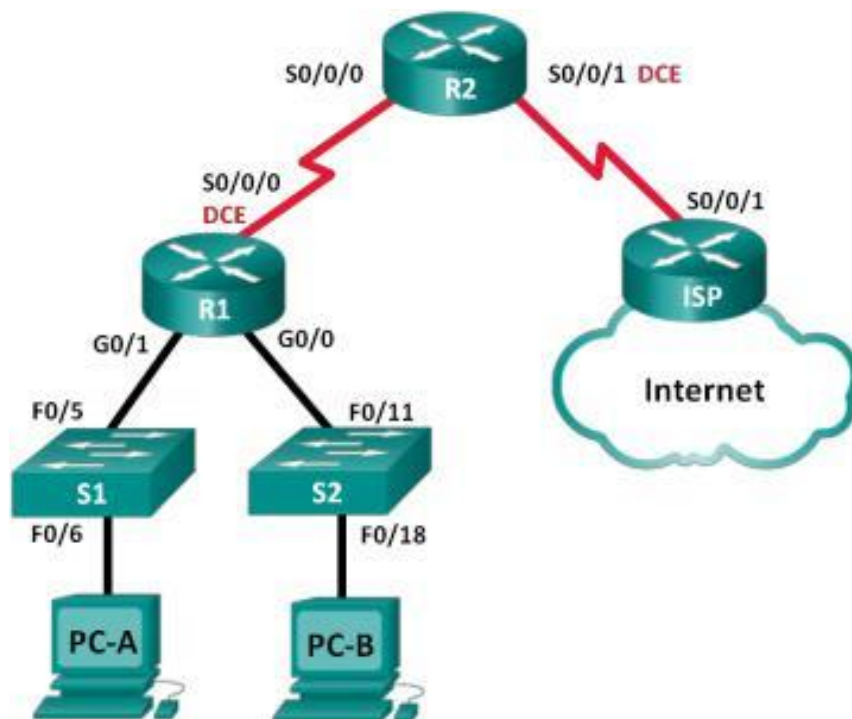
d. Si todas las interfaces OSPFv3 en el R2 son pasivas, no se anuncia ninguna información de routing. Si este es el caso, el R1 y el R3 ya no deberían tener una ruta a la red `2001:DB8:ACAD:B::/64`. Esto se puede verificar mediante el comando `show ipv6 route`.

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.

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

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

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

### **Recursos necesarios**

3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

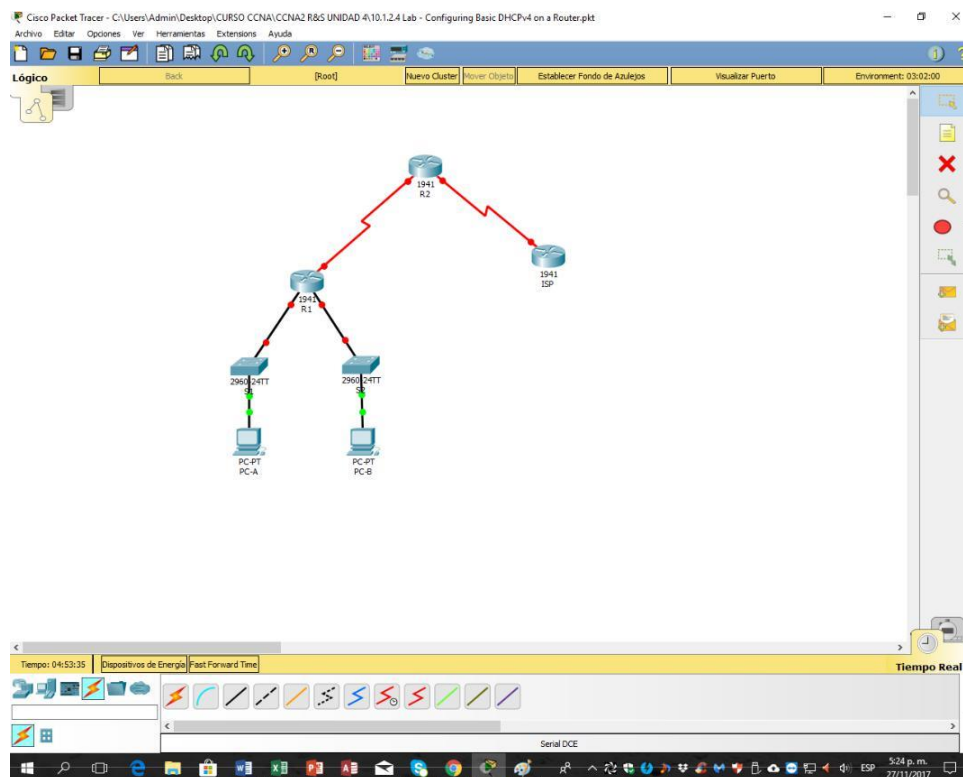
Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet y seriales, como se muestra en la topología

### **Parte 7. 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.**

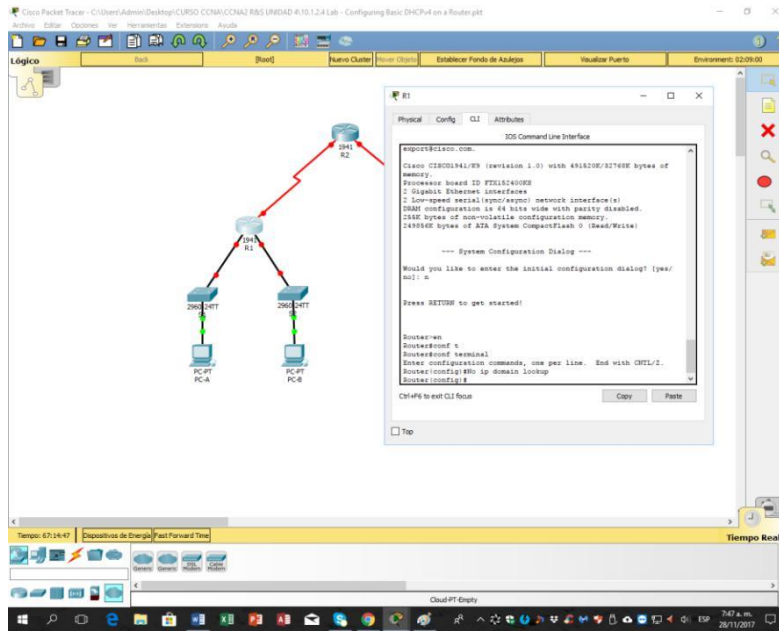


#### **Paso 2. inicializar y volver a cargar los routers y los switches.**

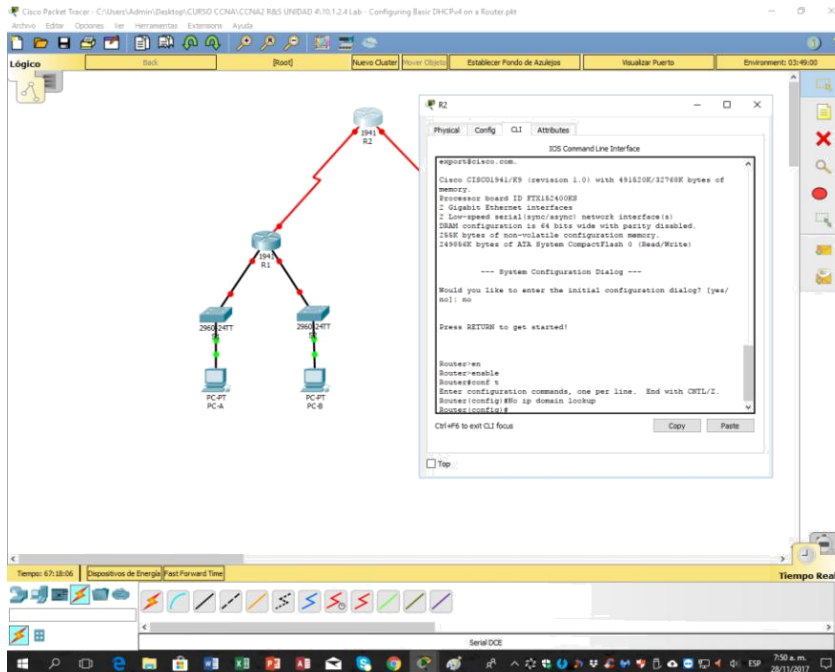
#### **Paso 3. configurar los parámetros básicos para cada router.**

- a. Desactive la búsqueda DNS.

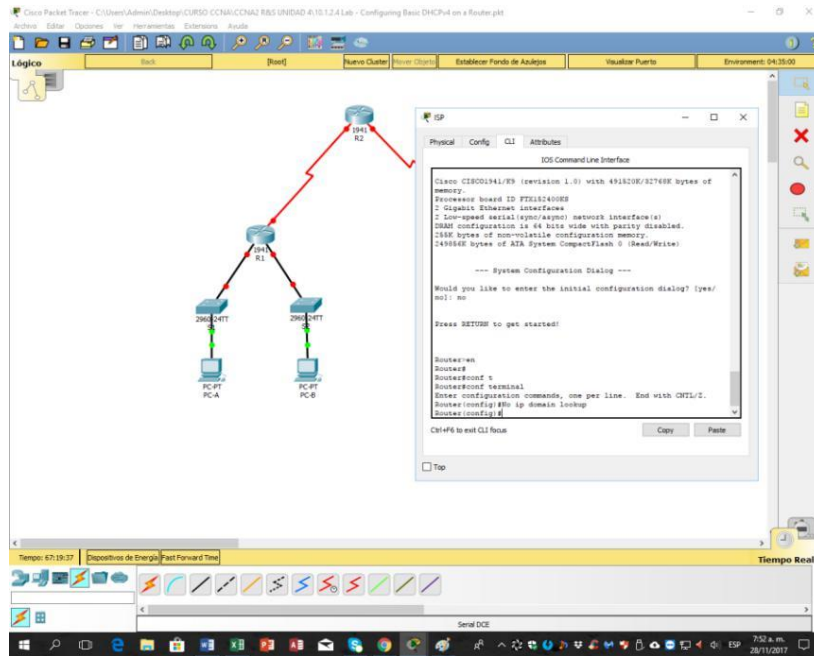
## Router 1:



## Router 2:

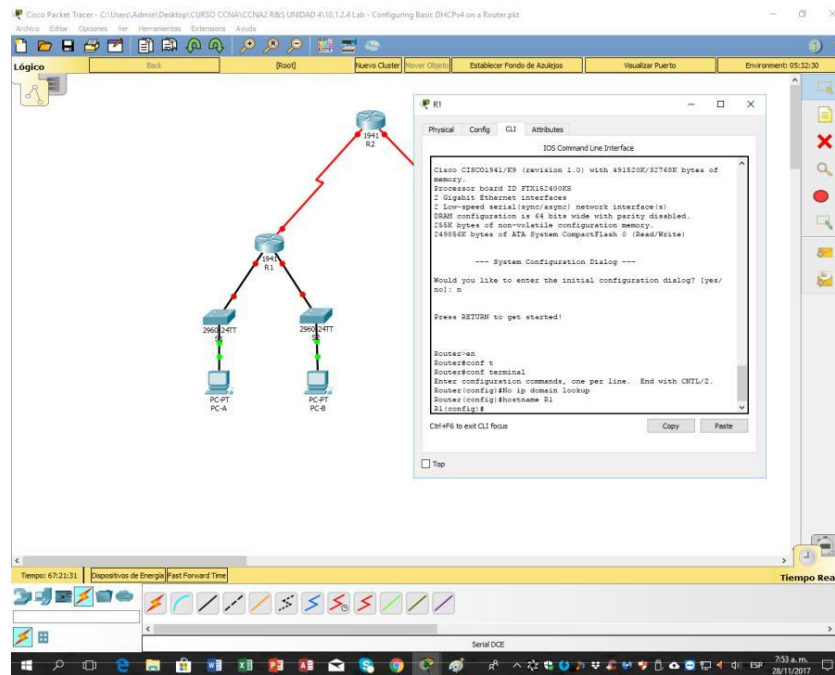


ISP:



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

Router 1:





## Router 2:

The screenshot shows the Cisco Packet Tracer interface with a network diagram and a configuration window for Router 2. The network diagram features a central Router 1 (R1) connected to two PCs (PC-A and PC-B) via 2960-SWT switches. Router 1 is also connected to Router 2 (R2) via a serial link. The configuration window for R2 is open, displaying the IOS Command Line Interface (CLI) with the following text:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#0 ip domain lookup
Router(config)#hostname R2
R2(config)#
Ctrl+C to exit CLI focus
```

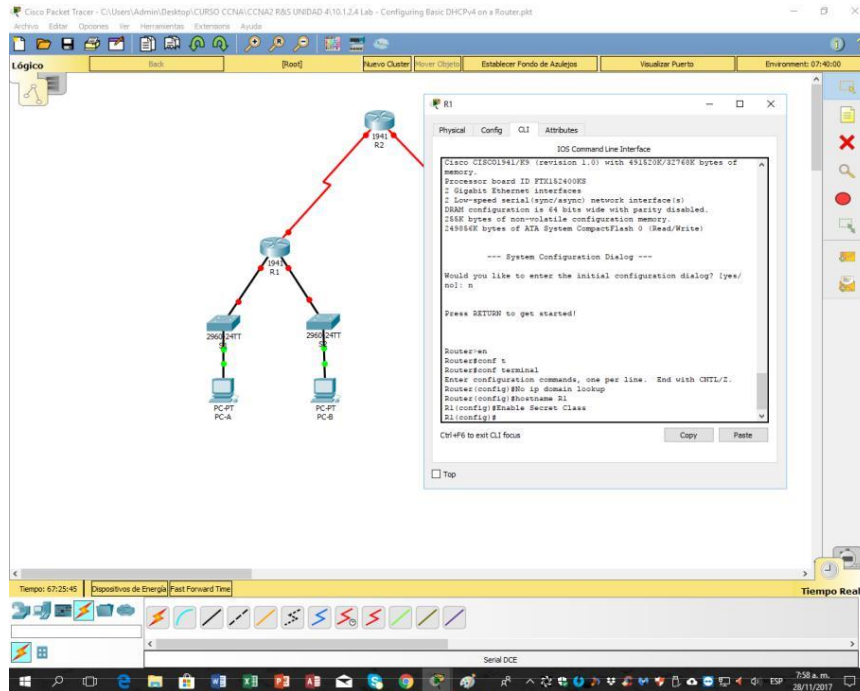
## ISP:

The screenshot shows the Cisco Packet Tracer interface with the same network diagram as above. The configuration window is now open for the ISP router. The CLI text is as follows:

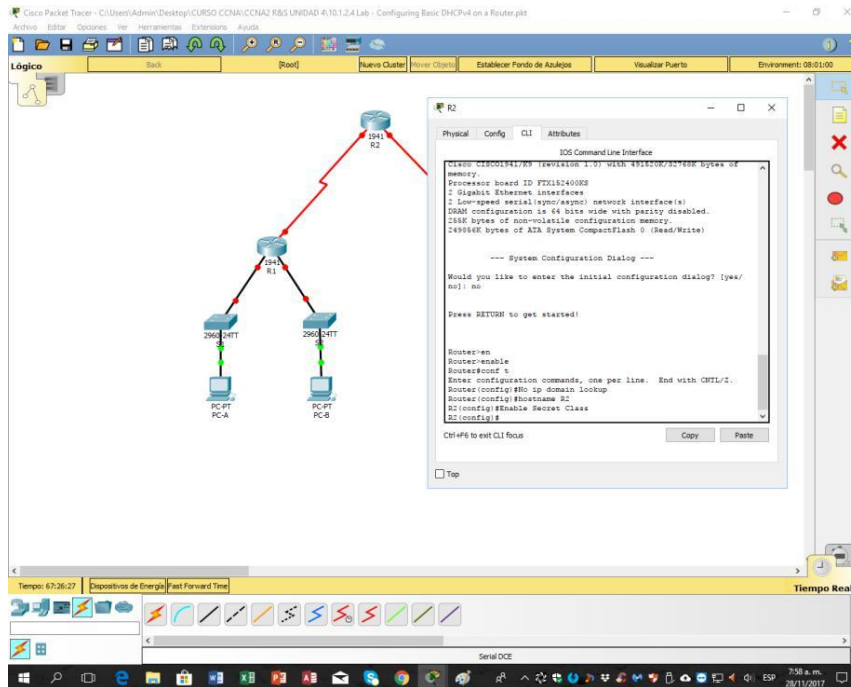
```
Router>en
Router#
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#0 ip domain lookup
Router(config)#hostname ISP
ISP(config)#
Ctrl+C to exit CLI focus
```

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

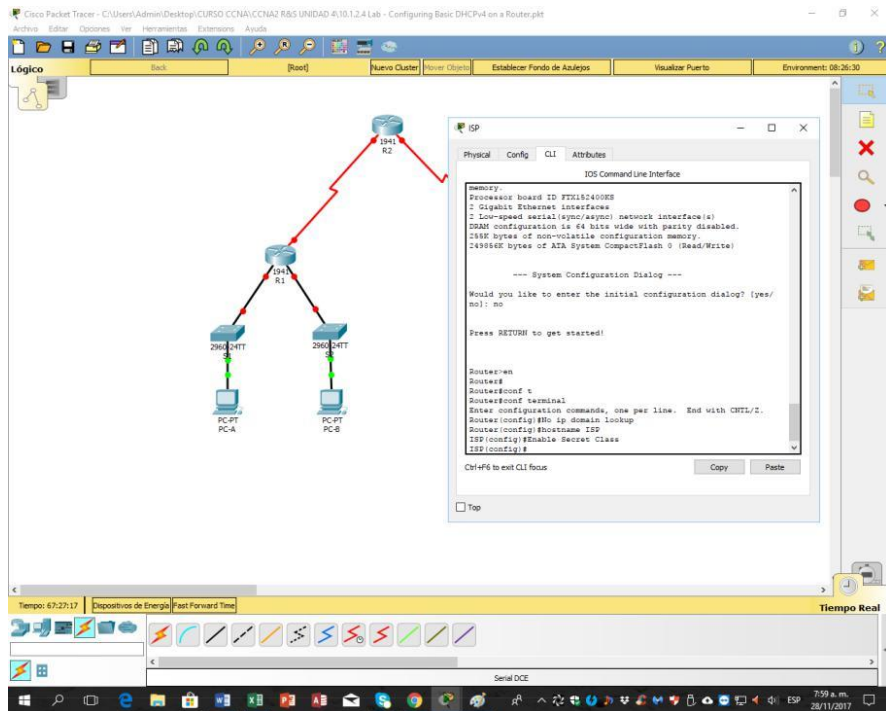
### Router 1:



### Router 2:

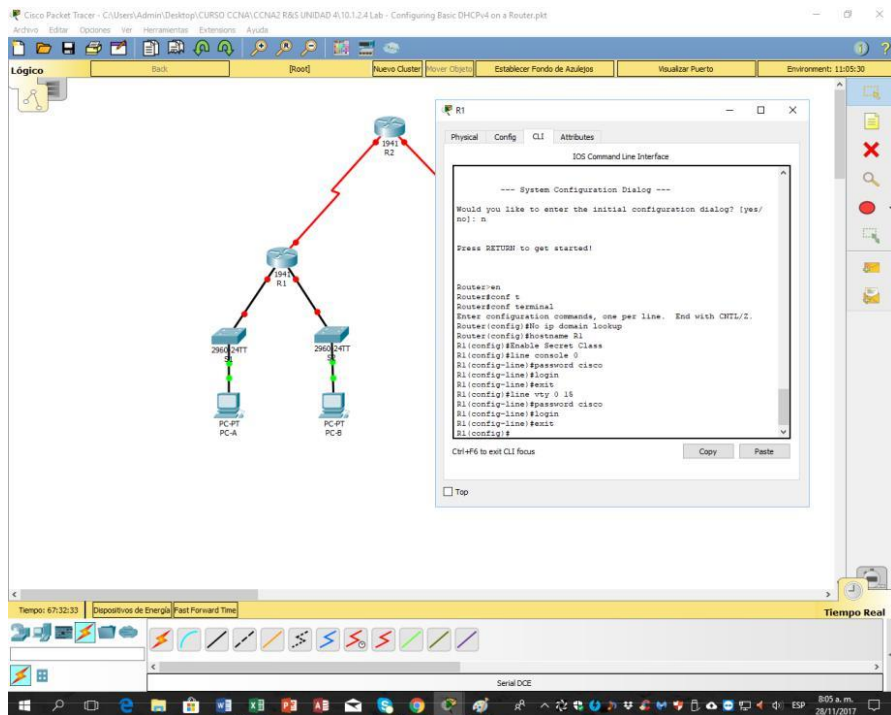


ISP:

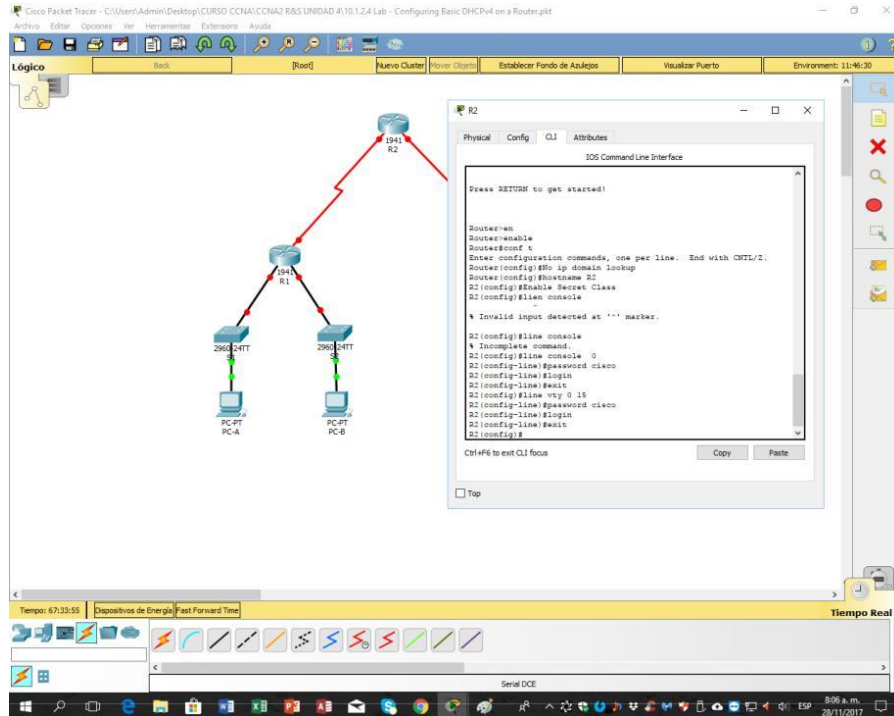


d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

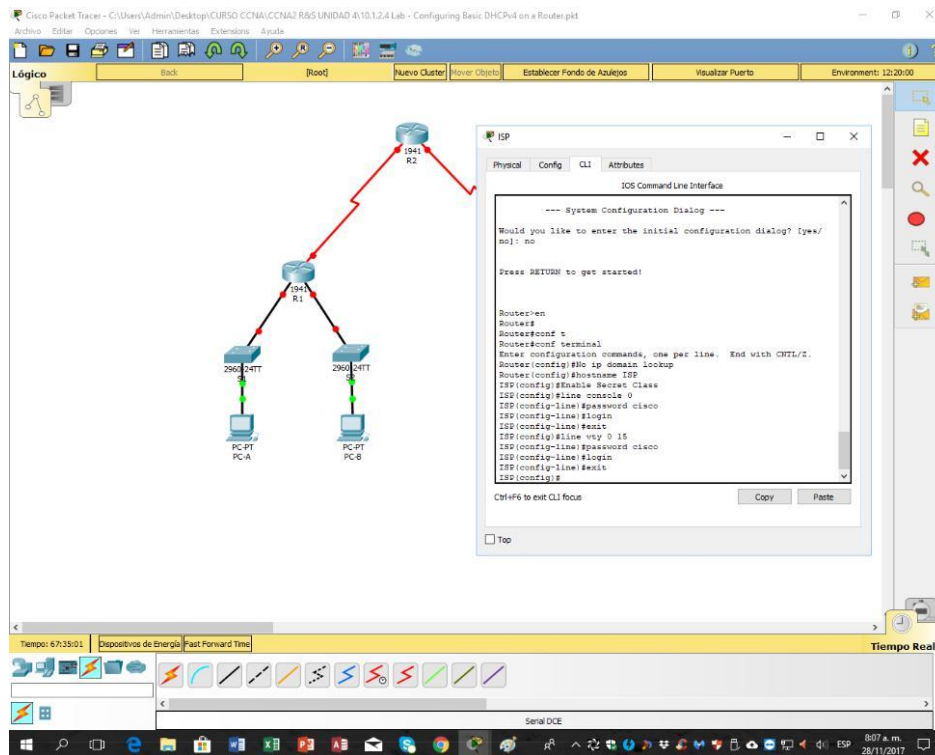
Router 1:



Router 2:

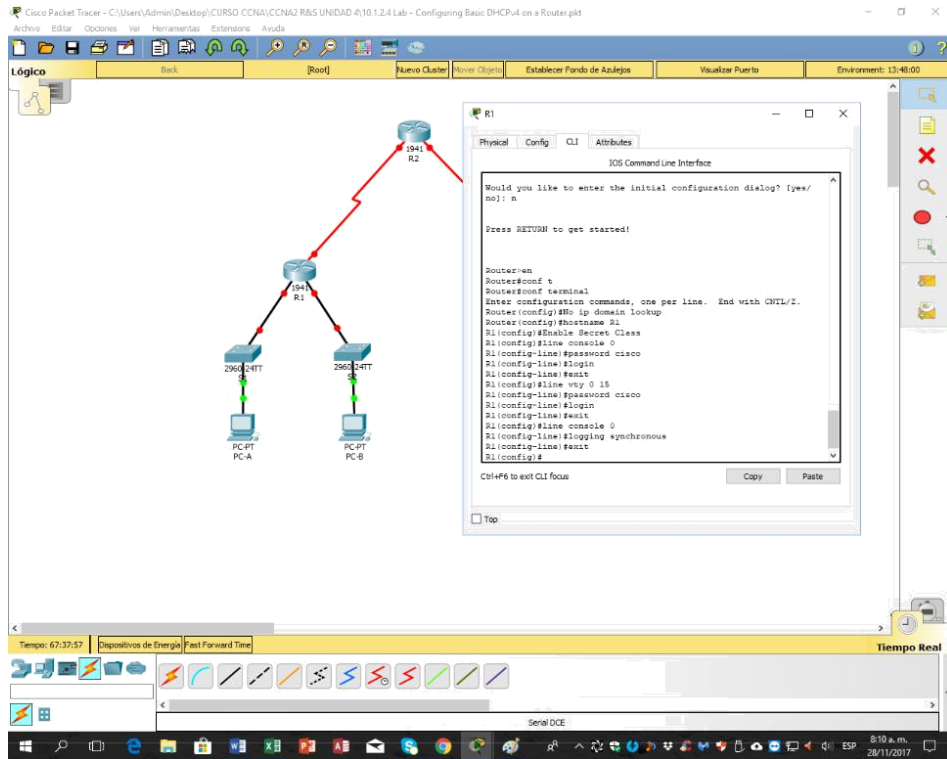


## Router IPS:



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

## Router 1:

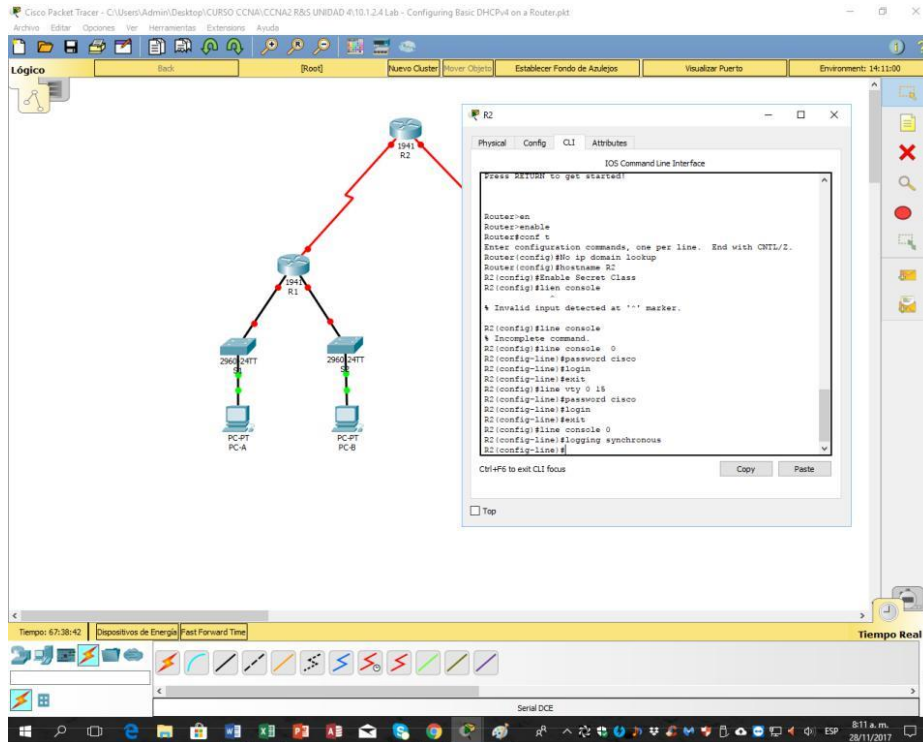


The screenshot shows the Cisco Packet Tracer interface for Router 1. The network diagram displays Router 1 (1941) connected to Router 2 (1941). Router 1 is connected to two PCs, PC-A and PC-B, via 2960-SWT switches. The CLI window for Router 1 shows the following configuration:

```
IOS Command Line Interface
Would you like to enter the initial configuration dialog? [yes/no]: n
Press RETURN to get started!

Router>en
Router#conf t
Router(config)#terminal
Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#enable secret Class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

## Router 2:

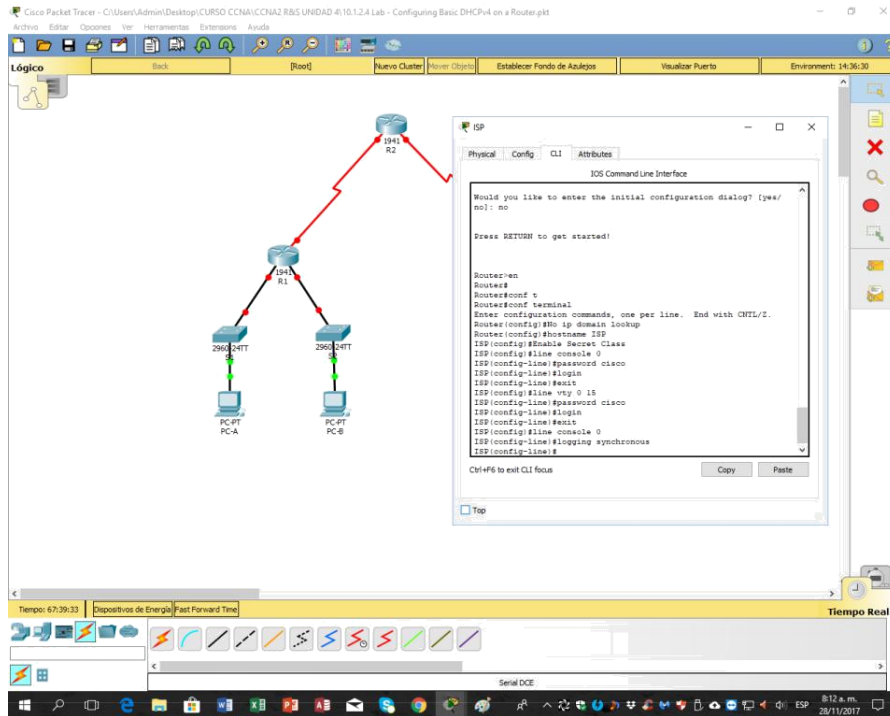


The screenshot shows the Cisco Packet Tracer interface for Router 2. The network diagram is the same as in the Router 1 screenshot. The CLI window for Router 2 shows the following configuration:

```
IOS Command Line Interface
Press RETURN to get started!

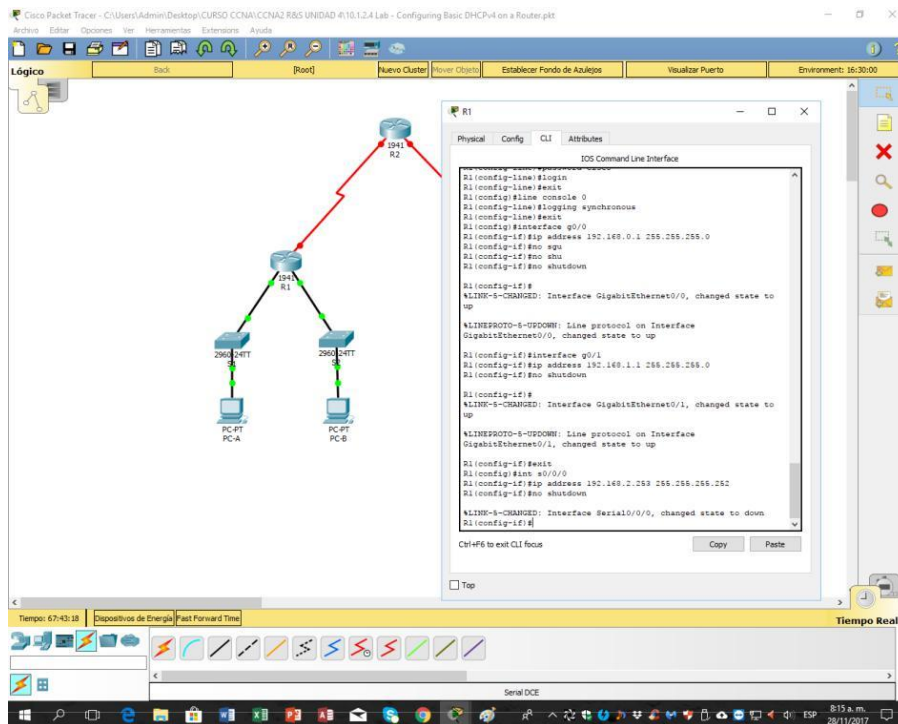
Router>en
Router#enable
Router#conf t
Router(config)#no ip domain lookup
Router(config)#hostname R2
R2(config)#enable secret Class
R2(config)#line console
R2(config-line)#
R2(config-line)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#
```

## ISP:



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

## Router 1:



## Router 2:

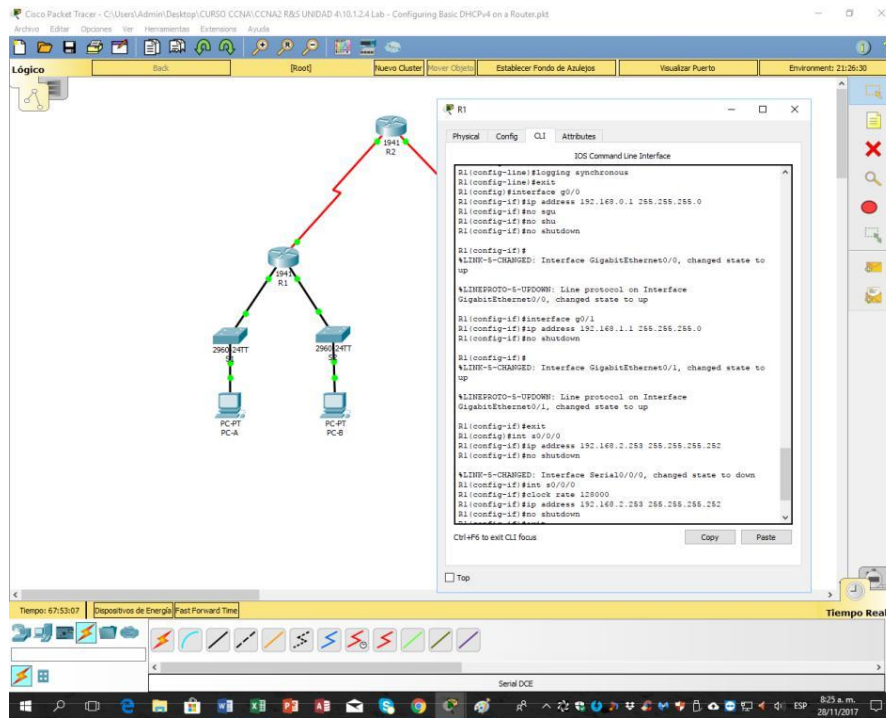
```
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#int s0/0/0
R2(config-if)#ip address 192.168.2.264 256.256.256.252
R2(config-if)#no shu
R2(config-if)#no shutdown
R2(config-if)#
%LINK-3-CHANGED: Interface Serial10/0/0, changed state to up
R2(config-if)#int s0/0/1
R2(config-if)#
%ETHERS0/0-0-UPDOWN: Line protocol on Interface Serial10/0/0,
changed state to up
R2(config-if)#clock rate 120000
R2(config-if)#ip address 209.168.200.224 256.256.256.224
R2(config-if)#no sh
R2(config-if)#no shutdown
R2(config-if)#
%DNR-1-CHANGED: Interface Serial10/0/1, changed state to down
R2(config-if)#
```

## ISP:

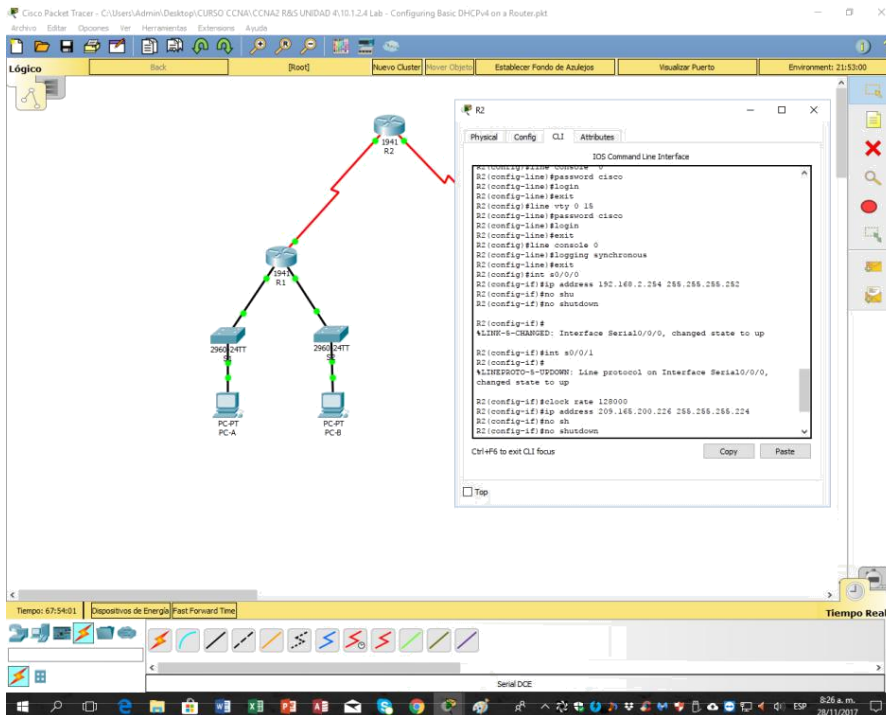
```
User Access Verification
Password:
ISP-en
ISP-enable
Password:
ISPconf t
ISPconf terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/1
ISP(config-if)#ip address 209.168.200.228 256.256.256.224
ISP(config-if)#no shu
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-3-CHANGED: Interface Serial10/0/1, changed state to up
ISP(config-if)#
```

