Paso 7 – Colaborativo 4

Por:
Ana María Fernández España
Leidy Paola Moncayo
Nubia Del Pilar Agreda Agreda
Jaccson Jairo Atis
Rocio Bernarda Jiménez

Diplomado de profundización cisco
(diseño e implementación de soluciones integradas lan / wan)
Código: 203092

No. De Grupo: 17

Presentado a:
Nancy Amparo Guaca

Universidad Nacional Abierta y a Distancia. UNAD
Zona Centro Sur
ECBTI
Noviembre 2017

Contenido

Introducción

Las redes de datos que usamos en nuestras vidas cotidianas para aprender, jugar y trabajar varían desde pequeñas redes locales hasta grandes internetworks globales. En el hogar, un usuario puede tener un router y dos o más computadoras. En el trabajo, una organización probablemente tenga varios routers y switches para atender las necesidades de comunicación de datos de cientos o hasta miles de computadoras. Los routers reenvían paquetes mediante el uso de la información de la tabla de routing. Los routers pueden descubrir las rutas hacia las redes remotas de dos maneras: de forma estática y de forma dinámica. En una red grande con muchas redes y subredes, la configuración y el mantenimiento de rutas estáticas entre dichas redes conllevan una sobrecarga administrativa y operativa. Esta sobrecarga administrativa es especialmente tediosa cuando se producen cambios en la red, como un enlace fuera de servicio o la implementación de una nueva subred. Implementar protocolos de routing dinámico puede aliviar la carga de las tareas de configuración y de mantenimiento, además de proporcionar escalabilidad a la red. Por tanto, los protocolos de routing dinámico, se exploran los beneficios de utilizar esta clase de protocolos, la forma en que se clasifican los distintos protocolos de routing y las métricas que utilizan los protocolos de routing para determinar la mejor ruta para el tráfico de la red. Entre otros temas que trataremos a lo largo del desarrollo de las prácticas propuestas e implementadas, se encuentran las características de los protocolos de routing dinámico y la forma en que se diferencian los distintos protocolos de routing.

Los profesionales de red deben comprender cuáles son los diferentes protocolos de routing disponibles, a fin de decidir fundadamente cuándo utilizar routing dinámico o estático. También necesitan saber cuál es el protocolo de routing dinámico más adecuado en un entorno de red determinado.

De este modo, en el desarrollo del presente informe trataremos los temas implementados en la segunda parte del curso de certificación de CISCO CP CCNA2 II-2017, en cuanto a los Principios básicos de routing y switching se refiere. Esto, detallado en una compilación de

prácticas que nos permiten poner a prueba nuestras habilidades e implementar soluciones a las mismas de acuerdo a los conocimientos adquiridos puntualmente en los capítulos 7 al 11.

Tratando temas fundamentales en nuestro estudio como lo son: Capítulo 7: Routing dinámico; Capítulo 8: OSPF de área única; Capítulo 9: Listas de control de acceso; Capítulo 10: DHCP; Capítulo 11: Traducción de direcciones de red para IPv4.

En las cuales empezaremos con el análisis de una topología propuesta, teniendo en cuenta los objetivos propuestos, como la lectura y comprensión de la situación que se presenta para posteriormente dar una adecuada solución a los interrogantes propuestos y a la implementación o verificación del montaje de la red según esto lo requiera.

Finalmente se concluirá en cada práctica de acuerdo a los objetivos planteados desde un principio y a los conocimientos adquiridos en el desarrollo de la misma.

De esta manera, se desarrollará el informe de prácticas presentado a nuestra tutora del curso de certificación, como constancia de la implementación de los conocimientos adquiridos a lo largo del estudio del material que nos ha brindado la universidad y la plataforma de CISCO.

4.4.1.2 Packet Tracer - Configure Ip Acls To Mitigate Attacks

Topology

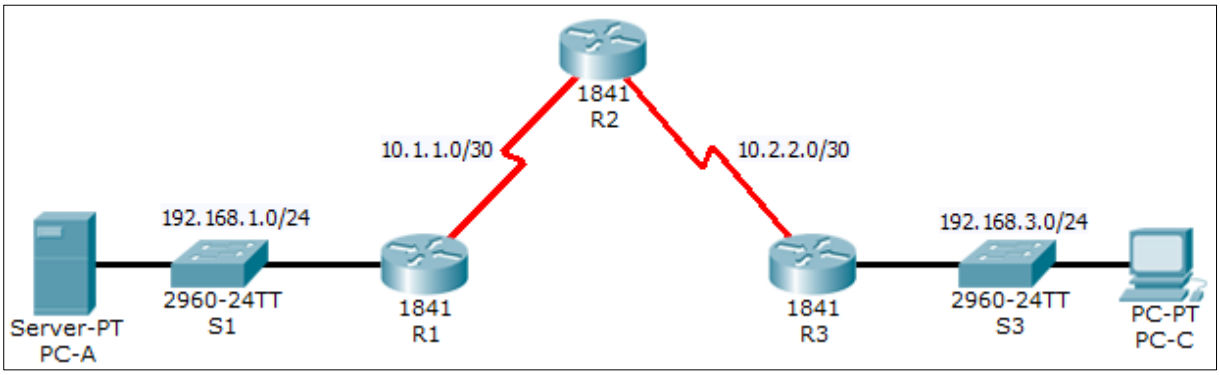


Imagen 1. Topología ejercicio 4.4.1.2

Tabla 1:

Addressing Table

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

Objetivos

- Verificar la conectividad entre los dispositivos antes de la configuración del firewall.
- Utilice las ACL para garantizar el acceso remoto a los enrutadores solo está disponible desde la estación de administración PC-C.
- Configure las ACL en R1 y R3 para mitigar los ataques.
- Verificar la funcionalidad de ACL.

Antecedentes I Escenario

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 preconfigurado con lo siguiente:

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

Parte 1. Verificar la conectividad de red básica: Verifique la conectividad de la red antes de configurar las IP ACLs.

Paso 1. Desde PC-A, verifique la conectividad a PC-C y R2.

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

```
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=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Imagen 2. Ping dse PC-A a PC-C (192.168.3.3).

b. Desde el símbolo del sistema, establezca una sesión SSH en 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.

```
C:\>ssh -l SSHadmin 192.168.2.1
Open
Password:



R2#exit

[Connection to 192.168.2.1 closed by foreign host]
```

Imagen 3. Sesión SSH en la interfaz R2 Lo0 (192.168.2.1).

Paso 2. Desde PC · C, verifique la conectividad con PC · A y R2.

a. Desde el símbolo del sistema, ping

PC-A (192.168.1.3).

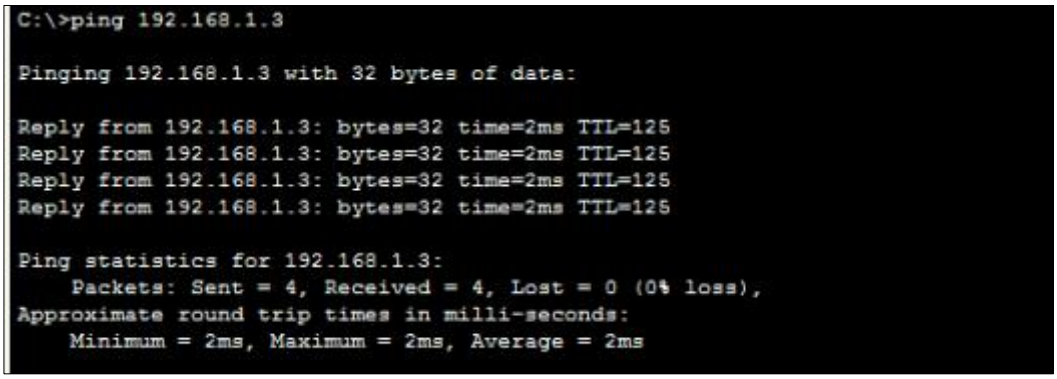


Imagen 4. Desde PC-C ping PC-A (192.168.1.3).

b. Desde el símbolo del sistema, establezca una sesión SSH en 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

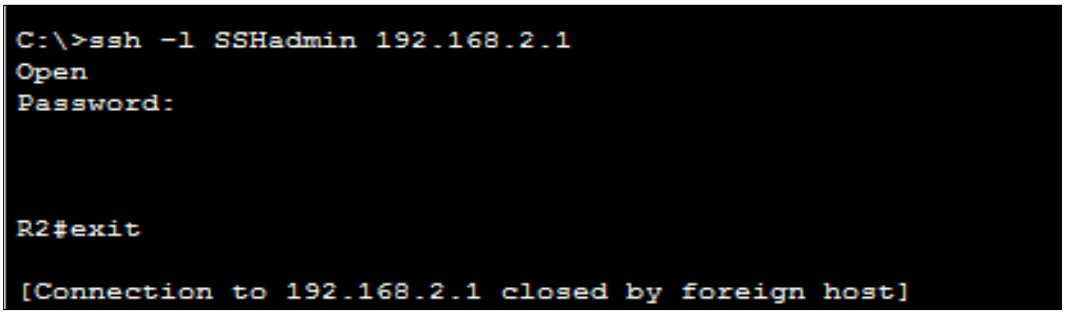


Imagen 5. Desde PC-C sesión SSH en la interfaz R2 Lo0 (192.168.2.1).

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

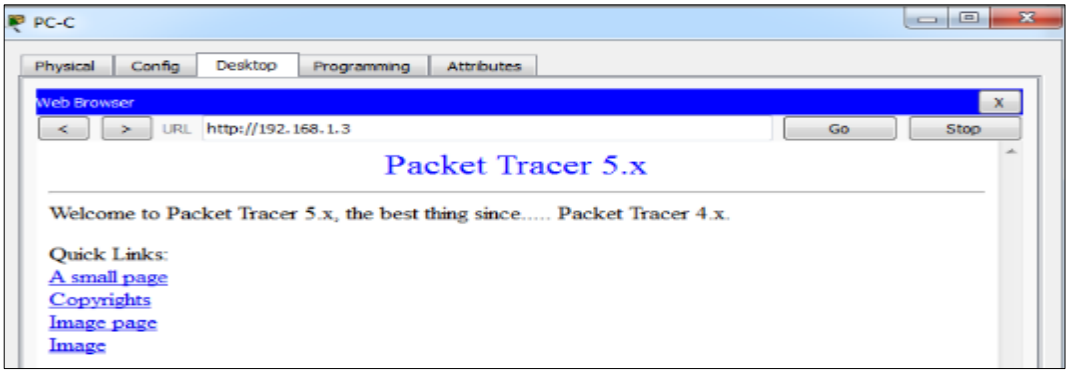


Imagen 6. Navegador web en la PC 192.168.1.3.

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.

Utilice el comando Access-list para crear una ACL IP numerada en R1, R2 y R3.

```
R1>enable
Password:
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#access-list 10 permit 192.168.3.3
R1(config)#
```

```
R2>enable
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3
R2(config)#
```

```
R3>enable
Password:
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#
```

Imagen 7. Comando Access-list para crear una ACL IP numerada en R1, R2 y R3

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 vty 0 4
R1(config-line)#access-class 10 in
```

```
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#
```

```
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#
```

Imagen 8. Comando access-class para aplicar la lista de acceso al tráfico entrante en las líneas VTY.

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

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

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

Password:

Password:

[Connection to 192.168.2.1 closed by foreign host]
```

Imagen 9. Sesión SSH a 192.168.2.1 desde PC-C

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

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

% Connection refused by remote host
```

Imagen 10. Sesión SSH a 192.168.2.1 desde PC-A

Parte 3. Cree una ACL IP numerada 120 en R1

Permitir que cualquier servidor externo acceda a los servicios DNS, SMTP y FTP en el servidor PC-A, denegar el acceso de cualquier host externo a los servicios HTTPS en PC-A, y permitir que PC-C acceda a R1 a través de SSH.

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

Asegúrese de deshabilitar HTTP y habilitar HTTPS en la PC del servidor · A.

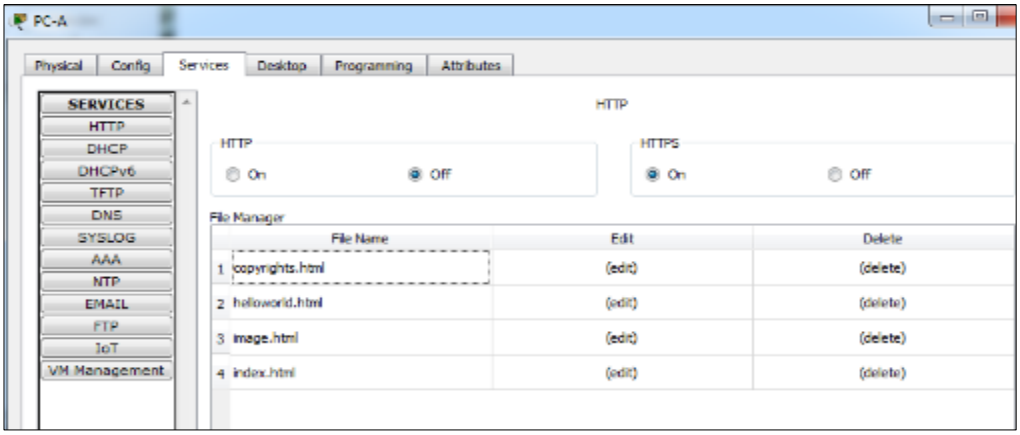


Imagen 11. Deshabilitar HTTP y habilitar HTTPS en la PC-A

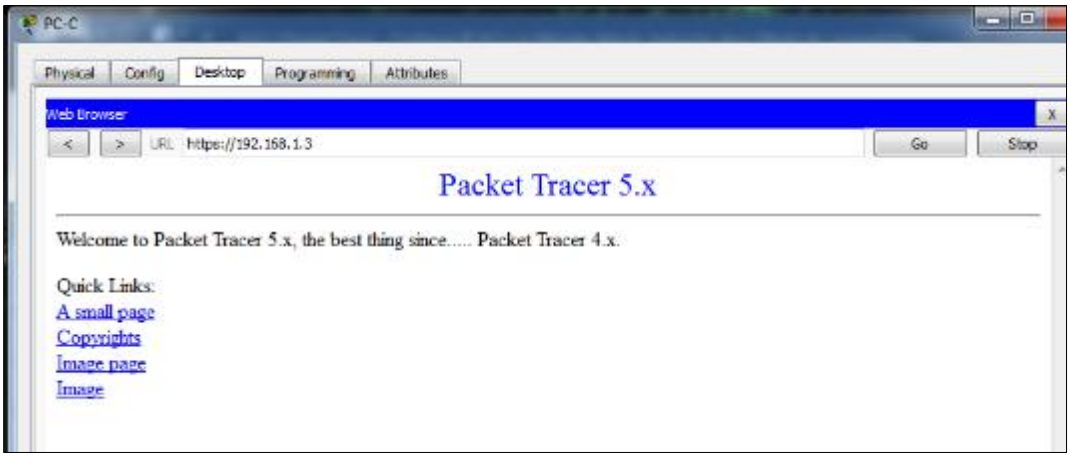


Imagen 12. La PC-C accede a la PC-A a través de HTTPS

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 10 permit 192.168.3.3
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq
domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq
smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host
10.1.1.1 eq 22
R1(config)#
```

Imagen 13. Comando access-list para crear una ACL IP numerada

Paso 3. Aplique la ACL a la interfaz S01010.

Utilice el comando ip access-group para aplicar la lista de acceso al tráfico entrante en la interfaz S0/0/0.

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

Paso 4. Verifique que la PC-C no pueda acceder a la PC-A a través de HTTPS utilizando el navegador web.

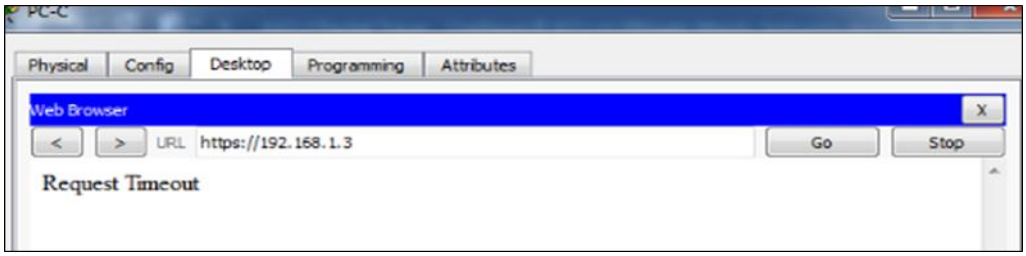


Imagen 14. PC-C no accede a la PC-A a través de HTTPS

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 con éxito en la interfaz de bucle invertido en R2.

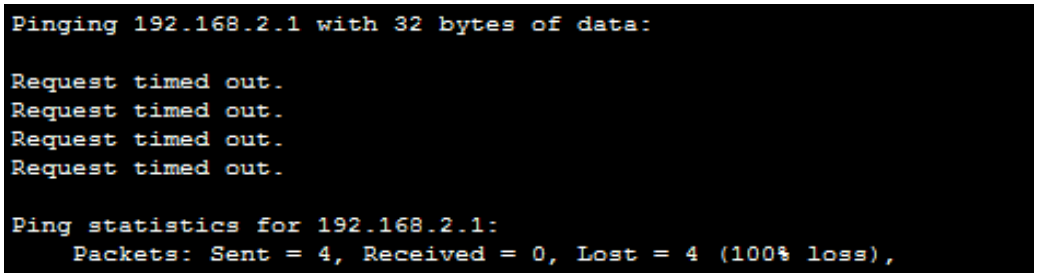


Imagen 15. PC-A no hace ping con éxito en la interfaz de bucle invertido en R2

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)#
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
```

Imagen 16. Comando access · list para crear una ACL IP numerada.

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

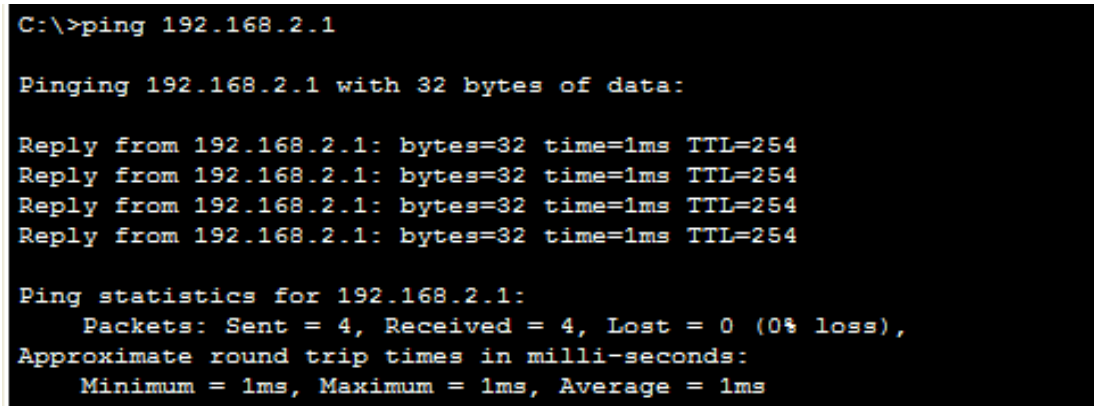


Imagen 17. PC-A hace ping con éxito en la interfaz loopback en R2

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 F011.

Utilice 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, any RFC 1918 private addresses, and any IP multicast address.

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
R3(config)#
```

Imagen 18. Comando access · list para crear una ACL IP numerada.

Paso 2. Aplique la ACL a la interfaz Serial 01011.

Utilice 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 01011 se descarta.

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.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

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

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Imagen 19. Respuestas del eco ICMP bloqueadas por el ACL.

Paso 4. Verifica los resultados.

Su porcentaje de finalización debe ser de 100%. Haga clic en Comprobar resultados para ver los comentarios y la verificación de cuáles componentes requeridos se han completado.

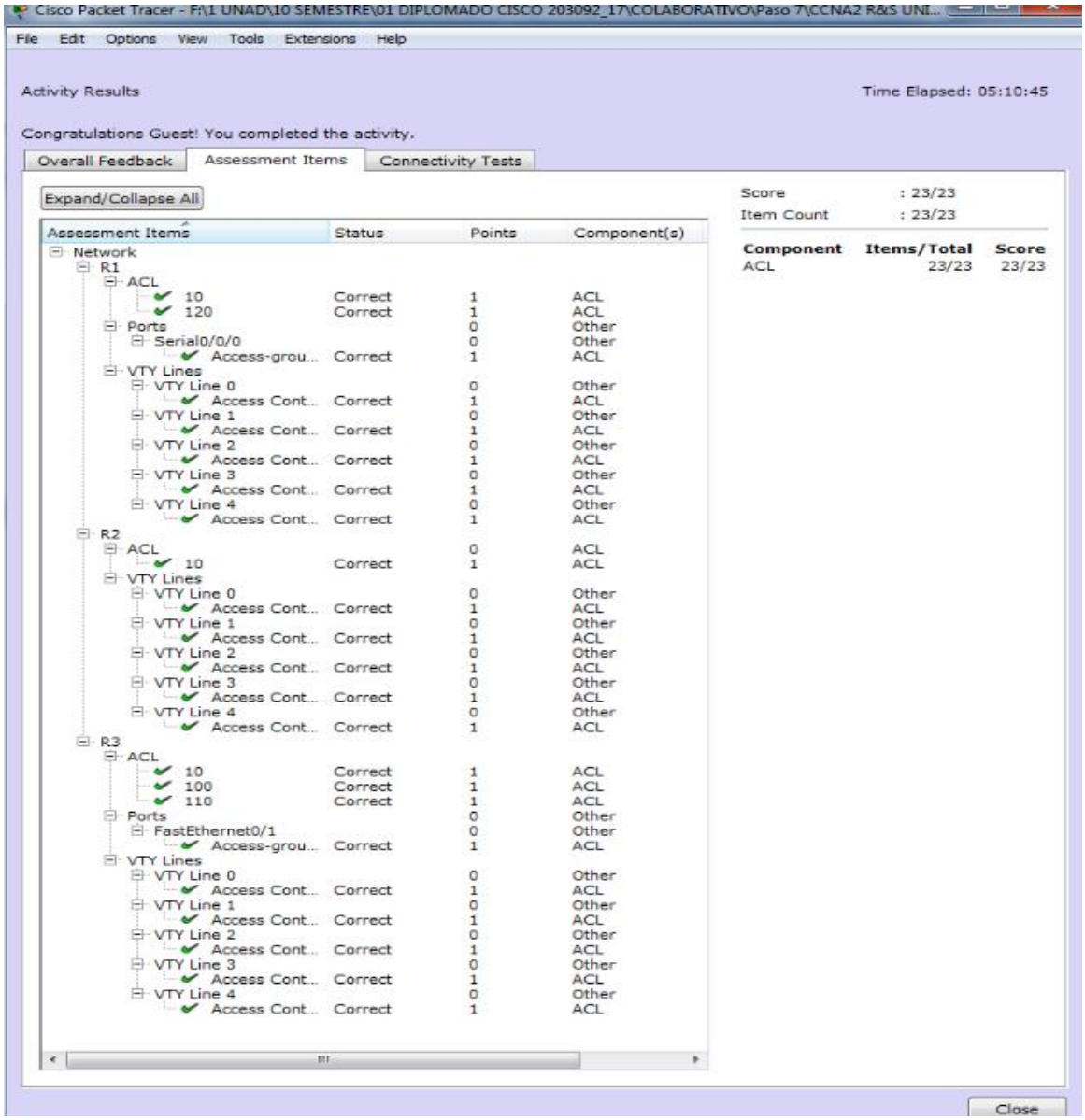


Imagen 20. Actividad Completa.

Conclusiones

- En el anterior ejercicio utilizamos el SSH que es una aplicación y un protocolo que proporciona un reemplazo seguro a las r-herramientas de Berkley. SSH es un protocolo que proporciona un seguro, conexión remota a una capa 2 o un dispositivo de la capa 3. Hay dos versiones de SSH: SSH versión 1 y SSH versión 2. Este soporte para la versión de software ambos SSH versión.

- Luego se realizaron configuraciones para mitigar el ataque externo en una red basándonos en IP ACL es una colección secuencial de permiso y niega las condiciones que se aplican a un paquete del IP. El router prueba los paquetes en relación con las condiciones en la ACL, uno por vez. La primera coincidencia determina si el Cisco IOS® Software acepta o rechaza el paquete.

- Para filtrar el tráfico de la red, las ACL controlan si los paquetes ruteados se reenvían o bloquean en la interfaz del router. Su router examina cada paquete para determinar si remitir o caer el paquete basado en los criterios que usted especifica dentro del ACL. Los criterios de ACL incluyen:

    - Dirección de origen del tráfico
    - Dirección de destino del tráfico
    - Protocolo de capa superior

7.3.2.4 LAB - CONFIGURING BASIC RIPV2 AND RIPNG

Topología

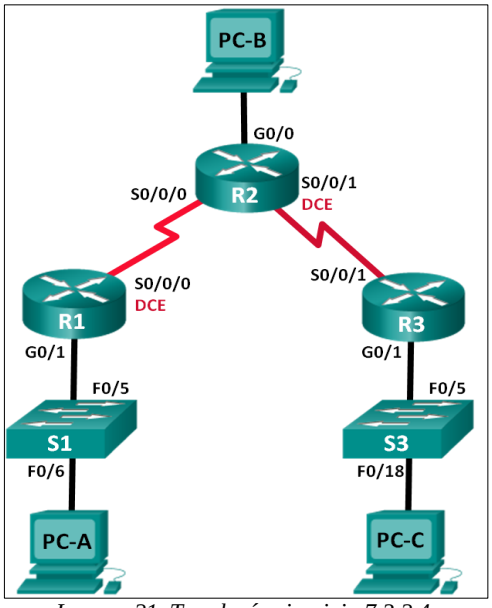


Imagen 21. Topología ejercicio 7.3.2.4.

Objetivo General

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.

Objetivos Específicos

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.

Tabla 2:

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

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.

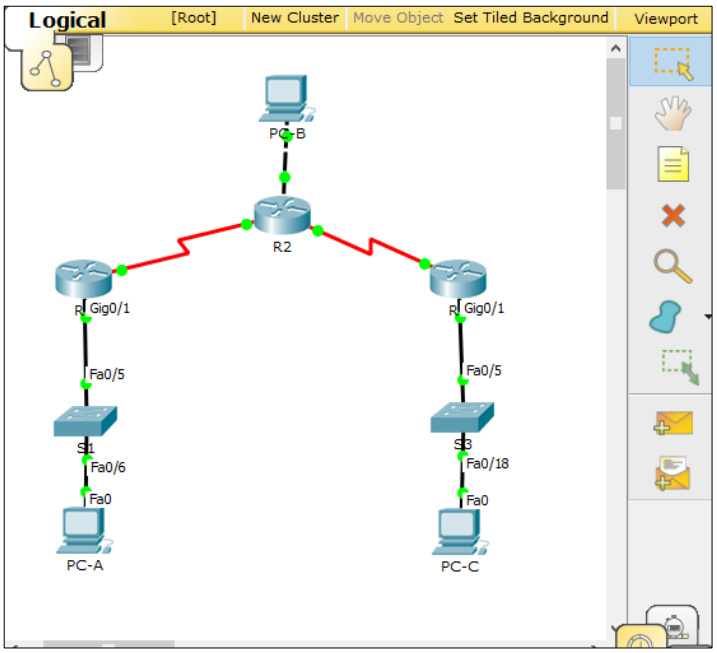


Imagen 22. Implementación de la red.

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. Configurar 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. (banner motd #Unauthroized access to this router is prohibited. #)

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

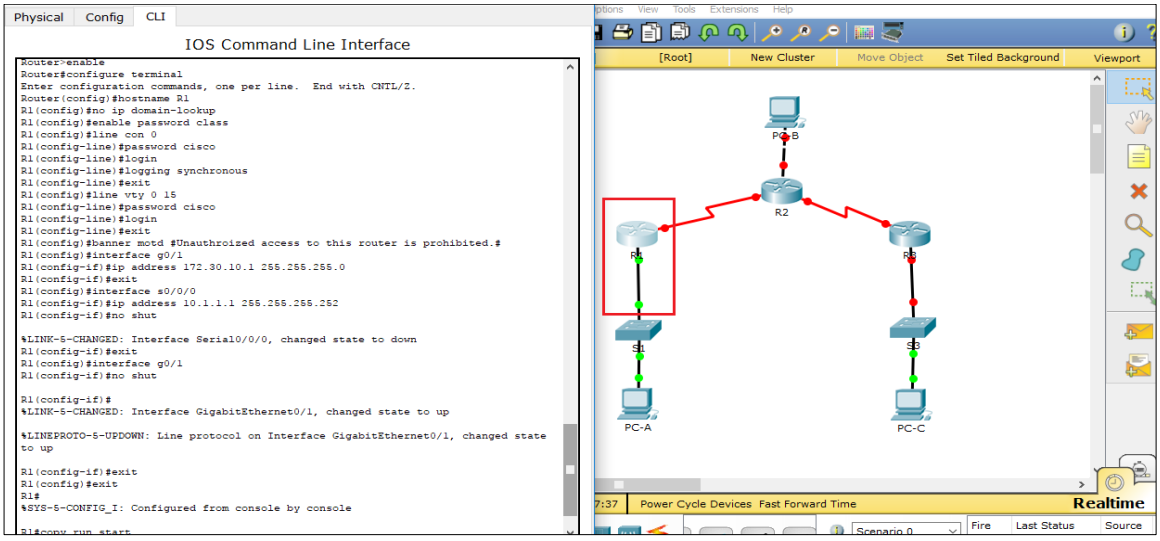


Imagen 23. Configuración R1.

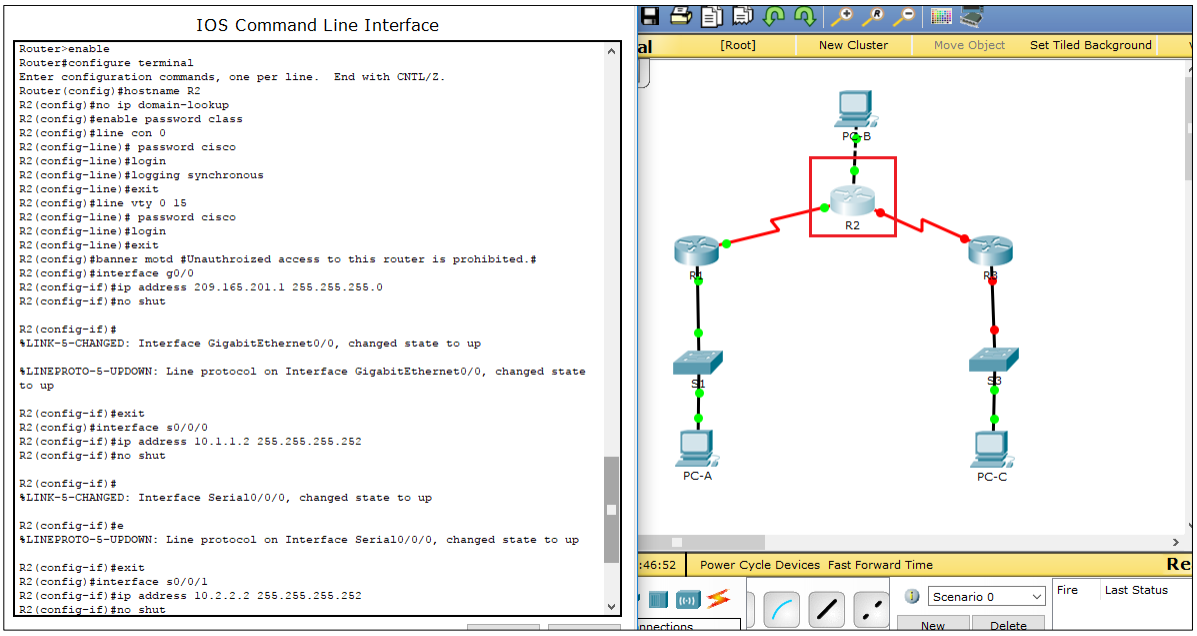


Imagen 24. Configuración R2.

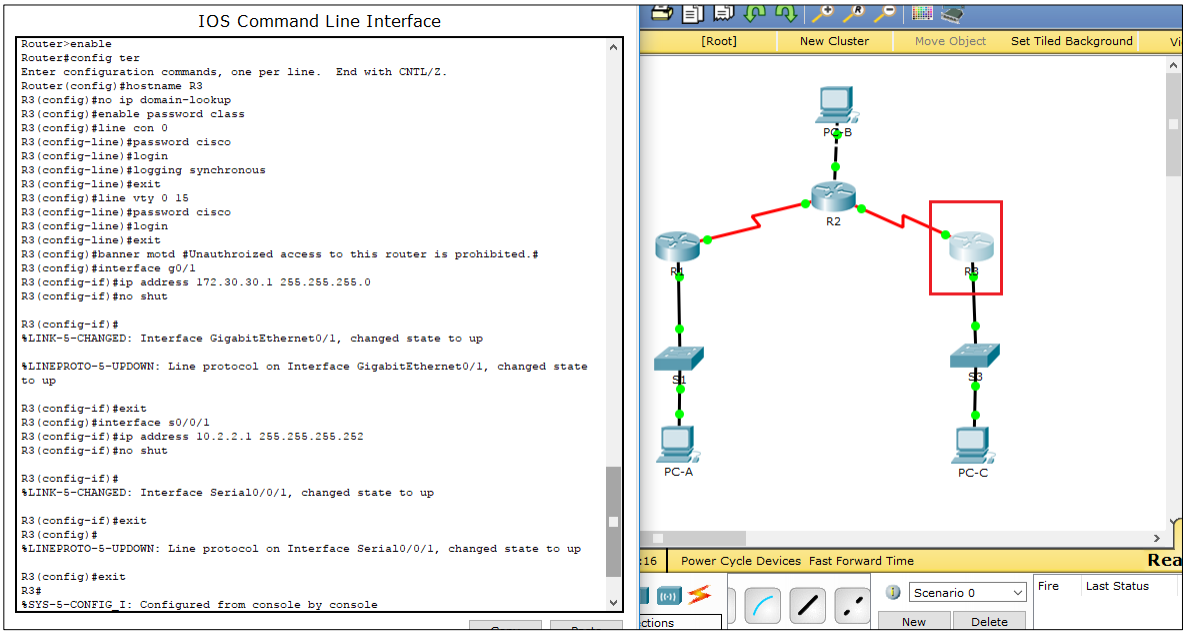


Imagen 25. Configuración R3.

Paso 4. Configurar los equipos host.

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

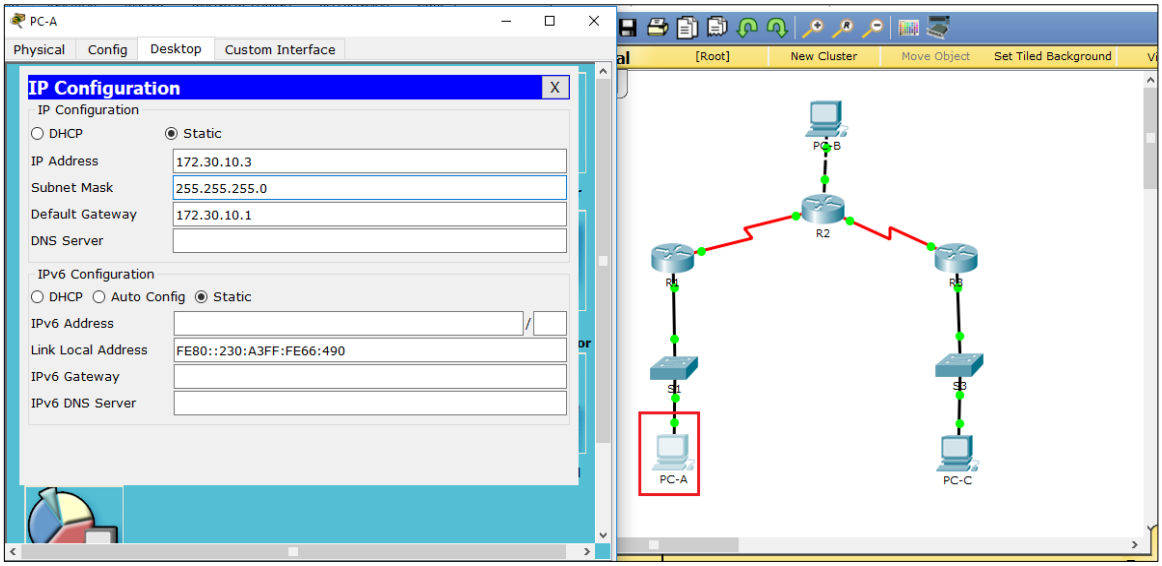


Imagen 26. Configuración PC-A.

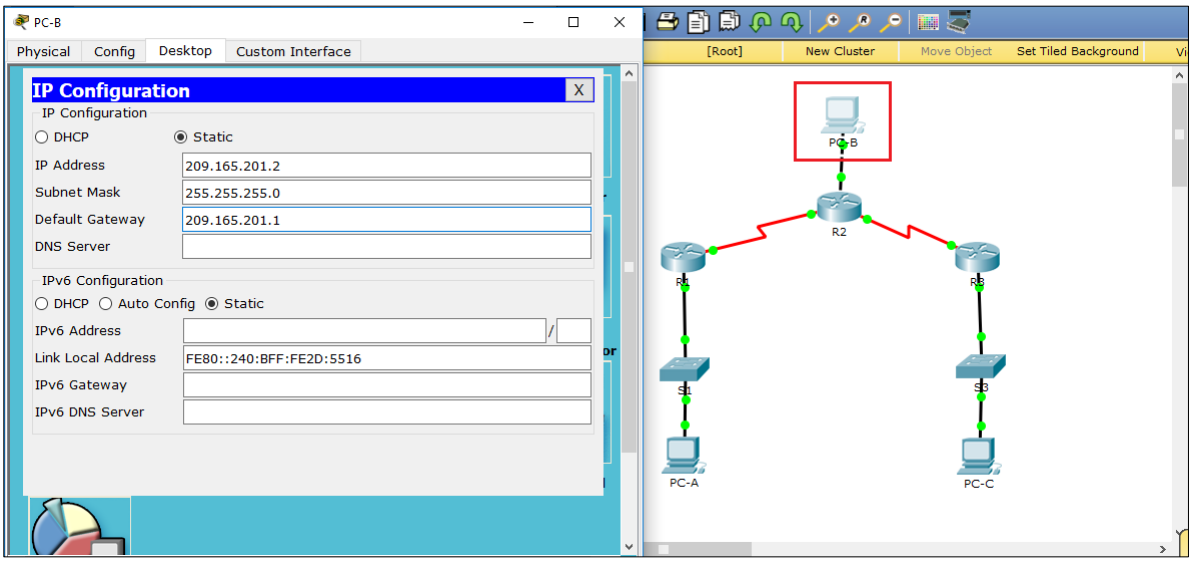


Imagen 27. Configuración PC-B.

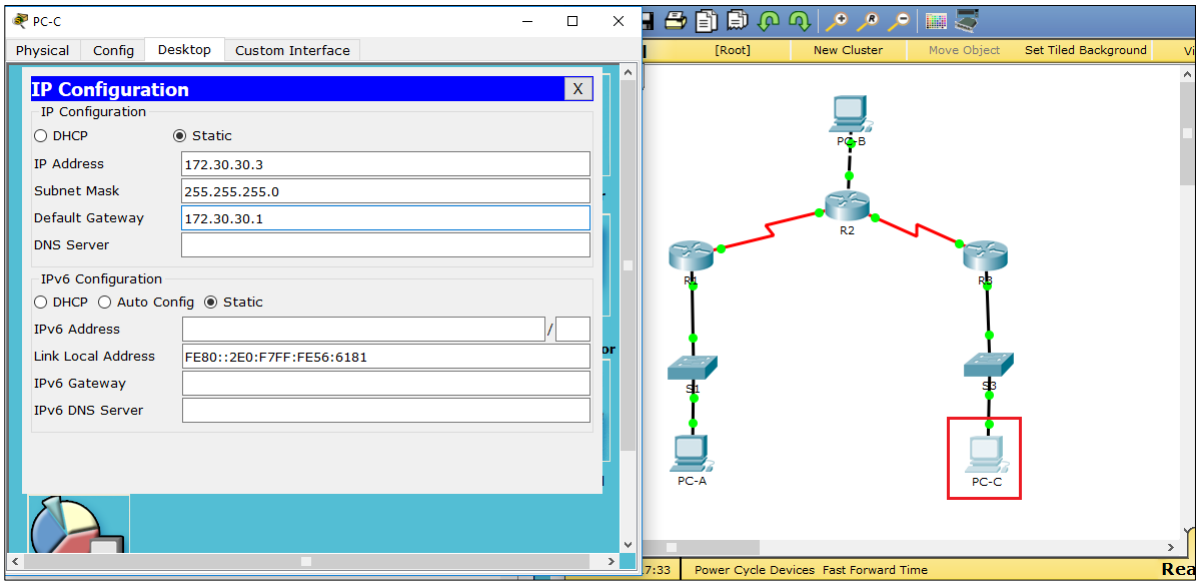


Imagen 28. Configuración PC-C.

Paso 5. Probar la conectividad.

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

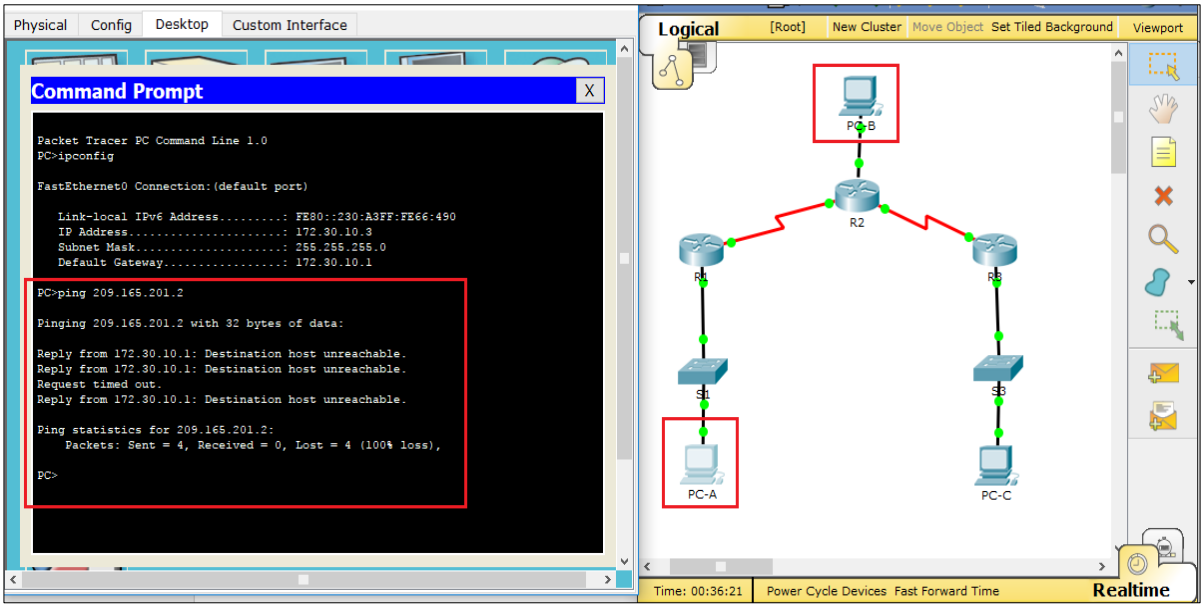


Imagen 29. Ping de PC-A a PC-B.

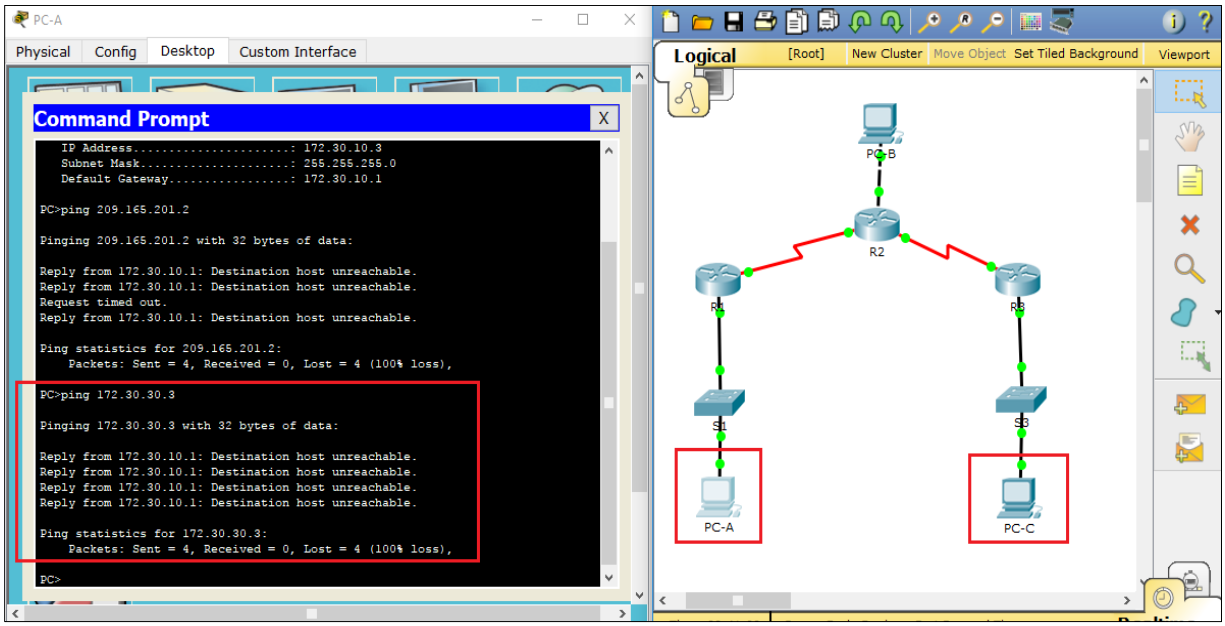


Imagen 30. Ping de PC-A a PC-C.

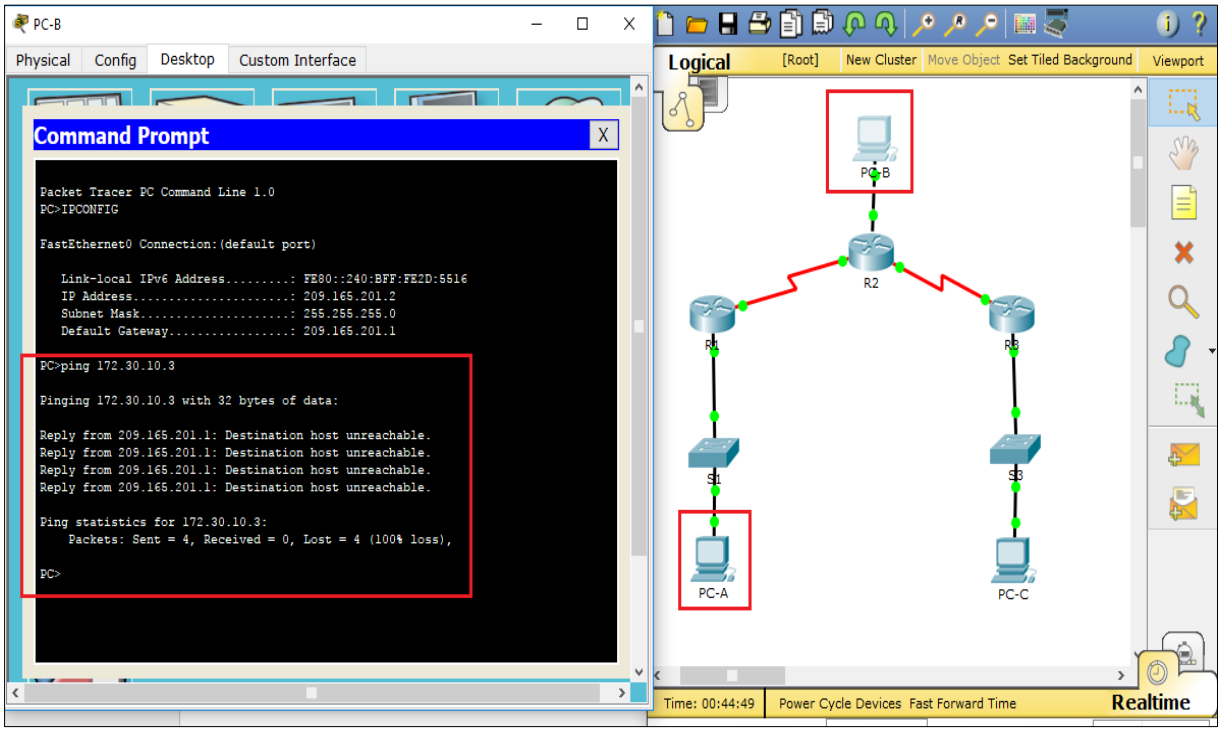


Imagen 31. Ping de PC-B a PC-A.

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

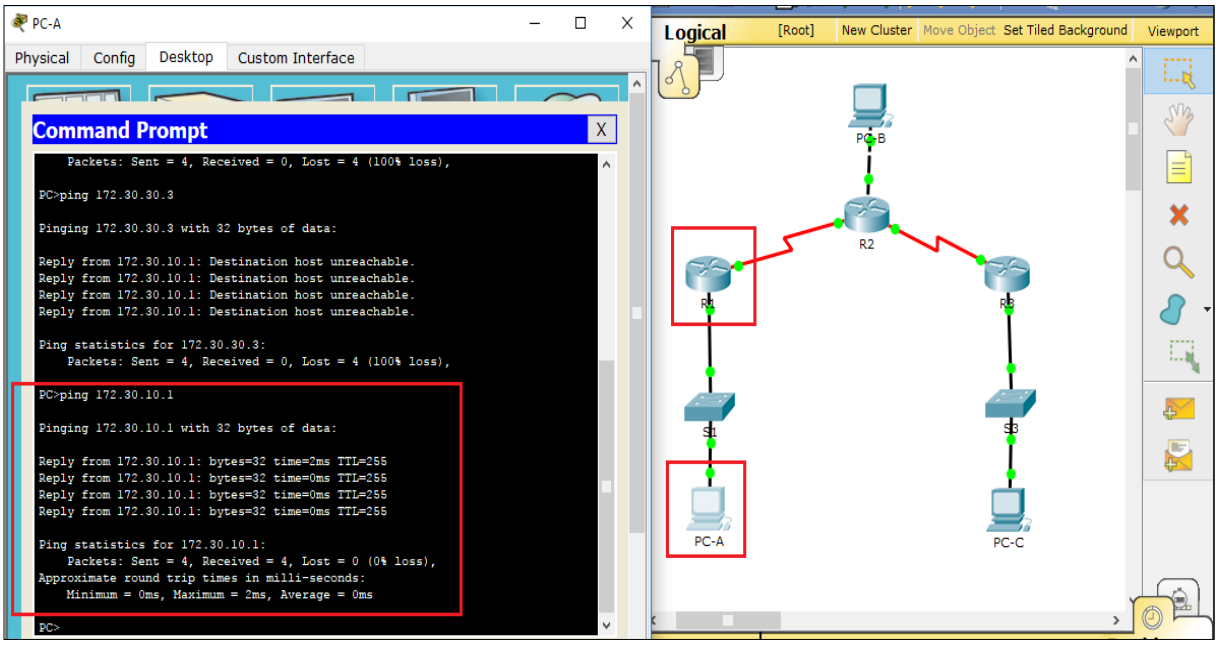


Imagen 32. Ping de PC-A a R1.

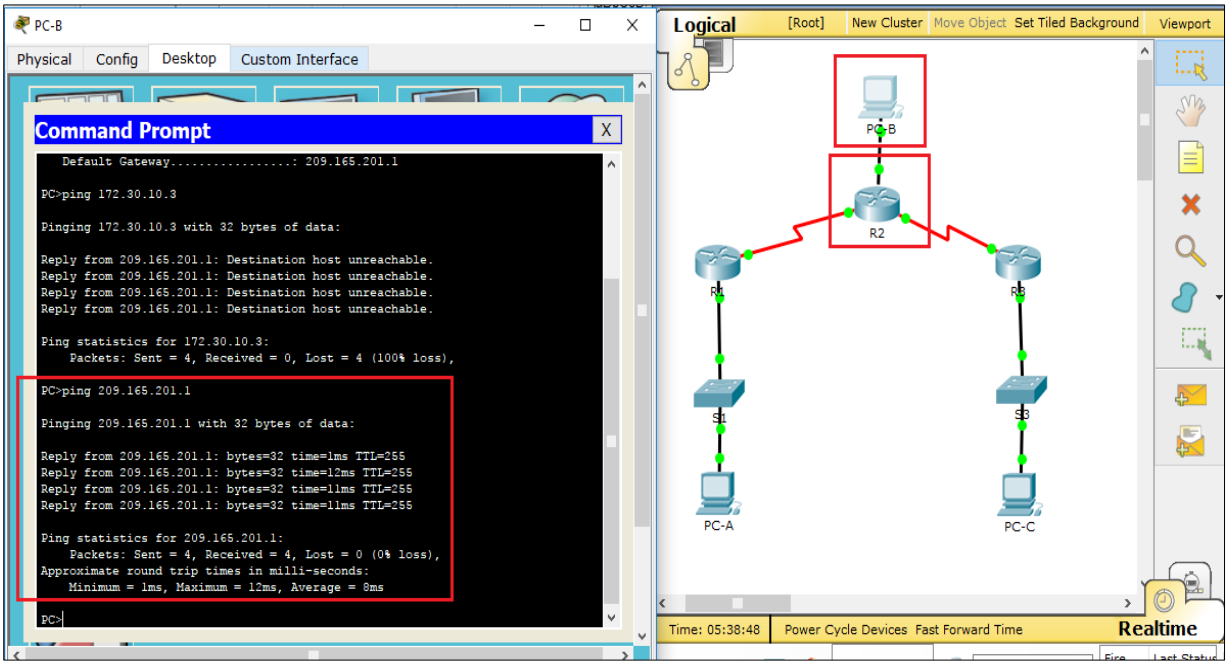


Imagen 33. Ping de PC-B a R2.

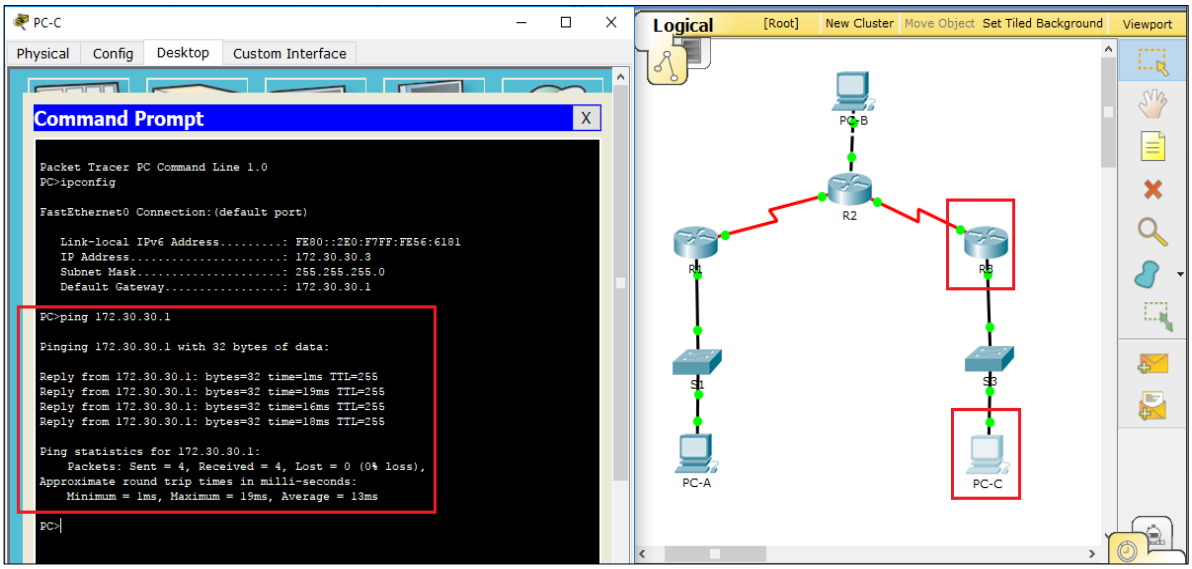


Imagen 34. Ping de PC-C a R3.

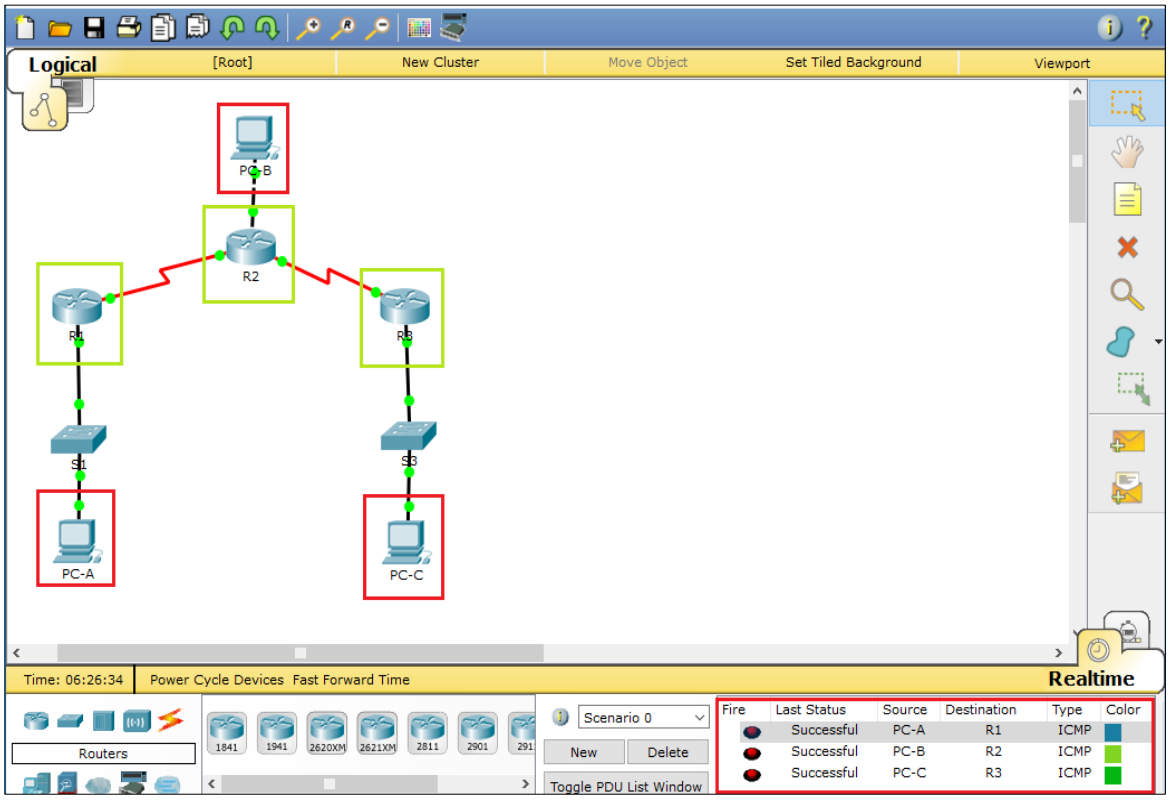


Imagen 35. Prueba de conectividad entre PC´S y Routers.

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

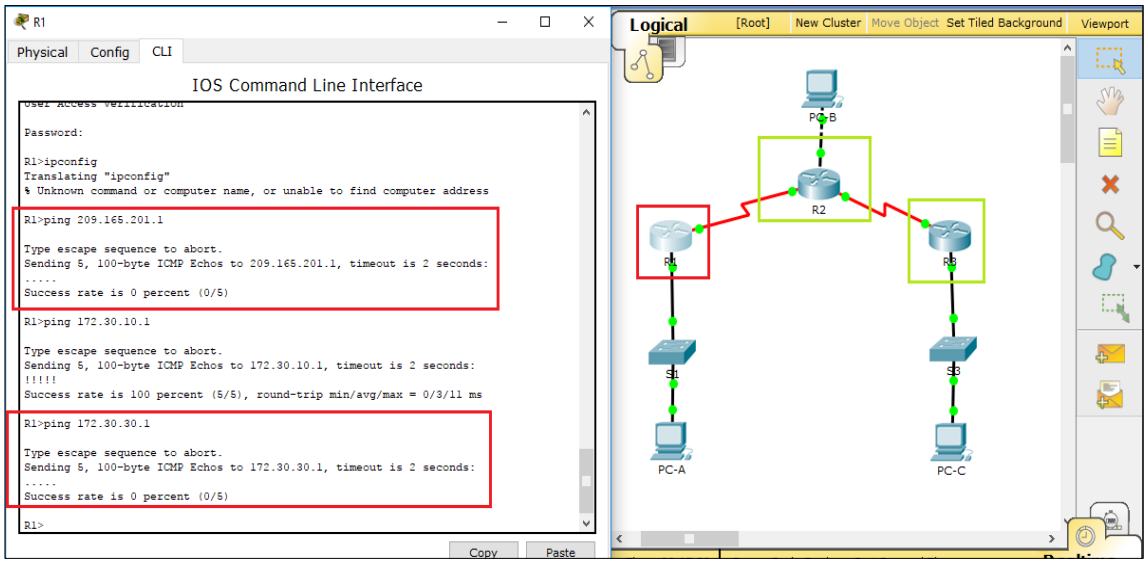


Imagen 36. Ping de R1 a R2 y R3.

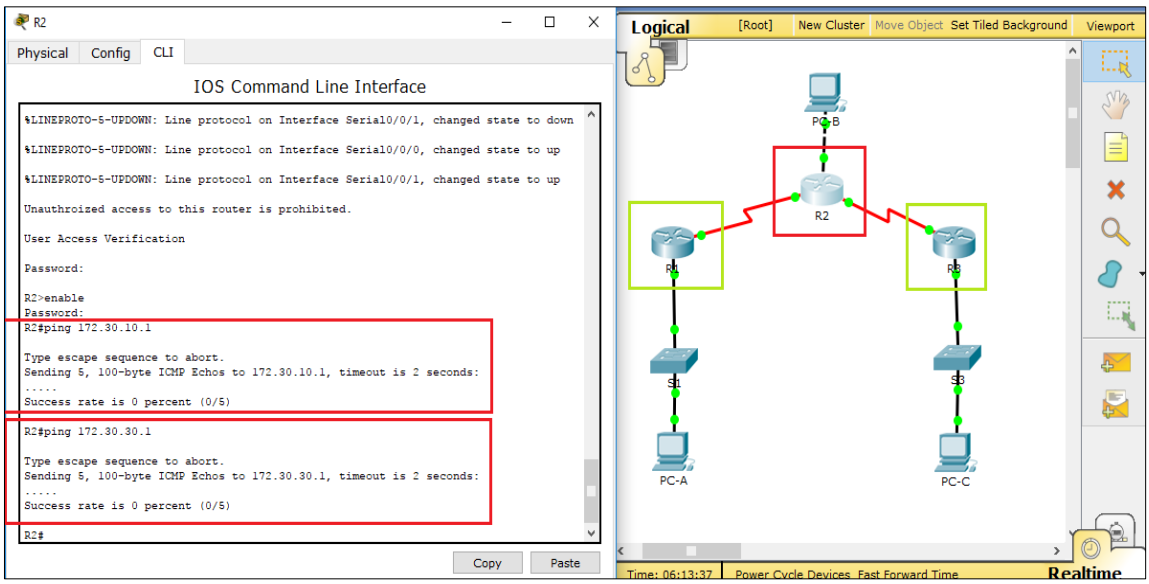


Imagen 37. Ping de R2 a R1 y R3.

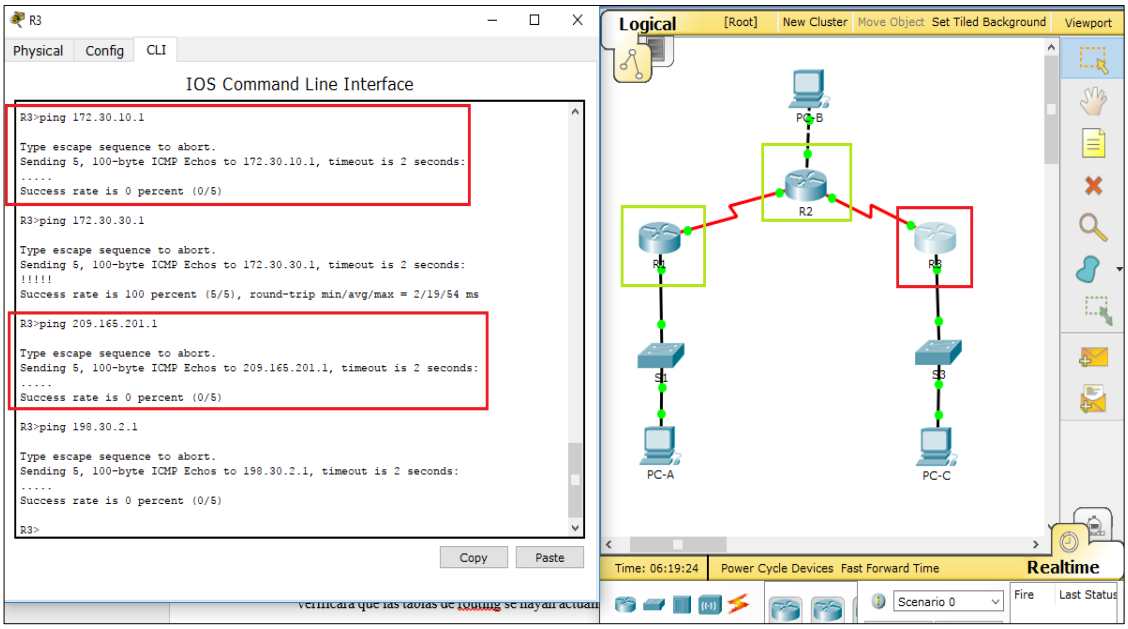


Imagen 38. Ping de R3 a R1 y R2.

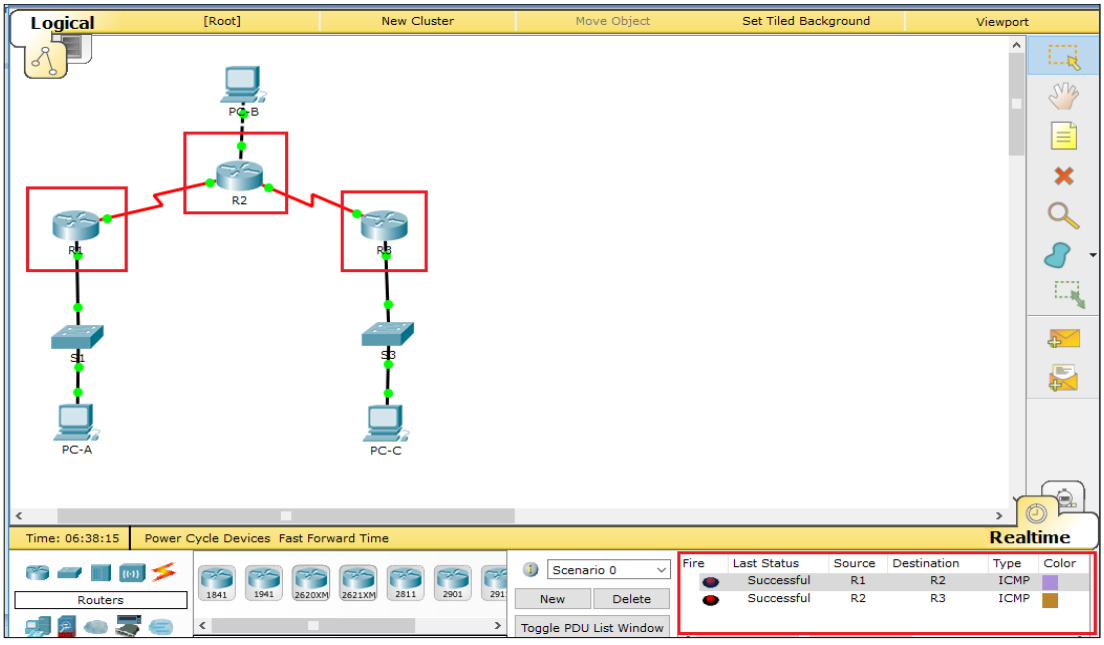


Imagen 39. Prueba de conectividad entre Routers.

Parte 2. Configurar y verificar el routing RIPv2

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

Paso 1. Configurar el enrutamiento RIPv2.

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

R1# ***config t***

R1(config)# ***router rip***

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

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

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

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

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

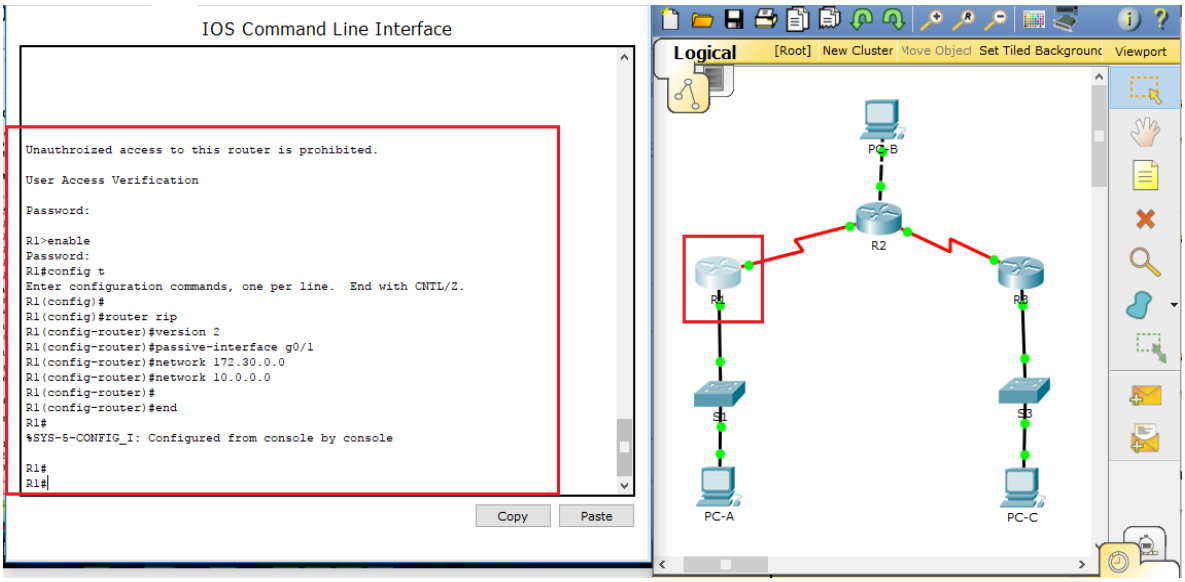


Imagen 40. Configuración del enrutamiento RIPv2.

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

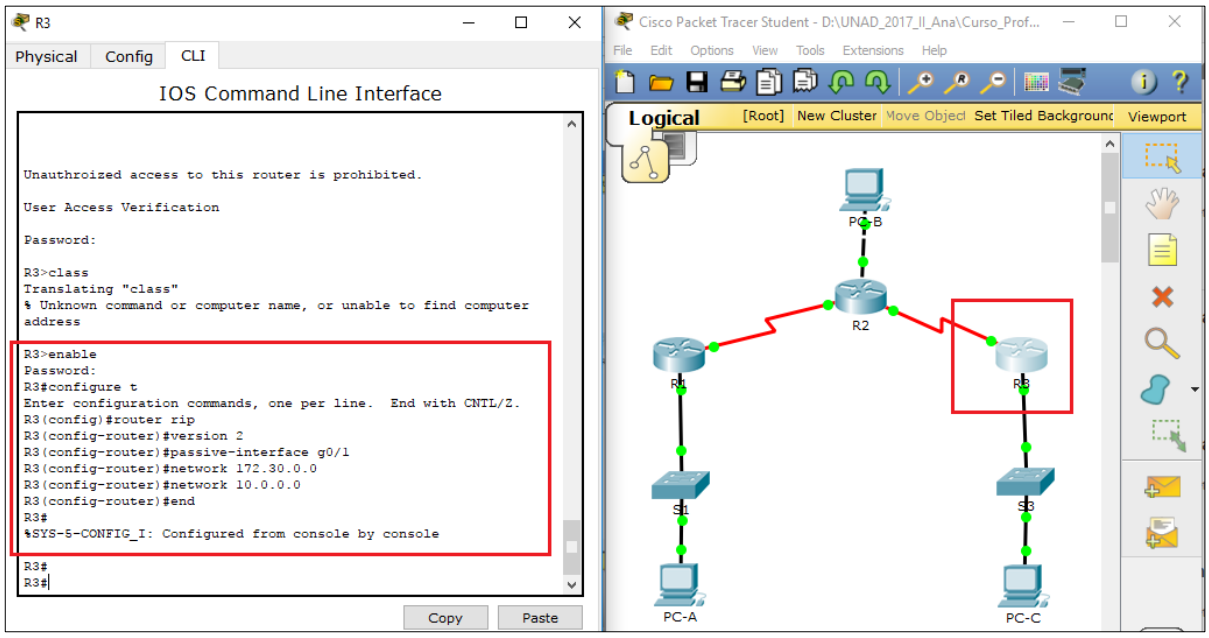


Imagen 41. Configuración del enrutamiento RIPv2 en el R3.

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

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

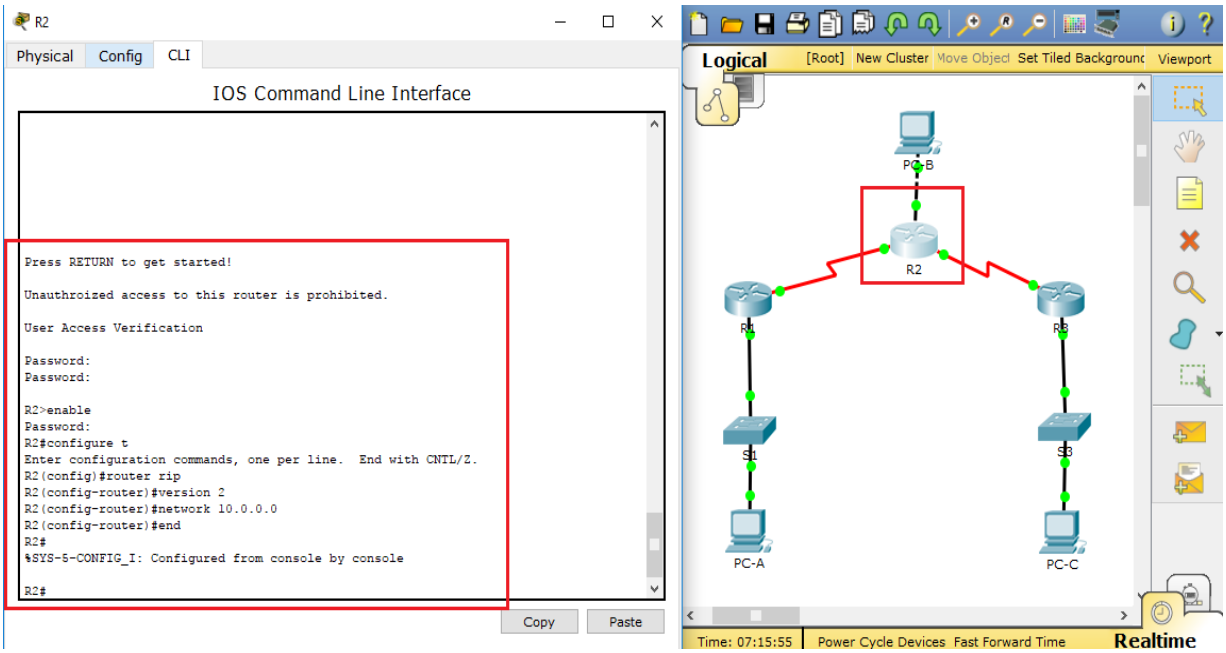


Imagen 42. Configuración del enrutamiento RIPv2 en el R3.

Paso 2. Examinar el estado actual de la red.

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

```
R2# show ip interface brief

Interface                  IP-Address      OK? Method Status
Protocol

Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down

GigabitEthernet0/0         209.165.201.1   YES manual up                    up

GigabitEthernet0/1         unassigned      YES unset  administratively down down

Serial0/0/0                10.1.1.2        YES manual up                    up

Serial0/0/1                10.2.2.2        YES manual up                    up
```

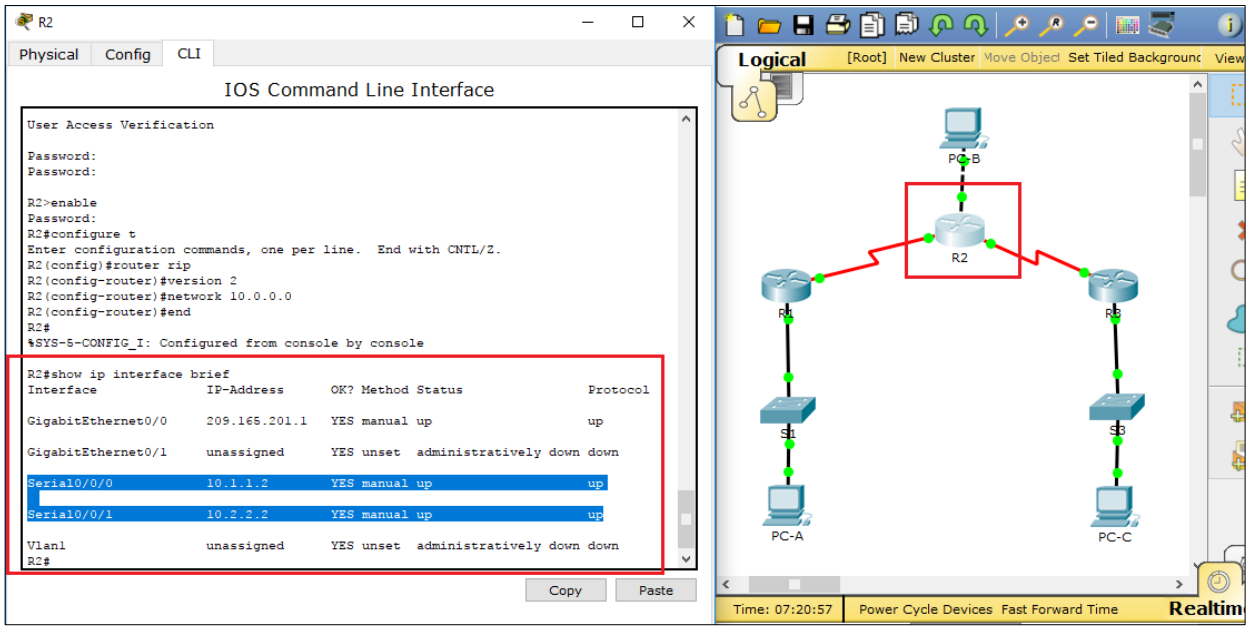


Imagen 43. Examinando el estado actual de la red.

b. Verifique la conectividad entre las computadoras.

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

Respuesta: No hay una ruta que llegue a PC-B esa red no está participando en RIP

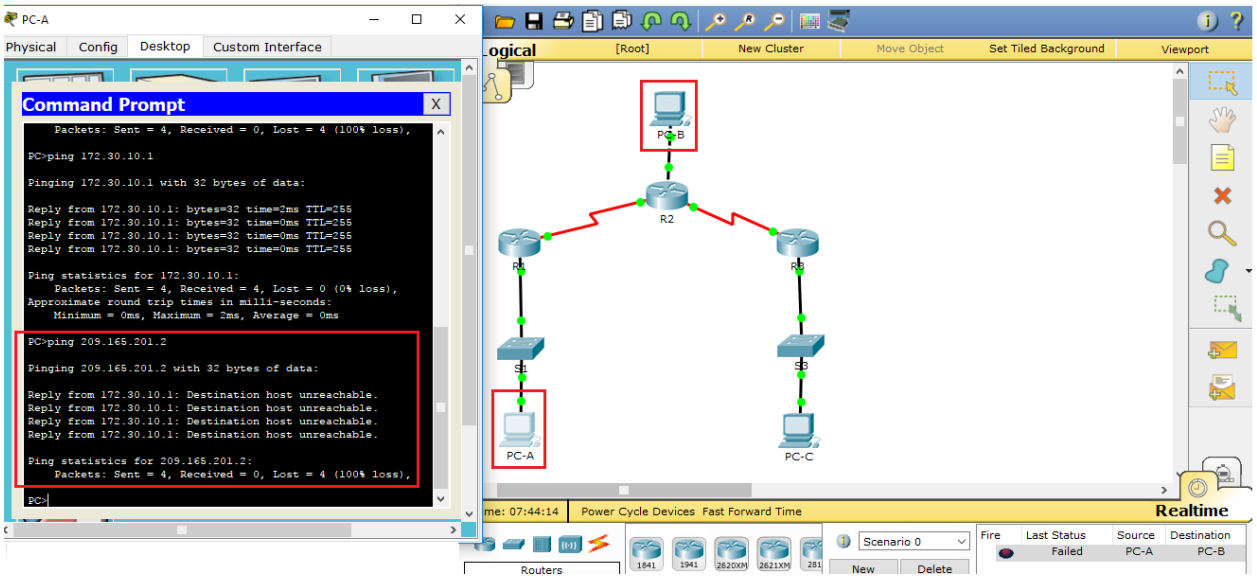


Imagen 44. Ping de la PC-A a la PC-B.

¿Es posible hacer ping de la PC-A a la PC-C? No. ¿Por qué?

Respuesta: R1 y R3 no tiene rutas hacia la subnets específica en el router remoto. No hay una ruta para la subnets del Router remoto.

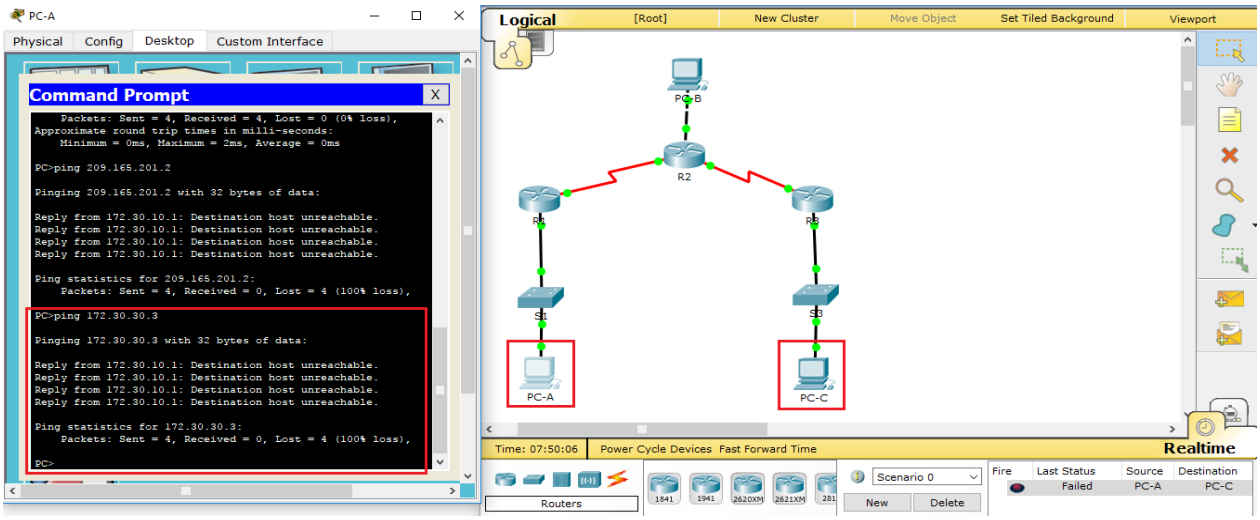


Imagen 45. Ping de la PC-A a la PC-C.

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

Respuesta: PC-B no participa en RIP, la LAN donde esta PC-B no participa en RIP, no existe una ruta.

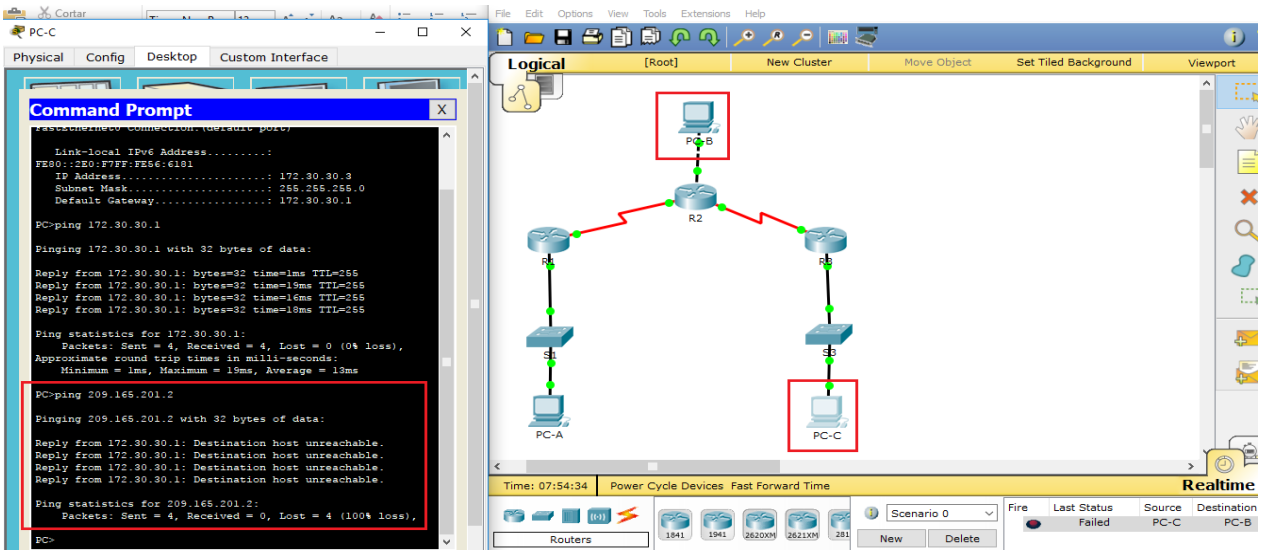


Imagen 46. Ping de la PC-C a la PC-B.

¿Es posible hacer ping de la PC-C a la PC-A? No. ¿Por qué?

Respuesta: R1 y R3 no tienen rutas hacia la subnet específica remota. No hay una ruta RIP específica hacia la subnet.

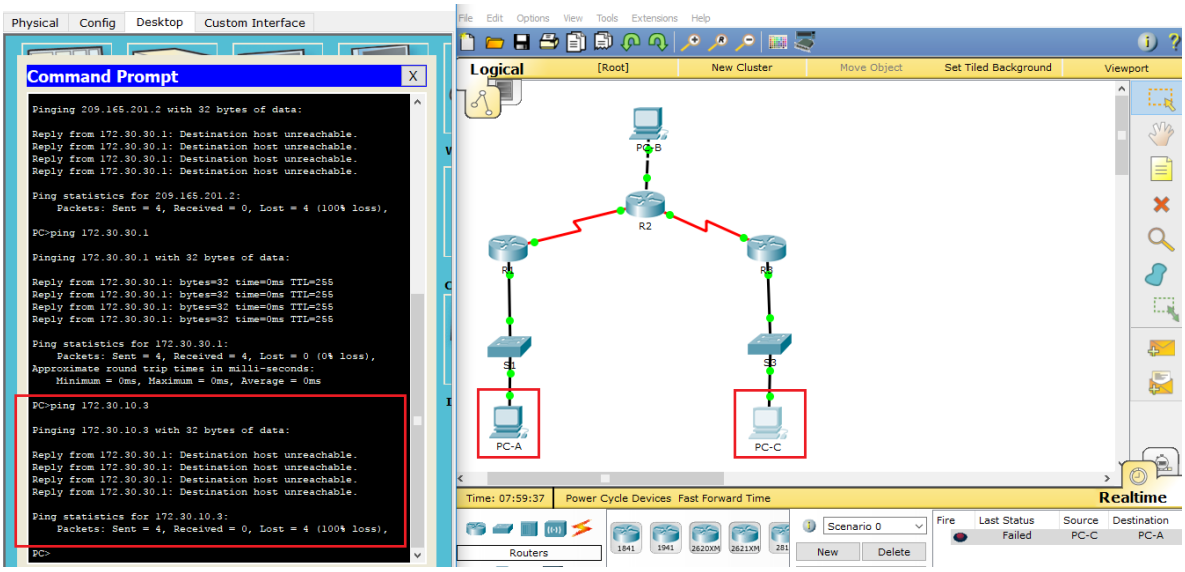


Imagen 47. Ping de la PC-C a la PC-A.

c. Verifique que RIPv2 se ejecute en los routers.

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

