

**DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN**

CCNA2

Paso 7 - Actividad Colaborativa 4

Alexander Ramírez Toro

Código: 1088285716

Yhon James Gómez Andrade Cód. 1076381807

Jorge Luis Quintero Cód.

Adriana Romero Cód. 40776458

Yolima Vargas Escobar Cód. 40.079.610

Grupo: 32

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas Tecnología e Ingeniería
Colombia, Noviembre de 2017

*Nilson Albeiro Ferreira Manzanares

INTRODUCCION

En el siguiente documento se podrá encontrar las prácticas de laboratorio de la unidad 4

Teniendo en cuenta la importancia que tienen los dispositivos que componen una red ya sea cableada o inalámbrica, los dispositivos que se interconectan tienen dos estados de funcionalidad en la red, la primera de ellas se conoce como routers o enrutadores, los cuales se encargan de la interconexión misma de la red y el encaminamiento o enrutamiento de los datos. En un segundo nivel, el Switch el cual se hace cargo de la interconexión de los dispositivos que junto con el cableado conforman una red de área local, convirtiéndose en un dispositivo de escalabilidad muy alto, cuya función es la de conectar los dispositivos en red; sin embargo un switch por sí solo no proporciona la conectividad con otras redes, ni la conexión a internet, por ello se hace indispensable contar con el router, que se encarga de cumplir con la función para conectividad de dispositivos de redes locales hacia internet, manteniendo la vigencia IPv4. Gracias a estos se sostiene el mecanismo NAT o traducción de red, la cual concentra gran cantidad de equipos con conexión bajo una sola IP pública, lo que disminuye en gran proporción el uso de conexiones individuales por cada dispositivo.

Toda esta información y la configuración de los ejercicios propuestos con el objetivo definido para cada caso permite entender mejor y ante todo lograr el objetivo de configurar dispositivos que componen una red, efectuar paso a paso cada planteamiento expuesto en la guía de manera que llevando a la practica en el simulador se comprenda mejor la funcionalidad de cada uno de los equipos activos y pasivos que componen la red.

7.3.2.4 Lab - Configuring Basic RIPv2 and RIPvng (Jhon James Gomes)

Topología

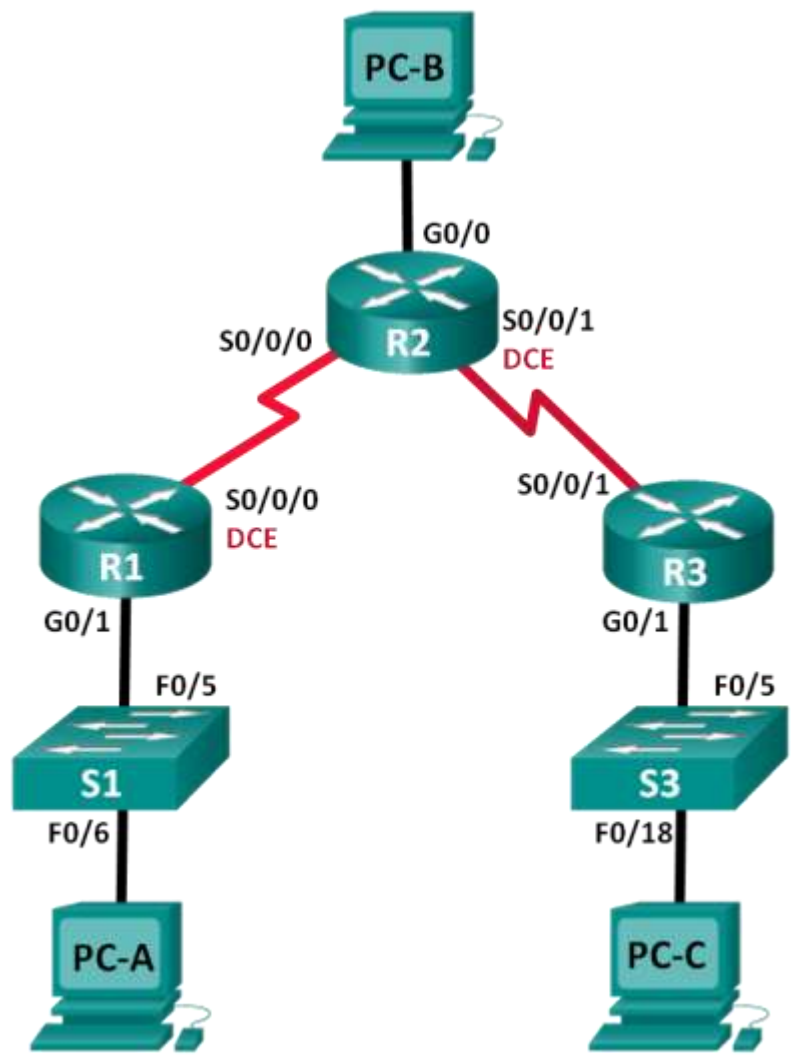


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing RIPv2

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

Parte 3: configurar IPv6 en los dispositivos

Parte 4: configurar y verificar el routing RIPvng

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

Información básica/situación

RIP versión 2 (RIPv2) se utiliza para enrutar direcciones IPv4 en redes pequeñas. RIPv2 es un protocolo de routing vector distancia sin clase, según la definición de RFC 1723. Debido a que RIPv2 es un protocolo de routing sin clase, las máscaras de subred se incluyen en las actualizaciones de routing. De manera predeterminada, RIPv2 resume automáticamente las redes en los límites de redes principales. Cuando se

deshabilita la sumarización automática, RIPv2 ya no resume las redes a su dirección con clase en routers fronterizos.

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

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

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

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

Recursos necesarios

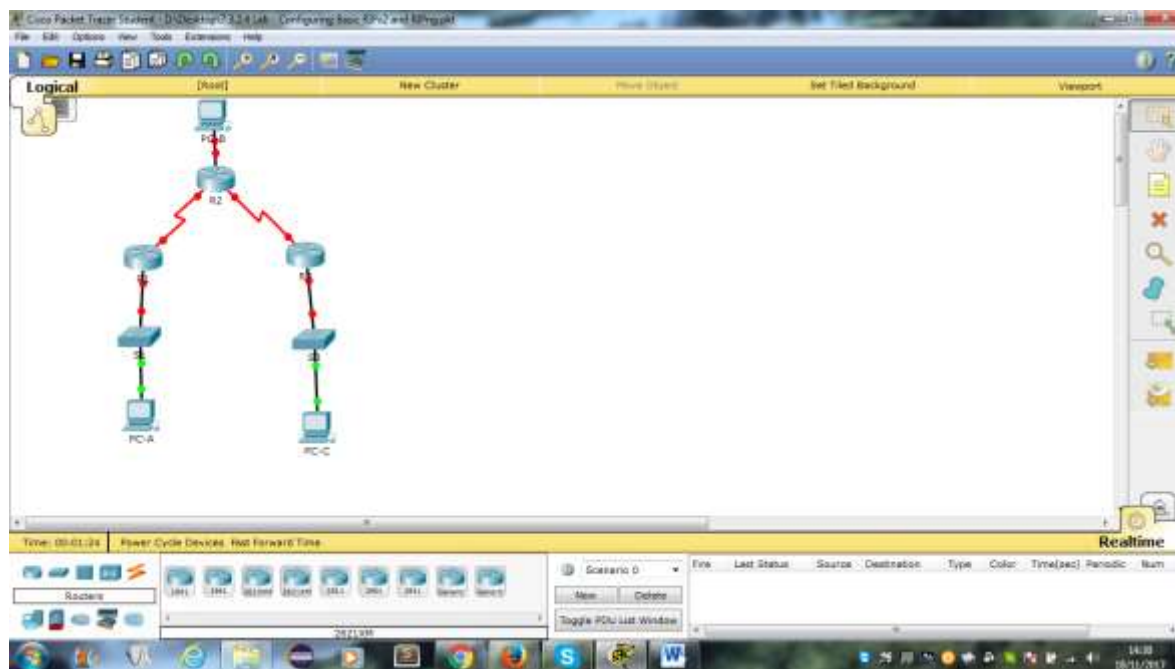
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

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

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

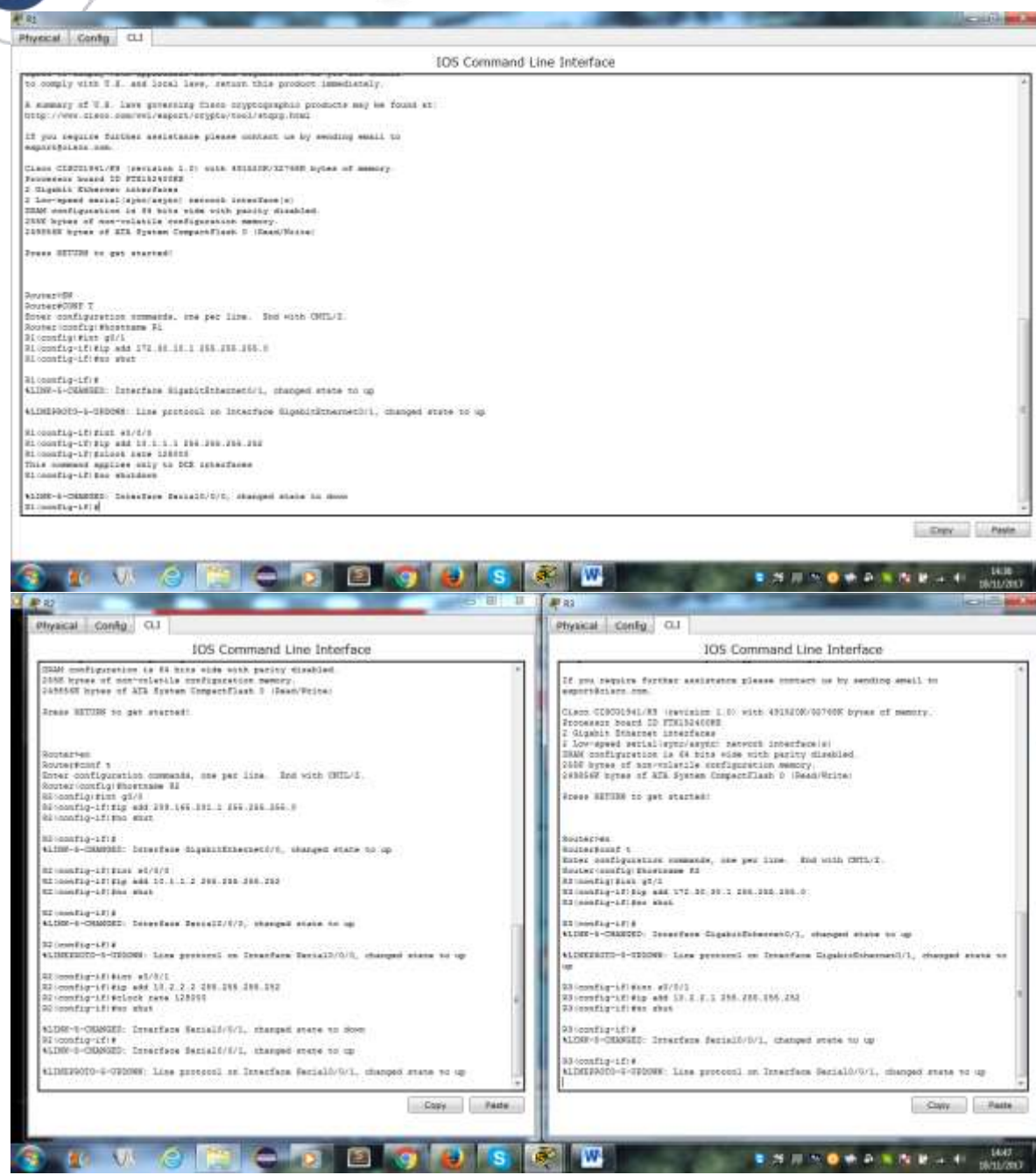
Paso 1. realizar el cableado de red tal como se muestra en la topología.

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



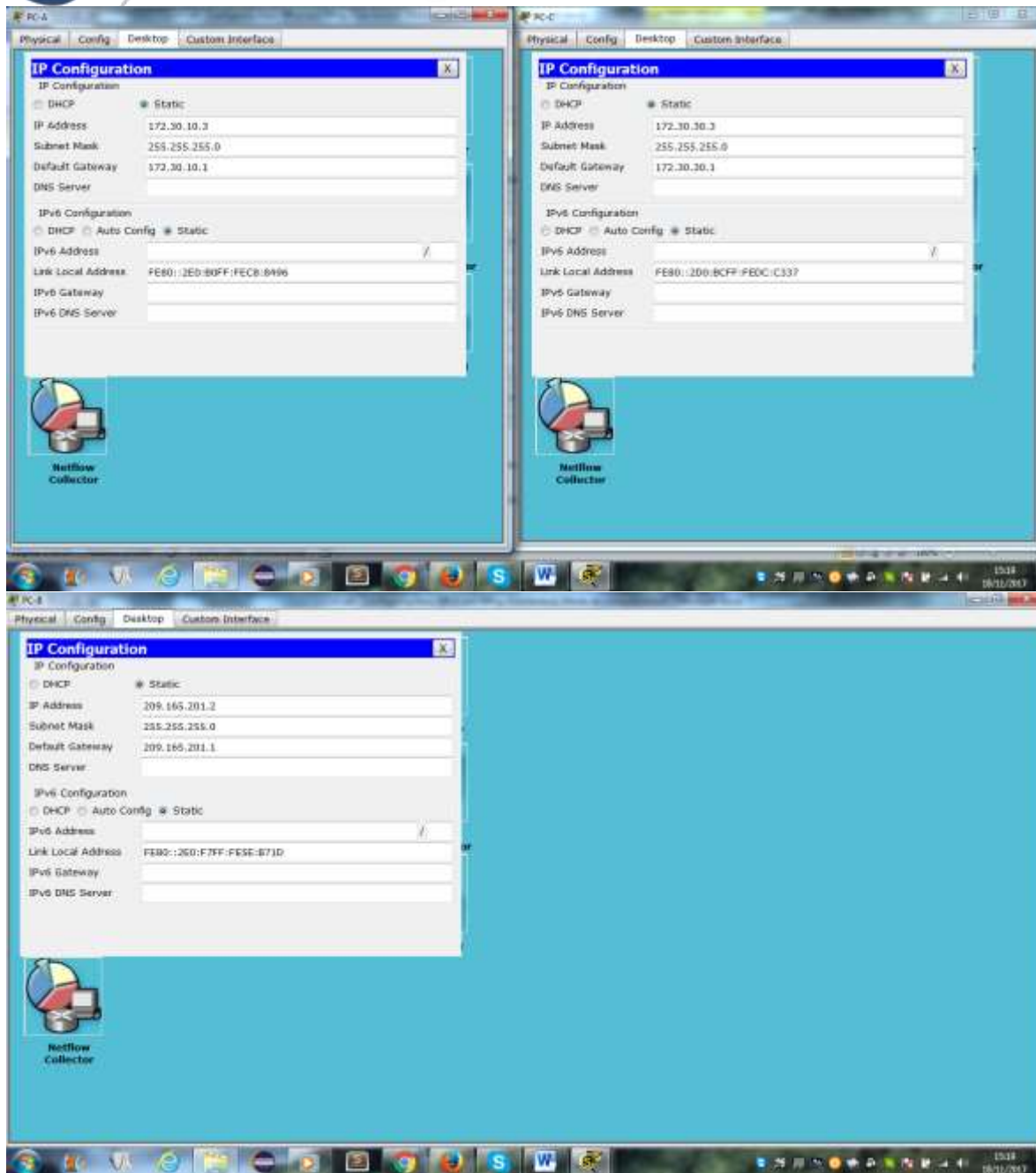
Paso 3. configurar los parámetros básicos para cada router y switch.

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



Paso 4. configurar los equipos host.

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



Paso 5. Probar la conectividad.

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

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

Parte 2: configurar y verificar el routing RIPv2

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

Paso 1. Configurar el enrutamiento RIPv2.

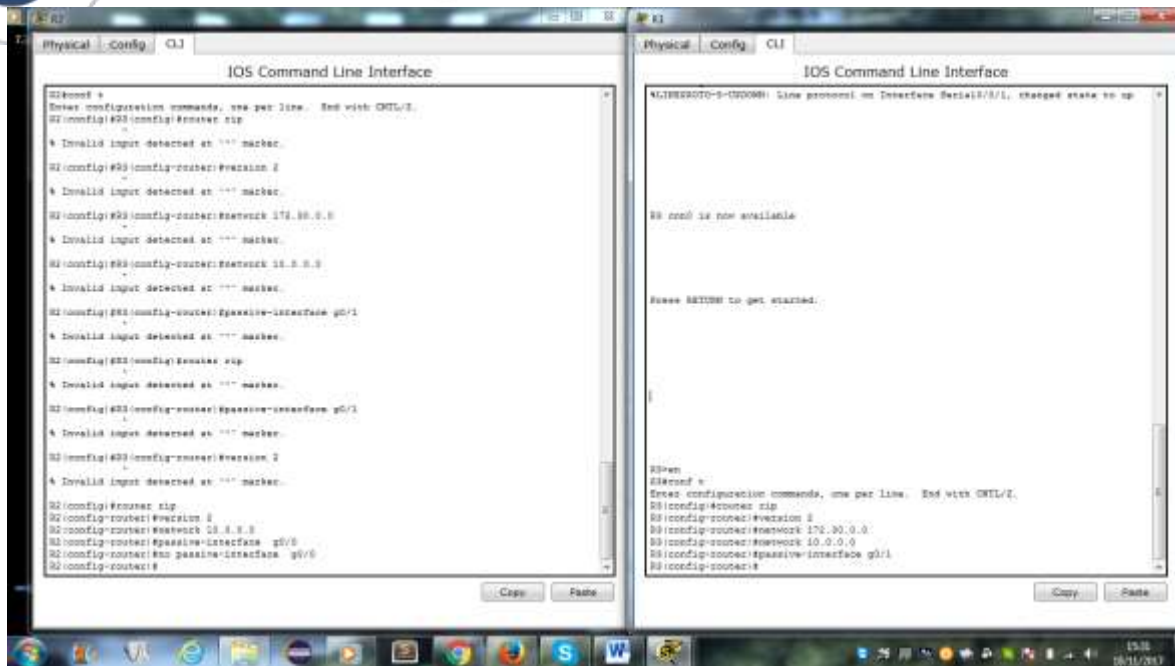
- c. En el R1, configure RIPv2 como el protocolo de routing y anuncie las redes correspondientes.



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

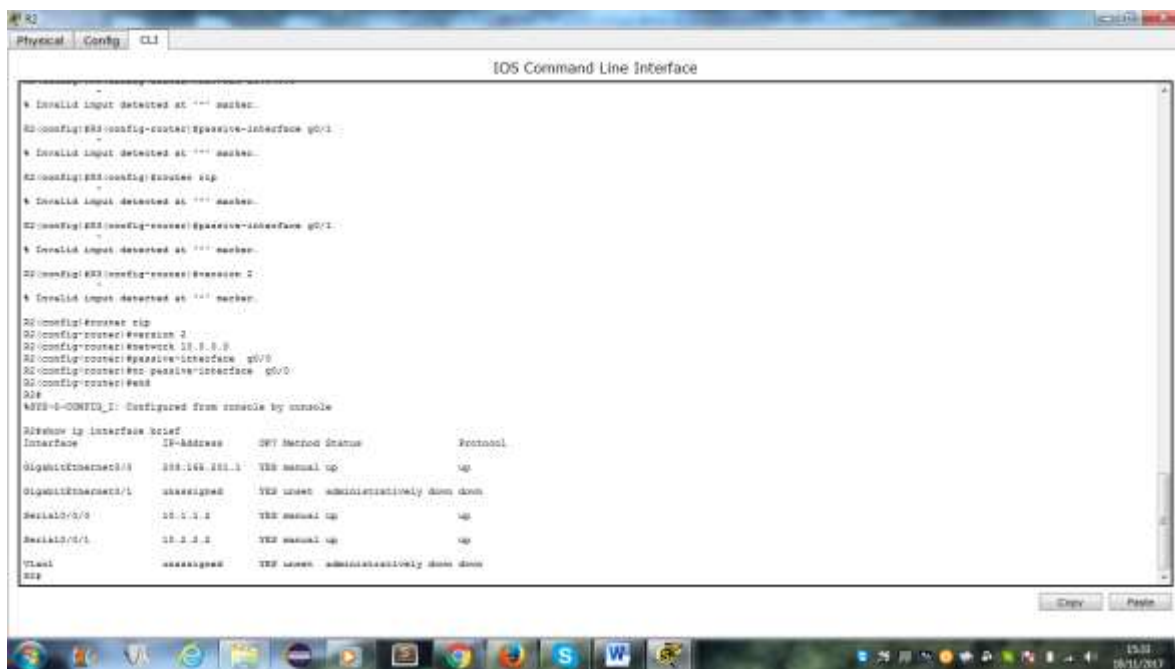
- d. Configure RIPv2 en el R3 y utilice la instrucción **network** para agregar las redes apropiadas y evitar actualizaciones de routing en la interfaz LAN.
- e. Configure RIPv2 en el R2. No anuncie la red 209.165.201.0.

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

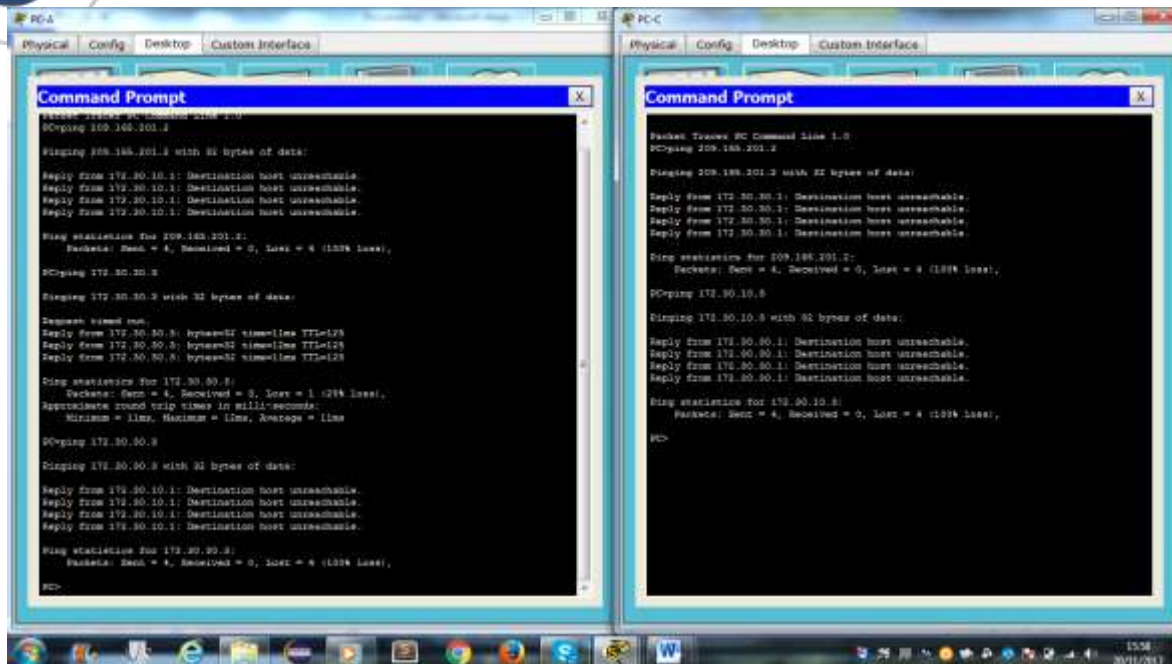


Paso 2. examinar el estado actual de la red.

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

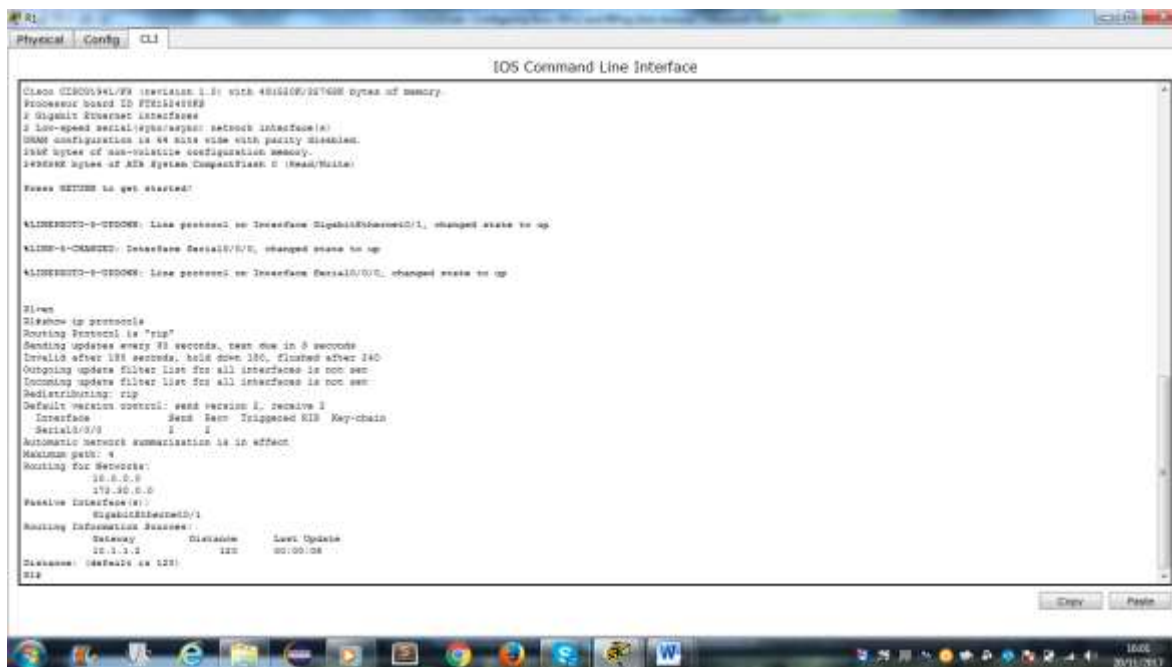


- b. Verifique la conectividad entre las computadoras.
 - ¿Es posible hacer ping de la PC-A a la PC-B? ¿Por qué?
 - ¿Es posible hacer ping de la PC-A a la PC-C? ¿Por qué?
 - ¿Es posible hacer ping de la PC-C a la PC-B? ¿Por qué?
 - ¿Es posible hacer ping de la PC-C a la PC-A? ¿Por qué?



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.

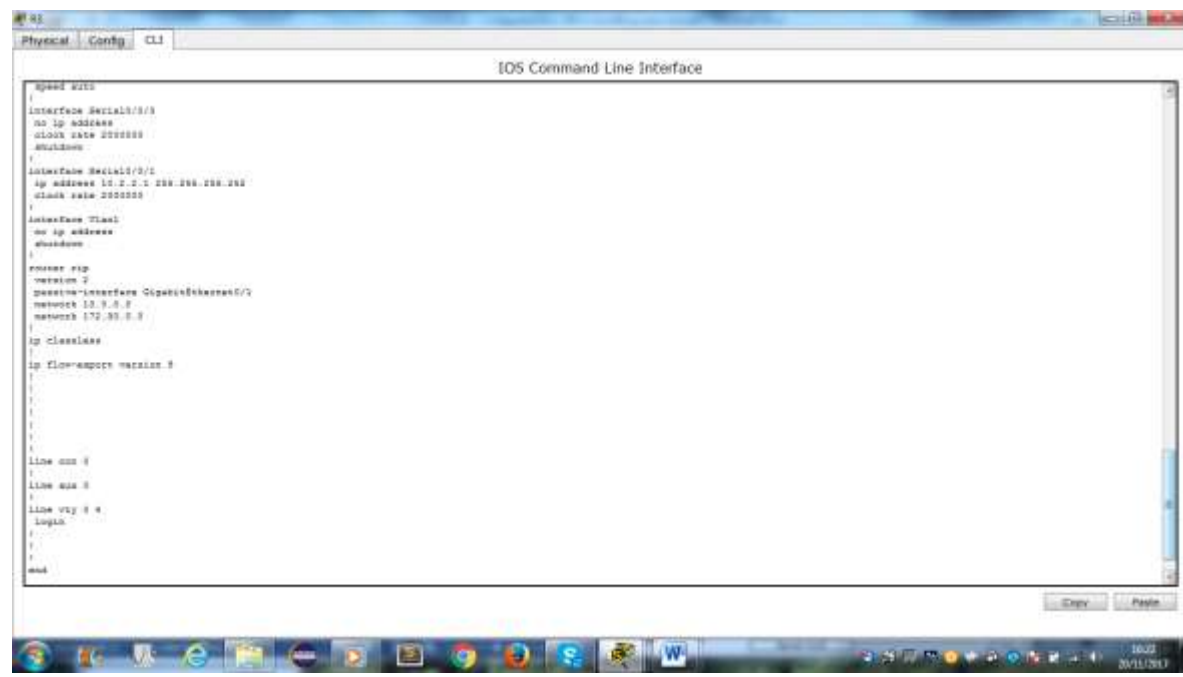


Al emitir el comando **debug ip rip** en el R2, ¿qué información se proporciona que confirma que RIPv2 está en ejecución?

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



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



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.

```

R3
Physical Config CLI
IOS Command Line Interface

R3# show ip route
R3:
IP: routing table entries
  10.1.1.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending v0 update to 224.0.0.0 via Serial0/0/0 (10.1.1.1)
RIP: build update entries
  10.2.0.0/24 via 0.0.0.0, metric 1, tag 0
RIP: received v0 update from 10.1.1.1 on Serial0/0/0
  172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v0 update from 10.1.1.1 on Serial0/0/1
  172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v0 update to 224.0.0.0 via Serial0/0/1 (10.1.1.1)
RIP: build update entries
  10.1.1.0/24 via 0.0.0.0, metric 0, tag 0
RIP: sending v0 update to 224.0.0.0 via Serial0/0/0 (10.1.1.1)
RIP: build update entries
  10.2.0.0/24 via 0.0.0.0, metric 1, tag 0
RIP: received v0 update from 10.1.1.1 on Serial0/0/0
  172.30.0.0/16 via 0.0.0.0 in 1 hops

RIPRouting all
All possible debugging has been turned off
RIPshow ip route
Codes: C - local, L - learned, D - static, E - EIGRP, H - mobile, N - NHRP
        O - OSPF, IA - OSPF interarea, 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, IS - IS-IS inter area
        * - candidate default, U - per-user static route, s - ODR
        ? - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.1.0/24 is directly connected, Serial0/0/0
L    10.1.1.0/24 is directly connected, Serial0/0/0
C    10.2.0.0/24 is directly connected, Serial0/0/1
L    10.2.0.0/24 is directly connected, Serial0/0/1
S    172.30.0.0/16 [100/0] via 10.1.1.1, 60:00:00, Serial0/0/1
      172.30.0.0/16 [100/0] via 10.1.1.1, 60:00:00, Serial0/0/0
C    209.148.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.148.201.0/24 is directly connected, GigabitEthernet0/0
L    209.148.201.0/24 is directly connected, GigabitEthernet0/0
R3#
  
```

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
Physical Config CLI
IOS Command Line Interface

R1 oodl is not available

Please RETURN to get started.

R1# show ip route
Codes: C - local, L - learned, D - static, R - RIP, H - mobile, S - BGP
        O - OSPF, IA - OSPF interarea, 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, IS - IS-IS inter area
        * - candidate default, U - per-user static route, s - ODR
        ? - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/24 is directly connected, Serial0/0/0
L    10.1.1.0/24 is directly connected, Serial0/0/0
S    172.30.0.0/16 [100/0] via 10.1.1.2, 60:00:00, Serial0/0/0
C    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.0/24 is directly connected, GigabitEthernet0/1
R1#
  
```

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

Paso 3. Desactivar la sumarización automática.

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

```

R1#
Physical Config CLI
IOS Command Line Interface

R1#show ip route
Codes: 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, S - BGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, Ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
C    10.1.1.0/24 is directly connected, Serial0/0/0
L    10.1.1.0/24 is directly connected, Serial0/0/0
S    10.2.2.0/24 [120/1] via 10.1.1.1, 00:00:18, Serial0/0/0
L    172.22.22.0/24 is variably subnetted, 3 subnets, 3 masks
C    172.22.22.0/24 is directly connected, GigabitEthernet0/1
L    172.22.22.0/24 is directly connected, GigabitEthernet0/1
RIP:
RIP-1-CONFID_2: Configured from console by console
R1#clear ip route *
R1#
  
```

- g. 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#
Physical Config CLI
IOS Command Line Interface

R2#show ip route
* Invalid input detected at '^' marker.
R2#show ip route
RIP
RIP-1-CONFID_1: Configured from console by console
R2#clear ip route *
R2#show ip route
Codes: 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, S - BGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, Ia - IS-IS inter area
       * - Candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C    10.1.1.0/24 is directly connected, Serial0/0/0
L    10.1.1.0/24 is directly connected, Serial0/0/0
C    10.2.2.0/24 is directly connected, Serial0/0/1
L    10.2.2.0/24 is directly connected, Serial0/0/1
L    172.22.22.0/24 is variably subnetted, 3 subnets, 3 masks
S    172.22.22.0/24 [120/1] via 10.2.2.1, 00:00:10, Serial0/0/1
L    172.22.22.0/24 [120/1] via 10.1.1.1, 00:00:13, Serial0/0/1
S    172.22.22.0/24 [120/1] via 10.2.2.1, 00:00:14, Serial0/0/1
S    228.188.201.0/24 is variably subnetted, 3 subnets, 3 masks
C    228.188.201.0/24 is directly connected, GigabitEthernet0/0
L    228.188.201.0/24 is directly connected, GigabitEthernet0/0
R2#
  
```

R1# **show ip route**

```

R1
Physical Config CLI
IOS Command Line Interface

Please RETURN to get started.

R1>
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, H - 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, S - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, Ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C    10.1.1.0/24 is directly connected, Serial0/0/0
L    10.1.1.0/24 is directly connected, Serial0/0/0
S    10.0.0.0/8 [100/0] via 10.1.1.1, 00:00:10, Serial0/0/0
R    172.22.0.0/24 [120/2] via 10.1.1.2, 00:00:10, Serial0/0/0
C    172.22.10.0/24 is directly connected, GigabitEthernet0/1
L    172.22.10.0/24 is directly connected, GigabitEthernet0/1
S    172.22.0.0/24 [120/2] via 10.1.1.2, 00:00:10, Serial0/0/0
R1#
    
```

R3# show ip route

```

R3
Physical Config CLI
IOS Command Line Interface

R3>
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, H - 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, S - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, Ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
R    10.1.1.0/24 [120/1] via 10.0.0.2, 00:00:10, Serial0/0/1
C    10.0.0.0/8 is directly connected, Serial0/0/1
L    10.0.0.0/8 is directly connected, Serial0/0/1
R    172.22.0.0/24 [120/2] via 10.0.0.2, 00:00:10, Serial0/0/1
C    172.22.10.0/24 is directly connected, GigabitEthernet0/1
L    172.22.10.0/24 is directly connected, GigabitEthernet0/1
R3#
    
```

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

R2# debug ip rip

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

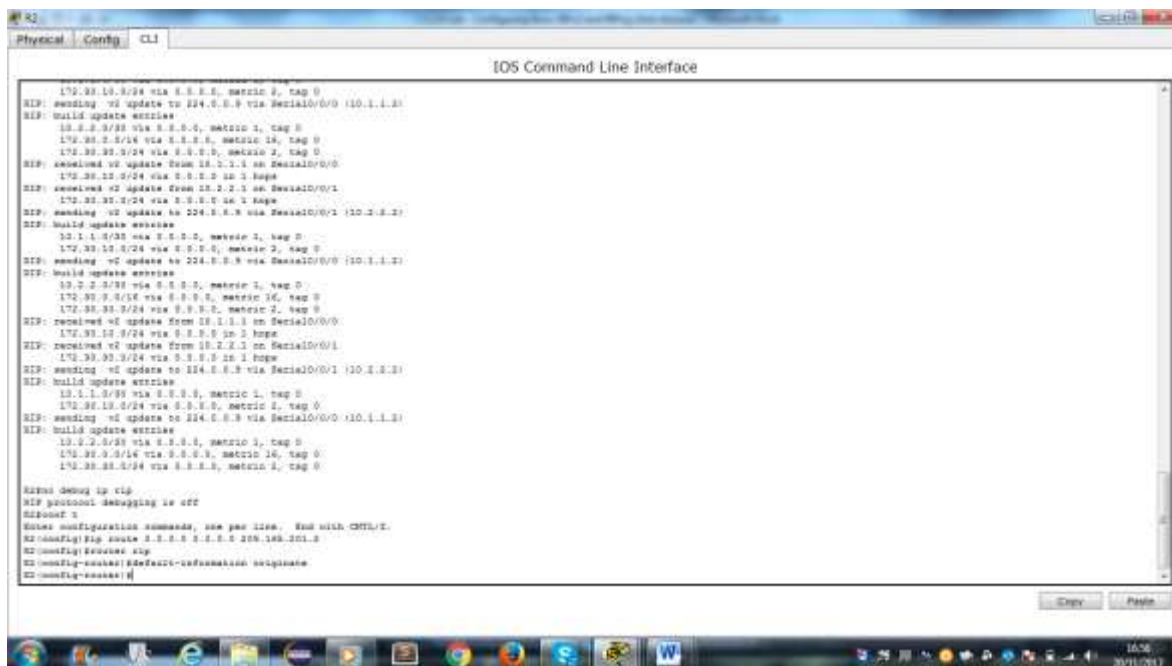
¿Qué rutas que se reciben del R3 se encuentran en las actualizaciones RIP?

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



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

- i. Desde el R2, cree una ruta estática a la red 0.0.0.0 0.0.0.0, con el comando **ip route**. Esto envía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet al establecer un gateway de último recurso en el router R2.
- j. El R2 anunciará una ruta a los otros routers si se agrega el comando **default-information originate** a la configuración de RIP.



Paso 5. Verificar la configuración de enrutamiento.

- k. Consulte la 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?

```

R1
Physical Config CLI
IOS Command Line Interface

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

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C    10.1.1.0/24 is directly connected, Serial0/0/0
L    10.1.1.0/24 is directly connected, Serial0/0/0
S    10.0.0.0/8 [120/0] via 10.1.1.1, 00:00:10, Serial0/0/0

172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
S    172.16.0.0/16 [120/0] via 10.1.1.1, 00:00:10, Serial0/0/0
C    172.16.10.0/24 is directly connected, GigabitEthernet0/1
L    172.16.10.0/24 is directly connected, GigabitEthernet0/1
S    172.16.0.0/24 [120/0] via 10.1.1.1, 00:00:10, Serial0/0/0

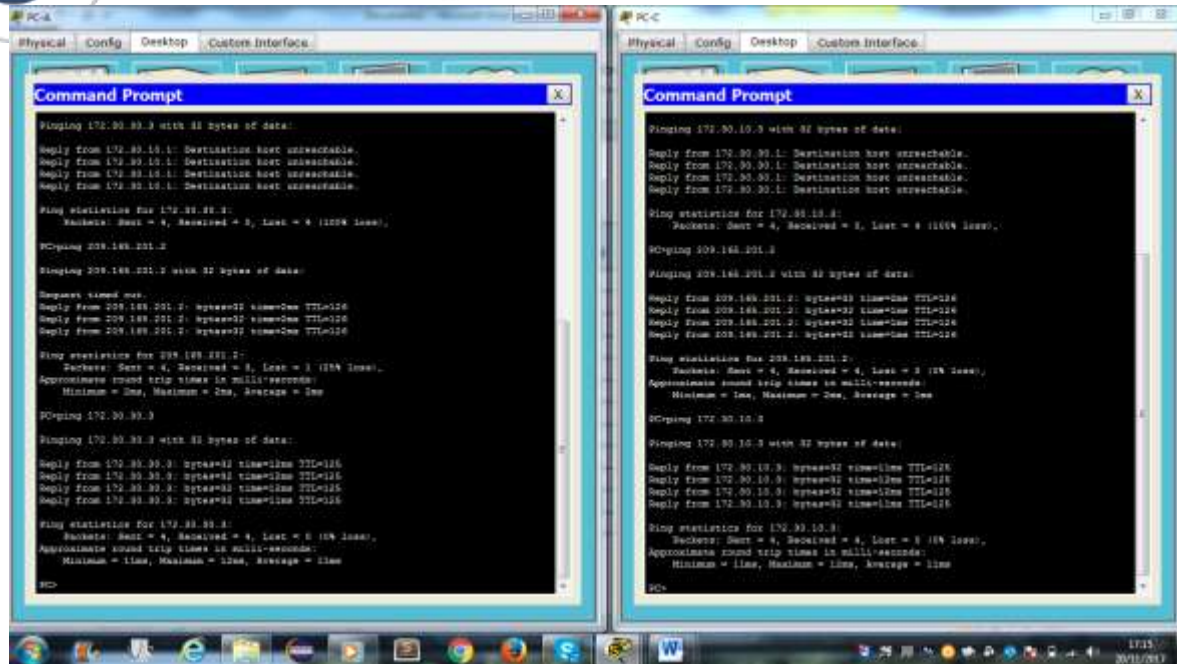
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       S - EIGRP, EX - EIGRP external, D - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
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

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C    10.1.1.0/24 is directly connected, Serial0/0/0
L    10.1.1.0/24 is directly connected, Serial0/0/0
S    10.0.0.0/8 [120/0] via 10.1.1.1, 00:00:06, Serial0/0/0

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.16.10.0/24 is directly connected, GigabitEthernet0/1
L    172.16.10.0/24 is directly connected, GigabitEthernet0/1
S    172.16.0.0/16 [120/0] via 10.1.1.1, 00:00:06, Serial0/0/0
S*  0.0.0.0/0 [120/0] via 10.1.1.1, 00:00:06, Serial0/0/0

R1#
    
```

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

Parte 3: configurar IPv6 en los dispositivos

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

Tabla de direccionamiento

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

Paso 1. configurar los equipos host.

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

Paso 2. configurar IPv6 en los routers.

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

- c. Para cada interfaz del router, asigne la dirección global y la dirección link local de la tabla de direccionamiento.
- d. Habilite el routing IPv6 en cada router.
- e. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.
- f. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.
- g. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

The image displays three sequential screenshots of an IOS Command Line Interface (CLI) window, showing the configuration of a network device. Each window has a title bar with 'Physical', 'Config', and 'CLI' tabs. The first two windows show the initial state and the beginning of configuration, while the third shows the completion of the configuration.

Window 1 (Top Left): Shows the initial CLI prompt and the start of configuration. The text is as follows:

```
IOS Command Line Interface

E1 con0 is now available.

Press RETURN to get started.

...

E1>en
E1>conf t
Enter configuration commands, one per line. End with CTRL/Z.
E1(config)#int g0/1
E1(config-if)#ipw add 2001:DB8:ACAD:A::1/64
E1(config-if)#ipw add FE80::1 link-local
E1(config-if)#
^ Invalid input detected at '^' marker.
E1(config-if)#ipw add 2001:DB8:ACAD:A::1/64
E1(config-if)#ipw add FE80::1 link-local
E1(config-if)#int g0/0/0
E1(config-if)#ipw add 2001:DB8:ACAD:11::1/64
E1(config-if)#ipw add FE80::1 link-local
E1(config-if)#
```

Window 2 (Top Right): Shows the continuation of configuration. The text is as follows:

```
IOS Command Line Interface

E1 con0 is now available.

Press RETURN to get started.

...

E1>en
E1>conf t
Enter configuration commands, one per line. End with CTRL/Z.
E1(config)#int g0/0
E1(config-if)#ipw add 2001:DB8:ACAD:8::2/64
E1(config-if)#int g0/0/0
E1(config-if)#ipw add 2001:DB8:ACAD:12::2/64
E1(config-if)#ipw add FE80::2 link-local
E1(config-if)#int g0/0/1
E1(config-if)#ipw add 2001:DB8:ACAD:23::2/64
E1(config-if)#ipw add FE80::2 link-local
E1(config-if)#
```

Window 3 (Bottom): Shows the completion of configuration. The text is as follows:

```
IOS Command Line Interface

E1 con0 is now available.

Press RETURN to get started.

...

E1>en
E1>conf t
Enter configuration commands, one per line. End with CTRL/Z.
E1(config)#int g0/1
E1(config-if)#ipw add 2001:DB8:ACAD:11::1/64
E1(config-if)#ipw add FE80::1 link-local
E1(config-if)#
^ Invalid input detected at '^' marker.
E1(config-if)#ipw add FE80::1 link-local
E1(config-if)#int g0/0/1
E1(config-if)#ipw add 2001:DB8:ACAD:23::2/64
E1(config-if)#ipw add FE80::2 link-local
E1(config-if)#
```

The image displays three screenshots of a network configuration interface, likely from a virtualization software like VMware Workstation. Each screenshot shows the configuration for a different PC (PC-A, PC-B, and PC-C) under the 'Custom Interface' tab. The interface includes sections for IP Configuration and IPv6 Configuration, with fields for IP Address, Subnet Mask, Default Gateway, DNS Server, IPv6 Address, Link Local Address, IPv6 Gateway, and IPv6 DNS Server. A 'Netflow Collector' icon is visible on the desktop of each PC.

PC-A Configuration:

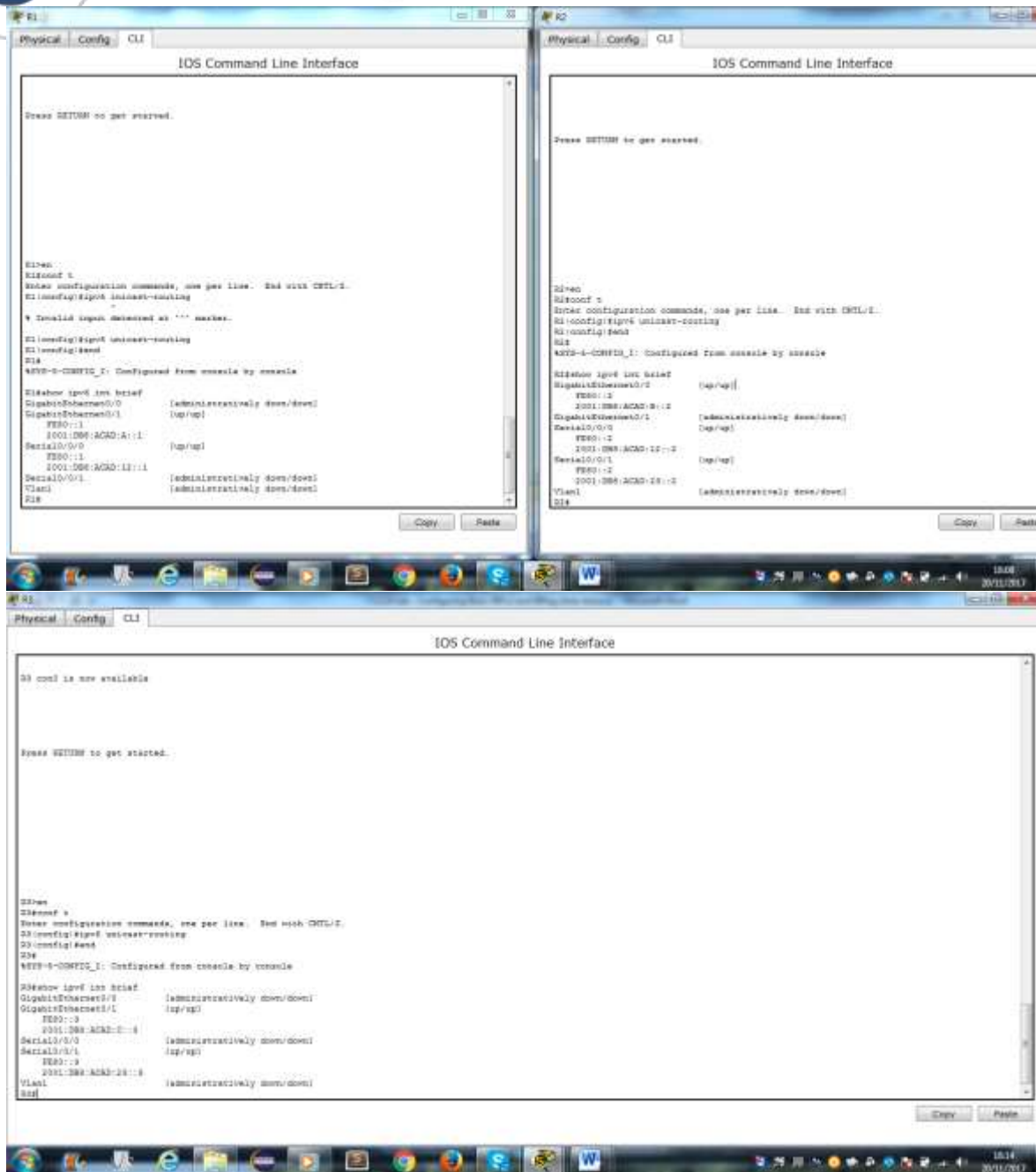
- IP Configuration: DHCP (Static), IP Address: 209.185.201.2, Subnet Mask: 255.255.255.0, Default Gateway: 209.185.201.1, DNS Server: [Empty]
- IPv6 Configuration: DHCP (Static), IPv6 Address: 2001:DB8:ACAD:B::B / 64, Link Local Address: FE80::2E0:F7FF:FE5E-B71D, IPv6 Gateway: FE80::2, IPv6 DNS Server: [Empty]

PC-B Configuration:

- IP Configuration: DHCP (Static), IP Address: 172.30.30.3, Subnet Mask: 255.255.255.0, Default Gateway: 172.30.30.1, DNS Server: [Empty]
- IPv6 Configuration: DHCP (Static), IPv6 Address: 2001:DB8:ACAD:C::C / 64, Link Local Address: FE80::2D0:BCFF:FE0C:C337, IPv6 Gateway: FE80::3, IPv6 DNS Server: [Empty]

PC-C Configuration:

- IP Configuration: DHCP (Static), IP Address: 172.30.10.3, Subnet Mask: 255.255.255.0, Default Gateway: 172.30.10.1, DNS Server: [Empty]
- IPv6 Configuration: DHCP (Static), IPv6 Address: 2001:DB8:ACAD:A::A / 64, Link Local Address: FE80::2E0:92FF:FE08:9496, IPv6 Gateway: FE80::1, IPv6 DNS Server: [Empty]



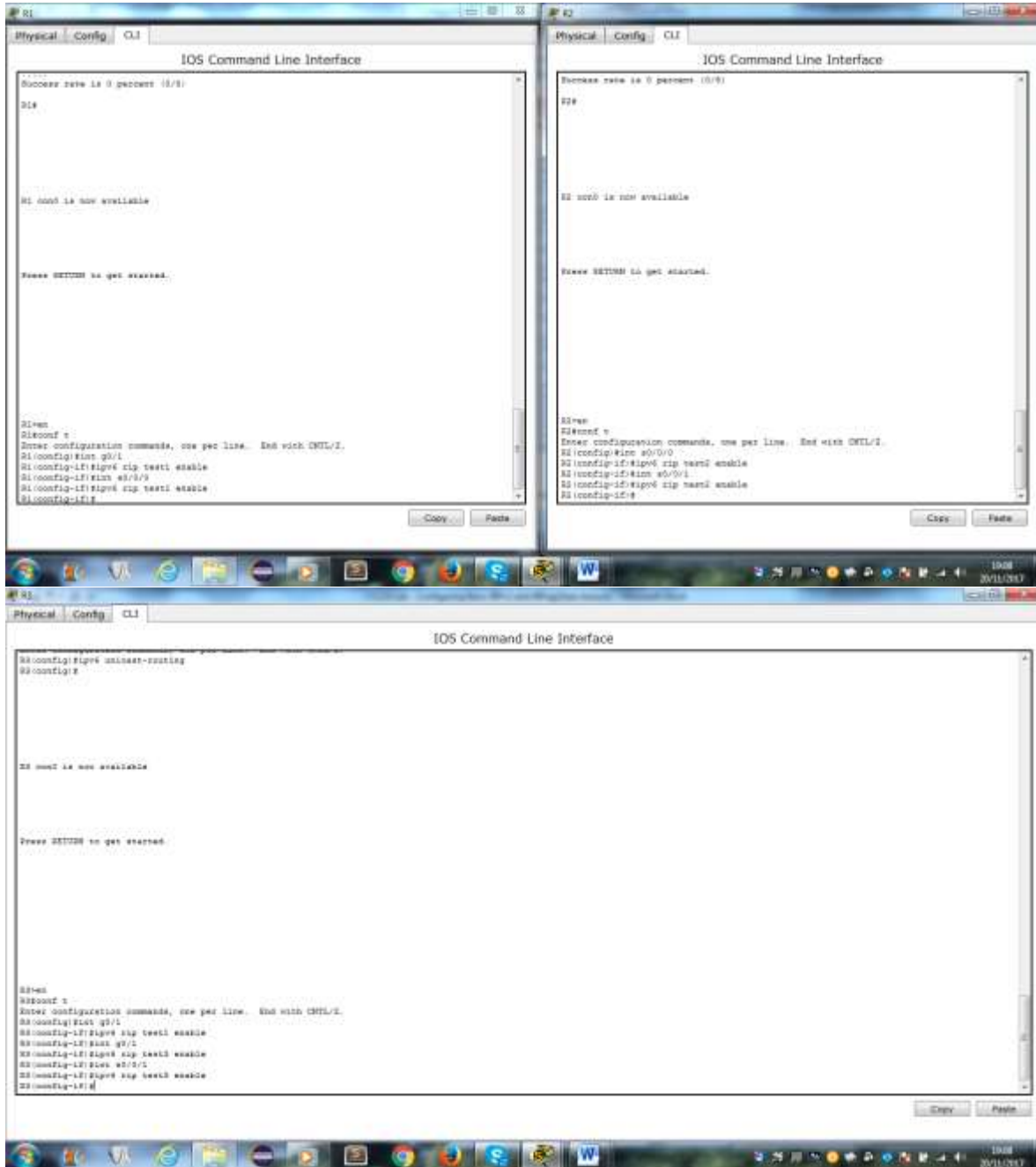
Parte 4: configurar y verificar el routing RIPng

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

Paso 1. configurar el routing RIPng.