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

### Router 1:

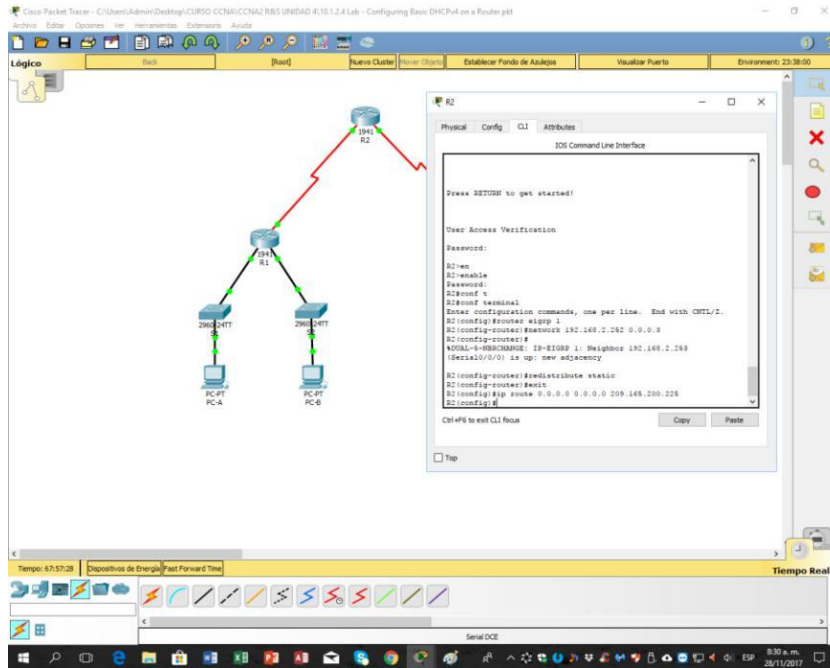


### Router 2:



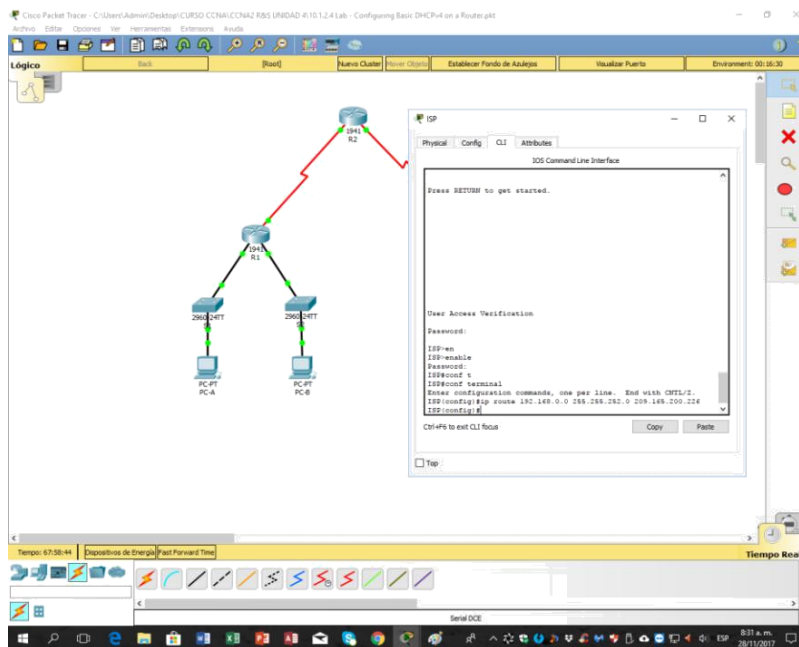






- j. Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.

```
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

### Router 1:

The screenshot shows the Cisco Packet Tracer interface with Router 1 selected. The network diagram on the left shows Router 1 (1941) connected to Router 2 (1941) via a serial link. Router 1 is also connected to two PCs (PC-A and PC-B) via Ethernet switches (2960-24TT). The CLI window on the right displays the following configuration:

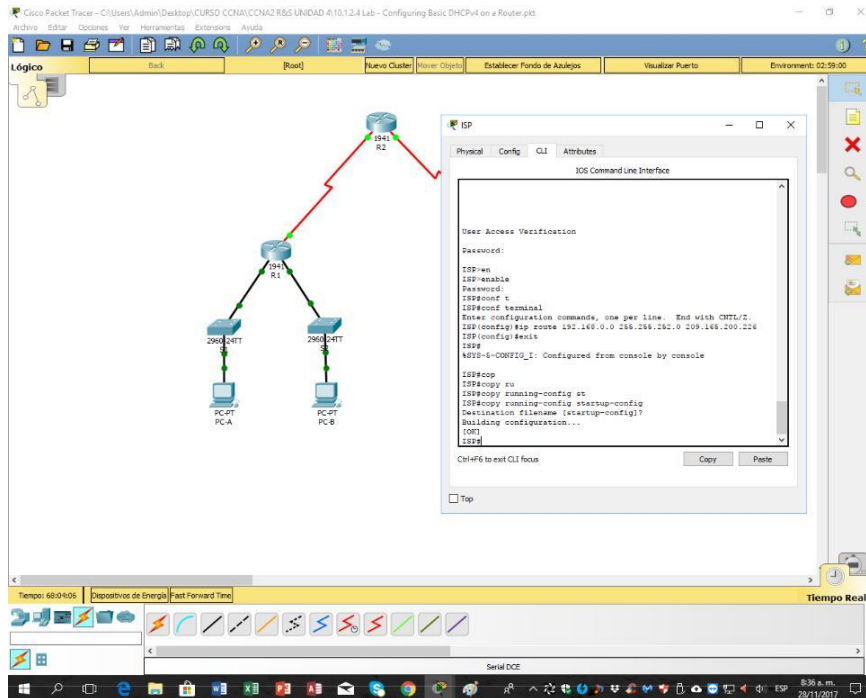
```
IOS Command Line Interface
User Access Verification
Password:
R1#enable
R1#configure terminal
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.169.1.0 0.0.0.255
R1(config-router)#network 192.169.2.252 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#
R1#show ip-rib-summary: IP-EGRP 1: Neighbor 192.169.2.254
(Serial0/0/0) is up: new adjacency
R1(config-router)#exit
R1#show ip route
R1#copy
R1#copy running-config *
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

### Router 2:

The screenshot shows the Cisco Packet Tracer interface with Router 2 selected. The network diagram on the left is identical to the Router 1 screenshot. The CLI window on the right displays the following configuration:

```
IOS Command Line Interface
R2#enable
R2#configure terminal
R2(config)#router eigrp 1
R2(config-router)#network 192.169.2.252 0.0.0.3
R2(config-router)#
R2#show ip-rib-summary: IP-EGRP 1: Neighbor 192.169.2.253
(Serial0/0/0) is up: new adjacency
R2(config-router)#redistribute static
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
R2(config)#exit
R2#
R2#show ip-rib-summary: Configured from console by console
R2#copy
R2#copy running-config *
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

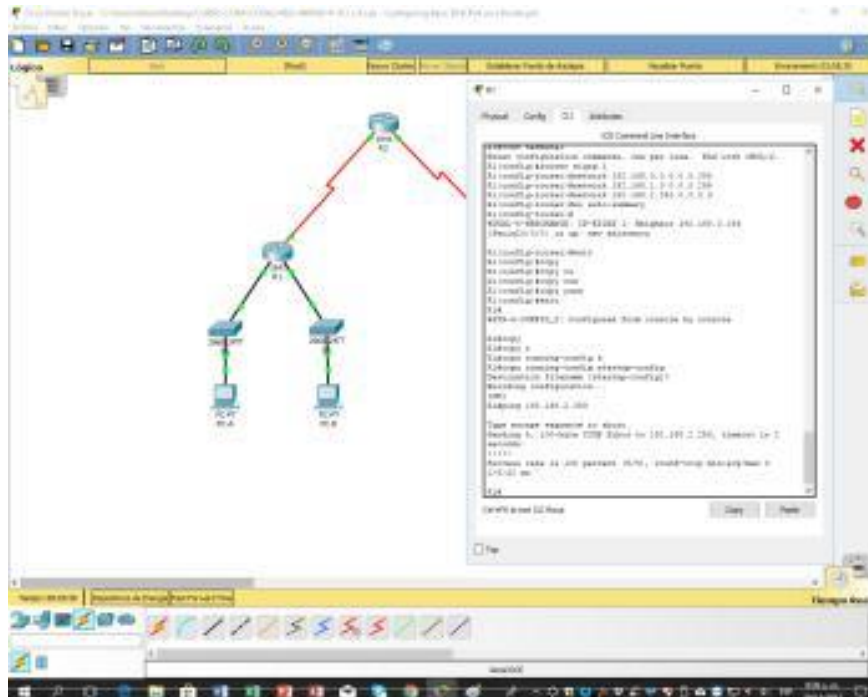
## ISP:



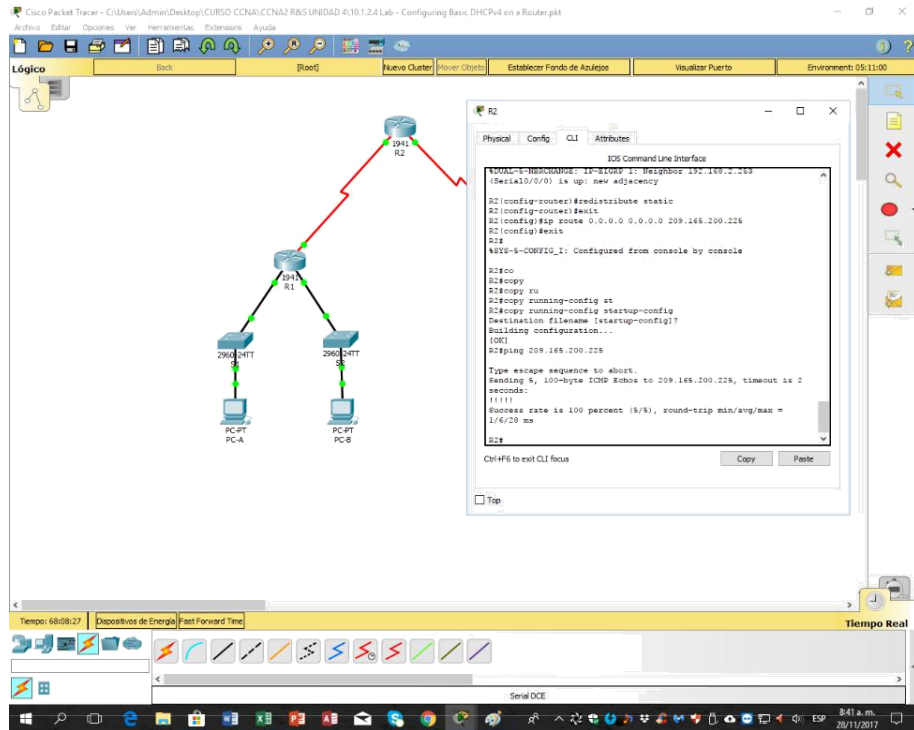
### Paso 4. verificar la conectividad de red entre los routers.

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.

### Ping de R1 a R2:

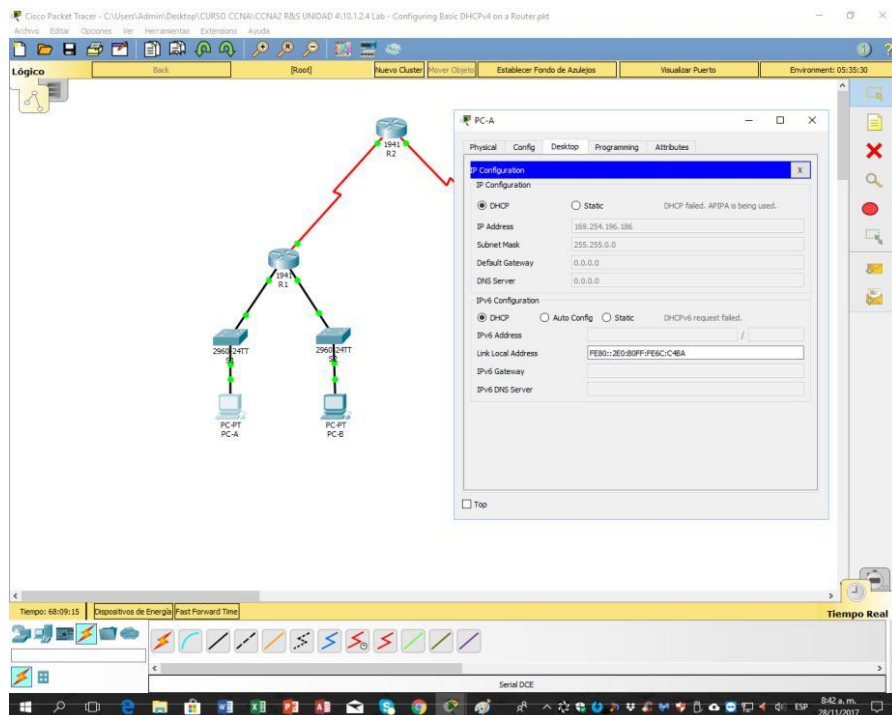


## Ping de R2 a ISP:

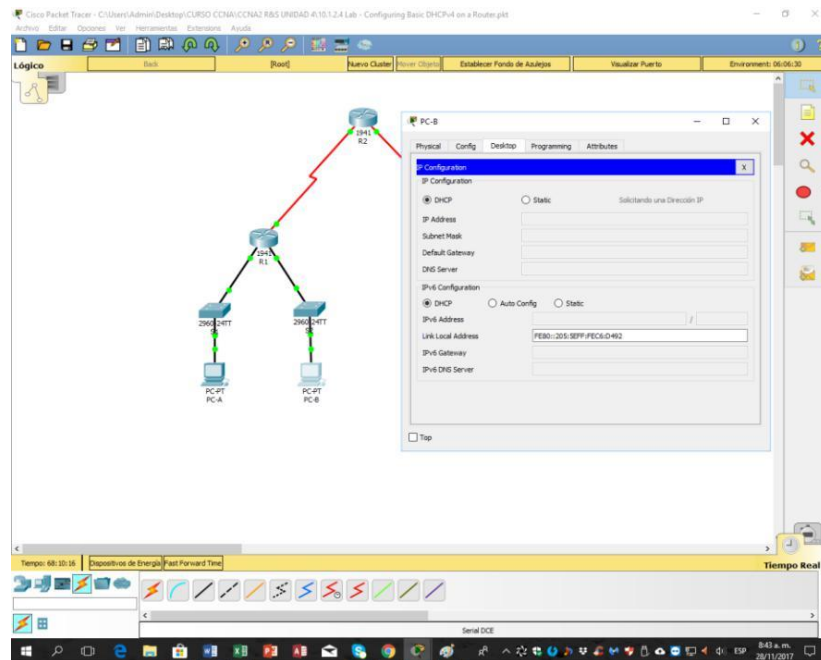


**Paso 5.** verificar que los equipos host estén configurados para DHCP.

**PC-A:**



## PC-B:



## Parte 8. 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.

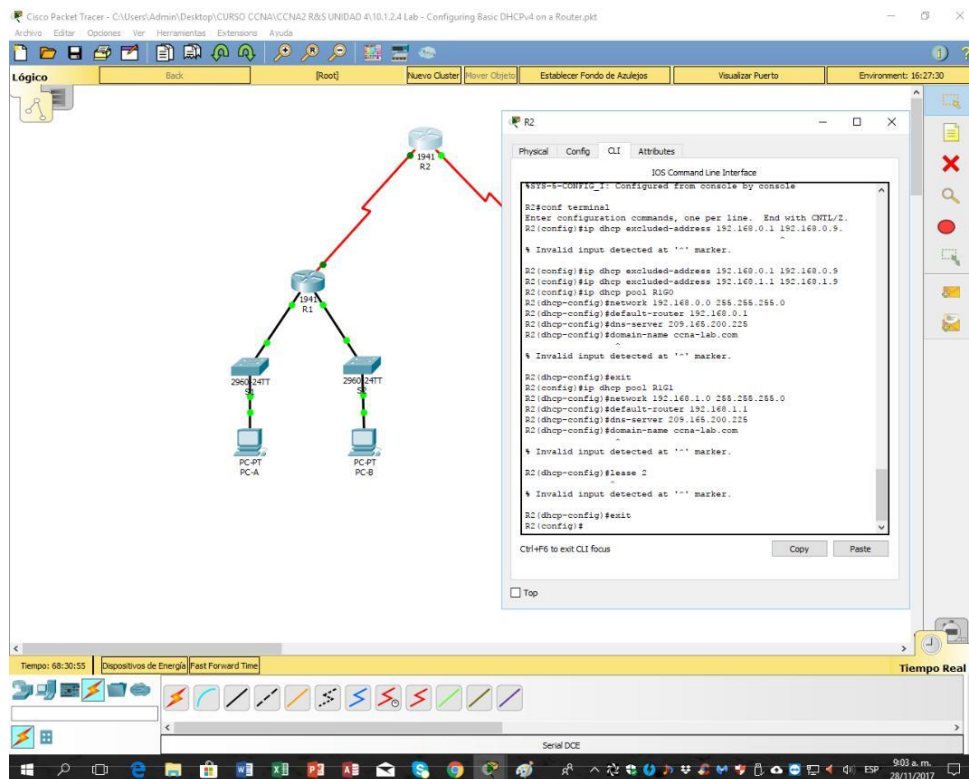
En el R2, configure un conjunto de direcciones DHCP para cada LAN del R1. Utilice el nombre de conjunto **R1G0** para G0/0 LAN y **R1G1** para G0/1 LAN. Asimismo, configure las direcciones que se excluirán de los conjuntos de direcciones. La práctica recomendada indica que primero se deben configurar 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.

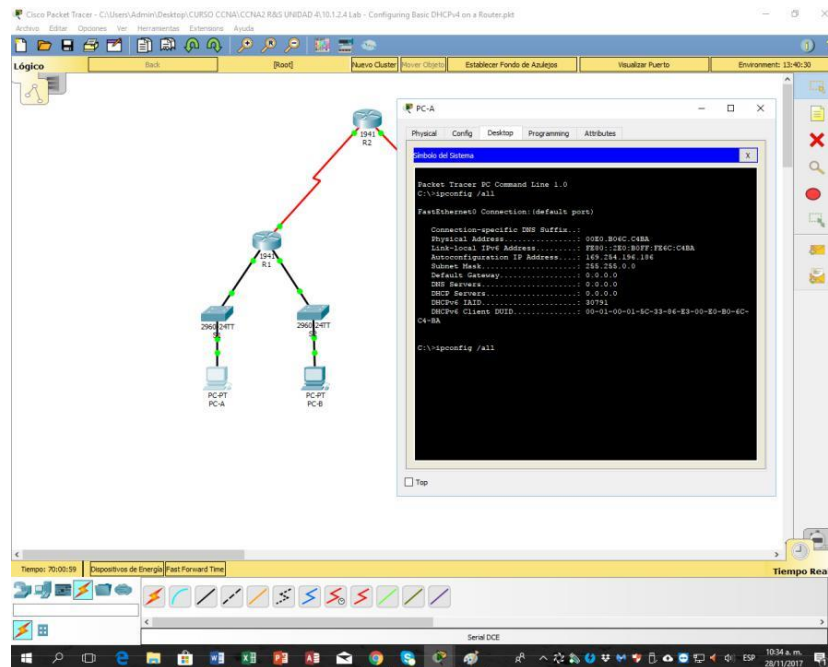
- **ip dhcp excluded-address**
- **ip dhcp pool**
- **network**
- **default-router**
- **dns-server**
- **domain-name**
- **lease**



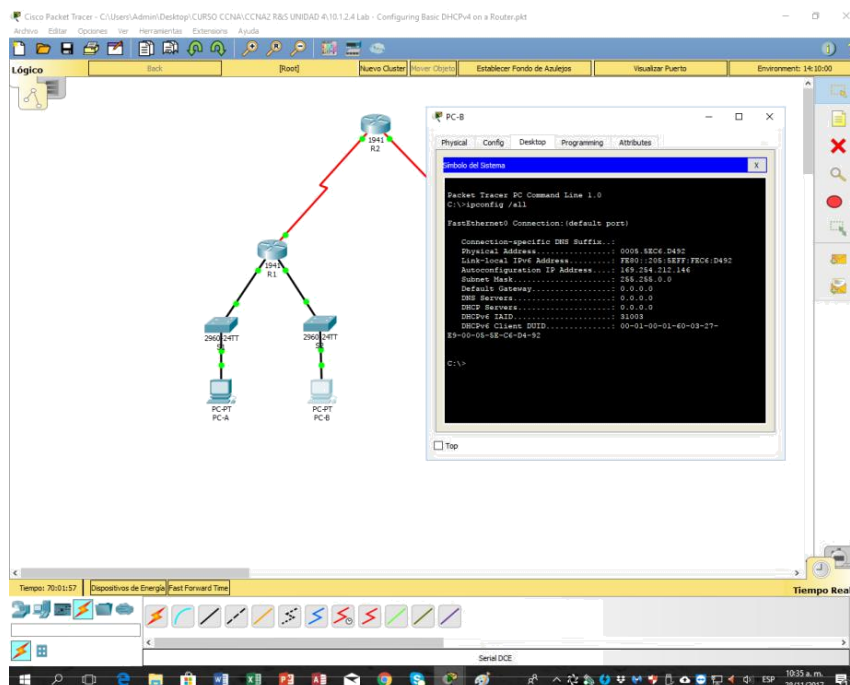
En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando **ipconfig /all**.  
¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué?

**Las PC no han recibido las direcciones IP desde el servidor DHCP en R2 puesto que en R1 sea configurado como un agente relay DHCP.**

**PC-A:**



**PC-B:**



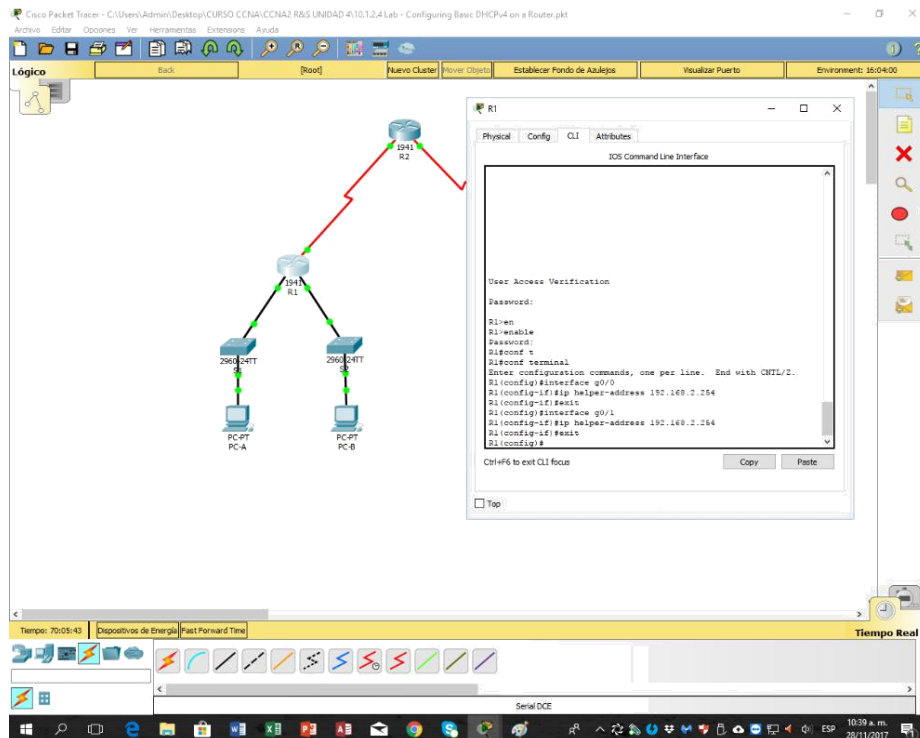


## Paso 2. configurar el R1 como agente de retransmisión DHCP.

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

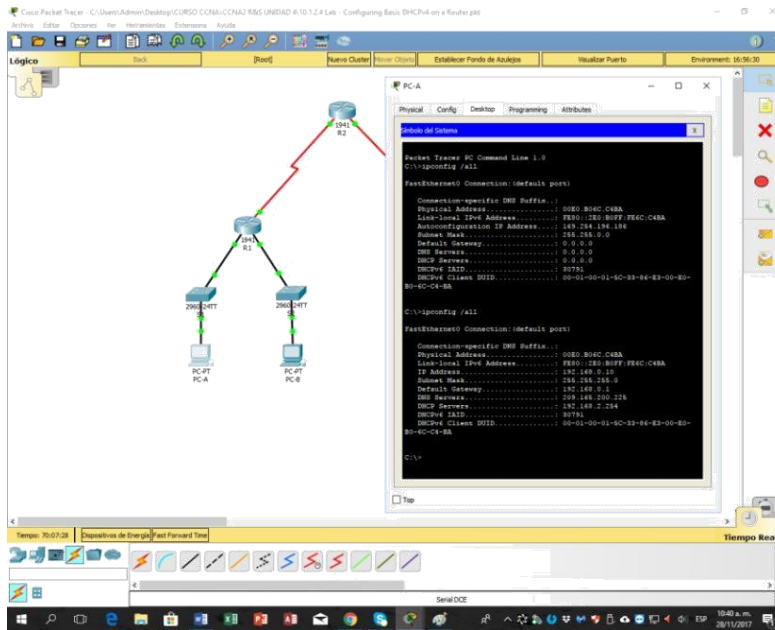
En las líneas a continuación, escriba los comandos necesarios para configurar el R1 como agente de retransmisión DHCP para las LAN del R1.

### - ip helper-address



## 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.

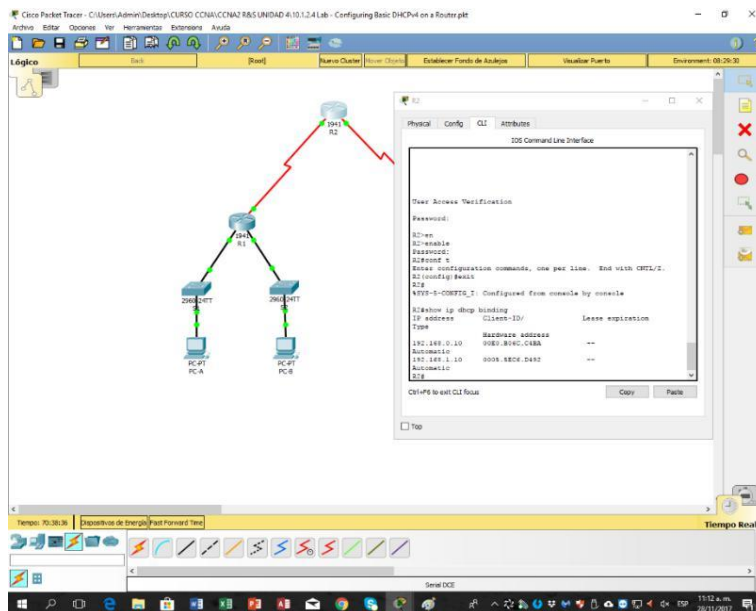


Según el pool de DHCP que se configuró en el R2, ¿cuáles son las primeras direcciones IP disponibles que la PC-A y la PC-B pueden arrendar?

**En PC-A: 192.168.0.10 y en PC-B: 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.



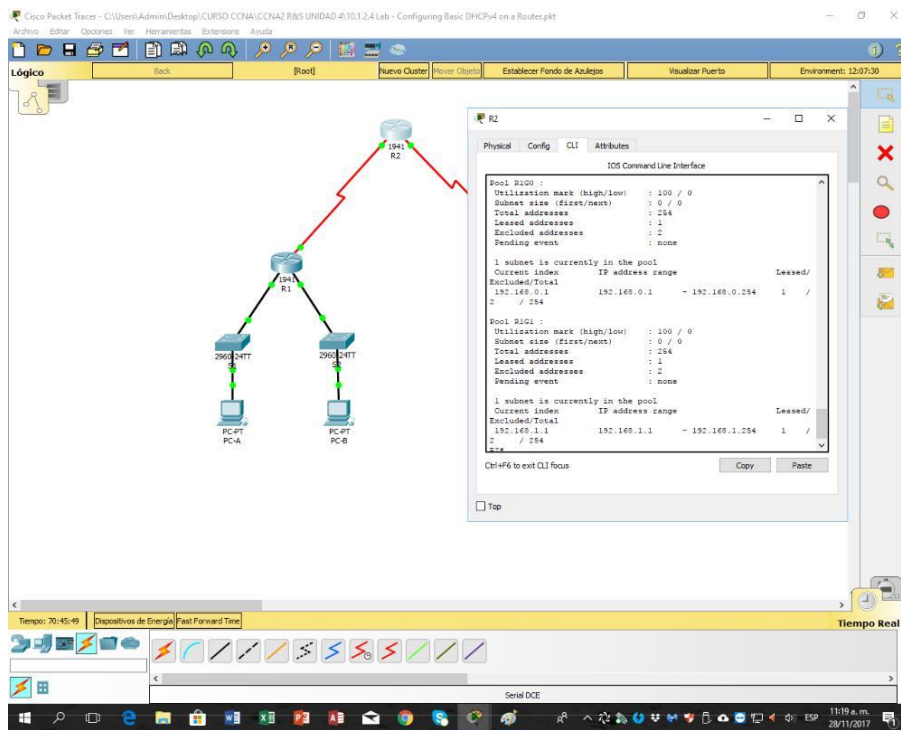
Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado?

### Las Direcciones MAC de los Puertos.

- 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?

- 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)?

### Es la Siguiente Dirección IP disponible para ser Arrendada.

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



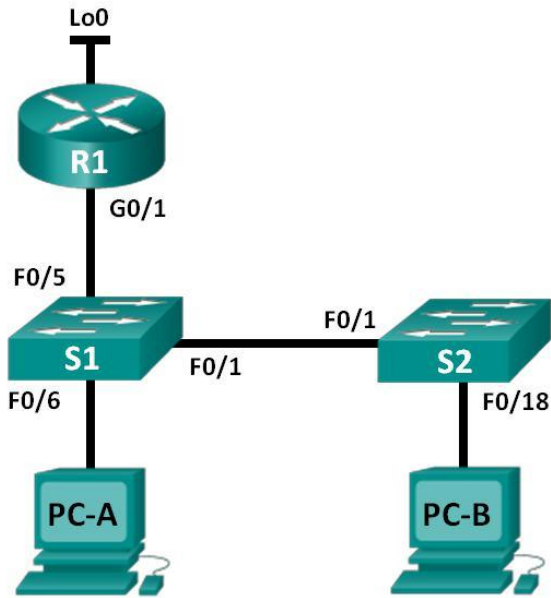
**Tabla de resumen de interfaces del router**

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

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

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

#### Topología



### Tabla de direccionamiento

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

### Objetivos

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

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

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

**Parte 3: configurar DHCPv4**

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

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

Asignar puertos a la VLAN 2.

Configurar DHCPv4 para la VLAN 2.

Verificar la conectividad y DHCPv4.

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

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

#### **Información básica/situación**

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

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

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

laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

### **Recursos necesarios**

1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet, como se muestra en la topología

### **Parte 9: armar la red y configurar los parámetros básicos de los dispositivos**

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

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

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

- a. Asigne los nombres de dispositivos como se muestra en la topología.
- b. Desactive la búsqueda del DNS.
- c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
- d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.
- e. Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.
- f. Guarde la configuración en ejecución en el archivo de configuración de inicio.

### **Parte 10: cambiar la preferencia de SDM**

Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch Cisco 2960. Las plantillas pueden habilitarse para admitir funciones específicas según el modo en



que se utilice el switch en la red. En esta práctica de laboratorio, la plantilla lanbase-routing está habilitada para permitir que el switch realice el routing entre VLAN y admita el routing estático.

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

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