```
R1# show ip protocols

Routing Protocol is "rip"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Sending updates every 30 seconds, next due in 7 seconds

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

Redistributing: rip

Default version control: send version 2, receive 2

  Interface             Send  Recv  Triggered RIP  Key-chain
```

```
  Serial0/0/0            2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
    GigabitEthernet0/1
Routing Information Sources:
  Gateway          Distance      Last Update
  10.1.1.2               120
Distance: (default is 120)
```

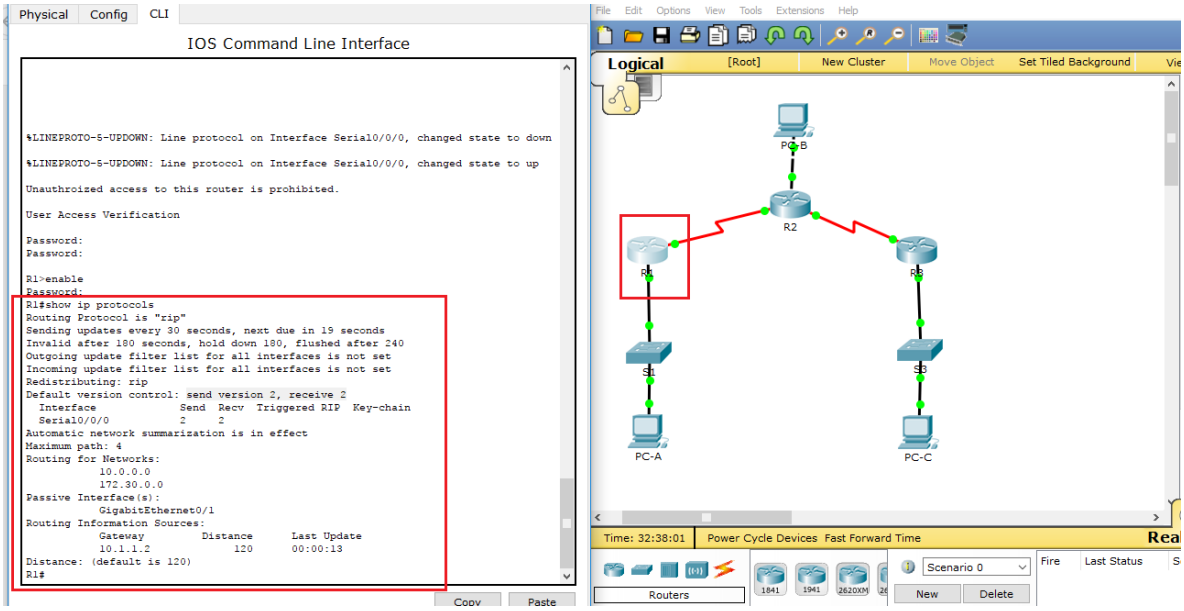


Imagen 48. Verificación de que RIPv2 se está ejecutando ejecute en R1.

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

R//- Este nos muestra las rutas en ejecución. Muestra los mensajes de actualización que envía y recibe el RIP, a través de: R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0.

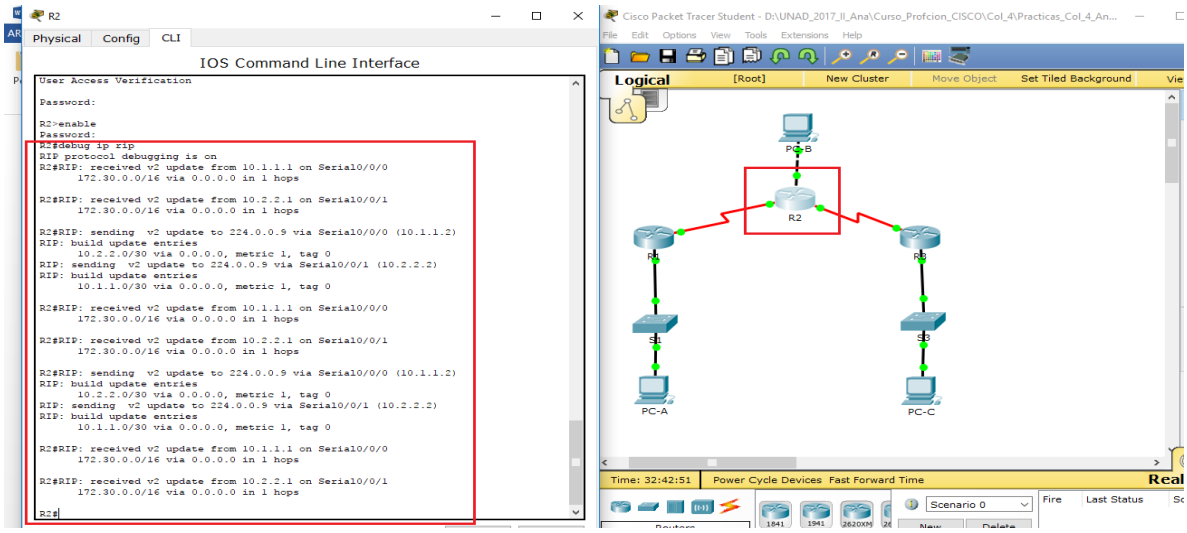


Imagen 49. Ejecución del comando debug ip rip en el R2.

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

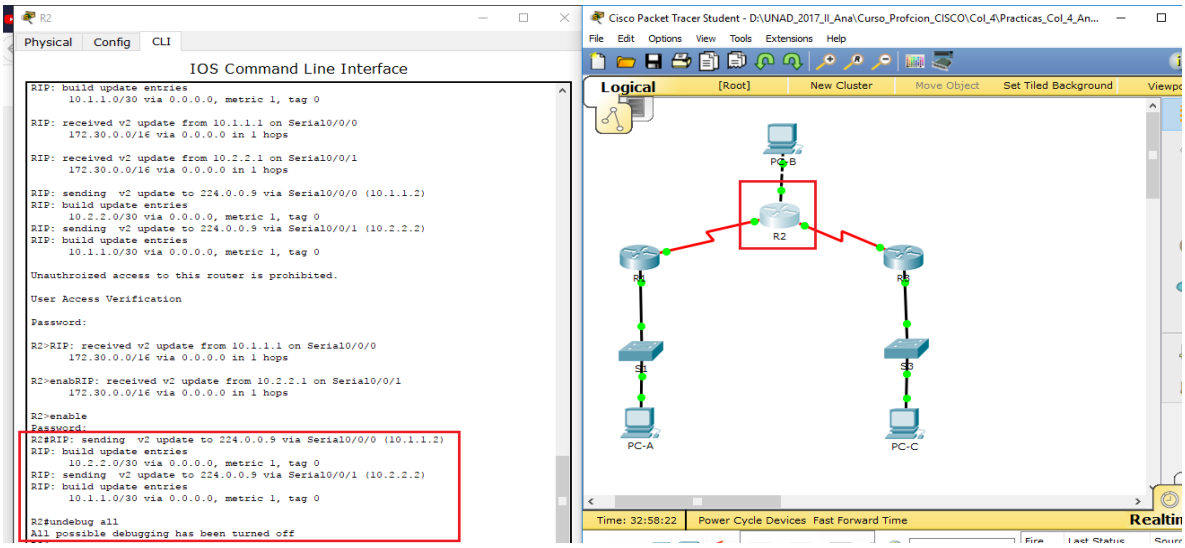


*Imagen 50. Ejecución del comando **undebug all** en la petición de entrada del modo EXEC privilegiado.*

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

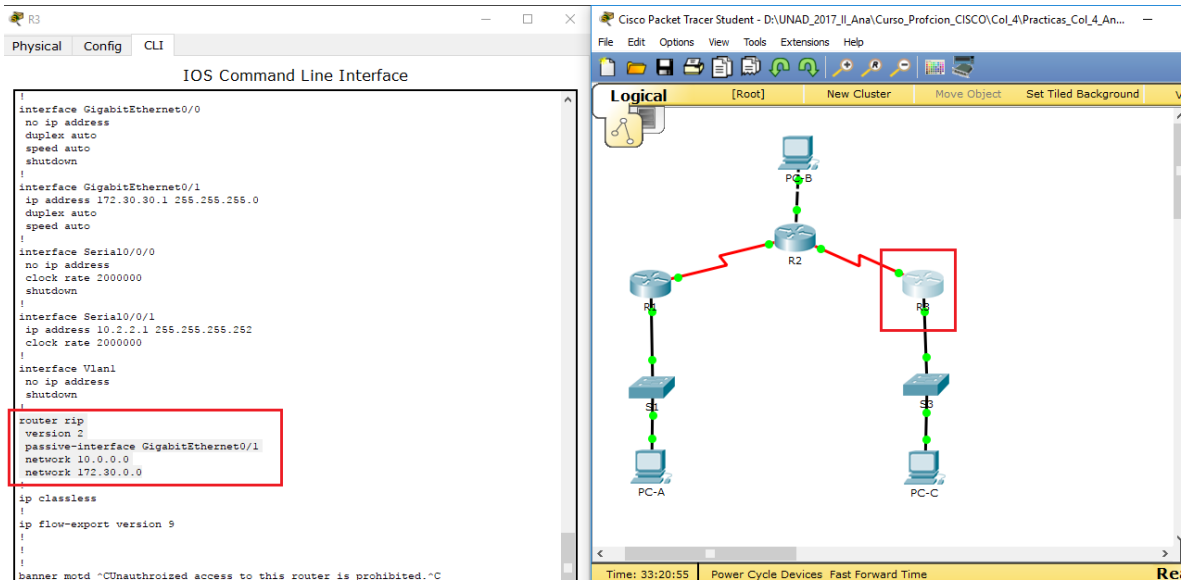


*Imagen 51. Ejecución del comando **show run** en el R3.*

Esta es la información que nos 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

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

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

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

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

R     172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1

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

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

C        209.165.201.0/24 is directly connected, GigabitEthernet0/0

L        209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

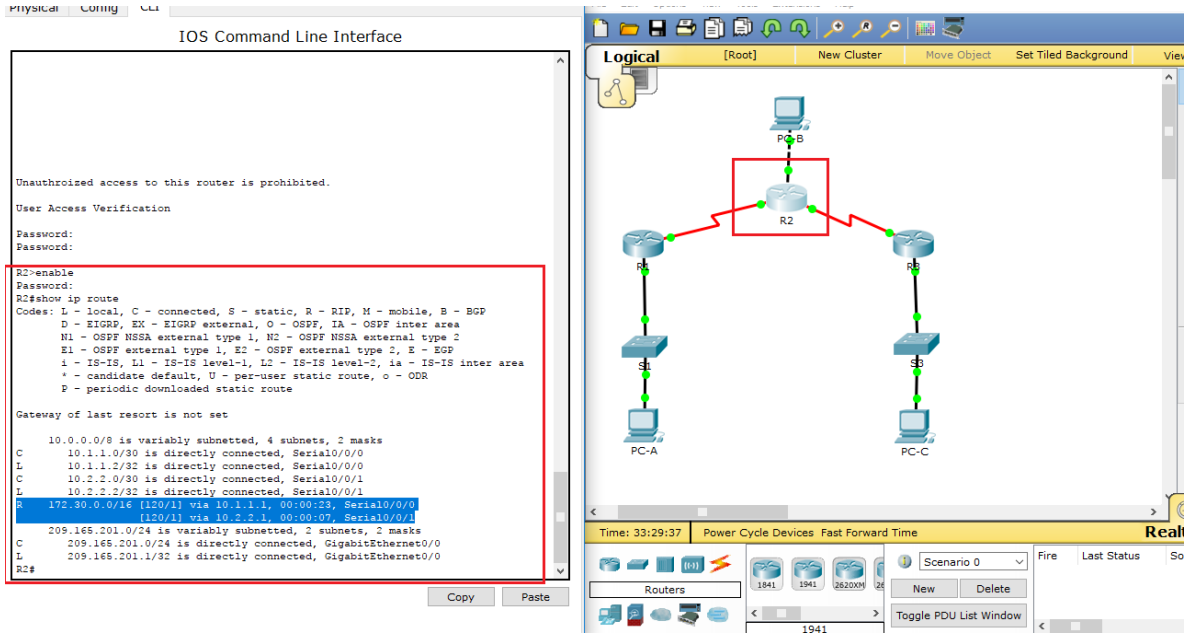


*Imagen 52. Ejecución del comando **show ip route** en el R2.*

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

```
R1# show ip route

<Output Omitted>

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

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

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

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

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

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

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

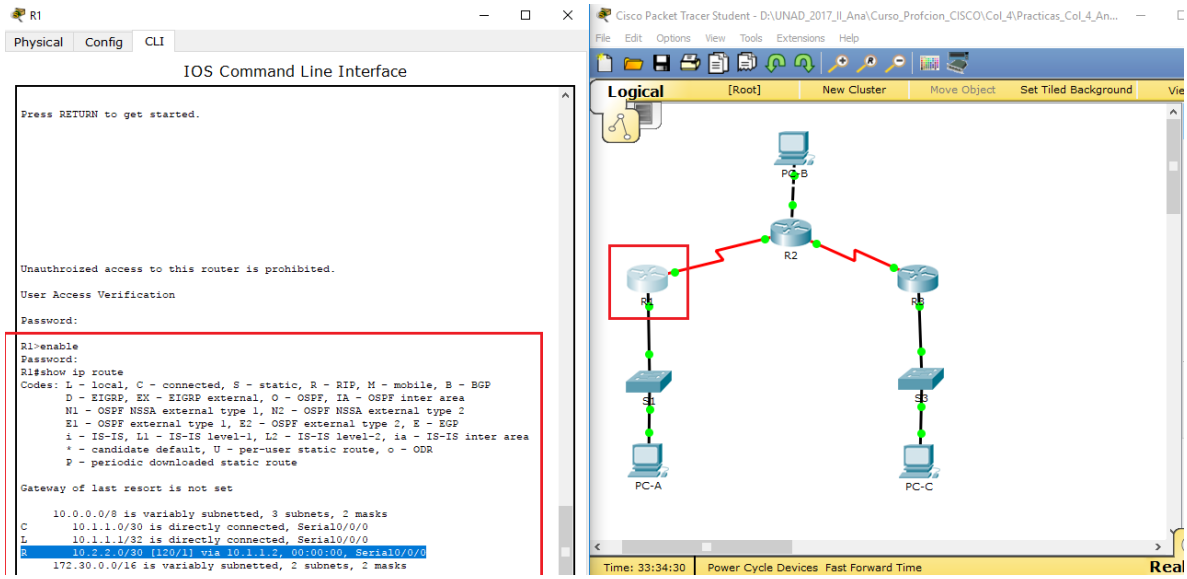


*Imagen 53. Ejecución del comando **show ip route** en el R1.*

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

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

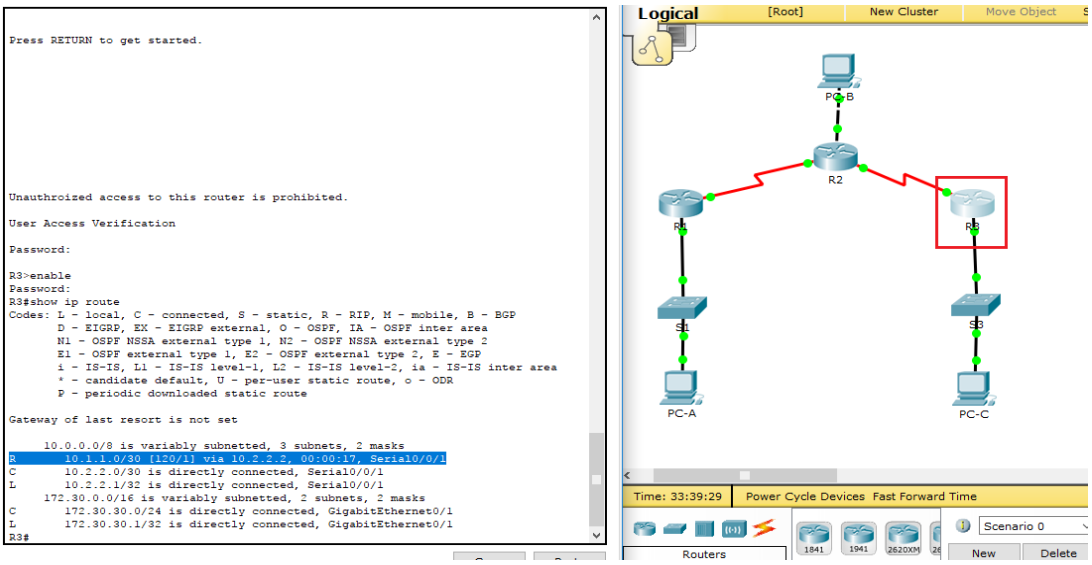


*Imagen 54. Ejecución del comando **show ip route** en el R3.*

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

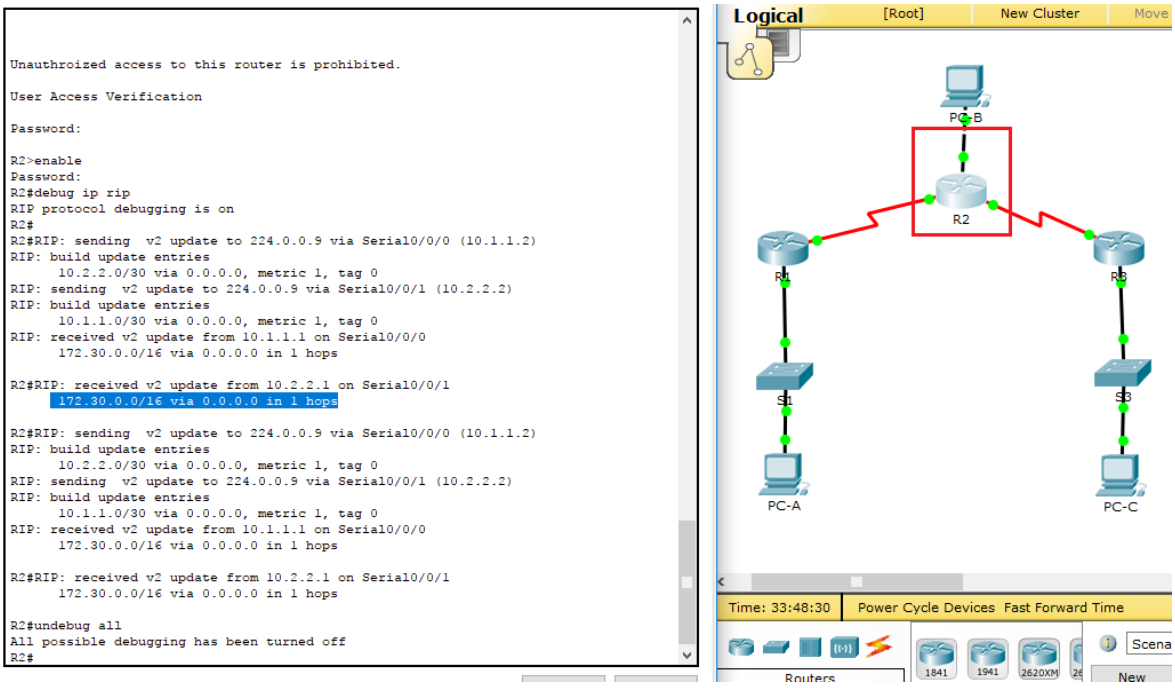


*Imagen 55. Ejecución del comando **debug ip rip en el R2**.*

Las rutas recibidas en las actualizaciones RIP del R3 son:

172.30.0.0/16 via 0.0.0.0 in 1 hops

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

Paso 3. Desactivar la sumarización automática.

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

R1(config)# **router rip**

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

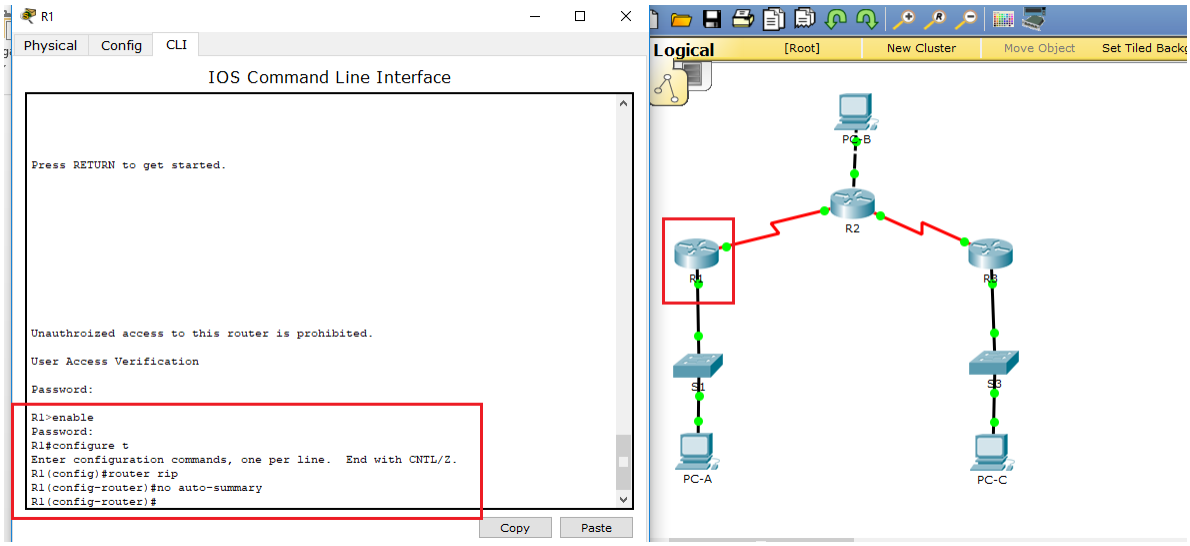


*Imagen 56. Desactivar la **sumarización automática** en el R1.*

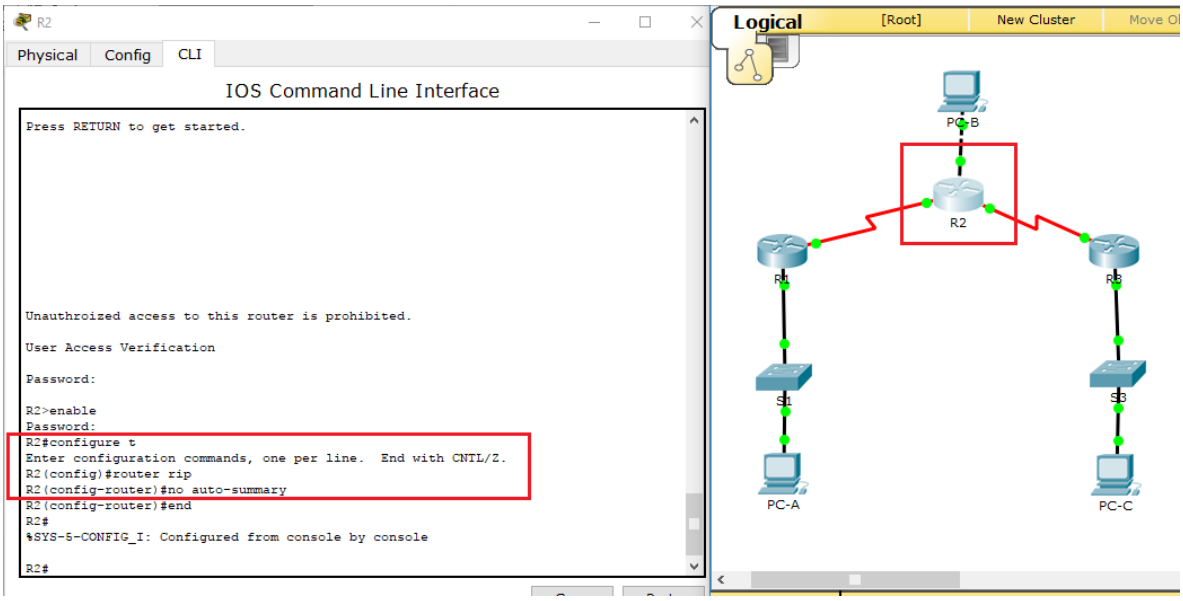


*Imagen 57. Desactivar la **sumarización automática** en el R2.*

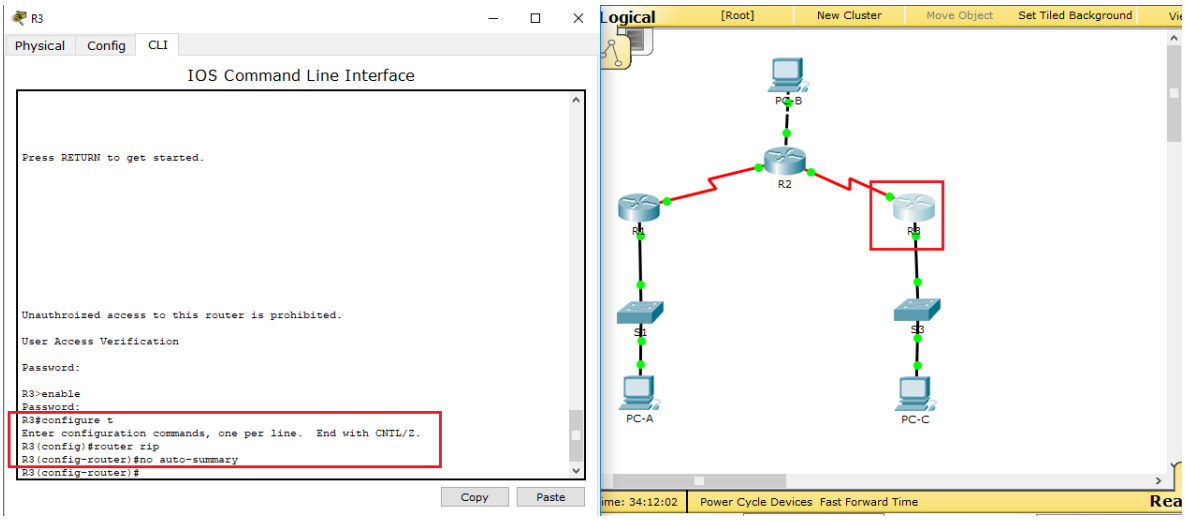


*Imagen 58. Desactivar la **sumarización automática** en el R3.*

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

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

R1# **clear ip route ***

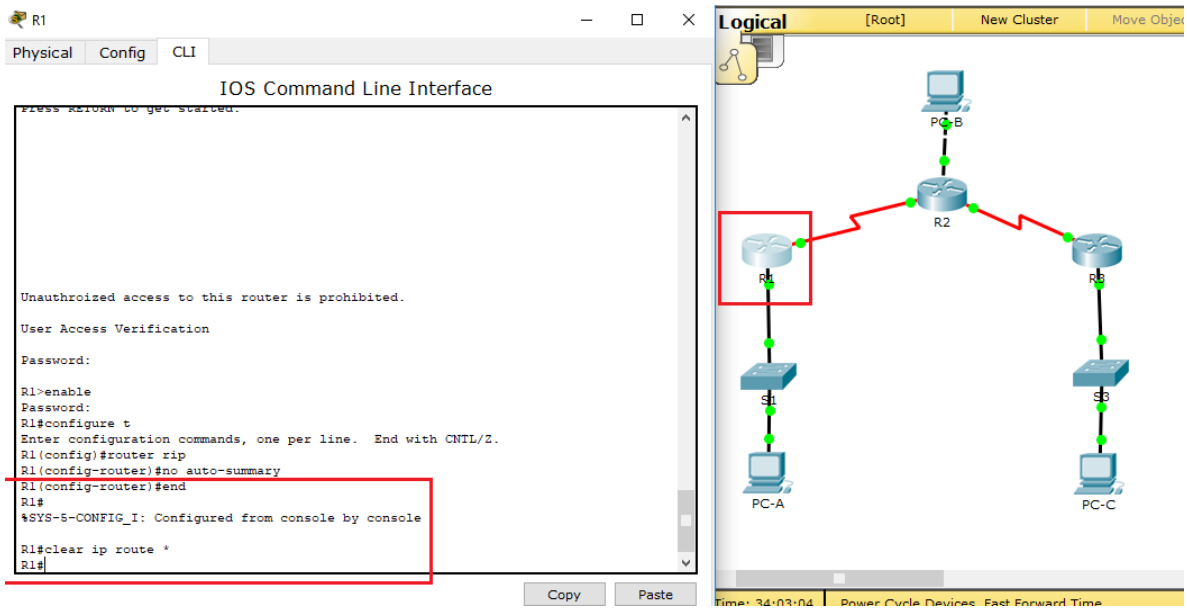


*Imagen 59. Desactivar la **sumarización automática** en el R1.*

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

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

```
R2# show ip route

<Output Omitted>

Gateway of last resort is not set


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

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

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

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

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

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

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

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

```
R        172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0
R        172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04, Serial0/0/1
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/24 is directly connected, GigabitEthernet0/0
L        209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

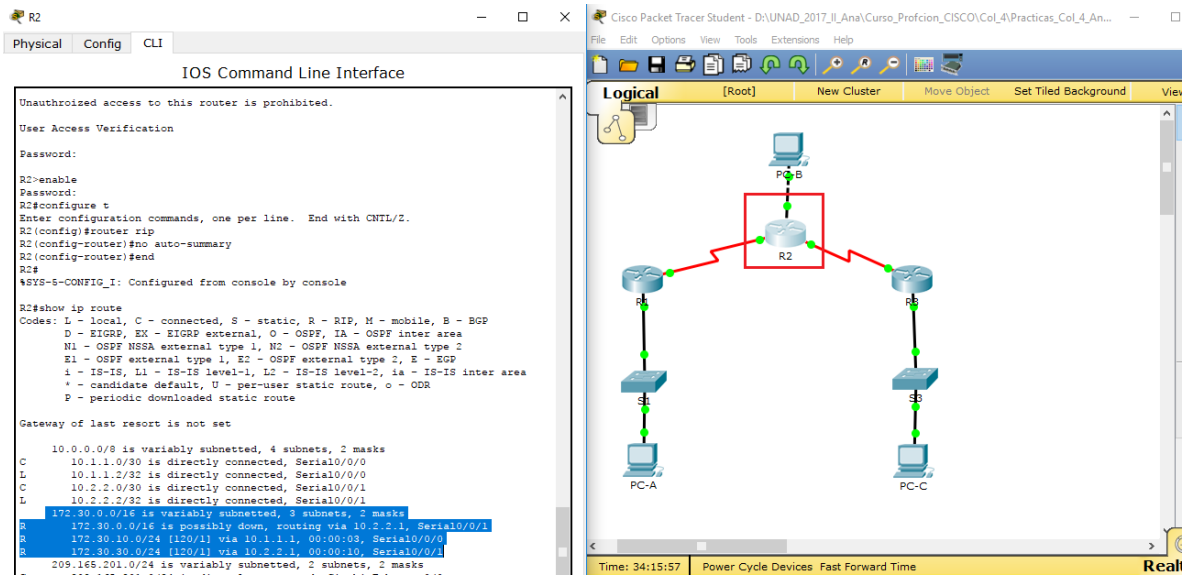


Imagen 60. Tabla de enrutamiento R2.

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

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

```
R        172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0
```

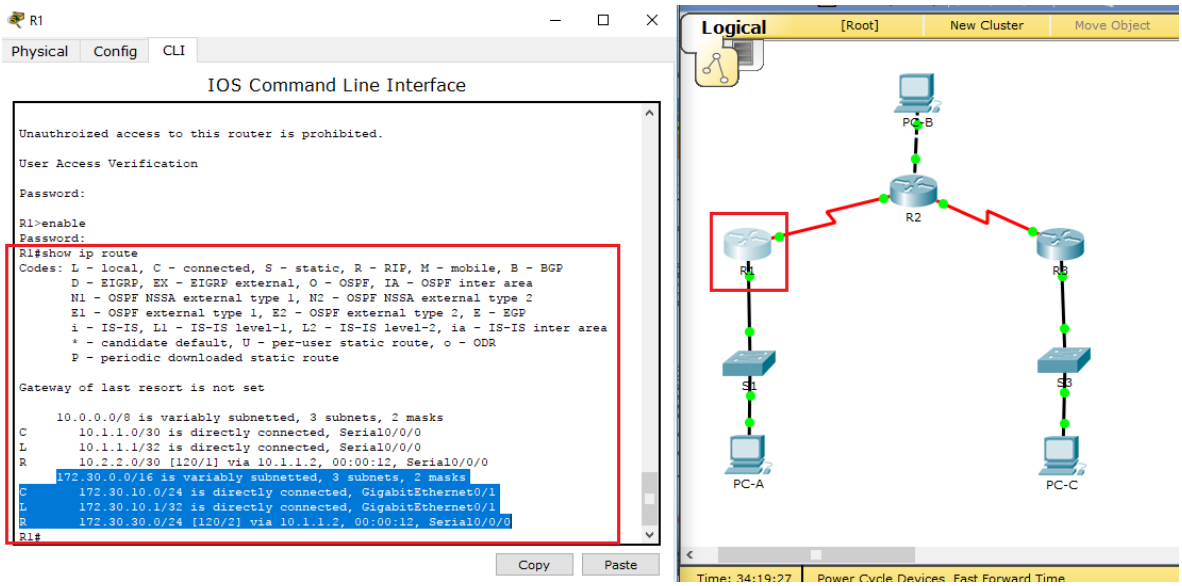


Imagen 61. Tabla de enrutamiento R1.

```
R3# show ip route

<Output Omitted>

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

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

L        10.2.2.1/32 is directly connected, Serial0/0/1

R        10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1

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

C        172.30.30.0/24 is directly connected, GigabitEthernet0/1

L        172.30.30.1/32 is directly connected, GigabitEthernet0/1

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

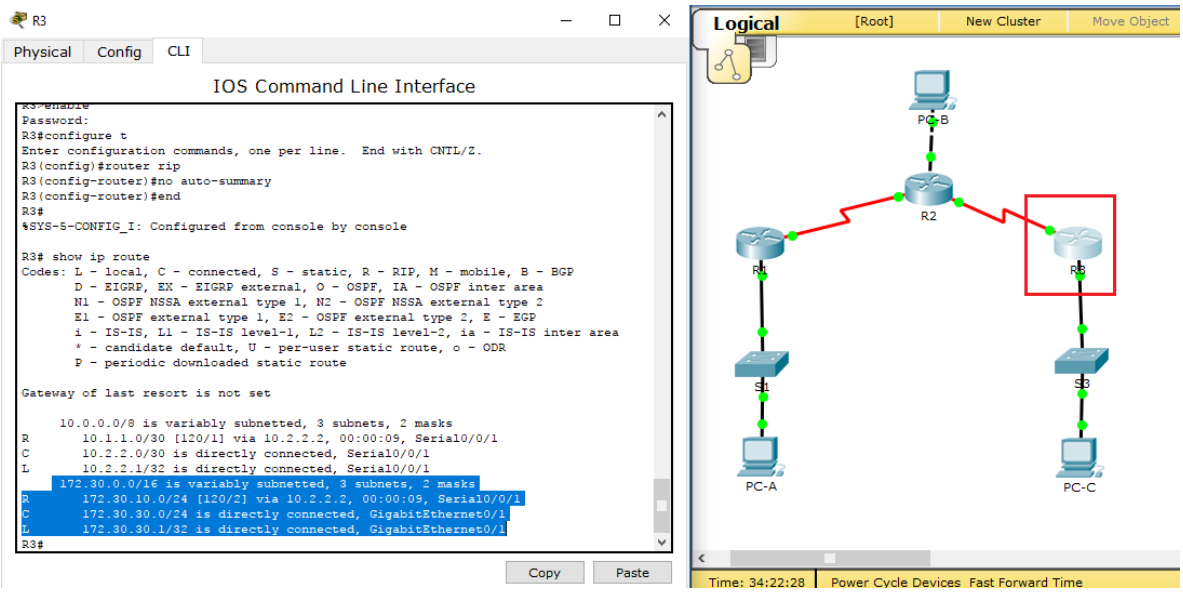


Imagen 62. Tabla de enrutamiento R3.

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

R2# debug ip rip

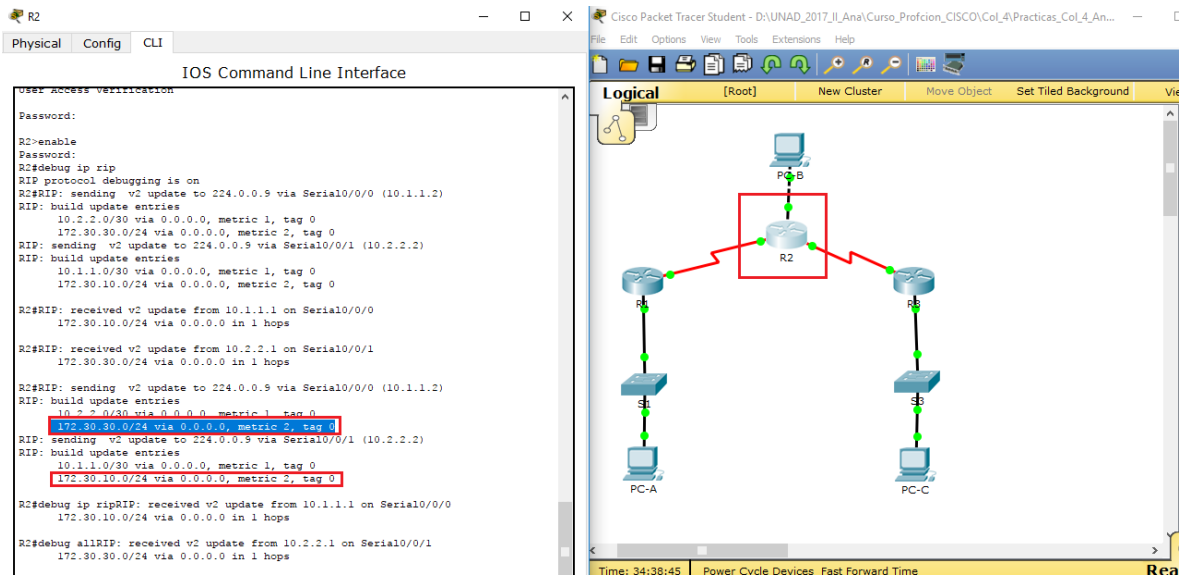


Imagen 63. Implementacion del comando debug ip rip en el R2.

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

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

Respuesta: Las rutas que se reciben del R3 que se encuentran en las actualizaciones RIP son: 172.30.30.0/24 y 172.30.10.0/24 sin clase.

¿Se incluyen ahora las máscaras de las subredes en las actualizaciones de enrutamiento? Respuesta: Si.

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

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

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

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

*R2(config)# **router rip***

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

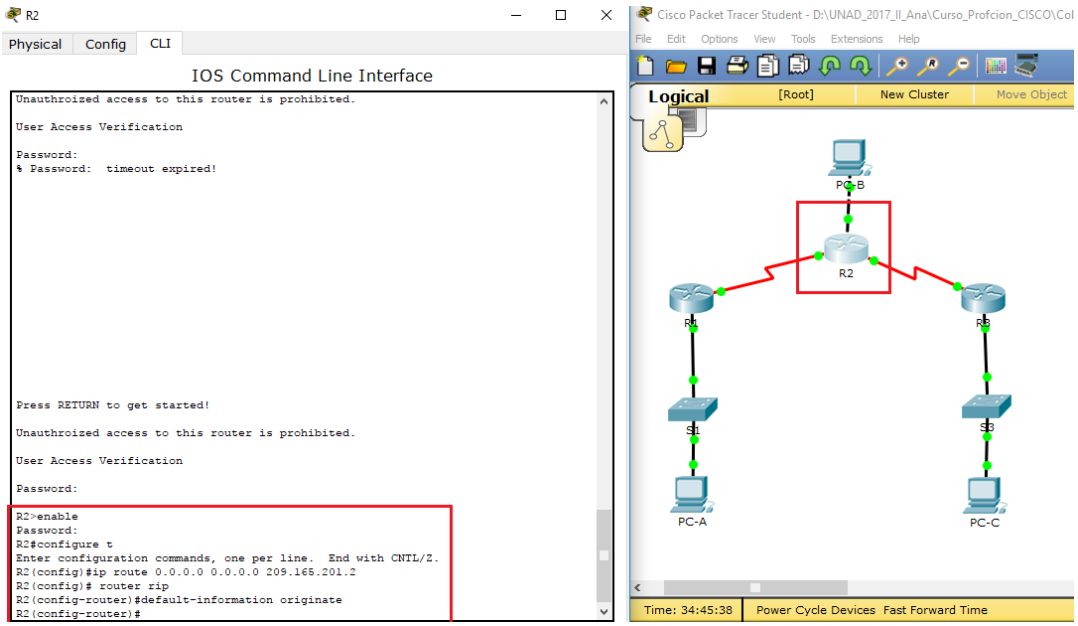


Imagen 64. Configuración y redistribución de una ruta predeterminada para el acceso a Internet en el R2.

Paso 5. Verificar la configuración de enrutamiento.

c. Consulte la tabla de routing en el R1.

```
R1# show ip route

<Output Omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0


R*     0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
       10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C         10.1.1.0/30 is directly connected, Serial0/0/0
L         10.1.1.1/32 is directly connected, Serial0/0/0
R         10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
       172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C         172.30.10.0/24 is directly connected, GigabitEthernet0/1
L         172.30.10.1/32 is directly connected, GigabitEthernet0/1
R         172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0
```

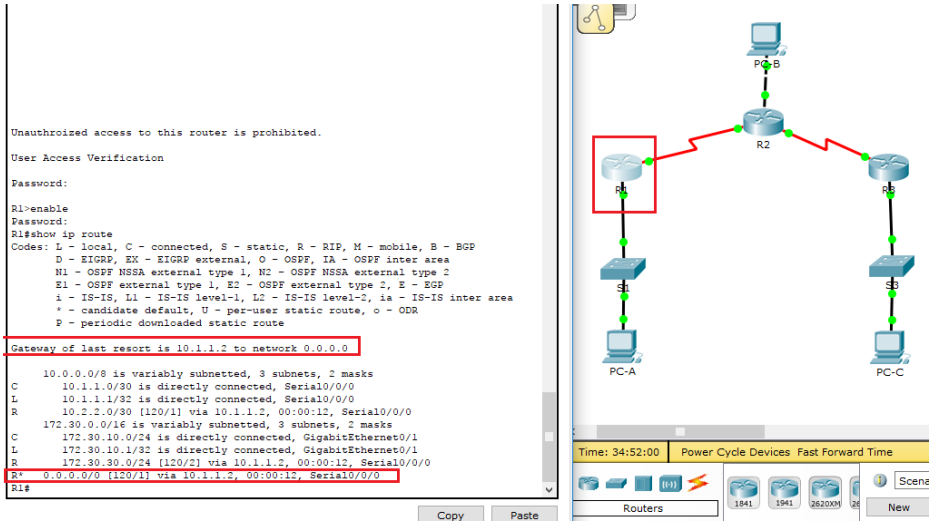


Imagen 65. Tabla de routing en el R1.

¿Cómo se puede saber, a partir de la tabla de routing, que la red dividida en subredes que comparten el R1 y el R3 tiene una ruta para el tráfico de Internet? Respuesta: Debido a que hay un Gateway de ultimo alcance, es decir una puerta de enlace, que nos conecta a internet y la ruta por defecto que se muestra en la tabla de ruteo esta aprendida por RIP.

d. Consulte la tabla de routing en el R2.

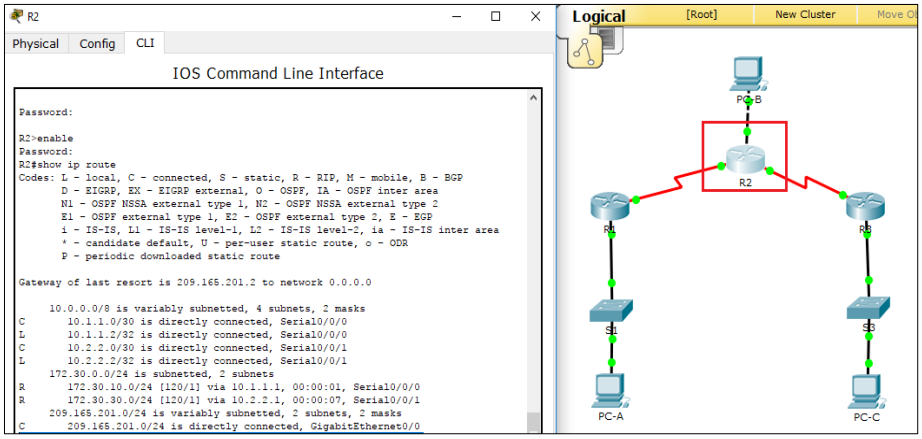


Imagen 66. Tabla de routing en el R2.

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

Respuesta: R2 tiene una ruta estática por defecto a través de la 0.0.0.0 209.165.201.2 que es directamente conectada en la G0/0, tal como se indica en la tabla.

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.

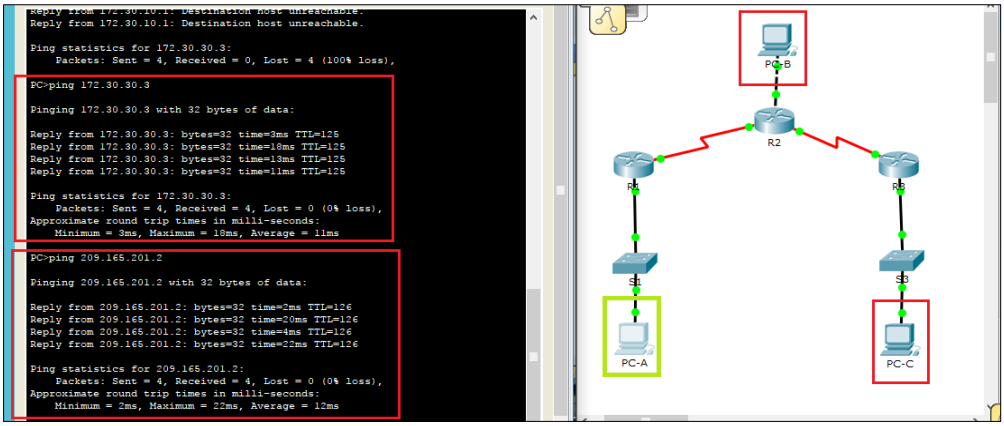


Imagen 67. Ping de PC-A a PC-C a PC-B.

¿Tuvieron éxito los pings? Respuesta: 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.

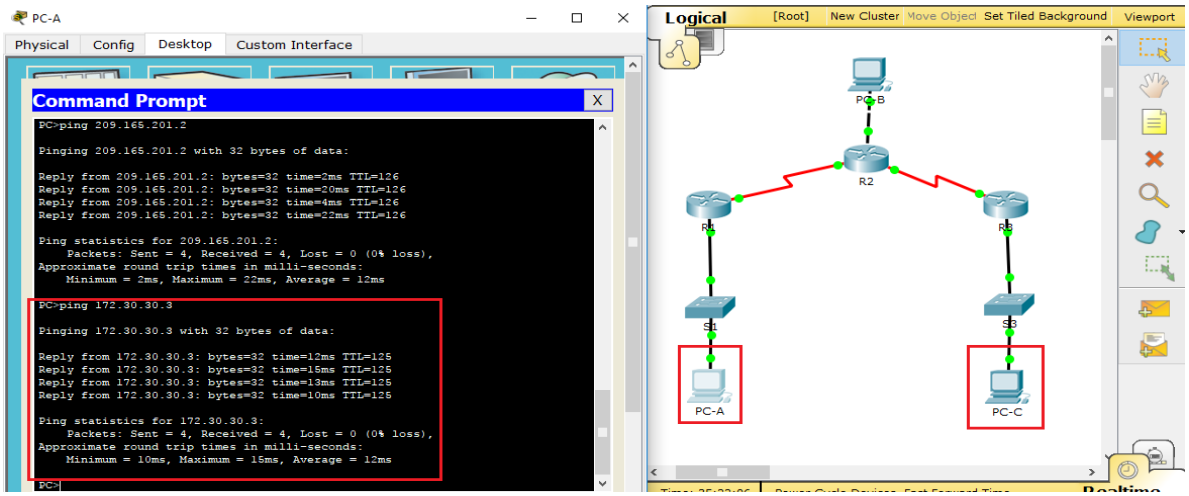


Imagen 68. Ping entre la PC-A y la PC-C.

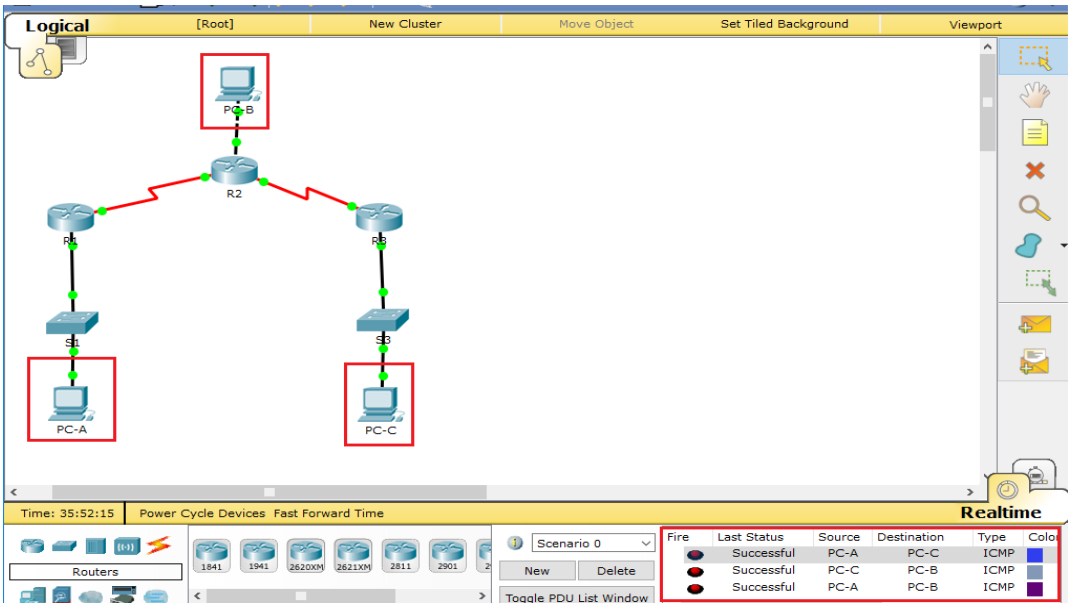


Imagen 69. Ping entre la PC´S.

¿Tuvieron éxito los pings? Respuesta: 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 3:

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.

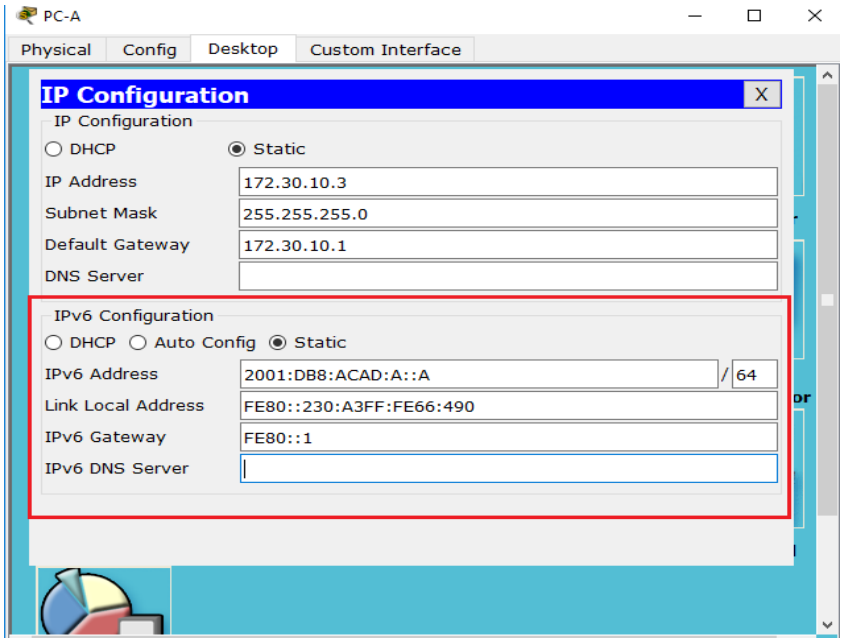


Imagen 70. Configuración PC-A.

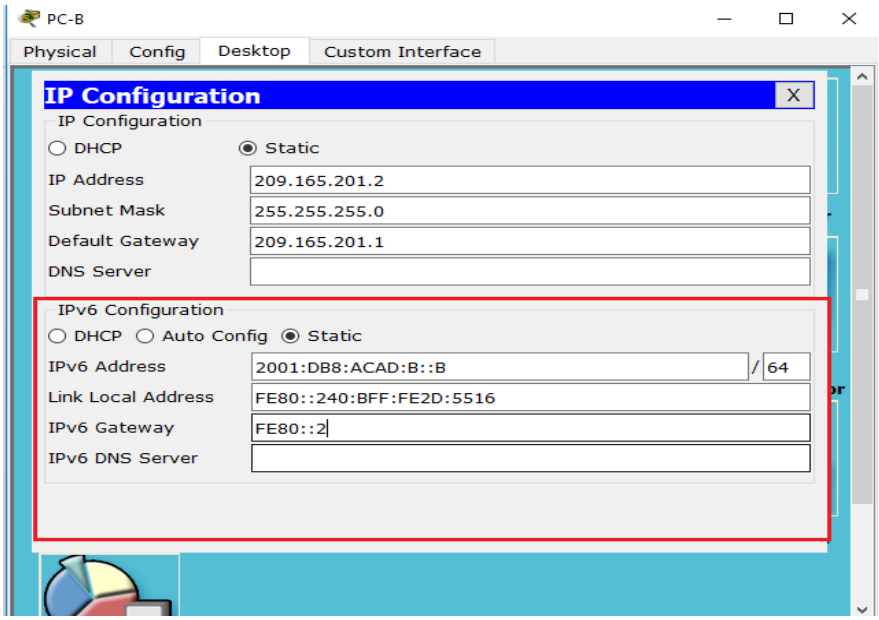


Imagen 71. Configuración PC-B.

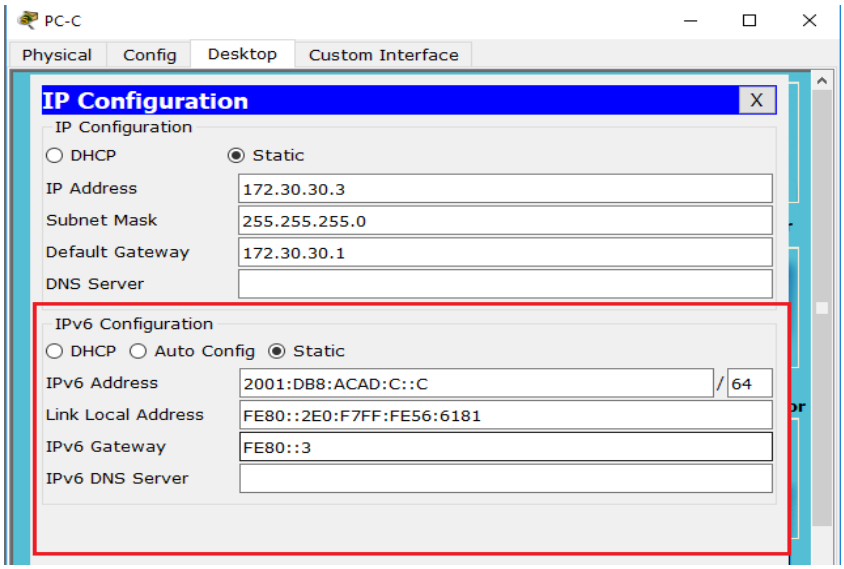


Imagen 72. Configuración PC-C.

Paso 2. Configurar IPv6 en los routers.

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

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

b. Habilite el routing IPv6 en cada router.

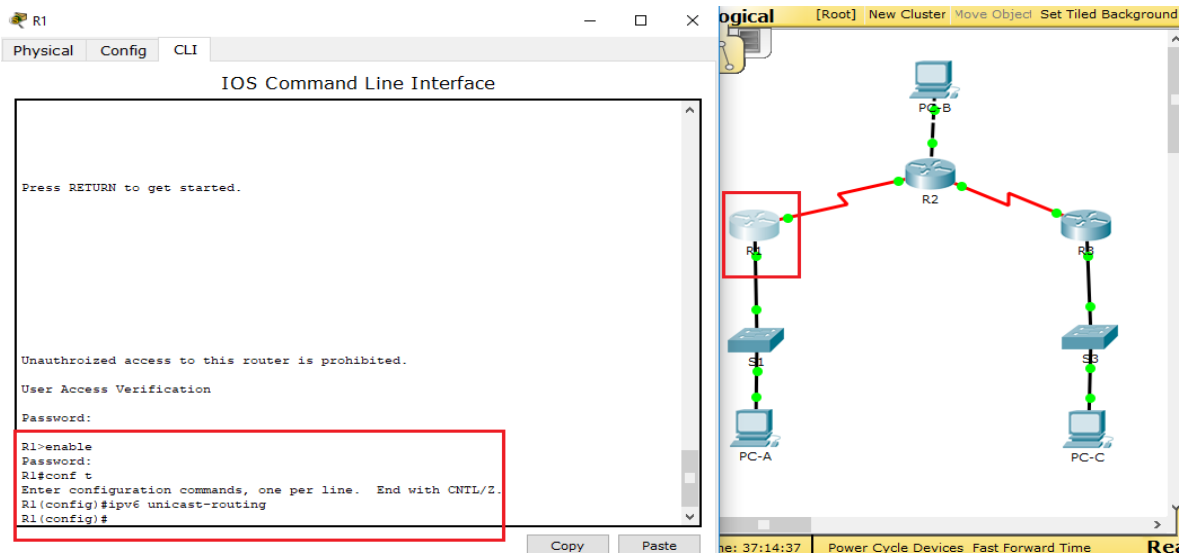


Imagen 73. Habilitación del routing IPv6 para R1.

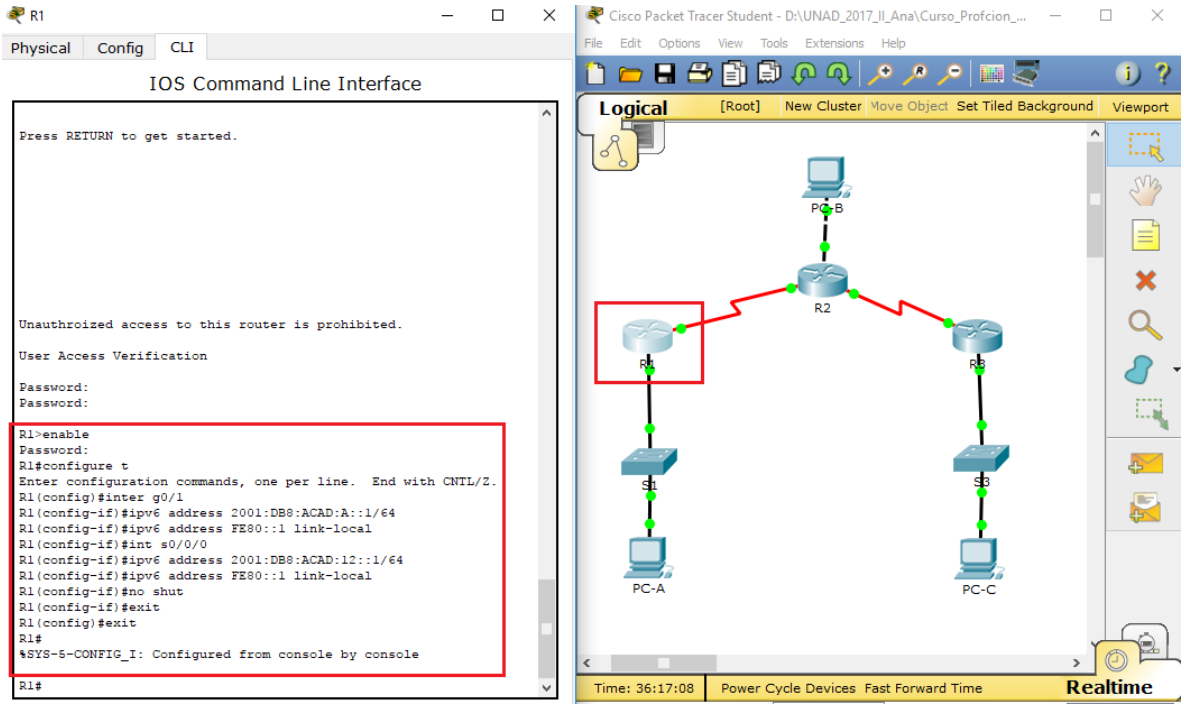


Imagen 74.Configuracion de IPv6 en R1.

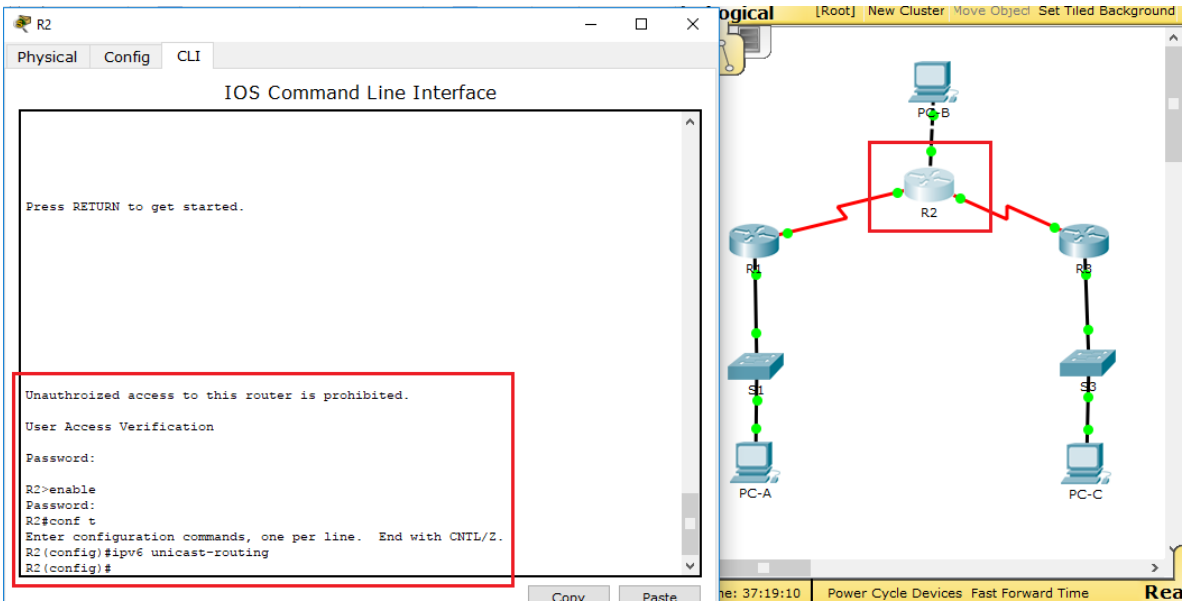


Imagen 75. Habilitación del routing IPv6 para R2.

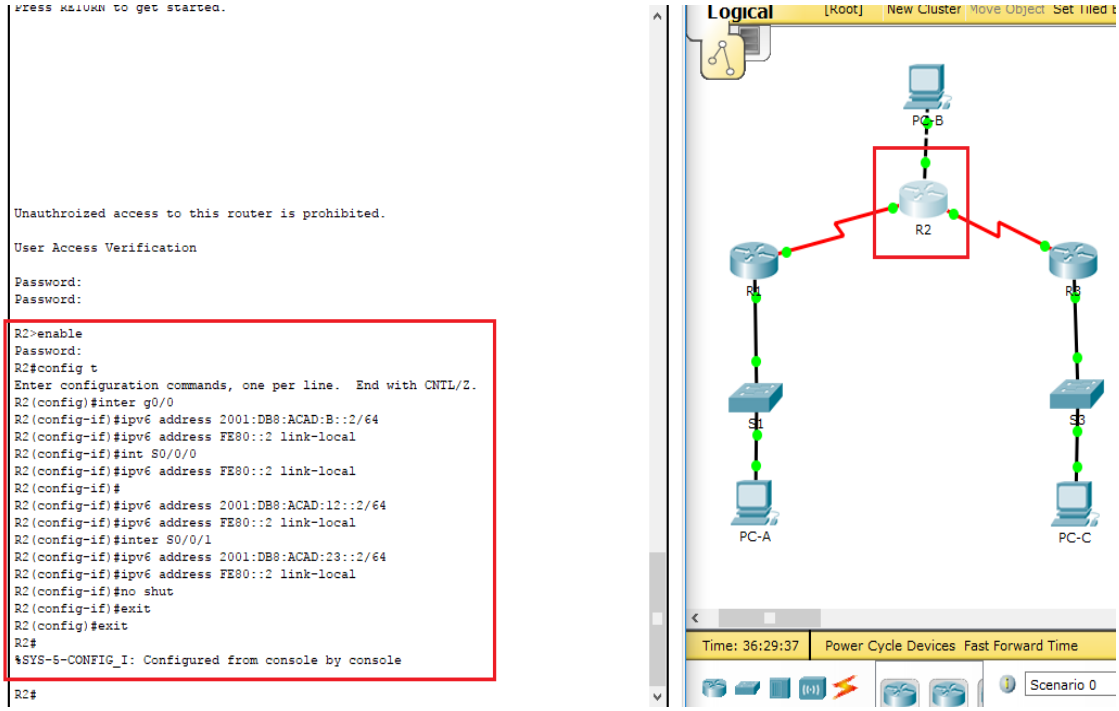


Imagen 76.Configuracion de IPv6 en R2.

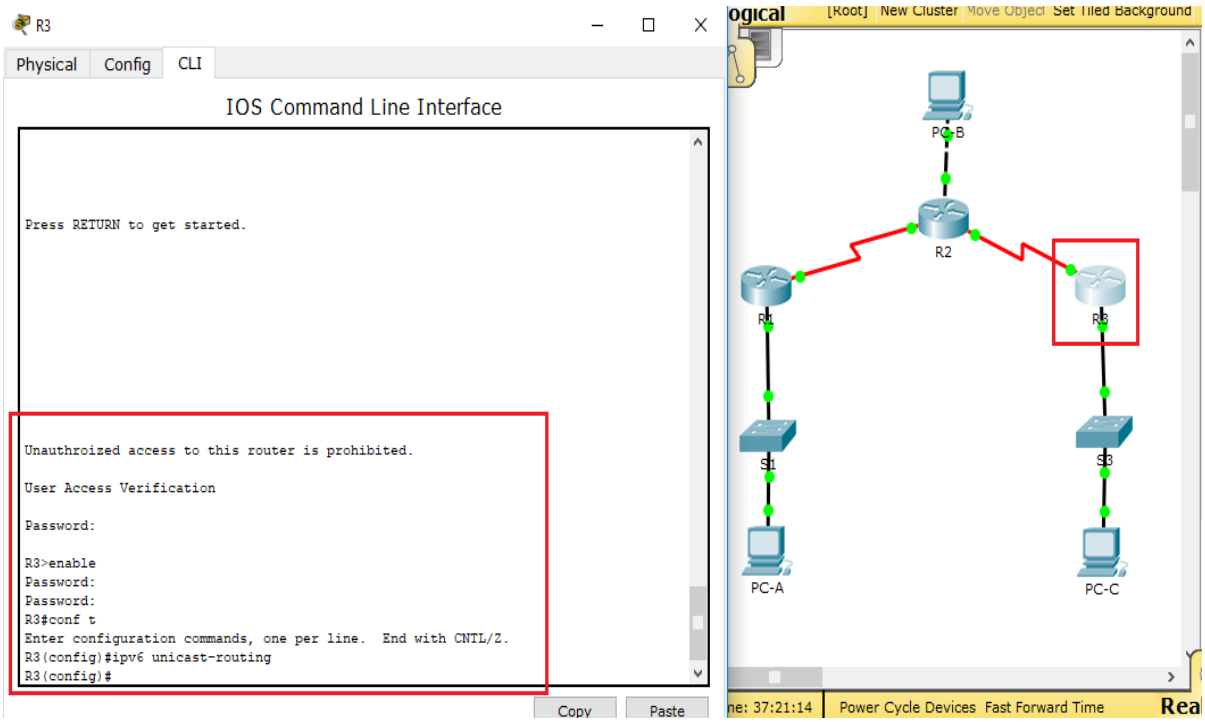


Imagen 77. Habilitación del routing IPv6 para R3.

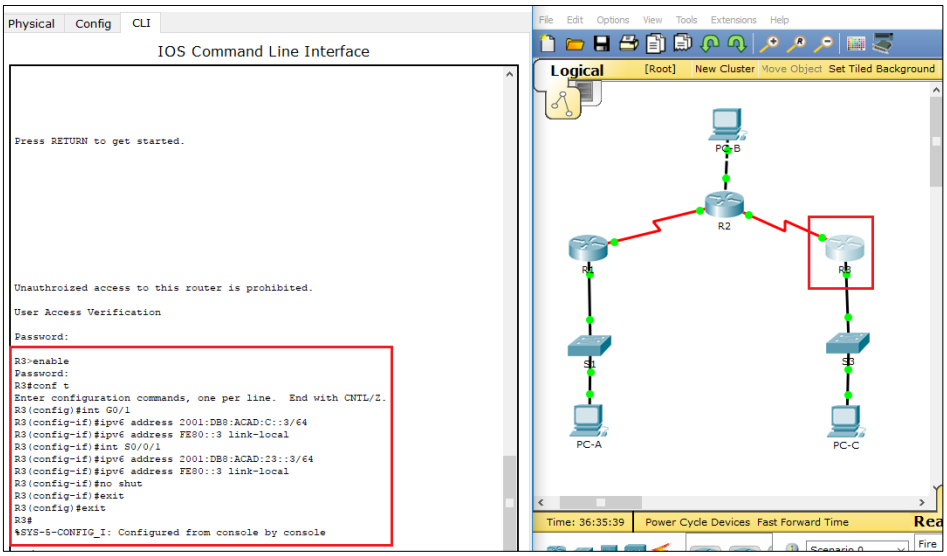


Imagen 78.Configuracion de IPv6 en R3.

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

R//- Los comandos apropiados para verificar las direcciones IPv6 y el estado de enlace son: **show ipv6 interface brief y show ipv6 route.**

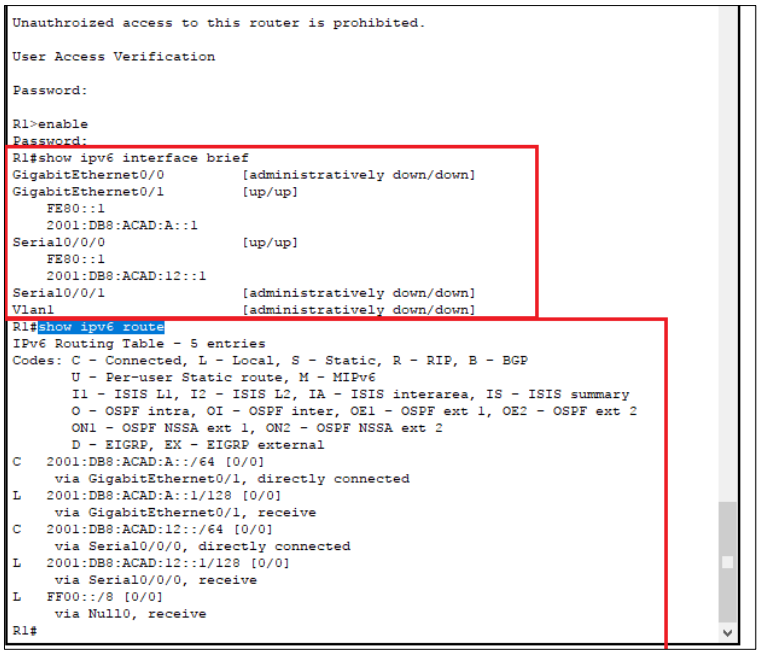


Imagen 79. Comandos apropiados para verificar las direcciones IPv6 y el estado de enlace en R1.

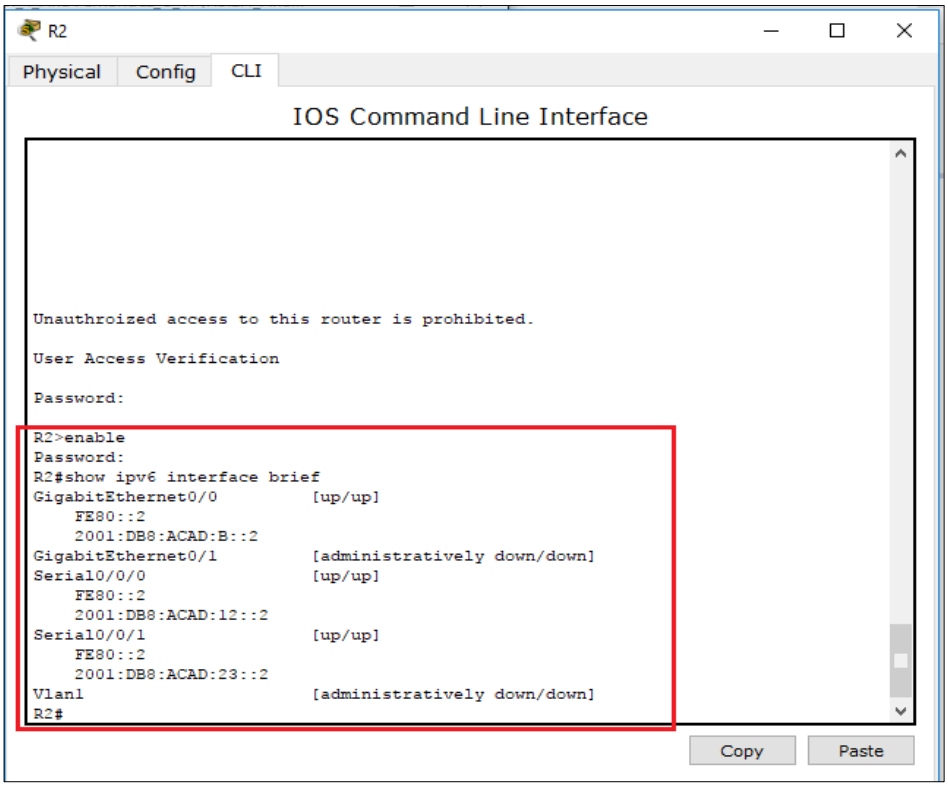


Imagen 80. Comandos apropiados para verificar las direcciones IPv6 y el estado de enlace en R2.

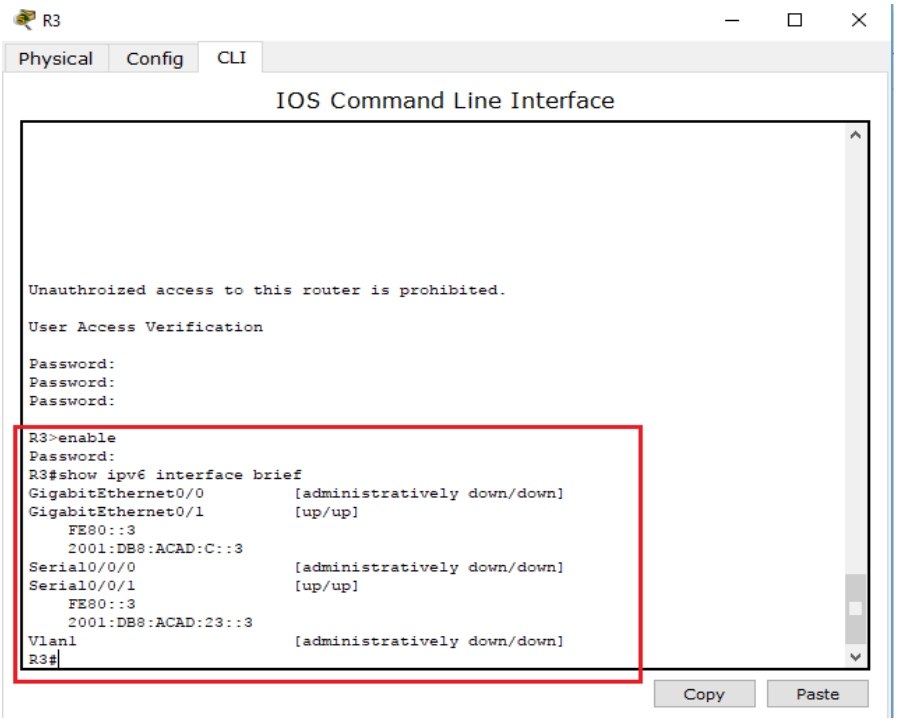


Imagen 81. Comandos apropiados para verificar las direcciones IPv6 y el estado de enlace en R3.

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

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

Parte 4. Configurar y verificar el routing RIPng

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

Paso 1. Configurar el routing RIPng.

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

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

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

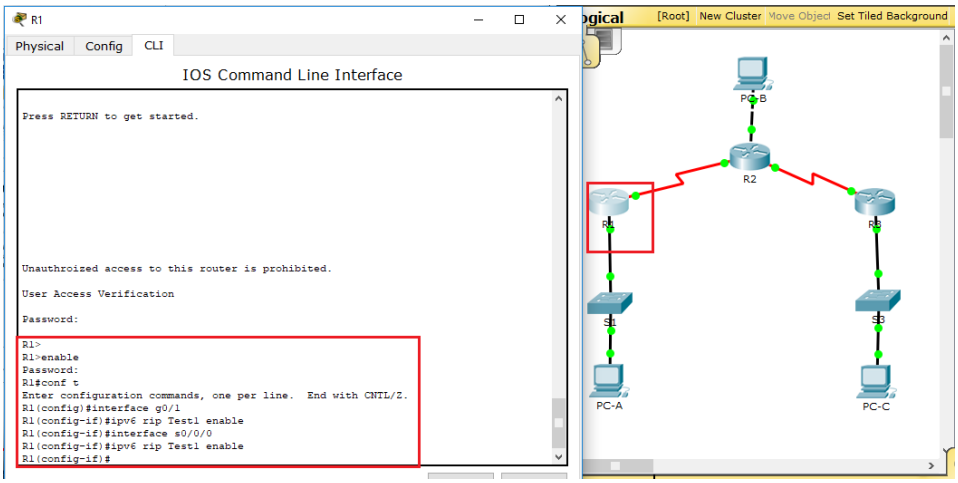


Imagen 82. Emisión del comando ipv6 rip Test1 enable para cada interfaz en el R1 que participará en el routing RIPng.

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

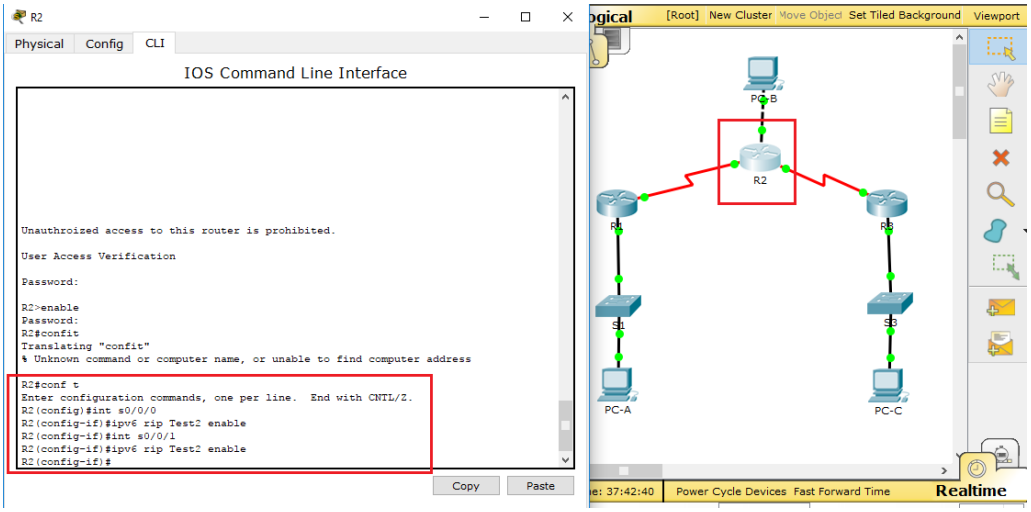


Imagen 83. Configuracion de RIPng para las interfaces seriales en el R2.

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

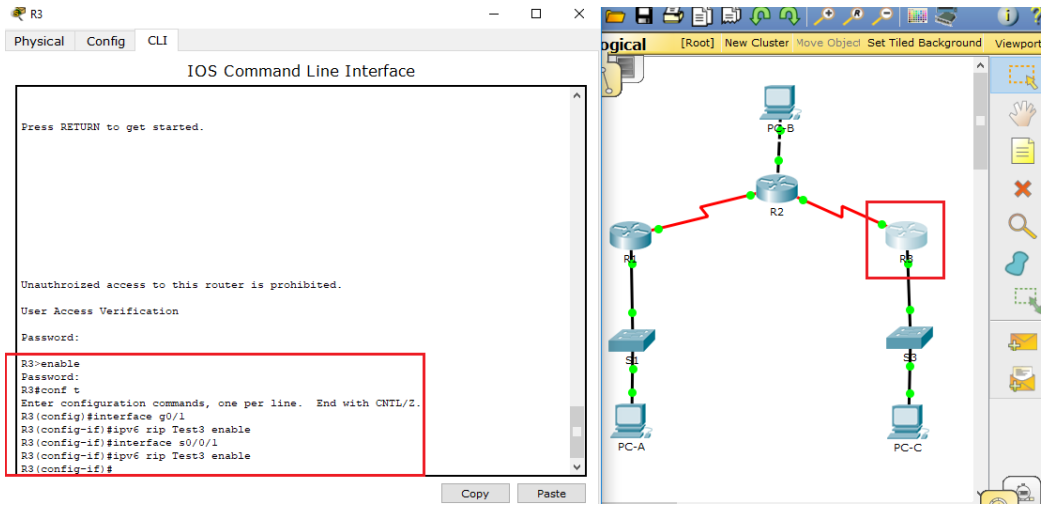


Imagen 84. Configuración RIPng para cada interfaz en el R3.

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

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