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

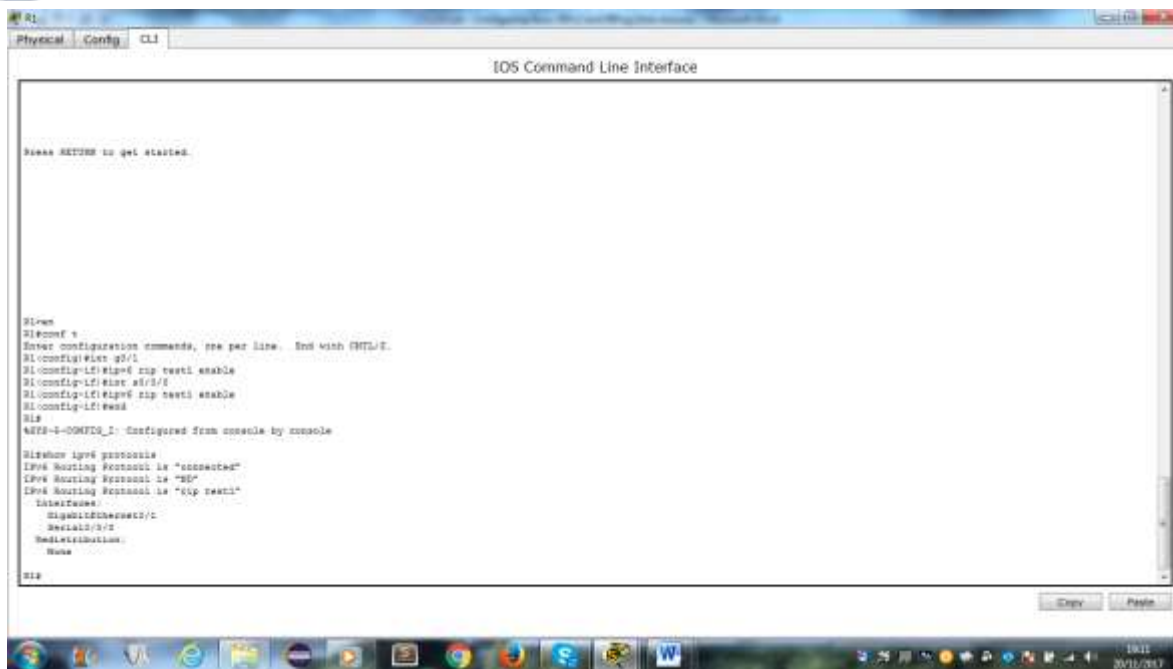
- h. Emita el comando **ipv6 rip Test1 enable** para cada interfaz en el R1 que participará en el routing RIPng, donde **Test1** es el nombre de proceso pertinente en el nivel local.
- i. Configure RIPng para las interfaces seriales en el R2, con **Test2** como el nombre de proceso. No lo configure para la interfaz G0/0
- j. Configure RIPng para cada interfaz en el R3, con **Test3** como el nombre de proceso.



- k. Verifique que RIPng se esté ejecutando en los routers.

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

¿En qué forma se indica RIPng en el resultado?



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

```

R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 314
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 1, trigger updates 0
  Full Advertisement 0, Delayed Events 0
Interfaces:
  GigabitEthernet0/1
  Serial0/0/0
Redistribution:
  None
    
```

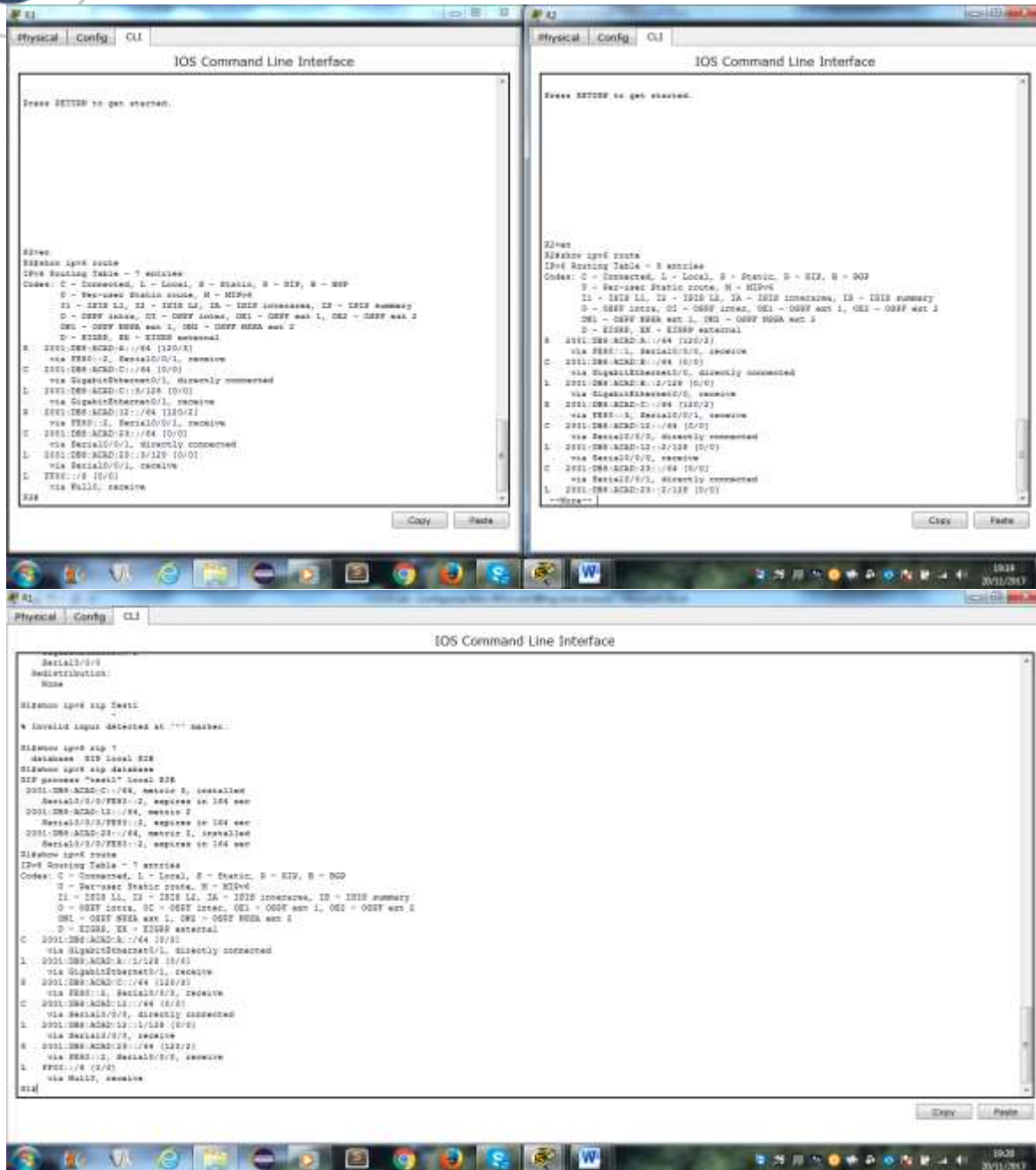
¿Cuáles son las similitudes entre RIPv2 y RIPng?

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

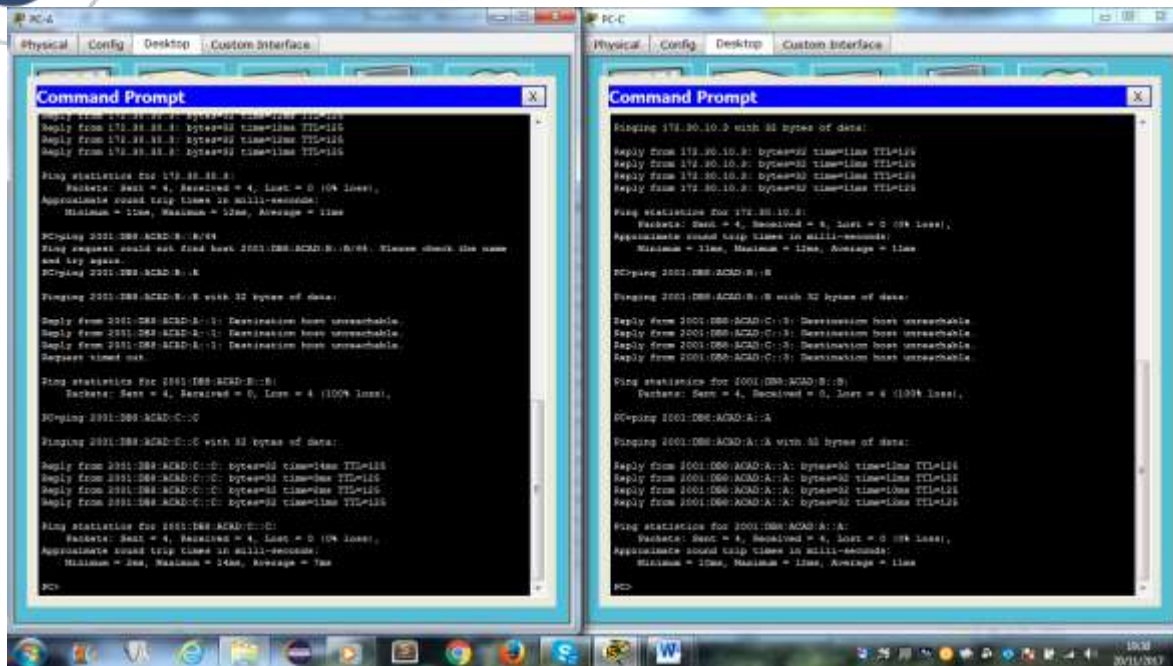
En el R1, ¿cuántas rutas se descubrieron mediante RIPng?

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

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



- n. Verifique la conectividad entre las computadoras.
- ¿Es posible hacer ping de la PC-A a la PC-B?
- ¿Es posible hacer ping de la PC-A a la PC-C?
- ¿Es posible hacer ping de la PC-C a la PC-B?
- ¿Es posible hacer ping de la PC-C a la PC-A?



¿Por qué algunos pings tuvieron éxito y otros no?

Porque no hay una ruta que se notifique para la PC-B para esa red

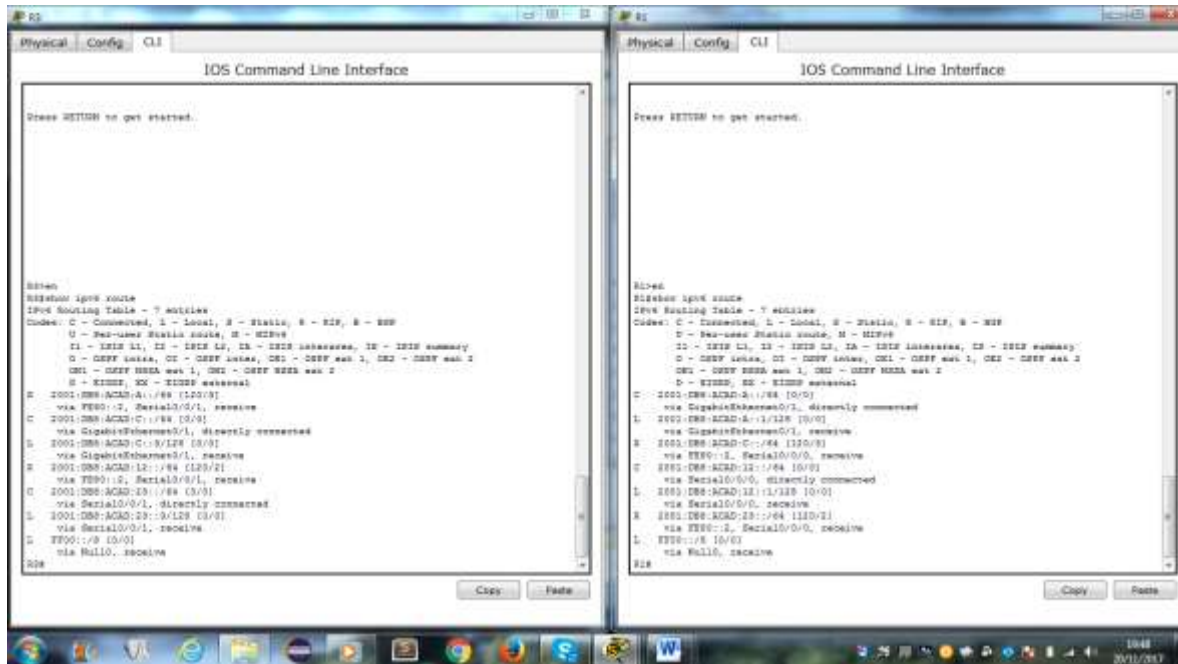
Paso 2. configurar y volver a distribuir una ruta predeterminada.

- 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.



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

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



Paso 4. Verifique la conectividad.

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

¿Tuvieron éxito los pings?

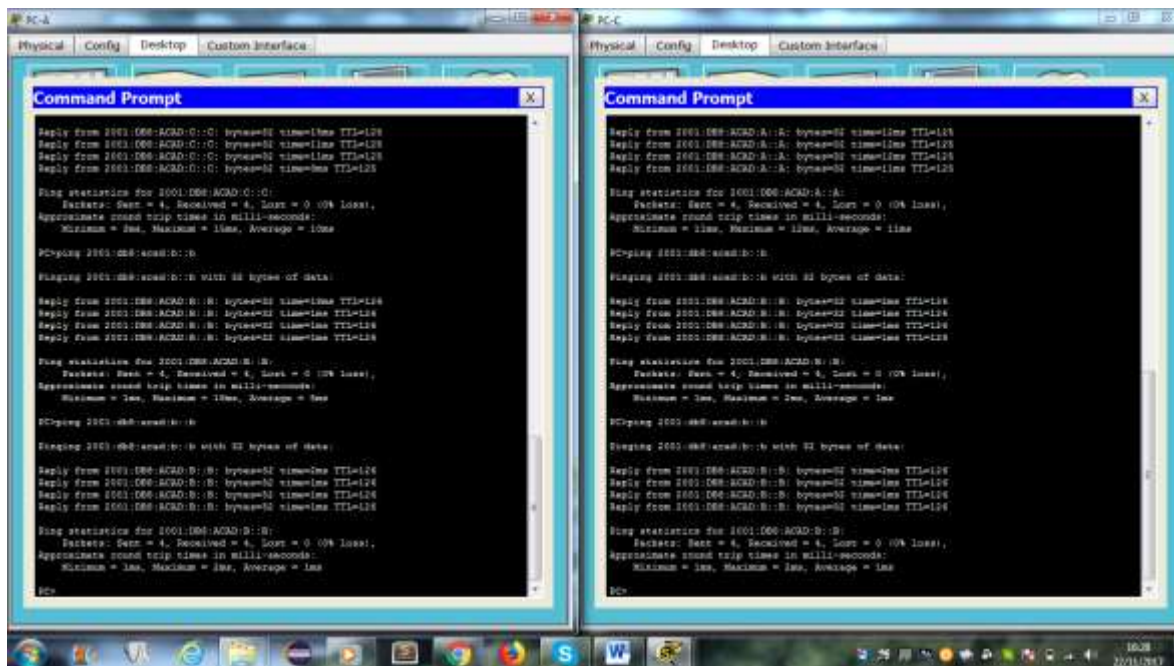


Tabla de resumen de interfaces del router

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

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

8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2 (Jhon James Gomes)

Topología

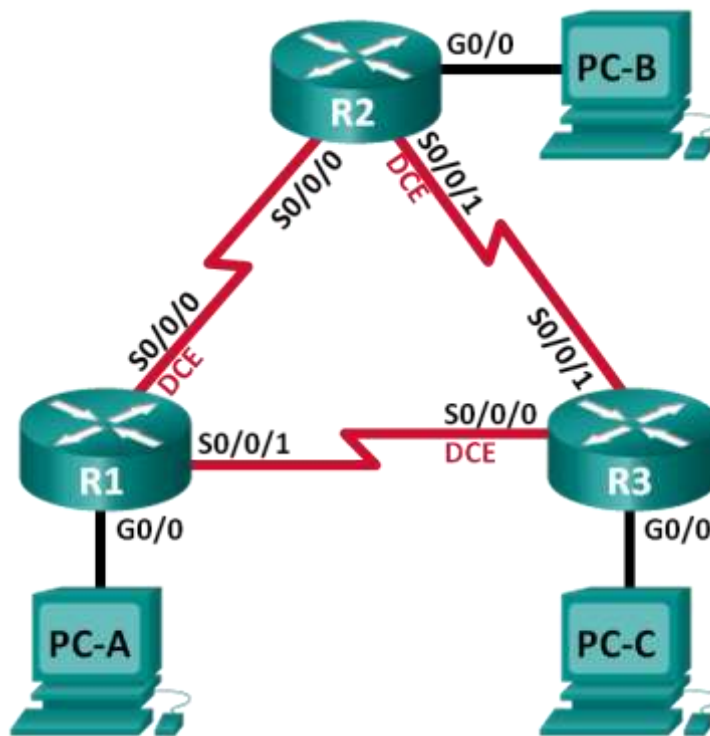


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPF

Parte 3: cambiar las asignaciones de ID del router

Parte 4: configurar interfaces OSPF pasivas

Parte 5: cambiar las métricas de OSPF

Información básica/situación

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

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

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

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

Recursos necesarios

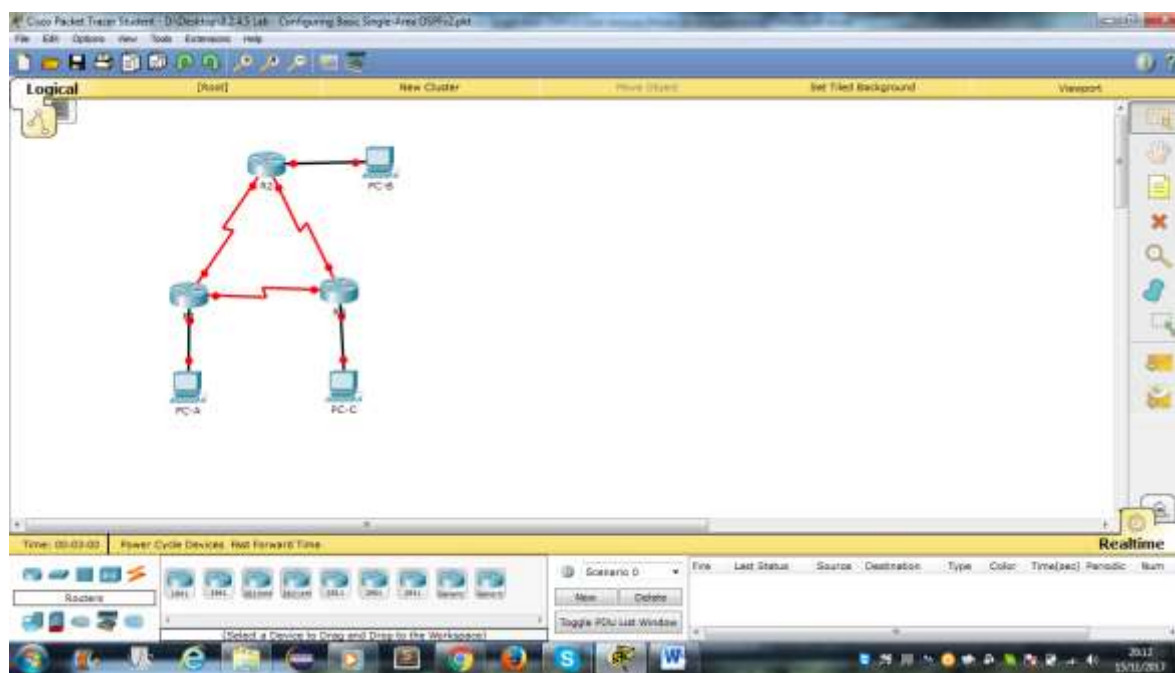
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet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

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

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

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

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

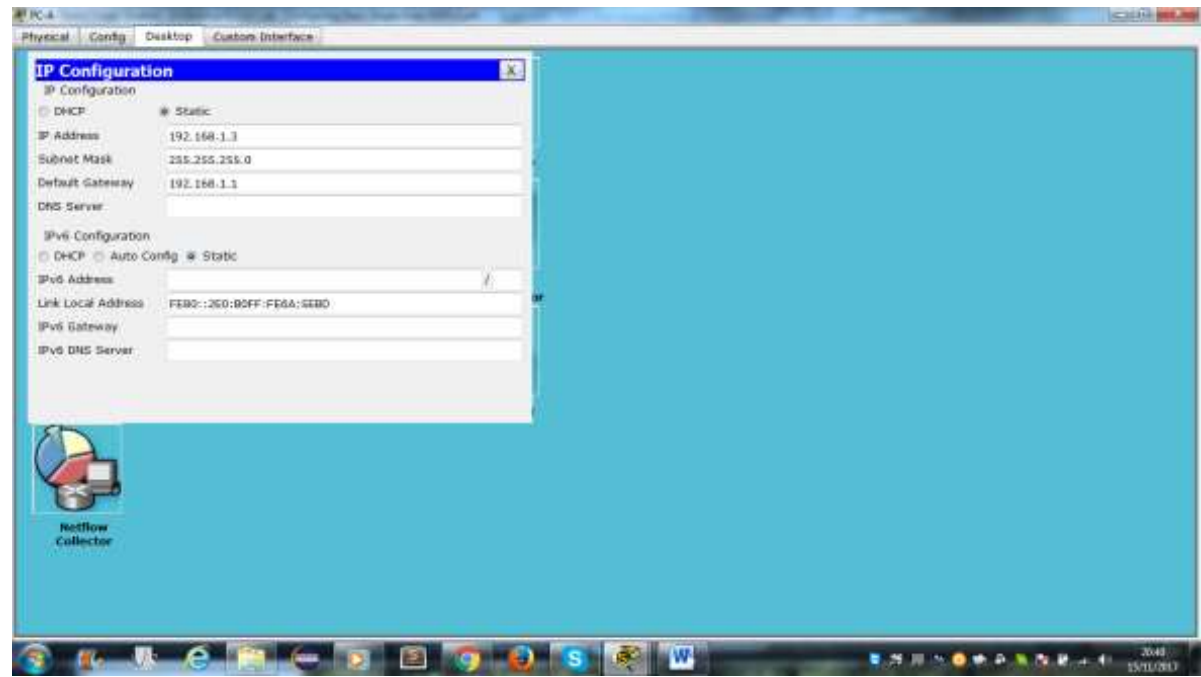
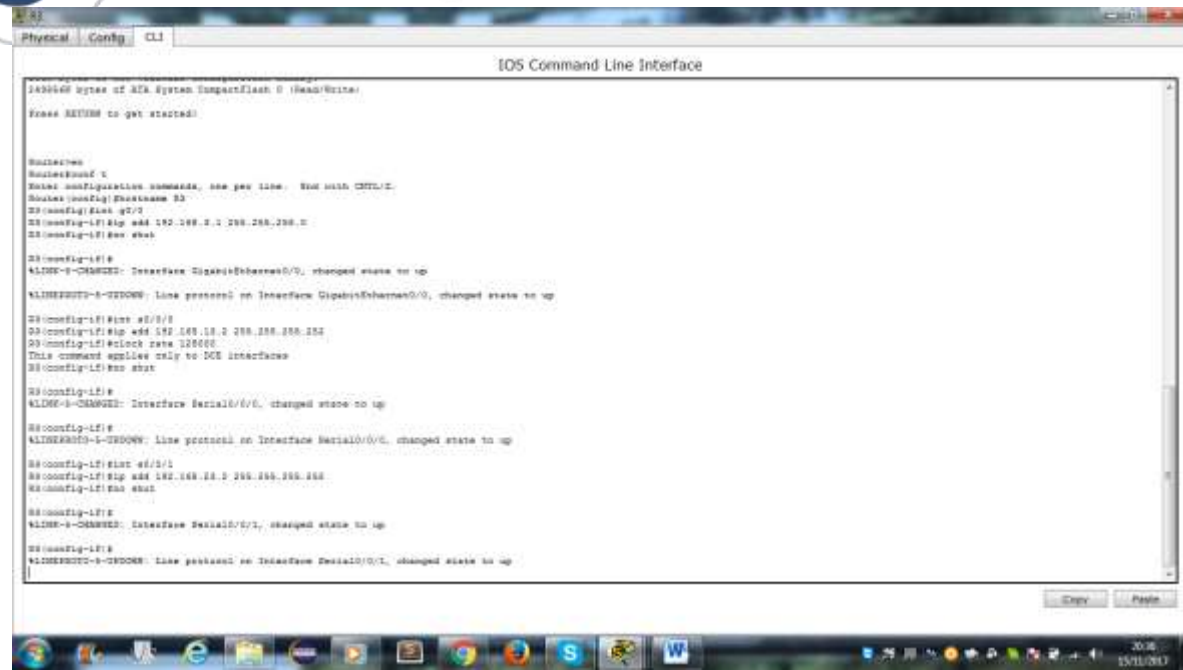


Paso 3. configurar los parámetros básicos para cada router.

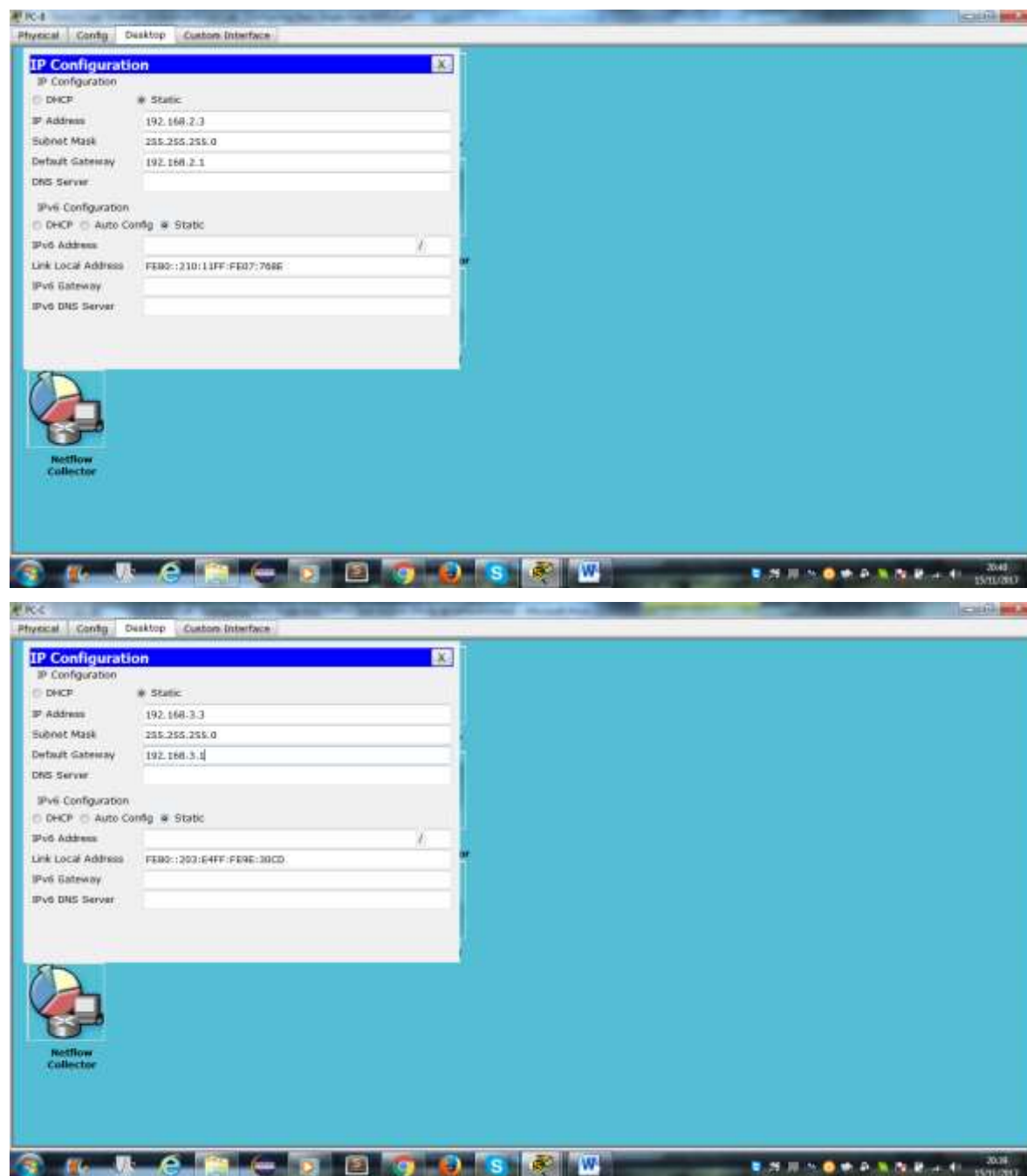
- Desactive la búsqueda del DNS.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **class** como la contraseña del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.
- Configure **logging synchronous** para la línea de consola.
- Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- 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 3. Configurar y verificar el enrutamiento OSPF

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

Paso 1. Configure el protocolo OSPF en R1.

- 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.

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

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

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

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

```
R1
Physical Config CLI
IOS Command Line Interface

ALINK0-0-CRDOWN: Interface Serial1/0/1, changed state to up
ALINK100-0-CRDOWN: Line protocol on Interface Serial10/0/1, changed state to up

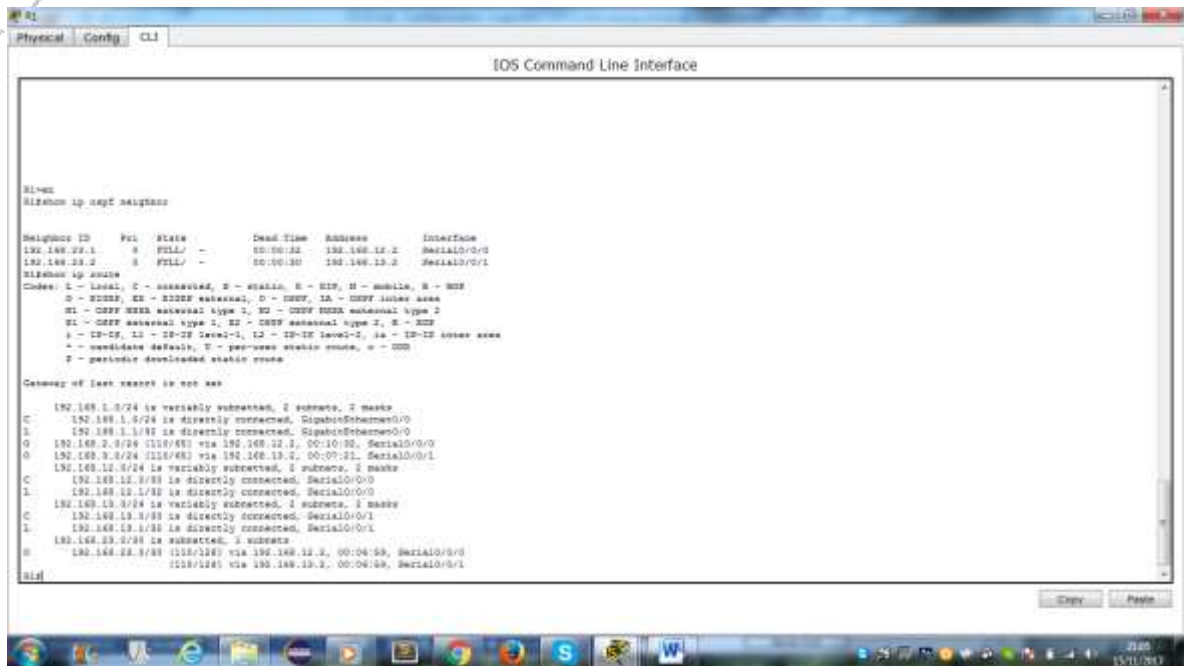
R1#ping 192.168.2.1
Type escape sequence to abort...
Sending 5, 150-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#ping 192.168.2.1
Type escape sequence to abort...
Sending 5, 150-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#
Enter configuration commands, one per line. End with CTRL-Z
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#
R1(config-router)#network 192.168.12.0 0.0.0.3 area 0
R1(config-router)#network 192.168.13.0 0.0.0.3 area 0
R1(config-router)#
```

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

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.

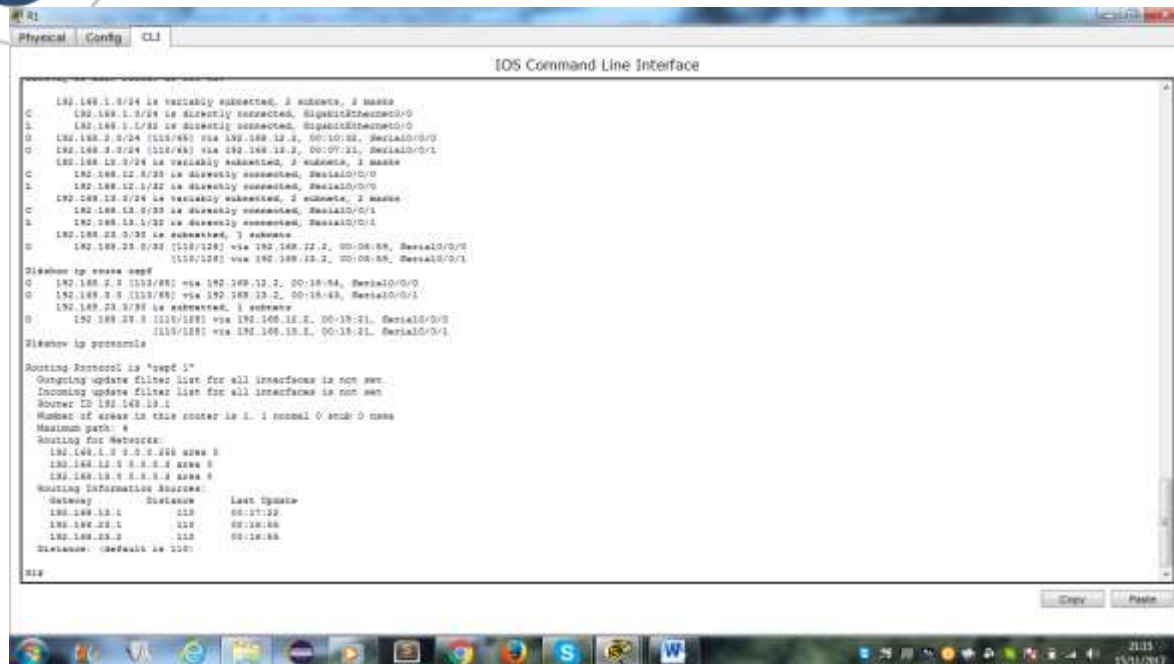


¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?



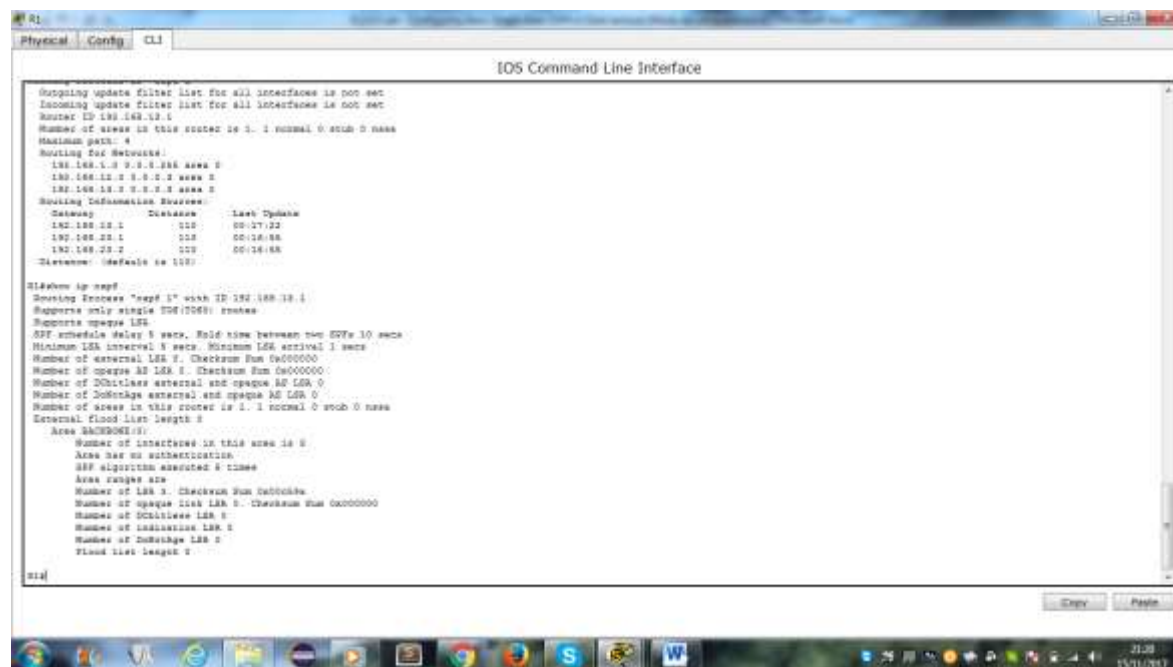
Paso 4. verificar la configuración del protocolo OSPF.

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



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.



Paso 6. verificar la configuración de la interfaz OSPF.

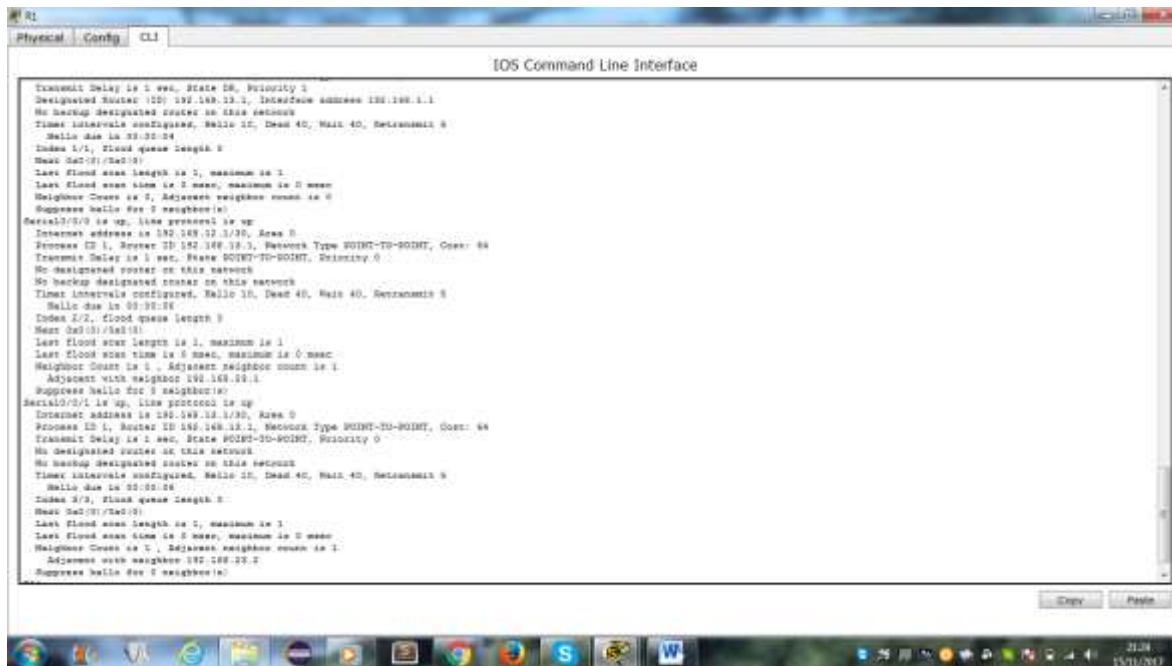
- Emita el comando **show ip ospf interface brief** para ver un resumen de las interfaces con OSPF habilitado.

R1# **show ip ospf interface brief**

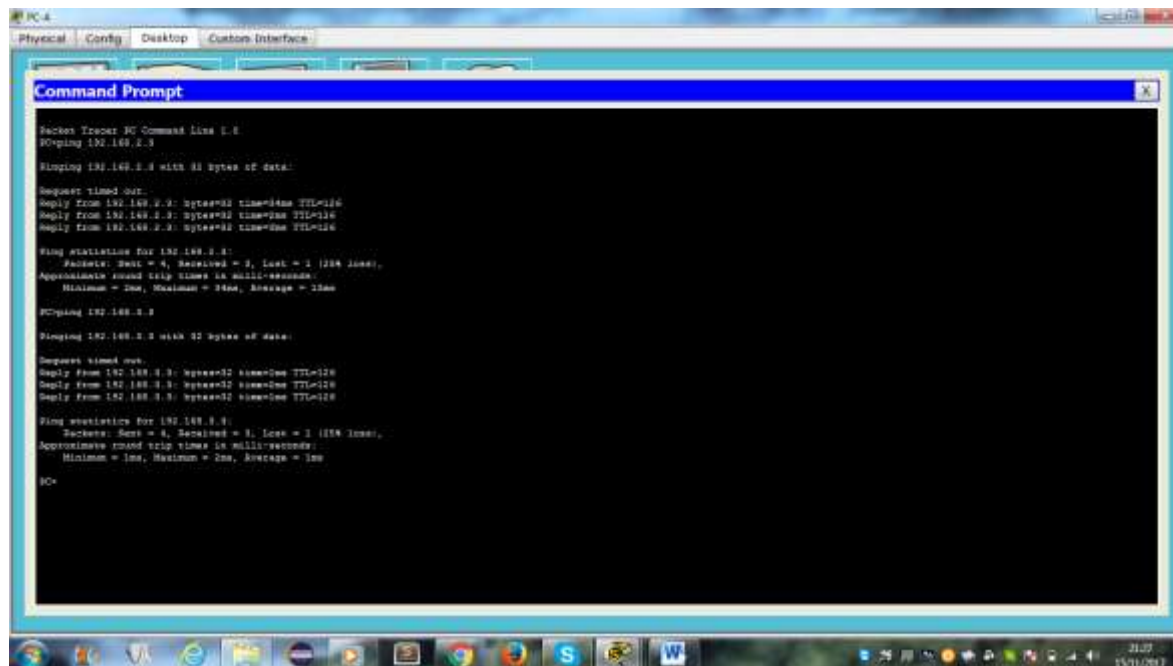
Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
-----------	-----	------	-----------------	------	-------	------	-----

Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	64	P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0

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



Paso 7. Verificar la conectividad de extremo a extremo.



Parte 4. cambiar las asignaciones de ID del router

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

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

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

En la parte 3, cambiará la asignación de ID 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.

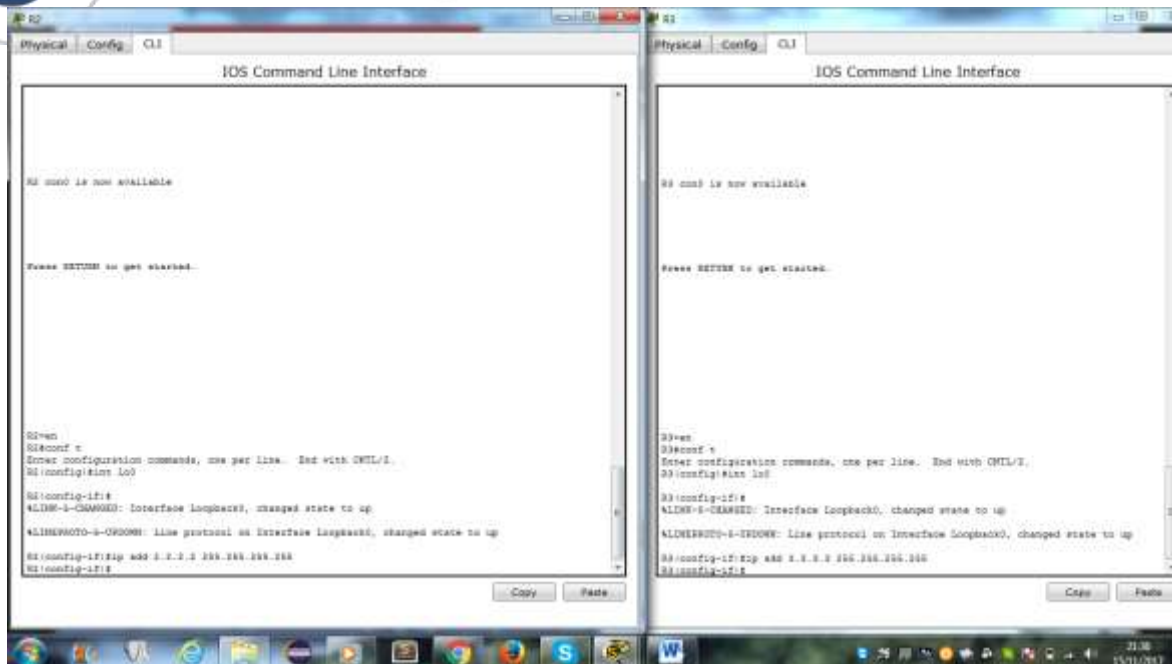
- a. Asigne una dirección IP al loopback 0 en el R1.

```

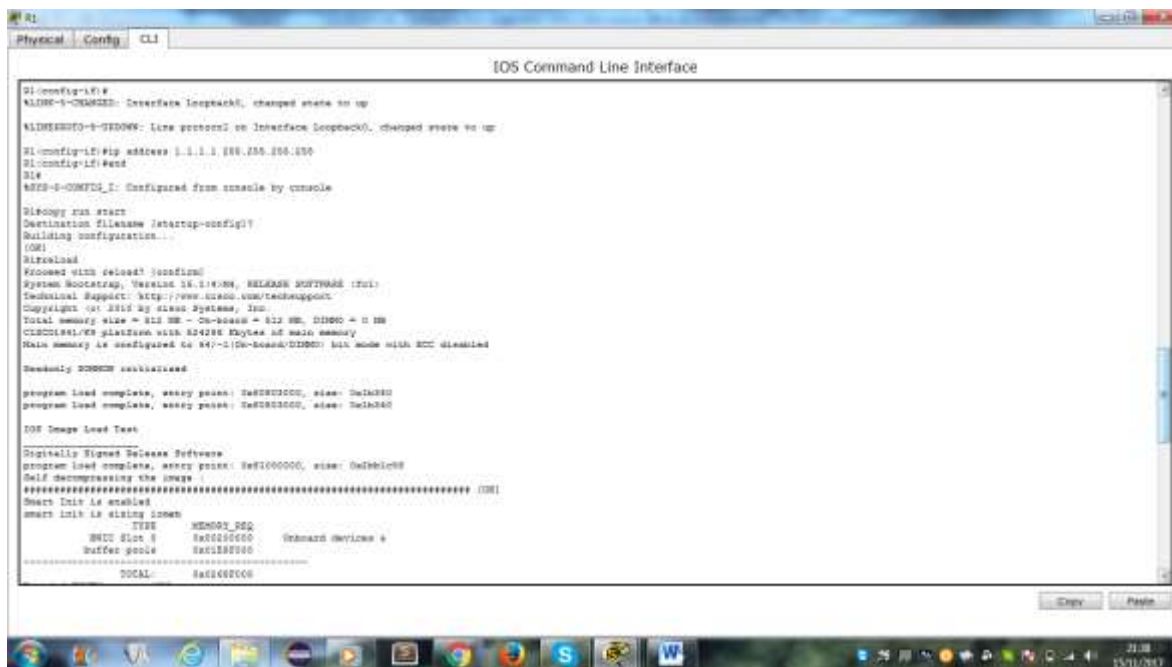
R1
Physical Config CLI
IOS Command Line Interface

Index 0/0, Flood queue length 0
Next 0x01/0x010
Last Flood sent length is 1, maximum is 1
Last Flood sent time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacency with neighbor 192.168.22.1
Suppress hello for 0 neighbor(s)
HelloID 0/0 is up, line protocol is up
Interface address is 192.168.22.1, Area 0
Process ID 1, Router ID 192.168.22.1, 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 6
Hello due in 01:30:28
Index 0/0, Flood queue length 0
Next 0x01/0x010
Last Flood sent length is 1, maximum is 1
Last Flood sent time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacency with neighbor 192.168.22.1
Suppress hello for 0 neighbor(s)
R1#
R1#show ip ospf int brief
% Invalid input detected at '^' marker.
R1conf t
Enter configuration commands, one per line. End with CTRL-Z.
R1(config)#interface lo0
R1(config-l0)#
R1(config-l0)#ip address 1.1.1.1 255.255.255.255
R1(config-l0)#end
R1#
R1#show ip ospf int brief
R1#
  
```

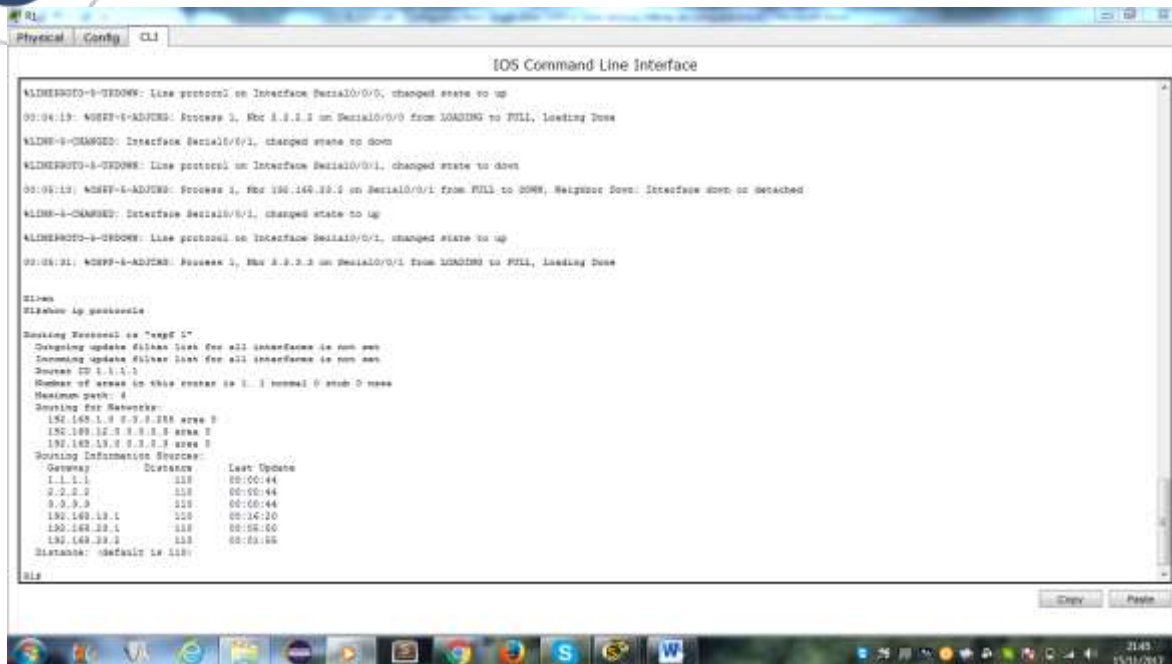
- b. Asigne direcciones IP al loopback 0 en el R2 y el R3. Utilice la dirección IP 2.2.2.2/32 para el R2 y 3.3.3.3/32 para el R3.



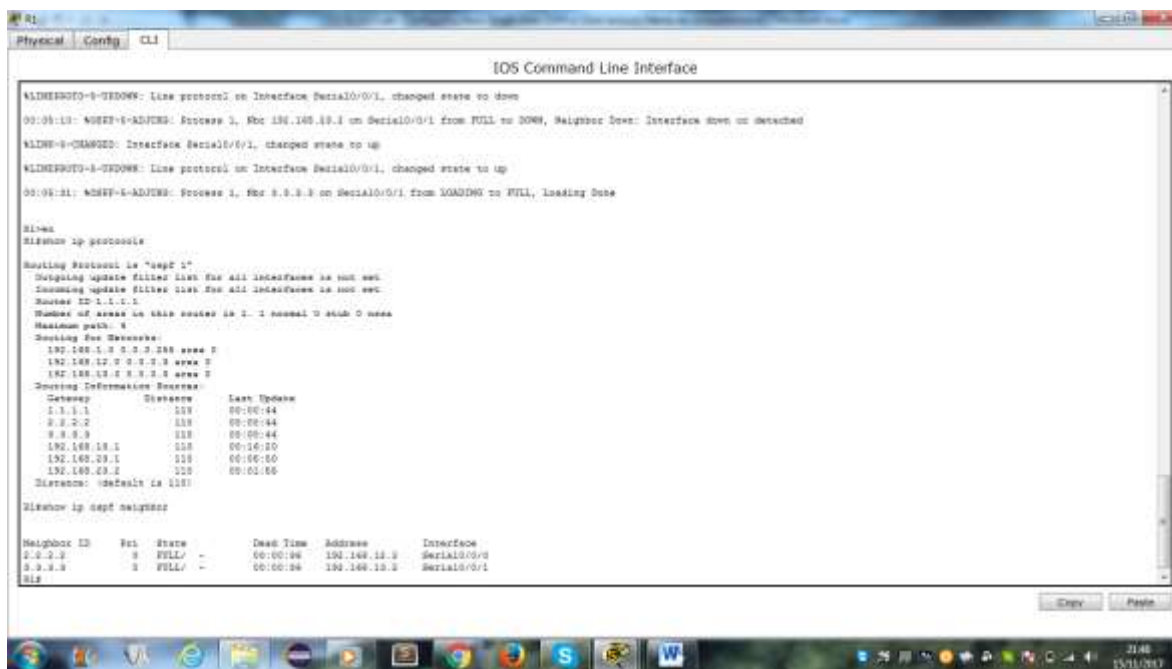
- c. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.
- d. Debe volver a cargar los routers para restablecer la ID del router a la dirección de loopback. Emita el comando **reload** en los tres routers. Presione Enter para confirmar la recarga.