```
S1# show sdm prefer
```

```
The current template is "default" template.
```

```
The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.
```

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

### **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:	
number of IPv6 security aces:	

## Parte 11: configurar DHCPv4

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

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

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

```
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

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

```
S1(config)#ip dhcp pool DHCP1
```

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

```
S1(dhcp-config)#NETWORK 192.168.1.0 255.255.255.0
```

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

```
S1(dhcp-config)#default-router 192.168.1.1
```

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

```
S1(dhcp-config)#dns-server 192.168.1.9
```

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

```
S1(dhcp-config)#lease 3
```

- 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: 192.168.1.11 Máscara

de subred: 255.255.255.0 Gateway

predeterminado: 192.168.1.1 Para la

PC-B, incluya lo siguiente: Dirección

IP: 192.168.1.12 Máscara de subred:

255.255.255.0

Gateway predeterminado: 192.168.1.1

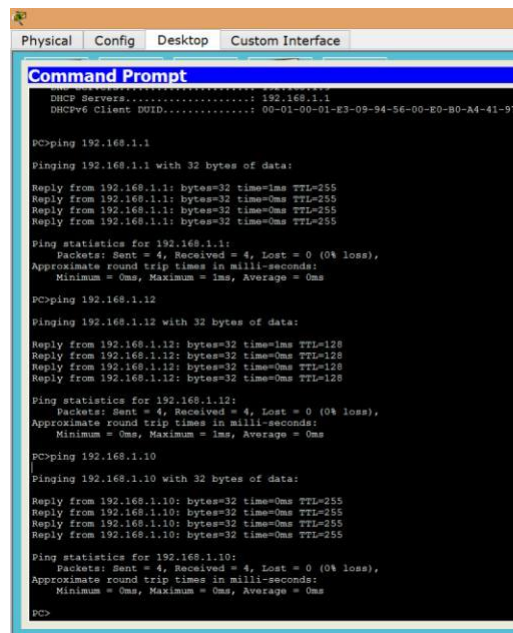
- b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

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

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

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

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



```
Physical Config Desktop Custom Interface
Command Prompt
DHCP Servers.....: 192.168.1.1
DHCPv6 Client DUID.....: 00-01-00-01-E3-09-94-56-00-E0-B0-A4-41-97

PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

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

PC>ping 192.168.1.12
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=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms 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 = 0ms, Average = 0ms

PC>
```

## Parte 12: configurar DHCPv4 para varias VLAN

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

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

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

```
S1(config)#int f0/6
```

```
S1(config-if)#switchport mode access
```

```
S1(config-if)#switchport access vlan 2
```

```
S1(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
```

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

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

```
S1(config-if)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
```

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

```
S1(config)#ip dhcp pool DHCP2
```

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

```
S1(dhcp-config)#network 192.168.2.0 255.255.255.0
```

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

```
S1(dhcp-config)#default-router 192.168.2.1
```

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

S1(dhcp-config)#dns-server 192.168.2.9

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

S1(dhcp-config)#lease 3

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

### Paso 3: verificar la conectividad y DHCPv4.

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

Para la PC-A, incluya lo siguiente:  
Dirección IP: 192.168.2.11 Máscara de subred: 255.255.255.0 Gateway predeterminado: 192.168.2.1

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

¿Es posible hacer ping de la PC-A al gateway predeterminado? SI ¿Es posible hacer ping de la PC-A a la PC-B? NO

¿Los pings eran correctos? ¿Por qué? No, porque no se ha aplicado un ruteo

- c. Emita el comando **show ip route** en el S1.  
¿Qué resultado arrojó este comando? S1#show ip route

Default gateway is not set

Host	Gateway	Last Use	Total Uses	Interface
------	---------	----------	------------	-----------

ICMP redirect cache is empty

### Parte 13: habilitar el routing IP

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

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

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

S1(config)# **ip routing**

- b. Verificar la conectividad entre las VLAN.

¿Es posible hacer ping de la PC-A a la PC-B? SI ¿Qué función realiza el switch?

Realiza una función como router

- c. Vea la información de la tabla de routing para el S1.

¿Qué información de la ruta está incluida en el resultado de este comando?  
Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, Vlan1 C  
192.168.2.0/24 is directly connected, Vlan2

- d. Vea la información de la tabla de routing para el R1.

¿Qué información de la ruta está incluida en el resultado de este comando?  
Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C192.168.1.0/24 is directly connected, GigabitEthernet0/1

L192.168.1.10/32 is directly connected, GigabitEthernet0/1  
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C209.165.200.224/27 is directly connected, Loopback0

L209.165.200.225/32 is directly connected, Loopback0

- e. ¿Es posible hacer ping de la PC-A al R1? NO

¿Es posible hacer ping de la PC-A a la interfaz Lo0? SI

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Se deben establecer rutas estáticas.

## 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.

```
S1(config)#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.

```
R1(config)#ip route 192.168.2.0 255.255.255.0 g0/1
```

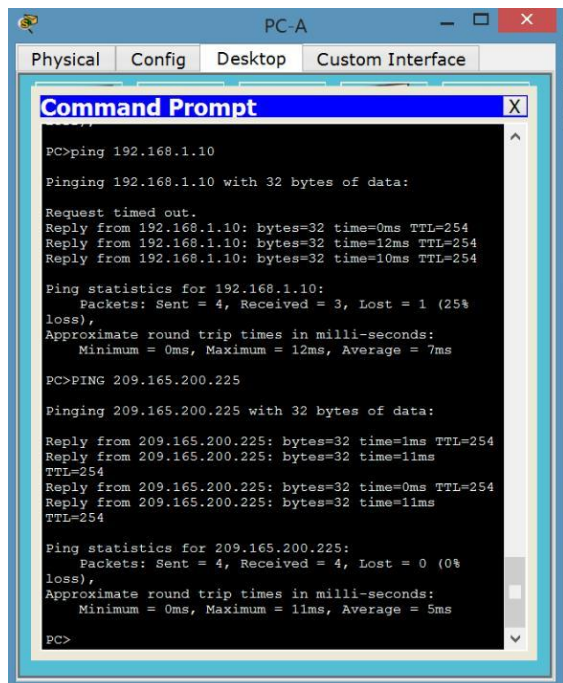
- c. Vea la información de la tabla de routing para el S1. ¿Cómo está representada la ruta estática predeterminada? S\* 0.0.0.0/0 [1/0] via 192.168.1.10

- d. Vea la información de la tabla de routing para el R1. ¿Cómo está representada la ruta estática?

```
S 192.168.2.0/24 is directly connected, GigabitEthernet0/1
```

- e. ¿Es posible hacer ping de la PC-A al R1? SI

¿Es posible hacer ping de la PC-A a la interfaz Lo0? SI



```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=12ms TTL=254
Reply from 192.168.1.10: bytes=32 time=10ms TTL=254
Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25%
    loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 7ms
PC>PING 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=11ms
TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=11ms
TTL=254
Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
    loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms
PC>
```



## Reflexión

1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

Porque si le damos las direcciones que ya hemos usado, va a haber un conflicto de IPs

2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

Se asignan puertos predeterminados para la VLAN 1 y para la VLAN 2.

3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960? Realiza funciones de CAPA 3

## Tabla de resumen de interfaces del router

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

**Nota:** para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de

todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

## **Apéndice A: comandos de configuración**

### **Configurar DHCPv4**

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

```
S1(config)# ip dhcp pool DHCP1 S1(dhcp-config)# network  
192.168.1.0 255.255.255.0 S1(dhcp-config)# default-router  
192.168.1.1 S1(dhcp-config)# dns-server 192.168.1.9 S1(dhcp-  
config)# lease 3
```

### **Configurar DHCPv4 para varias VLAN**