```
R1# show ipv6 protocols

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "rip Test1"

  Interfaces:

    Serial0/0/0

    GigabitEthernet0/1

  Redistribution:

    None
```

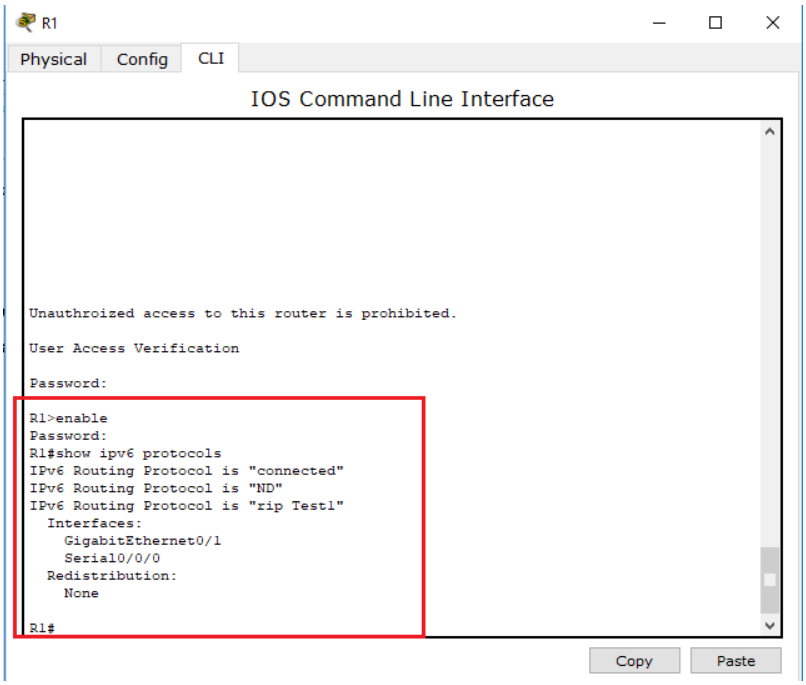


Imagen 85. Verificación que RIPng se esté ejecutando en R1.

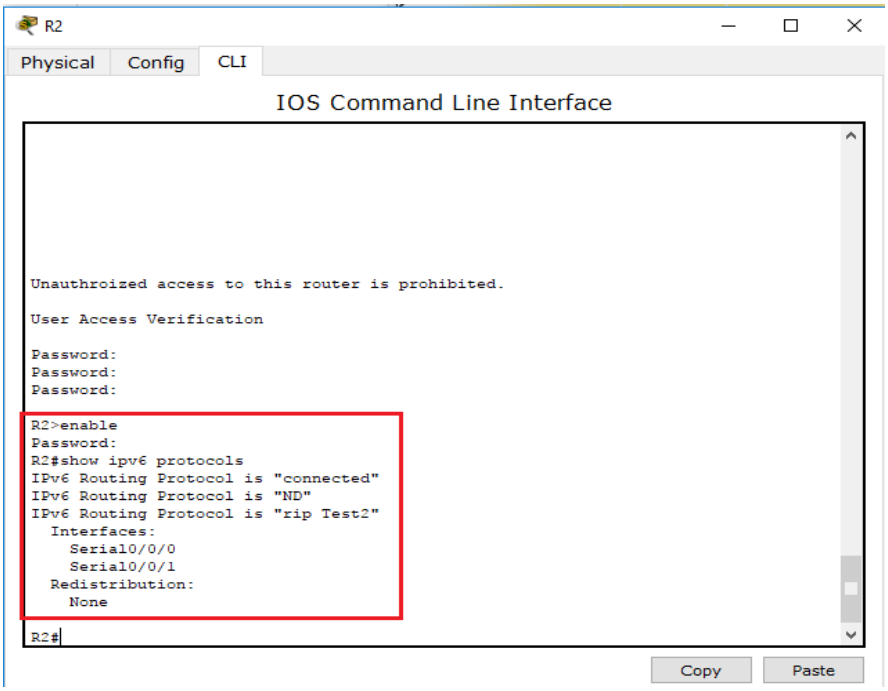


Imagen 86. Verificación que RIPng se esté ejecutando en R2.

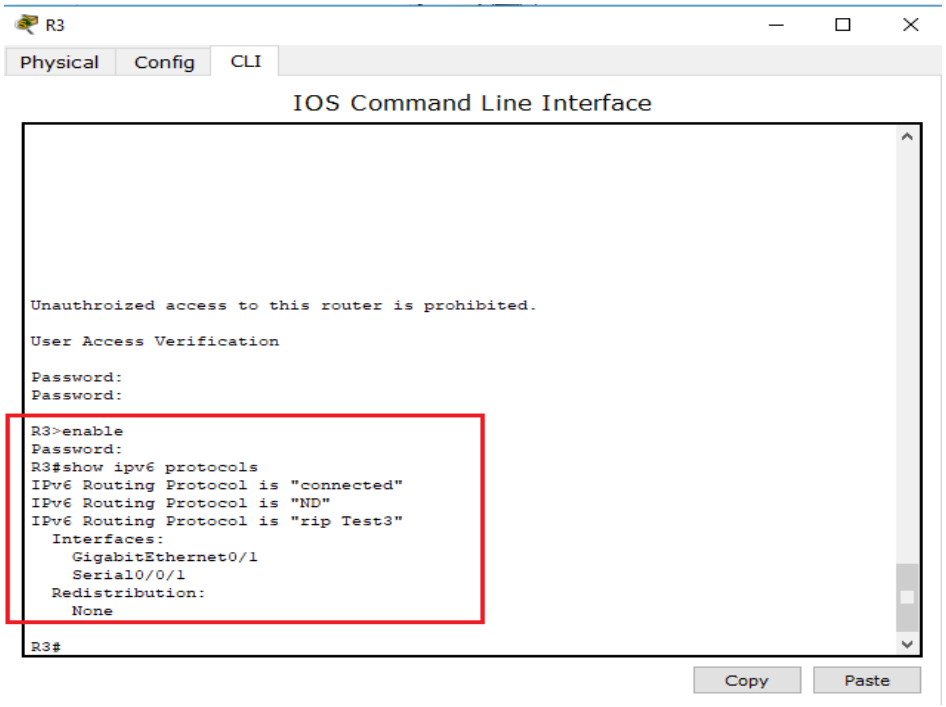


Imagen 87. Verificación que RIPng se esté ejecutando en R3.

¿En qué forma se indica RIPng en el resultado?

R//- RIPng esta listado por el nombre del proceso.

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

```
R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 314
     Administrative distance is 120. Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 1, trigger updates 0
     Full Advertisement 0, Delayed Events 0
```

```
Interfaces:
  GigabitEthernet0/1
  Serial0/0/0
Redistribution:
  None
```

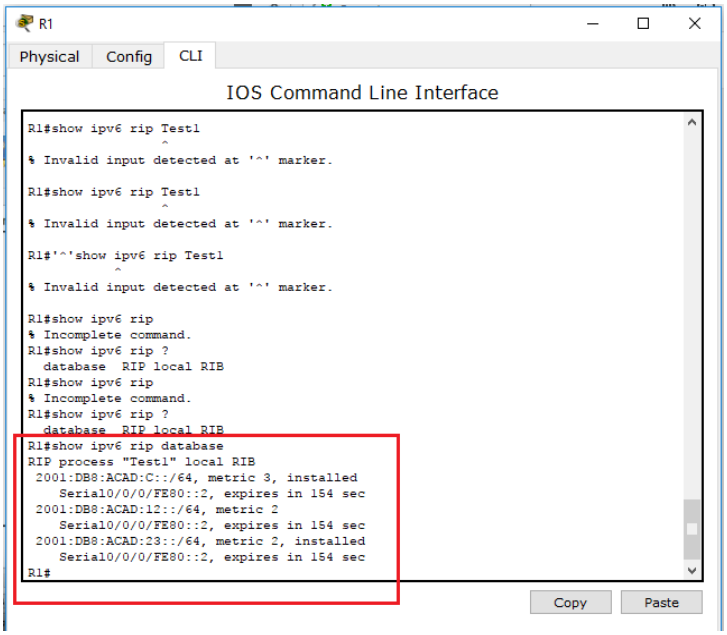


*Imagen 88. Emisión del comando **show ipv6 rip Test1**.*

¿Cuáles son las similitudes entre RIPv2 y RIPng?

Respuesta: Ambas RIPv2 y RIPng tienen la distancia administrativa de 120. Usan el conteo de saltos como la métrica y envían autorizaciones cada 30 segundos.

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

Respuesta: el comando apropiado que se usa para ver la tabla de routing es: **Show ipv6 route**.

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

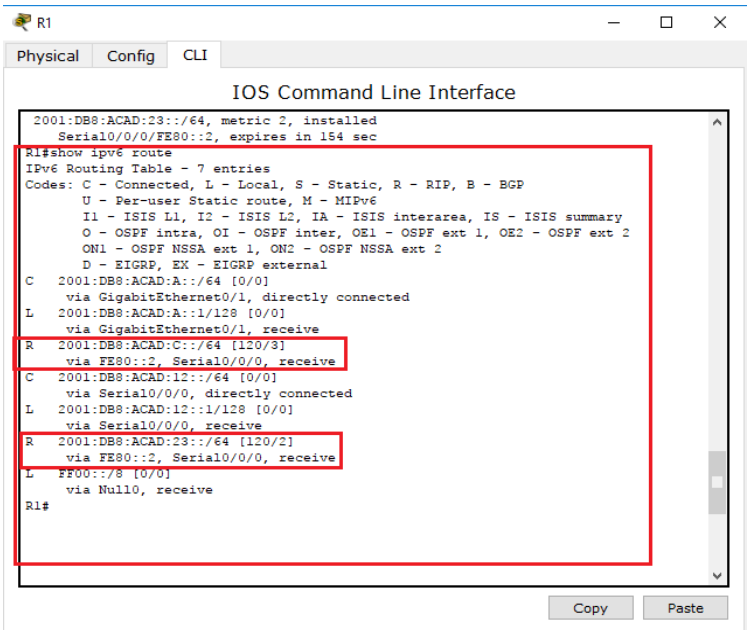


Imagen 89. Rutas descubiertas mediante RIPng en R1.

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

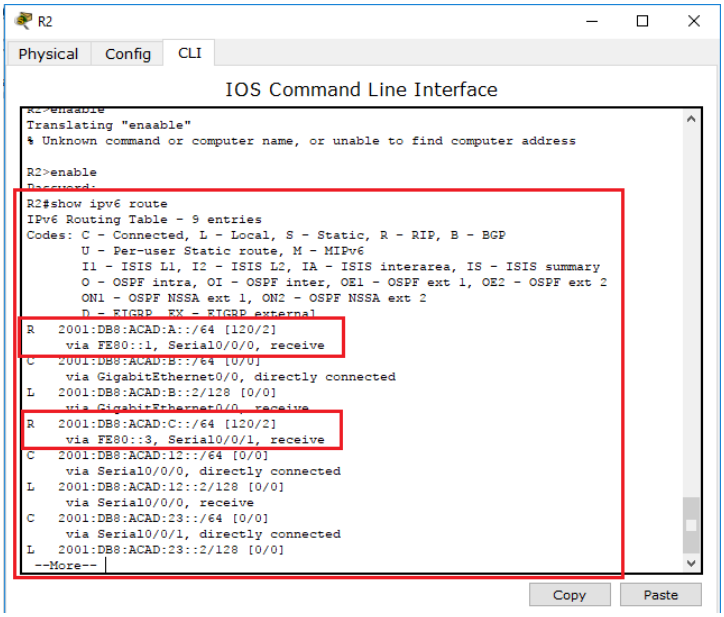


Imagen 90. Rutas descubiertas mediante RIPng en R2.

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

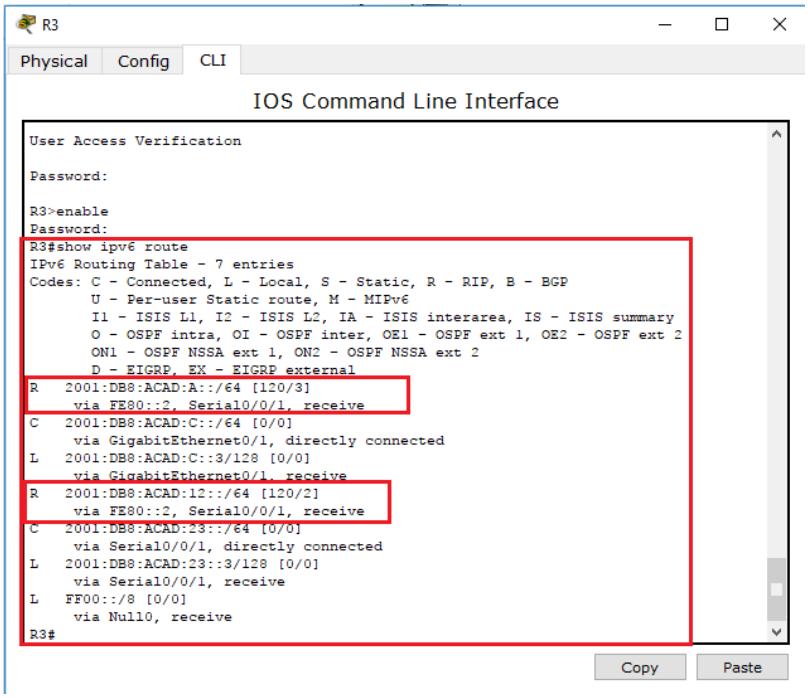


Imagen 91. Rutas descubiertas mediante RIPng en R3.

g. Verifique la conectividad entre las computadoras.

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

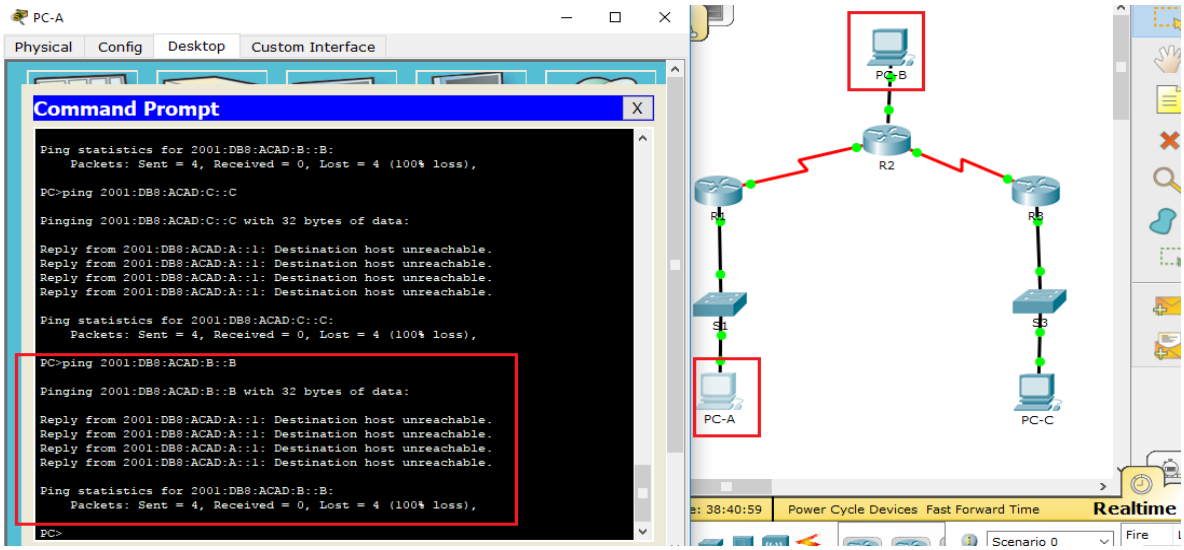


Imagen 92. Ping de la PC-A a la PC-B.

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

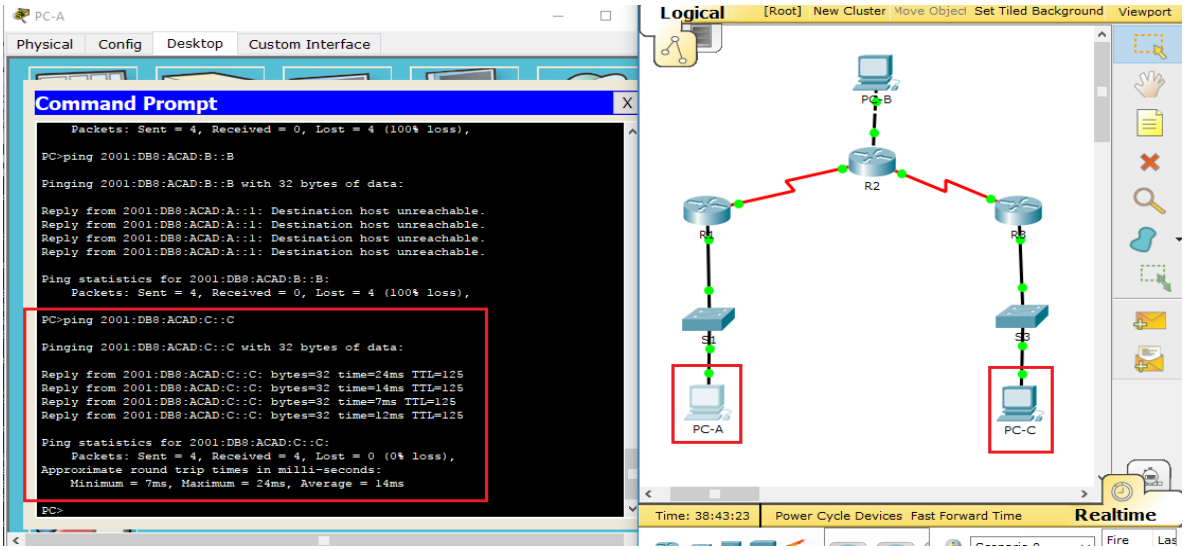


Imagen 93. Ping de la PC-A a la PC-C.

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

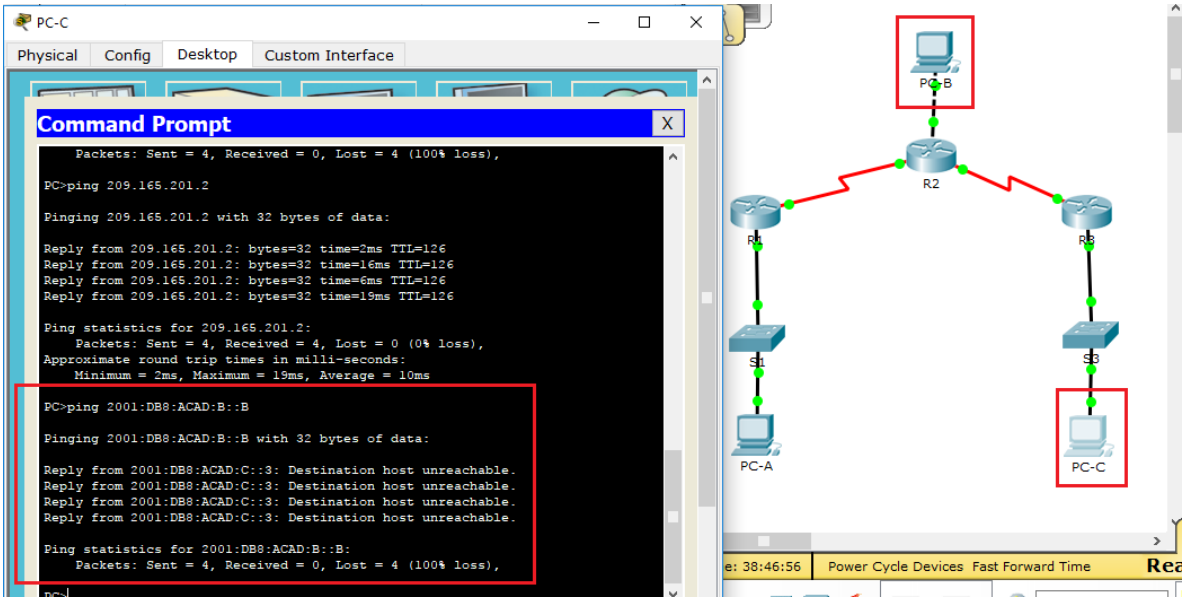


Imagen 94. Ping de la PC-C a la PC-B.

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

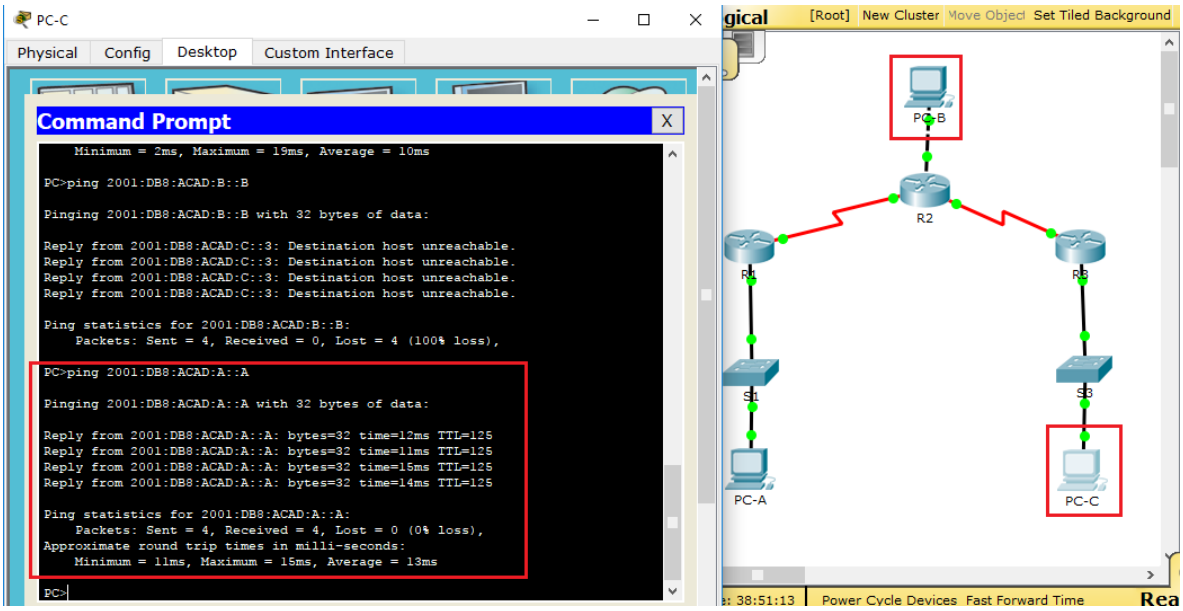


Imagen 95. Ping de la PC-C a la PC-A.

¿Por qué algunos pings tuvieron éxito y otros no?

Respuesta. Debido a que no hay una ruta que se especifique para PC-B. Para esta red 2001:DB8:ACAD:B::B/64.

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.

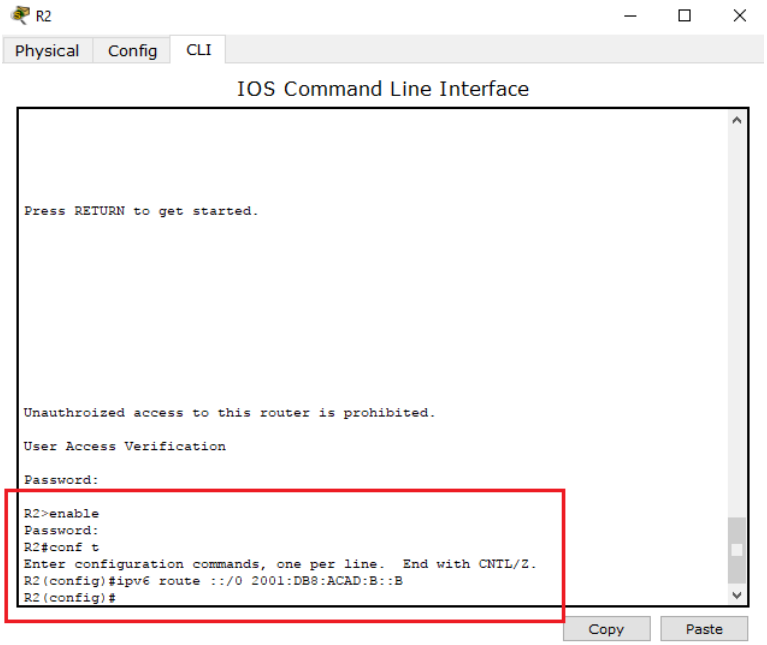


Imagen 96. Ruta estática predeterminada.

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

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

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

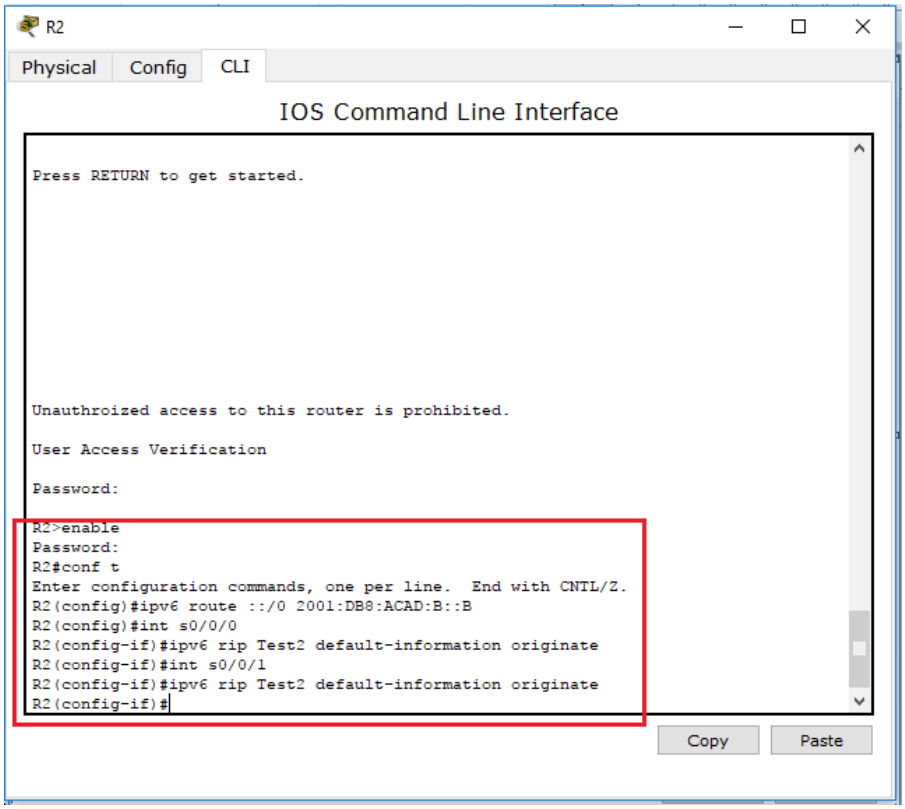


Imagen 97. Configuración los enlaces seriales en el R2 para enviar la ruta predeterminada en actualizaciones RIPng.

Paso 3. Verificar la configuración de enrutamiento.

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

```
R2# show ipv6 route

IPv6 Routing Table - 10 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/64 [1/0]
     via 2001:DB8:ACAD:B::B
R   2001:DB8:ACAD:A::/64 [120/2]
     via FE80::1, Serial0/0/0
```

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

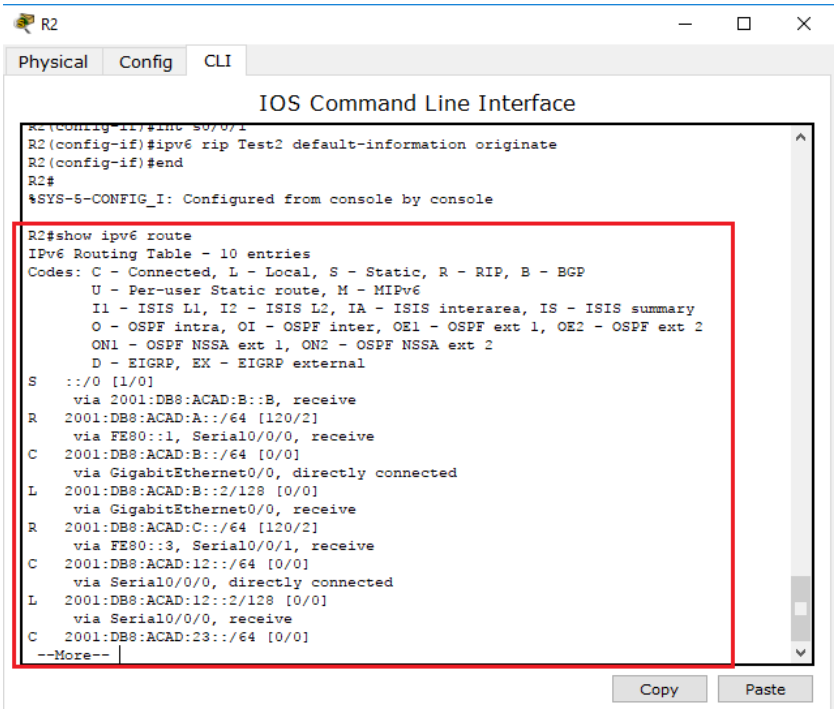


Imagen 98. Tabla de routing IPv6 en el router R2.

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

Respuesta: Debido a que tiene una ruta por defecto estática que se puede evidenciar en en R2___ S ::/0 [1/0].

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

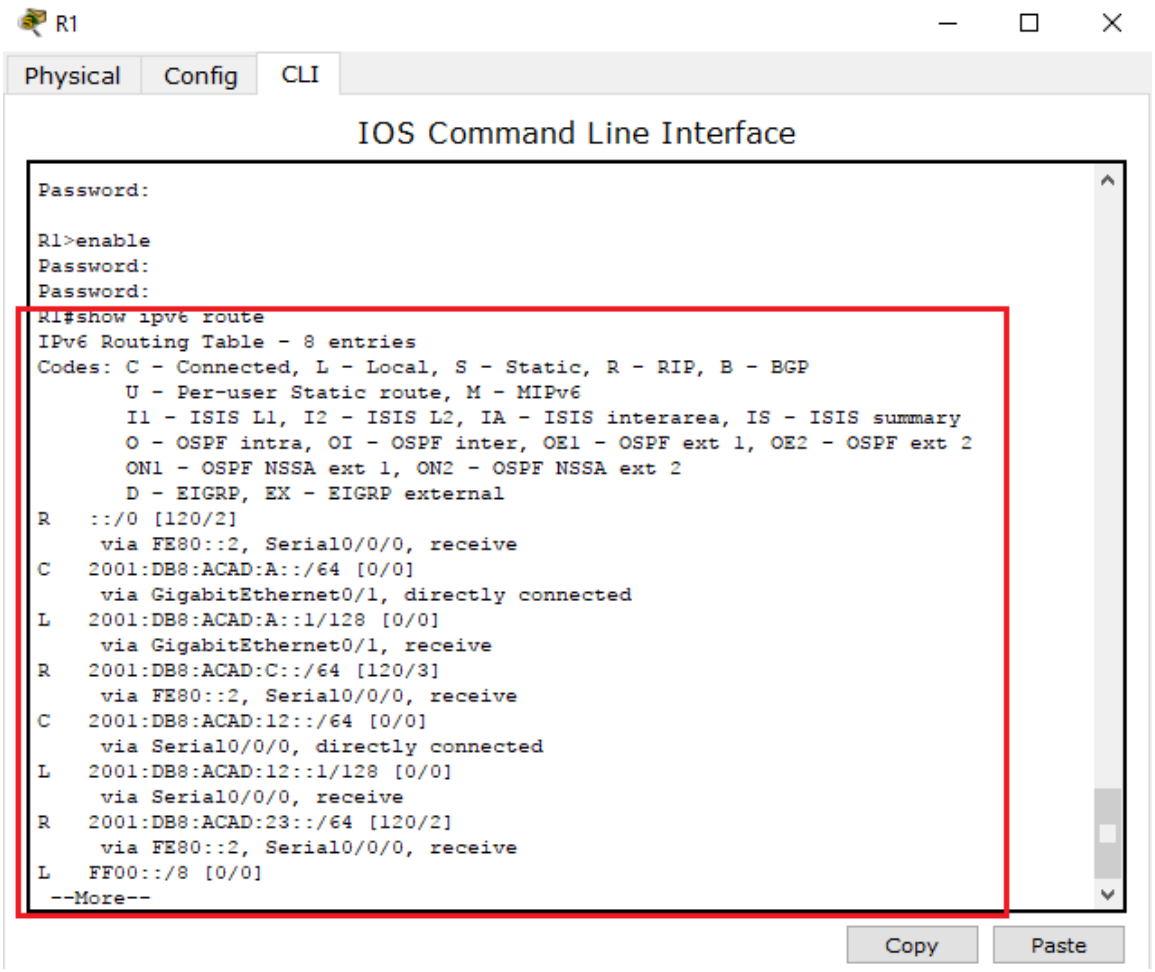


Imagen 99. Tabla de routing del R1

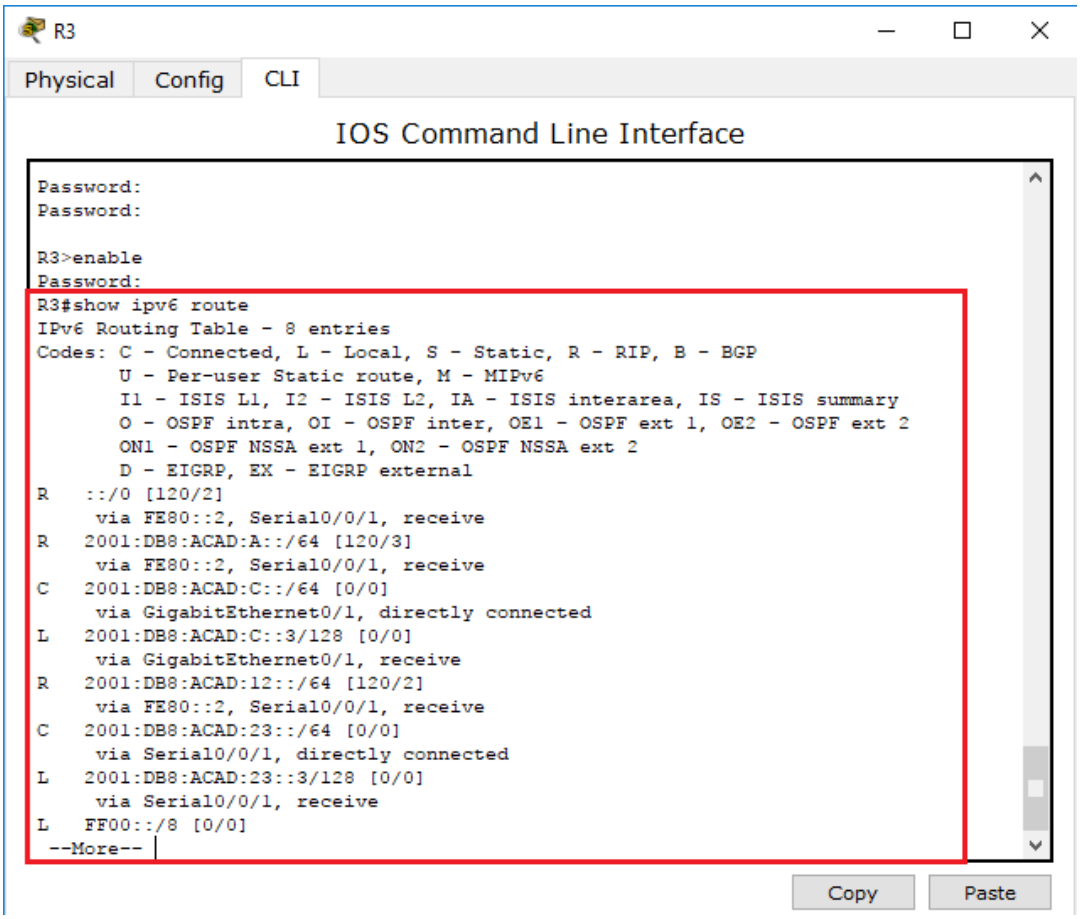


Imagen 100. Tabla de routing del R1

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

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

Paso 4. Verifique la conectividad.

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

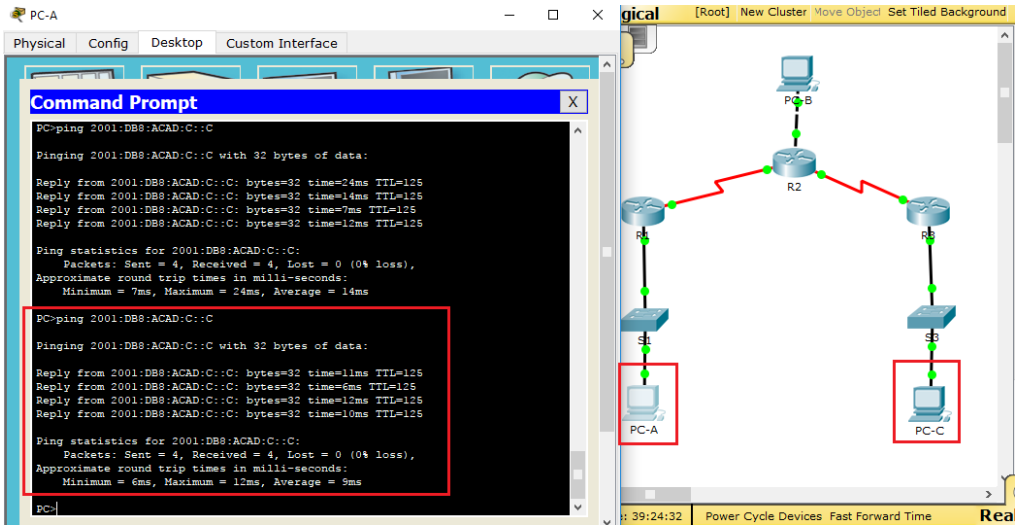


Imagen 101. Ping de la PC-A y la PC-C

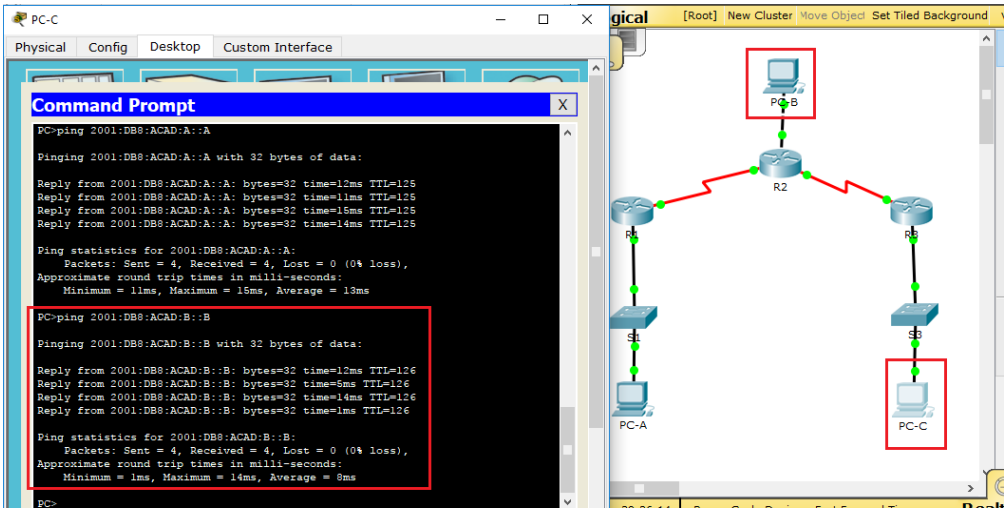


Imagen 102. Ping de la PC-A y la PC-C

¿Tuvieron éxito los pings? Respuesta: Si

Reflexión

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

   Respuesta: Estaría bien, para que los routers no sumaricen las rutas hacia la clase mayor y así podría haber conectividad entre redes discontiguas.

2. En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3? _R//-La descubrieron en las actualizaciones del RIP recibidas desde el router donde fue configurada la ruta por defecto en este caso R2.

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

   Respuesta: RIPv2 se configura notificando las redes y la de RIPng se configura en las interfaces.

Conclusiones.

- En esta práctica de laboratorio, configuráramos la topología de la red con routing RIPv2, deshabilitamos la sumarización automática, propagamos una ruta predeterminada y usamos comandos de CLI para ver y verificar la información de routing RIP. Luego, configuramos la topología de la red con direcciones IPv6, configuramos RIPng, propagamos una ruta predeterminada y usamos comandos de CLI para ver y verificar la información de routing RIPng.

8.2.4.5 Lab - Configuring Basic Single-Area Ospfv2

Topología

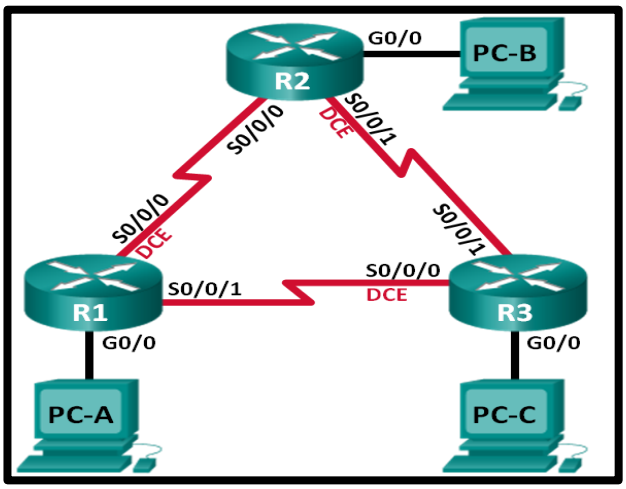


Imagen 103, Topología.

Tabla 3:

Tabla de direccionamiento

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

Objetivos

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

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.

Parte 2. Configurar y verificar el enrutamiento OSPF

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

Paso 1. Configure el protocolo OSPF en R1.

j. 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.

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

   R1(config-router)# **network 192.168.1.0 0.0.0.255 area 0**

   R1(config-router)# **network 192.168.12.0 0.0.0.3 area 0**

   R1(config-router)# **network 192.168.13.0 0.0.0.3 area 0**

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

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

R1#

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

R1#

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

R1#

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

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

R1# **show ip ospf neighbor**

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

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.1      0   FULL/  -        00:00:39    192.168.12.2    Serial0/0/0
192.168.23.2      0   FULL/  -        00:00:35    192.168.13.2    Serial0/0/1
R1#
```

Imagen 104, comando show ip ospf neighbor

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

R1# **show ip route**

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

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

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

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

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

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

P - periodic downloaded static route

Gateway of last resort is not set

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

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

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

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

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

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

L 192.168.12.1/32 is directly connected, Serial0/0/0

192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.13.0/30 is directly connected, Serial0/0/1

L 192.168.13.1/32 is directly connected, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

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

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

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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:03:00, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:01:46, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:02:00, Serial0/0/0
                        [110/128] via 192.168.13.2, 00:02:00, Serial0/0/1
R1#
```

Imagen 105, comando show ip route para verificar que todas las redes

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

- show ip route ospf

Paso 4. Verificar la configuración del protocolo OSPF.

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

R1# **show ip protocols**
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.168.13.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.1.0 0.0.0.255 area 0
192.168.12.0 0.0.0.3 area 0
192.168.13.0 0.0.0.3 area 0
Routing Information Sources:

Gateway	Distance	Last Update
192.168.23.2	110	00:19:16
192.168.23.1	110	00:20:03

Distance: (default is 110)

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.13.1         110      00:06:36
    192.168.23.1         110      00:06:53
    192.168.23.2         110      00:06:19
  Distance: (default is 110)

R1#
```

Imagen 106, Paso 4: verificar la configuración del protocolo OSPF

Paso 5. Verificar la información del proceso OSPF.

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

R1# **show ip ospf**

Routing Process "ospf 1" with ID 192.168.13.1

Start time: 00:20:23.260, Time elapsed: 00:25:08.296

Supports only single TOS(TOS0) routes

Supports opaque LSA

Supports Link-local Signaling (LLS)

Supports area transit capability

Supports NSSA (compatible with RFC 3101)

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

Router is not originating router-LSAs with maximum metric

Initial SPF schedule delay 5000 msecs

Minimum hold time between two consecutive SPFs 10000 msecs

Maximum wait time between two consecutive SPFs 10000 msecs

Incremental-SPF disabled

Minimum LSA interval 5 secs

Minimum LSA arrival 1000 msecs

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msecs

Retransmission pacing timer 66 msecs

Number of external LSA 0. Checksum Sum 0x000000

Number of opaque AS LSA 0. Checksum Sum 0x000000

Number of DCbitless external and opaque AS LSA 0

Number of DoNotAge external and opaque AS LSA 0

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

Number of areas transit capable is 0

External flood list length 0

IETF NSF helper support enabled

Cisco NSF helper support enabled

Reference bandwidth unit is 100 mbps

Area BACKBONE(0)

Number of interfaces in this area is 3

Area has no authentication

SPF algorithm last executed 00:22:53.756 ago

SPF algorithm executed 7 times

Area ranges are

Number of LSA 3. Checksum Sum 0x019A61

Number of opaque link LSA 0. Checksum Sum 0x000000

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

```
R1#show ip ospf
 Routing Process "ospf 1" with ID 192.168.13.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x01b5a9
        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

R1#
```

Imagen 107, comando show ip ospf para examinar la ID del proceso OSPF y la ID del router

Paso 6. Verificar la configuración de la interfaz OSPF.

n. 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

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

R1# **show ip ospf interface**

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

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

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

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

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.

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Imagen 108, ping 192.168.2.3.

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=36ms TTL=128
Reply from 192.168.3.3: bytes=32 time=16ms TTL=128
Reply from 192.168.3.3: bytes=32 time=0ms TTL=128
Reply from 192.168.3.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 13ms

PC>
```

Imagen 109, ping 192.168.3.3.

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

Parte 3. Cambiar las asignaciones de ID del router

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

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

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

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

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

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 lo0

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

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

R1(config-if)#ip addres 1.1.1.1 255.255.255.255
R1(config-if)#no shutdown
```

Imagen 110, Asigne una dirección IP al loopback 0 en el R1

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 lo0

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

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

R2(config-if)#ip addres 2.2.2.2 255.255.255.255
R2(config-if)#no shutdown
```

Imagen 111, Asigne direcciones IP al loopback 0 en el R2.

```
R3(config)#interface lo0

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

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

R3(config-if)#ip addres 3.3.3.3 255.255.255.255
R3(config-if)#no shutdown
R3(config-if)#
```

Imagen 112, Asigne direcciones IP al loopback 0 en el R3.

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

Routing Information Sources:

Gateway	Distance	Last Update
3.3.3.3	110	00:01:00
2.2.2.2	110	00:01:14

Distance: (default is 110)

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:00:08
    192.168.13.1         110      00:23:52
    192.168.23.1         110      00:01:04
    192.168.23.2         110      00:00:08
  Distance: (default is 110)

R1#
```

Imagen 113, R1# show ip protocols

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

R1#

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:36    192.168.12.2    Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:32    192.168.13.2    Serial0/0/1
R1#
```

Imagen 114, R1# show ip ospf neighbor.

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**

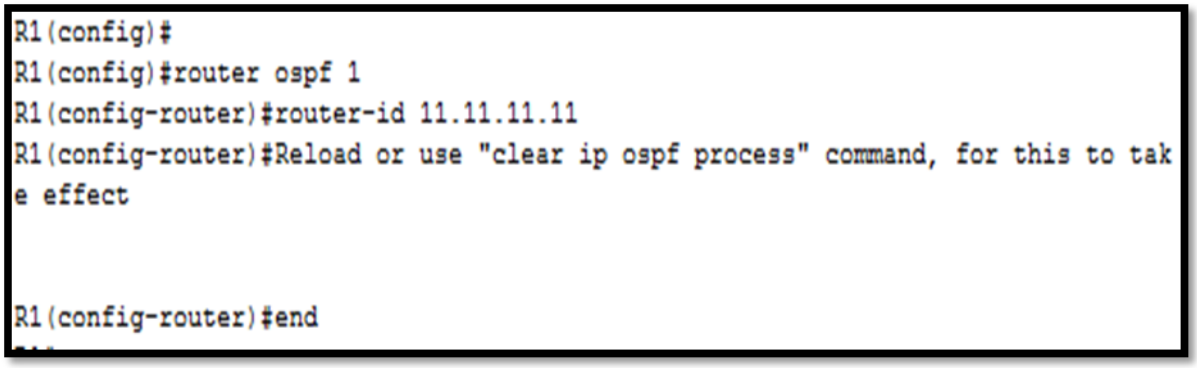


Imagen 115, comando router-id 11.11.11.11 en el R1 para reasignar la ID del router

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.

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.

R2(config)#router ospf 1
R2(config-router)#router-id 22.22.22.22
R2(config-router)#Reload or use "clear ip ospf process" command, for this to take effect

R3(config)#router ospf 1

R3(config-router)#router-id 33.33.33.33

R3(config-router)#Reload or use "clear ip ospf process" command, for this to take effect

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)

```
R1#show ip protoco

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
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:20:55
    2.2.2.2              110      00:08:21
    3.3.3.3              110      00:07:35
    11.11.11.11          110      00:00:10
    22.22.22.22          110      00:00:09
    33.33.33.33          110      00:00:10
    192.168.13.1         110      00:48:49
    192.168.23.1         110      00:26:00
    192.168.23.2         110      00:21:38
  Distance: (default is 110)

R1#
```

Imagen 116, R1# show ip protocols

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
22.22.22.22       0   FULL/  -        00:00:30    192.168.12.2    Serial0/0/0
33.33.33.33       0   FULL/  -        00:00:30    192.168.13.2    Serial0/0/1
R1#
```

Imagen 117, R1# show ip ospf neighbor R1.

- **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.

- **Configurar una interfaz pasiva.**

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    Cost    Disabled    Shutdown      Topology Name
        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)

```
R1#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  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
    Hello due in 00:00:04
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1#
```

Imagen 118, R1# show ip ospf interface g0/0

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
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#passive-interface g0/0
R1(config-router)#
```

Imagen 119, el comando passive-interface para cambiar la interfaz G0/0 en el R1 a pasiva

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	Cost	Disabled	Shutdown	Topology Name
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

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)

```
R1#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1#
```

Imagen 120, R1# show ip ospf interface g0/0

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

L 192.168.12.2/32 is directly connected, Serial0/0/0

192.168.13.0/30 is subnetted, 1 subnets

O 192.168.13.0 [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

L 192.168.23.1/32 is directly connected, Serial0/0/1

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

Gateway of last resort is not set

     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:06:46, 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, 00:07:41, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
     192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0/30 [110/128] via 192.168.23.2, 00:06:46, Serial0/0/1
                        [110/128] via 192.168.12.1, 00:06:46, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.1/32 is directly connected, Serial0/0/1
R2#
```

Imagen 121, comando show ip route en el R2 y el R3 disponibilidad ruta a la red 192.168.1.0/24

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, 00:07:41, Serial0/0/0
O 192.168.2.0/24 [110/65] via 192.168.23.1, 00:08:36, Serial0/0/1
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.3.0/24 is directly connected, GigabitEthernet0/0
L 192.168.3.1/32 is directly connected, GigabitEthernet0/0
192.168.12.0/30 is subnetted, 1 subnets
O 192.168.12.0/30 [110/128] via 192.168.23.1, 00:07:41, Serial0/0/1
[110/128] via 192.168.13.1, 00:07:41, Serial0/0/0
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.13.0/30 is directly connected, Serial0/0/0
L 192.168.13.2/32 is directly connected, Serial0/0/0
192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.23.0/30 is directly connected, Serial0/0/1
L 192.168.23.2/32 is directly connected, Serial0/0/1
R3#

```
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, 00:07:41, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:08:36, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:07:41, Serial0/0/1
                        [110/128] via 192.168.13.1, 00:07:41, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
R3#
```

Imagen 122, R3#show ip route

- **Establecer la interfaz pasiva como la interfaz predeterminada en un router.**

  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

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       0   FULL/  -        00:00:31    192.168.12.2    Serial0/0/0
33.33.33.33       0   FULL/  -        00:00:31    192.168.13.2    Serial0/0/1
R1#
```

Imagen 123, R1# show ip ospf neighbor.

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

```
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#passive-interface default
R2(config-router)#
00:19:47: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to
 DOWN, Neighbor Down: Interface down or detached

00:19:47: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to
 DOWN, Neighbor Down: Interface down or detached

R2(config-router)#
```

Imagen 124, comando passive-interface default en el R2 para establecer todas las interfaces OSPF

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

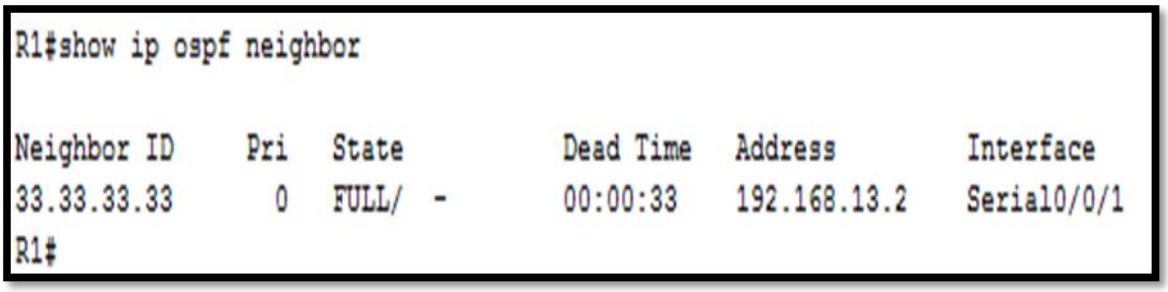


Imagen 125, comando show ip ospf neighbor en el R1.

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

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

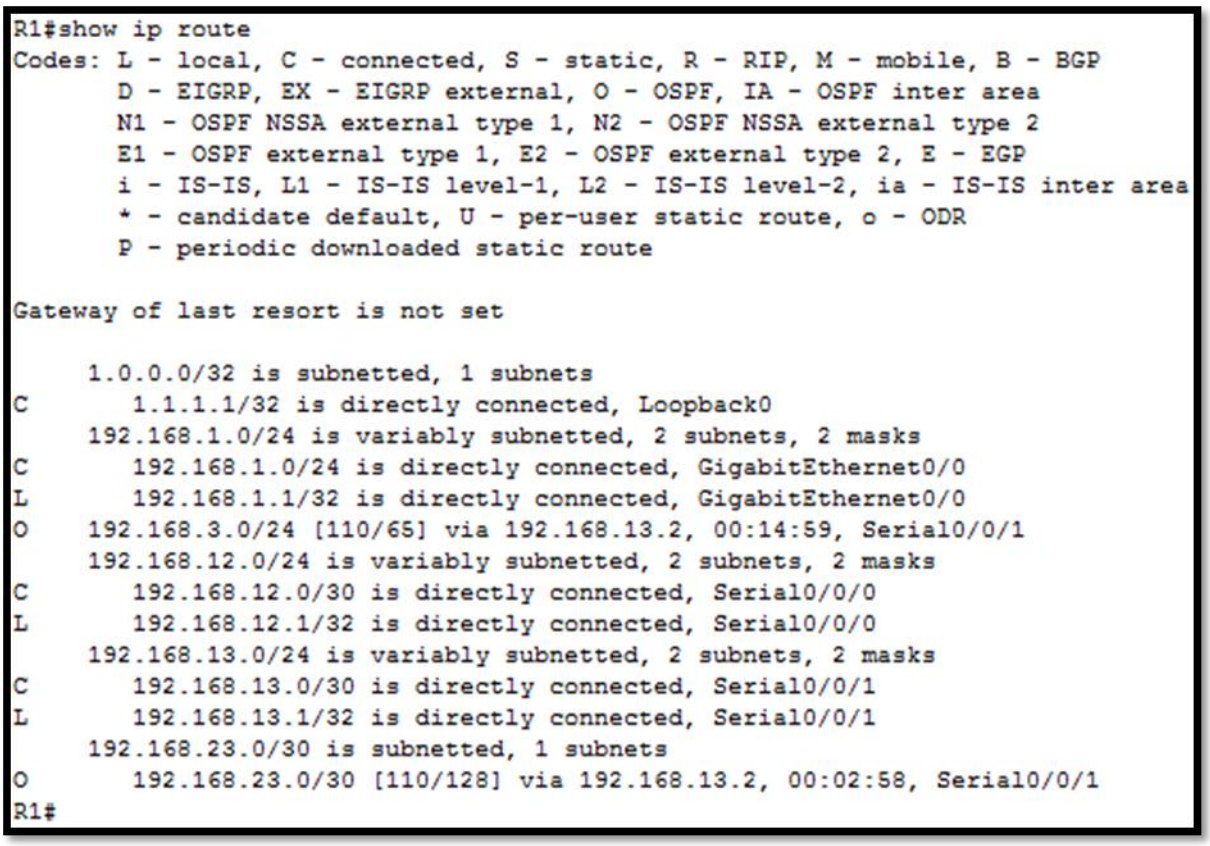
Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

```
R2#show ip ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.2/30, Area 0
  Process ID 1, Router ID 22.22.22.22, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    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#
```

Imagen 126, R2# show ip ospf interface s0/0/0

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**.



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

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:14:59, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.13.2, 00:02:58, Serial0/0/1
R1#
```

Imagen 127, comando show ip route, R1 y R3 sin ruta a la red 192.168.2.0/24

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

Gateway of last resort is not set

1.0.0.0/32 is subnetted, 1 subnets
C 1.1.1.1/32 is directly connected, Loopback0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:14:59, Serial0/0/1

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

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

L 192.168.12.1/32 is directly connected, Serial0/0/0

192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.13.0/30 is directly connected, Serial0/0/1

L 192.168.13.1/32 is directly connected, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0/30 [110/128] via 192.168.13.2, 00:02:58, Serial0/0/1

R1#

```
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, 00:15:27, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:02:52, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
R3#
```

Imagen 128, R1#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, 00:15:27, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:02:52, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
R3#
```

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

```
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#
00:26:17: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING
 to FULL, Loading Done
```

Imagen 129, R2, comando no passive-interface.

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

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

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:00:57, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:19:27, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
                        [110/128] via 192.168.12.2, 00:00:57, Serial0/0/0
R1#
```

Imagen 130, show ip route y show ipv6 ospf neighbor en el R1 y el R3

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

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:00:57, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:19:27, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
                        [110/128] via 192.168.12.2, 00:00:57, Serial0/0/0
R1#
```

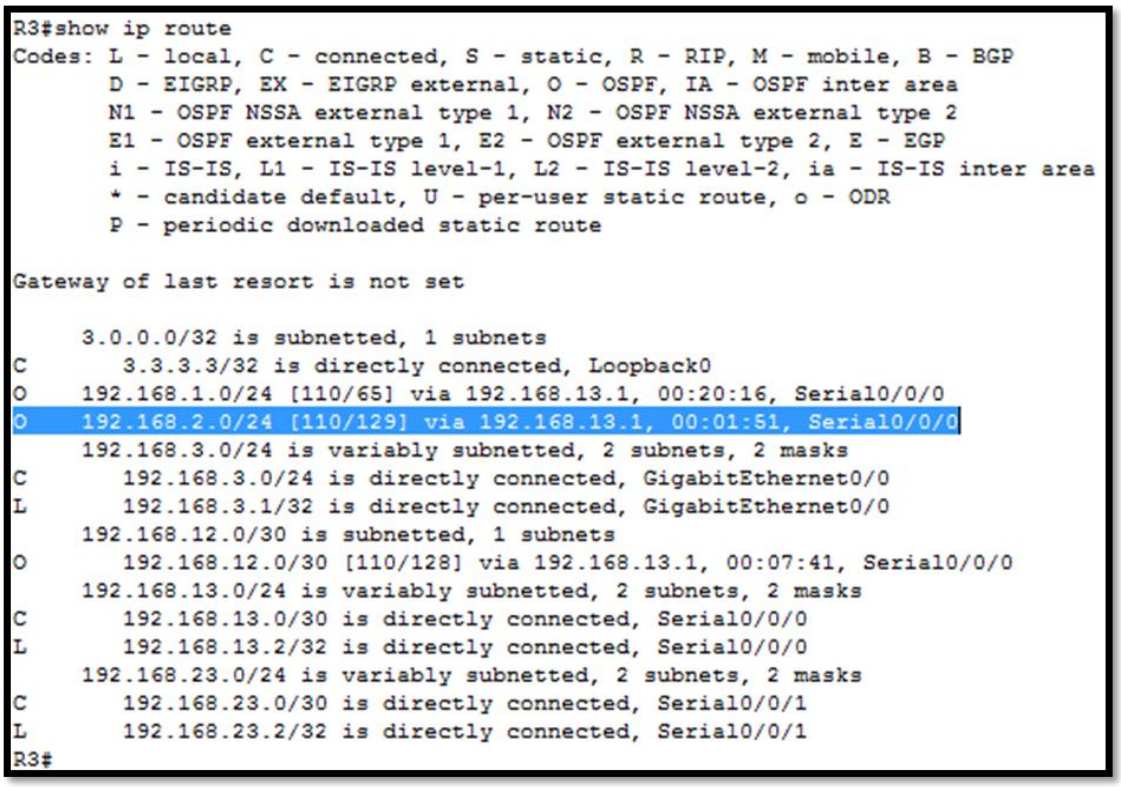


Imagen 131, R1#show ip route 192.168.2.0/24

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, 00:20:16, Serial0/0/0

O 192.168.2.0/24 [110/129] via 192.168.13.1, 00:01:51, Serial0/0/0

192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.3.0/24 is directly connected, GigabitEthernet0/0

L 192.168.3.1/32 is directly connected, GigabitEthernet0/0

192.168.12.0/30 is subnetted, 1 subnets

O 192.168.12.0/30 [110/128] via 192.168.13.1, 00:07:41, Serial0/0/0

192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.13.0/30 is directly connected, Serial0/0/0

L 192.168.13.2/32 is directly connected, Serial0/0/0

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

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

L 192.168.23.2/32 is directly connected, Serial0/0/1

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

- Respuesta: S0/0/0

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

- Respuesta: 129

¿El R2 aparece como vecino OSPF en el R1?

- Respuesta: SI

¿El R2 aparece como vecino OSPF en el R3?

- Respuesta: NO

¿Qué indica esta información?

- Respuesta: Todo el tráfico hacia la red 192.168.2.0/24 desde el R3 se enrutará a través del R1.
- La interfaz S0/0/1 en el R2 sigue configurada como interfaz pasiva, por lo que la información de routing OSPF no se envía por esta interfaz.
- El costo acumulado de 129: Se debe a que el tráfico del R3 a la red 192.168.2.0/24 debe pasar a través de dos enlaces seriales T1 (1,544 Mb/s) (con un costo igual de 64 cada uno), además del enlace LAN Gigabit 0/0 del R2 (con un costo de 1).

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 ospf 1

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

```
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/1
R2(config-router)#
00:34:37: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from LOADING
 to FULL, Loading Done

R2(config-router)#
```

Imagen 132, comandos router ospf 1 y no passive-interface s0/0/1

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

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

Gateway of last resort is not set

     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, 00:27:15, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:00:29, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:00:29, Serial0/0/1
                        [110/128] via 192.168.13.1, 00:00:29, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
R3#
```

Imagen 133, comando show ip route en el R3

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

Gateway of last resort is not set

     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, 00:27:15, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:00:29, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:00:29, Serial0/0/1
                        [110/128] via 192.168.13.1, 00:00:29, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
R3#
```

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

Respuesta: S0/0/1

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

Respuesta: 65

Serial T1 (1,544 Mb/s) (con un costo de 64) + el enlace LAN Gigabit 0/0 del R2 (con un costo de 1).

¿El R2 aparece como vecino OSPF del R3? Respuesta: SI

- **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.

- **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.

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

```
R1#show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 000d.bd8d.d001 (bia 000d.bd8d.d001
)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); 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 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 1017 multicast, 0 pause input
     0 input packets with dribble condition detected
     30 packets output, 1920 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R1#
```

Imagen 134, R1# show interface g0/0 para ver la configuración del ancho de banda G 0/0

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.

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

```
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 00:16:59, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:35:29, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 00:16:59, Serial0/0/1
                     [110/128] via 192.168.12.2, 00:16:59, Serial0/0/0
R1#
```

Imagen 135, comando show ip route ospf en el R1 para determinar la ruta a la red 192.168.3.0/24.

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

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 Cost Disabled Shutdown Topology Name

0 1 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 00:00:05

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)

```
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: 1
  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)
R3#
```

Imagen 136, comando show ip ospf interface en el R3 determinar el costo de routing para G0/0.

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	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 00:00:04

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)

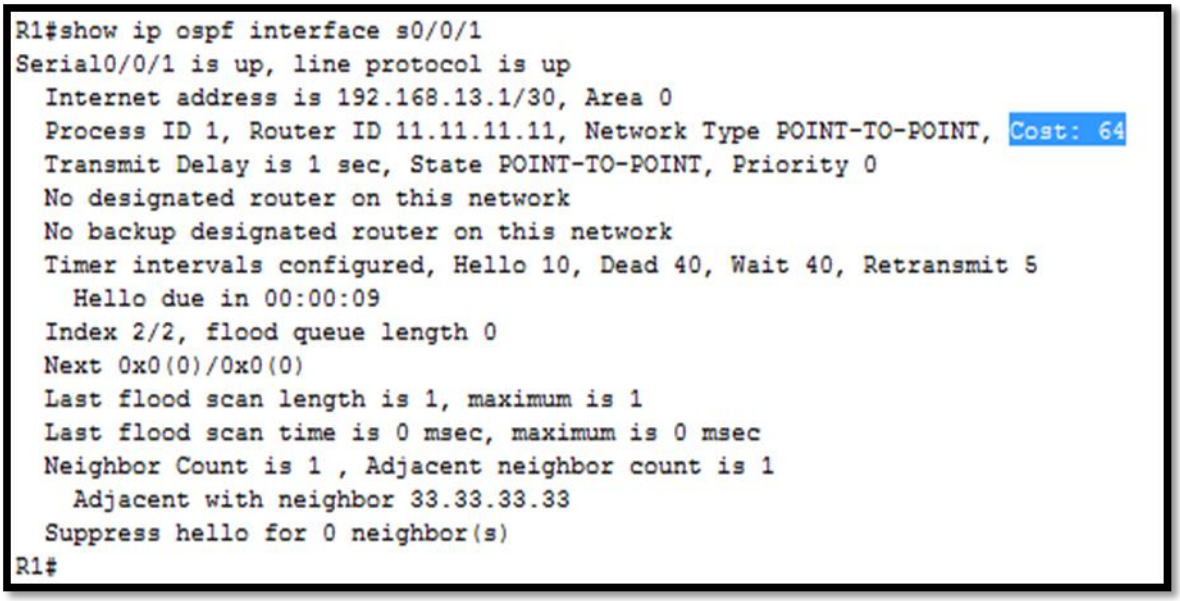


Imagen 137, comando show ip ospf interface s0/0/1 en el R1 para ver el costo de routing para S0/0/1.

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**.

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.
```

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

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   Cost    Disabled    Shutdown      Topology Name
        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)
```

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   Cost    Disabled    Shutdown      Topology Name
        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)

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.

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?

Esto se hace con el fin de calcular exactamente las métricas con los datos correctos, recordemos que estos equipos calculan los mismos con datos predeterminados.

- **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.

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>

```
R1#show interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 54 bits/sec, 0 packets/sec
  5 minute output rate 54 bits/sec, 0 packets/sec
     99 packets input, 6968 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     95 packets output, 6528 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R1#
```

Imagen 138, comando show interface s0/0/0 en el R1 para ver la configuración actual del ancho de banda de S0/0/0.

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

R1# **show ip route ospf**

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

```
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 00:15:33, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:15:43, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.12.2, 00:15:33, Serial0/0/0
                     [110/128] via 192.168.13.2, 00:15:33, Serial0/0/1
R1#
```

Imagen 139, 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

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

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

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

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

Imagen 140, comando bandwidth 128 para establecer el ancho de banda en S0/0/0 en 128 Kb/s

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

```
R1#show ip route ospf
O    192.168.2.0 [110/129] via 192.168.13.2, 00:00:37, Serial0/0/1
O    192.168.3.0 [110/65] via 192.168.13.2, 00:18:05, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 00:00:37, Serial0/0/1
R1#
```

Imagen 141, comando show ip route ospf sin la ruta 192.168.23.0/24

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	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	781	P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0

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

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

Imagen 142, ancho de banda de la interfaz S0/0/1 similar que S0/0/0

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

R1# **show ip route ospf**

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 [110/782] 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

```
R1#show ip route ospf
O    192.168.2.0 [110/782] via 192.168.12.2, 00:01:04, Serial0/0/0
O    192.168.3.0 [110/782] via 192.168.13.2, 00:01:04, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/845] via 192.168.12.2, 00:01:04, Serial0/0/0
                     [110/845] via 192.168.13.2, 00:01:04, Serial0/0/1
R1#
```

Imagen 143, comando show ip route ospf para ver el costo acumulado de ambas rutas a la red 192.168.23.0/24.

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.

Costo a 192.168.3.0/24:

- S0/0/1 del R1 + G0/0 del R3 (781+1=782).

Costo a 192.168.23.0/30:

- S0/0/1 del R1 y S0/0/1 del R3 (781+64=845).

Emita el comando **show ip route ospf** en el R3. El costo acumulado de 192.168.1.0/24 todavía se muestra como 65. A diferencia del comando **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

```
R3#show ip route ospf
O    192.168.1.0 [110/65] via 192.168.13.1, 00:26:50, Serial0/0/0
O    192.168.2.0 [110/65] via 192.168.23.1, 00:26:50, Serial0/0/1
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0 [110/845] via 192.168.13.1, 00:09:16, Serial0/0/0
R3#
```

Imagen 144, comando show ip route ospf en el R3. El costo acumulado de 192.168.1.0/24

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

```
R3(config)#interface s0/0/0
R3(config-if)#band?
bandwidth
R3(config-if)#band
R3(config-if)#bandwidth 128
R3(config-if)#interface s0/0/1
R3(config-if)#bandwidth 128
```

Imagen 145, 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?

Respuesta: 1562.
Porque Cada enlace serial tiene un costo de 781 y la ruta a la red 192.168.23.0/24 atraviesa dos enlaces seriales.
781 + 781 = 1562.

- **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.

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

```
R1#show ip route ospf
O    192.168.2.0 [110/782] via 192.168.12.2, 00:09:40, Serial0/0/0
O    192.168.3.0 [110/782] via 192.168.13.2, 00:09:40, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:01:26, Serial0/0/0
                     [110/1562] via 192.168.13.2, 00:01:26, Serial0/0/1
R1#
```

Imagen 146, R1# show ip route ospf

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

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

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

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

Imagen 147, comando ip ospf cost 1565 a la interfaz S0/0/1 en el R1

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, Serialg0/0/0

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