- 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.



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

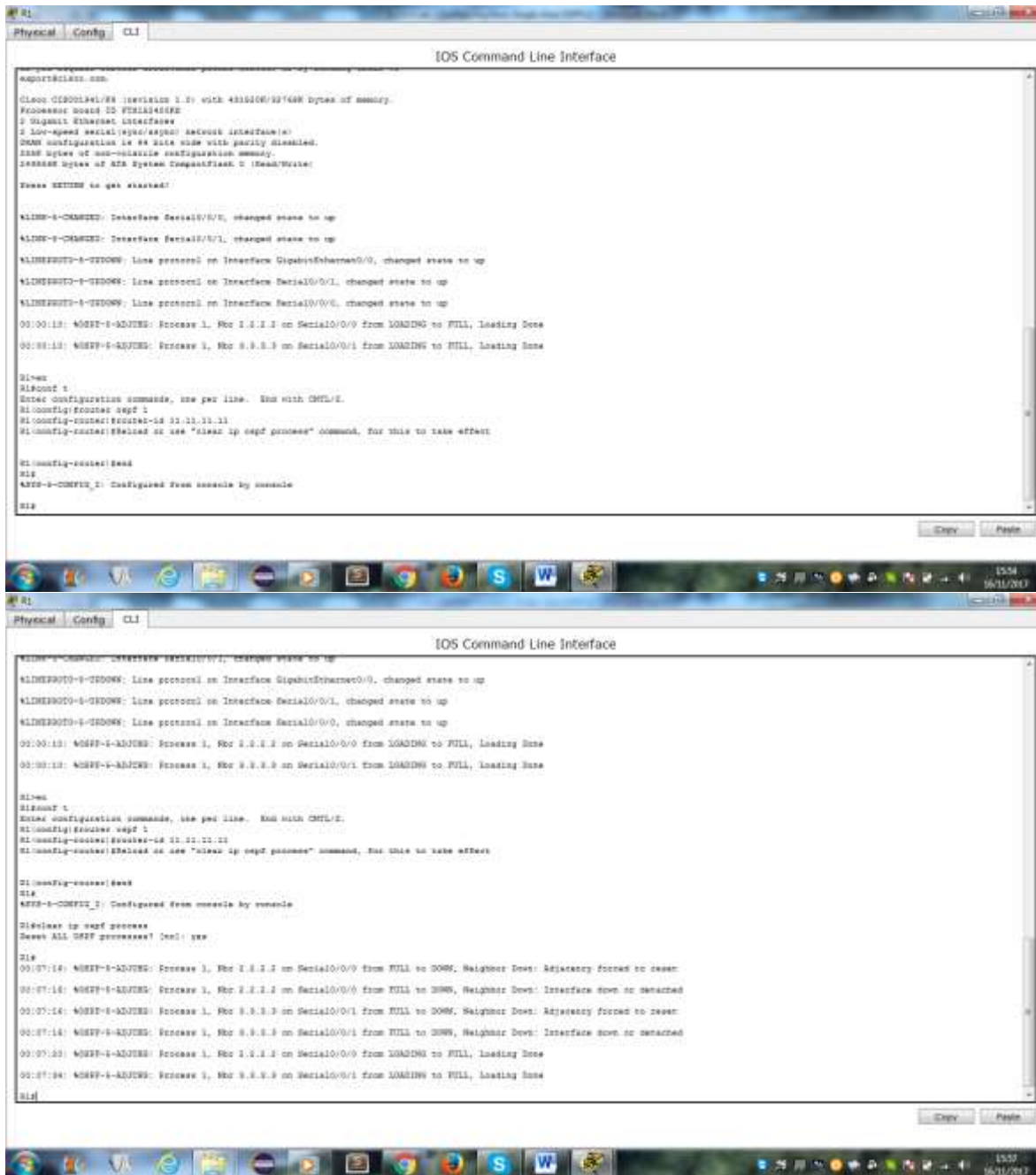


Paso 2. cambiar la ID del router R1 con el comando router-id.

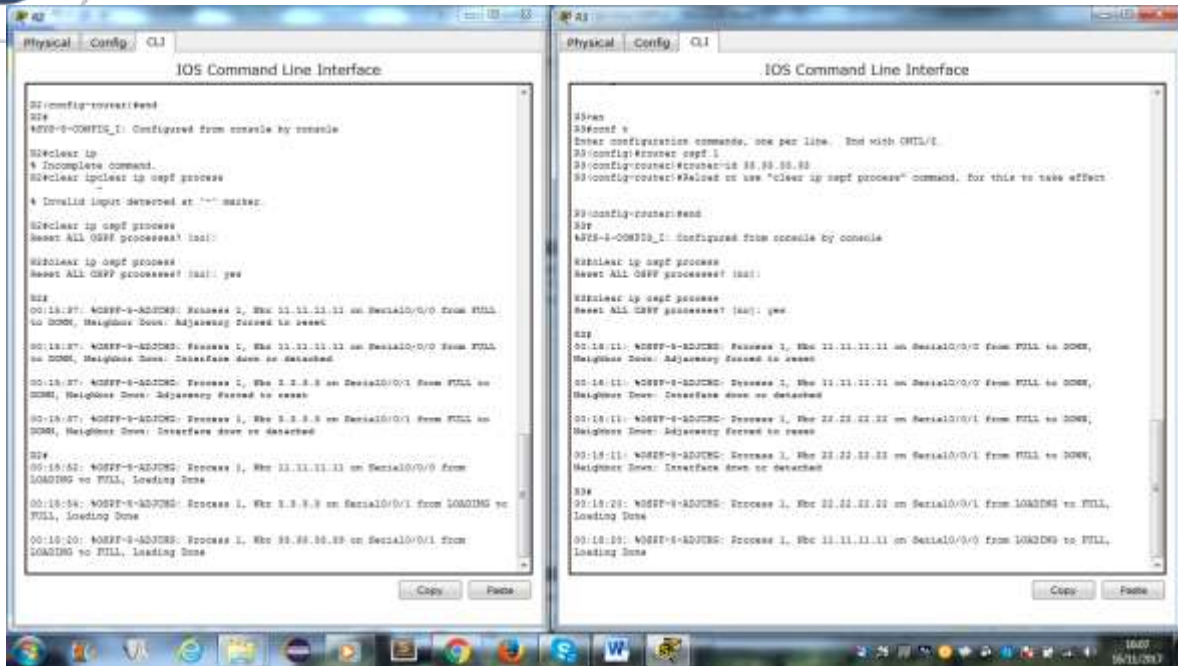
El método de preferencia para establecer la ID del router es mediante el comando **router-id**.

- 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**.
- b. Recibirá un mensaje informativo en el que se le indique que debe volver a cargar el router o usar el comando **clear ip ospf process** para que se aplique el cambio. Emita el comando **clear ip ospf**

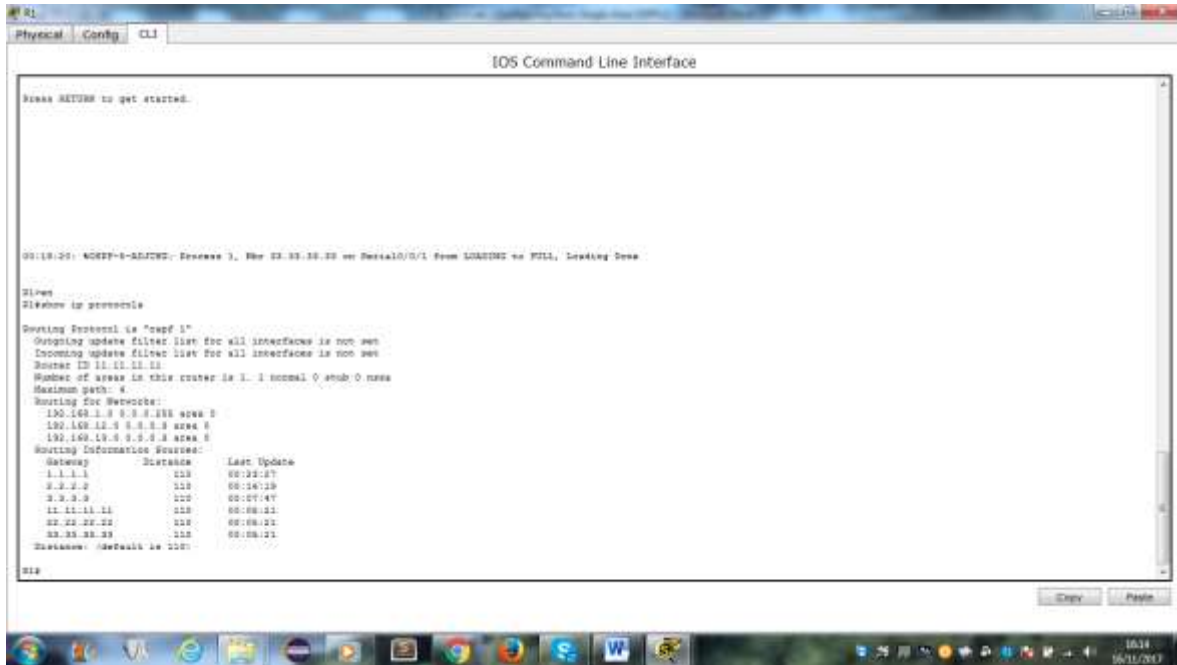
process en los tres routers. Escriba **yes** (sí) como respuesta al mensaje de verificación de restablecimiento y presione Enter.



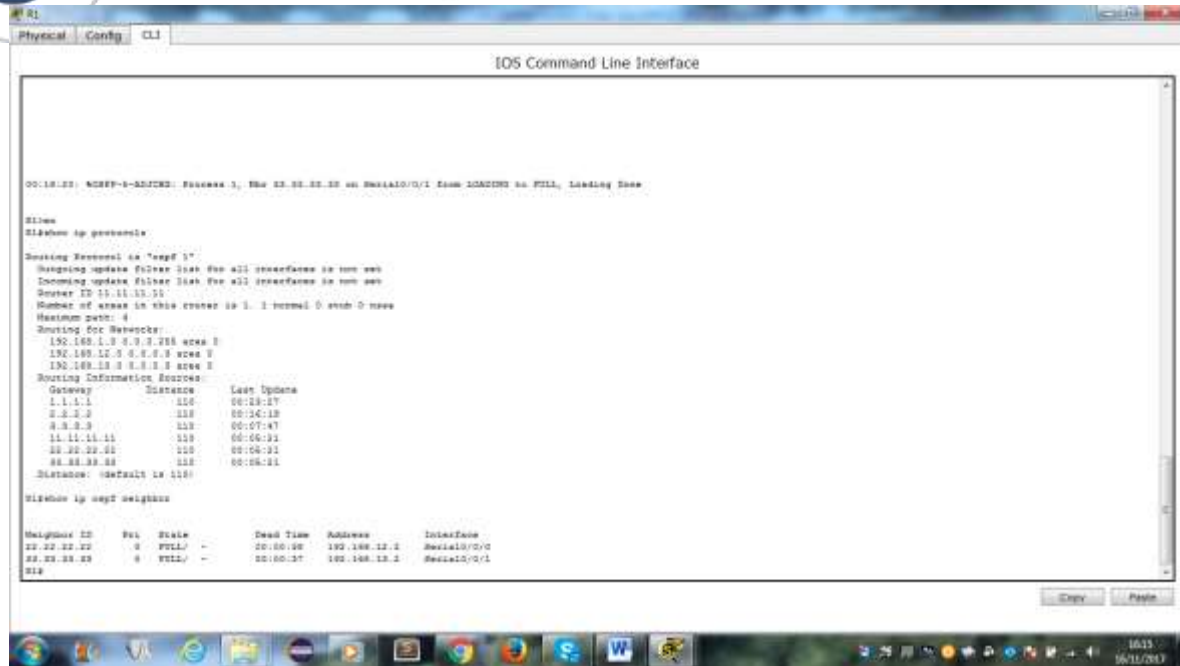
- c. Establezca la ID del router R2 **22.22.22.22** y la ID del router R3 **33.33.33.33**. Luego, use el comando **clear ip ospf process** para restablecer el proceso de routing de OSPF.



d. Emita el comando **show ip protocols** para verificar que la ID del router R1 haya cambiado.



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

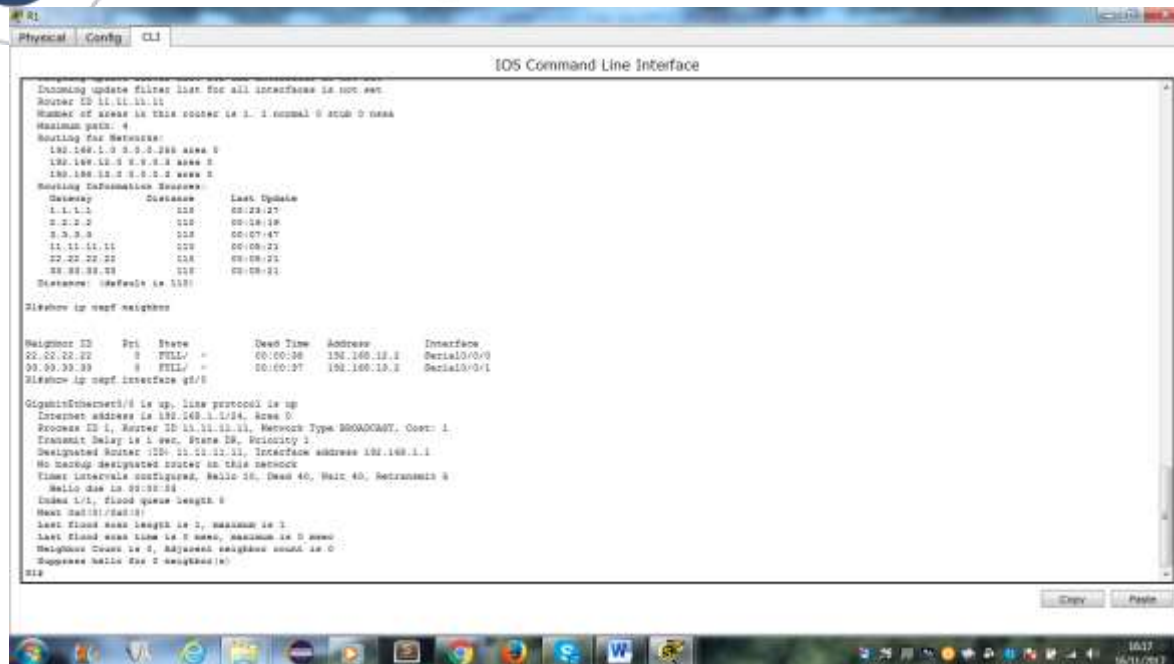


Parte 5. configurar las interfaces pasivas de OSPF

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

Paso 1. configurar una interfaz pasiva.

- 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.

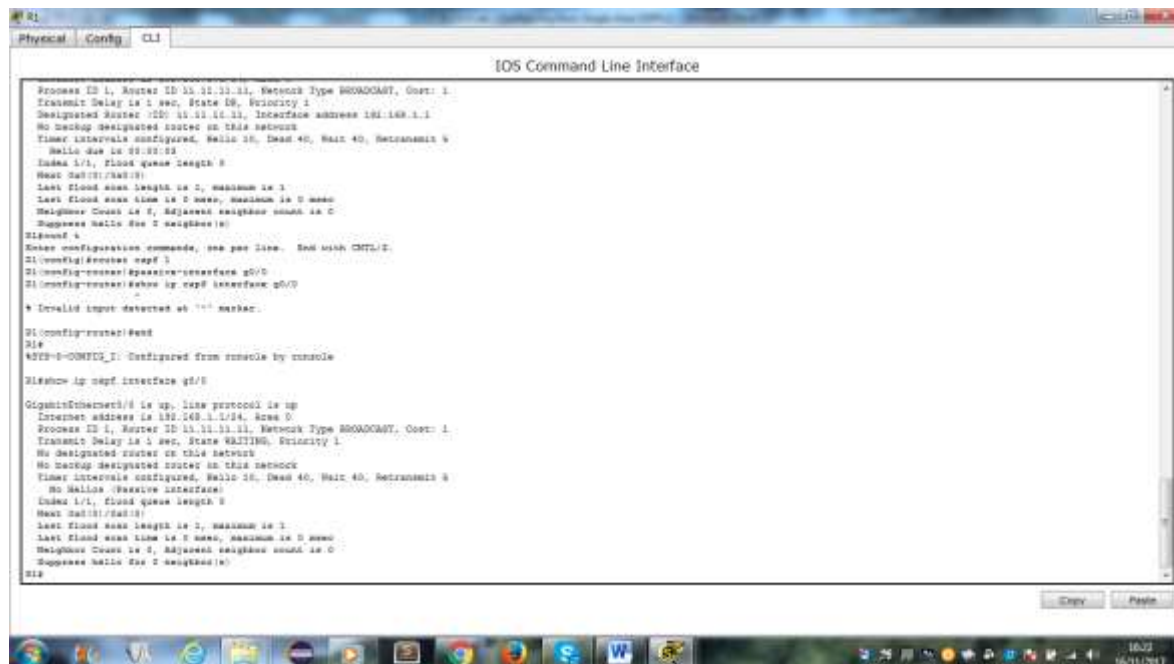


b. Emita el comando **passive-interface** para cambiar la interfaz G0/0 en el R1 a pasiva.

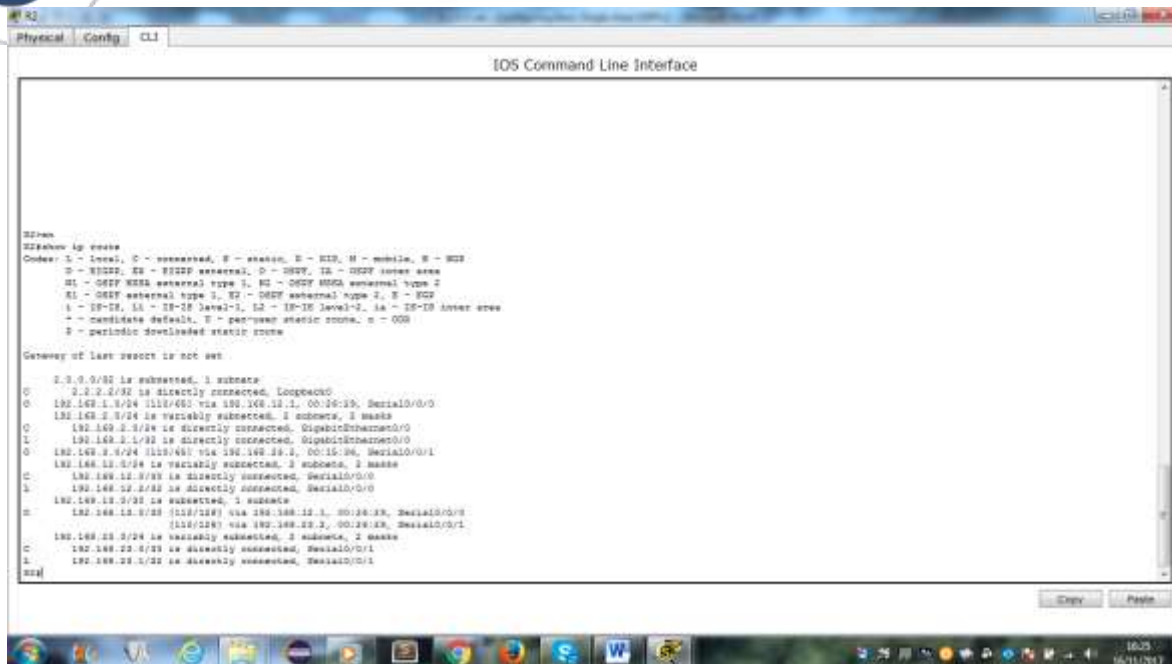
```

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

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

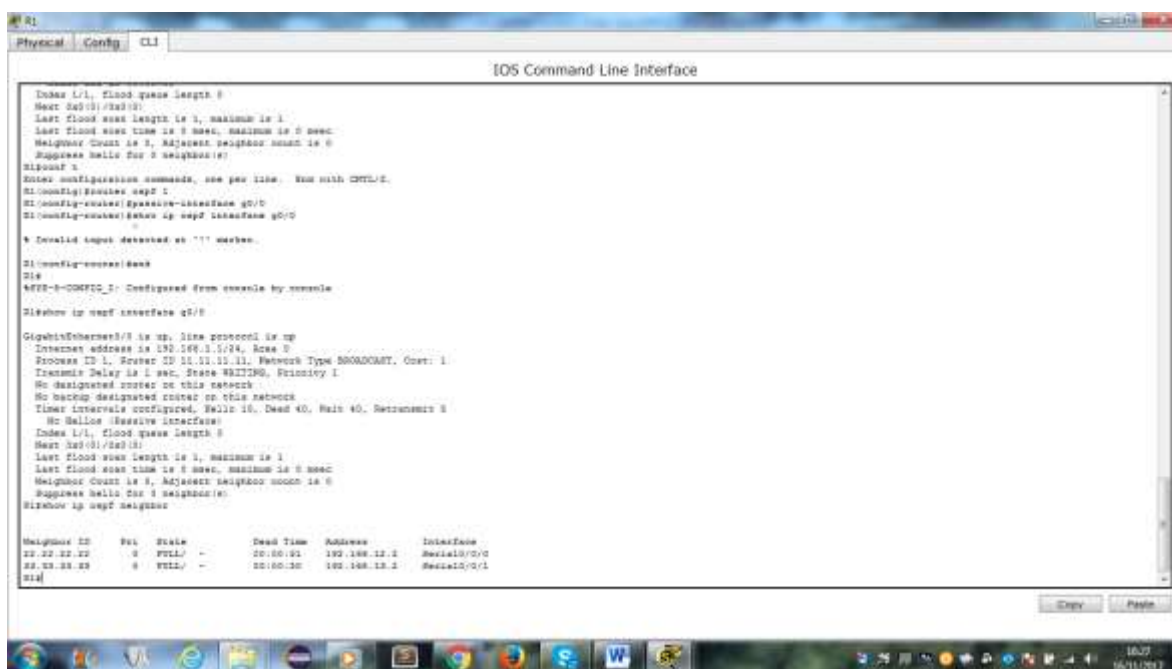


d. Emita el comando **show ip route** en el R2 y el R3 para verificar que todavía haya disponible una ruta a la red 192.168.1.0/24.

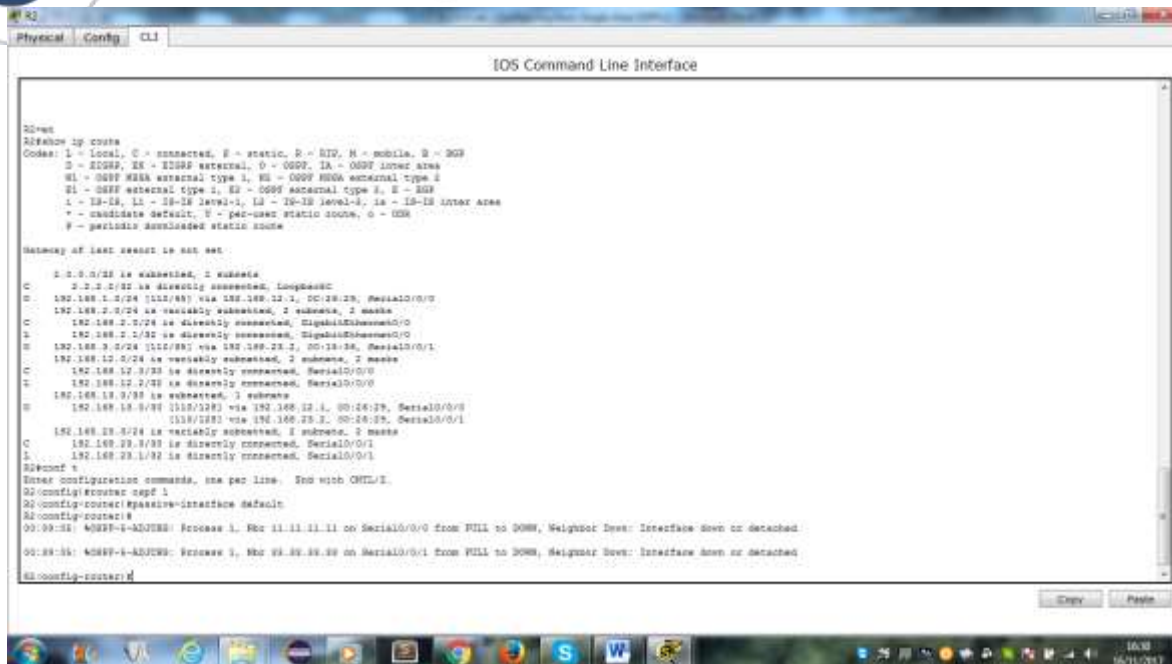


Paso 2. establecer la interfaz pasiva como la interfaz predeterminada en un router.

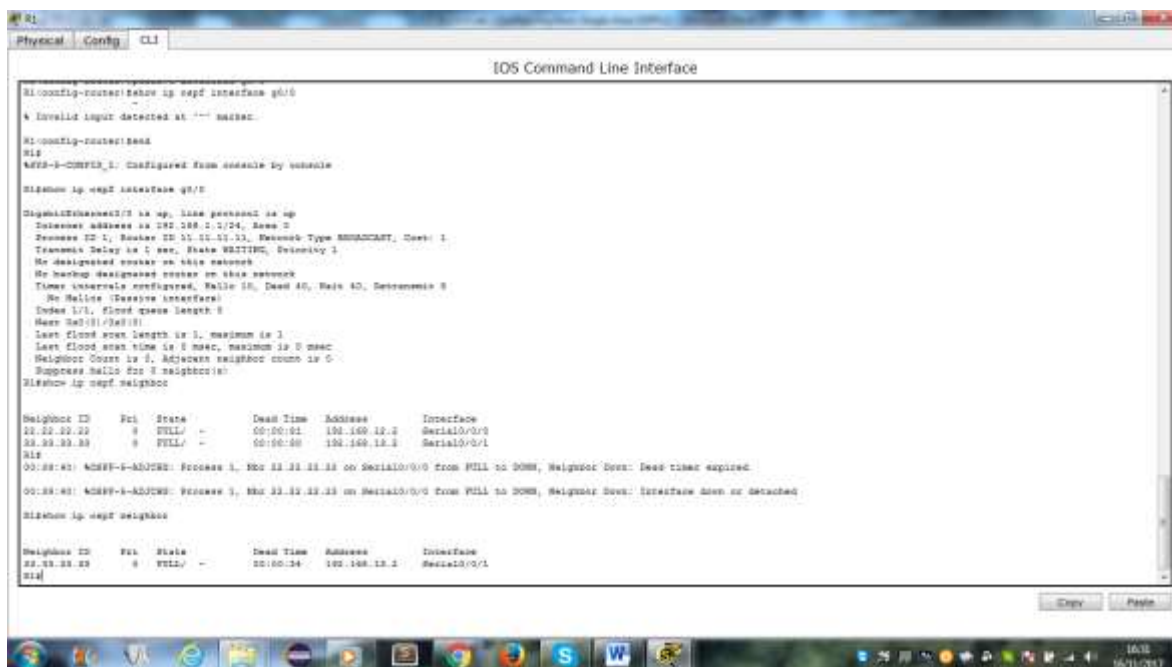
- a. Emita el comando **show ip ospf neighbor** en el R1 para verificar que el R2 aparezca como un vecino OSPF.



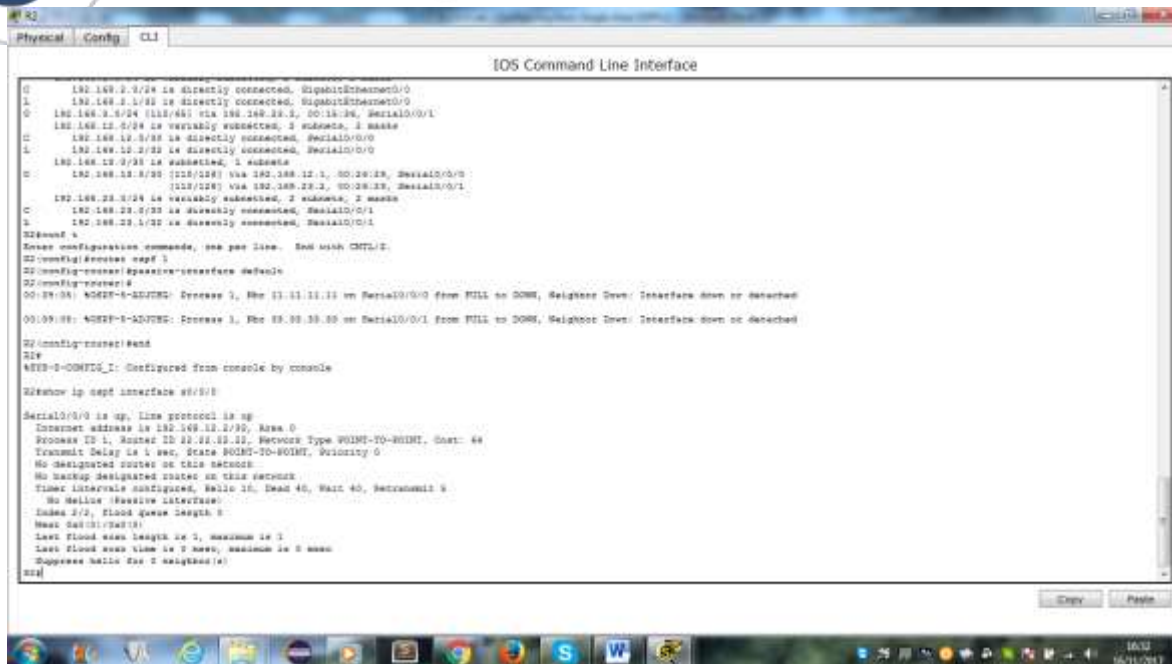
- b. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPF como pasivas de manera predeterminada.



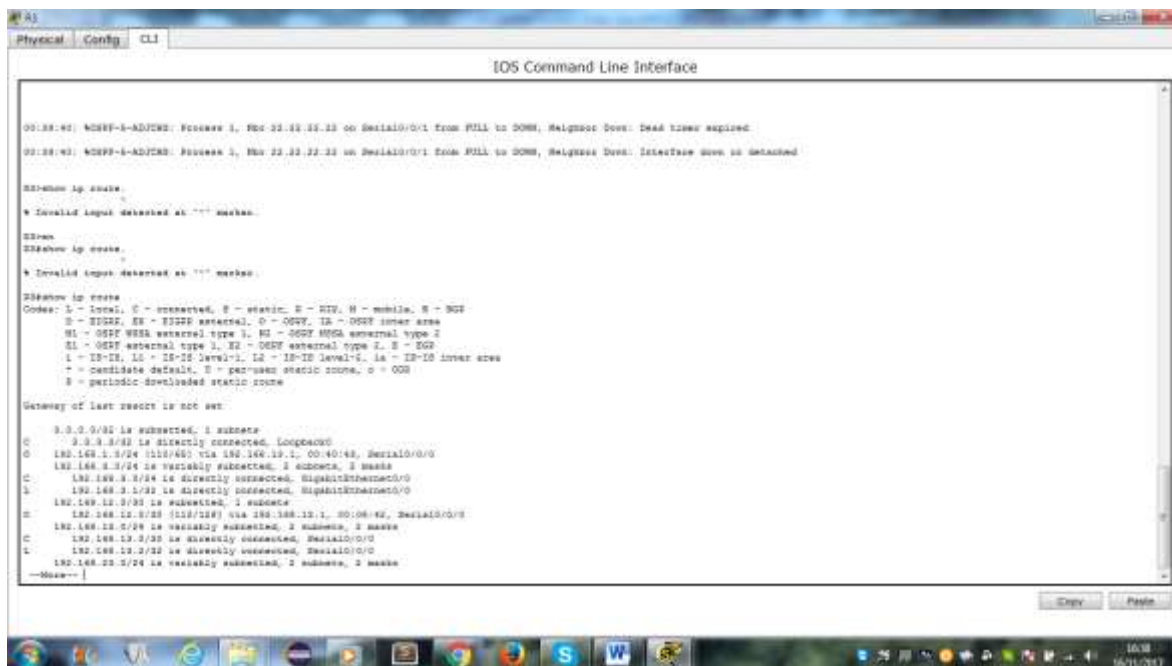
- c. Vuelva a emitir el comando **show ip ospf neighbor** en el R1. Una vez que el temporizador de tiempo muerto haya caducado, el R2 ya no se mostrará como un vecino OSPF.



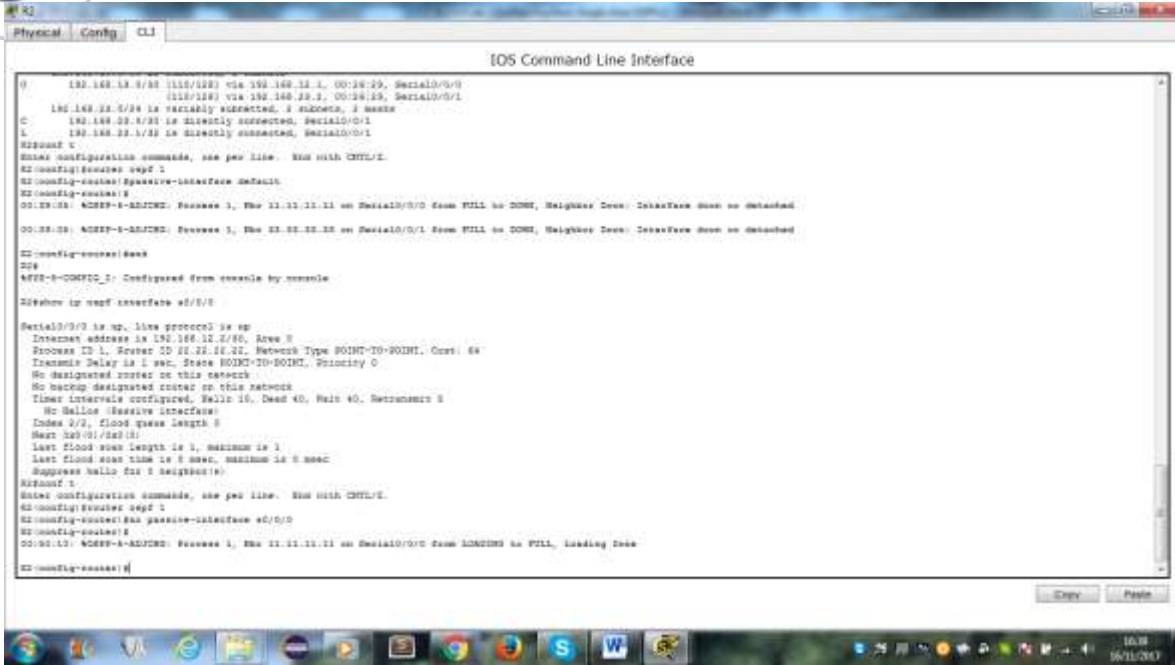
- d. Emita el comando **show ip ospf interface S0/0/0** en el R2 para ver el estado de OSPF de la interfaz S0/0/0.



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



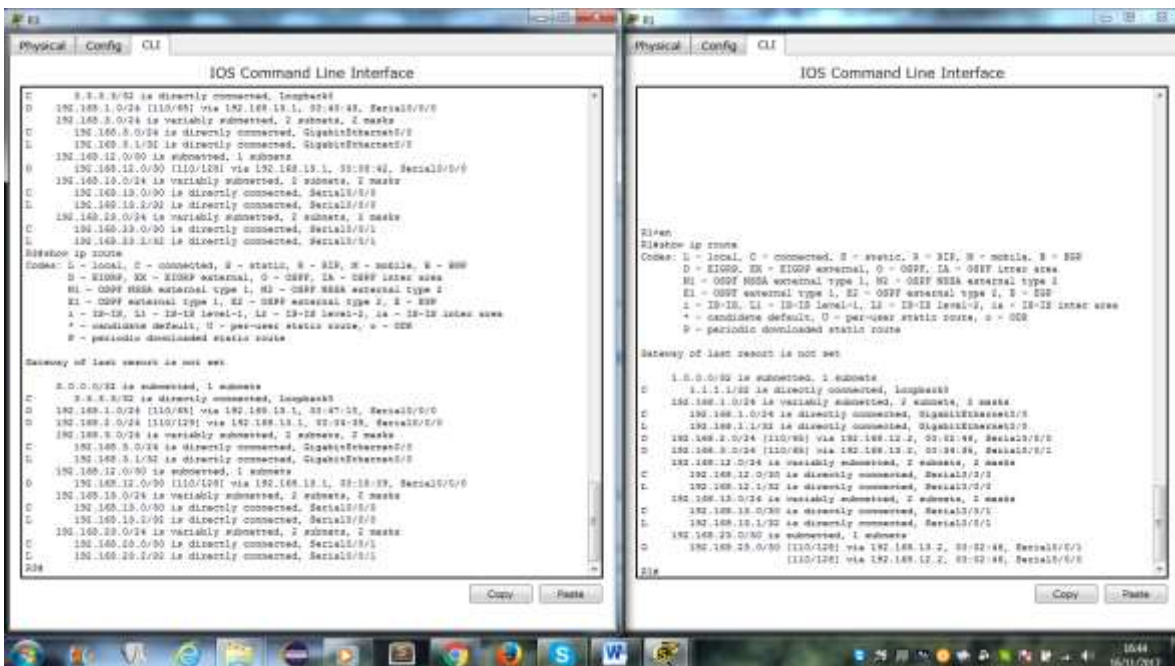
- f. En el R2, emita el comando **no passive-interface** para que el router envíe y reciba actualizaciones de routing OSPF. Después de introducir este comando, verá un mensaje informativo que explica que se estableció una adyacencia de vecino con el R1.



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

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

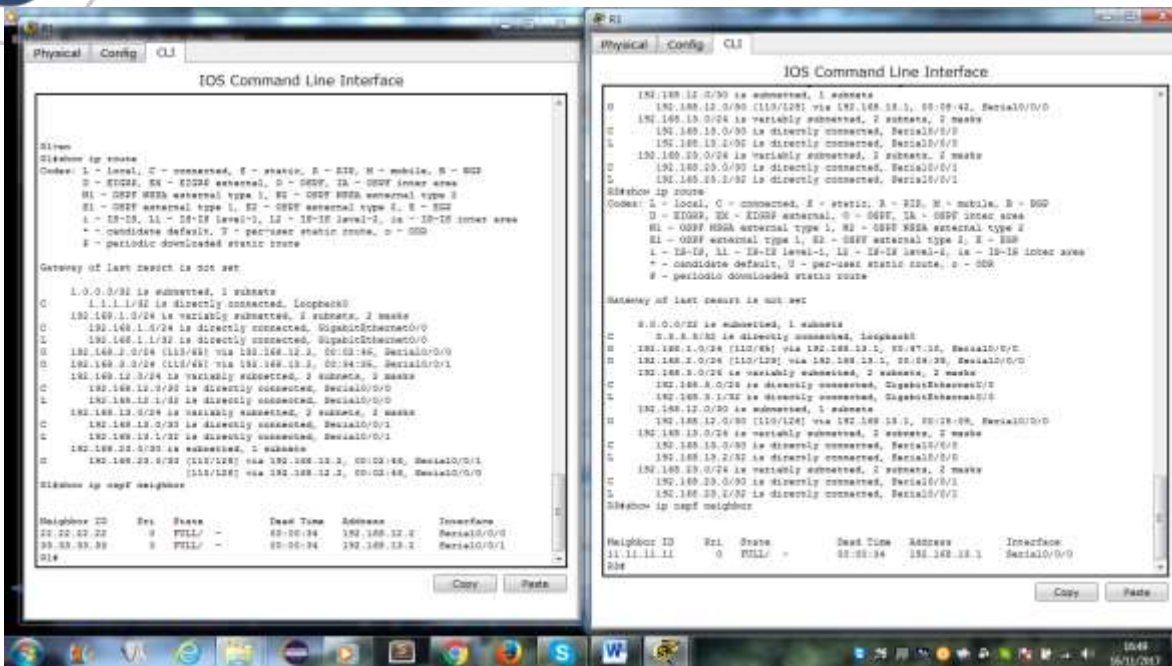
¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3?



¿El R2 aparece como vecino OSPF en el R1?

¿El R2 aparece como vecino OSPF en el R3?

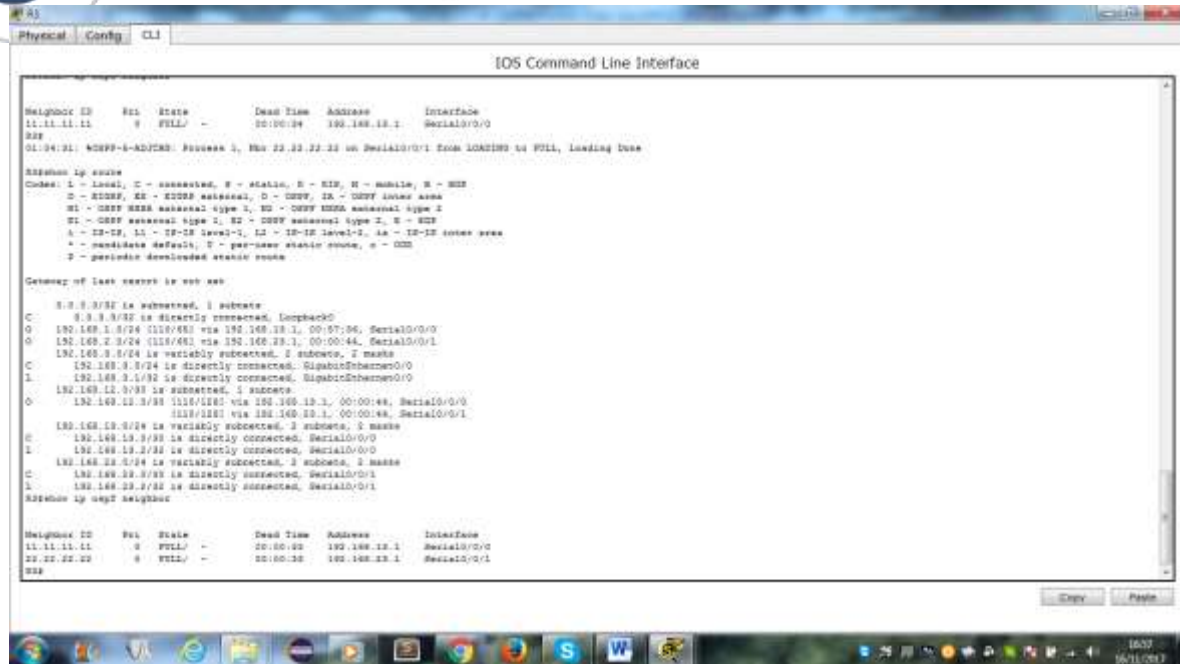
¿Qué indica esta información?



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



- i. Vuelva a emitir el comando **show ip route** en el R3.
 - ¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24?
 - ¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3 y cómo se calcula?
 - ¿El R2 aparece como vecino OSPF del R3?



Parte 6. cambiar las métricas de OSPF

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

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

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

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

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


```

R1
Physical Config CLI
IOS Command Line Interface

R1>show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (normal)
Hardware is CS Series Ethernet, address is 0000.0e00.0e01 (bia 0000.0e00.0e01)
Interface 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 BROADCAST, 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 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (64k/1843/0) Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
  0 minute input rate 0 bits/sec, 0 packets/sec
  0 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, 0 input discards, 0 pause input
    0 input packets with receive condition detected
    100 packets output, 11840 bytes, 0 unknown
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
R1#
    
```

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

```

R1
Physical Config CLI
IOS Command Line Interface

R1>show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (normal)
Hardware is CS Series Ethernet, address is 0000.0e00.0e01 (bia 0000.0e00.0e01)
Interface 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 BROADCAST, 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 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (64k/1843/0) Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
  0 minute input rate 0 bits/sec, 0 packets/sec
  0 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, 0 input discards, 0 pause input
    0 input packets with receive condition detected
    100 packets output, 11840 bytes, 0 unknown
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
R1>show ip route ospf
R
 192.168.2.0 (192/24) via 192.168.1.2, 00:11:02, Serial0/0/0
R
 192.168.3.0 (192/24) via 192.168.1.2, 00:10:51, Serial0/0/1
R
 192.168.2.0/24 is subnetted, 1 subnets
R
 192.168.2.0 (192/24) via 192.168.1.2, 00:11:02, Serial0/0/1
R
 192.168.2.0 (192/24) via 192.168.1.2, 00:11:02, Serial0/0/0
R1#
    
```

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

```

R1
Physical Config CLI
IOS Command Line Interface

Gateway of last resort is not set

R1.0.0/24 is subnetted, 1 subnets
C 1.1.1.1/24 is directly connected, Loopback0
D 192.168.1.0/24 [111/40] via 192.168.10.1, 00:00:00, Serial0/0/0
D 192.168.2.0/24 [111/40] via 192.168.10.1, 00:00:00, Serial0/0/1
R1.168.1.0/24 is subnetted, 1 subnets
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
D 192.168.1.0/24 is directly connected, GigabitEthernet0/0
R1.168.12.0/24 [111/20] via 192.168.10.1, 00:00:00, Serial0/0/0
D 192.168.12.0/24 [111/20] via 192.168.10.1, 00:00:00, Serial0/0/1
R1.168.13.0/24 is subnetted, 2 subnets
C 192.168.13.0/24 is directly connected, Serial0/0/0
D 192.168.13.0/24 is directly connected, Serial0/0/0
R1.168.13.0/24 is subnetted, 2 subnets
C 192.168.13.0/24 is directly connected, Serial0/0/1
D 192.168.13.0/24 is directly connected, Serial0/0/1
R1.168.22.0/24 is subnetted, 1 subnets
D 192.168.22.0/24 is directly connected, Serial0/0/1
R1#show ip ospf neighbors

Neighbor ID Pri State Dead Time Address Interface
11.11.11.11 0 FULL/ - 00:00:00 192.168.10.1 Serial0/0/0
22.22.22.22 0 FULL/ - 00:00:00 192.168.10.1 Serial0/0/1
R1#show ip ospf interface gi0/0

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 3
Hello due in 00:00:00
Link ID 1/0, Flood queue length 0
Next 0x0/0/0x0/0
Last flood send time is 1, maximum is 1
Last flood send time is 0 seen, maximum is 0 seen
Neighbor Count is 0, Adjacent neighbor count is 0
Suppressed hello due to neighbor(s)
R1#
    
```

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

```

R1
Physical Config CLI
IOS Command Line Interface

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)
0 minute input rate 0 bits/sec, 0 packets/sec
0 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 casts, 0 queries, 0 unknown
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 L2L3 multicast, 0 pause input
0 input packets with duplicate source identifier detected
100 packets output, 1000 bytes, 0 unknown
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collisions, 0 deferred
0 lost carriers, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
R1#show ip route ospf

O 192.168.1.0 [111/40] via 192.168.10.1, 00:21:01, Serial0/0/0
O 192.168.2.0 [111/40] via 192.168.10.1, 00:21:01, Serial0/0/1
O 192.168.13.0 [111/20] via 192.168.10.1, 00:21:01, Serial0/0/0
O 192.168.13.0 [111/20] via 192.168.10.1, 00:21:01, Serial0/0/1
R1#show ip ospf interface s0/0/1

Serial0/0/1 is up, line protocol is up
Internet address is 192.168.13.1/24, Area 0
Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 10
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 3
Hello due in 00:00:00
Link ID 1/0, Flood queue length 0
Next 0x0/0/0x0/0
Last flood send time is 1, maximum is 1
Last flood send time is 0 seen, maximum is 0 seen
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent vccv neighbor 22.22.22.22
Suppressed hello due to neighbor(s)
R1#
    
```

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

```

R1
Physical Config CLI
IOS Command Line Interface

0 packets input, 0 bytes, 0 no buffers
0 discarded, 0 broadcast, 0 runt, 0 giants, 0 chronicle
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 output, 0% multicast, 0 pause input
0 input packets with discard condition detected
104 packets output, 1046 bytes, 0 uncorrected
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collisions, 0 deferred
0 late packets, 0 no captures
0 output buffer failures, 0 output buffers stepped out

R1#show ip route ospf
R
 192.168.2.0 (110/80) via 192.168.12.1, 00:21:00, Serial0/0/0
 192.168.2.0 (110/80) via 192.168.12.1, 00:21:01, Serial0/0/1
 192.168.22.0 (100/80) via 192.168.12.1, 00:21:01, Serial0/0/1
 192.168.22.0 (100/80) via 192.168.12.1, 00:21:02, Serial0/0/0

R1#show ip ospf neighbors all/0/0
Serial0/0/1 is up, line protocol is up
 Internet address is 192.168.12.1/30, Area 0
 Process ID 1, Router ID 11.11.11.11, 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 6
 Hello due in 00:00:09
 Index 2/1, Flood queue length 0
 Next Seq 0/1/34033
 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 11.11.11.11
 Suppress hello for 0 neighbor(s)
 R1#end
 Enter configuration commands, one per line. End with CTRL/Z.
 R1(config)#router ospf 1
 R1(config-router)#auto-cost reference-bandwidth 10000
 * OSPF reference bandwidth is changed.
 Please ensure reference bandwidth is consistent across all routers.
 R1(config-router)#
  
```

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

```

R2
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

R2#
R2#end
 Enter configuration commands, one per line. End with CTRL/Z.
 R2(config)#router ospf 1
 R2(config-router)#auto-cost reference-bandwidth 10000
 * Invalid input detected at '^' marker.
 R2(config-router)#auto-cost reference-bandwidth 10000
 * Invalid input detected at '^' marker.
 R2(config-router)#auto-cost reference-bandwidth 10000
 * Invalid input detected at '^' marker.
 R2(config-router)#
 R2(config-router)#auto-cost reference-bandwidth 10000
 * OSPF reference bandwidth is changed.
 Please ensure reference bandwidth is consistent across all routers.
 R2(config-router)#

R3
Physical Config CLI
IOS Command Line Interface

R3
 192.168.2.0/24 is directly connected, Serial0/0/0/0/0
 192.168.3.1/30 is directly connected, Serial0/0/0/0/0
 192.168.12.0/30 is subnetted, 1 subnets
 192.168.12.0/30 (110/120) via 192.168.12.1, 00:00:44, Serial0/0/0
 192.168.12.0/30 (110/120) via 192.168.12.1, 00:00:44, Serial0/0/1
 192.168.10.0/24 is variably subnetted, 1 subnets, 1 masks
 192.168.10.0/30 is directly connected, Serial0/0/0
 192.168.10.1/30 is directly connected, Serial0/0/0
 192.168.22.0/24 is variably subnetted, 2 subnets, 1 masks
 192.168.22.0/30 is directly connected, Serial0/0/1
 192.168.22.0/30 is directly connected, Serial0/0/1

R3#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
11.11.11 0 FULL/- 00:00:29 192.168.12.1 Serial0/0/0
12.12.12 0 FULL/- 00:00:29 192.168.12.1 Serial0/0/1

R3#show ip ospf interface g0/0
Serial0/0/0/0/0 is up, line protocol is up
 Interface address is 192.168.2.1/24, Area 0
 Process ID 1, Router ID 22.22.22.22, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 22.22.22.22, Interface address 192.168.2.1
 Do backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 6
 Hello due in 00:00:08
 Index 1/1, Flood queue length 0
 Next Seq 0/1/34033
 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#end
 Enter configuration commands, one per line. End with CTRL/Z.
 R3(config)#router ospf 1
 R3(config-router)#auto-cost reference-bandwidth 10000
 * OSPF reference bandwidth is changed.
 Please ensure reference bandwidth is consistent across all routers.
 R3(config-router)#
  
```

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

```

R1>
Physical Config CLI
IOS Command Line Interface

R1(config)#ospf 100 area 0
R1(config)#network 192.168.3.0 0.0.0.255 area 0
R1(config)#cost 100
R1(config)#

R1#show ip ospf interface gi0/0

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 3
Hello due in 00:00:30
Index 1/1, Flood queue length 0
Next Set(1)/Set(1)
Last Flood send length is 1, maximum is 1
Last Flood send time is 0 secs, maximum is 0 secs
Neighbor Count is 1, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

Timerf 0
Enter configuration commands, one per line. End with CTRL/Z.
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 10000
R1(config-router)#cost 100
R1(config-router)#end
R1#

R1#show ip ospf interface gi0/1

GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.3.1/24, Area 0
Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 100
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 3
Hello due in 00:00:30
Index 1/1, Flood queue length 0
Next Set(1)/Set(1)
Last Flood send length is 1, maximum is 1
Last Flood send time is 0 secs, maximum is 0 secs
Neighbor Count is 1, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

R1#
    
```

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>
Physical Config CLI
IOS Command Line Interface

R1(config)#ospf 100 area 0
R1(config)#network 192.168.3.0 0.0.0.255 area 0
R1(config)#cost 100
R1(config)#

R1#show ip ospf interface s0/0/1

Serial0/0/1 is up, line protocol is up
Internet address is 192.168.3.1/30, Area 0
Process ID 1, Router ID 33.33.33.33, Network Type POINT-TO-POINT, Cost: 6476
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 3
Hello due in 00:00:30
Index 2/2, Flood queue length 0
Next Set(1)/Set(1)
Last Flood send length is 1, maximum is 1
Last Flood send time is 0 secs, maximum is 0 secs
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbors 33.33.33.33
Suppress hello for 0 neighbor(s)

Timerf 0
Enter configuration commands, one per line. End with CTRL/Z.
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 10000
R1(config-router)#cost 100
R1(config-router)#end
R1#

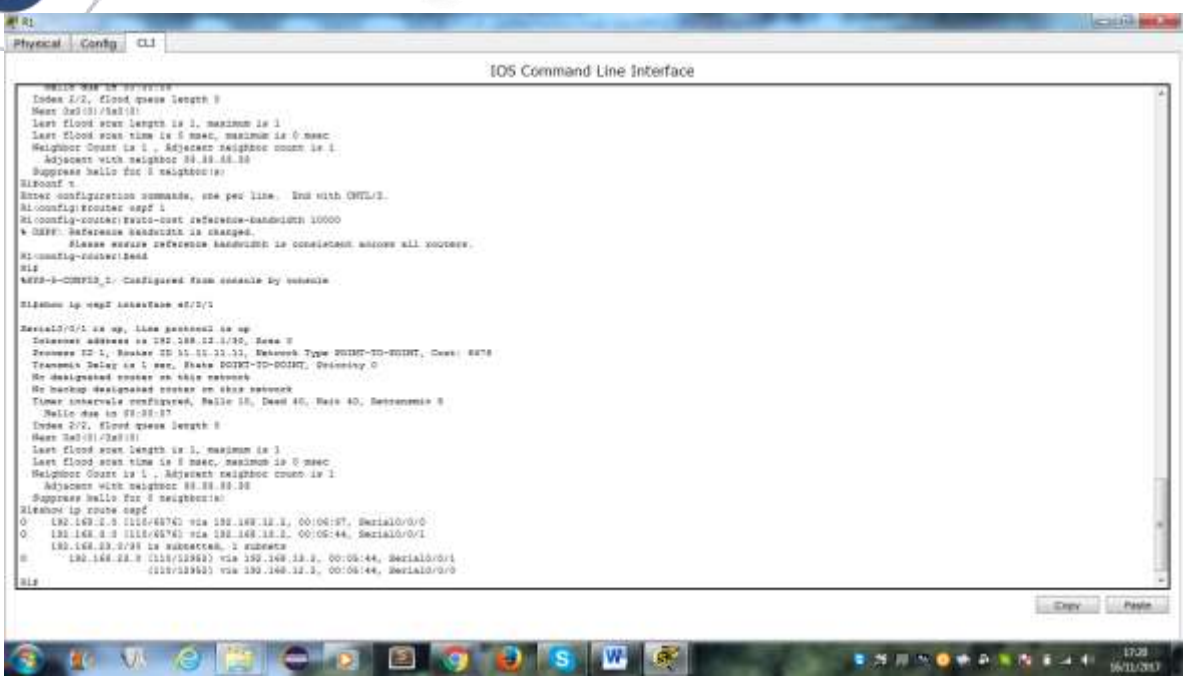
R1#show ip ospf interface s0/0/1

Serial0/0/1 is up, line protocol is up
Internet address is 192.168.3.1/30, Area 0
Process ID 1, Router ID 33.33.33.33, Network Type POINT-TO-POINT, Cost: 6476
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 3
Hello due in 00:00:30
Index 2/2, Flood queue length 0
Next Set(1)/Set(1)
Last Flood send length is 1, maximum is 1
Last Flood send time is 0 secs, maximum is 0 secs
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbors 33.33.33.33
Suppress hello for 0 neighbor(s)

R1#
    
```

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

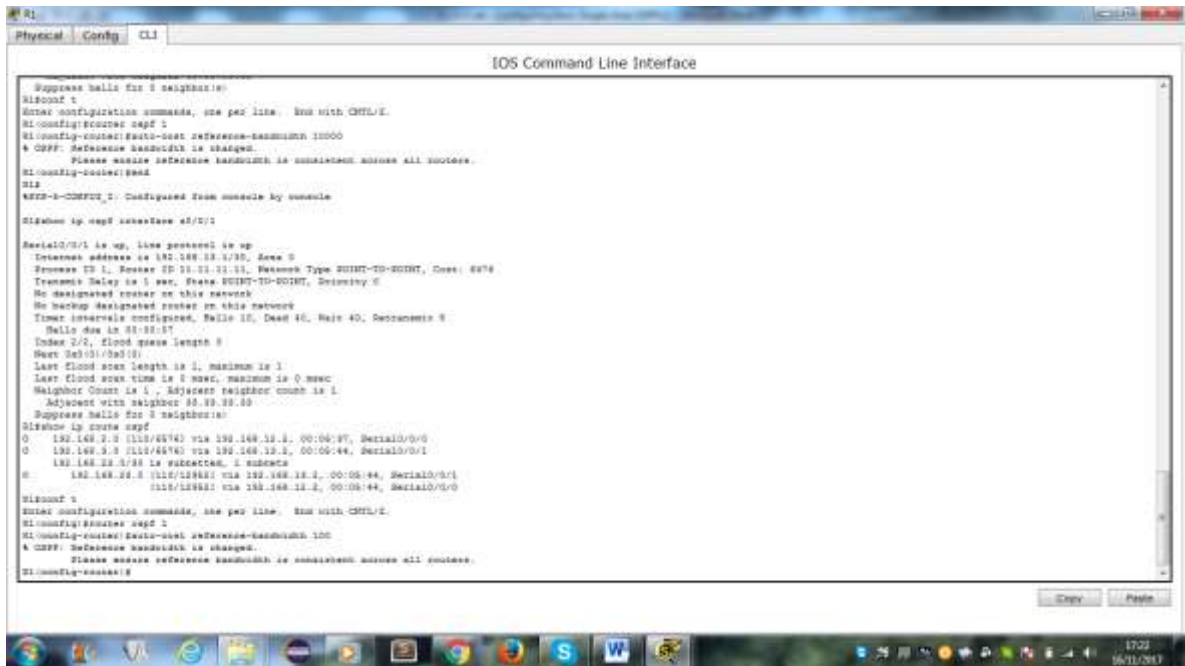
Nota: si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo total será diferente del que se muestra en el resultado. Por ejemplo, el costo acumulado será 6576 si G0/0 está funcionando con velocidad Fast Ethernet (100 Mb/s).



Nota: cambiar el ancho de banda de referencia en los routers de 100 a 10 000 cambi6 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 precisi6n.

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

¿Por qu6 querri6 cambiar el ancho de banda de referencia OSPF predeterminado?



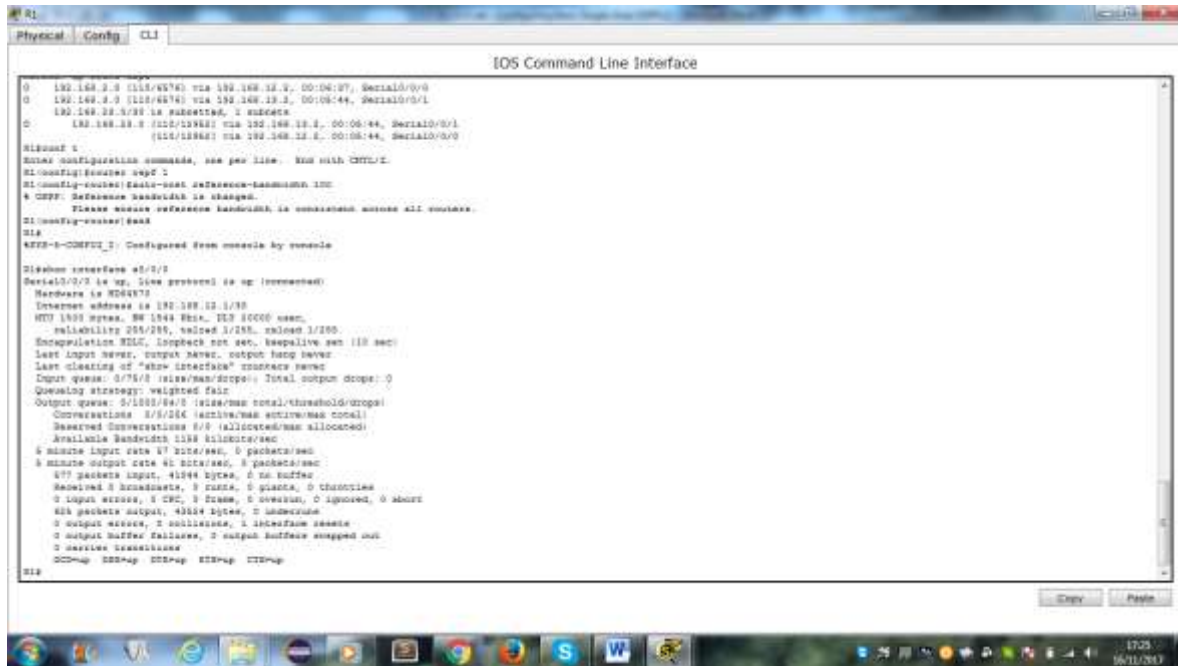
Paso 2. cambiar el ancho de banda de una interfaz.

En la mayori6 de los enlaces seriales, la m6trica del ancho de banda ser6 1544 Kbits de manera predeterminada (la de un T1). Si esta no es la velocidad real del enlace serial, se deber6 cambiar la

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

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

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



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

```

R1
Physical Config CLI
IOS Command Line Interface

Enter configuration commands, one per line. End with CTRL-Z.
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 128
^
***: reference-bandwidth is changed.
Please check reference-bandwidth is consistent across all routers.
R1(config-router)#end
R1
*RT2-0-CMPT2_1: Configured from console by ssmale

R1#show interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is SM887C
Internet address is 192.168.23.2/24
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive sec (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: 0/128/0 (size/max total/bytesin fifo/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1188 kbit/sec
5 minute input rate 67 bits/sec, 0 packets/sec
577 packets input, 4184 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
624 packets output, 4184 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transmissions
0DQmap DQmap DQmap DQmap DQmap
R1#show ip route ospf
R
 192.168.2.0 [128/128] via 192.168.23.2, 00:00:01, Serial0/0/0
R
 192.168.2.0 [128/128] via 192.168.23.2, 00:00:01, Serial0/0/1
R
 192.168.23.0/24 is subnetted, 1 subnets
R
 192.168.23.0 [128/640] via 192.168.23.2, 00:00:01, Serial0/0/1
R
 192.168.23.0 [128/640] via 192.168.23.2, 00:00:01, Serial0/0/0
R1#
  
```

- c. Emita el comando **bandwidth 128** para establecer el ancho de banda en S0/0/0 en 128 Kb/s.
- d. Vuelva a emitir el comando **show ip route ospf**. En la tabla de routing, ya no se muestra la ruta a la red 192.168.23.0/24 a través de la interfaz S0/0/0. Esto es porque la mejor ruta, la que tiene el costo más bajo, ahora es a través de S0/0/1.

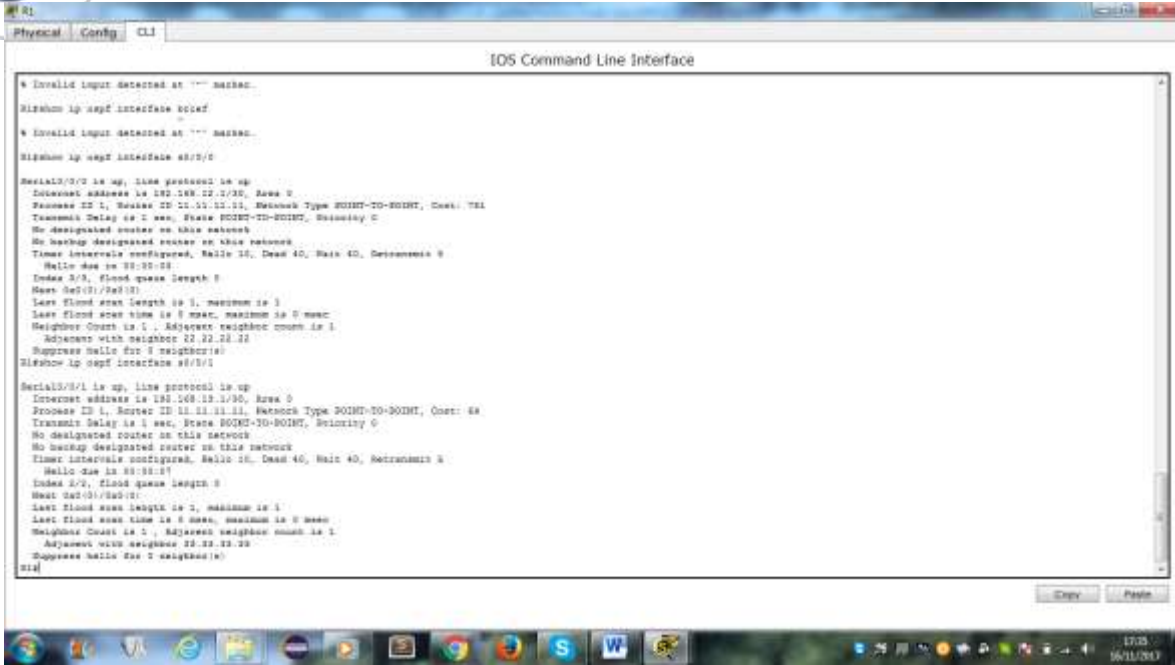
```

R1
Physical Config CLI
IOS Command Line Interface

MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive sec (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: 0/128/0 (size/max total/bytesin fifo/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1188 kbit/sec
5 minute input rate 67 bits/sec, 0 packets/sec
577 packets input, 4184 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
624 packets output, 4184 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transmissions
0DQmap DQmap DQmap DQmap DQmap
R1#show ip route ospf
R
 192.168.2.0 [128/640] via 192.168.23.1, 00:00:01, Serial0/0/0
O
 192.168.2.0 [128/128] via 192.168.23.1, 00:00:01, Serial0/0/1
R
 192.168.23.0/24 is subnetted, 1 subnets
R
 192.168.23.0 [128/640] via 192.168.23.2, 00:00:01, Serial0/0/1
R
 192.168.23.0 [128/640] via 192.168.23.2, 00:00:01, Serial0/0/0
R1#conf t
Enter configuration commands, one per line. End with CTRL-Z.
R1(config)#interface s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#end
R1
*RT2-0-CMPT2_1: Configured from console by ssmale

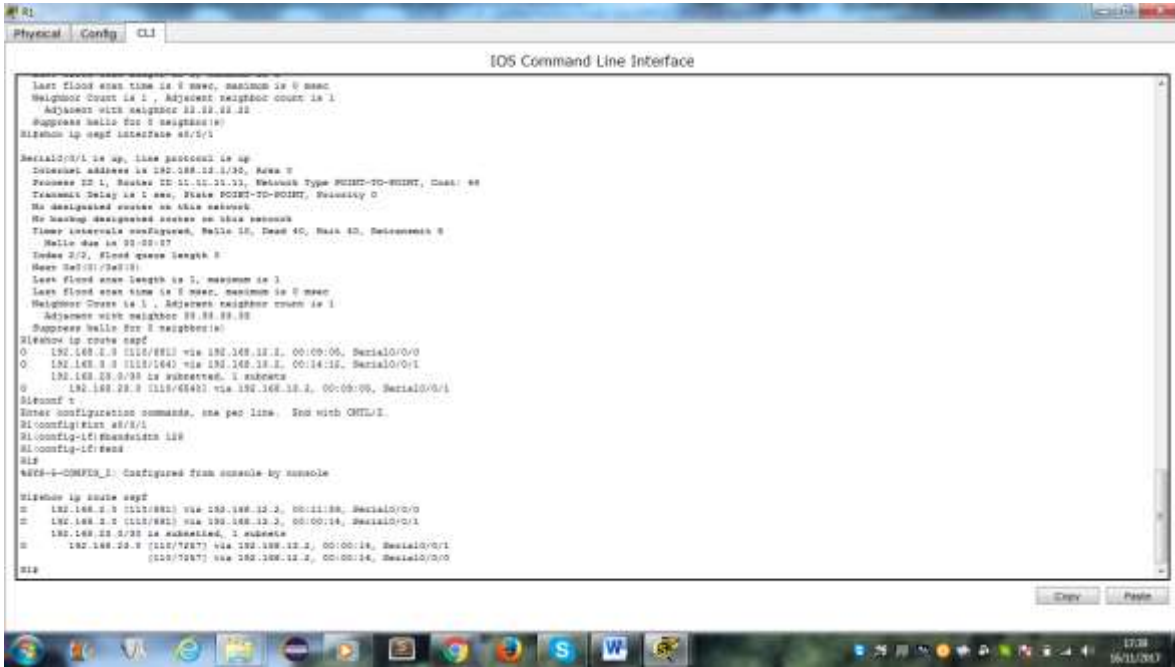
R1#show ip route ospf
R
 192.168.2.0 [128/781] via 192.168.23.2, 00:00:00, Serial0/0/0
O
 192.168.2.0 [128/128] via 192.168.23.2, 00:00:00, Serial0/0/1
R
 192.168.23.0/24 is subnetted, 1 subnets
R
 192.168.23.0 [128/640] via 192.168.23.2, 00:00:00, Serial0/0/1
R1#
  
```

- e. Emita el comando **show ip ospf interface brief**. El costo de S0/0/0 cambió de 64 a 781, que es una representación precisa del costo de la velocidad del enlace.
- f. Cambie el ancho de banda de la interfaz S0/0/1 a la misma configuración que S0/0/0 en el R1.



g. 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.

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



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

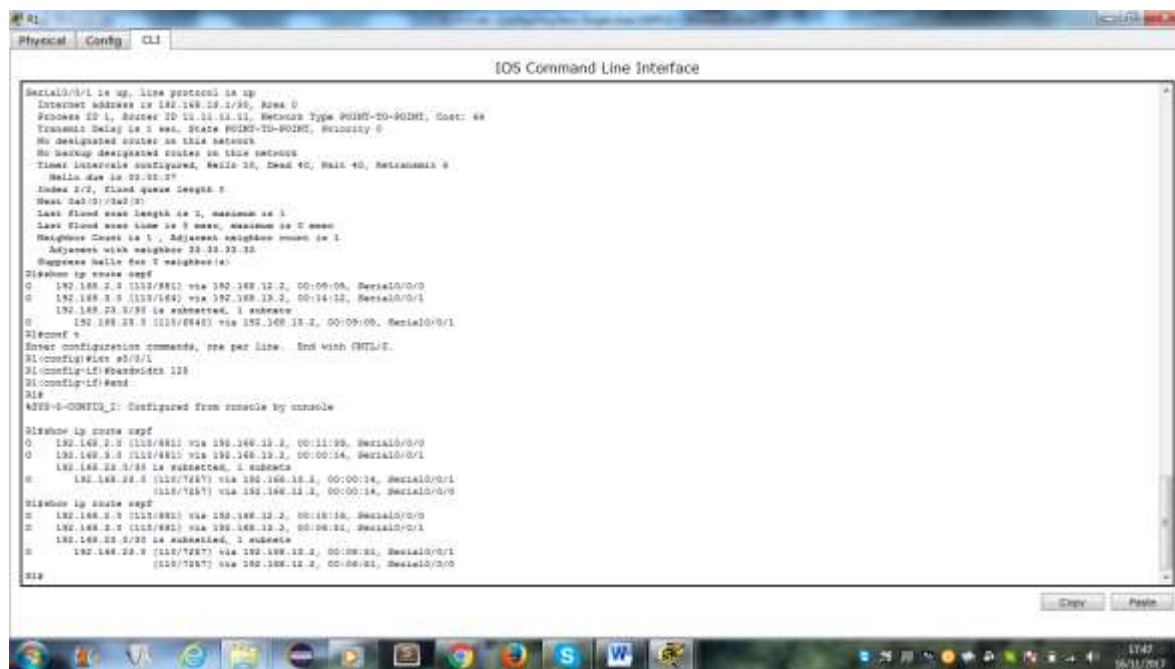


- i. Emita el comando **bandwidth 128** en todas las interfaces seriales restantes de la topología.
¿Cuál es el nuevo costo acumulado a la red 192.168.23.0/24 en el R1? ¿Por qué?

Paso 3. cambiar el costo de la ruta.

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

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



- b. Aplique el comando **ip ospf cost 1565** a la interfaz S0/0/1 en el R1. Un costo de 1565 es mayor que el costo acumulado de la ruta a través del R2, que es 1562.
- c. Vuelva a emitir el comando **show ip route ospf** en el R1 para mostrar el efecto que produjo este cambio en la tabla de routing. Todas las rutas OSPF para el R1 ahora se enrutan a través del R2.

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.

```

R1
Physical Config CLI
IOS Command Line Interface

Adjacency with neighbor 192.168.12.2
Suggests hello due to neighbors:
R1#show ip ospf ospf
O 192.168.2.0 [112/881] via 192.168.12.2, 00:09:04, Serial0/0/0
O 192.168.3.0 [112/144] via 192.168.12.2, 00:14:12, Serial0/0/1
O 192.168.22.0/24 is subnetted, 1 subnets
O 192.168.22.0 [112/881] via 192.168.12.2, 00:09:04, Serial0/0/1
R1#show r
Enter configuration commands, one per line. End with CTRL-Z.
R1(config)#sh ip route ospf
R1(config)#end
R1#
*RIP-6-CHANGES: Configured from console by rumbale

R1#show ip route ospf
O 192.168.2.0 [112/881] via 192.168.12.2, 00:11:59, Serial0/0/0
O 192.168.3.0 [112/881] via 192.168.12.2, 00:00:14, Serial0/0/1
O 192.168.22.0/24 is subnetted, 1 subnets
O 192.168.22.0 [112/7287] via 192.168.12.2, 00:00:14, Serial0/0/1
O 192.168.12.2 [112/7287] via 192.168.12.2, 00:00:14, Serial0/0/0
R1#show ip route ospf
O 192.168.2.0 [112/881] via 192.168.12.2, 00:12:16, Serial0/0/0
O 192.168.3.0 [112/881] via 192.168.12.2, 00:06:01, Serial0/0/1
O 192.168.22.0/24 is subnetted, 1 subnets
O 192.168.22.0 [112/7287] via 192.168.12.2, 00:06:01, Serial0/0/1
O 192.168.12.2 [112/7287] via 192.168.12.2, 00:06:01, Serial0/0/0
R1#show r
Enter configuration commands, one per line. End with CTRL-Z.
R1(config)#sh ip route ospf
R1(config)#sh ip route ospf cost 1565
R1(config)#end
R1#
*RIP-6-CHANGES: Configured from console by rumbale

R1#show ip route ospf
O 192.168.2.0 [112/881] via 192.168.12.2, 00:22:40, Serial0/0/0
O 192.168.3.0 [112/1444] via 192.168.12.2, 00:00:22, Serial0/0/1
O 192.168.22.0/24 is subnetted, 1 subnets
O 192.168.22.0 [112/7287] via 192.168.12.2, 00:00:22, Serial0/0/0
R1#
  
```

8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3 (Yolima Vargas Escobar)

Topología

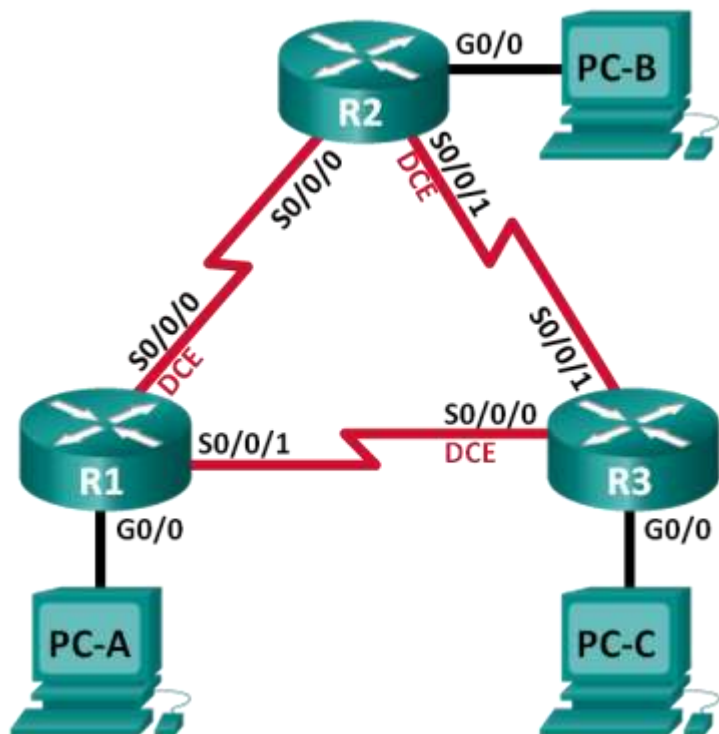


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

Información básica/situación

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

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

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio.

Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

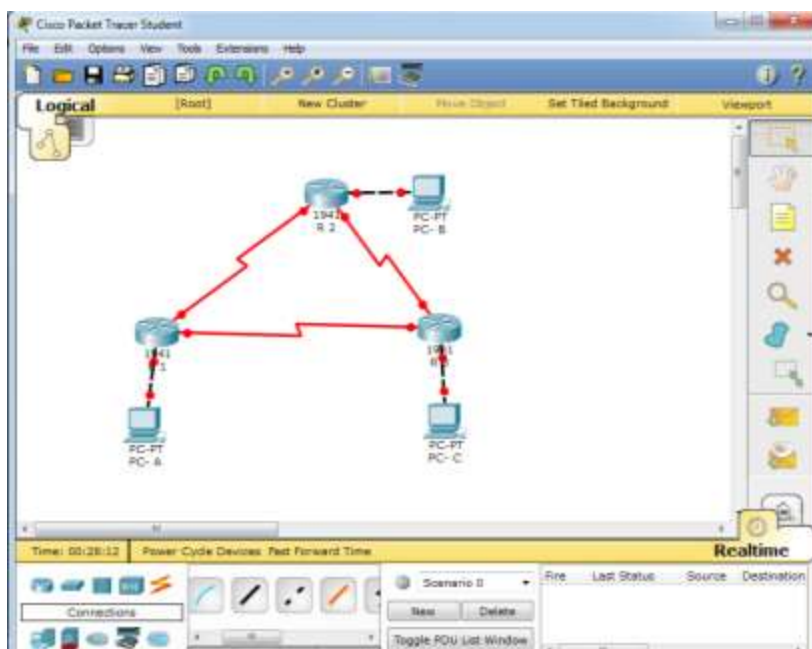
Recursos necesarios

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

Parte 7. armar la red y configurar los parámetros básicos de los dispositivos

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

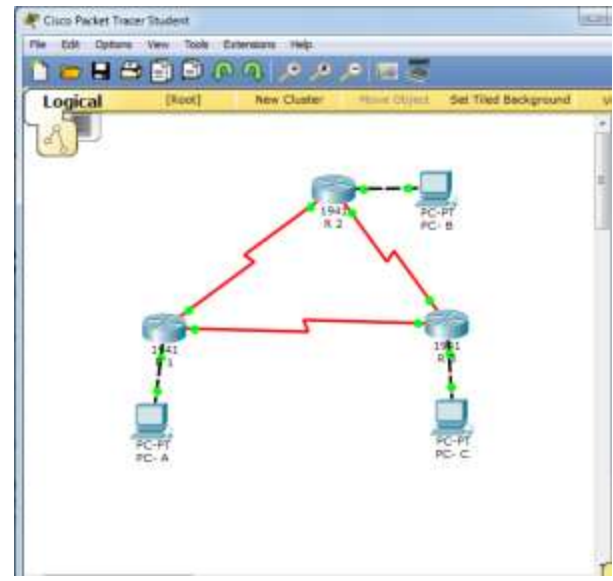
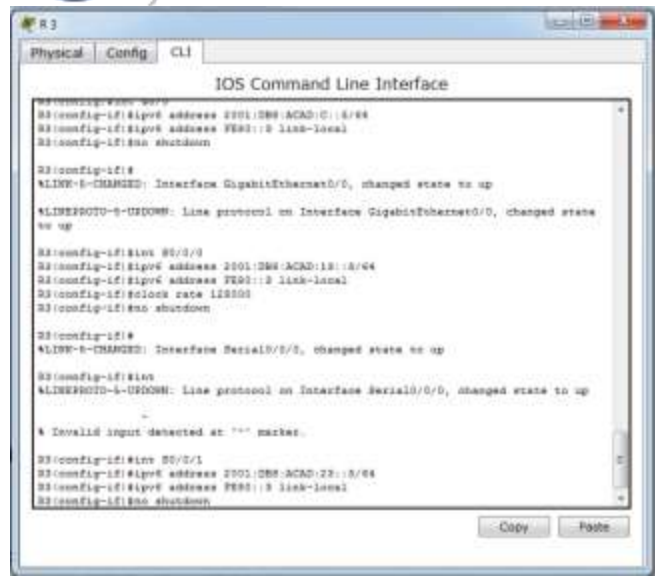
Paso 1. realizar el cableado de red tal como se muestra en la topología.



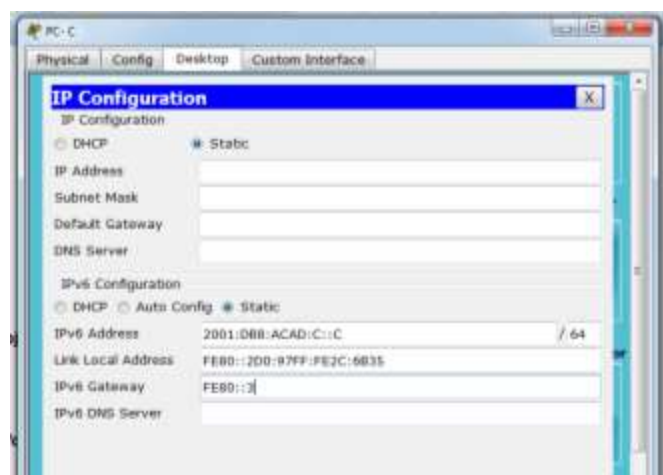
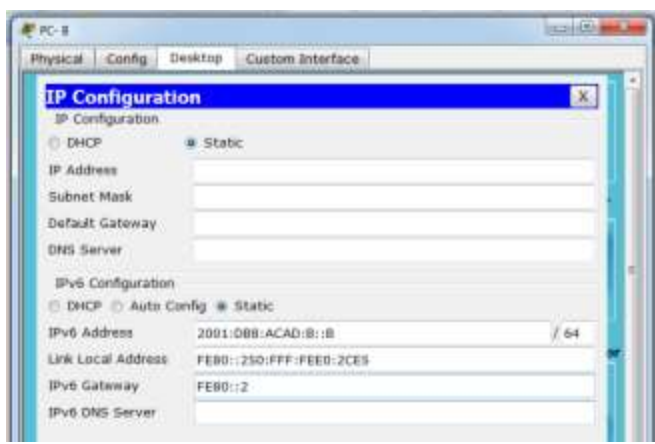
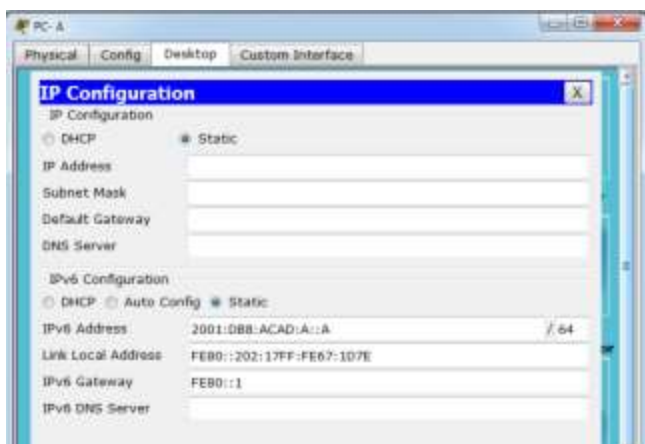
Paso 2. inicializar y volver a cargar los routers según sea necesario.

Paso 3. configurar los parámetros básicos para cada router.

- 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.

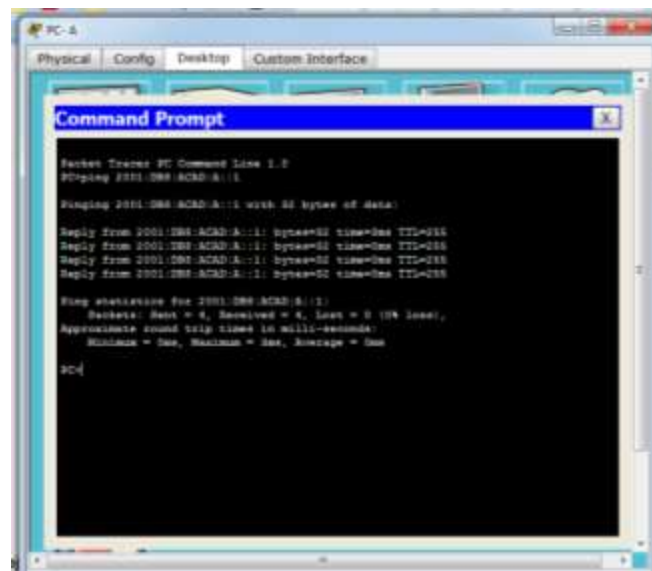
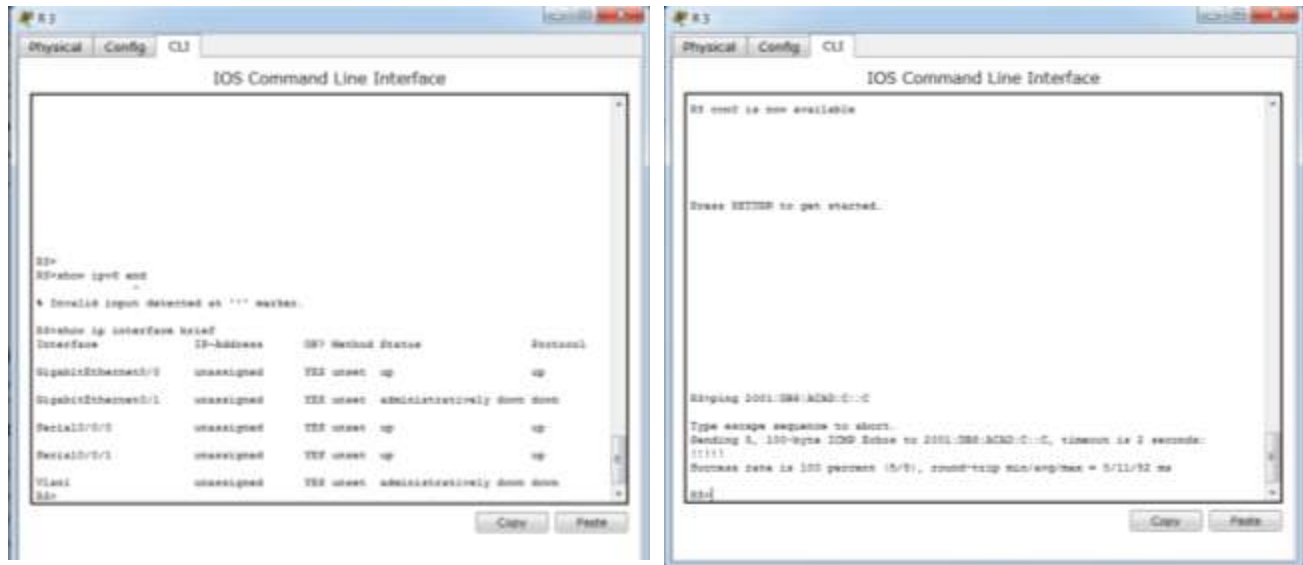


Paso 4. configurar los equipos host.



Paso 5. Probar la conectividad.

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



Parte 8. configurar el routing OSPFv3

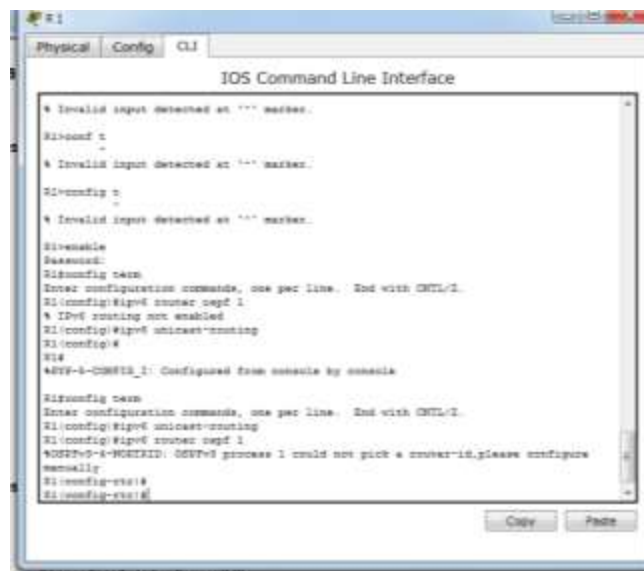
En la parte 2, configurará el routing OSPFv3 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente.

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
```



```
R1
Physical Config CLI
IOS Command Line Interface
% Invalid input detected at '^' marker.
R1>conf t
% Invalid input detected at '^' marker.
R1>conf t
% Invalid input detected at '^' marker.
R1>enable
R1>do conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
% IPv6 routing not enabled
R1(config)#ipv6 unicast-routing
R1(config)#
R1#
ADVF-1-CONF1_1: Configured from console by console
R1>do conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 1
%OSPFv3-4-MISSING: OSPFv3 process 1 could not pick a router-id, please configure manually
R1(config-rt1)#
R1(config-rt1)#
```

Para que nos deje insertar este comando debemos primero ingresar el comando **ipv6 unicast-routing** como lo muestra la grafica.

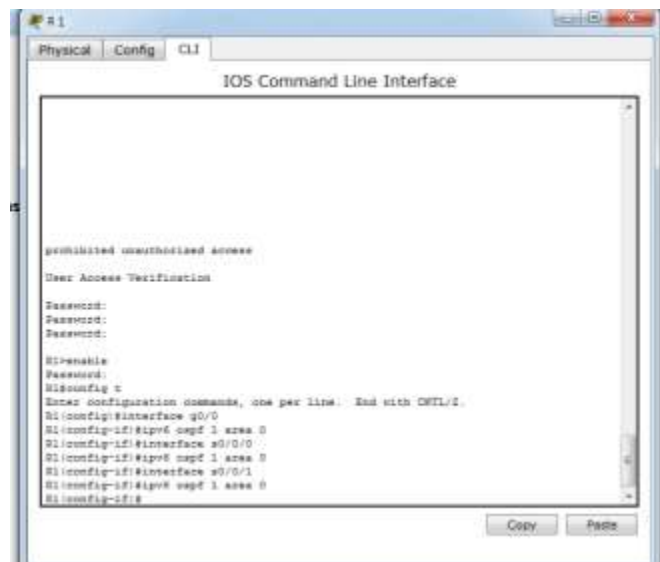
- d. Emita el comando **show ipv6 ospf** para verificar las ID de router de todos los routers.

R2# **show ipv6 ospf**

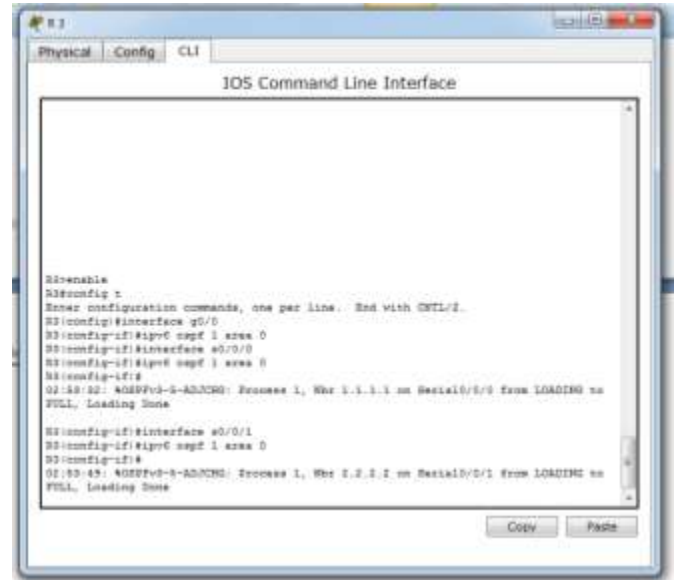
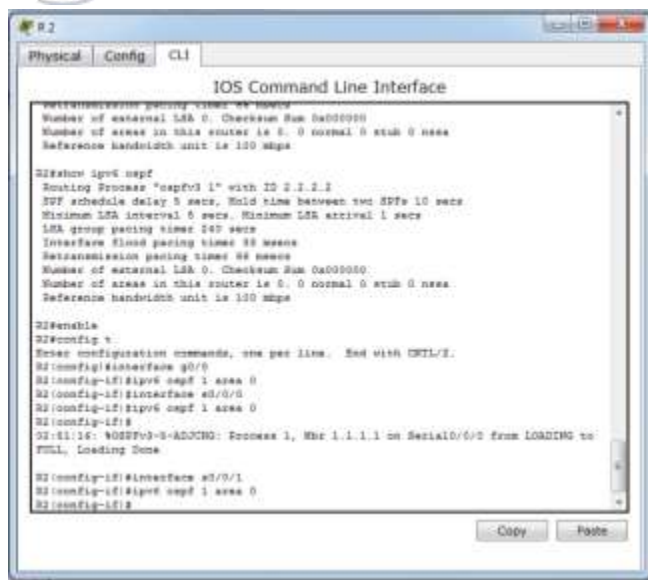


Con IPv6, es común tener varias direcciones IPv6 configuradas en una interfaz. La instrucción network se eliminó en OSPFv3. En cambio, el routing OSPFv3 se habilita en el nivel de la interfaz.

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



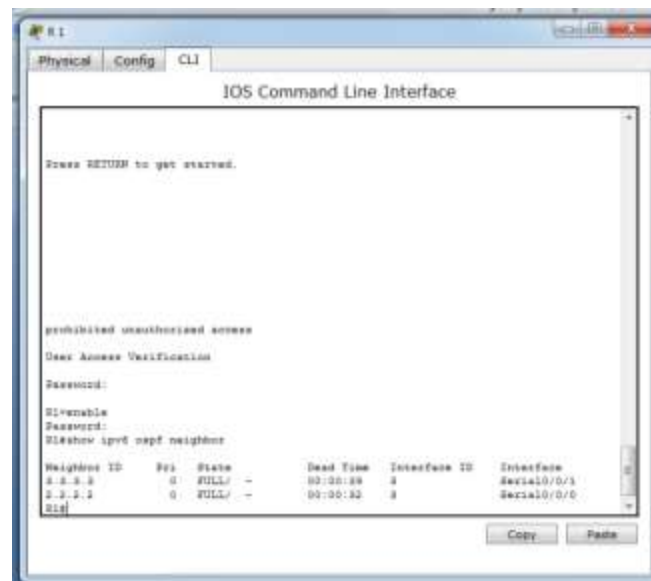
- f. Asigne las interfaces en el R2 y el R3 al área 0 de OSPFv3. Al agregar las interfaces al área 0, debería ver mensajes de adyacencia de vecino.



Paso 2. verificar vecinos de OSPFv3.

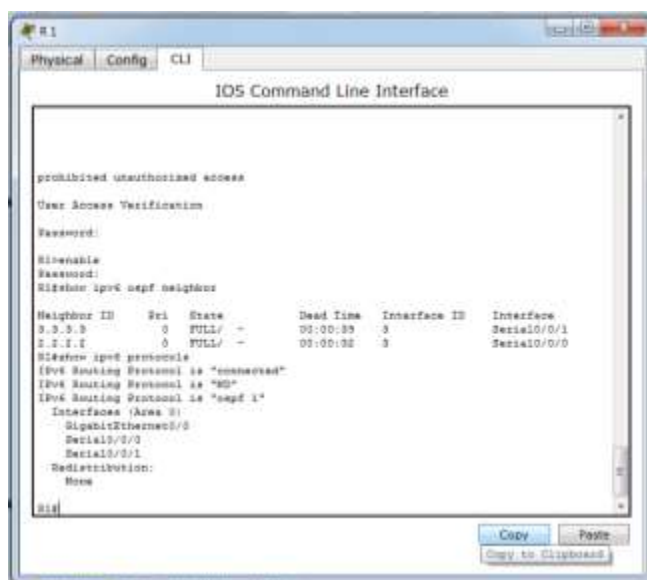
Emita el comando **show ipv6 ospf neighbor** para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.

R1# **show ipv6 ospf neighbor**



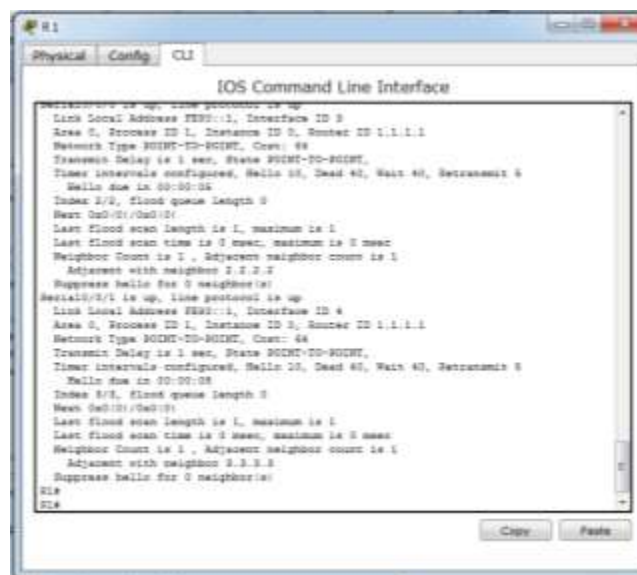
Paso 3. verificar la configuración del protocolo OSPFv3.

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.



Paso 4. verificar las interfaces OSPFv3.

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



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

```
R1# show ipv6 ospf interface brief
```

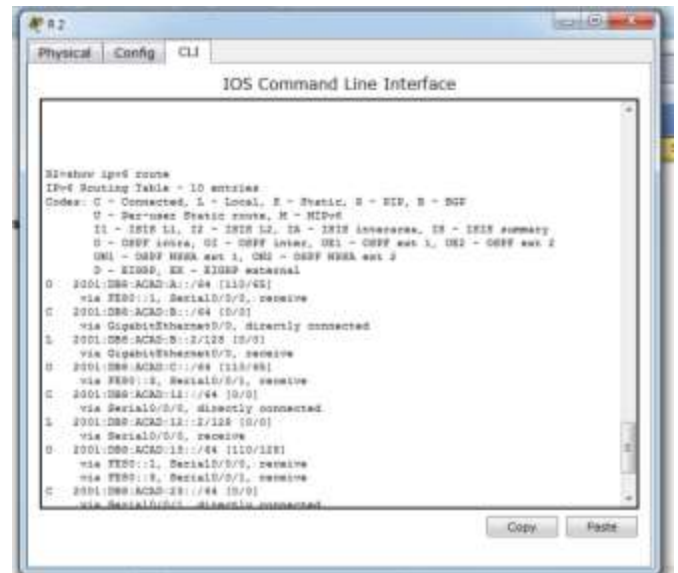
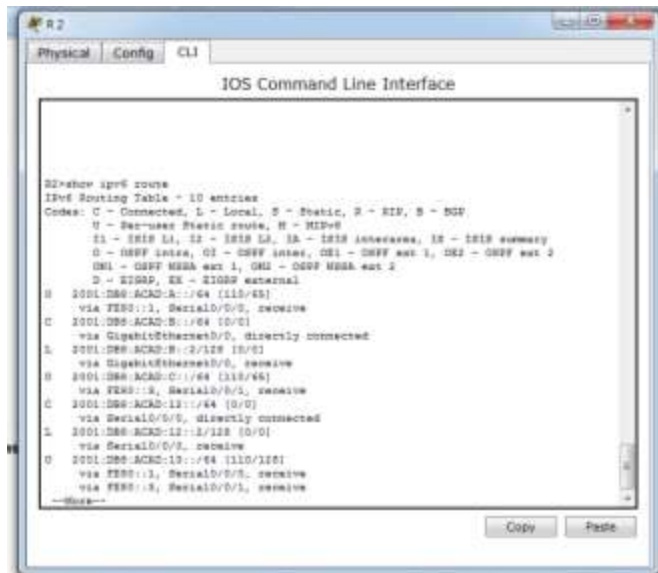
Este comando no permite ver la tabl de costos pero en eos anteriores pantallazos se sacaron con el anterior comando podemos ver los costos por eso diseñe esta tabla donde nos muestra.

Interface	PID	Area	Intf ID	Cost	State	Nbrs F/C
S0/0/1	1	0	7	64	P2P	1/1
S0/0/0	1	0	6	64	P2P	1/1
GI0/0	1	0	3	1	DR	0/0

Paso 5. 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
```



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

RTA: show ipv6 route ospf

Paso 6. 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-A
Physical Config Desktop Custom Interface
Command Prompt
Pinging 2001:DB8:ACAD:A::1
Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255

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

PC>ping 2001:DB8:ACAD:B::8
Pinging 2001:DB8:ACAD:B::8 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=23ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 23ms, Average = 11ms
    
```

```

PC-A
Physical Config Desktop Custom Interface
Command Prompt
Pinging 2001:DB8:ACAD:B::8
Pinging 2001:DB8:ACAD:B::8 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=23ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 23ms, Average = 11ms

PC>ping 2001:DB8:ACAD:C::1C
Pinging 2001:DB8:ACAD:C::1C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::1C: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:C::1C: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:C::1C: bytes=32 time=6ms TTL=126
Reply from 2001:DB8:ACAD:C::1C: bytes=32 time=11ms TTL=126

Ping statistics for 2001:DB8:ACAD:C::1C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 13ms, Average = 10ms
    
```

```

PC-B
Physical Config Desktop Custom Interface
Command Prompt
Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=12ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=12ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=12ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=126

Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 13ms, Average = 12ms

PC>2001:DB8:ACAD:C::C
Invalid Command

PC>ping 2001:DB8:ACAD:C::C
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=11ms TTL=126

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 11ms, Average = 11ms
    
```

```

PC-C
Physical Config Desktop Custom Interface
Command Prompt
Pinging 2001:DB8:ACAD:A::A
Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=14ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=4ms TTL=126

Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 14ms, Average = 10ms

PC>ping 2001:DB8:ACAD:B::8
Pinging 2001:DB8:ACAD:B::8 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=12ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=0ms TTL=126
Reply from 2001:DB8:ACAD:B::8: bytes=32 time=12ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 6ms
    
```

Parte 9. 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**

```

R1
-----
prohibited unauthorized access
User Access Verification

Password:

R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 0
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 0
Hello due in 00:00:04
Index 1/1, Flood queue length 0
Next Send(0)/Del(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#
  
```

- 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**

```

R1
-----
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 0
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 0
Hello due in 00:00:04
Index 1/1, Flood queue length 0
Next Send(0)/Del(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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#
R1#
  
```


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

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

```

R1# show ipv6 ospf interface g0/0
 GigabitEthernet0/0 is up, line protocol is up
 Link Local Address FE80::1, Interface ID 1
 Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
 Network Type BROADCAST, Cost: 1
 Transit 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 30, Dead 60, Wait 60, Retransmit 5
 No Hello received on interface
 Dead R/L, Flood queue length 0
 Max H/L/R/Ret: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#
  
```

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

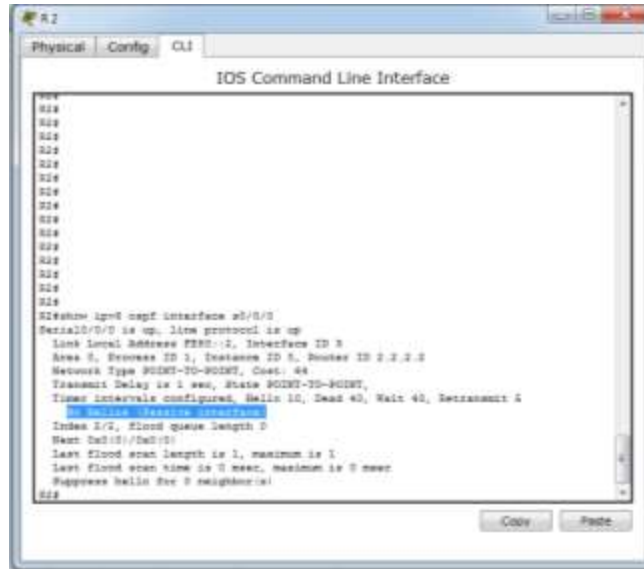
R2# **show ipv6 route ospf**

```

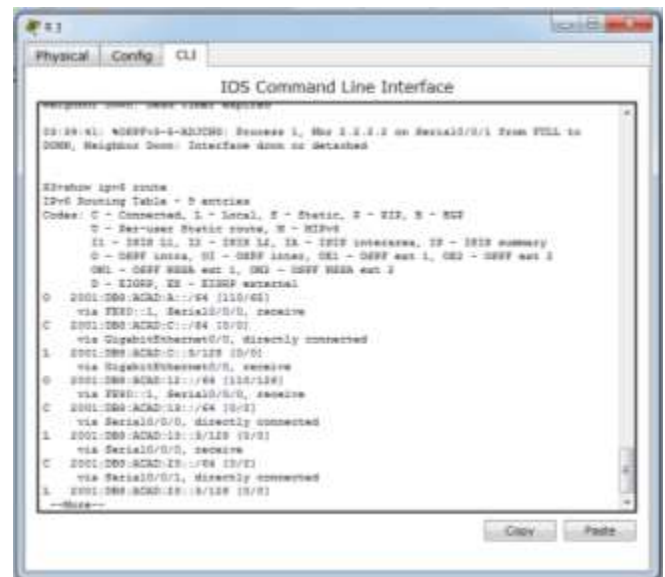
R2# show ipv6 route ospf
 IPv6 Routing Table = 10 entries
 Codes: C - Connected, L - Local, S - Static, D - RIP, B - BGP
 U - Per-user Static route, H - HIPv6
 H - ISIS H1, H2 - ISIS L2, HA - ISIS L1/HEA, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OI1 - OSPF ext 1, OI2 - OSPF ext 2
 OI1 - OSPF NBAR ext 1, OI2 - OSPF NBAR ext 2
 D - EIGRP, EX - EIGRP external
 2001:DB8:ACAD:A::/64 (110/64)
 via FE80::1, Serial0/0/0
 0: 2001:DB8:ACAD:C::/64 (110/64)
 via FE80::3, Serial0/0/0
 0: 2001:DB8:ACAD:19::/64 (110/120)
 via FE80::1, Serial0/0/0
 via FE80::3, Serial0/0/0
 R2#
  
```


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

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



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

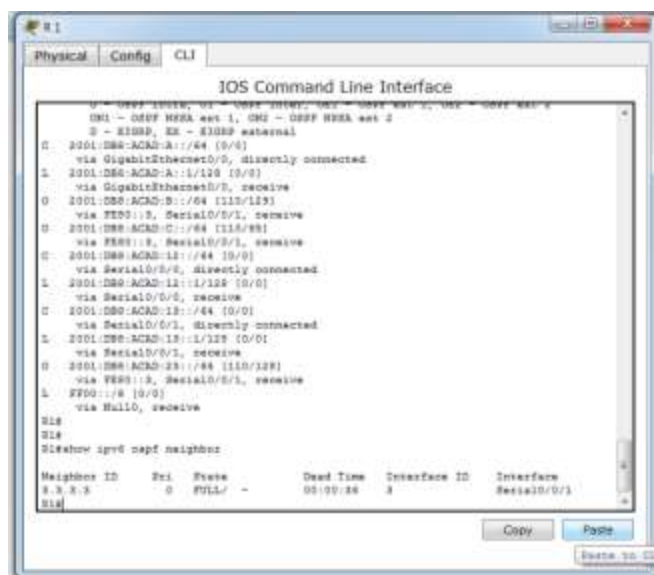
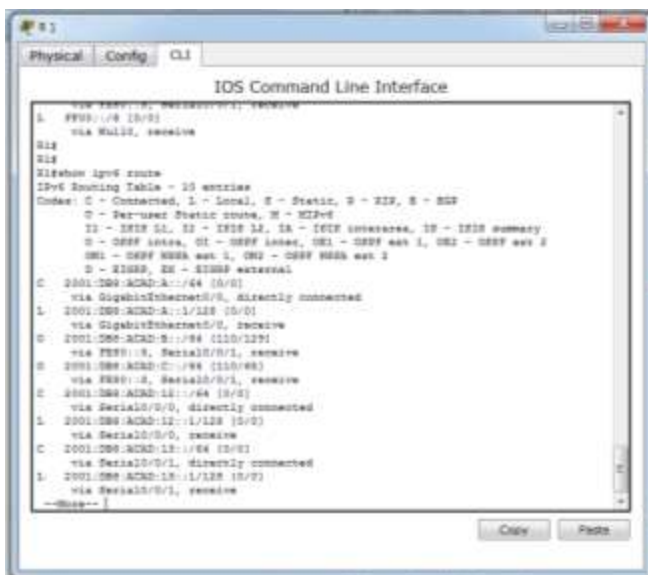


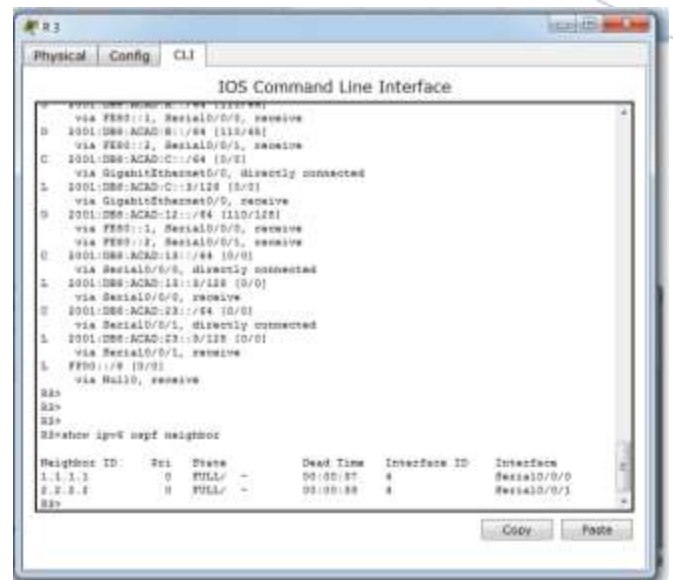
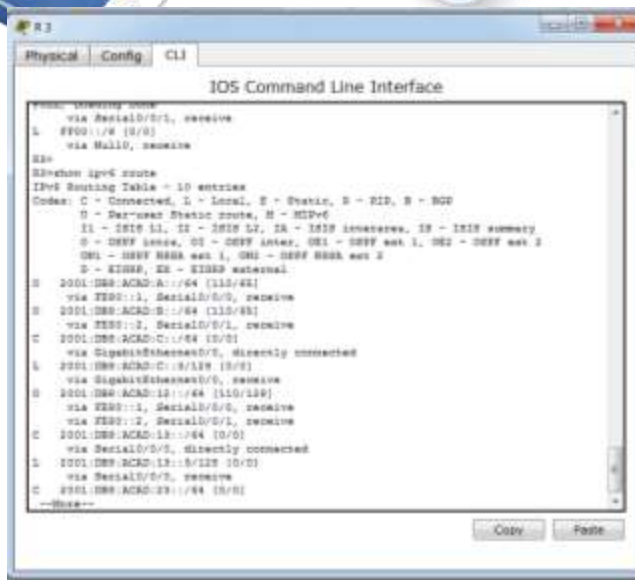
- e. Ejecute el comando **no passive-interface** para cambiar S0/0/1 en el R2 a fin de que envíe y reciba actualizaciones de routing OSPFv3. Después de introducir este comando, aparece un mensaje informativo que explica que se estableció una adyacencia de vecino con el R3.

```
R2(config)# ipv6 router ospf 1
R2(config-rtr)# no passive-interface s0/0/1
```



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





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

RTA. Interfaz S 0/0/1

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

RTA. Costo acumulado 129

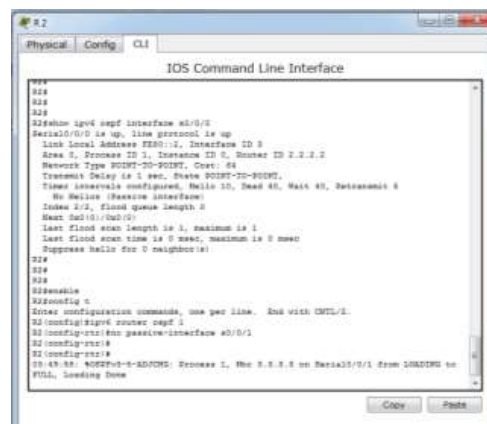
¿El R2 aparece como vecino OSPFv3 en el R1? **RTA** No

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

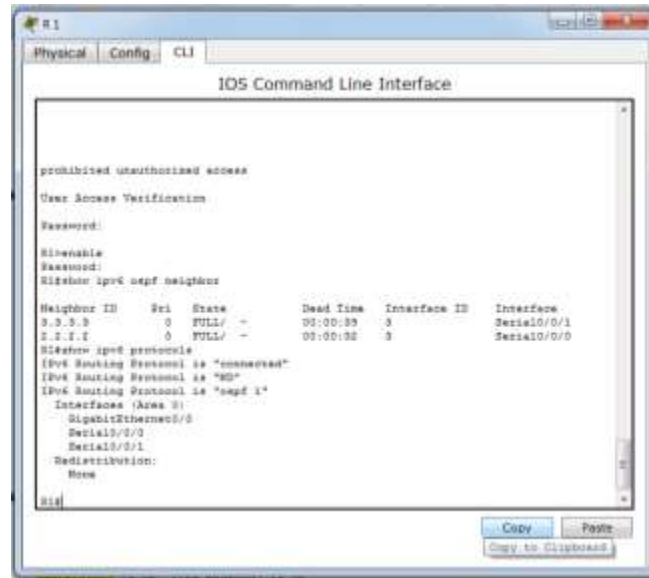
¿Qué indica esta información?

RTA: Que la configuración que se realiza al R 2 la interfaz conectada al R 1 se configuro como interfaz pasiva.

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



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



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, siempre y cuando el ID del proceso sea el mismo al crear el proceso de routing y al asignarlo a la interfaz.

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

RTA: OSPF V3 se configurara directamente en cada interfaz, y este usa el comando: `ipv6 ospf ID-proceso área ID área`, esto se hace porque en IPV6 podemos asignar diferentes direcciones a la misma interfaz, con agregar la interfaz se agregan todas las subredes.

Tabla de resumen de interfaces del router

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

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

10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router (Yolima Vargas Escobar)

Topología

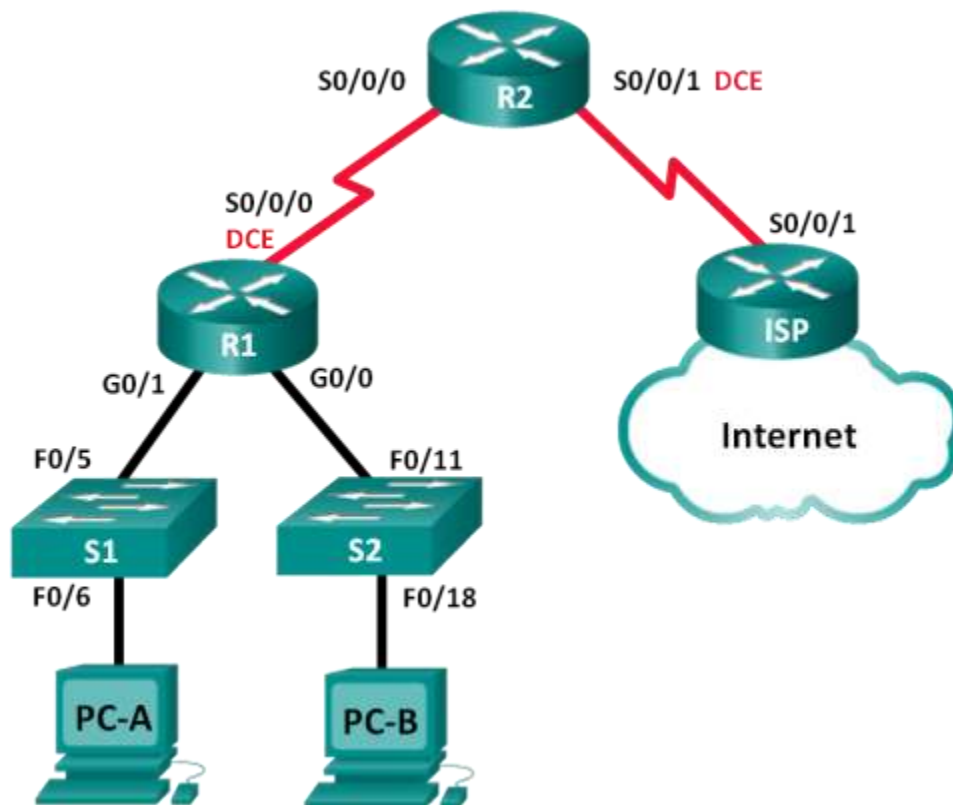


Tabla de direccionamiento

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

Objetivos

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

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

Información básica/situación

El protocolo de configuración dinámica de host (DHCP) es un protocolo de red que permite a los administradores de red administrar y automatizar la asignación de direcciones IP. Sin DHCP, el administrador debe asignar y configurar manualmente las direcciones IP, los servidores DNS preferidos y los gateways predeterminados. A medida que aumenta el tamaño de la red, esto se convierte en un problema administrativo cuando los dispositivos se trasladan de una red interna a otra.

En esta situación, la empresa creció en tamaño, y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su tarea es configurar el router R2 para asignar direcciones IPv4 en dos subredes diferentes conectadas al router R1.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen 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

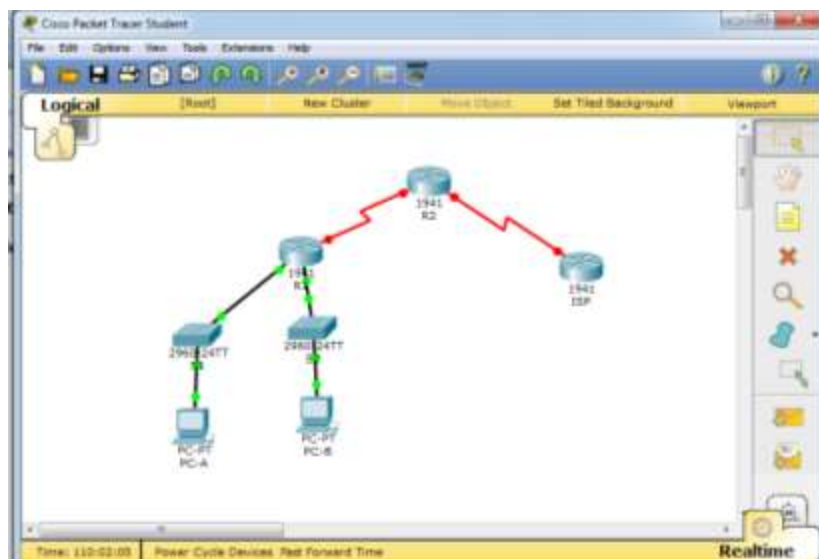
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

Parte 10. armar la red y configurar los parámetros básicos de los dispositivos

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

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

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



Paso 3. configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.



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

```

R1>
R1>
R1>
R1>conf t
  % Invalid input detected at '' marker.
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line console
  % Incomplete command.
R1(config)#line console 0
R1(config-line)#logging local
  % Invalid input detected at '' marker.
R1(config-line)#logging local
R1(config-line)#logging synchronous
  % Invalid input detected at '' marker.
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 4 15
R1(config-line)#exit
R1#conf t
  
```

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

```

R1#conf t
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#interface S0/0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-3-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1(config-if)#interface S0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-3-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1(config-if)#interface
  
```

```

R2
Cisco C1800-941/K9 (revision 1.0) with 491520K/927488 bytes of memory.
PowerPC board ID FTH13143982
3 Gigabit Ethernet interfaces
1 Low-speed serial (async/caprol) network interface(s)
1024K configuration memory at 8K bits wide with parity disabled.
256K bytes of non-volatile configuration memory.
249664K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no

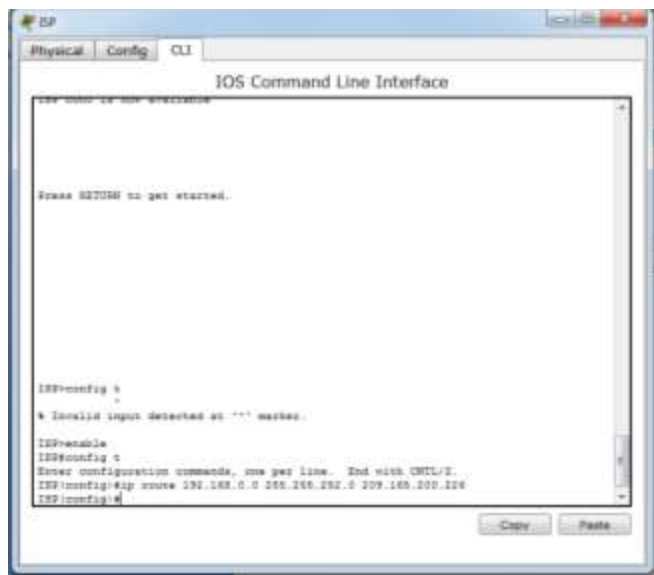
Press RETURN to get started!

Router#enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#name S0/0/0
R2(config-if)#ip address 192.168.2.254 255.255.255.252
R2(config-if)#no shutdown

%LINK-3-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#
  
```

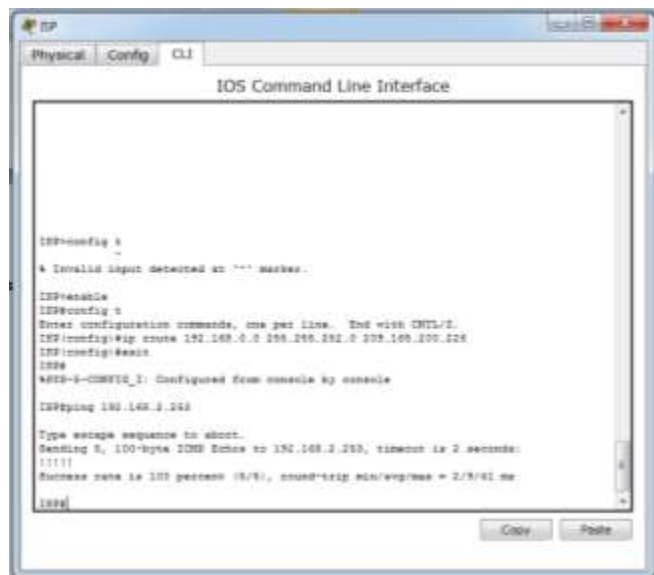

j. Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.

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

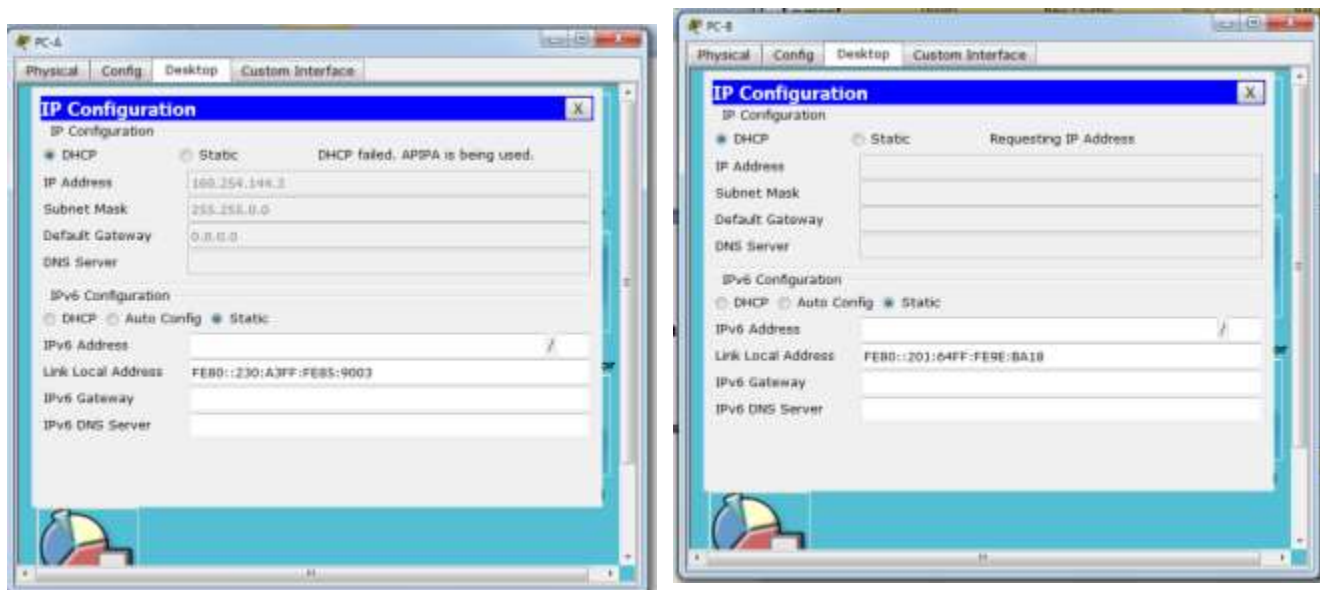


Paso 4. verificar la conectividad de red entre los routers.

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.



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



Parte 11. configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

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

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

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

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

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

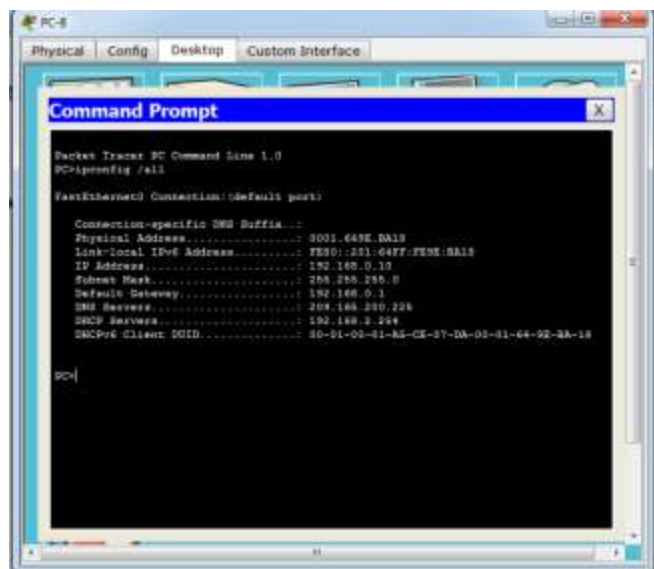
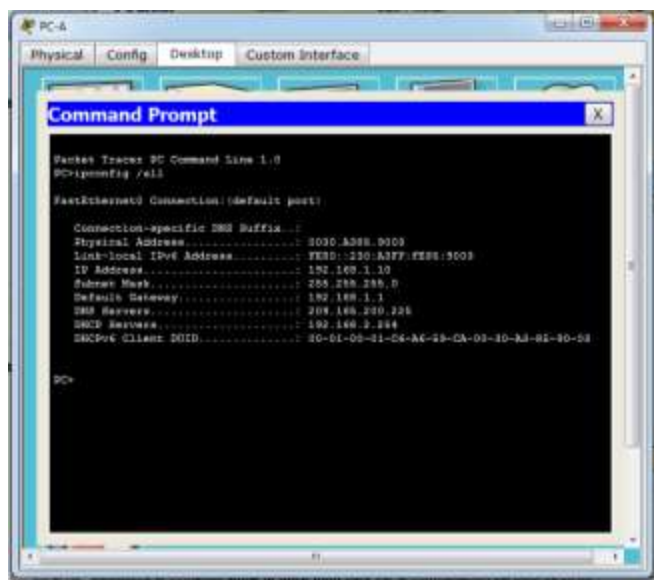
En las líneas a continuación, escriba los comandos necesarios para configurar el R1 como agente de retransmisión DHCP para las LAN del R1.

RTA:

```
R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
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)#
```

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 en la grafica podemos apreciar.

Physical Address.....: 0030.A385.9003
 Link-local IPv6 Address.....: FE80::230:A3FF:FE85:9003
 IP Address.....: 192.168.1.10

PC-B

Physical Address.....: 0001.649E.BA18
 Link-local IPv6 Address.....: FE80::201:64FF:FE9E:BA18
 IP Address.....: 192.168.0.10

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

RTA:

PC-A: 192.168.1.10

PC-B: 192.168.0.10

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

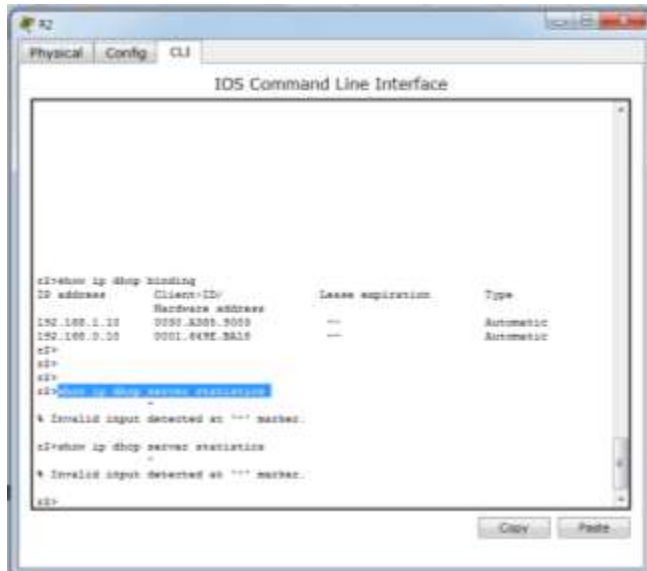
- a. En el R2, introduzca el comando **show ip dhcp binding** para ver los arrendamientos de direcciones DHCP.



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

RTA: Las direcciones de hardware del cliente permiten identificarlas computadoras que se unen a la red.

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

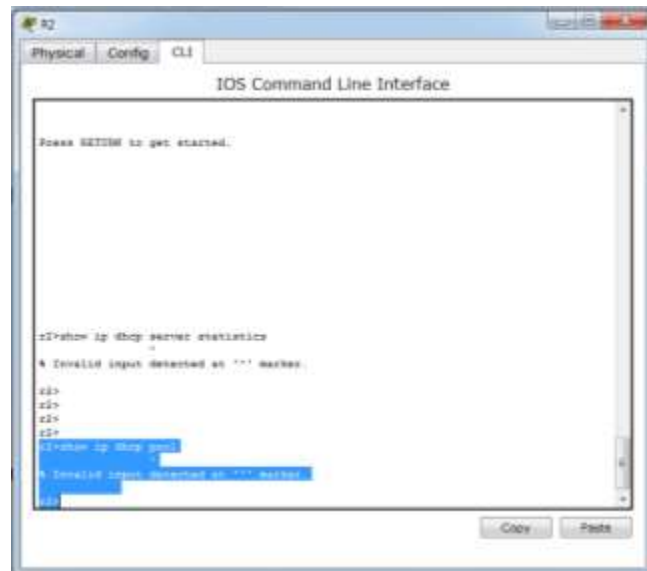


¿Cuántos tipos de mensajes DHCP se indican en el resultado?

RTA: como se puede apreciar en la grafica al ingresar este comando me genera invalidez.

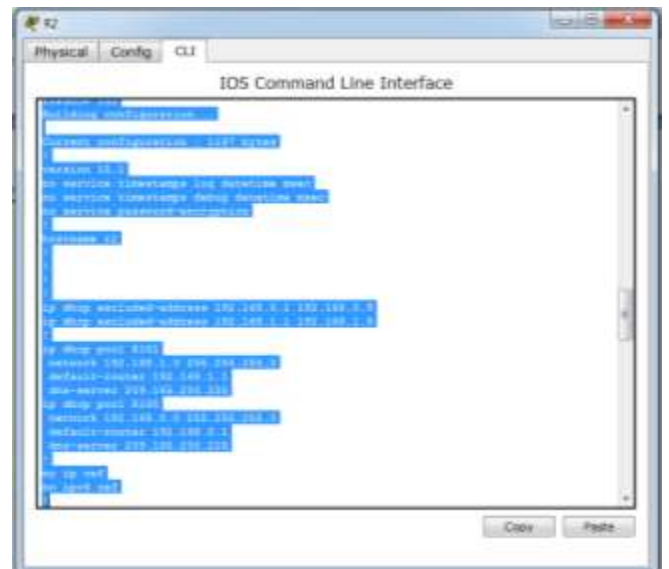
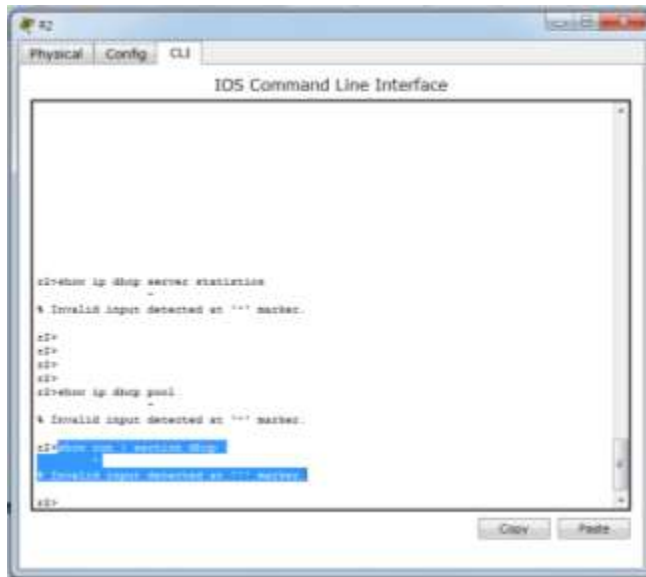
b. En el R2, introduzca el comando **show ip dhcp pool** para ver la configuración del pool de DHCP.

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



RTA: como se puede apreciar en la grafica al ingresar este comando me genera invalidez

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



Nota: con el comando completo me genera error invalide, pero si solo ingreso el comando show run sale como podemos apreciar en la grafica.

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



NOTA: en el R2 nos da invalidez este comando, pero si ingresamos el R1 y le damos el comando show run interface nos genera como esta en la grafica.

Reflexión

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

RTA: Tener un servidor DHCP independiente para cada subred lo que hace es que se vuelve más despacioso el equipo por eso es recomendable configurar en un solo router el DHCP, porque le quitamos hardware.

Lo otro es que si se le coloca DHCP a cada router se hace más difícil la administración de estos, por eso es recomendable en uno solo.

Tabla de resumen de interfaces del router

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

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

10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch (Adriana Romero Ramirez)

Topología

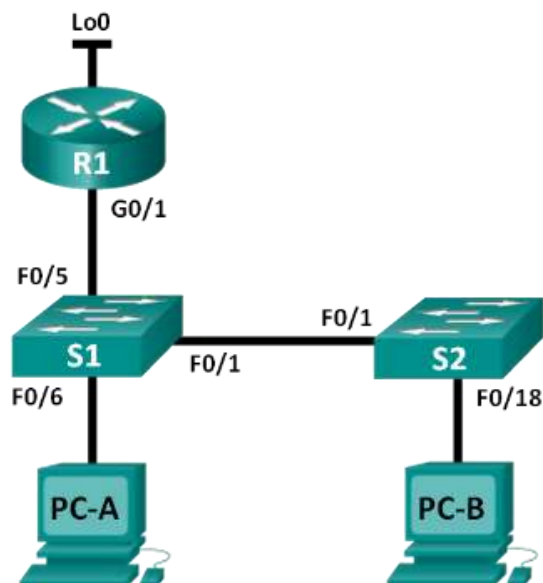


Tabla de direccionamiento

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

Objetivos

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

Parte 2: cambiar la preferencia de SDM

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

Parte 3: configurar DHCPv4

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

Parte 4: configurar DHCP para varias VLAN

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

Parte 5: habilitar el routing IP

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

Información básica/situación

Un switch Cisco 2960 puede funcionar como un servidor de DHCPv4. El servidor de DHCPv4 de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones identificados que están asociados a VLAN específicas e interfaces virtuales de switch (SVI). El switch Cisco 2960 también puede funcionar como un dispositivo de capa 3 y hacer routing entre VLAN y una cantidad limitada de rutas estáticas. En esta práctica de laboratorio, configurará DHCPv4 para VLAN únicas y múltiples en un switch Cisco 2960, habilitará el routing en el switch para permitir la comunicación entre las VLAN y agregará rutas estáticas para permitir la comunicación entre todos los hosts.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

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

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

Recursos necesarios

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

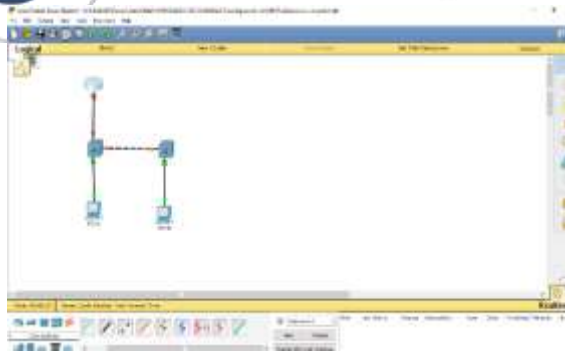
Parte 12: armar la red y configurar los parámetros básicos de los dispositivos

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

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

Paso 3: configurar los parámetros básicos en los dispositivos.

- a. Asigne los nombres de dispositivos como se muestra en la topología.



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

```

R1
Physical Config CLI
IOS Command Line Interface
*****
Processor board ID FTK1240000
0 Gigabit Ethernet interfaces
DRAM configuration is 64 Kbits wide with parity disabled.
1536 bytes of non-volatile configuration memory.
149856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CTRL/Z.
Router(config)#int g0/1
Router(config-if)#ip address 192.168.1.10 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Copy Paste
    
```

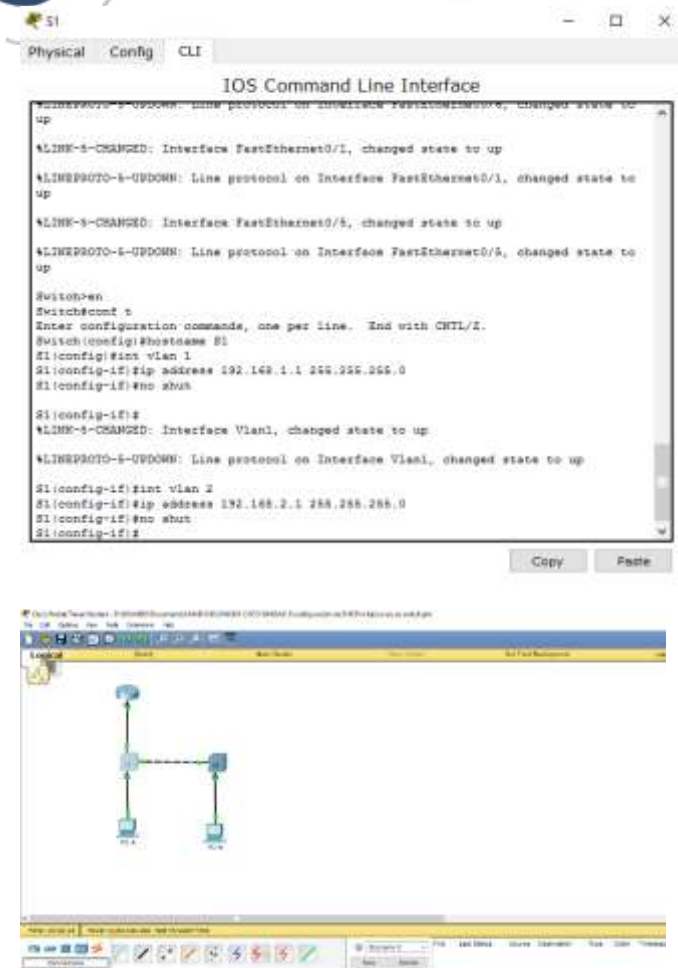
```

R1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CTRL/Z.
Router(config)#int lo 0
Router(config-if)#
%LINK-3-UPDOWN: Interface Loopback0, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ip address 209.148.200.228 255.255.255.224
Router(config-if)#ip address 209.148.200.229 255.255.255.224
Router(config-if)#no shut
Router(config-if)#
Copy Paste
    
```

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



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

Parte 13: 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
Physical Config CLI
IOS Command Line Interface
S1(config)#int vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shut

S1(config-if)#
%LINK-3-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
S1(config-if)#int vlan 2
S1(config-if)#ip address 192.168.2.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show sdm prefer
-
% Invalid input detected at '^' marker.

S1#
    
```

¿Cuál es la plantilla actual?

Las respuestas pueden variar , pero puede ser default o dual-ipv4and-ipv6 defaultl o lanbase-routing

Paso 2: cambiar la preferencia de SDM en el S1.

- a. Establezca la preferencia de SDM en **lanbase-routing**. (Si lanbase-routing es la plantilla actual, continúe con la parte 3). En el modo de configuración global, emita el comando **sdm prefer lanbase-routing**.

```

S1(config)# sdm prefer lanbase-routing
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
    
```

¿Qué plantilla estará disponible después de la recarga? _____

- b. Se debe volver a cargar el switch para que la plantilla esté habilitada.

```

S1# reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
    
```

Nota: la nueva plantilla se utilizará después del reinicio, incluso si no se guardó la configuración en ejecución. Para guardar la configuración en ejecución, responda **yes** (sí) para guardar la configuración modificada del sistema.



Paso 3: verificar que la plantilla lanbase-routing esté cargada.

Emita el comando **show sdm prefer** para verificar si la plantilla lanbase-routing se cargó en el S1.

S1# **show sdm prefer**

The current template is "lanbase-routing" template.
 The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

number of unicast mac addresses:	4K
number of IPv4 IGMP groups + multicast routes:	0.25K
number of IPv4 unicast routes:	0.75K
number of directly-connected IPv4 hosts:	0.75K
number of indirect IPv4 routes:	16
number of IPv6 multicast groups:	0.375k

```

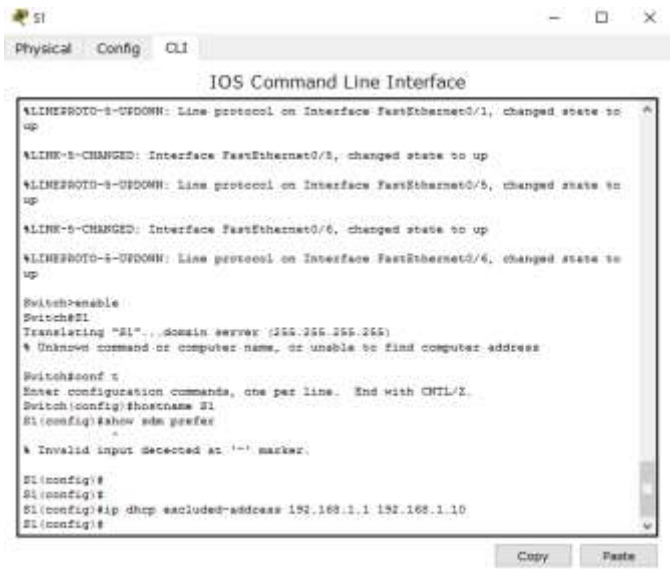
number of directly-connected IPv6 addresses:      0.75K
number of indirect IPv6 unicast routes:          16
number of IPv4 policy based routing aces:        0
number of IPv4/MAC qos aces:                    0.125k
number of IPv4/MAC security aces:               0.375k
number of IPv6 policy based routing aces:        0
number of IPv6 qos aces:                        0.375k
number of IPv6 security aces:                   127
    
```

Parte 14: 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.



dhcp excluded-address

- b. Cree un pool de DHCP con el nombre **DHCP1**. En el espacio proporcionado, escriba el comando que utilizó.

```

Switch#
%LINK-3-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-3-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

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

Switch#conf t
Enter configuration commands, one per line. End with CTRL/Z.
Switch(config)#hostname SI
SI(config)#show ip dhcp pool
% Invalid input detected at "" marker.

SI(config)#
SI(config)#
SI(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
SI(config)#ip dhcp pool DHCP1
SI(dhcp-config)#network 192.168.1.0 255.255.255.0
SI(dhcp-config)#
    
```

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.

```

Switch#
%LINK-3-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINK-3-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

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

Switch#conf t
Enter configuration commands, one per line. End with CTRL/Z.
Switch(config)#hostname SI
SI(config)#show ip dhcp pool
% Invalid input detected at "" marker.

SI(config)#
SI(config)#
SI(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
SI(config)#ip dhcp pool DHCP1
SI(dhcp-config)#network 192.168.1.0 255.255.255.0
SI(dhcp-config)#
    
```

Network 192.168.1.0

- d. Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.

```

Physical Config CLI
IOS Command Line Interface
%LINK-3-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-3-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
Switch#enable
Switch#
Switch#
Translating "SI"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Switch#conf t
Enter configuration commands, one per line. End with CTRL/Z.
Switch(config)#hostname SI
SI(config)#show sdn prefer
-
% Invalid input detected at '^' marker.

SI(config)#
SI(config)#
SI(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
SI(config)#ip dhcp pool DRCFI
SI(dhcp-config)#network 192.168.1.0 255.255.255.0
SI(dhcp-config)#default-router 192.168.1.1
SI(dhcp-config)#
SI(dhcp-config)#
  
```

default-router 192.168.1.0

- e. Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.

```

Physical Config CLI
IOS Command Line Interface
%LINK-3-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-3-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
Switch#enable
Switch#
Switch#
Translating "SI"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Switch#conf t
Enter configuration commands, one per line. End with CTRL/Z.
Switch(config)#hostname SI
SI(config)#show sdn prefer
-
% Invalid input detected at '^' marker.

SI(config)#
SI(config)#
SI(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
SI(config)#ip dhcp pool DRCFI
SI(dhcp-config)#network 192.168.1.0 255.255.255.0
SI(dhcp-config)#default-router 192.168.1.1
SI(dhcp-config)#dns-server 192.168.1.9
SI(dhcp-config)#
  
```

Dns-server

- f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

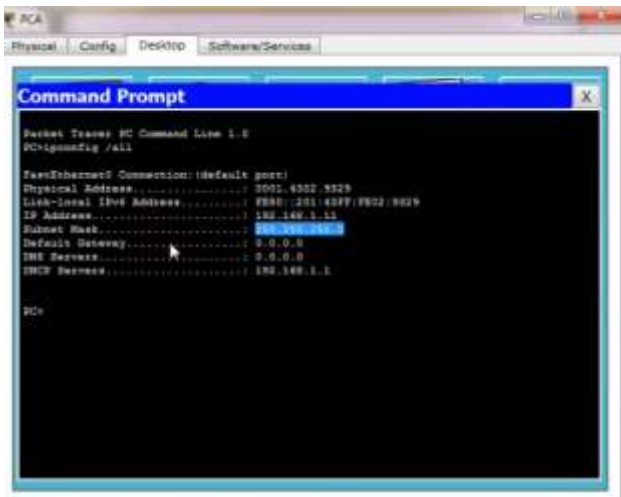


Lease, sin embargo packet tracer no soporta este comando

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

Paso 2: verificar la conectividad y DHCP.

- a. En la PC-A y la PC-B, abra el símbolo del sistema y emita el comando **ipconfig**. Si la información de IP no está presente, o si está incompleta, emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.



Para la PC-A, incluya lo siguiente:
 Dirección IP: 192.168.1.11
 Máscara de subred: 255.255.255.0
 Gateway predeterminado: 0.0.0


```

PC-B
Physical: Config Desktop Software/Services
Command Prompt
PC>ipconfig /all

Ethernet0 Connection (Default port):
Physical Address. . . . . 0001.4302.5029
Link-local IPv6 Address. . . . . FE80::201:42FF:FE14:5029
IP Address. . . . . 192.168.1.12
Subnet Mask. . . . . 255.255.255.0
Default Gateway. . . . . 192.168.1.1
DNS Servers. . . . . 192.168.1.1
WINS Servers. . . . .

PC>ipconfig /all

Ethernet0 Connection (Default port):
Physical Address. . . . . 0001.4302.5029
Link-local IPv6 Address. . . . . FE80::201:42FF:FE14:5029
IP Address. . . . . 192.168.1.12
Subnet Mask. . . . . 255.255.255.0
Default Gateway. . . . . 192.168.1.1
DNS Servers. . . . . 192.168.1.1
WINS Servers. . . . .
    
```

Para la PC-B, incluya lo siguiente:
 Dirección IP: 192.168.1.12
 Máscara de subred: 255.255.255.0
 Gateway predeterminado: 192.168.1.1

- b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.
 ¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? _____

```

PCA
Physical: Config Desktop Software/Services
Command Prompt
PC>ipconfig /all

Ethernet0 Connection (Default port):
Physical Address. . . . . 0001.4302.5029
Link-local IPv6 Address. . . . . FE80::201:42FF:FE14:5029
IP Address. . . . . 192.168.1.1
Subnet Mask. . . . . 255.255.255.0
Default Gateway. . . . . 192.168.1.1
DNS Servers. . . . . 192.168.1.1
WINS Servers. . . . .

PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

¿Es posible hacer ping de la PC-A a la PC-B? _____

```

PCA
Physical: Config Desktop Software/Services
Command Prompt
PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=255
Reply from 192.168.1.12: bytes=32 time=0ms TTL=255
Reply from 192.168.1.12: bytes=32 time=0ms TTL=255
Reply from 192.168.1.12: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
    
```

¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1? _____

Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.

Parte 15: configurar DHCPv4 para varias VLAN

En la parte 4, asignará la PC-A un puerto que accede a la VLAN 2, configurará DHCPv4 para la VLAN 2, renovará la configuración IP de la PC-A para validar DHCPv4 y verificará la conectividad dentro de la VLAN.

Paso 1: asignar un puerto a la VLAN 2.

Coloque el puerto F0/6 en la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

Paso 2: configurar DHCPv4 para la VLAN 2.

- Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.

- Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó.

- Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

- Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.

- Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.

- Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

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

Paso 3: verificar la conectividad y DHCPv4.

- 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: _____

Máscara de subred: _____

Gateway predeterminado: _____

- 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? _____

¿Es posible hacer ping de la PC-A a la PC-B? _____

¿Los pings eran correctos? ¿Por qué?

c. Emita el comando **show ip route** en el S1.

¿Qué resultado arrojó este comando?

Parte 16: habilitar el routing IP

En la parte 5, habilitará el routing IP en el switch, que permitirá la comunicación entre VLAN. Para que todas las redes se comuniquen, se deben implementar rutas estáticas en el S1 y el R1.

Paso 1: habilitar el routing IP en el S1.

a. En el modo de configuración global, utilice el comando **ip routing** para habilitar el routing en el S1.

```
S1(config)# ip routing
```

b. Verificar la conectividad entre las VLAN.

¿Es posible hacer ping de la PC-A a la PC-B? _____

¿Qué función realiza el switch?

c. Vea la información de la tabla de routing para el S1.

¿Qué información de la ruta está incluida en el resultado de este comando?

d. Vea la información de la tabla de routing para el R1.

¿Qué información de la ruta está incluida en el resultado de este comando?

e. ¿Es posible hacer ping de la PC-A al R1? _____

¿Es posible hacer ping de la PC-A a la interfaz Lo0? _____

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Paso 2: asignar rutas estáticas.

Habilitar el routing IP permite que el switch enrute entre VLAN asignadas en el switch. Para que todas las VLAN se comuniquen con el router, es necesario agregar rutas estáticas a la tabla de routing del switch y del router.

a. En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.

b. En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

c. Vea la información de la tabla de routing para el S1.
¿Cómo está representada la ruta estática predeterminada?

d. Vea la información de la tabla de routing para el R1.
¿Cómo está representada la ruta estática?

e. ¿Es posible hacer ping de la PC-A al R1? **SI**____
¿Es posible hacer ping de la PC-A a la interfaz Lo0? **SI**____

Reflexión

1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?

Tabla de resumen de interfaces del router

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

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

Apéndice A: comandos de configuración

Configurar DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
```

```
S1(dhcp-config)# lease 3
```

Configurar DHCPv4 para varias VLAN

```
S1(config)# interface f0/6  
S1(config-if)# switchport access vlan 2  
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10  
S1(config)# ip dhcp pool DHCP2  
S1(dhcp-config)# network 192.168.2.0 255.255.255.0  
S1(dhcp-config)# default-router 192.168.2.1  
S1(dhcp-config)# dns-server 192.168.2.9  
S1(dhcp-config)# lease 3
```

Habilitar routing IP

```
S1(config)# ip routing  
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10  
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```

10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6 (Yolima Vargas Escobar)

Topología



Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

Parte 4: configurar la red para DHCPv6 con estado

Recursos necesarios

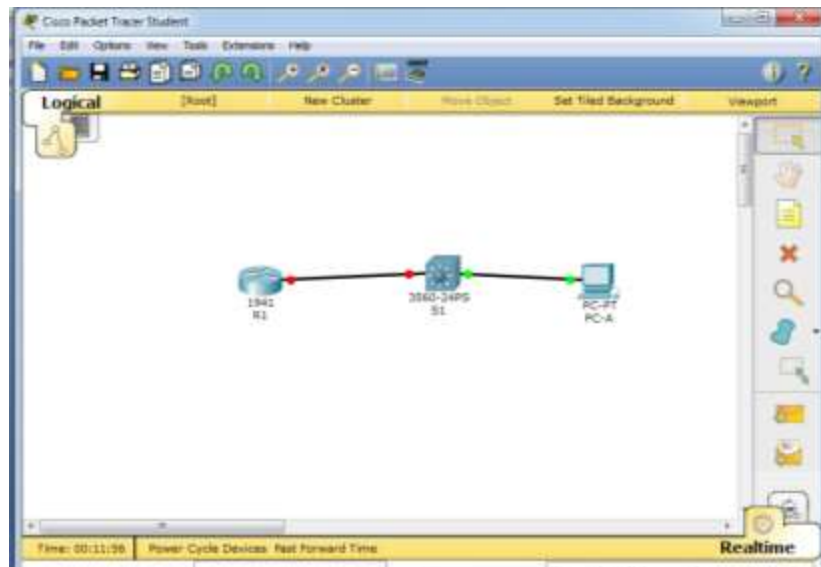
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para 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 17. armar la red y configurar los parámetros básicos de los dispositivos

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

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



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

Paso 3. Configurar R1

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.

```

IOS Command Line Interface

If you require further assistance please contact us by sending email to
support@cisco.com.

Class CISC01941/09 (revision 1.0) with 4914208/527680 bytes of memory,
Processor board ID F1N1A141094
3 Gigabit Ethernet interfaces
3 Low-speed serial (async/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
1024K bytes of non-volatile configuration memory.
149888K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: NO

Press RETURN to get started!

Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#
    
```


- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Guardar la configuración en ejecución en la configuración de inicio.

```

Router1
Physical Config CLI
IOS Command Line Interface
Switch#
Switch#enable
Switch#enable secret class
Switch#line console 0
% Denial input detected at "" marker.
Switch#line console 0
Switch#line password cisco
Switch#line login
Switch#line login why 0 0
Switch#line password class
Switch#line login
Switch#line logging synchronous
Switch#line banner motd #prohibited access to servers or unauthorized
personnel
Switch#service password-encryption
% Denial input detected at "" marker.
Switch#banner motd #prohibited access to or unauthorized personnel
Switch#service password-encryption
Switch#exit
Switch#
NATS-0-CONTRIC_1: Configured from console by console
Switch#
  
```

Paso 4. configurar el S1.

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.

```

S1
Physical Config CLI
IOS Command Line Interface

Switch cool is now available

Press RETURN to get started.

Switch#enable
Switch#configure t
Enter configuration commands, one per line. End with CTRL/Z.
Switch(config)#hostname S1
Switch(config)#
  
```

- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

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

```

Switch#enable
Switch#configure t
Enter configuration commands, one per line. End with CTRL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password class
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password class
S1(config-line)#login
S1(config-line)#
    
```

- g. Establezca el inicio de sesión de consola en modo sincrónico.
 h. Desactive administrativamente todas las interfaces inactivas.
 i. Guarde la configuración en ejecución en la configuración de inicio.

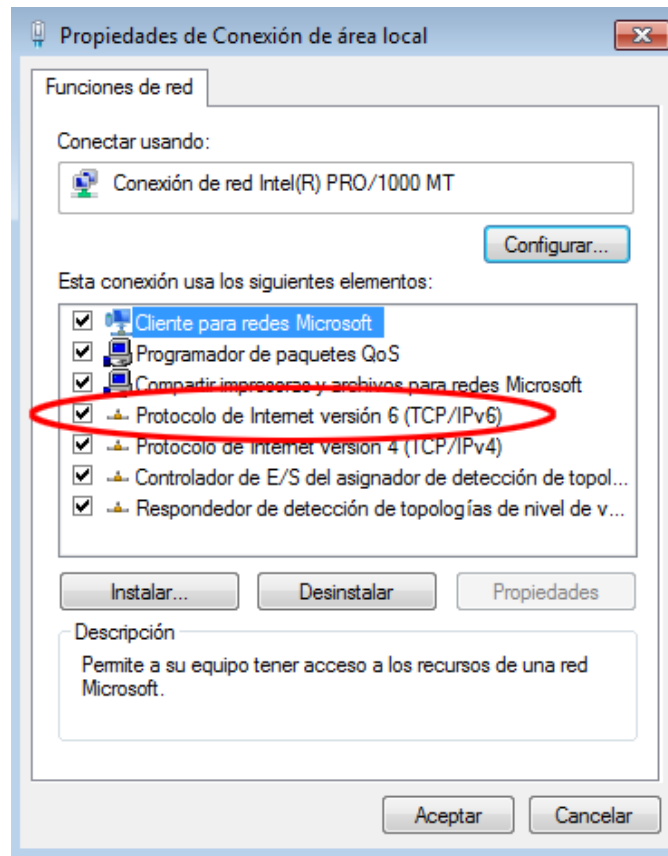
```

Switch#enable
Switch#configure t
Enter configuration commands, one per line. End with CTRL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password class
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password class
S1(config-line)#login
S1(config-line)#login synchronous
S1(config-line)#banner motd #prohibited unauthorized personal income#
S1(config)#service password-encryption
S1(config)#exit
S1#
*07/1-08/18/11: Configured from console by console
S1#
    
```

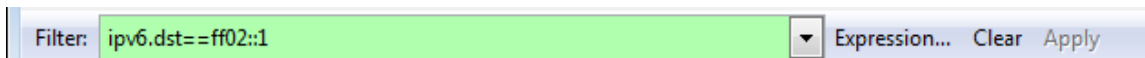
Parte 18. configurar la red para SLAAC

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.



- 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.



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.

```

Router1
Physical Config CLI
IOS Command Line Interface

Password:
R1#conf t
% Invalid input detected at '^' marker.

R1#enable
Translating "enable"...domain server (192.255.255.255)
% Unknown command or computer name, or unable to find computer address

R1#enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
ALINK-6-CRASHED: Interface GigabitEthernet0/1, changed state to up
ALINKS600-6-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up
R1(config-if)#

```

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

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

```

Router1
Physical Config CLI
IOS Command Line Interface

R1(config-if)#
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local addresses:
Global unicast addresses(we):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group addresses(we):
  FE80::1
  FF02::1:PT00:1
HDV is 1500 bytes
ICMP error message limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised neighbor interval is 0 (unspecified)
ND router advertisements are sent every 100 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Routers use stateless autoconfig for addresses.
R1#

```

Paso 4. configurar el S1.

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

```

S1
-----
Physical Config CLI
IOS Command Line Interface

%LINK-3-CHANGED: Interface FastEthernet0/24, changed state to up
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
Clear Access Verification

Password:
Password:
S1#conf t
Enter configuration commands, one per line. End with CTRL-Z.
S1(config)#interface vlan 1
S1(config-if)#ipv6 address autoconfig
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
    
```

Paso 5. verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

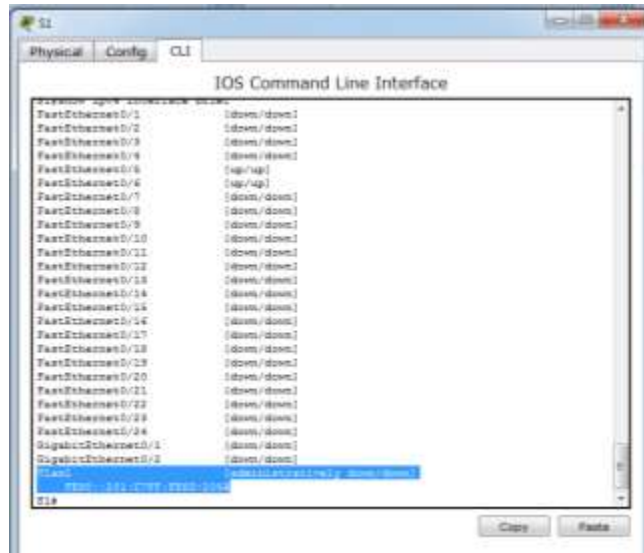
Use el comando **show ipv6 interface** para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

```

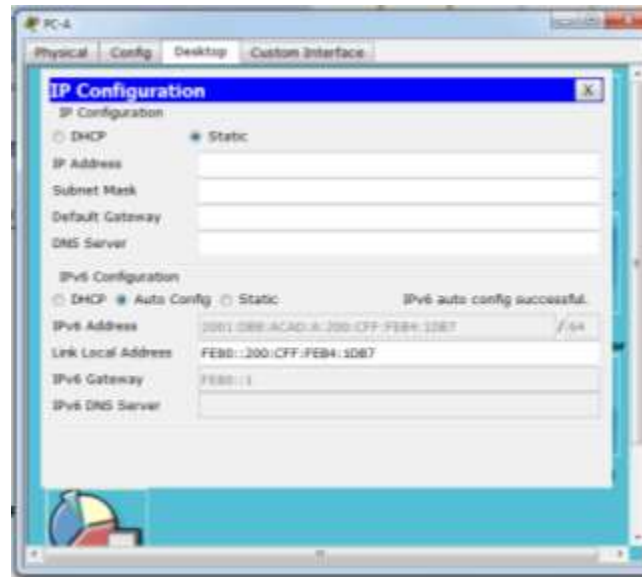
S1
-----
Physical Config CLI
IOS Command Line Interface

S1#
S1#
S1# show ipv6 interface brief
FastEthernet0/1          [down/down]
FastEthernet0/2          [down/down]
FastEthernet0/3          [down/down]
FastEthernet0/4          [down/down]
FastEthernet0/E          [up/up]
FastEthernet0/E          [up/up]
FastEthernet0/7          [down/down]
FastEthernet0/8          [down/down]
FastEthernet0/9          [down/down]
FastEthernet0/10         [down/down]
FastEthernet0/11         [down/down]
FastEthernet0/12         [down/down]
FastEthernet0/13         [down/down]
FastEthernet0/14         [down/down]
FastEthernet0/15         [down/down]
FastEthernet0/16         [down/down]
FastEthernet0/17         [down/down]
FastEthernet0/18         [down/down]
FastEthernet0/19         [down/down]
FastEthernet0/20         [down/down]
FastEthernet0/21         [down/down]
FastEthernet0/22         [down/down]
FastEthernet0/23         [down/down]
--More--
    
```

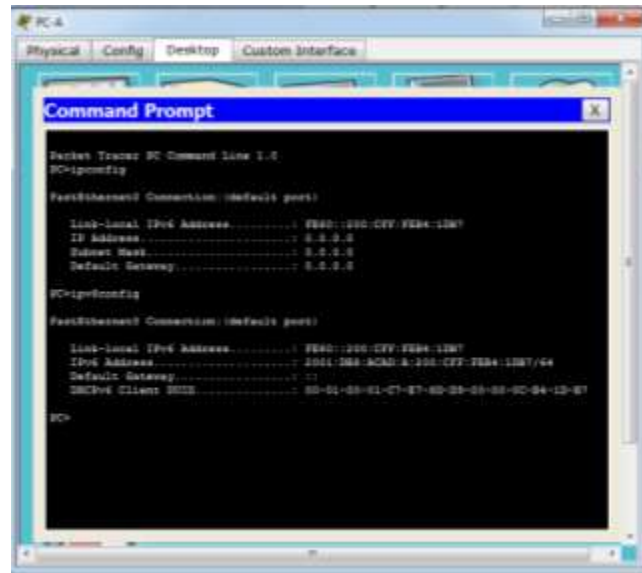
NOTA: con el comando **show ipv6 interface** no me genera o muestra nada, pero si al comando **show ipv6 interface** le agregamos el comando **brief** podemos ver en la siguiente imagen.



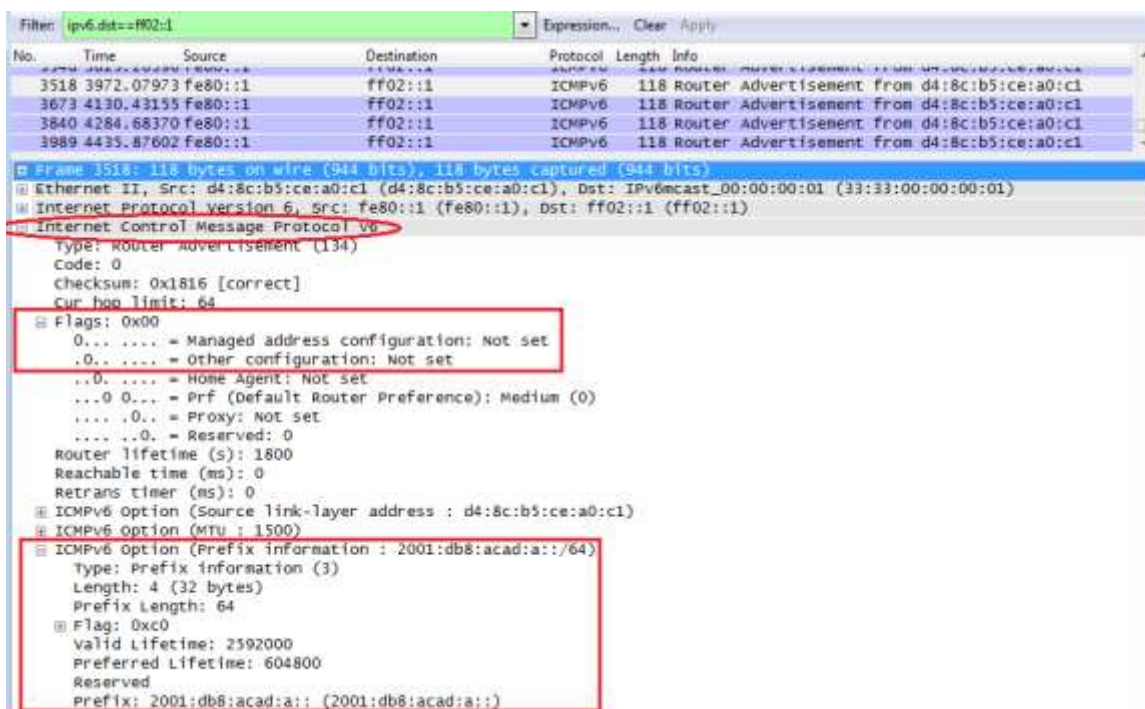
Paso 6. verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.



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



- b. En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.



Parte 19. configurar la red para DHCPv6 sin estado

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

- a. Cree un pool de DHCP IPv6.

```

Router1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

prohibited access to or unauthorized personnel.
User Access Verification
Password:
#enable
Password:
#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPv6POOL-A
R1(config-dhcp)#domain-name zona-estadosDHCPv6.com
R1(config-dhcp)#
    
```

- b. Asigne un nombre de dominio al pool.

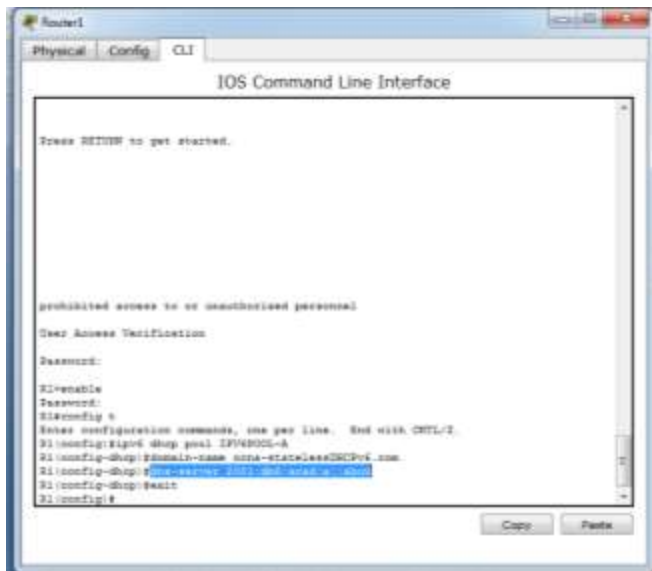
```

Router1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

prohibited access to or unauthorized personnel.
User Access Verification
Password:
#enable
Password:
#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPv6POOL-A
R1(config-dhcp)#domain-name zona-estadosDHCPv6.com
R1(config-dhcp)#
    
```

c. Asigne una dirección de servidor DNS.



```
Router1
Physical Config CLI
IOS Command Line Interface

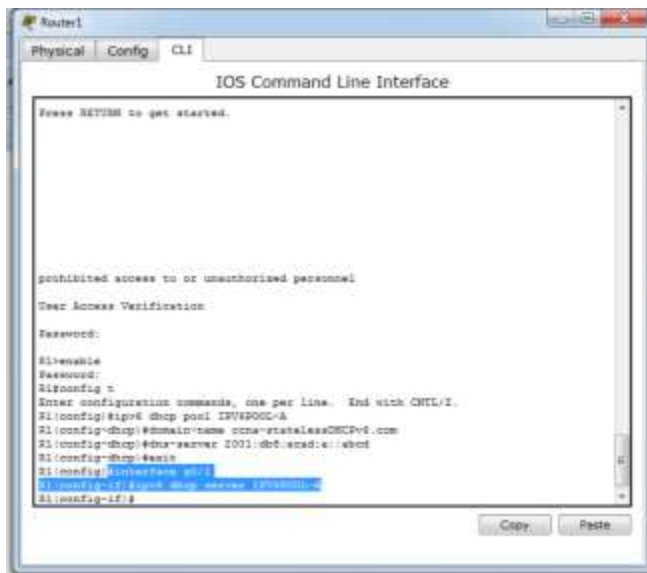
Press RETURN to get started.

prohibited access to or unauthorized personnel

User Access Verification

Password:
#
#enable
#
#configure
#
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#domain-name cna-estadocasaDHCPv6.com
R1(config-dhcp)#dns-server 2001:db8:acad:e::abcd
R1(config-dhcp)#exit
R1(config)#
```

d. Asigne el pool de DHCPv6 a la interfaz.



```
Router1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

prohibited access to or unauthorized personnel

User Access Verification

Password:
#
#enable
#
#configure
#
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#domain-name cna-estadocasaDHCPv6.com
R1(config-dhcp)#dns-server 2001:db8:acad:e::abcd
R1(config-dhcp)#exit
R1(config)#interface g0/0
R1(config-if)#ipv6 dhcp server IPV6POOL-A
R1(config-if)#
```

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

```

Router1
Physical Config CLI
IOS Command Line Interface

prohibited access to or unauthorized personnel

Guest Access Verification
Password:
R1#enable
R1#configure
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipvt dhcp pool FF02::1:2
R1(config-dhcp)#stateless-mode statelessDHCPv6.com
R1(config-dhcp)#dns-server 2001:DB8:ACAD:A::1:2
R1(config-dhcp)#exit
R1(config)#interface g0/1
R1(config-if)#ipvt dhcp server FF02::1:2
R1(config-if)#other-config-flag
R1#
*RTV-6-CONFID_1: Configured from console by console
    
```

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.

```

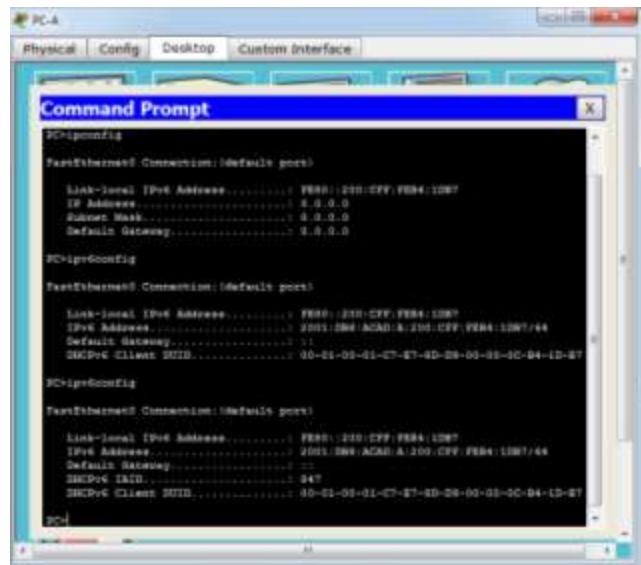
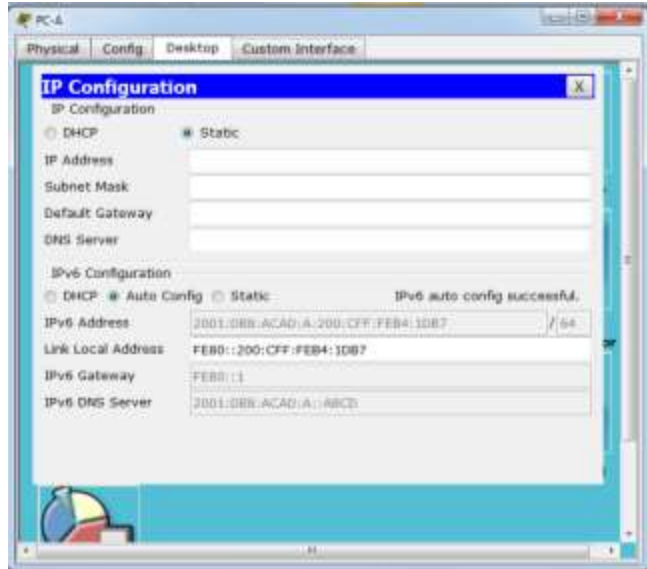
Router1
Physical Config CLI
IOS Command Line Interface

R1(config-if)#ipvt no other-config-flag
R1(config-if)#end
R1#
*RTV-6-CONFID_1: Configured from console by console

R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local addresses:
Global unicast addresses:
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group addresses:
  FF02::1
  FF02::5
  FF02::1:FF02::1
MTU is 1500 bytes
ICMPv6 error messages limited to one every 100 milliseconds
ICMPv6 redirects are enabled
ICMPv6 advertisements are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised reachability interval is 0 (unspecified)
ND router advertisements are sent every 300 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Routers use stateless autoconfig for addresses.
R1#
    
```

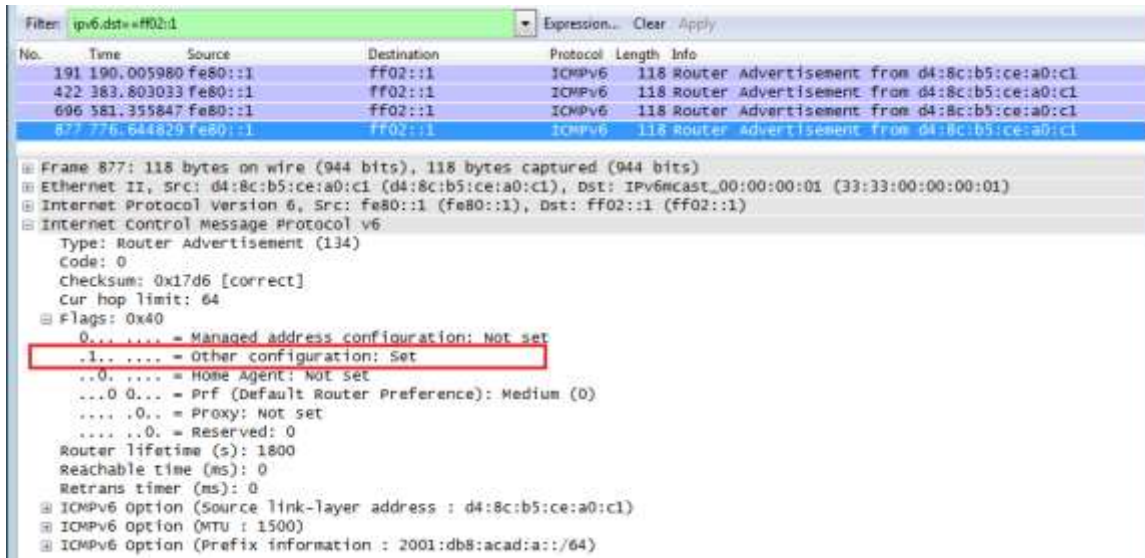
Paso 3. ver los cambios realizados en la red en la PC-A.

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



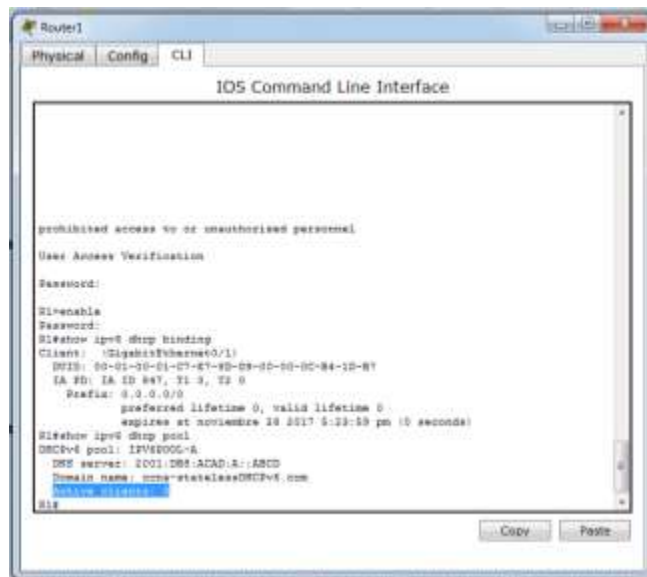
Paso 4. ver los mensajes RA en Wireshark.

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



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

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



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

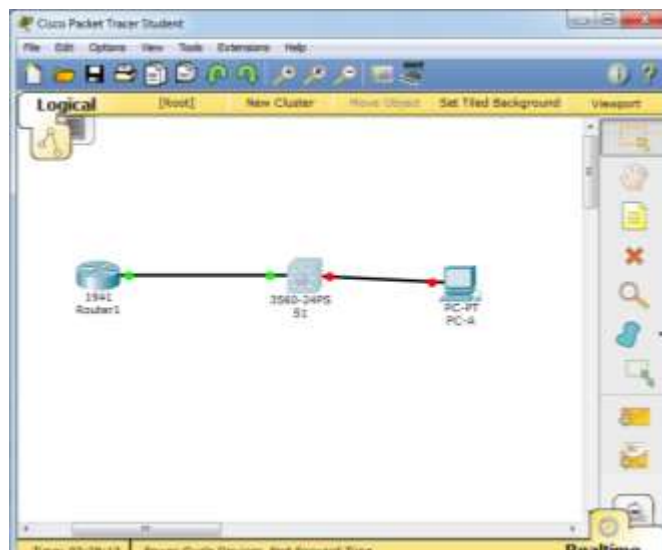
- a. Desactive la interfaz F0/6 del S1.

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

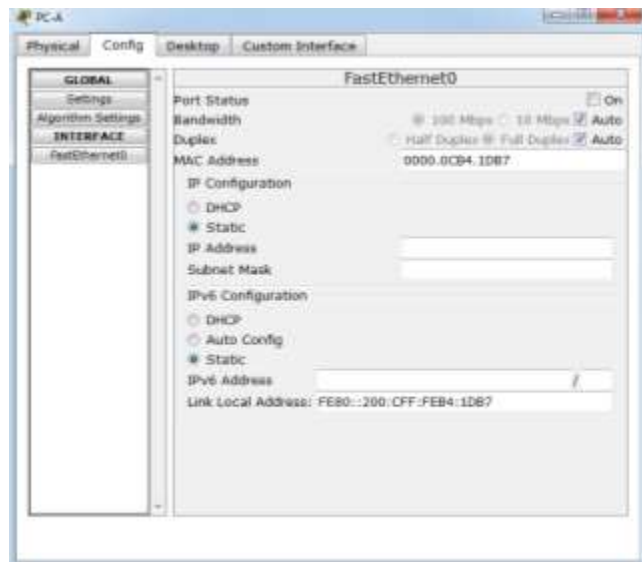
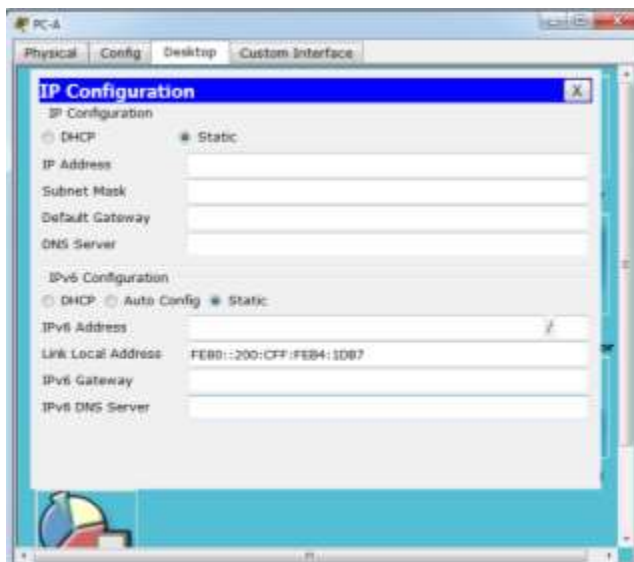
```

S1
Physical Config CLI
IOS Command Line Interface
Dear Access Verification
Succeeded:
Succeeded:
S1>interface F0/6
^ Invalid input detected at '^' marker.
S1#enable
Succeeded:
S1>interface F0/6
^ Invalid input detected at '^' marker.
S1#
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1>conf t>interface F0/6
S1>conf t>sh shutdown
S1>
S1>conf t>#
%LINK-3-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down
S1>conf t>#
    
```

- b. Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.



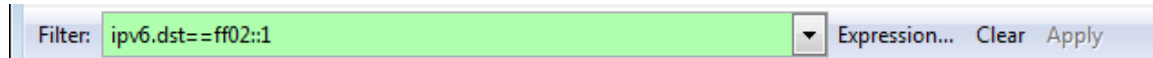
- c. Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.
- 1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.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



Parte 20. configurar la red para DHCPv6 con estado

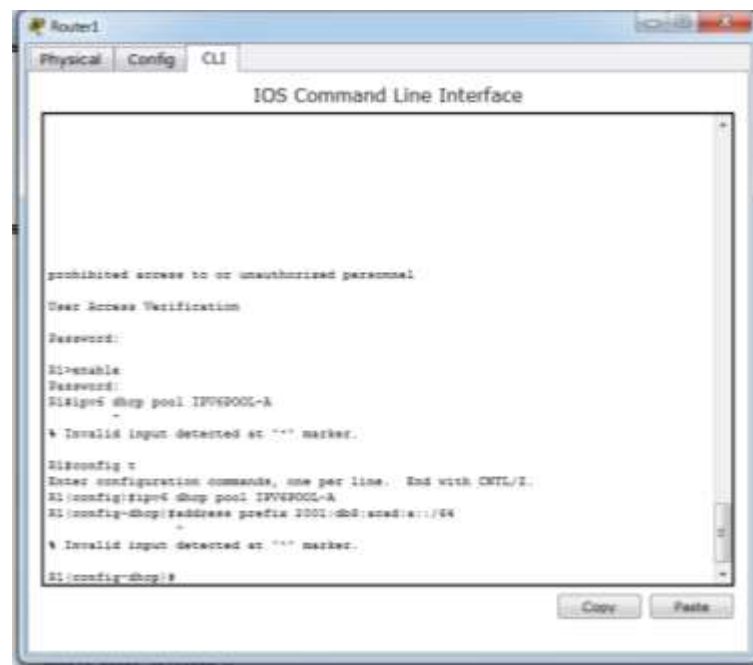
Paso 1. preparar la PC-A.

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



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

- Agregue el prefijo de red al pool.



- 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.

```

Router1
Physical Config CLI
IOS Command Line Interface

prohibited access to or unauthorized personnel
User Access Verification
Password:
R1#enable
Password:
R1#ipv6 dhcp pool IPV6POOL-A
-
% Invalid input detected at '^' marker.

R1#config t
Enter configuration commands, one per line. End with CTRL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#address prefix 2001:db8:acad:a::/64
-
% Invalid input detected at '^' marker.

R1(config-dhcp)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcp)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
    
```

- c. Verifique la configuración del pool de DHCPv6.

```

Router1
Physical Config CLI
IOS Command Line Interface

User Access Verification
Password:
R1#enable
Password:
R1#ipv6 dhcp pool IPV6POOL-A
-
% Invalid input detected at '^' marker.

R1#config t
Enter configuration commands, one per line. End with CTRL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#address prefix 2001:db8:acad:a::/64
-
% Invalid input detected at '^' marker.

R1(config-dhcp)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcp)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Service clients
R1#
    
```

d. Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

```

Route1
Physical Config CLI
IOS Command Line Interface

Password:
E#enable
Password:
E#ipconfig dhcp pool IPV6POOL-A
-
% Invalid input detected at '^' marker.

E#conf t
Enter configuration commands, one per line. End with CTRL-Z.
E#conf t ipconfig dhcp pool IPV6POOL-A
E#conf t ipconfig dhcp address prefix 2001:db8:acad::/64
-
% Invalid input detected at '^' marker.

E#conf t ipconfig dhcp domain-name cma-statefildhcpv6.com
E#conf t ipconfig dhcp domain-name cma-statefildhcpv6.com
E#conf t ipconfig dhcp #end
E#
%SYS-5-CMGIS_1: Configured from console by console

E#show ipconfig dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:db8:acad::1::abcd
Domain name: cma-statefildhcpv6.com
Active clients: 0
E#show ipconfig dhcp detail
DHCPv6 debugging is on (detailed)
E#enable
Enter configuration commands, one per line. End with CTRL-Z.
E#conf t ipconfig dhcp pool IPV6POOL-A
E#conf t ipconfig dhcp #end

E#conf t if G0/1
ALERT-3-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
E#conf t if ipconfig dhcp managed-config-flag
E#conf t if #end

E#conf t if G0/1
ALERT-3-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
E#conf t if #end
E#
%SYS-5-CMGIS_1: Configured from console by console
    
```

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.

```

Route1
Physical Config CLI
IOS Command Line Interface

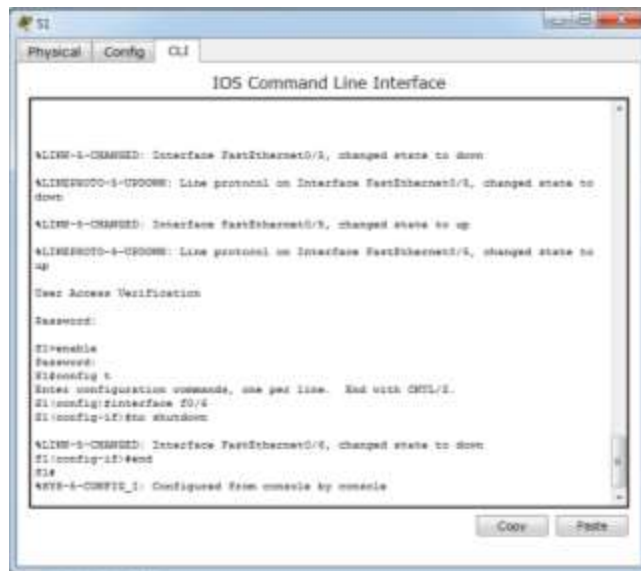
DNS server: 2001:db8:acad::1::abcd
Domain name: cma-statefildhcpv6.com
Active clients: 0
E#show ipconfig dhcp detail
DHCPv6 debugging is on (detailed)
E#enable
Enter configuration commands, one per line. End with CTRL-Z.
E#conf t ipconfig dhcp pool IPV6POOL-A
E#conf t ipconfig dhcp #end

E#conf t if G0/1
ALERT-3-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
E#conf t if ipconfig dhcp managed-config-flag
E#conf t if #end

E#conf t if G0/1
ALERT-3-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
E#conf t if #end
E#
%SYS-5-CMGIS_1: Configured from console by console
    
```

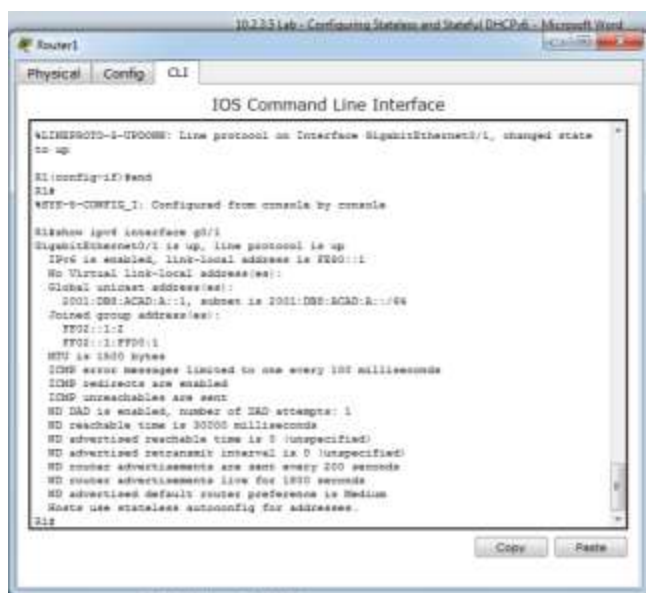
Paso 4. habilitar la interfaz F0/6 en el S1.

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.

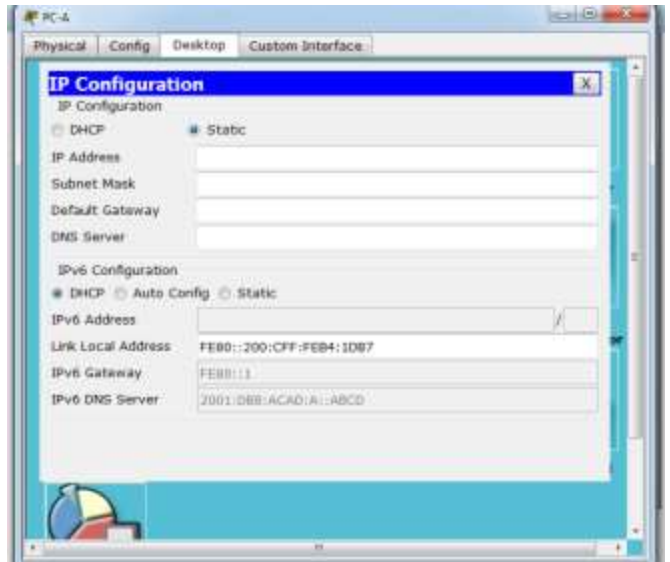
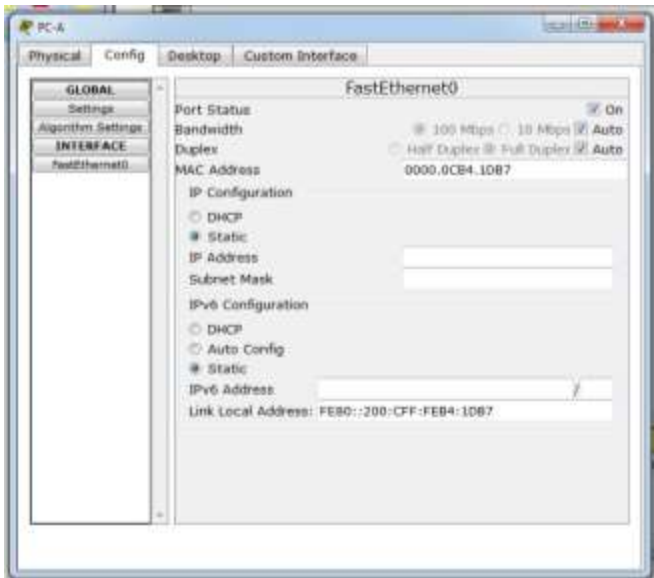


Paso 5. verificar la configuración de DHCPv6 con estado en el R1.

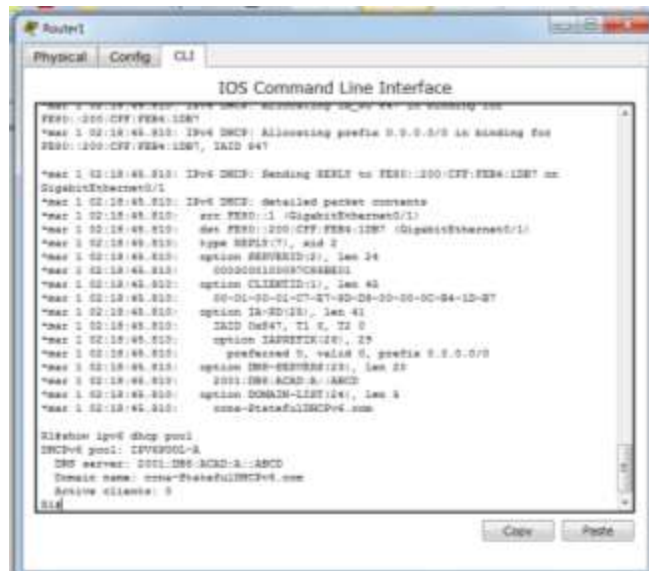
- Emita el comando **show ipv6 interface g0/1** para verificar que la interfaz esté en el modo DHCPv6 con estado.



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



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



- 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.

```

Router1
Physical Config CLI
IOS Command Line Interface
*Mar 1 02:18:45.812: conf t: DHCPv6 pool: IPV6POOL-A
*Mar 1 02:18:45.812: conf t:  net 2001:DB8:ACAD::1/64 (GigabitEthernet0/1)
*Mar 1 02:18:45.812: conf t:  type REPLY(T),xid 2
*Mar 1 02:18:45.812: conf t:  option SERVERID(2), len 24
*Mar 1 02:18:45.812: conf t:  0000001000970080E1
*Mar 1 02:18:45.812: conf t:  option CLIENTID(1), len 48
*Mar 1 02:18:45.812: conf t:  00-01-00-01-C7-E7-8D-09-00-00-00-00-00-04-1D-E7
*Mar 1 02:18:45.812: conf t:  option IA-PD(3), len 41
*Mar 1 02:18:45.812: conf t:  IAID 0x87, TI 0, TI 0
*Mar 1 02:18:45.812: conf t:  option IASREFIK(24), 24
*Mar 1 02:18:45.812: conf t:  preferred 0, valid 0, prefix 0.0.0.0/0
*Mar 1 02:18:45.812: conf t:  option DNS-SERVERS(19), len 28
*Mar 1 02:18:45.812: conf t:  2001:DB8:ACAD::1:ABCD
*Mar 1 02:18:45.812: conf t:  option DOMAIN-LIST(24), len 8
*Mar 1 02:18:45.812: conf t:  com-StatefulINCPv6.com

R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD::1:ABCD
Domain name: com-StatefulINCPv6.com
Active clients: 0

R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
IID: 00-01-00-01-C7-E7-8D-09-00-00-00-00-00-04-1D-E7
IA ID: IA ID 847, TI 0, TI 0
Prefix: 0.0.0.0/0
      preferred lifetime 0, valid lifetime 0
      expires at sunrise/03/28/2017 8:04:34 pm 10 seconds
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.

```

Router1
Physical Config CLI
IOS Command Line Interface
*Mar 1 02:18:45.812: conf t: DHCPv6 pool: IPV6POOL-A
*Mar 1 02:18:45.812: conf t:  net 2001:DB8:ACAD::1/64 (GigabitEthernet0/1)
*Mar 1 02:18:45.812: conf t:  type REPLY(T),xid 2
*Mar 1 02:18:45.812: conf t:  option SERVERID(2), len 24
*Mar 1 02:18:45.812: conf t:  0000001000970080E1
*Mar 1 02:18:45.812: conf t:  option CLIENTID(1), len 48
*Mar 1 02:18:45.812: conf t:  00-01-00-01-C7-E7-8D-09-00-00-00-00-00-04-1D-E7
*Mar 1 02:18:45.812: conf t:  option IA-PD(3), len 41
*Mar 1 02:18:45.812: conf t:  IAID 0x87, TI 0, TI 0
*Mar 1 02:18:45.812: conf t:  option IASREFIK(24), 24
*Mar 1 02:18:45.812: conf t:  preferred 0, valid 0, prefix 0.0.0.0/0
*Mar 1 02:18:45.812: conf t:  option DNS-SERVERS(19), len 28
*Mar 1 02:18:45.812: conf t:  2001:DB8:ACAD::1:ABCD
*Mar 1 02:18:45.812: conf t:  option DOMAIN-LIST(24), len 8
*Mar 1 02:18:45.812: conf t:  com-StatefulINCPv6.com

R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD::1:ABCD
Domain name: com-StatefulINCPv6.com
Active clients: 0

R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
IID: 00-01-00-01-C7-E7-8D-09-00-00-00-00-00-04-1D-E7
IA ID: IA ID 847, TI 0, TI 0
Prefix: 0.0.0.0/0
      preferred lifetime 0, valid lifetime 0
      expires at sunrise/03/28/2017 8:04:34 pm 10 seconds)
R1#undebug all
All possible debugging has been turned off
R1#
  
```

- f. Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.
 - 1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

```

Router1
Physical Config CLI
IOS Command Line Interface
As advertised default router preference is maximum
Hosts use stateless autoconfig for addresses.
R1#
*Mar 1 02:18:45.759: IPv6 DHCP: Received SOLICIT from FE80::200:CFF:FEB4:1DB7 on
GigabitEthernet0/1
*Mar 1 02:18:45.759: IPv6 DHCP: detailed packet contents
*Mar 1 02:18:45.759:   src FE80::1 (GigabitEthernet0/1)
*Mar 1 02:18:45.759:   dst FE80::1:2 (GigabitEthernet0/1)
*Mar 1 02:18:45.759:   type SOLICIT(1), aid 2
*Mar 1 02:18:45.759:   option ELAPSED-TIME(8), len 8
*Mar 1 02:18:45.759:     elapsed-time 0
*Mar 1 02:18:45.759:   option CLIENTID(1), len 45
*Mar 1 02:18:45.759:     00-01-00-01-C7-E7-8D-09-00-00-0C-84-1D-E7
*Mar 1 02:18:45.759:   option ORO(6), len 10
*Mar 1 02:18:45.759:     IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar 1 02:18:45.759:   option IA-PD(26), len 16
*Mar 1 02:18:45.759:     IAID 0a847, T1 0, T2 0
*Mar 1 02:18:45.759: IPv6 DHCP: Using interface pool IPV6POOL-A.

*Mar 1 02:18:45.759: IPv6 DHCP: Sending ADVERTISE to FE80::200:CFF:FEB4:1DB7 on
GigabitEthernet0/1
*Mar 1 02:18:45.759: IPv6 DHCP: detailed packet contents
*Mar 1 02:18:45.759:   src FE80::1 (GigabitEthernet0/1)
*Mar 1 02:18:45.759:   dst FE80::200:CFF:FEB4:1DB7 (GigabitEthernet0/1)
*Mar 1 02:18:45.759:   type ADVERTISE(2), aid 2
*Mar 1 02:18:45.759:   option SERVERID(2), len 24
*Mar 1 02:18:45.759:     0003000100097C88E01
*Mar 1 02:18:45.759:   option CLIENTID(1), len 24
*Mar 1 02:18:45.759:     0003000100097C88E01
    
```

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

```

Router1
Physical Config CLI
IOS Command Line Interface
*Mar 1 02:18:45.810:   option IA-PD(26), len 45
*Mar 1 02:18:45.810:     IAID 0a847, T1 0, T2 0
*Mar 1 02:18:45.810:   option IASREFIX(26), 29
*Mar 1 02:18:45.810:     preferred 0, valid 0, prefix 0.0.0.0/0
*Mar 1 02:18:45.810: IPv6 DHCP: Using interface pool IPV6POOL-A.
*Mar 1 02:18:45.810: IPv6 DHCP: Creating binding for FE80::200:CFF:FEB4:1DB7 in
pool IPV6POOL-A
*Mar 1 02:18:45.810: IPv6 DHCP: Allocating IA_PD 847 in binding for
FE80::200:CFF:FEB4:1DB7
*Mar 1 02:18:45.810: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for
FE80::200:CFF:FEB4:1DB7, IAID 847

*Mar 1 02:18:45.810: IPv6 DHCP: Sending REPLY to FE80::200:CFF:FEB4:1DB7 on
GigabitEthernet0/1
*Mar 1 02:18:45.810: IPv6 DHCP: detailed packet contents
*Mar 1 02:18:45.810:   src FE80::1 (GigabitEthernet0/1)
*Mar 1 02:18:45.810:   dst FE80::200:CFF:FEB4:1DB7 (GigabitEthernet0/1)
*Mar 1 02:18:45.810:   type REPLY(7), aid 2
*Mar 1 02:18:45.810:   option SERVERID(2), len 24
*Mar 1 02:18:45.810:     0003000100097C88E01
*Mar 1 02:18:45.810:   option CLIENTID(1), len 45
*Mar 1 02:18:45.810:     00-01-00-01-C7-E7-8D-09-00-00-0C-84-1D-E7
*Mar 1 02:18:45.810:   option IA-PD(26), len 41
*Mar 1 02:18:45.810:     IAID 0a847, T1 0, T2 0
*Mar 1 02:18:45.810:   option IASREFIX(26), 29
*Mar 1 02:18:45.810:     preferred 0, valid 0, prefix 0.0.0.0/0
*Mar 1 02:18:45.810:   option DNS-SERVERS(23), len 20
*Mar 1 02:18:45.810:     2001:DB8:ACAD:A::MDCD
*Mar 1 02:18:45.810:   option DOMAIN-LIST(24), len 8
    
```

Paso 6. verificar DHCPv6 con estado en la PC-A.

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

Filter: `ipv6.dst==ff02::1`

No.	Time	Source	Destination	Protocol	Length	Info
36	54.582255	Fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
265	215.309226	Fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
425	373.272435	Fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
553	554.893786	Fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
664	730.139576	Fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
775	922.720109	Fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1

Frame 775: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: Fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x3a82 [correct]
 - Cur hop limit: 64
 - Flags: 0x0c
 - 1... .. = Managed address configuration: Set
 - ..0... .. = Other configuration: Set
 - ..0... .. = Home Agent: Not set
 - ...0 0... = Prf (Default Router Preference): Medium (0)
 -0.. = Proxy: Not set
 -0.. = Reserved: 0
 - Router lifetime (s): 1800

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

Filter: `dhcpv6`

No.	Time	Source	Destination	Protocol	Length	Info
250	443.078236	Fe80::d428:7de2:997:ff02::1:2	ff02::1:2	DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
267	475.083284	Fe80::d428:7de2:997:ff02::1:2	ff02::1:2	DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
425	656.281211	Fe80::d428:7de2:997:ff02::1:2	ff02::1:2	DHCPv6	146	Solicit XID: 0xc86c32 CID: 0001000117f6723d000c2
429	656.282249	Fe80::1	Fe80::d428:7de2:997:ff02::1:2	DHCPv6	191	Advertise XID: 0xc86c32 CID: 0001000117f6723d000c2
460	657.292018	Fe80::1	Fe80::d428:7de2:997:ff02::1:2	DHCPv6	188	Request XID: 0xc86c32 CID: 0001000117f6723d000c2
462	657.292638	Fe80::1	Fe80::d428:7de2:997:ff02::1:2	DHCPv6	191	Reply XID: 0xc86c32 CID: 0001000117f6723d000c298

Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: Vmware_be:6c:89 (00:50:56:be:6c:89)

- Internet Protocol Version 6, Src: Fe80::1 (fe80::1), Dst: fe80::d428:7de2:997:c:b05a (fe80::d428:7de2:997:c:b05a)
- User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)
- DHCPv6
 - Message type: Reply (7)
 - Transaction ID: 0xc86c32
 - Server Identifier: 00030001fc994775c3e0
 - Client Identifier: 0001000117f6723d000c298d5444
 - Identity Association for Non-temporary Address
 - Option: Identity Association for Non-temporary Address (3)
 - Length: 40
 - Value: 0e000c290000a8c000010e000005001820010db8acad000a...
 - IAID: 0e000c29
 - T1: 43200
 - T2: 69120
 - IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce
 - DNS recursive name server
 - Option: DNS recursive name server (23)
 - Length: 16
 - Value: 2001:0db8:acad:000a:0000:0000:0000:abcd
 - DNS servers address: 2001:db8:acad:a:abcd
 - Domain Search List
 - Option: Domain Search List (24)
 - Length: 25
 - Value: 1363636e612d537461746566756c44484350763603636f6d...
 - DNS Domain Search List
 - Domain: ccna-StatelulDHCPv6.com

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?

RTA:

DHCPv6 con estado usa más recursos de memoria, pero DHCPv6 con estado requiere que el enrutador almacene información de estado dinámico sobre los clientes de DHCPv6 Los clientes.

DHCPv6 sin estado no usan el servidor DHCP para obtener información de dirección, por lo que esta información no necesita almacenarse

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

RTA:

Cisco recomienda la DHCPv6 sin estado cuando implementan y desarrollan redes en IPv6 sin un registro de Red Cisco (CNR)

Tabla de resumen de interfaces del router

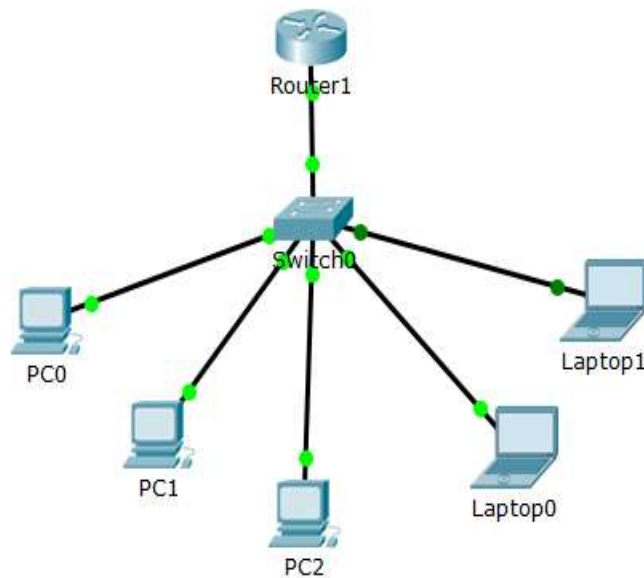
Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial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

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

10.3.1.1 IoE and DHCP Instructions (Jorge Luis Quintero)

Topología

Logical Back [Root] New Cluster Move Object Set Tiled Background Viewport Env



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

Situación

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

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

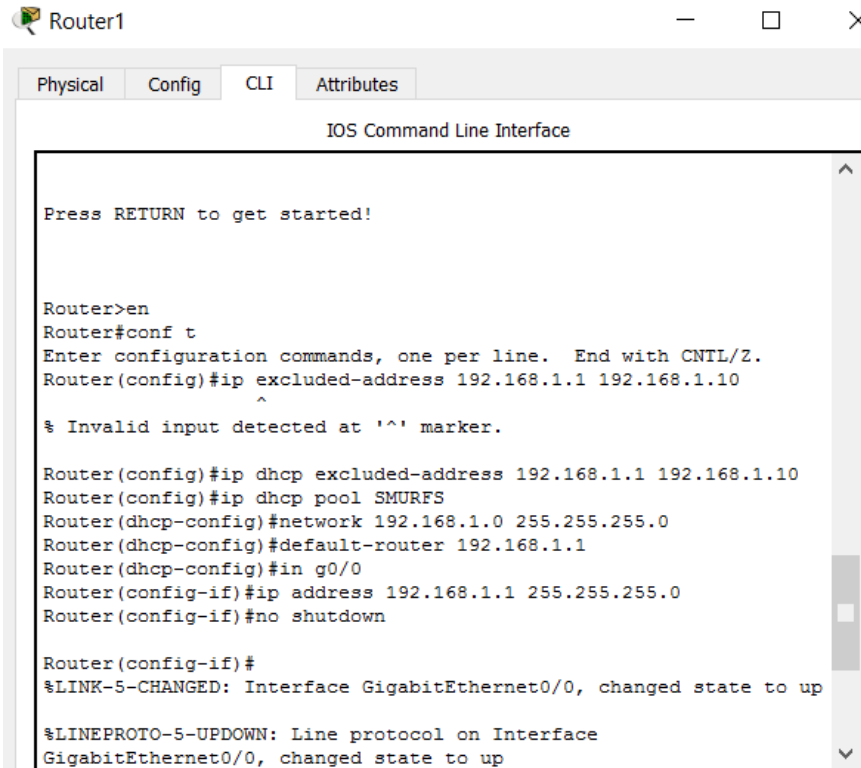
Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

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

- Presente sus conclusiones a un compañero de clase o a la clase.

Recursos necesarios

Software de Packet Tracer



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip excluded-address 192.168.1.1 192.168.1.10
^
% Invalid input detected at '^' marker.

Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
Router(config)#ip dhcp pool SMURFS
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#in g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

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

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

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
% Invalid input detected at '^' marker.  
  
Switch#conf t  
Enter configuration commands, one per line. End with  
CNTL/Z.  
Switch(config)#int g0/1  
Switch(config-if)#s  
Switch(config-if)#sw  
Switch(config-if)#switchport mode trunk  
  
Switch(config-if)#  
%LINEPROTO-5-UPDOWN: Line protocol on Interface  
GigabitEthernet0/1, changed state to down  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface  
GigabitEthernet0/1, changed state to up  
  
Switch(config-if)#no shut  
Switch(config-if)#exit  
Switch(config)#
```

Copy Paste

PC0

Physical Config Desktop Attributes Software/Services

IP Configuration X

IP Configuration

DHCP Static DHCP request successful.

IP Address 192.168.1.11

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

PC2



Physical Config Desktop Attributes Software/Services

IP Configuration [X]

IP Configuration

DHCP Static DHCP request successful.

IP Address: 192.168.1.13

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: [Empty]

Laptop0



Physical Config Desktop Attributes Software/Services

IP Configuration [X]

IP Configuration

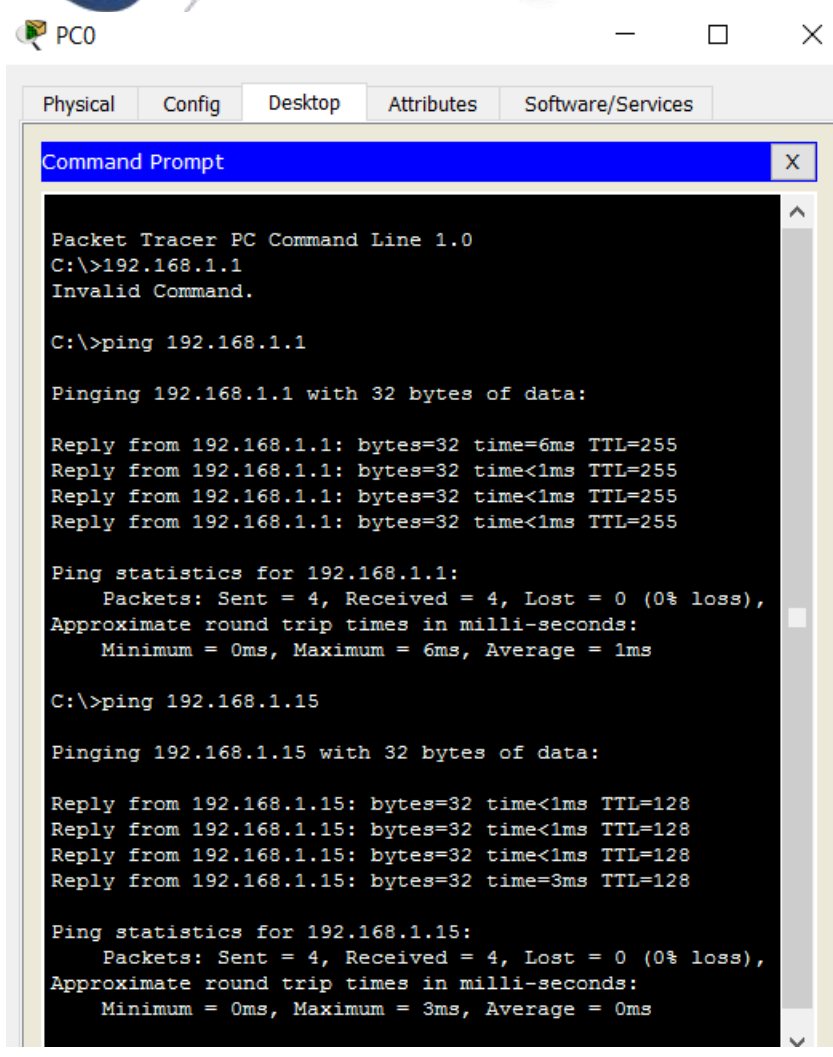
DHCP Static DHCP request successful.

IP Address: 192.168.1.14

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: [Empty]



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 expands 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

11.2.2.6 Lab - Configuring Dynamic and Static NAT (Alexander Ramirez)

Topología

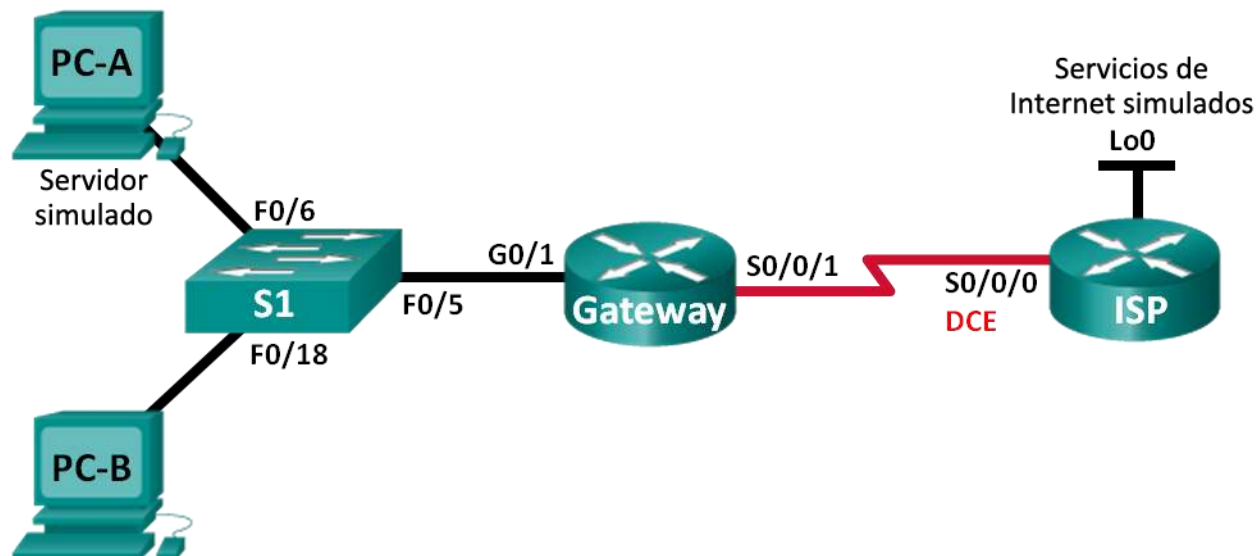


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	G0/0	192.31.7.1	255.255.255.0	N/A
Server ISP	NIC	192.31.7.2	255.255.255.0	192.31.7.1
PC-A (servidor simulado)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

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 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.

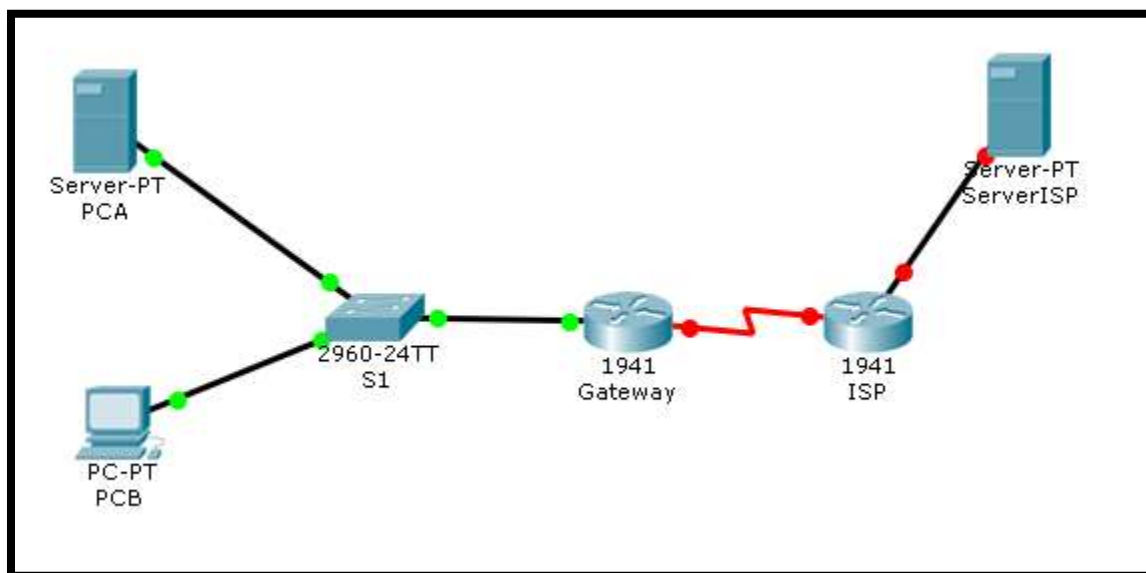
Nota: asegúrese de que los routers y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

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 21. armar la red y verificar la conectividad

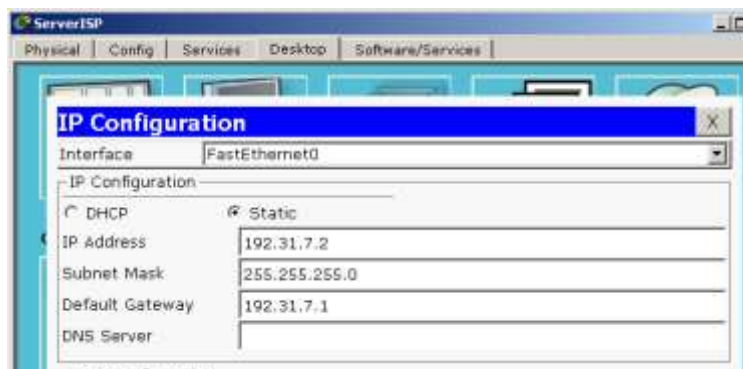
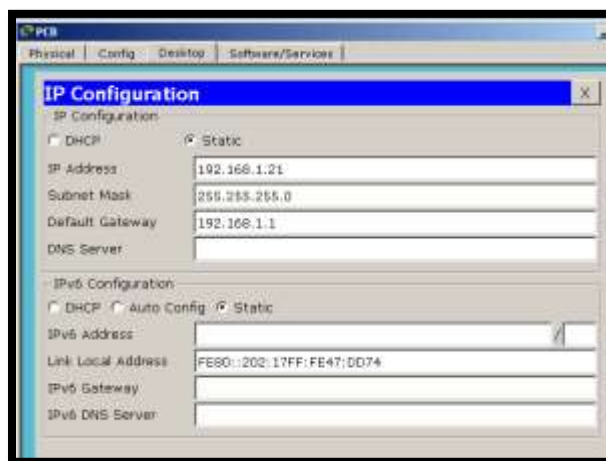
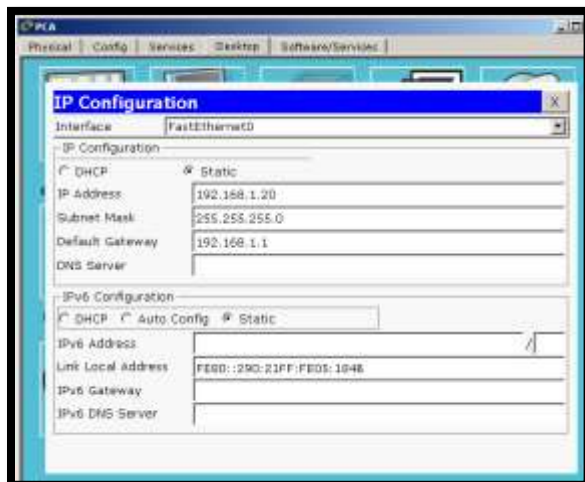
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.



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

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

Paso 2. configurar los equipos host.



Paso 3. inicializar y volver a cargar los routers y los switches según sea necesario.

Paso 4. configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda del DNS.
- b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- c. Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.
- d. Configure el nombre del dispositivo como se muestra en la topología.
- e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

```

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#int g0/1
Gateway(config-if)#ip 192.168.1.1 255.255.255.0
      ^
% Invalid input detected at '^' marker.

Gateway(config-if)#ip add 192.168.1.1 255.255.255.0
Gateway(config-if)#no shut

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

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

Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip add 209.165.201.18 255.255.255.252
Gateway(config-if)#no shut

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

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int s0/0/0
ISP(config-if)#clock rate 128000
ISP(config-if)#ip add 209.165.201.18
% Incomplete command.
ISP(config-if)#ip add 209.165.201.18 255.255.255.0
ISP(config-if)#no shut

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

ISP(config-if)#int
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
ISP(config-if)#int g0/0
ISP(config-if)#ip add 192.31.7.1 255.255.255.0
ISP(config-if)#no shut

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

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

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

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

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

- Habilite el servicio del servidor HTTP en el ISP.

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

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

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

Paso 6. configurar el routing estático.

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

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

```
ISP(config)#int s0/0/0
ISP(config-if)#ip add 209.165.201.17 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#end
ISP#
%SYS-5-CONFIG_I: Configured from console by console

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

ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.18
ISP(config)#
```

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

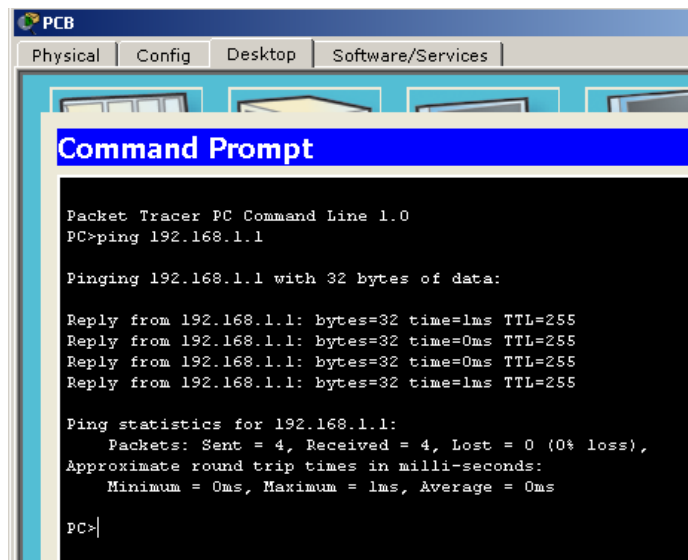
```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

```
Gateway>en
Gateway#config t
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

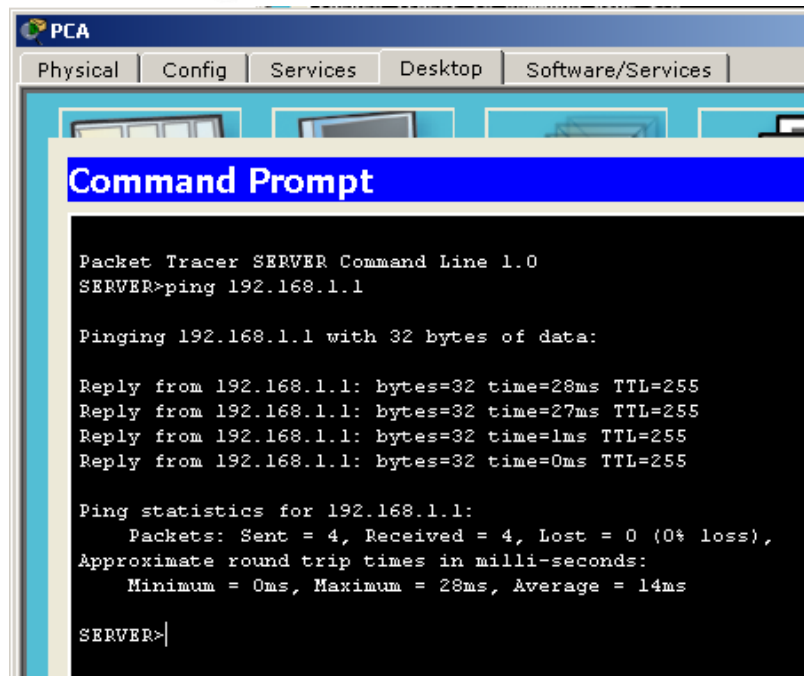
Paso 7. Guardar la configuración en ejecución en la configuración de inicio.

Paso 8. Verificar la conectividad de la red

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



```
PCB
Physical | Config | Desktop | Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=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 = 1ms, Average = 0ms
PC>
```



```

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

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/1
L       209.165.201.18/32 is directly connected, Serial0/0/1
S*    0.0.0.0/0 [1/0] via 209.165.201.17
    
```

```

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

Gateway of last resort is not set

    192.31.7.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.31.7.0/24 is directly connected, GigabitEthernet0/0
L       192.31.7.1/32 is directly connected, GigabitEthernet0/0
    209.165.200.0/27 is subnetted, 1 subnets
S       209.165.200.224/27 [1/0] via 209.165.201.18
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/0
L       209.165.201.17/32 is directly connected, Serial0/0/0
ISP#

```

- a. 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.

Parte 22. configurar y verificar la NAT estática.

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

Paso 1. configurar una asignación estática.

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

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

```

Gateway#
Gateway#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#ip nat inside source static 192.168.1.20 209.165.200.225
Gateway(config)#

```

Paso 2. Especifique las interfaces.

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

```

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

```

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

Paso 3. probar la configuración.

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

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

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

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = 209.165.200.225

¿Quién asigna la dirección global interna?

209.165.200.225

¿Quién asigna la dirección local interna?

EL ADMINISTRADOR DE RED

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

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

```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:17 192.168.1.20:17  192.31.7.2:17     192.31.7.2:17
icmp 209.165.200.225:18 192.168.1.20:18  192.31.7.2:18     192.31.7.2:18
icmp 209.165.200.225:19 192.168.1.20:19  192.31.7.2:19     192.31.7.2:19
icmp 209.165.200.225:20 192.168.1.20:20  192.31.7.2:20     192.31.7.2:20
icmp 209.165.200.225:21 192.168.1.20:21  192.31.7.2:21     192.31.7.2:21
icmp 209.165.200.225:22 192.168.1.20:22  192.31.7.2:22     192.31.7.2:22
icmp 209.165.200.225:23 192.168.1.20:23  192.31.7.2:23     192.31.7.2:23
icmp 209.165.200.225:24 192.168.1.20:24  192.31.7.2:24     192.31.7.2:24
--- 209.165.200.225    192.168.1.20      ---                ---
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? 17

Nota: puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

- c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

```
Pro Inside global      Inside local      Outside local      Outside global
```

```
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23
--- 209.165.200.225 192.168.1.20 --- ---
```

```
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.225:1025 192.168.1.20:1025 192.31.7.2:80 192.31.7.2:80
```

Nota: es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

¿Qué protocolo se usó para esta traducción? __WEB

¿Cuáles son los números de puerto que se usaron?

Global/local interno: ____1025

Global/local externo: _80



- d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.

```
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=2ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

SERVER>
```




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

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

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

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

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39 Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

```

Gateway#show ip nat statistics
Total translations: 4 (1 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 36 Misses: 27
Expired translations: 24
Dynamic mappings:

```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Parte 23. configurar y verificar la NAT dinámica

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

Paso 1. borrar las NAT.

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

```

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

```

```

Gateway#clear ip nat translation ?
* Deletes all dynamic translations
Gateway#clear ip nat translation *
Gateway#clear ip nat statistics

```

```

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

```

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

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

```

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

```

Paso 3. verificar que la configuración de interfaces NAT siga siendo válida.

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

Paso 4. definir el conjunto de direcciones IP públicas utilizables.

```

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

```

Paso 5. definir la NAT desde la lista de origen interna hasta el conjunto externo.

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

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

```
Gateway#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#ip nat pool public_access 209.165.200.242 209.165.200.254 netmask
255.255.255.224
Gateway(config)#ip nat inside source list 1 pool public_access
```

Paso 6. probar la configuración.

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

```
Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225    192.168.1.20     ---                ---
icmp 209.165.200.242:1 192.168.1.21:1   192.31.7.1:1      192.31.7.1:1
--- 209.165.200.242    192.168.1.21     ---                ---
```

```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.242:5 192.168.1.21:5   192.31.7.2:5      192.31.7.2:5
icmp 209.165.200.242:6 192.168.1.21:6   192.31.7.2:6      192.31.7.2:6
icmp 209.165.200.242:7 192.168.1.21:7   192.31.7.2:7      192.31.7.2:7
icmp 209.165.200.242:8 192.168.1.21:8   192.31.7.2:8      192.31.7.2:8
--- 209.165.200.225    192.168.1.20     ---                ---
```

¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = 209.165.200.242

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

¿Qué número de puerto se usó en este intercambio ICMP? 5, 6, 7, 8

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

```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225    192.168.1.20     ---                ---
tcp 209.165.200.242:1025 192.168.1.21:1025 192.31.7.2:80     192.31.7.2:80
```

- c. Muestre la tabla de NAT.

```
Pro  Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225    192.168.1.20     ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80     192.31.7.1:80
```

```

tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80 192.31.7.1:80
--- 209.165.200.242 192.168.1.22 --- ---

```

¿Qué protocolo se usó en esta traducción? **HTTP**

¿Qué números de puerto se usaron?

Interno: **1025**

Externo: **80**

¿Qué número de puerto bien conocido y qué servicio se usaron? **80**

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

```

Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345 Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

```

```

Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 47 Misses: 32
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13 , allocated 1 (7%), misses 0

```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Paso 7. eliminar la entrada de NAT estática.

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

- a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225
```

```
Static entry in use, do you want to delete child entries? [no]: yes
```

- b. Borre las NAT y las estadísticas.
- c. Haga ping al ISP (192.31.7.1) desde ambos hosts.
- d. Muestre la tabla y las estadísticas de NAT.

```
Gateway# show ip nat statistics
```

```
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
```

```
Peak translations: 15, occurred 00:00:43 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```

```
GigabitEthernet0/1
```

```
Hits: 16 Misses: 0
```

```
CEF Translated packets: 285, CEF Punted packets: 0
```

```
Expired translations: 11
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 1] access-list 1 pool public_access refcount 4
```

```
pool public_access: netmask 255.255.255.224
```

```
start 209.165.200.242 end 209.165.200.254
```

```
type generic, total addresses 13, allocated 2 (15%), misses 0
```

```
Total doors: 0
```

```
Appl doors: 0
```

```
Normal doors: 0
```

```
Queued Packets: 0
```

```

Gateway(config)#no ip nat inside source static 192.168.1.20 209.165.200.225
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console

Gateway#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 47 Misses: 32
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13 , allocated 1 (7%), misses 0
    
```

```

Gateway# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512    192.31.7.1:512
--- 209.165.200.243    192.168.1.20    ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512    192.31.7.1:512
--- 209.165.200.242    192.168.1.21    ---                ---
    
```

```

Gateway#show ip nat translation
Pro  Inside global      Inside local      Outside local      Outside global
tcp  209.165.200.242:1025 192.168.1.21:1025 192.31.7.2:80     192.31.7.2:80
    
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

_nat existe para IPV4, porque las IP estaban a punto de agotarse, para que todas las PC de una red privada con IP públicas puedan salir internas se utilizaban un rango de IP publicas o una IP publica.

Existe seguridad de los equipos internos de la red hacia el exterior, al no mostrar las IP de los equipos.

2. ¿Cuáles son las limitaciones de NAT?

Es que el Gateway hay pequeña demora y servicios que no pueden salir al internet.

Tabla de resumen de interfaces del router

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

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

11.2.3.7 Lab - Configuring NAT Pool Overload and PAT (Alexander Ramirez)

Topología

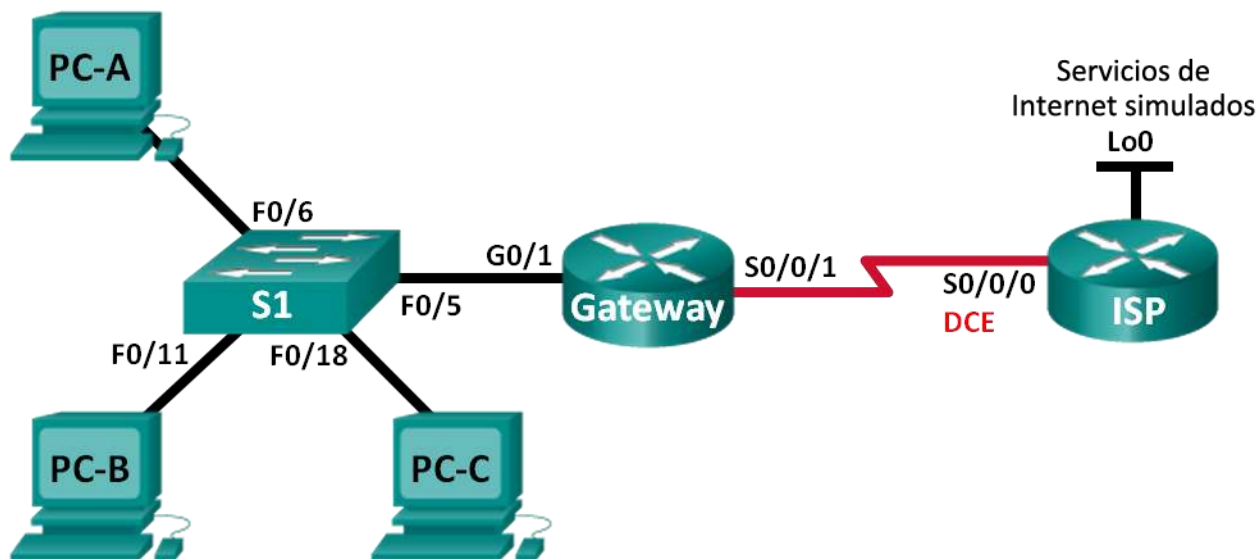


Tabla de direccionamiento

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

Objetivos

Parte 1: armar la red y verificar la conectividad

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

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de

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

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

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen 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.

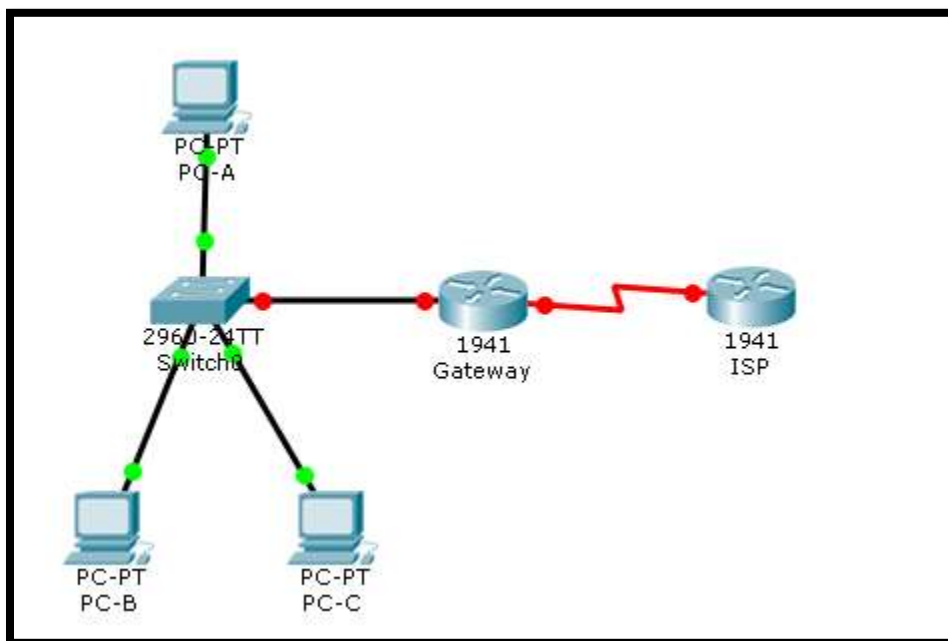
Recursos necesarios

- 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 24. armar la red y verificar la conectividad

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

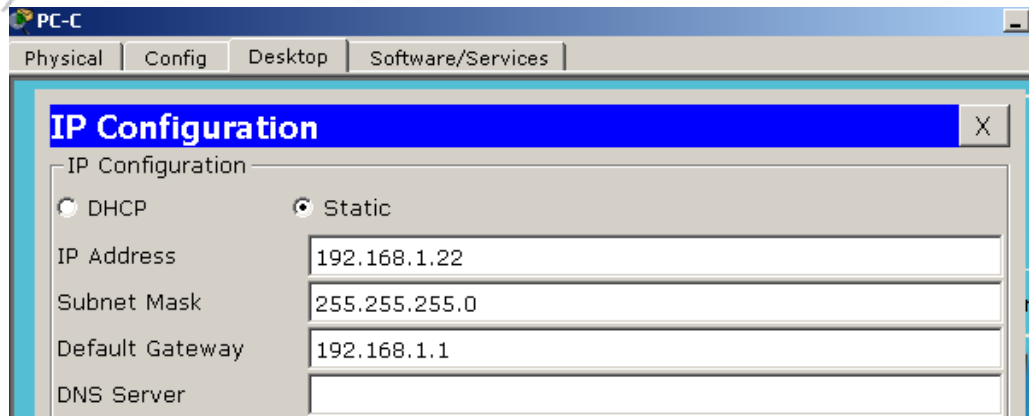
Paso 1. realizar el cableado de red tal como se muestra en la topología.



Paso 2. configurar los equipos host.

The image shows two screenshots of the IP Configuration window in a virtual PC environment. The top window is for PC-A, and the bottom window is for PC-B. Both windows show the following configuration:

Field	PC-A Value	PC-B Value
IP Configuration	Static	Static
IP Address	192.168.1.20	192.168.1.21
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	192.168.1.1
DNS Server		



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

Paso 4. configurar los parámetros básicos para cada router.

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

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#int g0/1
Gateway(config-if)#ip add 192.168.1.1 255.255.255.0
Gateway(config-if)#no shutdown

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

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

Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip add 209.165.201.18 255.255.255.252
Gateway(config-if)#no shut

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

```

Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int lo 0

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ip add 192.31.7.1 255.255.255.255
ISP(config-if)#int s0/0/0
ISP(config-if)#ip add 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

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

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

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
```

```
ISP(config-if)#exit
ISP(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

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

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

```
Gateway(config-if)#exit
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Paso 6. Verificar la conectividad de la red

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

```

PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

PC>|

```

Parte 25. configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

Paso 1. definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

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

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

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

```
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

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

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

Paso 4. Especifique las interfaces.

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

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

```

Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#ip nat pool public_access 209.165.200.225 209.165.200.230 netmask
255.255.255.248
Gateway(config)#ip nat inside source list 1 pool public_access overload
Gateway(config)#int g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip nat outside
      ^
% Invalid input detected at '^' marker.

Gateway(config-if)#ip nat outside

```

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

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

```

PC-A
Physical Config Desktop Software/Services

Command Prompt

PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
    
```

```

PC-B
Physical Config Desktop Software/Services

Command Prompt

PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
    
```

```

PC-C
Physical Config Desktop Software/Services

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>
    
```

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: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 20 Misses: 20
Expired translations: 16
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 4
  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

```

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

```

```
Gateway#show ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
icmp 209.165.200.225:1024 192.168.1.21:13    192.31.7.1:13      192.31.7.1:1024
icmp 209.165.200.225:1025 192.168.1.21:14    192.31.7.1:14      192.31.7.1:1025
icmp 209.165.200.225:1026 192.168.1.21:15    192.31.7.1:15      192.31.7.1:1026
icmp 209.165.200.225:1027 192.168.1.21:16    192.31.7.1:16      192.31.7.1:1027
icmp 209.165.200.225:131 192.168.1.20:13    192.31.7.1:13      192.31.7.1:13
icmp 209.165.200.225:141 192.168.1.20:14    192.31.7.1:14      192.31.7.1:14
icmp 209.165.200.225:151 192.168.1.20:15    192.31.7.1:15      192.31.7.1:15
icmp 209.165.200.225:161 192.168.1.20:16    192.31.7.1:16      192.31.7.1:16
icmp 209.165.200.225:5   192.168.1.22:5     192.31.7.1:5       192.31.7.1:5
icmp 209.165.200.225:6   192.168.1.22:6     192.31.7.1:6       192.31.7.1:6
icmp 209.165.200.225:7   192.168.1.22:7     192.31.7.1:7       192.31.7.1:7
icmp 209.165.200.225:8   192.168.1.22:8     192.31.7.1:8       192.31.7.1:8
```

Nota: es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

- ¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? **_3 direcciones**
- ¿Cuántas direcciones IP globales internas se indican? **_una sola dirección**
- ¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? **_ 12 puertos para 12 paquetes distintos**
- ¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

```
ISP>en
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)
```

No se puede porque cuando se configura NAT las IP internas no se permiten ver, el ISP no puede hacer un ping porque NAT las protege.

Parte 26. 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 *
Gateway#clear ip nat translation ?
* Deletes all dynamic translations
Gateway#clear ip nat translation *
```

Paso 2. verificar la configuración para NAT.

- a. Verifique que se hayan borrado las estadísticas.


```

Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 32 Misses: 32
Expired translations: 32
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

```

- b. Verifique que las interfaces externa e interna estén configuradas para NAT.
- c. Verifique que la ACL aún esté configurada para NAT.

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

SHOW IP NAT STATISTICS

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

```

Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248

```

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

```

Gateway(config)# no ip nat inside source list 1 pool public_access overload

```

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

```

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

```

```

Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
%Pool public_access in use, cannot destroy
Gateway(config)#no ip nat inside source list 1 pool public_access overload
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 overload

```

Paso 6. probar la configuración PAT.

- a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.
- b. Muestre las estadísticas de NAT en el router Gateway.

```

Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0

```

Dynamic mappings:

-- Inside Source

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

```
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:
```

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

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 192.168.1.21:21 192.31.7.1:21 192.31.7.1:1024
icmp 209.165.201.18:1025 192.168.1.21:22 192.31.7.1:22 192.31.7.1:1025
icmp 209.165.201.18:1026 192.168.1.21:23 192.31.7.1:23 192.31.7.1:1026
icmp 209.165.201.18:1027 192.168.1.21:24 192.31.7.1:24 192.31.7.1:1027
icmp 209.165.201.18:13 192.168.1.22:13 192.31.7.1:13 192.31.7.1:13
icmp 209.165.201.18:14 192.168.1.22:14 192.31.7.1:14 192.31.7.1:14
icmp 209.165.201.18:15 192.168.1.22:15 192.31.7.1:15 192.31.7.1:15
icmp 209.165.201.18:16 192.168.1.22:16 192.31.7.1:16 192.31.7.1:16
icmp 209.165.201.18:21 192.168.1.20:21 192.31.7.1:21 192.31.7.1:21
icmp 209.165.201.18:22 192.168.1.20:22 192.31.7.1:22 192.31.7.1:22
icmp 209.165.201.18:23 192.168.1.20:23 192.31.7.1:23 192.31.7.1:23
icmp 209.165.201.18:24 192.168.1.20:24 192.31.7.1:24 192.31.7.1:24
```

Reflexión

¿Qué ventajas tiene la PAT?

Al utilizarse la IP pública que es la de la interface se ahorran direcciones ip publicas, pueden salir 100 direcciones privadas con una sola ip publica y utilizando diferentes puertos para diferenciar los paquetes.

Es un método muy seguro.

Tabla de resumen de interfaces del router

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

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

4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks_Instructor (Alexander Ramirez)

Topology

Addressing Table

Objectives

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

Background / Scenario

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

Packet Tracer - Configure IP ACLs to Mitigate Attacks

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

The routers have been pre-configured with the following:

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

Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

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

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

```
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

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

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

PC> ssh -l SSHadmin 192.168.2.1

```
SERVER> ssh -l SSHadmin 192.168.2.1
Open
Password:
% Password: timeout expired!
% Login invalid

[Connection to 192.168.2.1 closed by foreign host]
SERVER> ssh -l SSHadmin 192.168.2.1
Open
Password:
R2#
```

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

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

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=3ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=7ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 3ms

PC>
```

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

```
PC> ssh -l SSHadmin 192.168.2.1
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

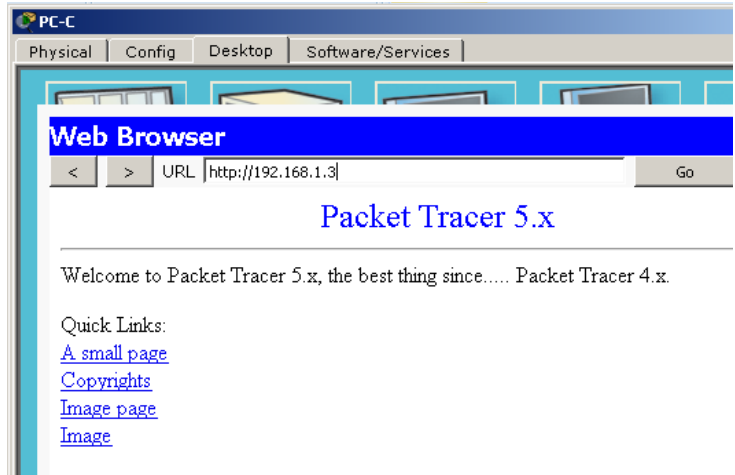
Reply from 192.168.1.3: bytes=32 time=3ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=7ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 3ms

PC>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#
```

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



Part 2: Secure Access to Routers

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

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

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

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

```
R2>en
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)#
```

```
R3>en
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#
```

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

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

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

```

line vty 0 4
password 7 0822455D0A1613030B1B0D517F
login local
transport input ssh
!
!
ntp update-calendar
!
end

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

```

```

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)#

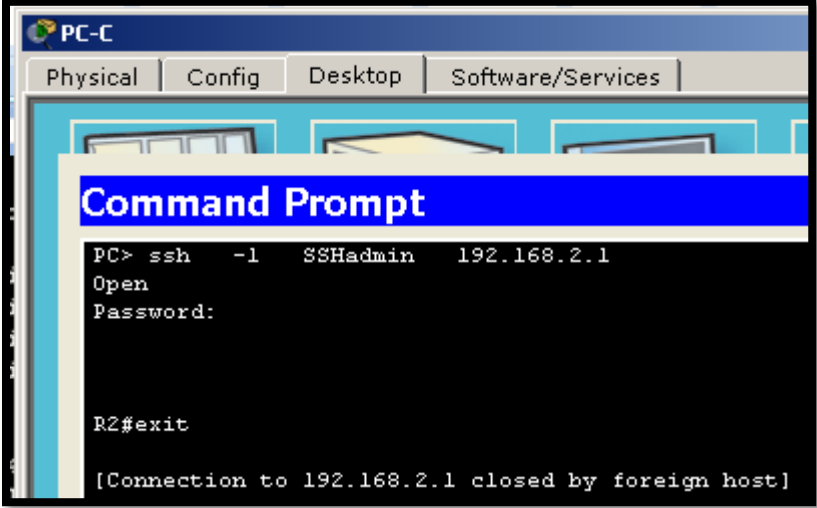
```

Packet Tracer - Configure IP ACLs to Mitigate Attacks

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

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

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



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

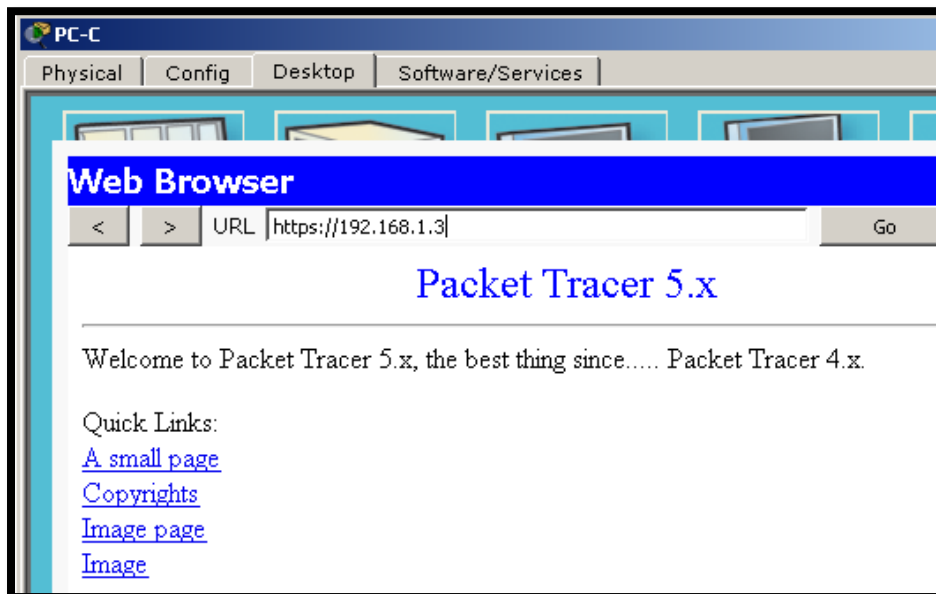


Part 3: Create a Numbered IP ACL 120 on R1

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

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

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



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

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

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

```
R1(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
```

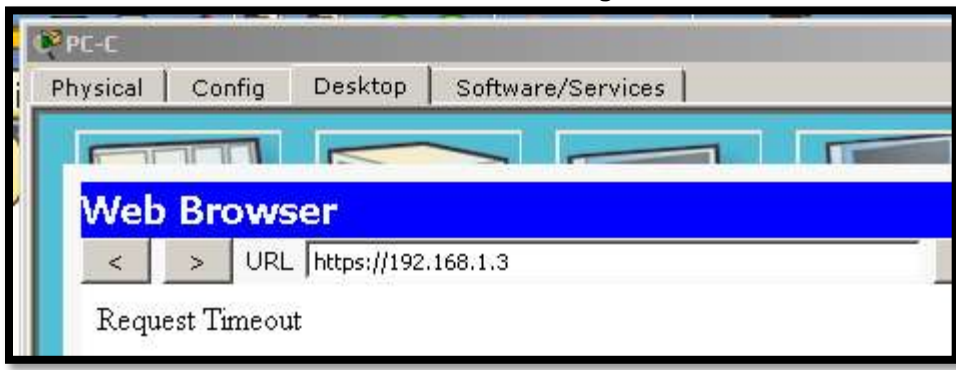
Step 3: Apply the ACL to interface S0/0/0.

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

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

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

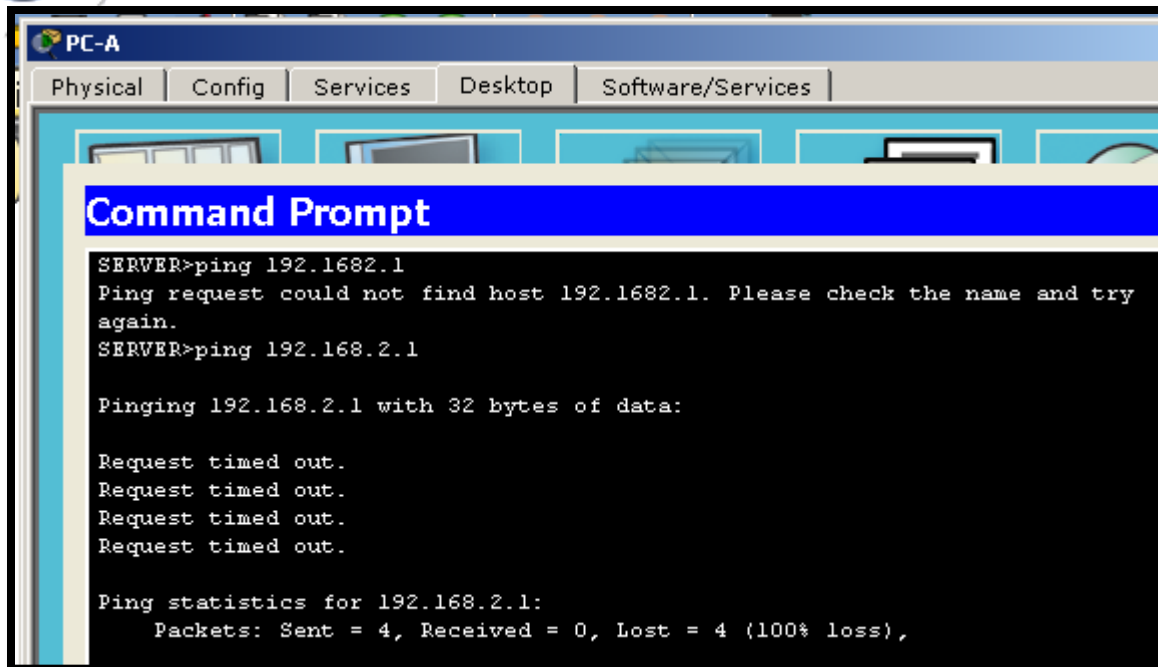
Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.



Part 4: Modify An Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to R1); deny all other incoming ICMP packets.

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



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

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

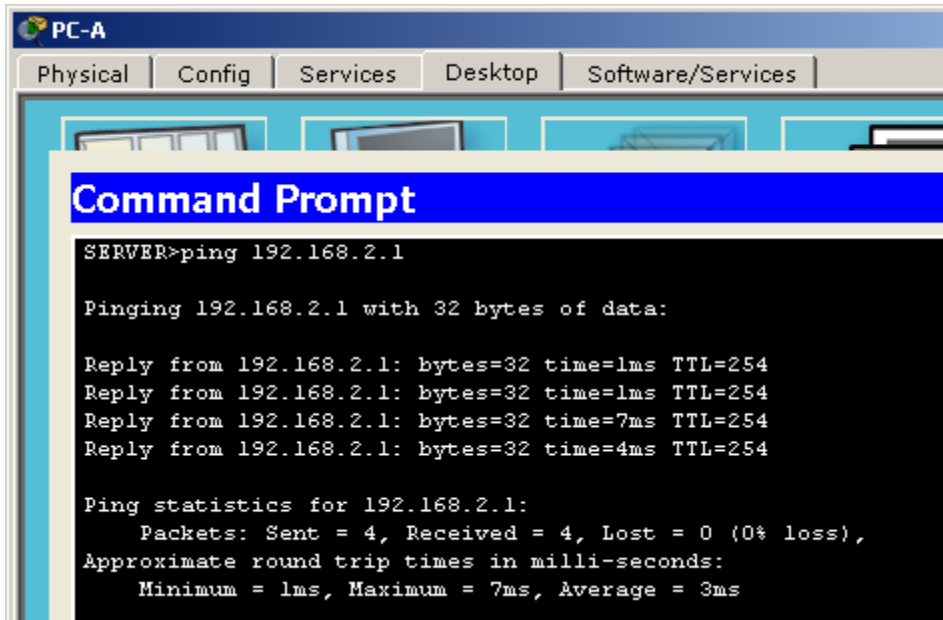
```

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

```

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

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



Part 5: Create a Numbered IP ACL 110 on R3

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

Packet Tracer - Configure IP ACLs to Mitigate Attacks

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

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

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

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

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

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

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

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)# ip access-group 110 in
R3(config-if)#
```

Part 6: Create a Numbered IP ACL 100 on R3

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

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

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

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

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

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

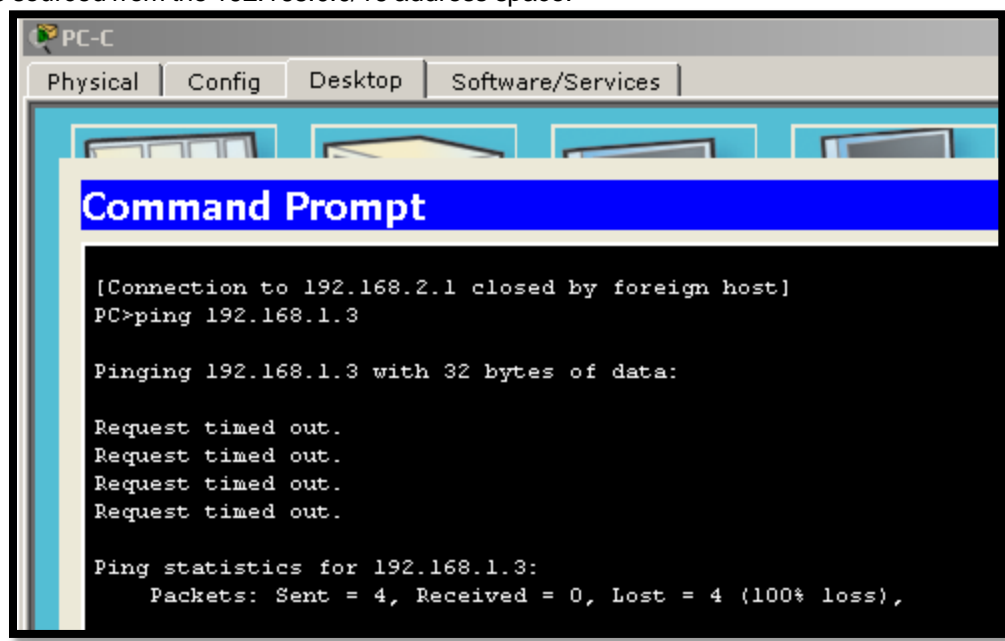
Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.

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

```
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#exit
```

Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

From the **PC-C** command prompt, ping the **PC-A** server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.



Step 4: Check results.

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

!!!Script for R1

```
access-list 10 permit 192.168.3.3 0.0.0.0
line vty 0 4
access-class 10 in
access-list 120 permit udp any host 192.168.1.3 eq domain
access-list 120 permit tcp any host 192.168.1.3 eq smtp
access-list 120 permit tcp any host 192.168.1.3 eq ftp
access-list 120 deny tcp any host 192.168.1.3 eq 443
```

Packet Tracer - Configure IP ACLs to Mitigate Attacks

```
access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
interface s0/0/0
ip access-group 120 in
access-list 120 permit icmp any any echo-reply
access-list 120 permit icmp any any unreachable
access-list 120 deny icmp any any
access-list 120 permit ip any any
```

!!!Script for R2

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

!!!Script for R3

```
access-list 10 permit 192.168.3.3 0.0.0.0
line vty 0 4
access-class 10 in
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 224.0.0.0 15.255.255.255 any
access-list 100 permit ip any any
interface s0/0/1
ip access-group 100 in
access-list 110 permit ip 192.168.3.0 0.0.0.255 any
interface fa0/1
ip access-group 110 in
```

Cisco Packet Tracer - D:\UNAD\2do. Semestre 2017\Diplomado\CCNA2\Colaborativo 2\CCNA2 R&S UNIDAD 4\LISTAS DE ACCESO\...

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 01:37:43

Congratulations Guest! You completed the activity.

Overall Feedback | **Assessment Items** | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)
[-] Network			
[-] R1			
[-] ACL			
✓ 10	Correct	1	ACL
✓ 120	Correct	1	ACL
[-] Ports		0	Other
[-] Serial0/0/0		0	Other
✓ Access-grou...	Correct	1	ACL
[-] VTY Lines			
[-] VTY Line 0		0	Physical
✓ Access Cont...	Correct	1	ACL
[-] VTY Line 1		0	Physical
✓ Access Cont...	Correct	1	ACL
[-] VTY Line 2		0	Physical
✓ Access Cont...	Correct	1	ACL
[-] VTY Line 3		0	Physical
✓ Access Cont...	Correct	1	ACL
[-] VTY Line 4		0	Physical
✓ Access Cont...	Correct	1	ACL
[-] R2			
[-] ACL		0	ACL
✓ 10	Correct	1	ACL
[-] VTY Lines			
[-] VTY Line 0		0	Physical
✓ Access Cont...	Correct	1	ACL
[-] VTY Line 1		0	Physical
✓ Access Cont...	Correct	1	ACL
[-] VTY Line 2		0	Physical
✓ Access Cont...	Correct	1	ACL

Score : 23/23

Item Count : 23/23

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

Close

9.2.1.10 Packet Tracer Configuring Standard ACLs (Adriana Romero Ramirez)

Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.

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

Step 2: Evaluate two network policies and plan ACL implementations.

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

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

To restrict access from the 192.168.11.0/24 network to the **WebServer** at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

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

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

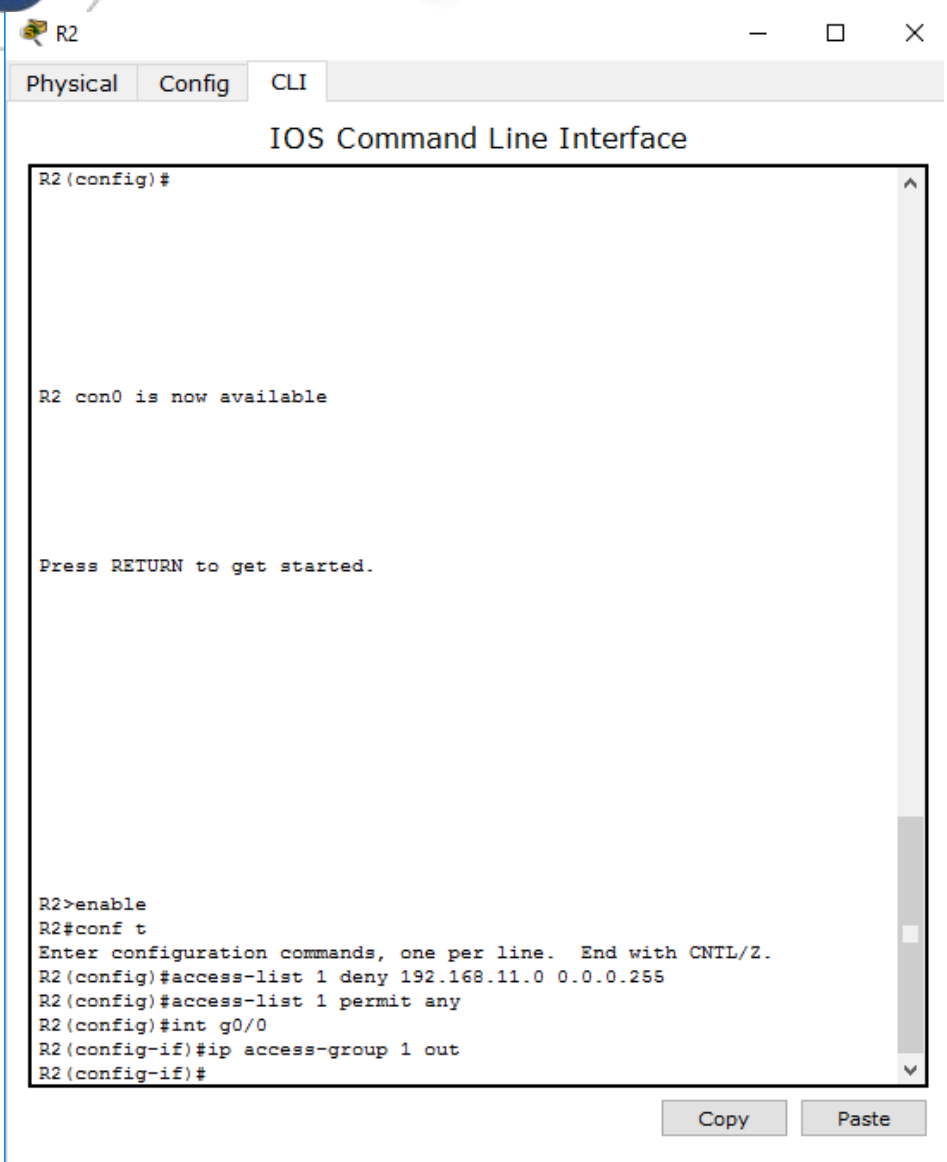
To restrict access from the 192.168.10.0/24 network to the 192.168.30.0/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must be placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

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

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

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

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

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

```
R2 (config)# interface GigabitEthernet0/0  
R2 (config-if)# ip access-group 1 out
```

Step 2: Configure and apply a numbered standard ACL on R3.

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

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

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

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

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

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

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

The screenshot shows a terminal window titled "R3" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" which displays the following text:

```

Press RETURN to get started!

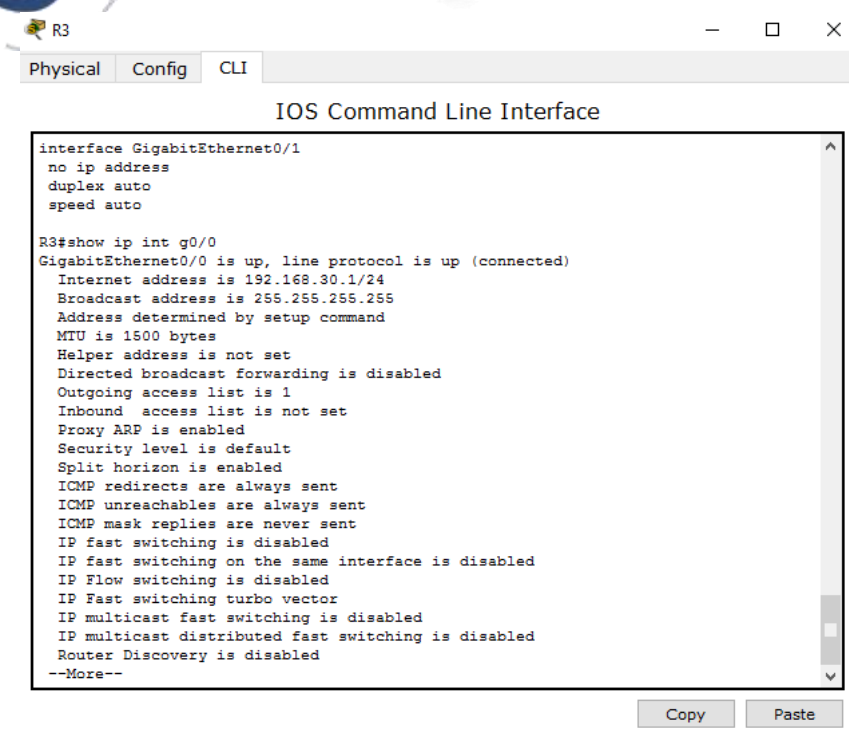
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.1 (Serial0/0/1) is up: new adjacency
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.3.3.1 (Serial0/0/0) is up: new adjacency

R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#int g0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
    
```

At the bottom right of the terminal window, there are "Copy" and "Paste" buttons.

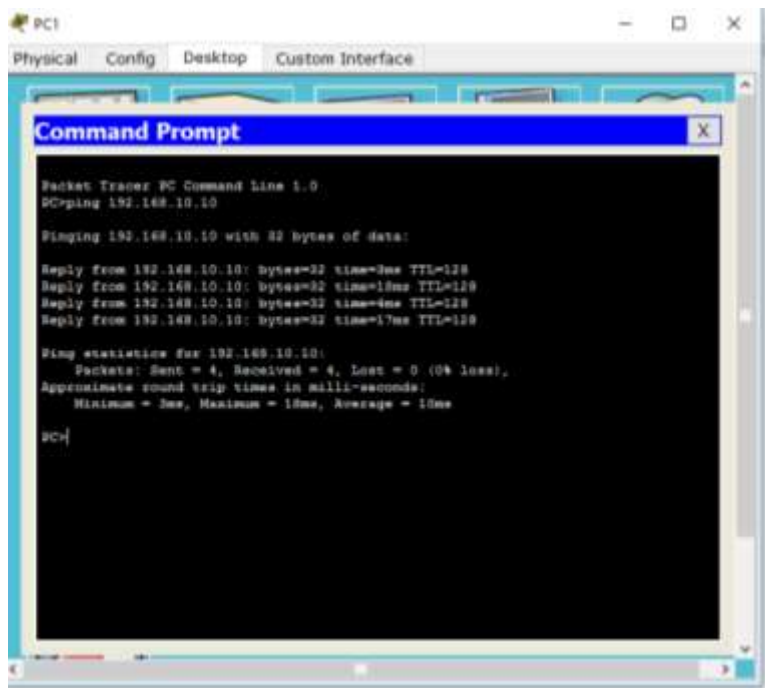
Step 3: Verify ACL configuration and functionality.

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

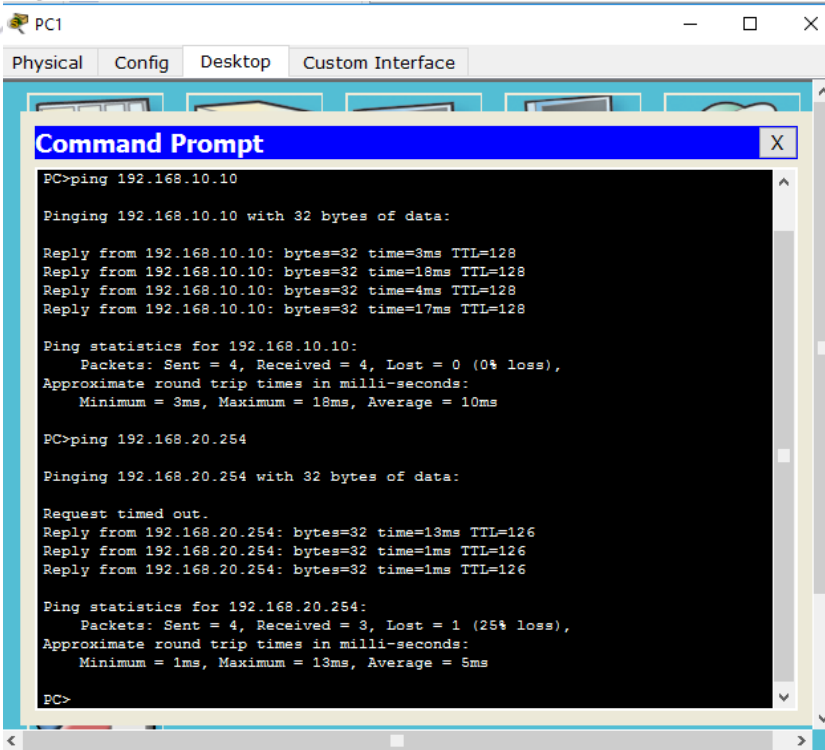


b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:

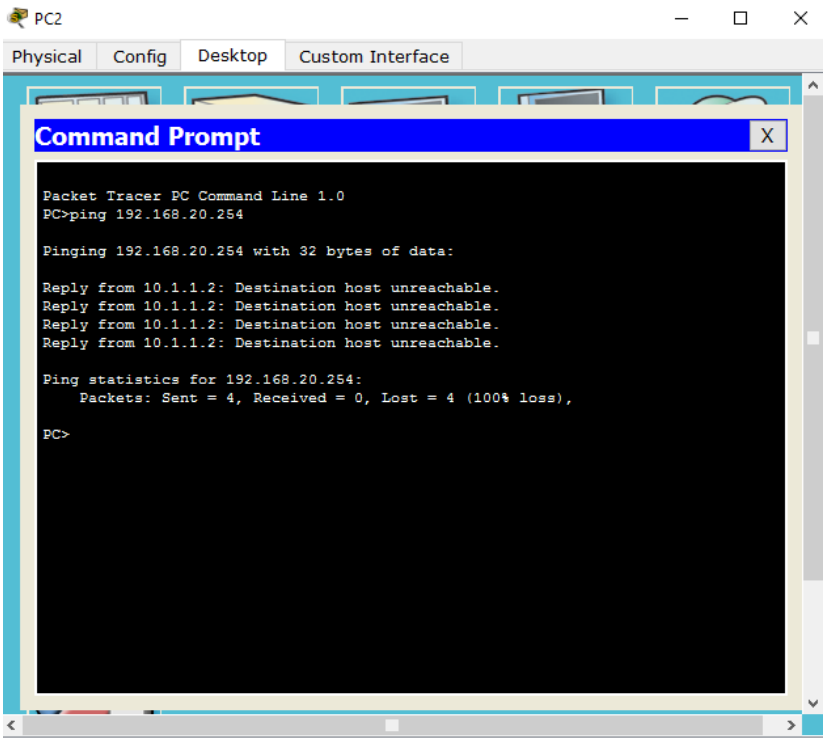
- A ping from 192.168.10.10 to 192.168.11.10 succeeds.



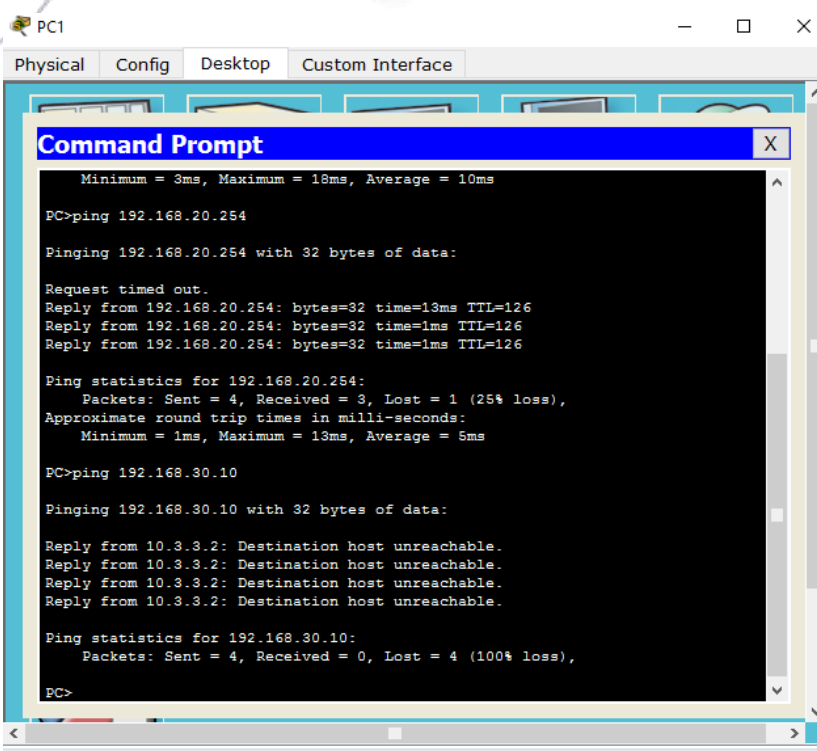
- A ping from 192.168.10.10 to 192.168.20.254 succeeds.



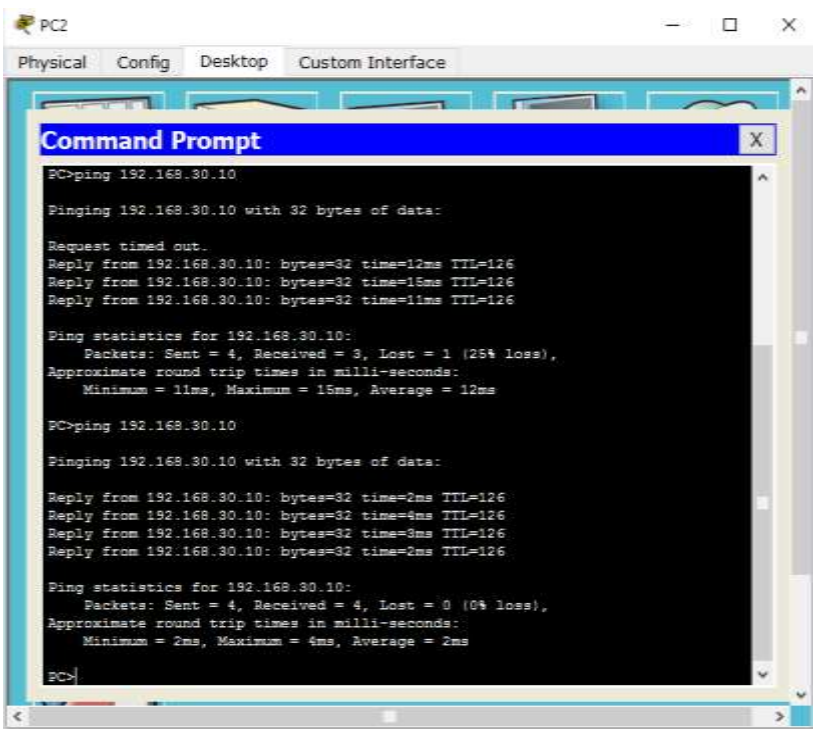
- A ping from 192.168.11.10 to 192.168.20.254 fails.



- A ping from 192.168.10.10 to 192.168.30.10 fails.

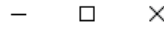


- A ping from 192.168.11.10 to 192.168.30.10 succeeds.



- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

PC1



Physical Config Desktop Custom Interface

Command Prompt

```

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

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

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

PC>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=12ms TTL=126
Reply from 192.168.20.254: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms

PC>
    
```

Case Packet Tracer Student - DIUSUARIO\Documents\UNAD\BLOQUEO CISCO\UNIDAD 3\COM2 285 UNAD\ALISTAS DE ACCESO\3.1.10 Packet Tracer Configuring Standard ACLs.pka



Activity Results

Time Elapsed: 00:27:24

Congratulations ADRIANA RONDEL D! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
<ul style="list-style-type: none"> ACL <ul style="list-style-type: none"> 1 <input checked="" type="checkbox"/> Correct 25 Ports <ul style="list-style-type: none"> GigabitEthernet0/0 0 Access-group <input checked="" type="checkbox"/> Correct 25 R3 <ul style="list-style-type: none"> ACL <ul style="list-style-type: none"> 1 <input checked="" type="checkbox"/> Correct 25 Ports <ul style="list-style-type: none"> GigabitEthernet0/0 0 Access-group <input checked="" type="checkbox"/> Correct 25 			ACL, IPv4 Standard, Other, IPv4 Standard, IPv4 Standard, IPv4 Standard, IPv4 Standard	

Score : 100/100

Item Count : 4/4

Component	Items/Total	Score
IPv4 Standard ACL Implementation	4/4	100/100

Close

9.2.1.11 Packet Tracer - Configuring Named Standard ACLs (Adriana Romero Ramirez)

Addressing Table

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

Objectives

Part 1: Configure and Apply a Named Standard ACL

Part 2: Verify the ACL Implementation

Background / Scenario

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

Part 1: Configure and Apply a Named Standard ACL

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

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

Step 2: Configure a named standard ACL.

Configure the following named ACL on R1.

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

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

Step 3: Apply the named ACL.

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

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

b. Save the configuration.

IOS Command Line Interface

```
Compiled Mon 16-May-06 14:34 by pc_ceam  
Press RETURN to get started!  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1/0, changed state to up  
  
R1>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)#ex  
R1(config)#int f0/1  
R1(config-if)#ip access-group File_Server_Restrictions out  
R1(config-if)#end  
R1#  
%SYS-5-CONFIG_I: Configured from console by console  
  
R1#
```

Copy Paste

```

R1
Physical Config CLI
IOS Command Line Interface

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

R1>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)#ex
R1(config)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Copy Paste

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the interface.

Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface fastethernet 0/1** command to verify that the ACL is applied correctly to the interface.

```

R1
Physical Config CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1/0, changed state to up

R1>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)#ex
R1(config)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#show access-lists
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.20.4
 20 deny any
R1#
Copy Paste

```

Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the **Web Server**, but only **PC1** should be able to ping the **File Server**.

```
PC0
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.100: bytes=32 time=10ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=8ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

PC>
```

```
PC1
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

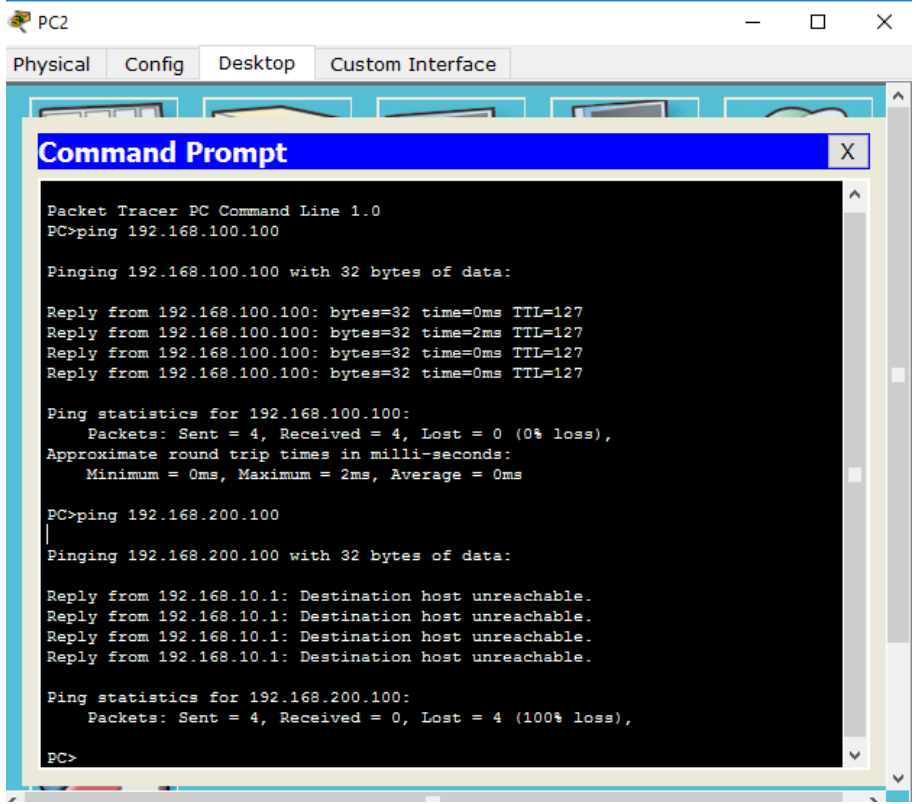
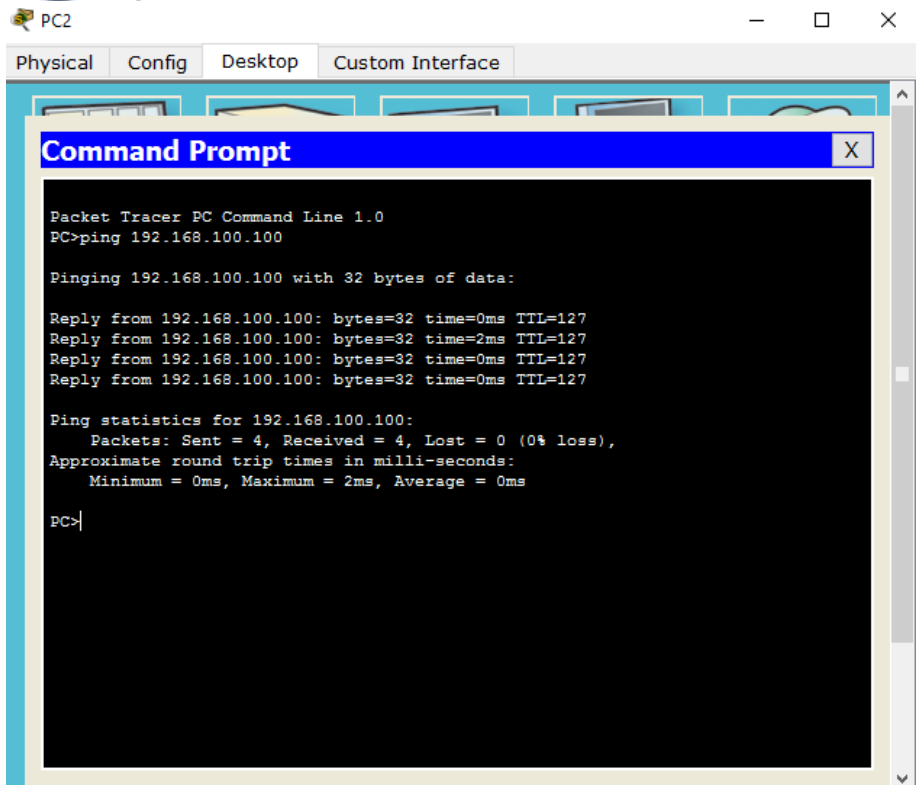
PC>ping 192.168.100.100

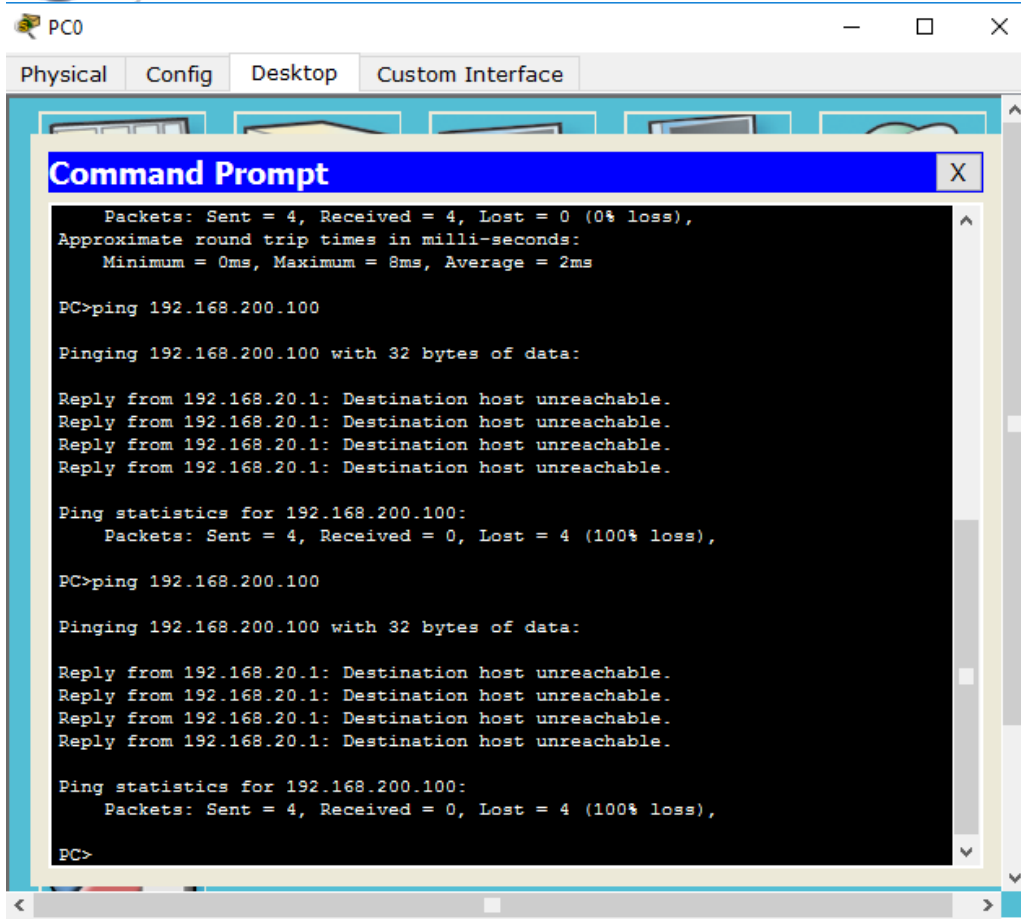
Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=8ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

PC>
```





Cisco Packet Tracer Student - D:\USUARIO\Documents\UNAD\DIPLOMADO CISCO\UNIDAD 3\CCNA2 R&S UNIDAD 4\LL... - □ X

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 00:09:07

Congratulations ADRIANA ROMERO RAMIREZ! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

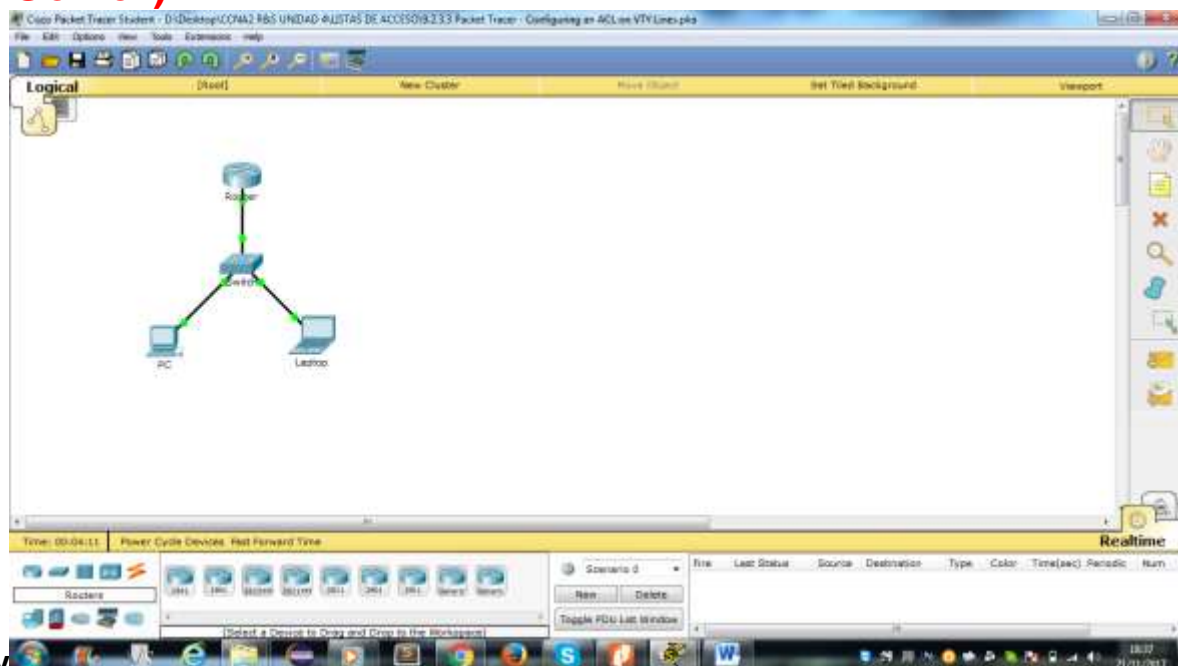
Assessment Items	Status	Points
Network		
R1		
ACL		0
✓ File_Server_Restric...	Correct	80
Ports		0
FastEthernet0/1		0
✓ Access-group Out	Correct	20

Component	Items/Total	Score
IPv4 Standard ACL Implementation	2/2	100/100

Score : 100/100
Item Count : 2/2

Close

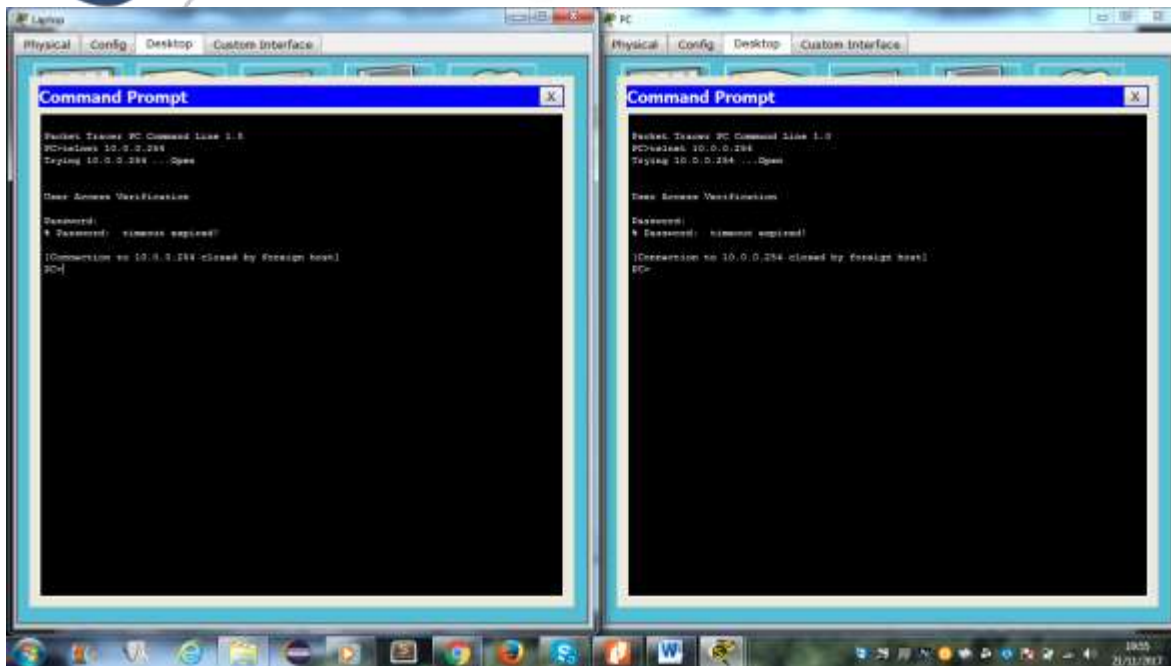
9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines (Jhon James Gomez)



Topology Addressing Table

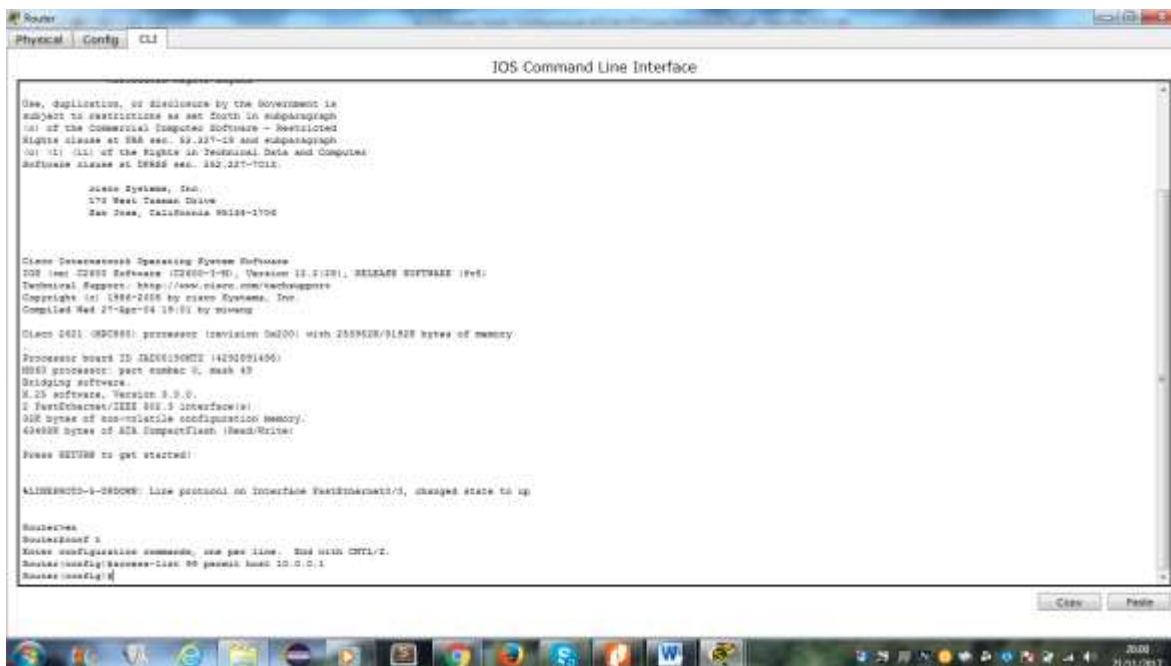
Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Laptop	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Part 1: Configure and Apply an ACL to VTY Lines
Step 1: Verify Telnet access before the ACL is configured.



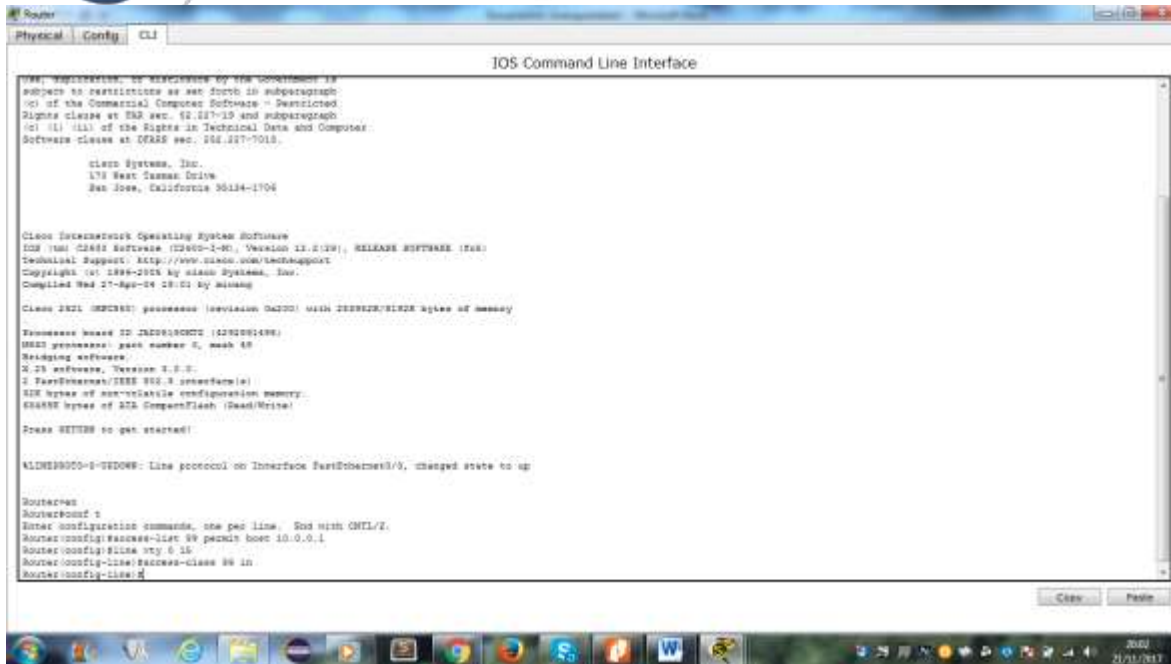
Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on Router



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

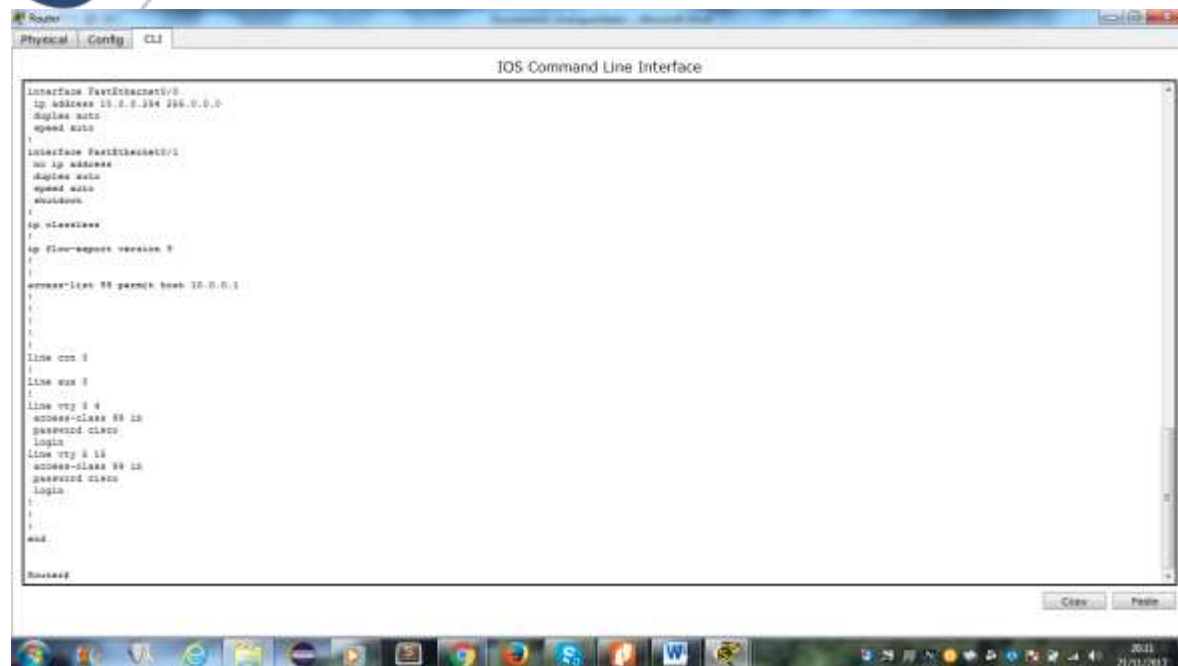
Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration mode for lines 0 – 4 and use the **access-class** command to apply the ACL to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



Part 2: Verify the ACL Implementation

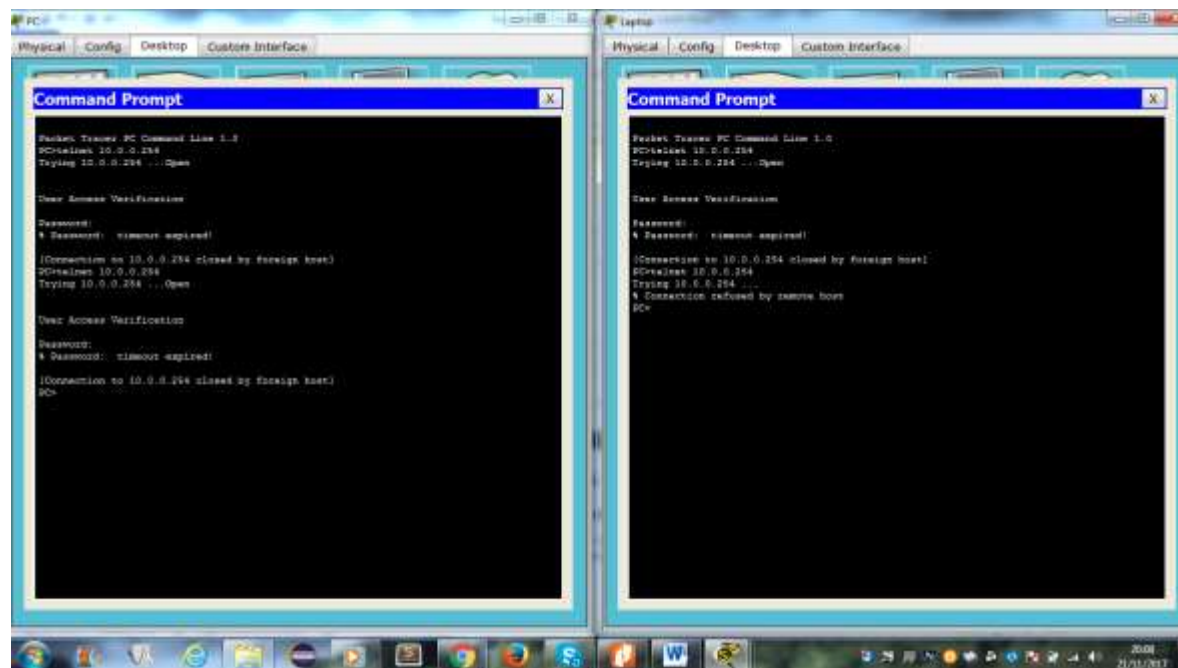
Step 1: Verify the ACL configuration and application to the VTY lines.

Use the **show access-lists** to verify the ACL configuration. Use the **show run** command to verify the ACL is applied to the VTY lines



Step 2: Verify that the ACL is working properly.

Both computers should be able to ping the Router, but only PC should be able to Telnet to it



9.5.2.6 Packet Tracer - Configuring IPv6 ACLs (Jorge Luis Quintero)

Topología

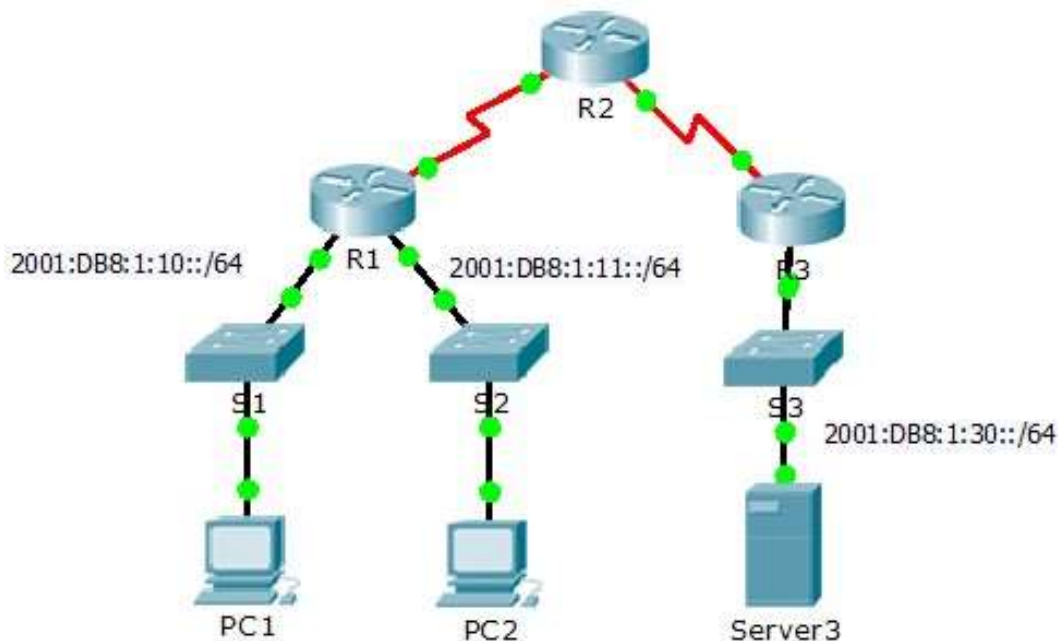


Tabla de enrutamiento

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

Objetivos

Parte 1: Configurar, aplicación y verificación de una ACL IPv6

Parte 2: Configurar, aplicación y verificación de un segundo IPv6 ACL

Parte 3: Configurar, aplicación y verificación de una ACL IPv6

Escenario

Registros indican que un ordenador en el 2001: DB8: 1:11::0/64 red es refrescante en repetidas ocasiones su página Web causando un ataque de denegación de servicio (DoS) contra Server3. Hasta que el cliente puede ser identificado y limpiado, debe bloquear el acceso HTTP y HTTPS a esa red con una lista de acceso.

Paso 1: Configurar una ACL que bloqueará el acceso HTTP y HTTPS.

Configurar una ACL nombrada BLOCK_HTTP en R1 con las siguientes afirmaciones.

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#
```

a. Bloquear el tráfico HTTP y HTTPS de alcanzar Server3

```
R1(config-ipv6-acl)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

```
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#|
```

b. Deje que el resto del tráfico IPv6 para pasar

```
R1(config-ipv6-acl)#permit ipv6 any any
```

```
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#
```

Paso 2: Aplicar la ACL a la interfaz correcta.

Aplicar la ACL en la interfaz más cercana al origen del tráfico que se bloquee.

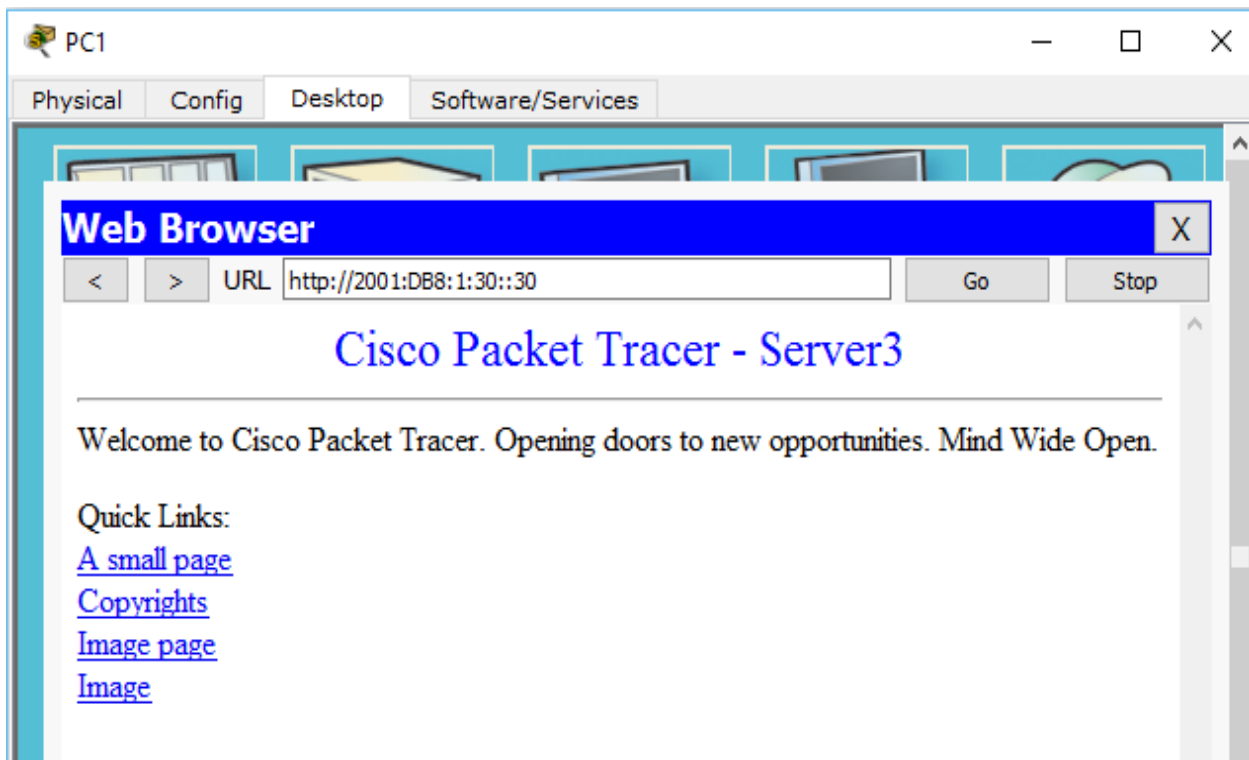
```
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

```
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#int g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
```

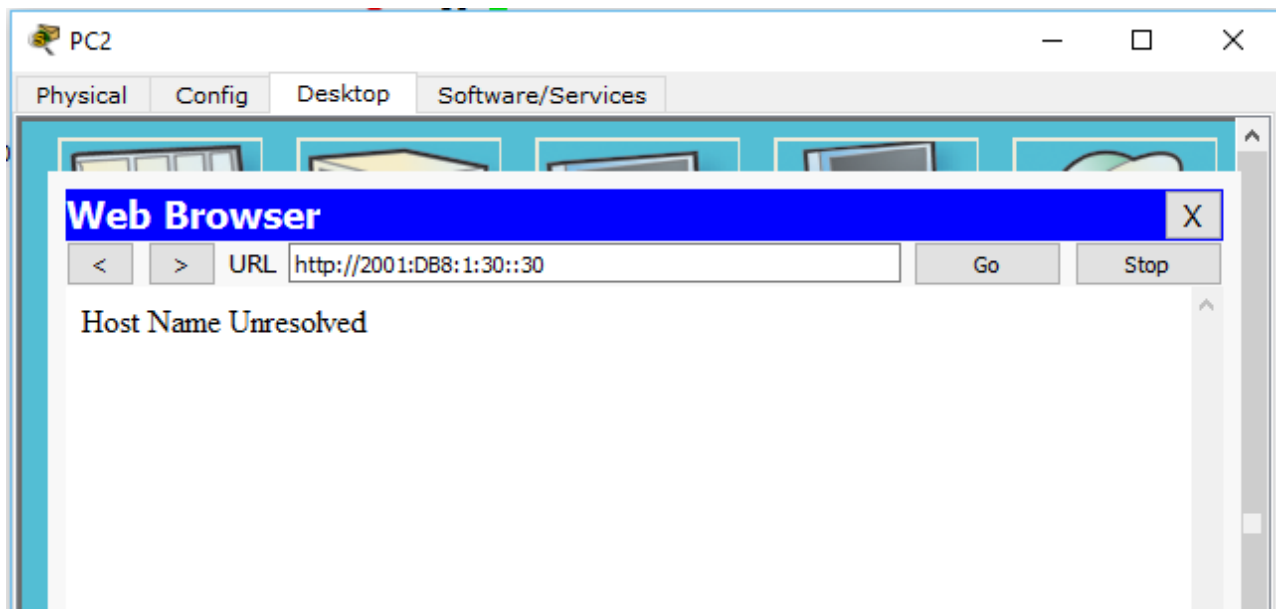
Paso 3: Verificar la implementación de ACL

Compruebe la ACL está funcionando según lo previsto por la realización de las siguientes pruebas:

- Abra el navegador web de PC1 a `http://2001:DB8:1:30::30` o `https://2001:DB8:1:30::30`. El sitio web debe aparecer.



- Abra el navegador web de PC2 a `http://2001:DB8:1:30::30` o `https://2001:DB8:1:30::30`. El sitio web debe ser bloqueada



- Ping de PC2 a 2001:DB8:1:30::30. El ping debe tener éxito

```

PC2
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:1:30::30

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

Reply from 2001:DB8:1:30::30: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=24ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=11ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 24ms, Average = 14ms

PC>
  
```

Parte 2: Configurar, aplicación y verificación de un segundo IPv6 ACL

Los registros indican ahora que el servidor está recibiendo pings de muchas diferentes direcciones IPv6 en un ataque de Denegación de Servicio Distribuida (DDoS). Debe filtrar las solicitudes de ping ICMP a su servidor.

Paso 1: Crear una lista de acceso para bloquear ICMP

Configurar una ACL nombrada BLOCK_ICMP en R3 con las siguientes afirmaciones:

```

R3>enable
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
  
```

- Bloquear todo el tráfico ICMP desde cualquier host a cualquier destino.

```
R3(config-ipv6-acl)# deny icmp any any
```

- Deje que el resto del tráfico IPv6 para pasar.

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

```
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
```

Paso 2: Aplicar la ACL a la interfaz correcta

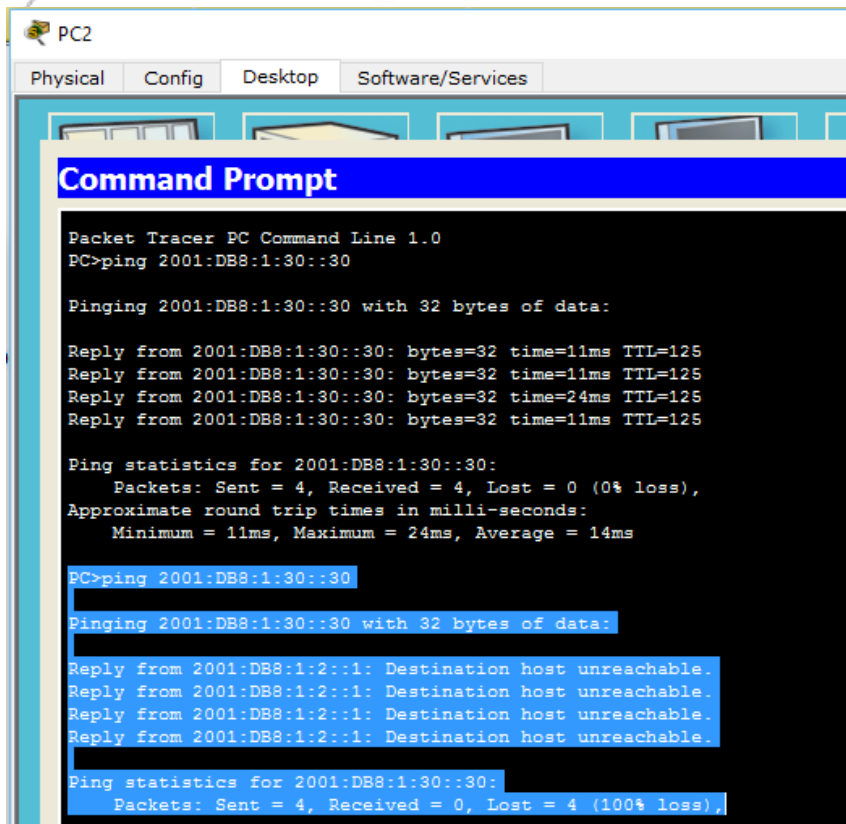
En este caso, el tráfico ICMP puede provenir de cualquier fuente. Para garantizar que el tráfico ICMP está bloqueado, independientemente de su origen o cambios que se producen a la topología de la red, aplique la ACL más cercano al destino.

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

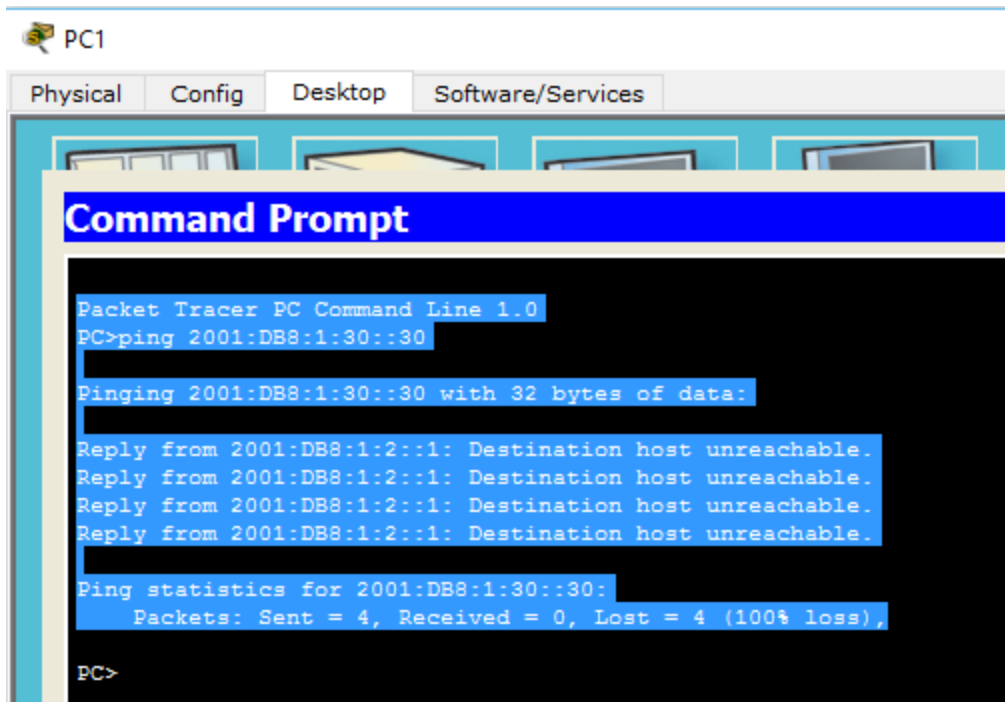
```
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

Paso 3: Verificar que las funciones de la lista de acceso adecuados

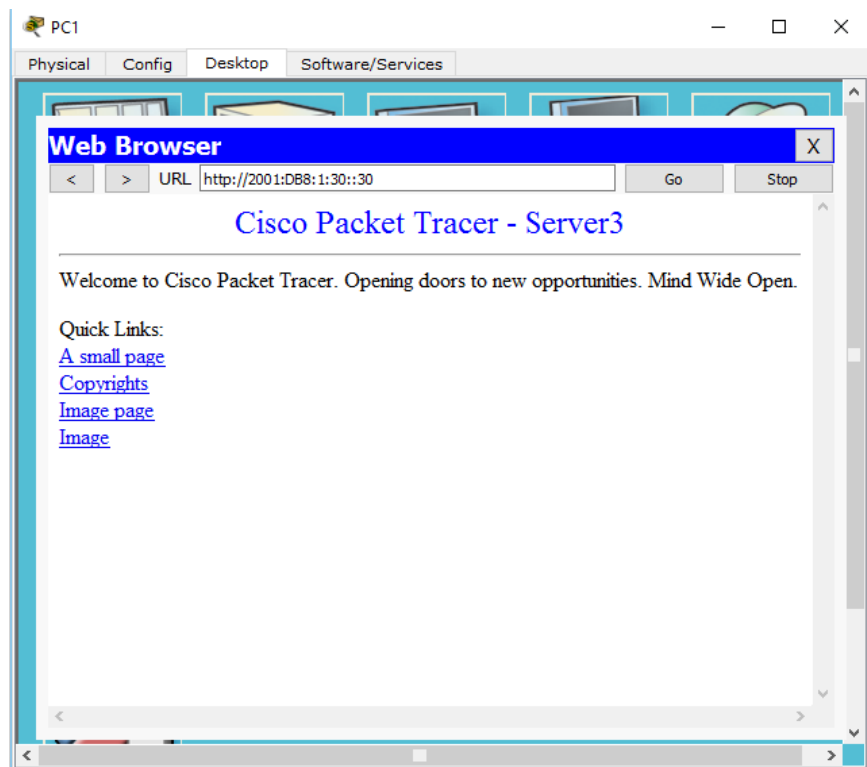
- a. Ping de PC2 a 2001:DB8:1:30::30. El ping debe fallar.



b. Ping desde PC1 a 2001:DB8:1:30::30. El ping debe fallar.



Abra el navegador web de PC1 a <http://2001:DB8:1:30::30> o <https://2001:DB8:1:30::30>. El sitio web debe mostrar.



Cisco Packet Tracer - D:\trabajos 2017_II\JORGE LUIS QUINTERO\unidad 4\9.5.2.6 Packet Tracer - Confi...

File Edit Options View Tools Extensions Help

Logical Back [Root] New Cluster Move Object Set Tiled Background Viewport Environment: 05:00:00

Packet Tracer - Configuring IPv6 ACLs

PT Activity: 01:13:22

Addressing Table

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

Objectives

Part 1: Configure, Apply, and Verify an IPv6 ACL
Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Time Elapsed: 01:13:22 Completion: 100/100

Top

PC1 PC2 Server3

Time: 00:02:31 Power Cycle Devices Fast Forward Time Realtime

1941 2901 2911 819IOX 819HGW 829 1240 Generic Generic 1841 2620XM 2621XM 2811

2811

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 01:09:20

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points
[-] Network		
[-] R1		
[-] ACLV6		0
✓ BLOCK_HTTP	Correct	40
[-] Ports		0
[-] GigabitEthernet0/1		0
✓ IPv6 Traffic Filte...	Correct	10
[-] R3		
[-] ACLV6		0
✓ BLOCK_ICMP	Correct	40
[-] Ports		0
[-] GigabitEthernet0/0		0
✓ IPv6 Traffic Filte...	Correct	10

Component	Items/Total	Score
IPv6 ACL Implementation	4/4	100/100

Close

REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