```
S1(config)# interface f0/6 S1(config-if)# switchport  
access vlan 2
```

```
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
```

```
S1(config)# ip dhcp pool DHCP2
```

```
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
```

```
S1(dhcp-config)# default-router 192.168.2.1
```

```
S1(dhcp-config)# dns-server 192.168.2.9
```

```
S1(dhcp-config)# lease 3
```

## Habilitar routing IP

```
S1(config)# ip routing
```

```
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10 R1(config)# ip route  
192.168.2.0 255.255.255.0 g0/1
```

### 10.3.1.1 IoE and DHCP Instructions

#### IdT y DHCP

##### Objetivo

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

##### Situación

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

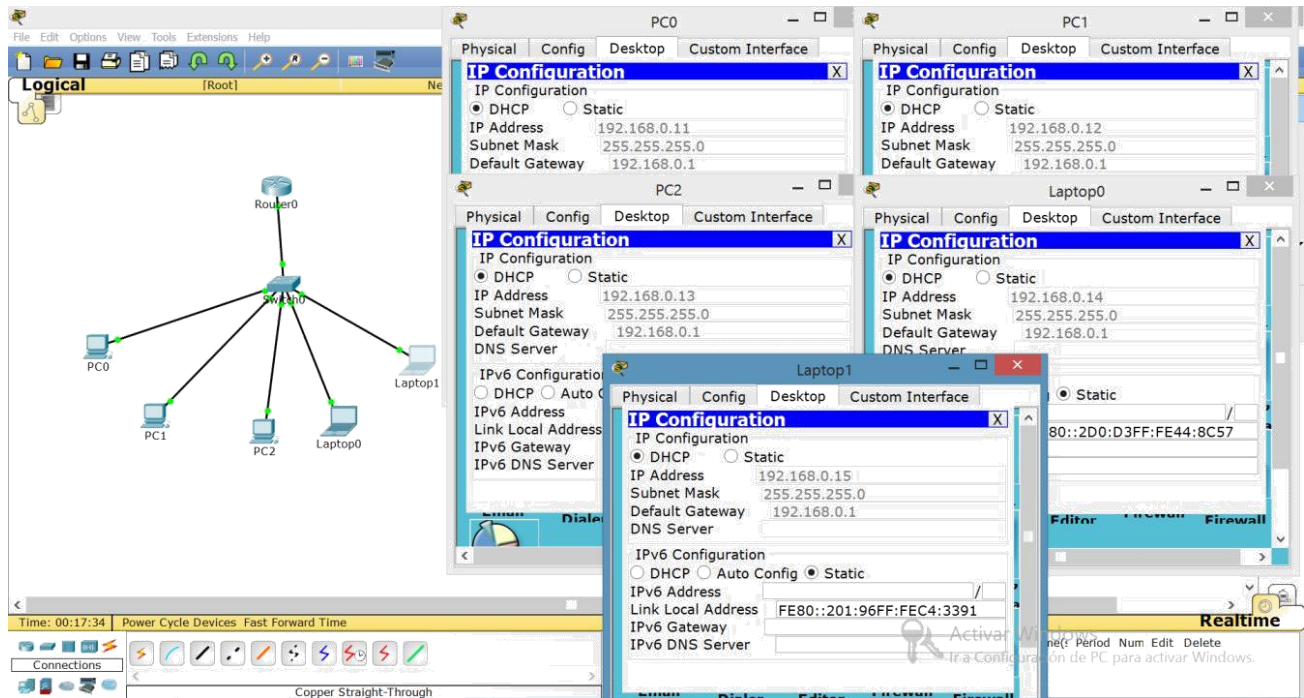
Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

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

Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.

Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones DHCP del servidor de DHCP.

Muestre los resultados que validen que cada terminal garantiza una dirección IP del servidor. Utilice un programa de captura de pantalla para guardar la información del resultado o emplee el comando de la tecla **ImprPant**.



Presente sus conclusiones a un compañero de clase o a la clase.

## Recursos necesarios

Software de Packet Tracer

## 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?

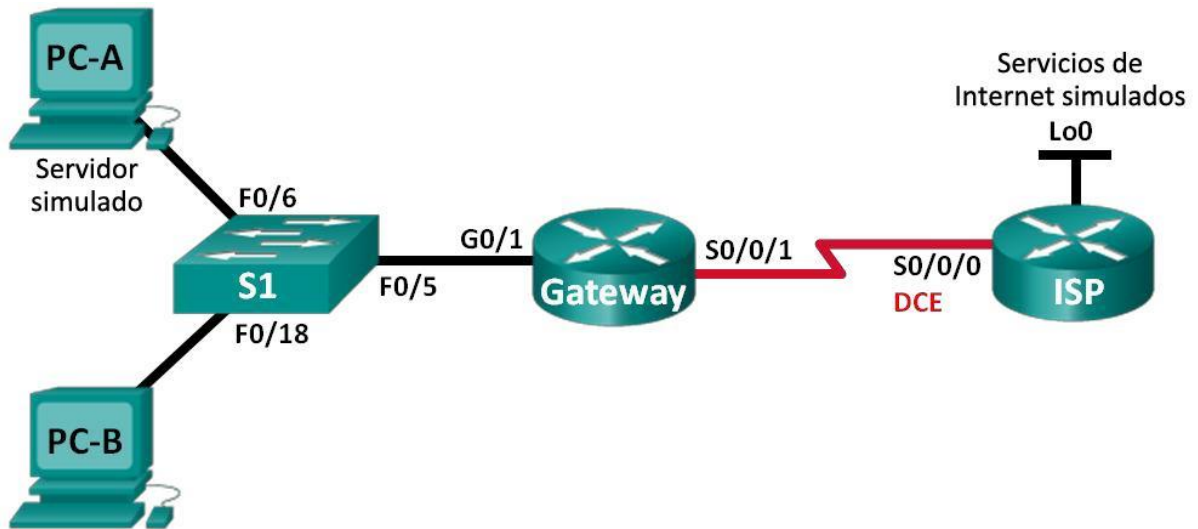
Un router 1941 permite que se tenga mayor seguridad a diferencia de los que puede tener un ISR. Para el caso del ejercicio se podría implementar, pero se tendría menor rendimiento en las actividades del mismo teniendo en cuenta también que la seguridad disminuiría.

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.

- En una empresa de vigilancia se podría controlar el sistema CCTV.
- Se pueden identificar intermitencias de comunicaciones en una empresa de realce de tarjetas plásticas.
- Controlar un PLC mediante un direccionamiento IP.

### 11.2.2.6 Lab - Configuring Dynamic and Static NAT

## Topología



## Tabla de direccionamiento

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

## Objetivos

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

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

## **Parte 3: configurar y verificar la NAT dinámica**

### **Información básica/situación**

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

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

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

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

## Recursos necesarios

2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

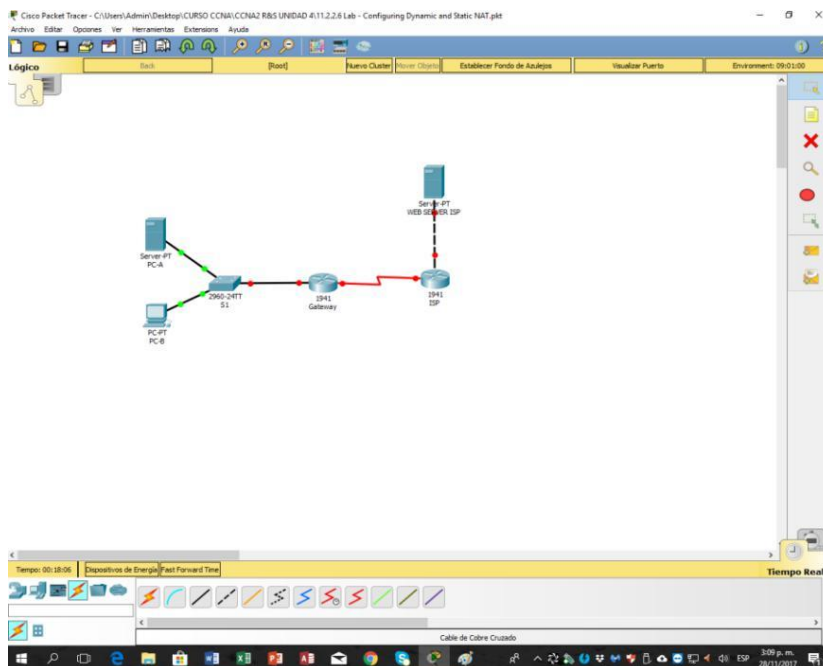
Cables Ethernet y seriales, como se muestra en la topología

## Parte 14. 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.

PC-A:

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a topology with a 2960-24TT S1 switch connected to a PC-PT PC-A and a PC-PT PC-B. The switch is connected to a 1941 Gateway, which is in turn connected to a 1941 ISP. A Server-PT WEB SERVER ISP is also connected to the ISP. The main window shows the configuration for PC-A. The IP Configuration tab is active, with the following settings:

- IP Configuration:  Static
- IP Address: 192.168.1.20
- Subnet Mask: 255.255.255.0
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0

The IPv6 Configuration section is also visible, with the following settings:

- IPv6 Configuration:  Static
- IPv6 Address: [Empty field]
- Link Local Address: FE80::260:3CFF:FE4A:D91B
- IPv6 Gateway: [Empty field]
- IPv6 DNS Server: [Empty field]

The status bar at the bottom indicates the time is 00:20:44 and the environment is 10:20:00.

PC-B:

The screenshot displays the Cisco Packet Tracer interface, showing the same network topology as the previous image. The main window shows the configuration for PC-B. The IP Configuration tab is active, with the following settings:

- IP Configuration:  Static
- IP Address: 192.168.1.21
- Subnet Mask: 255.255.255.0
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0

The IPv6 Configuration section is also visible, with the following settings:

- IPv6 Configuration:  Static
- IPv6 Address: [Empty field]
- Link Local Address: FE80::2D0:BCFF:FEB9:2813
- IPv6 Gateway: [Empty field]
- IPv6 DNS Server: [Empty field]

The status bar at the bottom indicates the time is 00:20:06 and the environment is 10:01:00.

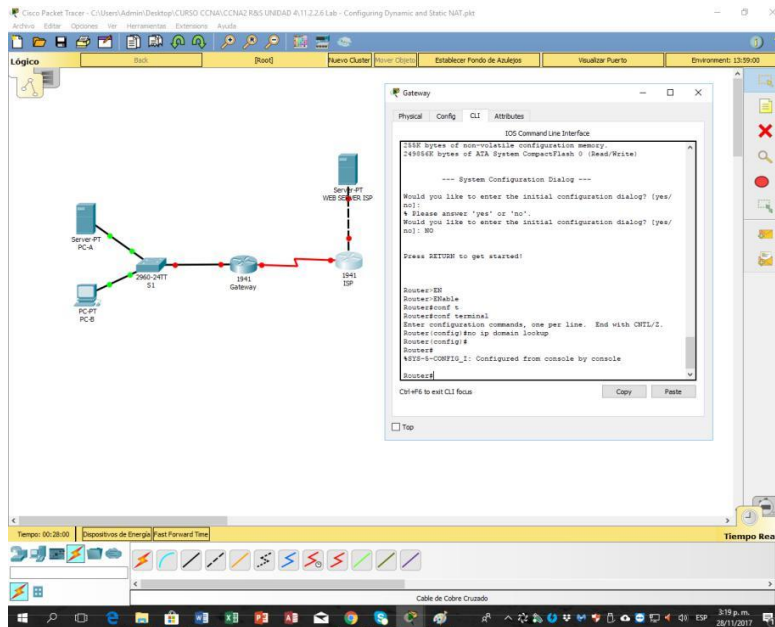


**Paso 3. inicializar y volver a cargar los routers y los switches según sea necesario.**

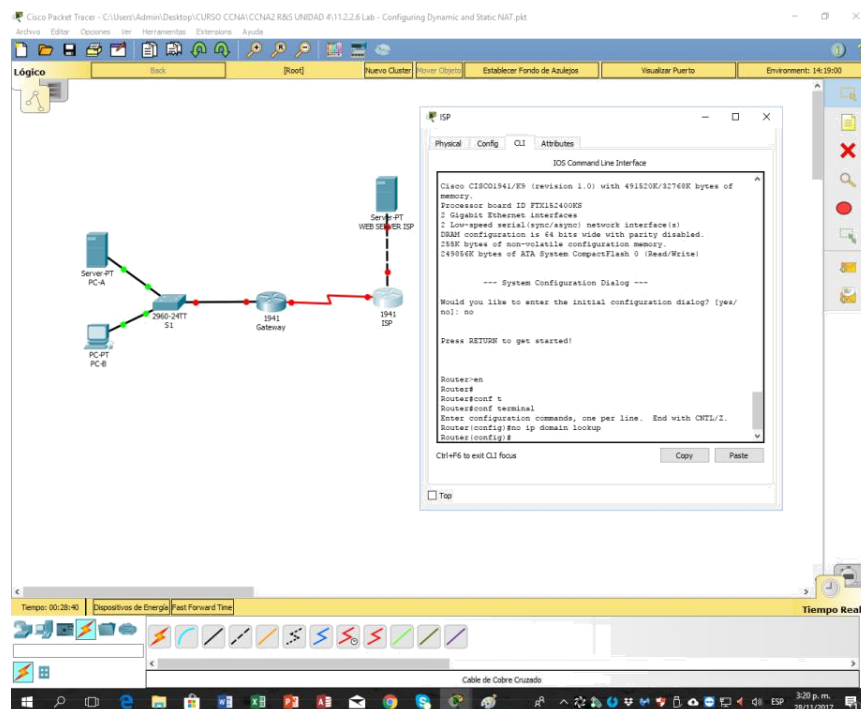
**Paso 4. configurar los parámetros básicos para cada router.**

a. Desactive la búsqueda del DNS.

**Gateway:**



**ISP:**

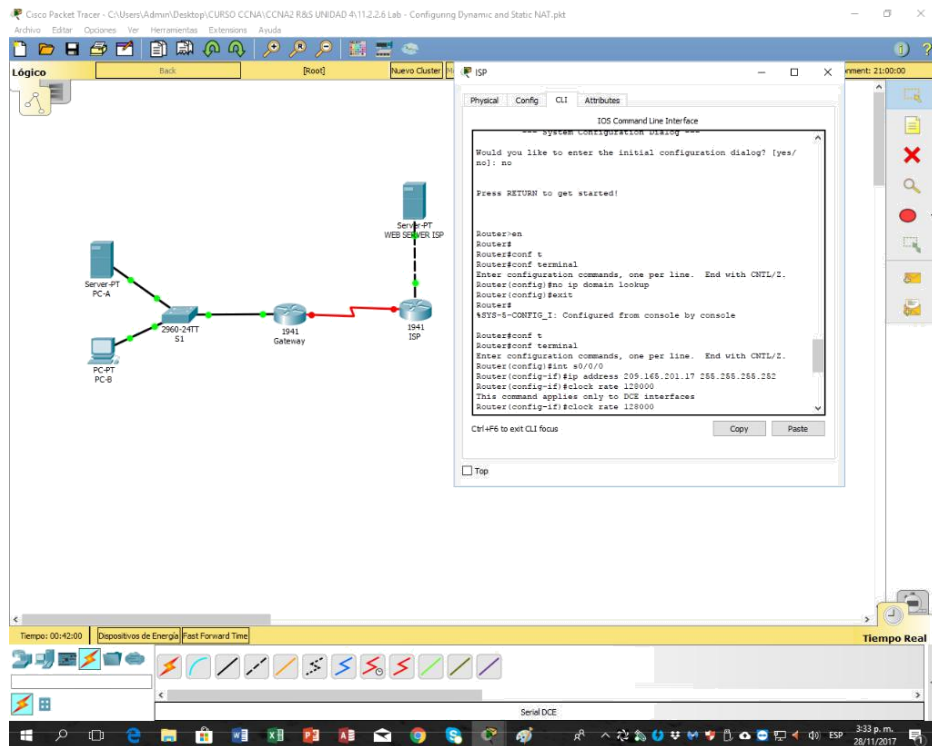


- b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

### Gateway:

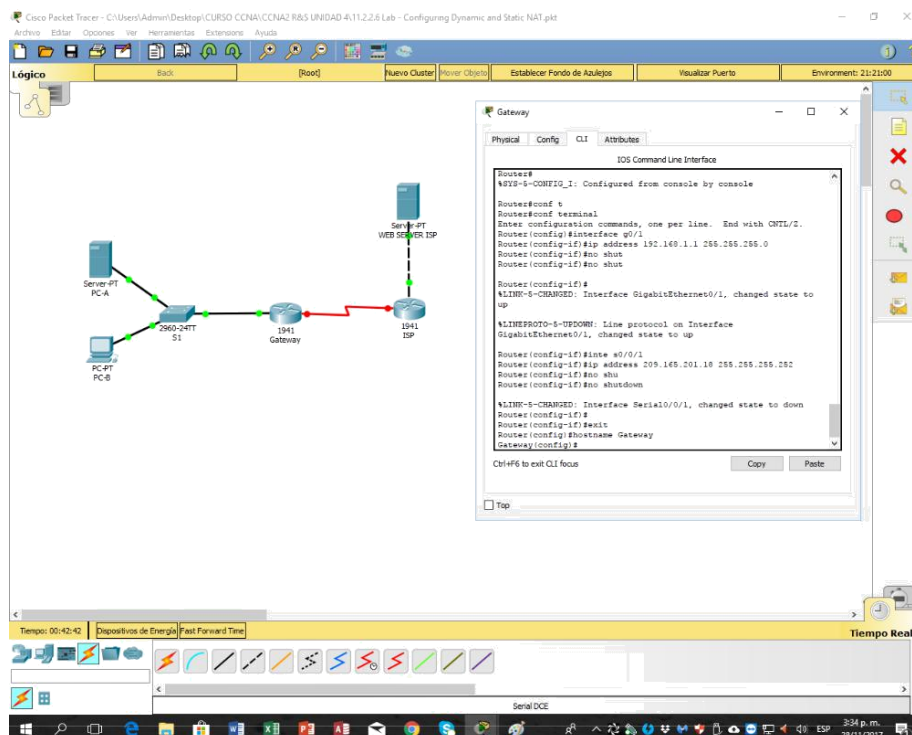
### ISP:

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



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

**Gateway:**



## ISP:

```
Router(config-if)#no clock rate 120000
Router(config-if)#int g0/1
Router(config-if)#exit
Router(config)#int g0/0
Router(config-if)#ip address 192.31.7.1 255.255.255.252
Router(config-if)#no shut
Router(config-if)#exit
Router(config-if)# Interface GigabitEthernet0/0, changed state to up
Router(config-if)#
*LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
no shutdown
Router(config-if)#exit
Router(config)#int g0/0/
* Invalid input detected at ... marker
Router(config)#int g0/0
Router(config-if)#ip address 192.31.7.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#hostname ISP
ISP(config)#
```

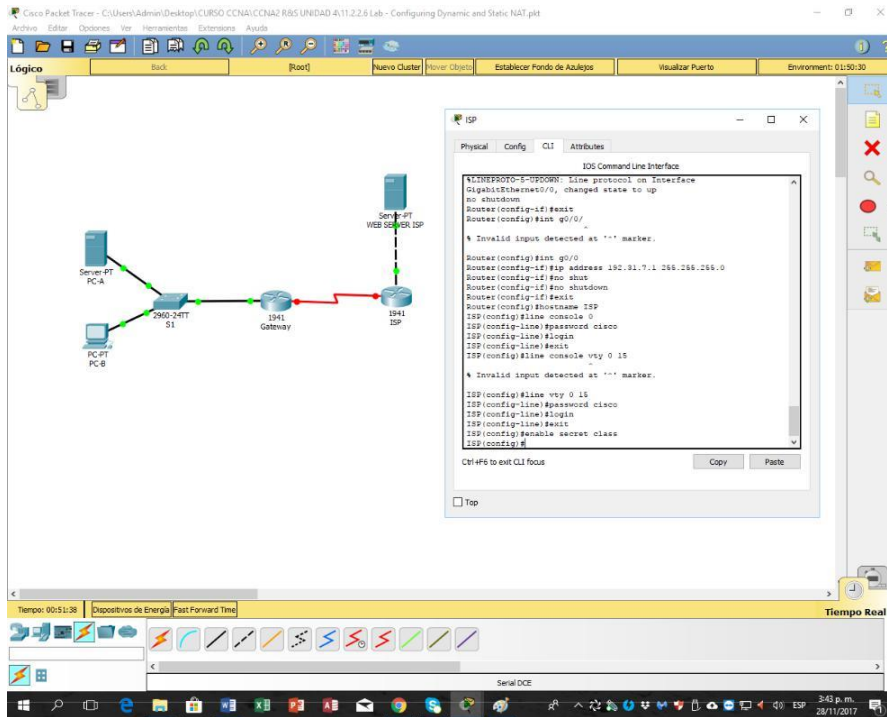
e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

## Gateway:

```
Router(config-if)#no shut
Router(config-if)#no shut
Router(config-if)#
*LINE-S-CHANGED: Interface GigabitEthernet0/1, changed state to up
*LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Router(config-if)#int e0/0/1
Router(config-if)#ip address 209.168.201.10 255.255.255.252
Router(config-if)#no shut
Router(config-if)#no shutdown
*LINE-S-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#
Router(config-if)#exit
Router(config)#hostname Gateway
Gateway(config)#line console 0
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#exit
Gateway(config)#line vty 0 15
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#exit
Gateway(config-line)#exit
Gateway(config)#
```

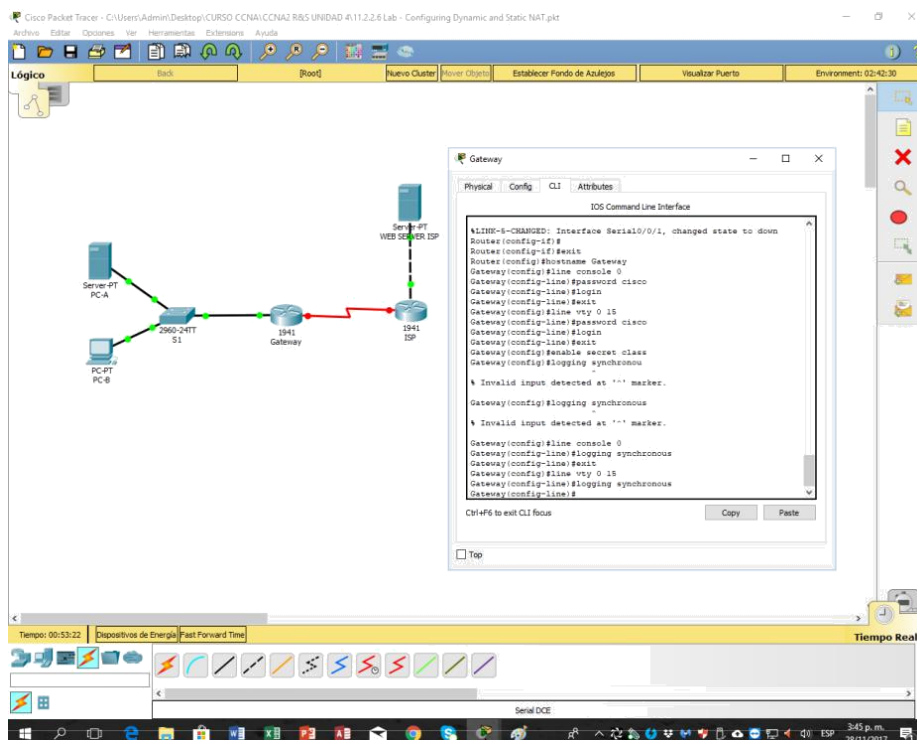


ISP:

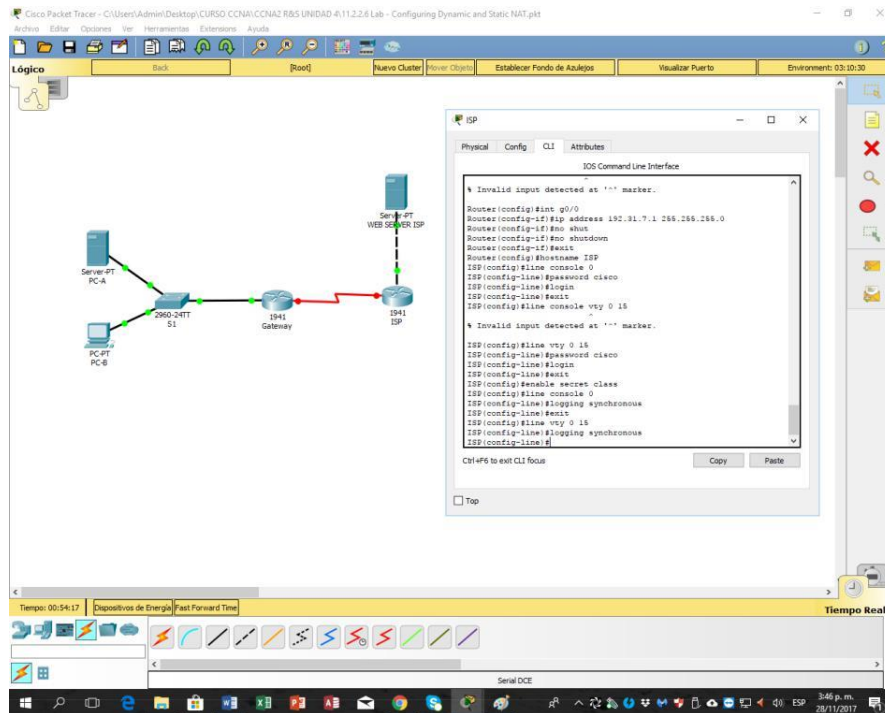


- g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpen la entrada del comando.

Gateway:



ISP:



### Paso 5. crear un servidor web simulado en el ISP.

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

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

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

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

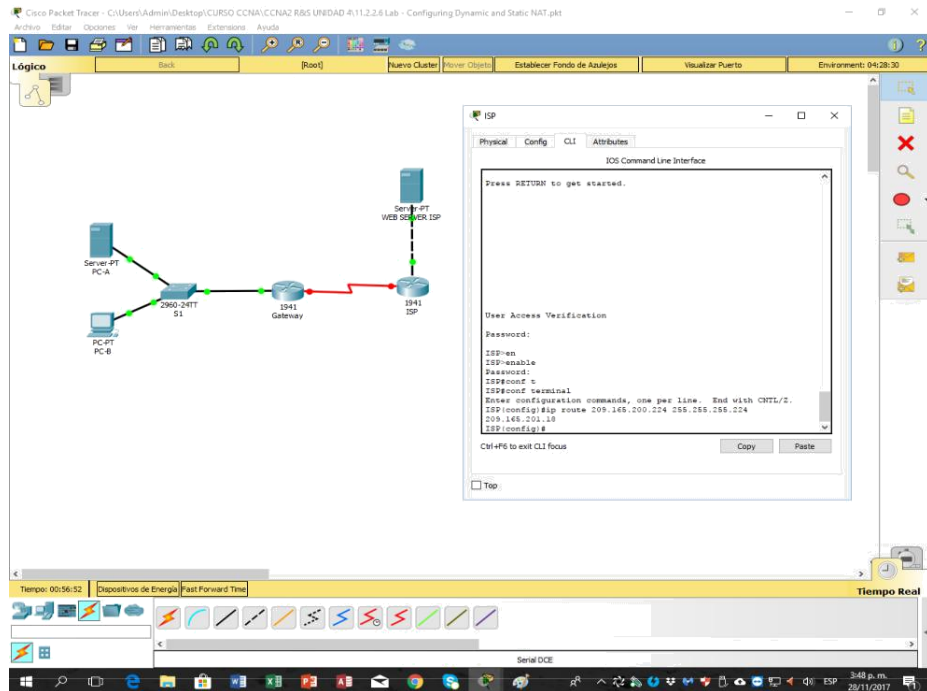
- c. Configure el servicio HTTP para utilizar la base de datos local.

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

### Paso 6. configurar el routing estático.

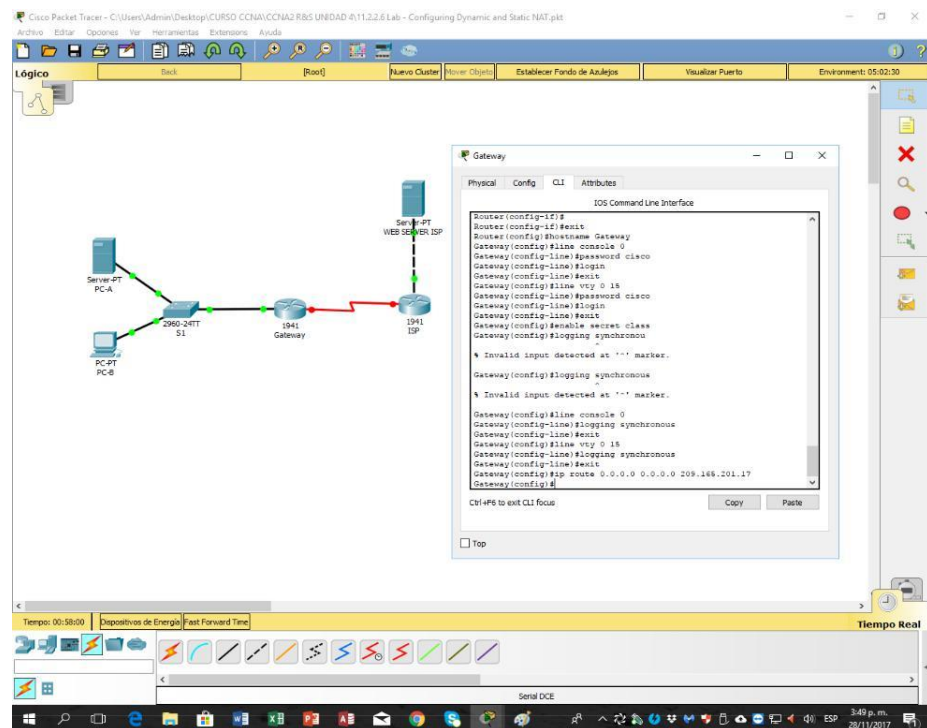
- a. Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.201.224/27.

```
ISP(config)# ip route 209.165.201.224 255.255.255.252 209.165.201.18
```



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

Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17





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

### Gateway:

```
Gateway
IOS Command Line Interface
Gateway(config)#logging synchronous
% Invalid input detected at ... marker.
Gateway(config)#line console 0
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#line vty 0 15
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.168.201.17
Gateway(config)#exit
Gateway#
*SYS-5-CONFIG_I: Configured from console by console
Gateway#copy
Gateway#copy run
Gateway#copy running-config ss
% Invalid input detected at ... marker.
Gateway#copy running-config s
Gateway#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Gateway#
```

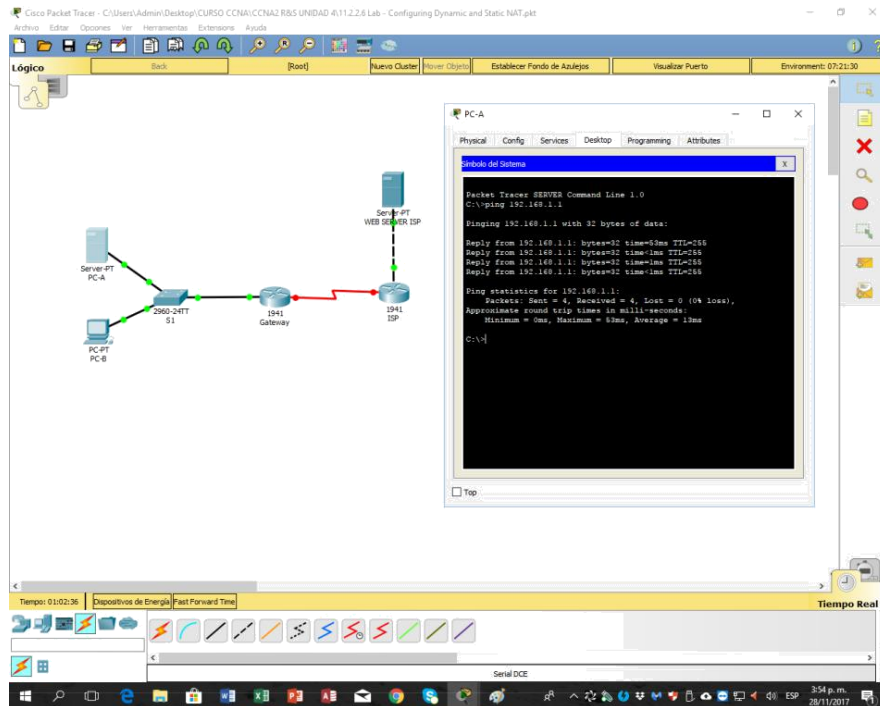
### ISP:

```
ISP
IOS Command Line Interface
User Access Verification
Password:
ISP>en
ISP>enable
Password: c
ISP#conf t
ISP#conf terminal
Enter configuration commands, one per line. End with CTRL/Z.
ISP(config)#ip route 209.168.200.224 255.255.255.224 209.168.201.15
ISP(config)#exit
ISP#
*SYS-5-CONFIG_I: Configured from console by console
ISP#copy
ISP#copy c
ISP#copy r
ISP#copy running-config s
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

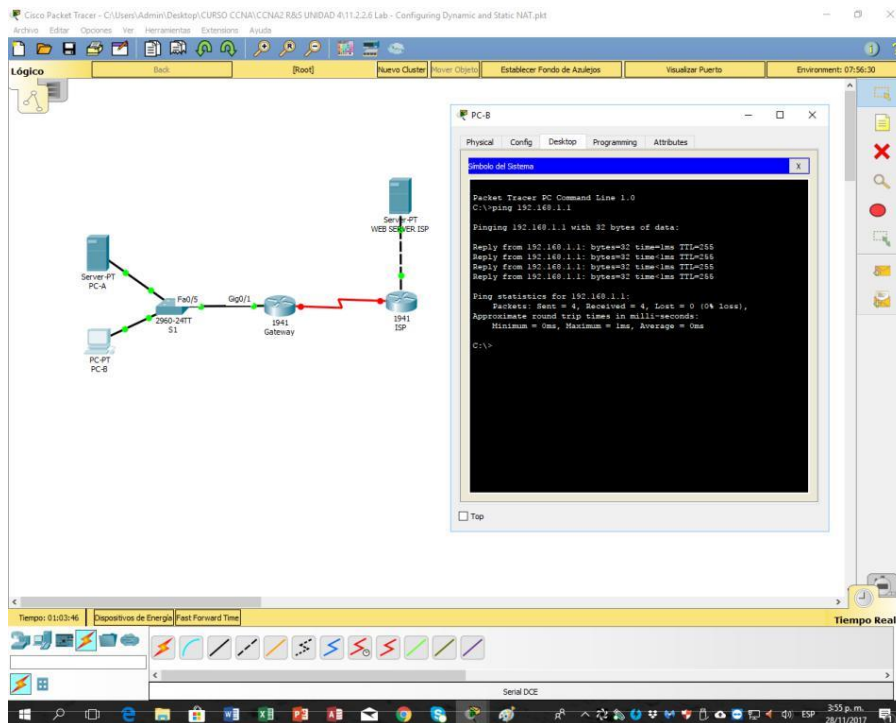
## Paso 8. Verificar la conectividad de la red

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

### PC-A:



### PC-B:



- b. Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.

### Gateway:

```

IOS Command Line Interface

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 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
S    192.168.1.1/32 is directly connected, GigabitEthernet0/1

Gateway#show ip interfaces brief
% Invalid input detected at '^' marker.

Gateway#conf t
Gateway#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.

Ctrl+Z to exit CLI flow
  
```

### ISP:

```

IOS Command Line Interface

ISP#copy c
ISP#copy r
ISP#copy running-config s
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
S    192.168.1.1/32 is directly connected, GigabitEthernet0/0

ISP#
Ctrl+Z to exit CLI flow
  
```

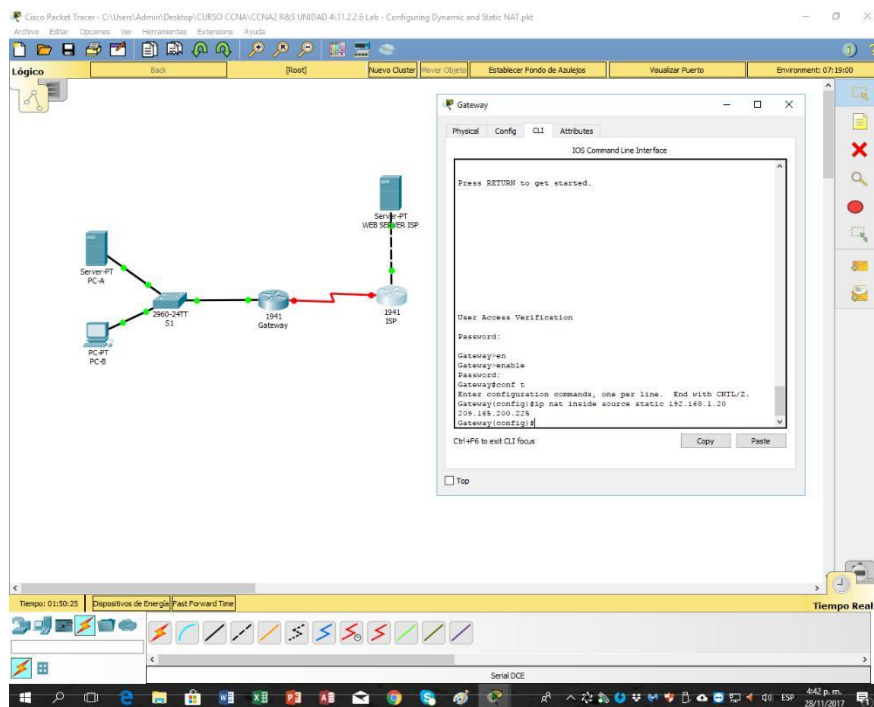
## Parte 15. configurar y verificar la NAT estática.

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

### Paso 1. configurar una asignación estática.

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

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



## Paso 2. Especifique las interfaces.

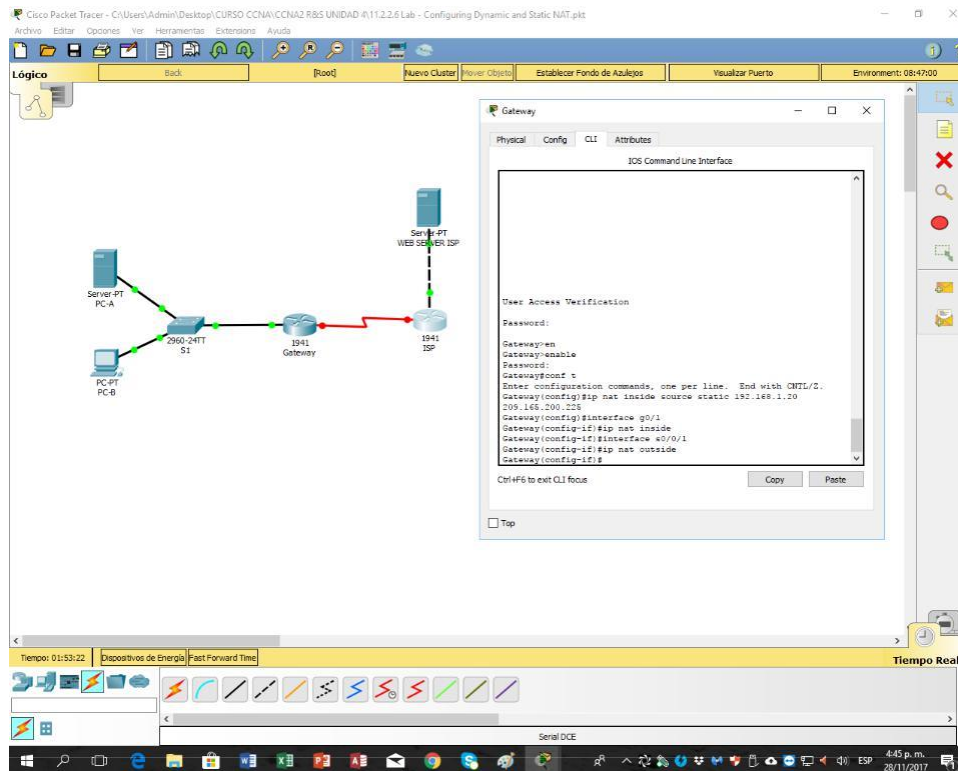
Emita los comandos ip nat inside e ip nat outside en las interfaces.