```
R1#show ip route ospf
O    192.168.2.0 [110/782] via 192.168.12.2, 00:11:34, Serial0/0/0
O    192.168.3.0 [110/1563] via 192.168.12.2, 00:00:27, Serial0/0/0
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:00:27, Serial0/0/0
R1#
```

Imagen 148, R1# show ip route ospf

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.

OSPF elige la ruta con el menor costo acumulado. La ruta con el menor costo acumulado es:
S0/0/0 del R1 + S0/0/1 del R2 + G0/0 del R3, o 781 + 781 + 1 = 1563.
S0/0/1 R1 + G0/0 R3, o 1565 + 1 = 1566.
De esta manera observamos claramente cual de estas es la ruta con menor costo acumulado.

Reflexión

1. ¿Por qué es importante controlar la asignación de ID de router al utilizar el protocolo OSPF?
   El ID es el que permite la elección del router ID y BDR.

2. ¿Por qué el proceso de elección de DR/BDR no es una preocupación en esta práctica de laboratorio?
   Este es fundamental en su configuración para las redes de acceso multiple.
   ¿Por qué querría configurar una interfaz OSPF como pasiva?
   Para no enviar información de ruteo innecesaria.

Tabla 4:

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.

- La configuración de rutas estáticas predeterminadas tanto en IPv4 como IPv6 simula el acceso a internet de las redes y permite la conectividad de extremo a extremo.

- El protocolo RIPv2 soporta la implementación de VLSM, tiene un alcance de máximo 15 saltos y las actualizaciones de enrutamientos las establece a través de multicast.

- La configuración de NAT hace uso de una dirección global pública para transmitir los paquetes, mientras que la configuración de PAT hace uso de interfaces para la trasmisión de paquetes.

8.3.3.6 Lab - Configuring Basic Single-Area Ospfv3

Topología

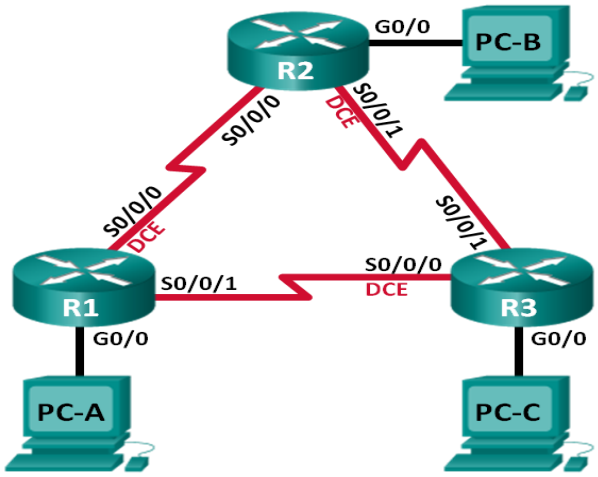


Imagen 149, Topología

Tabla 5:
Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

Información básica/situación

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

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

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

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

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 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.

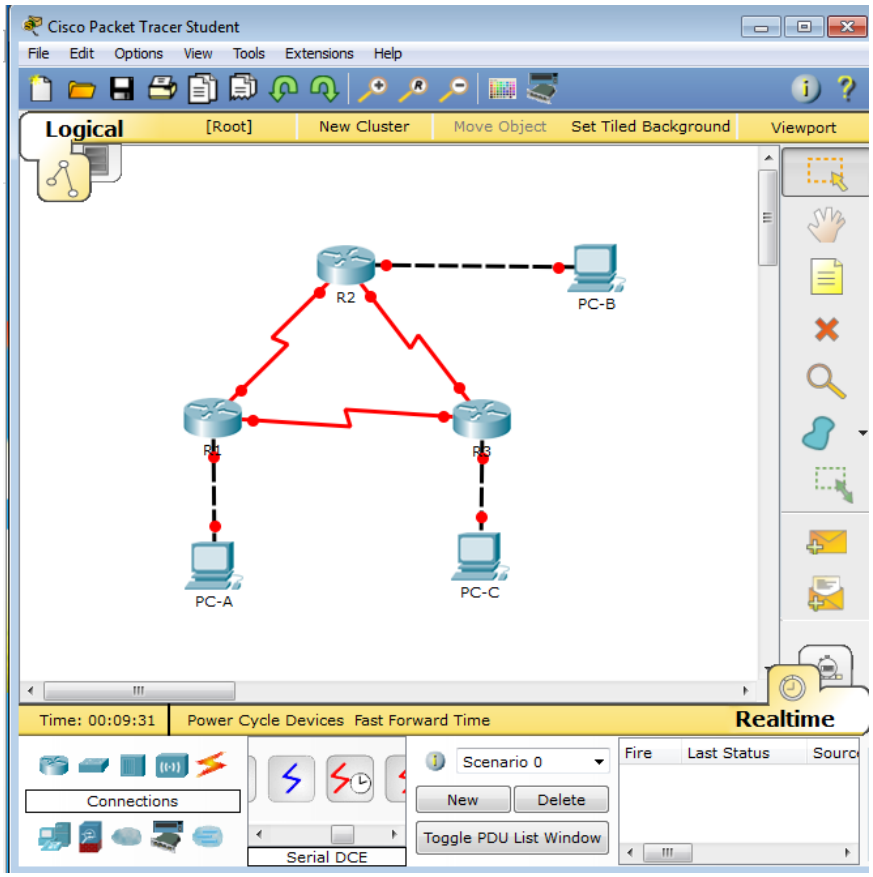


Imagen 150, topología implementada en Cisco Packet tracer

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

Paso 3. Configurar los parámetros básicos para cada router.

Desactive la búsqueda del DNS.

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

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

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

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

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

Cifre las contraseñas de texto no cifrado.

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

Habilite el routing de unidifusión IPv6 en cada router.

Copie la configuración en ejecución en la configuración de inicio

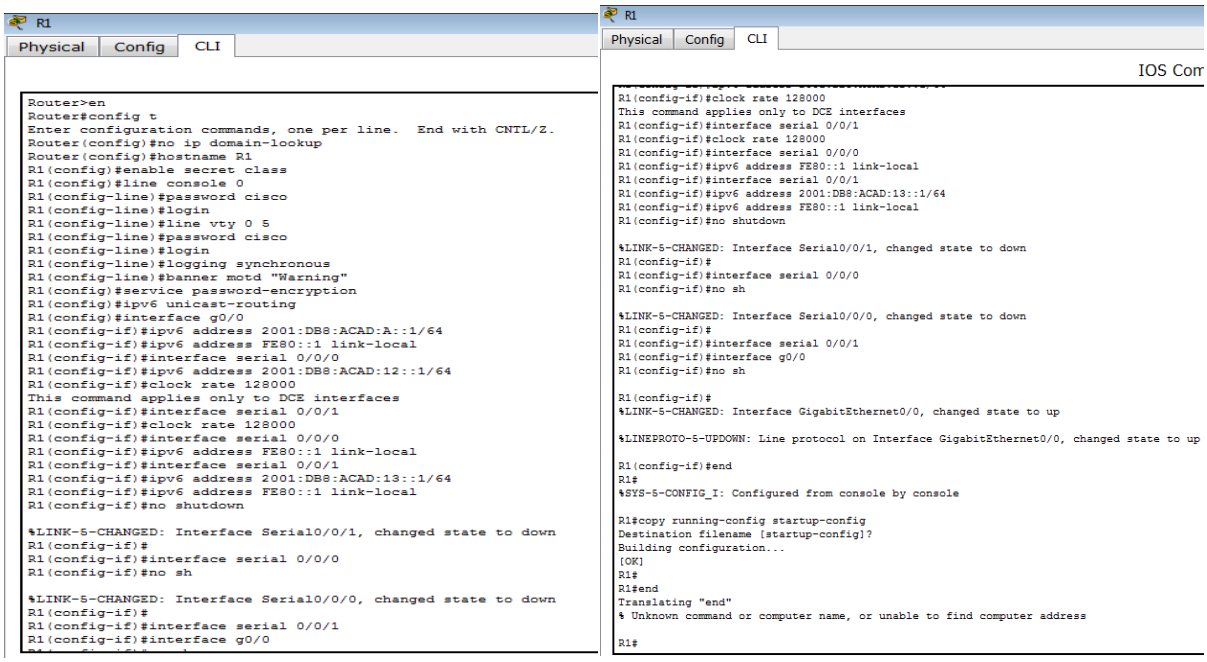


Imagen 151, configuración básica del router 1

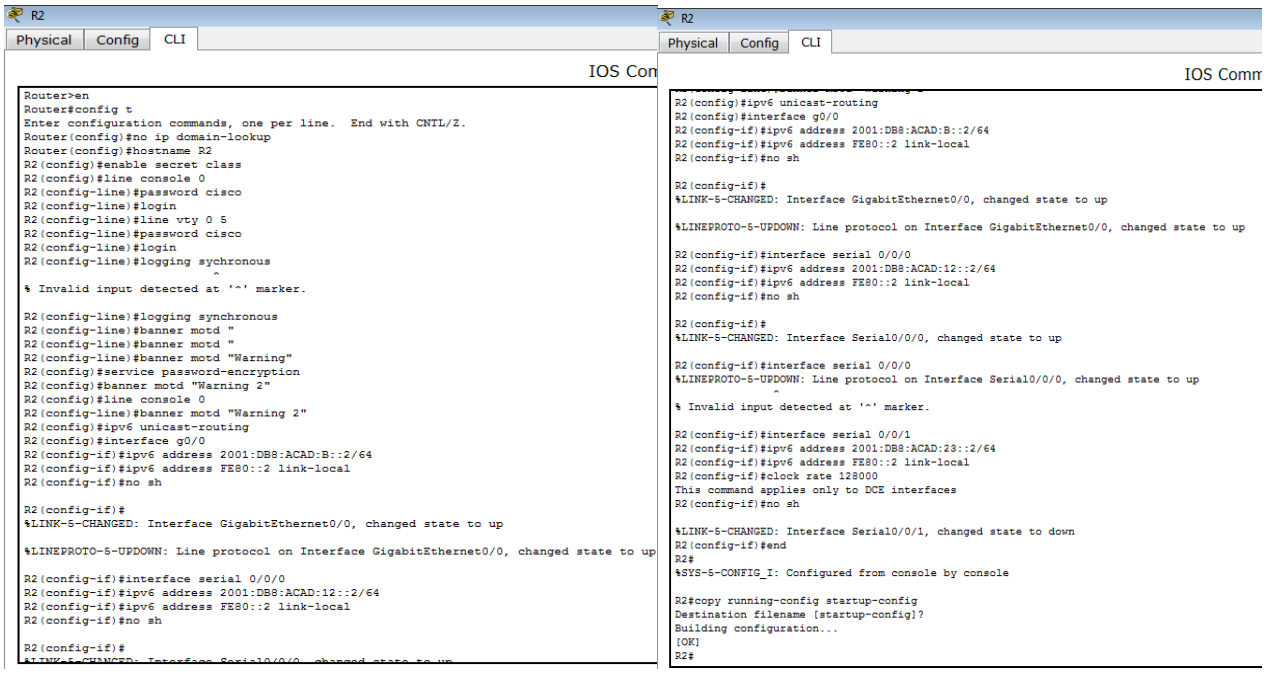


Imagen 152, configuración básica del router 2

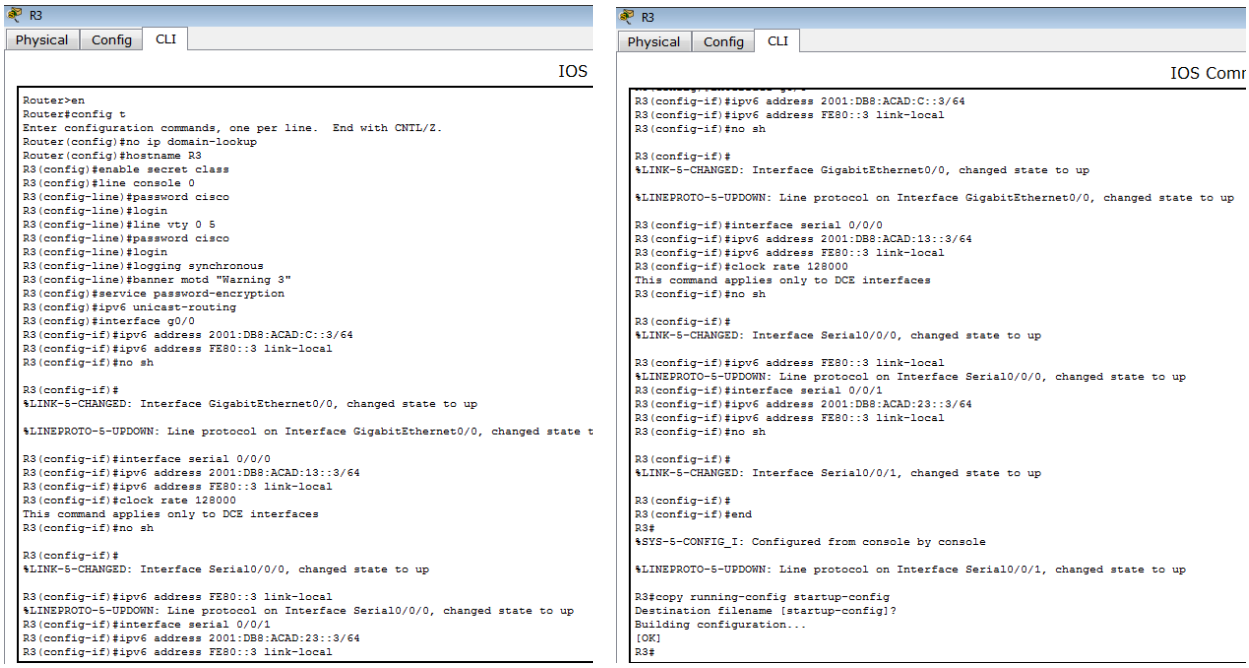


Imagen 153, configuración básica del router 3

Paso 4. Configurar los equipos host.

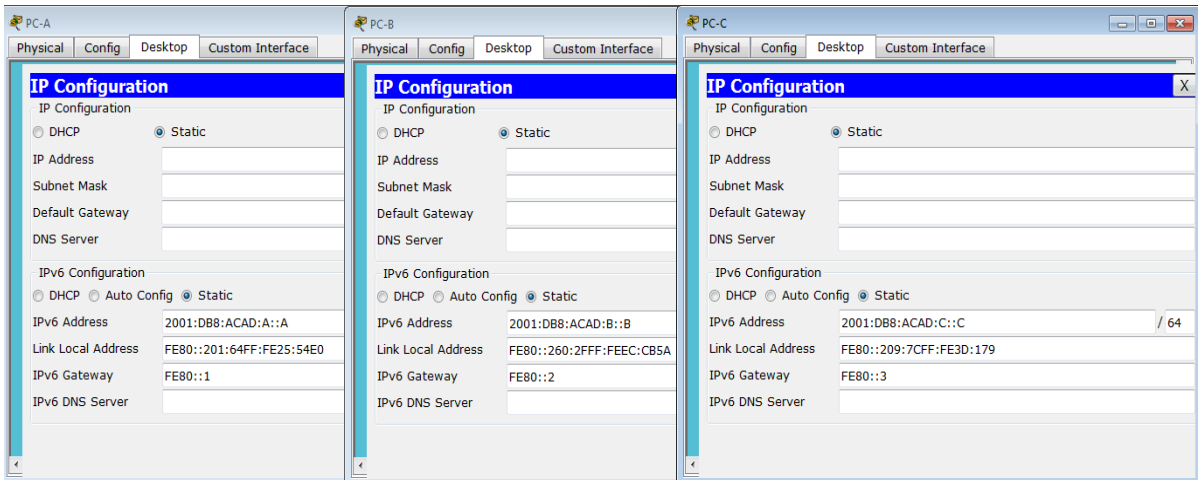


Imagen 154, configuración básica de los PC-A-B-C

Paso 5. Probar la conectividad.

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

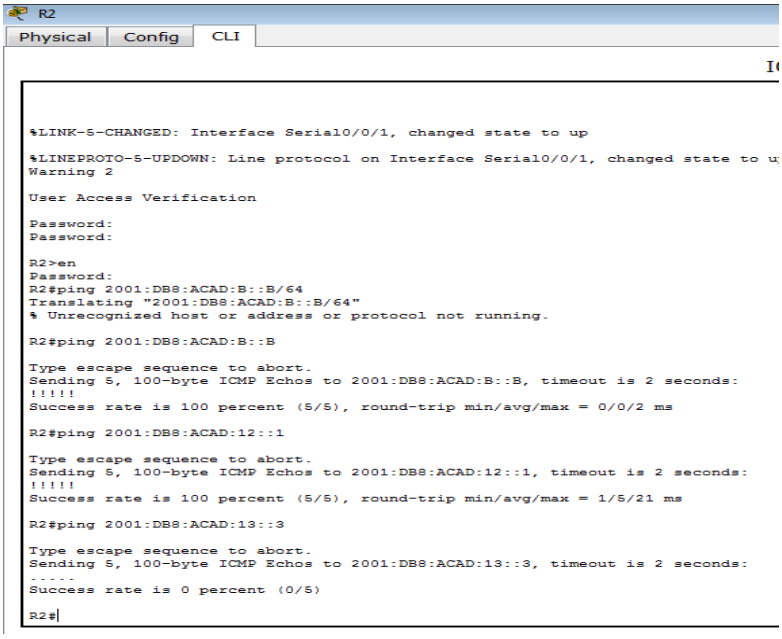


Imagen 155, Ping a los routers

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**.

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

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

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

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

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

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.

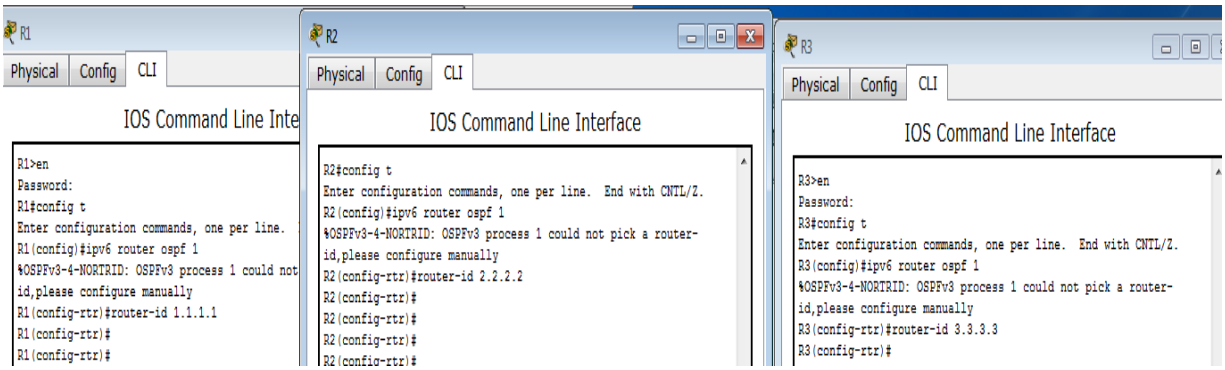


Imagen 156, asignación de id a los routers1,2,3

Emita el comando **show ipv6 ospf** para verificar las ID de router de todos los routers 1, 2, 3.

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>

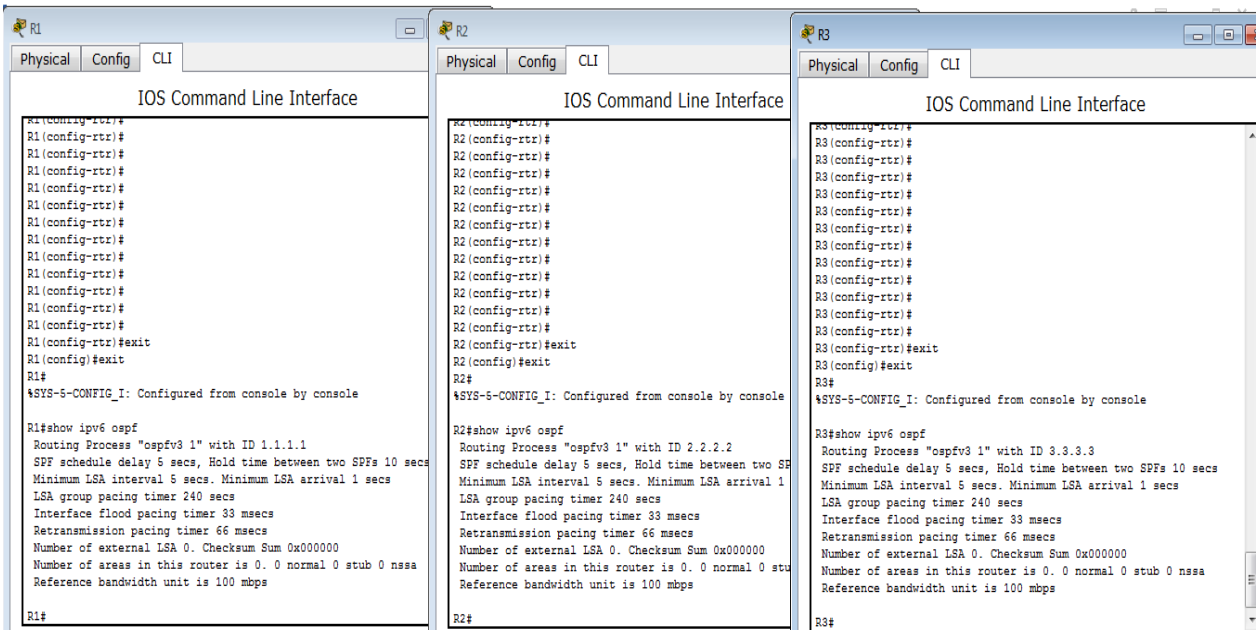


Imagen 157, verificación de los id a los routers 1,2,3

Paso 2. Configurar OSPFv6 en el R1.

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

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

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

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

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

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

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

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

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

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

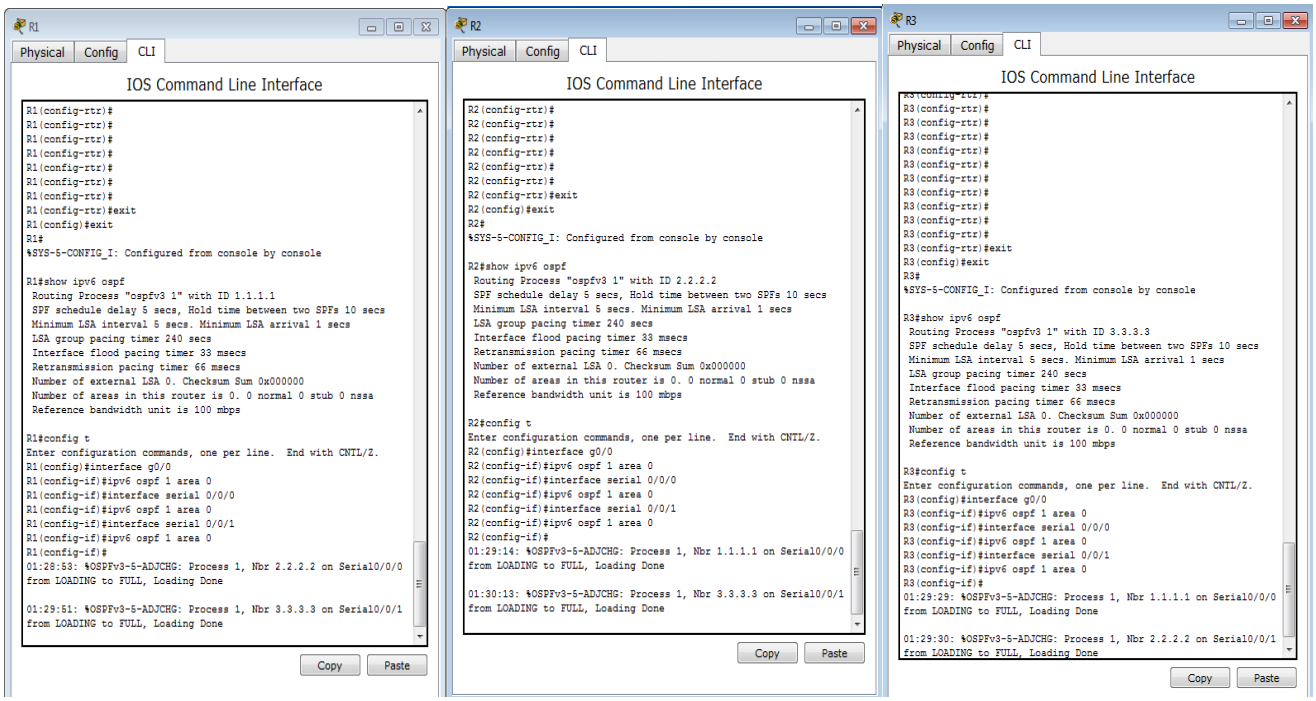


Imagen 158, configurar OSPFv6 en el R1, R2, R3.

Paso 3. Verificar vecinos de OSPFv3.

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

R1# **show ipv6 ospf neighbor**

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

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

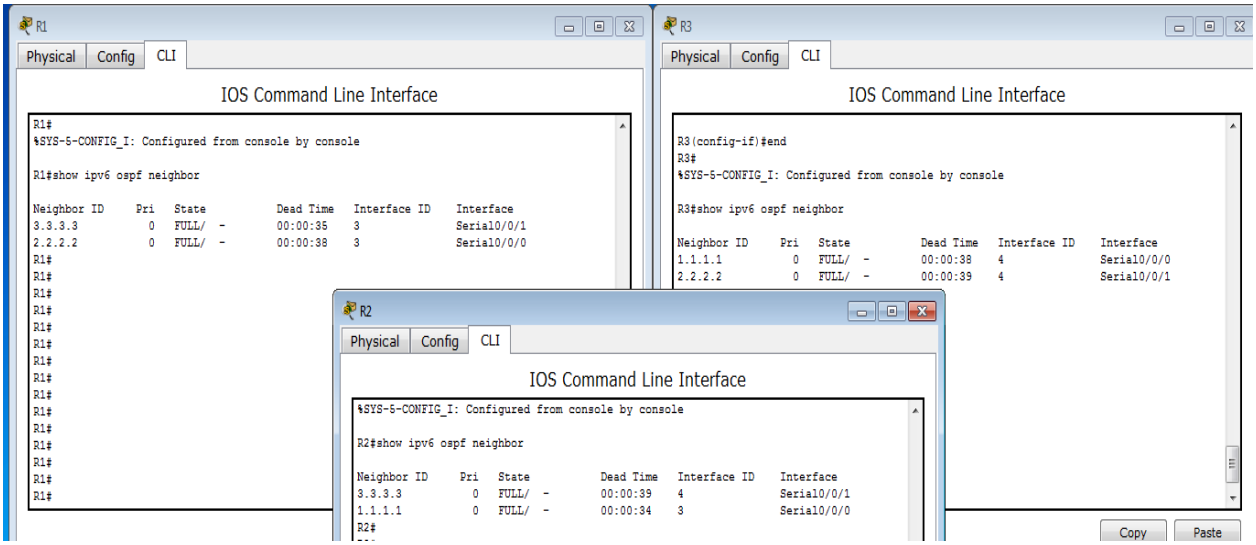


Imagen 159, verificar vecinos de OSPFv3.

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

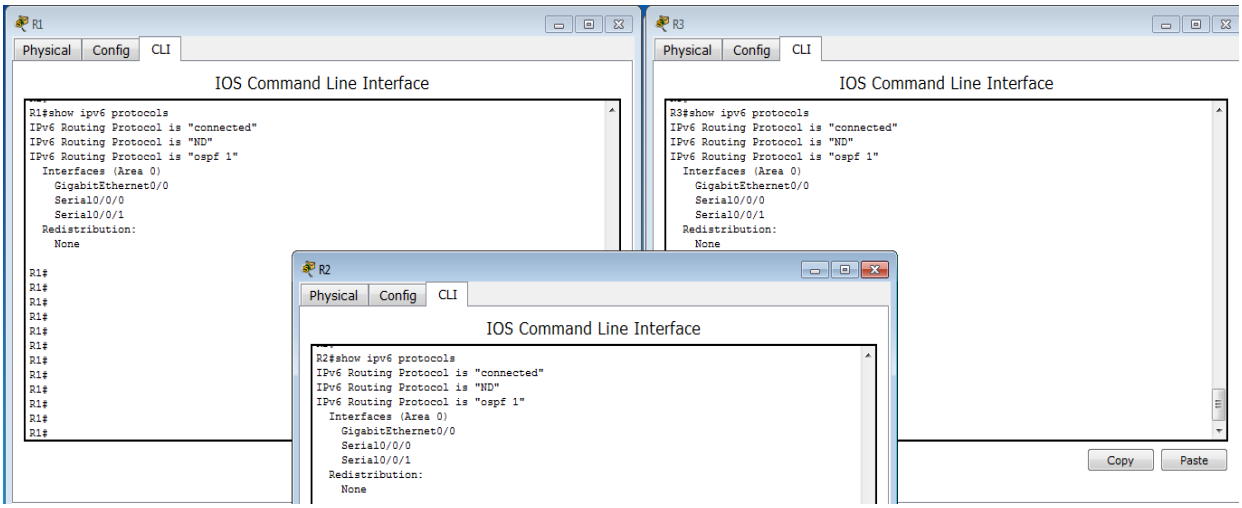


Imagen 160, verificar la configuración del protocolo OSPFv en los routers 1,2,3.

Paso 5. Verificar las interfaces OSPFv3.

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

R1# **show ipv6 ospf interface**

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

Link Local Address FE80::1, Interface ID 7

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

Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

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

Hello due in 00:00:05

Graceful restart helper support enabled

Index 1/3/3, flood queue length 0

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

Last flood scan length is 1, maximum is 1

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

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 3.3.3.3

Suppress hello for 0 neighbor(s)

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

Link Local Address FE80::1, Interface ID 6

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

Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

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

Hello due in 00:00:00

Graceful restart helper support enabled

Index 1/2/2, flood queue length 0

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

Last flood scan length is 1, maximum is 2

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

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 2.2.2.2

Suppress hello for 0 neighbor(s)

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3

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

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

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

No backup designated router on this network

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

Hello due in 00:00:03

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

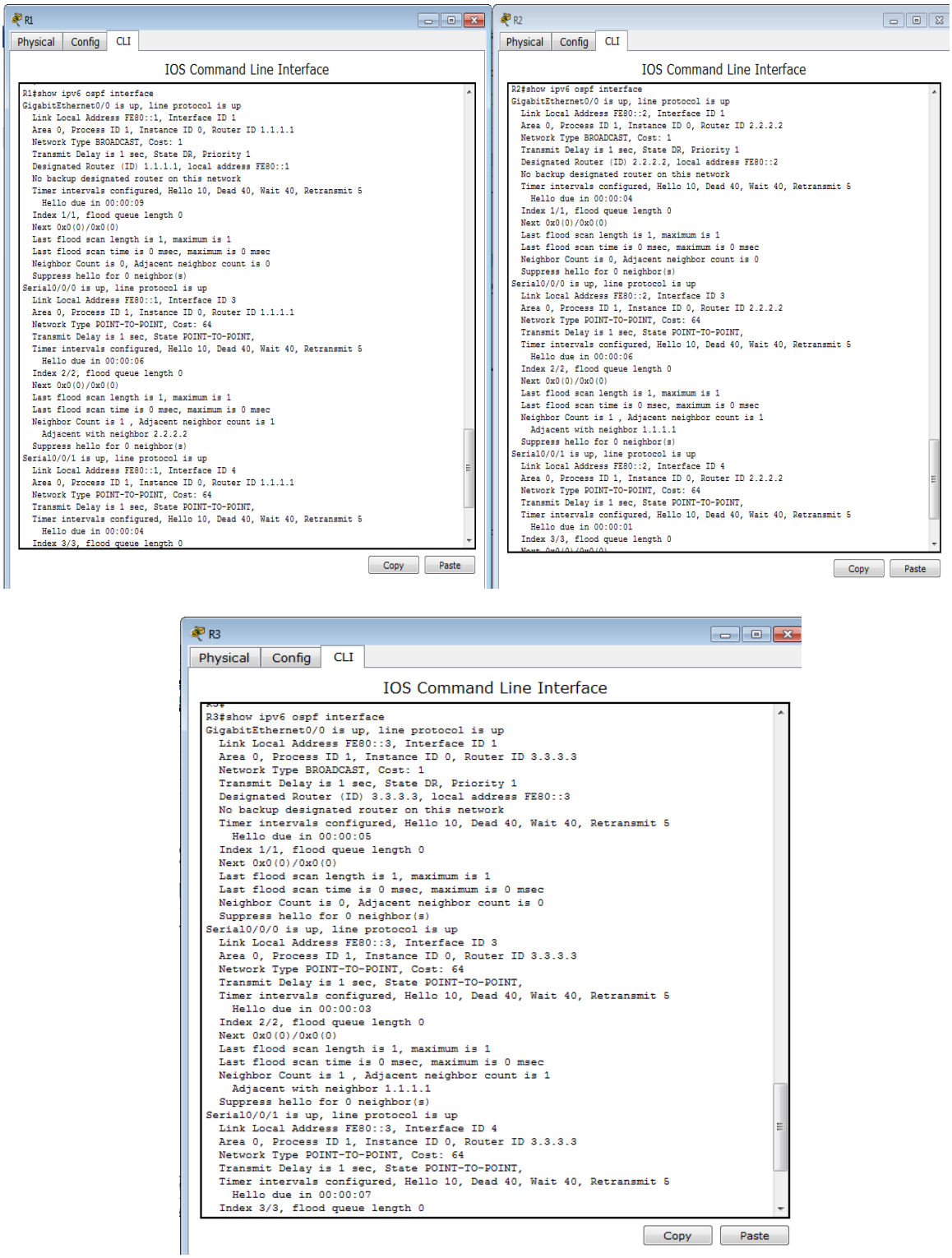


Imagen 161, verificar las interfaces OSPFv en los routers 1,2,3

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

R1# **show ipv6 ospf interface brief**

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

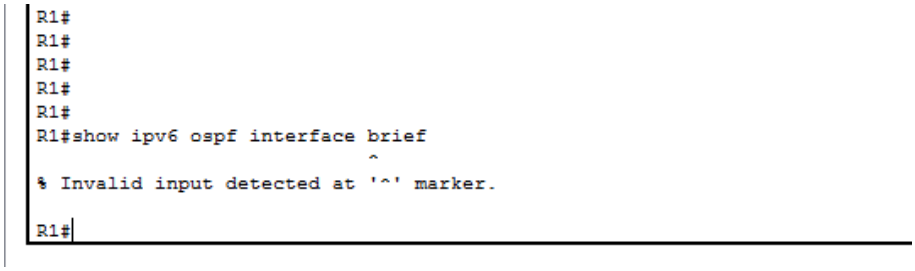


Imagen 162, Cisco no soporta el comando para ver el resumen de OSPF

Paso 6. Verificar la tabla de routing IPv6.

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

R2# **show ipv6 route**

IPv6 Routing Table - default - 10 entries

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

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

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

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

```
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:DB8:ACAD:A::/64 [110/65]
     via FE80::1, Serial0/0/0
C    2001:DB8:ACAD:B::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L    2001:DB8:ACAD:B::2/128 [0/0]
     via GigabitEthernet0/0, receive
O   2001:DB8:ACAD:C::/64 [110/65]
     via FE80::3, Serial0/0/1
C    2001:DB8:ACAD:12::/64 [0/0]
     via Serial0/0/0, directly connected
L    2001:DB8:ACAD:12::2/128 [0/0]
     via Serial0/0/0, receive
O   2001:DB8:ACAD:13::/64 [110/128]
     via FE80::3, Serial0/0/1
     via FE80::1, Serial0/0/0
C    2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L    2001:DB8:ACAD:23::2/128 [0/0]
     via Serial0/0/1, receive
L    FF00::/8 [0/0]
```

via Null0, receive

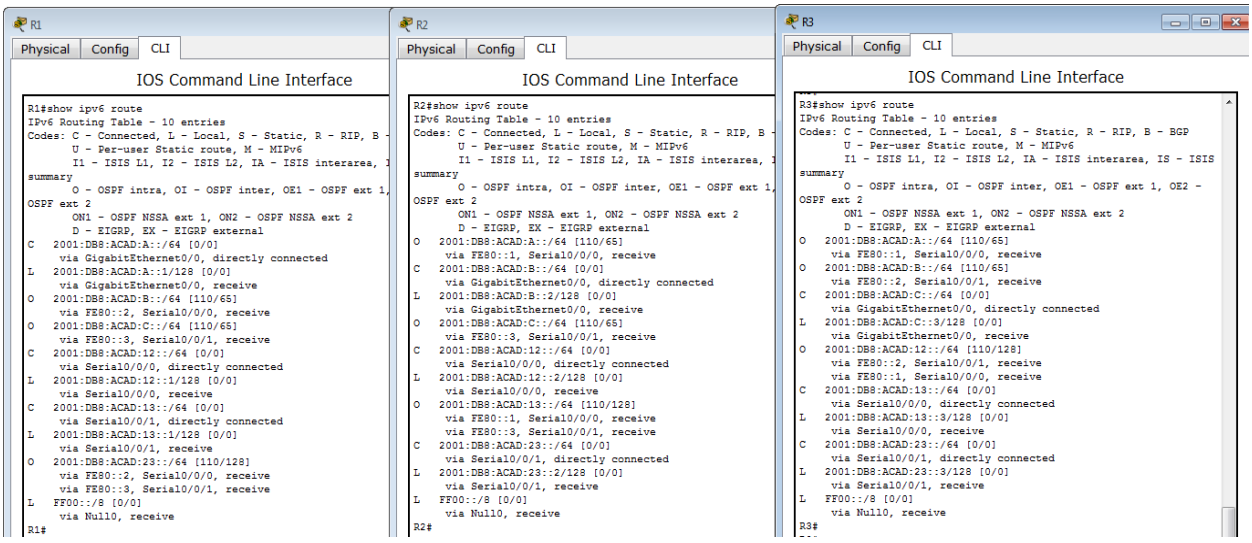


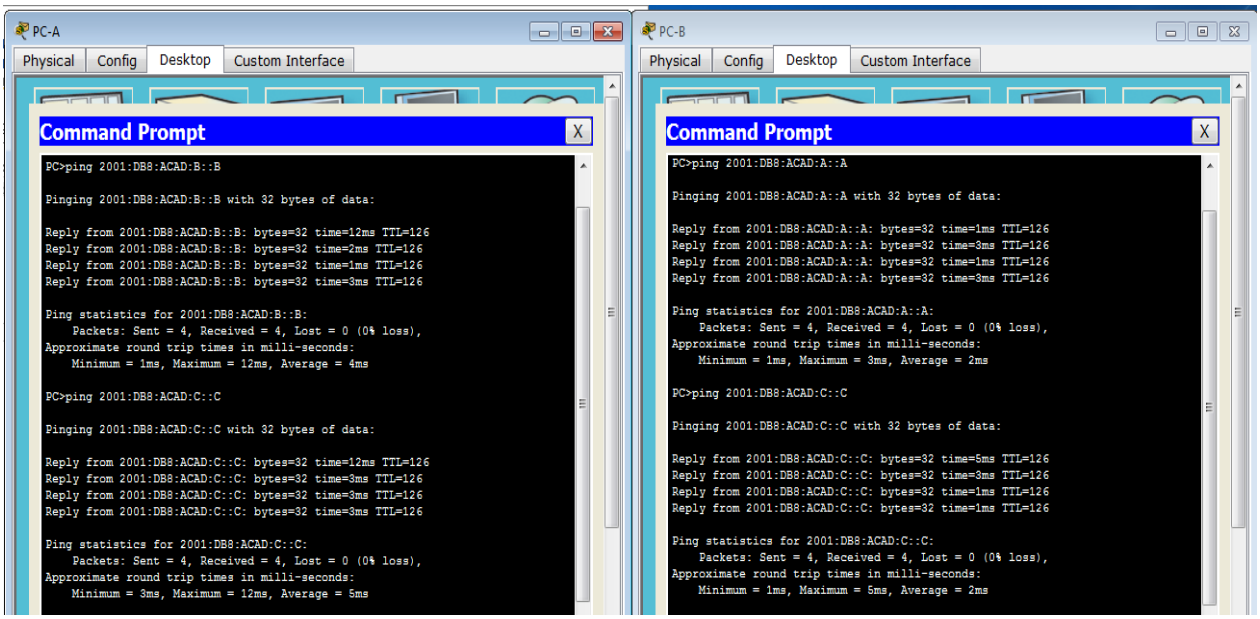
Imagen 163, tabla de routing IPV6

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

Respuesta: show ipv6 route ospf

Paso 7. Verificar la conectividad de extremo a extremo.

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



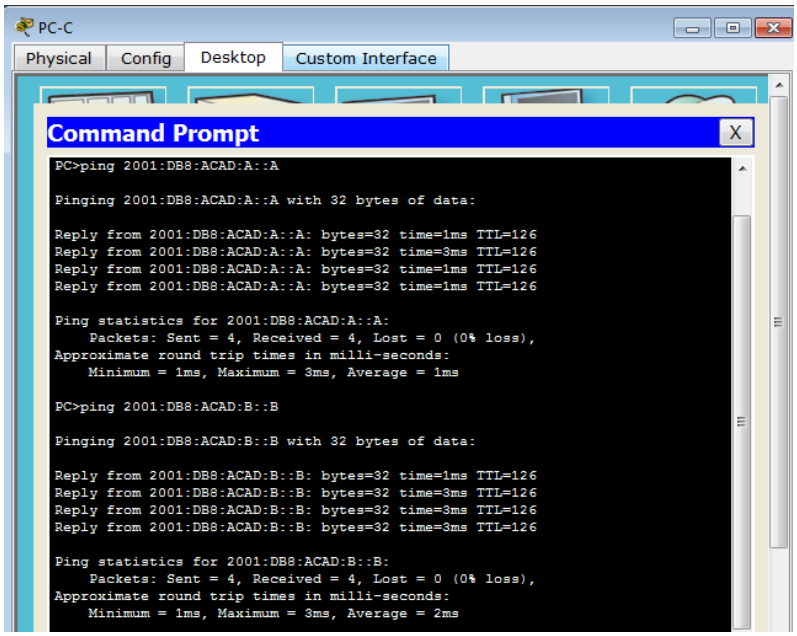


Imagen 164, Ping entre PC-A-B-C

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

Parte. 3. Configurar las interfaces pasivas de ospfv3

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

Paso 1. Configurar una interfaz pasiva.

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

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

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3

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

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

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

No backup designated router on this network

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

Hello due in 00:00:05

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

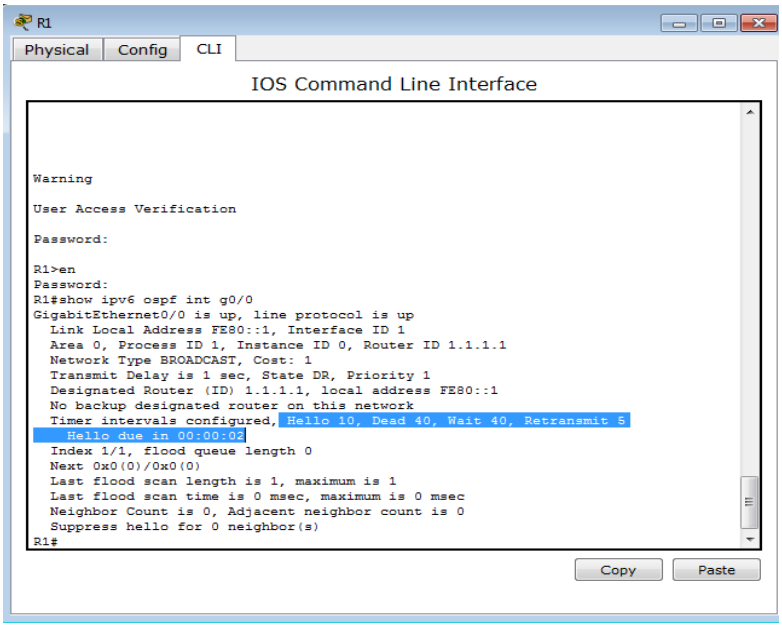


Imagen 165, temporizador en R1

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

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

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

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

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

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3

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

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State WAITING, Priority 1

No designated router on this network

No backup designated router on this network

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

No Hellos (Passive interface)

Wait time before Designated router selection 00:00:34

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

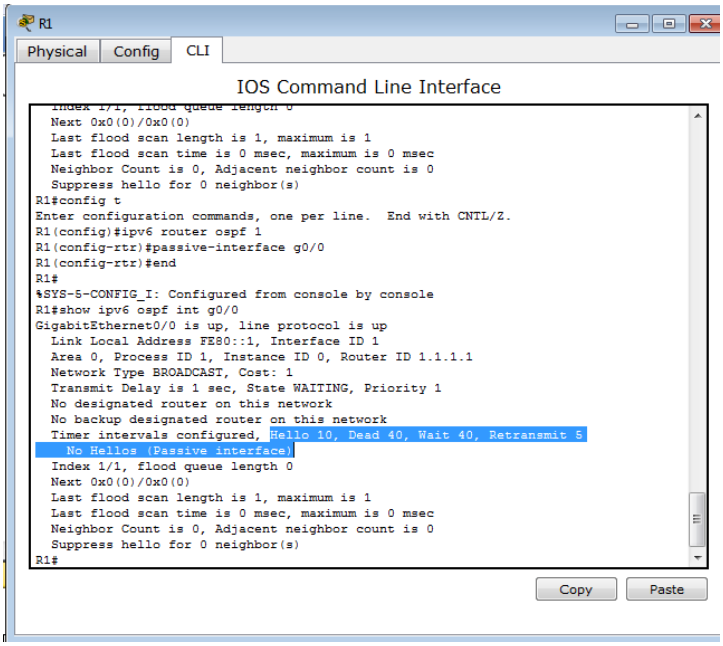


Imagen 166, Configuración de la interface pasiva en R1

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

R2# **show ipv6 route ospf**

IPv6 Routing Table - default - 10 entries

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

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

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

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

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

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

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

via FE80::1, Serial0/0/0

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

via FE80::3, Serial0/0/1

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

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

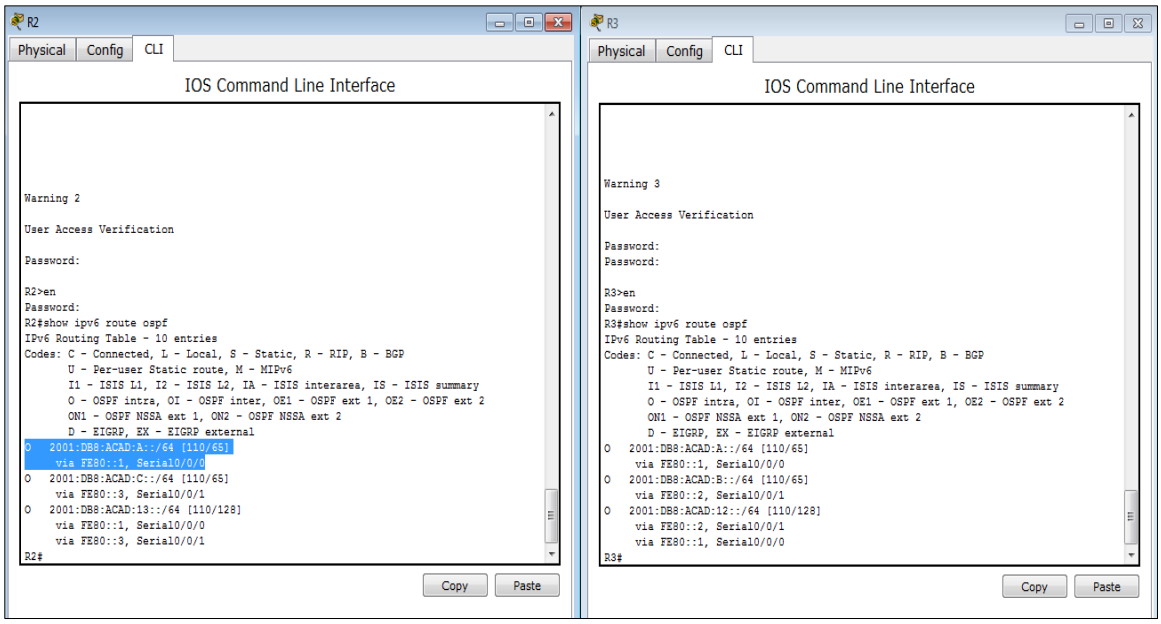


Imagen 167, comando show ipv6 route ospf en R2 y R3

Paso 2. Establecer la interfaz pasiva como la interfaz predeterminada en el router.

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

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

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

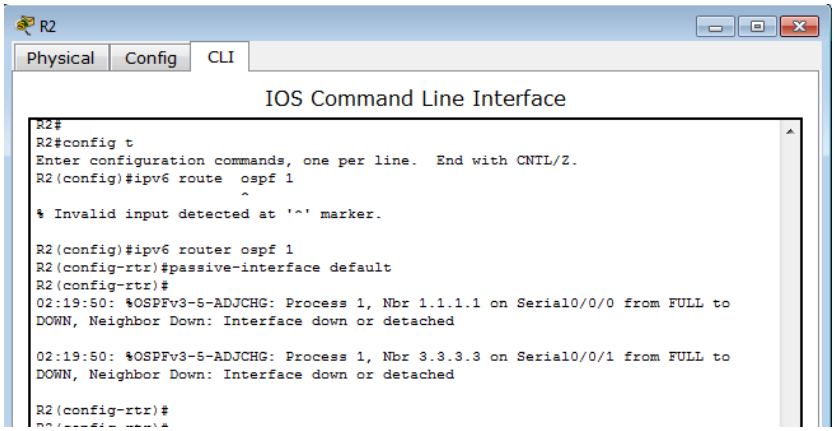


Imagen 168, la interfaz pasiva como la interfaz predeterminada en el router R2

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

R1# **show ipv6 ospf neighbor**

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

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

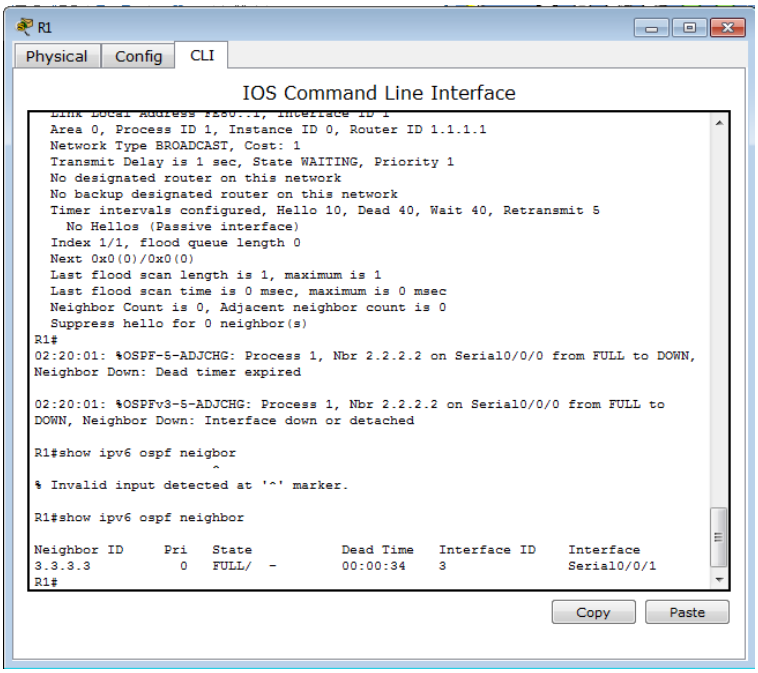


Imagen 169, comando show ipv6 ospf neighbor en R1

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

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

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

Link Local Address FE80::2, Interface ID 6

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

Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

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

No Hellos (Passive interface)

Graceful restart helper support enabled

Index 1/2/2, flood queue length 0

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

Last flood scan length is 2, maximum is 3

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

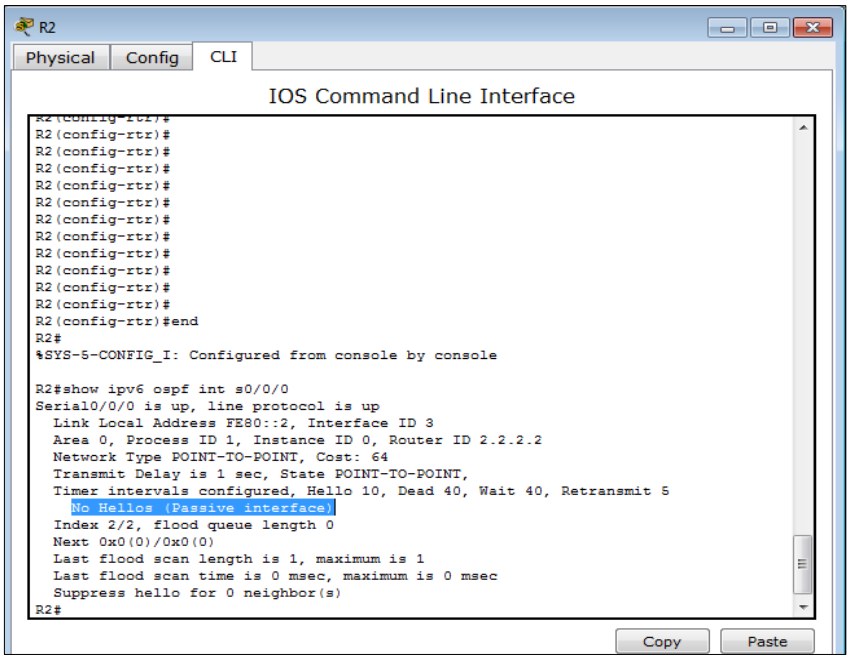


Imagen 170, comando show ipv6 ospf interface s0/0/0 en R2

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**.

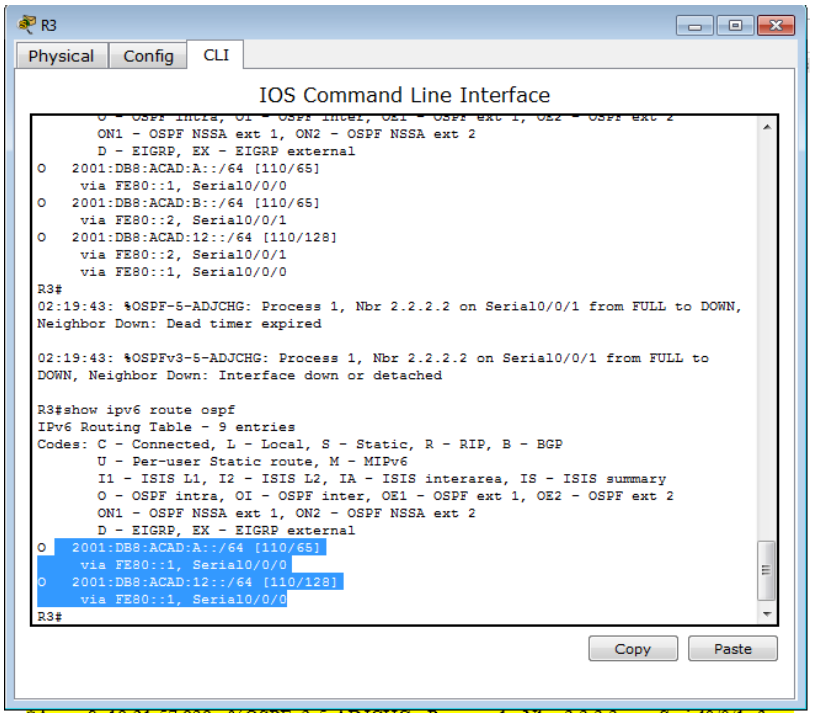


Imagen 171, la Ruta en R2 no se encuentra.

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

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

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

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

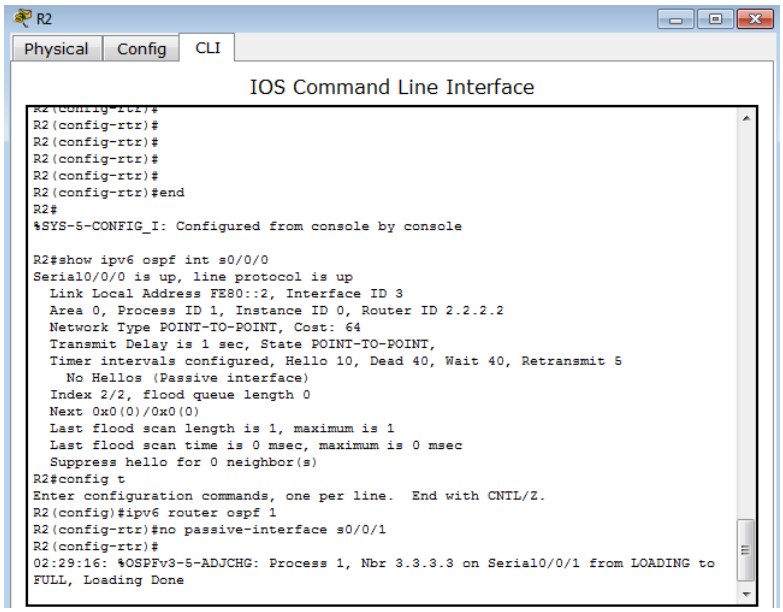


Imagen 172, actualización de Ospf

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

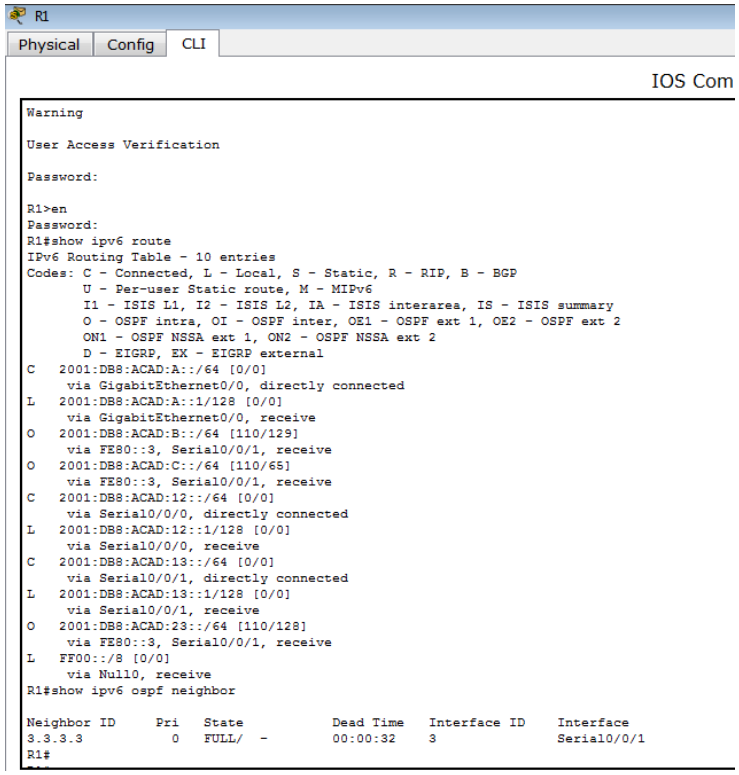


Imagen 173, show ipv6 route y show ipv6 ospf neighbor en R1

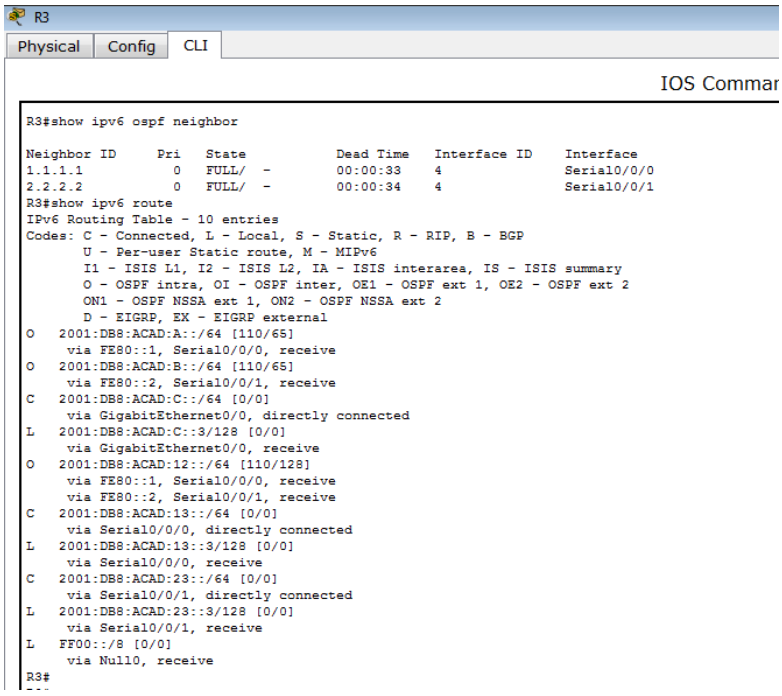


Imagen 174, show ipv6 route y show ipv6 ospf neighbor en R3

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64?

Respuesta: Serial 0/0/1

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

Respuesta: 129

¿El R2 aparece como vecino OSPFv3 en el R1?

Respuesta: Solo esta R3

¿El R2 aparece como vecino OSPFv3 en el R3?

Respuesta: si

¿Qué indica esta información?

Respuesta: todo el tráfico hacia la red B desde R1 será ruteado a través de R3, la interfaz serial 0/0/0 en R2 está configurada como pasiva de tal manera que OSPF v3 no manda información de ruteo notificándose a través de esta interfaz, el costo 129 acumulado resulta del tráfico que pasa por R3, este tráfico pasa por dos serialesT1 de un costo de 64 cada 1 y más una interfaz gigabit de la interface LAN con el costo de 1.

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

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

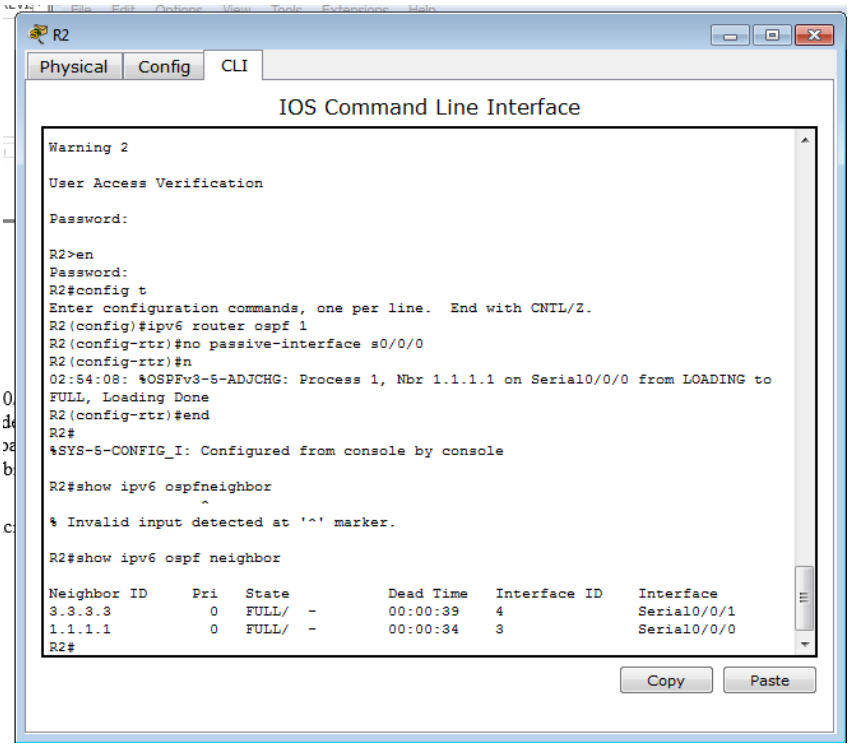


Imagen 175, literal g y h

Reflexión

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

   Rta/Si, por que el proceso de OSPF es solamente usando y es significativamente local en un router, no necesita coincidir el proceso usando en otro router en la misma área.

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

   Rta/Removiendo la entrada Network ayuda a prevenir los errores en las direcciones Ipv6 en la interface Ipv6 puede tener múltiples direcciones asignadas a ella.

Tabla 6:

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.

- Con la práctica realizada se aprendió a armar la red y configurar los parámetros básicos de los dispositivos, configurar y verificar el routing OSPFv3 y configurar interfaces pasivas OSPFv3
- De igual manera se comprendió que 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 y con esta práctica de laboratorio, se configuro la topología de la red con routing OSPFv3 y se asignó el ID de los Routers.

9.2.1.10 Packet Tracer Configuring Standard Acls Instructions Ig

Topology

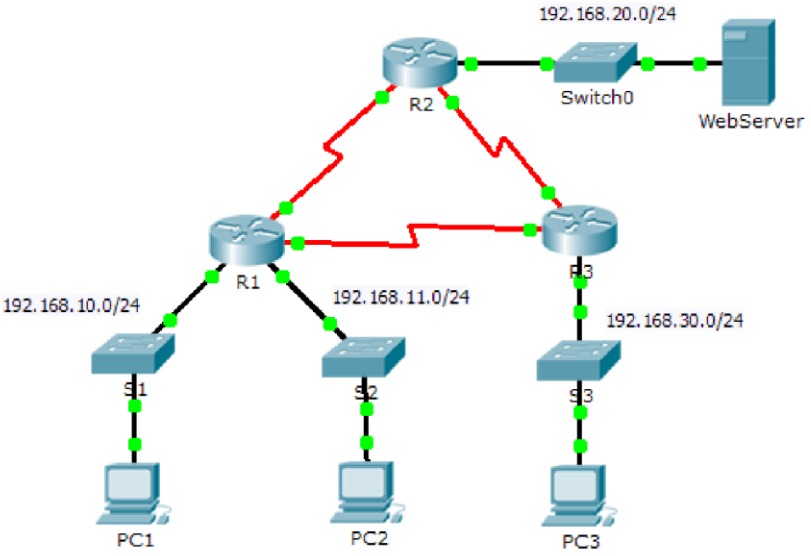


Imagen 176. Topología.

Tabla 7:

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

Objectives

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

Background / Scenario

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

Parte 1: Plan an acl implementation.

Paso 1. Investigate the current network configuration.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.

Paso 2. Evaluate two network policies and plan ACL implementations.

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

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

To restrict access from the 192.168.11.0/24 network to the **WebServer** at 192.168.20.254 without interfering with other traffic, an ACL must be created

on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

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

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

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

Parte 2. Configure, apply, and verify a standard acl

Paso 1. Configure and apply a numbered standard ACL on R2.

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

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

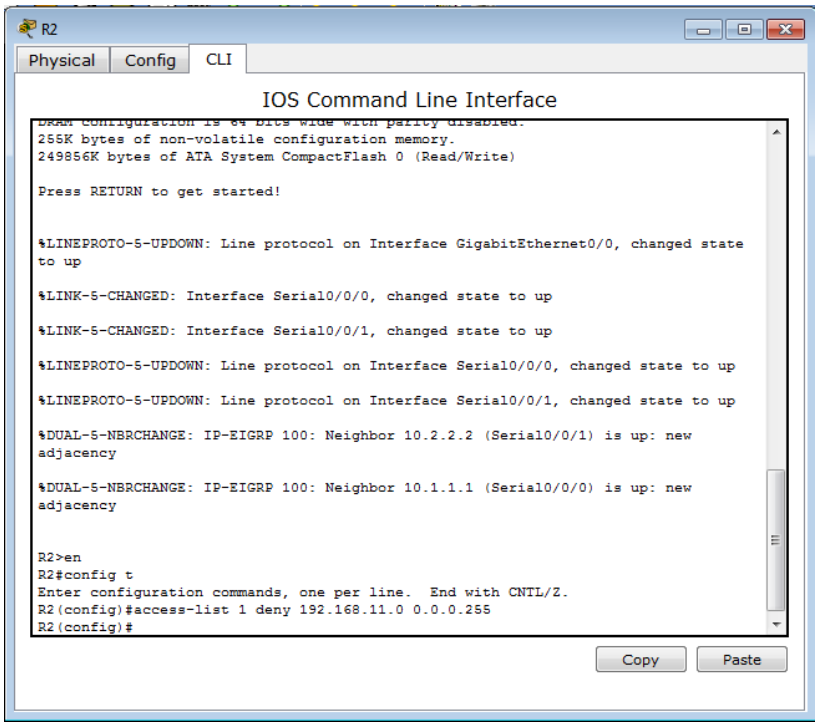


Imagen 177, configuración ACL en R2

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

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

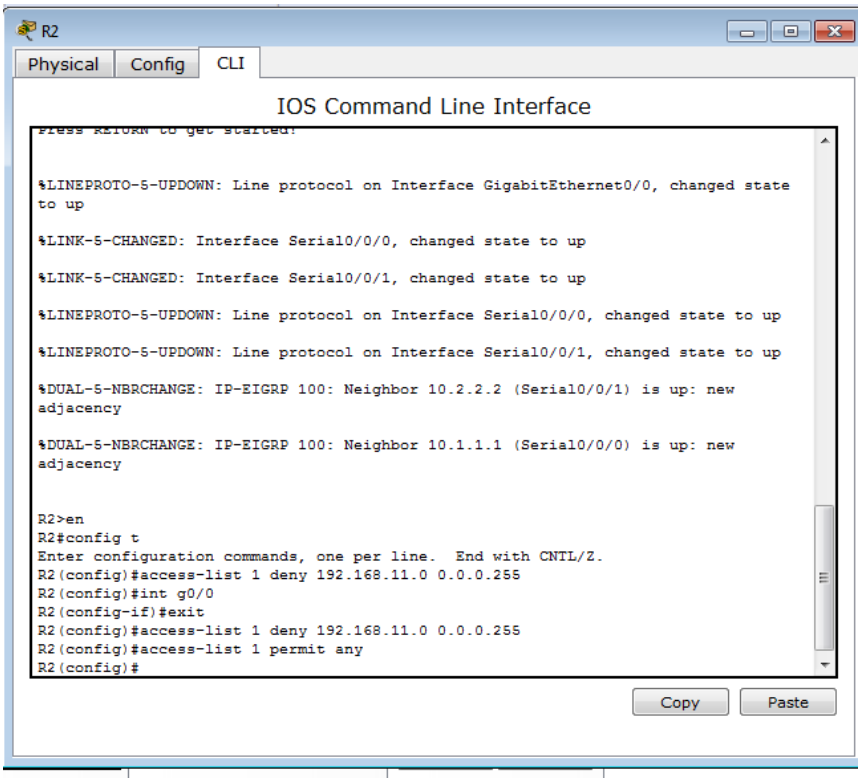


Imagen 178, configuración ACL en R2

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

R2(config)# **interface GigabitEthernet0/0**

R2(config-if)# **ip access-group 1 out**

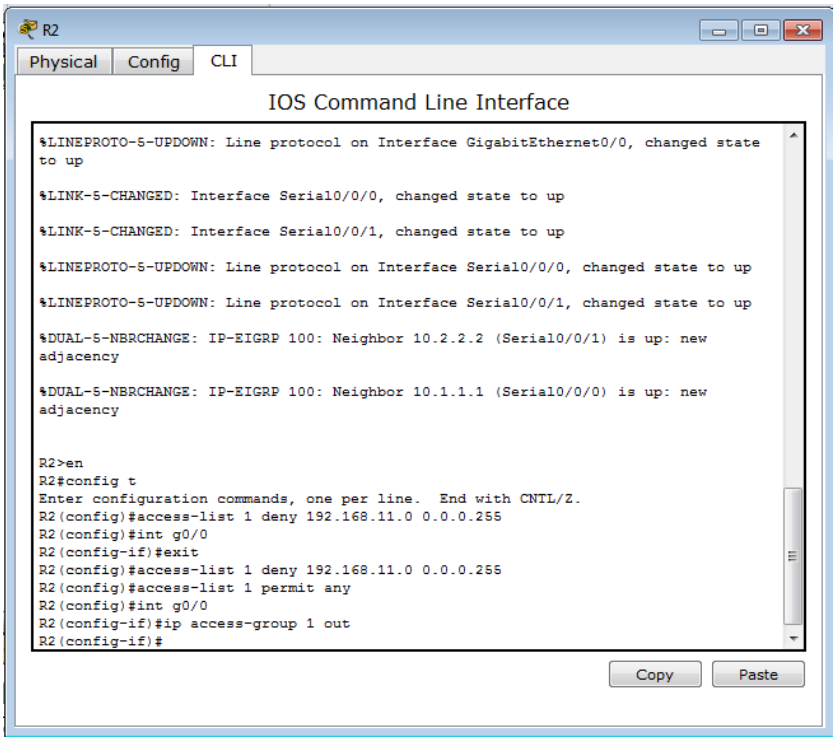


Imagen 179, configuración ACL en R2

Paso 2. Configure and apply a numbered standard ACL on R3.

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

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

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

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

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

R3(config)# **interface GigabitEthernet0/0**

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

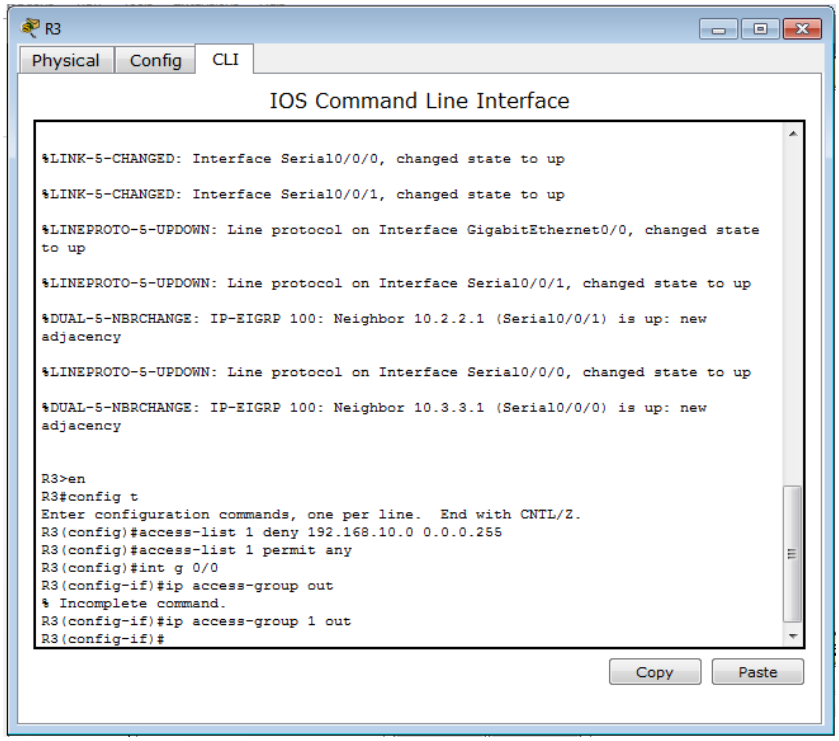


Imagen 180, configuración ACL en R3

Paso 3. Verify ACL configuration and functionality.

a. On **R2** and **R3**, enter the **show access-list** command to verify the ACL configurations. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.

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

- A ping from 192.168.10.10 to 192.168.11.10 succeeds.

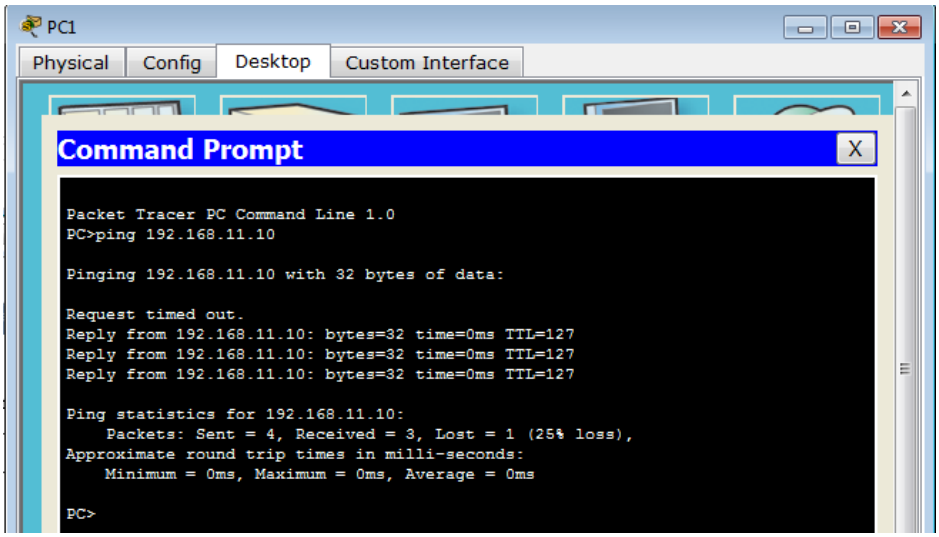


Imagen 181, ping de PC1 a 192.168.11.10

- A ping from 192.168.10.10 to 192.168.20.254 succeeds.

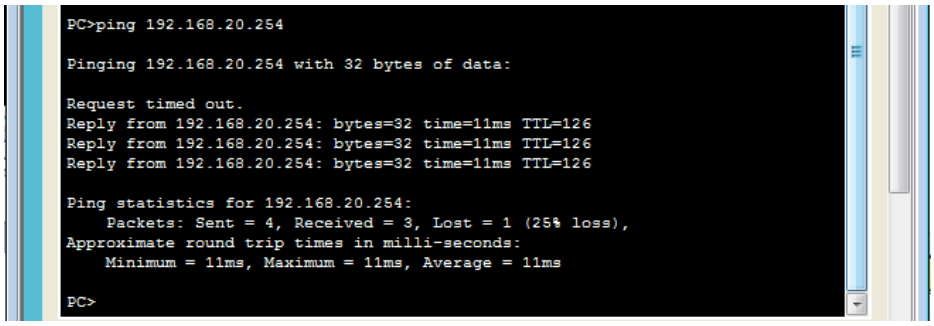


Imagen 182, ping de PC1 a 192.168.20.254

- A ping from 192.168.11.10 to 192.168.20.254 fails.

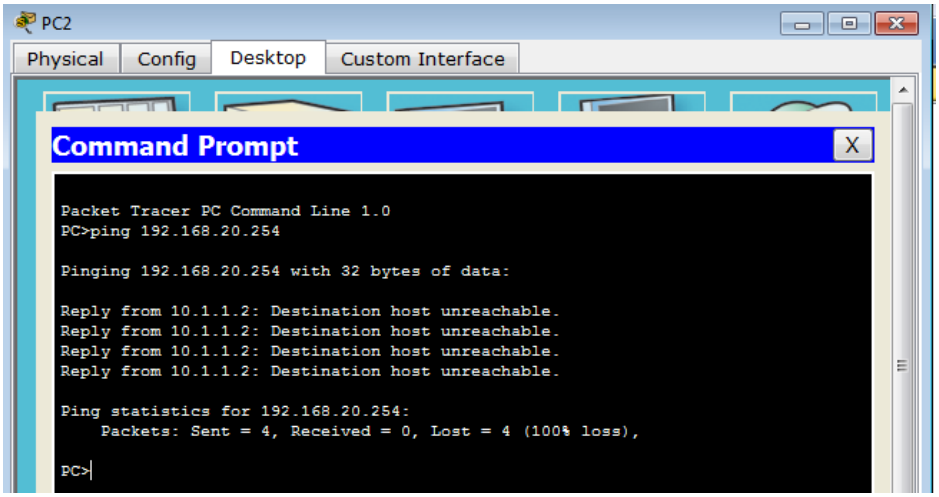


Imagen 183, ping de PC2 a 192.168.20.254

- A ping from 192.168.10.10 to 192.168.30.10 fails.

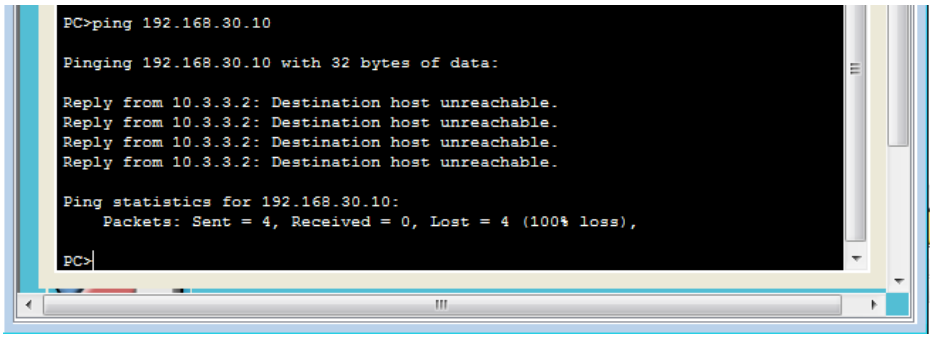


Imagen 184, ping de PC2 a 192.168.30.10

- A ping from 192.168.11.10 to 192.168.30.10 succeeds.

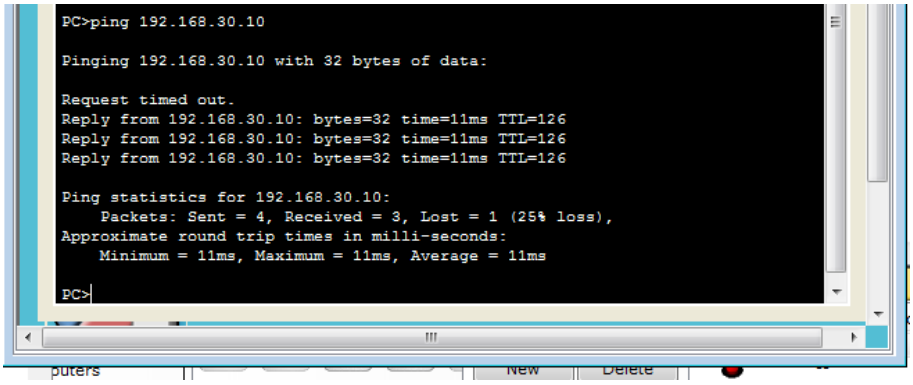


Imagen 185, ping de PC1 a 192.168.30.10

- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

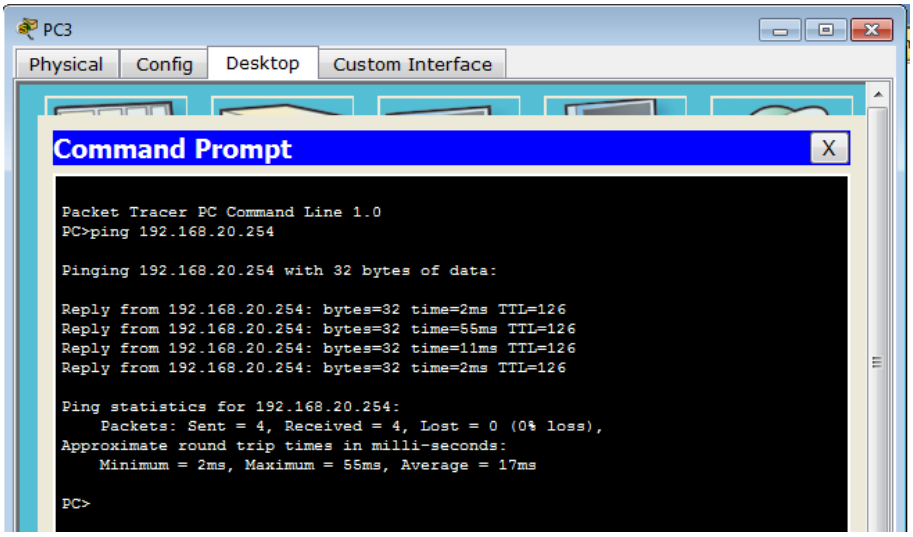


Imagen 186, ping de PC3 a 192.168.20.254

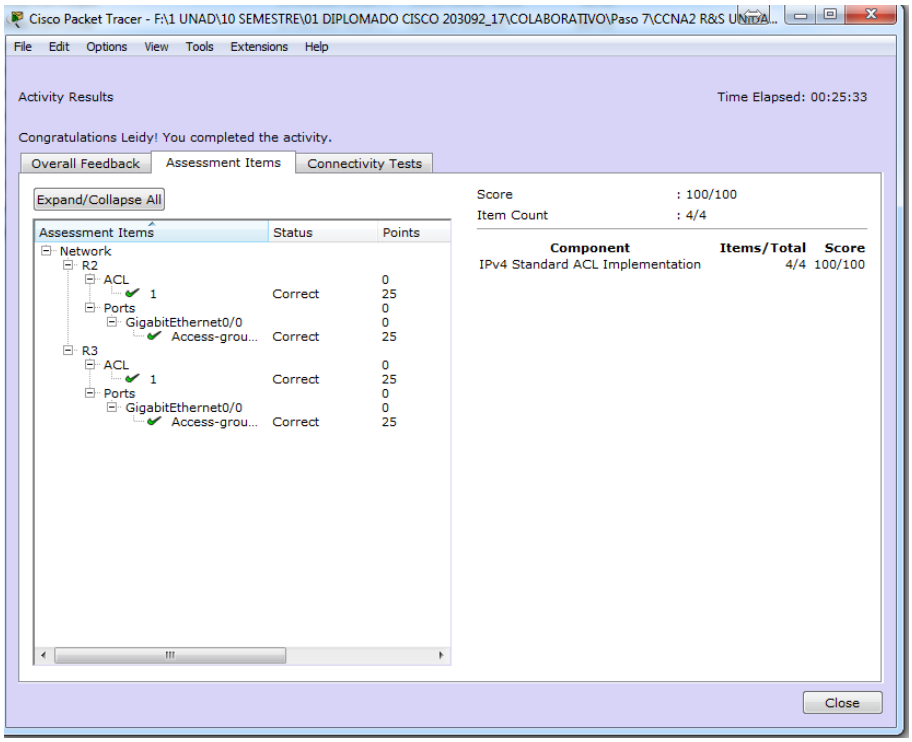


Imagen 187. Actividad Completa.

Conclusiones

- Con la práctica anterior se aprendió a realizar la implementación ACL, configuración y aplicación, verificación y estándar ACL.

- El acceso estándar del control de la lista ACLs es un router de configuración (scripst), el control del permite el acceso a paquetes basados en el (address). Esa actividad está enfocada en definir, filtrar configuraciones estándares ACLs, aplica ACLs a la interfaz del router, y verifica el examen de la implementación de ACL. El router está configurado con direcciones ip y puertas de enlaces Gateway del protocolo del router (EIGRP) ruteado.

9.2.1.11 Packet Tracer - Configuring Named Standard Acls

Topología

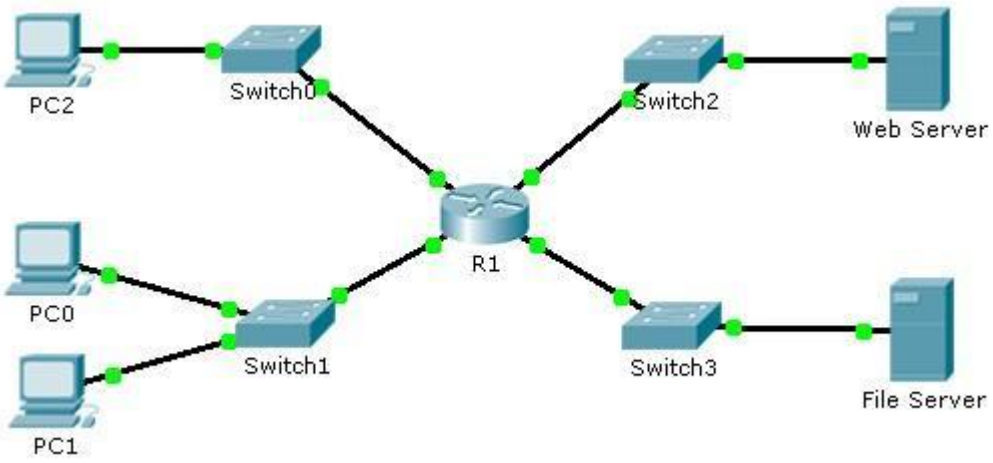


Imagen 188, topología 9.2.1.11

Tabla 7:

Tabla de direcciones

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

Objetivos

Parte 1: Configurar y aplicar una ACL estándar con nombre

Parte 2: Verificar la implementación del ACL

Escenario.

El administrador de red senior le ha encargado que cree un ACL de nombre estándar para impedir el acceso a un servidor de archivos. Se debe denegar el acceso a todos los clientes de una red y una estación de trabajo específica de una red diferente.

Parte 1. Configurar y aplicar una ACL estándar con nombre

Paso 1. Verificar la conectividad antes de configurar y aplicar la ACL.

Las tres estaciones de trabajo deben poder hacer ping tanto en el servidor Web como en el servidor de archivos.

Realizamos el ping desde PC0 (192.168.20.3) primero a File Server (192.168.200.100) y luego a Web Server (192.168.100.100)

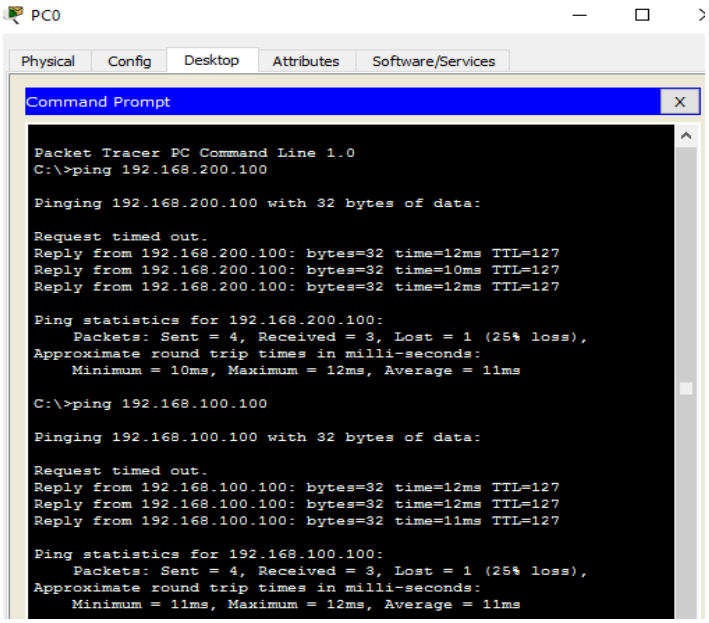


Imagen 189, ping desde PC0 (192.168.20.3) primero a File Server (192.168.200.100) y luego a Web Server (192.168.100.100)

Respuesta: en los dos casos el ping es satisfactorio.

Ahora desde PC2 (192.168.10.3) primero a File Server (192.168.200.100) y luego a Web Server (192.168.100.100)

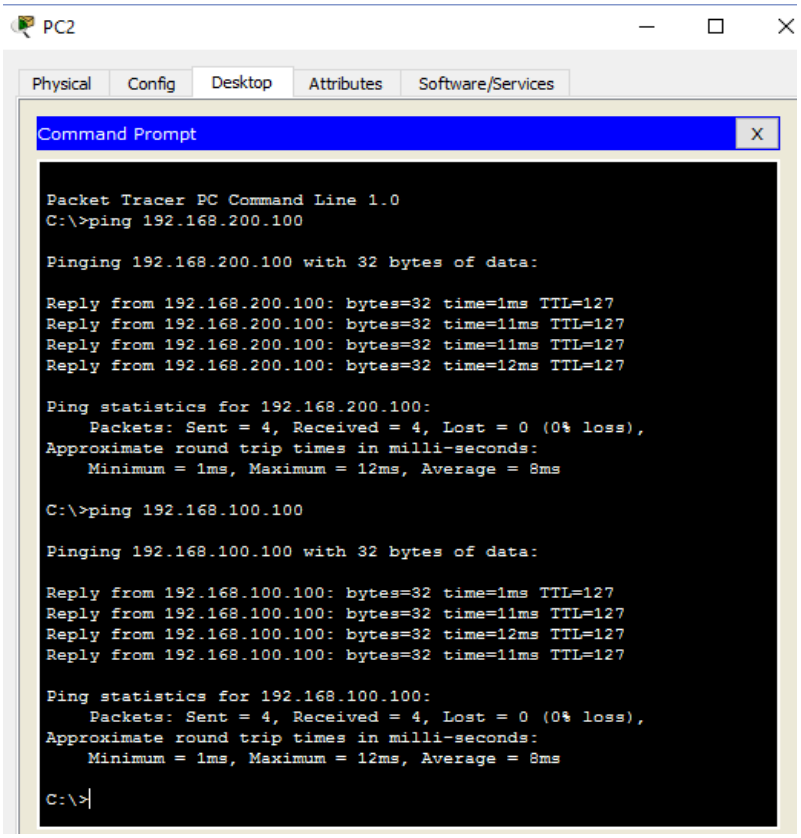


Imagen 190. Ping desde PC2 (192.168.10.3) primero a File Server (192.168.200.100) y luego a Web Server (192.168.100.100)

R/ en los dos casos el ping es satisfactorio.

Paso 2. Configure una ACL estándar nombrada.

Configure la siguiente ACL con nombre en R1.

Ingresamos a R1 para permitir que la lista de acceso permita el paso de la PC1 (192.168.20.4) y niegue cualquier otro tráfico

R1>en

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)#

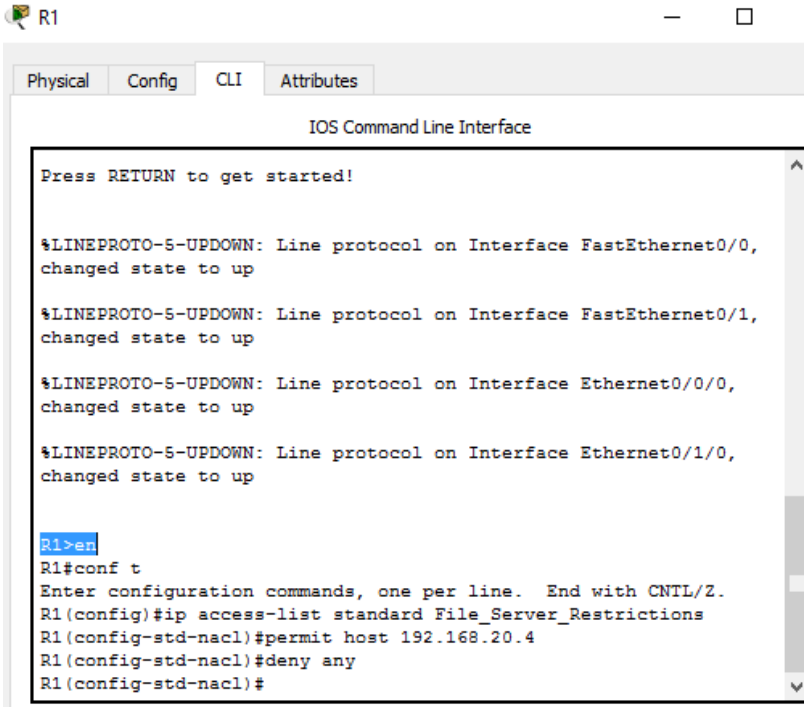


Imagen 191, Configure la siguiente ACL con nombre en R1.

Nota: Para propósitos de puntuación, el nombre ACL distingue entre mayúsculas y minúsculas

Paso 3. Aplicar la ACL nombrada.

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

R1(config-std-nacl)#exit

R1(config)#int f0/1

R1(config-if)#ip access-group File_Server_Restrictions out

R1(config-if)#

