

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ECBTI.

CURSO.

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

GRUPO.

CÓDIGO: 203092_10

ACTIVIDAD COLABORATIVA UNIDAD 4.

INTEGRANTES.

YESENIA IBET BRITO.

LORAINE RANGEL.

ANDRES ALFONSO MENDOZA GONZALEZ.

IVÁN DAVID LÓPEZ HOYOS.

ARIEL FERNANDO AGUIRRE MARTINEZ.

FECHA.

21/05/2017

TABLA DE CONTENIDO.

INTRODUCCIÓN.

OBJETIVOS.

INFORME DE EJERCICIOS.

- 7.3.2.4 Lab - Configuring Basic RIPv2 and RIPv2
- 8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2
- 8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3
- 10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router
- 10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch
- 10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6
- 10.3.1.1 IoE and DHCP
- 11.2.2.6 Lab - Configuring Dynamic and Static NAT
- 11.2.3.7 Lab - Configuring NAT Pool Overload and PAT

EJERCICIOS PKA

- 4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks
- 9.2.1.10 Packet Tracer Configuring Standard ACLs
- 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs
- 9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines
- 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs

CONCLUSIÓN.

BIBLIOGRAFÍAS.

INTRODUCCIÓN.

Cuando hablamos de compartir información y de realizar la comunicación entre distintos sistemas tecnológicos, el enrutamiento dinámico es uno de los primeros conceptos que nos vienen a la cabeza. Bajo este proceso una serie de máquinas que se encuentren dentro de una misma red tendrán capacidad para llevar a cabo una comunicación entre ellas de forma permanente. Su comunicación se ocupará de que las tablas de enrutamiento estén siempre en una actualización adecuada, se controlará el estado vinculado a los enlaces y además se podrán comprobar cuáles son las rutas más convenientes en base al estado del análisis de la red.

En esta actividad y teniendo en cuenta cada uno de los conceptos de los diferentes capítulos del enrutamiento en soluciones de red, donde se desarrollaran una serie de ejercicios prácticos que permitirán adquirir los conocimientos básicos en el mundo de las redes; no obstante cabe recalcar que dichos conocimientos a través de estos son llevados a la práctica, lo cual permiten abordar profundamente muchos más las diferentes temáticas.

OBJETIVOS.

Objetivo General.

Comprender los conceptos más importantes del enrutamiento en soluciones de red.

Objetivos específicos.

Conocer los conceptos básicos de lista de control de acceso.

Identificar el enrutamiento dinámico.

Establecer DHCP.

INFORME DE EJERCICIOS.

7.3.2.4 Lab: configuración básica de RIPv2 y RIPv6

Topología

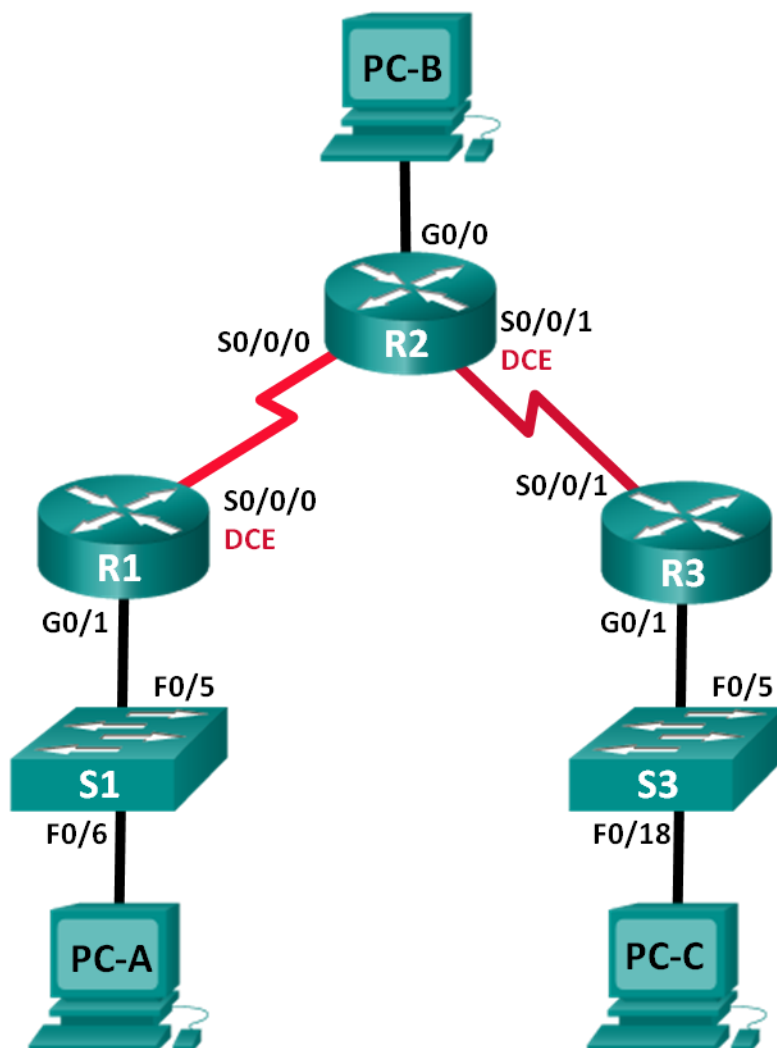


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing RIPv2

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

Parte 3: configurar IPv6 en los dispositivos

Parte 4: configurar y verificar el routing RIPv2

- Configurar y verificar que se esté ejecutando RIPv2 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 (RIPv2) es un protocolo de routing vector distancia para enrutar direcciones IPv6, según la definición de RFC 2080. RIPv2 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 universal9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbase9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de 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 lanbase9 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.

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

```
R1# config t
```

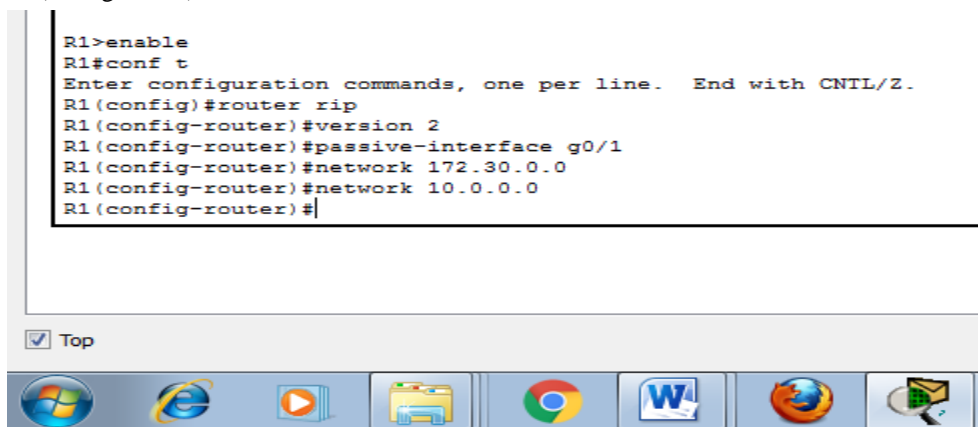
```
R1(config)# router rip
```

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

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

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

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



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

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.

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

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

```
R2# show ip interface brief
```

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

R2

Physical Config CLI Attributes

IOS Command Line Interface

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

b. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? No ¿Por qué? Porque no hay una ruta que llegue a PC-B, y esta red no participa en rip.

PCA

Physical Config Desktop Attributes Software/Services

Command Prompt

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

Pinging 209.165.201.2 with 32 bytes of data:

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

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

C:\>
```

¿Es posible hacer ping de la PC-A a la PC-C? No ¿Por qué? R1 y R3 no tienen rutas a las subredes específicas al router remoto.

```
C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

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

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

C:\>
```

¿Es posible hacer ping de la PC-C a la PC-B? No ¿Por qué? La red donde esta PC-B no participa en rip y no existe una ruta.

```

PCC
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Link-local IPv6 Address . . . . . : FE80::2E0:8FFF:FE7E:BEE3
    IP Address. . . . . : 172.30.30.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.30.30.1

C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

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

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

C:\>|

```

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

```

C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

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

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

C:\>|

```

No ¿Por qué? R1 y R3 no tiene rutas en la subredes específica del router remoto.

```

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:15, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1

R3#|

```

c. Verifique que RIPv2 se ejecute en los routers.

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

R1# **show ip protocols**

```

R1>enable
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 3 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0        2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway            Distance      Last Update
  10.1.1.2           120          00:00:13
Distance: (default is 120)
R1#

```

Routing Protocol is "rip"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Sending updates every 30 seconds, next due in 7 seconds
 Invalid after 180 seconds, hold down 180, flushed after 240
 Redistributing: rip
 Default version control: send version 2, receive 2
 Interface Send Recv Triggered RIP Key-chain
 Serial0/0/0 2 2
 Automatic network summarization is in effect
 Maximum path: 4
 Routing for Networks:
 10.0.0.0
 172.30.0.0
 Passive Interface(s):
 GigabitEthernet0/1
 Routing Information Sources:
 Gateway Distance Last Update
 10.1.1.2 120 00:00:13
 Distance: (default is 120)

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

```

R2>enable
R2#debug ip rip
RIP protocol debugging is on
R2#

```

Nos envía versión 2 por esta dirección multicast 224.0.0.9 via s0/0/0 y via s0/0/1, y se envían actualizaciones.

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?

```

interface Vlan1
no ip address
shutdown
!
router rip
version 2
passive-interface GigabitEthernet0/1
network 10.0.0.0
network 172.30.0.0
!
ip classless

```

- d. Examinar el sumarización automática de las rutas.

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

R2# show ip route

```

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R       172.30.0.0/16 [120/1] via 10.1.1.1, 00:00:10, Serial0/0/0
          [120/1] via 10.2.2.1, 00:00:22, Serial0/0/1

```

<Output Omitted>

```

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

```

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

R1# show ip route

```

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

Gateway of last resort is not set

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

R1#

```

<Output Omitted>

```

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C   10.1.1.0/30 is directly connected, Serial0/0/0
L   10.1.1.1/32 is directly connected, Serial0/0/0
R   10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C   172.30.10.0/24 is directly connected, GigabitEthernet0/1
L   172.30.10.1/32 is directly connected, GigabitEthernet0/1

```

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

R3# show ip route

```

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:11, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1

R3#

```

<Output Omitted>

```

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

```

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

```
R2>enable
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
    10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
    10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
    172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.0.0/16 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
    10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
    10.1.1.0/30 via 0.0.0.0, metric 1, tag 0

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

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

R2#undebug all
All possible debugging has been turned off
R2#
```

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

Paso 3. Desactivar la sumarización automática.

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

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

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

```
R1>
R1>enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#no auto-summary
R1(config-router)#
```

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

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

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

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

R1#clear ip route *
R1#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

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

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

R2# show ip route

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

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.2/32 is directly connected, Serial0/0/0
C    10.2.2.0/30 is directly connected, Serial0/0/1
L    10.2.2.2/32 is directly connected, Serial0/0/1
R    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R    172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:26, Serial0/0/1
R    172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:27, Serial0/0/0
R    172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:02, Serial0/0/1

R2#
```

<Output Omitted>

Gateway of last resort is not set

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

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

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

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

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

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

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

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

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

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

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

C 209.165.201.0/24 is directly connected, GigabitEthernet0/0

L 209.165.201.1/32 is directly connected, GigabitEthernet0/0

R1# show ip route

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

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
R    10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:15, Serial0/0/0
R    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R    172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:15, Serial0/0/0

R1#
```

<Output Omitted>

Gateway of last resort is not set

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

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

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

```

R    10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R    172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0

```

R3# show ip route

```

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

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R    10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:05, Serial0/0/1
C    10.2.2.0/30 is directly connected, Serial0/0/1
L    10.2.2.1/32 is directly connected, Serial0/0/1
R    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R    172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:05, Serial0/0/1
C    172.30.30.0/24 is directly connected, GigabitEthernet0/1
L    172.30.30.1/32 is directly connected, GigabitEthernet0/1

R3#

```

<Output Omitted>

```

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

```

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

R2# debug ip rip

```

R2>enable
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.30.0/24 via 0.0.0.0 in 1 hops
|

```

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

```

R2#no debug ip rip
RIP protocol debugging is off
R2#

```


¿Qué rutas que se reciben del R3 se encuentran en las actualizaciones RIP. **172.30.30.0/24**

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

R2#no debug ip rip
RIP protocol debugging is off
R2#
```

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

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

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

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

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

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

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

```
R2>
R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#route rip
R2(config-router)#default-information originate
R2(config-router)#
```

Top

Paso 5. Verificar la configuración de enrutamiento.

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

```
R1# show ip route
```

```

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

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:02, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
R       172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:02, Serial0/0/0
R*    0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:02, Serial0/0/0

R1#

```

<Output Omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

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

```

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

```

¿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.

A través de un gateway de último lance, es decir una puerta de enlace que nos conecta a internet, y la ruta por defecto que se muestra en la tabla de ruteo este prendida por rip.

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

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
    172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:26, Serial0/0/1

R2#
```

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

R2 tiene una ruta estática por defecto 0.0.0.0 a través de la 209.165.201.2 que directamente está conectada a la g0/0

Paso 6. Verifique la conectividad.

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

¿Tuvieron éxito los pings? Si

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

¿Tuvieron éxito los pings? Si

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

Parte 3: configurar IPv6 en los dispositivos

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

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

Parte 4: configurar y verificar el routing RIPng

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

Paso 1. configurar el routing RIPng.

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

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

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

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

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

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

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#ipv6 rip test1 enable
R1(config-if)#int s0/0/0
R1(config-if)#ipv6 rip test1 enable
R1(config-if)#
```

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

```
R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip test2 enable
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip test2 enable
R2(config-if)#
```

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

```
R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#int g0/1
R3(config-if)#ipv6 rip test3 enable
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 rip test3 enable
R3(config-if)#
```

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

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

```

R1>enable
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip test1"
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
  Redistribution:
    None
R1#

```

R1# show ipv6 protocols

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "rip Test1"

Interfaces:

Serial0/0/0

GigabitEthernet0/1

Redistribution:

None

¿En qué forma se indica RIPng en el resultado. Por el nombre del proceso.

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

R1# show ipv6 rip Test1

```

R1#show ipv6 rip database
RIP process "test1" local RIB
  2001:DB8:ACAD:C::/64, metric 3, installed
    Serial0/0/0/FE80::2, expires in 174 sec
  2001:DB8:ACAD:12::/64, metric 2
    Serial0/0/0/FE80::2, expires in 174 sec
  2001:DB8:ACAD:23::/64, metric 2, installed
    Serial0/0/0/FE80::2, expires in 174 sec
R1#

```

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?

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

- f. Inspeccione 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.

```

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

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
       C       10.1.1.0/30 is directly connected, Serial0/0/0
       L       10.1.1.1/32 is directly connected, Serial0/0/0
       R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:22, Serial0/0/0
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
       C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
       L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
       R       172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:22, Serial0/0/0
R+      0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:22, Serial0/0/0

R1#

```

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

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

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

g. Verifique la conectividad entre las computadoras.

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

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

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

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

¿Por qué algunos pings tuvieron éxito y otros no? No hay una ruta que se notifique para esta red 2001:DB8:ACAD:B::/64

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

- Desde el R2, cree una ruta estática predeterminada a la red:: 0/64 con el comando **ipv6 route** y la dirección IP de la interfaz de salida G0/0. Esto reenvía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet. Escriba el comando que utilizó en el espacio a continuación.
- Las rutas estáticas se pueden incluir en las actualizaciones RIPng mediante el comando **ipv6 rip nombre de proceso default-information originate** en el modo de configuración de interfaz. Configure los enlaces seriales en el R2 para enviar la ruta predeterminada en actualizaciones RIPng.

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

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

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

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

```

R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/0 2001:db8:acad:b::b
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip test2 default-information originate
R2(config-if)#s0/0/1
^
% Invalid input detected at '^' marker.

R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip test2 default-information originate
R2(config-if)#|

```

Paso 3. Verificar la configuración de enrutamiento.

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

R2# show ipv6 route

```
R2#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:DB8:ACAD:A::/64 [120/2]
    via FE80::1, Serial0/0/0
R   2001:DB8:ACAD:C::/64 [120/2]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
    via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
    via Serial0/0/1, receive
L   FF00::/8 [0/0]
    via Null0, receive
R2#
```

IPv6 Routing Table - 10 entries

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

U - Per-user Static route, M - MIPv6

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

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

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

D - EIGRP, EX - EIGRP external

S ::/64 [1/0]

via 2001:DB8:ACAD:B::B

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

via FE80::1, Serial0/0/0

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

via ::, GigabitEthernet0/1

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

via ::, GigabitEthernet0/1

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

via FE80::3, Serial0/0/1

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

via ::, Serial0/0/0

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

via ::, Serial0/0/0

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

via ::, Serial0/0/1

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

via ::, Serial0/0/1

L FF00::/8 [0/0]

via ::, Null0

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

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

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

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

Se muestra distribuida gracias a ripng con una métrica 2.

Paso 4. Verifique la conectividad.

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

¿Tuvieron éxito los pings? Si

Reflexión

1. **¿Por qué desactivaría la summarización automática para RIPv2?** Sería bueno para que los routers no sumaricen las rutas hacia la clase mayor, y así pueda ver conectividad entre redes discontinuas.
2. **En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3?**
Aprendieron de las actualizaciones de rip recibidas desde el router donde fue configurada la ruta por defecto en este caso el R2.
3. **¿En qué se diferencian la configuración de RIPv2 y la de RIPv6?**
Rip2 se configura como notificando las redes, y rip se configura en las interfaces.

8.2.4.5 Lab: configuración de OSPFv2 básico de área única

Topología

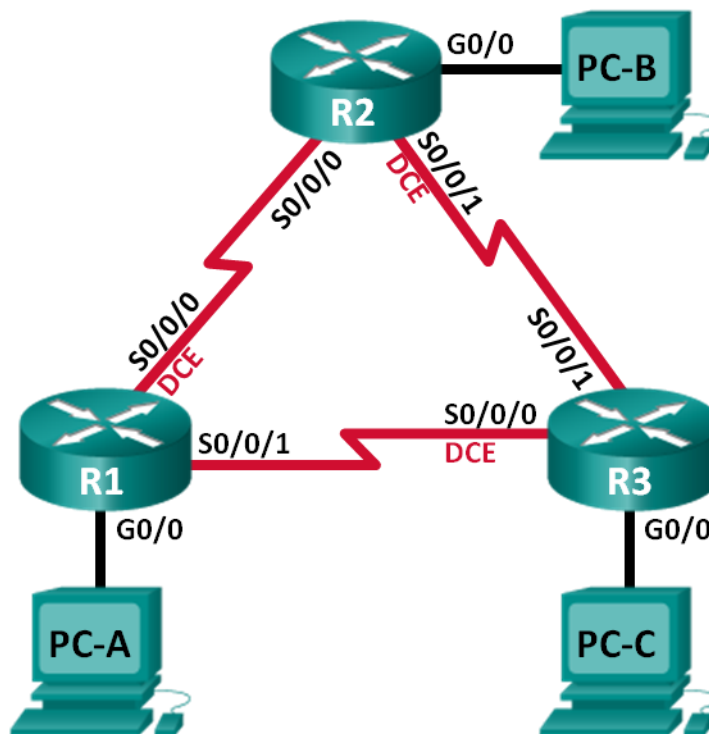


Tabla de direccionamiento

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.

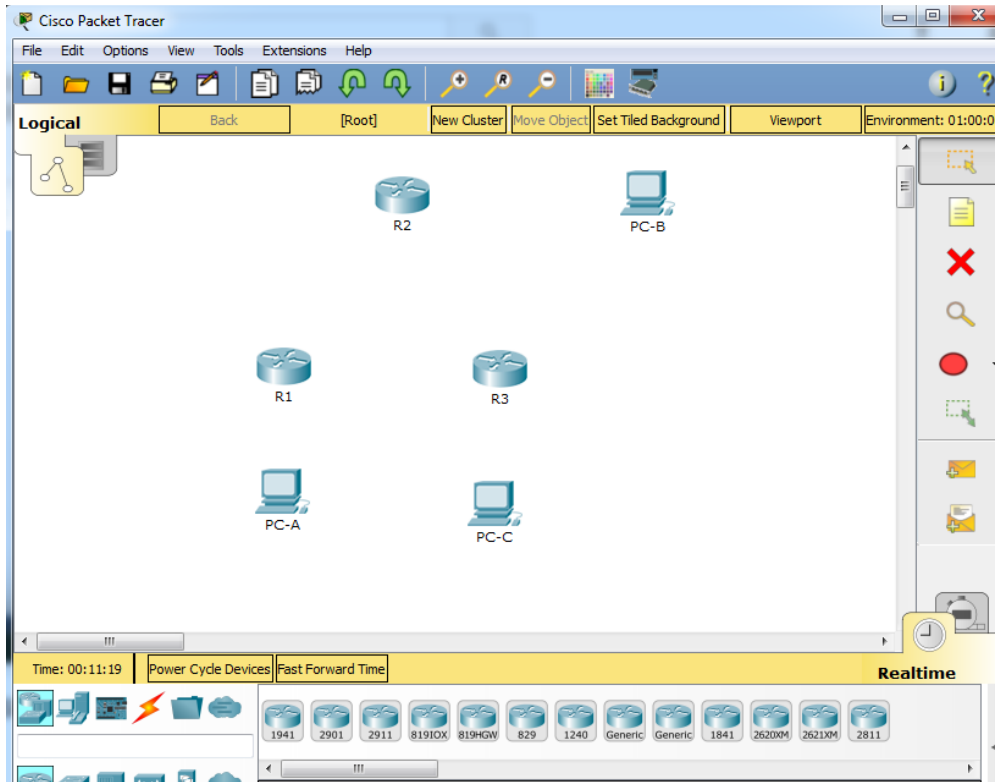
Nota: asegúrese de que los routers se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

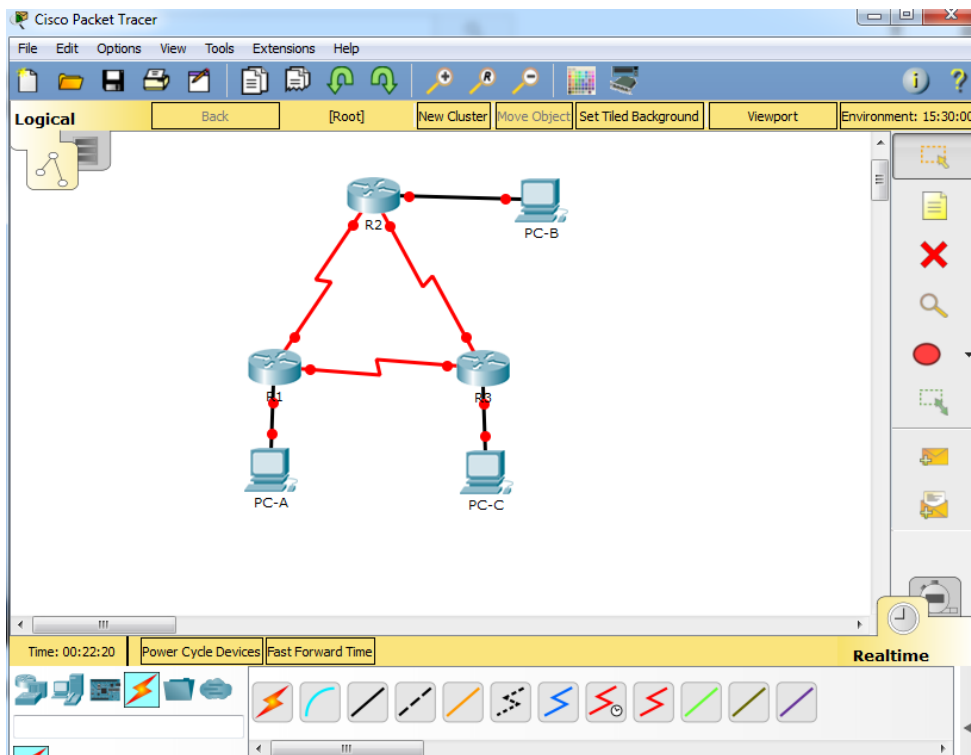
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet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

- a. Desactive la búsqueda del DNS.

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

ROUTER 1

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#loggin synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd #
Enter TEXT message. End with the character '#'.
ACCESO RESTRINGIDO POR CONTRASENA

#

R1(config)#int g0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut

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

R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ip add 192.168.12.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#exit
R1(config)#int s0/0/1
R1(config-if)#ip add 192.168.13.1 255.255.255.252
R1(config-if)#no shut

R1(config-if)#
```

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

R1(config-if)#

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

R1(config-if)#int s0/0/0

R1(config-if)#no shut

R1(config-if)#

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

R1(config-if)#

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

R1(config-if)#end

R1#

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

R1#copy run start

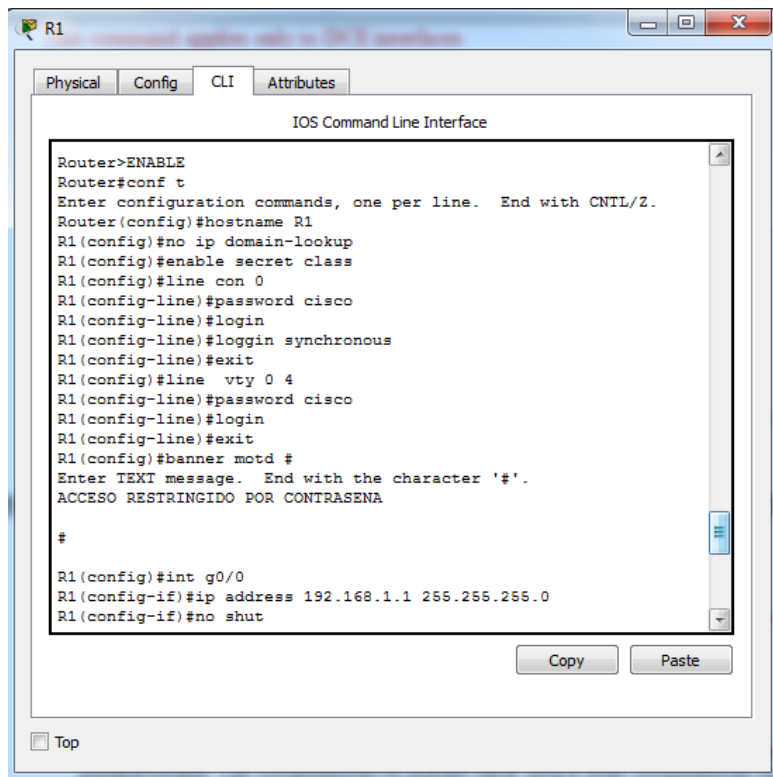
Destination filename [startup-config]?

Building configuration...

[OK]

R1#

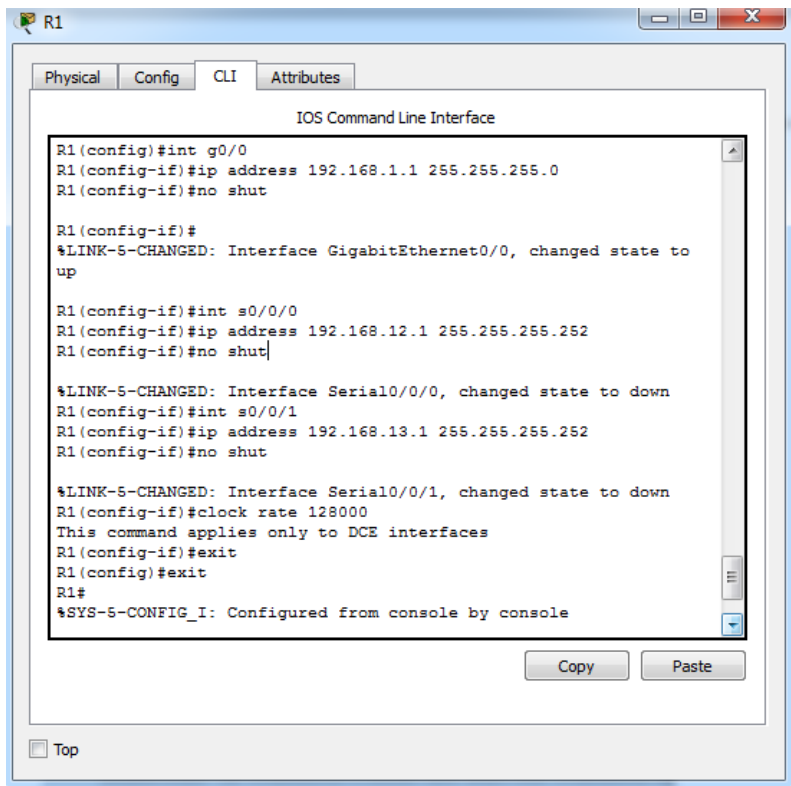
R1#



The screenshot shows a window titled 'R1' with a tabbed interface containing 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following sequence of commands and responses:

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#login synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd #
Enter TEXT message. End with the character '#'.
ACCESO RESTRINGIDO POR CONTRASENA
#
R1(config)#int g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
```

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



The screenshot shows the CLI of Router 1. The user has configured the following:

```
R1(config)#int g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

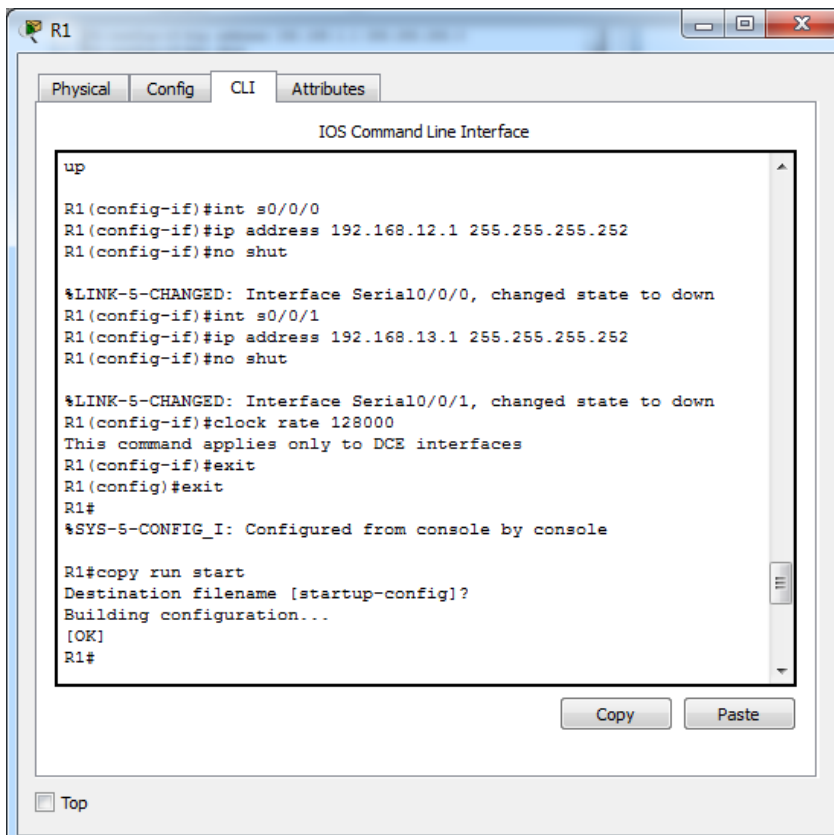
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial10/0/0, changed state to down
R1(config-if)#int s0/0/1
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial10/0/1, changed state to down
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Buttons for Copy and Paste are visible at the bottom of the terminal window.



The screenshot shows the CLI of Router 2. The user has configured the following:

```
up

R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial10/0/0, changed state to down
R1(config-if)#int s0/0/1
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial10/0/1, changed state to down
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Buttons for Copy and Paste are visible at the bottom of the terminal window.