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

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

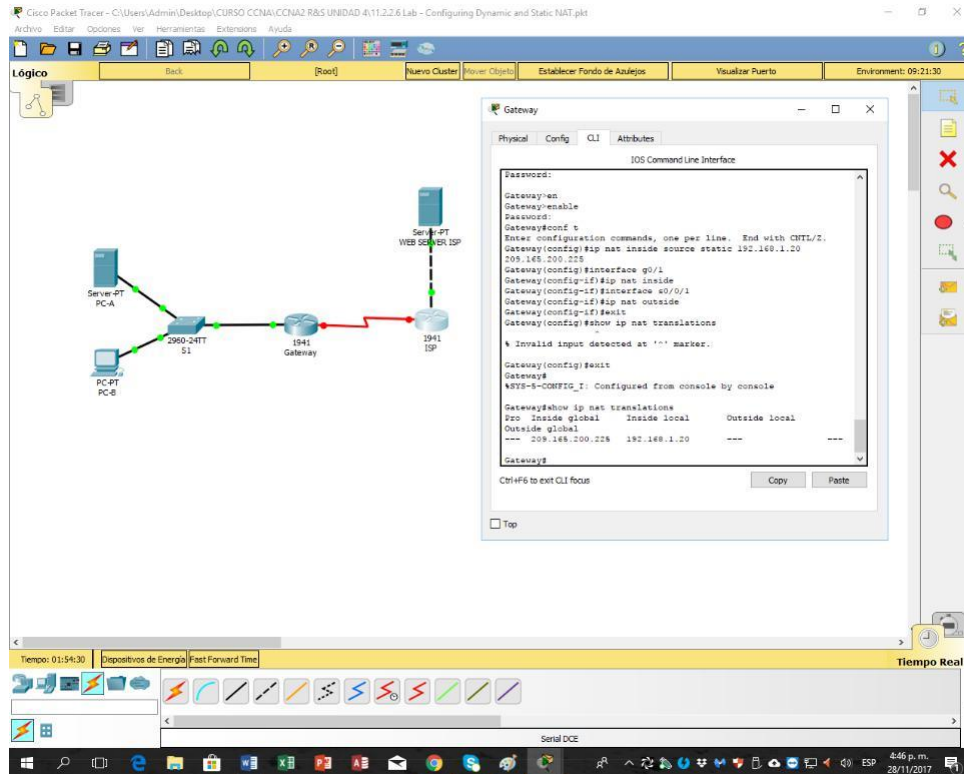
```
Gateway(config-if)# interface s0/0/1
```

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



### Paso 3. probar la configuración.

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



Gateway# **show ip nat translations**

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = 209.165.200.225

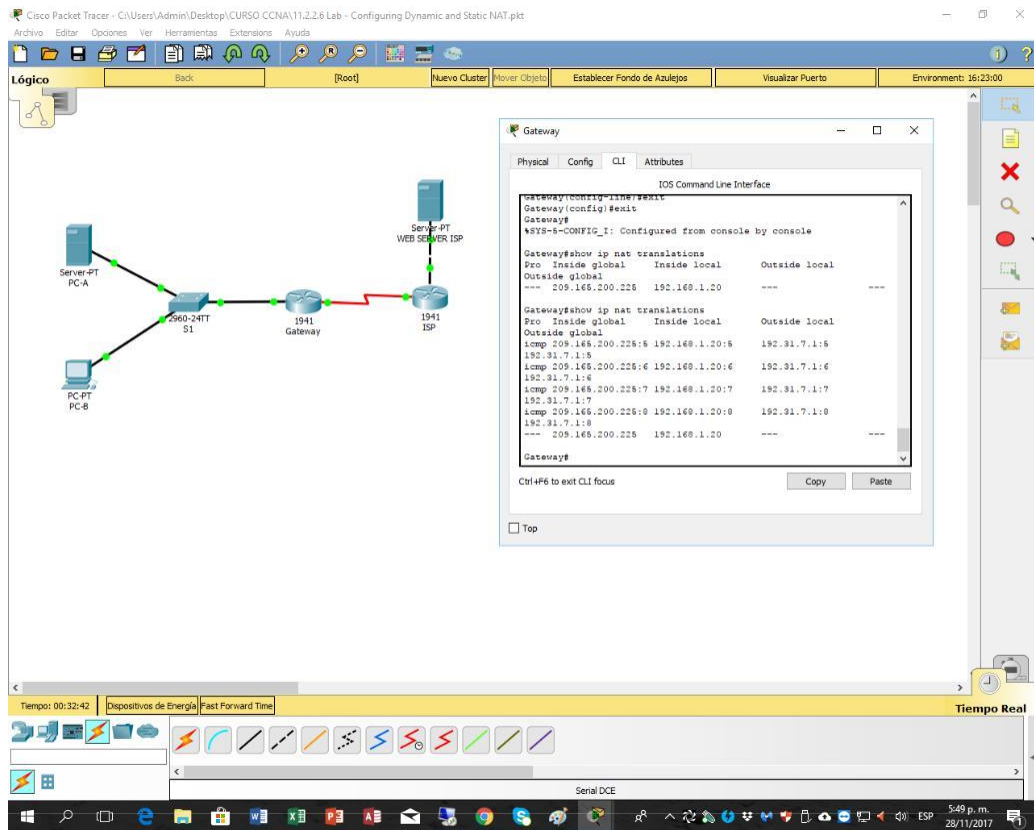
¿Quién asigna la dirección global interna?

- El router desde el Pool de NAT

¿Quién asigna la dirección local interna?

- Por el administrador de los Host

- 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

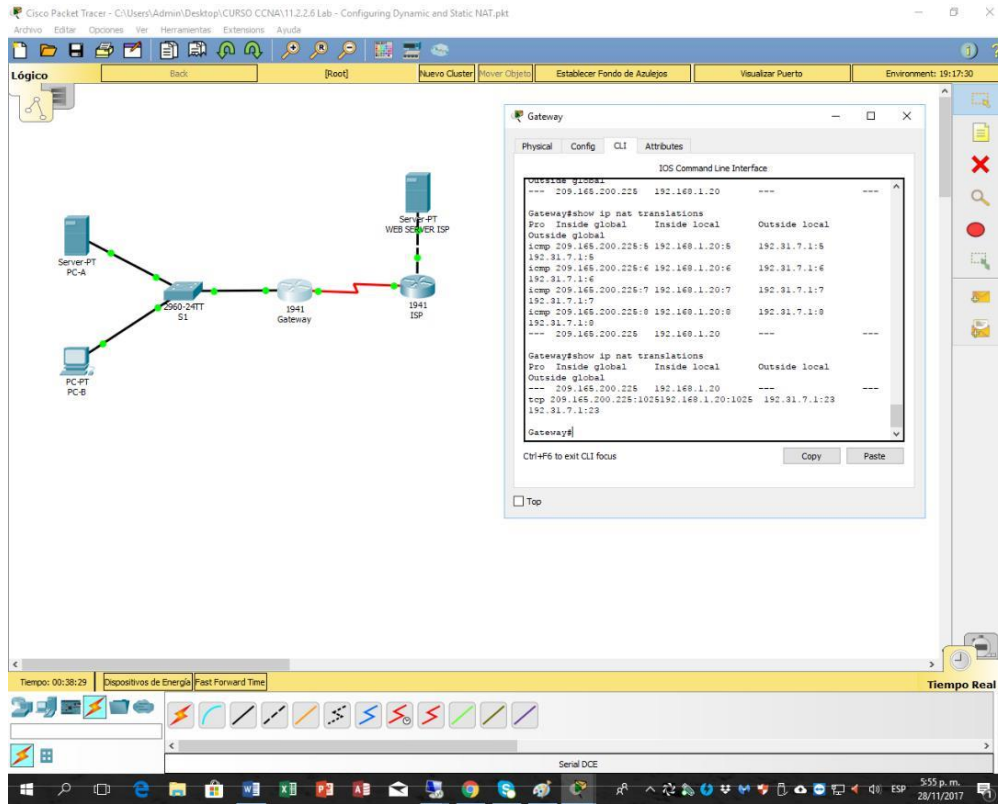
Pro	Inside global	Inside local	Outside local
icmp	209.165.200.225:5	192.168.1.20:5	192.31.7.1:5
			192.31.7.1:8
---	209.165.200.225	192.168.1.20	---
---			

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? 5,6,7 y 8

**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	---
---		

**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? TCP

¿Cuáles son los números de puerto que se usaron?

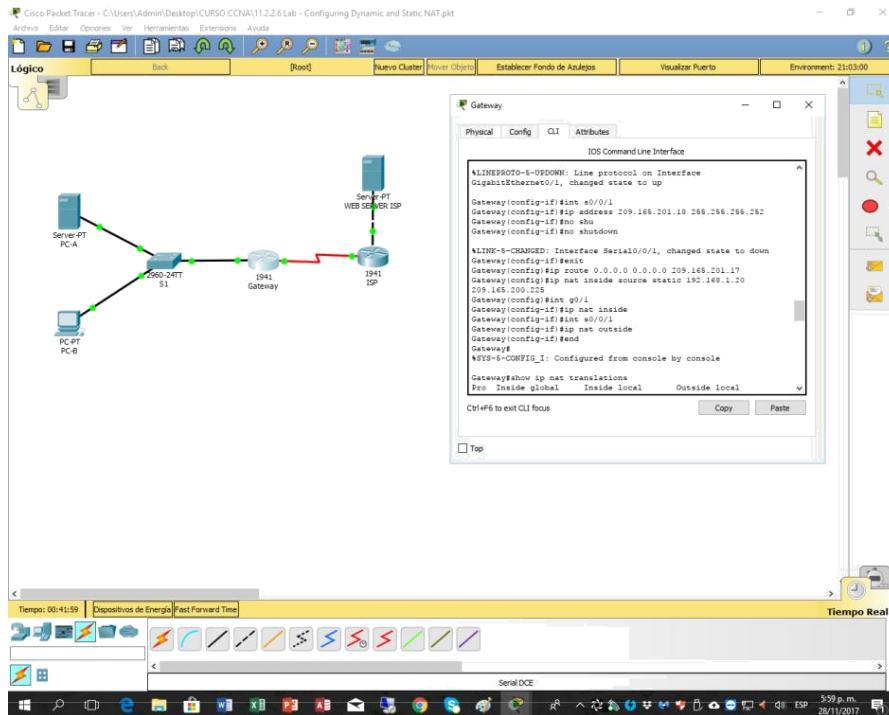
Global/local interno: **23**



Global/local externo: 23

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.

- d. 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
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).

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

Gateway# **show ip nat statics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 00:02:12 ago Outside interfaces:

Serial0/0/1 Inside interfaces:

GigabitEthernet0/1 Hits: 39 Misses:

0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

**Nota:** este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

## **Parte 16. 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

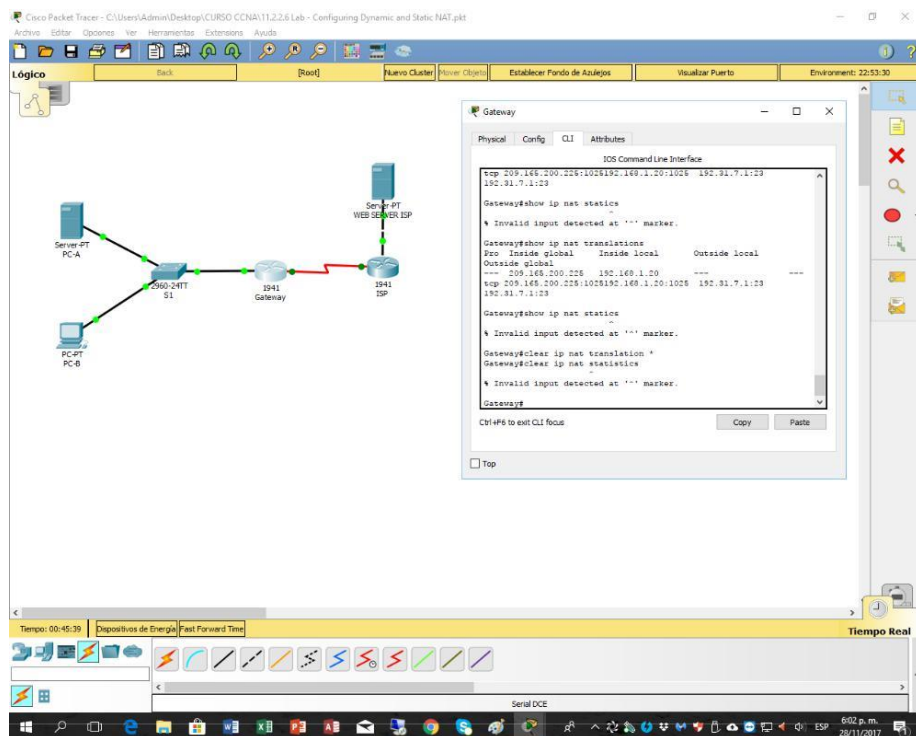
produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

### 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 *
```

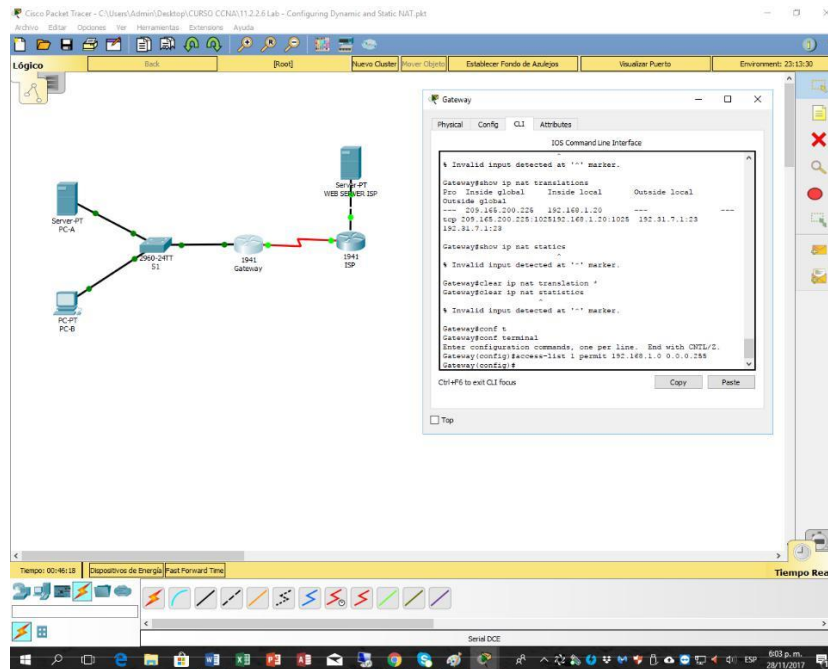
```
Gateway# clear ip nat statistics
```



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

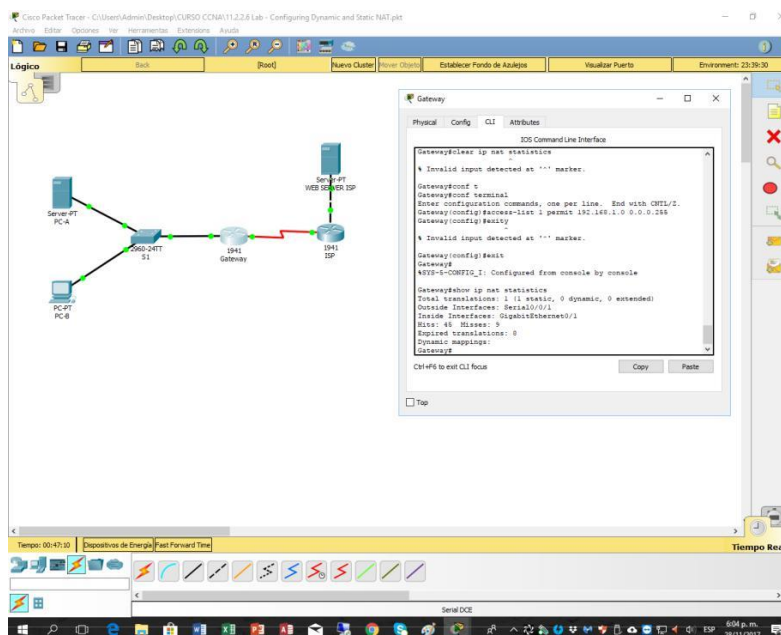
La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

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



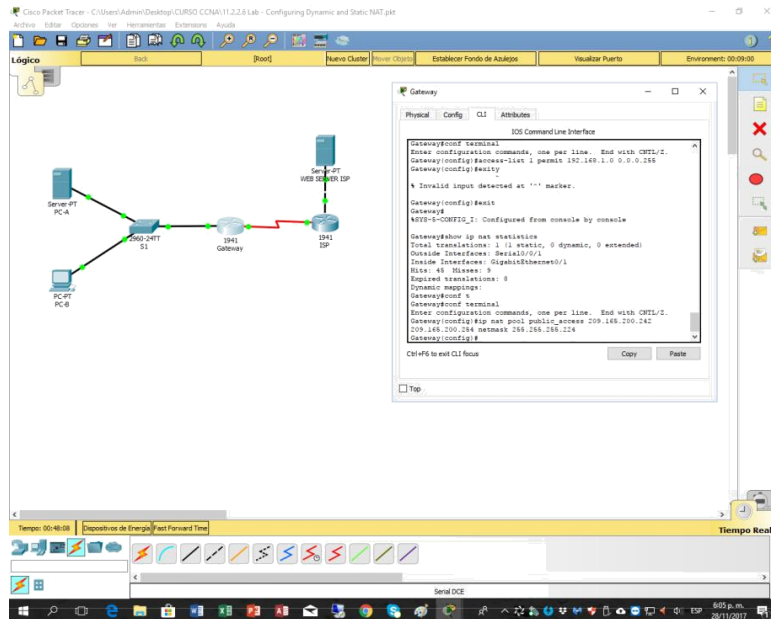
## Paso 3. verificar que la configuración de interfaces NAT siga siendo válida.

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.

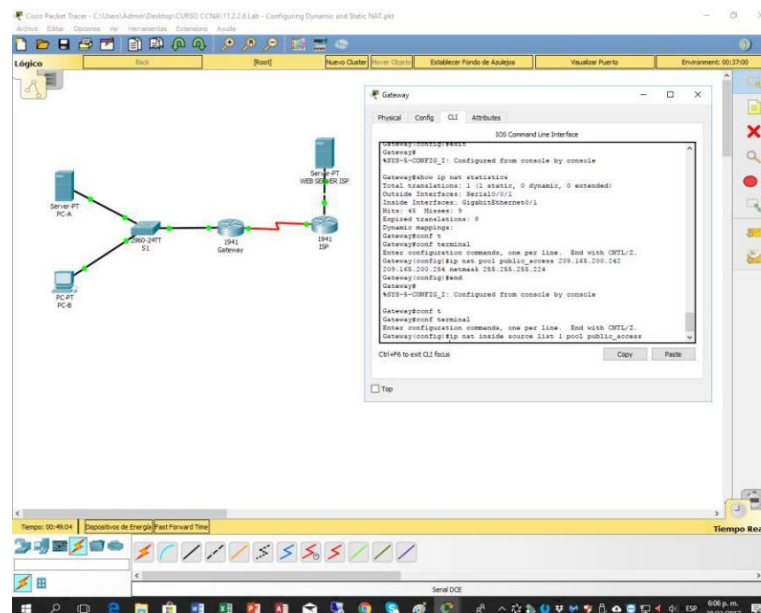
Gateway(config)# ip nat pool public\_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224



#### 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



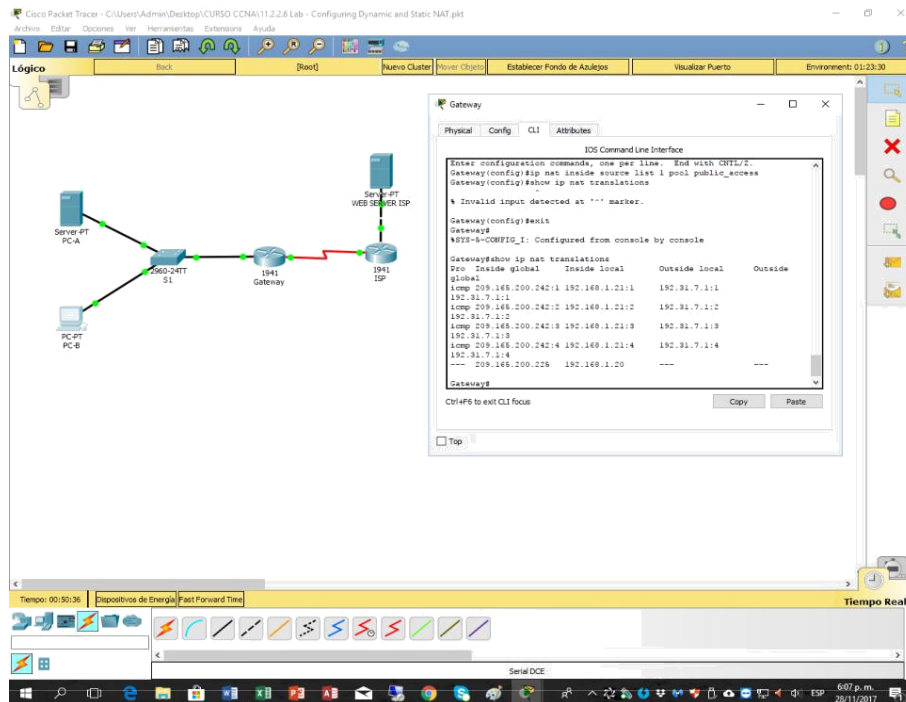
## Paso 6. probar la configuración.

- 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
---	209.165.200.225	192.168.1.20	---
---			

icmp	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1
---	209.165.200.242	192.168.1.21	---
---			



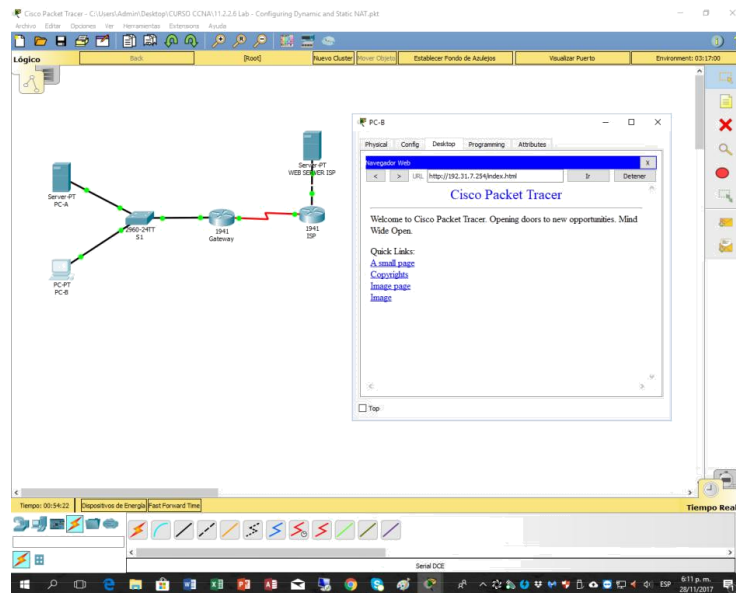
¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = **209.165.200.242**

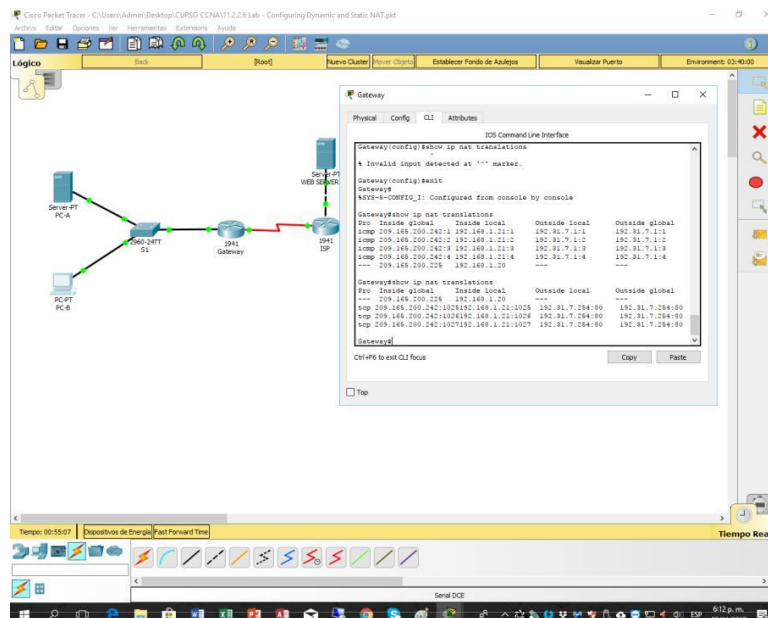
Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

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

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



- c. Muestre la tabla de NAT.