```
R1(config)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#
```

b. Guardar la configuración.
R1(config-if)#end

Part 2. Verificar la implementación del ACL

Paso 1. Verificar la configuración y la aplicación de ACL en la interfaz.

Utilice 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 aplica correctamente a la interfaz.

Ingresamos nuevamente a R1 para ver las configuraciones

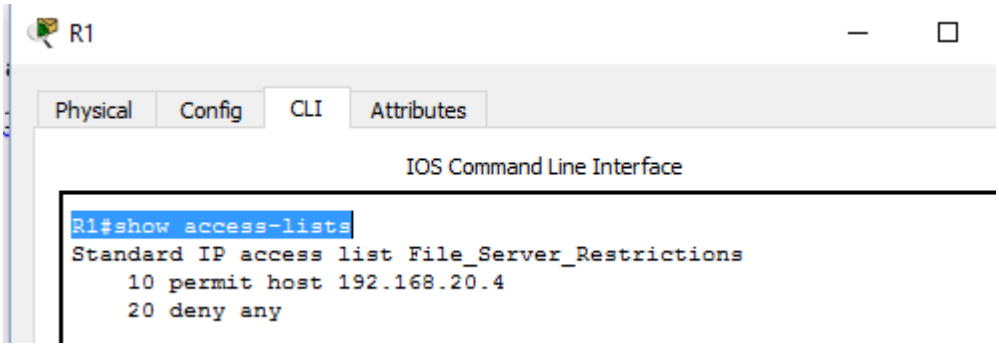


Imagen 192, comando show access-list en R1.

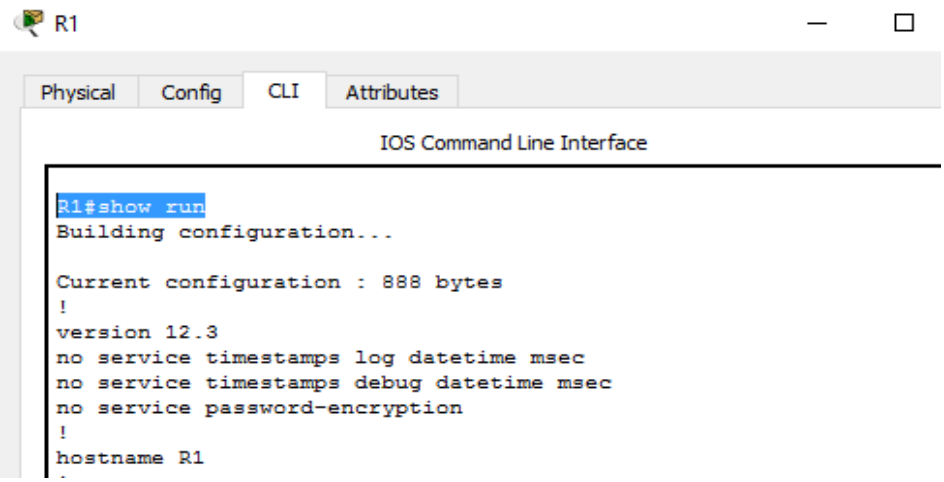


Imagen 193, comando show run.

Y podemos comprobar las restricciones de la configuración realizada previamente

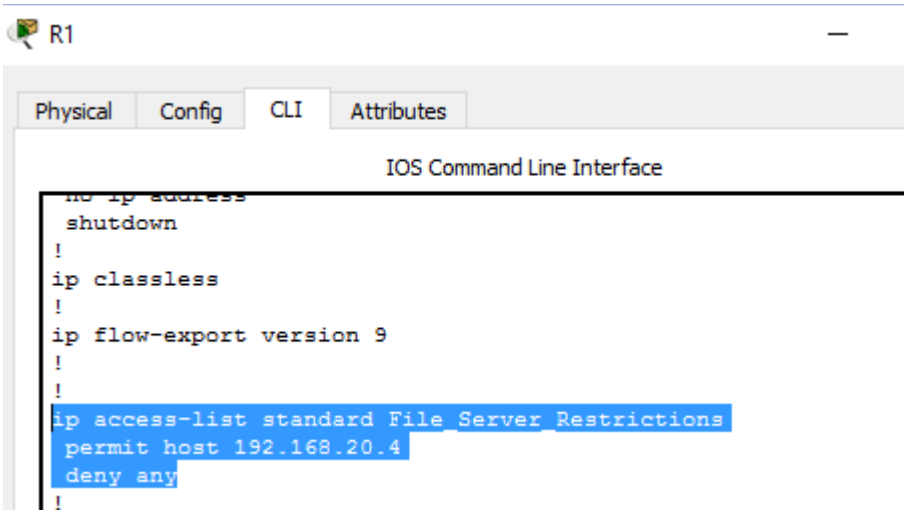


Imagen 194, comprobación de restricciones IP.

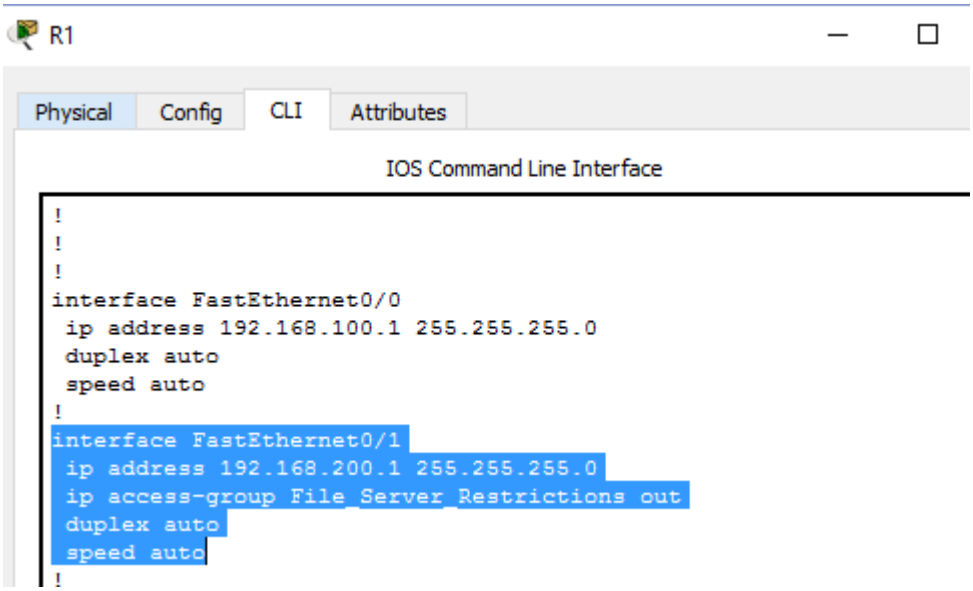


Imagen 195, comprobación de restricciones interfaz F0/0.

Ahora revisamos para interface F0/1

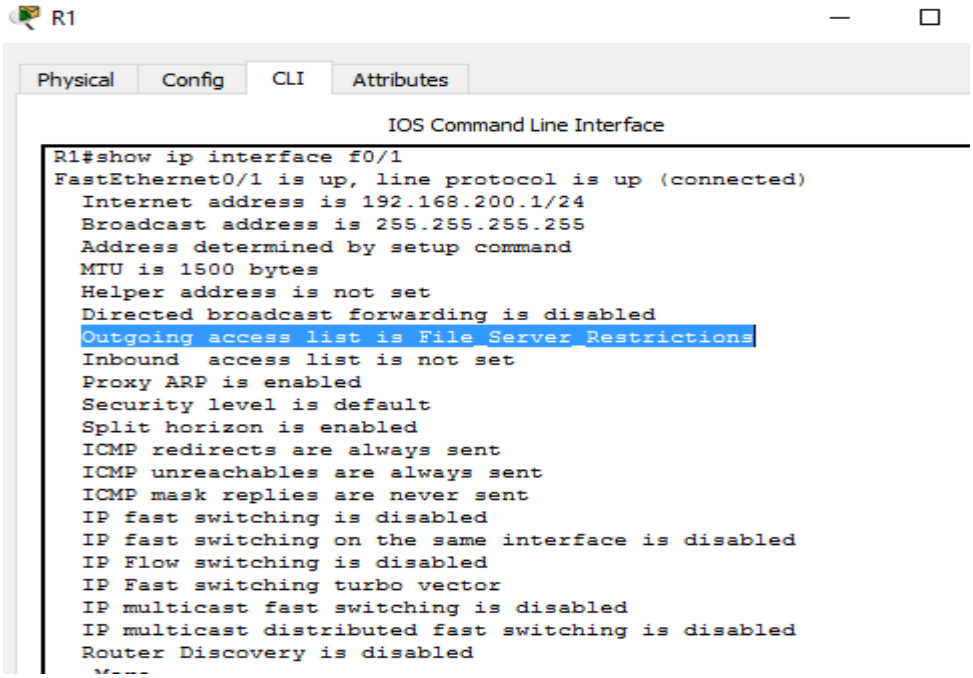


Imagen 196, interfaz interface F0/1.

Paso 2. Compruebe que la ACL funciona correctamente.

Las tres estaciones de trabajo deben poder hacer ping al servidor Web, pero sólo PC1 debe poder hacer ping al servidor de archivos.

Hacemos ping desde todas las terminales ping hacia File Server o servidor de archivos (192.168.200.100)

Iniciamos con PC2

```
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),

C:\>
```

Imagen 197, Hacemos ping desde PC2 hacia servidor de archivos (192.168.200.100)

Respuesta: El ping falla

Ahora desde PC0 a File Server

```
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),

C:\>
```

Imagen 198, Hacemos ping desde PC0 hacia servidor de archivos (192.168.200.100)

Respuesta: El ping falla

Probamos desde PC1

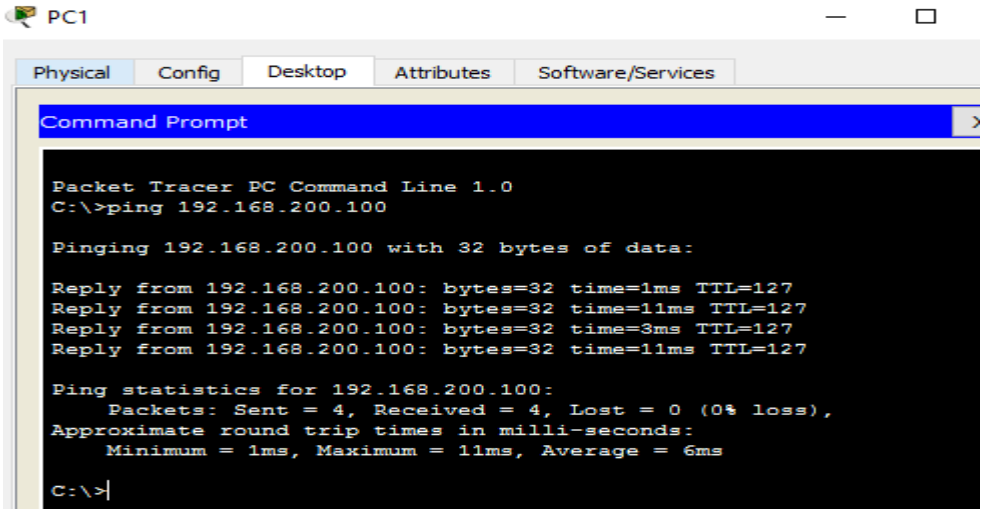


Imagen 199, Hacemos ping desde PC1 hacia servidor de archivos (192.168.200.100)

Respuesta: El ping es satisfactorio

Ahora probamos con el Servidor web haciendo ping desde las tres estaciones.

Desde PC0 a WebServer (192.168.100.100)

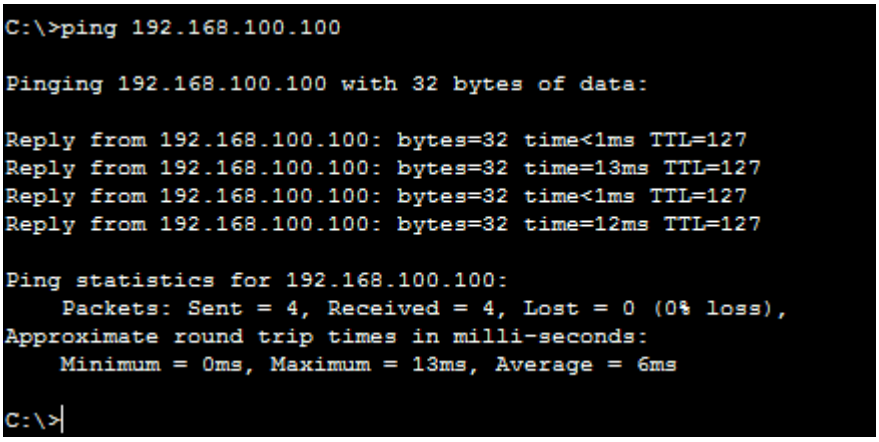


Imagen 200, ping Desde PC0 a WebServer (192.168.100.100)

Respuesta: El ping es satisfactorio

Desde PC1 a WebServer (192.168.100.100)

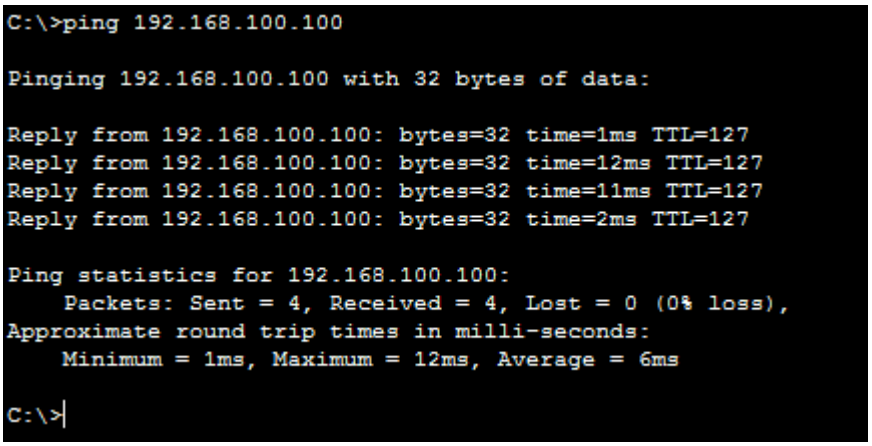


Imagen 201, ping Desde PC1 a WebServer (192.168.100.100)

R/ El ping es satisfactorio

Desde PC2 a WebServer (192.168.100.100)

```
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=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=13ms 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 = 13ms, Average = 7ms

C:\>
```

Imagen 202, ping Desde PC2 a WebServer (192.168.100.100)

Respuesta: El ping es satisfactorio

Se comprueba que todas las estaciones PC0, PC1 y PC2 pueden hacer ping a Web Server pero únicamente la PC1 hace ping a File Server o servidor de archivos.

Lista de resultados

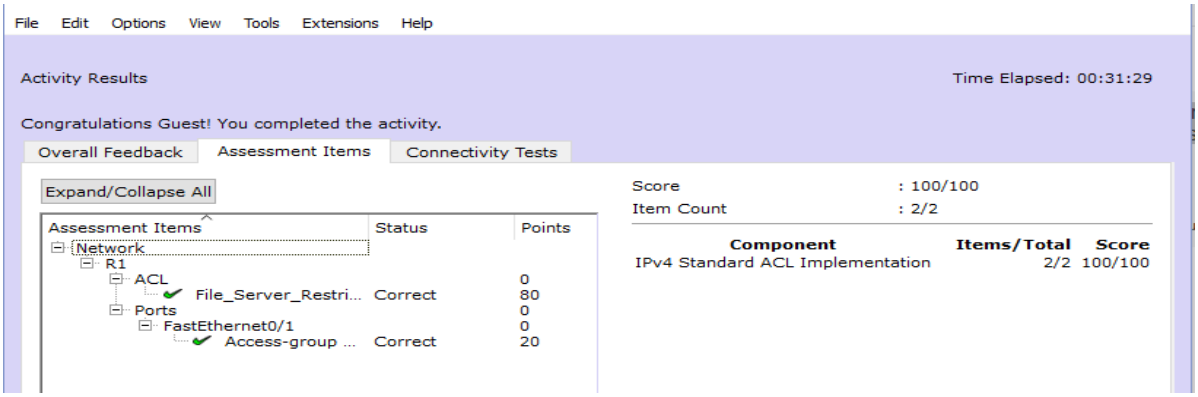


Imagen 203. Actividad Completa.

Conclusiones

- En esta actividad se realiza un numero amplio de tareas importantes para el buen desarrollo de los ejercicios propuestos, en este se ejecutan funciones como la de verificar una conexión entre los dispositivos proporcionada en la configuración inicial de la topología, se configura la ACL de los Routers, esto con el objetivo de mitigar los ataques de forma remota y por supuesto no podrían faltar la verificación de la funcionalidad de las actividades ejecutadas con anterioridad. (ACL) para permitir el acceso de direcciones IP específicas, lo que asegura que solo la computadora del administrador tenga permiso para acceder al router mediante telnet o SSH.

- A través de la configuración de listas de control de acceso (ACL) podemos permitir o denegar que determinados hosts en una red tengan acceso o no, a servicios como DNS, FTP, HTTPS entre otros, misma forma podemos realizar este tipo de configuraciones por puertos o por direcciones IP específicas.

9.2.3.3 Packet Tracer - Configuring An Acl On Vty Lines

Topology

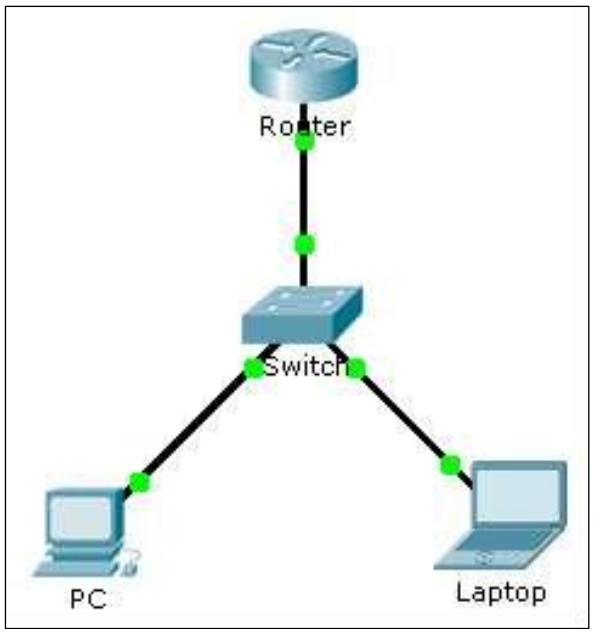


Imagen 204, topología práctica 9.2.3.3.

Tabla 8:

Tabla de direccionamiento

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

Objetivos

- Parte 1: configurar y aplicar una ACL a líneas VTY
- Parte 2: Verificar la implementación de ACL

Situacion.

Como administrador de red, debe tener acceso remoto a su enrutador. Este acceso no debería estar disponible para otros usuarios de la red. Por lo tanto, configurará y aplicará una lista de control de acceso (ACL) que permite el acceso de la PC a las líneas Telnet, pero niega todas las demás direcciones IP de origen.

Parte 1. Configurar y aplicar una ACL a líneas VTY

Paso 1. Verifique el acceso de Telnet antes de que se configure la ACL.
Ambas computadoras deberían poder Telnet al Enrutador. La contraseña es Cisco.

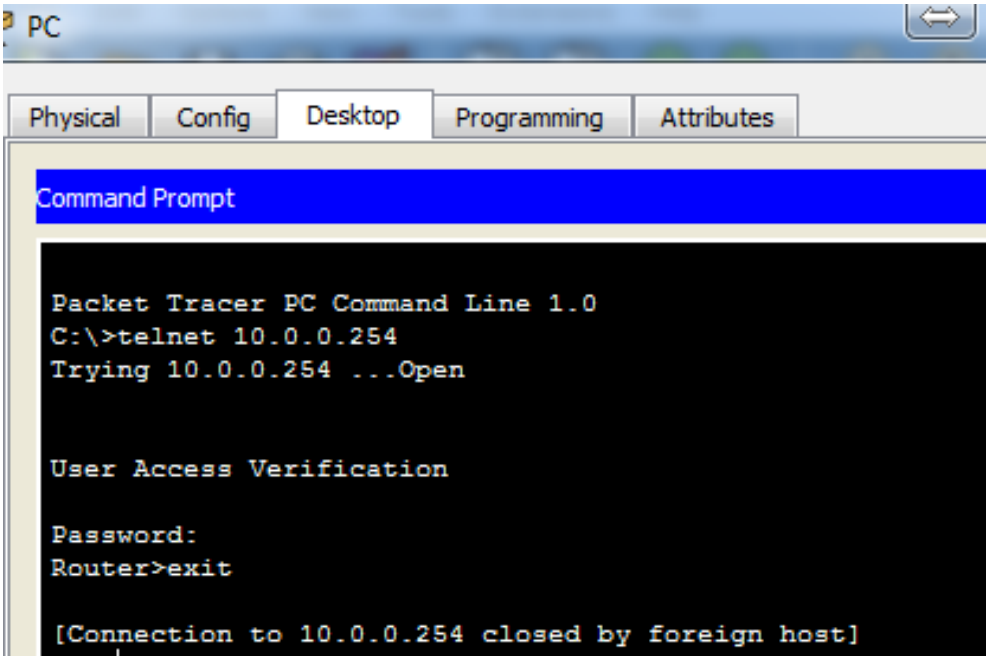


Imagen 205, acceso Telnet PC al Enrutador

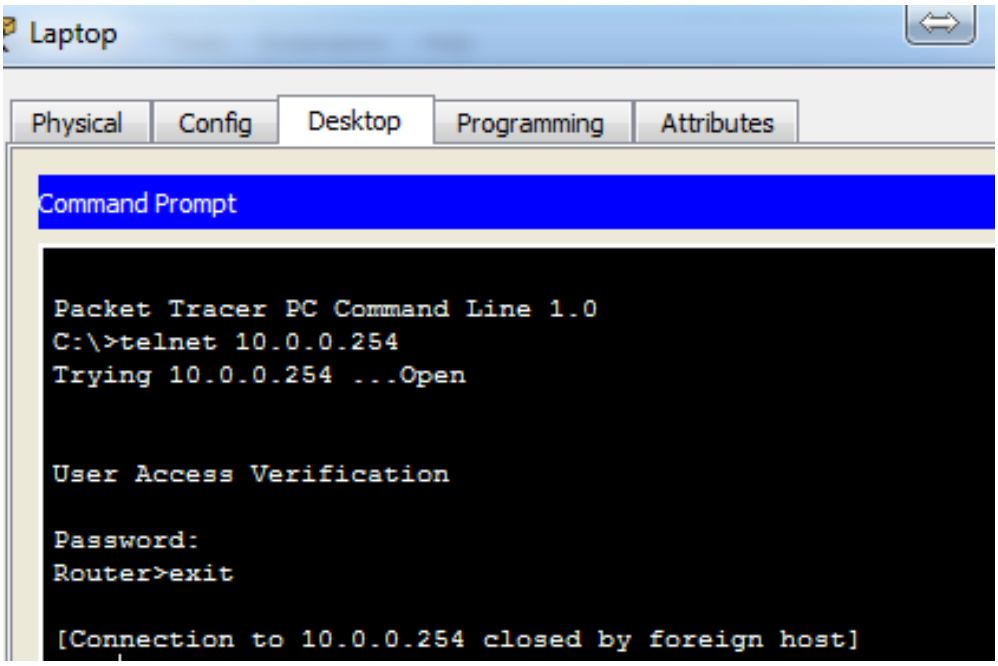


Imagen 206, acceso Telnet Laptop al Enrutador

Paso 2. Configure una ACL estándar numerada.

Configure la siguiente ACL numerada en el enrutador.

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

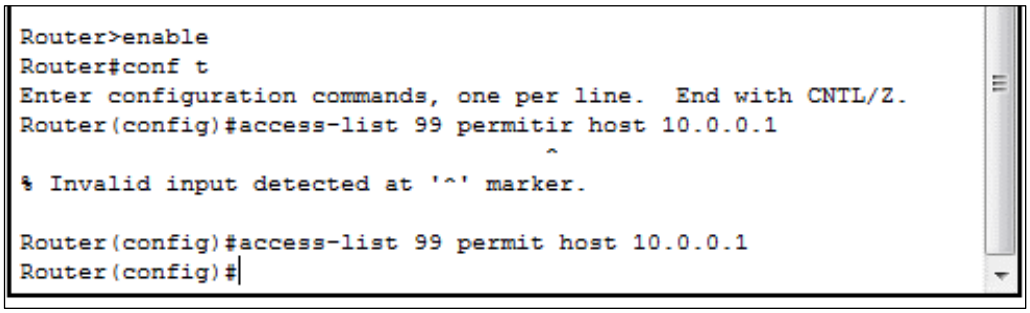


Imagen 207, ACL numerada en el enrutador

Como no queremos permitir el acceso desde ninguna otra computadora, la propiedad de denegación implícita de la lista de acceso satisface nuestros requisitos.

Paso 3. Coloque una ACL estándar nombrada en el enrutador.

Se debe permitir el acceso a las interfaces del enrutador, mientras que el acceso a Telnet debe estar restringido. Por lo tanto, debemos colocar la ACL en las líneas Telnet O a 4. Desde el indicador de configuración de Router, ingrese el modo de configuración de línea para las líneas O - 4 y use el comando access-class para aplicar la ACL a todas las líneas VTY:

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

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 99 permitir host 10.0.0.1
                                    ^
% Invalid input detected at '^' marker.

Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#
```

Imagen 208, ACL estándar nombrada en el enrutador

Parte 2. Verificar la implementación de ACL

Paso 1. Verifique la configuración de ACL y la aplicación a las líneas VTY.

Use las listas de acceso del programa para verificar la configuración de ACL. Use el comando show run para verificar que la ACL se aplica a las líneas VTY.

```
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Imagen 209, verificar la configuración de ACL comando show access-lists

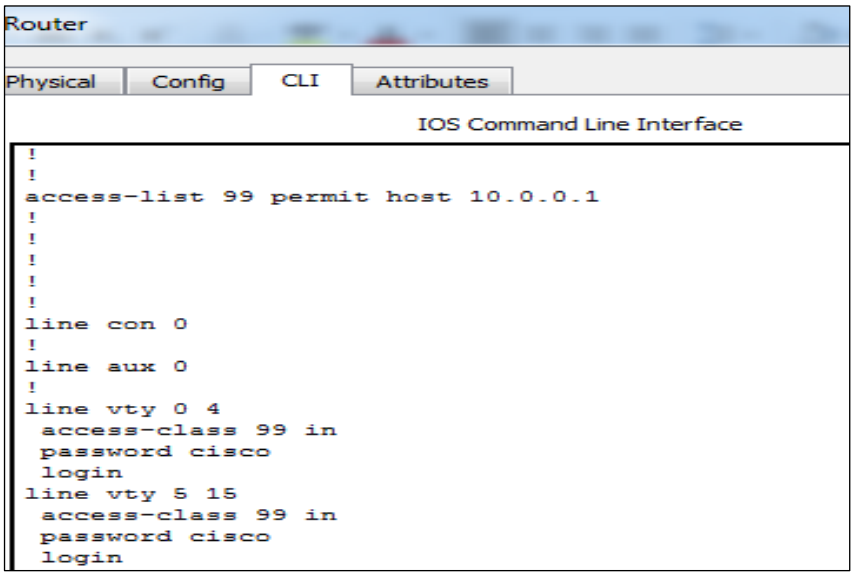


Imagen 210, verificar la configuración de ACL comando show running-config

Paso 2. Verifique que la ACL esté funcionando correctamente.

Ambas computadoras deberían poder hacer ping al Enrutador, pero solo las PC deberían poder usar Telnet.

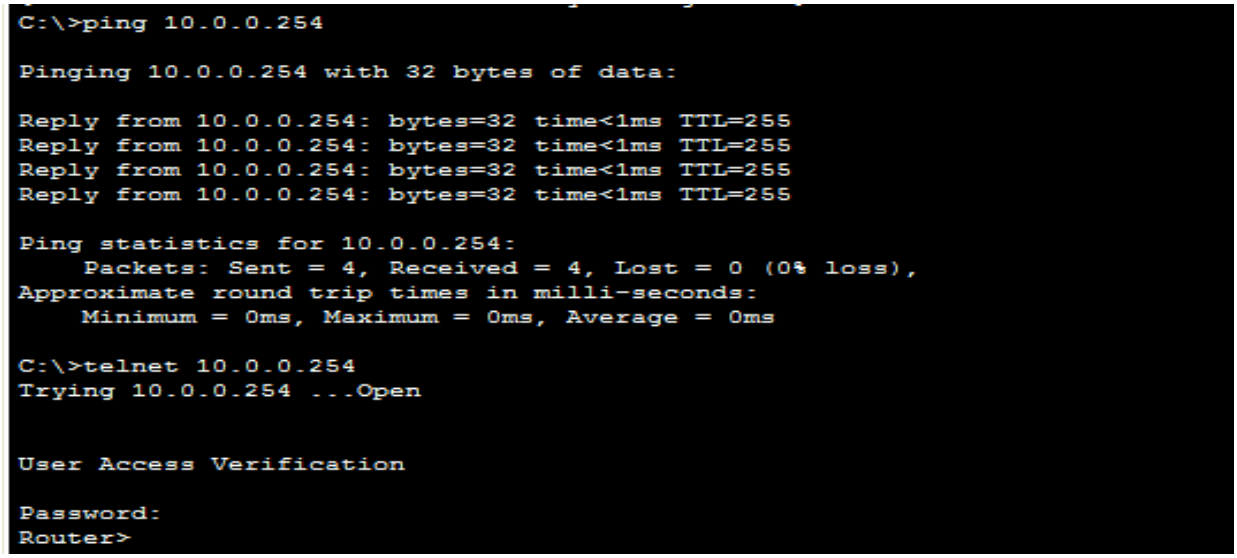


Imagen 211, Verifique que la ACL esté funcionando en el PC. Con acceso.

```
Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
C:\>
```

Imagen 212, Verifique que la ACL esté funcionando en el Laptop sin acceso.

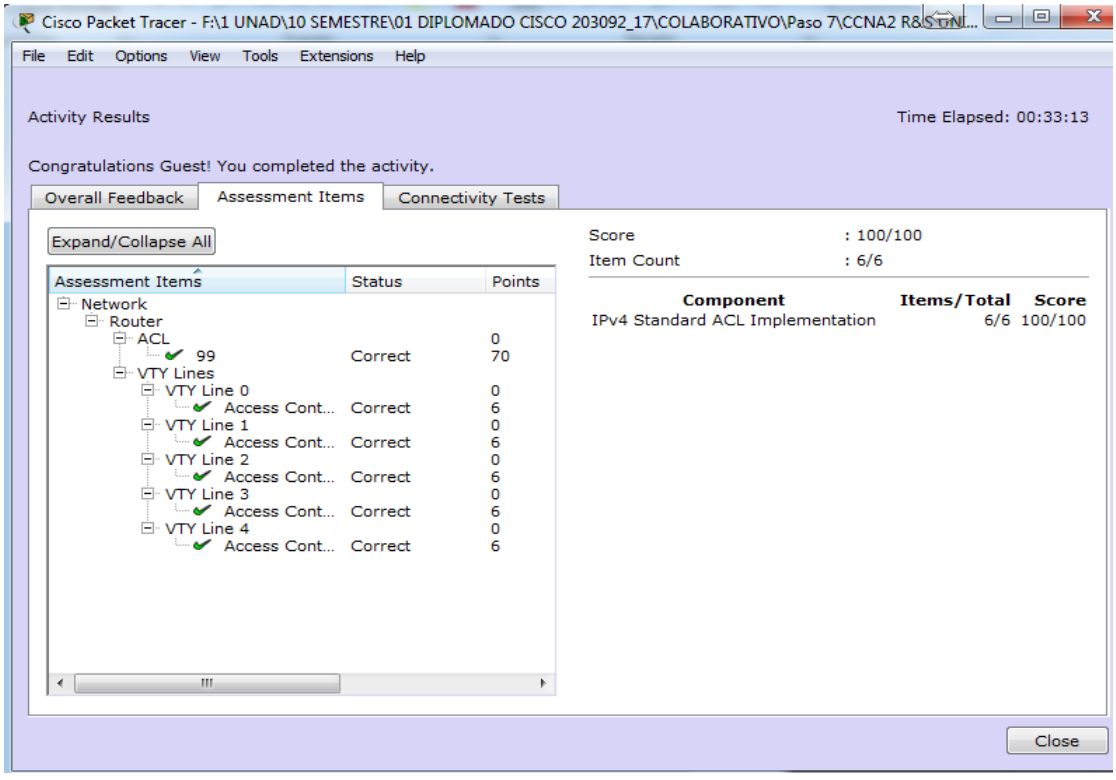


Imagen 213 .Actividad Completa.

Conclusiones

- La restricción del acceso a VTY es una técnica que permite definir las direcciones IP a las que se les permite acceder por Telnet al proceso de EXEC del router. Puede controlar qué estación de trabajo administrativa o qué red administra el router mediante la configuración de una ACL y una instrucción access-class en las líneas VTY. También puede utilizar esta técnica con SSH para mejorar aún más la seguridad de acceso administrativo.

- El filtrado del tráfico de Telnet o SSH es una función de una ACL de IP extendida, porque filtra un protocolo de nivel superior. Sin embargo, debido a que se utiliza el comando access-class para filtrar sesiones de Telnet/SSH entrantes o salientes por dirección de origen, se puede utilizar una ACL estándar.

- Después de configurar la ACL para restringir el acceso a las líneas VTY, es importante verificar que funcione correctamente utilizando el comando show access-lists.

9.5.2.6 Packet Tracer - Configuring Ipv6 Acls

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topología

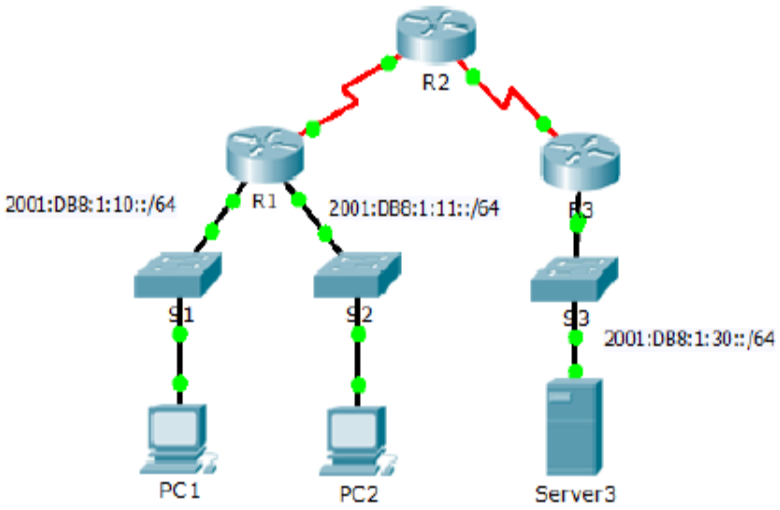


Imagen 214. Topología 9.5.2.6.

Tabla 9:

Tabla de Direccionamiento.

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

Parte 1. Configure, Apply, and Verify an IPv6 ACL

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

Los registros indican que un computador sobre la red 2001:DB8:1:11::0/64 está repetidamente refrescando su página web causando un ataque de servicio denegado contra Server3. Hasta que el cliente pueda ser identificado y limpiado, usted debe bloquear los accesos a HTTP y HTTPS a esa red con una lista de acceso.

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

Configure an ACL named **BLOCK_HTTP** on **R1** with the following statements.
Configure una Lista de Accesos nombrada BLOCK _HTTP en R1 con las siguientes instrucciones:

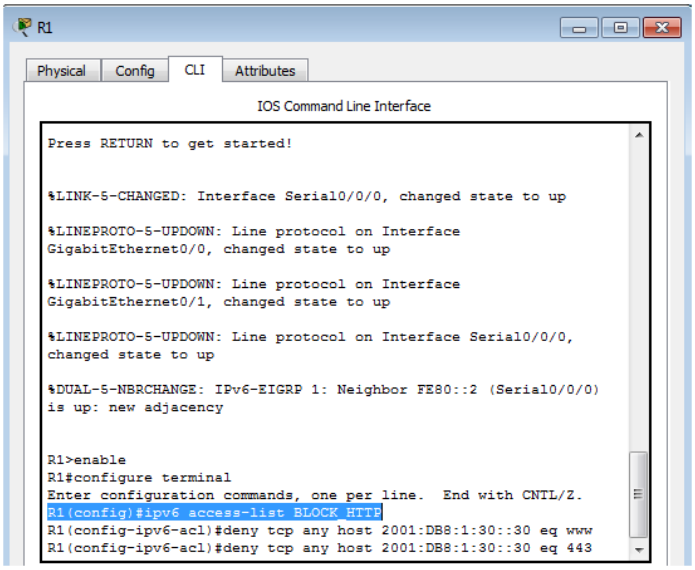


*Imagen 215. Configurando una ACL llamada **BLOCK_HTTP**.*

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***

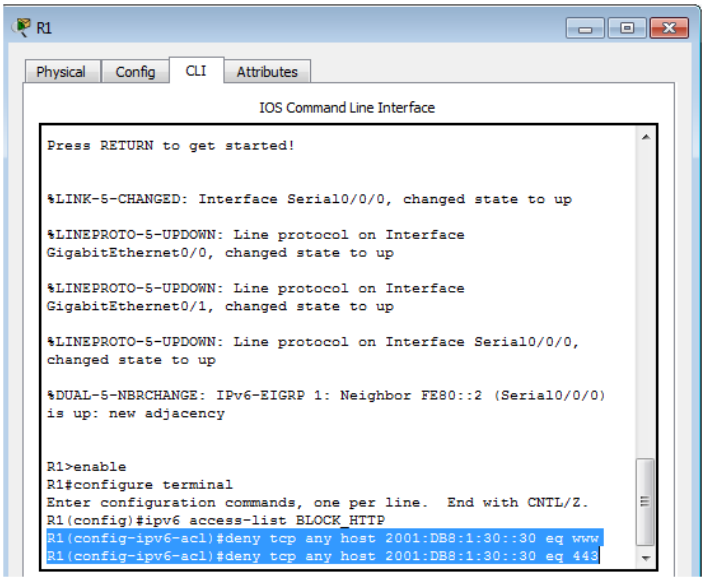


Imagen 216. Bloqueando el Tráfico de HTTP y HTTPS.

- **Allow all other IPv6 traffic to pass.**

  *R1(config)# **permit ipv6 any any***

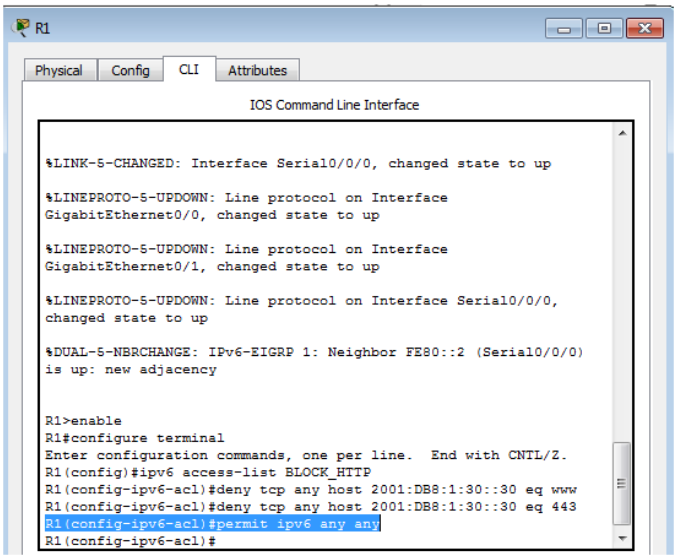


Imagen 217. Permitiendo que todo el tráfico IPV6 pase.

Paso 2. Apply the ACL to the correct interface.

Apply the ACL on the interface closest the source of the traffic to be blocked.
Aplique las Listas de Acceso sobre la interface más cercana del origen del tráfico para ser bloqueada.

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

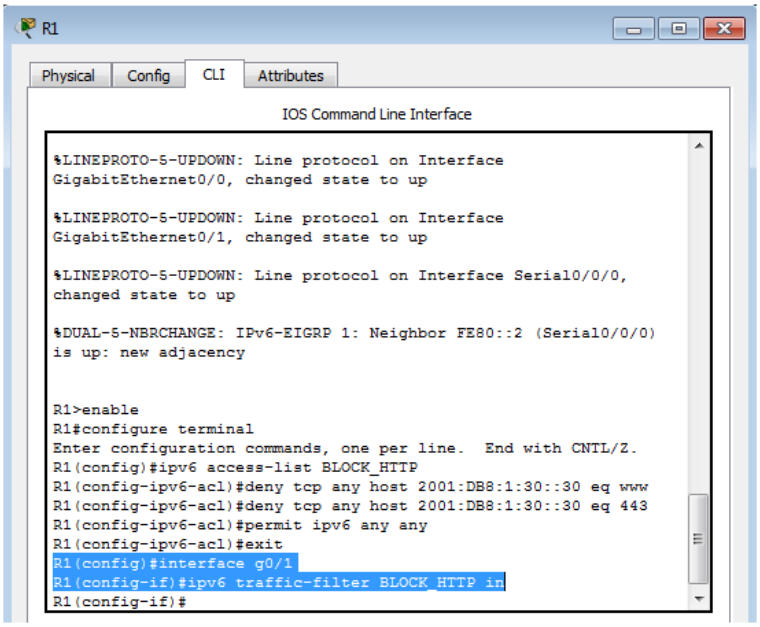


Imagen 218. Interface Cercana Bloqueada.

Paso 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.

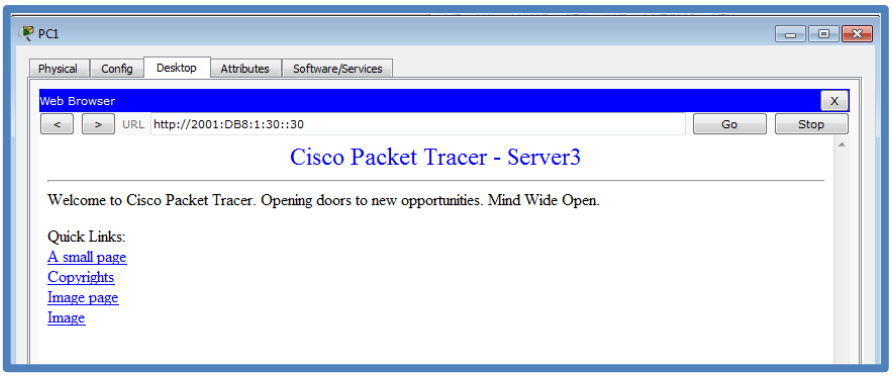


Imagen 219. Verificando la operatividad de la ACL en PC1.

- 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

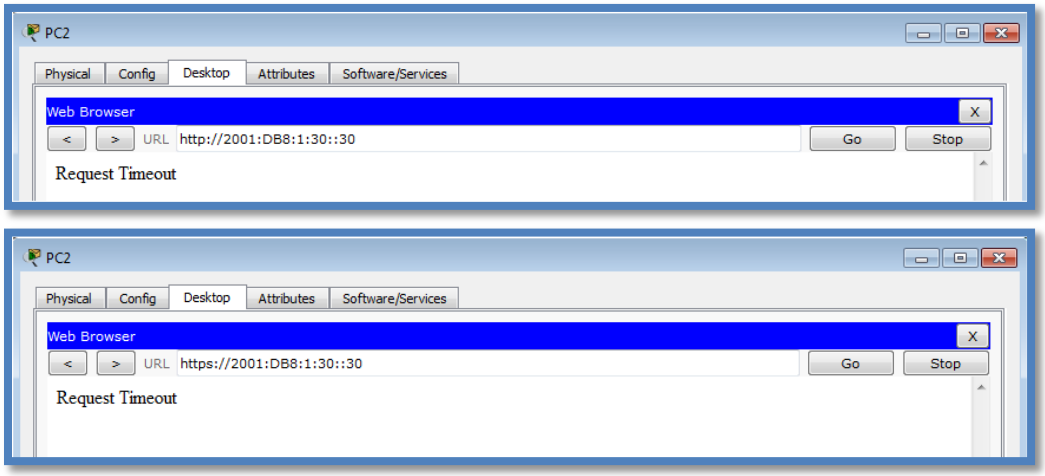


Imagen 220. Verificando Bloqueo de la Website en PC2.

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

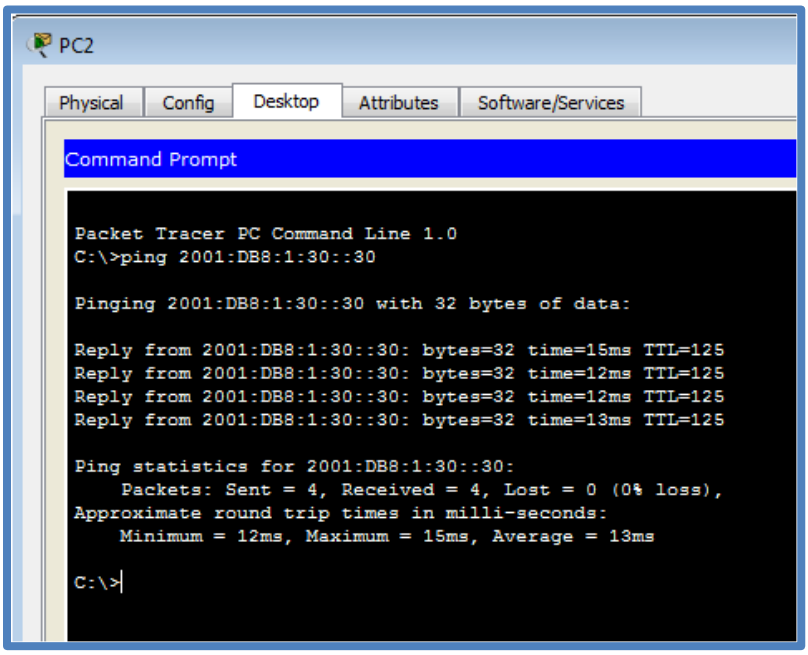


Imagen 221. Verificando la ACL desde PC2.

Parte 2. Configure, Apply, and Verify a Second IPv6 ACL

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

Los registros ahora indican que tu servidor está recibiendo ping desde muchas direcciones diferentes IPv6 en un ataque de Servicio Denegado Distribuido. Usted debe filtrar ping ICMP requerido para su servidor.

Paso 1. Create an access list to block ICMP.

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

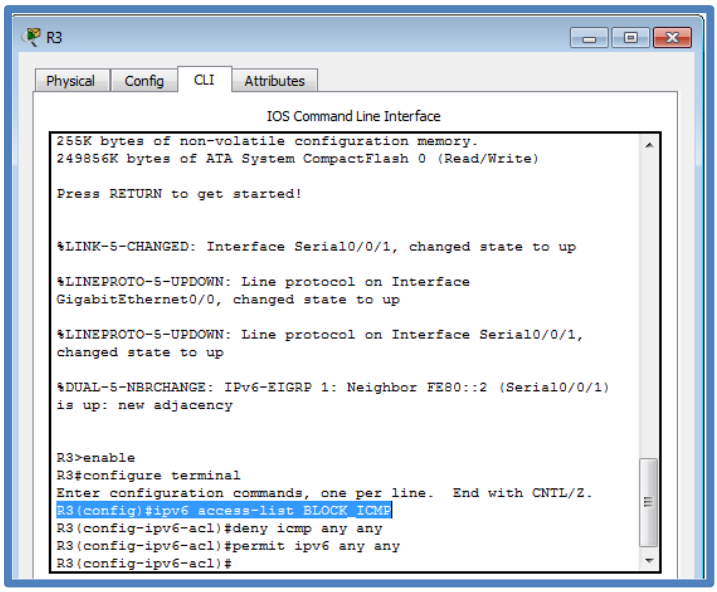


*Imagen 222. Configurando ACL llamada **BLOCK_ICMP**.*

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

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

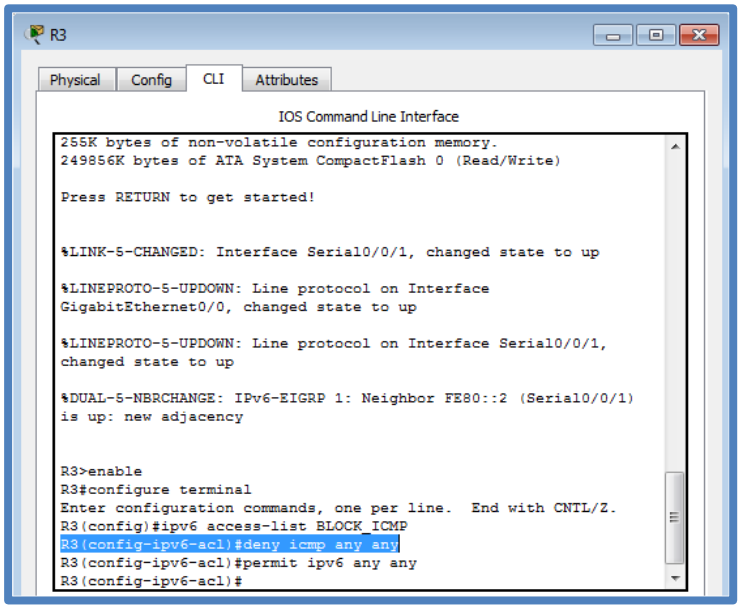


Imagen 223. Bloqueando Tráfico ICMP desde cualquier Host.

b. Allow all other IPv6 traffic to pass.

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

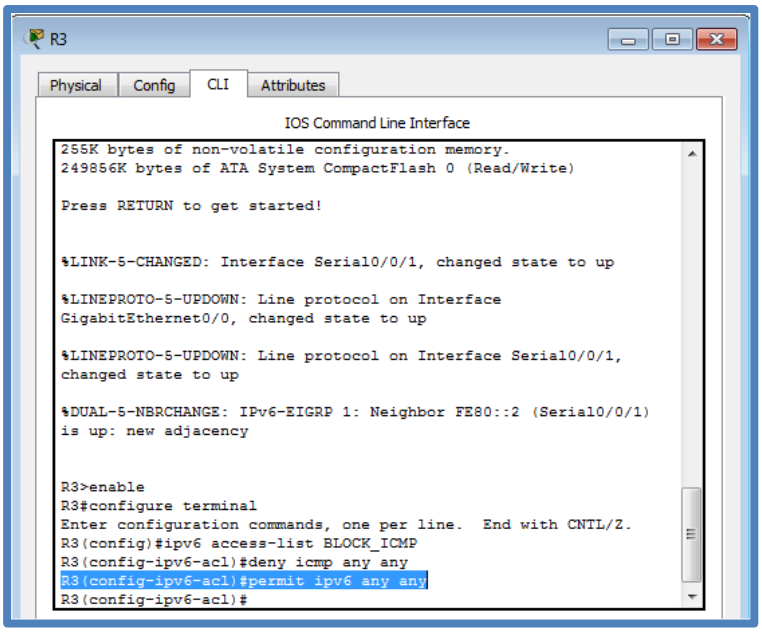


Imagen 224. Bloqueando Tráfico ICMP desde cualquier Host.

Paso 2. Apply the ACL to the correct interface.

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

En este caso, el tráfico ICMP puede venir de cualquier Fuente. Asegure que el tráfico ICMP este bloqueado más allá de su origen o cambios que pueden ocurrir en la topología de red, aplique las ACL más cercanas al destino.

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

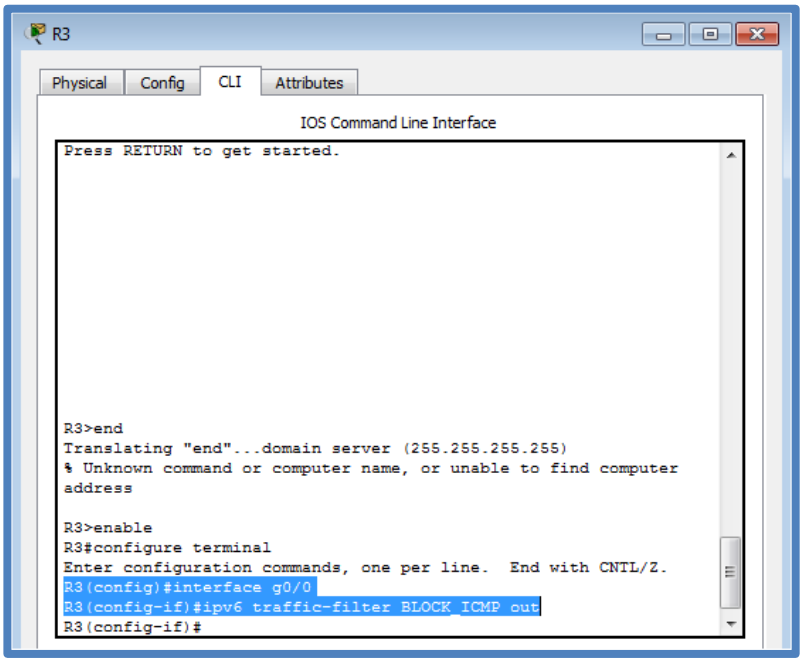


Imagen 225. Aplicando ACL a la Interface Correcta.

Paso 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),

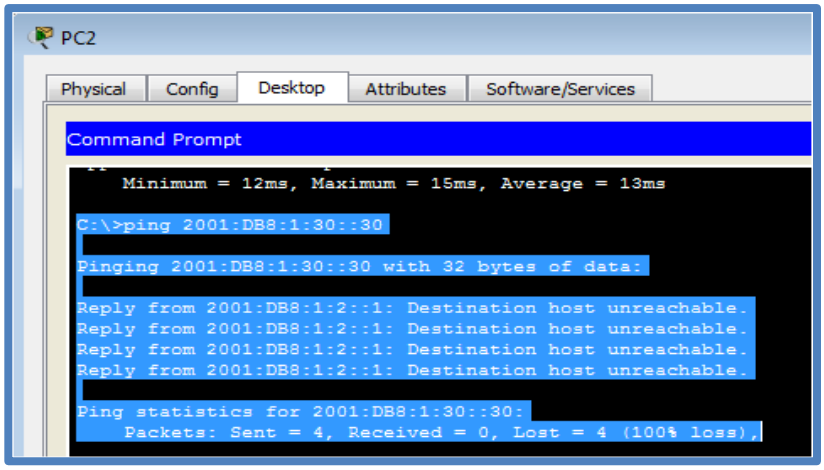


Imagen 226. Aplicando ACL a la Interface Correcta.

b. Ping from **PC1** 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),

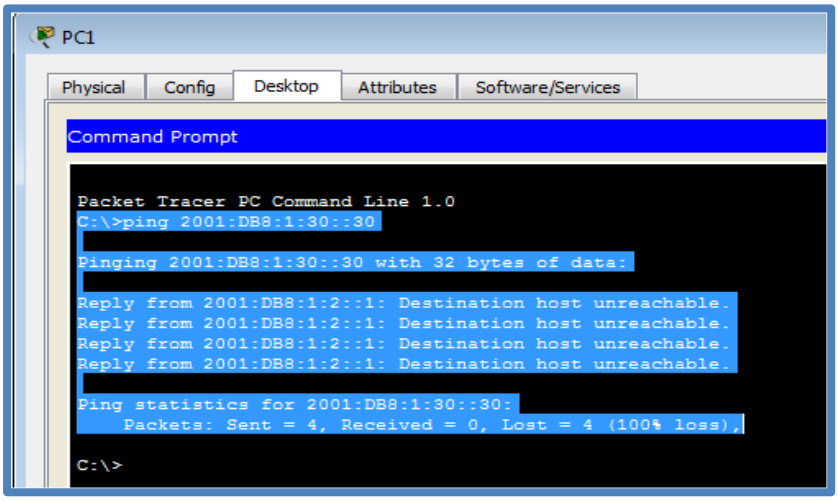


Imagen 227. Aplicando ACL a la Interface Correcta.

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

The website should display.

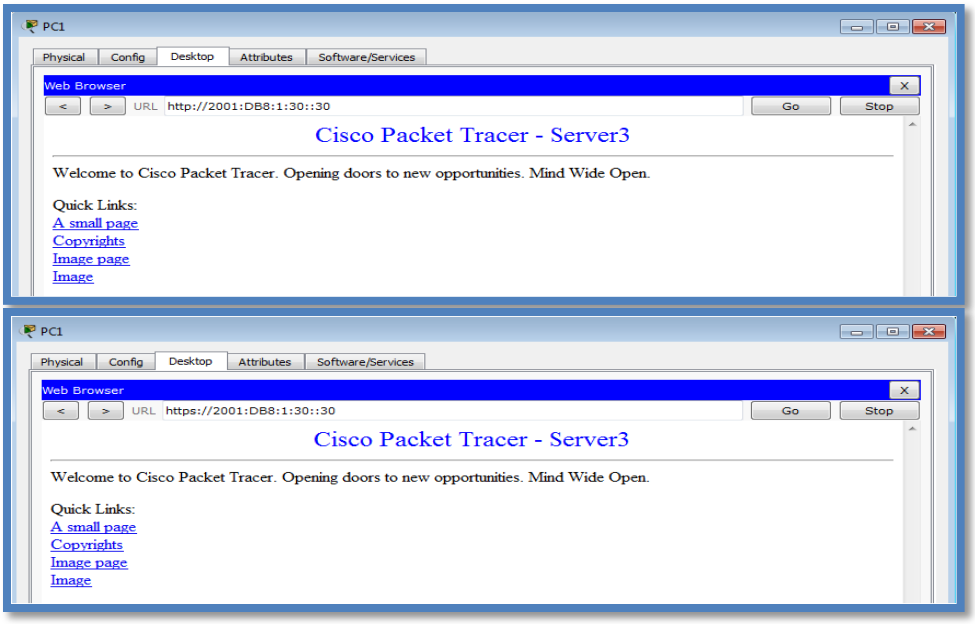


Imagen 228. Mostrando Website desde PC1.

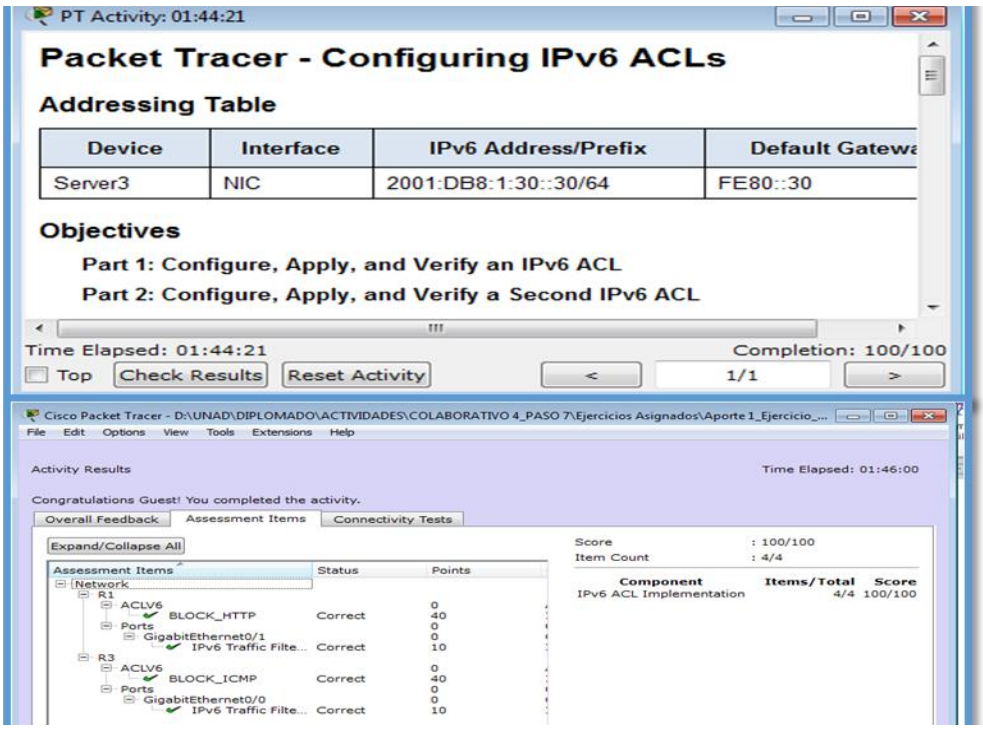


Imagen 229. Actividad Completa.

Conclusiones

- En la práctica anterior se revisó lo referente a una ACL como una lista secuencial de instrucciones que permite o impide el acceso a algunos dispositivos con el fin de darle seguridad a la red. Éstas se aplican a los protocolos de capa superior o a las direcciones. Las ACL son una herramienta potente para controlar el tráfico hacia y desde la red. Se pueden configurar ACL para todos los protocolos de red enrutada.

- Por tanto en el R1 y R3 se creó una ACL y a las interfaces cercanas se las configuró con una serie de instrucciones, para que finalmente se realice la comprobación para poder saber si fue posible tener acceso o no a los dispositivos. Con el comando ping se pudo verificar que las funciones de la lista de acceso fueron las adecuadas.

10.1.2.4 Lab - Configuring Basic Dhcpv4 On A Router

- **Topología**

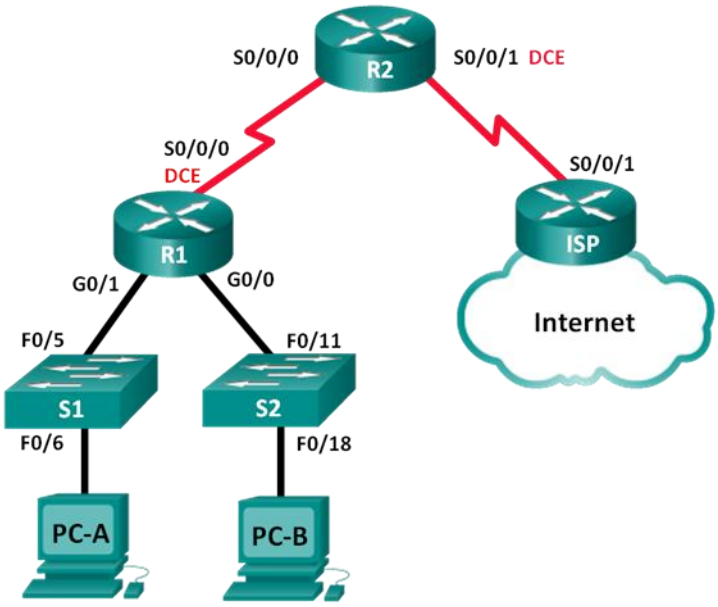


Imagen 230 Topología. 10.1.2.4.

Tabla 10:

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) 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: 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 1. Armar la red y configurar los parámetros básicos de los dispositivos

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

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

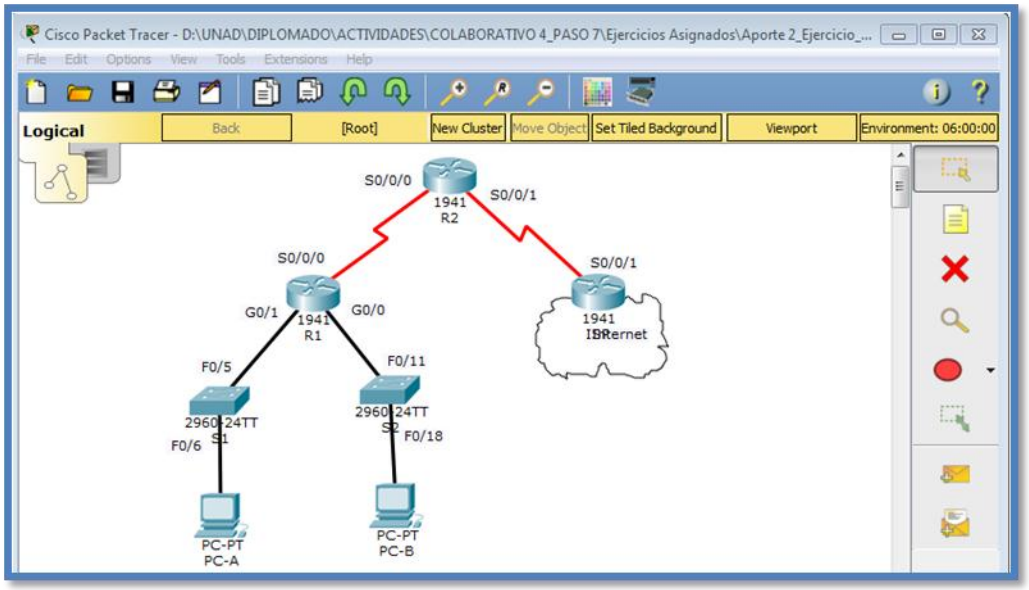


Imagen 231. Cableado de la Red.

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

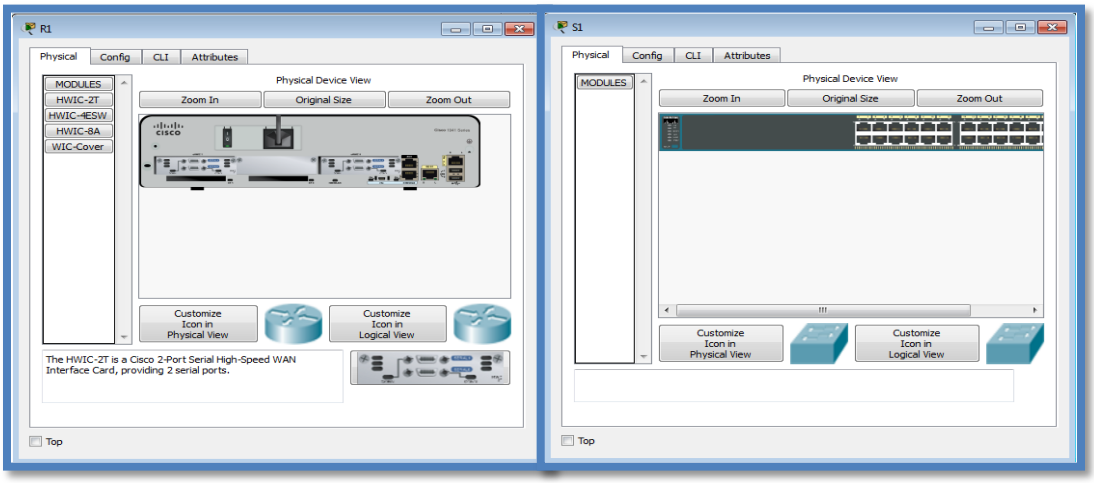


Imagen 232, Inicializando Router y Switches.

Paso 3. Configurar los parámetros básicos para cada router.

i) Desactive la búsqueda DNS.

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

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

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

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

R1

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R1

R1(config)#no ip domain-lookup

R1(config)#enable password class

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#loggin synchronous

R1(config-line)#exit

R1(config)#line vty 0 15

R1(config-line)#password cisco

R1(config-line)#login

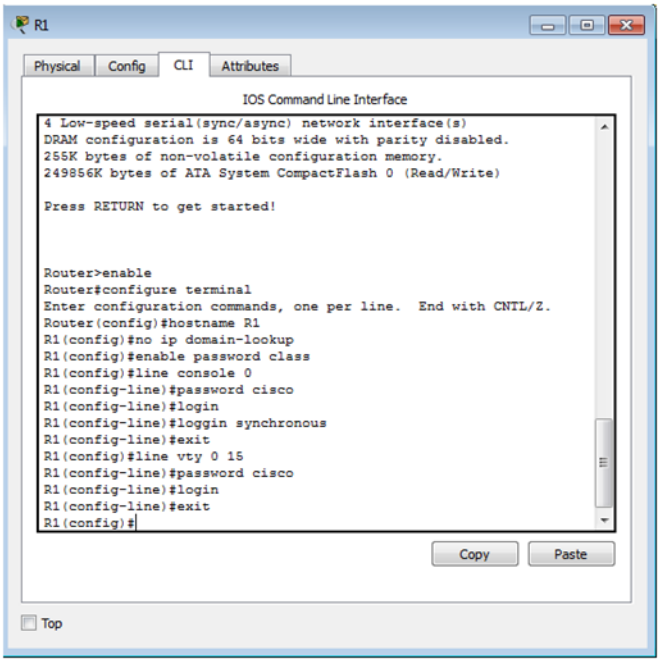


Imagen 233. Configuración Parámetros Básicos R1.

R2

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R2

R2(config)#no ip domain-lookup

R2(config)#enable password class

R2(config)#line console 0

R2(config-line)#password cisco

R2(config-line)#login

R2(config-line)#loggin synchronous

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)#

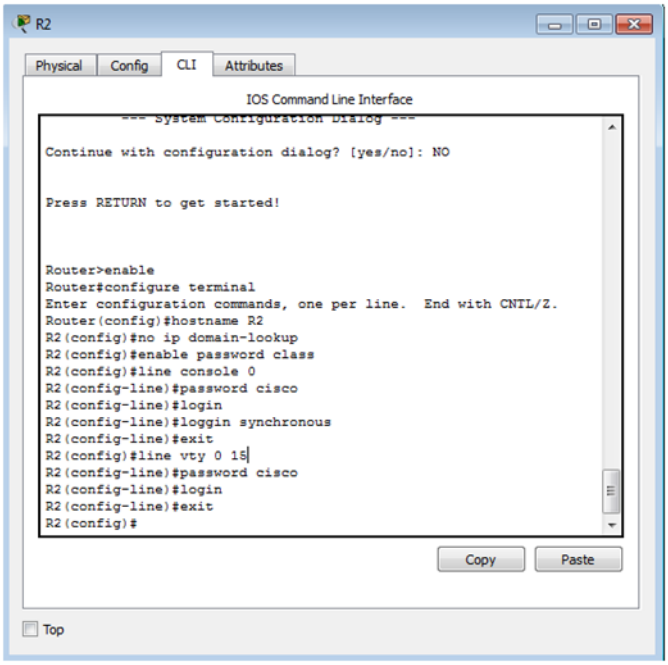


Imagen 234. Configuración Parámetros Básicos R2.

ISP

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname ISP

ISP(config)#no ip domain-lookup

ISP(config)#enable password class

ISP(config)#line console 0

ISP(config-line)#password cisco

ISP(config-line)#login

ISP(config-line)#loggin synchronous

ISP(config-line)#exit

ISP(config)#line vty 0 15

ISP(config-line)#password cisco

ISP(config-line)#login

ISP(config-line)#exit

ISP(config)#

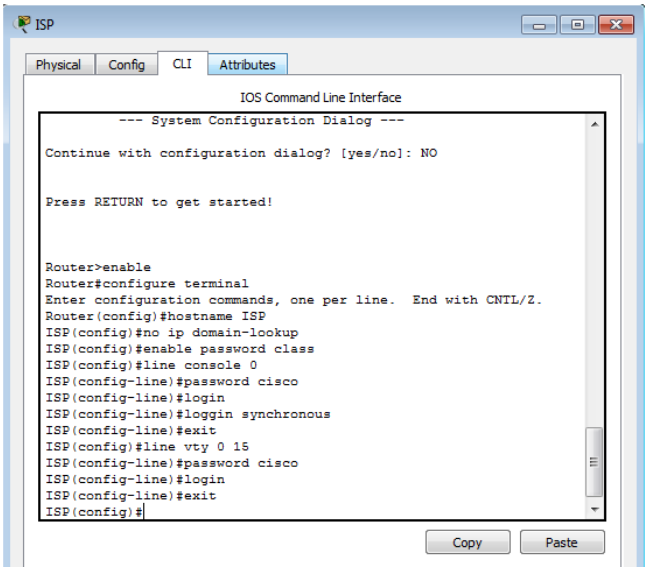


Imagen 235. Configuración Parámetros Básicos ISP.

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

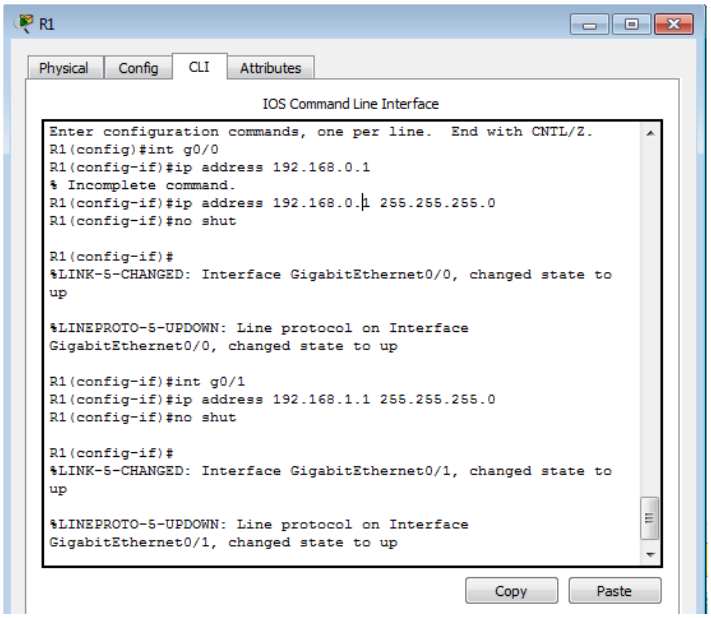


Imagen 236. Configuración Direcciones IP R1.

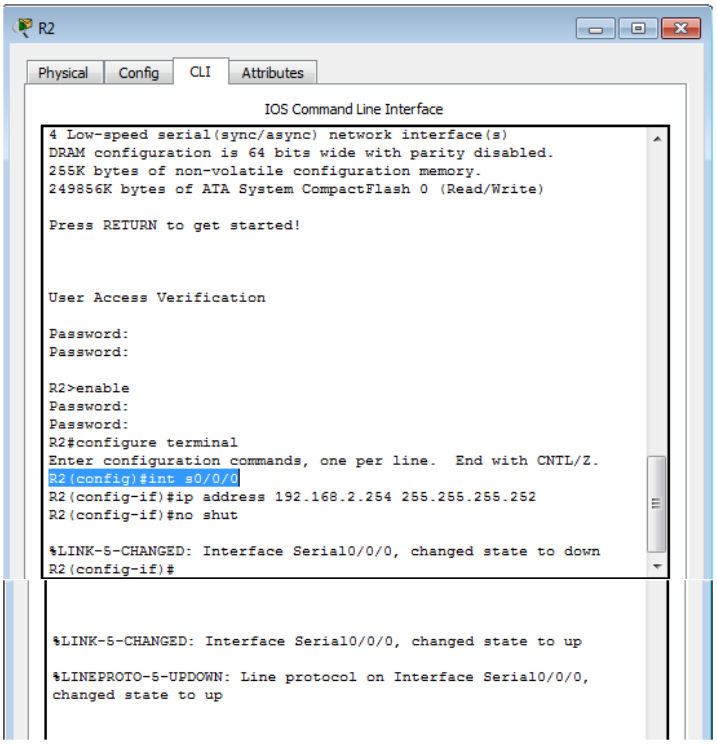


Imagen 237. Configuración Direcciones IP R2.

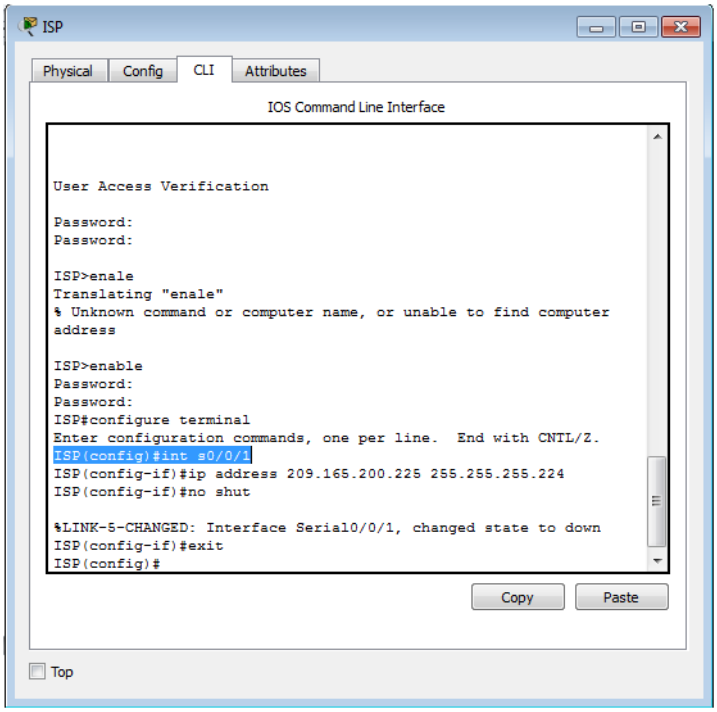


Imagen 238. Configuración Direcciones IP ISP.

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

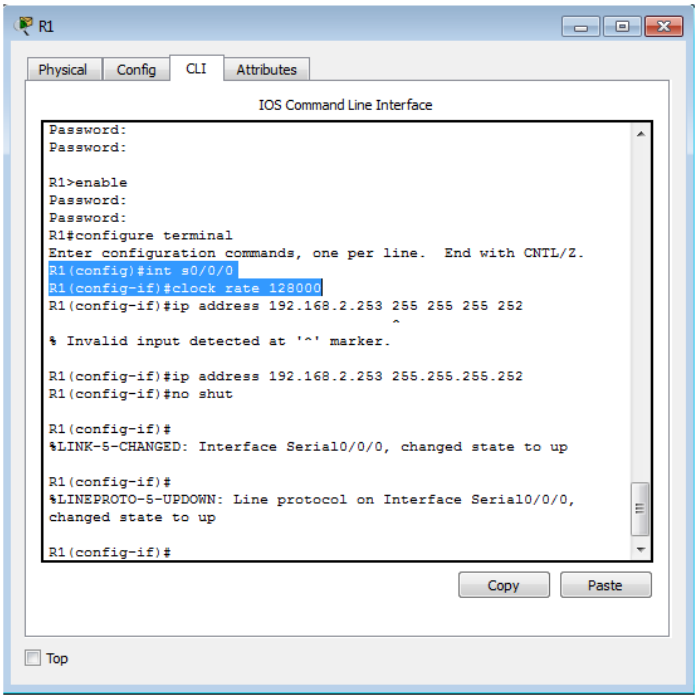


Imagen 239. Configuración Interfaz DCE S0/0/0 en R1

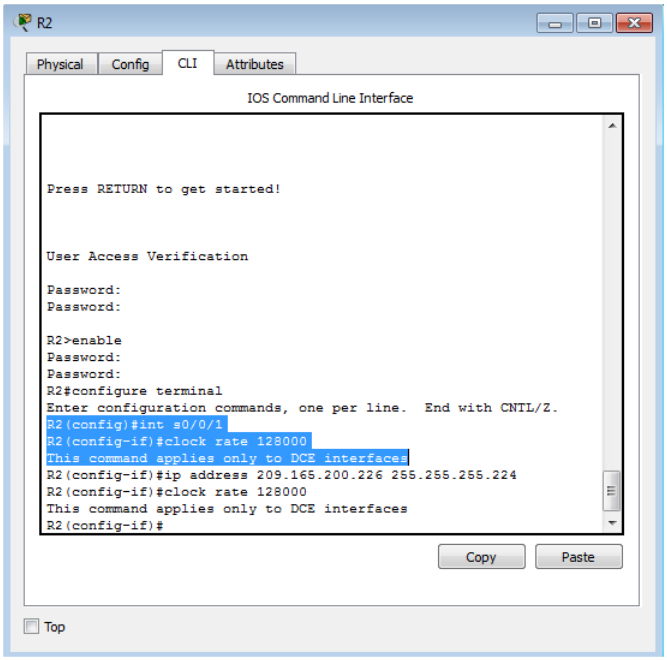


Imagen 240. Configuración Interfaz DCE S0/0/1 en R2.

Configure EIGRP for R1.

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

R1(config-router)# ***network 192.168.0.0 0.0.0.255***

R1(config-router)# ***network 192.168.1.0 0.0.0.255***

R1(config-router)# ***network 192.168.2.252 0.0.0.3***

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

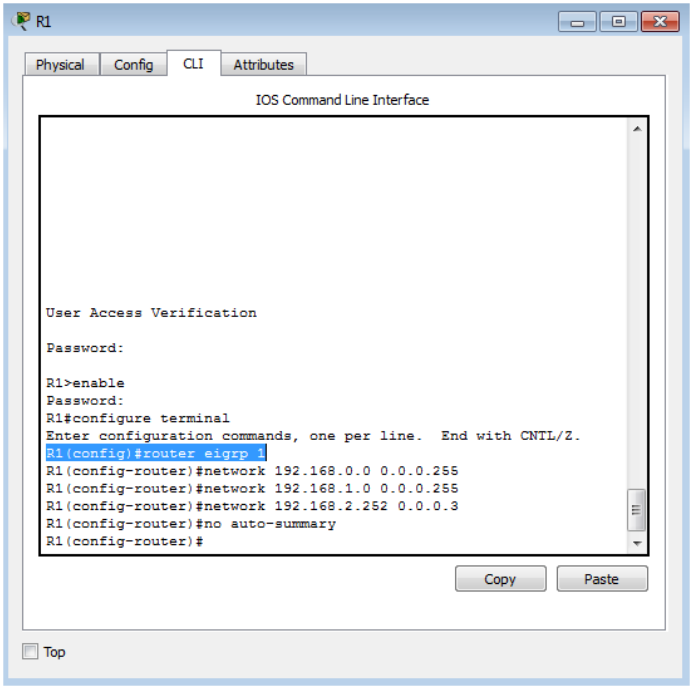


Imagen 241. Configuración EIGRP para R1.

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

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

R2(config-router)# ***network 192.168.2.252 0.0.0.3***

R2(config-router)# ***redistribute static***

R2(config-router)# ***exit***

R2(config)# ***ip route 0.0.0.0 0.0.0.0 209.165.200.225***

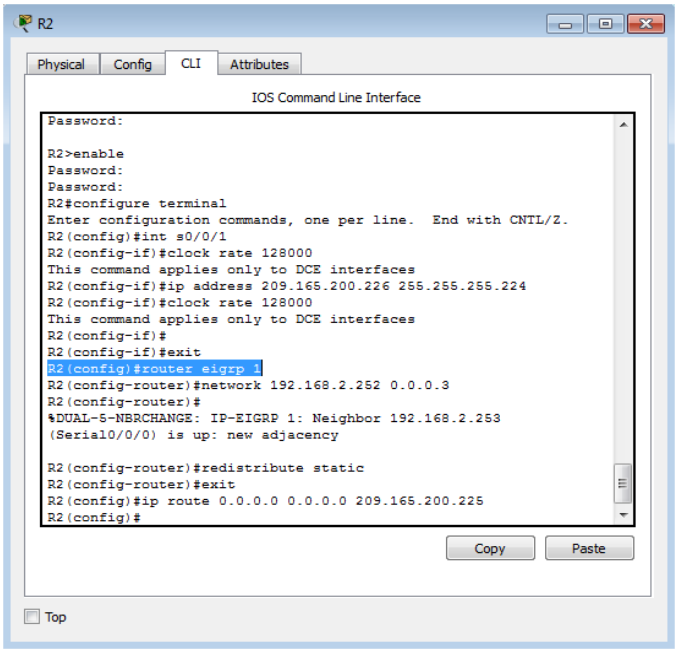


Imagen 242. Configuración EIGRP y Ruta Determinada al ISP en R2.

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***

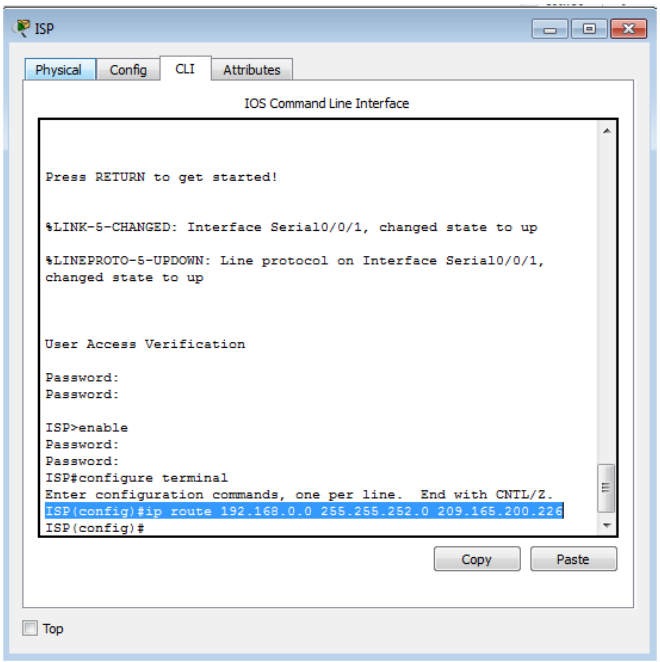


Imagen 243. Configuración Ruta Estática Resumida en ISP.

Copie la configuración en ejecución en la configuración de inicio

R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

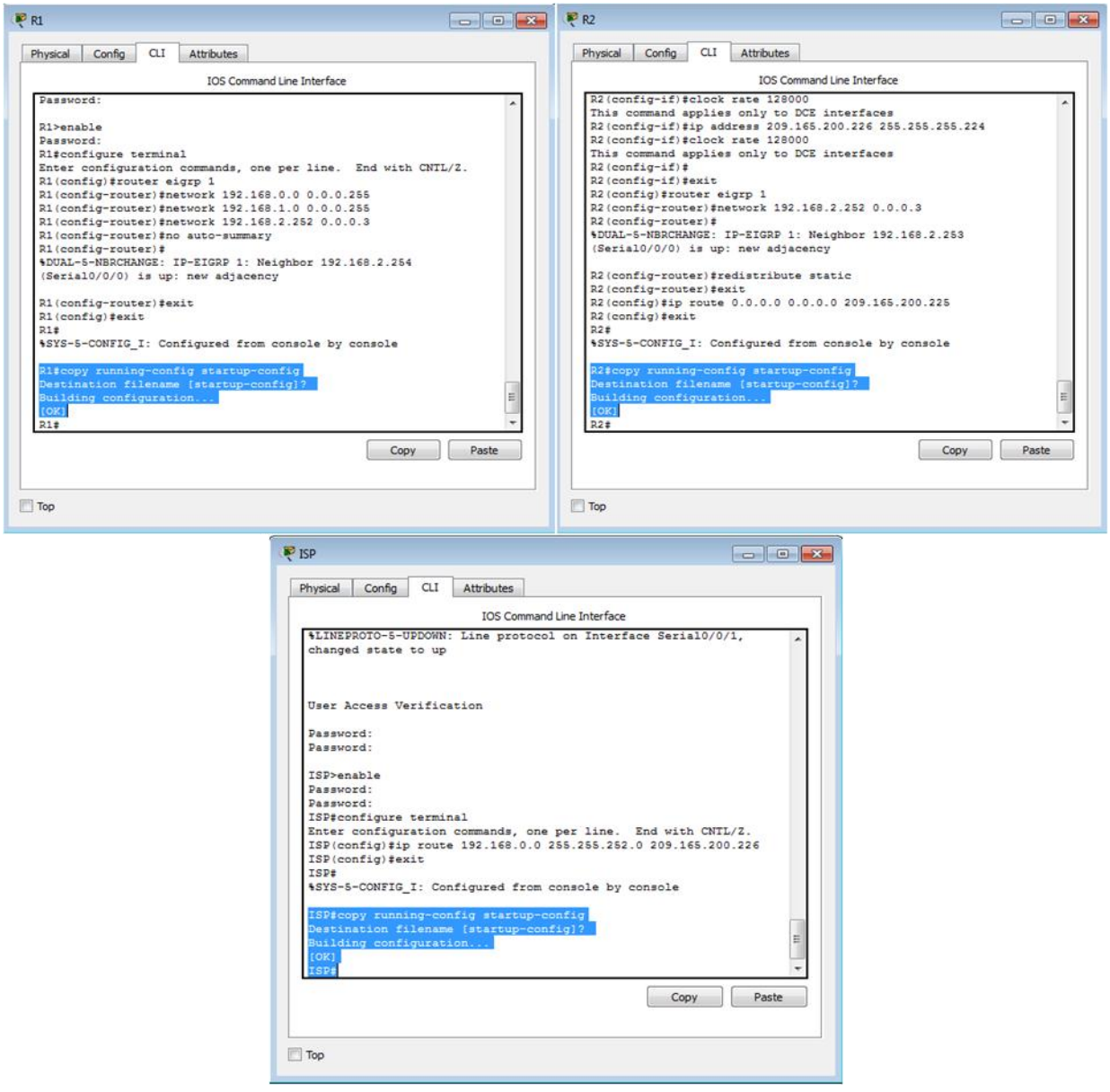


Imagen 244. Copia Configuración en la Configuración de Inicio

Paso 4. Verificar la conectividad de red entre los routers.

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

R1#ping 192.168.2.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms

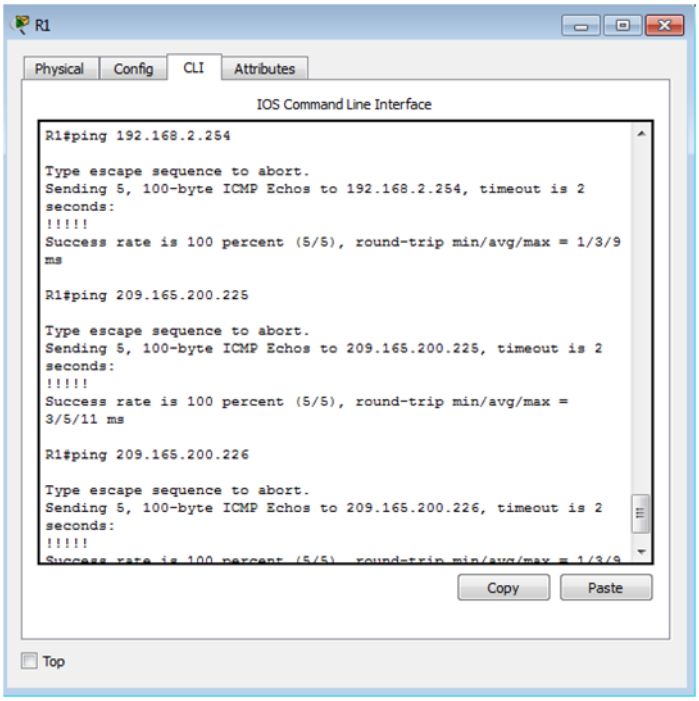


Imagen 245. Verificando Conectividad R1 hacia R2.

R1#ping 209.165.200.225

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 3/5/11 ms

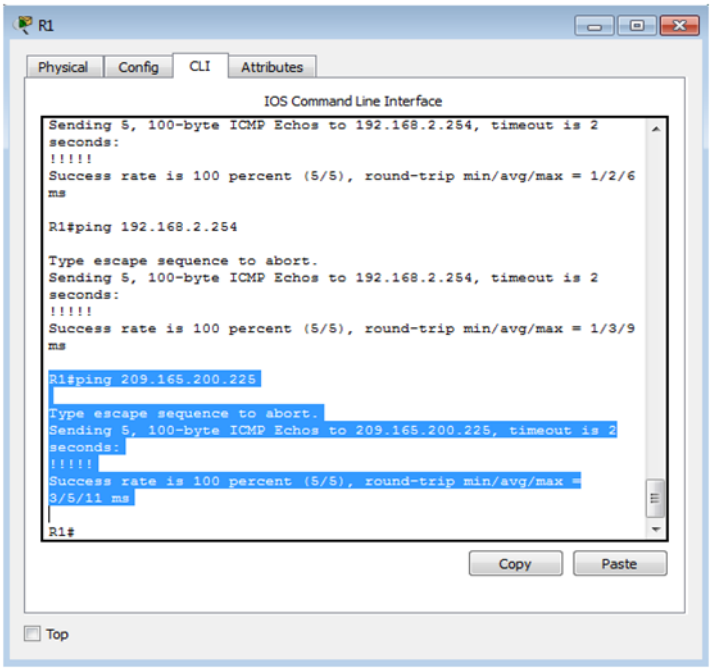


Imagen 246. Verificando Conectividad R1 hacia ISP.

R2#ping 192.168.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms

R2#ping 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2#ping 192.168.2.253

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

R2#

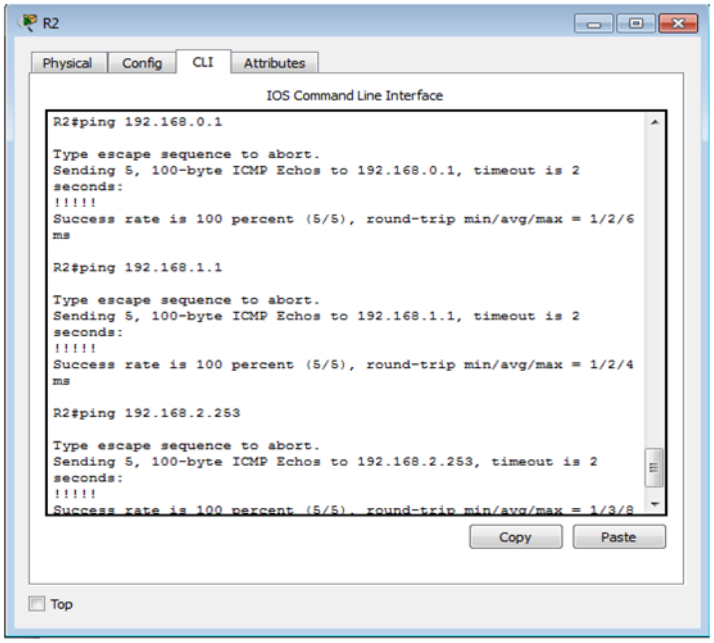


Imagen 247. Verificando Conectividad R2 hacia R1.

R2#ping 209.165.200.225

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms

R2#

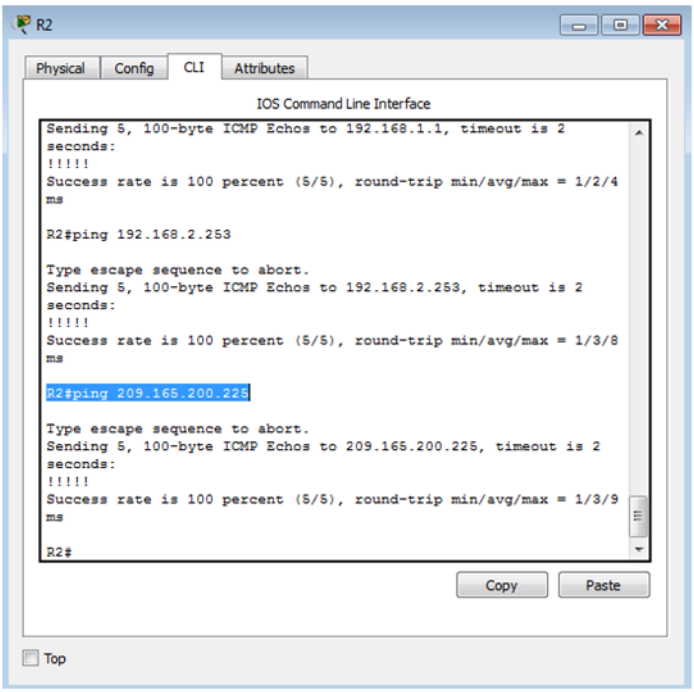


Imagen 248. Verificando Conectividad R2 hacia ISP.

ISP#ping 192.168.2.254

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5 ms

ISP#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/5/11 ms

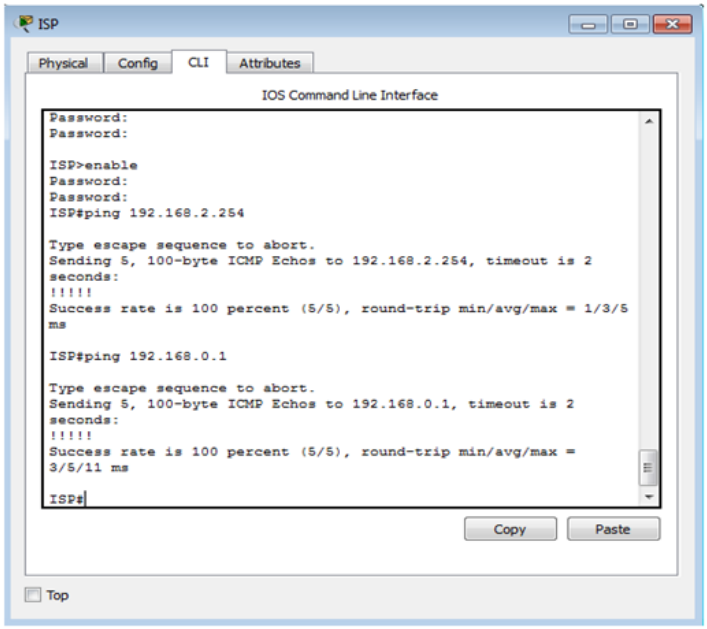


Imagen 249. Verificando Conectividad desde ISP hacia R1/R2.

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

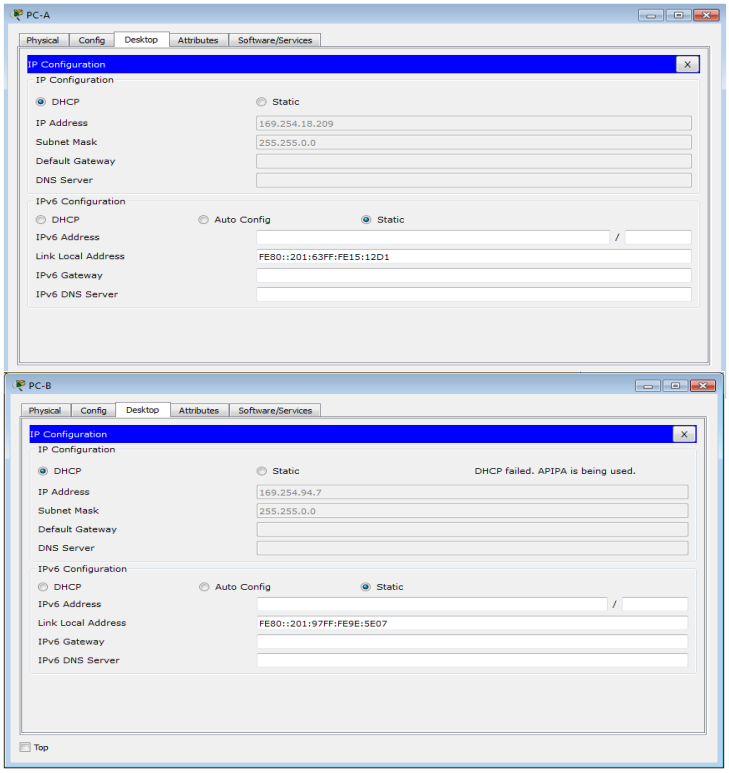


Imagen 250. Verificando Host Configurados para DHCP.

Parte 2. Configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

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

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

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

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

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

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

R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
^ % Invalid input detected at '^' marker.
R2(dhcp-config)#lease 2
^ % Invalid input detected at '^' marker.
R2(dhcp-config)#exit
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
^ % Invalid input detected at '^' marker.
R2(dhcp-config)#lease 2
^ % Invalid input detected at '^' marker.

R2(dhcp-config)#

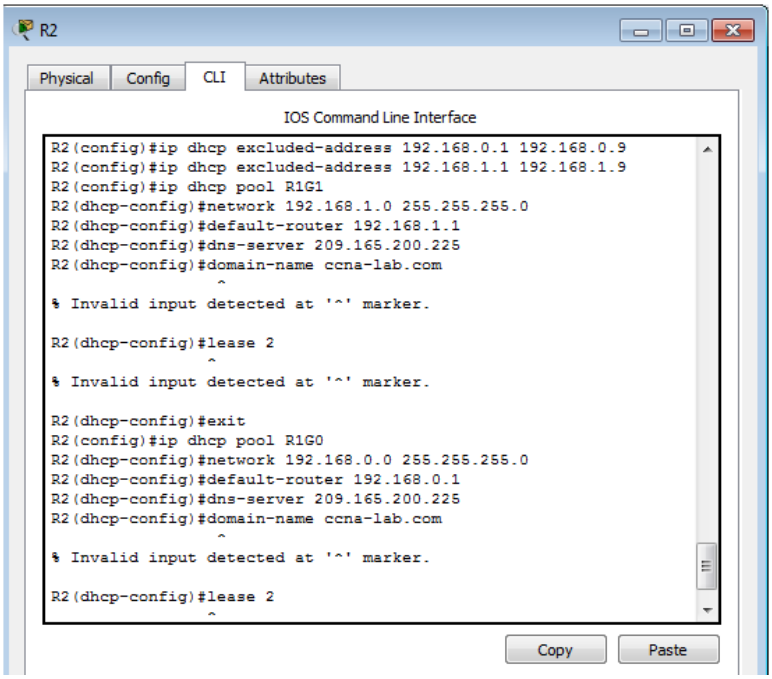


Imagen 251. Configuración Parámetros del servidor de DHCPv4 en R2.

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

No, porque el R1 no se ha configurado aún como agente de retransmisión DHCP.

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address.....: *0001.6315.12D1*
Link-local IPv6 Address.....: *FE80::201:63FF:FE15:12D1*
Autoconfiguration IP Address....: *169.254.18.209*
Subnet Mask.....: *255.255.0.0*
Default Gateway.....: *0.0.0.0*
DNS Servers.....: *0.0.0.0*

DHCP Servers.....: *0.0.0.0*

DHCPv6 Client DUID.....: *00-01-00-01-19-0B-6D-46-00-01-63-15-12-D1*

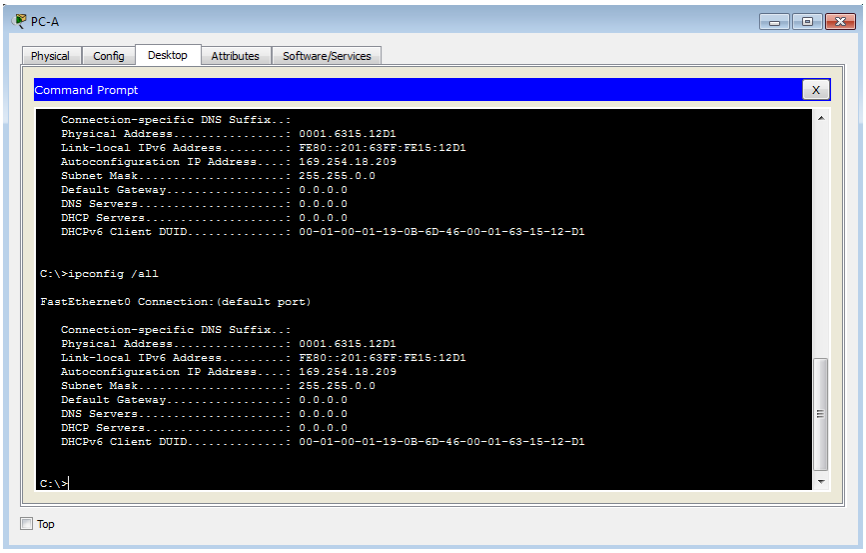


Imagen 252. Verificando Si Host Recibió una dirección IP del servidor de DHCP.

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

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

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

R1(config)#interface g0/0

R1(config-if)#ip helper-address 192.168.2.254

R1(config-if)#exit

R1(config)#interface g0/1

R1(config-if)#ip helper-address 192.168.2.254

R1(config-if)#

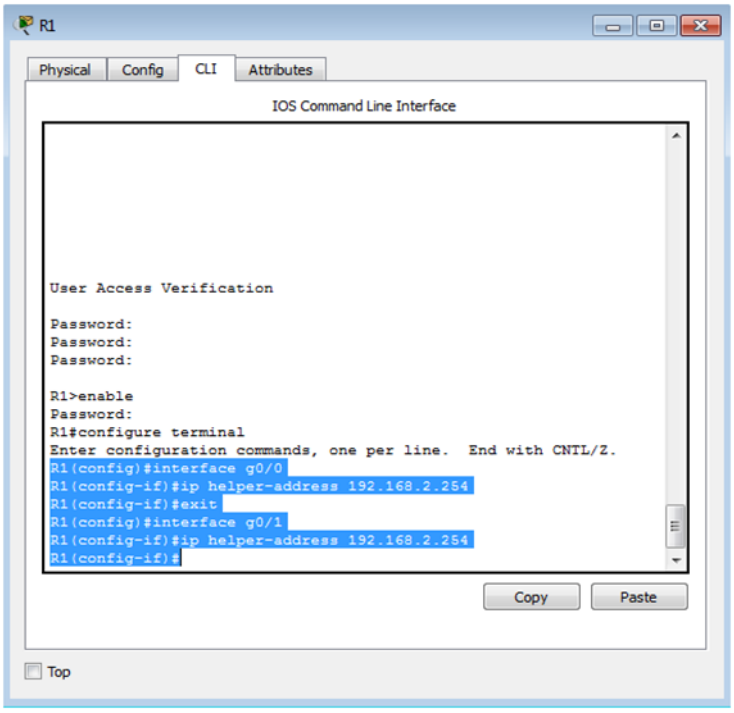


Imagen 253. Configurando el R1 como Agente de Retransmisión DHCP

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

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

PC-A

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address.....: *0001.6315.12D1*
Link-local IPv6 Address.....: *FE80::201:63FF:FE15:12D1*

IP Address.....: *192.168.1.10*

Subnet Mask.....: *255.255.255.0*

Default Gateway.....: *192.168.1.1*

DNS Servers.....: *209.165.200.225*

DHCP Servers.....: *192.168.2.254*

DHCPv6 Client DUID.....: *00-01-00-01-19-0B-6D-46-00-01-63-15-12-D1*

PC-B

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:

Physical Address.....: 0001.979E.5E07

Link-local IPv6 Address.....: FE80::201:97FF:FE9E:5E07

IP Address.....: 192.168.0.10

Subnet Mask.....: 255.255.255.0

Default Gateway.....: 192.168.0.1

DNS Servers.....: 209.165.200.225

DHCP Servers.....: 192.168.2.254

DHCPv6 Client DUID.....: 00-01-00-01-4A-DA-7C-AC-00-01-97-9E-5E-07

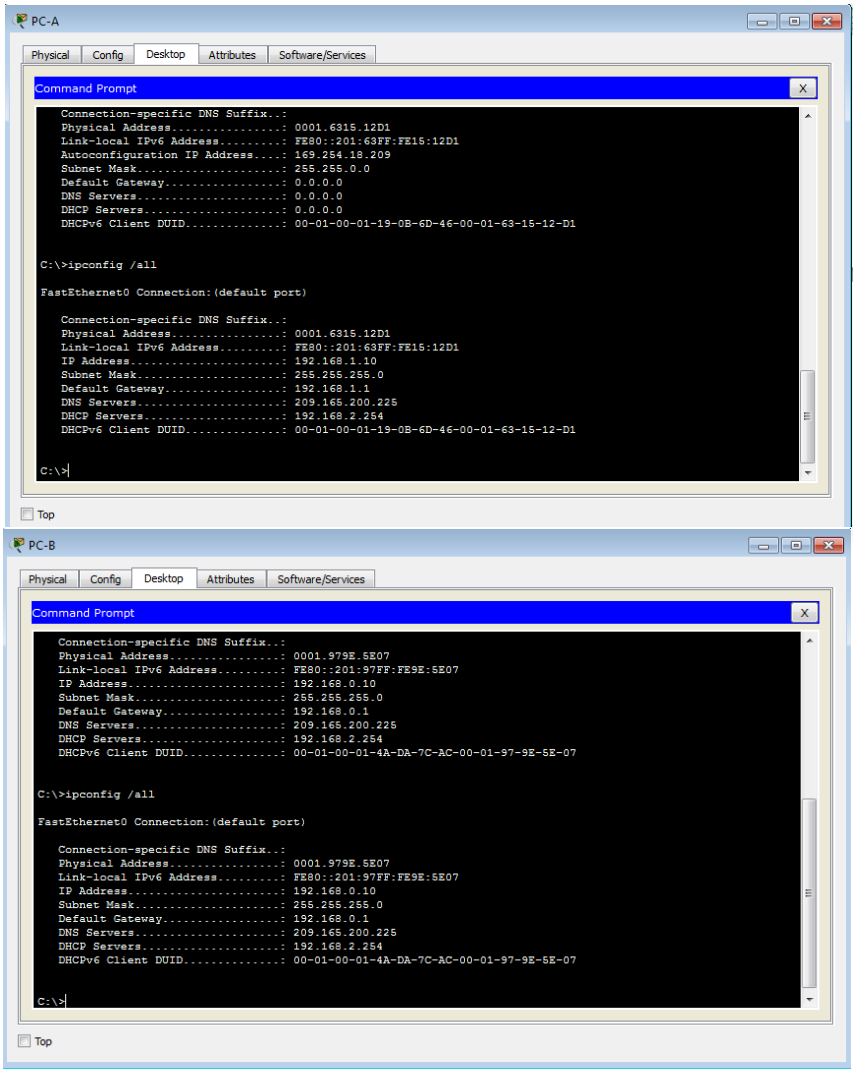


Imagen 254. Configuración IP para la PC-A y la PC-B.

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

Para PCA: 192.168.1.10 y

Para PCB: 192.168.0.10

Paso 4. Verificar los servicios DHCP y los arrendamientos de direcciones en el R2.

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

R2>show ip dhcp binding

IP address	*Client-ID/ Hardware address*	*Lease expiration*	*Type*
192.168.1.10	*0001.6315.12D1*	*--*	*Automatic*
192.168.0.10	*0001.979E.5E07*	*--*	*Automatic*

R2>

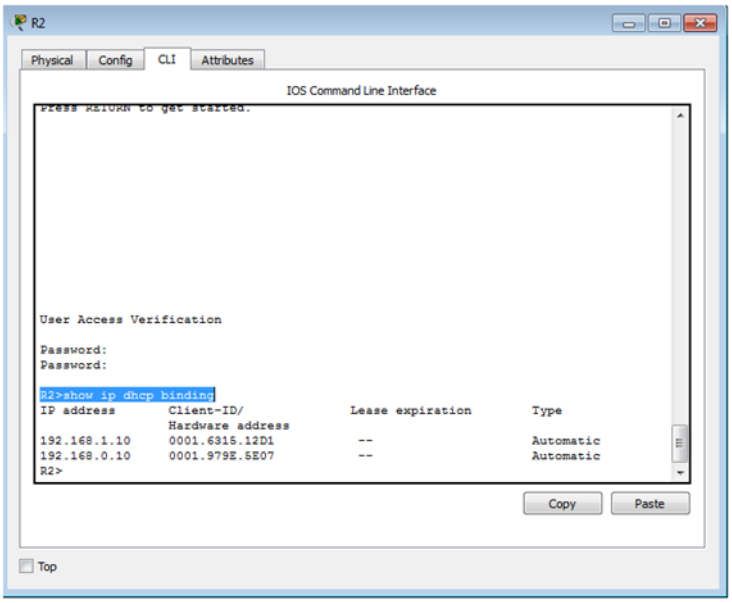


Imagen 255. Verificando los Servicios DHCP y los Arrendamientos de Direcciones en el R2.

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

Se observan las direcciones de hardware que identifican los computadores que se unieron a la red.

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.

Packet Tracer 7.0 no soporta este comando

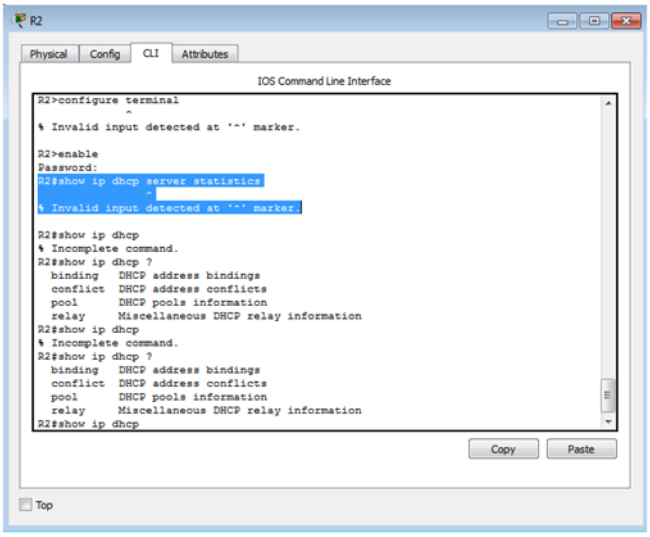


*Imagen 256. Comando **show ip dhcp server statistics***

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

Se indican 10 tipos diferentes de DHCP

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

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

El índice actual (Current index), hace referencia a la siguiente dirección de arrendamiento que está disponible

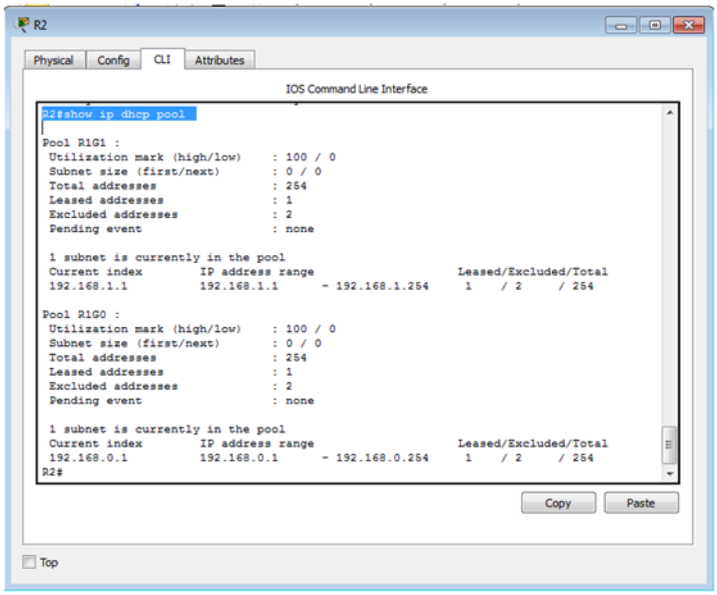


Imagen 257. Configuración del Pool de DHCP

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

Packet Tracer 7.0 no soporta este comando

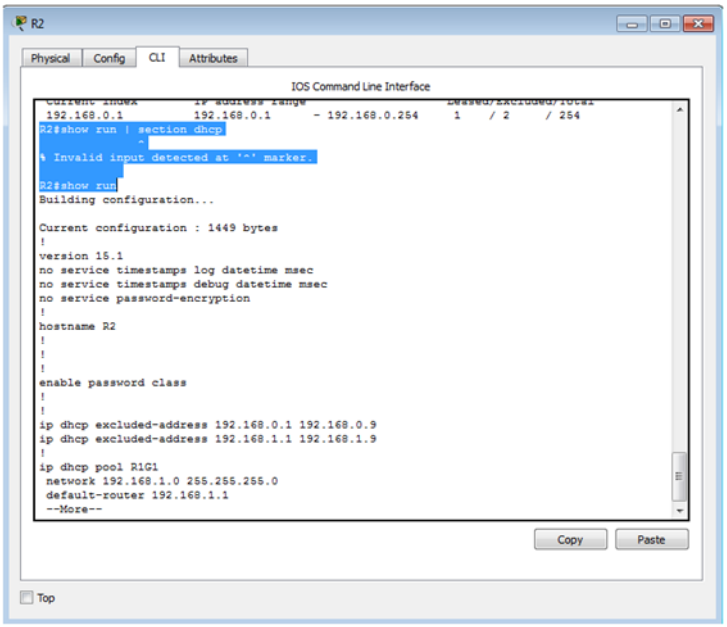


Imagen 258. Mirar la Configuración DHCP en la Configuración en Ejecución

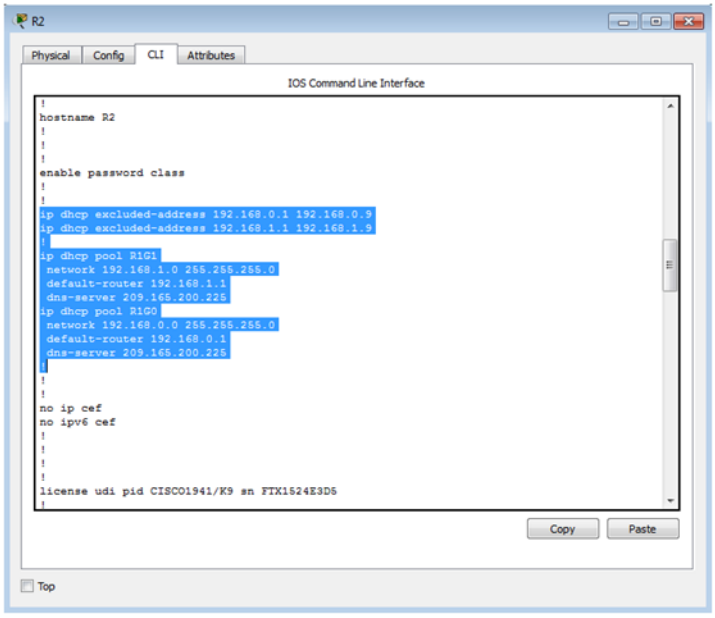


Imagen 259. Configuración DHCP.

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

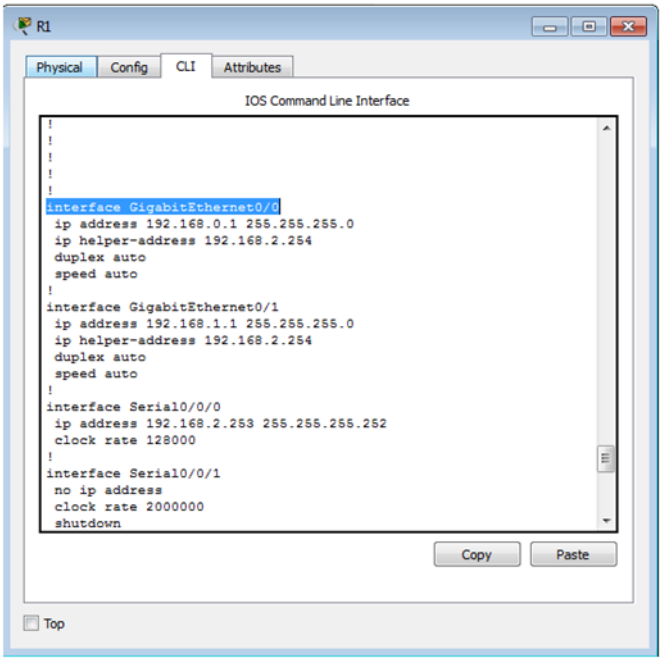


Imagen 260. Configuración de Retransmisión DHCP para G0/0 y G0/1.

Reflexión

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

Respuesta: Tener un servidor de DHCP en el Router disminuye la administración centralizada en la red por lo que cada router se dedica a la administración de su propia red.

Tabla 11**:**

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

La introducción de un servidor de protocolo de configuración dinámica de host (DHCP) en la red local simplifica la asignación de direcciones IP tanto a los dispositivos de escritorio como a los móviles. El uso de un servidor de DHCP centralizado permite a las organizaciones administrar todas las asignaciones de direcciones IP desde un único servidor. Esta práctica hace que la administración de direcciones IP sea más eficaz y asegura la coherencia en toda la organización, incluso en las sucursales, por tanto en la presente práctica se ha realizado:

- ➢ El armado de la red con dispositivos y cables referidos en la guía.
- ➢ Configuración adecuada de los dispositivos con los parámetros básicos para el buen funcionamiento de la red y su conectividad.
- ➢ Configuración de R2 como servidor de DHCPv4 y R1 como agente de retransmisión DHCP.

10.1.2.5. Lab - Configuring Basic Dhcpv4 On A Switch

Topología

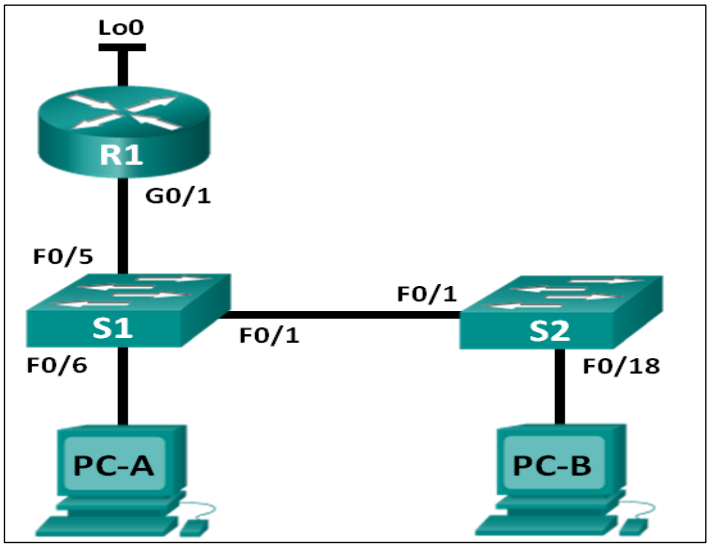


Imagen 261, topología práctica 10.1.2.5.

Tabla 12:

Tabla de direccionamiento

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

Objetivos

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

Parte 2: cambiar la preferencia de SDM

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

Parte 3: configurar DHCPv4

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

Parte 4: configurar DHCP para varias VLAN

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

Parte 5: habilitar el routing IP

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

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

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

Para la práctica se reemplaza el switch 2960 por un switch 3560 debido a que no admite los comandos para las preferencias SDM.

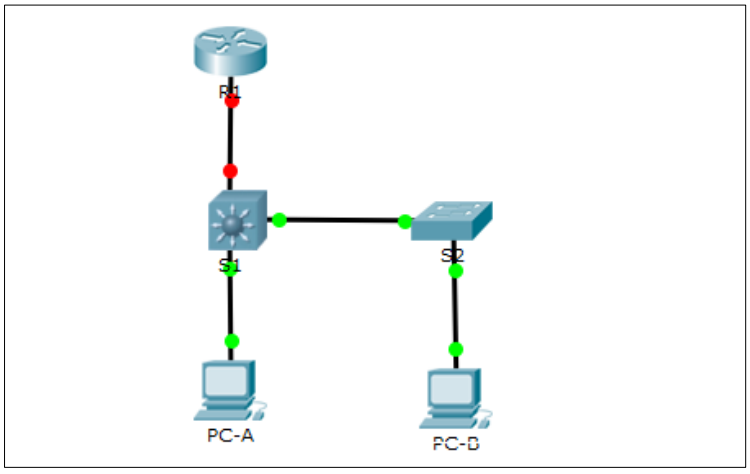


Imagen 262, armar el cableado.

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

Router

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################ [OK]
```

Imagen 263, inicializar y volver a cargar router R1.

Switch S1

```
Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0002.162E.D659
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
################################################################################ [OK]
```

Imagen 264, inicializar y volver a cargar Switch S1

Switch S2

```
Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0001.C9B7.1290
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
################################################################################ [OK]
```

Imagen 265, inicializar y volver a cargar Switch S2

Paso 3. Configurar los parámetros básicos en los dispositivos.

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

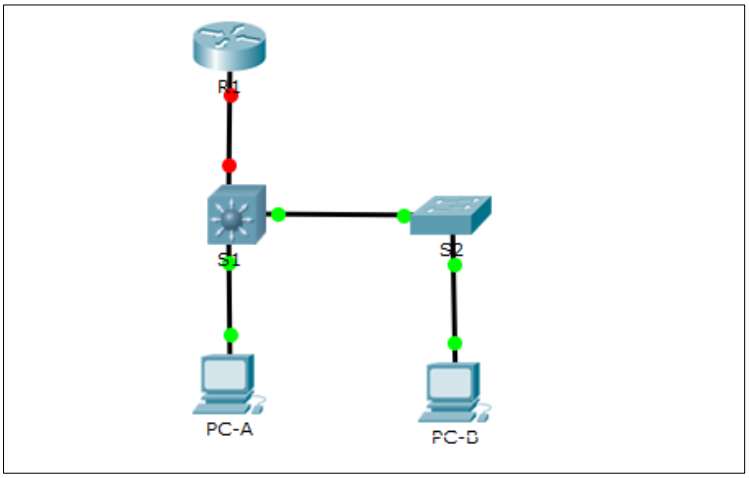


Imagen 266, asignación de los nombres de dispositivos.

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.

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Imagen 267, asignación de contraseñas y desactivar búsqueda DNS en R1.

```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Imagen 268, asignación de contraseñas y desactivar búsqueda DNS en S1.

```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#enable secret class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line vty 0 4
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Imagen 269, asignación de contraseñas y desactivar búsqueda DNS en S2.

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

```
R1(config)#int g0/1
R1(config-if)#ip add 192.168.1.10 255.255.255.0
R1(config-if)#no shut

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

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

R1(config-if)#int lo0

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

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

R1(config-if)#ip add 209.165.200.225 225.255.255.224
Bad mask 0xE1FFFFE0 for address 209.165.200.225
R1(config-if)#no shut
R1(config-if)#ip add 209.165.200.225 255.255.255.224
R1(config-if)#no shut
```

Imagen 270, Configurar las direcciones IP en las interfaces G0/1 y Lo0 del R1.

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

```
S1(config)#int vlan 1
S1(config-if)#ip add 192.168.1.1 255.255.255.0
S1(config-if)#no shut

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

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

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

S1(config-if)#ip add 192.168.2.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#
```

Imagen 271, Configurar las direcciones IP en las interfaces G0/1 y Lo0 del R1.

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

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Imagen 272 Configurar las direcciones IP en las interfaces G0/1 y Lo0 del R1.

Parte 2. Cambiar la preferencia de SDM

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

Paso 1. Mostrar la preferencia de SDM en el S1.

En el S1, emita el comando **show sdm prefer** en modo EXEC privilegiado. Si no se cambió la plantilla predeterminada de fábrica, debería seguir siendo **default**. La plantilla **default** no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será **dual-ipv4-and-ipv6 default**.

S1# **show sdm prefer**

The current template is "default" template.

The selected template optimizes the resources in

the switch to support this level of features for

0 routed interfaces and 255 VLANs.

number of unicast mac addresses: 8K

number of IPv4 IGMP groups: 0.25K

number of IPv4/MAC qos aces: 0.125k

number of IPv4/MAC security aces: 0.375k

```
S1(config-if)#ip add 192.168.2.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#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:                       256
  number of IPv4/MAC qos aces:                      128
  number of IPv4/MAC security aces:                 384
```

Imagen 273, Comando show sdm prefer.

¿Cuál es la plantilla actual?

Respuesta: la plantilla actual es “desktop default”

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? Respuesta: la plantilla disponible será “Routing”

```
S1(config)#sdm prefer lanbase-routing
                      ^
% Invalid input detected at '^' marker.

S1(config)#sdm prefer ?
  access               Access bias
  default              Default bias
  dual-ipv4-and-ipv6   Support both IPv4 and IPv6
  routing              Unicast bias
  vlan                 Vlan bias
S1(config)#sdm prefer sdm prefer routing
                      ^
% Invalid input detected at '^' marker.

S1(config)#sdm prefer 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.
```

Imagen 274, preferencia de SDM en routing.

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

S1# **reload**

System configuration has been modified. Save? [yes/no]: **no**

Proceed with reload? [confirm]

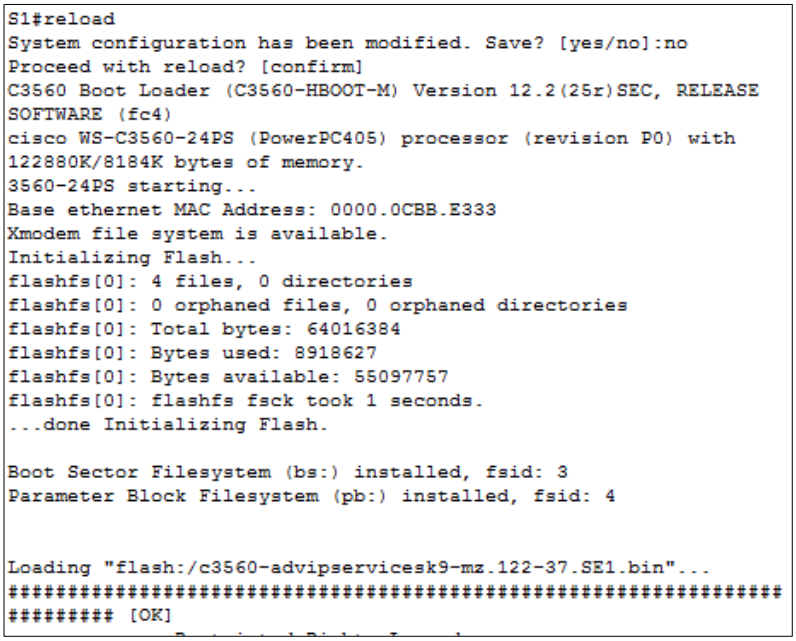


Imagen 275, recargar el switch comando reload.

Paso 3. Verificar que la plantilla lanbase-routing esté cargada.

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

S1# **show sdm prefer**

The current template is "lanbase-routing" template.

The selected template optimizes the resources in

the switch to support this level of features for

0 routed interfaces and 255 VLANs.

number of unicast mac addresses: 4K

number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes: 0.75K
number of directly-connected IPv4 hosts: 0.75K
number of indirect IPv4 routes: 16
number of IPv6 multicast groups: 0.375k
number of directly-connected IPv6 addresses: 0.75K
number of indirect IPv6 unicast routes: 16
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.125k
number of IPv4/MAC security aces: 0.375k
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 0.375k
number of IPv6 security aces: 127

```
S1#show sdm prefer
 The current template is "routing" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  3K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    11K
  number of directly-connected IPv6 addresses:      3K
  number of indirect IPv6 unicast routes:           8K
  number of IPv4 policy based routing aces:         0.5K
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
```

Imagen 276, comando show sdm prefer.

Parte 3. 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. **Respuesta:** 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. **Respuesta:** 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. **Respuesta:** 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. **Respuesta**: 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. **Respuesta**: dns-server 192.168.1.9
f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó. **Respuesta**: lease 3
g. Guarde la configuración en ejecución en el archivo de configuración de inicio. **Respuesta:** copy run start

```
S1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#ip dhcp pool DHCP1
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.1.1
S1(dhcp-config)#dns-server 192.168.1.9
S1(dhcp-config)#lease 3
                  ^
% Invalid input detected at '^' marker.

S1(dhcp-config)#copy run start
                  ^
% Invalid input detected at '^' marker.

S1(dhcp-config)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Imagen 277, configurar DHCP para la VLAN 1.

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: **192.168.1.12**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.1.1**

Para la PC-B, incluya lo siguiente:

Dirección IP: **192.168.1.11**

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

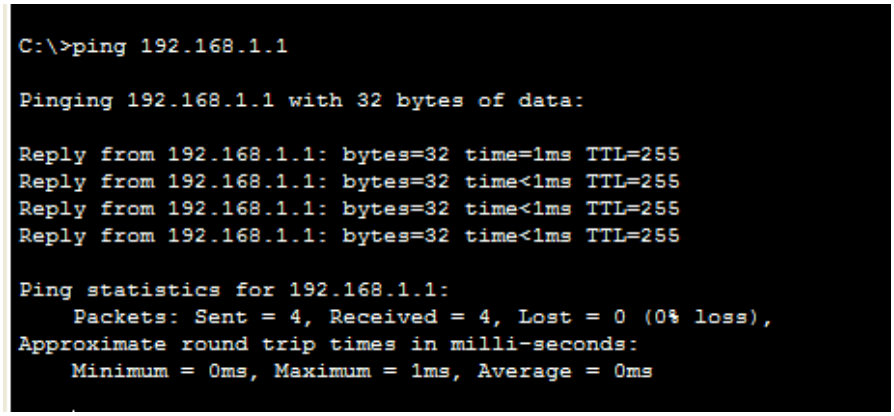


Imagen 278, ping de la PC-A al gateway predeterminado de la VLAN 1

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

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Imagen 279, ping de la PC-A a la PC-B.

¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1? Si es posible

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Imagen 280, ping de la PC-A a la interfaz G0/1 del R1.

Parte 4. 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.

Parte 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 fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
```

Paso 2. Configurar DHCPv4 para la VLAN 2.

a. Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.
   Respuesta: ip dhcp excluded-address 192.168.2.1 192.168.2.10
b. Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó.
   Respuesta: ip dhcp pool DHCP2
c. Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.
   Respuesta: network 192.168.2.0 255.255.255.0
d. Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.
   Respuesta: default-router 192.168.2.1
e. Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.
   Respuesta: dns-server 192.168.2.9
f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.
   Respuesta: lease 3
g. Guarde la configuración en ejecución en el archivo de configuración de inicio.
   Respuesta: copy run start

```
S1(config)#int fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to
up

S1(config-if)#
S1(config-if)#exit
S1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)#ip dhcp pool DHCP2
S1(dhcp-config)#network 192.168.2.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.2.1
S1(dhcp-config)#dns-server 192.168.2.9
```

Imagen 281, configurar DHCPv4 para la VLAN 2.

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
¿Es posible hacer ping de la PC-A a la PC-B? no es posible
¿Los pings eran correctos? Respuesta: La puerta de enlace de la PC-A esta en la misma red por lo tanto el ping es satisfactorio, la PC-B está en otra red por lo tanto el ping no es satisfactorio.

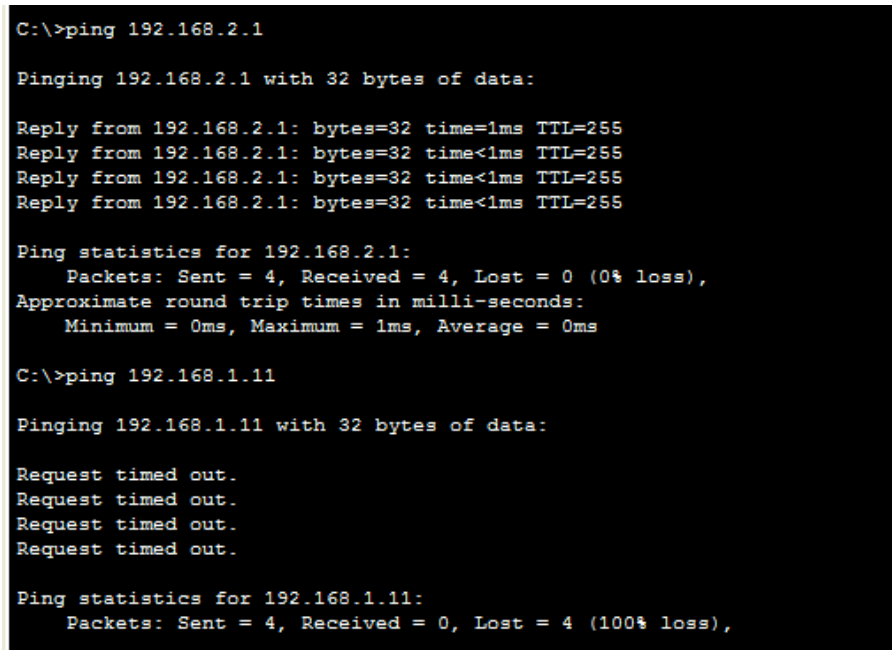


Imagen 282, verificar la conectividad y DHCPv4.

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

¿Qué resultado arrojó este comando?

Respuesta: no hay puerta de enlace establecida ni tabla de routing presente en el switch

Parte 5. 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.

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

S1(config)# **ip routing**

Verificar la conectividad entre las VLAN.

¿Es posible hacer ping de la PC-A a la PC-B? **Respuesta:** si es posible

¿Qué función realiza el switch? **Respuesta:** el switch esta routeando los paquetes entre vlan

Vea la información de la tabla de routing para el S1.

¿Qué información de la ruta está incluida en el resultado de este comando? **Respuesta:** hay dos redes directamente conectadas, el switch exhibe una tabla de routing mostrando dos vlan directamente conectadas.

C 192.168.1.0/24 is directly connected, Vlan1

C 192.168.2.0/24 is directly connected, Vlan2

Vea la información de la tabla de routing para el R1.

¿Qué información de la ruta está incluida en el resultado de este comando?

Respuesta: el router muestra dos redes directamente conectadas192.168.1.0 y 209.165.200.224 pero no tienen una entrada para la red 192.168.2.0.

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

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1

L 192.168.1.10/32 is directly connected, GigabitEthernet0/1

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.200.224/27 is directly connected, Loopback0

L 209.165.200.225/32 is directly connected, Loopback0

¿Es posible hacer ping de la PC-A al R1? **Respuesta:** No es posible hacer ping

¿Es posible hacer ping de la PC-A a la interfaz Lo0? **Respuesta:** No es posible hacer ping

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Respuesta: para que la comunicación se realice entre todas las redes las rutas deben ser agregadas en la tabla de routing.

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.

En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.

Respuesta: ip route 0.0.0.0 0.0.0.0 192.168.1.10

En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

Respuesta: ip route 192.168.2.0 255.255.255.0 g0/1

Vea la información de la tabla de routing para el S1.

```
S1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, Vlan1
C    192.168.2.0/24 is directly connected, Vlan2
S*   0.0.0.0/0 [1/0] via 192.168.1.10
```

Imagen 283, información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?

Respuesta: la puerta de enlace de último recurso es 192.168.1.10.

Vea la información de la tabla de routing para el R1.

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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.10/32 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
```

Imagen 284, información de la tabla de routing para el R1.

¿Cómo está representada la ruta estática?

Respuesta: la ruta estática está representada por 192.168.2.0/24 está directamente conectada a gigabit ethernet 0/1

¿Es posible hacer ping de la PC-A al R1? **Respuesta:** Si es posible

¿Es posible hacer ping de la PC-A a la interfaz Lo0? **Respuesta:** Si es posible

```
C:\>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<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=254
Reply from 192.168.1.10: bytes=32 time<1ms TTL=254
Reply from 192.168.1.10: bytes=32 time<1ms TTL=254
Reply from 192.168.1.10: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Imagen 285, ping PC-A al R1 y PC-A a la interfaz Lo0.

Reflexión

- Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

  Respuesta: las direcciones estáticas fueron excluidas antes de crear el pool DHCP, existe una ventana de tiempo donde se excluyen las direcciones y podrían ser dadas dinámicamente hacia unos hosts.

- Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

  Respuesta: el switch asigna las direcciones IP basándose en el asignamiento de puerto de la vlan cuando el host está conectado.

- Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?

  Respuesta: ofrecen una serie de funciones que protegen el acceso a la red e implementan las políticas de seguridad.

Estas funciones incluyen autenticación flexible con una sólida tecnología 802.1x, SXP Cisco TrustSec® para la implementación de políticas, acceso de seguridad y control basados en mfunciones con Cisco ISE y seguridad de primer salto de IPv6. Por otra parte, estos switches Cisco protegen la confidencialidad e integridad de los datos en la red con cifrado a nivel de puerto.

Conclusiones

- Un dispositivo Cisco que ejecuta el software IOS de Cisco puede configurarse para que funcione como servidor de DHCPv4. El servidor de DHCPv4 que utiliza IOS de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones especificados dentro del router para los clientes DHCPv4.
- 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. Comandos utilizados (show sdm prefer), (sdm prefer lanbase-routing).

- El dispositivo que funciona como servidor de DHCPv4 asigna todas las direcciones IPv4 en un conjunto de direcciones DHCPv4, a menos que esté configurado para excluir direcciones específicas, también se configura DHCP para las VLAN 1 y VLAN 2.

- El routing IP en el switch, permite la comunicación entre VLAN, para que todas las redes se comuniquen, se implementó rutas estáticas en el S1 y el R1.

10.2.3.5 LAB - Configuración de Dhcpv6 Sin Estado y Con Estado

Topología

Imagen 286. Topología de red.

Tabla 13:

Tabla de direccionamiento

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

Objetivos

Objetivo general

- Configurar la red para que utilice SLAAC. Una vez que se verifique la conectividad, configurar los parámetros de DHCPv6 y modificar la red para que utilice DHCPv6 sin estado. Una vez que verificado que DHCPv6 sin estado funcione correctamente, modificar la configuración del R1 para que utilice DHCPv6 con estado. Finalmente usar Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

Objetivos Especificos

- ➢ Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- ➢ Parte 2: configurar la red para SLAAC
- ➢ Parte 3: configurar la red para DHCPv6 sin estado
- ➢ Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación.

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

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

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

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6. La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

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

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

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

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

S1# **show sdm prefer**

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

S1# **config t**

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

S1(config)# **end**

S1# **reload**

Nota. Packet tracert no soporta estos comandos.

Recursos necesarios

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

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

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

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

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

Nota. La implementación de la red en packet tracert la desarrollamos con un swich 3500, debido a que el swich 2960 no soporta todas la capacidades de IPV6

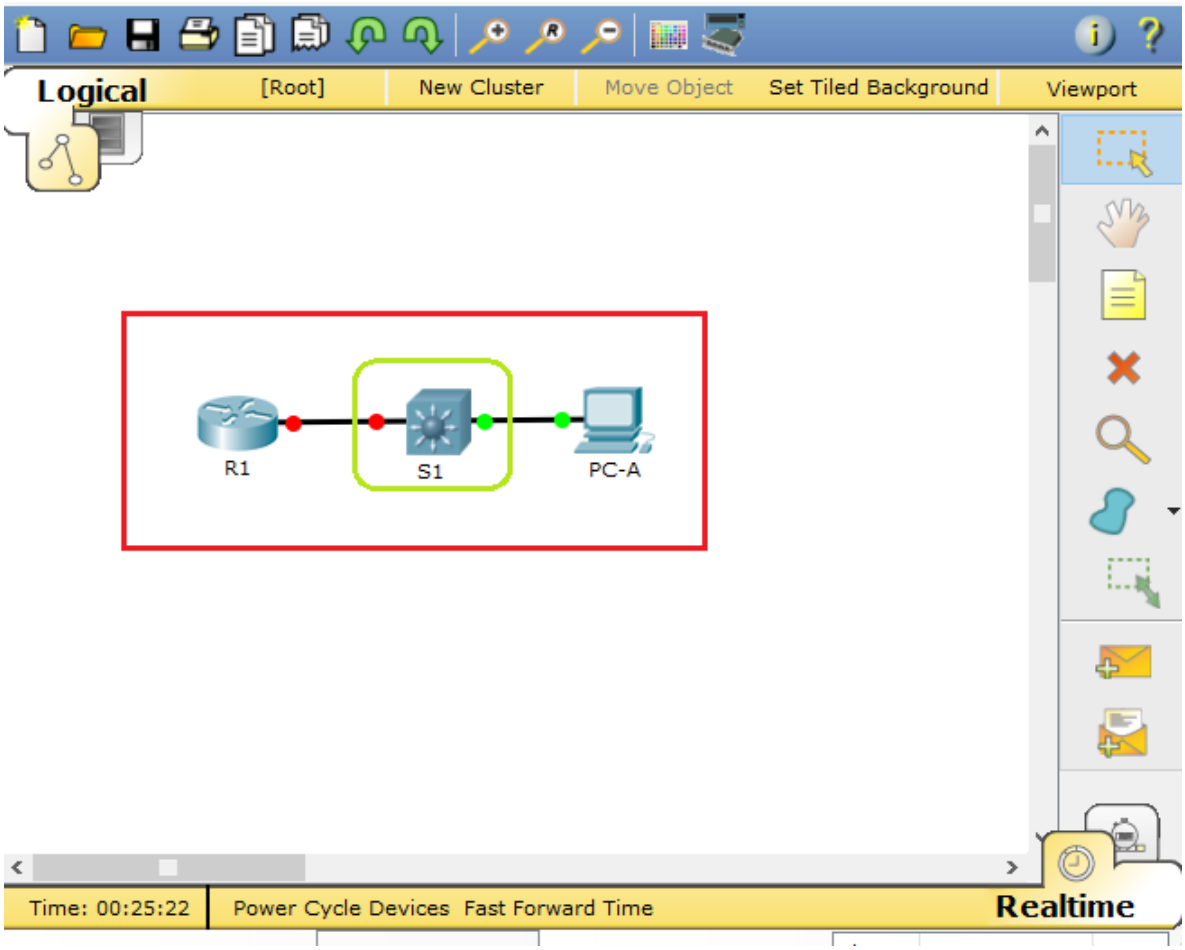


Imagen 287. Implementación de la topología de red.

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

Paso 3. Configurar R1

Desactive la búsqueda del DNS.

Configure el nombre del dispositivo.

Cifre las contraseñas de texto no cifrado.

Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado. (banner motd #Unauthroized access to this router is prohibited. #)

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

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

Establezca el inicio de sesión de consola en modo sincrónico.

Guardar la configuración en ejecución en la configuración de inicio.

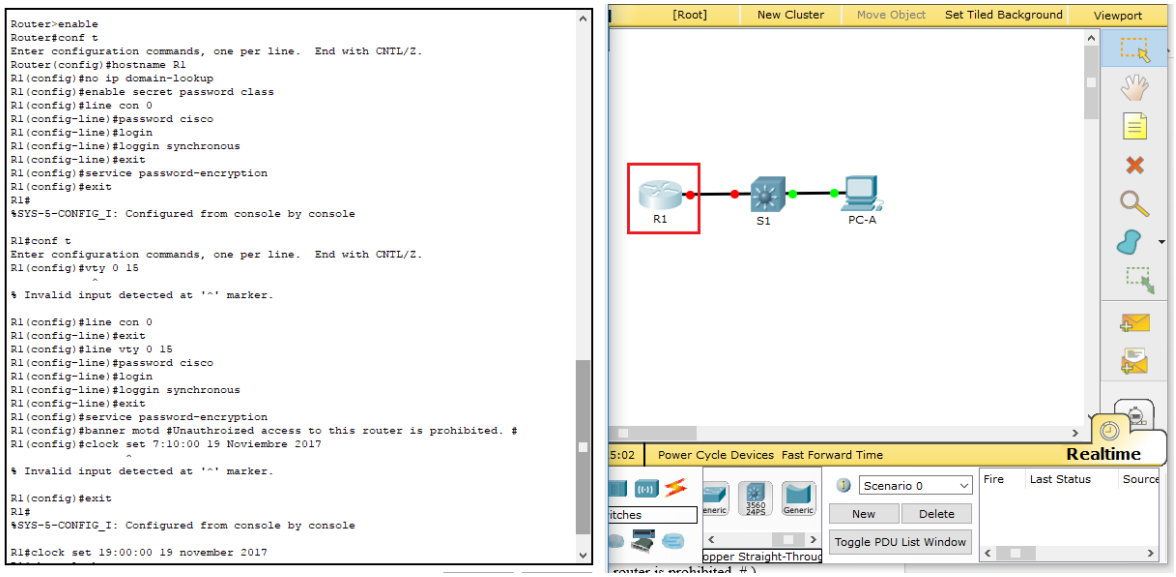


Imagen 288. Configuración R1.

Paso 4. Configurar el S1.

Desactive la búsqueda del DNS.

Configure el nombre del dispositivo.

Cifre las contraseñas de texto no cifrado.

Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado. (banner motd #Unauthroized access to this router is prohibited. #)

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

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

Establezca el inicio de sesión de consola en modo sincrónico.

Desactive administrativamente todas las interfaces inactivas.

Guarde la configuración en ejecución en la configuración de inicio.

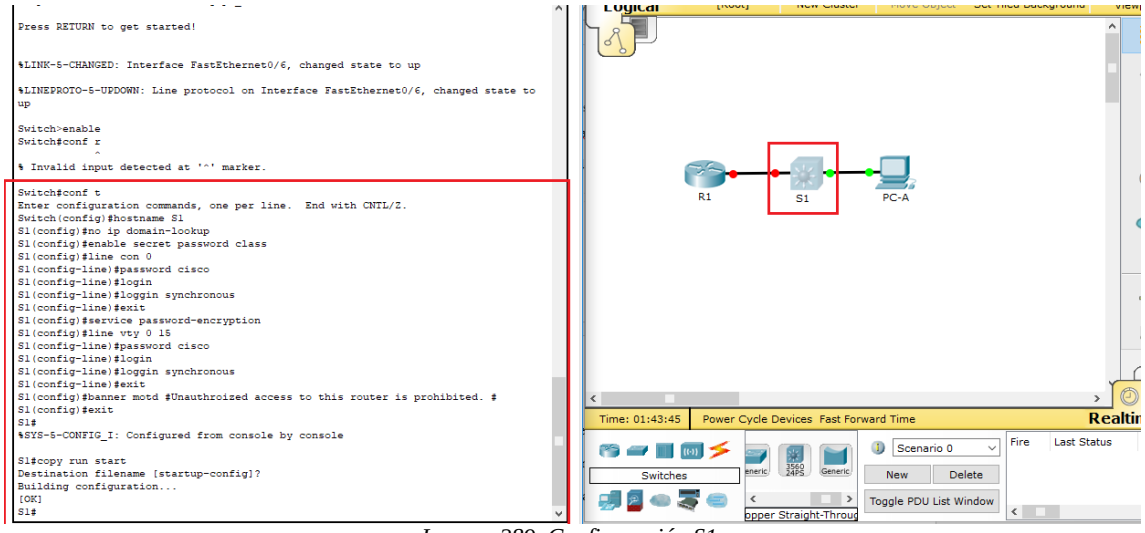


Imagen 289. Configuración S1.

Parte 2: Configurar la red para SLAAC

Paso 1. Preparar la PC-A.

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

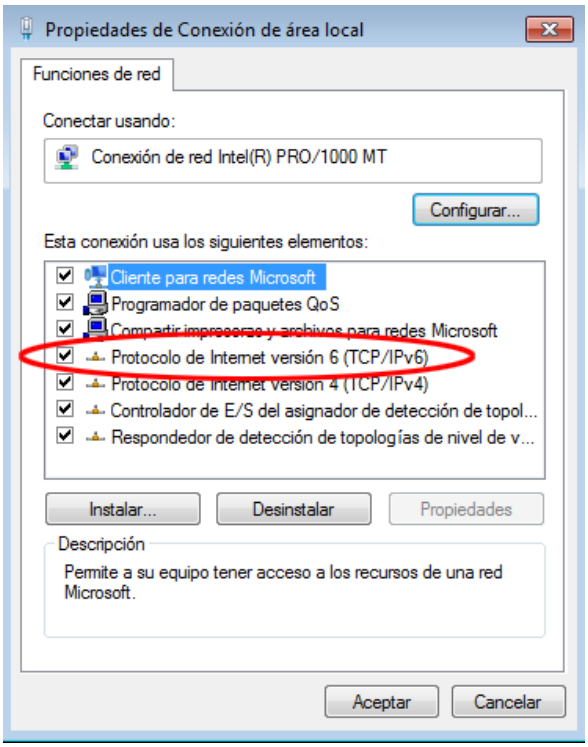


Imagen 290. Preparar la PC-A.

Inicie una captura del tráfico en la NIC con Wireshark.

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

Imagen 291. Configuración mensajes RA.

Paso 2. Configurar R1

Habilite el routing de unidifusión IPv6.

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

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

Active la interfaz G0/1.

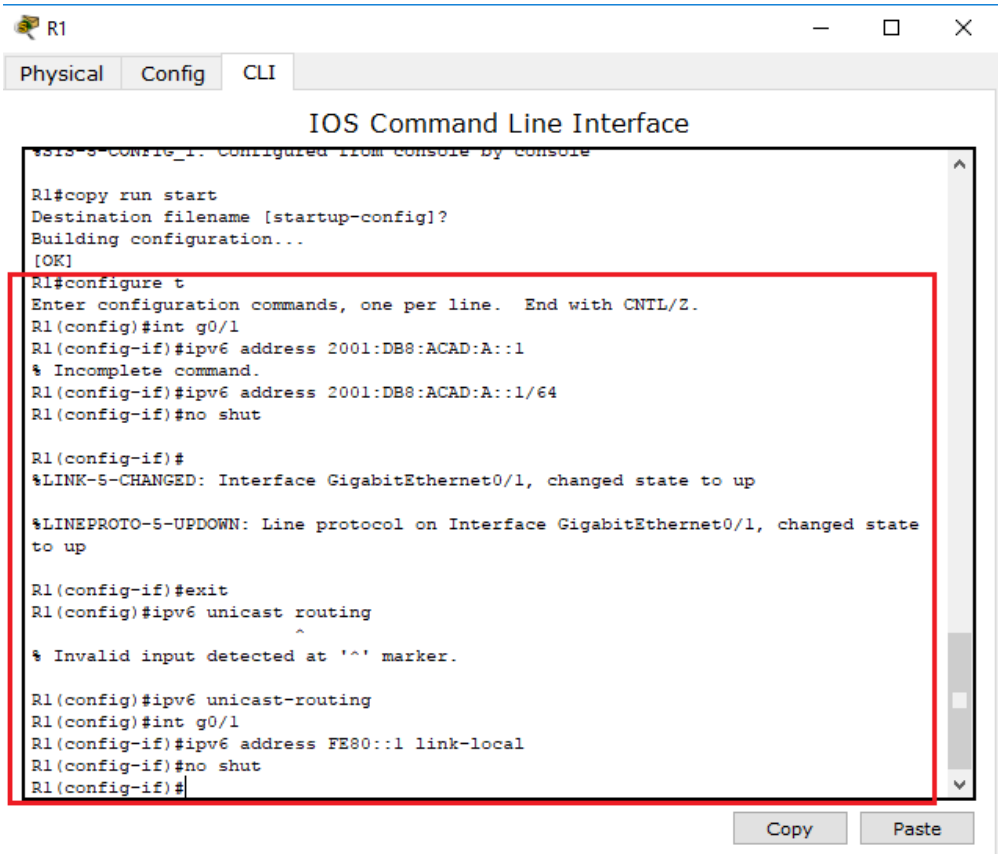


Imagen 292. Configuracion R1.

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

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

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

```
  FF02::2

  FF02::1:FF00:1

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.
```

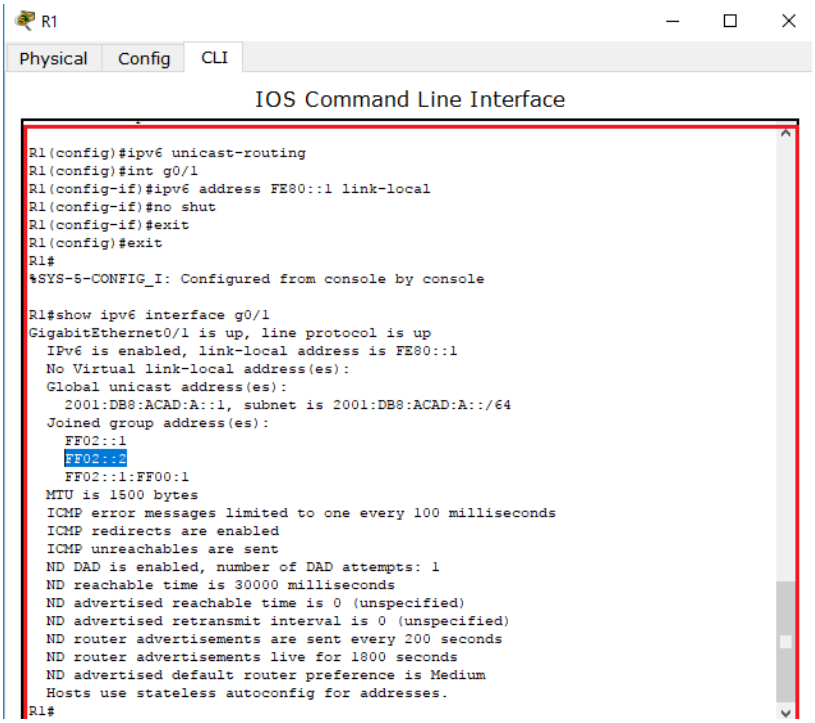


Imagen 293. Verificacion que el R1 forme parte del grupo de multidifusión de todos los routers R1.

Paso 4. Configurar el S1.

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

S1(config)# **interface vlan 1**

S1(config-if)# **ipv6 address autoconfig**

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

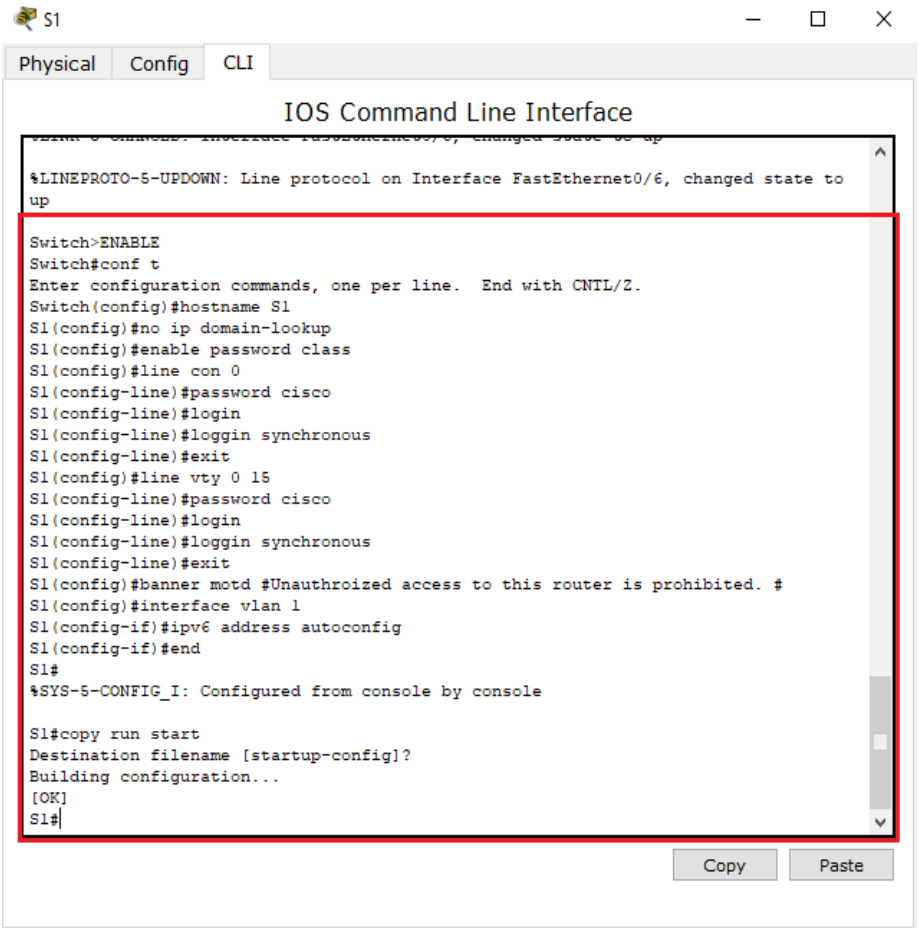


Imagen 294. Configurarcion de S1

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

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

```
S1# show ipv6 interface
```

```
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
  No Virtual link-local address(es):
  Stateless address autoconfig enabled
  Global unicast address(es):
    2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64
[EUI/CAL/PRE]
      valid lifetime 2591988 preferred lifetime 604788
  Joined group address(es):
    FF02::1
    FF02::1:FFE8:8A40
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Output features: Check hwidb
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
  Default router is FE80::1 on Vlan1
```

Nota. Packet tracert no soporta esta caracteristica.

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

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

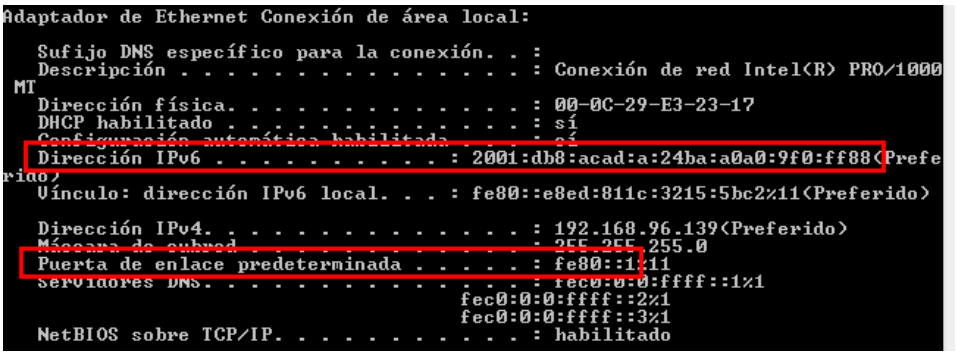


Imagen 295. Comando ipconfig /all.

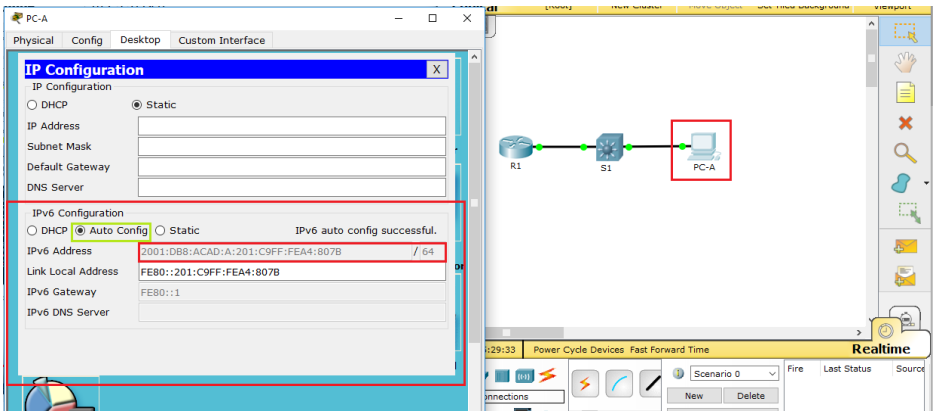


Imagen 296. Configuracion automatica para PC-A.

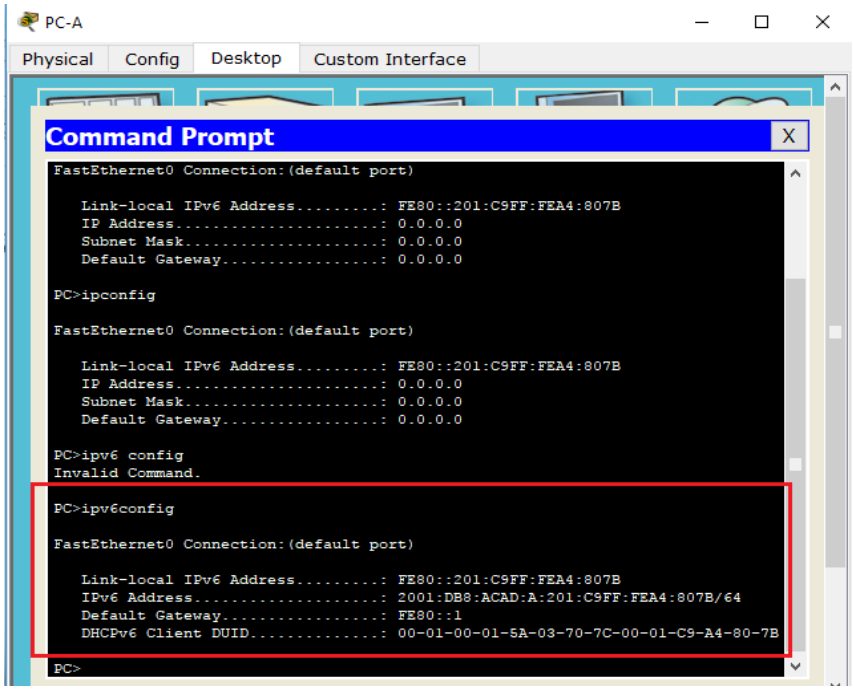


Imagen 297. Verificacion de la configuracion automatica para PC-A.

En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.

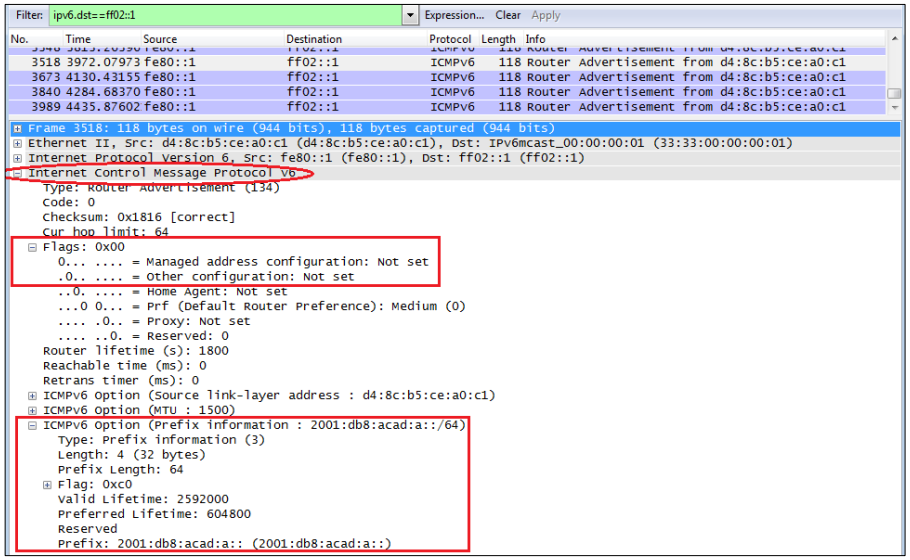


Imagen 298. Mensajes RA.

Parte 3. Configurar la red para DHCPv6 sin estado

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

Cree un pool de DHCP IPv6.

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

Asigne un nombre de dominio al pool.

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

Asigne una dirección de servidor DNS.

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

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

Asigne el pool de DHCPv6 a la interfaz.

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

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

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

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

R1(config-if)# end
```

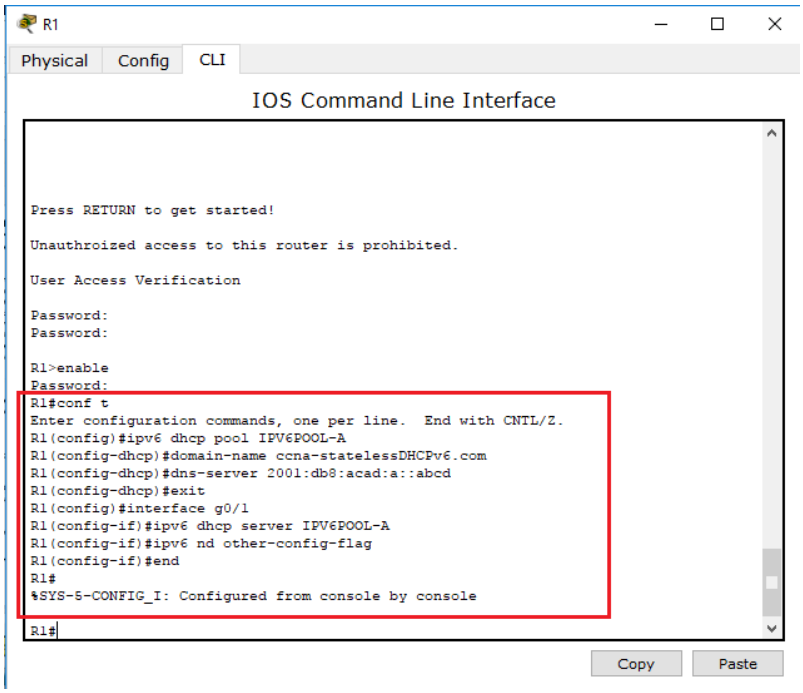


Imagen 299. Configuración de un servidor de DHCP IPv6 en el R1.

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

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

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

```
  FF02::1

  FF02::2

  FF02::1:2

  FF02::1:FF00:1

  FF05::1:3

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.

Hosts use DHCP to obtain other configuration.
```

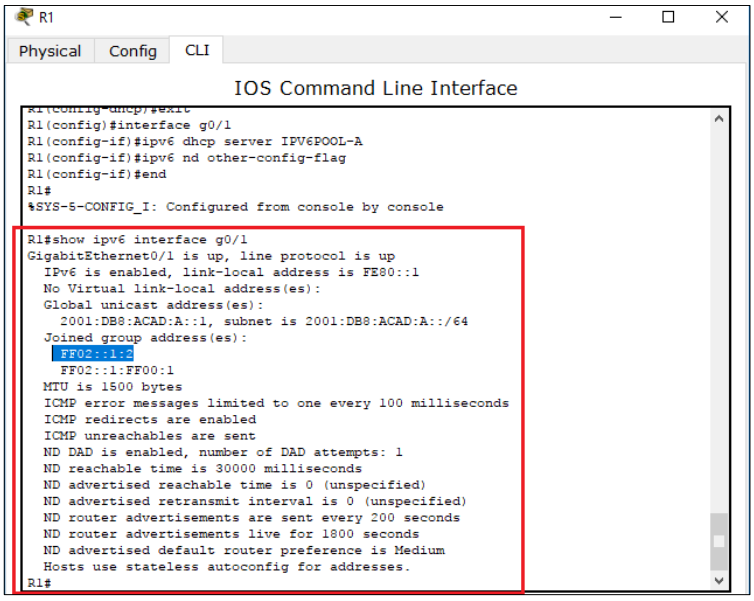


Imagen 300. Verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

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

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

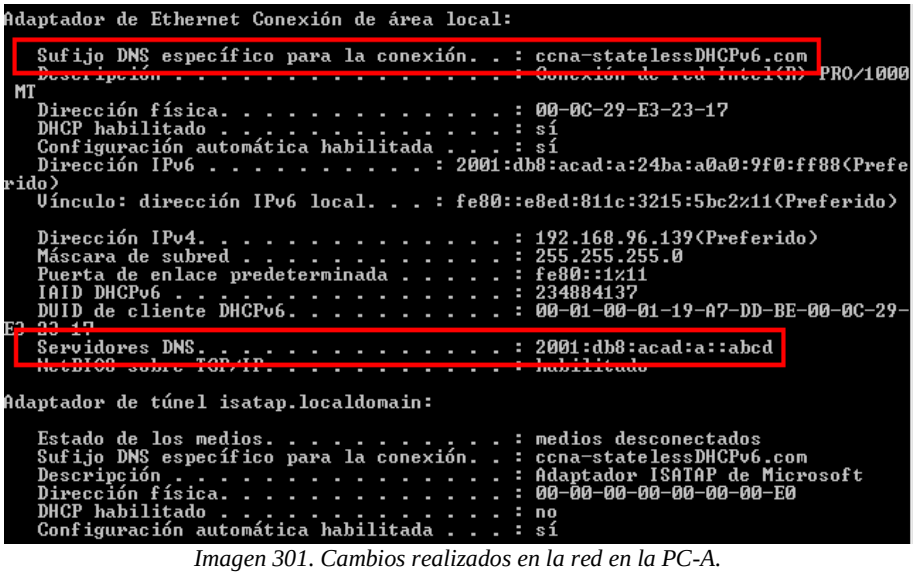


Imagen 301. Cambios realizados en la red en la PC-A.

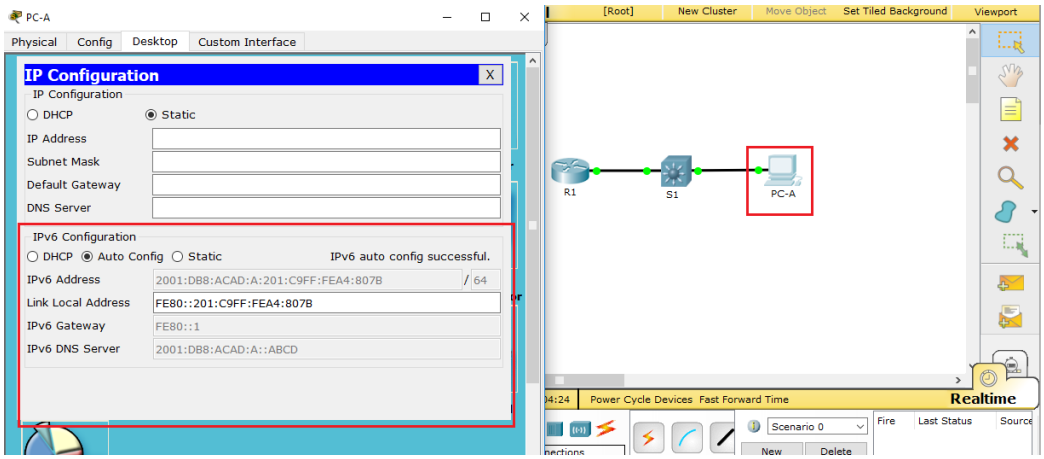


Imagen 302. Cambios realizados en la red en la PC-A.

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

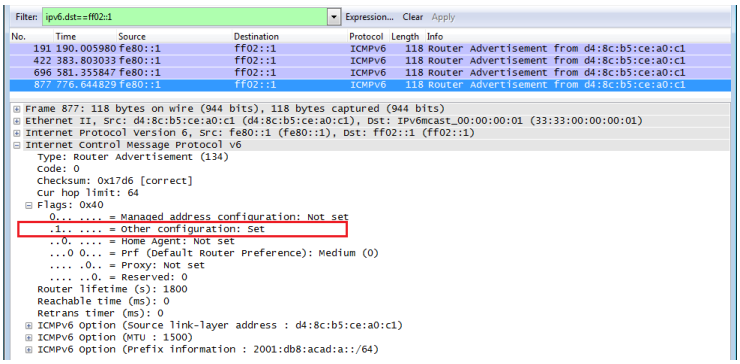


Imagen 303. Mensajes RA.

Paso 4. Verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.

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

R1# **show ipv6 dhcp binding**

R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

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

Domain name: ccna-statelessDHCPv6.com

Active clients: 0

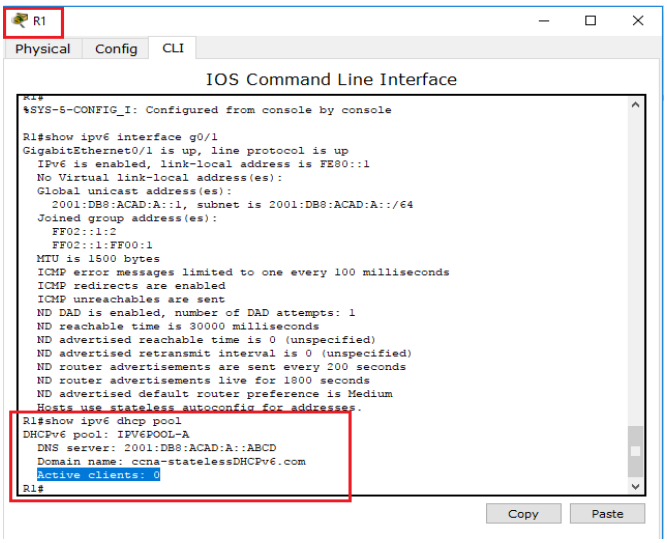


Imagen 304. Verificación de que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6

Paso 5. Restablecer la configuración de red IPv6 de la PC-A.

Desactive la interfaz F0/6 del S1.

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

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

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

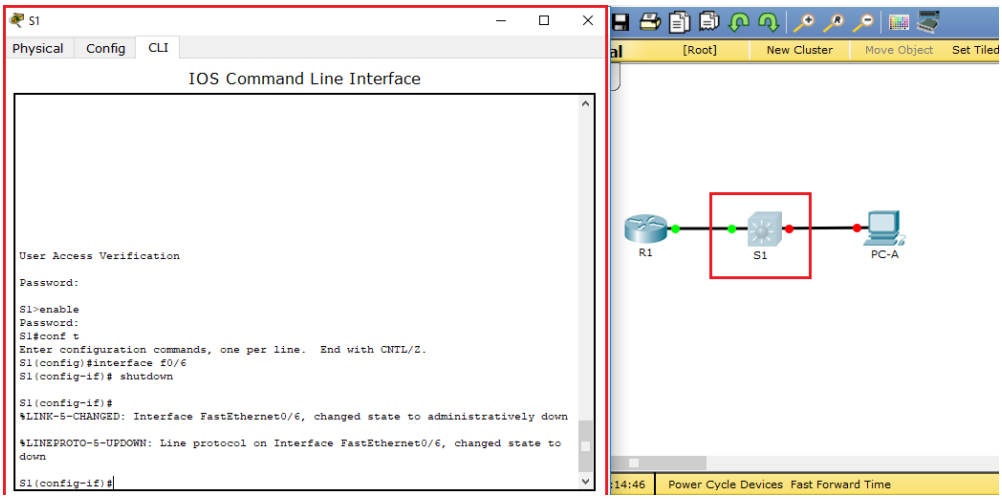


Imagen 305. Desactivacion de la interfaz F0/6 del S1.

Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.

Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.

Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.

Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

Parte 4. Configurar la red para DHCPv6 con estado

Paso 1. Preparar la PC-A.

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

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

Imagen 21. Prepararando la PC-A

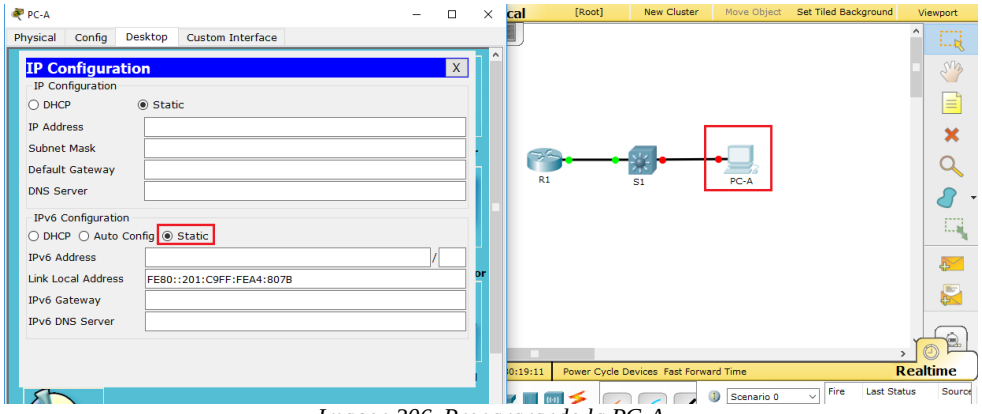


Imagen 306. Prepararando la PC-A

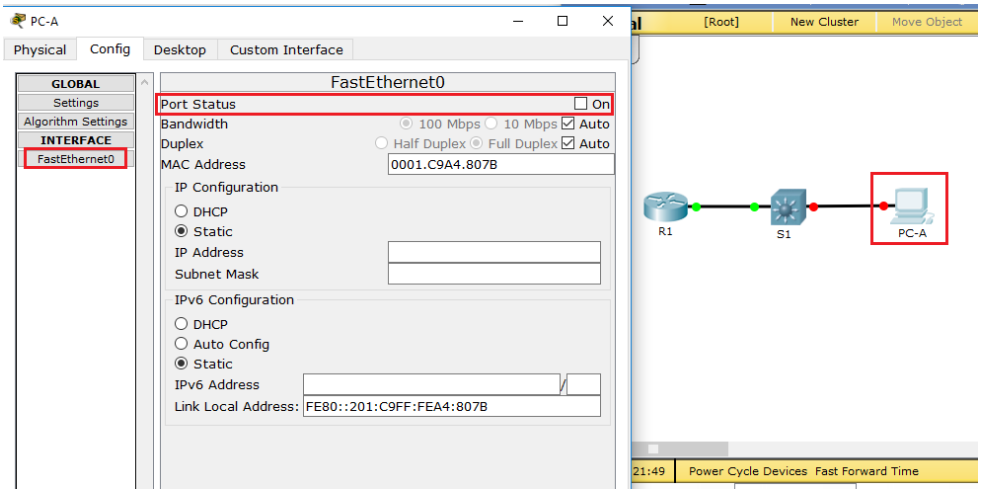


Imagen 307. Prepararando la PC-A

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

a. Agregue el prefijo de red al pool.

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

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

Nota. Packet tracert no soporta este comando.

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

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

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

R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com

R1(config-dhcpv6)# end
```

c. Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool

DHCPv6 pool: IPV6POOL-A

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

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

Domain name: ccna-StatefulDHCPv6.com

Active clients: 0
```

d. Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

```
R1# debug ipv6 dhcp detail

   IPv6 DHCP debugging is on (detailed)
```

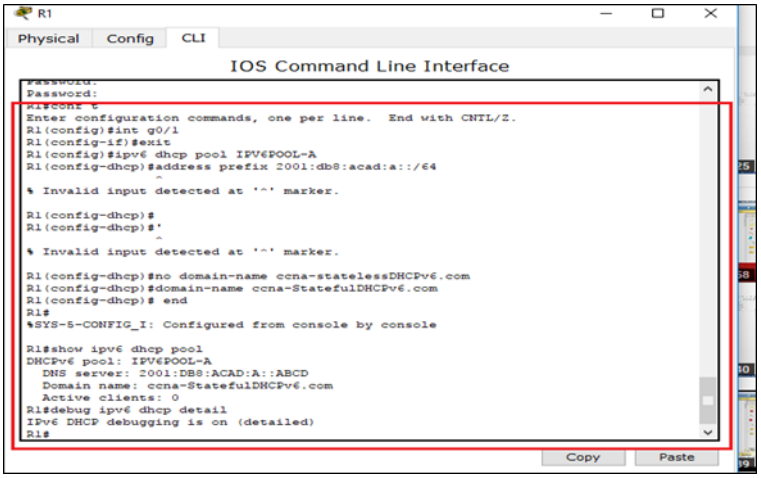


Imagen 308. Cambio del pool de DHCPv6 en el R1.

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

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

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

R1(config-if)# shutdown

R1(config-if)# ipv6 nd managed-config-flag

R1(config-if)# no shutdown

R1(config-if)# end
```

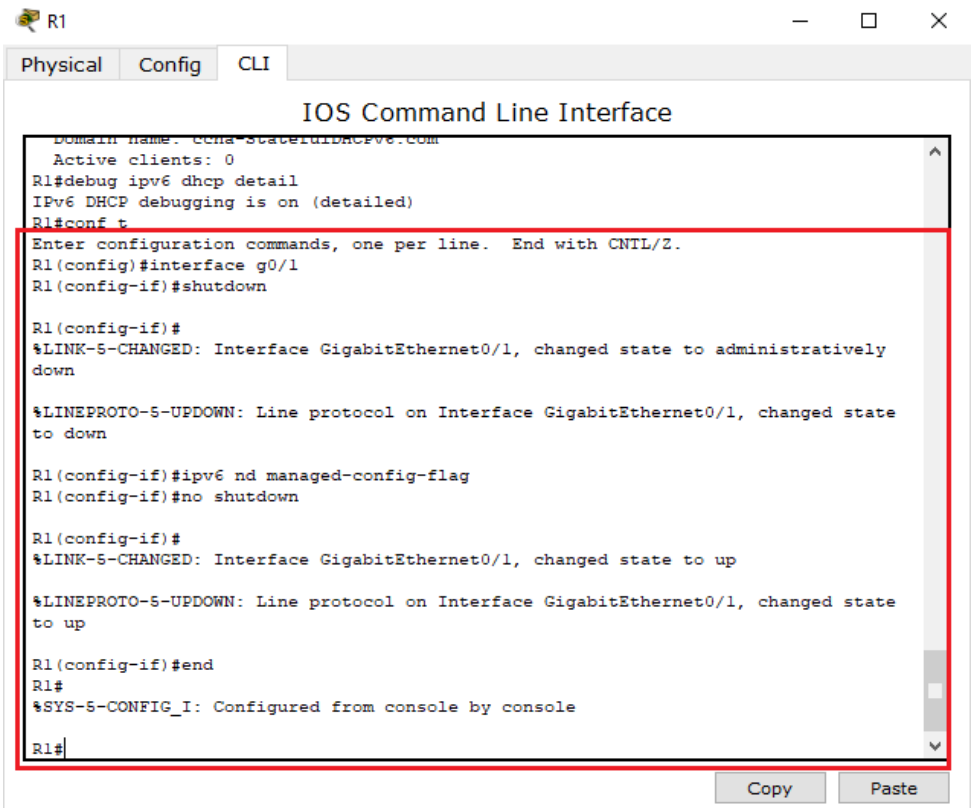


Imagen 309. Eestablecimiento del indicador en G0/1 para DHCPv6 con estado.

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

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

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

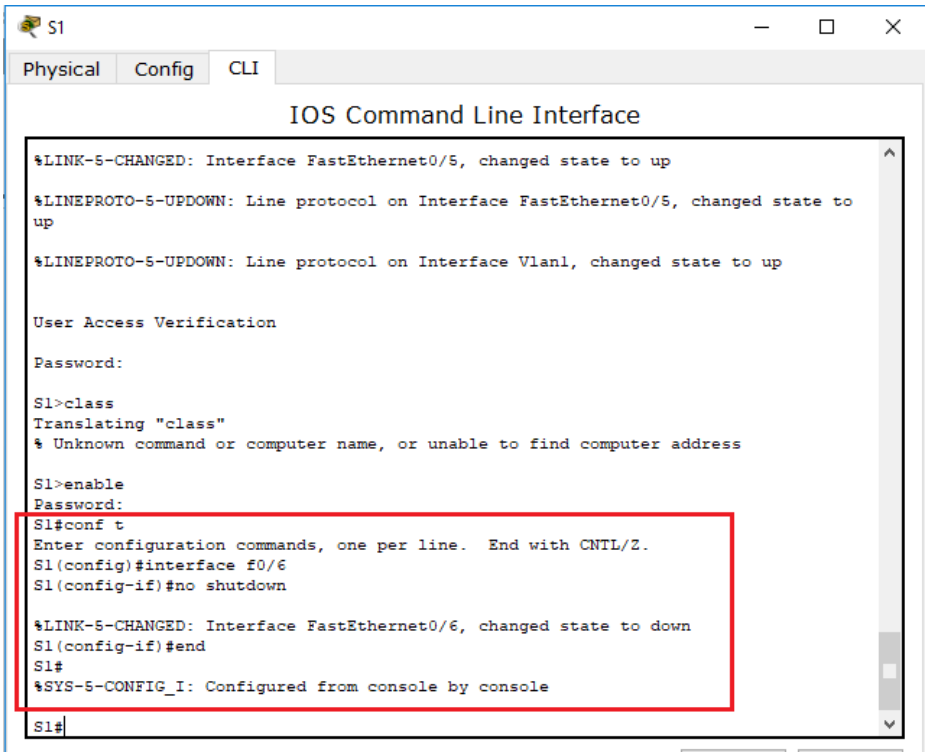


Imagen 310. Habilitacion de la interfaz F0/6 en el S1

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

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

```
R1# show ipv6 interface g0/1

GigabitEthernet0/1 is up, line protocol is up

  IPv6 is enabled, link-local address is FE80::1

  No Virtual link-local address(es):

  Global unicast address(es):

    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

  Joined group address(es):

    FF02::1

    FF02::2

    FF02::1:2

    FF02::1:FF00:1
```

```
  FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
```

Hosts use DHCP to obtain other configuration.

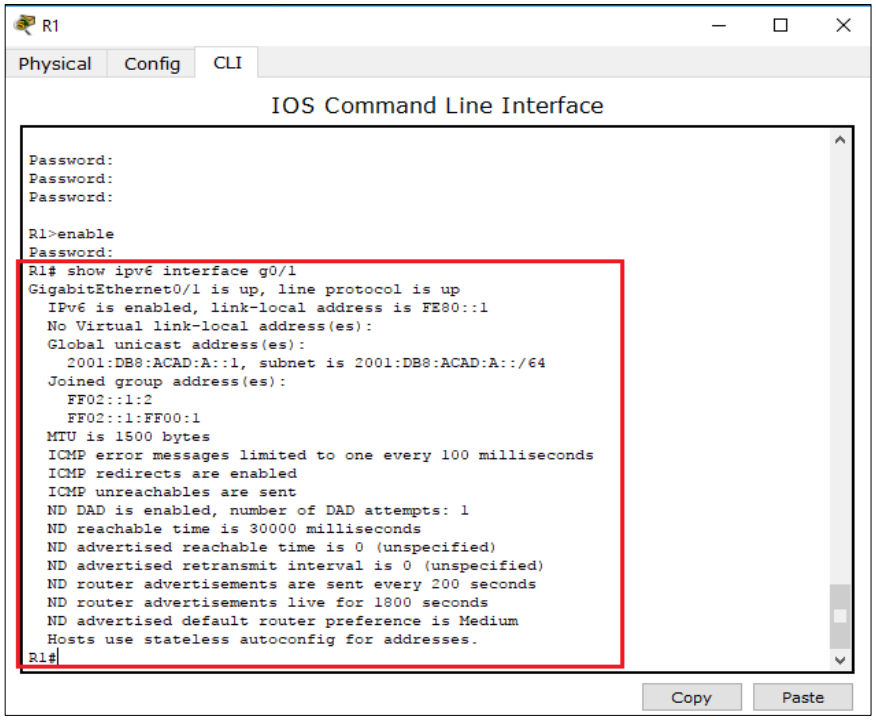


Imagen 311. Verificando la configuración de DHCPv6 con estado en el R1

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

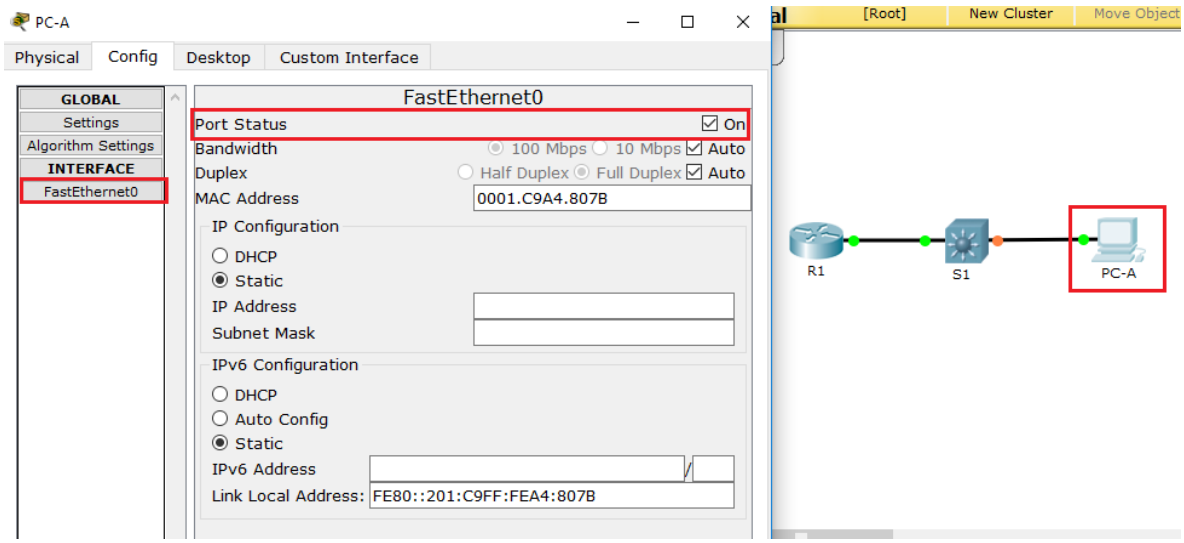


Imagen 312. Configuracion PC-A

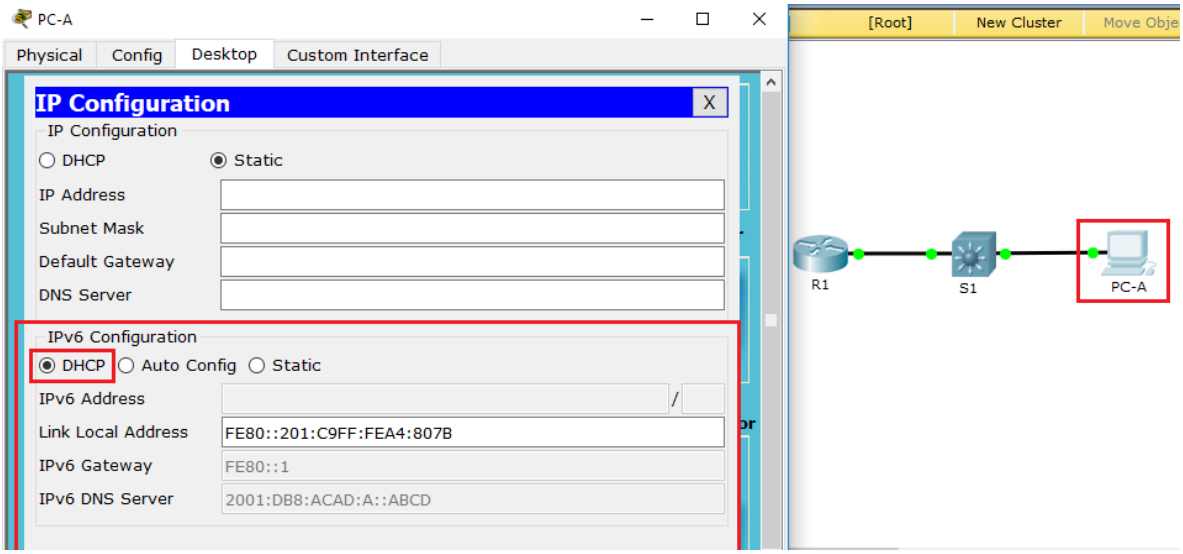


Imagen 313. Configuracion PC-A

Nota: *no hay IP Address debido a que packect tracert no soporta el comando* `R1(config-dhcpv6)#` **`address prefix 2001:db8:acad:a::/64`**

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

```
R1# show ipv6 dhcp pool

DHCPv6 pool: IPV6POOL-A
```

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

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

  Domain name: ccna-StatefulDHCPv6.com

  Active clients: 1
```

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

```
R1# show ipv6 dhcp binding
Client: FE80::D428:7DE2:997C:B05A
  DUID: 0001000117F6723D000C298D5444
  Username : unassigned
  IA NA: IA ID 0x0E000C29, T1 43200, T2 69120
    Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE
            preferred lifetime 86400, valid lifetime 172800
            expires at Mar 07 2013 04:09 PM (171595 seconds)
```

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : ccna-StatefulDHCPv6.com
   Descripción . . . . . . . . . . . . . . . : Conexión de red Intel(R) PRO/1000
 MT
   Dirección física. . . . . . . . . . . . . : 00-0C-29-E3-23-17
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce(Pref
erido)
   Concesión obtenida. . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:07:59
   La concesión expira . . . . . . . . . . . : jueves, 05 de septiembre de 2013
16:38:03
   Dirección IPv6 . . . . . . . . . . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Prefe
rido)
   Vínculo: dirección IPv6 local. . . . : fe80::d428:7de2:997c:b05a%11(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 192.168.96.139(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::1%11
   IAID DHCPv6 . . . . . . . . . . . . . . . : 234884137
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-
E3-23-17
   Servidores DNS. . . . . . . . . . . . . . : 2001:db8:acad:a::abcd
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

Imagen 314. Verificando la configuración de DHCPv6 con estado en el R1

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

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

```
R1# u all

Se ha desactivado toda depuración posible
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Mar  5 16:42:39.779:   type REPLY(7), xid 1039238

*Mar  5 16:42:39.779:   option SERVERID(2), len 10

*Mar  5 16:42:39.779:     00030001FC994775C3E0
```

```
*Mar  5 16:42:39.779:   option CLIENTID(1), len 14
*Mar  5 16:42:39.779:     00010001
R1#17F6723D000C298D5444
*Mar  5 16:42:39.779:   option IA-NA(3), len 40
*Mar  5 16:42:39.779:     IAID 0x0E000C29, T1 43200, T2 69120
*Mar  5 16:42:39.779:     option IAADDR(5), len 24
*Mar  5 16:42:39.779:       IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar  5 16:42:39.779:       preferred 86400, valid 172800
*Mar  5 16:42:39.779:   option DNS-SERVERS(23), len 16
*Mar  5 16:42:39.779:     2001:DB8:ACAD:A::ABCD
*Mar  5 16:42:39.779:   option DOMAIN-LIST(24), len 26
*Mar  5 16:42:39.779:     ccna-StatefulDHCPv6.com
```

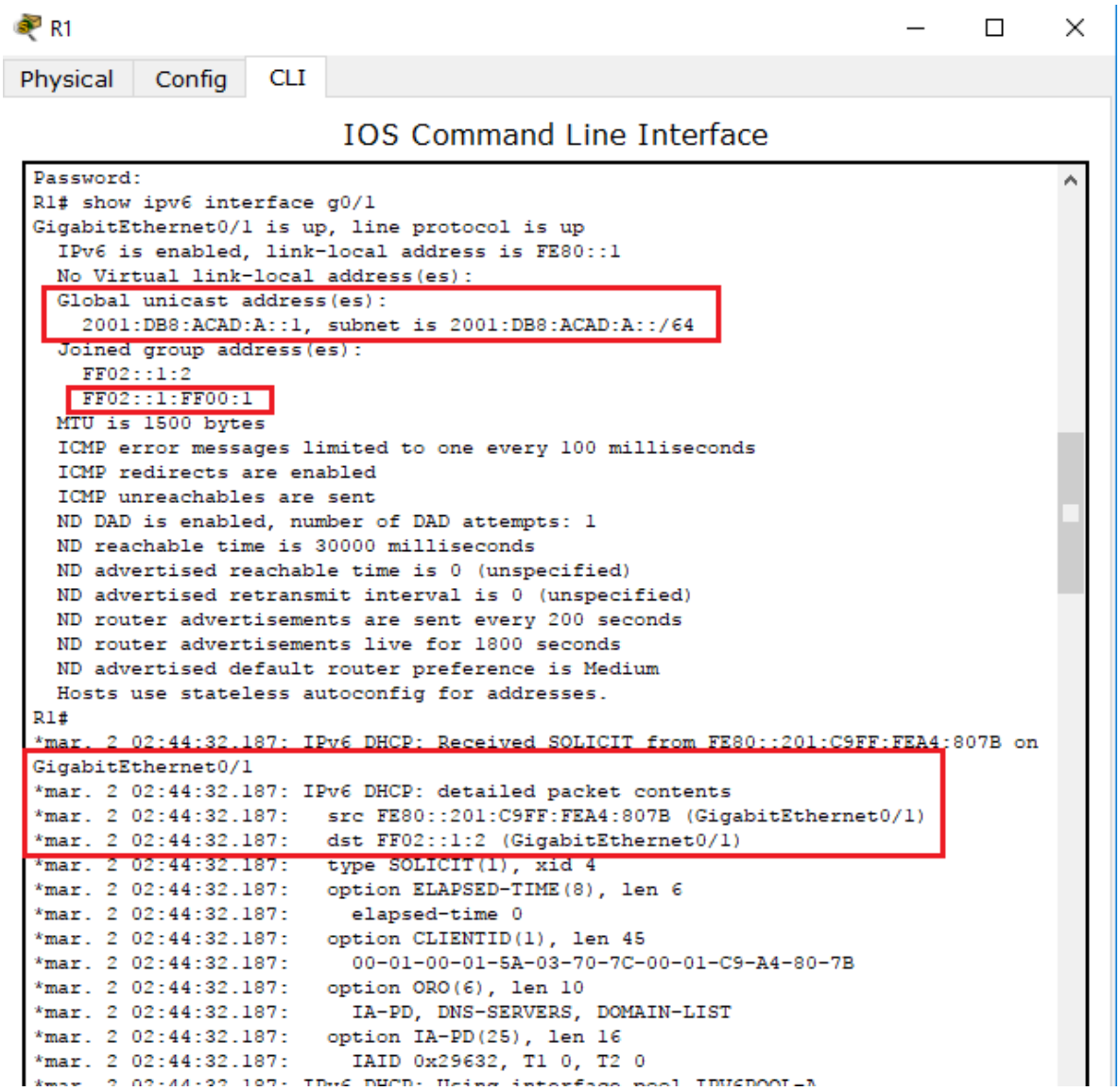


Imagen 315. Análisis de la información de red

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

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

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

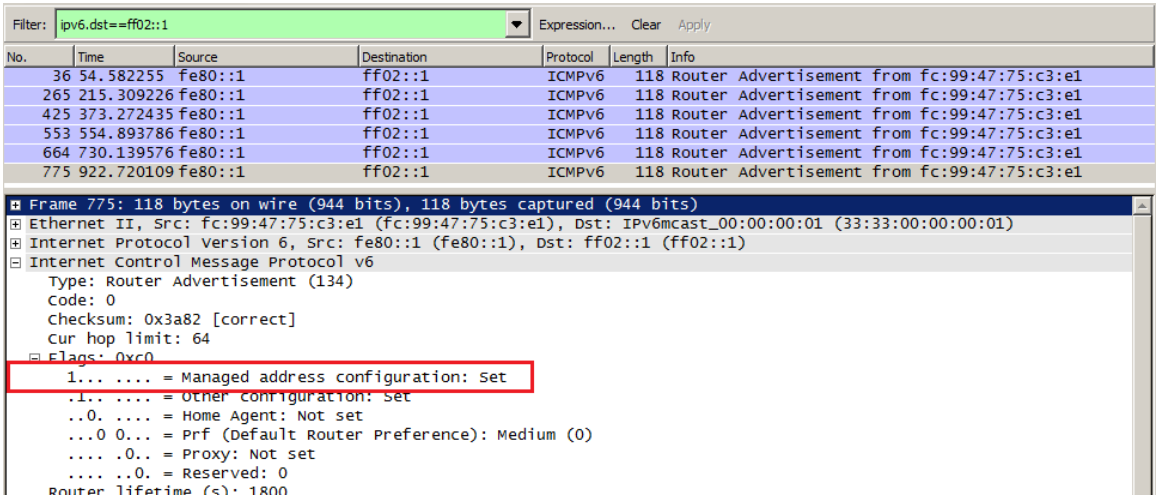


Imagen 316. Verificación DHCPv6 con estado en la PC-A

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

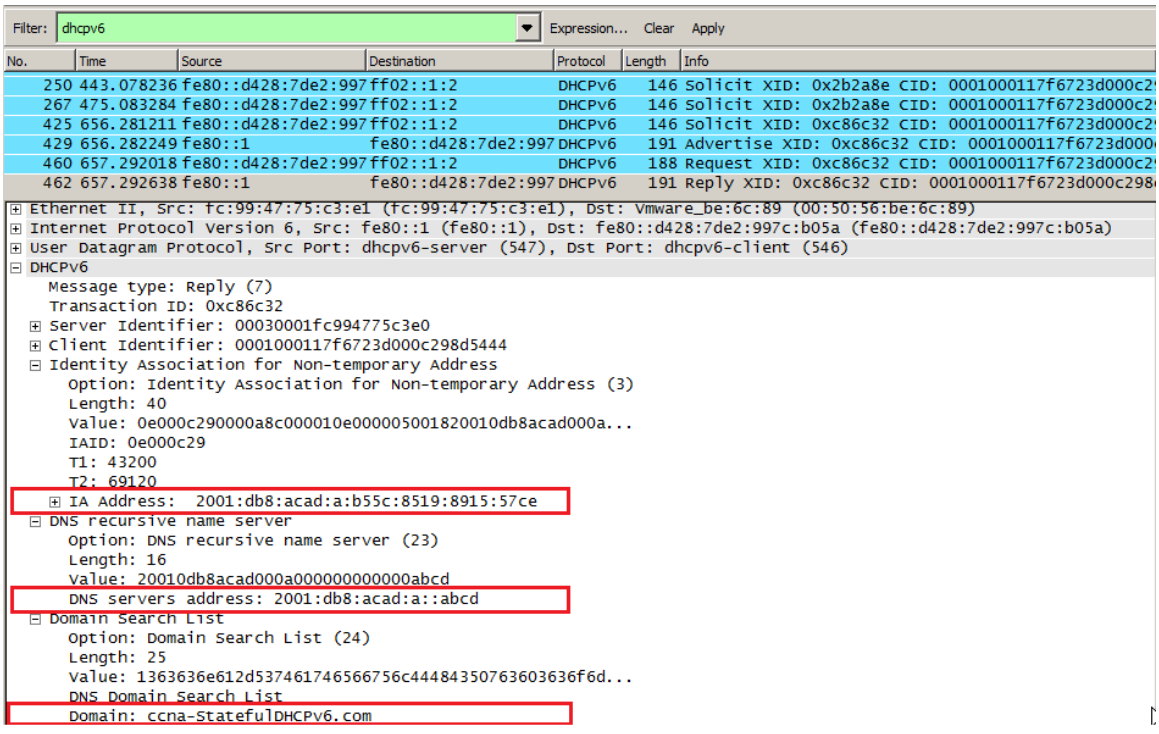


Imagen 317. Cambio del filtro en Wireshark

Reflexión

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

   Respuesta: ***DHCPv6 con estado***: usa más recursos de memoria, además requiere que el router guarde dinámicamente el estado de información acerca de los clientes de DHCPv6. ***DHCPv6 sin estado:*** los clientes no usan el servidor DHCP para obtener las direcciones así que no necesitan ser guardadas.

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

   Respuesta: Cisco recomienda la ***DHCPv6 sin estado*** cuando implementa y desarrolla redes en ipv6 sin un registro de red CISCO (CNR).

Conclusiones

- Configuramos la red para que utilice SLAAC. Una vez que se verifico la conectividad, configuramos los parámetros de DHCPv6 y modificamos la red para que utilice DHCPv6 sin estado. Una vez que verificamos que DHCPv6 sin estado funcionaba correctamente, modificamos la configuración del R1 para que utilizara DHCPv6 con estado. Finalmente usamos Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.
- De esta forma en el desarrollo de la presente práctica implementamos las instrucciones dadas que nos permitieron:
  - Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
  - Parte 2: configurar la red para SLAAC
  - Parte 3: configurar la red para DHCPv6 sin estado
  - Parte 4: configurar la red para DHCPv6 con estado

  - Esto con el fin de adquirir las competencias necesarias en la implementación de los comandos y configuración vistas en la Unidad.

10.3.1.1 IoE and DHCP Instructions

Topología

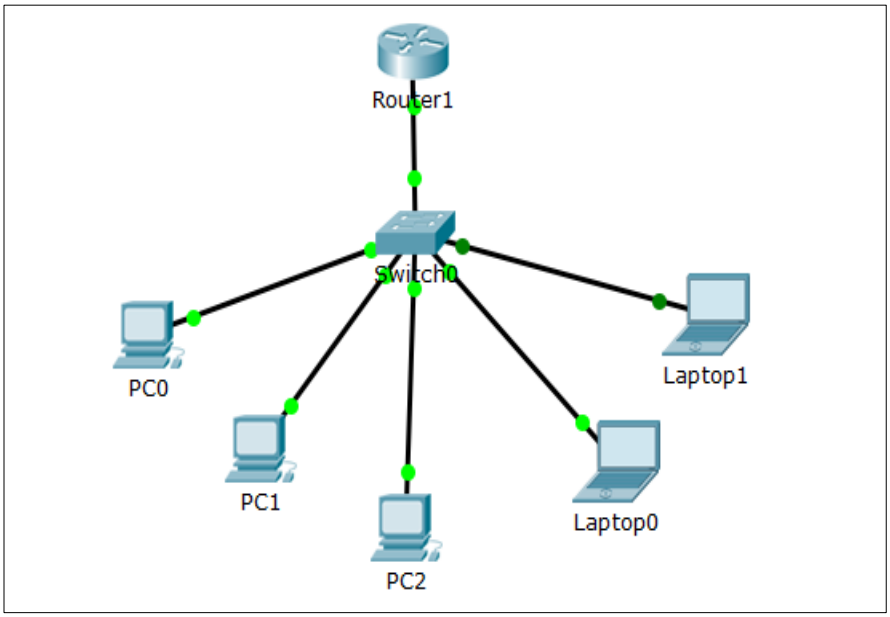


Imagen 318. Topología.

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.

Actividad

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

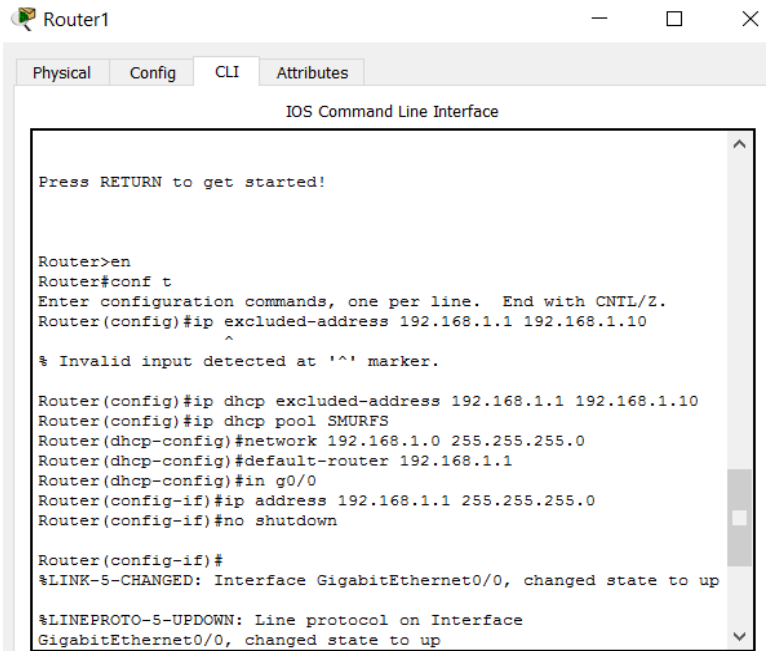


Imagen 319, configuración Router1 admitir servidor DHCP.

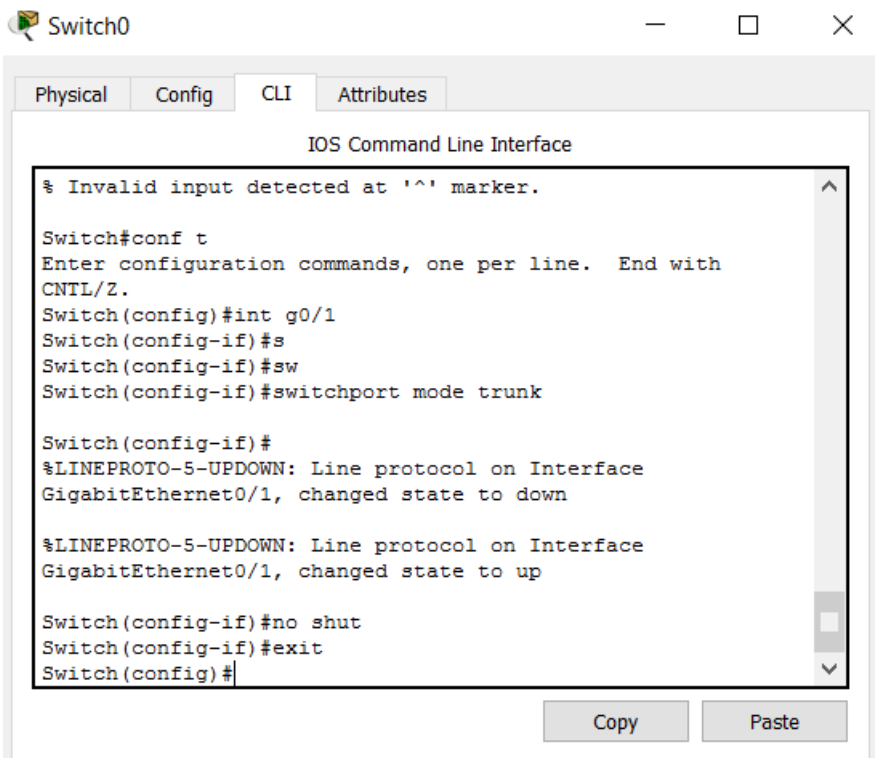


Imagen 320, configuración switch admitir servidor DHCP.

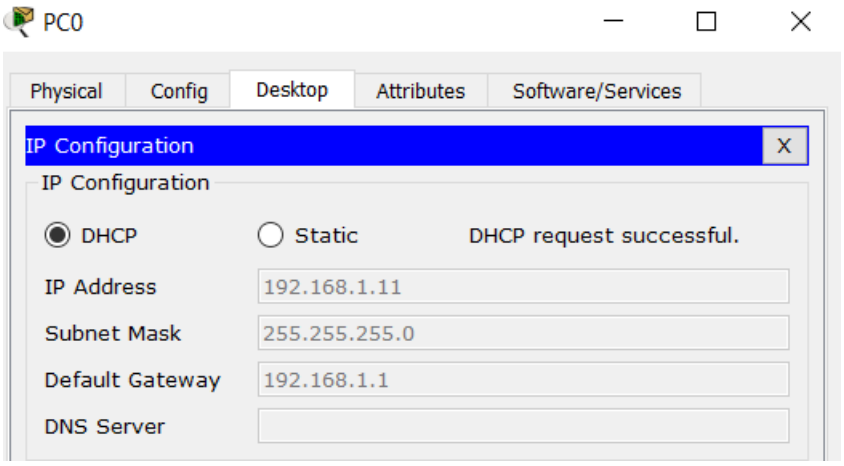


Imagen 321, configuración dispositivo PC0 admitir DHCP.

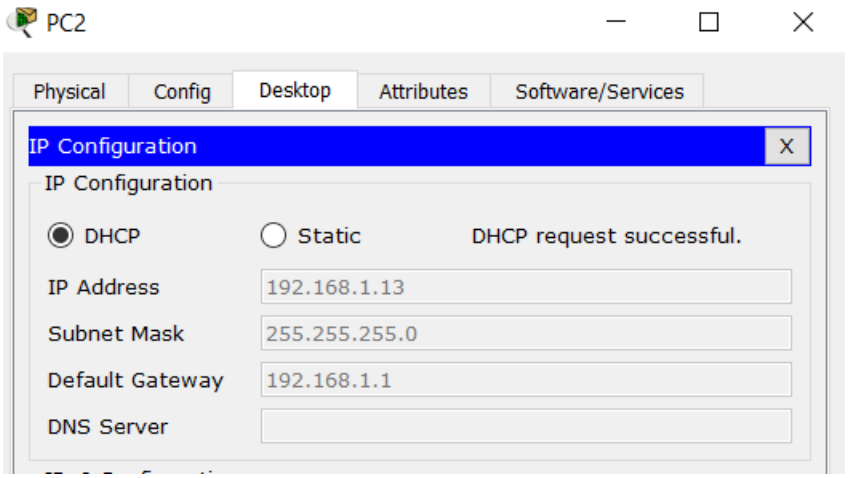


Imagen 322, configuración dispositivo PC2 admitir DHCP.

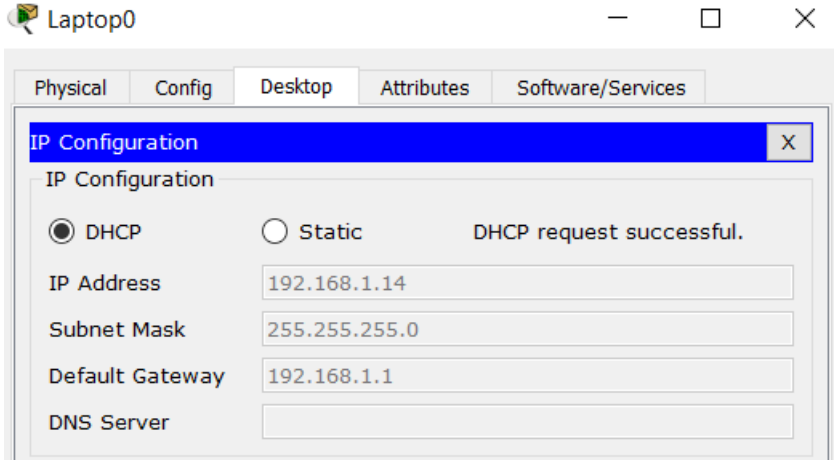


Imagen 323, configuración dispositivo Laptop admitir DHCP.

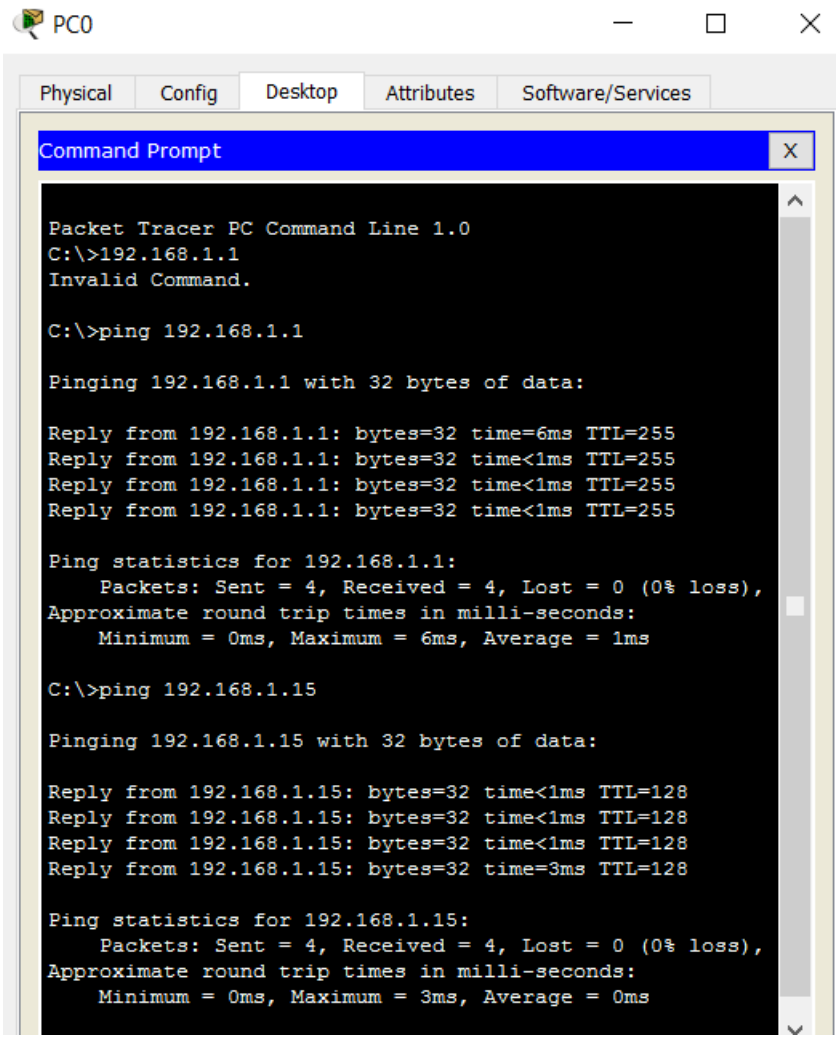


Imagen 324, verificación conexiones usando comando ping.

Reflexión

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

   El router 1941 es una alternativa de bajo costo para redes pequeñas.

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.

   - IPV6 has more addresses available so if a business expandas they won`t run out of IP addresses
   - IPV6 is mainly dynamic and it makes it easy to configure
   - IPV6 can create Security that you might not get with basic router

Conclusiones

- Cuando tenemos Routers separados DHCP para cada subred estamos agregando más complejidad y decrementamos la administración central de la red. Requiriendo que cada Router trabaje para sus propias direcciones DHCP, teniendo la función primaria el tráfico del ruteo y siendo más fácil de administrar.
- PAT resulta más sencillo de implementar que NAT debido a que solo es necesario especificar el puerto a la red externa para realizar la traducción de direcciones IP privadas a públicas y no un rango de direcciones.
- Se logró hacer un reconocimiento a los comandos básicos de direccionamiento IPv6.
- El tiempo de vida o TTL de los paquetes que se envían de una red LAN a otra es mucho menor que el TTL de los paquetes que recorren una misma red debido a que tiene que atravesar R1 y R2.
- TTL de paquetes entre los dispositivos de una misma red LAN es 127 ms mientras que el TTL de los paquetes entre los dispositivos de diferente LAN es 126 ms. Para la asignación de subredes IPv6 es importante conocer la conversión de números Hexadecimales.

11.2.2.6 Lab - Configuring Dynamic And Static Nat

- **Topología**

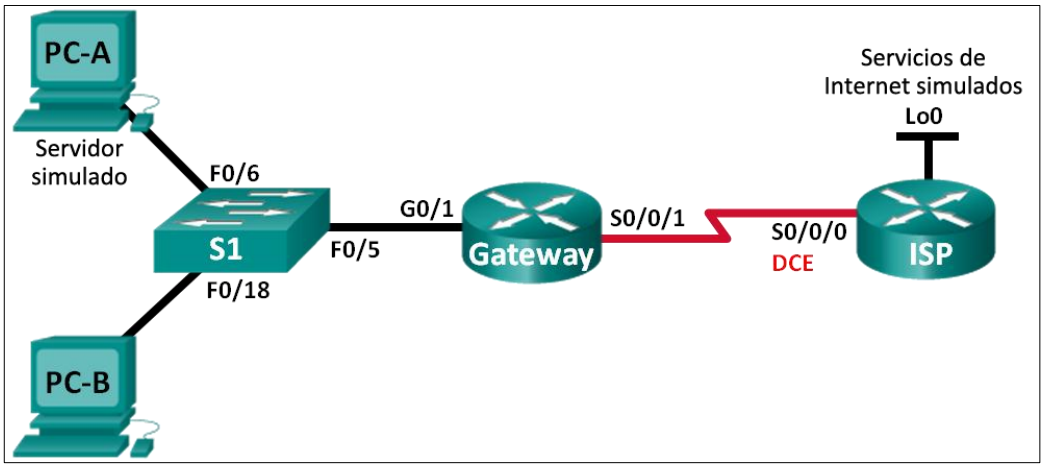


Imagen 325, Topología.

Tabla 13:

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 1. Armar la red y verificar la conectividad

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

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

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

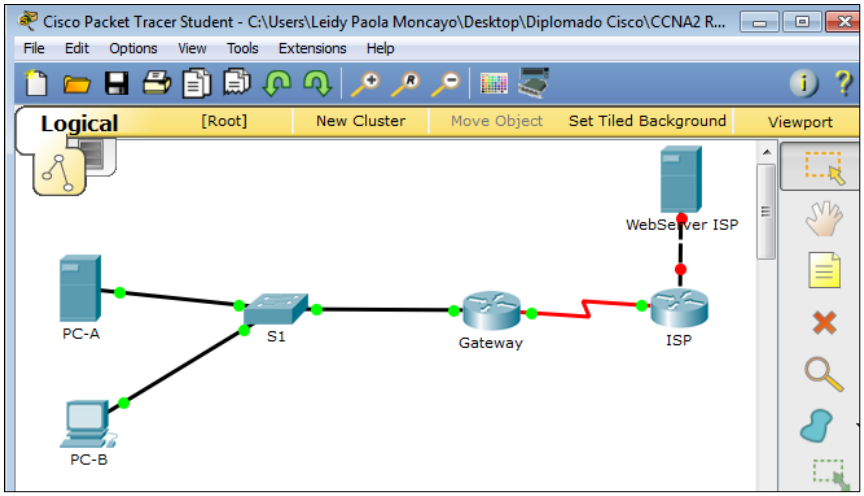


Imagen 326, Conexión de la topología

Paso 2. Configurar los equipos host.

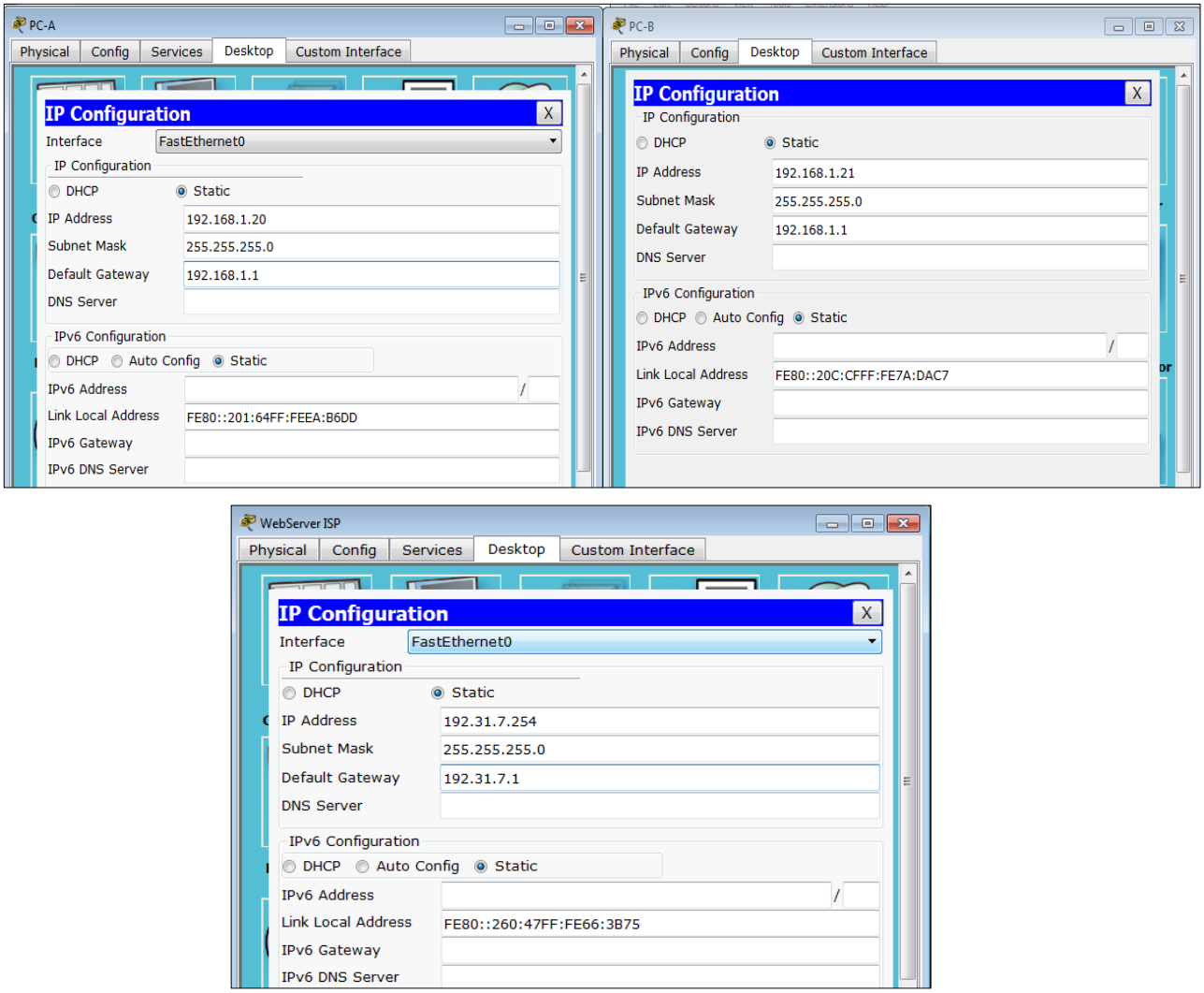


Imagen 327, Configuración de los Host A – B y el Web Server de ISP

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

Paso 4. Configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

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

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

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

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

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

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

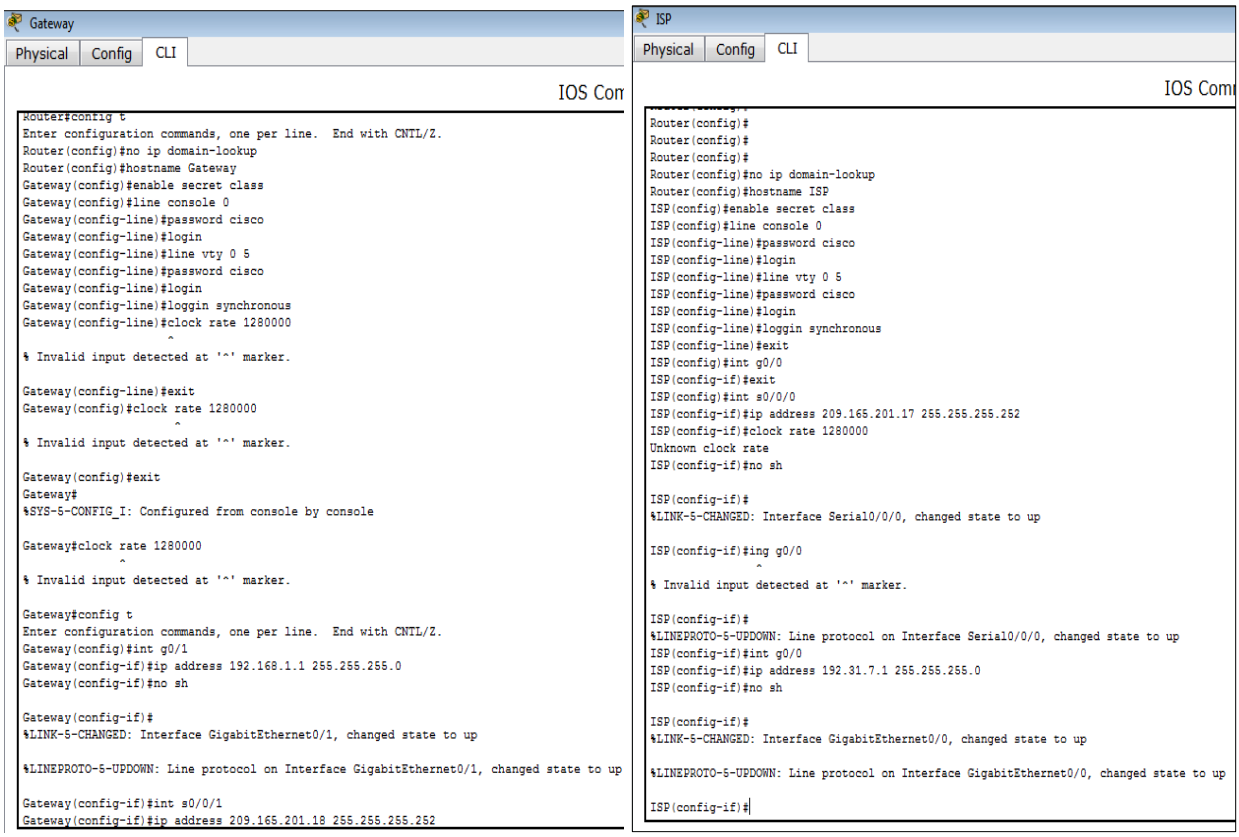


Imagen 328, Configuración básica d los routers Gateway y ISP

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

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

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

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

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

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

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

Nota: Packet tracer no soporta estos comandos para establecer el servidor web en ISP por lo tanto se instaló un servidor web en la parte de arriba del router ISP que se puede observar en la topología.

Paso 6. Configurar el routing estático.

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

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

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

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

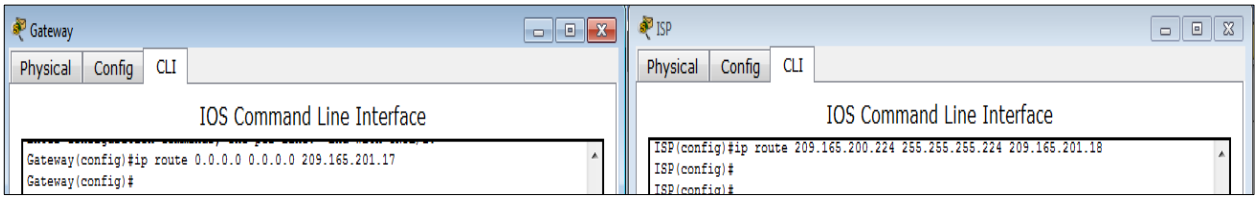


Imagen 329, Configuración de las rutas estáticas en los Routers.

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

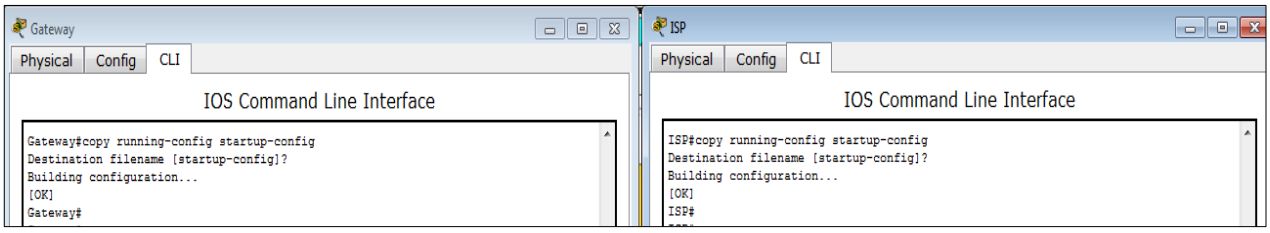


Imagen 330, configuración guardada de inicio

Paso 8. Verificar la conectividad de la red

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

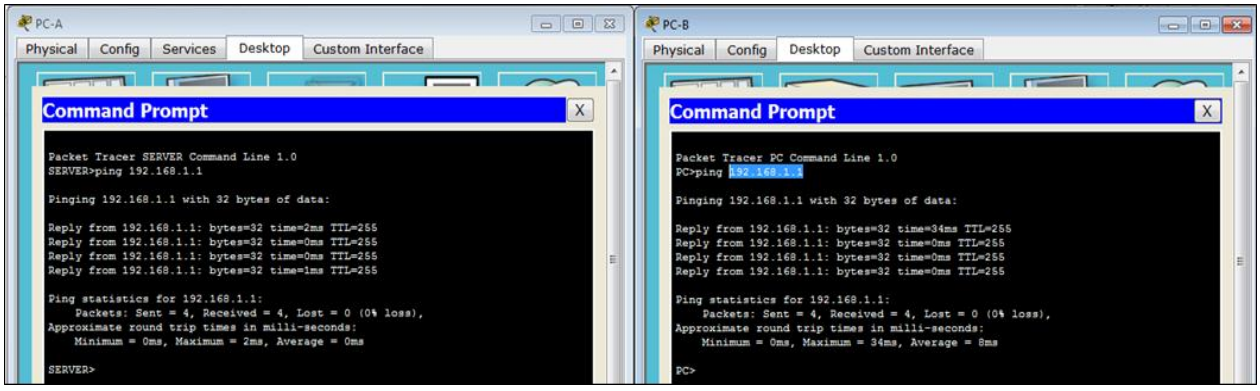


Imagen 331, ping a la int g0/1

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.

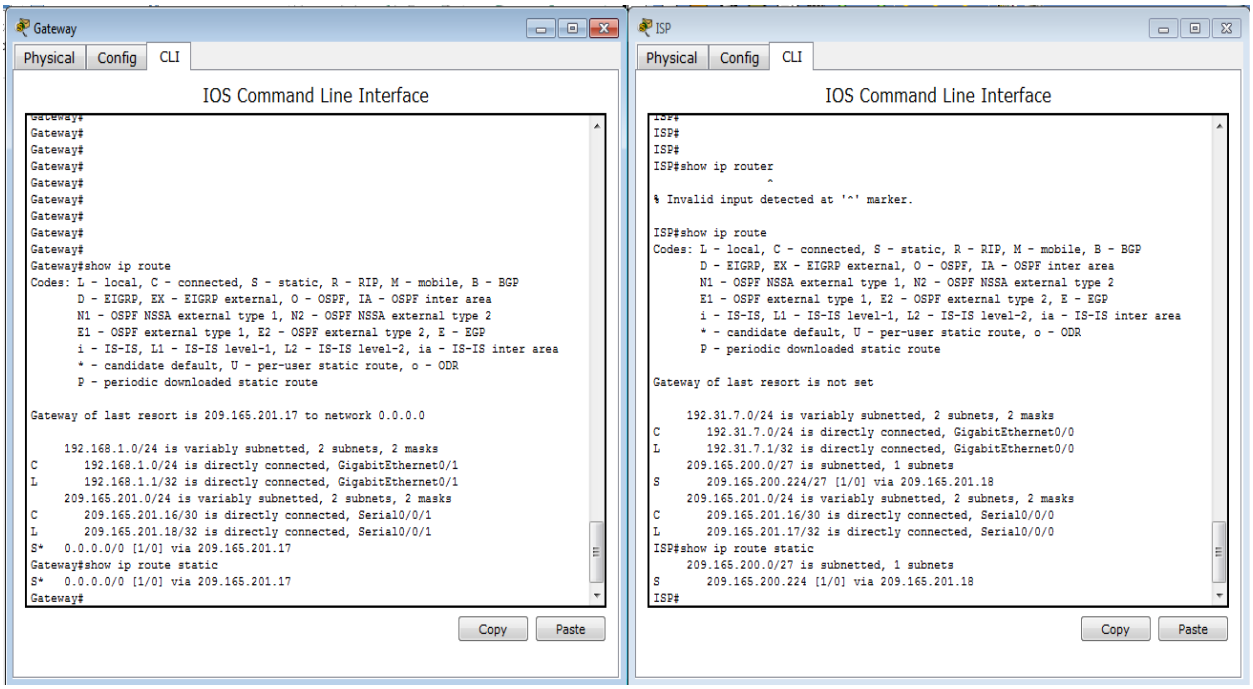


Imagen 332, rutas estáticas de los routers.

Parte 2. Configurar y verificar la NAT estática.

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

Paso 1. Configurar una asignación estática.

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

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

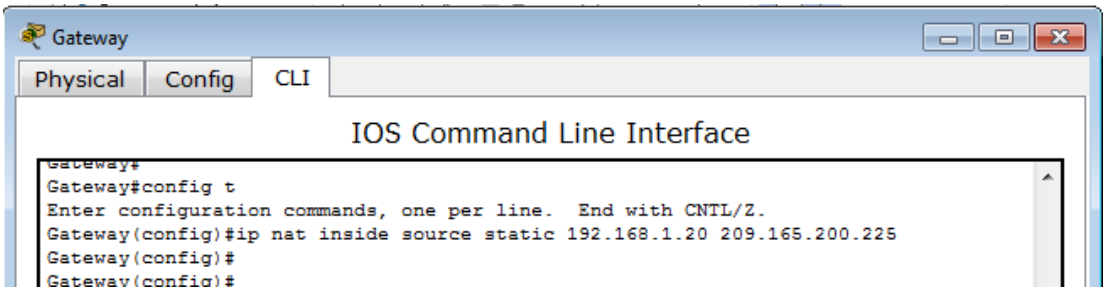


Imagen 333, configuración de la ip nat en Gateway

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**

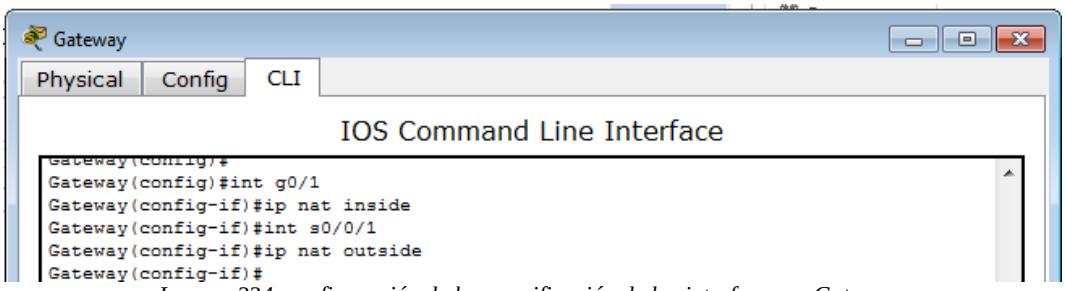


Imagen 334, configuración de la especificación de las interfaces en Gateway.

Paso 3. Probar la configuración.

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

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---

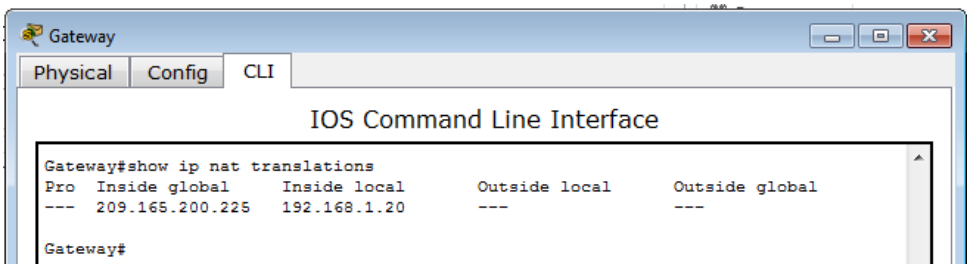


Imagen 335, comando show ip nat translations

¿Cuál es la traducción de la dirección host local interna?

Respuesta: 192.168.1.20 = 209.165.200.225

¿Quién asigna la dirección global interna?

Respuesta: Por el router desde Pool NAT

¿Quién asigna la dirección local interna?

Respuesta: por el administrador de las PC.

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.

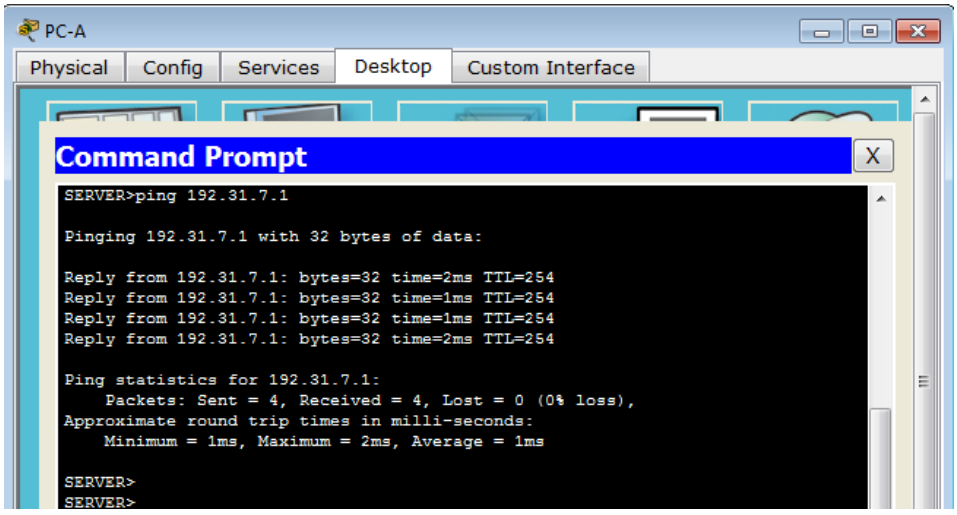


Imagen 336, ping al router ISP satisfactorio.

En el router Gateway, muestre la tabla de NAT.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1

--- 209.165.200.225 192.168.1.20 --- ---

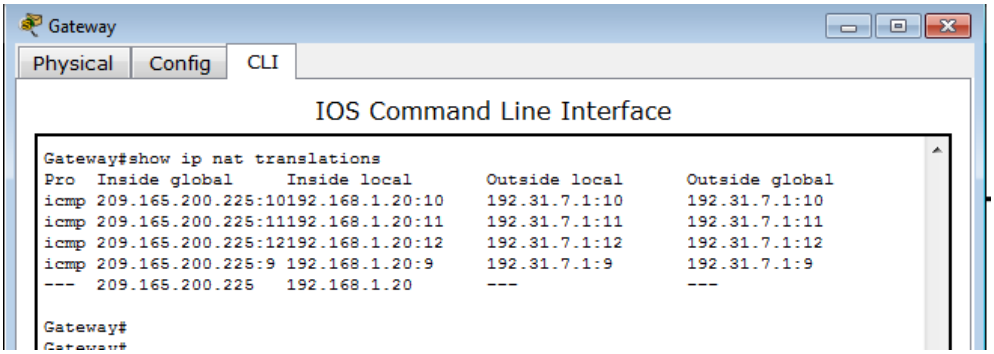


Imagen 337, tabla de NAT

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP?

Respuesta: 9, 10, 11, 12

Nota: puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

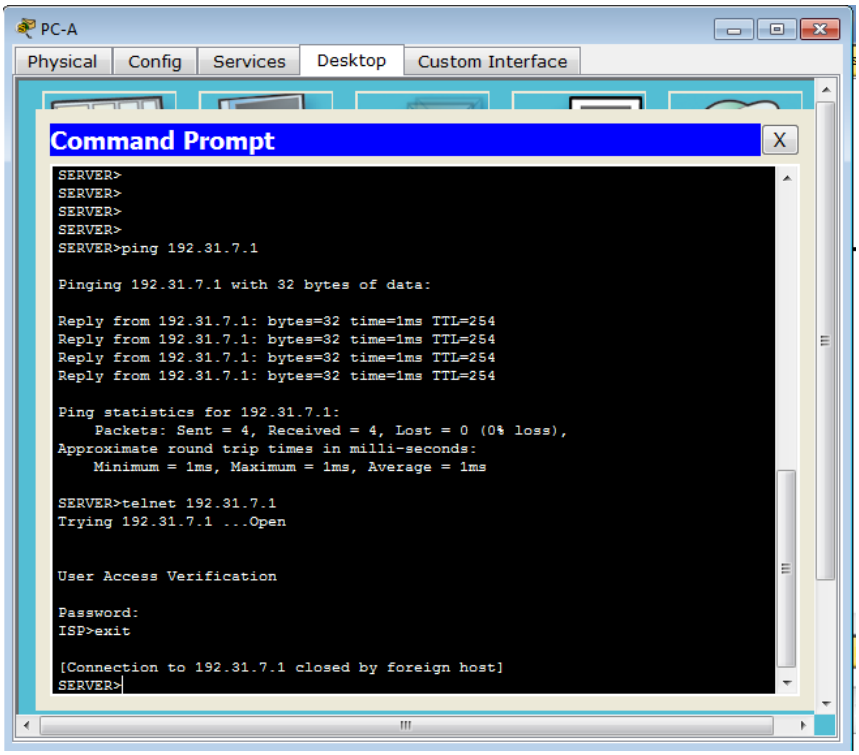


Imagen 338, ping tracert PC-A

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 --- ---

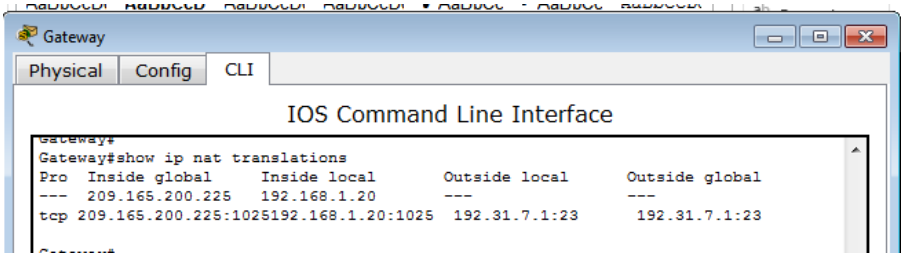


Imagen 339, tabla de NAT

Nota: es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

¿Qué protocolo se usó para esta traducción?

Respuesta: Protocolo TCP/IP

¿Cuáles son los números de puerto que se usaron?

Global/local interno:

Respuesta: 1025

Global/local externo:

Rta/23

d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.}

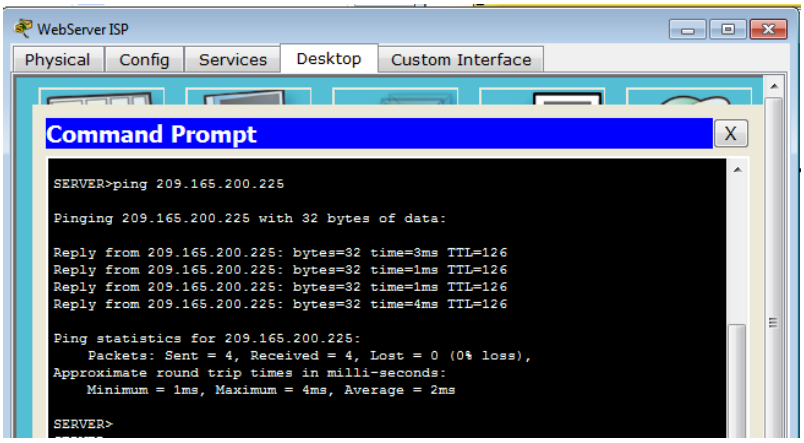


Imagen 340, ping a PC-A

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

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12

--- 209.165.200.225 192.168.1.20 --- ---

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

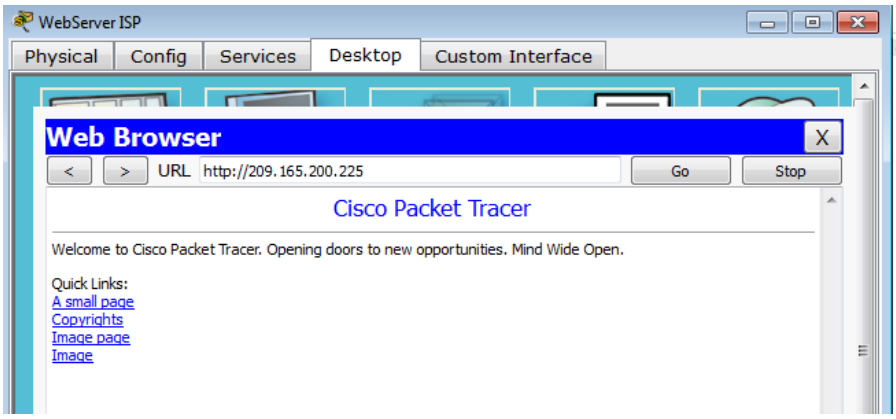


Imagen 341, direccion 209.165.200.225 en el Web server ISP

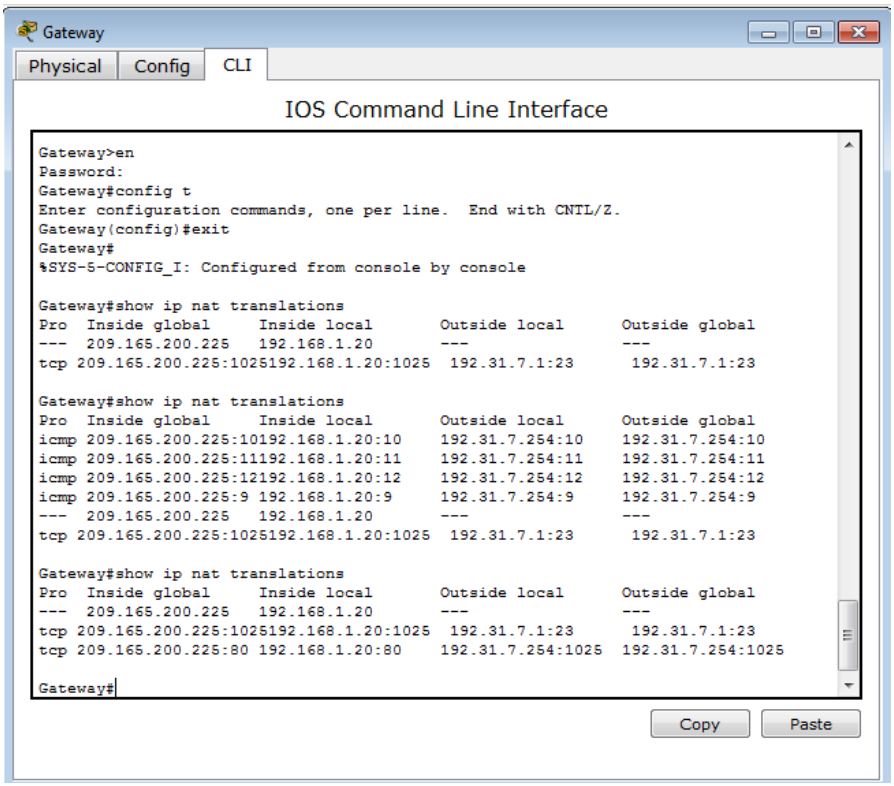


Imagen 342, comando show ip nat translations

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

Gateway# **show ip nat statics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 00:02:12 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

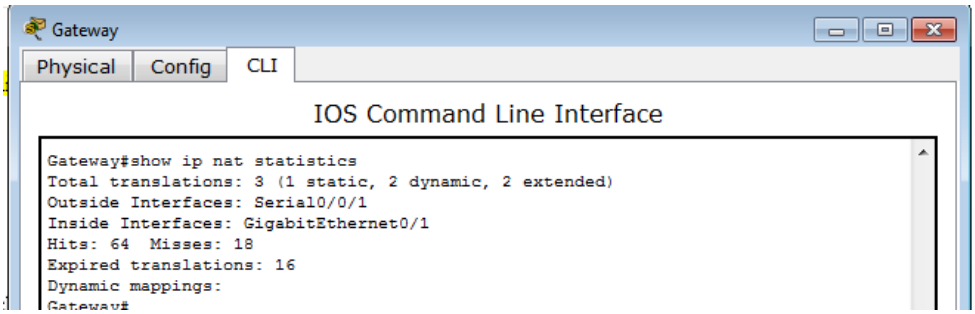


Imagen 343, comando show ip nat statistics

Parte 3. 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**

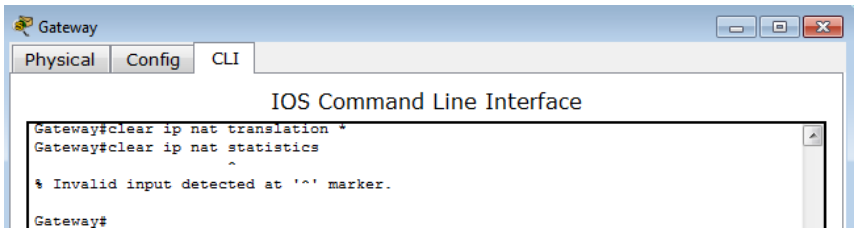


Imagen 344, comando clear ip nat statistics no es soportado por packet tracer

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**

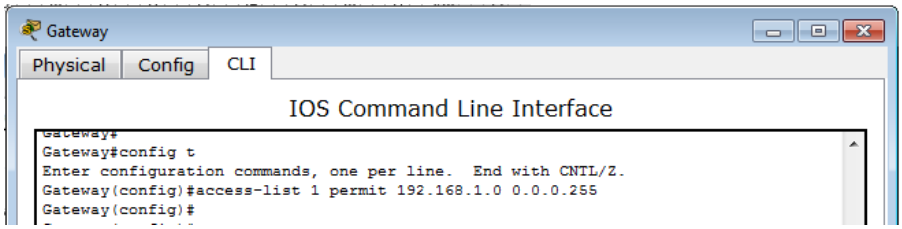


Imagen 345, define lista de control de acceso en la LAN

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.

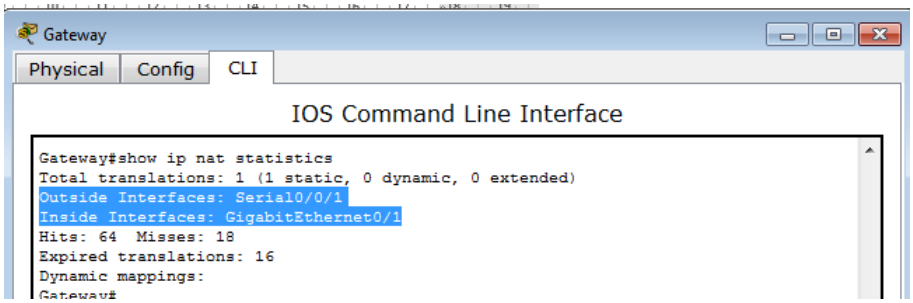


Imagen 346, verificación de la configuración NAT

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**

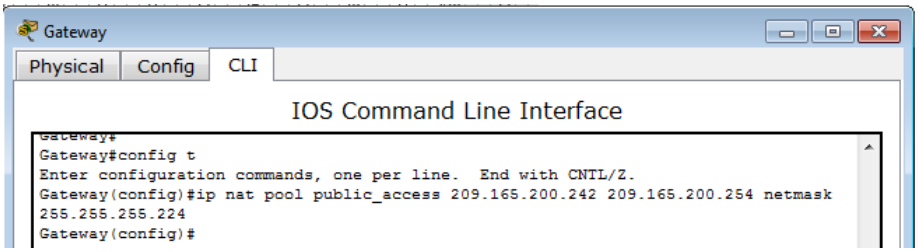


Imagen 347, definición del conjunto de direcciones públicas utilizables

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**

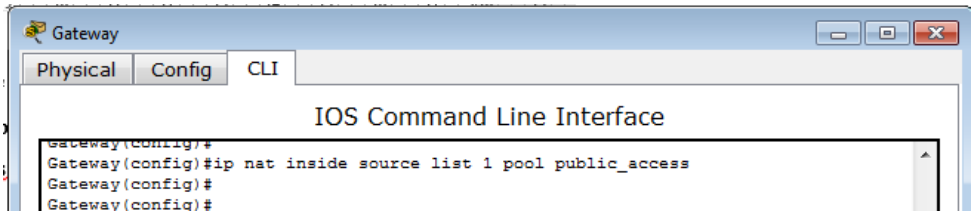


Imagen 348, definición de NAT desde la lista de origen hasta el conjunto externo

Paso 6. Probar la configuración.

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

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.225 192.168.1.20 --- ---

icmp 209.165.200.242:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1

--- 209.165.200.242 192.168.1.21 --- ---

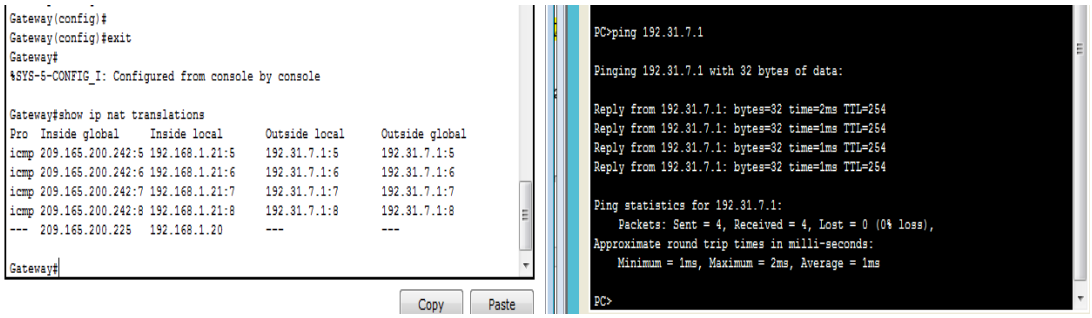


Imagen 349, se comprueba la configuración

¿Cuál es la traducción de la dirección host local interna de la PC-B?

Respuesta: 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?

Respuesta: 1, 2, 3, 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**.

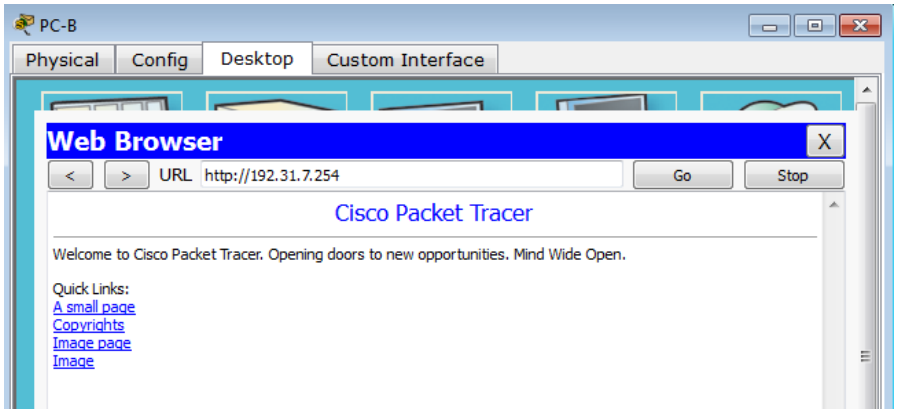


Imagen 350, ip satisfactoria

c. Muestre la tabla de NAT.

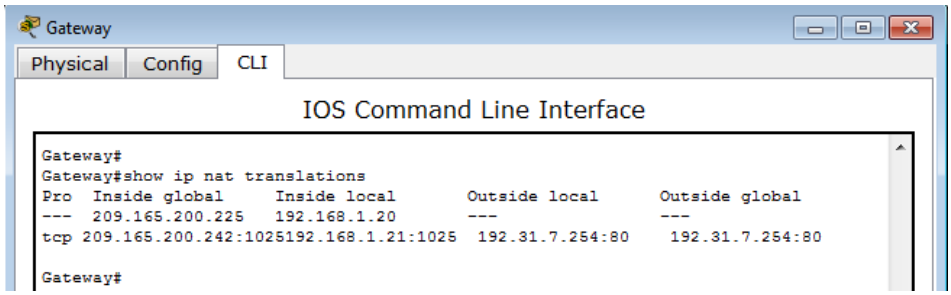


Imagen 351, tabla NAT

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.225 192.168.1.20 --- ---

tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80 192.31.7.1:80

tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80 192.31.7.1:80

--- 209.165.200.242 192.168.1.22 --- ---

¿Qué protocolo se usó en esta traducción?

Respuesta: TCP

¿Qué números de puerto se usaron?

Respuesta: Interno: 1025

Respuesta: Externo: 80

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

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

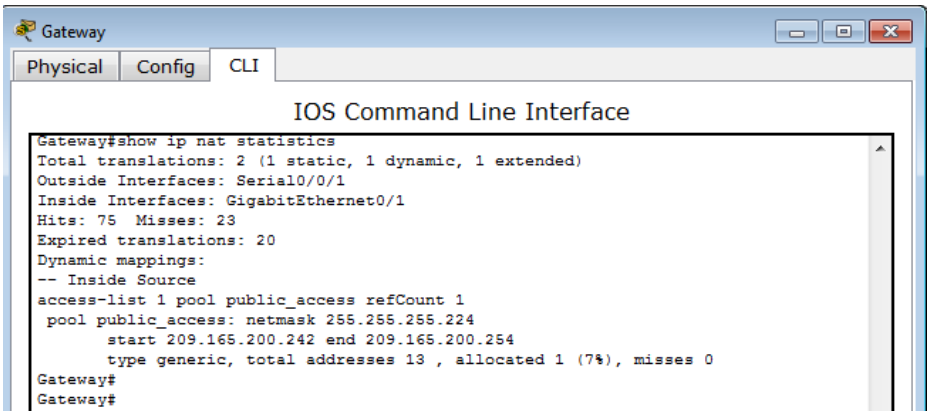


Imagen 352, comando show ip statistics.

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**

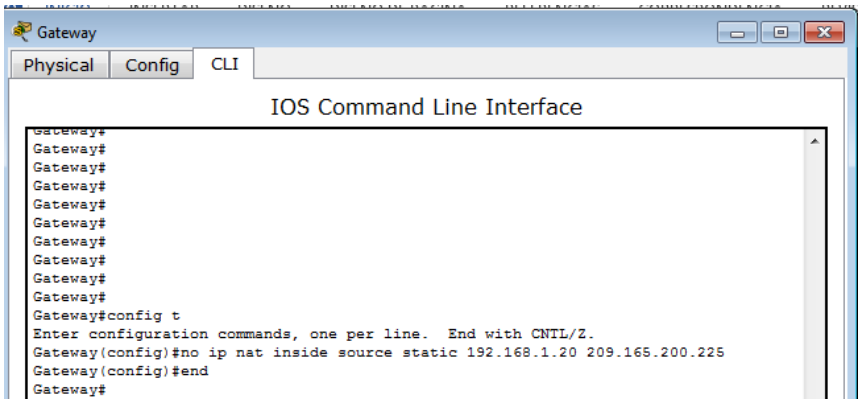


Imagen 353, comando no ip nat inside source static 192.168.1.20 209.165.200.225

b. Borre las NAT y las estadísticas.

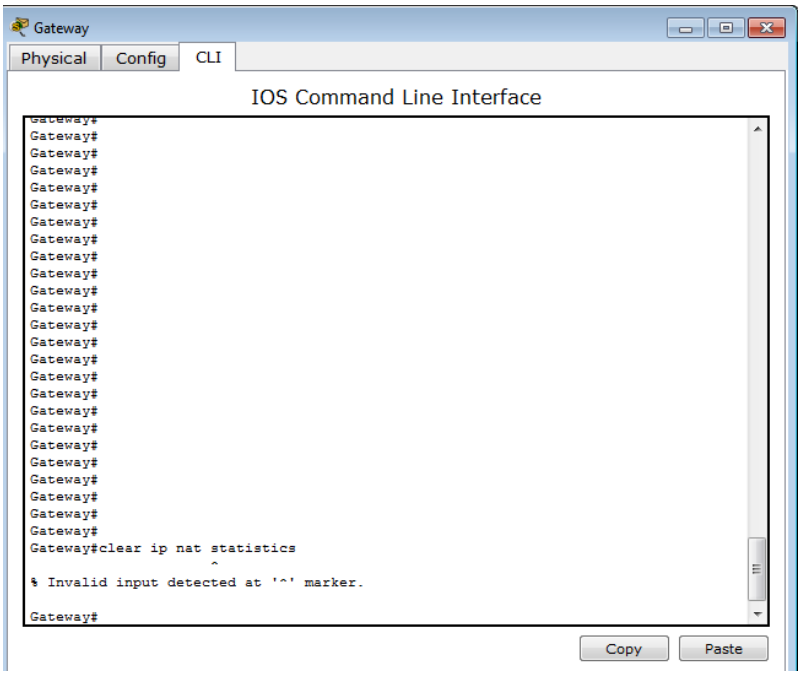


Imagen 354, packet tracer no soporta el comando para statistics

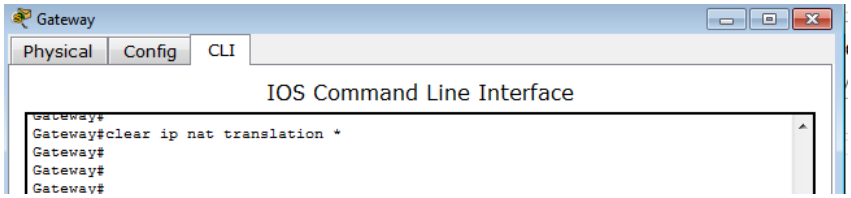


Imagen 355, translation eliminada

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

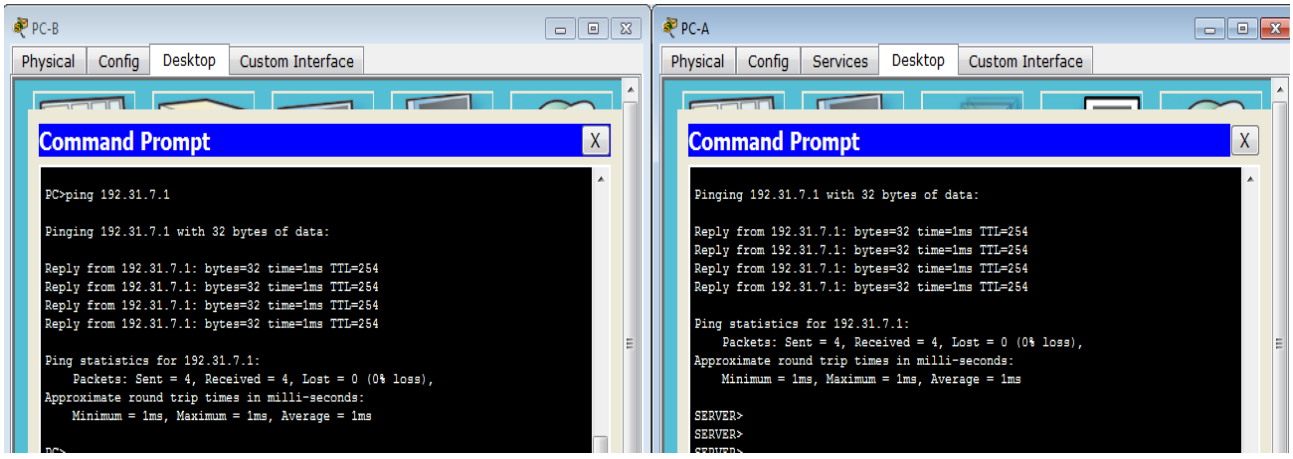


Imagen 356, ping a ISP satisfactorio

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
```

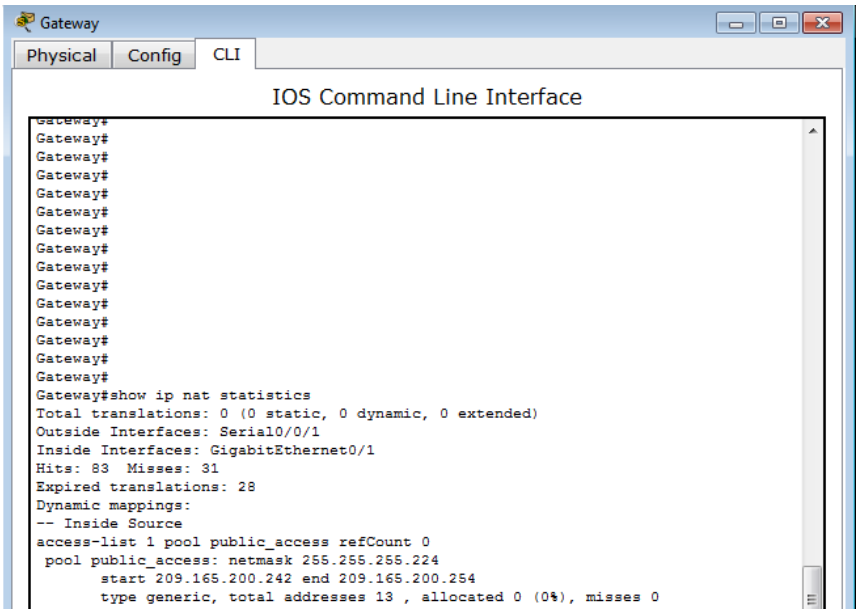


Imagen 357, comando show ip nat statistics

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.

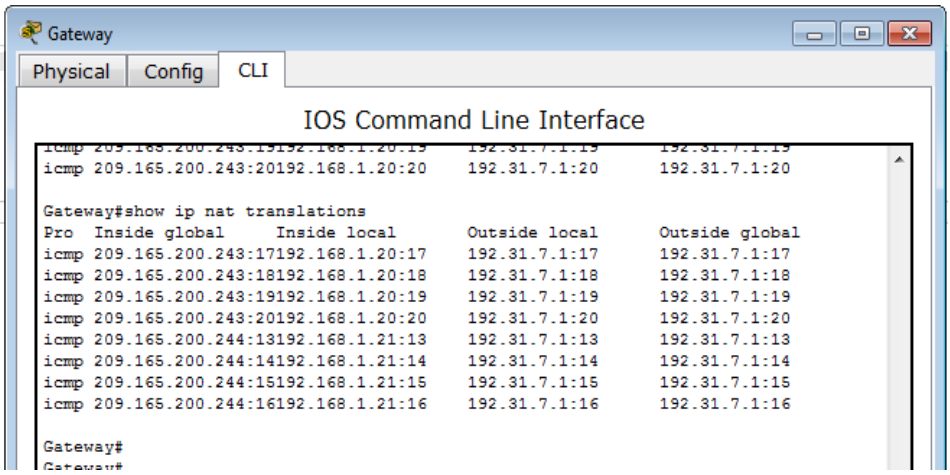


Imagen 358, comando show ip nat translations

Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

   Respuesta: no hay suficientes direcciones publicas ip, también sirve para esquivar y comprar direcciones públicas de un servidor, puede ser utilizado para una forma de seguridad ocultando las direcciones ip internas hacia la red externa.

2. ¿Cuáles son las limitaciones de NAT?

   Respuesta: la NAT necesita la información ip o la información del número de puerto en la cabecera de IP y de TCP, para la translación hay una lista parcial de protocolos que no puede ser usada en NAT por ejemplo SNMP, LDAP y Kerberos V5, otra ventaja de NAT es que aumenta un poco la latencia.

Conclusión.

- Con la practica se aprendió a realizar el armado de la red, verificar la conectividad, configurar y verificar la NAT estática y por ultimo configurar y verificar la NAT dinámica

11.2.3.7 Lab - Configuring Nat Pool Overload And Pat

Topología

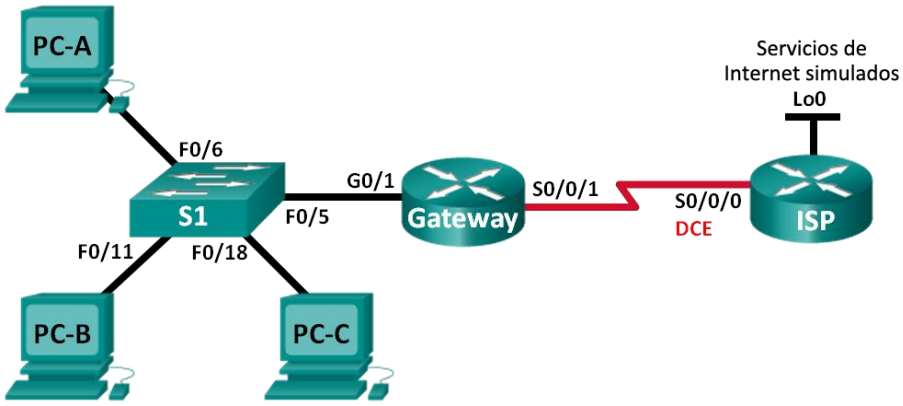


Imagen 359. Topología.

Tabla 14:

Tabla de direccionamiento

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

Objetivos

Parte 1: armar la red y verificar la conectividad

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

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

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

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

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

Recursos necesarios

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

Parte 1. Armar la red y verificar la conectividad

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

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

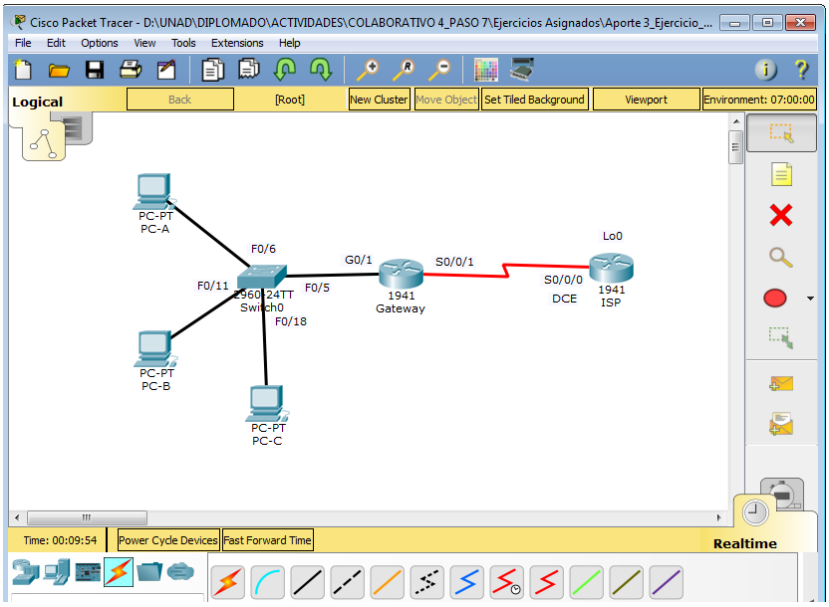


Imagen 360. Cableado de Red

Paso 2. Configurar los equipos host.

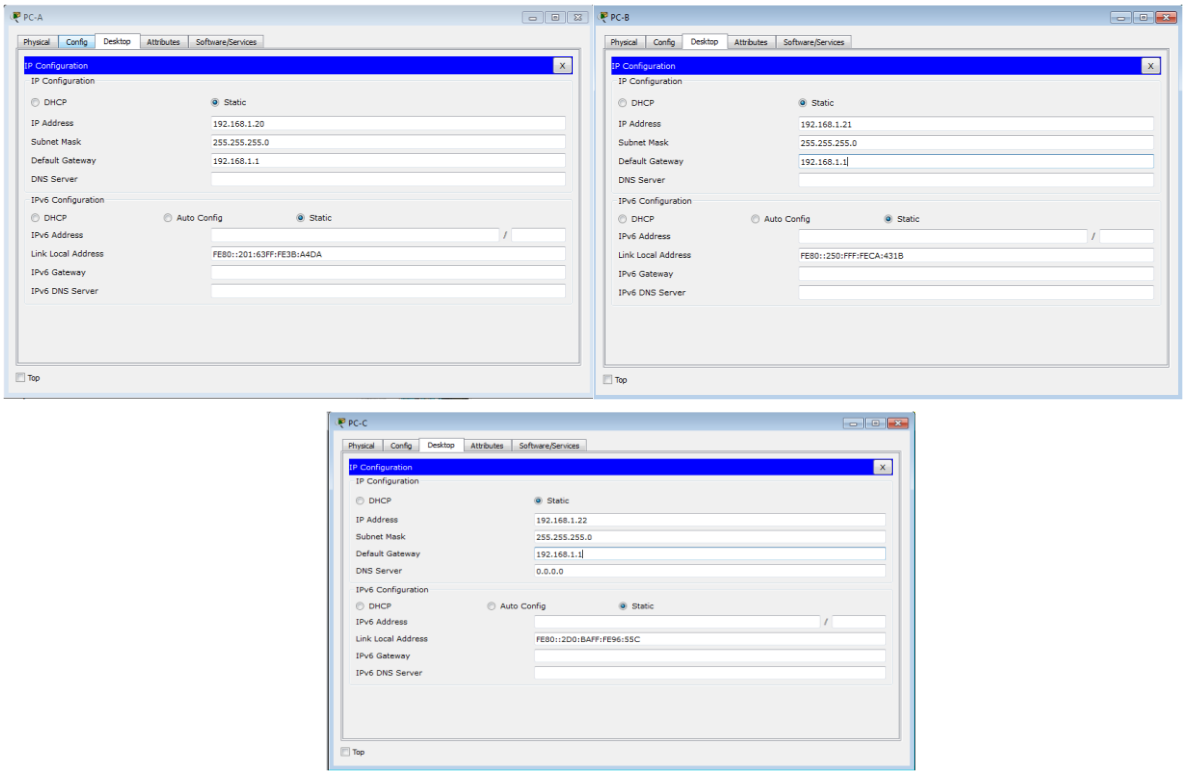


Imagen 361. Configuración de Host

Paso 3. Inicializar y volver a cargar los routers y los switches.

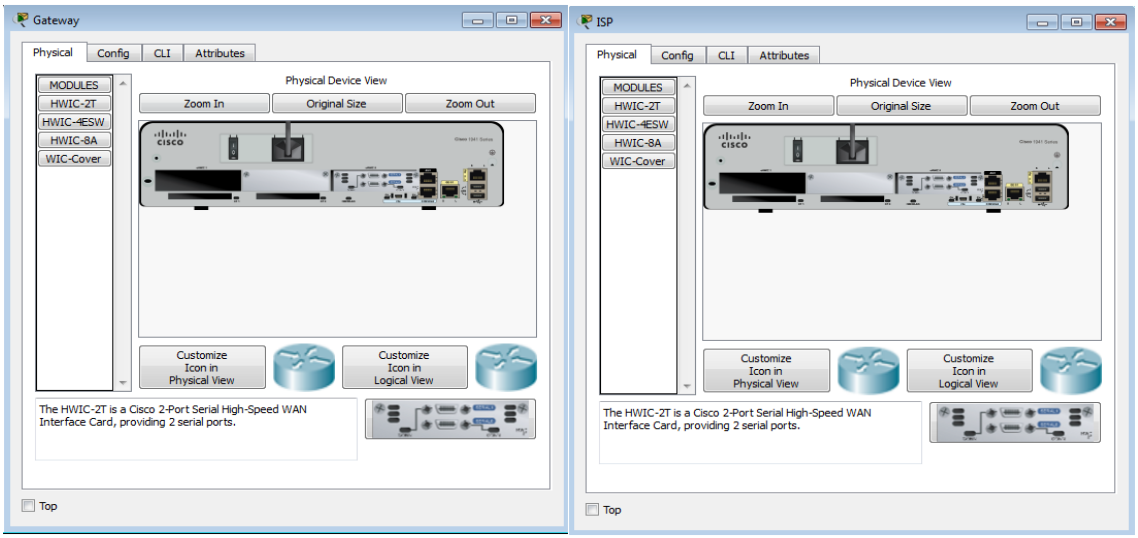


Imagen 362. Inicializando Dispositivos.

Paso 4. Configurar los parámetros básicos para cada router.

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

f. Desactive la búsqueda del DNS.

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

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

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

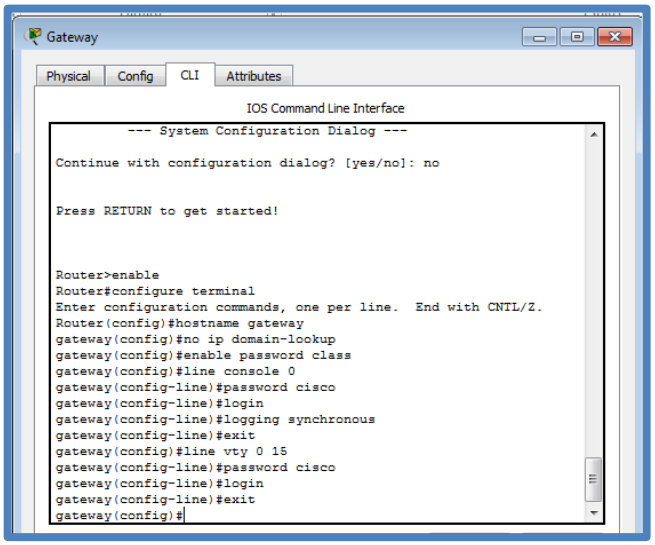


Imagen 363. Configuración Parámetros Básicos Gateway.

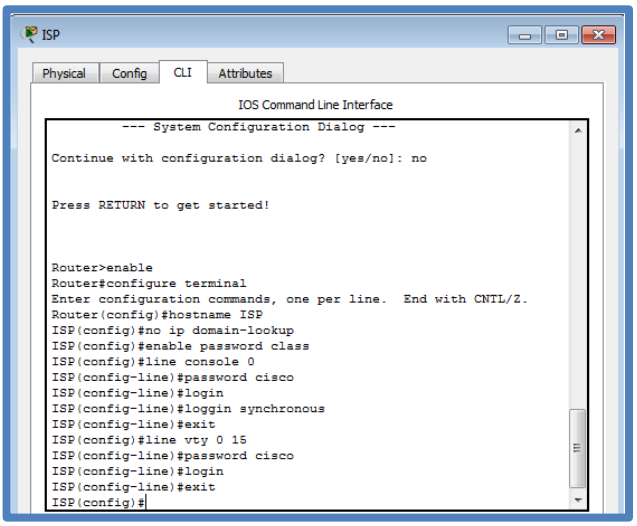


Imagen 364. Configuración Parámetros Básicos ISP.

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

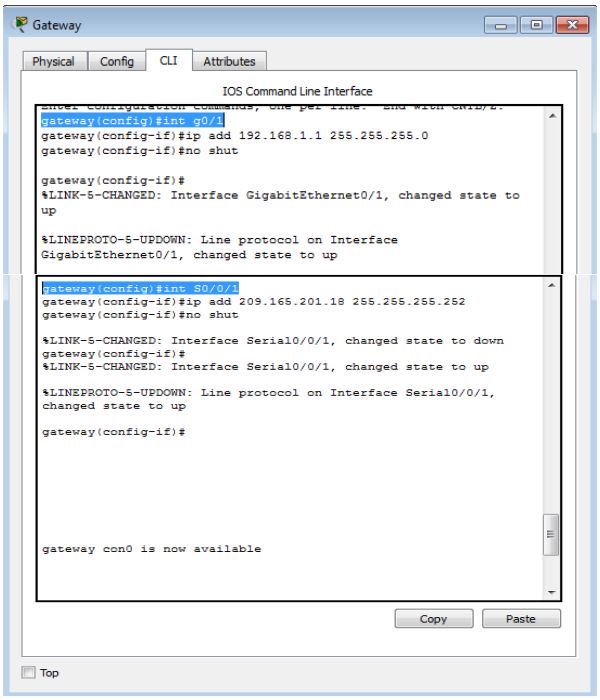


Imagen 365. Configuración Direcciones IP Gateway.

k. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

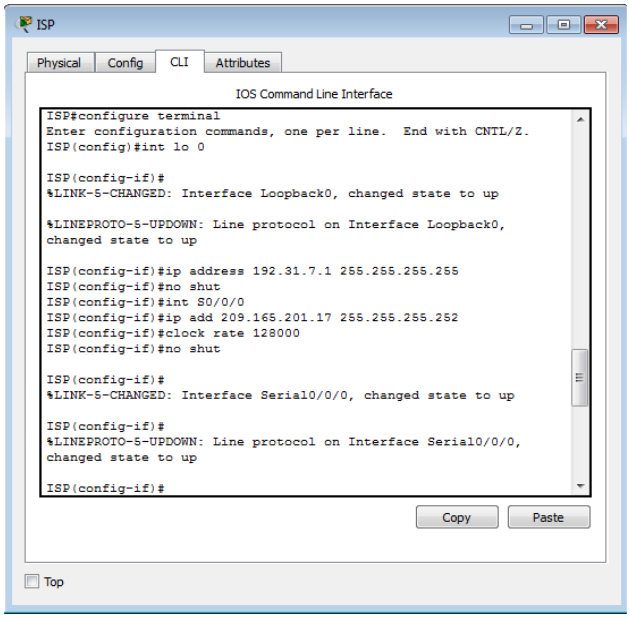


Imagen 366. Configuración Direcciones IP ISP y Frecuencia Reloj.

Paso 5. Configurar el routing estático.

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

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

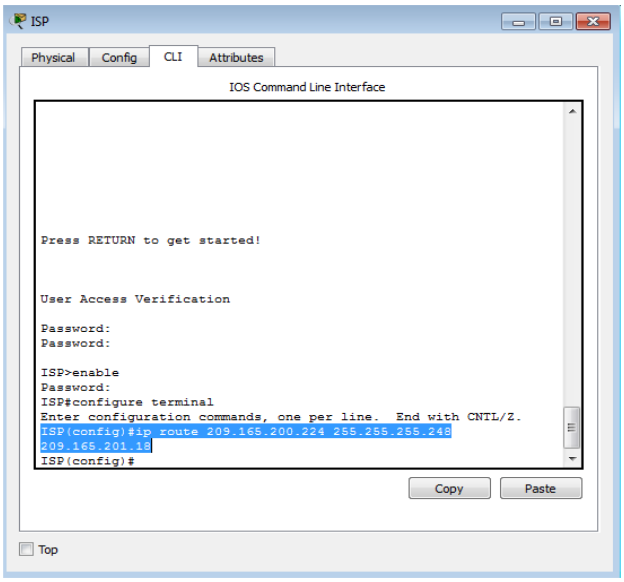


Imagen 367. Configuración Ruta Estática desde ISP a Gateway.

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**

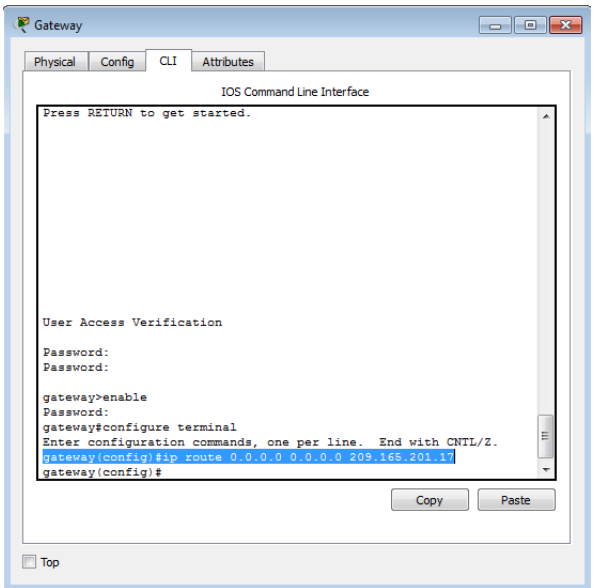


Imagen 368. Configuración Ruta Predeterminada desde Gateway a ISP.

Paso 6. Verificar la conectividad de la red

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

b) Verifique que las rutas estáticas estén bien configuradas en ambos routers.

PC-A

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=44ms 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 = 44ms, Average = 11ms

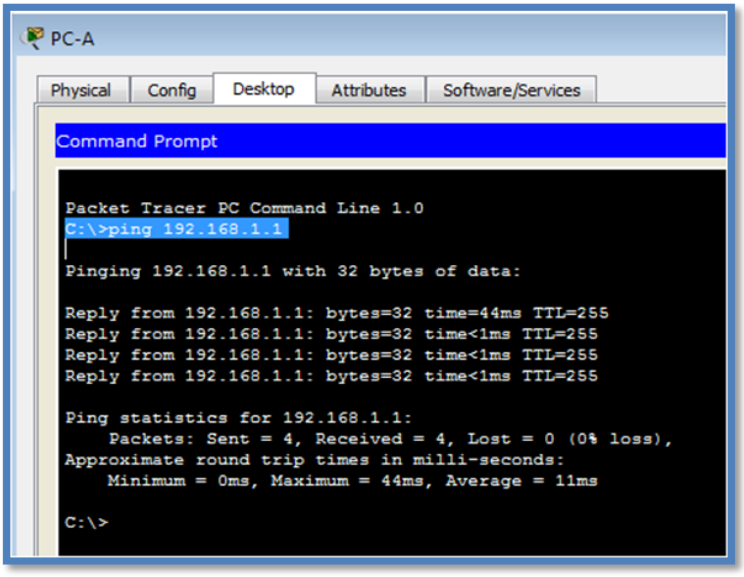


Imagen 369. Verificando Conectividad desde PC-A a Gateway.

PC-B

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=12ms 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 = 12ms, Average = 3ms

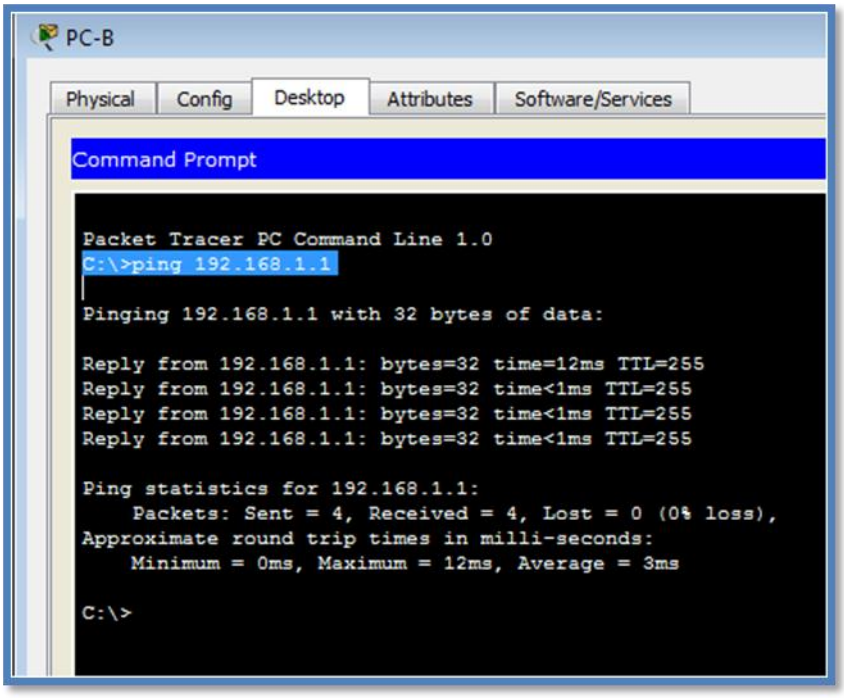


Imagen 370. Verificando Conectividad desde PC-B a Gateway.

PC-C

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=16ms 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 = 16ms, Average = 4ms

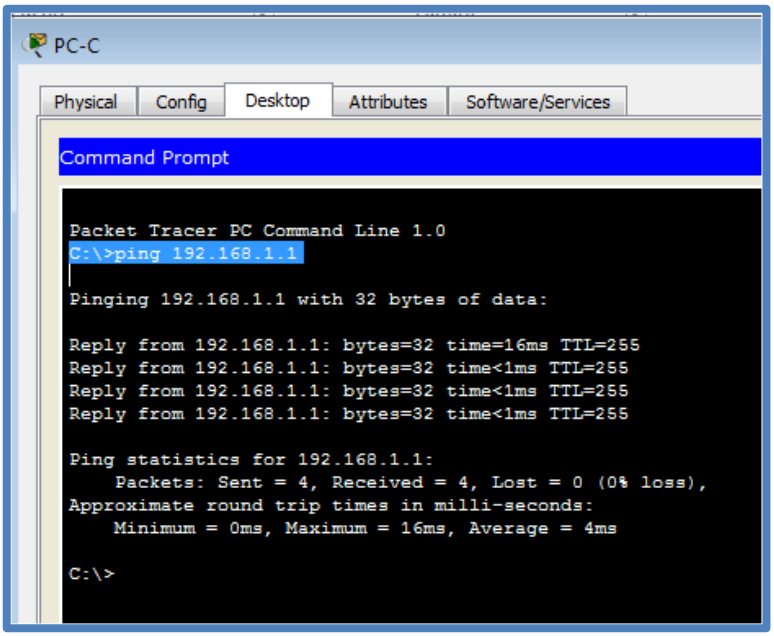


Imagen 371. Verificando Conectividad desde PC-C a Gateway.

Parte 2. Configurar y verificar el conjunto de NAT con sobrecarga

Configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

Paso 1. Definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN. La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

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

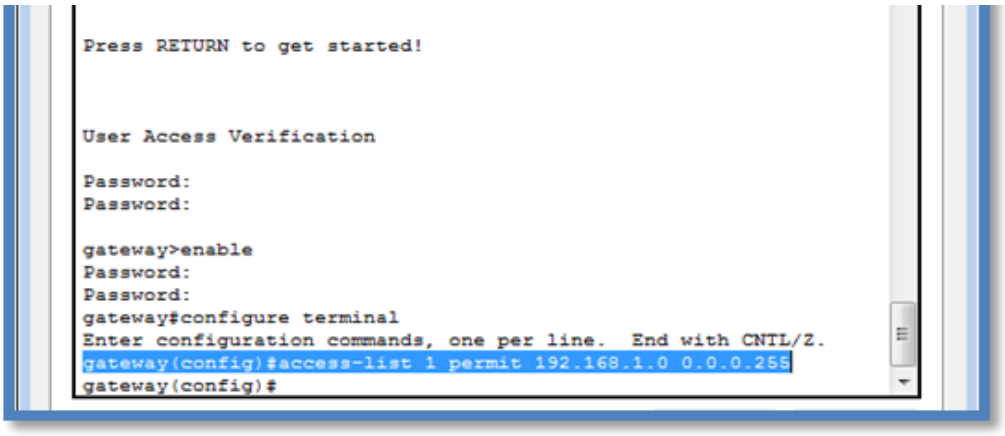


Imagen 372. Definiendo Lista de Control de Acceso 1.

Paso 2. Definir el conjunto de direcciones IP públicas utilizables.

Gateway(config)# ***ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248***

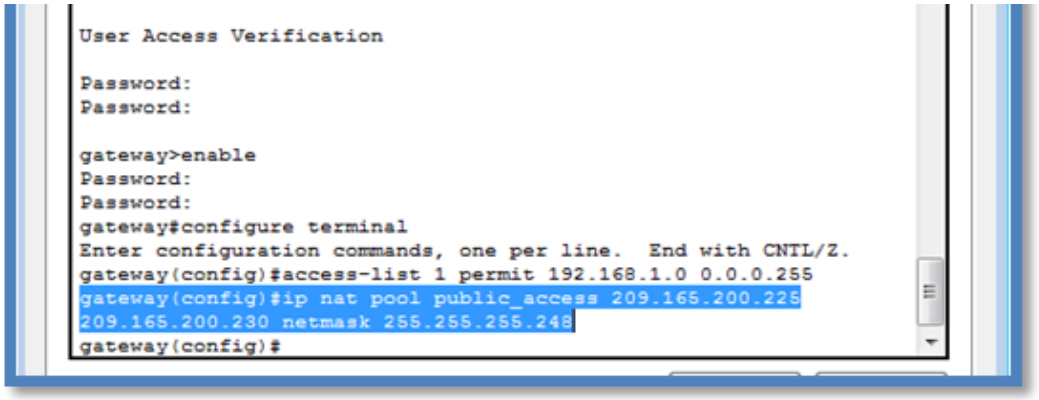


Imagen 373. Definiendo Conjunto de IP Públicas Utilizables.

Paso 3. Definir la NAT desde la lista de origen interna hasta el conjunto externo.

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

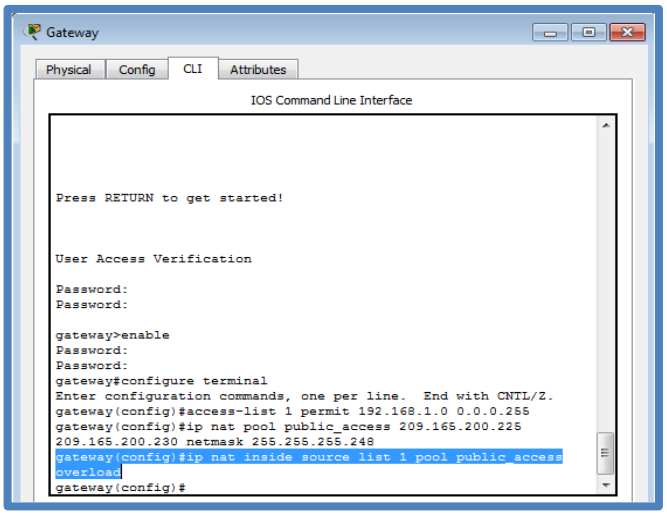


Imagen 374. Definición de la NAT.

Paso 4. Especifique las interfaces.

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

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

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

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

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

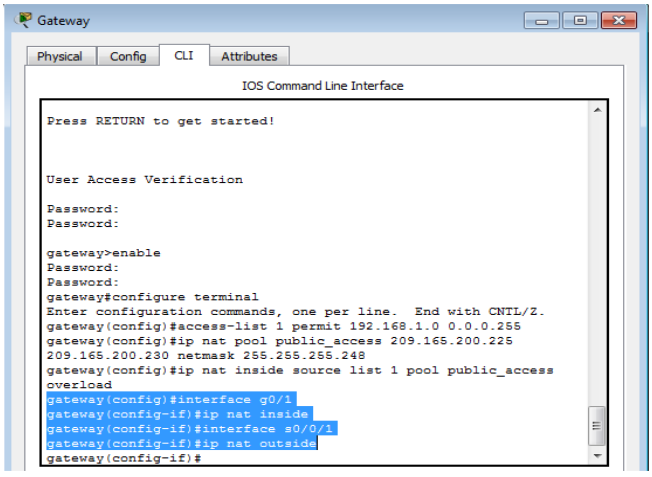


Imagen 375. Especificando las Interfaces.

Paso 5. Verificar la configuración del conjunto de NAT con sobrecarga.

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

PC-A

C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 2ms, Average = 1ms

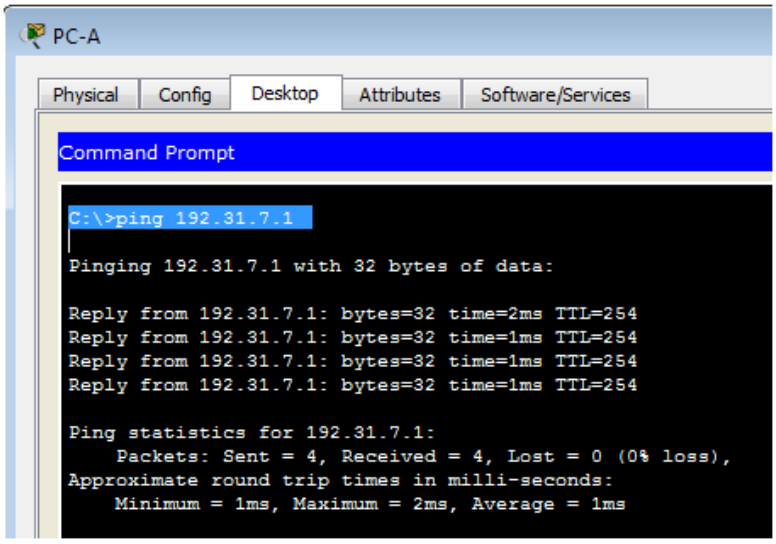


Imagen 376. Verificando configuración del conjunto de NAT desde PC-A.

PC-B

C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254

Ping statistics for 192.31.7.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms

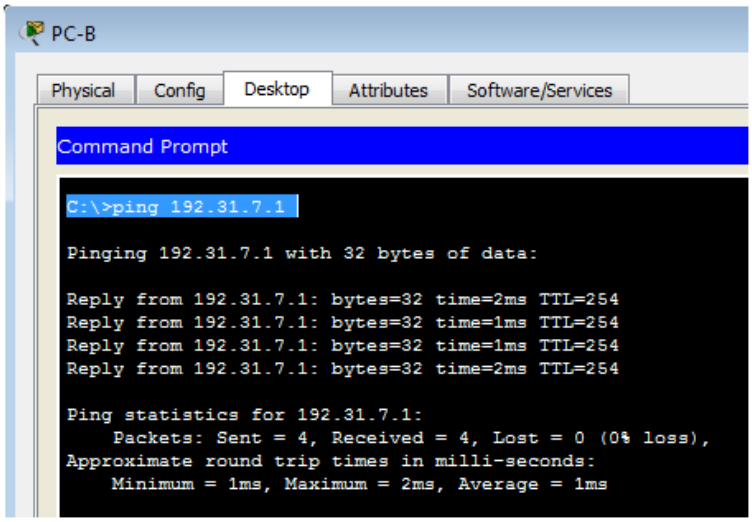


Imagen 377. Verificando configuración del conjunto de NAT desde PC-B.

PC-C

C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms

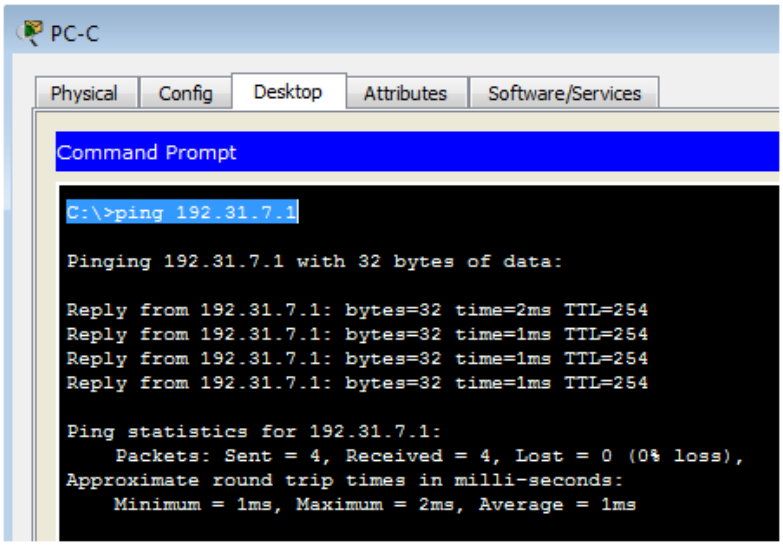


Imagen 378. Verificando configuración del conjunto de NAT desde PC-C.

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

Gateway# **show ip nat statistics**

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

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

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 3

pool public_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

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

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

gateway#show ip nat statistics

Total translations: 12 (0 static, 12 dynamic, 12 extended)

Outside Interfaces: Serial0/0/1

Inside Interfaces: GigabitEthernet0/1

Hits: 44 Misses: 44

Expired translations: 32

Dynamic mappings:

-- Inside Source

access-list 1 pool public_access refCount 12

pool public_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

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

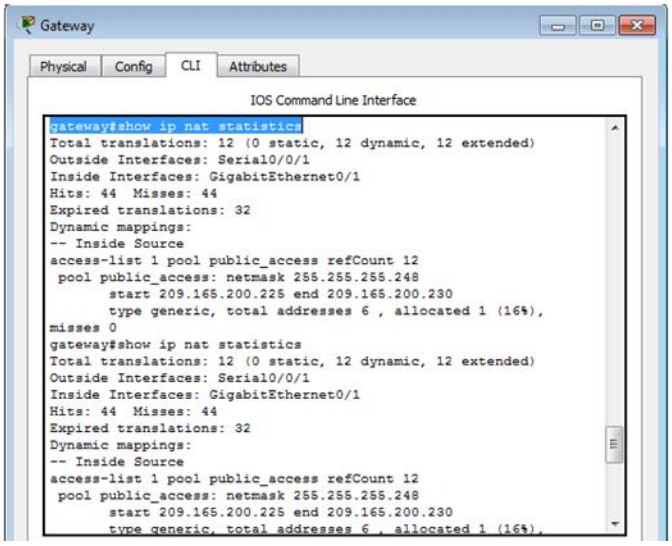


Imagen 379. Estadísticas de NAT.

c. Muestre las NAT en el router Gateway.

Gateway# **show ip nat translations**

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

Nota: es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

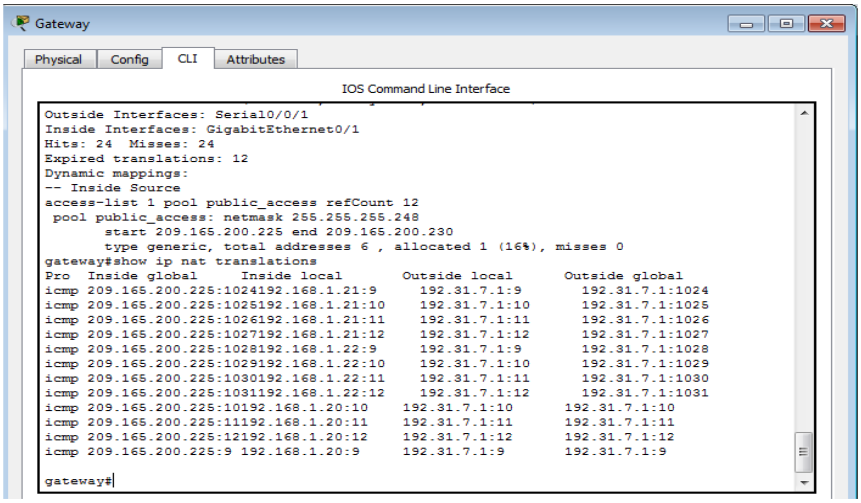


Imagen 380. Mostrando las NAT.

gateway#show ip nat translations

Pro Inside global	*Inside local*	*Outside local*	*Outside global*
icmp 209.165.200.225:1024	*192.168.1.21:9*	*192.31.7.1:9*	*192.31.7.1:1024*
icmp 209.165.200.225:1025	*192.168.1.21:10*	*192.31.7.1:10*	*192.31.7.1:1025*
icmp 209.165.200.225:1026	*192.168.1.21:11*	*192.31.7.1:11*	*192.31.7.1:1026*
icmp 209.165.200.225:1027	*192.168.1.21:12*	*192.31.7.1:12*	*192.31.7.1:1027*
icmp 209.165.200.225:1028	*192.168.1.22:9*	*192.31.7.1:9*	*192.31.7.1:1028*
icmp 209.165.200.225:1029	*192.168.1.22:10*	*192.31.7.1:10*	*192.31.7.1:1029*
icmp 209.165.200.225:1030	*192.168.1.22:11*	*192.31.7.1:11*	*192.31.7.1:1030*
icmp 209.165.200.225:1031	*192.168.1.22:12*	*192.31.7.1:12*	*192.31.7.1:1031*
icmp 209.165.200.225:10	*192.168.1.20:10*	*192.31.7.1:10*	*192.31.7.1:10*
icmp 209.165.200.225:11	*192.168.1.20:11*	*192.31.7.1:11*	*192.31.7.1:11*
icmp 209.165.200.225:12	*192.168.1.20:12*	*192.31.7.1:12*	*192.31.7.1:12*
icmp 209.165.200.225:9	*192.168.1.20:9*	*192.31.7.1:9*	*192.31.7.1:9*

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior?

Se indican 3 Direcciones IP locales:

- **192.168.1.20**
- **192.168.1.21**
- **192.168.1.22**

¿Cuántas direcciones IP globales internas se indican? **Se indica una (1) Dirección IP Global: 209.165.200.225**

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

Se usan 12 puertos distintos.

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué? **El ping falla porque el router sólo conoce las direcciones inside global en su tabla de ruteo, estas direcciones no están notificadas. NAT (Gateway) no deja ver las direcciones de los pcs.**

ISP>ping 192.168.1.20

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

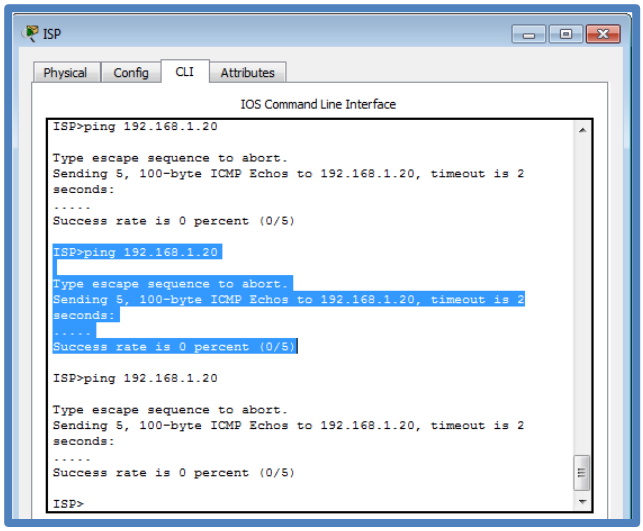


Imagen 381. Ping desde ISP a PC-A.

Parte 3. Configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Paso 1. Borrar las NAT y las estadísticas en el router Gateway.

*gateway#clear ip nat translation **

Paso 2. Verificar la configuración para NAT.

a. Verifique que se hayan borrado las estadísticas.

*gateway#clear ip nat translation **

gateway#show ip nat translations

gateway#show ip nat statistics

Total translations: 0 (0 static, 0 dynamic, 0 extended)

Outside Interfaces: Serial0/0/1

Inside Interfaces: GigabitEthernet0/1

Hits: 24 Misses: 24

Expired translations: 24

Dynamic mappings:

-- Inside Source

access-list 1 pool public_access refCount 0

pool public_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

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

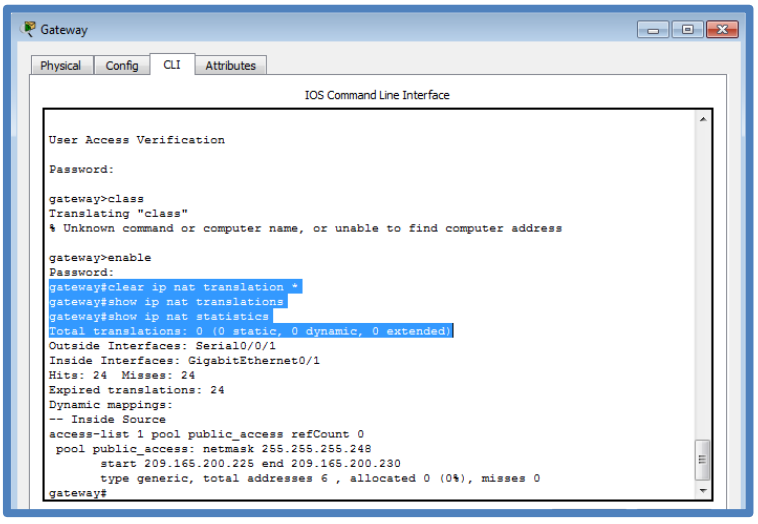


Imagen 382. Borrado de las NAT y las Estadísticas en el Router.

b. Verifique que las interfaces externa e interna estén configuradas para NAT.

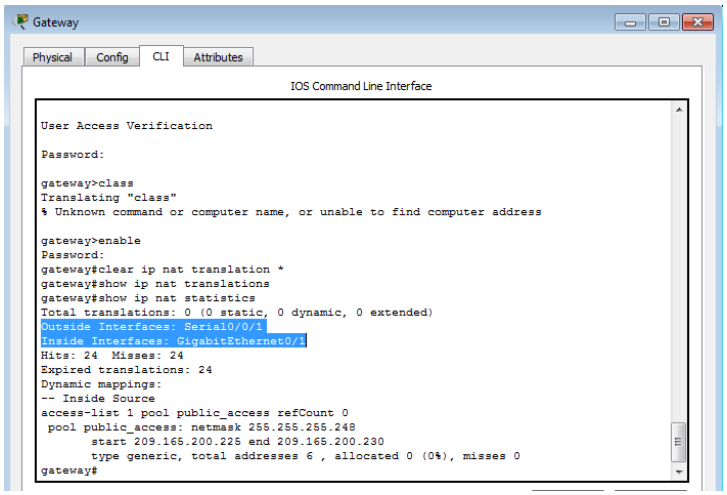


Imagen 383. Verificando Interfaces Internas y Externas.

c. Verifique que la ACL aún esté configurada para NAT.

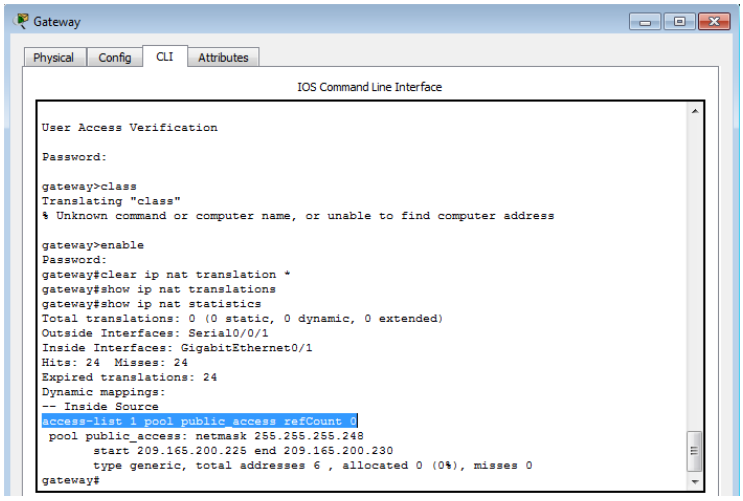


Imagen 384. Verificando ACL Configurada para NAT.

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

Se utilizó el commando: *show ip nat statistics*

Paso 3. Eliminar la traducción NAT de la lista de origen interna al conjunto externo.

*Gateway(config)# **no ip nat inside source list 1 pool public_access overload***

Paso 4. Eliminar el conjunto de direcciones IP públicas utilizables.

*Gateway(config)# **no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248***

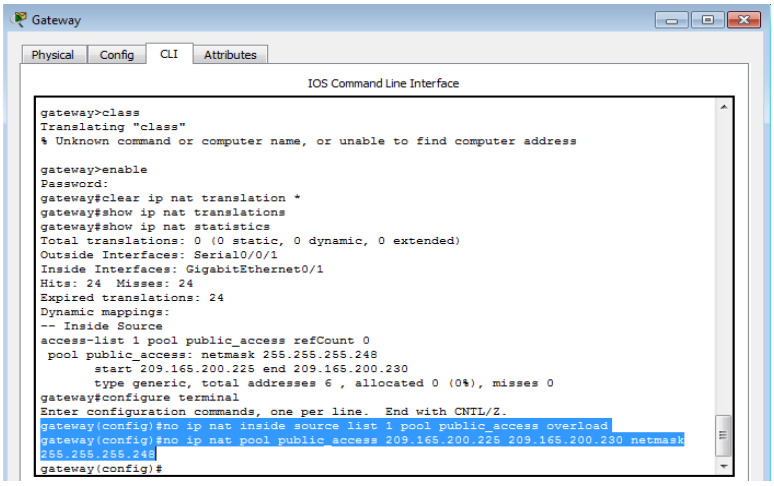


Imagen 385. Eliminación de la traducción NAT y conjunto de direcciones IP públicas.

Paso 5. Asociar la lista de origen a la interfaz externa.

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

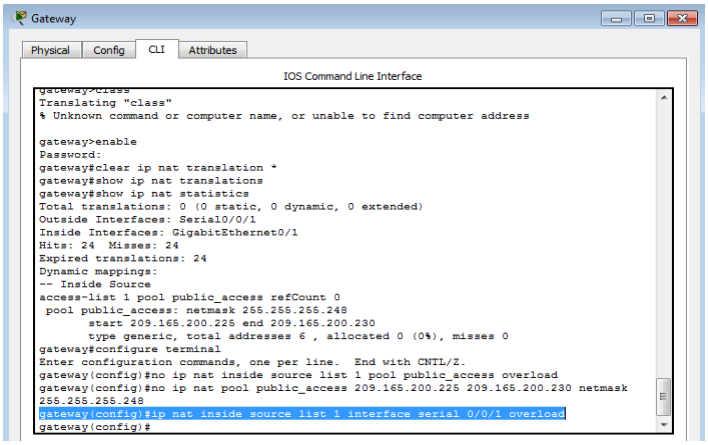


Imagen 386. Asociar la Lista de Origen.

Paso 6. Probar la configuración PAT.

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

PC-A

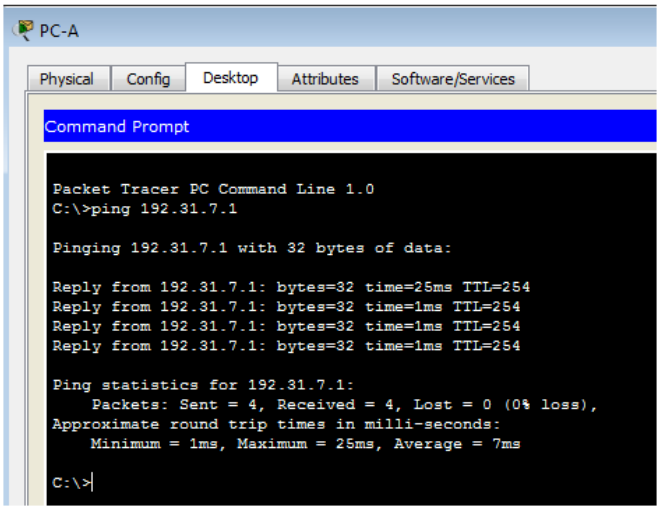


Imagen 387. Verificando Conectividad desde PC-A a ISP.

PC-B

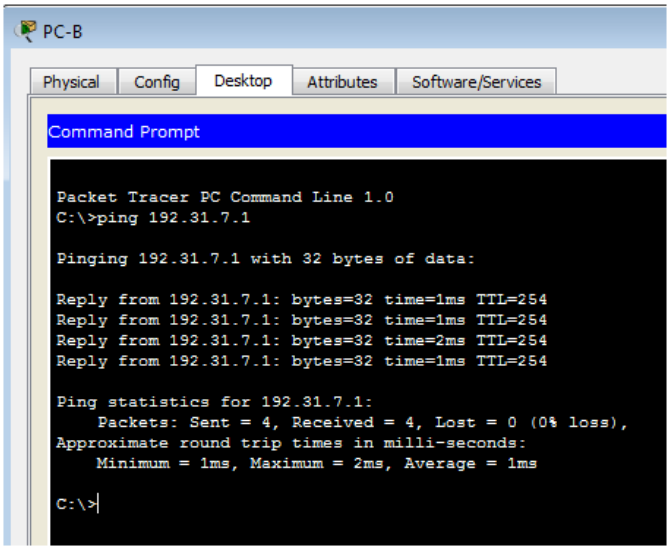


Imagen 388. Verificando Conectividad desde PC-B a ISP.

PC-C

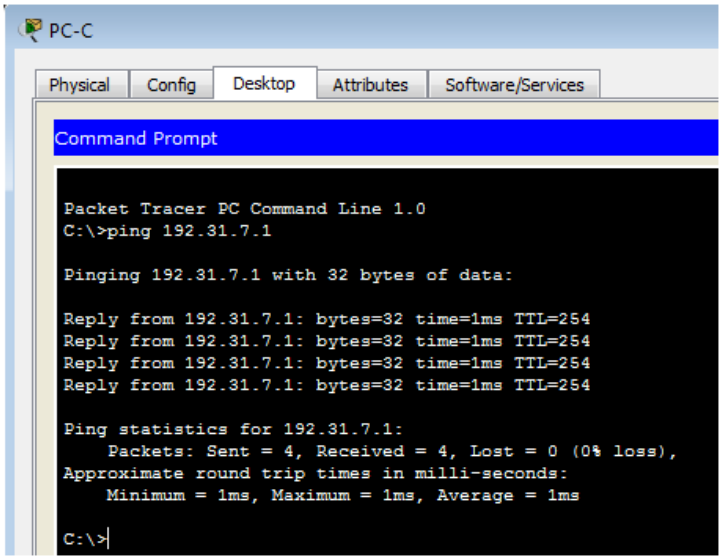


Imagen 389. Verificando Conectividad desde PC-C a ISP.

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

Gateway# **show ip nat statistics**

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

Peak translations: 3, occurred 00:00:19 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

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

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

gateway#show ip nat statistics

Total translations: 12 (0 static, 12 dynamic, 12 extended)

Outside Interfaces: Serial0/0/1

Inside Interfaces: GigabitEthernet0/1

Hits: 24 Misses: 24

Expired translations: 12

Dynamic mappings:

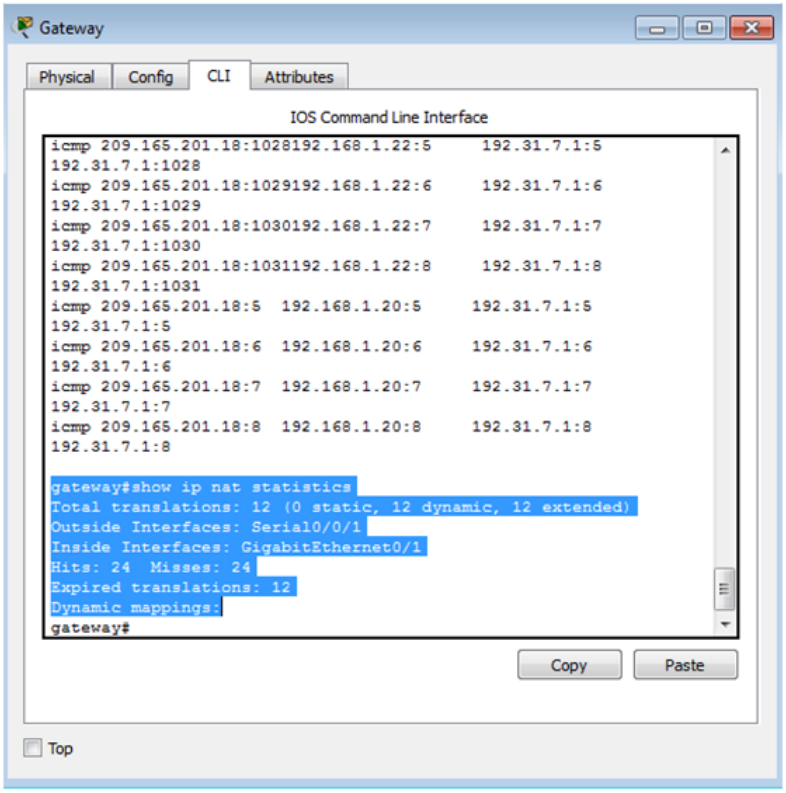


Imagen 390. Mostrando Estadísticas de NAT.

c. Muestre las traducciones NAT en el Gateway.

Gateway# **show ip nat translations**

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

gateway#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.18:1024	192.168.1.21:5	192.31.7.1:5	192.31.7.1:1024
icmp	209.165.201.18:1025	192.168.1.21:6	192.31.7.1:6	192.31.7.1:1025
icmp	209.165.201.18:1026	192.168.1.21:7	192.31.7.1:7	192.31.7.1:1026
icmp	209.165.201.18:1027	192.168.1.21:8	192.31.7.1:8	192.31.7.1:1027
icmp	209.165.201.18:1028	192.168.1.22:5	192.31.7.1:5	192.31.7.1:1028

icmp 209.165.201.18:1029	192.168.1.22:6	192.31.7.1:6	192.31.7.1:1029
icmp 209.165.201.18:1030	192.168.1.22:7	192.31.7.1:7	192.31.7.1:1030
icmp 209.165.201.18:1031	192.168.1.22:8	192.31.7.1:8	192.31.7.1:1031
icmp 209.165.201.18:5	192.168.1.20:5	192.31.7.1:5	192.31.7.1:5
icmp 209.165.201.18:6	192.168.1.20:6	192.31.7.1:6	192.31.7.1:6
icmp 209.165.201.18:7	192.168.1.20:7	192.31.7.1:7	192.31.7.1:7
icmp 209.165.201.18:8	192.168.1.20:8	192.31.7.1:8	192.31.7.1:8

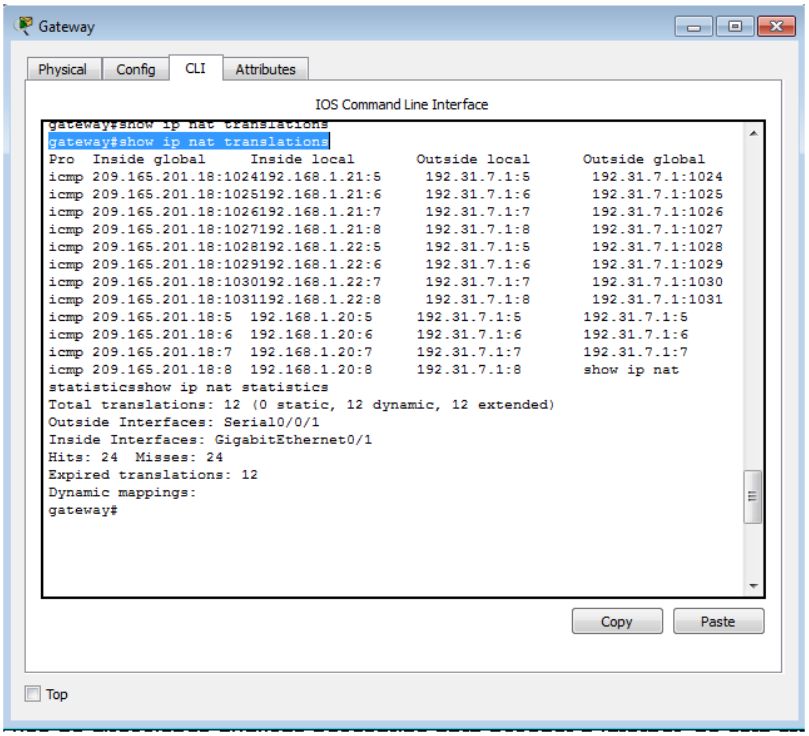


Imagen 391. Mostrando Estadísticas de NAT.

Reflexión

¿Qué ventajas tiene la PAT?

Al utilizar solo una IP pública, la de la interface, se ahorran direcciones IPs públicas, es así como pueden salir varios computadores con direcciones privada con solo una Ip pública y utilizando distintos puertos para diferenciar cada paquete que sale, además, hay seguridad.

PAT minimiza el número de direcciones públicas necesitadas para permitir el acceso a internet y esa PAT, como NAT sirve para ocultar, direcciones privadas hacia l red externa.

Conclusiones.

En la práctica de laboratorio se puede concluir que:

- ➢ Se realizó la topología de la red y se verificó su conectividad.

- ➢ Se aplicó los diferentes comandos para la configuración y verificación de un conjunto de NAT con sobrecarga, lo que permitió que una red local se comunique con la red externa con una sola IP publica, a través de procesos de traducción de un grupo de direcciones IP privadas a la dirección pública asignada, reduciendo de esta manera el uso de direcciones. Además del gran ahorro de direcciones NAT permite mejorar la seguridad de las redes, pues las terminales internas no serán visibles desde el exterior, reduciendo riesgos de ataques.

- ➢ Para configurar de manera adecuada NAT debe contar con una ACL por medio de la cual se autoricen direcciones para el tráfico.

- ➢ Se configuró y verificó el uso de las PAT, cuya importancia en una red es minimizar el número de direcciones públicas necesitadas para ingresar a internet, y PAT al igual que NAT sirve para ocultar las direcciones privadas hacia la red externa.

- ➢ Cuando se realiza ping desde el Router ISP a una de los hots, sucede que el ping falla porque solo conoce el lugar de las direcciones Ip Inside global en su tabla de ruteo, pero las direcciones IP Inside local no están notificadas.

- ➢ Al usar PAT estamos logrando minimizar el uso de direcciones IP, pues su funcionamiento al igual que NAT es traducir varias direcciones privadas de una red local, a una única dirección pública hacia la red externa, la diferencia es que PAT usa los puertos, pudiendo

usar la misma IP pública a la salida, pero con diferente puerto, incrementando la usabilidad de la IP pública.

Conclusiones

- En esta actividad se realiza un número amplio de tareas importantes para el buen desarrollo de los ejercicios propuestos, en este se ejecutan funciones como la de verificar una conexión entre los dispositivos proporcionada en la configuración inicial de la topología, se configura la ACL de los Routers, esto con el objetivo de mitigar los ataques de forma remota y por supuesto no podrían faltar la verificación de la funcionalidad de las actividades ejecutadas con anterioridad. (ACL) para permitir el acceso de direcciones IP específicas, lo que asegura que solo la computadora del administrador tenga permiso para acceder al router mediante telnet o SSH.

- A través de la configuración de listas de control de acceso (ACL) podemos permitir o denegar que determinados hosts en una red tengan acceso o no, a servicios como DNS, FTP, HTTPS entre otros, misma forma podemos realizar este tipo de configuraciones por puertos o por direcciones IP específicas.

- La configuración de rutas estáticas predeterminadas tanto en IPv4 como IPv6 simula el acceso a internet de las redes y permite la conectividad de extremo a extremo.

- El protocolo RIPv2 soporta la implementación de VLSM, tiene un alcance de máximo 15 saltos y las actualizaciones de enrutamientos las establece a través de multicast.

- La configuración de NAT hace uso de una dirección global pública para transmitir los paquetes, mientras que la configuración de PAT hace uso de interfaces para la trasmisión de paquetes.

- En la configuración NAT y PAT se tiene niveles de seguridad importantes, pues un router ISP solo puede responder solicitudes mas no puede hacer solicitudes a los hosts que conforman una red privada, pues no conoce sus direcciones IPs.

- NAT necesita información de la IP o a información del número del puerto en la cabecera IP y encabezado TCP de paquetes para traducción; además hay una lista parcial de protocolos que no se pueden utilizar con NAT, por ejemplo, LDAP, SNMP, Kerveros versión 5; también encontramos que NAT tiene otra desventaja la cual es que se retrasa en el proceso de traducción.

- Cuando tenemos Routers separados DHCP para cada subred estamos agregando más complejidad y decrementamos la administración central de la red. Requiriendo que cada Router trabaje para sus propias direcciones DHCP, teniendo como función primaria el tráfico del ruteo y siendo más fácil de administrar.

- PAT resulta más sencillo de implementar que NAT debido a que solo es necesario especificar el puerto a la red externa para realizar la traducción de direcciones IP privadas a públicas y no un rango de direcciones.

- Se logró hacer un reconocimiento a los comandos básicos de direccionamiento IPv6.

- El tiempo de vida o TTL de los paquetes que se envían de una red LAN a otra es mucho menor que el TTL de los paquetes que recorren una misma red debido a que tiene que atravesar R1 y R2.

- TTL de paquetes entre los dispositivos de una misma red LAN es 127 ms mientras que el TTL de los paquetes entre los dispositivos de diferente LAN es 126 ms. Para la asignación de subredes IPv6 es importante conocer la conversión de números Hexadecimales.

- La implementación de un adecuado sistema de redes, y la elección de los medios, materiales y del personal, son elemento clave para la buena ejecución y consecución de la misma. Toda red de computadoras está sujeta a limitaciones y depende del equipo de diseño y análisis, el elegir aquella topología y el protocolo adecuado, así como también el hardware necesario.

- En cuanto al os fundamentos de redes podemos decir que ya se tiene un concepto claro de lo que es una red, es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat), etc.

- En cuanto a redes conmutadas entendimos por conmutación en un nodo, a la conexión física o lógica, de un camino de entrada al nodo con un camino de salida del nodo, con el fin de transferir la información. Así, se puede decir que una red conmutada es aquella que permite la comunicación de nodo a nodo a través de su conexión, para facilitar el traslado de información.

- Los protocolos de enrutamiento dinámico generalmente se usan en redes de mayor tamaño para facilitar la sobrecarga administrativa y operativa que implica el uso de rutas estáticas únicamente. Normalmente, una red usa una combinación de un protocolo de enrutamiento dinámico y rutas estáticas. En la mayoría de las redes, se usa un único protocolo de enrutamiento dinámico; sin embargo, hay casos en que las distintas partes de la red pueden usar diferentes protocolos de enrutamiento.

- El protocolo OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.

- Las listas de control de acceso desempeñan un gran papel como medida de seguridad lógica, ya que su cometido siempre es controlar el acceso a los recursos o activos del sistema.

- DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP está activo en un servidor donde se centraliza la gestión de la direcciones IP de la red.

- Una desventaja de NAPT es cuando se debe traducir paquetes fragmentados TCP/UDP, sólo el primer fragmento contiene el encabezado TCP/UDP que sería necesario para asociar el paquete a una sesión para la traducción. Los fragmentos siguientes no contienen información del puerto TU, simplemente llevan el mismo identificador de fragmentación especificado en el primer fragmento.

- El problema se presenta cuando dos hosts de la red privada originan paquetes TCP/UDP fragmentados al mismo host destino, si por coincidencia usaron el mismo identificador de fragmentación, cuando el host destino recibe los datagramas de ambas fuentes (que no tienen relación entre sí) con el mismo identificador de fragmentación y desde la misma dirección de host asignada, es incapaz de determinar a cuál de las dos sesiones pertenece cada datagrama y las dos sesiones se corrompen.

Referencias Bibliográficas

CISCO. (s.f.). *Principios básicos de routing y switching: Listas de Control de Acceso*. Recuperado el 12 de noviembre de 2017, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#9.0.1

_____. (s.f.). *DHCP*. Recuperado el 15 de noviembre de 2017, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#10.0.1.1

_____. (s.f.). *Principios básicos de routing y switching:Traducción de direcciones de red para IPv4*. Recuperado el 15 de noviembre de 2017, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#11.0

_____. *(2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1*

_____. *(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*