ROUTER 2

Router>enable

Router#conf t

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

```
Router(config)#hostname R2
R2(config)#no ip domain-lookup

R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#loggin synchronous
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#banner motd #
Enter TEXT message. End with the character '#'.
ACCESO RESTRINGIDO POR CONTRASENA

#

R2(config)#
R2(config)#int g0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#no shut

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

R2(config-if)#exit
R2(config)#int s0/0/0
R2(config-if)#ip add 192.168.12.2 255.255.255.252
R2(config-if)#no shut

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

R2(config-if)#exit
R2(config)#
R2(config)#int s0/0/1
R2(config-if)#ip add 192.168.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shut

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

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

R2#

The screenshot shows the 'CLI' tab of the R2 configuration window. The terminal text is as follows:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#loggin synchronous
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#banner motd #
Enter TEXT message. End with the character '#'.
ACCESO RESTRINGIDO POR CONTRASENA
#
R2(config)#
R2(config)#int g0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
```

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

The screenshot shows the 'CLI' tab of the R2 configuration window. The terminal text is as follows:

```
ACCESO RESTRINGIDO POR CONTRASENA
#
R2(config)#
R2(config)#int g0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#no shut

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

R2(config-if)#exit
R2(config)#int s0/0/0
R2(config-if)#ip add 192.168.12.2 255.255.255.252
R2(config-if)#no shut

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

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

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


```

R2(config)#int s0/0/1
R2(config-if)#ip add 192.168.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shut

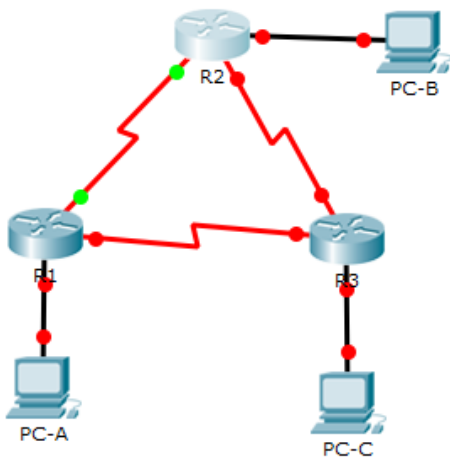
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

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

```

Copy Paste

Top



ROUTER 3

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#loggin synchronous
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#banner motd #
Enter TEXT message. End with the character '#'.
ACCESO RESTRINGIDO POR CONTRASENA

#

R3(config)#int g0/0
R3(config-if)#ip add 192.168.3.1 255.255.255.0

```

```
R3(config-if)#no shut
```

```
R3(config-if)#
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

```
R3(config-if)#exit
```

```
R3(config)#int s0/0/0
```

```
R3(config-if)#ip add 192.168.13.2 255.255.255.252
```

```
R3(config-if)#clock rate 128000
```

```
R3(config-if)#no shut
```

```
R3(config-if)#
```

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

```
R3(config-if)#exit
```

```
R3(config)#
```

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

```
R3(config)#int s0/0/1
```

```
R3(config-if)#ip add 192.168.23.2 255.255.255.252
```

```
R3(config-if)#no shut
```

```
R3(config-if)#
```

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

```
R3(config-if)#
```

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

```
R3(config-if)#end
```

```
R3#
```

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

```
R3#copy run start
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
R3#
```

```
R3#
```

R3

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#loggin synchronous
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#banner motd #
Enter TEXT message. End with the character '#'.
ACCESO RESTRINGIDO POR CONTRASENA
#
R3(config)#int g0/0
R3(config-if)#ip add 192.168.3.1 255.255.255.0
```

Copy Paste

Top

R3

Physical Config CLI Attributes

IOS Command Line Interface

```
R3(config)#int g0/0
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#no shut

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

R3(config-if)#exit
R3(config)#int s0/0/0
R3(config-if)#ip add 192.168.13.2 255.255.255.252
R3(config-if)#clock rate 128000
R3(config-if)#no shut

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

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

R3(config)#int s0/0/1
R3(config-if)#ip add 192.168.23.2 255.255.255.252
R3(config-if)#no shut
```

Copy Paste

Top

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

R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
R3#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

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

R3#
```

Copy Paste

PC-A

The screenshot shows a window titled "PC-A" with tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The "Config" tab is active, and the "IP Configuration" window is open. It contains two sections: "IP Configuration" and "IPv6 Configuration".

IP Configuration:

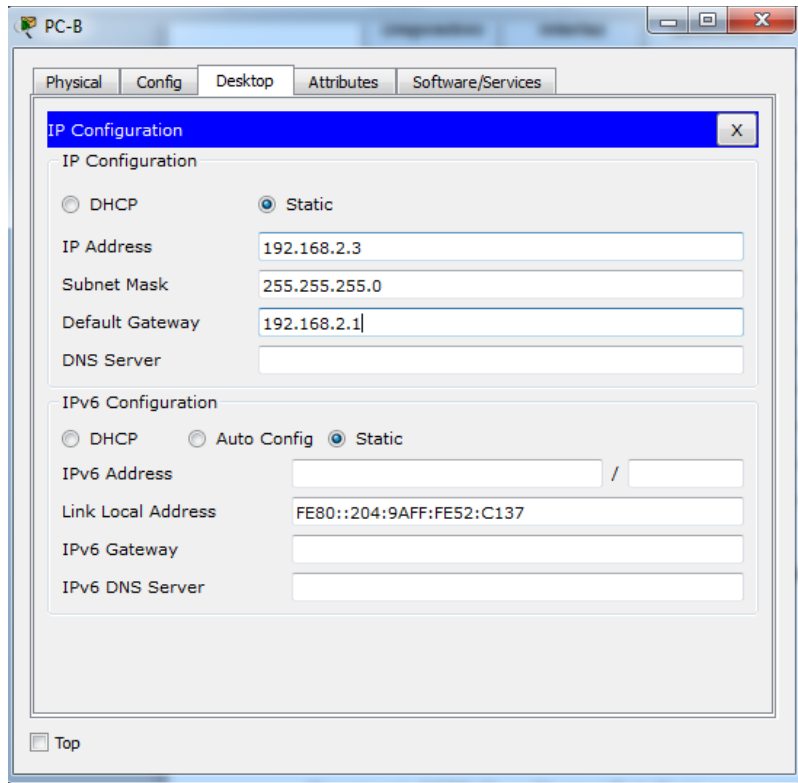
- DHCP
- Static
- IP Address: 192.168.1.3
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1
- DNS Server: (empty)

IPv6 Configuration:

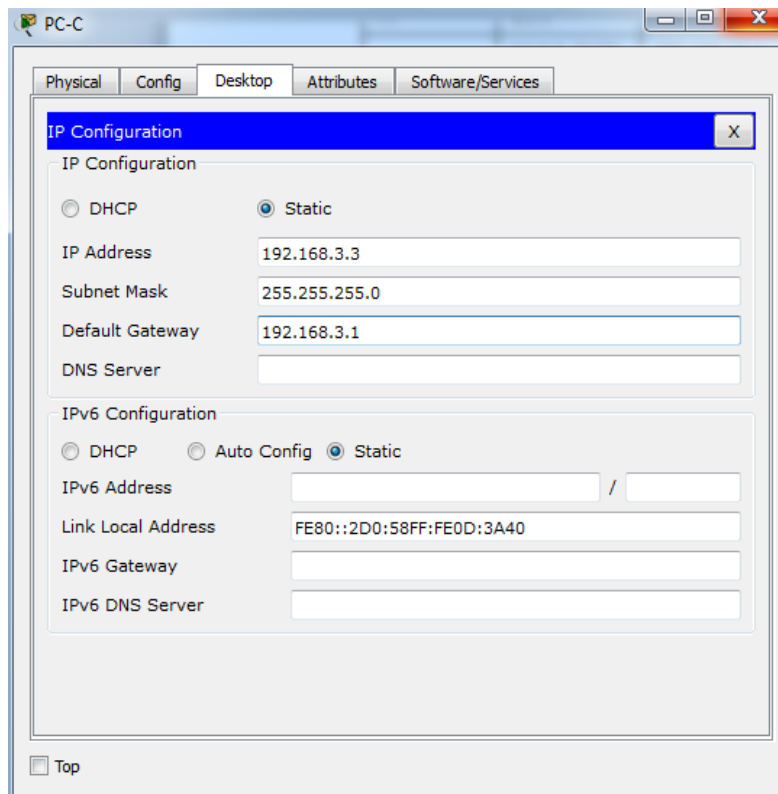
- DHCP
- Auto Config
- Static
- IPv6 Address: (empty) / (empty)
- Link Local Address: FE80::201:97FF:FE12:D353
- IPv6 Gateway: (empty)
- IPv6 DNS Server: (empty)

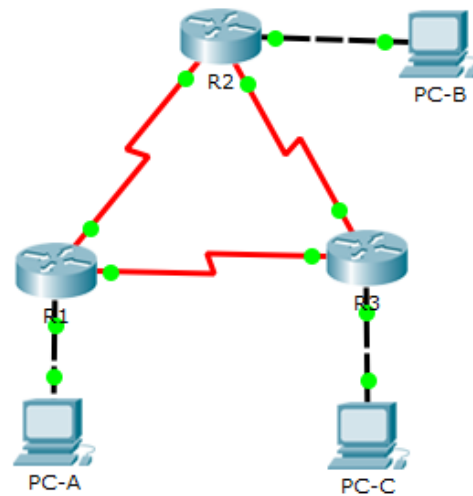
At the bottom left of the window is a "Top" button.

PC-B



PC-C





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.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#
```

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

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

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.

```

R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
R2(config-router)#network 192.168.23.0 0.0.0.3 area 0
R2(config-router)#
02:09:26: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-router)#

```

```

R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0
R3(config-router)#network 192.168.23.0 0.0.0.3 area 0
R3(config-router)#
02:14:02: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

```

R1#

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

R1#

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

R1#

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

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

R1# show ip ospf neighbor

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

```
R1>show ip ospf neighbor
```

```

Neighbor ID      Pri   State           Dead Time   Address
Interface
192.168.23.1     0    FULL/ -         00:00:38   192.168.12.2
Serial0/0/0
192.168.23.2     0    FULL/ -         00:00:35   192.168.13.2
Serial0/0/1
R1>

```

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

R1# show ip route

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

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

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

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

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

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

P - periodic downloaded static route

Gateway of last resort is not set

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

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

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

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

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

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

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

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

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

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

192.168.23.0/30 is subnetted, 1 subnets

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

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

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

Gateway of last resort is not set

  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 01:11:58, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 01:11:58, Serial0/0/1
  192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.1/32 is directly connected, Serial0/0/0
  192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/1
L    192.168.13.1/32 is directly connected, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
--More-- |
```

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

```
R1>
R1>show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 01:14:46, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 01:14:46, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0 [110/128] via 192.168.12.2, 01:19:30, Serial0/0/0
      [110/128] via 192.168.13.2, 01:19:30, Serial0/0/1
R1>
```

Paso 4: verificar la configuración del protocolo OSPF.

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

R1# show ip protocols

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 192.168.13.1

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

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Routing Information Sources:

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

Distance: (default is 110)

```
R1>show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.13.1    110          00:18:02
    192.168.23.1    110          00:17:51
    192.168.23.2    110          00:17:56
  Distance: (default is 110)

R1>
```

Paso 5: verificar la información del proceso OSPF.

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

R1# **show ip ospf**

Routing Process "ospf 1" with ID 192.168.13.1

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

Supports only single TOS(TOS0) routes

Supports opaque LSA

Supports Link-local Signaling (LLS)

Supports area transit capability

Supports NSSA (compatible with RFC 3101)

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

Router is not originating router-LSAs with maximum metric

Initial SPF schedule delay 5000 msec

Minimum hold time between two consecutive SPFs 10000 msec

Maximum wait time between two consecutive SPFs 10000 msec

Incremental-SPF disabled

Minimum LSA interval 5 secs

Minimum LSA arrival 1000 msec

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps

Area BACKBONE(0)

Number of interfaces in this area is 3
Area has no authentication
SPF algorithm last executed 00:22:53.756 ago
SPF algorithm executed 7 times
Area ranges are
Number of LSA 3. Checksum Sum 0x019A61
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```
R1>show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 10 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x01a6b2
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
--More--
```

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	

```

R1#
R1#show ip ospf interface brief
      ^
% Invalid input detected at '^' marker.

R1#show ip ospf interface

GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:00
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
 Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.12.1/30, Area 0
 Process ID 1, Router ID 192.168.13.1, 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 5
--More--

```

```

R1>show ip ospf interface brief
      ^
% Invalid input detected at '^' marker.

R1>show ip ospf interface brief
      ^
% Invalid input detected at '^' marker.

R1>show ip ospf interface

```

```

R1>show ip ospf neighbor

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.23.1	0	FULL/ -	00:00:38	192.168.12.2	Serial0/0/0
192.168.23.2	0	FULL/ -	00:00:35	192.168.13.2	Serial0/0/1

```

R1>

```

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

R1# show ip ospf interface

```

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

```

Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID Cost Disabled Shutdown Topology Name
0 64 no no Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:03
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.1
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
0 1 no no Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```
R1>show ip ospf interface
```

```
Serial0/0/0 is up, line protocol is up
Internet address is 192.168.12.1/30, Area 0
Process ID 1, Router ID 192.168.13.1, 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 5
Hello due in 00:00:08
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.1
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
Internet address is 192.168.13.1/30, Area 0
Process ID 1, Router ID 192.168.13.1, 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 5
Hello due in 00:00:04
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24, Area 0
Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

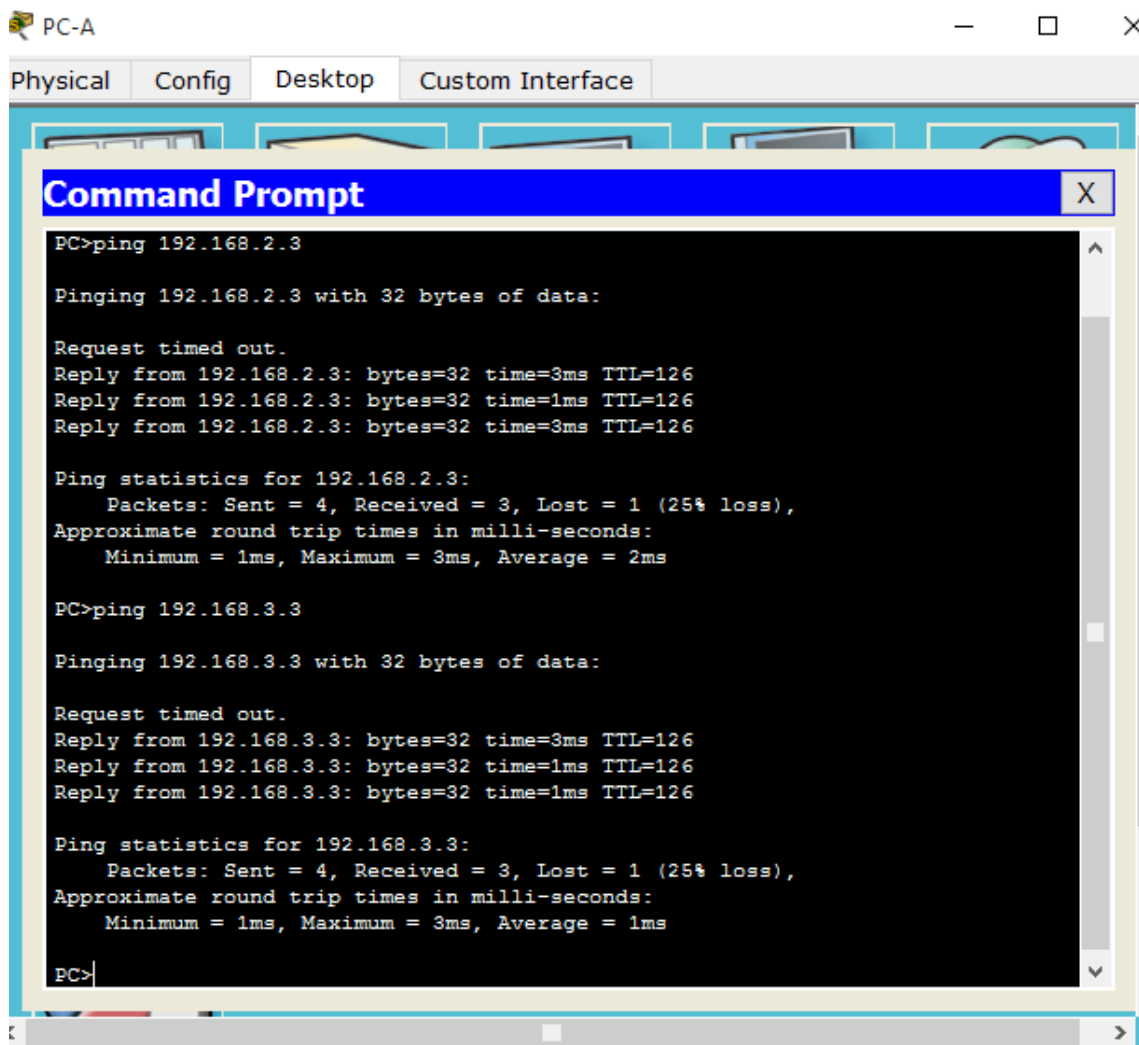
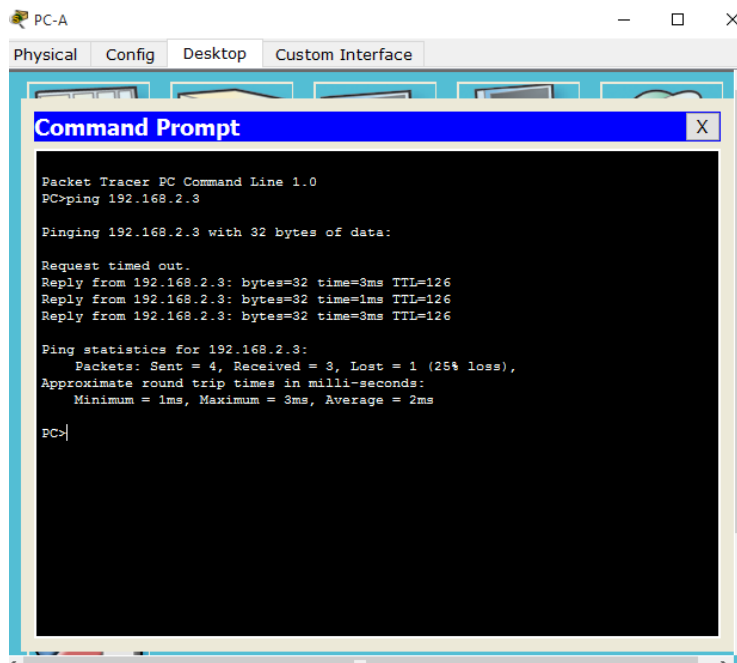
```

Hello due in 00:00:00
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.1
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
Internet address is 192.168.13.1/30, Area 0
Process ID 1, Router ID 192.168.13.1, 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 5
Hello due in 00:00:04
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24, Area 0
Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1>
R1>
```

Paso 7: Verificar la conectividad de extremo a extremo.

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

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



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(config)# interface lo0

R1(config-if)# ip address 1.1.1.1 255.255.255.255

R1(config-if)# end

```
R1(config-if)#int lo0
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

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

R2 Loopback Configuration

R2(config)#int lo0

R2(config-if)#ip add 2.2.2.2 255.255.255.255

```
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.255
^
% Invalid input detected at '^' marker.

R2(config-if)#ip add 2.2.2.2 255.255.255.255
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

R3 Loopback Configuration

R3(config)#int lo0

R3(config-if)#ip add 3.3.3.3 255.255.255.255

R3(config-if)#end

```
R3(config-if)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.255
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
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.

R1

R1#reload

Proceed with reload? [confirm]

```
R1>enable
Password:
R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

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

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
##### [OK]
Smart Init is enabled
smart init is sizing iomem

          TYPE          MEMORY_REQ          Onboard devices &
          HWIC Slot 0    0x00200000
          buffer pools   0x01E8F000
-----
          TOTAL:        0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]

          Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
```

R2

R2#reload

Proceed with reload? [confirm]


```

R2#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

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

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
##### [OK]
Smart Init is enabled
smart init is sizing iomem
      TYPE      MEMORY_REQ      Onboard devices &
      HWIC Slot 0  0x00200000
      buffer pools 0x01E8F000
-----
TOTAL:          0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive

```

R3

R3#reload

Proceed with reload? [confirm]

...

```

R3#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

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

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
##### [OK]
Smart Init is enabled
smart init is sizing iomem
      TYPE      MEMORY_REQ      Onboard devices &
      HWIC Slot 0  0x00200000
      buffer pools 0x01E8F000
-----
TOTAL:          0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph

```

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

R1# show ip protocols

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

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

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Routing Information Sources:

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

3.3.3.3	110	00:01:00
---------	-----	----------

2.2.2.2	110	00:01:14
---------	-----	----------

Distance: (default is 110)

R1#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

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

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Routing Information Sources:

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

1.1.1.1	110	00:00:18
---------	-----	----------

2.2.2.2	110	00:00:18
---------	-----	----------

3.3.3.3	110	00:00:18
---------	-----	----------

192.168.13.1	110	00:00:44
--------------	-----	----------

192.168.23.1	110	00:01:03
--------------	-----	----------

192.168.23.2	110	00:05:47
--------------	-----	----------

Distance: (default is 110)

R1#

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

R1# show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
-------------	-----	-------	-----------	---------	-----------

3.3.3.3	0	FULL/ -	00:00:35	192.168.13.2	Serial0/0/1
---------	---	---------	----------	--------------	-------------

2.2.2.2	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0
---------	---	---------	----------	--------------	-------------

R1#

R1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:39	192.168.12.2	Serial0/0/0
3.3.3.3	0	FULL/ -	00:00:39	192.168.13.2	Serial0/0/0

R1#

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

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

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

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

R1(config-router)# **router-id 11.11.11.11**

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

R1(config)# **end**

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 11.11.11.11
R1(config-router)#Reload or use "clear ip ospf process" command, for this to take
effect

R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#

```

- 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.

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

```
R2(config-router)#router-id 22.22.22.22
```

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

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

```
R2#
```

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

```
R2#
```

```

R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 22.22.22.22
R2(config-router)#Reload or use "clear ip ospf process" command, for this to take
effect

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

R2#

```

```
R3(config)#router ospf 1
```

```
R3(config-router)#router-id 33.33.33.33
```

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

```
R3(config-router)#end
```

```
R3#
```

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

R3#

```
R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 33.33.33.33
R3(config-router)#Reload or use "clear ip ospf process" command, for this to take
effect

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

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

R1# **show ip protocols**

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 11.11.11.11

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

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

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

33.33.33.33	110	00:00:19
-------------	-----	----------

22.22.22.22	110	00:00:31
-------------	-----	----------

3.3.3.3	110	00:00:41
---------	-----	----------

2.2.2.2	110	00:00:41
---------	-----	----------

Distance: (default is 110)

```

R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:08:50
    2.2.2.2          110          00:08:50
    3.3.3.3          110          00:08:50
    192.168.13.1     110          00:09:16
    192.168.23.1     110          00:09:35
    192.168.23.2     110          00:14:19
  Distance: (default is 110)

R1#

```

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

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

```

Neighbor ID  Pri  State      Dead Time  Address    Interface
33.33.33.33  0  FULL/-    00:00:36  192.168.13.2  Serial0/0/1
22.22.22.22  0  FULL/-    00:00:32  192.168.12.2  Serial0/0/0

```

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

```

Neighbor ID    Pri  State      Dead Time  Address          Interface
2.2.2.2        0  FULL/-    00:00:39  192.168.12.2    Serial0/0/0
3.3.3.3        0  FULL/-    00:00:39  192.168.13.2    Serial0/0/1
R1#

```

Parte 5: configurar las interfaces pasivas de OSPF

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

Paso 1: configurar una interfaz pasiva.

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

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

```

GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
    0      1    no       no        Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1

```

```

No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24, Area 0
Process ID 1, Router ID 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, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#

```

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

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

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

```

Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#passive-interface g0/0
R1(config-router)#

```

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

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

```

GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
0 1 no no Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)

```

Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

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

GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#
```

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

R2# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

```
2.0.0.0/32 is subnetted, 1 subnets
C    2.2.2.2 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, GigabitEthernet0/0
L    192.168.2.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.2/32 is directly connected, Serial0/0/0
192.168.13.0/30 is subnetted, 1 subnets
O    192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
      [110/128] via 192.168.12.1, 00:58:32, Serial0/0/0
192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.23.0/30 is directly connected, Serial0/0/1
L    192.168.23.1/32 is directly connected, Serial0/0/1
```

```

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

Gateway of last resort is not set

    2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.12.1, 00:14:09, Serial0/0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O       192.168.3.0/24 [110/65] via 192.168.23.2, 00:14:30, Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
    192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0/30 [110/128] via 192.168.23.2, 00:14:09, Serial0/0/1
           [110/128] via 192.168.12.1, 00:14:09, Serial0/0/0
    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.1/32 is directly connected, Serial0/0/1

```

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

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

R1# show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

R1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:38	192.168.12.2	Serial0/0/0
3.3.3.3	0	FULL/ -	00:00:38	192.168.13.2	Serial0/0/1

R1#

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

R2(config)# router ospf 1

R2(config-router)# passive-interface default

R2(config-router)#

*Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

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

```

R2 (config)#router ospf 1
R2 (config-router)#
R2 (config-router)#passive-interface default
R2 (config-router)#
00:17:19: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

00:17:19: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached

R2 (config-router)#

```


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

R1# show ip ospf neighbor

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

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

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

R2# show ip ospf interface s0/0/0

```
Serial0/0/0 is up, line protocol is up
Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID Cost Disabled Shutdown Topology Name
 0 64 no no Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
No Hellos (Passive interface)
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

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

Serial0/0/0 is up, line protocol is up
Internet address is 192.168.12.2/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
R2#
```

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

R3

Physical Config CLI

IOS Command Line Interface

```

R3>enable
Password:
R3#show ip route.
^
% Invalid input detected at '^' marker.

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

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:57:57, Serial0/0/0
       192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
O       192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:56:22, Serial0/0/0
       192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
       192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
--More--

```

Copy Paste

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

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

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

R2(config-router)#

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

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#
01:15:56: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
R2(config-router)#

```

- 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.

Show ip route

R1

R1

Physical Config CLI

IOS Command Line Interface

```

User Access Verification

Password:

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

Gateway of last resort is not set

  1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
C       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:02:16, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 01:01:52, Serial0/0/1
C       192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
C       192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
--More--

```

Copy Paste

R2

R2

Physical Config CLI

IOS Command Line Interface

```

* Invalid input detected at '^' marker.

R2#Show ip router
^
* Invalid input detected at '^' marker.

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

Gateway of last resort is not set

  2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.12.1, 00:03:32, Serial0/0/0
C       192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O       192.168.3.0/24 [110/129] via 192.168.12.1, 00:03:32, Serial0/0/0
C       192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
C       192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0/30 [110/128] via 192.168.12.1, 00:03:32, Serial0/0/0
--More--

```

Copy Paste

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? **Serial0/0/0**

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

¿El R2 aparece como vecino OSPF en el R1? **si**

¿El R2 aparece como vecino OSPF en el R3? **no**

¿Qué indica esta información?

Que el router 2 tiene la interfaz pasiva

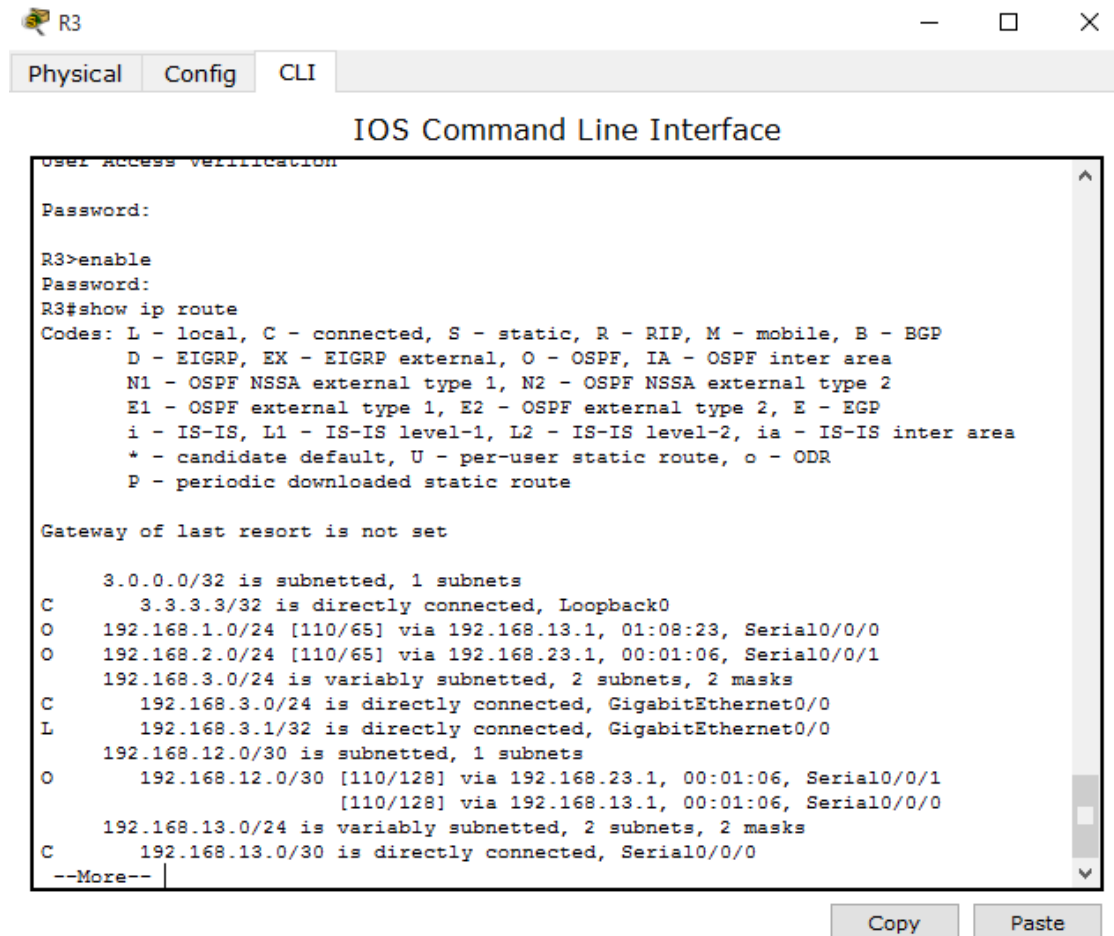
- h. Cambie la interfaz S0/0/1 en el R2 para permitir que anuncie las rutas OSPF. Registre los comandos utilizados a continuación.

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

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

```
R2(config)#
```

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



```

R3
Physical Config CLI
IOS Command Line Interface

User Access Verification

Password:

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

Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 01:08:23, Serial0/0/0
O       192.168.2.0/24 [110/65] via 192.168.23.1, 00:01:06, Serial0/0/1
       192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
       192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:01:06, Serial0/0/1
           [110/128] via 192.168.13.1, 00:01:06, Serial0/0/0
       192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
--More--
Copy Paste
```

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? **Serial0/0/1**

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

65

(One T1 (1.544 Mb/s) serial link (at a cost of 64) plus the R2 Gigabit 0/0 LAN link (at a cost of 1).

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

Parte 6: cambiar las métricas de OSPF

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

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

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

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

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

R1# show interface g0/0

```
GigabitEthernet0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full Duplex, 100Mbps, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:17:31, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  279 packets output, 89865 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  1 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out
```

IOS Command Line Interface

```

R1#show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0001.64be.7c01 (bia 0001.64be.7c01)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 1017 multicast, 0 pause input
    0 input packets with dribble condition detected
    74 packets output, 4736 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
R1#

```

Copy

Paste

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

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

R1# show ip route ospf

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

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

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

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

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

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

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
 [110/128] via 192.168.12.2, 00:01:08, Serial0/0/0

```

R1#
R1#
R1#show ip route ospf
O   192.168.2.0 [110/65] via 192.168.12.2, 00:12:55, Serial0/0/0
O   192.168.3.0 [110/65] via 192.168.13.2, 01:12:31, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O     192.168.23.0 [110/128] via 192.168.12.2, 00:12:55, Serial0/0/0
    [110/128] via 192.168.13.2, 00:12:55, Serial0/0/1
R1#

```

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

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

R3# show ip ospf interface g0/0

```

GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
  0      1    no    no      Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

```

R3#
R3#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)

```

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

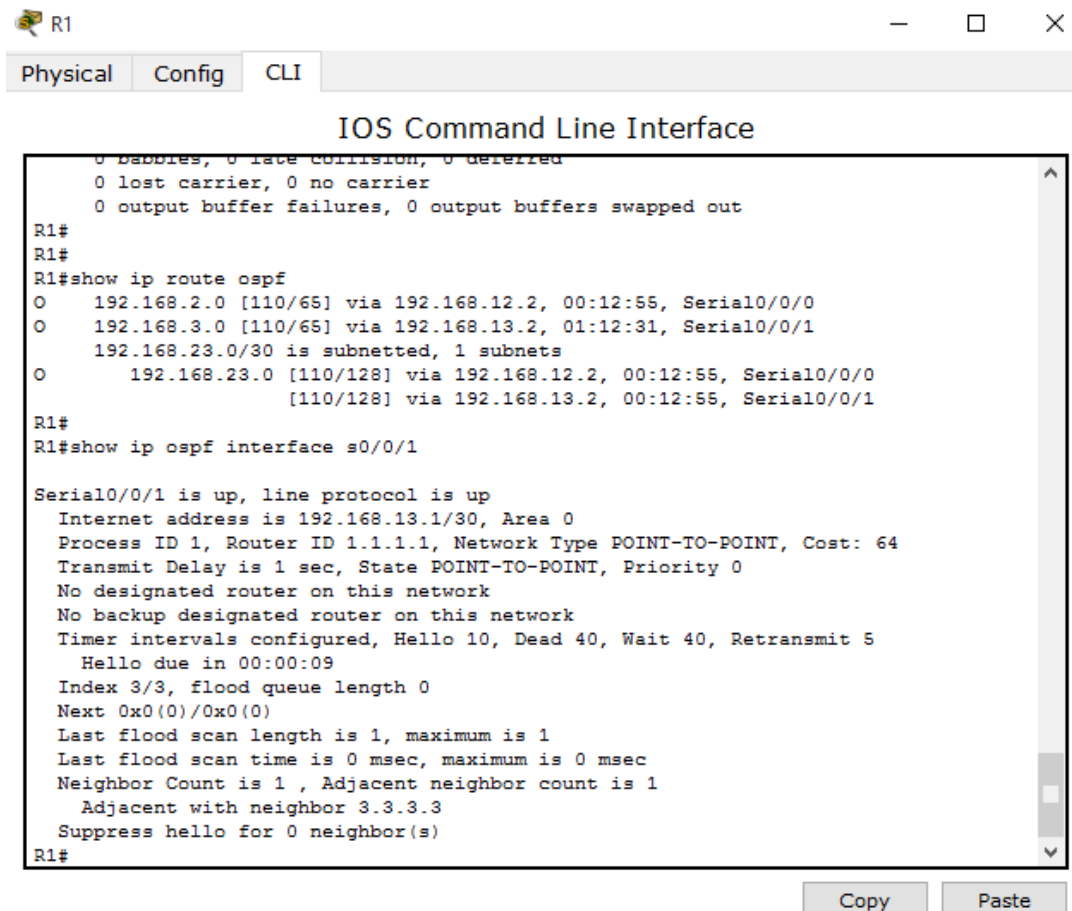
R1# show ip ospf interface s0/0/1

```

Serial0/0/1 is up, line protocol is up
Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID Cost Disabled Shutdown Topology Name
  0      64    no    no      Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40

```

Hello due in 00:00:04
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)



```
R1#  
R1#  
R1#show ip route ospf  
O   192.168.2.0 [110/65] via 192.168.12.2, 00:12:55, Serial0/0/0  
O   192.168.3.0 [110/65] via 192.168.13.2, 01:12:31, Serial0/0/1  
   192.168.23.0/30 is subnetted, 1 subnets  
O     192.168.23.0 [110/128] via 192.168.12.2, 00:12:55, Serial0/0/0  
      [110/128] via 192.168.13.2, 00:12:55, Serial0/0/1  
R1#  
R1#show ip ospf interface s0/0/1  
  
Serial0/0/1 is up, line protocol is up  
  Internet address is 192.168.13.1/30, Area 0  
  Process ID 1, Router ID 1.1.1.1, 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 5  
    Hello due in 00:00:09  
  Index 3/3, flood queue length 0  
  Next 0x0(0)/0x0(0)  
  Last flood scan length is 1, maximum is 1  
  Last flood scan time is 0 msec, maximum is 0 msec  
  Neighbor Count is 1 , Adjacent neighbor count is 1  
    Adjacent with neighbor 3.3.3.3  
  Suppress hello for 0 neighbor(s)  
R1#
```

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


```

Neighbor Count is 0, Adjacent Neighbor Count is 0
Suppress hello for 0 neighbor(s)
R3#
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

 3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 01:15:53, Serial0/0/0
O       192.168.2.0/24 [110/65] via 192.168.23.1, 00:08:37, Serial0/0/1
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:08:37, Serial0/0/1
        [110/128] via 192.168.13.1, 00:08:37, Serial0/0/0
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
--More--

```

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

R1(config)# router ospf 1

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

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/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)#

```

R2(config)#router ospf 1

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)#

R2#

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

```
R2(config)#router ospf 1|
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)#
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

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)#

```
-----
R3#conf t
Enter configuration commands, one per line.  End with CNTL/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)#
```

- f. Emita el comando **auto-cost reference-bandwidth 10000** en los routers R2 y R3.
- g. Vuelva a emitir el comando **show ip ospf interface** para ver el nuevo costo de G0/0 en el R3 y de S0/0/1 en el R1.

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

```
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
Topology-MTID  Cost  Disabled  Shutdown  Topology Name
    0    10    no    no    Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 oob-resync timeout 40
 Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

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

GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.3.1/24, Area 0
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 100
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 3.3.3.3, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:04
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R3#
```

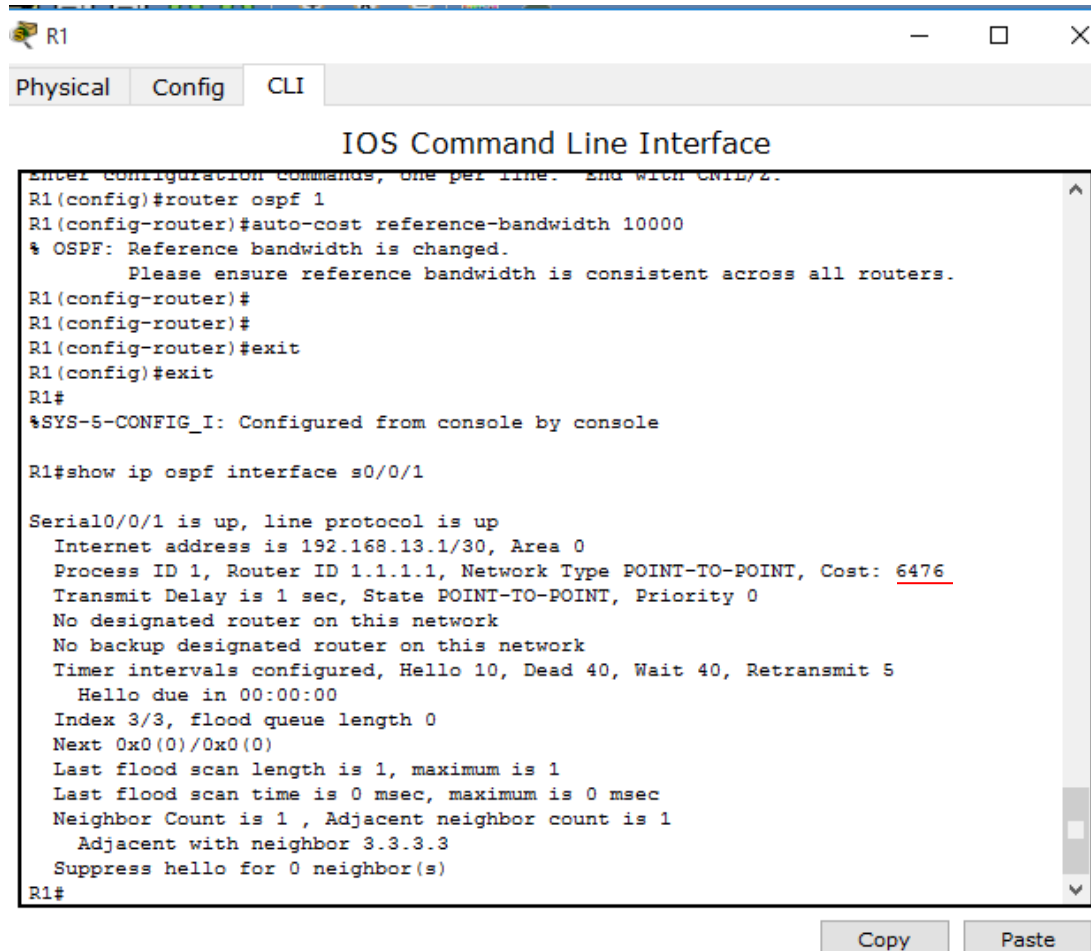
Copy

Paste

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

R1# show ip ospf interface s0/0/1

```
Serial0/0/1 is up, line protocol is up
Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 6476
Topology-MTID Cost Disabled Shutdown Topology Name
  0 6476 no no Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)
```



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

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

R1# show ip route ospf

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

```
O 192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
O 192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
[110/12952] via 192.168.12.2, 00:05:17, Serial0/0/
```

```
R1#show ip route ospf
O 192.168.2.0 [110/6576] via 192.168.12.2, 00:06:58, Serial0/0/0
O 192.168.3.0 [110/6576] via 192.168.13.2, 00:05:29, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/12952] via 192.168.12.2, 00:05:29, Serial0/0/0
[110/12952] via 192.168.13.2, 00:05:29, Serial0/0/1
R1#
```

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

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

R1(config)# router ospf 1

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

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

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

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

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

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

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

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

Para obtener un cálculo de costes más precisa para estos enlaces más rápidos

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

En la mayoría de los enlaces seriales, la métrica del ancho de banda será 1544 Kbits de manera predeterminada (la de un T1). Si esta no es la velocidad real del enlace serial, se deberá cambiar la configuración del ancho de banda para que coincida con la velocidad real, a fin de permitir que el costo de la ruta se calcule correctamente en OSPF. Use el comando **bandwidth** para ajusta la configuración del ancho de banda de una interfaz.

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

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

R1# show interface s0/0/0

```
Serial0/0/0 is up, line protocol is up
Hardware is WIC MBRD Serial
Internet address is 192.168.12.1/30
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
<Output Omitted>
```

```
R1#
R1#show interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations  0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 57 bits/sec, 0 packets/sec
  5 minute output rate 59 bits/sec, 0 packets/sec
    330 packets input, 23812 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
    672 packets output, 44988 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
--More--
```

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

R1# show ip route ospf

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
       + - replicated route, % - next hop override
```

Gateway of last resort is not set

- ```
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1
 [110/128] via 192.168.12.2, 00:00:42, Serial0/0/0
```

```

R1#show ip route ospf
O 192.168.2.0 [110/164] via 192.168.12.2, 00:02:52, Serial0/0/0
O 192.168.3.0 [110/164] via 192.168.13.2, 00:02:52, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/6540] via 192.168.12.2, 00:02:52, Serial0/0/0
 [110/6540] via 192.168.13.2, 00:02:52, Serial0/0/1

```

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

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

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

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

R1(config)#interface s0/0/0

R1(config-if)#bandwidth 128

R1(config-if)#|

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

**R1# show ip route ospf**

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

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

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

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

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

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

192.168.23.0/30 is subnetted, 1 subnets

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

```

R1#show ip route ospf
O 192.168.2.0 [110/881] via 192.168.12.2, 00:00:42, Serial0/0/0
O 192.168.3.0 [110/164] via 192.168.13.2, 00:04:33, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/6540] via 192.168.13.2, 00:00:42, 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.

**R1# show ip ospf interface brief**

| Interface | PID | Area | IP Address/Mask | Cost | State | Nbrs | F/C |
|-----------|-----|------|-----------------|------|-------|------|-----|
| Se0/0/1   | 1   | 0    | 192.168.13.1/30 | 64   | P2P   | 1/1  |     |
| Se0/0/0   | 1   | 0    | 192.168.12.1/30 | 781  | P2P   | 1/1  |     |
| Gi0/0     | 1   | 0    | 192.168.1.1/24  | 1    | DR    | 0/0  |     |

```

R1#show ip ospf interface

GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State WAITING, Priority 1
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 No Hellos (Passive interface)
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.12.1/30, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 781
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:04
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 2.2.2.2
 Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
 Internet address is 192.168.13.1/30, Area 0
 Process ID 1, Router ID 1.1.1.1, 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 5
 Hello due in 00:00:05
 Index 3/3, flood queue length 0
 Next 0x0(0)/0x0(0)

```

- 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.

### R1# show ip route ospf

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

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2  
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
 ia - IS-IS inter area, \* - candidate default, U - per-user static route  
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP  
 + - replicated route, % - next hop override

Gateway of last resort is not set

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

192.168.23.0/30 is subnetted, 1 subnets

- O 192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1  
[110/845] via 192.168.12.2, 00:00:09, Serial0/0/0

```
R1#show ip route ospf
O 192.168.2.0 [110/881] via 192.168.12.2, 00:03:51, Serial0/0/0
O 192.168.3.0 [110/164] via 192.168.13.2, 00:07:42, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/6540] via 192.168.13.2, 00:03:51, Serial0/0/1
R1#
```

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.

El costo para 192.168.3.0/24: R1 S0 / 0/1 + R3 G0 / 0 (781 + 1 = 782). El costo para

192.168.23.0/30: R1 S0 / 0/1 y R3 S0 / 0/1 (781 + 64 = 845).

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

**R3# show ip route ospf**

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

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

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

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

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

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

192.168.12.0/30 is subnetted, 1 subnets

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

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

```
R3#show ip route ospf
O 192.168.1.0 [110/6477] via 192.168.13.1, 00:12:36, Serial0/0/0
O 192.168.2.0 [110/6576] via 192.168.23.1, 00:20:30, Serial0/0/1
 192.168.12.0/30 is subnetted, 1 subnets
O 192.168.12.0 [110/12952] via 192.168.23.1, 00:12:26, Serial0/0/1
R3#
```

- 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?

1562. Cada enlace serie ahora tiene un costo de 781, y la ruta a la red 192.168.23.0/24

viaja sobre dos enlaces seriales.  $781 + 781 = 1.562$ .

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

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

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

**R1# show ip route ospf**

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

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

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



E1 - OSPF external type 1, E2 - OSPF external type 2  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP  
+ - replicated route, % - next hop override

```
R1>enable
Password:
R1#show ip route ospf
O 192.168.2.0 [110/881] via 192.168.12.2, 00:15:13, Serial0/0/0
O 192.168.3.0 [110/164] via 192.168.13.2, 00:19:04, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/6540] via 192.168.13.2, 00:15:13, Serial0/0/1
R1#
```

Gateway of last resort is not set

```
O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
 [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0
```

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

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

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

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

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

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

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

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

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

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

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

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

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

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

```
O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
O 192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0
```

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/1
R1(config-if)#ip ospf cost 1565
R1(config-if)#
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip route ospf
O 192.168.2.0 [110/881] via 192.168.12.2, 00:19:06, Serial0/0/0
O 192.168.3.0 [110/1665] via 192.168.13.2, 00:01:27, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/7257] via 192.168.12.2, 00:01:27, Serial0/0/0
R1#

```

**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.

Podríamos decir que es porque OSPF elegirá la ruta con el menor costo acumulado.

## Reflexión

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

Asignaciones de ID Router controlan el router designado (DR) y BDR (BDR) elección /proceso en una red de acceso múltiple

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

El proceso de elección DR / BDR es sólo un problema en una red multiacceso como Ethernet o Frame Relay

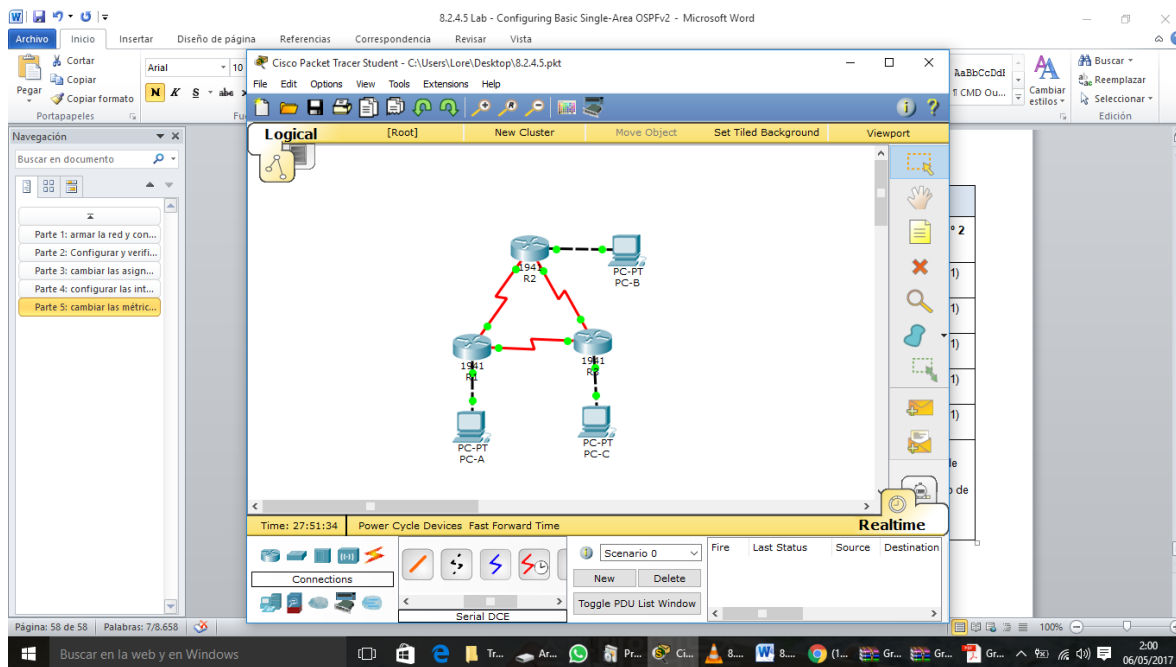
3. ¿Por qué querría configurar una interfaz OSPF como pasiva?

Elimina innecesaria información de enrutamiento OSPF en esa interfaz, liberando ancho de banda

## 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.

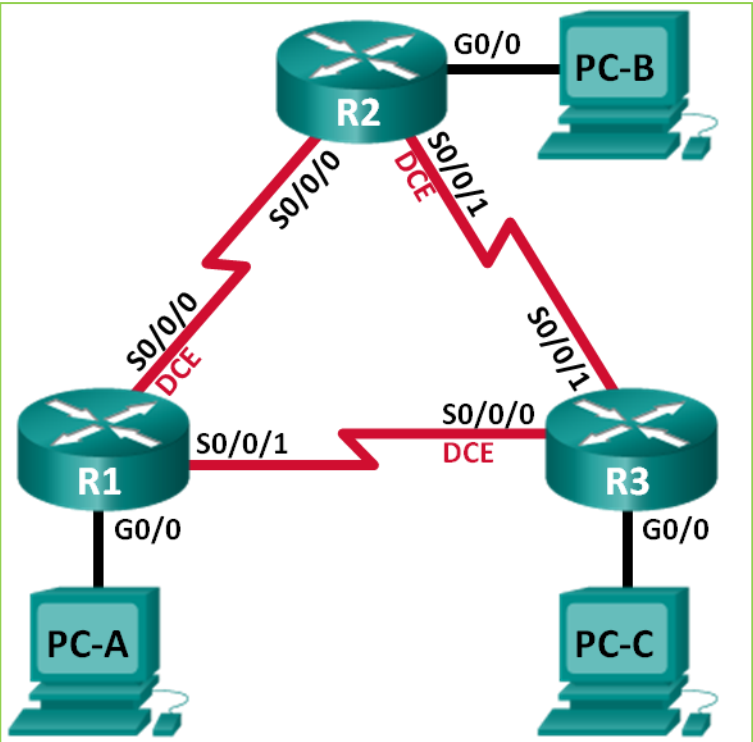


### Nota

Quizás se vea un poco cambiada la plataforma, es que empecé a realizar el ejercicio en el Packet Tracer versión 7, pero tuve un inconveniente y me tocó terminarlo en la versión 6

### 8.3.3.6 Lab: configuración de OSPFv3 básico de área única.

Topología



## Tabla de direccionamiento

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

## Objetivos

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

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

**Parte 3: configurar interfaces pasivas OSPFv3**

## Información básica/situación

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

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

**Nota:** los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones

del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

## Recursos necesarios

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

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

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

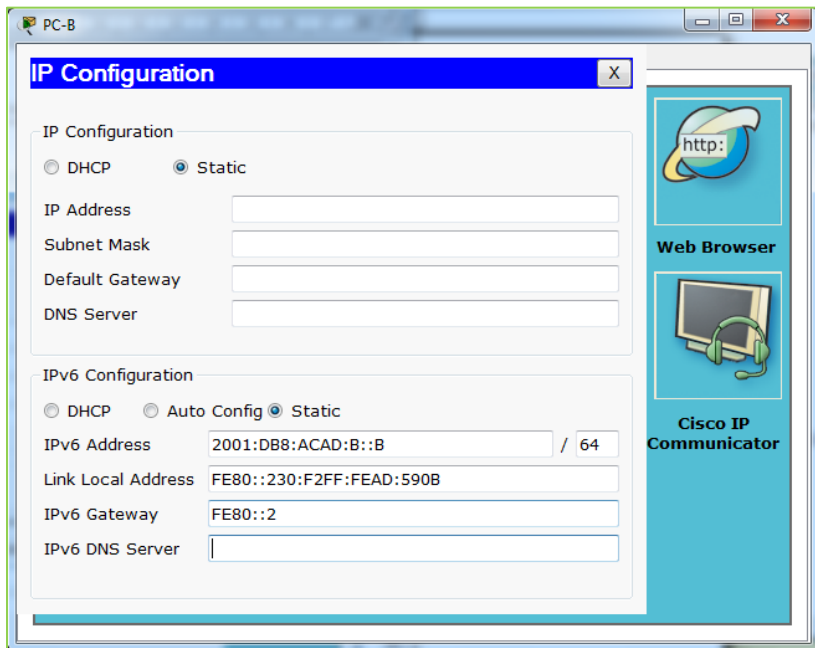
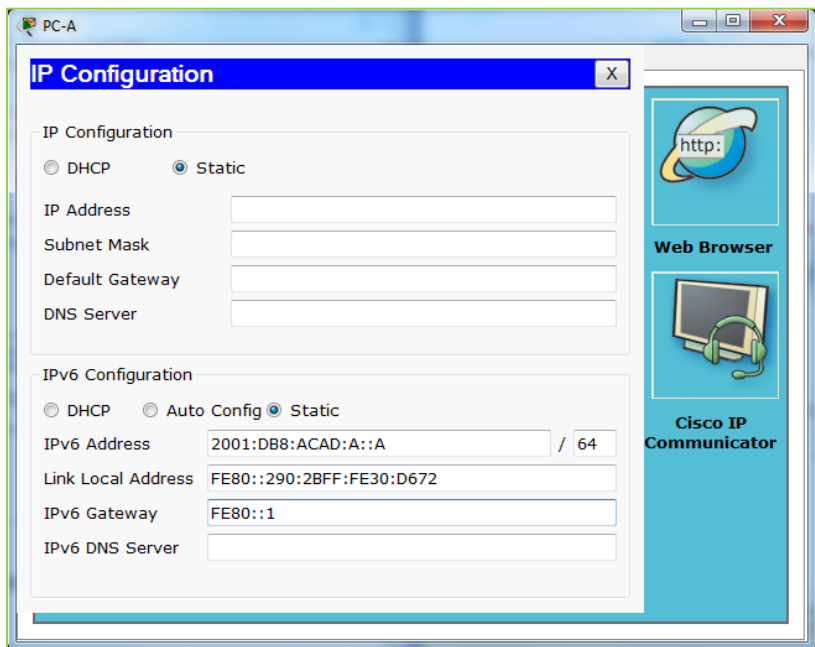
**Paso 1: realizar el cableado de red tal como se muestra en la topología.**

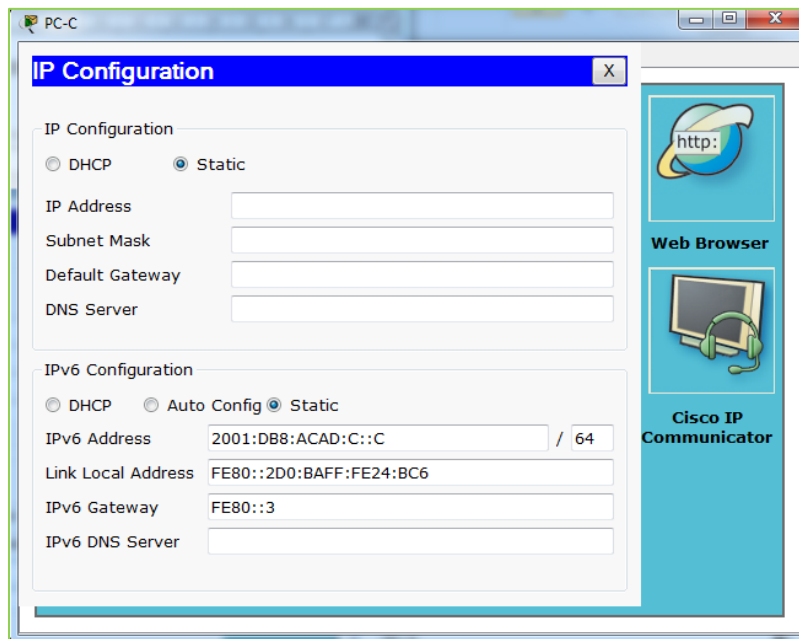
**Paso 2: inicializar y volver a cargar los routers según sea necesario.**

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

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

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





### Paso 5: Probar la conectividad.

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

## Parte 2: configurar el routing OSPFv3

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

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

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

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

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

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

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

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

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

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

- Inicie el proceso de routing de OSPFv3 y asigne la ID de router **2.2.2.2** al R2 y la ID de router **3.3.3.3** al R3.



```
R2(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
R2(config-rtr)#router-id 2.2.2.2
```

```
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
R3(config-rtr)#router-id 3.3.3.3
```

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

R2# **show ipv6 ospf**

Routing Process "ospfv3 1" with ID 2.2.2.2

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

Router is not originating router-LSAs with maximum metric

<Output Omitted>

```
R2#show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
 Area BACKBONE(0)
 Number of interfaces in this area is 3
 SPF algorithm executed 3 times
 Number of LSA 2. Checksum Sum 0x0123a5
 Number of DCbitless LSA 0
 Number of indication LSA 0
 Number of DoNotAge LSA 0
 Flood list length 0

R2#
```

R2#show ipv6 ospf

Routing Process "ospfv3 1" with ID 2.2.2.2

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msec

Retransmission pacing timer 66 msec

Number of external LSA 0. Checksum Sum 0x000000

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

Reference bandwidth unit is 100 mbps

Area BACKBONE(0)

Number of interfaces in this area is 3

SPF algorithm executed 3 times

Number of LSA 2. Checksum Sum 0x0123a5

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

R2#

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

R1#
```

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

R1#

```
R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps

R3#
```

```
R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
```

R3#

## Paso 2: configurar OSPFv6 en el R1.

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

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

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

```
R2(config)#int g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#int s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
```

```
R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
```

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

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

R1#

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

R1#

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

```
R2(config)#interface g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
```

```
R1(config)#interface g0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 ospf 1 area 0
01:04:09: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING t
o FULL, Loading Done
R1(config-if)#ipv6 ospf 1 area 0
```

```

R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
01:04:59: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING t
o FULL, Loading Done

01:05:04: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING t
o FULL, Loading Done

R3(config-if)#

```

### Paso 3: verificar vecinos de OSPFv3.

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

R1# **show ipv6 ospf neighbor**

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

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

```

R1#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
2.2.2.2 0 FULL/ - 00:00:31 3 Serial0/0/0
3.3.3.3 0 FULL/ - 00:00:36 3 Serial0/0/1
R1#
R1#

```

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

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

R1# **show ipv6 protocols**

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "ospf 1"

Router ID 1.1.1.1

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

Interfaces (Area 0):

Serial0/0/1

Serial0/0/0

GigabitEthernet0/0

Redistribution:

None

```

R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "ospf 1"
 Interfaces (Area 0)
 GigabitEthernet0/0
 Serial0/0/0
 Serial0/0/1
R1#

```

## Paso 5: verificar las interfaces OSPFv3.

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

R1# **show ipv6 ospf interface**

```
Serial0/0/1 is up, line protocol is up
 Link Local Address FE80::1, Interface ID 7
 Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
 Network Type POINT_TO_POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT_TO_POINT
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:05
 Graceful restart helper support enabled
 Index 1/3/3, flood queue length 0
 Next 0x0(0)/0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 3.3.3.3
 Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
 Link Local Address FE80::1, Interface ID 6
 Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
 Network Type POINT_TO_POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT_TO_POINT
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:00
 Graceful restart helper support enabled
 Index 1/2/2, flood queue length 0
 Next 0x0(0)/0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 2
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 2.2.2.2
 Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
 Link Local Address FE80::1, Interface ID 3
 Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
 Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 1.1.1.1, local address FE80::1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:03
 Graceful restart helper support enabled
 Index 1/1/1, flood queue length 0
 Next 0x0(0)/0x0(0)/0x0(0)
 Last flood scan length is 0, maximum is 0
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
```

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

R1# **show ipv6 ospf interface brief**

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

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

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

R2# **show ipv6 route**

IPv6 Routing Table - default - 10 entries

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

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

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

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

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

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

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

via FE80::1, Serial0/0/0

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

via GigabitEthernet0/0, directly connected

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

via GigabitEthernet0/0, receive

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

via FE80::3, Serial0/0/1

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

via Serial0/0/0, directly connected

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

via Serial0/0/0, receive

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

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

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

via Serial0/0/1, directly connected

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

via Serial0/0/1, receive

L FF00::8 [0/0]

via Null0, receive

```

R2#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:B::/64 [0/0]
 via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:B::2/128 [0/0]
 via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:C::/64 [110/65]
 via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
 via ::, Serial0/0/0
L 2001:DB8:ACAD:12::2/128 [0/0]
 via ::, Serial0/0/0
O 2001:DB8:ACAD:13::/64 [110/128]
 via FE80::1, Serial0/0/0
 via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:23::/64 [0/0]
 via ::, Serial0/0/1
L 2001:DB8:ACAD:23::2/128 [0/0]
 via ::, Serial0/0/1
L FF00::/8 [0/0]
 via ::, Null0
R2#

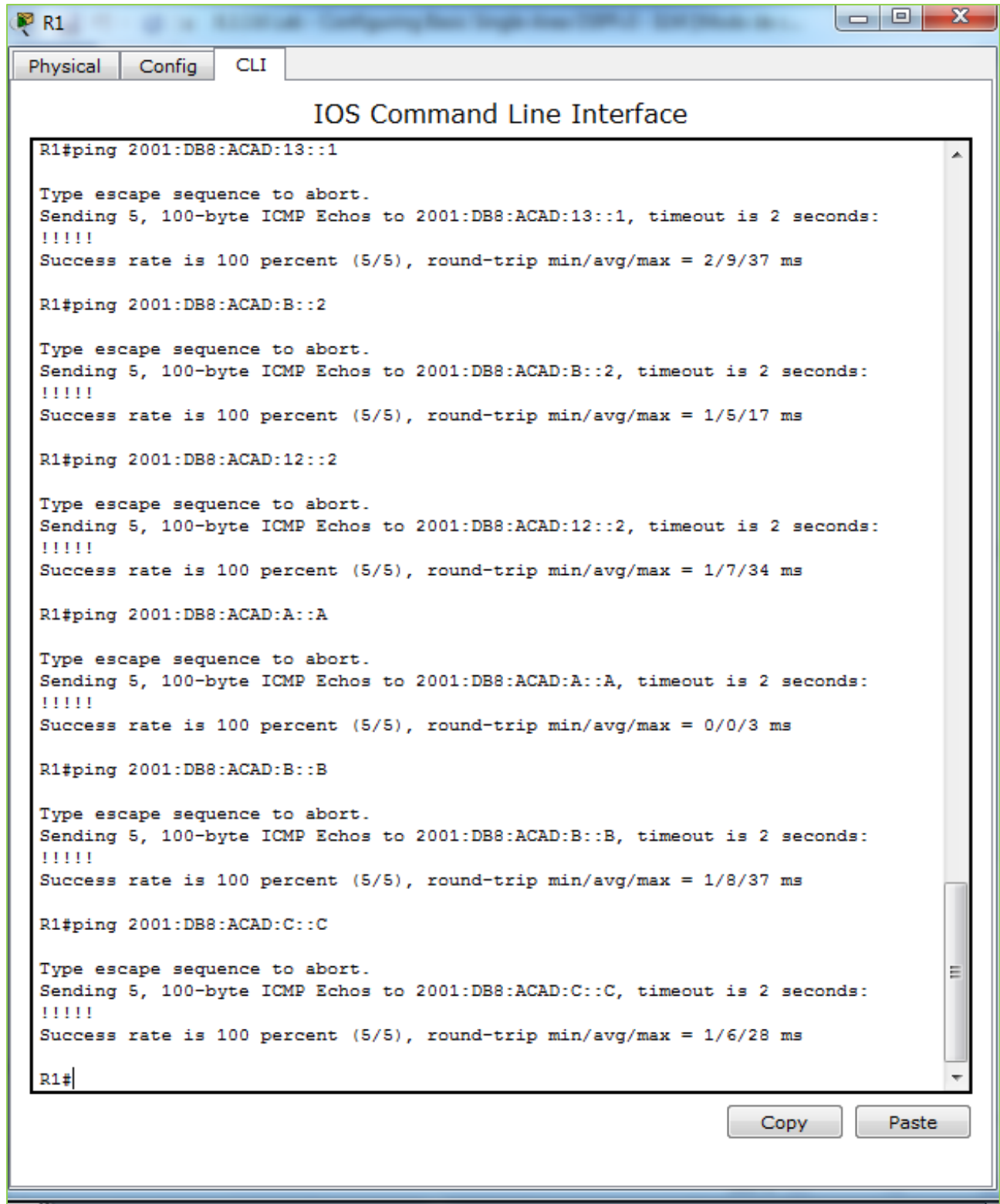
```

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

- `show ipv6 route ospf`

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

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



```
R1#ping 2001:DB8:ACAD:13::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/37 ms

R1#ping 2001:DB8:ACAD:B::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:B::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/17 ms

R1#ping 2001:DB8:ACAD:12::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/34 ms

R1#ping 2001:DB8:ACAD:A::A
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:A::A, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

R1#ping 2001:DB8:ACAD:B::B
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:B::B, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/37 ms

R1#ping 2001:DB8:ACAD:C::C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:C::C, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/28 ms

R1#
```

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

## Parte 3: configurar las interfaces pasivas de OSPFv3

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



una única interfaz como pasiva. También configurará OSPFv3 para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

### Paso 1: configurar una interfaz pasiva.

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

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

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

```
R1#
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1 , Interface ID 1
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#
```

- 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(config)#ipv6 router ospf 1
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#
```

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

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

```
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
```

No designated router on this network  
No backup designated router on this network  
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
**No Hellos (Passive interface)**  
Wait time before Designated router selection 00:00:34  
Graceful restart helper support enabled  
Index 1/1/1, flood queue length 0  
Next 0x0(0)/0x0(0)/0x0(0)  
Last flood scan length is 0, maximum is 0  
Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 0, Adjacent neighbor count is 0  
Suppress hello for 0 neighbor(s)

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

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

**R2# show ipv6 route ospf**

IPv6 Routing Table - default - 10 entries

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

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

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

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

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

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

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

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

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

via FE80::3, Serial0/0/1

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

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

```

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

```

```

R3#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:B::/64 [110/65]
 via FE80::2, Serial0/0/1
O 2001:DB8:ACAD:12::/64 [110/128]
 via FE80::2, Serial0/0/1
 via FE80::1, Serial0/0/0
R3#

```

```

R3#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:B::/64 [110/65]
 via FE80::2, Serial0/0/1
O 2001:DB8:ACAD:12::/64 [110/128]
 via FE80::2, Serial0/0/1
 via FE80::1, Serial0/0/0
R3#

```

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

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

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

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

```

R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
01:24:28: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to D
OWN, Neighbor Down: Interface down or detached

01:24:28: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to D
OWN, Neighbor Down: Interface down or detached

R2(config-rtr)#

```

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

R1# **show ipv6 ospf neighbor**

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

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

```
R1#show ipv6 ospf neighbor
```

| Neighbor ID | Pri | State   | Dead Time | Interface ID | Interface   |
|-------------|-----|---------|-----------|--------------|-------------|
| 3.3.3.3     | 0   | FULL/ - | 00:00:31  | 3            | Serial0/0/1 |

R1#

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

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

```

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

```

```

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

```

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

```

R1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
- OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:A::1/128 [0/0]
via ::, GigabitEthernet0/0
2001:DB8:ACAD:C::/64 [110/65]
via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
via ::, Serial0/0/0
L 2001:DB8:ACAD:12::1/128 [0/0]
via ::, Serial0/0/0
C 2001:DB8:ACAD:13::/64 [0/0]
via ::, Serial0/0/1
L 2001:DB8:ACAD:13::1/128 [0/0]
via ::, Serial0/0/1
2001:DB8:ACAD:23::/64 [110/128]
via FE80::3, Serial0/0/1
L FF00::/8 [0/0]
via ::, Null0
R1#

```

```

R1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:A::1/128 [0/0]
via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:C::/64 [110/65]
via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
via ::, Serial0/0/0
L 2001:DB8:ACAD:12::1/128 [0/0]
via ::, Serial0/0/0
C 2001:DB8:ACAD:13::/64 [0/0]
via ::, Serial0/0/1
L 2001:DB8:ACAD:13::1/128 [0/0]
via ::, Serial0/0/1
O 2001:DB8:ACAD:23::/64 [110/128]
via FE80::3, Serial0/0/1
L FF00::/8 [0/0]
via ::, Null0
R1#

```

```

R3#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```

```

 D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:C::/64 [0/0]
 via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:C::3/128 [0/0]
 via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:12::/64 [110/128]
 via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:13::/64 [0/0]
 via ::, Serial0/0/0
L 2001:DB8:ACAD:13::3/128 [0/0]
 via ::, Serial0/0/0
C 2001:DB8:ACAD:23::/64 [0/0]
 via ::, Serial0/0/1
L 2001:DB8:ACAD:23::3/128 [0/0]
 via ::, Serial0/0/1
L FF00::/8 [0/0]
 via ::, Null0
R3#

```

```

R3#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:C::/64 [0/0]
 via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:C::3/128 [0/0]
 via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:12::/64 [110/128]
 via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:13::/64 [0/0]
 via ::, Serial0/0/0
L 2001:DB8:ACAD:13::3/128 [0/0]
 via ::, Serial0/0/0
C 2001:DB8:ACAD:23::/64 [0/0]
 via ::, Serial0/0/1
L 2001:DB8:ACAD:23::3/128 [0/0]
 via ::, Serial0/0/1
L FF00::/8 [0/0]
 via ::, Null0
R3#

```

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

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

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

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

```

R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
01:30:24: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING t
o FULL, Loading Done

R2(config-rtr)#

```

- 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.

```

R1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
 via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:A::1/128 [0/0]
 via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:B::/64 [110/129]
 via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:C::/64 [110/65]
 via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
 via ::, Serial0/0/0
L 2001:DB8:ACAD:12::1/128 [0/0]
 via ::, Serial0/0/0
C 2001:DB8:ACAD:13::/64 [0/0]
 via ::, Serial0/0/1
L 2001:DB8:ACAD:13::1/128 [0/0]
 via ::, Serial0/0/1
O 2001:DB8:ACAD:23::/64 [110/128]
 via FE80::3, Serial0/0/1
L FF00::/8 [0/0]
 via ::, Null0
R1#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
3.3.3.3 0 FULL/ - 00:00:34 3 Serial0/0/1
R1#

```

```

R1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
 via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:A::1/128 [0/0]
 via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:B::/64 [110/129]
 via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:C::/64 [110/65]
 via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
 via ::, Serial0/0/0
L 2001:DB8:ACAD:12::1/128 [0/0]
 via ::, Serial0/0/0

```

```

C 2001:DB8:ACAD:13::/64 [0/0]
 via ::, Serial0/0/1
L 2001:DB8:ACAD:13::1/128 [0/0]
 via ::, Serial0/0/1
O 2001:DB8:ACAD:23::/64 [110/128]
 via FE80::3, Serial0/0/1
L FF00::/8 [0/0]
 via ::, Null0

```

R1#show ipv6 ospf neighbor

```

Neighbor ID Pri State Dead Time Interface ID Interface
3.3.3.3 0 FULL/ - 00:00:34 3 Serial0/0/1
R1#

```

```

R3#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:B::/64 [110/65]
 via FE80::2, Serial0/0/1
C 2001:DB8:ACAD:C::/64 [0/0]
 via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:C::3/128 [0/0]
 via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:12::/64 [110/128]
 via FE80::1, Serial0/0/0
 via FE80::2, Serial0/0/1
C 2001:DB8:ACAD:13::/64 [0/0]
 via ::, Serial0/0/0
L 2001:DB8:ACAD:13::3/128 [0/0]
 via ::, Serial0/0/0
C 2001:DB8:ACAD:23::/64 [0/0]
 via ::, Serial0/0/1
L 2001:DB8:ACAD:23::3/128 [0/0]
 via ::, Serial0/0/1
L FF00::/8 [0/0]
 via ::, Null0
R3#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
2.2.2.2 0 FULL/ - 00:00:36 4 Serial0/0/1
1.1.1.1 0 FULL/ - 00:00:31 4 Serial0/0/0
R3#

```

```

R3#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 U - Per-user Static route, M - MIPv6
 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
 O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
 via FE80::1, Serial0/0/0
O 2001:DB8:ACAD:B::/64 [110/65]
 via FE80::2, Serial0/0/1
C 2001:DB8:ACAD:C::/64 [0/0]
 via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:C::3/128 [0/0]
 via ::, GigabitEthernet0/0

```



```

O 2001:DB8:ACAD:12::/64 [110/128]
 via FE80::1, Serial0/0/0
 via FE80::2, Serial0/0/1
C 2001:DB8:ACAD:13::/64 [0/0]
 via ::, Serial0/0/0
L 2001:DB8:ACAD:13::3/128 [0/0]
 via ::, Serial0/0/0
C 2001:DB8:ACAD:23::/64 [0/0]
 via ::, Serial0/0/1
L 2001:DB8:ACAD:23::3/128 [0/0]
 via ::, Serial0/0/1
L FF00::/8 [0/0]
 via ::, Null0
R3#show ipv6 ospf neighbor

```

| Neighbor ID | Pri | State   | Dead Time | Interface ID | Interface   |
|-------------|-----|---------|-----------|--------------|-------------|
| 2.2.2.2     | 0   | FULL/ - | 00:00:36  | 4            | Serial0/0/1 |
| 1.1.1.1     | 0   | FULL/ - | 00:00:31  | 4            | Serial0/0/0 |

R3#

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

S0/0/1

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

129

¿El R2 aparece como vecino OSPFv3 en el R1?

NO

¿El R2 aparece como vecino OSPFv3 en el R3?

SI

¿Qué indica esta información?

Todo el tráfico hacia la red 2001:DB8:ACAD:B::/64 desde el R1 se enrutará a través del R3.

La interfaz S0/0/0 en el R2 sigue configurada como interfaz pasiva, por lo que la información de routing OSPFv3 no se anuncia en esa interfaz.

El costo acumulado de 129:

Se debe a que el tráfico del R3 a la red 192.168.2.0/24 debe pasar a través de dos enlaces seriales T1 (1,544 Mb/s) (con un costo igual de 64 cada uno), además del enlace LAN Gigabit 0/0 del R2 (con un costo de 1).

$64 + 64 + 1 = 129$

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

R2(config)#ipv6 router ospf 1

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

R2(config-rtr)#

```

R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#
01:38:38: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING t
o FULL, Loading Done
R2(config-rtr)#

```

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

```

R1#show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
2.2.2.2 0 FULL/ - 00:00:35 3 Serial0/0/0
3.3.3.3 0 FULL/ - 00:00:30 3 Serial0/0/1
R1#
R1#

```

R1#show ipv6 ospf neighbor

```

Neighbor ID Pri State Dead Time Interface ID Interface
2.2.2.2 0 FULL/ - 00:00:35 3 Serial0/0/0
3.3.3.3 0 FULL/ - 00:00:30 3 Serial0/0/1
R1#

```

## Reflexión

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

Sí. La ID del proceso OSPFv3 se usa solo localmente en el router, no es necesario que coincida con la ID del proceso que se usa en los otros routers en el área OSPFv3.

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

- Eliminar la instrucción network ayuda a evitar erratas en direcciones IPv6.
- Además, una interfaz IPv6 puede tener varias direcciones IPv6 asignadas a ella.
- Al asignar una interfaz a un área OSPFv3, todas las redes de multidifusión en esa interfaz se asignan automáticamente al área OSPFv6 y se crea una ruta para ellas en la tabla de routing IPv6.

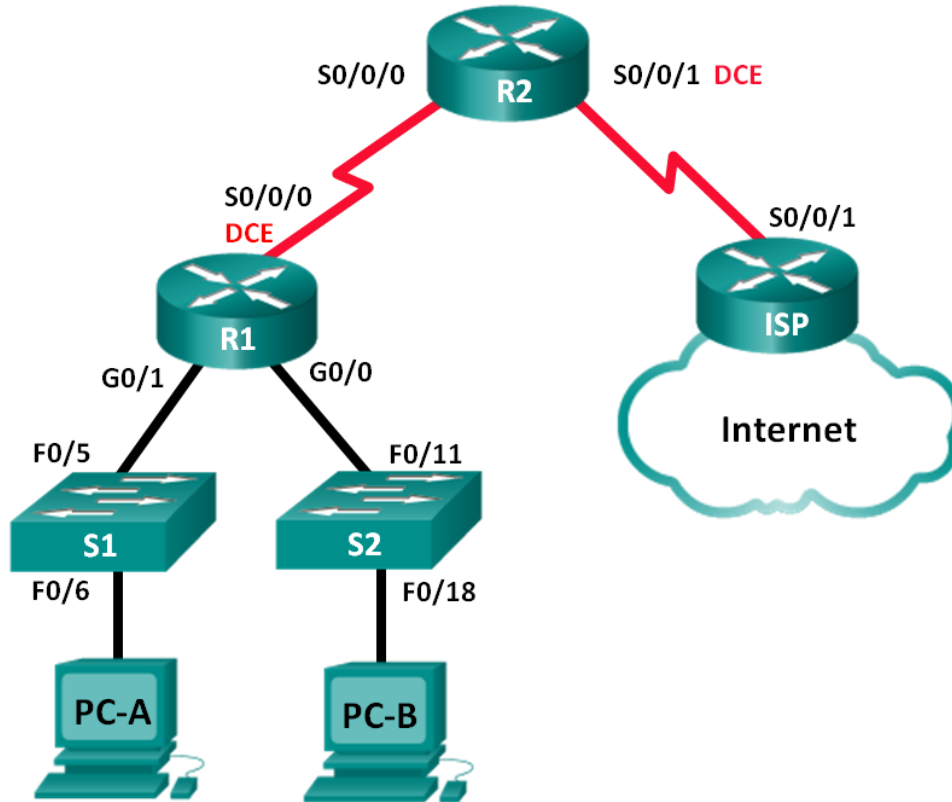
- **Tabla de resumen de interfaces del router**

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

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

## 10.1.2.4 Lab: configuración de DHCPv4 básico en un router

### Topología



### Tabla de direccionamiento

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

### Objetivos

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

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

### Información básica/situación

El protocolo de configuración dinámica de host (DHCP) es un protocolo de red que permite a los administradores de red administrar y automatizar la asignación de direcciones IP. Sin DHCP, el administrador debe asignar y configurar manualmente las direcciones IP, los servidores DNS preferidos y los gateways predeterminados. A medida que aumenta

el tamaño de la red, esto se convierte en un problema administrativo cuando los dispositivos se trasladan de una red interna a otra.

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

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

**Nota:** los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universal9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbase9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

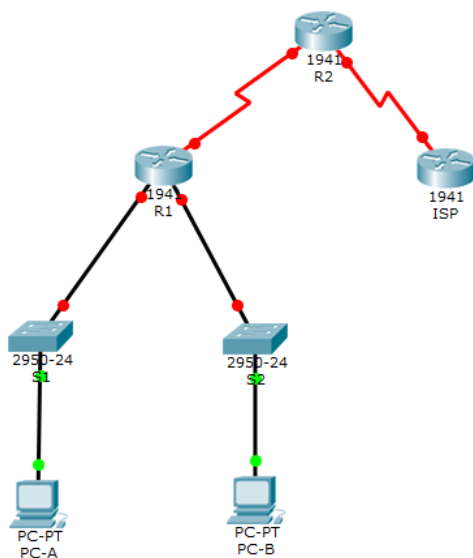
## Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbase9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

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

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

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



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

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

- a. Desactive la búsqueda DNS.

- b. Configure el nombre del dispositivo como se muestra en la topología.
  - c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
  - d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
  - e. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.
- R1.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#security passwords min-length 5
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
R1(config)#
R1(config)#
```

Top

R2.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#security passwords min-length 5
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#exec-timeout 5 0
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#exec-timeout 5 0
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#
R2(config)#
R2(config)#
```

Top

ISP.

```

Router>
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#security passwords min-length 5
ISP(config)#enable secret class
ISP(config)#line con 0
ISP(config-line)#password cisco
ISP(config-line)#exec-timeout 5 0
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#exec-timeout 5 0
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#
ISP(config)#
ISP(config)#

```

Top

- f. Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.
- g. Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.

R1.

```

Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut

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

R1(config-if)#int g0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

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

R1(config-if)#int s0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#ip address 192.168.2.253 255.255.255.252
R1(config-if)#no shut

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

```

Top

R2.

```
User Access Verification
Password:
Password:

R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#int s0/0/0
R2 (config-if)#ip address 192.168.2.254 255.255.255.252
R2 (config-if)#no shut

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

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

R2 (config-if)#int s0/0/1
R2 (config-if)#clock rate 128000
R2 (config-if)#ip address 209.165.200.226 255.255.255.224
R2 (config-if)#no shut

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

Top

ISP.

```

ISP (config)#
ISP (config)#
ISP (config)#int s0/0/1
ISP (config-if)#ip address 209.165.200.225 255.255.255.224
ISP (config-if)#no shut

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

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

ISP (config-if)#|
```

Top

h. Configure EIGRP for R1.

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

```
User Access Verification

Password:

R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 192.168.2.252 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#
```

Top

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

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.252 0.0.0.3
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

```
User Access Verification

Password:

R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router eigrp 1
R2(config-router)#network 192.168.2.252 0.0.0.3
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is up: new adjacency
R2(config-router)#redistribute static
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
R2(config)#
```

Top

- 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
```

```
User Access Verification

Password:

ISP>enable
Password:
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#
ISP(config)#
ISP(config)#
```

Top

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



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

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

ISP a R1.

```
ISP#ping 192.168.2.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/7/14 ms

ISP#
ISP#
ISP#
```

Top

R1 a ISP, R1 a R2

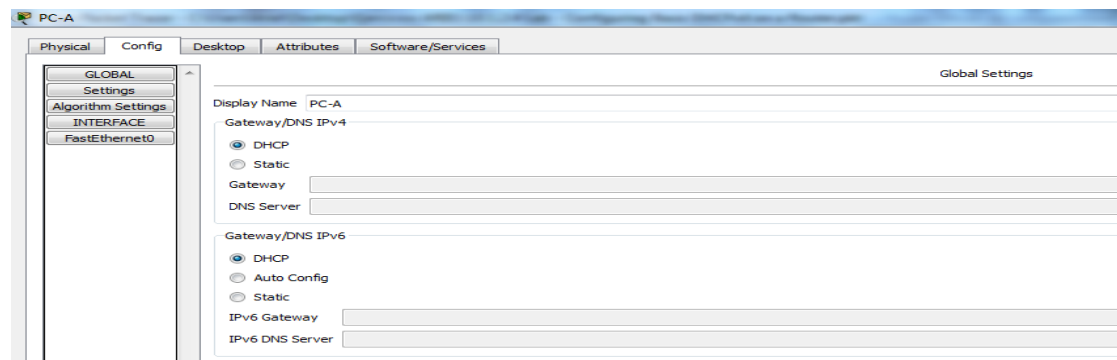
```
Password:
R1>enable
Password:
R1#ping 209.165.200.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/18/65 ms

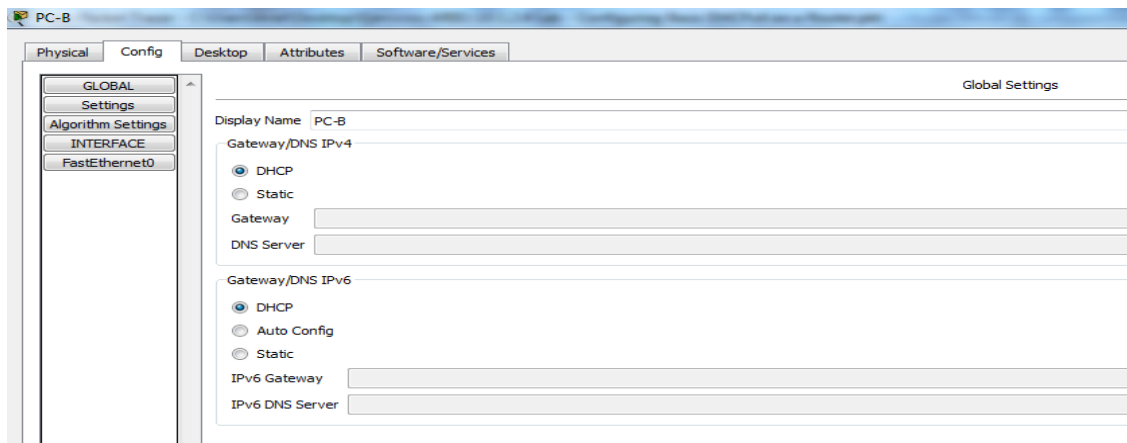
R1#
R1#
R1#ping 192.168.2.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/63 ms

R1#
R1#
R1#
```

Top

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





## Parte 5: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

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

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

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

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

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

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

R2

```

Password:
Password:
Password:

R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
^
% Invalid input detected at '^' marker.

R2(dhcp-config)#lease 2
^
% Invalid input detected at '^' marker.

R2(dhcp-config)#exit
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
^
% Invalid input detected at '^' marker.

R2(dhcp-config)#lease 2
^
% Invalid input detected at '^' marker.

R2(dhcp-config)#
R2(dhcp-config)#

```

Top

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

Los equipos host no reciben direcciones IP del servidor de DHCP en el R2 hasta que el R1 esté configurado como agente de retransmisión DHCP.

```

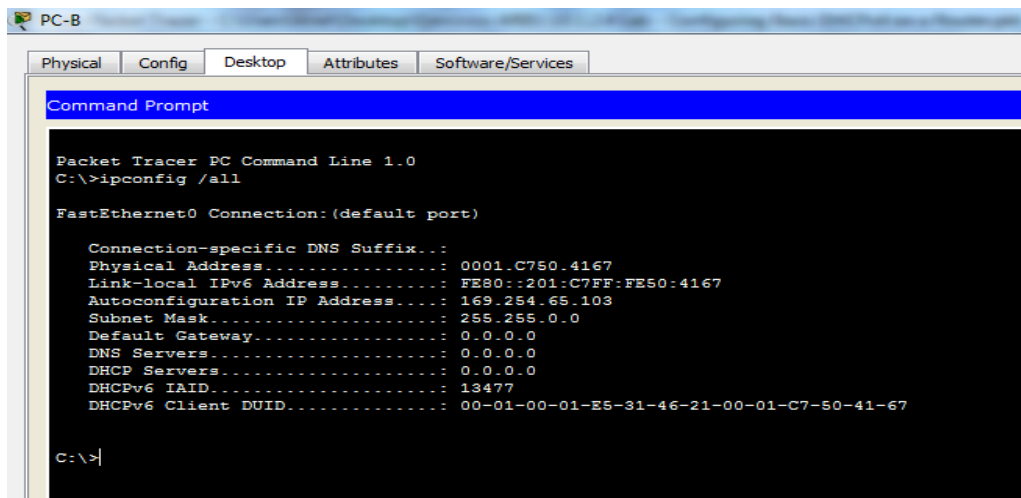
PC-A
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address...: 000A.F3B1.E836
Link-local IPv6 Address...: FE80::20A:F3FF:FEB1:E836
Autoconfiguration IP Address...: 169.254.232.54
Subnet Mask...: 255.255.0.0
Default Gateway...: 0.0.0.0
DNS Servers...: 0.0.0.0
DHCP Servers...: 0.0.0.0
DHCPv6 IAID...: 13209
DHCPv6 Client DUID...: 00-01-00-01-68-B0-81-5B-00-0A-F3-B1-E8-36

C:\>

```



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

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address...: 0001.C750.4167
Link-local IPv6 Address...: FE80::201:C7FF:FE50:4167
Autoconfiguration IP Address...: 169.254.65.103
Subnet Mask...: 255.255.0.0
Default Gateway...: 0.0.0.0
DNS Servers...: 0.0.0.0
DHCP Servers...: 0.0.0.0
DHCPv6 IAID...: 13477
DHCPv6 Client DUID...: 00-01-00-01-E5-31-46-21-00-01-C7-50-41-67

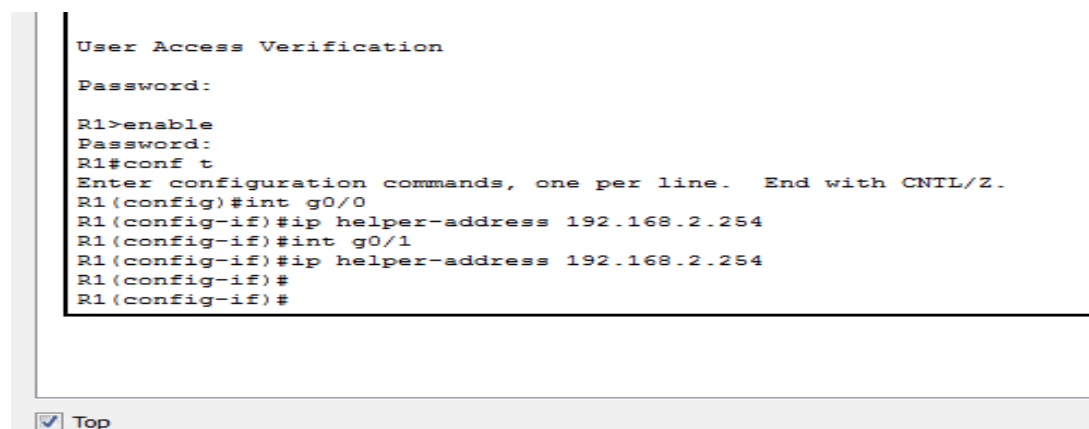
C:\>
```

### Paso 2: configurar el R1 como agente de retransmisión DHCP.

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

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

```
R1#conf t
R1(config)#int g0/0
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#int g0/1
R1(config-if)#ip helper-address 192.168.2.254
```



```
User Access Verification
Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#int g0/1
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#
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

```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

 Connection-specific DNS Suffix...:
 Physical Address.: 000A.F3B1.E836
 Link-local IPv6 Address: FE80::20A:F3FF:FEB1:E836
 IP Address.: 192.168.1.10
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.1.1
 DNS Servers: 209.165.200.225
 DHCP Servers: 192.168.2.254
 DHCPv6 IAID: 13209
 DHCPv6 Client DUID.: 00-01-00-01-68-B0-81-5B-00-0A-F3-B1-E8-36

C:\>|
```

Top

#### PC-B

```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

 Connection-specific DNS Suffix...:
 Physical Address.: 0001.C750.4167
 Link-local IPv6 Address: FE80::201:C7FF:FE50:4167
 IP Address.: 192.168.0.10
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.0.1
 DNS Servers: 209.165.200.225
 DHCP Servers: 192.168.2.254
 DHCPv6 IAID: 13477
 DHCPv6 Client DUID.: 00-01-00-01-E5-31-46-21-00-01-C7-50-41-67

C:\>|
```

Top

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?

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.

```

Password:

R2>enable
Password:
R2#show ip dhcp binding
IP address Client-ID/ Lease expiration Type
 Hardware address
192.168.1.10 000A.F3B1.E836 -- Automatic
192.168.0.10 0001.C750.4167 -- Automatic
R2#
R2#
R2#

```

Top

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

Las direcciones MAC, de hardware del cliente permiten identificar las computadoras específicas que se unieron a la red

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

```

User Access Verification

Password:

R2>enable
Password:
R2#show ip dhcp server statistics
^
% Invalid input detected at '^' marker.

R2#
R2#
R2#

```

Top

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

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

```

R2#
R2#
R2#show ip dhcp pool

Pool R1G1 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 1
Excluded addresses : 2
Pending event : none

1 subnet is currently in the pool
Current index IP address range Leased/Excluded/Total
192.168.1.1 192.168.1.1 - 192.168.1.254 1 / 2 / 254

Pool R1G0 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 1
Excluded addresses : 2
Pending event : none

1 subnet is currently in the pool
Current index IP address range Leased/Excluded/Total
192.168.0.1 192.168.0.1 - 192.168.0.254 1 / 2 / 254
R2#

```

Top

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

Muestra la siguiente dirección disponible para arrendamiento.

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

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

R2#show run
Building configuration...

Current configuration : 1407 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
security passwords min-length 5
!
hostname R2
!
!
!
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 209.165.200.225
ip dhcp pool R1G0
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 209.165.200.225
!
!
!
```

Top

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

```
!
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
ip helper-address 192.168.2.254
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.254
duplex auto
speed auto
!
interface Serial10/0/0
ip address 192.168.2.253 255.255.255.252
clock rate 128000
!
interface Serial10/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
network 192.168.0.0
network 192.168.1.0
network 192.168.2.252 0.0.0.3
!
ip classless
!
```

Top

## Reflexión

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

Tener router separados para DHCP agrega más complicación, y esto disminuye la administración central de la red por ende también requiere que cada router funcione más para administrar su propio direccionamiento DHCP.

Un servidor de DHCP funcionando como router o computadora, que esté dedicado al trabajo es más fácil de administrar.

## 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 de DHCP

### Router R1

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config-if)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

### Router R2

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```



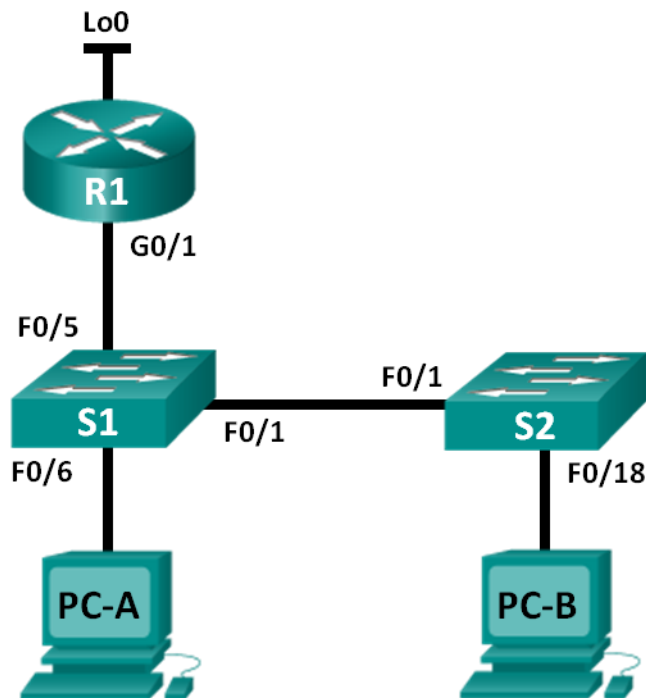
```

R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2

```

## 10.1.2.5 Lab: configuración de DHCPv4 básico en un switch

### Topología



### Tabla de direccionamiento

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

### Objetivos

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

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

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

**Parte 3: configurar DHCPv4**

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

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

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

#### Parte 5: habilitar el routing IP

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

### Información básica/situación

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

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

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

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

### Recursos necesarios

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

### Parte 6: 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.

R1

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 5
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging-synchronous
R1(config-line)#
% Invalid input detected at '^' marker.

R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
R1(config)#
```

Top

S1.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#service password-encryption
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#
S1(config)#linr con 0
S1(config-line)#
% Invalid input detected at '^' marker.

S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#exec-timeout 5 0
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0
S1(config-line)#password cisco
S1(config-line)#exec-timeout 5 0
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#
S1(config)#
```

Top

```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#service password-encryption
S2(config)#enable secret class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#exec-timeout 5 0
S2(config-line)#login
S2(config-line)#logging synchronous
S2(config-line)#exit
S2(config)#line vty 0
S2(config-line)#password cisco
S2(config-line)#exec-timeout 5 0
S2(config-line)#login
S2(config-line)#logging synchronous
S2(config-line)#exit
S2(config)#
S2(config)#
S2(config)#

```

Top

- d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

```

R1(config)#
R1(config)#int g0/1
R1(config-if)#ip address 192.168.1.10 255.255.255.0
R1(config-if)#no shut

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

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

R1(config-if)#int lo 0

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

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

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

```

Top

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

```
User Access Verification

Password:
Password:

S1>enable
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-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)#
S1(config-if)#
```

Top

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

## Parte 7: 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`.

```
User Access Verification

Password:
Password:

S1>enable
Password:
S1#show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

number of unicast mac addresses: 8K
number of IPv4 IGMP groups: 256
number of IPv4/MAC qos aces: 128
number of IPv4/MAC security aces: 384

S1#
```

Top

¿Cuál es la plantilla actual?

la plantilla será `dual-ipv4-and-ipv6 default`.

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

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

```
S1(config)# sdm prefer lanbase-routing
```

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

¿Qué plantilla estará disponible después de la recarga? **lanbase-routing**

- 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]

```
User Access Verification
Password:
S1>enable
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#sdm prefer lanbase-routing
^
% Invalid input detected at '^' marker.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#reload
Proceed with reload? [confirm]#
S1#
```

Top

**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 8: 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.

- Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.
- Cree un pool de DHCP con el nombre **DHCP1**. En el espacio proporcionado, escriba el comando que utilizó.
- Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.
- Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.
- Asigne el servidor DNS como 192.168.1.9. 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.

```
S1#
S1#
S1#
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#ip dhcp pool DHCP1
S1(dhcp-config)#network 192.168.1.1 255.255.255.0
S1(dhcp-config)#default-router 192.168.1.1
S1(dhcp-config)#dns-server 192.168.1.9
S1(dhcp-config)#lease 3
^
% Invalid input detected at '^' marker.

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

Top

### Paso 2: verificar la conectividad y DHCP.

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

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.1.11

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1

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

FastEthernet0 Connection: (default port)

 Link-local IPv6 Address : FE80::250:FFF:FE66:EEC7
 IP Address. : 192.168.1.11
 Subnet Mask : 255.255.255.0
 Default Gateway : 192.168.1.1

C:\>
```

Para la PC-B, incluya lo siguiente:

Dirección IP: 192.168.1.12

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1

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

FastEthernet0 Connection: (default port)

 Link-local IPv6 Address : FE80::20B:BEFF:FE1E:267C
 IP Address. : 192.168.1.12
 Subnet Mask : 255.255.255.0
 Default Gateway : 192.168.1.1

C:\>
```

Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? Si

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



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

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=27ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128
Reply from 192.168.1.12: bytes=32 time=10ms TTL=128
Reply from 192.168.1.12: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.1.12:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 3ms, Maximum = 27ms, Average = 11ms

C:\>
```

Top

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

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=16ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time=10ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.10:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 16ms, Average = 6ms

C:\>
```

Top

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

## Parte 9: 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.

```

User Access Verification

Password:

S1>enable
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int fa0/1
S1(config-if)#switchport mode access
^
% Invalid input detected at '^' marker.

S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
S1(config-if)#
%LINK-S-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-S-UPDOWN: Line protocol on Interface Vlan2, changed state to up

S1(config-if)#

```

Top

## 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.

```

S1(config-if)#
S1(config-if)#exit
S1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)#ip dhcp pool DHCP2
S1(dhcp-config)#network 192.168.2.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.2.9
S1(dhcp-config)#dns-server 192.168.2.9
S1(dhcp-config)#lease 3
^
% Invalid input detected at '^' marker.

S1(dhcp-config)#

```

Top

## 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:

```
C:\>
C:\>
C:\>ipconfig /release

IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
DNS Server.....: 0.0.0.0

C:\>ipconfig /renew

IP Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Server.....: 192.168.1.9

C:\>|
```

Top

- b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado de la VLAN 2 y a la PC-B.  
¿Es posible hacer ping de la PC-A al gateway predeterminado? Si  
¿Es posible hacer ping de la PC-A a la PC-B? No

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=3ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

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

Ping statistics for 192.168.1.12:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

¿Los pings eran correctos? ¿Por qué?

El ping de la PC-A si fue satisfactorio ya que la puesta de enlace se encuentra en la misma red, la PC-B no está en la misma red por esto no es satisfactorio.

- c. Emita el comando **show ip route** en el S1.  
¿Qué resultado arrojó este comando?

```
User Access Verification

Password:

S1>enable
Password:
S1#show ip route

^
% Invalid input detected at '^' marker.

S1#
```

## Parte 10:habilitar el routing IP

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

### Paso 1: habilitar el routing IP en el S1.

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

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

- Verificar la conectividad entre las VLAN.

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

¿Qué función realiza el switch?

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

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

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

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

Gateway of last resort is not set

 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.10/32 is directly connected, GigabitEthernet0/1
 209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/27 is directly connected, Loopback0
L 209.165.200.225/32 is directly connected, Loopback0

R1#
```

Top

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

El router muestra dos redes directamente conectadas,

- ¿Es posible hacer ping de la PC-A al R1? Si

¿Es posible hacer ping de la PC-A a la interfaz Lo0? No

```
C:\>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=18ms TTL=255
Reply from 192.168.1.10: bytes=32 time=15ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time=16ms 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 = 18ms, Average = 12ms

C:\>ping 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.225:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

Top

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

Para que la comunicación ocurra entre todas las redes, las rutas deben ser agregadas a la tabla de ruteo.

## Paso 2: asignar rutas estáticas.

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

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

```
User Access Verification

Password:

S1>enable
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.10
 ^
% Invalid input detected at '^' marker.

S1(config)#|
```

Top

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

```
User Access Verification

Password:

R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 192.168.2.0 255.255.255.0 g0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#|
```

Top

- Vea la información de la tabla de routing para el S1.  
¿Cómo está representada la ruta estática predeterminada?
- Vea la información de la tabla de routing para el R1.

```

Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 192.168.2.0 255.255.255.0 g0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway of last resort is not set

 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.10/32 is directly connected, GigabitEthernet0/1
S 192.168.2.0/24 is directly connected, GigabitEthernet0/1
 209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/27 is directly connected, Loopback0
L 209.165.200.225/32 is directly connected, Loopback0

R1#

```

¿Cómo está representada la ruta estática?

S 192.168.2.0

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

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

```

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=255
Reply from 192.168.1.10: bytes=32 time=1ms TTL=255
Reply from 192.168.1.10: bytes=32 time=10ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.10:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>

```

Top

## Reflexión

1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?  
Las direcciones estáticas fueron excluidas antes de crear el pool de DHCPv4 por a ventana de tiempo que existe y estas podrían ser asignada dinámicamente a otros host.
2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?  
El switch asigna las direcciones IP basándose en el asignamiento de la vlan, en el asignamiento a las vlan hay un puerto que se puede asignar un host.
3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?  
Este dispositivo puede tener funciones DHCP, y puede establecer rutas estáticas, pero no permite el ruteo entre vlans.

## Tabla de resumen de interfaces del router

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

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

## Apéndice A: comandos de configuración

### Configurar DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

### Configurar DHCPv4 para varias VLAN

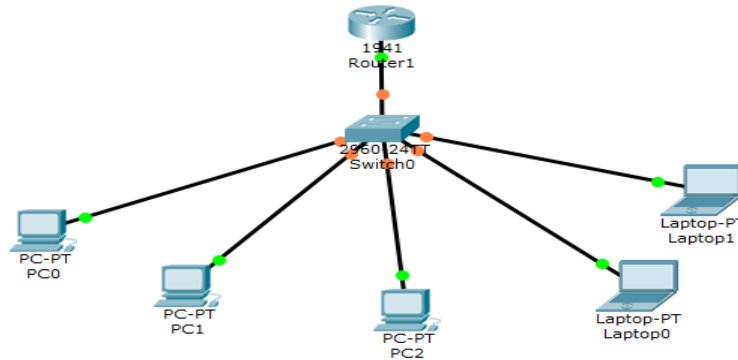
```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)# ip dhcp pool DHCP2
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.2.1
S1(dhcp-config)# dns-server 192.168.2.9
S1(dhcp-config)#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

## Habilitar routing IP

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

### 10.3.1.1 IoE and DHCP

Topología.



## Objetivo

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

## Situación

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

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

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

Cisco Packet Tracer Student - C:\Users\Lore\Desktop\unad loraine\ejercicio unidad 4\10.3.1.1 IoE and DHCP Instructions...

File Edit Options View Tools Extensions Help

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

1941 Router1

2960-24 Switch0

PC-PT PC0

PC-PT PC1

PC-PT PC2

Laptop-PT Laptop1

Laptop-PT Laptop0

Time: 00:26:26 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

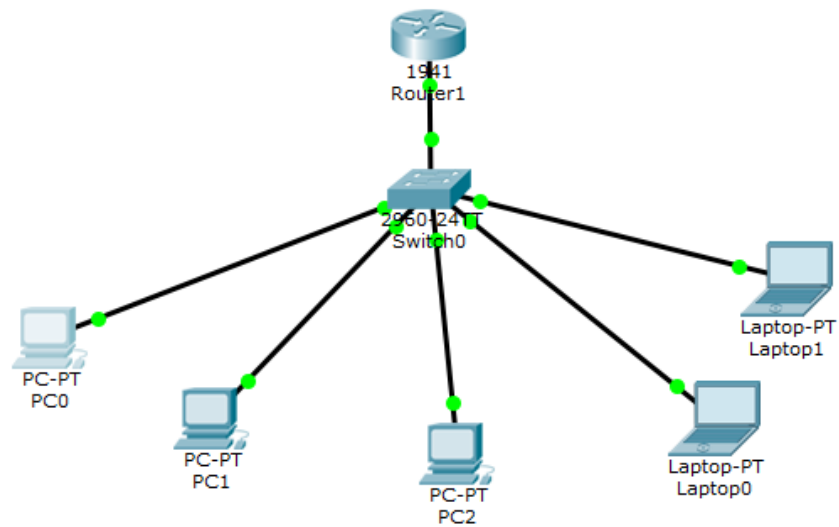
Fire Last Status Source Destination

Connections

Copper Straight-Through

New Delete

Toggle PDU List Window



## IOS Command Line Interface

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/1
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut

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

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

R1(config-if)#exit
R1(config)#dhcp excluded-address 192.168.0.1 192.168.0.10
^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.10
R1(config)#ip dhcp pool LAN
R1(dhcp-config)#network 192.168.0.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.0.1
R1(dhcp-config)#exit
R1(config)#
```

Copy

Paste

PC0

Physical Config Desktop Custom Interface

### IP Configuration

IP Configuration

DHCP     Static    Requesting IP Address

IP Address: 192.168.0.13

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server:

IPv6 Configuration


DHCP     Auto Config     Static

IPv6 Address:

Link Local Address: FE80::260:70FF:FE7B:2C83

IPv6 Gateway:

IPv6 DNS Server:



PC1

Physical Config Desktop Custom Interface

### IP Configuration

IP Configuration

DHCP     Static    DHCP request successful.

IP Address: 192.168.0.15

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server:

IPv6 Configuration


DHCP     Auto Config     Static

IPv6 Address:

Link Local Address: FE80::207:ECFF:FE10:1802

IPv6 Gateway:

IPv6 DNS Server:



PC2

Physical Config Desktop Custom Interface

### IP Configuration

IP Configuration

DHCP  Static DHCP request successful.

IP Address: 192.168.0.14

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server:

IPv6 Configuration

DHCP  Auto Config  Static

IPv6 Address: /

Link Local Address: FE80::201:63FF:FEBA:535

IPv6 Gateway:

IPv6 DNS Server:

Laptop0

Physical Config Desktop Custom Interface

### Global Settings

Display Name: Laptop0

Gateway/DNS

DHCP  Static

Gateway: 192.168.0.1

DNS Server:

Gateway/DNS Ipv6

DHCP  Auto Config  Static

IPv6 Gateway:

IPv6 DNS Server:

Laptop0

Physical Config Desktop Custom Interface

### IP Configuration

IP Configuration

DHCP  Static

IP Address: 192.168.0.12

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server:

IPv6 Configuration

DHCP  Auto Config  Static

IPv6 Address:

Link Local Address: FE80::260:2FFF:FECD:47D2

IPv6 Gateway:

IPv6 DNS Server:

Laptop1

Physical Config Desktop Custom Interface

### Global Settings

Display Name: Laptop1

Gateway/DNS

DHCP  Static

Gateway: 192.168.0.1

DNS Server:

Gateway/DNS Ipv6

DHCP  Auto Config  Static

IPv6 Gateway:

IPv6 DNS Server:

Laptop1

Physical Config Desktop Custom Interface

### IP Configuration

IP Configuration

DHCP  Static

IP Address: 192.168.0.16

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server:

IPv6 Configuration

DHCP  Auto Config  Static

IPv6 Address: /

Link Local Address: FE80::2E0:F9FF:FE03:A54C

IPv6 Gateway:

IPv6 DNS Server:

PC0

Physical Config Desktop Custom Interface

### Command Prompt

```
PC>ping 192.168.0.15
Pinging 192.168.0.15 with 32 bytes of data:

Reply from 192.168.0.15: bytes=32 time=1ms TTL=128
Reply from 192.168.0.15: bytes=32 time=15ms TTL=128
Reply from 192.168.0.15: bytes=32 time=0ms TTL=128
Reply from 192.168.0.15: bytes=32 time=14ms TTL=128

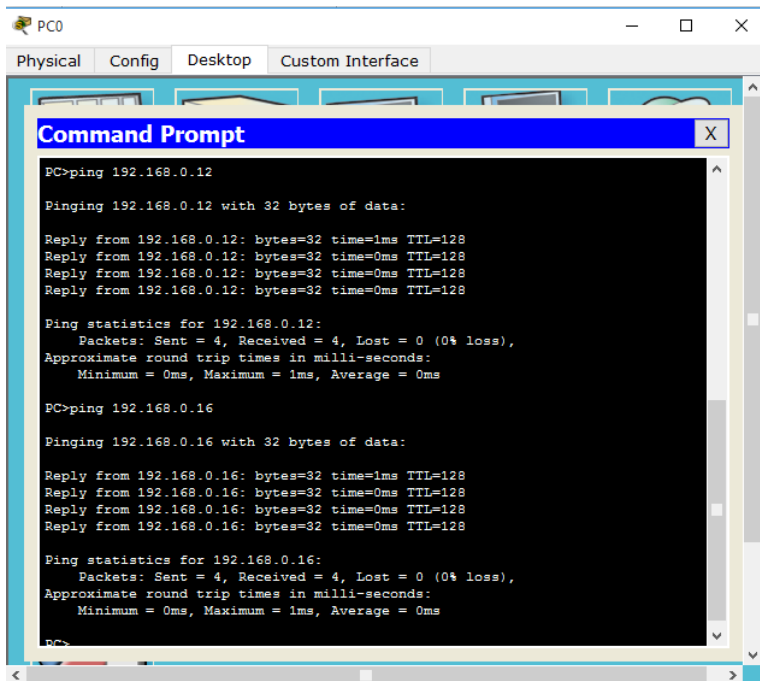
Ping statistics for 192.168.0.15:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 15ms, Average = 7ms

PC>ping 194.168.0.14
Pinging 194.168.0.14 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 194.168.0.14:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.0.12
Pinging 192.168.0.12 with 32 bytes of data:
```



```
PC0
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.0.12
Pinging 192.168.0.12 with 32 bytes of data:
Reply from 192.168.0.12: bytes=32 time=1ms TTL=128
Reply from 192.168.0.12: bytes=32 time=0ms TTL=128
Reply from 192.168.0.12: bytes=32 time=0ms TTL=128
Reply from 192.168.0.12: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.0.12:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.168.0.16
Pinging 192.168.0.16 with 32 bytes of data:
Reply from 192.168.0.16: bytes=32 time=1ms TTL=128
Reply from 192.168.0.16: bytes=32 time=0ms TTL=128
Reply from 192.168.0.16: bytes=32 time=0ms TTL=128
Reply from 192.168.0.16: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.0.16:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>
```

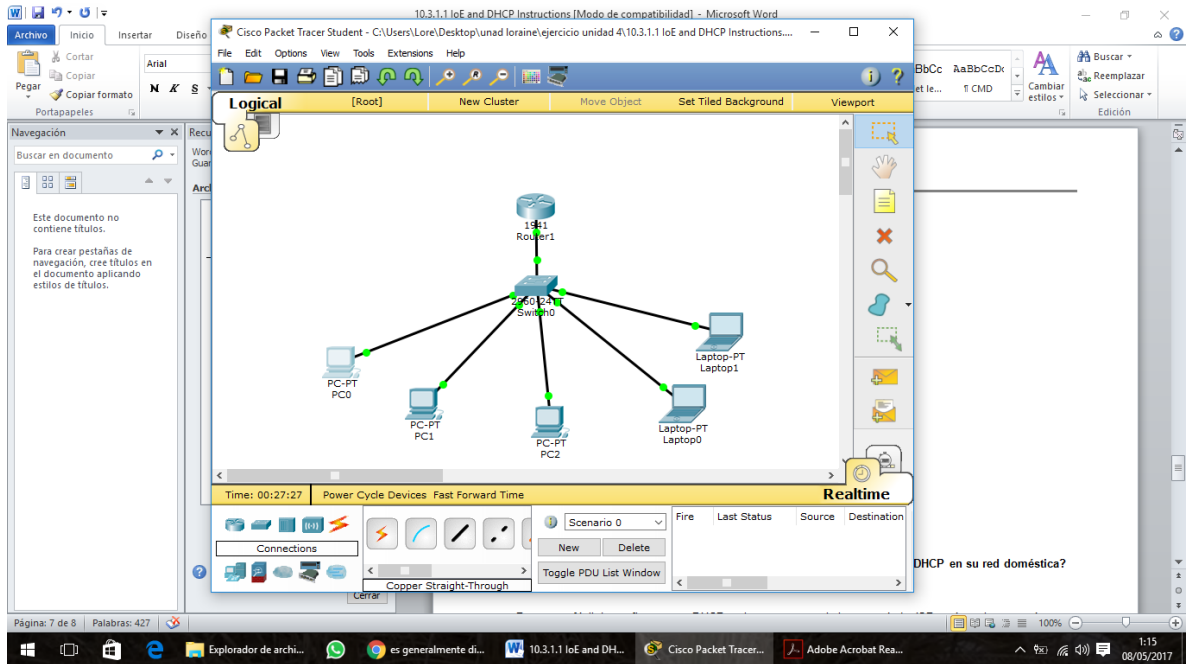
## Reflexión

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

Porque es fácil de configurar para DHCP, y tiene un costo relativamente bajo. ISRs más recientes sería mucho más que "lo suficientemente bueno" nuevo ISR tendría más funcionalidad de lo que las pequeñas empresas es probable que necesite, por lo que un simple y menos caro 1941 sería la mejor opción

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 permite más direccionamiento, por lo tanto, más dispositivos finales, pero con una configuración similar en el enrutador.
  - IPv6 es generalmente dinámico, por lo que configurarlo una vez en el enrutador evita que los técnicos de red tengan que configurar cada dispositivo.
  - IPv6 puede ser configurado con seguridad mejorada en comparación con ipv4, permite a los administradores de red controlar mejor los recursos de una conectividad de red / dispositivo y acceso a los recursos.

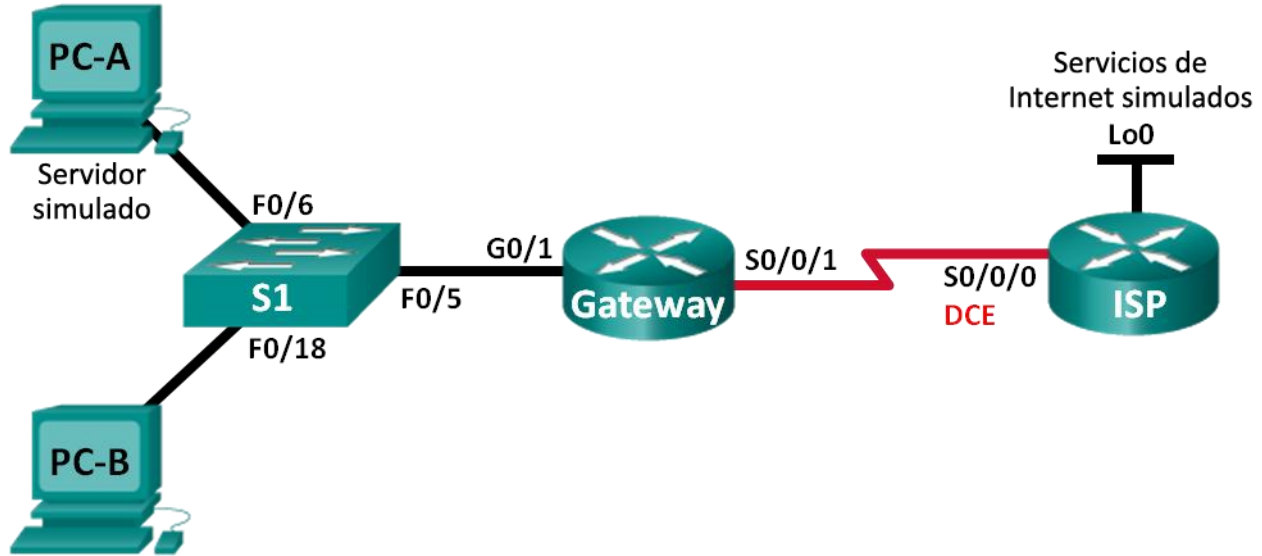
- Permite a las empresas soportar múltiples tipos de dispositivos, tales como teléfonos ip y portátiles
- Permite a los administradores de red configurar algunos dispositivos para facilitar el acceso remoto.





## 11.2.2.6 Lab: configuración de NAT dinámica y estática

### Topología



### Tabla de direccionamiento

| Dispositivo              | Interfaz     | Dirección IP   | Máscara de subred | Gateway predeterminado |
|--------------------------|--------------|----------------|-------------------|------------------------|
| Gateway                  | G0/1         | 192.168.1.1    | 255.255.255.0     | N/A                    |
|                          | S0/0/1       | 209.165.201.18 | 255.255.255.252   | N/A                    |
| ISP                      | S0/0/0 (DCE) | 209.165.201.17 | 255.255.255.252   | N/A                    |
|                          | Lo0 (G0/0)   | 192.31.7.1     | 255.255.255.255   | N/A                    |
| SERVER ISP               | NIC          | 192.31.7.2     | 255.255.255.255   | 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 universal9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbase9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota:** asegúrese de que los routers y 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 lanbase9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

## Parte 11: armar la red y verificar la conectividad

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

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

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

### Paso 2: configurar los equipos host.

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

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

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

### 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

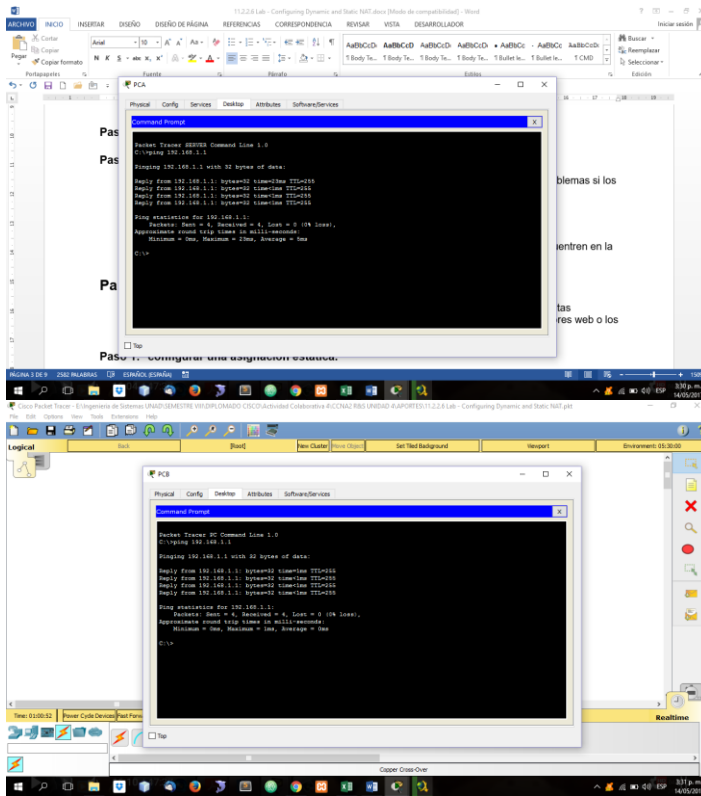
- b. Cree una ruta predeterminada del router Gateway al router ISP.

Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17

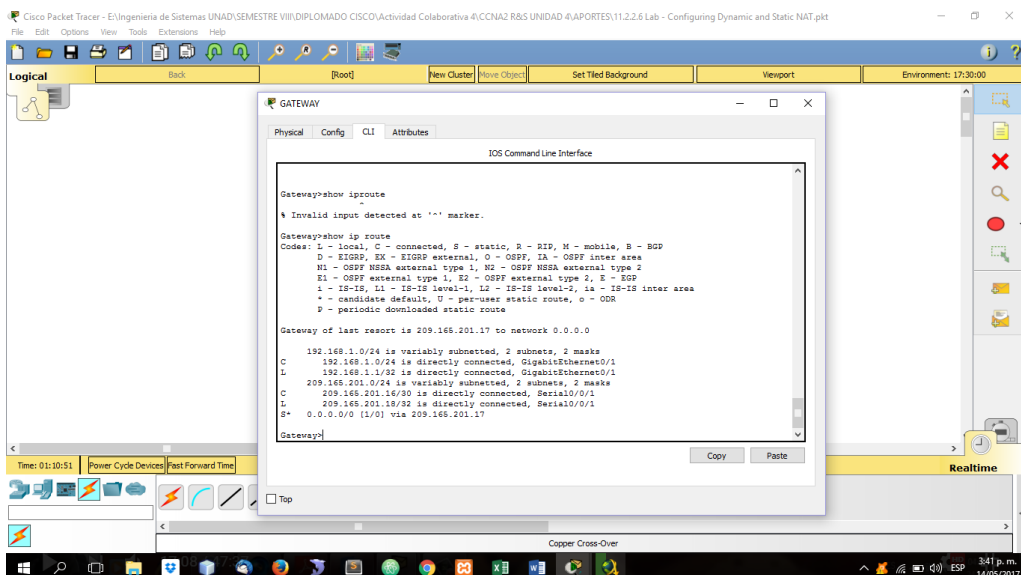
### Paso 7: Guardar la configuración en ejecución en la configuración de inicio.

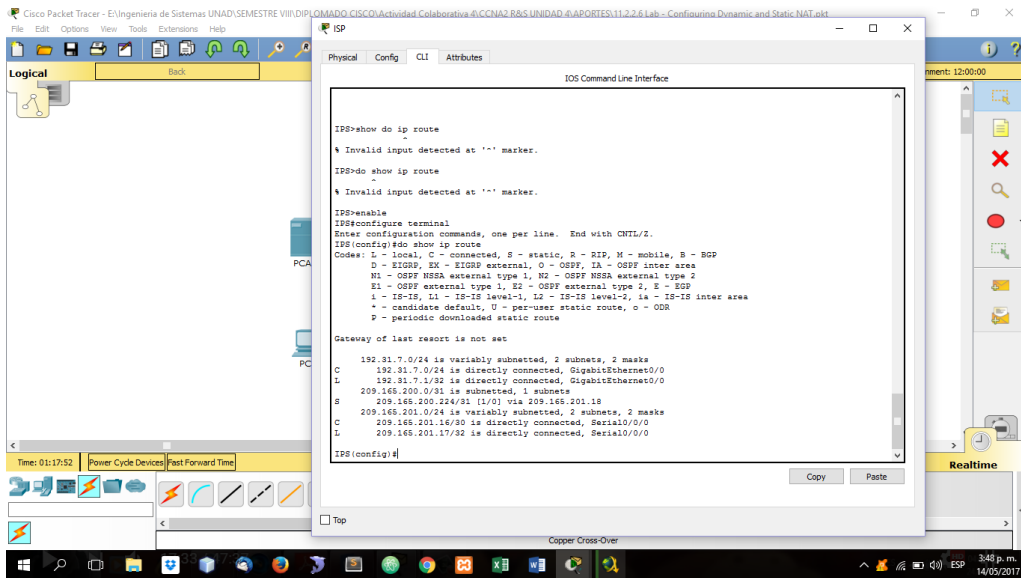
### Paso 8: Verificar la conectividad de la red

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



- b. Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.





## Parte 12: configurar y verificar la NAT estática.

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

### Paso 1: configurar una asignación estática.

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

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

### Paso 2: Especifique las interfaces.

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

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

### Paso 3: probar la configuración.

- 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 --- ---
```

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

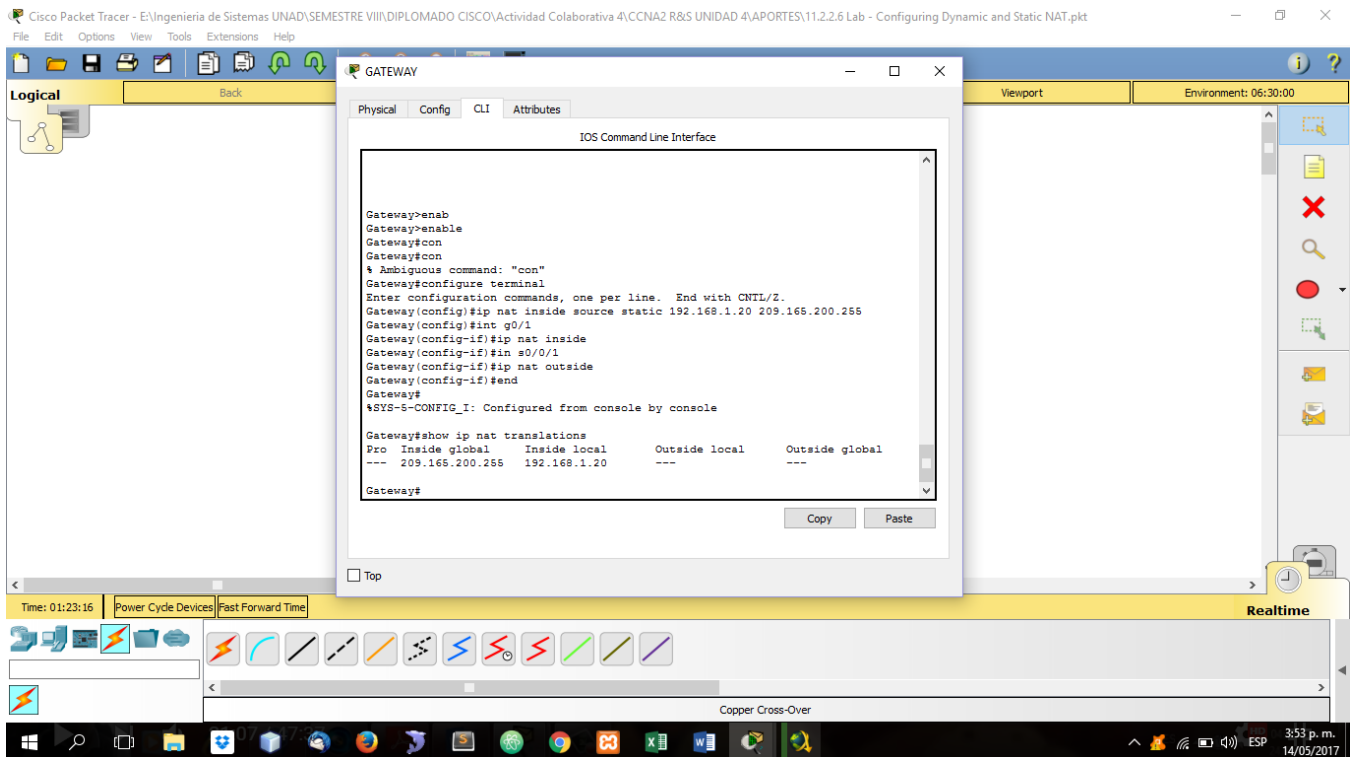
192.168.1.20 = 209.165.200.225

¿Quién asigna la dirección global interna?

El router

¿Quién asigna la dirección local interna?

El Administrador del equipo



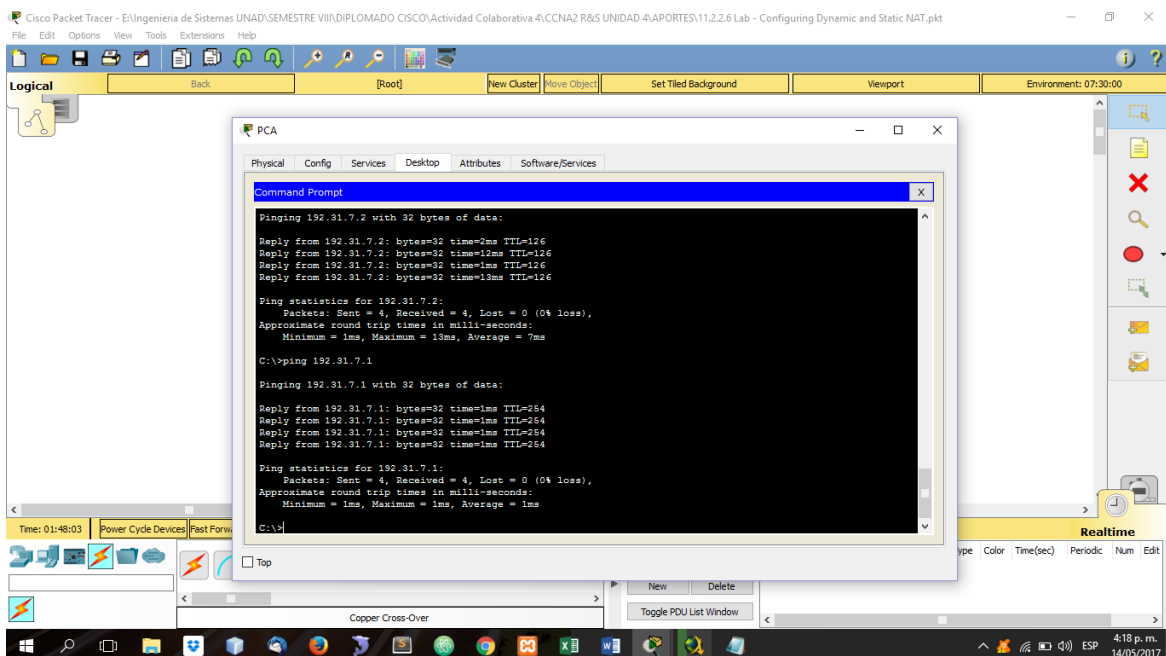
- b. En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

**icmp 209.165.200.255:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1**

--- 209.165.200.255 192.168.1.20 --- ---



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? \_\_\_\_\_

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

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

```
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23
--- 209.165.200.225 192.168.1.20 --- ---
```

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

¿Qué protocolo se usó para esta traducción? telnet / web en el ejemplo

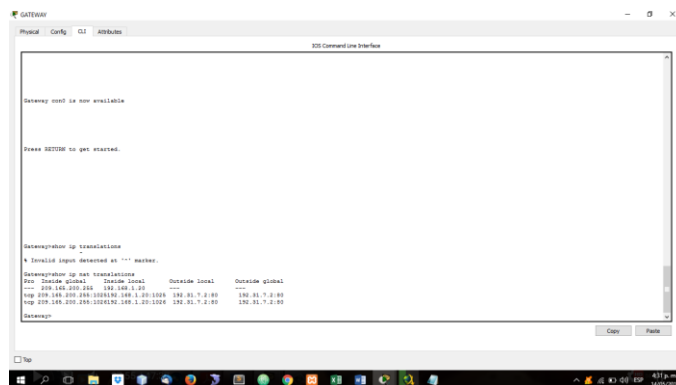
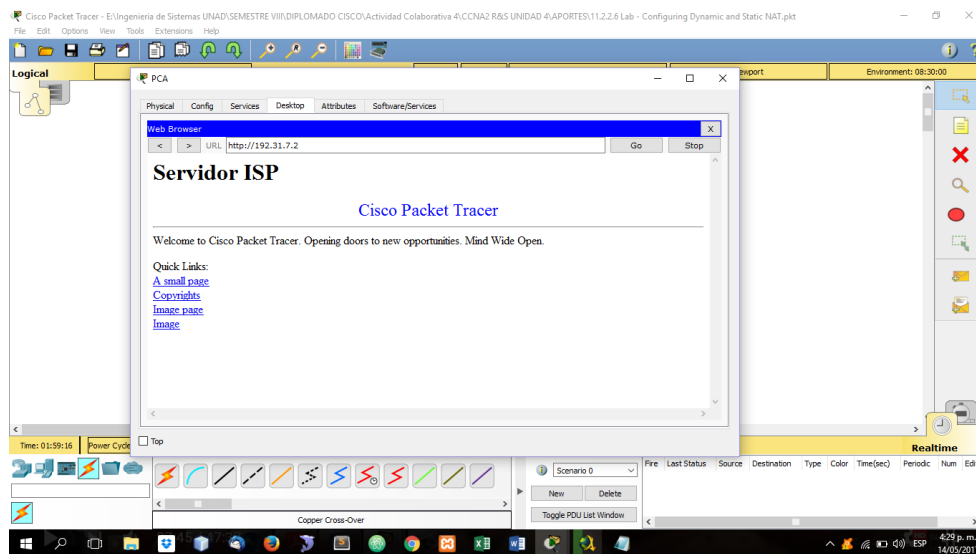
¿Cuáles son los números de puerto que se usaron?

Global/local interno: 1025

Global/local externo: 80 – 80, 23 para telnet

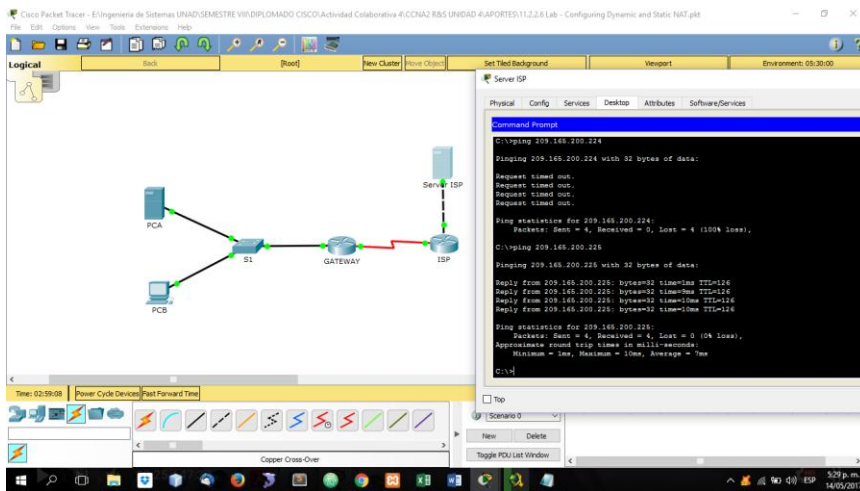
- d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.
- e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

### Gateway# show ip nat translations



```
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12
--- 209.165.200.225 192.168.1.20 --- ---
```

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



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

Gateway# **show ip nat statistics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 00:02:12 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

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



## Parte 13: configurar y verificar la NAT dinámica

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

### Paso 1: borrar las NAT.

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

```
Gateway# clear ip nat translation *
```

```
Gateway# clear ip nat statistics
```

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

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

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

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

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

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

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

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

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

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

**Paso 6: probar la configuración.**

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

```
Gateway# show ip nat translations
```

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

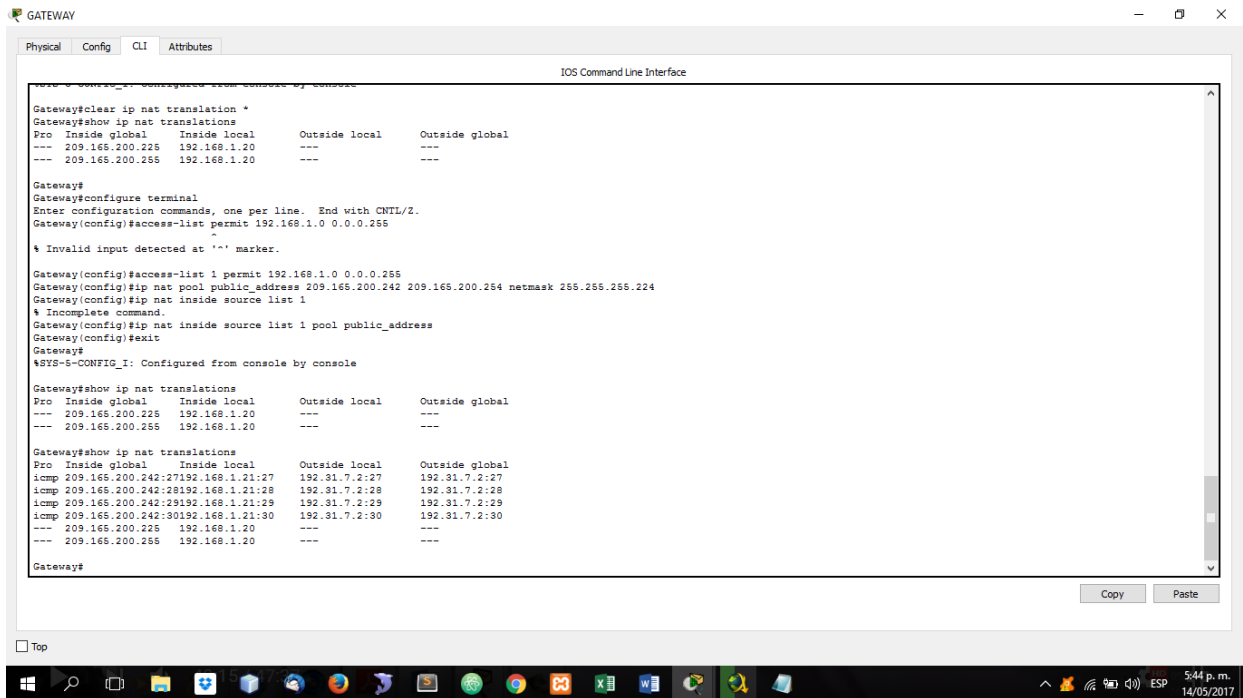
¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = 209.165.200.242:27192.168.1.21:27

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? 27,28,29,30 Origen y destino.

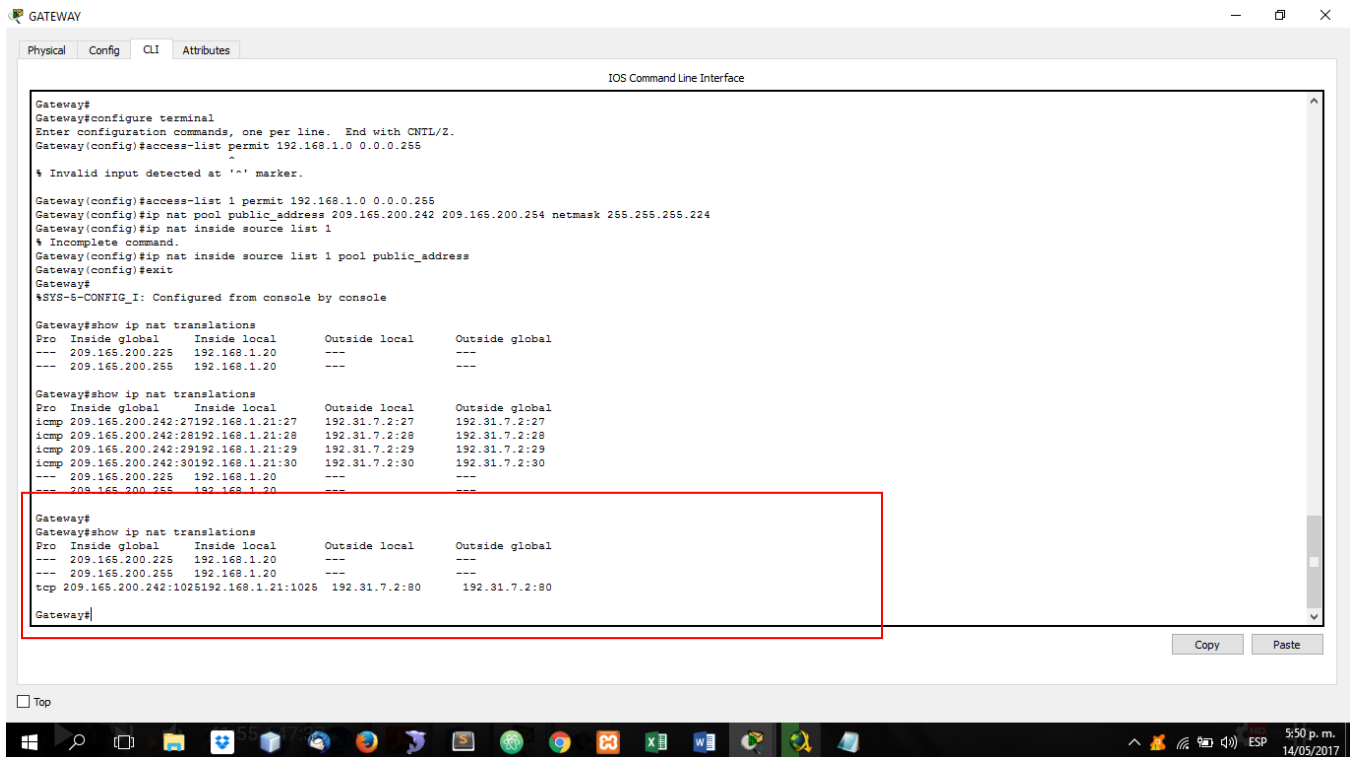




- b. En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.



- c. Muestre la tabla de NAT.



| Pro | Inside global        | Inside local      | Outside local | Outside global |
|-----|----------------------|-------------------|---------------|----------------|
| --- | 209.165.200.225      | 192.168.1.20      | ---           | ---            |
| --- | 209.165.200.255      | 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

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

```
GATEWAY
Physical Config CLI Attributes
IOS Command Line Interface
Gateway(config)#ip nat inside source list 1 pool public_access
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console

Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
--- 209.165.200.255 192.168.1.20 --- ---

Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.242:29192.168.1.21:27 192.31.7.2:27 192.31.7.2:27
icmp 209.165.200.242:28192.168.1.21:28 192.31.7.2:28 192.31.7.2:28
icmp 209.165.200.242:29192.168.1.21:29 192.31.7.2:29 192.31.7.2:29
icmp 209.165.200.242:30192.168.1.21:30 192.31.7.2:30 192.31.7.2:30
--- 209.165.200.255 192.168.1.20 --- ---
--- 209.165.200.255 192.168.1.20 --- ---

Gateway#
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
--- 209.165.200.255 192.168.1.20 --- ---
tcp 209.165.200.242:1025192.168.1.21:1025 192.31.7.2:80 192.31.7.2:80

Gateway#show ip nat statistics
Total translations: 3 (2 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 77 Misses: 906
Expired translations: 83
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#
```

### 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# show ip nat translation

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512 192.31.7.1:512

--- 209.165.200.243 192.168.1.20 --- ---

icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512 192.31.7.1:512

--- 209.165.200.242 192.168.1.21 --- ---

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

The screenshot shows the Cisco Packet Tracer interface. In the background, a network diagram is visible with two PCs (PCA and PCB) connected to a central Gateway. The foreground features a CLI window for the Gateway device, displaying the output of the 'show ip nat statistics' command. The output shows that there are 2 total translations (0 static, 1 dynamic, 1 extended) on the outside interface Serial10/0/1 and the inside interface GigabitEthernet0/1. It also shows 77 hits and 906 misses, with 83 expired translations. Dynamic mappings are shown for an inside source pool named 'public\_address' with a netmask of 255.255.255.224, starting at 209.165.200.242 and ending at 209.165.200.254. The pool has 13 total addresses, with 2 allocated (15%) and 0 misses.

```
IOS Command Line Interface
type generic, total addresses 13 , allocated 1 (7%),
misses 0
Gateway#con
Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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: 2 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial10/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 77 Misses: 906
Expired translations: 83
Dynamic mappings:
-- Inside Source
access-list 1 pool public_address refCount 1
pool public_address: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13 , allocated 1 (7%),
misses 0
Gateway#
```

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

Gateway#show ip nat statistics
Total translations: 3 (2 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 77 Misses: 906
Expired translations: 83
Dynamic mappings:
-- Inside Source
access-list 1 pool public_address refCount 1
pool public_address: 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#con
Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#no ip nat inside source static 192.168.1.20 209.165.200.225
Gateway(config)#exit
Gateway#
*SYS-6-CONFIG_I: Configured from console by console

Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 77 Misses: 906
Expired translations: 83
Dynamic mappings:
-- Inside Source
access-list 1 pool public_address refCount 1
pool public_address: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13 , allocated 1 (7%), misses 0
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.242:1025 192.168.1.21:1025 192.31.7.2:80 192.31.7.2:80

Gateway#
```

## Reflexión

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

Se debe utilizar siempre que no haya suficientes direcciones IP públicas y para evitar el costo de adquisición de direcciones públicas de un ISP. NAT también puede proporcionar una medida de seguridad al ocultar las direcciones internas de las redes externas.

2. ¿Cuáles son las limitaciones de NAT?

NAT necesita la información de IP o de números de puerto en el encabezado IP y el encabezado TCP de los paquetes para la traducción. Esta es una lista parcial de los protocolos que no se pueden utilizar con NAT: SNMP, LDAP, Kerberos versión. 5.

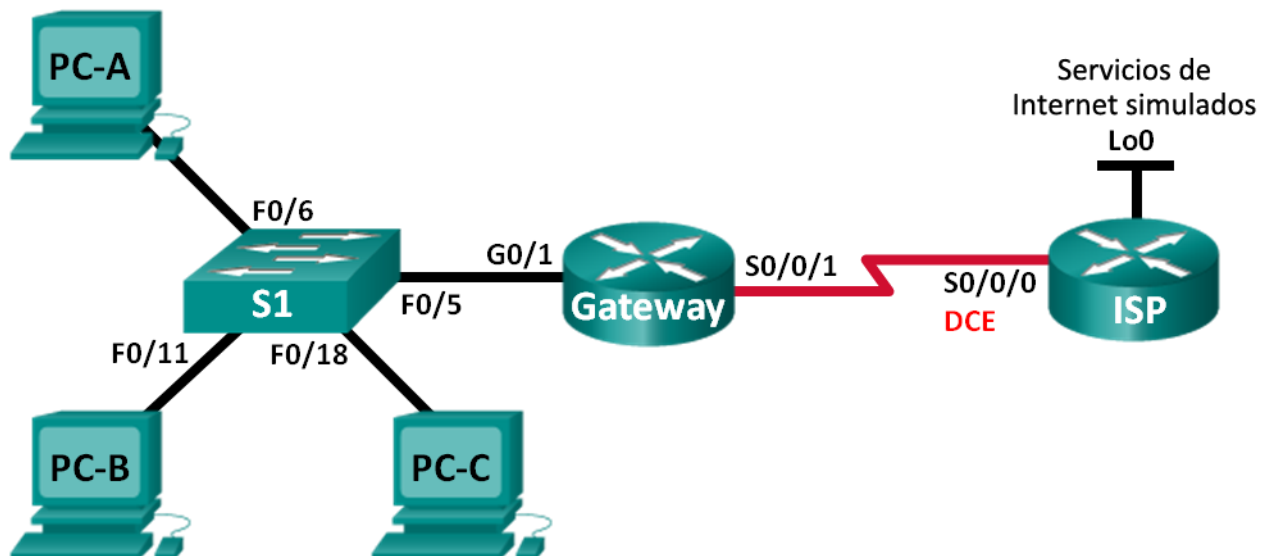
## Tabla de resumen de interfaces del router

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

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

## 11.2.3.7 Lab: configuración de un conjunto de NAT con sobrecarga y PAT

### Topología



## Tabla de direccionamiento

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

## Objetivos

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

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

**Parte 3: configurar y verificar PAT**

## Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

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

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

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

## Recursos necesarios

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

## Parte 14: armar la red y verificar la conectividad

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

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

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

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

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

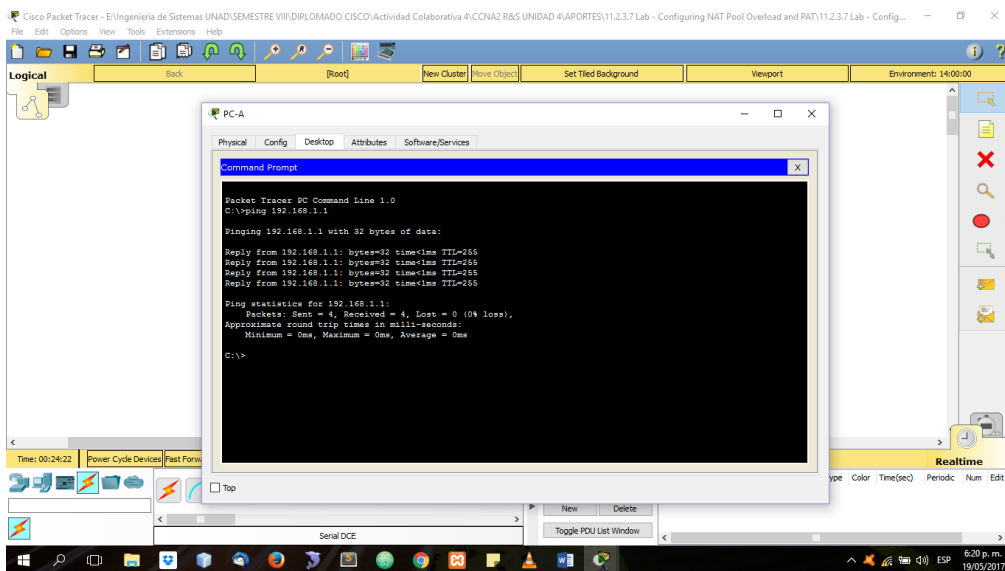
- Desactive la búsqueda del DNS.
- Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **cisco** como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

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

- 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**
- Cree una ruta predeterminada del router Gateway al router ISP.  
Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

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

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



- Verifique que las rutas estáticas estén bien configuradas en ambos routers.

## Parte 15: configurar y verificar el conjunto de NAT con sobrecarga

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

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

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

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



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

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

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

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

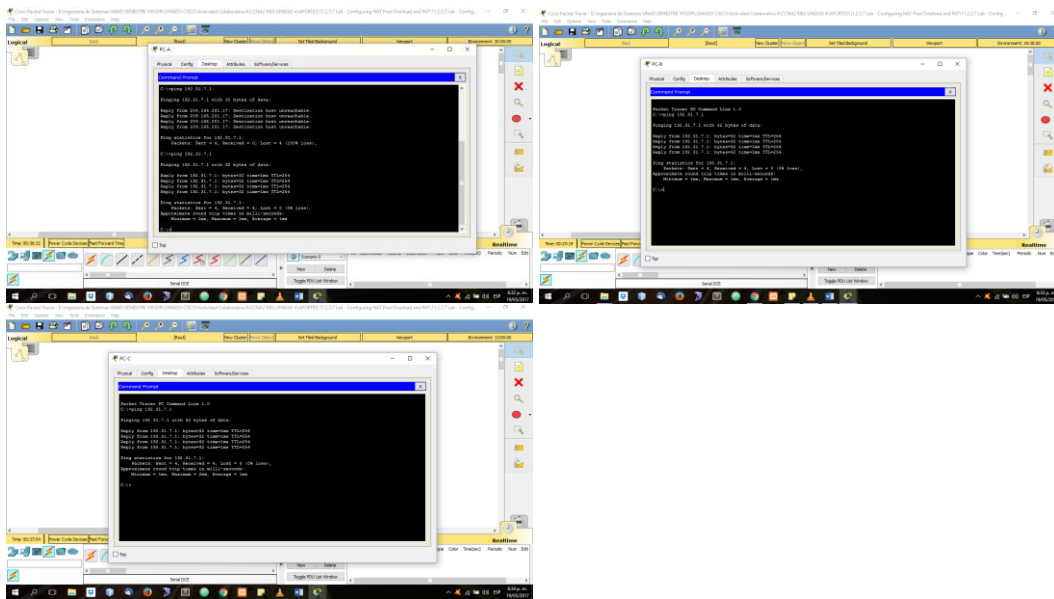
**Paso 4: Especifique las interfaces.**

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

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

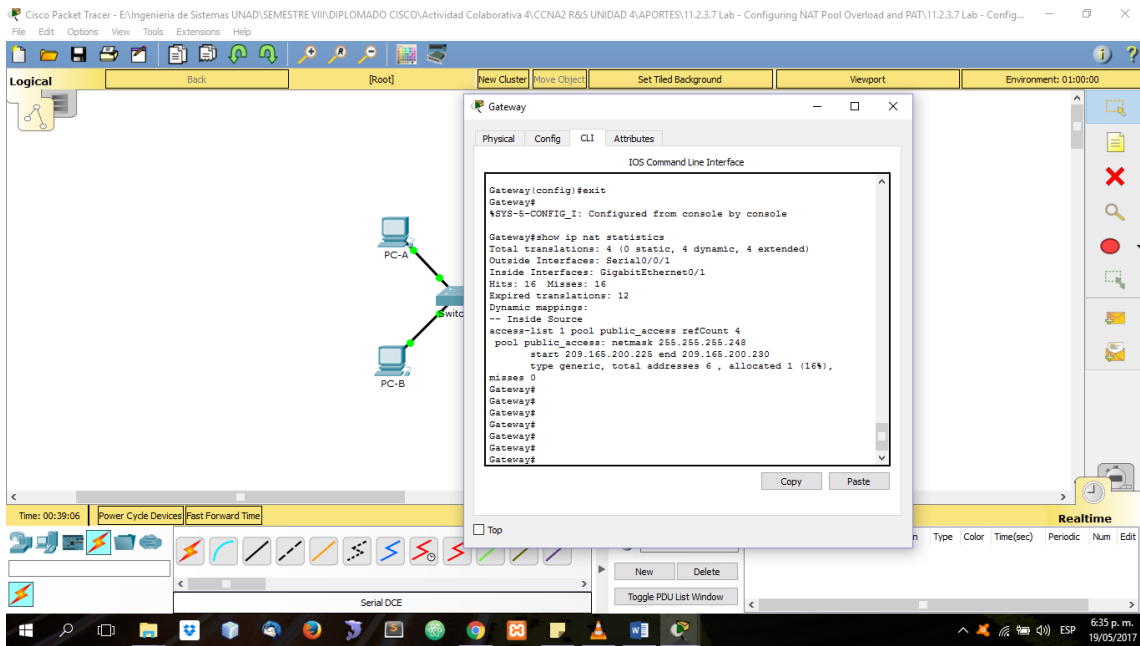
**Paso 5: verificar la configuración del conjunto de NAT con sobrecarga.**

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



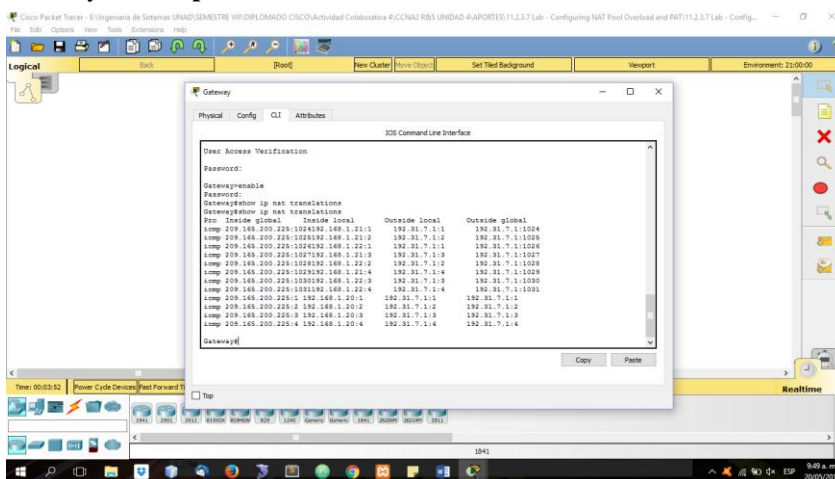
- b. Muestre las estadísticas de NAT en el router Gateway.

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



c. Muestre las NAT en el router Gateway.

### Gateway# show ip nat translations



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

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

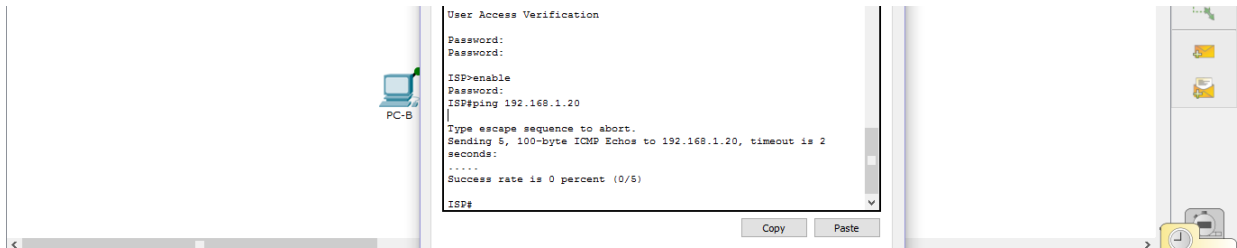
¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? 3

¿Cuántas direcciones IP globales internas se indican? 1

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? 3

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

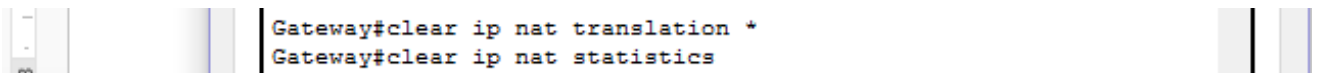
El ping falla ya que el router conoce la ubicación de la dirección global interna de la tabla de routing, mas sin embargo la dirección interna no se anuncia.



## Parte 16: configurar y verificar PAT

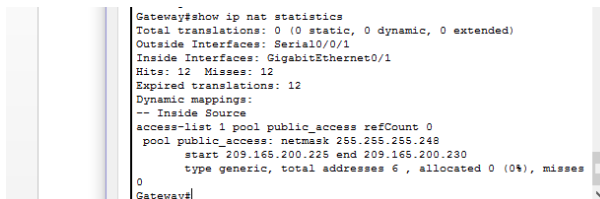
En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

### Paso 1: borrar las NAT y las estadísticas en el router Gateway.

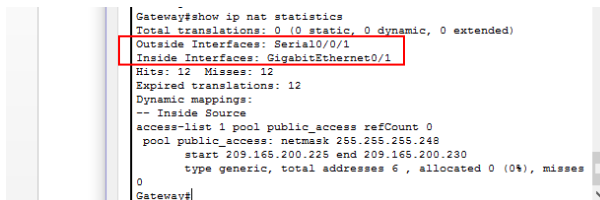


### Paso 2: verificar la configuración para NAT.

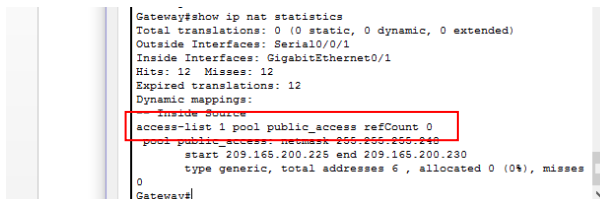
- a. Verifique que se hayan borrado las estadísticas.



- 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.

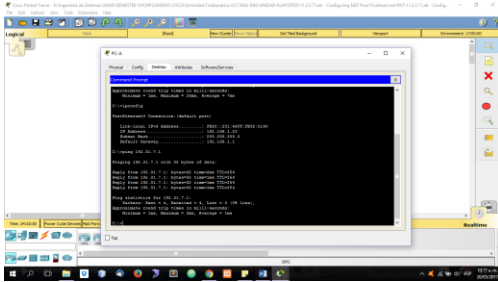
Gateway(config)# ~~no ip nat inside source list 1 pool public\_access overload~~

### 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~~

## Paso 6: probar la configuración PAT.

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



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

Gateway# **show ip nat statistics**

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

Peak translations: 3, occurred 00:00:19 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

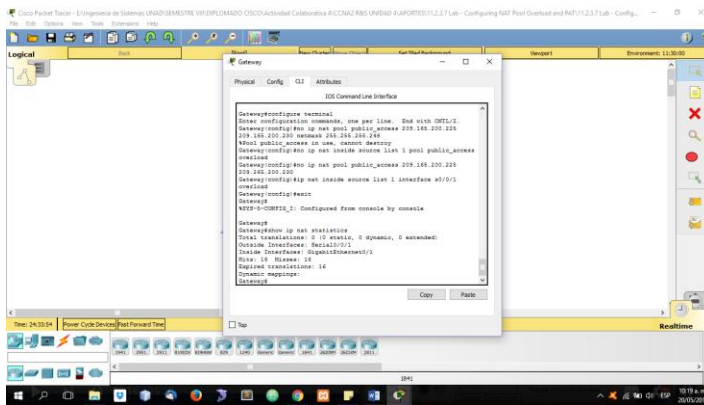
**[Id: 2] access-list 1 interface Serial0/0/1 refcount 3**

Total doors: 0

Appl doors: 0

Normal doors: 0

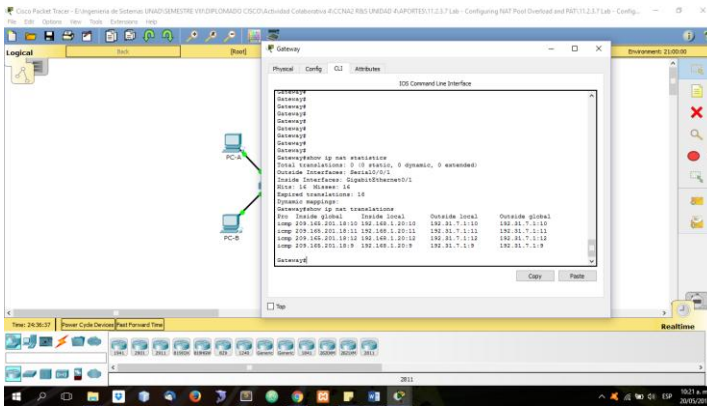
Queued Packets: 0



- c. Muestre las traducciones NAT en el Gateway.

Gateway# **show ip nat translations**

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



## Reflexión

¿Qué ventajas tiene la PAT?

Una de las respuestas más acertadas sería que incluir PAT minimiza la cantidad de direcciones públicas que se necesitan para proporcionar acceso a Internet, además los servicios PAT y NAT nos sirven para ocultar las direcciones privadas de las redes externas.

## Tabla de resumen de interfaces del router

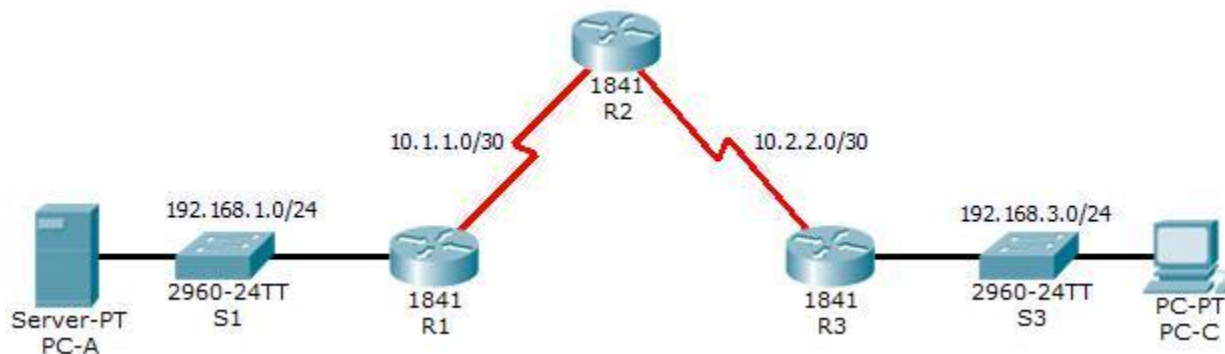
| Resumen de interfaces del router |                             |                             |                       |                       |
|----------------------------------|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de 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.

## EJERCICIOS PKA.

### 4.4.1.2 - Configure IP ACLs to Mitigate Attacks

#### Topology



#### Addressing Table

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

## Objectives

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

## Background / Scenario

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

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

The routers have been pre-configured with the following:

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

## Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

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

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

```
PC-A
Physical Config Services Desktop Attributes Software/Services
Command Prompt
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=26ms TTL=125
Reply from 192.168.3.3: bytes=32 time=29ms TTL=125
Reply from 192.168.3.3: bytes=32 time=31ms TTL=125

Ping statistics for 192.168.3.3:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 26ms, Maximum = 31ms, Average = 28ms

C:\>
```

- b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **cisco55**. When finished, exit the SSH session.

PC> ssh -l SSHadmin 192.168.2.1

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

R2#exit

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

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

- a. From the command prompt, ping **PC-A** (192.168.1.3).
- b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **cisco55**. Close the SSH session when finished.

PC> ssh -l SSHadmin 192.168.2.1



```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=45ms TTL=125
Reply from 192.168.1.3: bytes=32 time=27ms TTL=125
Reply from 192.168.1.3: bytes=32 time=30ms TTL=125
Reply from 192.168.1.3: bytes=32 time=24ms TTL=125

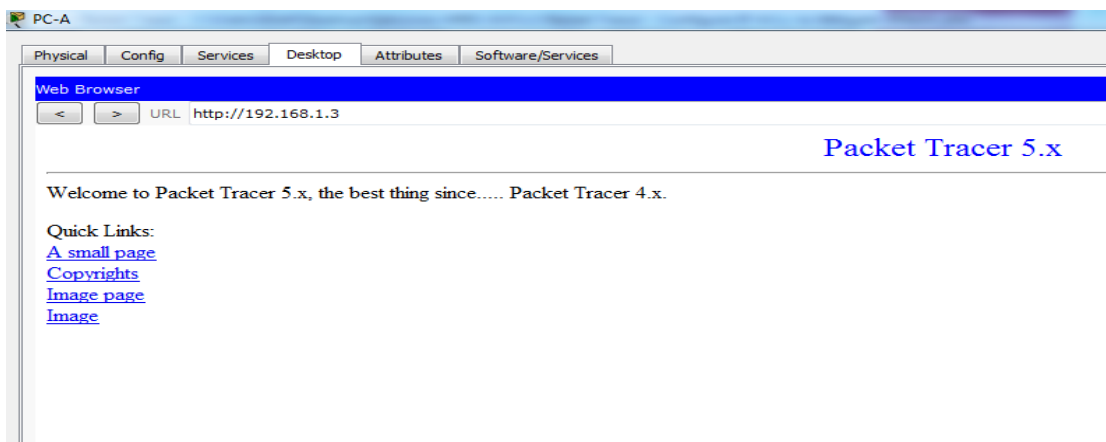
Ping statistics for 192.168.1.3:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 24ms, Maximum = 45ms, Average = 31ms

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

R2#exit

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

- 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
```

```
Press RETURN to get started!

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

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

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

User Access Verification

Password:
Password:

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

Top

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

```
Press RETURN to get started!

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

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

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

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

User Access Verification

Password:
Password:

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

Top

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

```
Press RETURN to get started!

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

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

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

User Access Verification

Password:

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

Top

**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**

```
line aux 0
!
line vty 0 4
 password 7 0822455D0A1613030B1B0D517F
 login local
 transport input ssh
!
!
ntp update-calendar
!
end

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

Top

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

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

Top

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

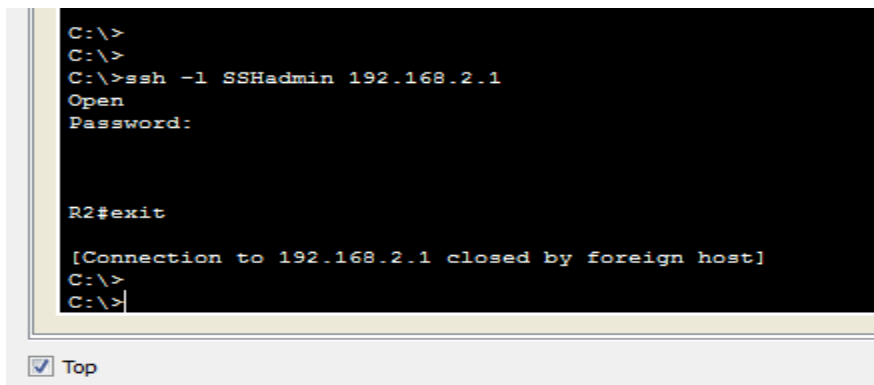
```
R3(config)#
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#
R3(config-line)#
```

Top

**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

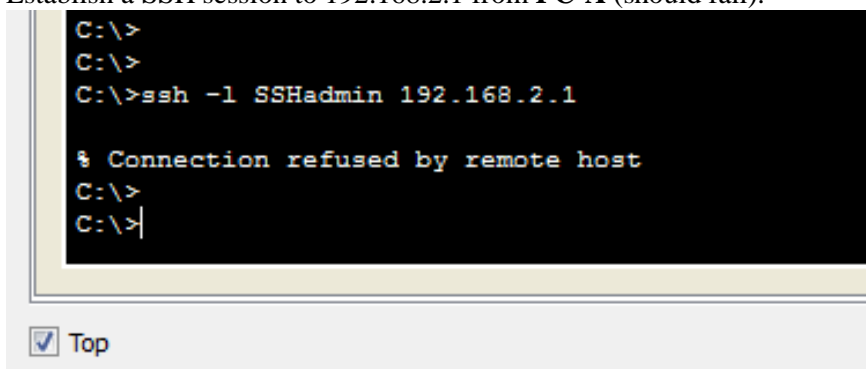


```
C:\>
C:\>
C:\>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#exit

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

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



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

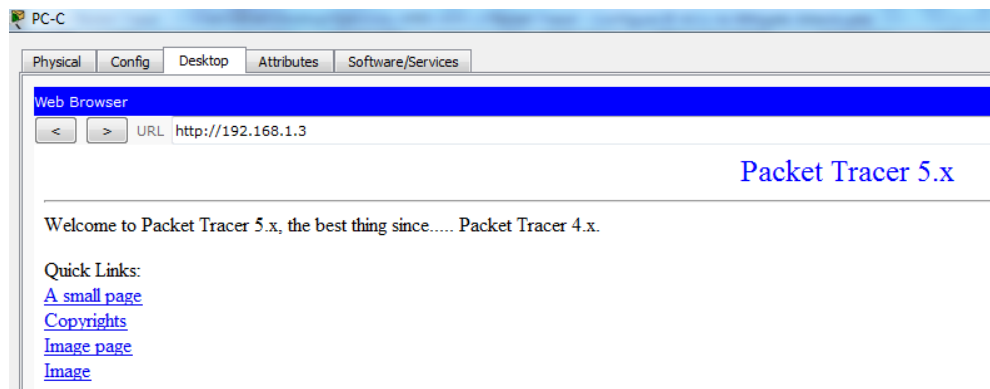
% Connection refused by remote host
C:\>
C:\>
```

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

Top

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

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

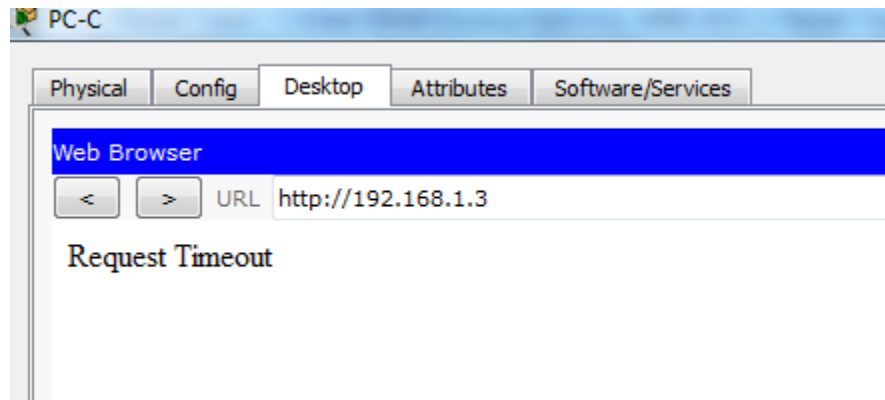
```
R1(config)# interface s0/0/0
```

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

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

Top

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



## Part 4: Modify An Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to **R1**); deny all other incoming ICMP packets.

**Step 1:** Verify that PC-A cannot successfully ping the loopback interface on R2.

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

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

C:\>
C:\>
```

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

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

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

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

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

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

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

Top

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

```
C:\>
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=19ms TTL=254
Reply from 192.168.2.1: bytes=32 time=5ms TTL=254
Reply from 192.168.2.1: bytes=32 time=13ms TTL=254
Reply from 192.168.2.1: bytes=32 time=18ms TTL=254

Ping statistics for 192.168.2.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 5ms, Maximum = 19ms, Average = 13ms

C:\>
C:\>
```

Top

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

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

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

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

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

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

Top

## 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)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#
```

Top

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

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

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

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

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

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

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



```
R3(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
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)#
```

Top

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

Top

**Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.**

From the **PC-C** command prompt, ping the **PC-A** server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

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

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

C:\>
```

Top

#### 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
```

```
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
```

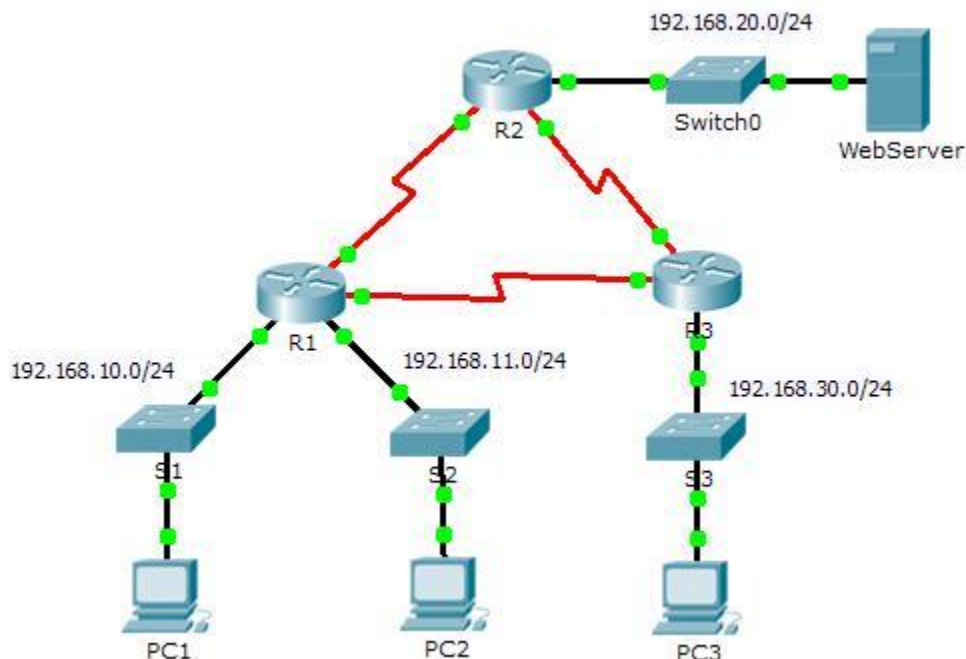
```
ip access-group 100 in
```

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

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

## 9.2.1.10 - Configuring Standard ACLs

### Topology



### Addressing Table

| Device | Interface | IP Address   | Subnet Mask     | Default Gateway |
|--------|-----------|--------------|-----------------|-----------------|
| R1     | F0/0      | 192.168.10.1 | 255.255.255.0   | N/A             |
|        | F0/1      | 192.168.11.1 | 255.255.255.0   | N/A             |
|        | S0/0/0    | 10.1.1.1     | 255.255.255.252 | N/A             |
|        | S0/0/1    | 10.3.3.1     | 255.255.255.252 | N/A             |
| R2     | F0/0      | 192.168.20.1 | 255.255.255.0   | N/A             |
|        | S0/0/0    | 10.1.1.2     | 255.255.255.252 | N/A             |
|        | S0/0/1    | 10.2.2.1     | 255.255.255.252 | N/A             |
|        | F0/0      | 192.168.30.1 | 255.255.255.0   | N/A             |

|           |        |                |                 |              |
|-----------|--------|----------------|-----------------|--------------|
| R3        | S0/0/0 | 10.3.3.2       | 255.255.255.252 | N/A          |
|           | S0/0/1 | 10.2.2.2       | 255.255.255.252 | N/A          |
| PC1       | NIC    | 192.168.10.10  | 255.255.255.0   | 192.168.10.1 |
| PC2       | NIC    | 192.168.11.10  | 255.255.255.0   | 192.168.11.1 |
| PC3       | NIC    | 192.168.30.10  | 255.255.255.0   | 192.168.30.1 |
| WebServer | NIC    | 192.168.20.254 | 255.255.255.0   | 192.168.20.1 |

## Objectives

### Part 1: Plan an ACL Implementation

### Part 2: Configure, Apply, and Verify a Standard ACL

## Background / Scenario

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

## Part 1: Plan an ACL Implementation

### Paso 1: Investigue la configuración actual de la red.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tiene una conectividad completa. Compruebe que la red tiene una conectividad completa eligiendo un PC y haciendo ping a otros dispositivos en la red. Debe poder ejecutar con éxito ping en cada dispositivo.

### Paso 2: evalúe dos políticas de red y planifique las implementaciones de ACL.

- Las siguientes políticas de red se implementan en R2:
  - La red 192.168.11.0/24 no tiene acceso al WebServer en la red 192.168.20.0/24.
  - Todo otro acceso está permitido.

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

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

- The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network. All other  
La red 192.168.10.0/24 no puede comunicarse con la red 192.168.30.0/24.
- Todo otro acceso está permitido.access is permitted.

Para restringir el acceso desde la red 192.168.10.0/24 a la red 192.168.30 / 24 sin interferir con otro tráfico, habrá que crear una lista de acceso en R3. La ACL debe colocarse en la interfaz de salida a PC3. Una segunda regla debe ser creada en R3 para permitir todo el otro tráfico.

## Part 2: Configure, Apply, and Verify a Standard ACL

### Paso 1: Configure y aplique una ACL estándar numerada en R2

- d. Cree una ACL usando el número 1 en R2 con una instrucción que niega el acceso a la red 192.168.20.0/24 de la red 192.168.11.0/24.

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

```
R2>
R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#
```

- e. De forma predeterminada, una lista de acceso deniega todo el tráfico que no coincide con una regla. Para permitir todo el otro tráfico, configure la siguiente instrucción:

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

```
R2>
R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#
R2(config)#access-list 1 permit any
R2(config)#
R2(config)#
```

- f. Para que la ACL filtre realmente el tráfico, debe aplicarse a alguna operación del enrutador. Aplique la ACL colocándola para tráfico saliente en la interfaz Gigabit Ethernet 0/0.

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

```
R2>
R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#
R2(config)#access-list 1 permit any
R2(config)#
R2(config)#int g0/0
R2(config-if)#
```

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

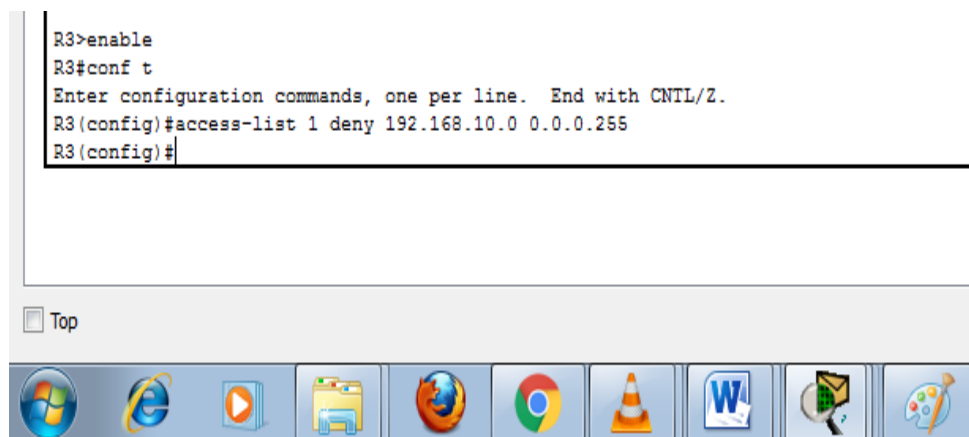
```
R2>
R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#
R2(config)#access-list 1 permit any
R2(config)#
R2(config)#int g0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

## Paso 2: Configure y aplique una ACL estándar numerada en R3.

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

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

```
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)#
```



- d. De forma predeterminada, una ACL deniega todo el tráfico que no coincide con una regla. Para permitir todo el otro tráfico, cree una segunda regla para ACL 1.

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

```
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)#
```

- e. Aplique la ACL colocándola para tráfico saliente en la interfaz Gigabit Ethernet 0/0.

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

```
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)#
```

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

```
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
```

### Step 3: Verify ACL configuration and functionality.

- a. En R2 y R3, ingrese el comando show access-list para verificar las configuraciones ACL.

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



```

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

```

Introduzca el comando show run o show ip interface gigabitethernet 0/0 para verificar las ubicaciones de ACL.

```

R2#show ip interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
 Internet address is 192.168.20.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is 1
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
 --More--

```

```

R3#show ip interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
 Internet address is 192.168.30.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is 1
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
 --More--

```

b. Con las dos ACL instaladas, el tráfico de red está restringido de acuerdo con las políticas detalladas en la Parte 1. Utilice las pruebas siguientes para verificar las implementaciones de ACL:

- A ping from 192.168.10.10 to 192.168.11.10 succeeds.**  
Se enviaron 4 paquetes, pero se recibieron 3 y se perdió 1 paquete.

```
PC1
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.11.10: bytes=32 time=26ms TTL=127
Reply from 192.168.11.10: bytes=32 time=19ms TTL=127
Reply from 192.168.11.10: bytes=32 time=27ms TTL=127

Ping statistics for 192.168.11.10:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 19ms, Maximum = 27ms, Average = 24ms

C:\>
```

- A ping from 192.168.10.10 to 192.168.20.254 succeeds. Sucede los mismo que en el anterior se pierde un paquete

```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.254: bytes=32 time=29ms TTL=126
Reply from 192.168.20.254: bytes=32 time=28ms TTL=126
Reply from 192.168.20.254: bytes=32 time=24ms TTL=126

Ping statistics for 192.168.20.254:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 24ms, Maximum = 29ms, Average = 27ms

C:\>
```

- A ping from 192.168.11.10 to 192.168.20.254 fails.

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

Pinging 192.168.20.254 with 32 bytes of data:

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

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

C:\>
```

- A ping from 192.168.10.10 to 192.168.30.10 fails.

```
Pinging 192.168.30.10 with 32 bytes of data:

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

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

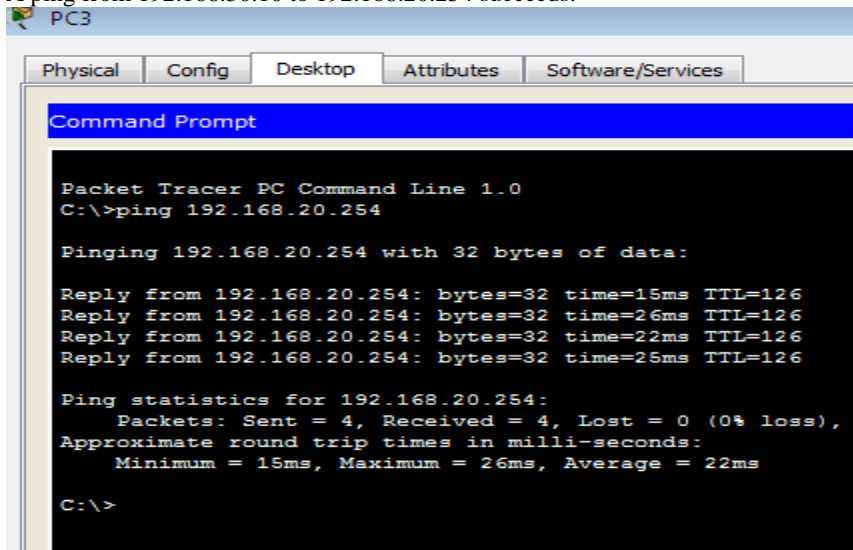
C:\>
```

- A ping from 192.168.11.10 to 192.168.30.10 succeeds.

```
Ping statistics for 192.168.30.10:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
 Minimum = 22ms, Maximum = 31ms, Average = 27ms

C:\>
```

- A ping from 192.168.30.10 to 192.168.20.254 succeeds.



The screenshot shows a Windows PC window titled "PC3" with tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The "Command Prompt" window is open, displaying the output of a ping command to 192.168.20.254. The output shows four successful replies with varying round-trip times and a 0% loss rate.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254

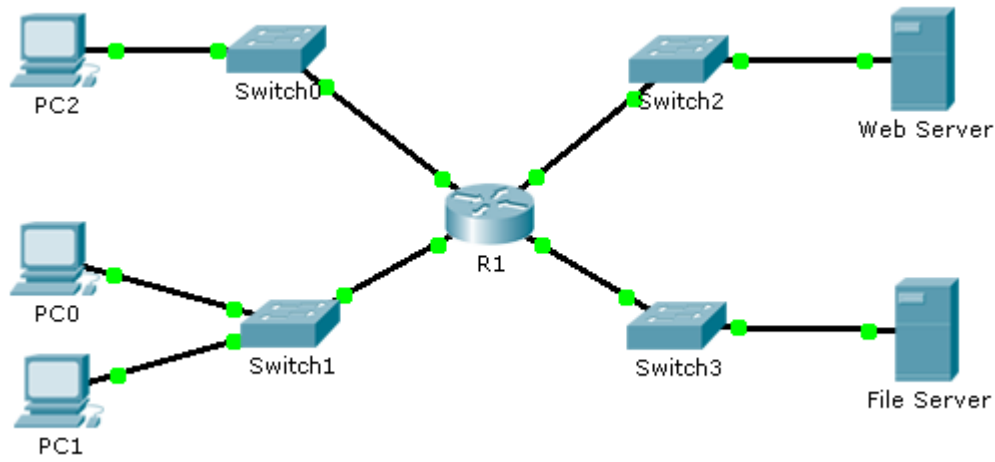
Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=15ms TTL=126
Reply from 192.168.20.254: bytes=32 time=26ms TTL=126
Reply from 192.168.20.254: bytes=32 time=22ms TTL=126
Reply from 192.168.20.254: bytes=32 time=25ms 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 = 15ms, Maximum = 26ms, Average = 22ms

C:\>
```

# Packet Tracer - Configuring Named Standard ACLs



## Topology

### Addressing Table

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

## Objectives

- Part 1: Configure and Apply a Named Standard ACL**
- Part 2: Verify the ACL Implementation**

## Background / Scenario

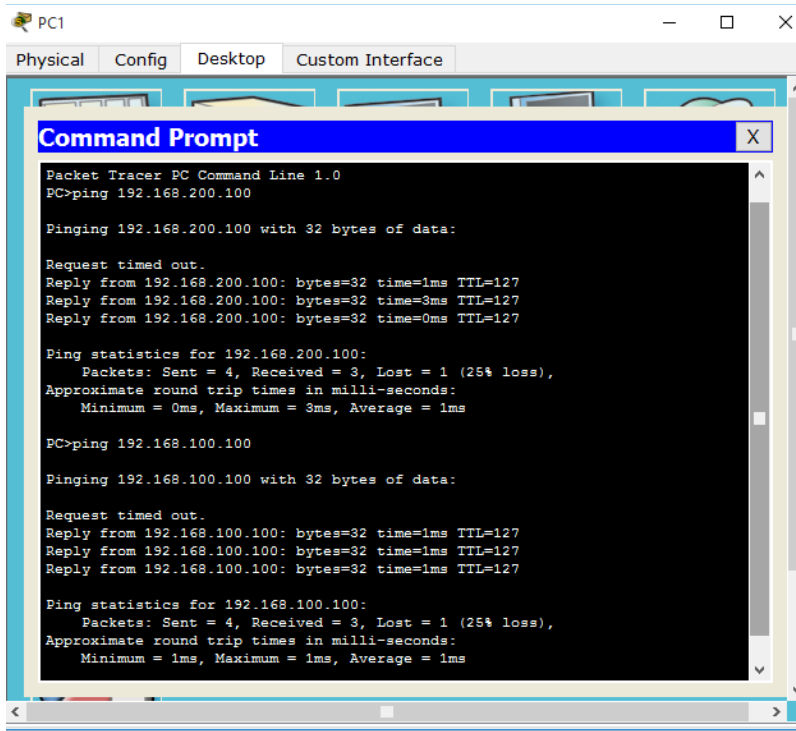
The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied

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

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

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

Pc1



```
PC1
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=3ms 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 = 3ms, Average = 1ms

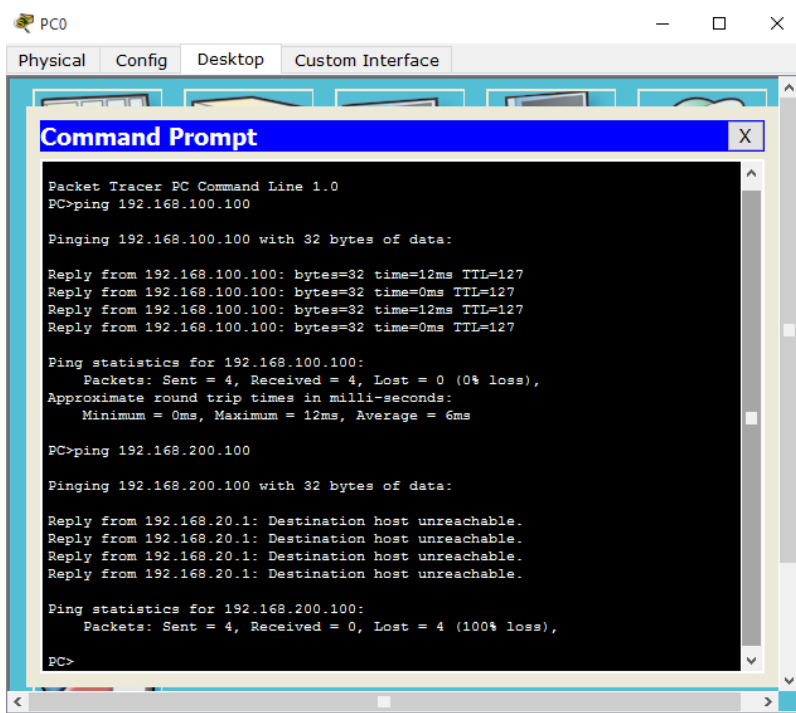
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127

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

Pc0



```
PC0
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127

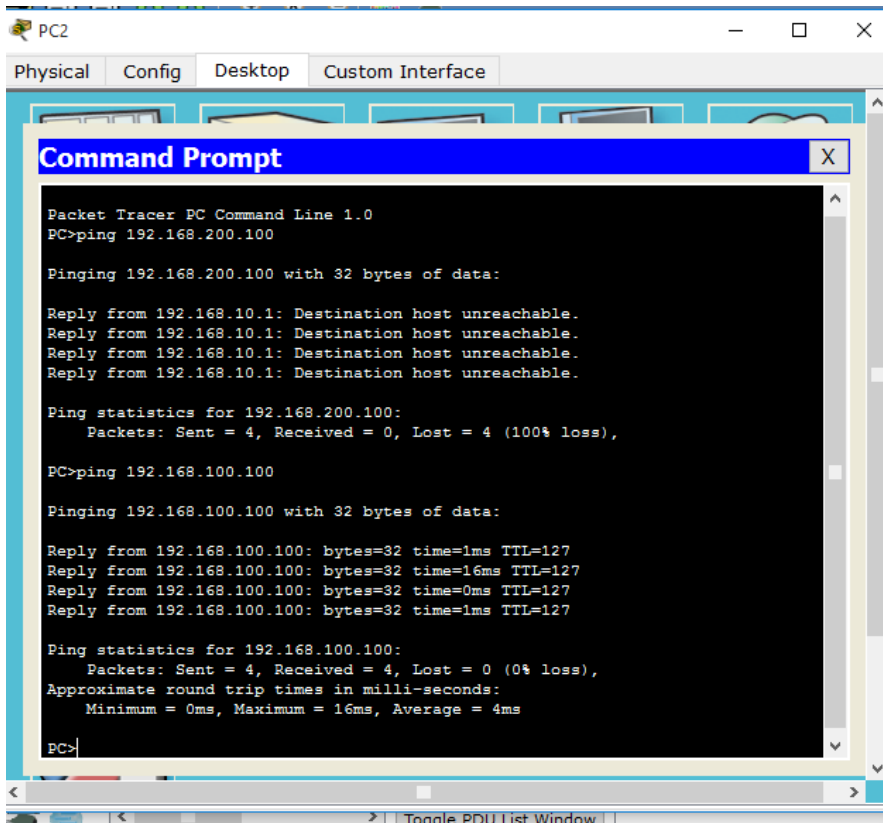
Ping statistics for 192.168.100.100:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 12ms, Average = 6ms

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

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

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



## Step 2: Configure a named standard ACL.

Configure the following named ACL on **R1**.

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

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

**R1(config-std-nacl)# deny any**

```

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

```

**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.

```

R1(config)#int fa0/1
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 r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

```

## Part 2: Verify the ACL Implementation

### Step 1: Verify the ACL configuration and application to the interface.

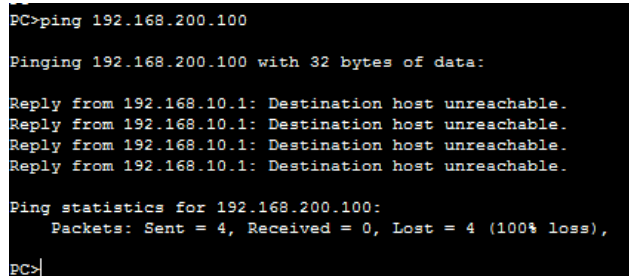
Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface fastethernet 0/1** command to verify that the ACL is applied correctly to the interface.

```
R1#show access-lists
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.20.4
 20 deny any
R1#show ip interface fastethernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
 Internet address is 192.168.200.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is File_Server_Restrictions
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
--More-- |
```

### 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**.

Pc2



```
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Ping statistics for 192.168.200.100:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

Pc0

```

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

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

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

```

Pc1

```

Pinging 192.168.100.100 with 32 bytes of data:

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

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

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=2ms TTL=127

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

```

Cisco Packet Tracer Student - C:\Users\Lore\Desktop\unad loraine\ejercicio unidad 4\9.2.1.11 Packet Tracer - Configurin... - □ ×

File Edit Options View Tools Extensions Help

## Activity Results

Time Elapsed: 00:10:53

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

| Assessment Items |                        | Status  | Points |
|------------------|------------------------|---------|--------|
| Network          |                        |         |        |
| R1               |                        |         |        |
| ACL              | File_Server_Restric... | Correct | 80     |
| Ports            |                        |         | 0      |
| FastEthernet0/1  | Access-group Out       | Correct | 20     |

**Score** : 100/100

**Item Count** : 2/2

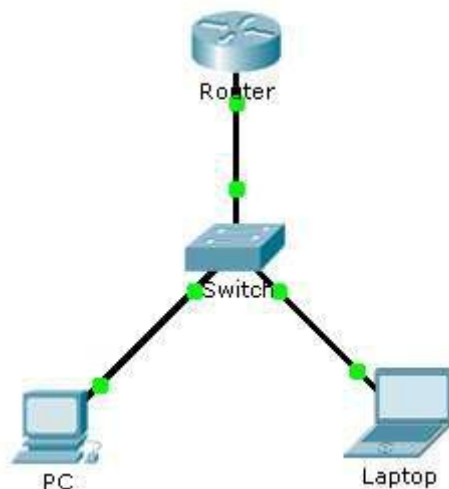
| Component                        | Items/Total | Score   |
|----------------------------------|-------------|---------|
| IPv4 Standard ACL Implementation | 2/2         | 100/100 |

Close



## 9.2.3.3 -Packet Tracer - Configuring an ACL on VTY Lines

### Topology



### Addressing Table

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

### Objetivos

Parte 1: Configurar y aplicar una ACL a líneas VTY

Parte 2: Verificar la implementación del LCA

### Fondo

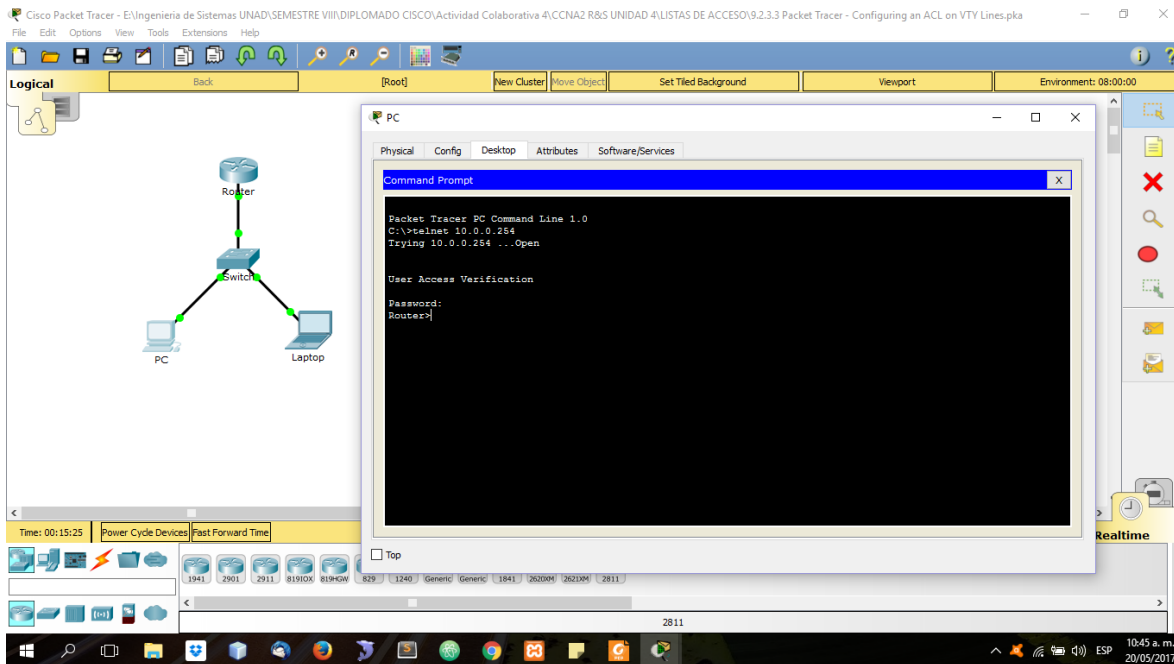
Como administrador de red, debe tener acceso remoto a su enrutador. Este acceso no debería estar disponible para otros usuarios de la red. Por lo tanto, configurará y aplicará una lista de control de acceso (ACL) que permite el acceso de PC a las líneas Telnet, pero deniega todas las demás direcciones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

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

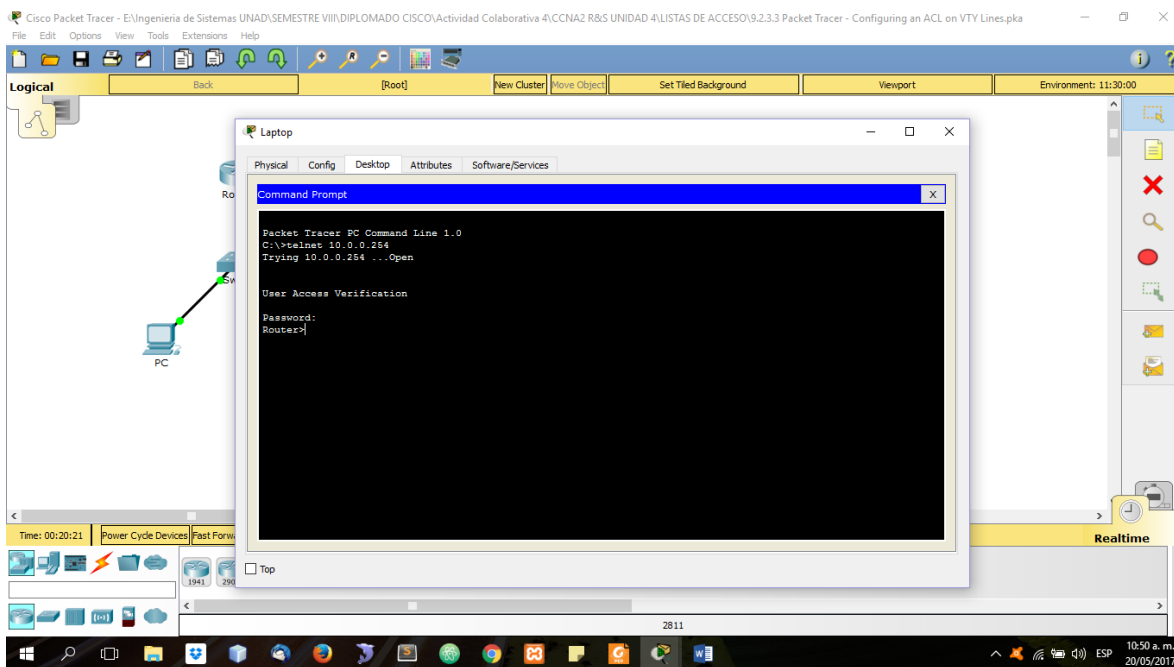
### Step 1: Verify Telnet access before the ACL is configured.

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

Verificado acceso a telnet desde el PC

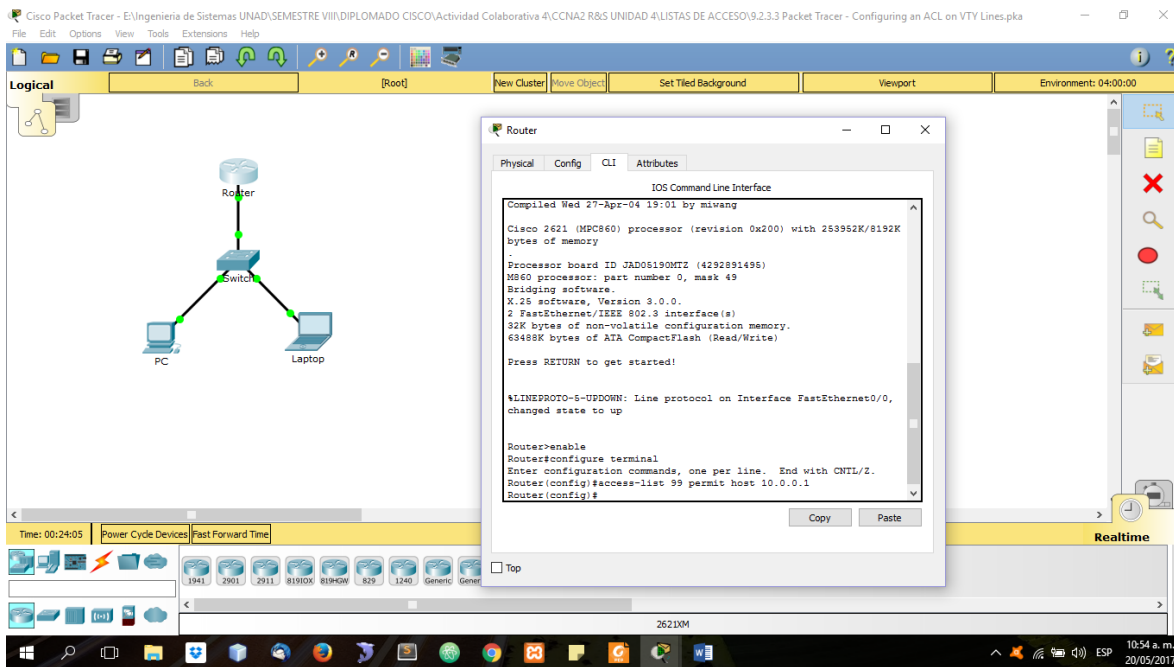


Verificando acceso a telnet desde la Laptop



Paso 2: Configure una ACL estándar numerada.

Configure la siguiente ACL numerada en el enrutador



Debido a que no queremos permitir el acceso desde ninguna otra computadora, la propiedad de denegación implícita del acceso

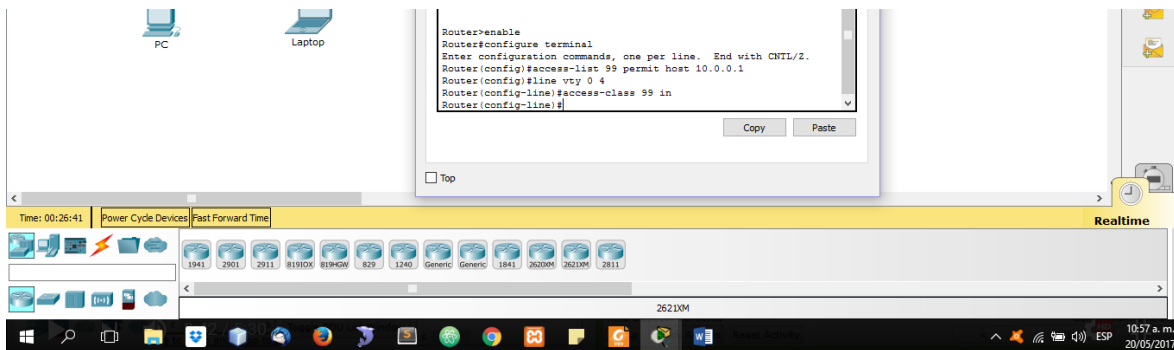
Lista cumple con nuestros requisitos.

Paso 3: Coloque una ACL estándar con nombre en el enrutador.

Se debe permitir el acceso a las interfaces del enrutador, mientras que el acceso Telnet debe estar restringido. Por lo tanto, debemos

Coloque la ACL en las líneas Telnet de 0 a 4. Desde el indicador de configuración de Router, ingrese la configuración de la línea

Para las líneas 0 - 4 y utilice el comando access-class para aplicar la ACL a todas las líneas VTY:

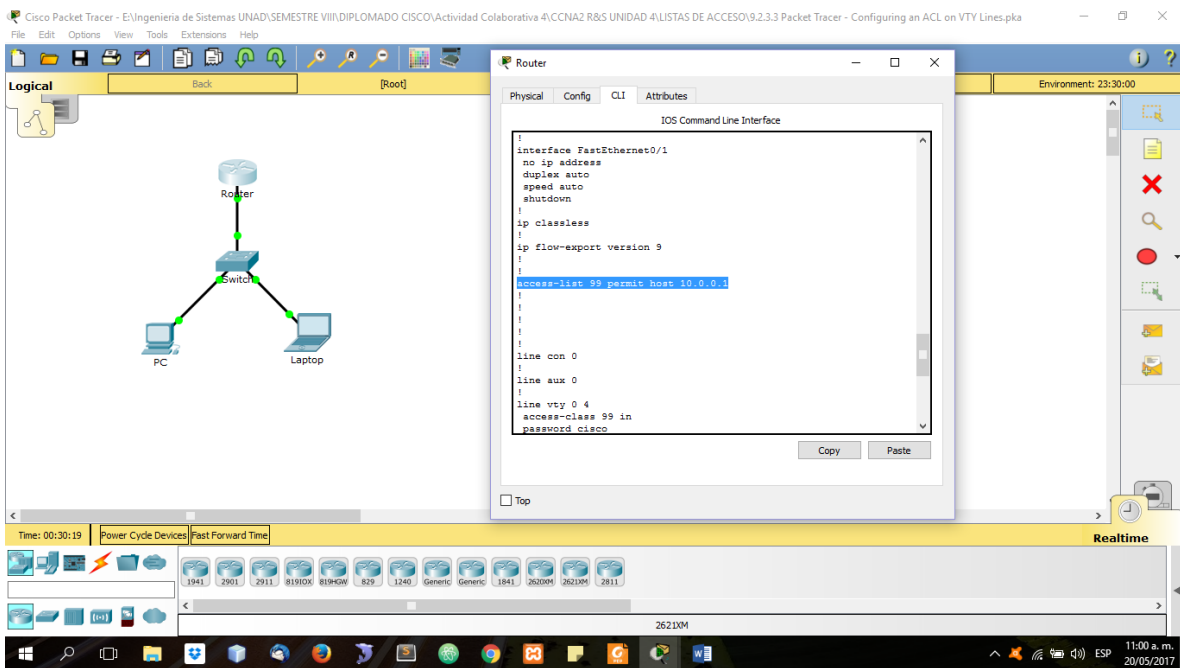
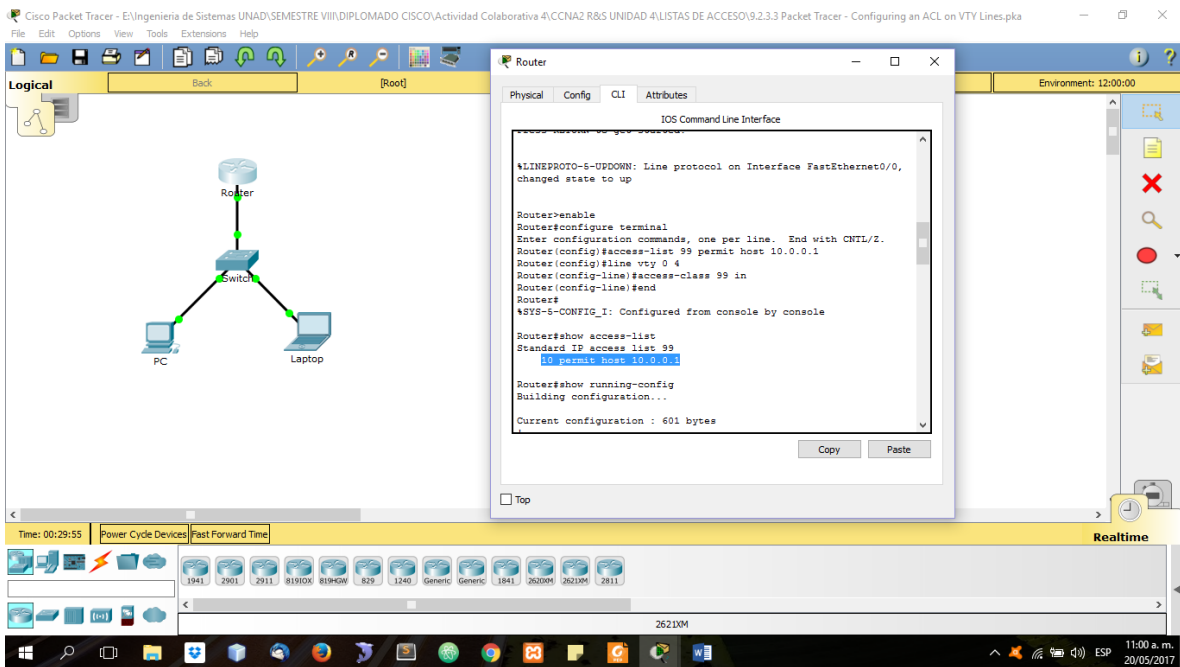


Parte 2: Verificar la implementación del ACL

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

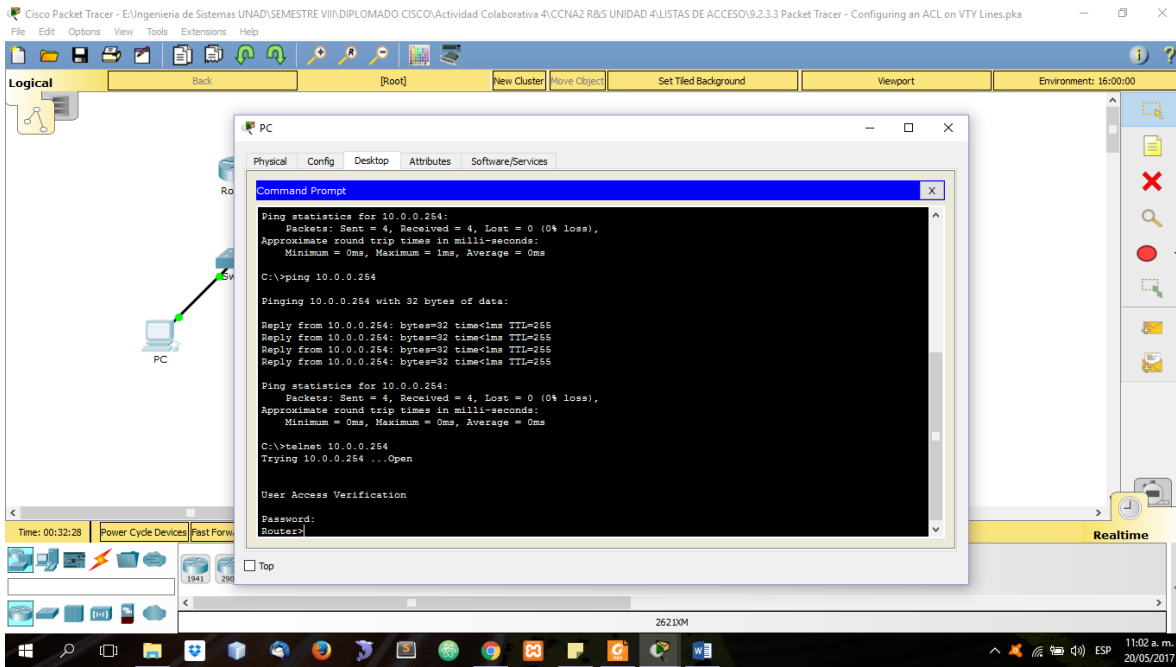
Utilice las listas de acceso a la demostración para verificar la configuración de la ACL. Utilice el comando show run para verificar que la ACL esté

Aplicado a las líneas VTY.



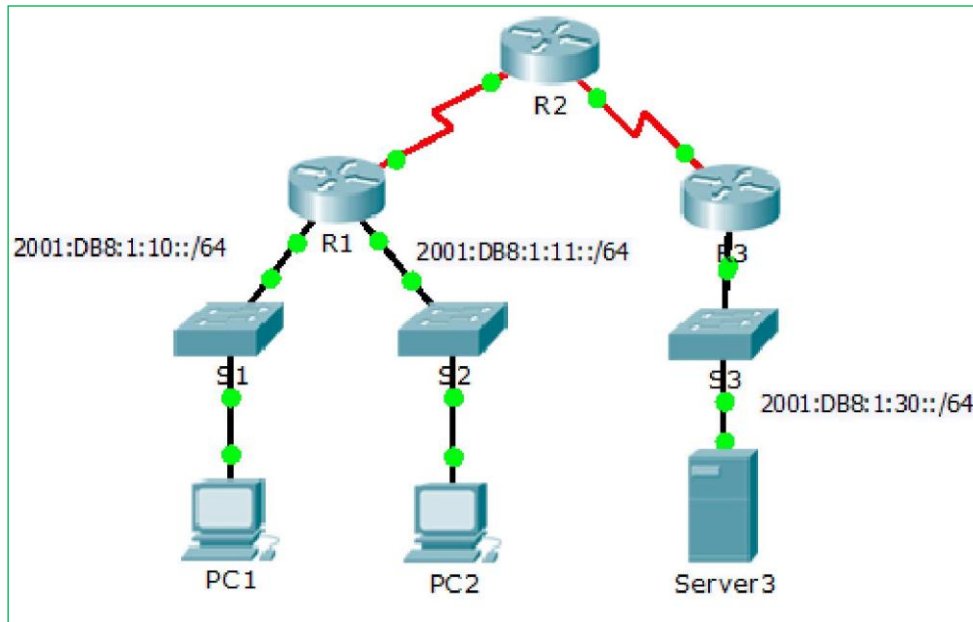
Paso 2: Compruebe que la ACL funciona correctamente.

Ambos equipos deben ser capaces de hacer ping al enrutador, pero sólo la PC debe ser capaz de Telnet a ella.



## 9.5.2.6 -Packet Tracer - Configuring IPv6 ACLs

### Topology



### Addressing Table

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

### Objectives

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

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

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

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

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

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

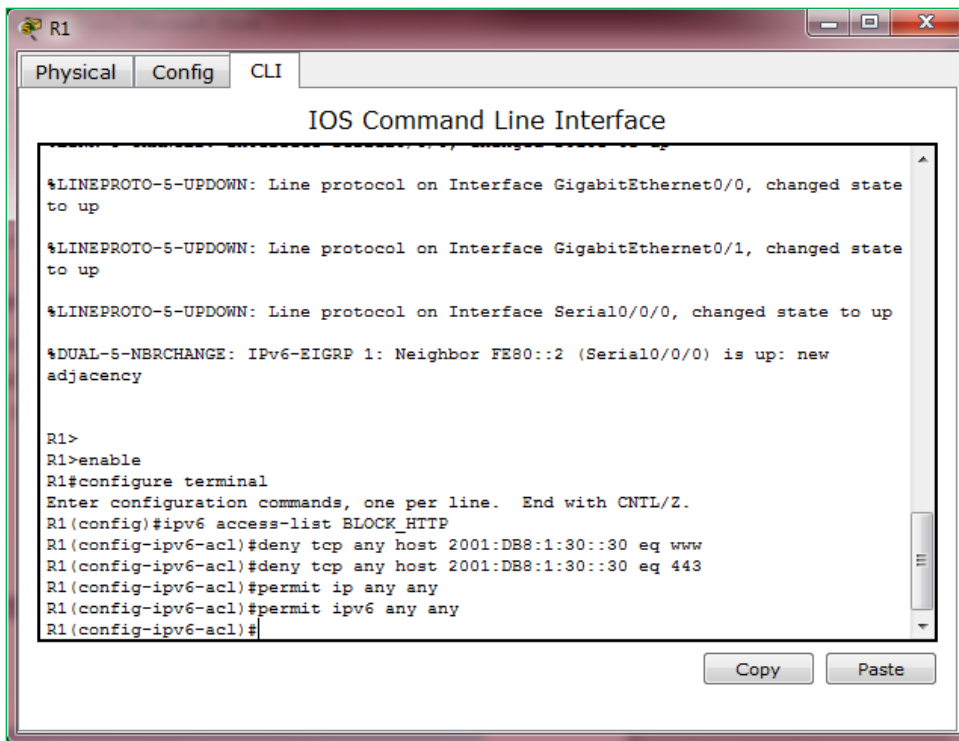
- a. Block HTTP and HTTPS traffic from reaching **Server3**.

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

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

- b. Allow all other IPv6 traffic to pass.

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



```
R1
Physical Config CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::2 (Serial0/0/0) is up: new adjacency

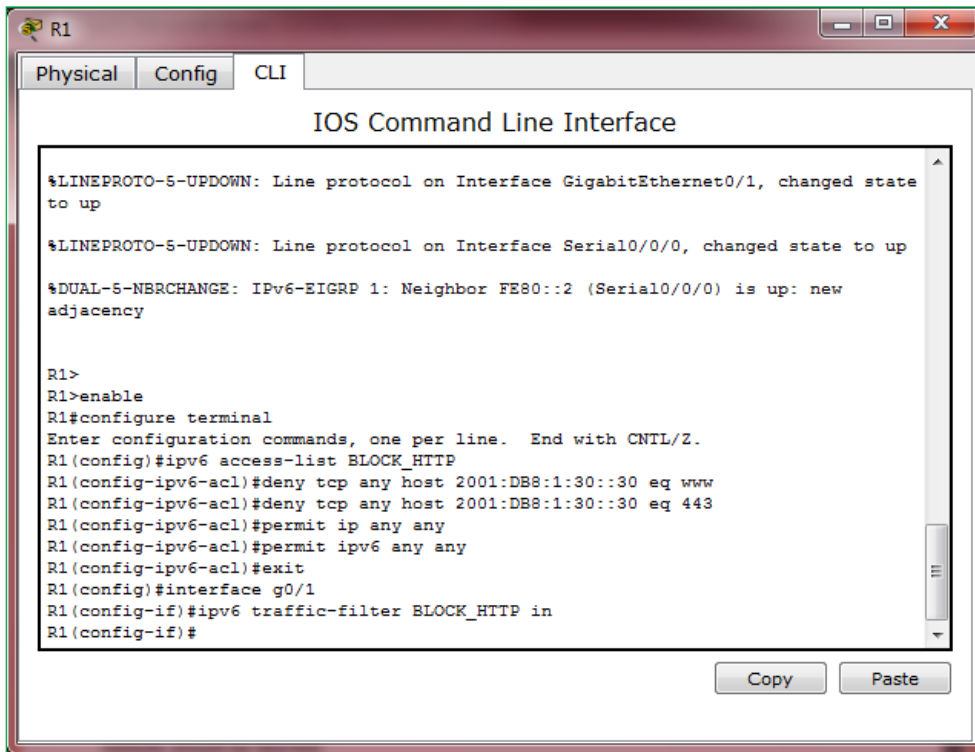
R1>
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ip any any
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#
```

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

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

```
R1(config)# interface GigabitEthernet0/1
```

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```



```
R1
Physical Config CLI
IOS Command Line Interface

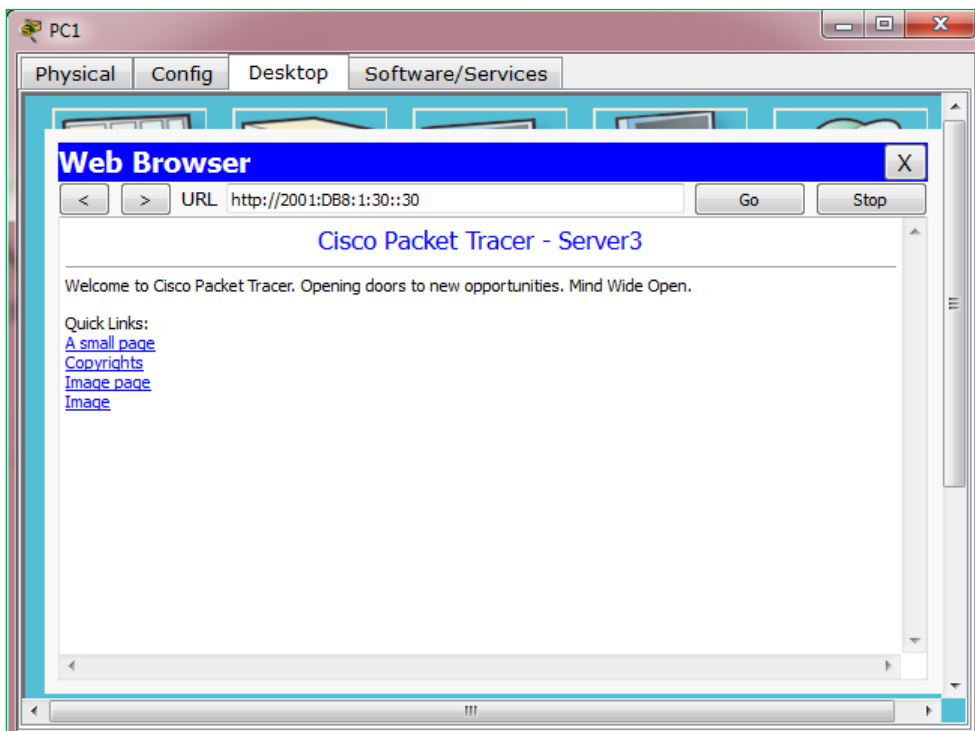
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::2 (Serial0/0/0) is up: new adjacency

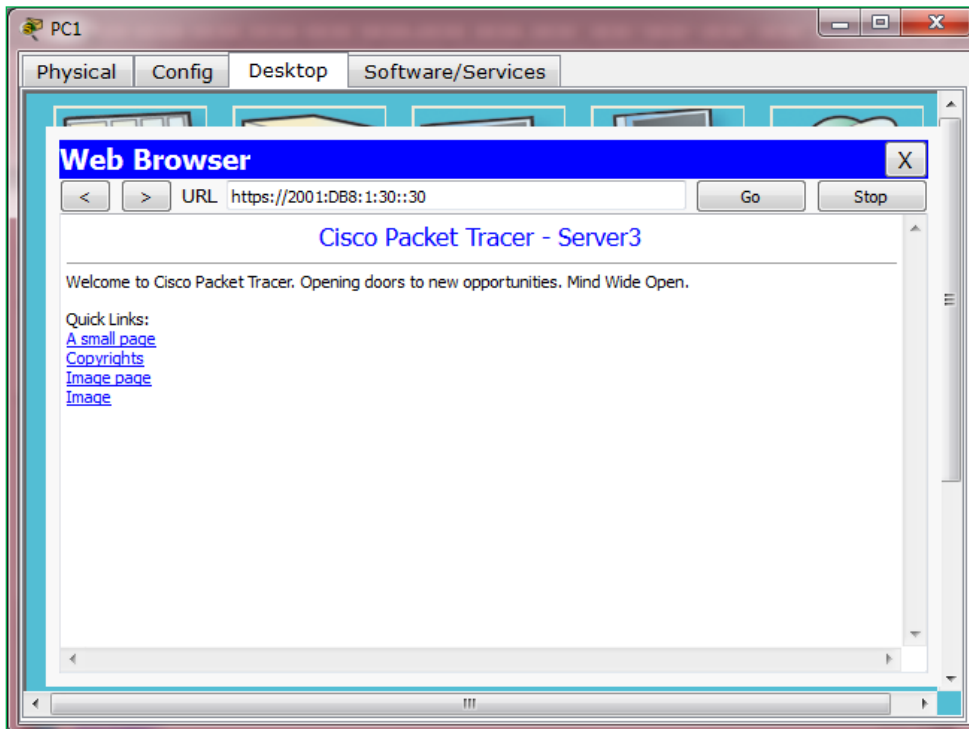
R1>
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ip any any
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#interface g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

### Step 3: Verify the ACL implementation.

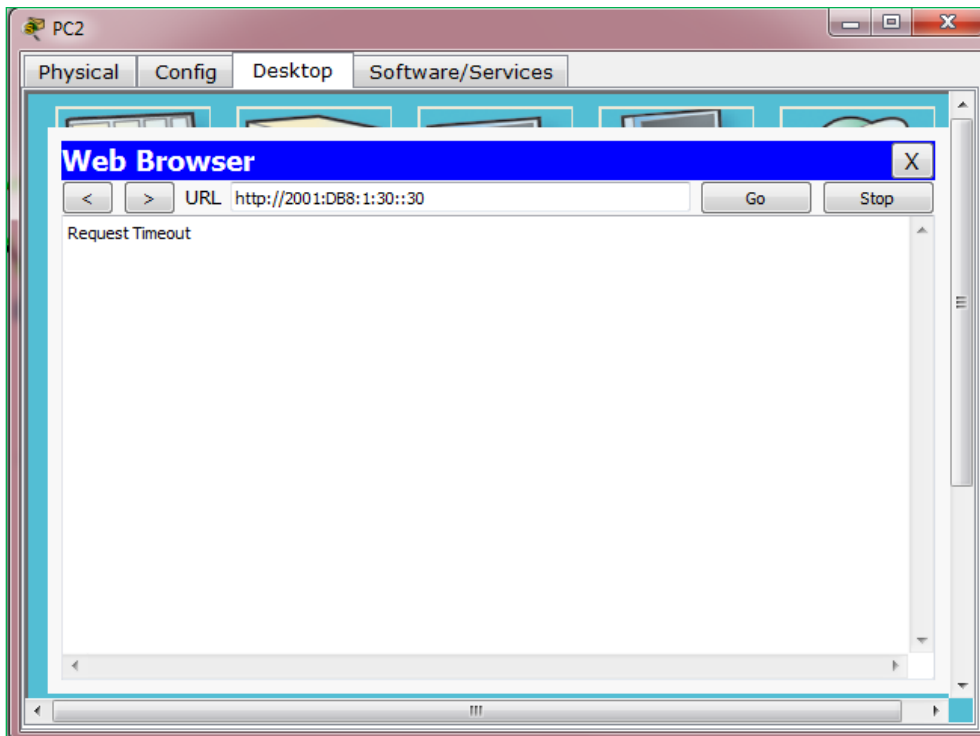
Verify the ACL is operating as intended by conducting the following tests:

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

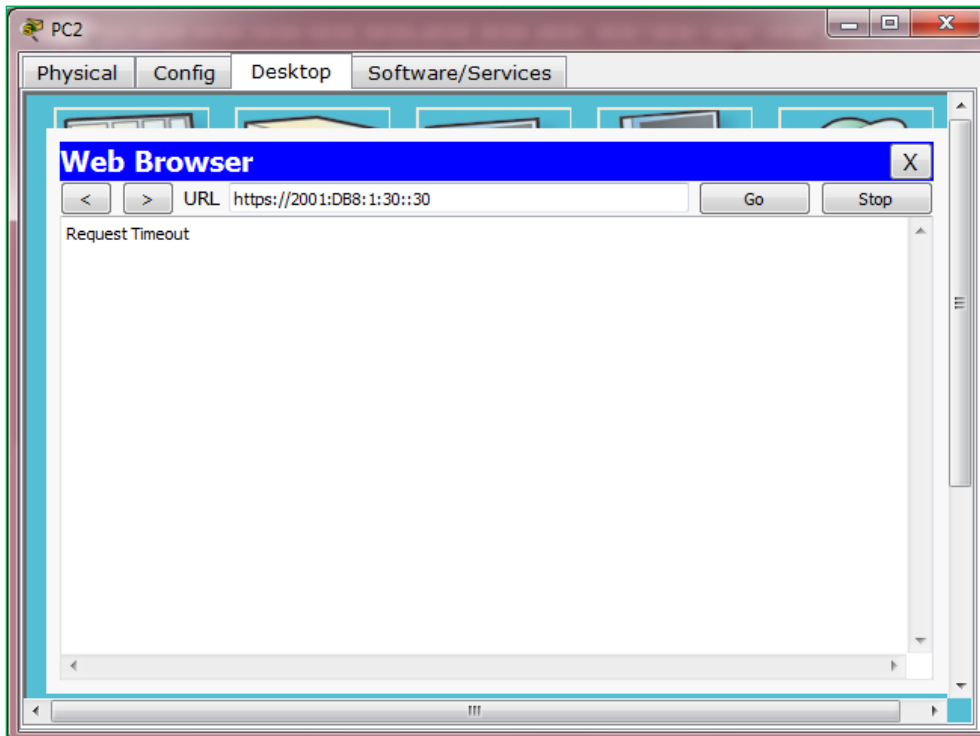




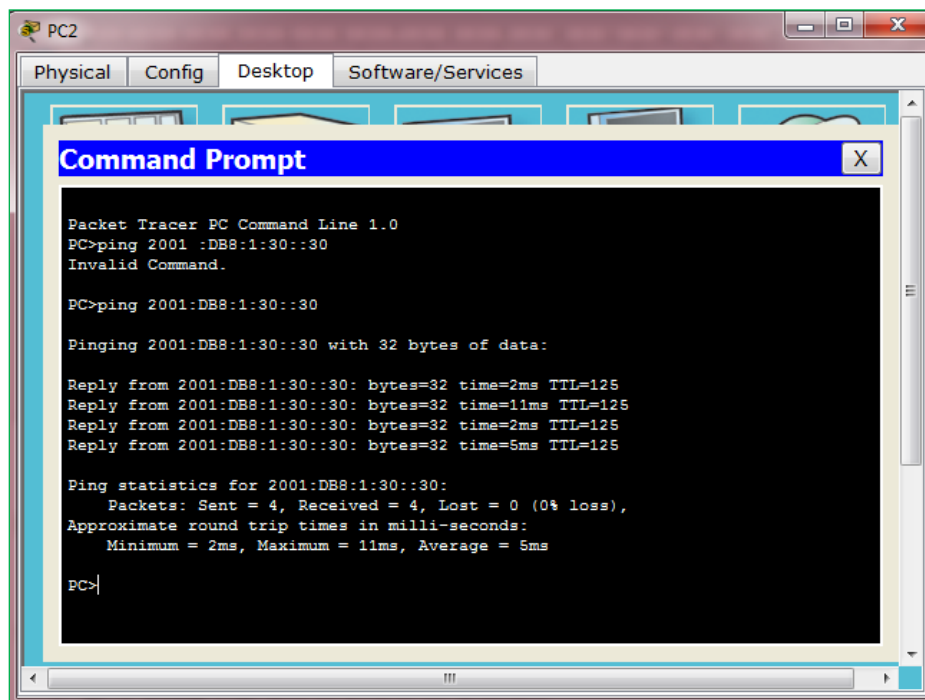
- Open the **web browser** of **PC2** to <http://2001:DB8:1:30::30> or <https://2001:DB8:1:30::30>. The website should be blocked







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



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

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

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

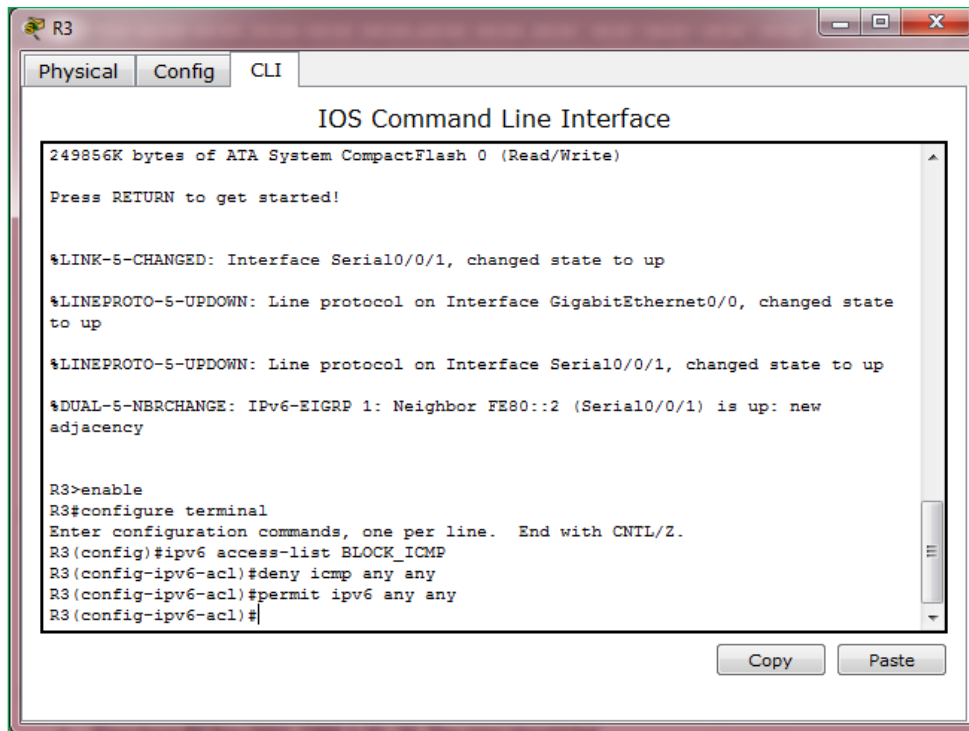
Configure an ACL named **BLOCK\_ICMP** on **R3** with the following statements:

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

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

- b. Allow all other IPv6 traffic to pass.

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



```
R3
Physical Config CLI
IOS Command Line Interface
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!

%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: IPv6-EIGRP 1: Neighbor FE80::2 (Serial0/0/1) is up: new adjacency

R3>enable
R3#configure 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
R3(config-ipv6-acl)#

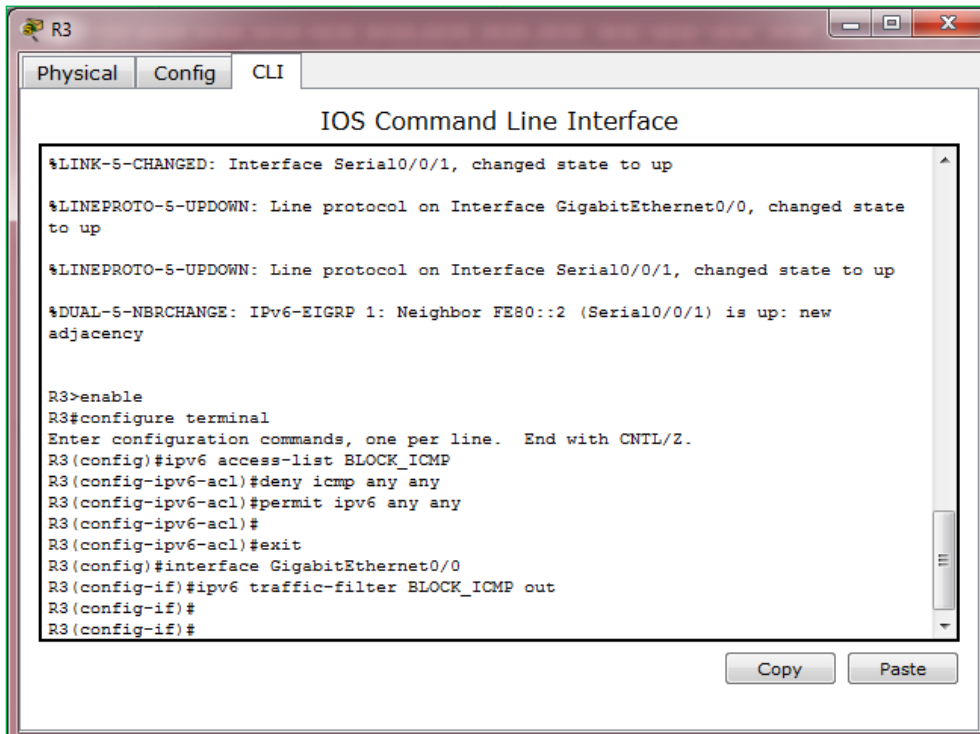
Copy Paste
```

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

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

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

```
R3(config-if)# ipv6 traffic-filter BLOCK_ICMP out
```



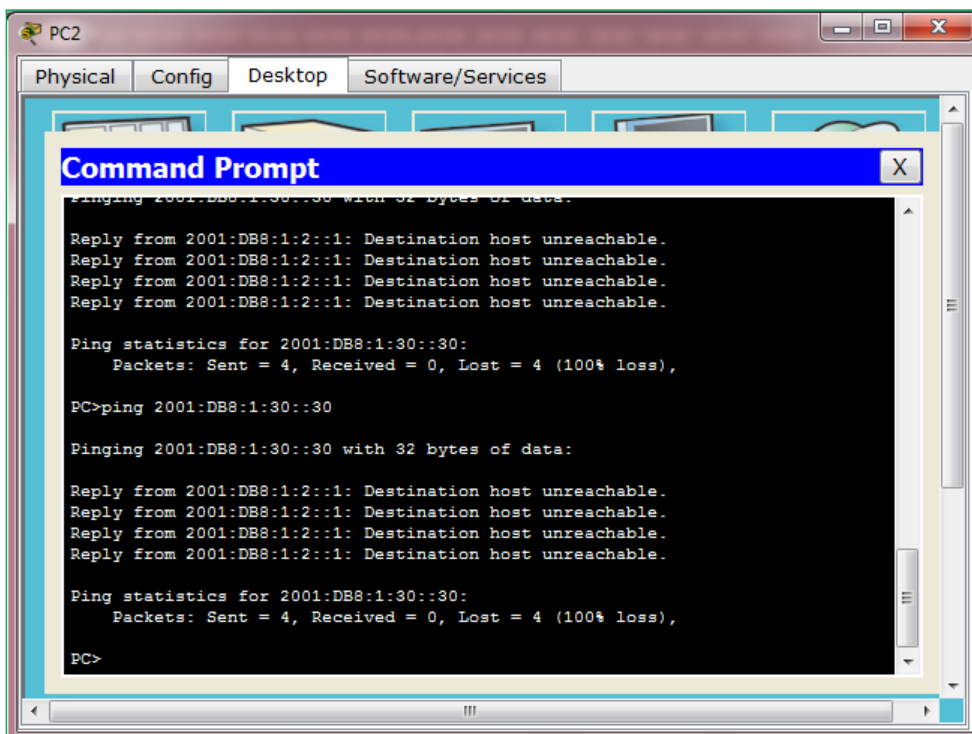
```
R3
Physical Config CLI
IOS Command Line Interface

%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: IPv6-EIGRP 1: Neighbor FE80::2 (Serial0/0/1) is up: new adjacency

R3>enable
R3#configure 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
R3(config-ipv6-acl)#
R3(config-ipv6-acl)#exit
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
R3(config-if)#
```

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

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



```
PC2
Physical Config Desktop Software/Services
Command Prompt

Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

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

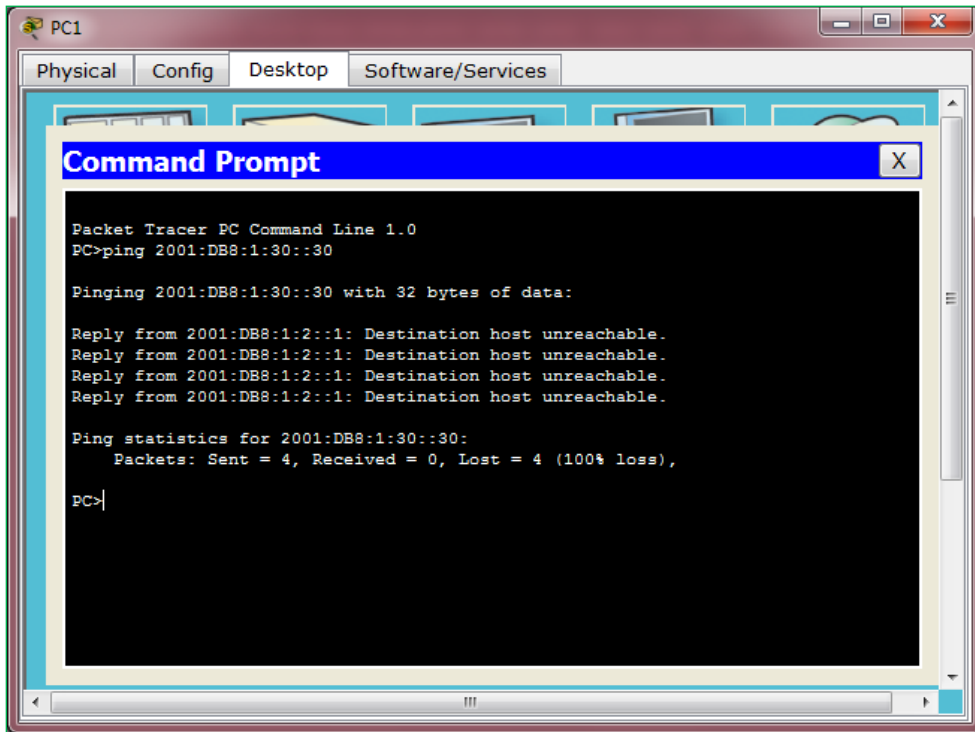
PC>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

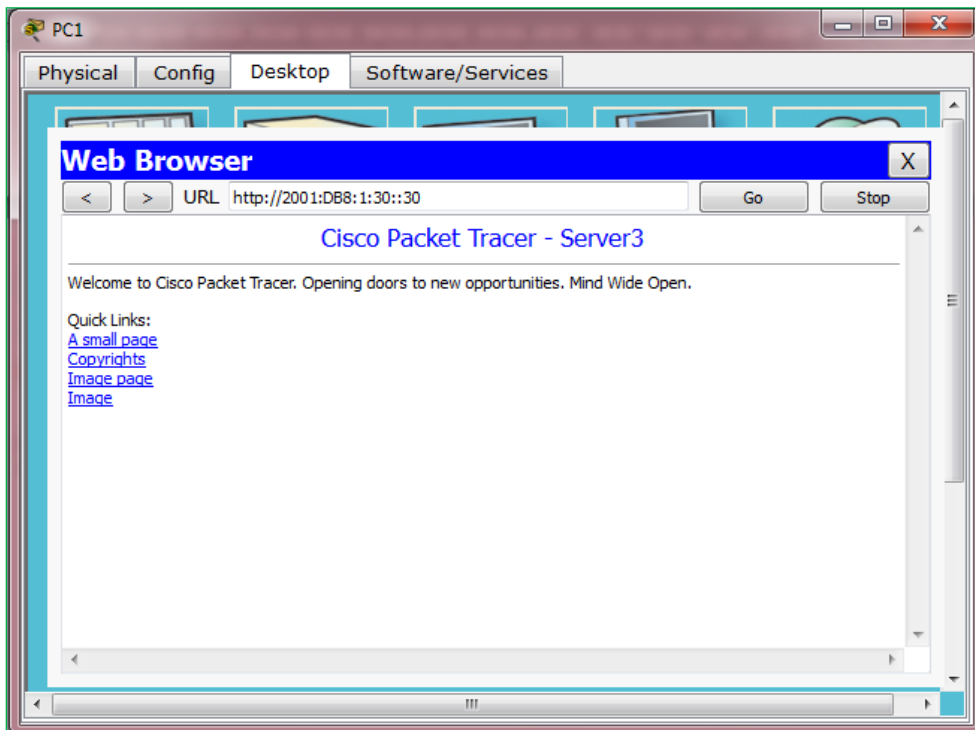
Ping statistics for 2001:DB8:1:30::30:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

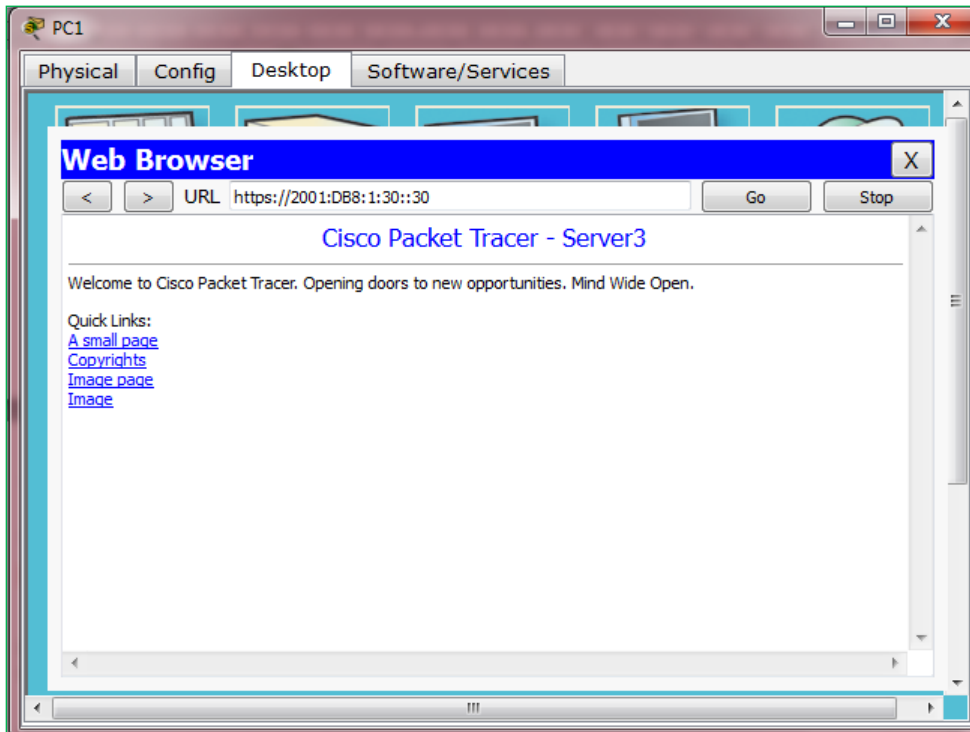
PC>
```

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



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





- Observamos también el simulador y vemos que este se encuentra al 100%.

**Packet Tracer - Configuring IPv6 ACLs**

**Addressing Table**

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

**Objectives**

Part 1: Configure, Apply, and Verify an IPv6 ACL  
 Part 2: Configure, Apply, and Verify a Second IPv6 ACL

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

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing  
 Address Resolution Protocol (ARP) table against Server3. Hosts do not

Time Elapsed: 00:54:05      Completion: 100/100

Top    Check Results    Reset Activity    <    1/1    >

## CONCLUSIÓN.

El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red, y presenta una solución frente al crecimiento de las redes, este protocolo de enrutamiento dinámico es de gran ayuda puesto que permiten a los routers modificar sus tablas de enrutamiento sin la necesidad de intervención del administrador. Se trata de un protocolo cliente-servidor, el DHCP permite la asignación automática de información de direccionamiento, como una dirección IP que permite que los host obtengan su configuración de red de manera totalmente automática, sin que tengamos que configurar IP, máscara de subred y puerta de enlace en cada una de las terminales de nuestra red local.

En esencia los protocolos de enrutamiento dinámico permiten a los routers aprendan a medida que la red cambia, con ello es posible determinar la mejor ruta a la red destino para compartir automáticamente la información acerca de las redes remotas, determinan la mejor ruta para cada red y agregan esta información a sus tablas de enrutamiento, en comparación con el routing estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa.

La configuración del servidor de DHCP requiere que se utilice un bloque de direcciones, para la asignación a los clientes DHCP en una red, las direcciones asignadas a este conjunto deben planificarse de modo que excluyan cualquier dirección estática que utilicen otros dispositivos. DHCP es generalmente el método preferido para asignar direcciones IPv4 a los hosts de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada.

## **BIBLIOGRAFÍAS.**

Lammle, T. (2008). Todd Lammle's CCNA IOS Commands Survival Guide. Indianapolis, Ind: Sybex. <http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=218603&lang=es&site=ehost-live>

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de: <http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxiliary%20materials/Cisco-ICND2.pdf>