```
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80 192.31.7.1:80
--- 209.165.200.242          192.168.1.22          ---
---
```

¿Qué protocolo se usó en esta traducción? TCP

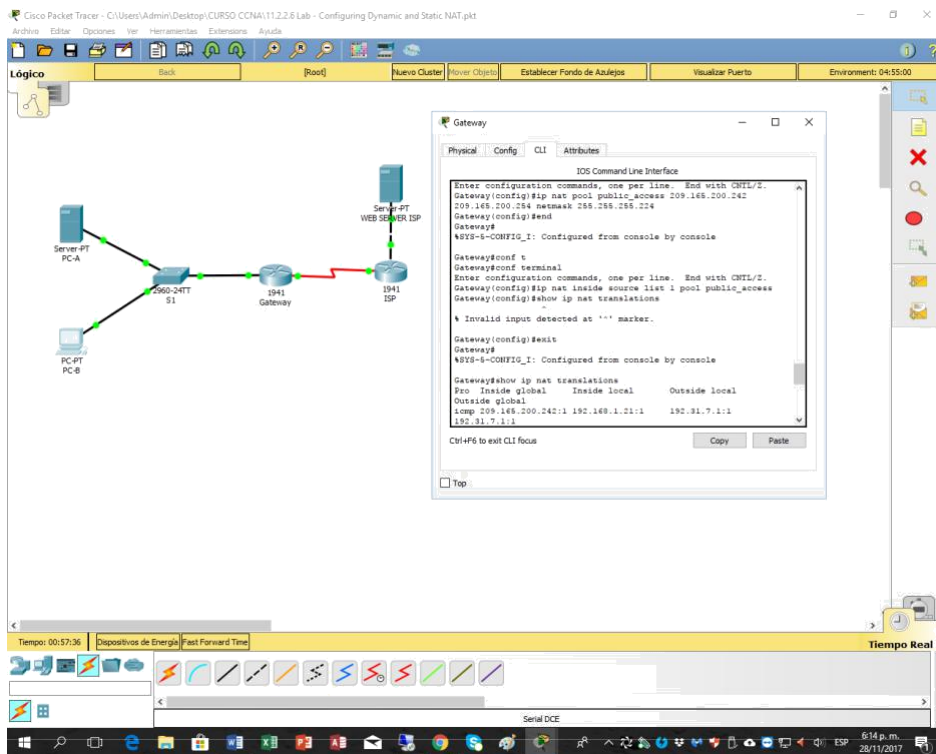
¿Qué números de puerto se usaron? Interno: 80

Externo: 80

¿Qué número de puerto bien conocido y qué servicio se usaron? 80, 1025, 1026 y 1027



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.

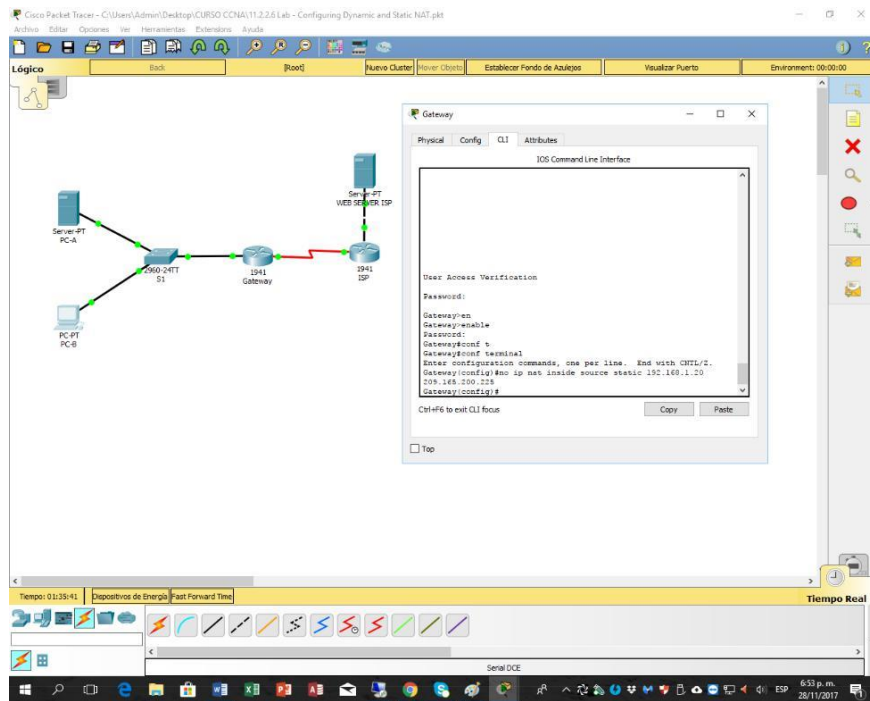
**Paso 7.     eliminar la entrada de NAT estática.**

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

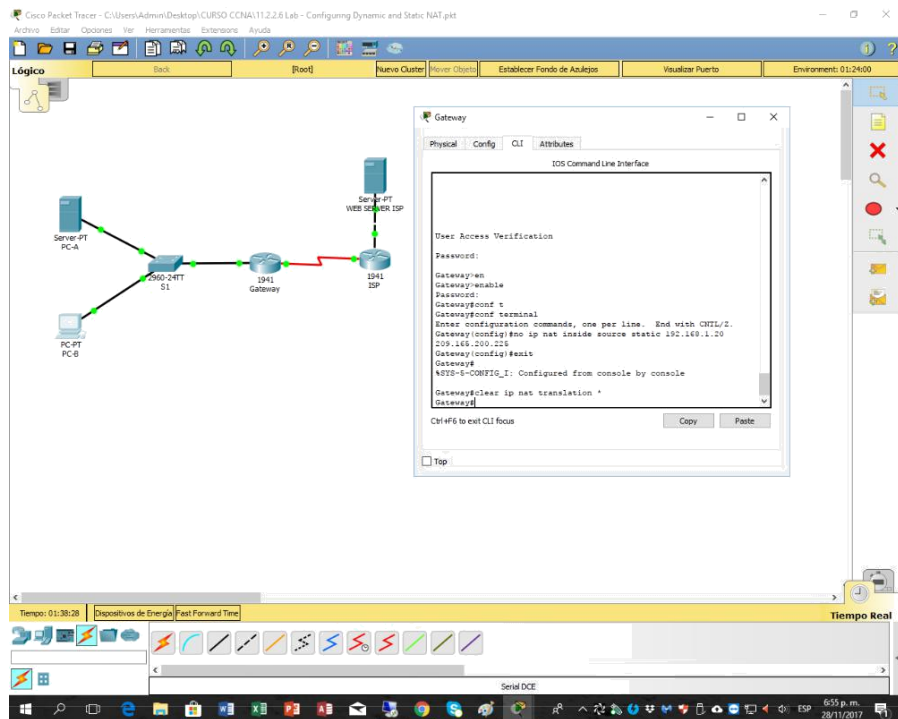
- a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

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**

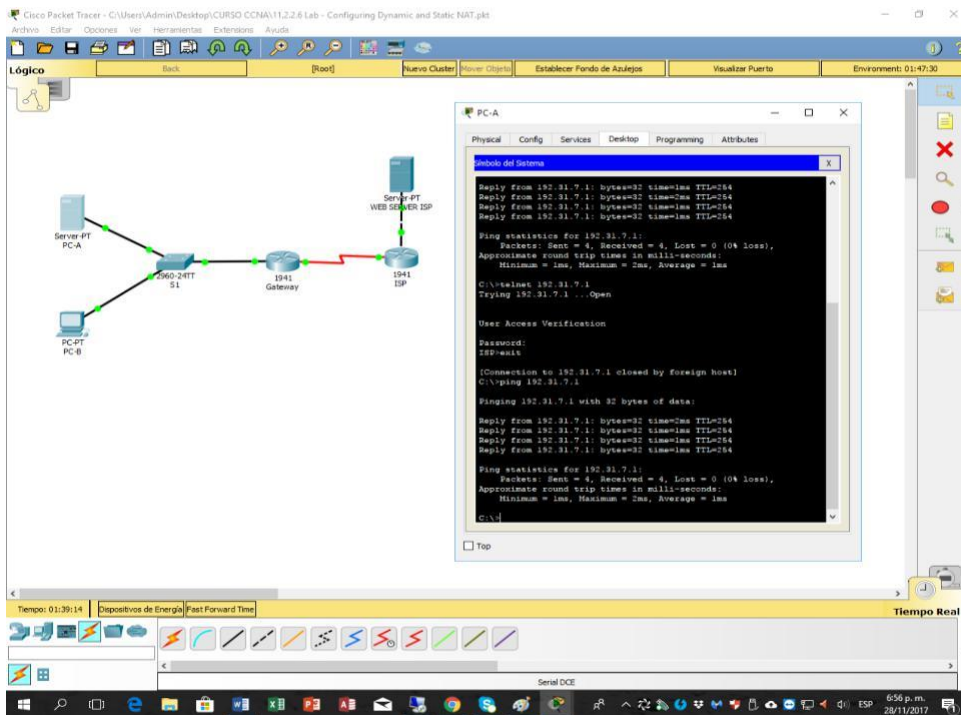


b. Borre las NAT y las estadísticas.

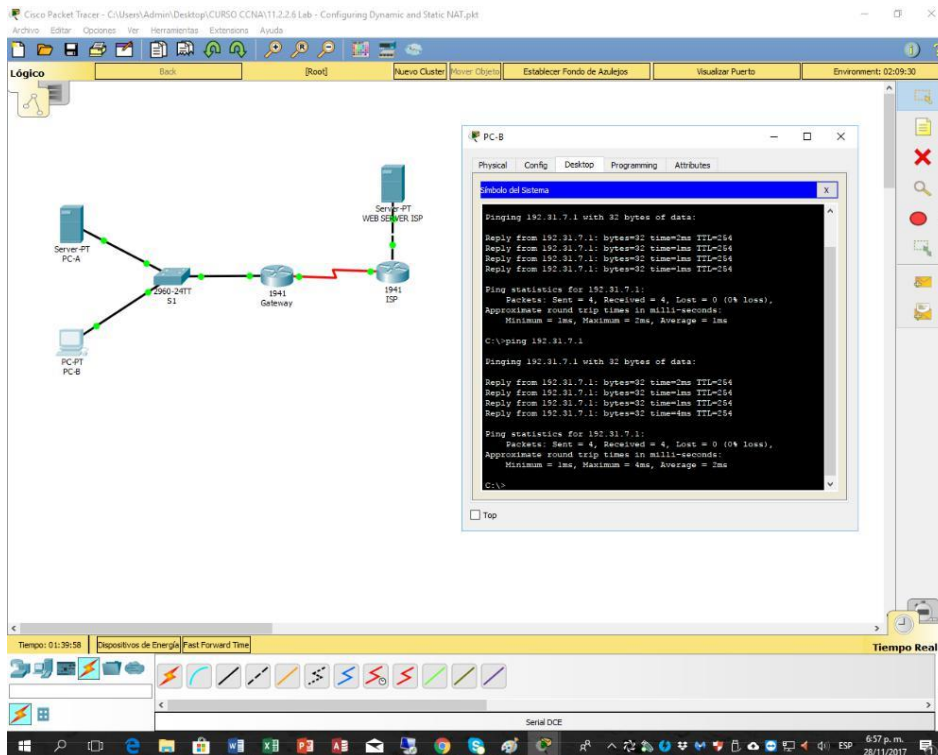


c. Haga ping al ISP (192.31.7.1) desde ambos hosts.

### PC-A:

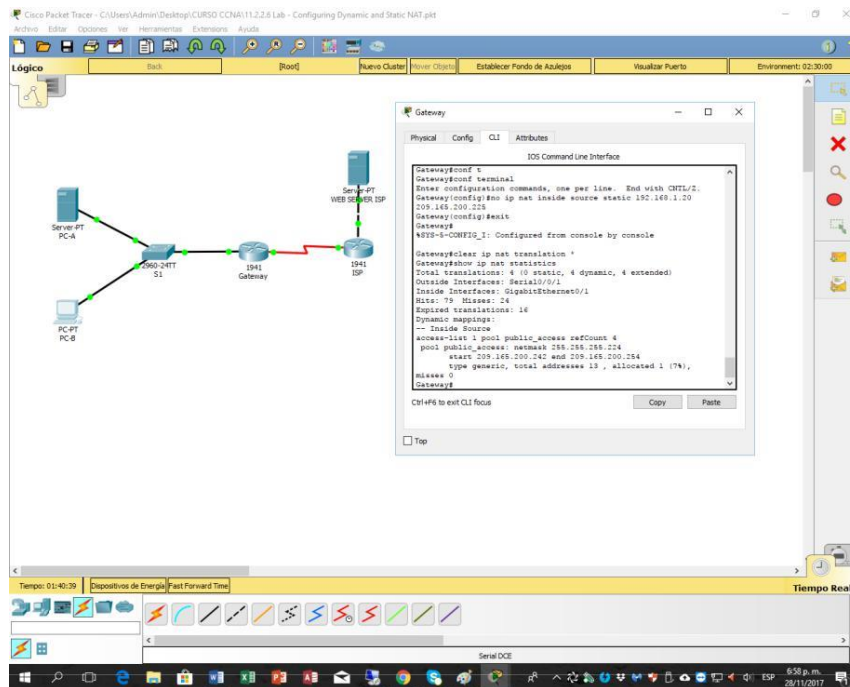


### PC-B:



d. Muestre la tabla y las estadísticas de NAT.

Gateway# **show ip nat statistics**



Total active translations: 4 (0 static, 4 dynamic; 2 extended)

Peak translations: 15, occurred 00:00:43 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 16

Misses: 0

CEF Translated packets: 285, CEF Punted packets: 0

Expired translations: 11

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public\_access refcount 4

pool public\_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 2 (15%), misses 0

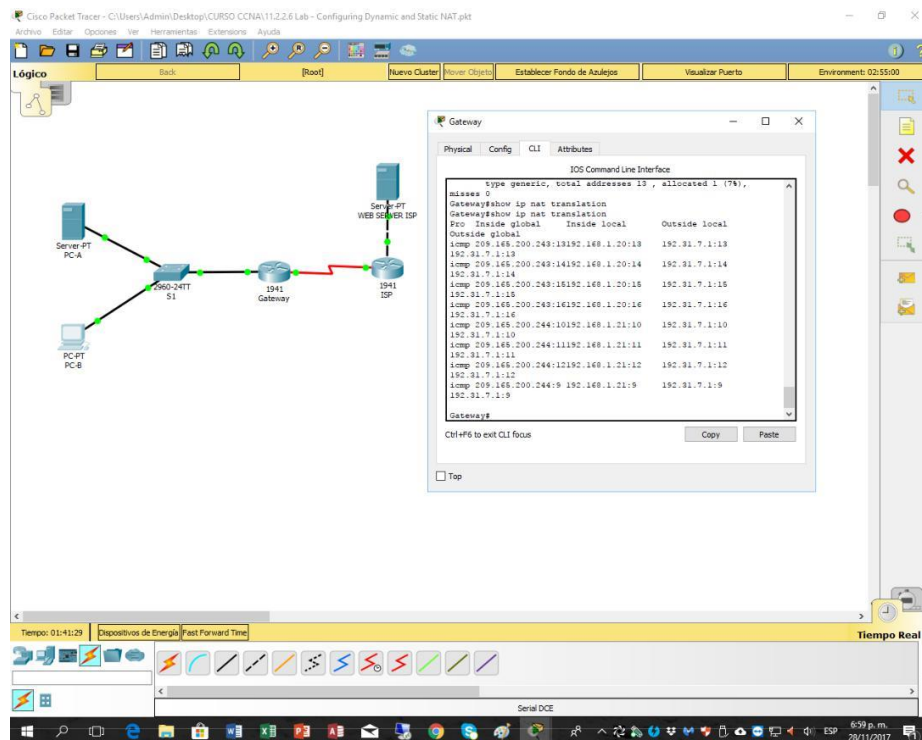
Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

Gateway# show ip nat translation



Pro Inside global

Inside local

Outside local

Outside global

icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512 192.31.7.1:512

--- 209.165.200.243

192.168.1.20

---

---

icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512 192.31.7.1:512

--- 209.165.200.242

192.168.1.21

---

---

**Nota:** este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

## Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

No hay suficientes direcciones Ip Publicas y para también minimizar costos por el hecho de adquirir muchas más ip Publicas con un proveedor de servicios.

2. ¿Cuáles son las limitaciones de NAT?

La NAT necesita la información IP o Numero de información, luego la información de numero de Puerto en la cabecera de IP y también en la Cabecera de TCP para la traslación.

Y una lista parcial de protocolos que no pueden ser usados como NAT: SNMP, LDAP, Kerberos Version 5.

**Tabla de resumen de interfaces del router**

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

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



## Conclusiones

- Identificar y solucionar problemas propios de enrutamiento mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces.
- Permitted comprender y describir el propósito y los tipos de las listas de control de acceso (ACL).
- Configurar y supervisar las ACL para IPv4 e IPv6 y resolver los problemas relacionados.
- Llevar a cabo la configuración y resolución de problemas operacionales NAT.
- Diseñar, calcular y aplicar mascarar de subred y direcciones para cumplir con determinados requisitos en redes IPv4 e IPv6.
- Utilizar los comandos de la interfaz de línea de comandos (CLI) de Cisco para realizar configuraciones básicas de routers y switches.
- Usar utilidades comunes de red para verificar operaciones de redes pequeñas y analizar el tráfico de datos.

## Referencia Bibliográficas

OVA Unidad 4 - Video - Principios de Enrutamiento Este Objeto Virtual de Aprendizaje, titulado Video - Principios de Enrutamiento, tiene como objetivo, orientar al estudiante sobre la configuración básica de Switches y Routers.

Temática: Enrutamiento Dinámico 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>

Temática: OSPF de una sola área 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>

Temática: Listas de control de acceso 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>

Temática: DHCP 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>

Temática: Traducción de direcciones IP para IPv4 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-NT1IhgOyjWeh6timi\\_Tm](https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm)