

**CCNA2: UNIDAD 4
ACTIVIDAD COLABORATIVA
MOMENTO 6 –ENRUTAMIENTO EN SOLUCIONES DE RED**

**HECTOR NARANJO VILLAMIZAR- 85463791
JOSE GREGORIO REYES- 7380754
SIRELYS JIMÉNEZ ESCORCIA-1082880422
WILDER MANUEL BRAVO-78381004
CURSO 203092 GRUPO 42
ESTUDIANTES**

**EDGAR RODRIGO ENRÍQUEZ ROSERO
TUTOR DE CURSO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN
DE SOLUCIONES INTEGRADAS LAN / WAN)
INGENIERIA DE SISTEMAS
DICIEMBRE 6 2016**

INTRODUCCION

Esta actividad comprende los alcances de configuración y administración del IOS en terminales de enrutamiento iguales con cada una de las políticas que rigen el comportamiento de la red de datos de igual forma comprende la arquitectura de Redes de Cisco para implementar niveles básicos de seguridad al interior de redes corporativas. En este trabajo se encontrara la práctica desarrollada mediante el uso de la herramienta de Simulación **PACKET TRACER** el Enrutamiento en soluciones de red: el cual contiene enrutamiento dinámico, OSPF de una sola área, listas de control de acceso, DHCP y traducción de direcciones IP para IPv4. Estudiado en la unidad cuatro del diplomado de profundización Cisco.

El enrutamiento es el paso de reenviar paquetes entre redes, constantemente buscando la mejor ruta (la más corta). Para hallar esa ruta más óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda. Ningún paquete puede ser enviado sin una ruta. La ruta es elegida según el protocolo de enrutamiento que se utilice. El dispositivo primario que realiza el proceso de enrutamiento es el Router.

Entre los tipos de enrutamiento encontramos Estático es aquel en la cual los Hosts y redes de tamaño reducido que obtienen las rutas de un enrutador predeterminado y enrutadores predeterminados que sólo necesitan conocer uno o dos enrutadores en los siguientes saltos. Dinámico podríamos decir que son Interredes de mayor tamaño, enrutadores en redes locales con múltiples hosts y hosts de sistemas autónomos de gran tamaño. El enrutamiento dinámico es la mejor opción para los sistemas en la mayoría de las redes. Estático y dinámico combinados, es aquel en la cual los enrutadores que conectan una red con enrutamiento estático y una red con enrutamiento dinámico y enrutadores de límite que conectan un sistema autónomo interior con redes externas. La combinación del enrutamiento estático y dinámico en un sistema es una práctica habitual.

En este trabajo el estudiante hará prácticas con relación a Enrutamiento Dinámico, OSPF de una sola área, Listas de control de acceso, DHCP, Traducción de direcciones IP para IPv4

Así mismo, con la implementación de estos temas se puede compartir y crecer interpersonalmente con los compañeros de aula situados en otras ciudades del país, es claro que no hay impedimentos de tiempo y espacio. Por ende, Es primordial asimilar la teoría, participar, exponer e intercambiar ideas y poner en práctica las diversas actividades expuestas en el Diplomado, porque éstas abrirán paso a la experiencia y al cumplimiento de los logros propuestos.

La actividad está desarrollada y explicada a través de imágenes, archivos pka, haciéndolo más fácil para el lector. Se agradecen las críticas y sugerencias constructivas las cuales se tendrán en cuenta para el enriquecimiento de nuestros conocimientos.

7.3.2.4 CONFIGURACIÓN BÁSICA DE RIPV2 Y RIPNG

7.3.2.4 PACKET TRACER - CONFIGURACIÓN BÁSICA DE RIPV2 Y RIPNG

Topología

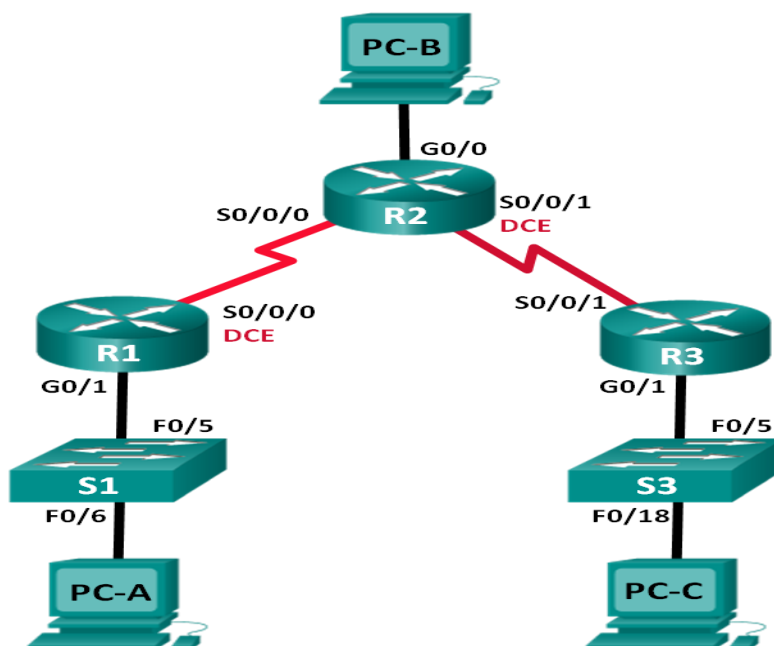


Tabla de direccionamiento

| 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 RIPv2. Luego, configurará la topología de la red con direcciones IPv6, configurará RIPv2, propagará una ruta predeterminada y usará comandos de CLI para ver y verificar la información de routing RIPv2.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión

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

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

Recursos necesarios

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

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

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos. Realizar el cableado de red tal como se muestra en la topología.

Paso 1. inicializar y volver a cargar el router y el switch.

Paso 2. 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.

Part 2: configurar los equipos host.

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

Part 3: 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.

```
PC>ipconfig /all
```

```
FastEthernet0 Connection:(default port)
Physical Address.....: 0009.7C6A.46B9
Link-local IPv6 Address.....: FE80::209:7CFF:FE6A:46B9
IP Address.....: 172.30.10.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 172.30.10.1
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
```

```
PC>ping 172.30.10.1
```

```
Pinging 172.30.10.1 with 32 bytes of data:
```

```
Reply from 172.30.10.1: bytes=32 time=82ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
```

```
Ping statistics for 172.30.10.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 82ms, Average = 20ms
```

```
PC>
```

```
PC>ipconfig /all
```

```
FastEthernet0 Connection:(default port)
Physical Address.....: 000D.BDE0.E8AB
Link-local IPv6 Address.....: FE80::20D:BDFF:FEE0:E8AB
IP Address.....: 209.165.201.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 209.165.201.1
DNS Servers.....: 0.0.0.0
```


DHCP Servers.....: 0.0.0.0

PC>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time=2ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.201.1:

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

PC>

PC>ipconfig /all

FastEthernet0 Connection:(default port)
Physical Address.....: 0001.96D0.B509
Link-local IPv6 Address.....: FE80::201:96FF:FED0:B509
IP Address.....: 172.30.30.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 172.30.30.1
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0

PC>ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

Reply from 172.30.30.1: bytes=32 time=2ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.30.30.1:

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

PC>

- 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.

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

```
R1# config t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# passive-interface g0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```

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

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

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 209.165.201.1
R2(config-router)#network 10.1.1.2
R2(config-router)#network 10.2.2.2
R2(config-router)#no auto-summary
```

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

```
R3 (config) #router rip
R3 (config-router) #version 2
R3 (config-router) #network 172.30.30.1
R3 (config-router) #network 10.2.2.1
R3 (config-router) #passive-interface g0/1
R3 (config-router) #no auto-summary
```

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

Paso 2. examinar el estado actual de la red.

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

```
R2# show ip interface brief
Interface                IP-Address      OK? Method Status
Protocol
```

```

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

```

b. Verifique la conectividad entre las computadoras.

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

NO ¿Por qué? R2 no está distribuyendo la información de PC-B.

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

NO ¿Por qué? el R1 y el R3 no tienen rutas a las subredes específicas en el router remoto.

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

NO ¿Por qué? R2 no está distribuyendo la información de PC-B.

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

NO ¿Por qué? R1 y el R3 no tienen rutas para las subredes especificadas.

c. Verifique que RIPv2 se ejecute en los routers.

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

```

R1# show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv  Triggered RIP  Key-chain
  Serial0/0/0         2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway            Distance      Last Update

```

```
10.1.1.2          120
Distance: (default is 120)
```

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

sending v2 update to 224.0.0.9 via GigabitEthernet0/0 (209.165.201.1)

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

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

router rip
version 2

d.

Examinar el sumarización automática de las rutas.

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

```
R2# show ip route
<Output Omitted>
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
          [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

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

```
R1# show ip route
<Output Omitted>
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
```

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

```
R3# show ip route
```

```
<Output Omitted>
```

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

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

172.30.0.0/16

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

Paso 3. Desactivar la sumarización automática.

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

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

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

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

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

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

```
R2# show ip route
```

```
<Output Omitted>
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
```

```
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**

<Output Omitted>

Gateway of last resort is not set

```
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
R    10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R    172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0
```

R3# **show ip route**

<Output Omitted>

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

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

R2# **debug ip rip**

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

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

172.30.30.0/24

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

S/

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

- j. 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
```

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

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

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

Paso 5. Verificar la configuración de enrutamiento.

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

```
R1# show ip route
```

```
<Output Omitted>
```

```
Gateway of last resort is 10.1.1.2 to network 0.0.0.0
```

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

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

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

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

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

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

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

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

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

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

Hay un Gateway de último recurso, y la ruta predeterminada aparece en la tabla como detectada a través de RIP.

m. Consulte la tabla de routing en el 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 209.165.201.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
    172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:15, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:06, Serial0/0/1
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
S*    0.0.0.0/0 [1/0] via 209.165.201.2
R2#
```

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

El R2 tiene una ruta estática predeterminada a 0.0.0.0 a través de 209.165.201.2, la cual está conectada directamente a 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.

```
PC>ping 209.165.201.2
```

```
Pinging 209.165.201.2 with 32 bytes of data:
```

```
Reply from 209.165.201.2: bytes=32 time=2ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=4ms TTL=126
Reply from 209.165.201.2: bytes=32 time=10ms TTL=126
```

```
Ping statistics for 209.165.201.2:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 4ms
```

```
PC>
```

```
PC>ping 209.165.201.2
```

```
Pinging 209.165.201.2 with 32 bytes of data:
```

```
Reply from 209.165.201.2: bytes=32 time=2ms TTL=126
```



```
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>
```

¿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

```
PC>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.30.3: bytes=32 time=25ms TTL=125
Reply from 172.30.30.3: bytes=32 time=12ms TTL=125
Reply from 172.30.30.3: bytes=32 time=13ms TTL=125
Reply from 172.30.30.3: bytes=32 time=11ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 25ms, Average = 15ms
PC>
```

```
PC>ping 172.30.10.3
Pinging 172.30.10.3 with 32 bytes of data:
Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Reply from 172.30.10.3: bytes=32 time=11ms TTL=125
Reply from 172.30.10.3: bytes=32 time=11ms TTL=125
Reply from 172.30.10.3: bytes=32 time=11ms TTL=125

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms
PC>
```

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

Parte 3: configurar IPv6 en los dispositivos

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

Tabla de direccionamiento

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

Paso 7. configurar los equipos host.

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

Paso 8. configurar IPv6 en los routers.

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

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

show ipv6 interface brief

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

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

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 9. 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.

- g. 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
```

- h. 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(config)#interface s0/0/0
R2(config-if)#ipv6 rip test2 enable
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 rip test2 enable
R2(config-if)#
```

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

```
R3(config)#interface g0/1
R3(config-if)#ipv6 rip test3 enable
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 rip test3 enable
R3(config-if)#
```

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

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

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
```

```
IPv6 Routing Protocol is "rip Test1"
  Interfaces:
    Serial0/0/0
    GigabitEthernet0/1
  Redistribution:
    None
```

¿En qué forma se indica RIPng en el resultado?

RIPng se indica por medio del nombre de proceso.

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

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

Interfaces:

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

Este Comando no es soportado por Packet Tracer.

¿Cuáles son las similitudes entre RIPv2 y RIPng?

RIPv2 y RIPng:

Tienen una distancia administrativa de 120.

Usan el conteo de saltos como métrica.

Envían actualizaciones cada 30 segundos.

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

Show ipv6 route

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

```
R 2001:DB8:ACAD:C::/64 [120/3]
  via FE80::2, Serial0/0/0
C 2001:DB8:ACAD:12::/64 [0/0]
  via ::, Serial0/0/0
L 2001:DB8:ACAD:12::1/128 [0/0]
  via ::, Serial0/0/0
R 2001:DB8:ACAD:23::/64 [120/2]
  via FE80::2, Serial0/0/0
L FF00::/8 [0/0]
  via ::, Null0
R1#
```

```
R2#show ipv6 route
```

```
IPv6 Routing Table - 9 entries
```

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

```
U - Per-user Static route, M - MIPv6
```

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

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

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

```
D - EIGRP, EX - EIGRP external
```

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

```
R3#show ipv6 route
```

```
IPv6 Routing Table - 7 entries
```

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

```
U - Per-user Static route, M - MIPv6
```

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

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

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

```
D - EIGRP, EX - EIGRP external
```

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

```
via FE80::2, Serial0/0/1
C 2001:DB8:ACAD:23::/64 [0/0]
via ::, Serial0/0/1
L 2001:DB8:ACAD:23::3/128 [0/0]
via ::, Serial0/0/1
L FF00::/8 [0/0]
via ::, Null0
R3#
```

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

m. Verifique la conectividad entre las computadoras.

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

```
PC>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

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

```
Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=4ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=13ms TTL=125
Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 13ms, Average = 10ms
PC>
```

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

```
PC>ping 2001:DB8:ACAD:B::B
Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:
```

```
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

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

```
PC>ping 2001:DB8:ACAD:A::A
Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=24ms TTL=125
Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 24ms, Average = 14ms
PC>
```

¿Por qué algunos pings tuvieron éxito y otros no?

Porque el router 2 no está anunciando ninguna ruta a la red 2001:DB8:ACAD:B::/64.

Paso 10. configurar y volver a distribuir una ruta predeterminada.

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

R2(config)# ipv6 route ::0/64 2001:db8:acad:b::2

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

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

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

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

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

Paso 11. Verificar la configuración de enrutamiento.

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

```
R2# show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/64 [1/0]
    via 2001:DB8:ACAD:B::B
R   2001:DB8:ACAD:A::/64 [120/2]
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
    via ::, GigabitEthernet0/1
L   2001:DB8:ACAD:B::2/128 [0/0]
    via ::, GigabitEthernet0/1
R   2001:DB8:ACAD:C::/64 [120/2]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via ::, Serial0/0/0
L   2001:DB8:ACAD:12::2/128 [0/0]
    via ::, Serial0/0/0
C   2001:DB8:ACAD:23::/64 [0/0]
    via ::, Serial0/0/1
L   2001:DB8:ACAD:23::2/128 [0/0]
    via ::, Serial0/0/1
L   FF00::/8 [0/0]
    via ::, Null0
```

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

S ::/64 [1/0] via 2001:DB8:ACAD:B::B

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

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

La ruta predeterminada aparece como una ruta RIPng distribuida con el valor de métrica 2.

R1:

R ::/0 [120/2] via FE80::2, Serial0/0/0

```
R1#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
```


U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external

```
R ::/0 [120/1]
  via FE80::2, Serial0/0/0
C 2001:DB8:ACAD:A::/64 [0/0]
  via ::, GigabitEthernet0/1
L 2001:DB8:ACAD:A::1/128 [0/0]
  via ::, GigabitEthernet0/1
R 2001:DB8:ACAD:C::/64 [120/3]
  via FE80::2, Serial0/0/0
C 2001:DB8:ACAD:12::/64 [0/0]
  via ::, Serial0/0/0
L 2001:DB8:ACAD:12::1/128 [0/0]
  via ::, Serial0/0/0
R 2001:DB8:ACAD:23::/64 [120/2]
  via FE80::2, Serial0/0/0
L FF00::/8 [0/0]
  via ::, Null0
R1#
```

R3:

R ::/0 [120/2] via FE80::2, Serial0/0/1

R3#show ipv6 route

IPv6 Routing Table - 8 entries

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

U - Per-user Static route, M - MIPv6

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

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

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

D - EIGRP, EX - EIGRP external

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

Verifique la conectividad.

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

¿Tuvieron éxito los pings? SI

Reflexión

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

Esto se hace porque los routers resumen las rutas en los límites automáticamente.

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

Por las actualizaciones de routing RIP recibidas del router en el que estaba configurada la ruta predeterminada (R2).

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

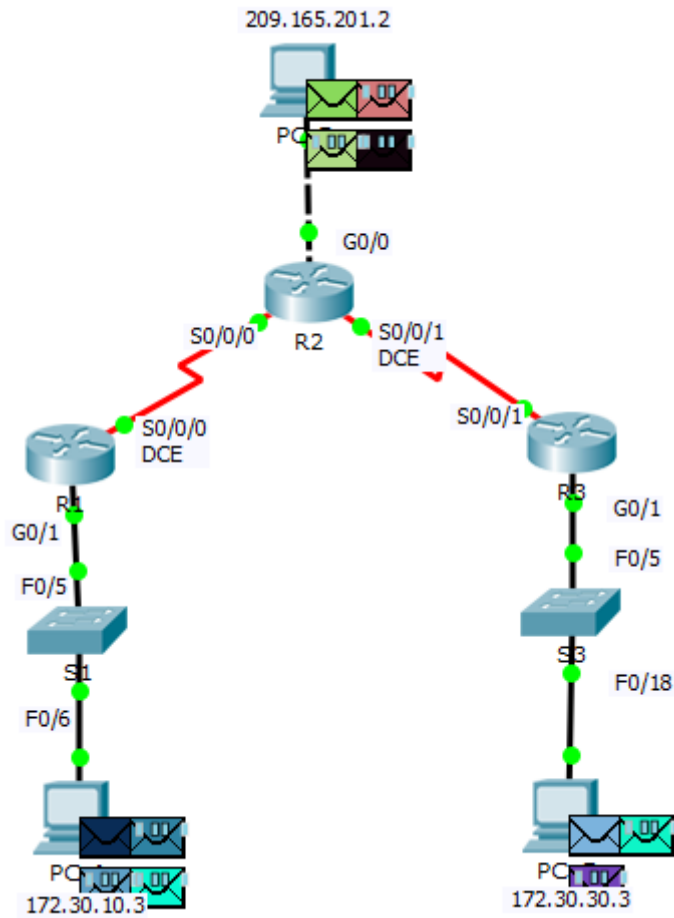
RIPv2 se configura mediante instrucciones network.

RIPv6 se configura en las interfaces.

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.



| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|------|-------------|--------|-------------|------|-------|-----------|----------|-----|--------|--------|
| | Successful | PC-B | R1 | ICMP | | 0.000 | N | 0 | (edit) | |
| | Successful | PC-B | R3 | ICMP | | 0.000 | N | 1 | (edit) | |
| | Successful | PC-B | PC-C | ICMP | | 0.000 | N | 2 | (edit) | |
| | Successful | PC-B | PC-A | ICMP | | 0.000 | N | 3 | (edit) | |
| | Successful | PC-A | PC-C | ICMP | | 0.000 | N | 4 | (edit) | |
| | Successful | PC-A | R3 | ICMP | | 0.000 | N | 5 | (edit) | |
| | Successful | PC-A | R2 | ICMP | | 0.000 | N | 6 | (edit) | |
| | Successful | PC-A | PC-B | ICMP | | 0.000 | N | 7 | (edit) | |
| | Successful | PC-C | R1 | ICMP | | 0.000 | N | 8 | (edit) | |
| | Successful | PC-C | PC-B | ICMP | | 0.000 | N | 9 | (edit) | |
| | Successful | PC-C | R3 | ICMP | | 0.000 | N | 10 | (edit) | |

8.2.4.5 CONFIGURACIÓN DE OSPFV2 BÁSICO DE ÁREA ÚNICA

8.2.4.5 CONFIGURACIÓN DE OSPFV2 BÁSICO DE ÁREA ÚNICA

Topología

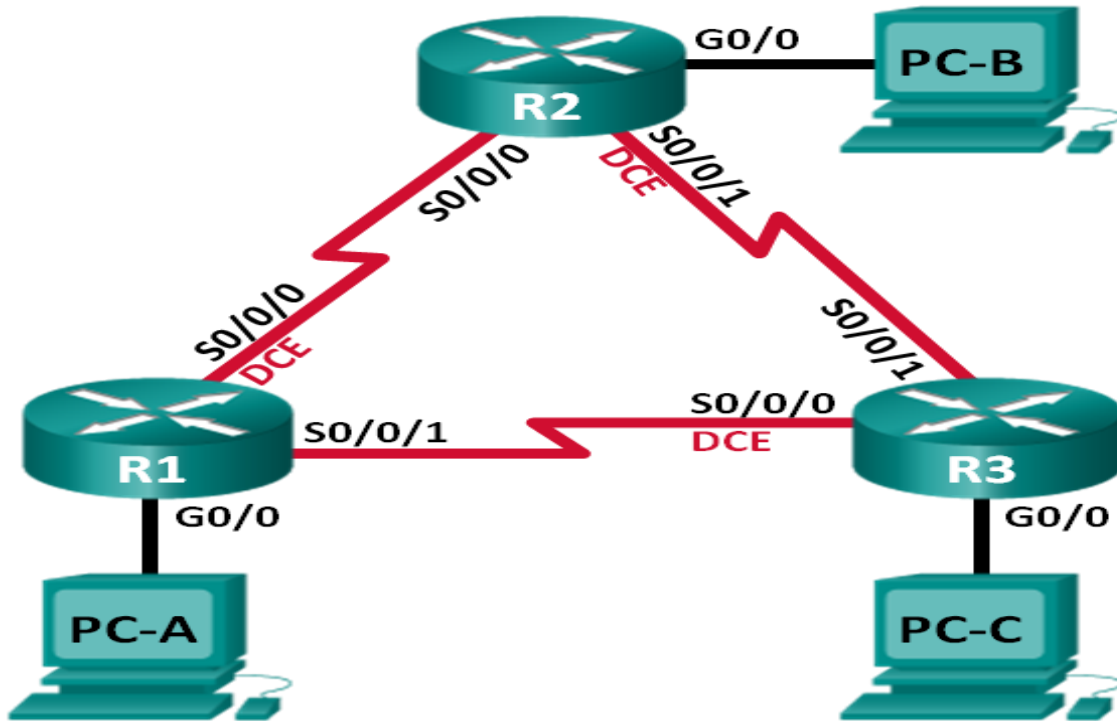


Tabla de direccionamiento

| 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

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

Parte1. 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.

Step 2: realizar el cableado de red tal como se muestra en la topología.

Step 3: inicializar y volver a cargar los routers según sea necesario.

Step 4: configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de 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

Step 5: configurar los equipos host.

Step 6: 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.

Part 4: 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.

Step 1: Configure el protocolo OSPF en R1.

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

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

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

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

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

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

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

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

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

```
R1#
```

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

```
R1#
```

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

```
R1#
```

Step 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/ | - | 00:00:39 | 192.168.12.2 | Serial0/0/0 |
| 192.168.23.2 | 0 | FULL/ | - | 00:00:35 | 192.168.13.2 | Serial0/0/1 |

```
R1#
```

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

```
R1# show ip route
```

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

```
Gateway of last resort is not set
```

```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.1/32 is directly connected, Serial0/0/0
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/1
L    192.168.13.1/32 is directly connected, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
    [110/128] via 192.168.13.2, 00:31:38, Serial0/0/1
```



```

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

Gateway of last resort is not set

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

```

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

show ip route ospf

Step 4: verificar la configuración del protocolo OSPF.

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

```

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

```

```

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

```

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

Distance: (default is 110)

```

R1#show ip protocols

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

R1#

```

Step 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 9 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x01b5a9
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
R1#
```

Step 6: verificar la configuración de la interfaz OSPF.

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

```
R1# show ip ospf interface brief
```

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

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

```
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)
```

Step 7: Verificar la conectividad de extremo a extremo.

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

```
PC>ping 192.168.2.3
```

```
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

```
PC>ping 192.168.3.3
```

```
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

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

Part 5: 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.

Step 1: Cambie las ID de router con direcciones de loopback.

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

```
R1(config)# interface lo0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```

```
R1(config)#interface lo0

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

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

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

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

```
R2(config)#interface lo0

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

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

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

```

R3(config)#interface lo0

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

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

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

```

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

```

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

```

```

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3          110          00:01:00
    2.2.2.2          110          00:01:14
  Distance: (default is 110)

```

```

R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:00:08
    192.168.13.1     110          00:23:52
    192.168.23.1     110          00:01:04
    192.168.23.2     110          00:00:08
  Distance: (default is 110)

R1#

```

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

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

```
Neighbor ID      Pri   State           Dead Time   Address      Interface
3.3.3.3          0    FULL/ -         00:00:35   192.168.13.2
Serial0/0/1
2.2.2.2          0    FULL/ -         00:00:32   192.168.12.2
Serial0/0/0
R1#
```

```
R1#show ip ospf neighbor

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

Step 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(config)#
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
```

- 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
```



```
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
```

- 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 protoco
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1         110          00:20:55
    2.2.2.2         110          00:08:21
    3.3.3.3         110          00:07:35
    11.11.11.11     110          00:00:10
    22.22.22.22     110          00:00:09
    33.33.33.33     110          00:00:10
    192.168.13.1    110          00:48:49
    192.168.23.1    110          00:26:00
    192.168.23.2    110          00:21:38
  Distance: (default is 110)
R1#
```

- 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 |
|-------------|-----|---------|-----------|--------------|-------------|
| 22.22.22.22 | 0 | FULL/ - | 00:00:30 | 192.168.12.2 | Serial0/0/0 |
| 33.33.33.33 | 0 | FULL/ - | 00:00:30 | 192.168.13.2 | Serial0/0/1 |

```
R1#
```

Part 6: 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.

Step 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 11.11.11.11, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:04
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
R1#
```

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

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

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

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

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

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

```
R2# show ip route
```

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

```
Gateway of last resort is not set
```

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

```
C    192.168.23.0/30 is directly connected, Serial0/0/1
L    192.168.23.1/32 is directly connected, Serial0/0/1
```

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

Gateway of last resort is not set

    2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.12.1, 00:06:46, Serial0/0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O       192.168.3.0/24 [110/65] via 192.168.23.2, 00:07:41, Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
    192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0/30 [110/128] via 192.168.23.2, 00:06:46, Serial0/0/1
           [110/128] via 192.168.12.1, 00:06:46, Serial0/0/0
    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.1/32 is directly connected, Serial0/0/1
R2#
```

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

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:07:41, Serial0/0/0
O       192.168.2.0/24 [110/65] via 192.168.23.1, 00:08:36, Serial0/0/1
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
    192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:07:41, Serial0/0/1
           [110/128] via 192.168.13.1, 00:07:41, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
```

```

C      192.168.13.0/30 is directly connected, Serial0/0/0
L      192.168.13.2/32 is directly connected, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.23.0/30 is directly connected, Serial0/0/1
L      192.168.23.2/32 is directly connected, Serial0/0/1
R3#

```

```

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

Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
C      3.3.3.3/32 is directly connected, Loopback0
O      192.168.1.0/24 [110/65] via 192.168.13.1, 00:07:41, Serial0/0/0
O      192.168.2.0/24 [110/65] via 192.168.23.1, 00:08:36, Serial0/0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.3.0/24 is directly connected, GigabitEthernet0/0
L      192.168.3.1/32 is directly connected, GigabitEthernet0/0
      192.168.12.0/30 is subnetted, 1 subnets
O      192.168.12.0/30 [110/128] via 192.168.23.1, 00:07:41, Serial0/0/1
           [110/128] via 192.168.13.1, 00:07:41, Serial0/0/0
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.13.0/30 is directly connected, Serial0/0/0
L      192.168.13.2/32 is directly connected, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.23.0/30 is directly connected, Serial0/0/1
L      192.168.23.2/32 is directly connected, Serial0/0/1
R3#

```

Step 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
22.22.22.22     0     FULL/ -         00:00:31   192.168.12.2  Serial0/0/0
33.33.33.33     0     FULL/ -         00:00:31   192.168.13.2  Serial0/0/1
R1#

```

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

```
R2(config)# router ospf 1
R2(config-router)# passive-interface default
R2(config-router)#
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

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

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

R2(config-router)#
```

- 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 |

```
R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
33.33.33.33      0    FULL/ -         00:00:33    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 22.22.22.22, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
R2#
```

- 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**.

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

Gateway of last resort is not set

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



```

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

Gateway of last resort is not set

 3.0.0.0/32 is subnetted, 1 subnets
C    3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:15:27, Serial0/0/0
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, GigabitEthernet0/0
L    192.168.3.1/32 is directly connected, GigabitEthernet0/0
O    192.168.12.0/30 is subnetted, 1 subnets
    192.168.12.0/30 [110/128] via 192.168.13.1, 00:02:52, Serial0/0/0
O    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/0
L    192.168.13.2/32 is directly connected, Serial0/0/0
O    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.23.0/30 is directly connected, Serial0/0/1
L    192.168.23.2/32 is directly connected, Serial0/0/1
R3#

```

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

```

- 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.

```

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
L       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:00:57, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 00:19:27, Serial0/0/1
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
L       192.168.13.1/32 is directly connected, Serial0/0/1
C       192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
           [110/128] via 192.168.12.2, 00:00:57, Serial0/0/0
R1#

```

```

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

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:20:16, Serial0/0/0
O       192.168.2.0/24 [110/129] via 192.168.13.1, 00:01:51, Serial0/0/0
C       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
C       192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:07:41, Serial0/0/0
C       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
C       192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
R3#

```

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? S0/0/0

¿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?

La información que enviamos para la red 192.168.2.0/24 desde el router R3 sera enrutada hacia el router R1.

Interfaz S0/0/1 del R2 esta como interfaz pasiva, por lo que la información de routing OSPF no se anuncia en esa interfaz.

- 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-router)# no passive-interface s0/0/1

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

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

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

Gateway of last resort is not set

 3.0.0.0/32 is subnetted, 1 subnets
C    3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:27:15, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:00:29, Serial0/0/1
O    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, GigabitEthernet0/0
L    192.168.3.1/32 is directly connected, GigabitEthernet0/0
O    192.168.12.0/30 is subnetted, 1 subnets
O    192.168.12.0/30 [110/128] via 192.168.23.1, 00:00:29, Serial0/0/1
      [110/128] via 192.168.13.1, 00:00:29, Serial0/0/0
O    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/0
L    192.168.13.2/32 is directly connected, Serial0/0/0
O    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.23.0/30 is directly connected, Serial0/0/1
L    192.168.23.2/32 is directly connected, Serial0/0/1
R3#
```

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? S0/0/1

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

¿El R2 aparece como vecino OSPF del R3? S/

Part 7: 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.

Step 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
```

```
R1#show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 000d.bd8d.d001 (bia 000d.bd8d.d001
)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 1017 multicast, 0 pause input
    0 input packets with dribble condition detected
    30 packets output, 1920 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
R1#
```

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

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

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set
```

- O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
- O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
[110/128] via 192.168.12.2, 00:01:08, Serial0/0/0

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

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#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R3#
```

- 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#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 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  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 33.33.33.33
  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**.

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

```
R1(config)# router ospf 1
R1(config-router)# auto-cost reference-bandwidth 10000
```

% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.

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

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, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

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

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

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

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

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

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

```
Please ensure reference bandwidth is consistent across all routers.
```

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

Esto solo se hace porque en la actualidad los enlaces son mucho mas veloces entonces debemos realizar un cálculo más preciso de estas métricas con el fin de que los resultados arrojados sena ajustados a la realidad.

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

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

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

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

```
Gateway of last resort is not set
```

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

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

- 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
```

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

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

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

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
```

Gateway of last resort is not set

```
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1
```

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

- e. Emita el comando **show ip ospf interface brief**. El costo de S0/0/0 cambi6 de 64 a 781, que es una representaci6n 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 | |

- f. Cambie el ancho de banda de la interfaz S0/0/1 a la misma configuraci6n que S0/0/0 en el R1.

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

- 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 trav6s de S0/0/0 y otra a trav6s de S0/0/1.

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

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

Gateway of last resort is not set

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

```

192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1
        [110/845] via 192.168.12.2, 00:00:09, Serial0/0/0

```

```

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

```

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.

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, l - LISP
       + - replicated route, % - next hop override

```

Gateway of last resort is not set

```

O      192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
        192.168.12.0/30 is subnetted, 1 subnets
O      192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1
        [110/128] via 192.168.13.1, 00:30:58, Serial0/0/0

```

```

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

```

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

```

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

```

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

Atraviesa dos enlaces seriales con igual costo

781 + 781 = 1562.

Step 3: cambiar el costo de la ruta.

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

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

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set
O    192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
O    192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
    [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0
```

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

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
```

```
R1(config)#int s 0/0/1
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, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

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

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

Nota: la manipulación de costos de enlace mediante el comando **ip ospf cost** es el método de preferencia y el más fácil para cambiar los costos de las rutas OSPF. Además de cambiar el costo basado en el ancho de banda, un administrador de red puede tener otros motivos para cambiar el costo de una ruta, como la preferencia por un proveedor de servicios específico o el costo monetario real de un enlace o de una ruta.

Explique la razón por la que la ruta a la red 192.168.3.0/24 en el R1 ahora atraviesa el R2.

OSPF elige la ruta con el menor costo acumulado.

➤ La ruta con el menor costo acumulado es:

S0/0/0 del R1 + S0/0/1 del R2 + G0/0 del R3, o $781 + 781 + 1 = 1563$.

➤ Este métrica es menor que el costo acumulado de:

S0/0/1 R1 + G0/0 R3, o $1565 + 1 = 1566$.

Reflexión

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

La asignación de ID se hace para poder realizar la elección de router DR y BDR, con el ID asignado a las interfaces loopback podemos forzar la elección de este.

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

-----.

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

Esto lo hacemos porque hay algunas interfaces que no necesitan que se envíen actualizaciones, esto solo consume recursos de red.

Tabla de resumen de interfaces del router

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

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

8.3.3.6 CONFIGURACIÓN DE OSPFV3 BÁSICO DE ÁREA ÚNICA

8.3.3.6 CONFIGURACIÓN DE OSPFV3 BÁSICO DE ÁREA ÚNICA

Topología

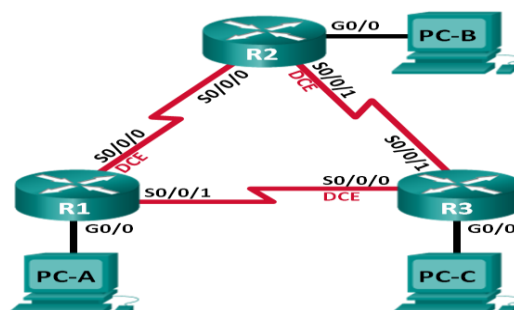


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

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

Part 8: armar la red y configurar los parámetros básicos de los dispositivos

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

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

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

Step 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.

Copie la configuración en ejecución en la configuración de inicio

Step 4: configurar los equipos host.

Step 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.

Part 9: configurar el routing OSPFv3

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

Step 1: asignar ID a los routers.

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

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

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

```
R1(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.

- b. 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)#
```

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

```
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
```

- a. 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#
```

```
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#
```

Step 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
```

```
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)#

```

Step 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 Serial0/0/1 | 0 | FULL/ - | 00:00:39 | 6 | |
| 2.2.2.2 Serial0/0/0 | 0 | FULL/ - | 00:00:36 | 6 | |

```
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#

```

Step 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#
```

Step 5: verificar las interfaces OSPFv3.

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

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

```
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 7
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/3/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 6
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
```



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

- 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
```

Step 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.

```
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
```

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

➤ *show ipv6 route ospf*

Step 7: Verificar la conectividad de extremo a extremo.

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

```
PC>ping 2001:DB8:ACAD:A::A

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

Reply from 2001:DB8:ACAD:A::A: bytes=32 time=6ms TTL=128
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=128
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=26ms TTL=128
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=26ms TTL=128

Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 26ms, Average = 14ms
```

```
PC>ping 2001:DB8:ACAD:B::B

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

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

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

```

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

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

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms TTL=126

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms

PC>

```

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

Part 10: configurar las interfaces pasivas de OSPFv3

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

Step 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)
```

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

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

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

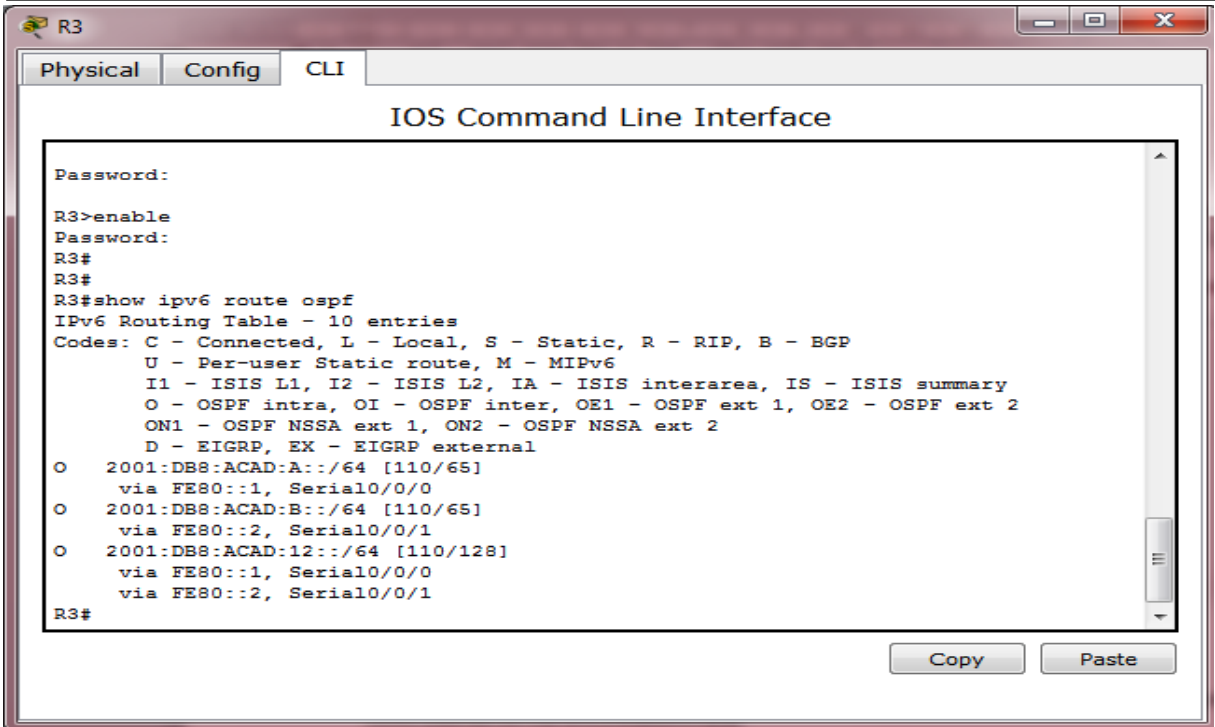
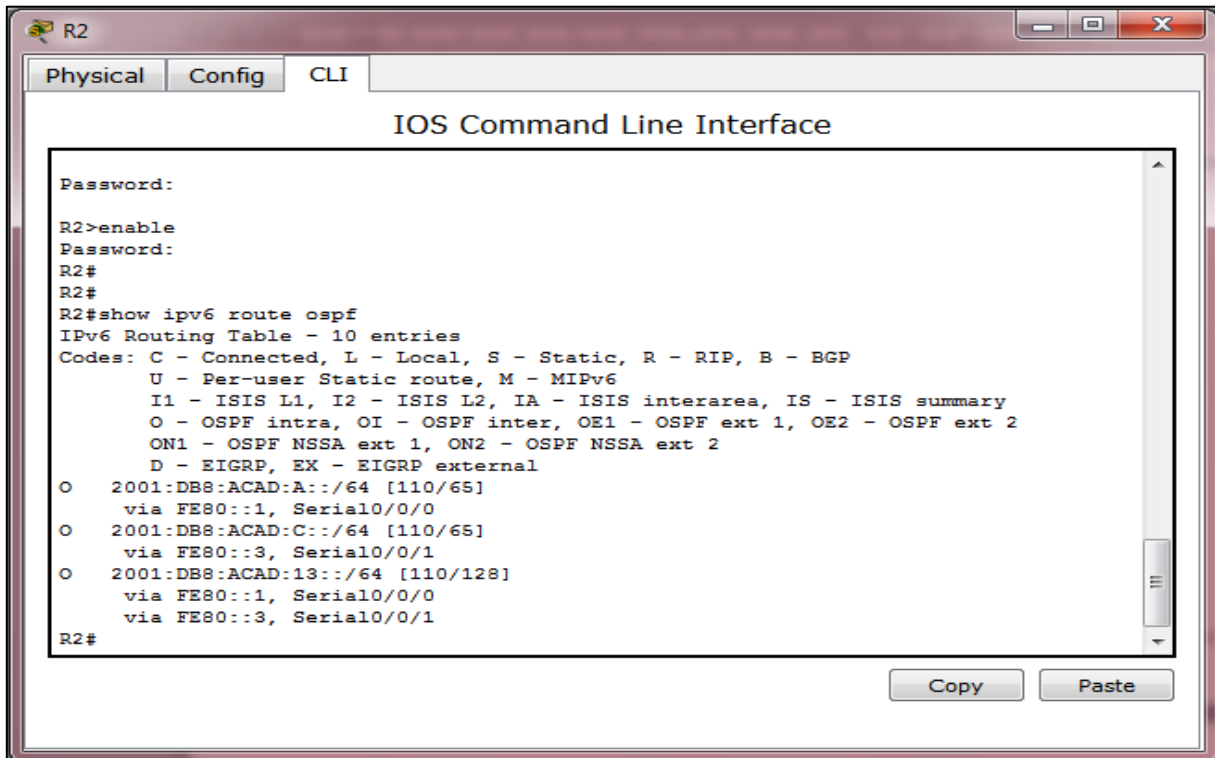
- a. Vuelva a emitir el comando **show ipv6 ospf interface g0/0** para verificar que la interfaz G0/0 ahora sea pasiva.

```
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)
```

- b. 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



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

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

```
R2(config)# ipv6 router ospf 1
R2(config-rtr)# passive-interface default
```

```
./2(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)#
```

- a. 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#
```

- a. 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)
```

```
<#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#
```

- a. 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**.

```
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#

```

- a. 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)#

```

- a. 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#

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?

El tráfico hacia 2001:DB8:ACAD:B::/64 enviados desde el router R1 será enviada hacia el router R3 ya que la interfaz S0/0/0 en el R2 fue configurada como pasiva por lo cual la información de ruteo no la envía en sus actualizaciones.

- b. 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)#
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)#
```

- a. 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#
```

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?

Estas ID no es necesario que coincida.

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

Por facilitar el proceso de configuración de 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 CONFIGURACIÓN DE DHCPV4 BÁSICO EN UN ROUTER

10.1.2.4 CONFIGURACIÓN DE DHCPV4 BÁSICO EN UN ROUTER

Topología

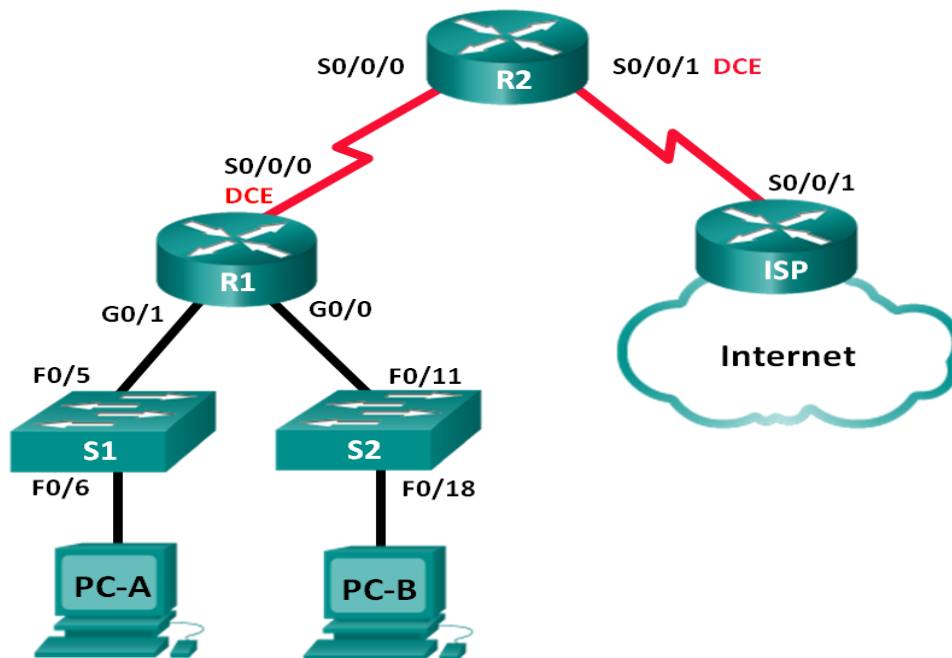


Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
|-------------|--------------|----------------|-------------------|------------------------|
| R1 | G0/0 | 192.168.0.1 | 255.255.255.0 | N/A |
| | G0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| | S0/0/0 (DCE) | 192.168.2.253 | 255.255.255.252 | N/A |
| R2 | S0/0/0 | 192.168.2.254 | 255.255.255.252 | N/A |
| | S0/0/1 (DCE) | 209.165.200.26 | 255.255.255.24 | N/A |
| ISP | S0/0/1 | 209.165.200.25 | 255.255.255.24 | 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

Recursos necesarios

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

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

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

Step 3: realizar el cableado de red tal como se muestra en la topología.

Step 4: inicializar y volver a cargar los routers y los switches.

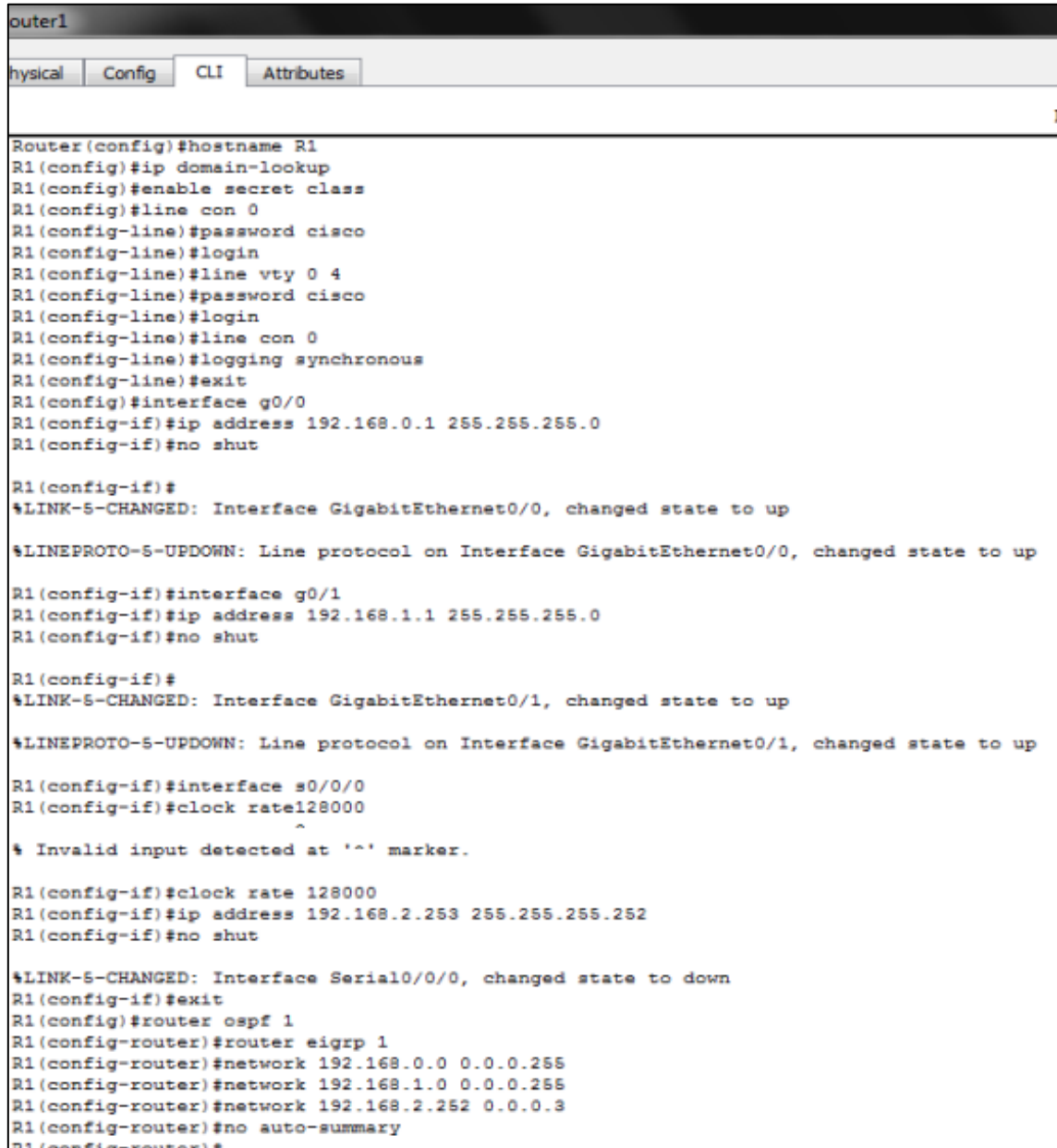
Step 5: configurar los parámetros básicos para cada router.

- 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 interrumpen la entrada de comandos.
- f. Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.
- g. Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.
- h. Configure EIGRP for R1.

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

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

```
R1(config-router)# network 192.168.1.0 0.0.0.255  
R1(config-router)# network 192.168.2.252 0.0.0.3  
R1(config-router)# no auto-summary
```



```
outer1  
Physical Config CLI Attributes  
Router(config)#hostname R1  
R1(config)#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)#line vty 0 4  
R1(config-line)#password cisco  
R1(config-line)#login  
R1(config-line)#line con 0  
R1(config-line)#logging synchronous  
R1(config-line)#exit  
R1(config)#interface 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)#interface 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)#interface s0/0/0  
R1(config-if)#clock rate128000  
^  
% Invalid input detected at '^' marker.  
  
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)#exit  
R1(config)#router ospf 1  
R1(config-router)#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)#
```

- 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
```

```

Router2
-----
Physical  Config  CLI  Attributes
-----
Router>en
Router>conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#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)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line con 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface 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)#i
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config-if)#interface s0/0/1
R2(config-if)#clock rate 128000
R2(config-if)#ip address 209.168.200.226 255.255.255.224
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
R2(config-if)#exit
R2(config)#router eigrp 1
R2(config-router)#network 192.168.2.252 0.0.0.3
R2(config-router)#
%DUAL-5-NBCHANGE: 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 0.0.0.0 209.168.200.226
R2(config)#

```

- 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**

```

ISP
-----
Physical  Config  CLI  Attributes
-----
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wvl/export/crypto/tool/stqrg.html

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

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
256K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>en
Router>conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#ip domain-lookup
ISP(config)#enable secret class
ISP(config)#line con 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line con 0
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#interface 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)#exit
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#

```


k. Copie la configuración en ejecución en la configuración de inicio

Step 6: 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.

```
R2#ping 209.165.200.225

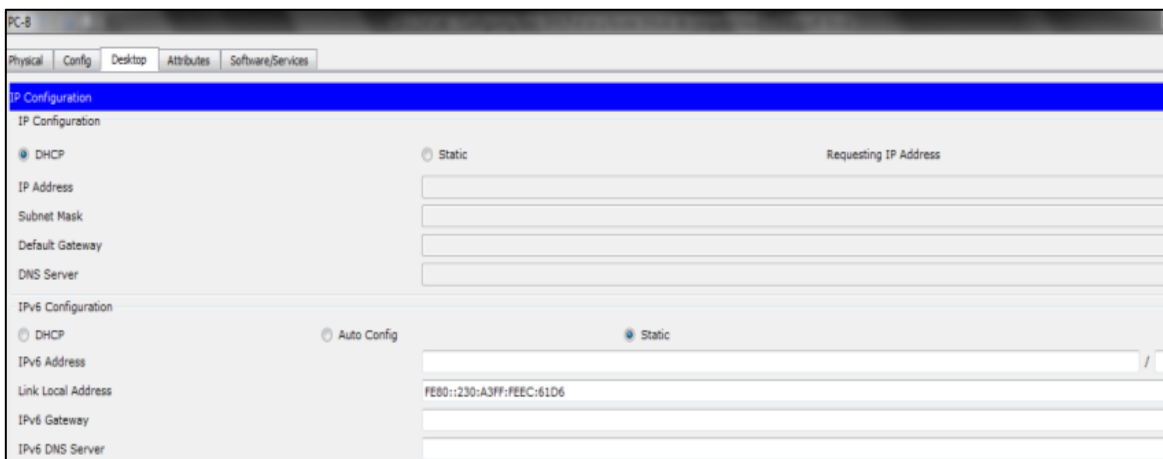
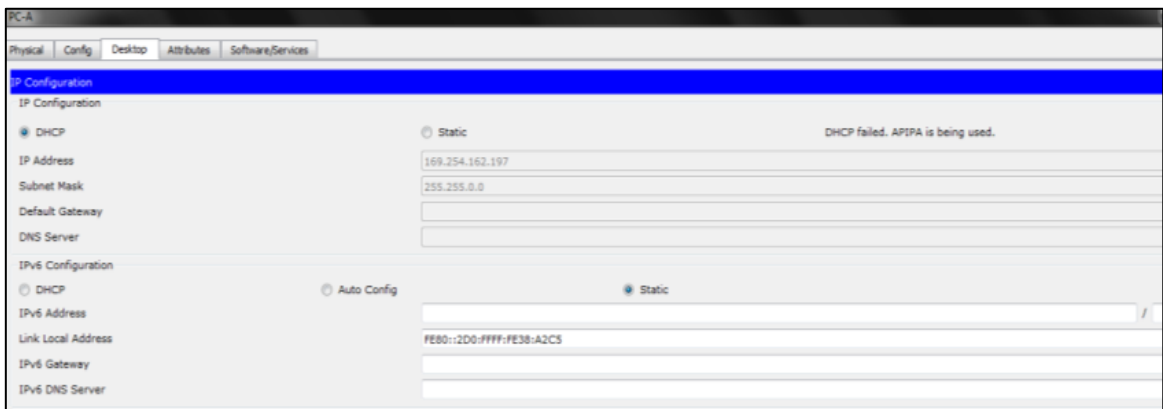
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R2#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms

R2#
```

Step 7: verificar que los equipos host estén configurados para DHCP.



Part 11: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

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

Step 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.

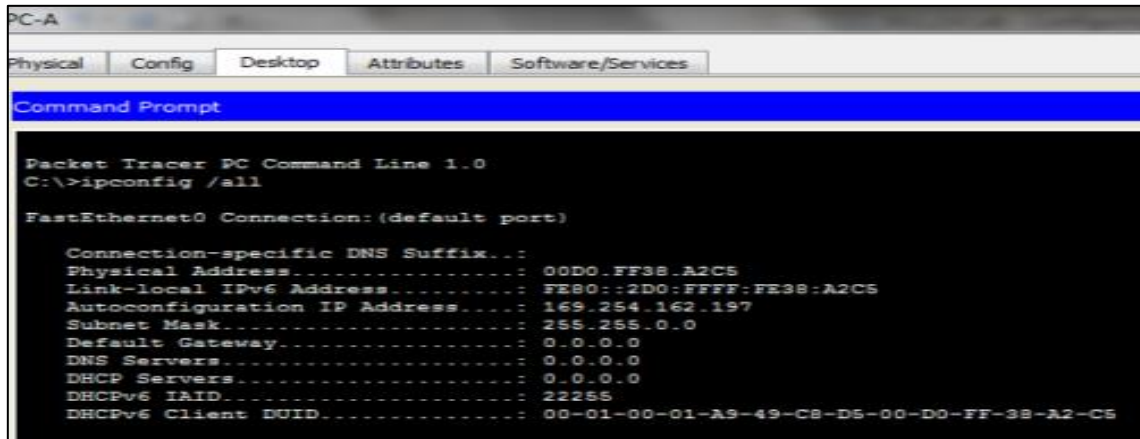
En las líneas a continuación, escriba los comandos necesarios para configurar los servicios DHCP en el router R2, incluso las direcciones DHCP excluidas y los conjuntos de direcciones DHCP.

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.

```
router2
physical  Config  CLI  Attributes
-----
User Access Verification
Password:
R2>wn
Translating "wn"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
R2>en
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)#dom
~
% 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)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

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

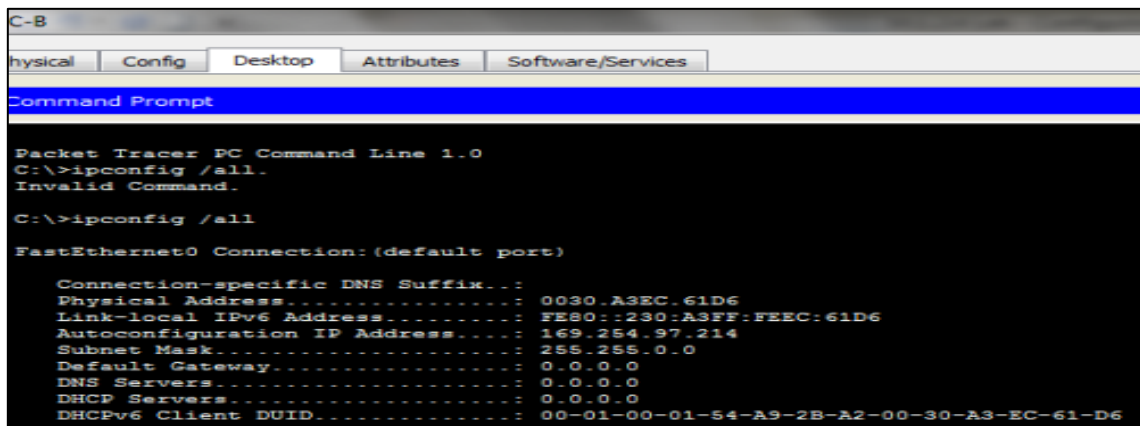
El router 2 se encuentra en otra red, no realiza la interface de conexión



```
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. . . . . : 00D0.FF38.A2C5
Link-local IPv6 Address . . . . . : FE80::2D0:FFFF:FE38:A2C5
Autoconfiguration IP Address. . . . : 169.254.162.197
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 . . . . . : 22255
DHCPv6 Client DUID. . . . . : 00-01-00-01-A9-49-C8-D5-00-D0-FF-38-A2-C5
```



```
C-B
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all.
Invalid Command.

C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix... : 
Physical Address. . . . . : 0030.A3EC.61D6
Link-local IPv6 Address . . . . . : FE80::230:A3FF:FEEC:61D6
Autoconfiguration IP Address. . . . : 169.254.97.214
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 . . . . . : 00-01-00-01-54-A9-2B-A2-00-30-A3-EC-61-D6
```

Step 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.

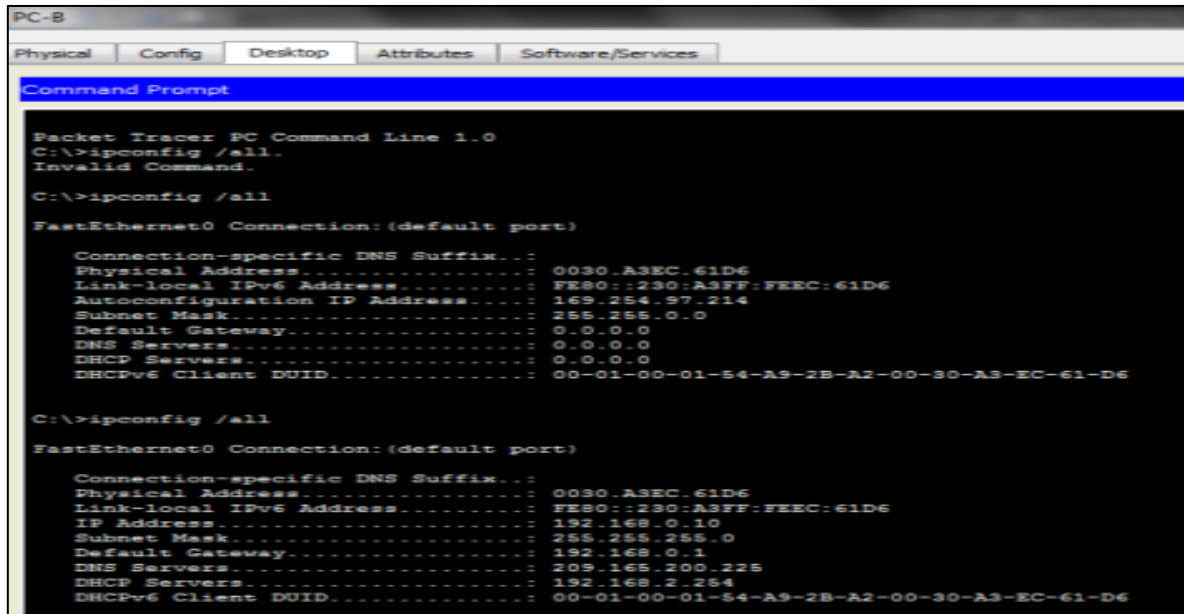
En las líneas a continuación, escriba los comandos necesarios para configurar el R1 como agente de retransmisión DHCP para las LAN del R1.

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
R1(config)#interface g0/1
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#
```

Step 3: registrar la configuración IP para la PC-A y la PC-B.

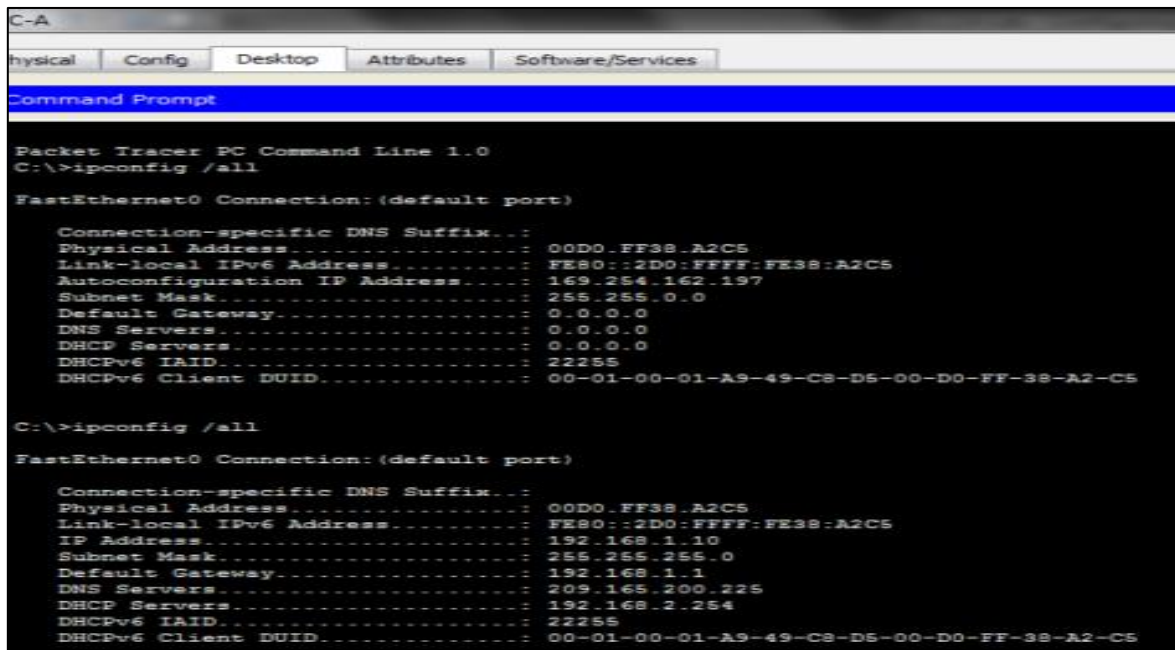
En la PC-A y la PC-B, emita el comando **ipconfig /all** para verificar que las computadoras recibieron la información de la dirección IP del servidor de DHCP en el R2. Registre la dirección IP y la dirección MAC de cada computadora.

PCA = 192.168.1.10 MAC = 00D0.FF38.A2C5
PCB = 192.168.0.10 MAC = 0030.A3EC.61D6



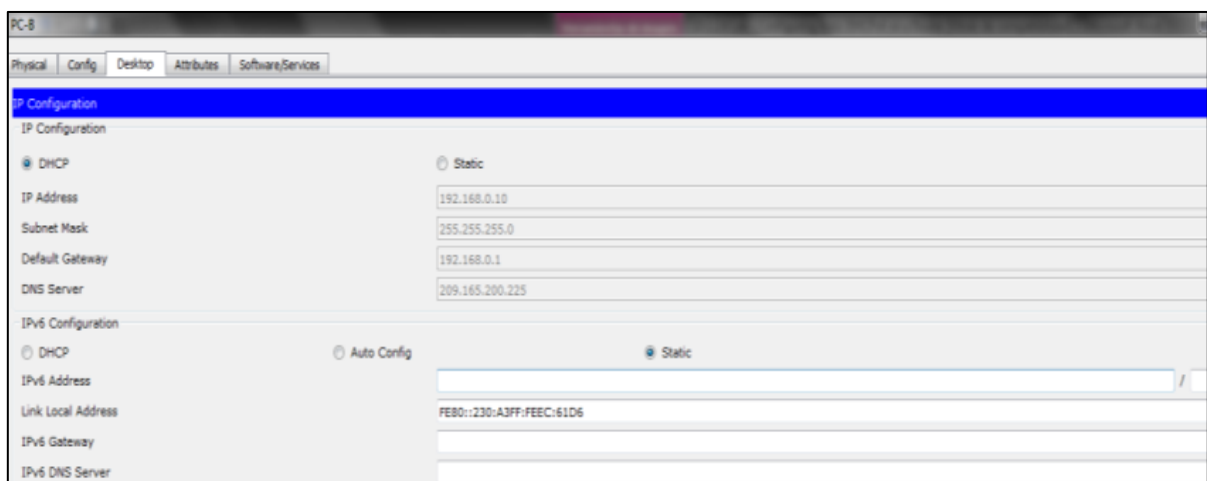
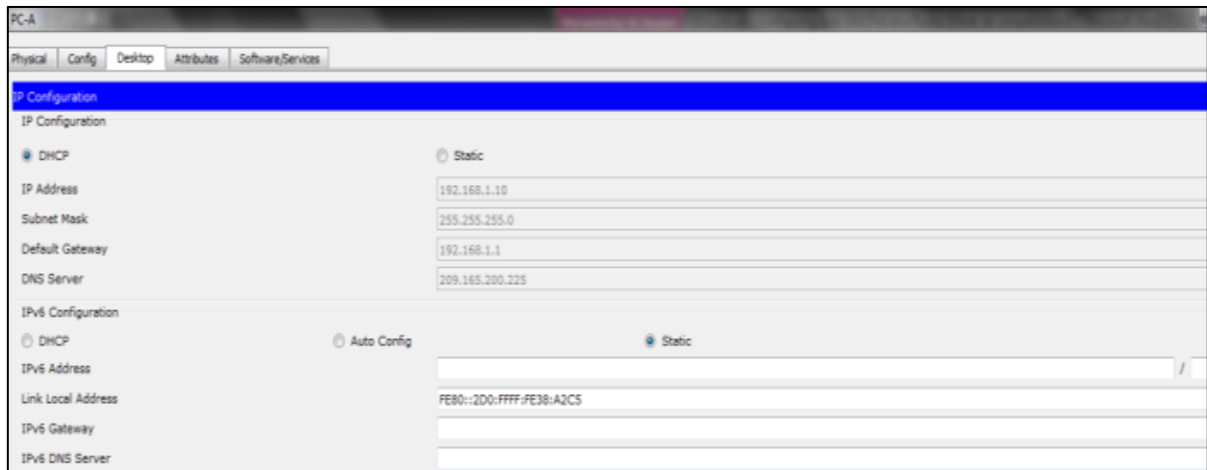
```
PC-B
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all.
Invalid Command.
C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix... :
Physical Address... : 0030.A3EC.61D6
Link-local IPv6 Address... : FE80::230:A3FF:FEEC:61D6
Autoconfiguration IP Address... : 169.254.97.214
Subnet Mask... : 255.255.0.0
Default Gateway... : 0.0.0.0
DNS Servers... : 0.0.0.0
DHCP Servers... : 0.0.0.0
DHCPv6 Client DUID... : 00-01-00-01-54-A9-2B-A2-00-30-A3-EC-61-D6

C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix... :
Physical Address... : 0030.A3EC.61D6
Link-local IPv6 Address... : FE80::230:A3FF:FEEC:61D6
IP Address... : 192.168.0.10
Subnet Mask... : 255.255.255.0
Default Gateway... : 192.168.0.1
DNS Servers... : 209.165.200.225
DHCP Servers... : 192.168.2.254
DHCPv6 Client DUID... : 00-01-00-01-54-A9-2B-A2-00-30-A3-EC-61-D6
```



```
C-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... : 00D0.FF38.A2C5
Link-local IPv6 Address... : FE80::2D0:FFFF:FE38:A2C5
Autoconfiguration IP Address... : 169.254.162.197
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... : 22255
DHCPv6 Client DUID... : 00-01-00-01-A9-49-C8-D5-00-D0-FF-38-A2-C5

C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix... :
Physical Address... : 00D0.FF38.A2C5
Link-local IPv6 Address... : FE80::2D0:FFFF:FE38:A2C5
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... : 22255
DHCPv6 Client DUID... : 00-01-00-01-A9-49-C8-D5-00-D0-FF-38-A2-C5
```



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

Para PCA de la 1 a la 10

Para PCB de la 0 a la 10

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

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



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

Aparecen las direcciones ip, las MAC, el tiempo de arrendamiento y el tipo en este caso es automático.

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

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

No está activado el comando show ip dhcp server statistics, el router no es real

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

No está activo comando

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

Ip dhcp pool RG1 Y RG2, la red, la máscara de red, default router, dns-server.

```
!
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 209.165.200.225
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 209.165.200.225
```

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

Se utilizó solo el comando show run

```
!
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
```

- 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.

```
R2#show ip interface g0/0
GigabitEthernet0/0 is administratively down, line protocol is down (disabled)
  Internet protocol processing disabled

R2#show ip interface g0/1
GigabitEthernet0/1 is administratively down, line protocol is down (disabled)
  Internet protocol processing disabled
```

NOTA: Se aplicó el comando show ip interface G0/0 y g0/1 en R, porque en R2 no aparece

```
outer1
Physical Config CLI Attributes
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.0.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 192.168.2.254
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
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
IP output packet accounting is disabled

R1#show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 192.168.2.254
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
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
```

Reflexión

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

Hacer que un solo router tenga solo la función de DHCP, para que los otros Routers hagan sus funciones normales

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 CONFIGURACIÓN DE DHCPV4 BÁSICO EN UN SWITCH.

10.1.2.5 CONFIGURACIÓN DE DHCPV4 BÁSICO EN UN SWITCH.

Topología

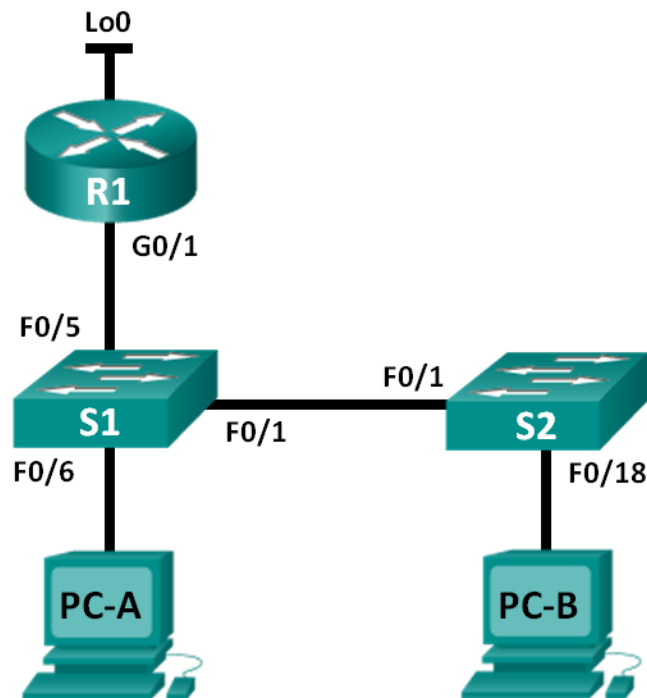


Tabla de direccionamiento

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

Objetivos

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

Parte 2: cambiar la preferencia de SDM

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

Parte 3: configurar DHCPv4

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

Parte 4: configurar DHCP para varias VLAN

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

Parte 5: habilitar el routing IP

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

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 1. armar la red y configurar los parámetros básicos de los dispositivos

Paso 5: realizar el cableado de red tal como se muestra en la topología.

Paso 6: inicializar y volver a cargar los routers y switches.

Paso 7: configurar los parámetros básicos en los dispositivos.

- a. Asigne los nombres de dispositivos como se muestra en la topología.
- b. Desactive la búsqueda del DNS.
- c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
- d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.
- e. Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.
- f. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```

interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 ip address 192.168.1.10 255.255.255.0
 duplex auto
 speed auto

```

```

interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 ip address 192.168.2.1 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.10
!
ip flow-export version 9

```

Parte 2.cambiar la preferencia de SDM

Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch Cisco 2960. Las plantillas pueden habilitarse para admitir funciones específicas según el modo en que se utilice el switch en la red. En esta práctica de laboratorio, la plantilla lanbase-routing está habilitada para permitir que el switch realice el routing entre VLAN y admita el routing estático.

Paso 8: mostrar la preferencia de SDM en el S1.

En el S1, emita el comando **show sdm prefer** en modo EXEC privilegiado. Si no se cambió la plantilla predeterminada de fábrica, debería seguir siendo **default**. La plantilla **default** no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será **dual-ipv4-and-ipv6 default**.

```
S1# show sdm prefer
```

```
The current template is "default" template.
```

```
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.
```

```

number of unicast mac addresses:           8K
number of IPv4 IGMP groups:                0.25K
number of IPv4/MAC qos aces:               0.125k
number of IPv4/MAC security aces:         0.375k

```

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

¿Cuál es la plantilla actual?

- “default” o “default dual-ipv4-and-ipv6” o “lanbase-routing”.
- Comndo no soportado por packet tracer.

Paso 9: 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
- Comndo no soportado por packet Tracer – estos solo se puede en un dispositivo real.

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

```
S1# reload

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

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

Paso 10: 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 |

➤ commando no soportado por packet tracer.

Parte 12: 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.

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

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

```
S1(config)# ip dhcp pool DHCP1
```

- Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

```
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
```

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

```
S1(dhcp-config)# default-router 192.168.1.1
```

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

```
S1(dhcp-config)# dns-server 192.168.1.9
```

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

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

No soportado por Packet Tracer.

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

```
ip dhcp excluded-address 192.168.1.1 192.168.1.10
!  
ip dhcp pool DHCP1  
network 192.168.1.0 255.255.255.0  
default-router 192.168.1.1  
dns-server 192.168.1.9
```

Paso 2: verificar la conectividad y DHCP.

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

Para la PC-A, incluya lo siguiente:

Dirección IP:

192.168.1.11

Máscara de subred:

255.255.255.0

Gateway predeterminado:

192.168.1.1

Para la PC-B, incluya lo siguiente:

Dirección IP:

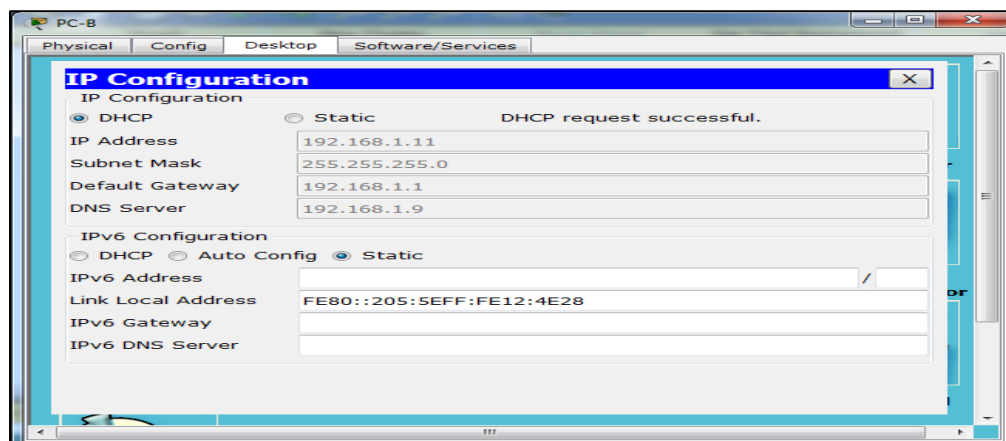
192.168.1.12

Máscara de subred:

255.255.255.0

Gateway predeterminado:

192.168.1.1



- b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? Sí

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

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

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

Parte 13: configurar DHCPv4 para varias VLAN

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

Paso 1: asignar un puerto a la VLAN 2.

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

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
```

```
interface FastEthernet0/6
switchport access vlan 2
switchport mode access
!
```

Paso 2: configurar DHCPv4 para la VLAN 2.

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

```
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
```

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

```
S1(config)# ip dhcp pool DHCP2
```

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

```
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
```

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

```
S1(dhcp-config)# default-router 192.168.2.1
```

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

```
S1(dhcp-config)# dns-server 192.168.2.9
```

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

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

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

```
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.2.1 192.168.2.10
!
ip dhcp pool DHCP1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.1.9
ip dhcp pool DHCP2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 192.168.2.9
```

Paso 3: verificar la conectividad y DHCPv4.

- a. En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP:

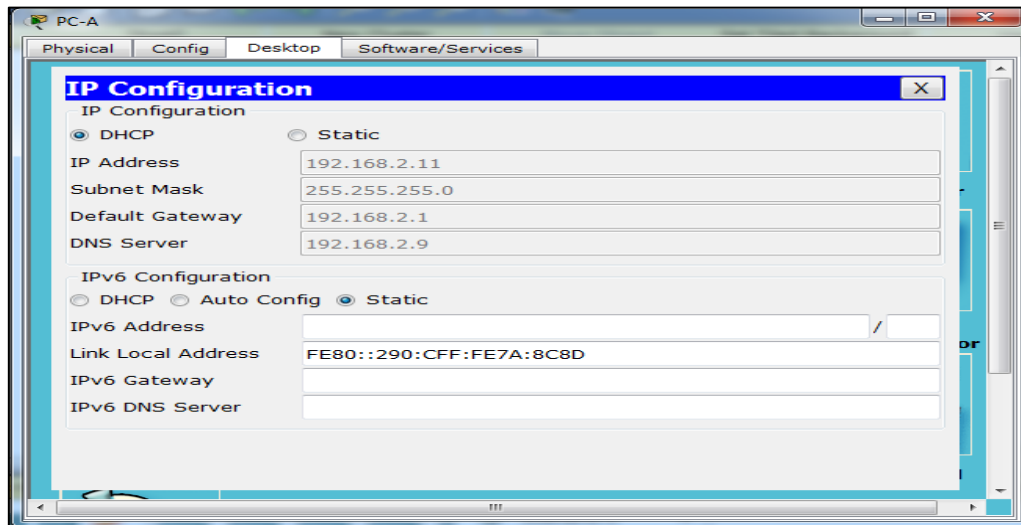
192.168.2.11

Máscara de subred:

255.255.255.0

Gateway predeterminado:

192.168.2.1



- b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado de la VLAN 2 y a la PC-B.

¿Es posible hacer ping de la PC-A al gateway predeterminado? Sí

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

¿Los pings eran correctos? ¿Por qué?

La razón por la cual no se puede hacer PING entre las dos PC es porque PC-B está en una red diferente; por lo tanto, el ping de la PC-A no es correcto.

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

```
S1# show ip route
Default gateway is not set
```

```
Host          Gateway          Last Use      Total Uses   Interface
ICMP redirect cache is empty
```

¿Qué resultado arrojó este comando?

No se estableció un gateway predeterminado y no hay una tabla de routing presente en el switch.

Parte 14: habilitar el routing IP

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

Paso 1: habilitar el routing IP en el S1.

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

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

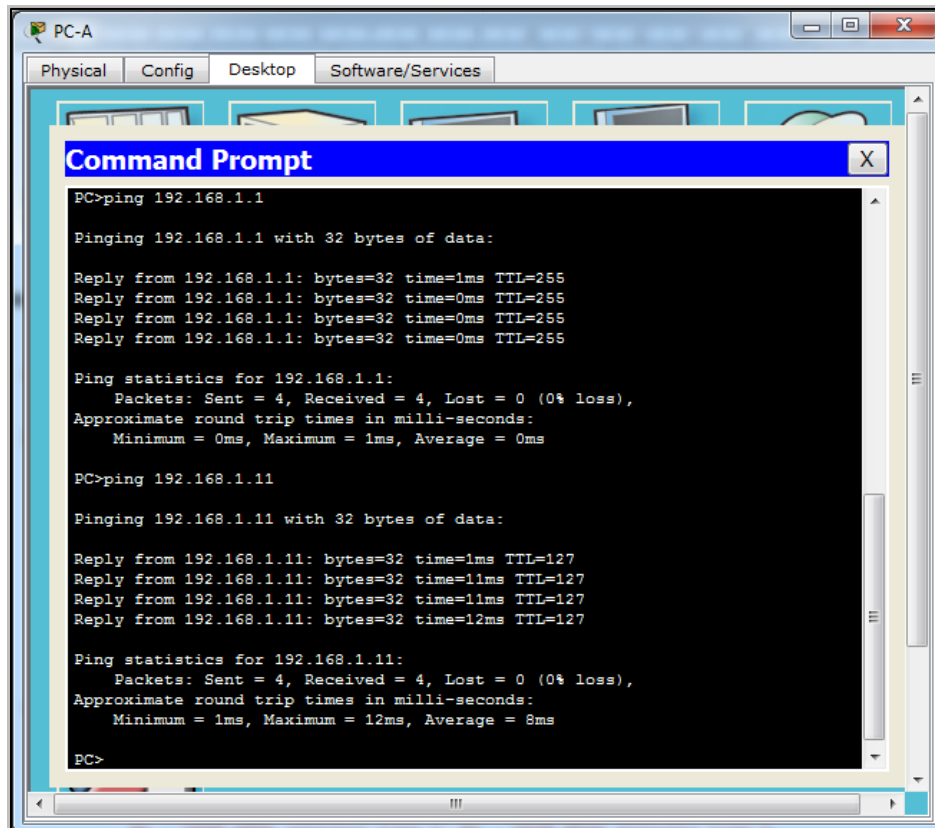
- b. Verificar la conectividad entre las VLAN.

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

Sí

¿Qué función realiza el switch?

El switch hace routing entre VLAN.



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

S1# **show ip route**

```

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

```

Gateway of last resort is not set

```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Vlan1
C       192.168.2.0/24 is directly connected, Vlan2

```

```

S1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, Vlan1
C    192.168.2.0/24 is directly connected, Vlan2
S1#

```

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

El switch exhibe una tabla de routing que muestra las VLAN como las redes conectadas directamente 192.168.1.0/24 y 192.168.2.0/24.

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

```

R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1
C      209.165.200.0/27 is directly connected, Loopback0

```

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

Se muestra las redes conectadas directamente a una de sus interfaces 192.168.1.0 y 209.165.200.224.

Observemos que no tenemos una ruta para 192.168.2.0.

e. ¿Es posible hacer ping de la PC-A al R1? No

¿Es posible hacer ping de la PC-A a la interfaz Lo0? No

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

Debemos tener rutas que permitan la unión de estas redes distantes.

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.

```
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.10
!
ip flow-export version 9
```

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

```
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```

```
!
ip classless
ip route 192.168.2.0 255.255.255.0 GigabitEthernet0/1
!
ip flow-export version 9
```

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

```
S1# show ip route
```

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

```
Gateway of last resort is 192.168.1.10 to network 0.0.0.0
```

```
S* 0.0.0.0/0 [1/0] via 192.168.1.10
C   192.168.1.0/24 is directly connected, Vlan1
C   192.168.2.0/24 is directly connected, Vlan2
```

```
S1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

C   192.168.1.0/24 is directly connected, Vlan1
C   192.168.2.0/24 is directly connected, Vlan2
S* 0.0.0.0/0 [1/0] via 192.168.1.10
S1#
```

¿Cómo está representada la ruta estática predeterminada?

```
S* 0.0.0.0/0 [1/0] via 192.168.1.10
```

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

```
R# show ip route
```

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

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 is directly connected, GigabitEthernet0/1
C    209.165.200.0/27 is directly connected, Loopback0
```

```
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

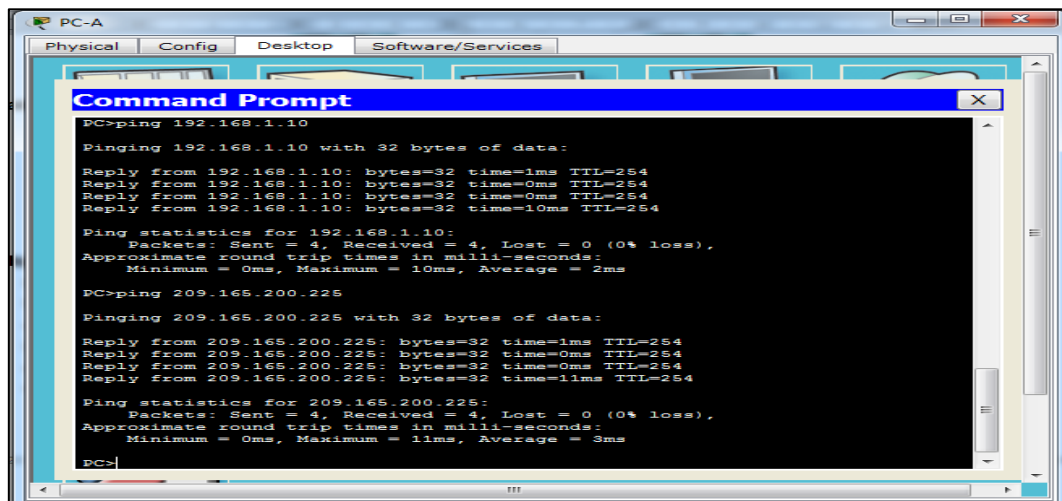
Gateway of last resort is not set

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
L    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 192.168.2.0/24 is directly connected, GigabitEthernet0/1

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

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



Reflexión

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

Si las direcciones estáticas se excluyeran después de la creación del pool de DHCPv4, existiría un lapso durante el cual las direcciones excluidas podrían pasarse dinámicamente a hosts, generando conflictos con las direcciones IP que ya están asignadas.

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

Recordemos que cada uno de los puertos está asignado a determinado VLAN, esta es la forma de controlar el switch que dirección debe asignar y a que interfaz.

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

Este en un dispositivo real puede hacer la función de router, pero en el caso del simulador este ni puede hacer, por esto fue cambiado por otro tipo de switch que me permita realizar la práctica.

Tabla de resumen de interfaces del router

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

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

Apéndice A: comandos de configuración

Configurar DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

Configurar DHCPv4 para varias VLAN

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

Habilitar routing IP

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


10.2.3.5 CONFIGURACIÓN DE DHCPV6 SIN ESTADO Y CON ESTADO

10.2.3.5 CONFIGURACIÓN DE DHCPV6 SIN ESTADO Y CON ESTADO

Topología



Tabla de direccionamiento

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

Objetivos

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar la red para SLAAC
- Parte 3: configurar la red para DHCPv6 sin estado
- Parte 4: configurar la red para DHCPv6 con estado

Recursos necesarios

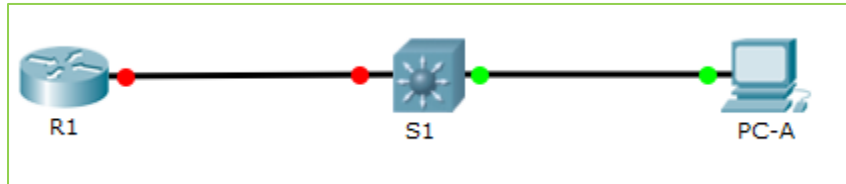
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para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

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

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

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

Step 3: realizar el cableado de red tal como se muestra en la topología.



Step 4: inicializar y volver a cargar el router y el switch según sea necesario.

Step 5: Configurar R1

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

```
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#enable password cisco
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#
R1(config-line)#exit
R1(config)#
R1(config)#interface g0/1
R1(config-if)#ip address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#do wr
Building configuration...
[OK]
R1(config-if)#exit
R1(config)#
R1(config)#banner motd
% Incomplete command.
R1(config)#banner motd &
Enter TEXT message. End with the character '&'.

NO INGRESAR SIN AUTORIZACION
&
R1(config)#
```

Step 6: configurar el S1.

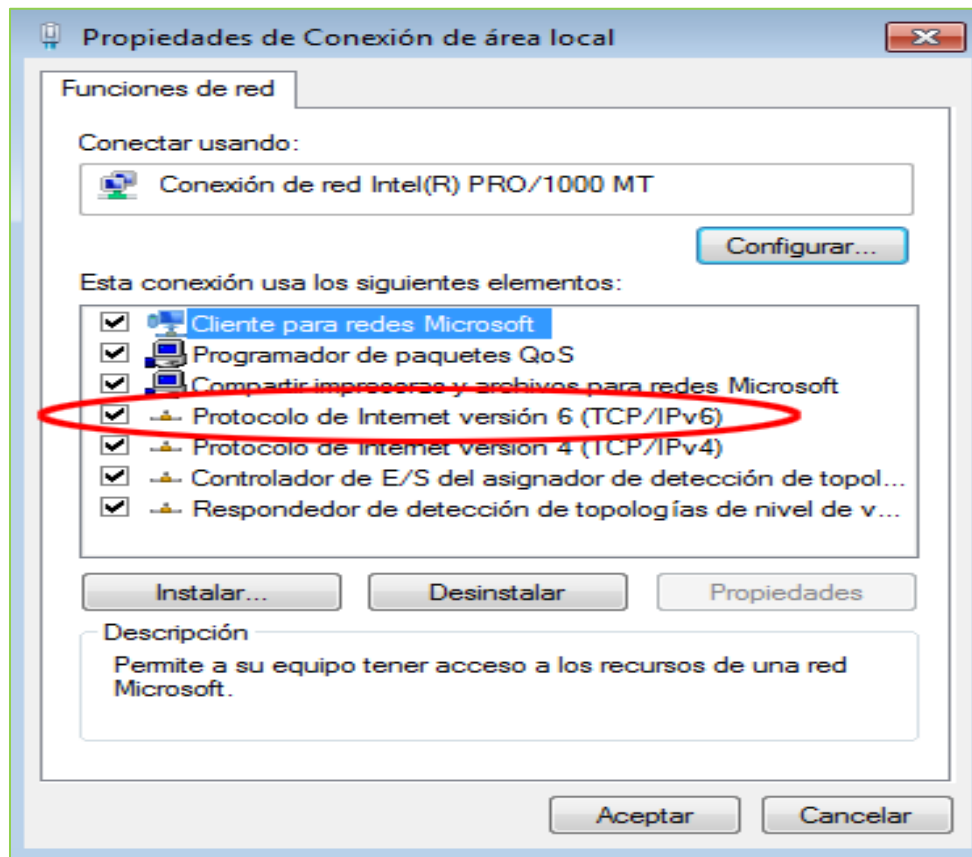
- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f.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

```
Switch(config)#no ip domain-lo?
domain-lookup
Switch(config)#no ip domain-lo
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#enable password cisco
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#servi?
% Unrecognized command
S1(config-line)#exit
S1(config)#
S1(config)#serv?
service
S1(config)#service pass?
password-encryption
S1(config)#service pass
S1(config)#service password-encryption
S1(config)#do wr
Building configuration...
[OK]
S1(config)#
```

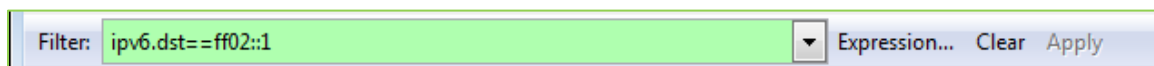
Part 15: configurar la red para SLAAC

Step 1: preparar la PC-A.

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



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



Step 2: Configurar R1

- a. Habilite el routing de unidifusión IPv6.

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#ipv6 unicast-routing
R1(config)#
```

- b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.

```
R1(config)#interface g 0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
```

- c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.

```
R1(config-if)#ipv6 address FE80::1 link-local
```

- d. Active la interfaz G0/1.

```
R1(config-if)#no shutdown
```

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

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

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

```
R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::, subnet is 2001:DB8:ACAD:A::/64
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:0
  FF02::1:FF00:1
MTU is 1500 bytes
```

Step 4: configurar el S1.

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

```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
S1(config-if)# end
```

```
S1#
S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 1
S1(config-if)#ipv6 address autoconfig
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

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

```
S1# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
No Virtual link-local address(es):
Stateless address autoconfig enabled
Global unicast address(es):
  2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64
[EUI/CAL/PRE]
  valid lifetime 2591988 preferred lifetime 604788
Joined group address(es):
  FF02::1
  FF02::1:FEE8:8A40
```

```
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
Output features: Check hwidb
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
Default router is FE80::1 on Vlan1
```

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

| IPv6 Configuration | |
|--|---|
| <input type="radio"/> DHCP <input checked="" type="radio"/> Auto Config <input type="radio"/> Static | IPv6 auto config successful. |
| IPv6 Address | 2001:DB8:ACAD:A:202:16FF:FE21:E396 / 64 |
| Link Local Address | FE80::202:16FF:FE21:E396 |
| IPv6 Gateway | FE80::1 |
| IPv6 DNS Server | |

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

```
Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . :
    Descripción . . . . . : Conexión de red Intel(R) PRO/1000
    MT
    Dirección física. . . . . : 00-0C-29-E3-23-17
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Preferido)
    Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11(Preferido)
    Dirección IPv4. . . . . : 192.168.96.139(Preferido)
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : fe80::1:11
    Servidores DNS . . . . . : fec0:0:0:ffff::1%1
    . . . . . : fec0:0:0:ffff::2%1
    . . . . . : fec0:0:0:ffff::3%1
    NetBIOS sobre TCP/IP. . . . . : habilitado
```

```
PC>ipconfig /all

FastEthernet0 Connection: (default port)

    Physical Address. . . . . : 0002.1621.E396
    Link-local IPv6 Address . . . . . : FE80::202:16FF:FE21:E396
    IPv6 Address. . . . . : 2001:DB8:ACAD:A:202:16FF:FE21:E396/64
    Default Gateway. . . . . : ::
    DNS Servers . . . . . : ::
    DHCPv6 Client DUID. . . . . : 00-01-00-01-64-60-25-1E-00-02-16-21-E3-96

PC>
```


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

Part 16: configurar la red para DHCPv6 sin estado.

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

- Cree un pool de DHCP IPv6.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
```
- Asigne un nombre de dominio al pool.

```
R1(config-dhcpv6)# domain-name ccna-statelessDHCPv6.com
```
- Asigne una dirección de servidor DNS.

```
R1(config-dhcpv6)# dns-server 2001:db8:acad:a::abcd
R1(config-dhcpv6)# exit
```
- Asigne el pool de DHCPv6 a la interfaz.

```
R1(config)# interface g0/1
R1(config-if)# ipv6 dhcp server IPV6POOL-A
```
- Establezca la detección de redes (ND) DHCPv6 **other-config-flag**.

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

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#dns-server 2001:db8:acad:a::abcd
R1(config-dhcp)#exit
R1(config)#interface g0/1
R1(config-if)#ipv6 dhcp server IPV6POOL-A
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#end
R1#
```

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

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

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:2
    FF02::1:FF00:1
    FF05::1:3
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachable are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
  Hosts use DHCP to obtain other configuration.
```

```

R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::, subnet is 2001:DB8:ACAD:A::/64
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2|
  FF02::1:FF00:0
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#

```

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

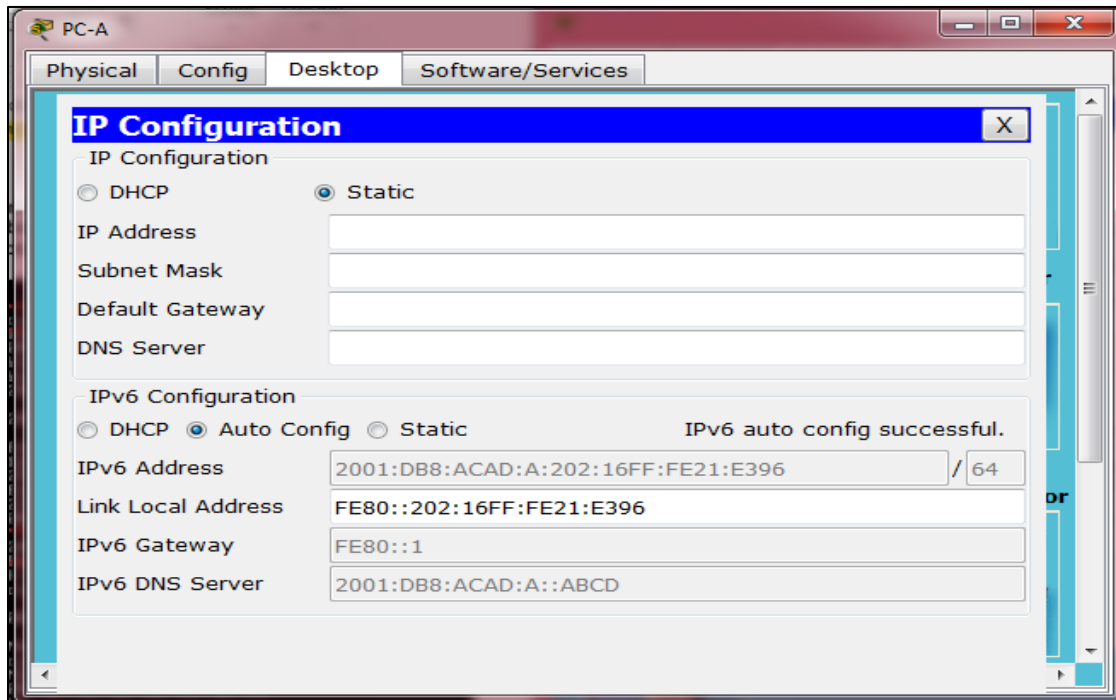
Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente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

```

Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
Dirección física. . . . . : 00-0C-29-E3-23-17
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
Uínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>
Dirección IPv4. . . . . : 192.168.96.139<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::1%11
IAD DHCPv6 . . . . . : 234884137
DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-
E3-23-17
Servidores DNS. . . . . : 2001:db8:acad:a::abcd
NetBIOS sobre TCP/IP. . . . . : habilitado

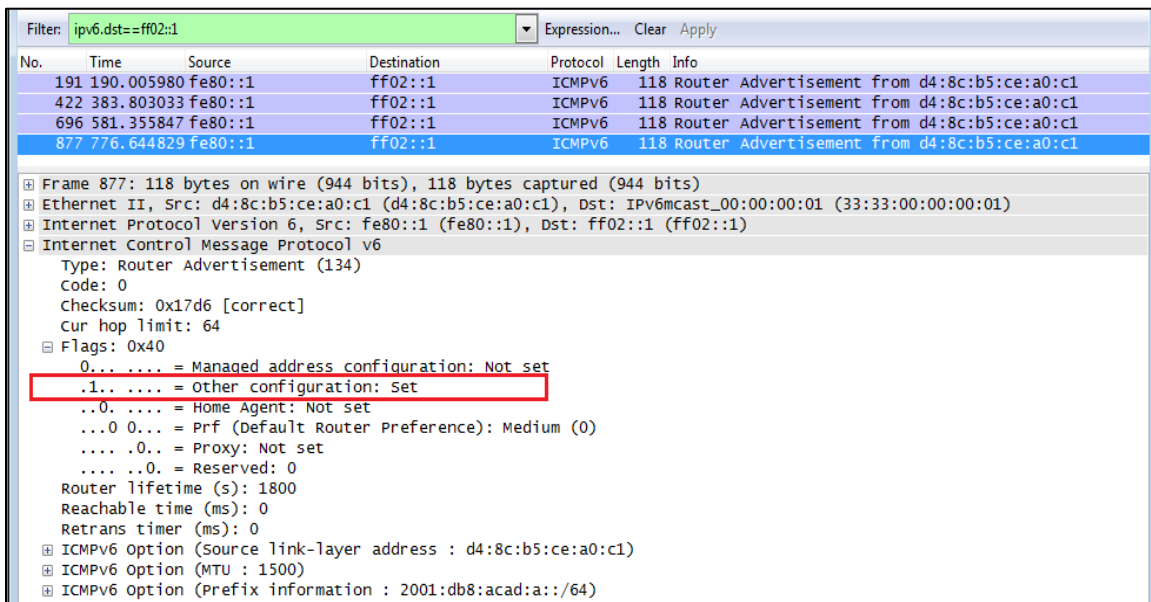
Adaptador de túnel isatap.localdomain:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
Descripción . . . . . : Adaptador ISATAP de Microsoft
Dirección física. . . . . : 00-00-00-00-00-00-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí

```



Step 4: ver los mensajes RA en Wireshark.

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



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

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

```
R1# show ipv6 dhcp binding
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
```

```
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-64-60-25-1E-00-02-16-21-E3-96
IA PD: IA ID 31356, T1 0, T2 0
Prefix: 0.0.0.0/0
preferred lifetime 0, valid lifetime 0
expires at mayo 18 2015 6:54:52 pm (0 seconds)
R1#
R1#
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
R1#
```

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

- Desactive la interfaz F0/6 del S1.

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

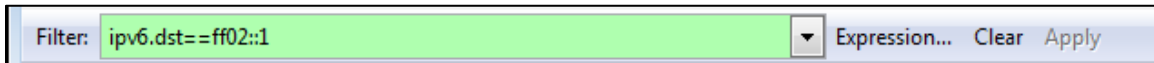
```
S1(config)# interface f0/6
S1(config-if)# shutdown
```

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

Part 17: configurar la red para DHCPv6 con estado

Step 1: preparar la PC-A.

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



Step 2: cambiar el pool de DHCPv6 en el R1.

- Agregue el prefijo de red al pool.

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

➤ Este comando no es soportado por el simulador Packet Tracer.

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

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

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

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

- Verifique la configuración del pool de DHCPv6.

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

```
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
R1#
```

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

```
R1# debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
```

```
R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R1#
```

Step 3: establecer el indicador en G0/1 para DHCPv6 con estado.

Nota: la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.

```
R1(config)# interface g0/1
R1(config-if)# shutdown
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# no shutdown
R1(config-if)# end
```

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

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

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

R1(config-if)#ipv6 nd managed-config-flag
R1(config-if)#no shutdown

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

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

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

R1#
```

Step 4: habilitar la interfaz F0/6 en el S1.

Ahora que configuró el R1 para DHCPv6 con estado, puede volver a conectar la PC-A a la red activando la interfaz F0/6 en el S1.

```
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# end
```

```
S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#no shutdown

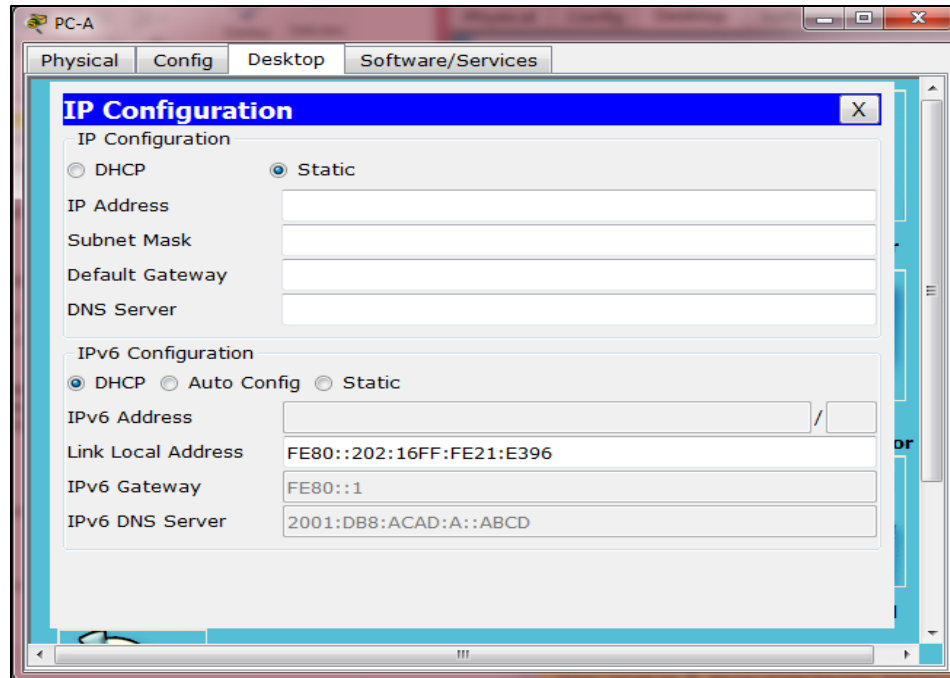
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to down
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

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

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

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:2
    FF02::1:FF00:1
    FF05::1:3
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use DHCP to obtain routable addresses.
  Hosts use DHCP to obtain other configuration.
```


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



➤ No hay un resultado en el campo de dirección IPv6 simplemente porque el simulador no soporta el comando `R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64`

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

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred
  86400 (1 in use, 0 conflicts)
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 1
```

```
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
R1#
```

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

```
R1# show ipv6 dhcp binding
```

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

```
DUID: 0001000117F6723D000C298D5444
```

```
Username : unassigned
```

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

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

```
preferred lifetime 86400, valid lifetime 172800
```

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

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

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

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

```
R1# u all
```

```
Se ha desactivado toda depuración posible
```

```
R1#
R1#undebg all
All possible debugging has been turned off
R1#
```

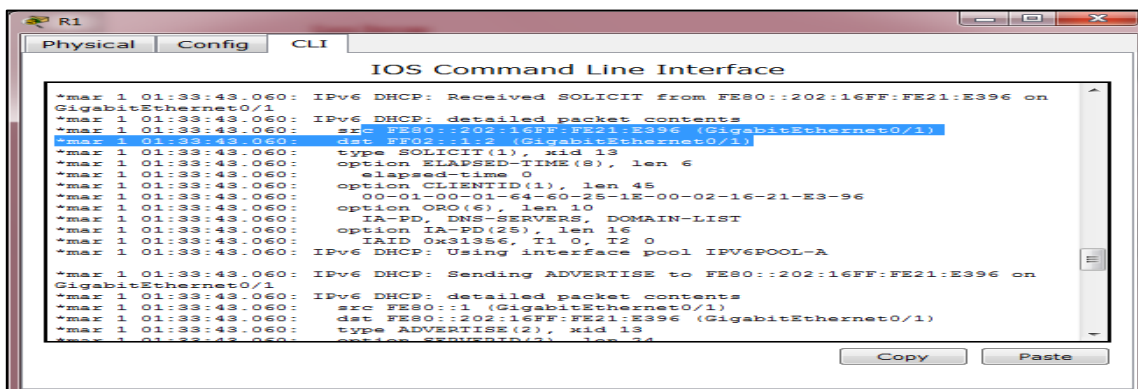
f. Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.

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

```
*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from
FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1
*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.775: dst FF02::1:2
*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238
*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2
*Mar 5 16:42:39.775: elapsed-time 6300
*Mar 5 16:42:39.775: option CLIENTID(1), len 14
```

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

```
*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A
on GigabitEthernet0/1
*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.779: src FE80::1
*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.779: type REPLY(7), xid 1039238
*Mar 5 16:42:39.779: option SERVERID(2), len 10
*Mar 5 16:42:39.779: 00030001FC994775C3E0
*Mar 5 16:42:39.779: option CLIENTID(1), len 14
*Mar 5 16:42:39.779: 00010001
R1#17F6723D000C298D5444
*Mar 5 16:42:39.779: option IA-NA(3), len 40
*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120
*Mar 5 16:42:39.779: option IAADDR(5), len 24
*Mar 5 16:42:39.779: IPv6 address
2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar 5 16:42:39.779: preferred 86400, valid 172800
*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com
```



```
R1
Physical Config CLI
IOS Command Line Interface
*Mar 1 01:33:43.060: IPv6 DHCP: Received SOLICIT from FE80::202:16FF:FE21:E396 on
GigabitEthernet0/1
*Mar 1 01:33:43.060: IPv6 DHCP: detailed packet contents
*Mar 1 01:33:43.060: src FE80::202:16FF:FE21:E396 (GigabitEthernet0/1)
*Mar 1 01:33:43.060: dst FF02::1:2 (GigabitEthernet0/1)
*Mar 1 01:33:43.060: type SOLICIT(1), xid 13
*Mar 1 01:33:43.060: option ELAPSED-TIME(8), len 6
*Mar 1 01:33:43.060: elapsed-time 0
*Mar 1 01:33:43.060: option CLIENTID(1), len 45
*Mar 1 01:33:43.060: 00-01-00-01-64-60-25-1E-00-02-16-21-E3-96
*Mar 1 01:33:43.060: option ORO(6), len 10
*Mar 1 01:33:43.060: IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar 1 01:33:43.060: option IA-PD(25), len 16
*Mar 1 01:33:43.060: IAID 0x31356, T1 0, T2 0
*Mar 1 01:33:43.060: IPv6 DHCP: Using interface pool IPV6POOL-A
*Mar 1 01:33:43.060: IPv6 DHCP: Sending ADVERTISE to FE80::202:16FF:FE21:E396 on
GigabitEthernet0/1
*Mar 1 01:33:43.060: IPv6 DHCP: detailed packet contents
*Mar 1 01:33:43.060: src FE80::1 (GigabitEthernet0/1)
*Mar 1 01:33:43.060: dst FE80::202:16FF:FE21:E396 (GigabitEthernet0/1)
*Mar 1 01:33:43.060: type ADVERTISE(2), xid 13
*Mar 1 01:33:43.060: option SERVERID(2), len 10
*Mar 1 01:33:43.060: 00030001FC994775C3E0
R1#
```

```

R1
Physical Config CLI
IOS Command Line Interface

*mar 1 01:33:42.373: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for
FE80::202:16FF:FE21:E396, IAID 31356

*mar 1 01:33:42.373: IPv6 DHCP: Sending REPLY to FE80::202:16FF:FE21:E396 on
GigabitEthernet0/1
*mar 1 01:33:42.373: IPv6 DHCP: detailed packet contents
*mar 1 01:33:42.373:   src FE80::1 (GigabitEthernet0/1)
*mar 1 01:33:42.373:   dst FE80::202:16FF:FE21:E396 (GigabitEthernet0/1)
*mar 1 01:33:42.373:   type REPLY(7), xid 12
*mar 1 01:33:42.373:   option SERVERID(2), len 24
*mar 1 01:33:42.373:     0003000100603E511701
*mar 1 01:33:42.373:   option CLIENTID(1), len 45
*mar 1 01:33:42.373:     00-01-00-01-64-60-25-1E-00-02-16-21-E3-96
*mar 1 01:33:42.373:   option IA-PD(25), len 41
*mar 1 01:33:42.373:     IAID 0x31356, T1 0, T2 0
*mar 1 01:33:42.373:     option IAPREFIX(26), 29
*mar 1 01:33:42.373:       preferred 0, valid 0, prefix 0.0.0.0/0
*mar 1 01:33:42.373:   option DNS-SERVERS(23), len 20
*mar 1 01:33:42.373:     2001:DB8:ACAD:A::ABCD
*mar 1 01:33:42.373:   option DOMAIN-LIST(24), len 5
*mar 1 01:33:42.373:     ccna-StatefulDHCPv6.com

*mar 1 01:33:43.060: IPv6 DHCP: Received SOLICIT from FE80::202:16FF:FE21:E396 on
  
```

Step 6: verificar DHCPv6 con estado en la PC-A.

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

Filter: `ipv6.dst==ff02::1` Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|---------|-------------|----------|--------|---|
| 36 | 54.582255 | fe80::1 | ff02::1 | ICMPv6 | 118 | Router Advertisement from fc:99:47:75:c3:e1 |
| 265 | 215.309226 | fe80::1 | ff02::1 | ICMPv6 | 118 | Router Advertisement from fc:99:47:75:c3:e1 |
| 425 | 373.272435 | fe80::1 | ff02::1 | ICMPv6 | 118 | Router Advertisement from fc:99:47:75:c3:e1 |
| 553 | 554.893786 | fe80::1 | ff02::1 | ICMPv6 | 118 | Router Advertisement from fc:99:47:75:c3:e1 |
| 664 | 730.139576 | fe80::1 | ff02::1 | ICMPv6 | 118 | Router Advertisement from fc:99:47:75:c3:e1 |
| 775 | 922.720109 | fe80::1 | ff02::1 | ICMPv6 | 118 | Router Advertisement from fc:99:47:75:c3:e1 |

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

- Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x3a82 [correct]
 - Cur hop limit: 64
 - Flags: 0xc0
 - 1... .. = Managed address configuration: Set
 - .1... .. = Other configuration: Set
 - .0... .. = Home Agent: Not set
 - ...0 0... = Prf (Default Router Preference): Medium (0)
 -0.. = Proxy: Not set
 -0. = Reserved: 0
 - Router lifetime (s): 1800

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|------------|------------------------------|------------------------------|----------|--------|---|
| 250 | 443.078236 | fe80::d428:7de2:997ff02::1:2 | | DHCPv6 | 146 | Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c298d5444 |
| 267 | 475.083284 | fe80::d428:7de2:997ff02::1:2 | | DHCPv6 | 146 | Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c298d5444 |
| 425 | 656.281211 | fe80::d428:7de2:997ff02::1:2 | | DHCPv6 | 146 | Solicit XID: 0xc86c32 CID: 0001000117f6723d000c298d5444 |
| 429 | 656.282249 | fe80::1 | fe80::d428:7de2:997ff02::1:2 | DHCPv6 | 191 | Advertise XID: 0xc86c32 CID: 0001000117f6723d000c298d5444 |
| 460 | 657.292018 | fe80::d428:7de2:997ff02::1:2 | | DHCPv6 | 188 | Request XID: 0xc86c32 CID: 0001000117f6723d000c298d5444 |
| 462 | 657.292638 | fe80::1 | fe80::d428:7de2:997ff02::1:2 | DHCPv6 | 191 | Reply XID: 0xc86c32 CID: 0001000117f6723d000c298d5444 |
| <div style="border: 1px solid gray; padding: 5px;"> <div style="border: 1px solid gray; padding: 2px;">Ethernet II, Src: fc:99:47:75:c3:e1 (Fc:99:47:75:c3:e1), Dst: Vmware_be:6c:89 (00:50:56:be:6c:89)</div> <div style="border: 1px solid gray; padding: 2px;">Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)</div> <div style="border: 1px solid gray; padding: 2px;">User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)</div> <div style="border: 1px solid gray; padding: 2px;">DHCPv6 <ul style="list-style-type: none"> Message type: Reply (7) Transaction ID: 0xc86c32 Server Identifier: 00030001fc994775c3e0 Client Identifier: 0001000117f6723d000c298d5444 Identity Association for Non-temporary Address <ul style="list-style-type: none"> Option: Identity Association for Non-temporary Address (3) Length: 40 Value: 0e000c290000a8c000010e000005001820010db8acad000a... IAID: 0e000c29 T1: 43200 T2: 69120 IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce DNS recursive name server <ul style="list-style-type: none"> Option: DNS recursive name server (23) Length: 16 Value: 20010db8acad000a000000000000abcd DNS servers address: 2001:db8:acad:a:abcd Domain Search List <ul style="list-style-type: none"> Option: Domain Search List (24) Length: 25 Value: 1363636e612d537461746566756c44484350763603636f6d... DNS Domain Search List <ul style="list-style-type: none"> Domain: ccna-StatefulDHCPv6.com </div> </div> | | | | | | |

Reflexión

1. ¿Qué método de direccionamiento IPv6 utiliza más recursos de memoria en el router configurado como servidor de DHCPv6: DHCPv6 sin estado o DHCPv6 con estado? ¿Por qué?
 - DHCP V6 con estado usa más recursos ya que requiere que el router guarde dinámicamente el estado de cada uno de los clientes.
 - En el caso de DHCP V6 sin estado entendemos que los clientes no usan el servidor DCHP para obtener las direcciones por tal motivo estas no necesitan ser guardadas.

2. ¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado?
 - CISCO recomienda DHCPV6 sin estado cuando se implementa redes V6 sin un registro de red CISCO.

Tabla de resumen de interfaces del router

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

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

10.3.1.1 IDT Y DHCP

10.3.1.1 PACKET TRACER - IDT Y DHCP

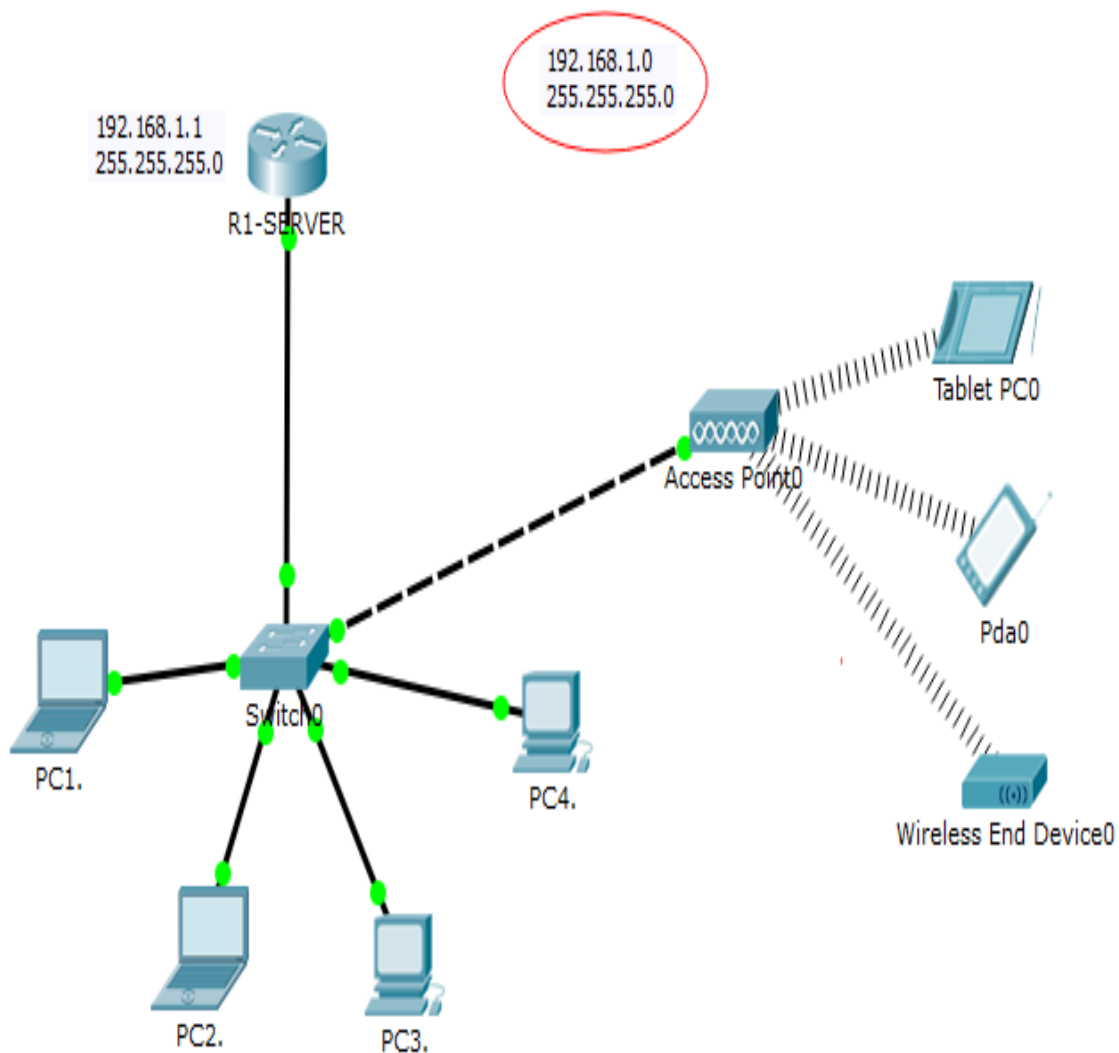
Objetivo

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

Situación

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

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



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

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

Recursos necesarios

Software de Packet Tracer

Reflexión

1. ¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica? ¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?
Utilizaríamos un router 1941 ya que este dispositivo funciona para brindarnos el servicio DHCP, de esta manera estaríamos posibilitando la opción de obviar la adquisición de un servidor DHCP.
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.
 - *El hecho de utilizar e implementar el servicio DHCP dentro de una empresa nos posibilita como administradores la posibilidad de ahorrar mucho tiempo de administración de la red, además de conectar infinidad de dispositivos que gracias a los adelantos en la tecnología de nuestros días han posibilitado.*
 - *Por el crecimiento exponencial que ha vivido internet fue necesario cambiar al direccionamiento IPV6 con el cual se puede asignar direcciones IPV6 a infinidad de dispositivos, dentro de muy poco todo estará conectado y con más razón necesitaremos de un método que realice esta asignación de manera automática DHCP.*
 - *Tenemos en la actualidad la posibilidad de tener acceso a la información en tiempo real, los dispositivos los podemos manejar de manera distante gracias a que cada uno de ellos está conectado a la red, lo podemos modificar de acuerdo a las necesidades que nosotros tengamos.*
 - *Todas las empresas están sacando el mayor provecho de las tecnologías que surgen en el momento, muchas de las tareas de las mismas ya se realizan conectadas, actualizando y teniendo acceso a infinidad de información que se les refleja en utilidades para la misma.*
 - *Gracias a la tecnología el crecimiento que han vivido las empresas ha sido posible, hay mucho más control de cada una de sus parte posibilitando el crecimiento en muchos casos de manera automática con una simple autorización.*

11.2.2.6 CONFIGURACIÓN DE NAT DINÁMICA Y ESTÁTICA

11.2.2.6 PACKET TRACER - CONFIGURACIÓN DE NAT DINÁMICA Y ESTÁTICA

Topología

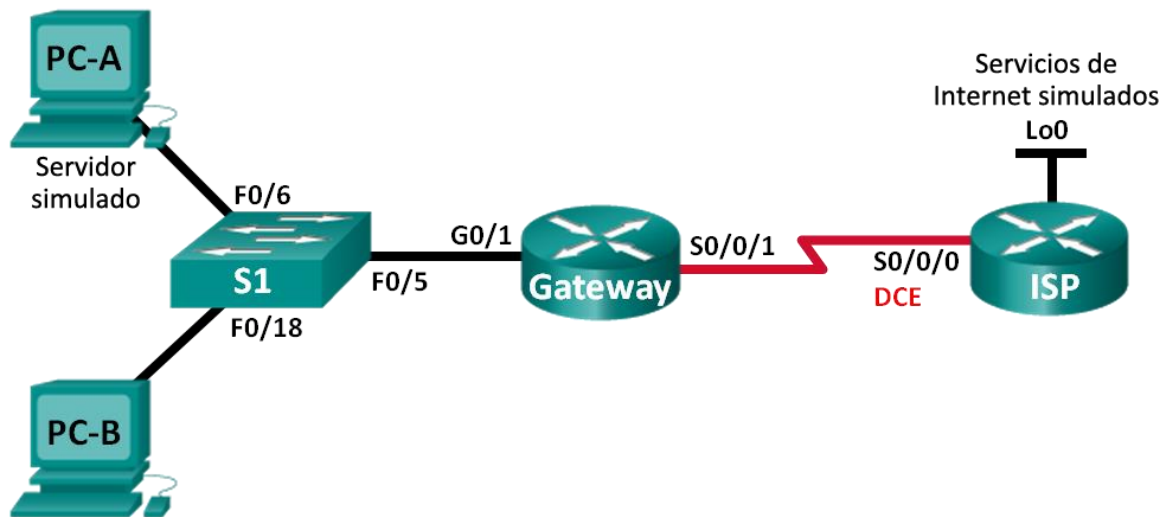


Tabla de direccionamiento

| 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 | 192.31.7.1 | 255.255.255.255 | N/A |
| PC-A (servidor simulado) | NIC | 192.168.1.20 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.1.21 | 255.255.255.0 | 192.168.1.1 |

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

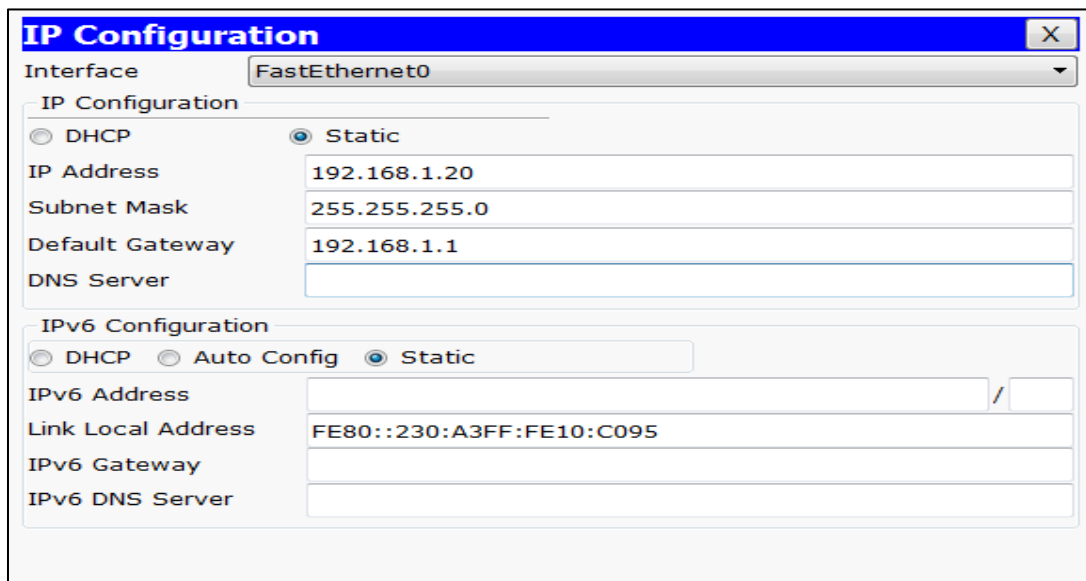
Parte1. armar la red y verificar la conectividad

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.

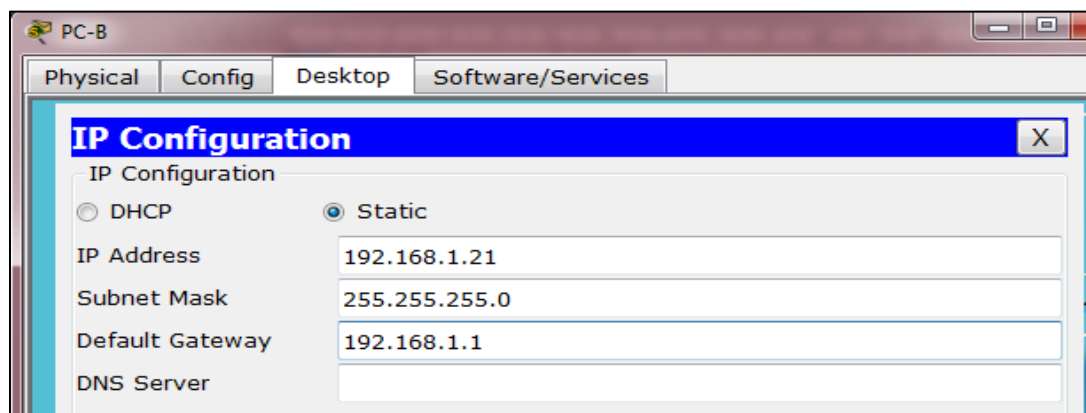
Step 7: realizar el cableado de red tal como se muestra en la topología.

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

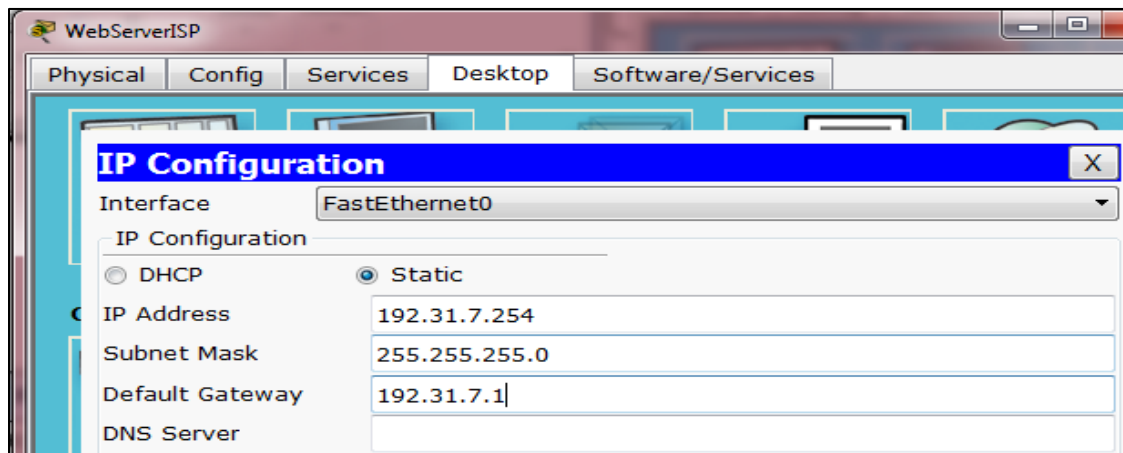
Step 8: configurar los equipos host.



The screenshot shows the 'IP Configuration' window in Cisco IOS. The 'Interface' is set to 'FastEthernet0'. Under 'IP Configuration', 'Static' is selected. The fields are filled with: IP Address: 192.168.1.20, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1, and DNS Server: (empty). Under 'IPv6 Configuration', 'Static' is selected. The fields are filled with: IPv6 Address: (empty), Link Local Address: FE80::230:A3FF:FE10:C095, IPv6 Gateway: (empty), and IPv6 DNS Server: (empty).



The screenshot shows a Windows PC window titled 'PC-B' with tabs for 'Physical', 'Config', 'Desktop', and 'Software/Services'. The 'Config' tab is active, showing the 'IP Configuration' window. Under 'IP Configuration', 'Static' is selected. The fields are filled with: IP Address: 192.168.1.21, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1, and DNS Server: (empty).



Step 9: inicializar y volver a cargar los routers y los switches según sea necesario.

Step 10: configurar los parámetros básicos para cada router.

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

Step 11: crear un servidor web simulado en el ISP.

➤ Comando no soportados por Packet Tracer.

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

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

- b. Habilite el servicio del servidor HTTP en el ISP.

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

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

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

Step 12: configurar el routing estático.

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

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

```
ISP#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

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

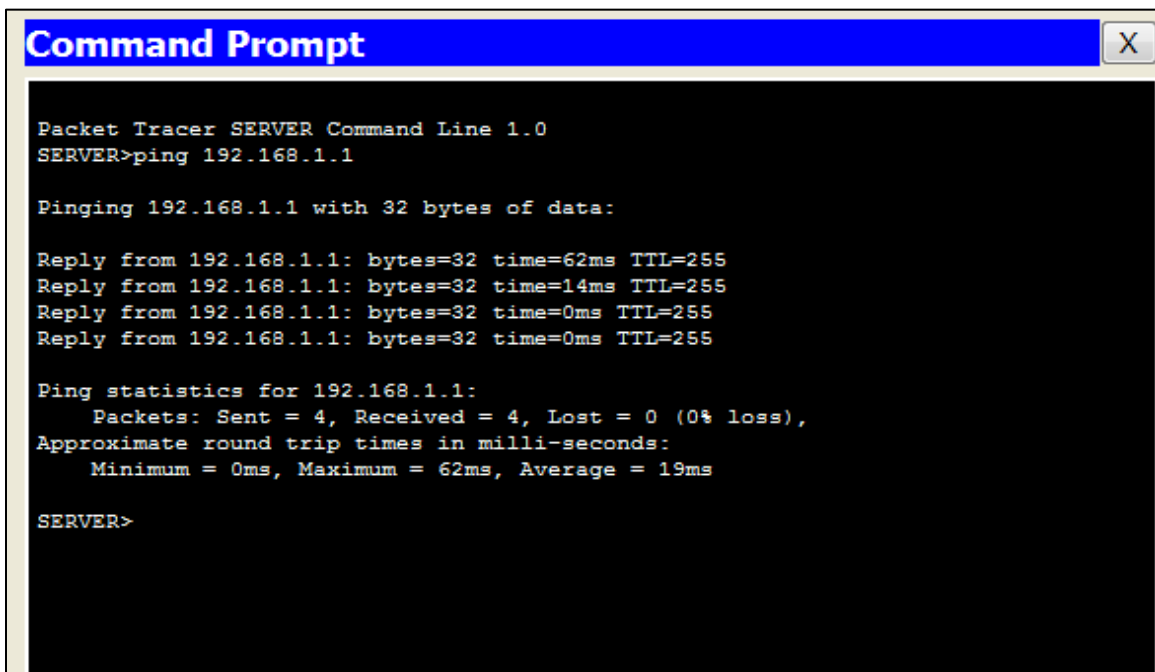
```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

```
Gateway#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Step 13: Guardar la configuración en ejecución en la configuración de inicio.

Step 14: 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.



```
Command Prompt
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=62ms TTL=255
Reply from 192.168.1.1: bytes=32 time=14ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 62ms, Average = 19ms

SERVER>
```

Command Prompt

X

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=13ms 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=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms

PC>
```

- Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.

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

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

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

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

Gateway of last resort is not set

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

Part 18: 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.

Step 1: configurar una asignación estática.

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

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

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

Step 2: Especifique las interfaces.

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

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



```

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

```

Step 3: probar la configuración.

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

```

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

```

```

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

```

Gateway#

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

192.168.1.20 =

209.165.200.225

¿Quién asigna la dirección global interna?

Esta dirección es asignada por el ROUTER del POOL que hemos asignado.

¿Quién asigna la dirección local interna?

Esto solo lo hace el administrador de la red.

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

```

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

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 26ms, Average = 7ms

SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

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

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

SERVER>

```

```

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

```

```

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

Gateway#
Gateway#
Gateway#
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:13 192.168.1.20:13  192.31.7.1:13     192.31.7.1:13
icmp 209.165.200.225:14 192.168.1.20:14  192.31.7.1:14     192.31.7.1:14
icmp 209.165.200.225:15 192.168.1.20:15  192.31.7.1:15     192.31.7.1:15
icmp 209.165.200.225:16 192.168.1.20:16  192.31.7.1:16     192.31.7.1:16
icmp 209.165.200.225:17 192.168.1.20:17  192.31.7.1:17     192.31.7.1:17
icmp 209.165.200.225:18 192.168.1.20:18  192.31.7.1:18     192.31.7.1:18
icmp 209.165.200.225:19 192.168.1.20:19  192.31.7.1:19     192.31.7.1:19
icmp 209.165.200.225:20 192.168.1.20:20  192.31.7.1:20     192.31.7.1:20
--- 209.165.200.225    192.168.1.20    ---                ---

Gateway#
Gateway#
Gateway#

```

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?

13.....20.

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

Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225    192.168.1.20    ---                ---
tcp 209.165.200.225:1025 192.168.1.20:1025 192.31.7.1:23     192.31.7.1:23

Gateway#

```

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

¿Qué protocolo se usó para esta traducción?

TCP

¿Cuáles son los números de puerto que se usaron?

1025 - 23

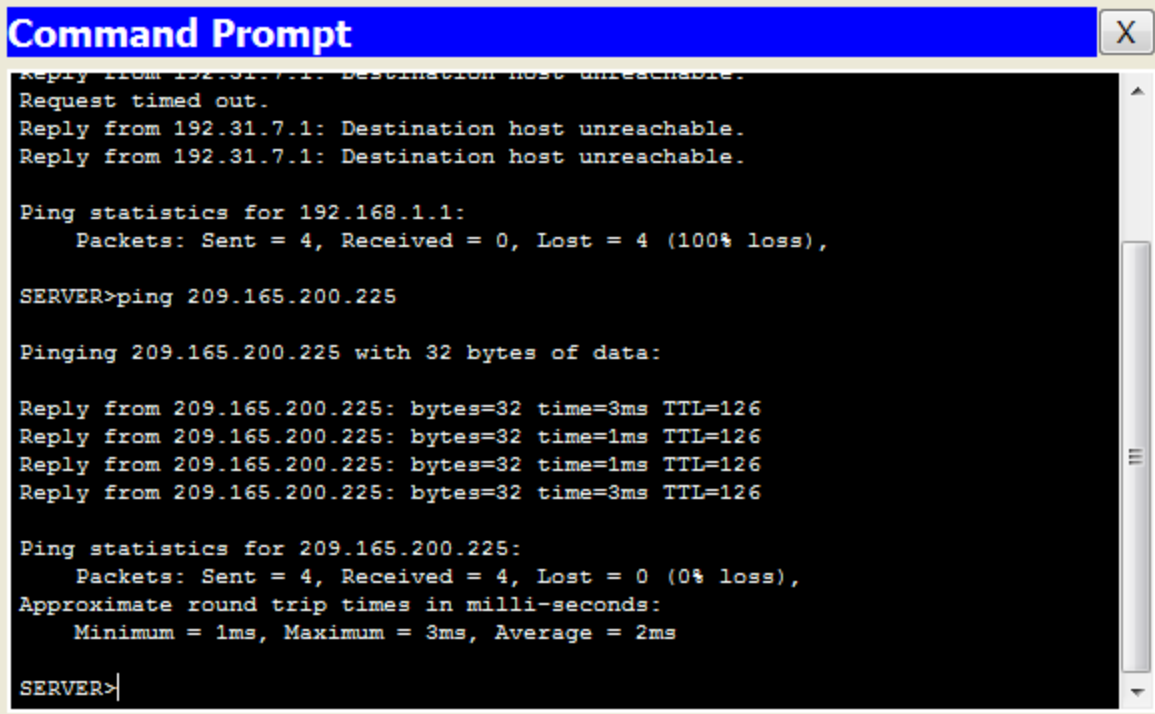
Global/local interno:

1025.

Global/local externo:

23

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



```
Command Prompt
Reply from 192.31.7.1: Destination host unreachable.
Request timed out.
Reply from 192.31.7.1: Destination host unreachable.
Reply from 192.31.7.1: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=3ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126
Reply from 209.165.200.225: bytes=32 time=1ms TTL=126
Reply from 209.165.200.225: bytes=32 time=3ms TTL=126

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

SERVER>
```

a. 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    ---                ---
```

```
tcp 209.165.200.225:1025192.168.1.20:1025 192.31.7.1:23 192.31.7.1:23
Gateway#
Gateway#
Gateway#
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.225:1025192.168.1.20:1025 192.31.7.1:23 192.31.7.1:23

Gateway#
Gateway#
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:10192.168.1.20:10 192.31.7.254:10 192.31.7.254:10
icmp 209.165.200.225:11192.168.1.20:11 192.31.7.254:11 192.31.7.254:11
icmp 209.165.200.225:12192.168.1.20:12 192.31.7.254:12 192.31.7.254:12
icmp 209.165.200.225:9 192.168.1.20:9 192.31.7.254:9 192.31.7.254:9
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.225:1025192.168.1.20:1025 192.31.7.1:23 192.31.7.1:23

Gateway#
Gateway#
```

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).

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

```
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
```

```
Peak translations: 2, occurred 00:02:12 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```

```
GigabitEthernet0/1
```

```
Hits: 39 Misses: 0
```

```
CEF Translated packets: 39, CEF Punted packets: 0
```

```
Expired translations: 3
```

```
Dynamic mappings:
```

```

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
-
Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 74 Misses: 29
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 0 (0%), misses 0
Gateway#

```

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

Part 19: 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.

Step 1: borrar las NAT.

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

```

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

Gateway#clear ip nat translation *
Gateway#clear ip nat statistics
      ^
% Invalid input detected at '^' marker.

Gateway#

```

Step 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
Gateway#
Gateway#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#

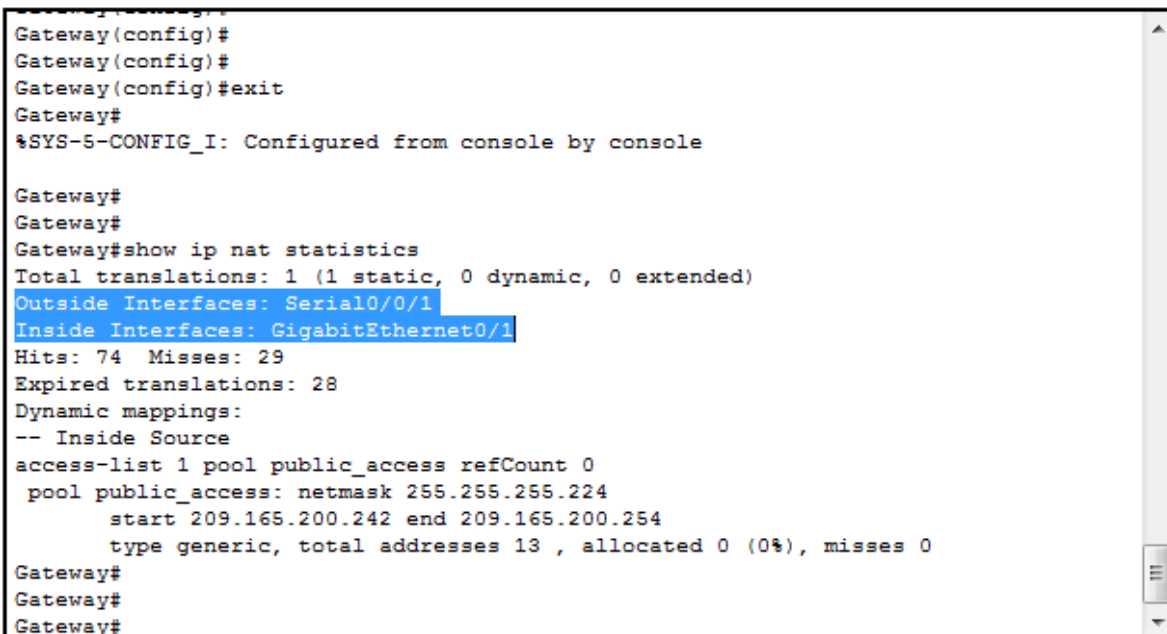
```

Step 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.

```
Gateway# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  FastEthernet0/1
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:

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



```
Gateway(config)#
Gateway(config)#
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console

Gateway#
Gateway#
Gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 74 Misses: 29
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13 , allocated 0 (0%), misses 0
Gateway#
Gateway#
Gateway#
```

Step 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
```

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

Gateway#
Gateway#
Gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 74 Misses: 29
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 0 (0%), misses 0
Gateway#
Gateway#
Gateway#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224
Gateway(config)#
```

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

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

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

Step 6: probar la configuración.

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=15ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=20ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 20ms, Average = 9ms

PC>
```

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

Gateway# show ip nat translations

Pro Inside global Inside local Outside local Outside global

```

--- 209.165.200.225    192.168.1.20    ---    ---
icmp 209.165.200.242:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1
--- 209.165.200.242    192.168.1.21    ---    ---
Gateway#
Gateway#show ip nat translations
Pro Inside global    Inside local    Outside local    Outside global
icmp 209.165.200.242:12 192.168.1.21:12 192.31.7.1:12 192.31.7.1:12
--- 209.165.200.225    192.168.1.20    ---    ---
Gateway#

```

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

192.168.1.21 =

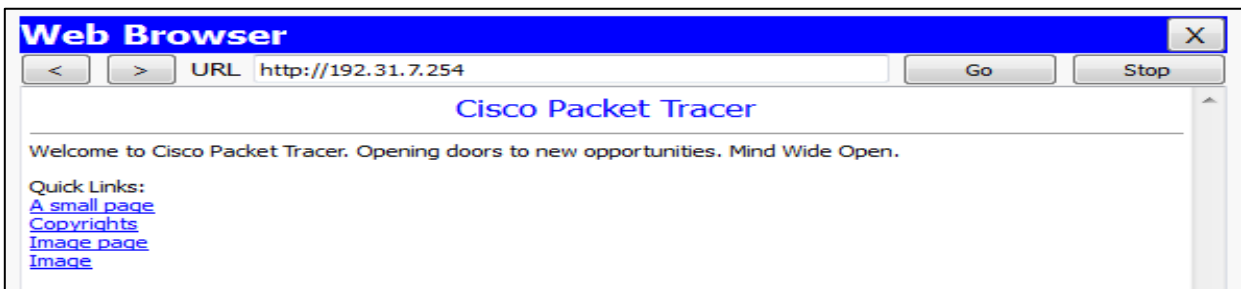
209.165.200.242

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

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

12

- 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**.



- a. Muestre la tabla de NAT.

```

Pro Inside global    Inside local    Outside local    Outside global
--- 209.165.200.225    192.168.1.20    ---    ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80 192.31.7.1:80

```



```

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

```

```

icmp 209.165.200.242:16192.168.1.21:16 192.31.7.1:16 192.31.7.1:16
--- 209.165.200.225 192.168.1.20 --- ---

Gateway#
Gateway#
Gateway#
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.242:1025192.168.1.21:1025 192.31.7.254:80 192.31.7.254:80

Gateway#
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.242:1025192.168.1.21:1025 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1026192.168.1.21:1026 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1027192.168.1.21:1027 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1028192.168.1.21:1028 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1029192.168.1.21:1029 192.31.7.254:80 192.31.7.254:80
tcp 209.165.200.242:1030192.168.1.21:1030 192.31.7.254:80 192.31.7.254:80

Gateway#|

```

Qué protocolo se usó en esta traducción? TCP

¿Qué números de puerto se usaron? Interno: 1025 a 1030. Externo: 80 ¿Qué número de puerto bien conocido y qué servicio se usaron? 80: WWW O HTTP

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

```

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

```

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

```
Gateway#show ip nat statistics
Total translations: 12 (1 static, 11 dynamic, 11 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 169 Misses: 53
Expired translations: 41
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 11
 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#
```

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

Step 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.

- 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
```

```
Gateway#config
Configuring from terminal, memory, or network [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)#
```

- Borre las NAT y las estadísticas.
- Haga ping al ISP (192.31.7.1) desde ambos hosts.
- 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 | --- | --- |

```
% Incomplete command.
Gateway#
Gateway#clear ip nat translation ?
  * Deletes all dynamic translations
Gateway#clear ip nat translation *
Gateway#
Gateway#
Gateway#
Gateway#
Gateway#show ip nat statistics
Total translations: 8 (0 static, 8 dynamic, 8 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 177 Misses: 61
Expired translations: 41
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 8
  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
Gateway#
Gateway#
```

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

```

Gateway#show ip nat translation
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.243:29 192.168.1.20:29  192.31.7.1:29     192.31.7.1:29
icmp 209.165.200.243:30 192.168.1.20:30  192.31.7.1:30     192.31.7.1:30
icmp 209.165.200.243:31 192.168.1.20:31  192.31.7.1:31     192.31.7.1:31
icmp 209.165.200.243:32 192.168.1.20:32  192.31.7.1:32     192.31.7.1:32
icmp 209.165.200.244:21 192.168.1.21:21  192.31.7.1:21     192.31.7.1:21
icmp 209.165.200.244:22 192.168.1.21:22  192.31.7.1:22     192.31.7.1:22
icmp 209.165.200.244:23 192.168.1.21:23  192.31.7.1:23     192.31.7.1:23
icmp 209.165.200.244:24 192.168.1.21:24  192.31.7.1:24     192.31.7.1:24

```

Gateway#

Reflexión

- ¿Por qué debe utilizarse la NAT en una red?
 - NAT es una muy buena alternativa poder salir a internet sin la necesidad de tener una gran cantidad de direcciones PUBLICAS que cuestan mucho.
- ¿Cuáles son las limitaciones de NAT?
 - Necesita información adicional como numero de Puerto e IP para la traducción.
 - Aún no soporta todos los protocolos.
 - Por los calculos adicionales que hay que realizar aumenta la LATENCIA.

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 CONFIGURACIÓN DE UN CONJUNTO DE NAT CON SOBRECARGA Y PAT

11.2.3.7 CONFIGURACIÓN DE UN CONJUNTO DE NAT CON SOBRECARGA Y PAT

Topología

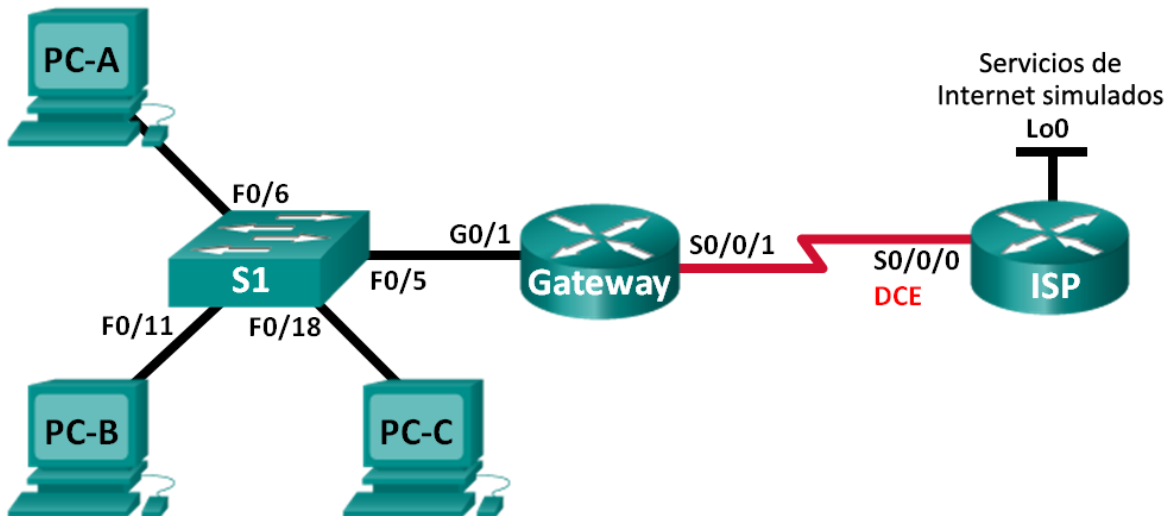


Tabla de direccionamiento

| 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

Recursos necesarios

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

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

Parte 1. armar la red y verificar la conectividad

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

Step 8: realizar el cableado de red tal como se muestra en la topología.

Step 9: configurar los equipos host.

Step 10: inicializar y volver a cargar los routers y los switches.

Step 11: configurar los parámetros básicos para cada router.

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

Step 12: configurar el routing estático.

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

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

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

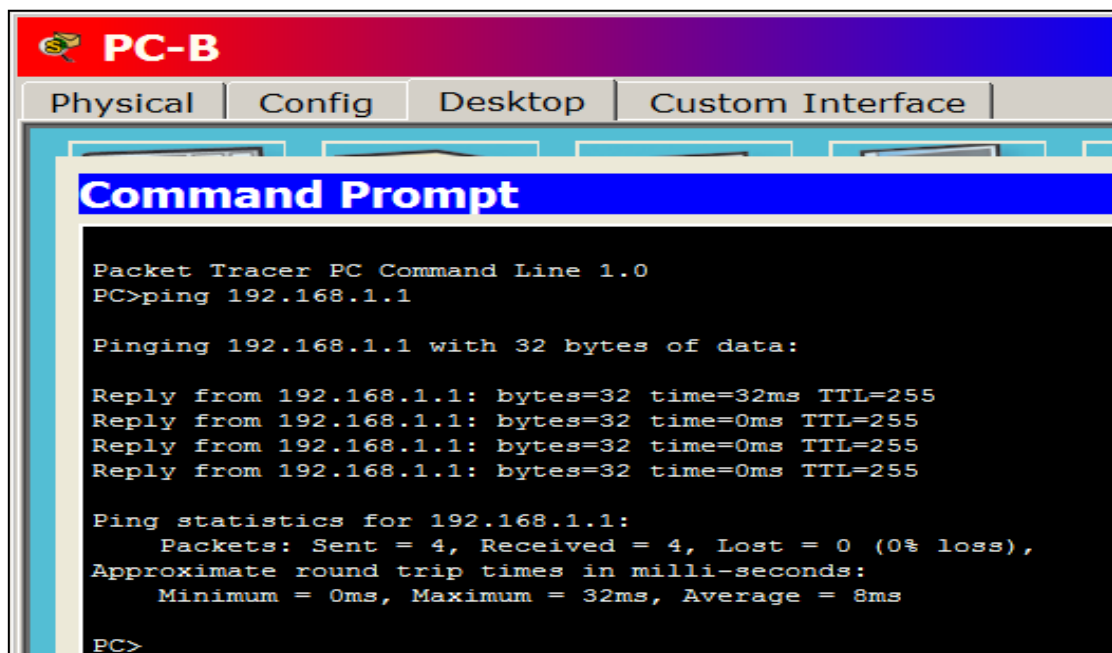
```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
Router(config)#hostname ISP
ISP(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
ISP(config)#
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.168.201.17
Gateway(config)#
```

Step 13: 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.



The screenshot shows a PC window titled "PC-B" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". A "Command Prompt" window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 32ms, Average = 8ms

PC>
```

Part 20: 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.

Step 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
```

Step 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
```

Step 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
```

Step 4: Especifique las interfaces.

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

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

```
Gateway(config)#  
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255  
Gateway(config)#ip nat pool public_access 209.165.200.225  
209.165.200.230 netmask 255.255.255.248  
Gateway(config)#ip nat inside source list 1 pool public_access overload  
Gateway(config)#interface g0/1  
Gateway(config-if)#ip nat inside  
Gateway(config-if)#interface s0/0/1  
Gateway(config-if)#ip nat outside  
Gateway(config-if)#exit  
Gateway(config)#exit  
Gateway#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Gateway#
```

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

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

```
Gateway# show ip nat statistics  
Total active translations: 3 (0 static, 3 dynamic; 3 extended)  
Peak translations: 3, occurred 00:00:25 ago  
Outside interfaces:  
Serial0/0/1
```

```

Inside interfaces:
  GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
  pool public_access: netmask 255.255.255.248
  start 209.165.200.225 end 209.165.200.230
  type generic, total addresses 6, allocated 1 (16%), misses 0

```

```

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

```

- c. Muestre las NAT en el router Gateway.

```

Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
icmp 209.165.200.225:0 192.168.1.20:1   192.31.7.1:1     192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1   192.31.7.1:1     192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1   192.31.7.1:1     192.31.7.1:2

```

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

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? 3

¿Cuántas direcciones IP globales internas se indican? 1

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? 12

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

El Ping fallaría ya que su dirección no se muestra para la salida sino se muestra una IP para salir hacia Internet. Porque NAT las protege y no deja que ISP las conozca por su IP original si no las que les pone NAT 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.

Step 6: borrar las NAT y las estadísticas en el router Gateway.

Step 7: verificar la configuración para NAT.

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

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

Show ip nat etatistics

Step 8: 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
```

Step 9: 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
```

Step 10: asociar la lista de origen a la interfaz externa.

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

Step 11: probar la configuración PAT.

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

- 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?

- Al utilizarse solo una IP pública que es la del interface se ahorran direcciones IP públicas, pueden salir 100 computadoras de una red privada con direcciones privadas con una sola IP pública y utilizando distintos puertos para diferenciar cada paquete que sale.
- Nivel de seguridad

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) |

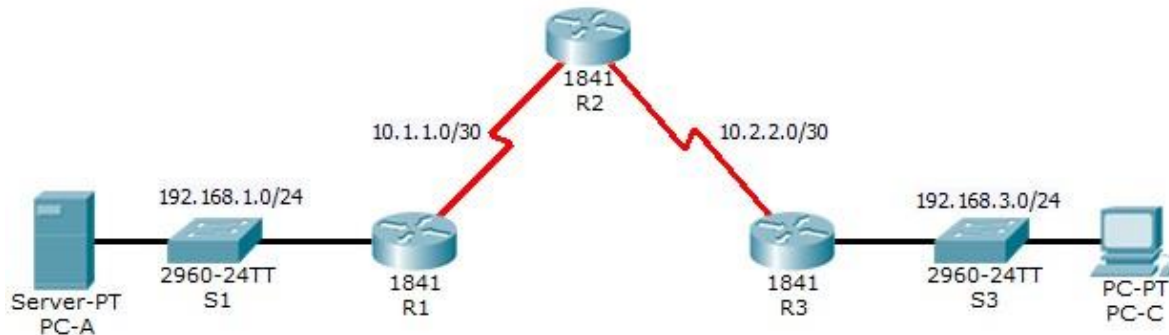
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores 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.

LISTAS DE ACCESO

4.4.1.2 CONFIGURE IP ACLS TO MITIGATE ATTACKS

4.4.1.2 PACKET TRACER - CONFIGURE IP ACLS TO MITIGATE ATTACKS

Topologia



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.

Part 1: Verify Basic Network Connectivity

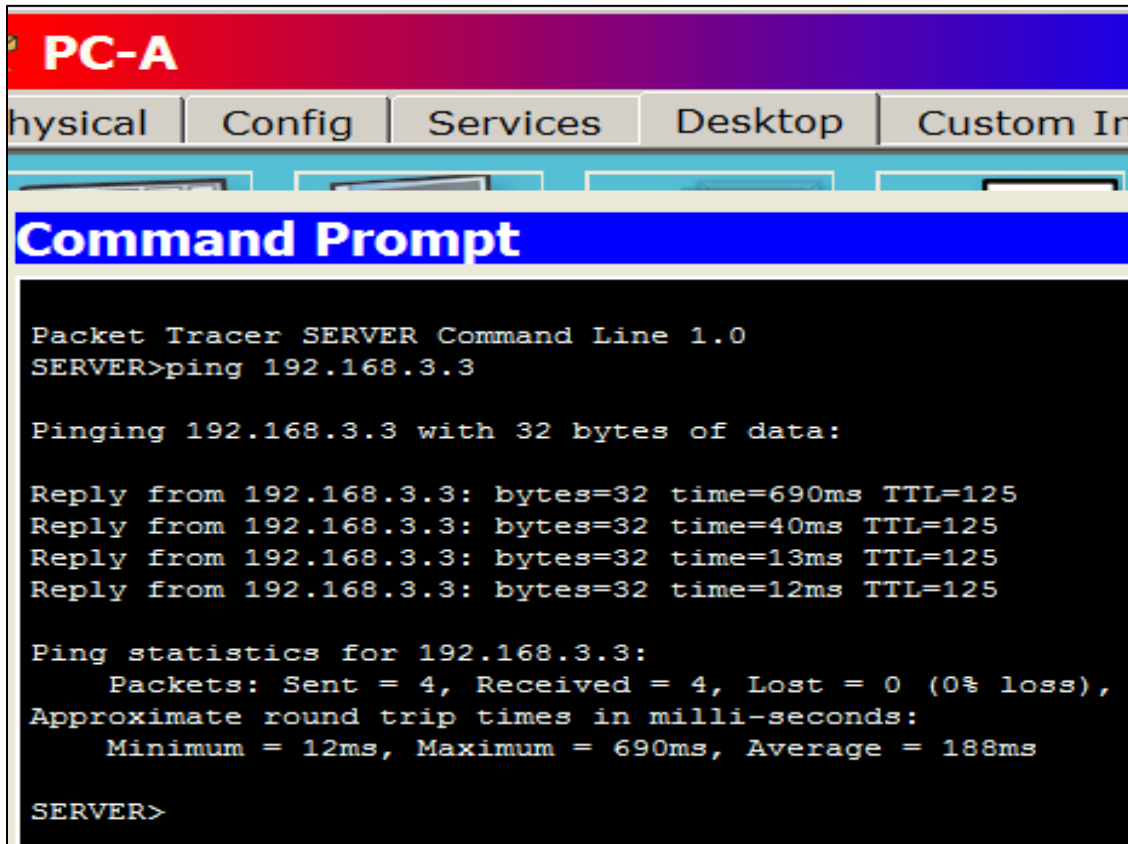
Verify network connectivity prior to configuring the IP ACLs.

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

- From the command prompt, ping **PC-C** (192.168.3.3).
- From the command prompt, establish a SSH session to **R2** Lo0 interface

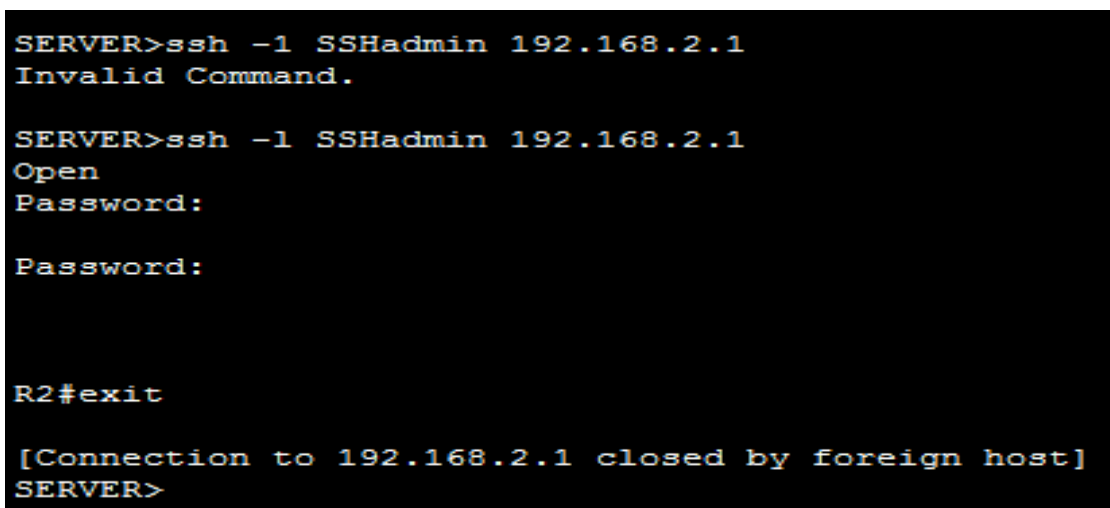
(192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. When finished, exit the SSH session.

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



The screenshot shows a Packet Tracer interface for PC-A. The 'Command Prompt' window is open, displaying the output of a ping command to 192.168.3.3. The output shows four successful replies with varying round-trip times (690ms, 40ms, 13ms, and 12ms) and a TTL of 125. Ping statistics indicate 4 packets sent, 4 received, and 0% loss, with an average round-trip time of 188ms.

```
PC-A  
Physical | Config | Services | Desktop | Custom In  
  
Command Prompt  
Packet Tracer SERVER Command Line 1.0  
SERVER>ping 192.168.3.3  
  
Pinging 192.168.3.3 with 32 bytes of data:  
  
Reply from 192.168.3.3: bytes=32 time=690ms TTL=125  
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125  
Reply from 192.168.3.3: bytes=32 time=13ms TTL=125  
Reply from 192.168.3.3: bytes=32 time=12ms TTL=125  
  
Ping statistics for 192.168.3.3:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 12ms, Maximum = 690ms, Average = 188ms  
  
SERVER>
```



The screenshot shows the SERVER Command Prompt. The user attempts to run the command 'ssh -l SSHadmin 192.168.2.1', which initially returns 'Invalid Command.'. After a second attempt, the session opens, and the user is prompted for a password. The user enters the password, and the session is closed with the message '[Connection to 192.168.2.1 closed by foreign host]'. The user then enters 'R2#exit' to return to the R2 prompt.

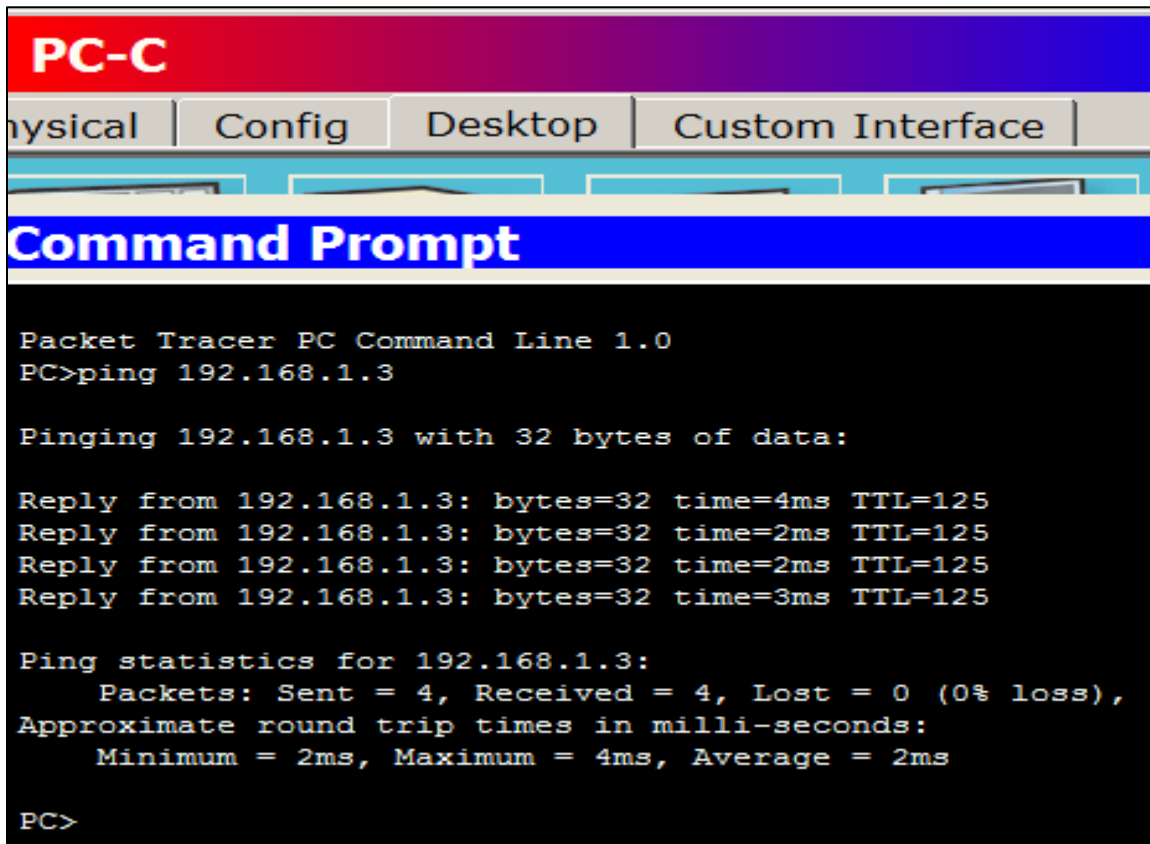
```
SERVER>ssh -l SSHadmin 192.168.2.1  
Invalid Command.  
  
SERVER>ssh -l SSHadmin 192.168.2.1  
Open  
Password:  
  
Password:  
  
R2#exit  
  
[Connection to 192.168.2.1 closed by foreign host]  
SERVER>
```

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

- a. From the command prompt, ping **PC-A** (192.168.1.3).
- b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. Close the SSH session when finished.

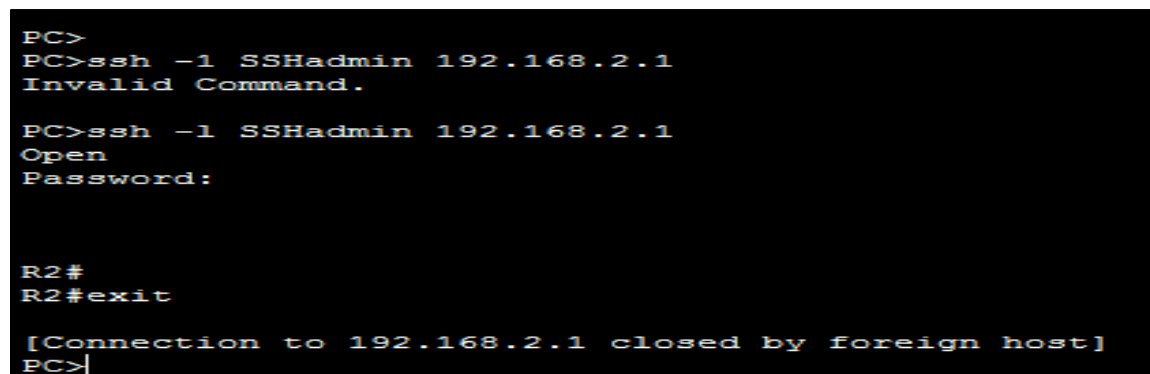
```
PC> ssh -l  
SSHadmin  
192.168.2.1
```

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



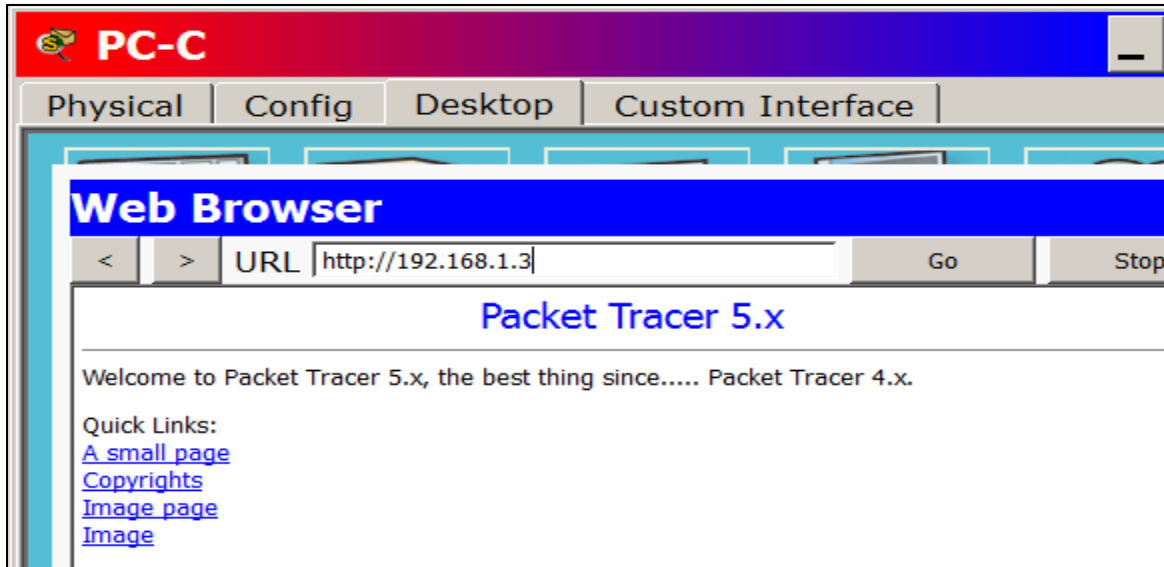
The screenshot shows the Packet Tracer interface for PC-C. The top navigation bar includes 'Physical', 'Config', 'Desktop', and 'Custom Interface'. Below this is a 'Command Prompt' window. The terminal output shows a successful ping to 192.168.1.3 with 4 packets sent and received, 0% loss, and round trip times between 2ms and 4ms.

```
Packet Tracer PC Command Line 1.0  
PC>ping 192.168.1.3  
  
Pinging 192.168.1.3 with 32 bytes of data:  
  
Reply from 192.168.1.3: bytes=32 time=4ms TTL=125  
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125  
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125  
Reply from 192.168.1.3: bytes=32 time=3ms TTL=125  
  
Ping statistics for 192.168.1.3:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 2ms, Maximum = 4ms, Average = 2ms  
  
PC>
```



The screenshot shows the Packet Tracer interface for PC-C. The terminal output shows an invalid SSH command followed by a successful SSH session to R2 (192.168.2.1) using the username SSHadmin. The session ends with the message '[Connection to 192.168.2.1 closed by foreign host]'.

```
PC>  
PC>ssh -l SSHadmin 192.168.2.1  
Invalid Command.  
  
PC>ssh -l SSHadmin 192.168.2.1  
Open  
Password:  
  
R2#  
R2#exit  
  
[Connection to 192.168.2.1 closed by foreign host]  
PC>
```



Part 2: Secure Access to Routers

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

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

```
R1(config)# access-list 10 permit  
192.168.3.3 0.0.0.0  
R2(config)# access-list 10 permit  
192.168.3.3 0.0.0.0  
R3(config)# access-list 10 permit  
192.168.3.3 0.0.0.0
```

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

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

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

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

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

```
R1 (config-line) #
access-class 10 in
R2 (config-line) #
access-class 10 in
R3 (config-line) #
access-class 10 in
```

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

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

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

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

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

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

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

```
R2#
R2#exit

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

R2#
```

```
R2#exit

[Connection to 192.168.2.1 closed by foreign host]
SERVER>
SERVER>ssh -l SSHadmin 192.168.2.1

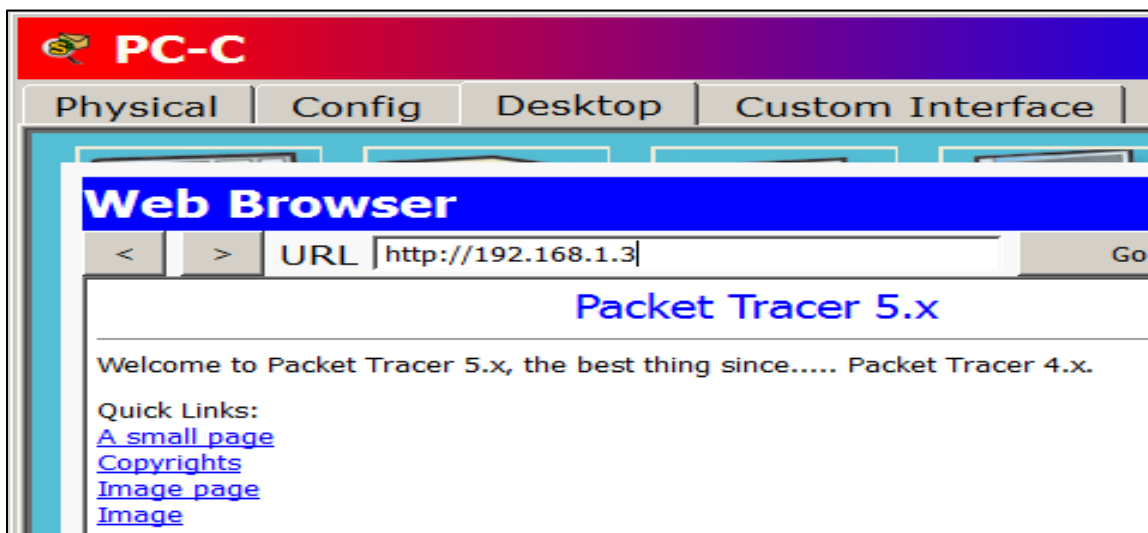
% Connection refused by remote host
SERVER>
```

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

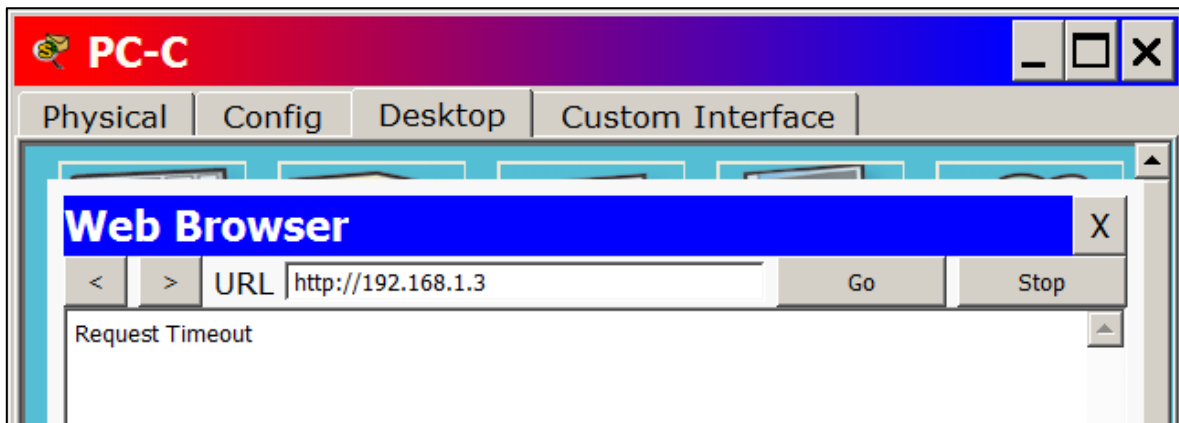
Step 3: Apply the ACL to interface S0/0/0.

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

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

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

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



Part 4: Modify An Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the

outside network (relative to R1);
deny all other incoming ICMP packets.

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.

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

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

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

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

```
% Connection refused by remote host  
SERVER>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),  
SERVER>
```

```
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)#
```

```

SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

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

SERVER>

```

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

```

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

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

```

R3(config)# interface fa0/1
R3(config-if)# ip access-group 110 in

R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#

```

Part 6: Create a Numbered IP ACL 100 on R3

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

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

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

address space specified in RFC 1918). Use the **access-list** command to create a numbered IP ACL.

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

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

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

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

Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

From the **PC-C** command prompt, ping the **PC-A** server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.

Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

```
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)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#
R3(config-if)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#
```


!!!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
```

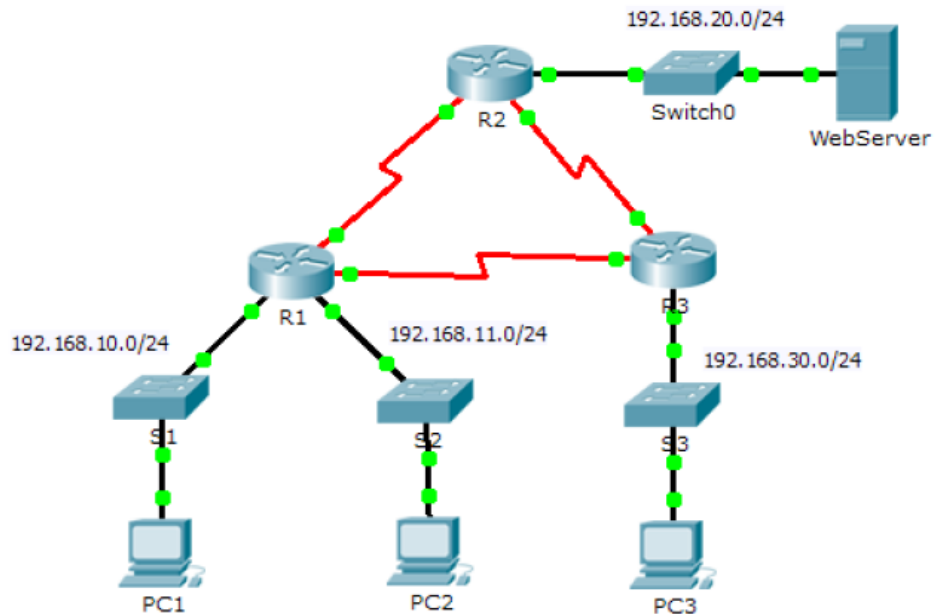
!!!Script for R3

```
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

9.2.1.10 PACKET TRACER -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 |
| R3 | F0/0 | 192.168.30.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 10.3.3.2 | 255.255.255.252 | N/A |
| | S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A |
| PC1 | NIC | 192.168.10.10 | 255.255.255.0 | 192.168.10.1 |
| PC2 | NIC | 192.168.11.10 | 255.255.255.0 | 192.168.11.1 |
| PC3 | NIC | 192.168.30.10 | 255.255.255.0 | 192.168.30.1 |
| WebServer | NIC | 192.168.20.254 | 255.255.255.0 | 192.168.20.1 |

Objectives

Part 1: Plan an ACL Implementation

Part 2: Configure, Apply, and Verify a Standard ACL Background / Scenario

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

Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.

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

Verificacion de conectividad:

```
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=2ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms 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 = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.10: bytes=32 time=2ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

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=3ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

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

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
```

```

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
C:\>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=2ms TTL=254
Reply from 192.168.20.1: bytes=32 time=1ms TTL=254
Reply from 192.168.20.1: bytes=32 time=1ms TTL=254
Reply from 192.168.20.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>ping 192.168.30.1
Pinging 192.168.30.1 with 32 bytes of data:
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=4ms TTL=254
Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 1ms
C:\>|

```

Step 2: Evaluate two network policies and plan ACL implementations.

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

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

To restrict access from the 192.168.11.0/24 network to the **WebServer** at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

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

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

To restrict access from the 192.168.10.0/24 network to the 192.168.30.0/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must be placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

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

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

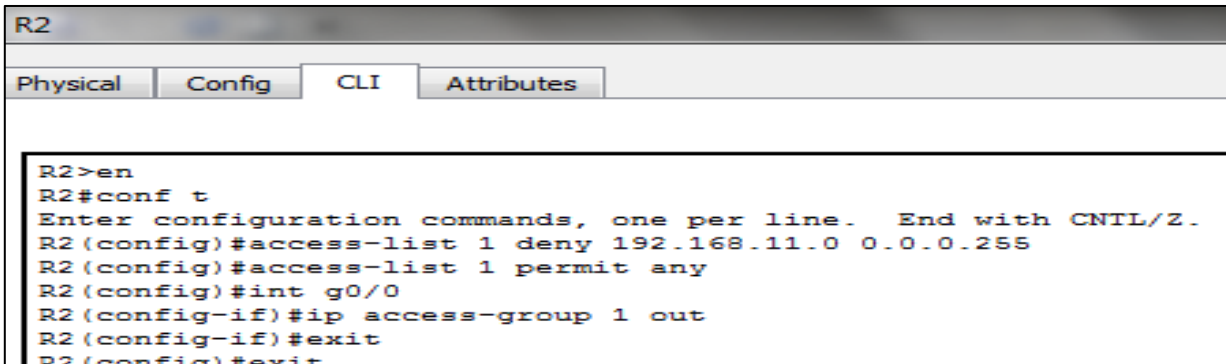
b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:

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

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

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

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

A screenshot of a network device's CLI interface for router R2. The interface has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The terminal output shows the following commands and prompts:

```
R2>en
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)#access-list 1 permit any
R2(config)#int g0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#exit
R2(config)#exit
```

Step 2: Configure and apply a numbered standard ACL on R3.

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

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

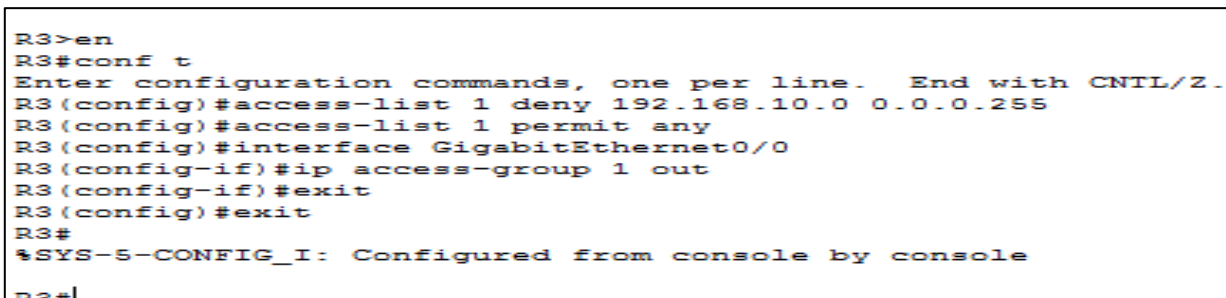
b. By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, create a second rule for ACL 1.

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

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

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

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

A screenshot of a network device's CLI interface for router R3. The terminal output shows the following commands and prompts:

```
R3>en
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)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

Step 3: Verify ACL configuration and functionality.

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

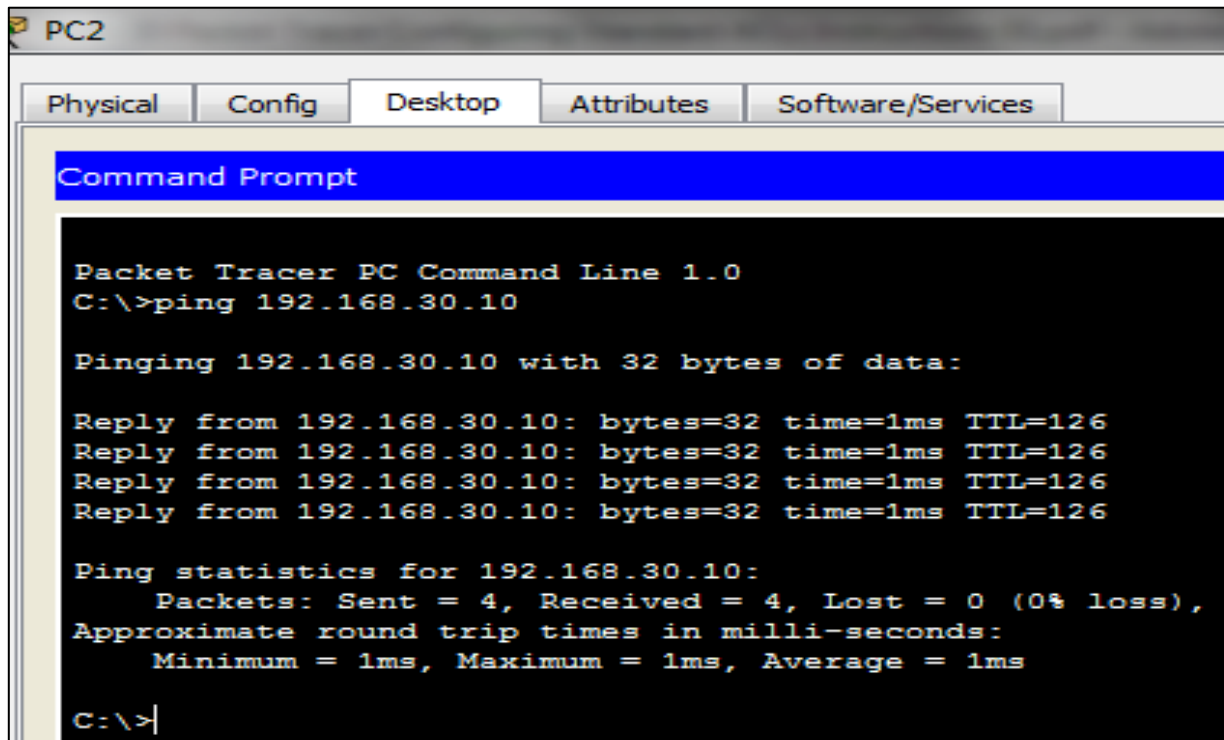
```
R2#show access-list
Standard IP access list 1
 10 deny 192.168.11.0 0.0.0.255
 20 permit any

R2#show run
Building configuration...

Current configuration : 1003 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
```

```
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description Link to R1
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 description Link to R3
 ip address 10.2.2.1 255.255.255.252
 clock rate 4000000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 passive-interface GigabitEthernet0/0
 network 192.168.20.0
 network 10.0.0.0
!
ip classless
!
ip flow-export version 9
!
!
access-list 1 deny 192.168.11.0 0.0.0.255
access-list 1 permit any
!
!
!
!
!
!
line con 0
 login
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```


PC-2:



The screenshot shows a Packet Tracer PC window for PC2. The 'Desktop' tab is active, displaying a Command Prompt window. The prompt shows the execution of a ping command to 192.168.30.10. The output indicates that all four packets were received with a 0% loss rate and a consistent 1ms round-trip time.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.10

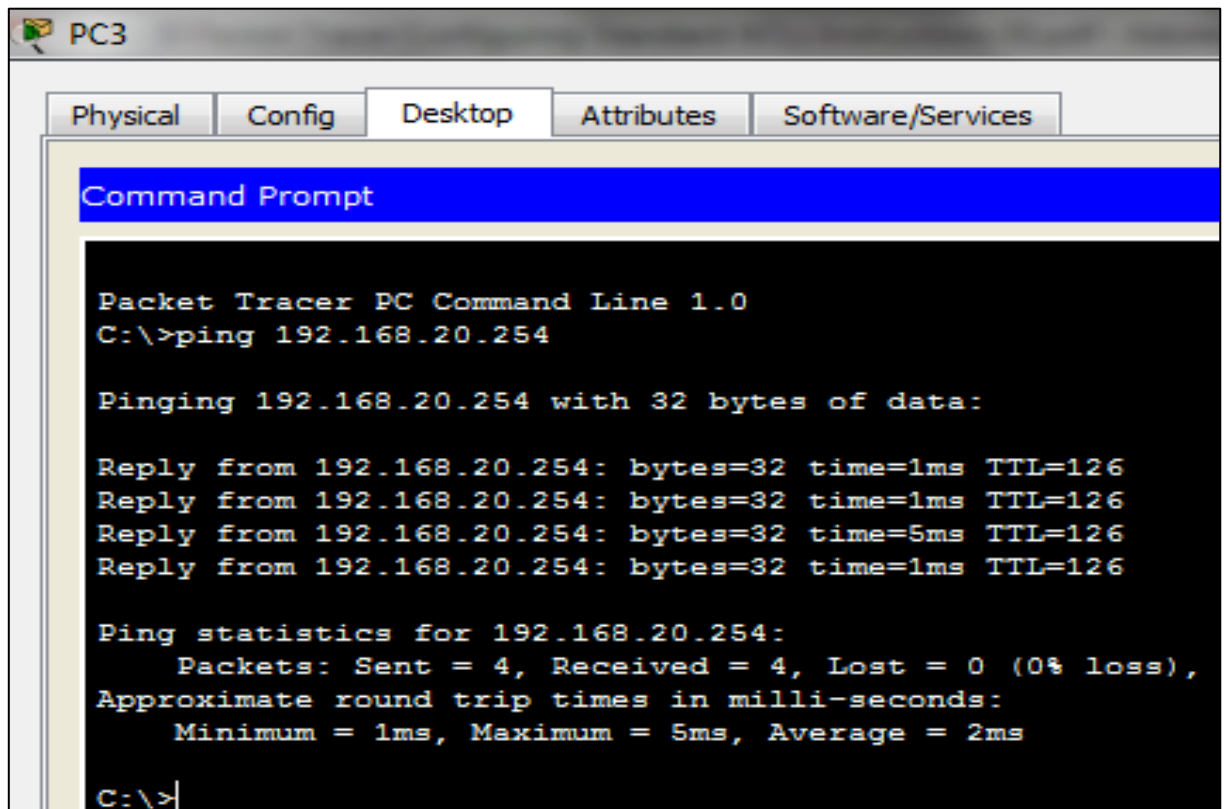
Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

PC-3:



The screenshot shows a Packet Tracer PC window for PC3. The 'Desktop' tab is active, displaying a Command Prompt window. The prompt shows the execution of a ping command to 192.168.20.254. The output indicates that all four packets were received with a 0% loss rate and round-trip times of 1ms, 1ms, 5ms, and 1ms.

```
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=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=5ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>
```

CHECK LIST

Activity Results Time Elapsed: 00:23:03

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

| Assessment Item | Status | Points | Component(s) | Feedback |
|--------------------|---------|--------|-----------------|-----------------|
| Network | | | | |
| R2 | | | | |
| ACL | Correct | 25 | ACL | IPV4 Standard.. |
| Ports | | 0 | Other | Other |
| GigabitEthernet0/0 | | 0 | Other | Other |
| Access-grou... | Correct | 25 | IPV4 Standard.. | |
| R3 | | | | |
| ACL | Correct | 25 | ACL | IPV4 Standard.. |
| Ports | | 0 | Other | Other |
| GigabitEthernet0/0 | | 0 | Other | Other |
| Access-grou... | Correct | 25 | IPV4 Standard.. | |

| Component | Items/Total | Score |
|----------------------------------|-------------|---------|
| IPV4 Standard ACL Implementation | 4/4 | 100/100 |

Score: 100/100
Item Count: 4/4

Cisco Packet Tracer - DiDiplomato Cisco/UNIDAD #2/CONJ R65 UNIDAD #1/USTAS DE ACCESO/9.1.1.30 Packet Tracer: Configuring Standard ACLs.pka Time Elapsed: 00:26:03

File | Edit | Options | View | Tools | Extensions | Help

Activity Results

Congratulations Guest! You completed the activity.

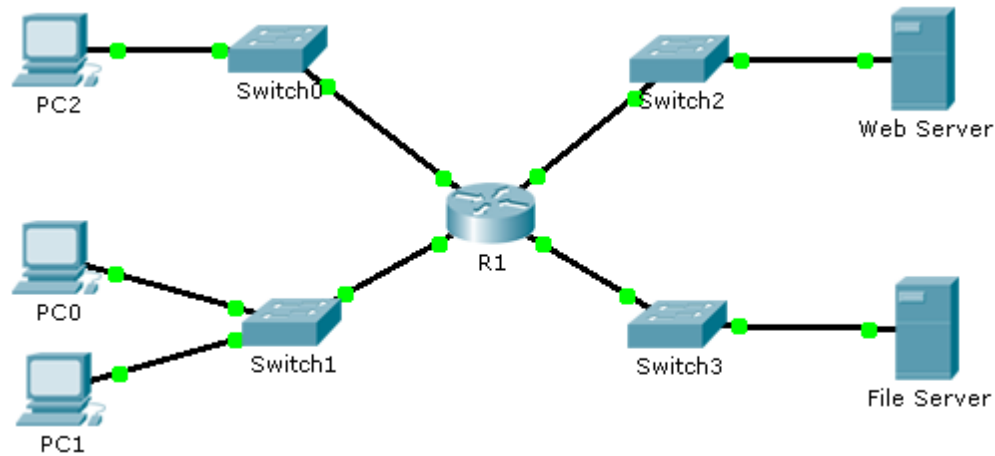
Overall Feedback | Assessment Items | Connectivity Tests

Congratulations! You successfully completed the Packet Tracer - Configuring Standard ACLs activity.

**9.2.1.11 PACKET TRACER -
CONFIGURING NAMED
STANDARD ACLS**

9.2.1.11 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

Part 1: Configure and Apply a Named Standard ACL

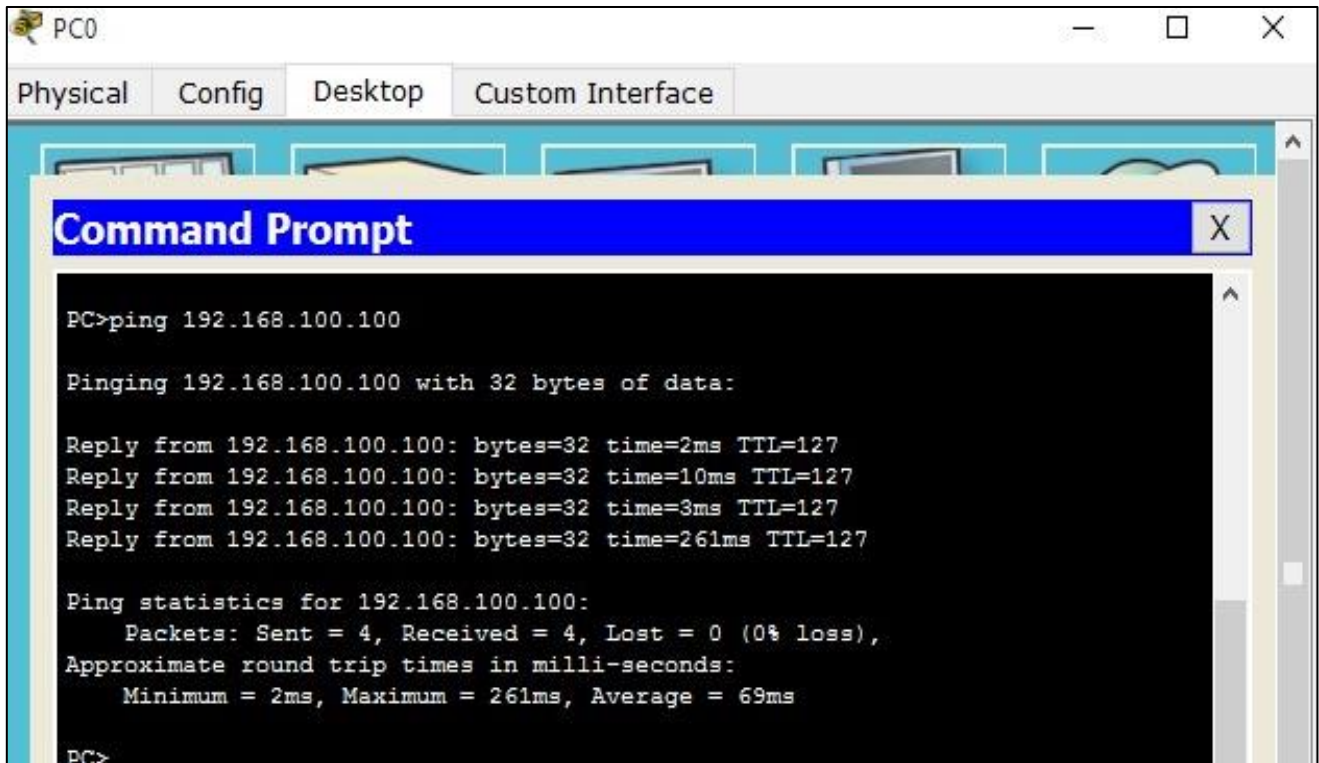
Step 1: Verify connectivity before the ACL is configured and applied.

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

Hacemos pings para probar conectividad desde los 3 PC's hacia los servidores.

Asi:

- Desde el PC0 al Web Server. (PC0 al 192.168.100.100)



The screenshot shows a window titled "PC0" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". A "Command Prompt" window is open, displaying the following text:

```
PC>ping 192.168.100.100

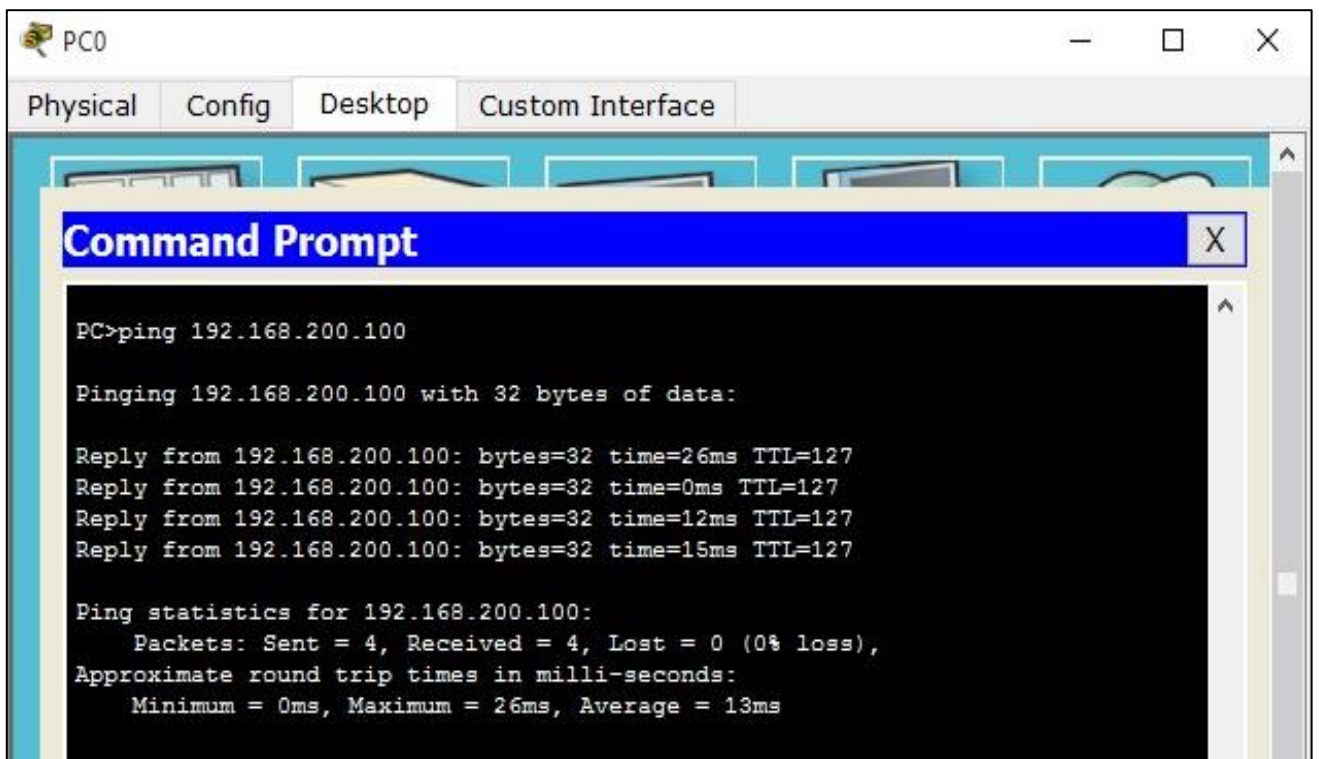
Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time=10ms TTL=127
Reply from 192.168.100.100: bytes=32 time=3ms TTL=127
Reply from 192.168.100.100: bytes=32 time=261ms 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 = 2ms, Maximum = 261ms, Average = 69ms

PC>
```

- Ping desde el PC0 al File Server: (PC0 al 192.168.200.100) : ping exitoso.



The screenshot shows a window titled "PC0" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". A "Command Prompt" window is open, displaying the following text:

```
PC>ping 192.168.200.100

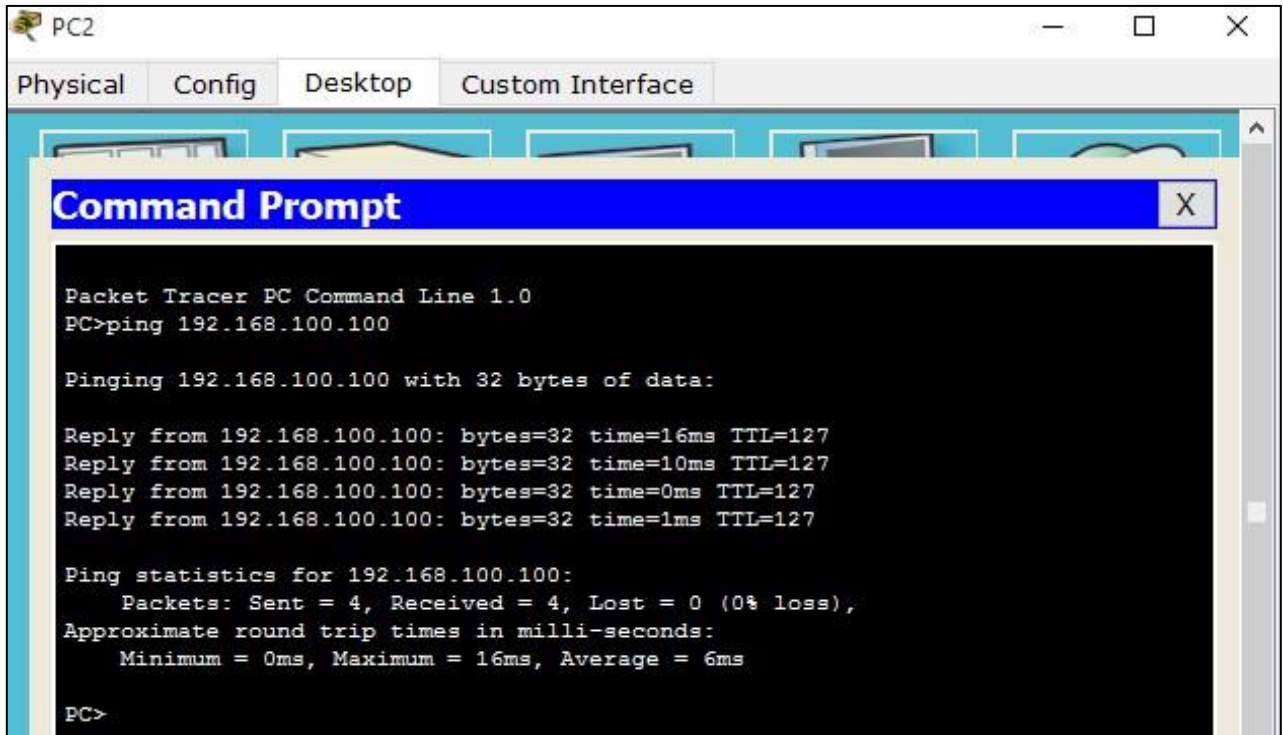
Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=26ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=12ms TTL=127
Reply from 192.168.200.100: bytes=32 time=15ms 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 = 26ms, Average = 13ms

--
```

- Ping desde el PC2 al Web Sever: (PC2 al 192.168.100.100):ping exitoso.



The screenshot shows a Packet Tracer PC window titled 'PC2' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. A 'Command Prompt' window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.100

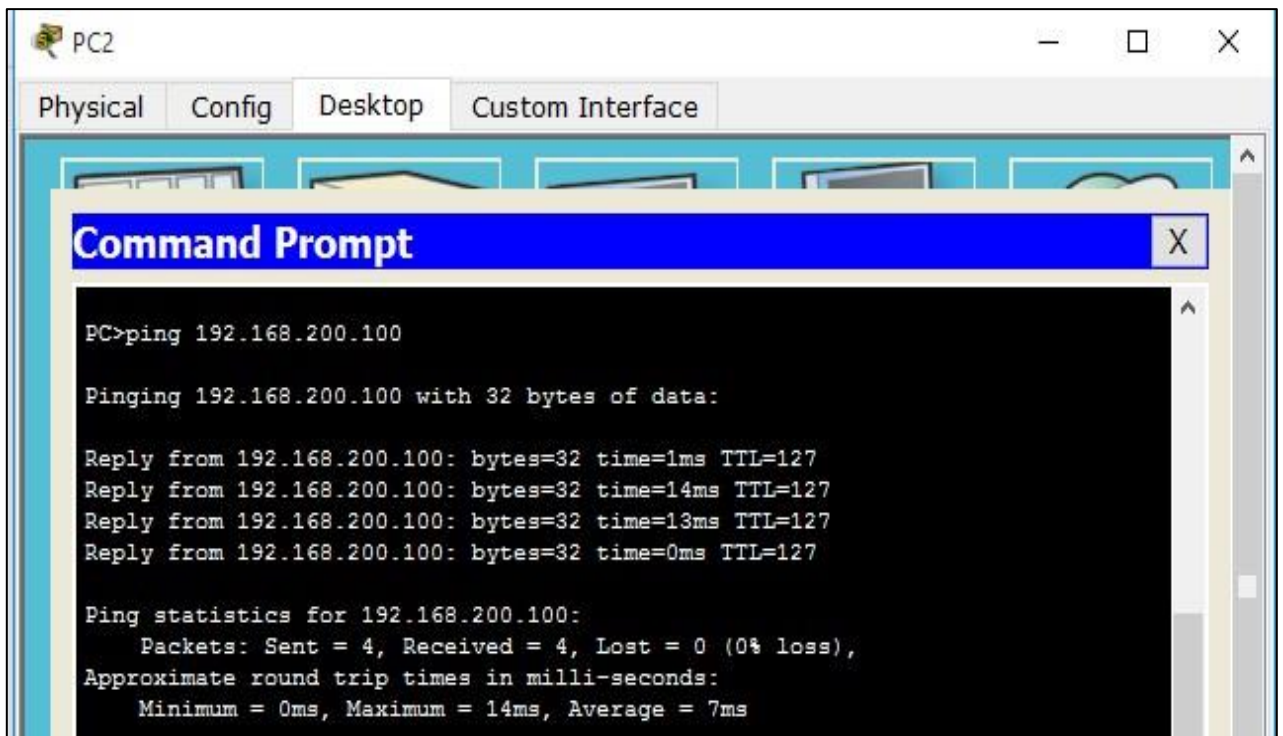
Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=16ms TTL=127
Reply from 192.168.100.100: bytes=32 time=10ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 6ms

PC>
```

- Ping desde el PC2 al Fileserver: (PC2 al 192.168.200.100): ping exitoso



The screenshot shows a Packet Tracer PC window titled 'PC2' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. A 'Command Prompt' window is open, displaying the following text:

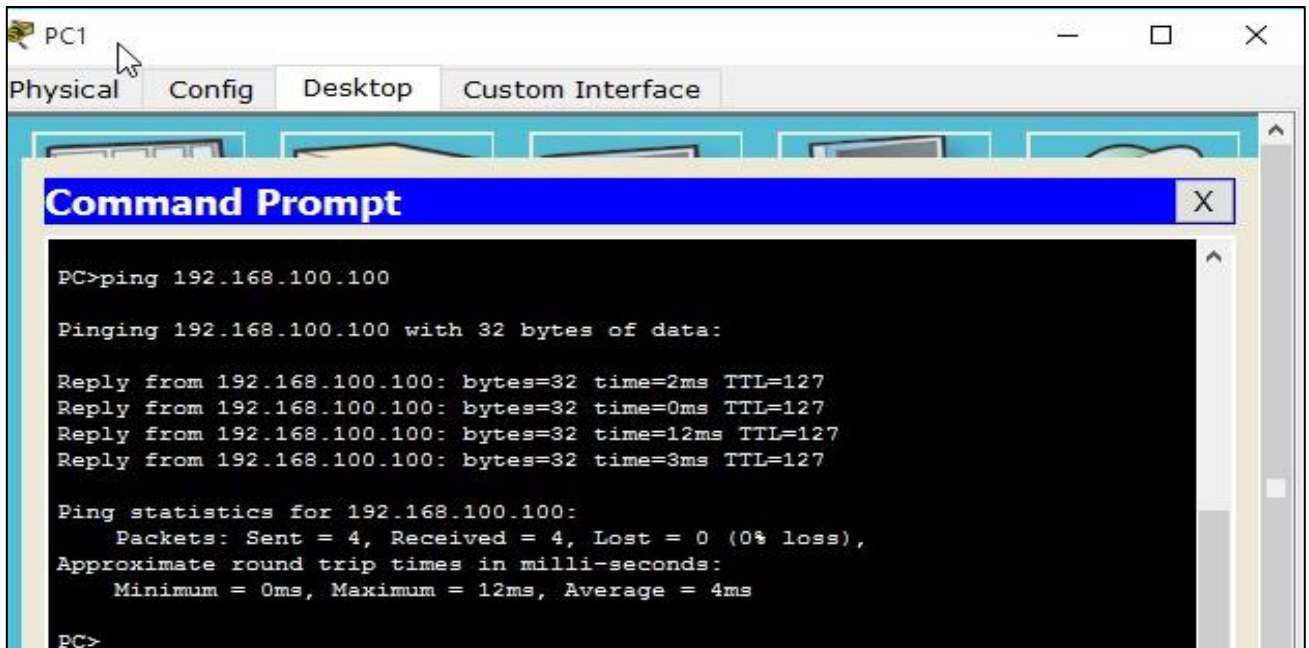
```
PC>ping 192.168.200.100

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=14ms TTL=127
Reply from 192.168.200.100: bytes=32 time=13ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 7ms
```

- Ping desde PC1 al Webserver: (PC1 al 192.168.100.100): ping exitoso



The screenshot shows a PC1 desktop environment with a 'Command Prompt' window open. The window title is 'Command Prompt' and it has a close button (X). The command prompt shows the following output:

```
PC>ping 192.168.100.100

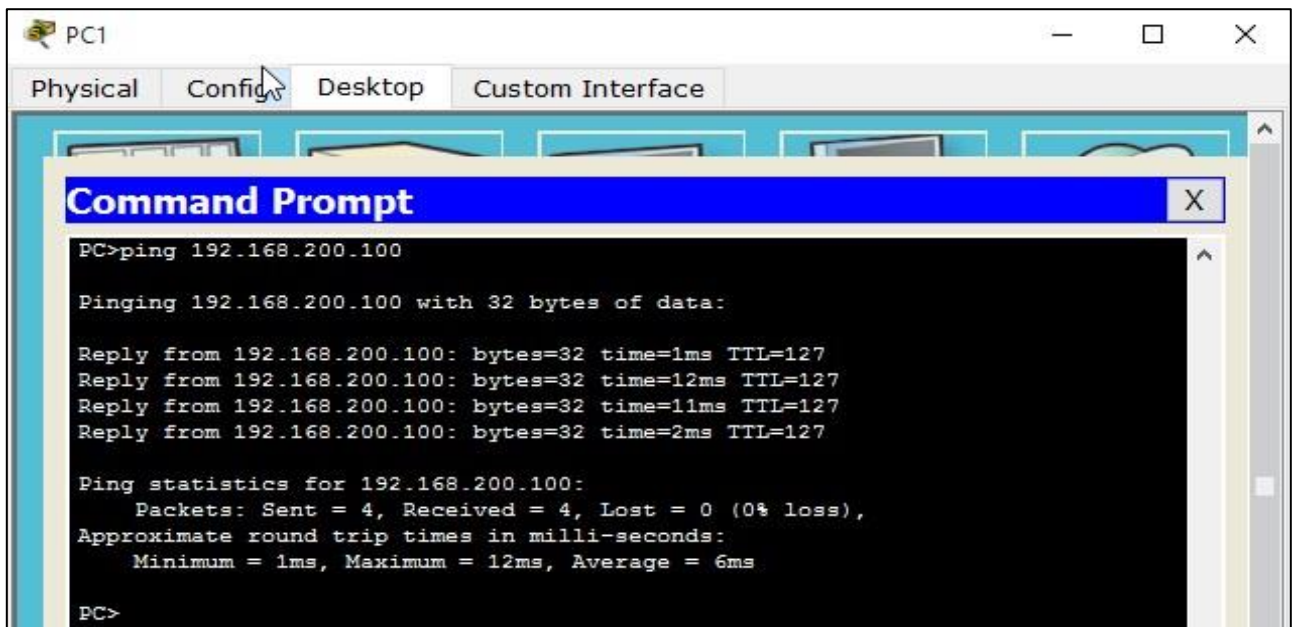
Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=3ms 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 = 4ms

PC>
```

- Ping PC1 al FileServer: PC1 al 192.168.200.100:



The screenshot shows a PC1 desktop environment with a 'Command Prompt' window open. The window title is 'Command Prompt' and it has a close button (X). The command prompt shows the following output:

```
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=12ms TTL=127
Reply from 192.168.200.100: bytes=32 time=11ms 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 = 1ms, Maximum = 12ms, Average = 6ms

PC>
```

Step 2: Configure a named standard ACL.

Configure the following named ACL on R1.:

Step 3: Apply the named ACL.

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

b. Save the configuration.

Hacemos la configuración de los pasos 2 y 3:



```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#deny any
R1(config-std-nacl)#exit
R1(config)#interface f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#
```

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the interface.

Usando el comando **show access-lists** . (para mostrar las listas de acceso configuradas): donde solo hay una lista...

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

En la siguiente imagen muestra la lista de acceso con su nombre y la restricción de solo permitir un host que es el PC1 con dirección IP=192.168.20.4



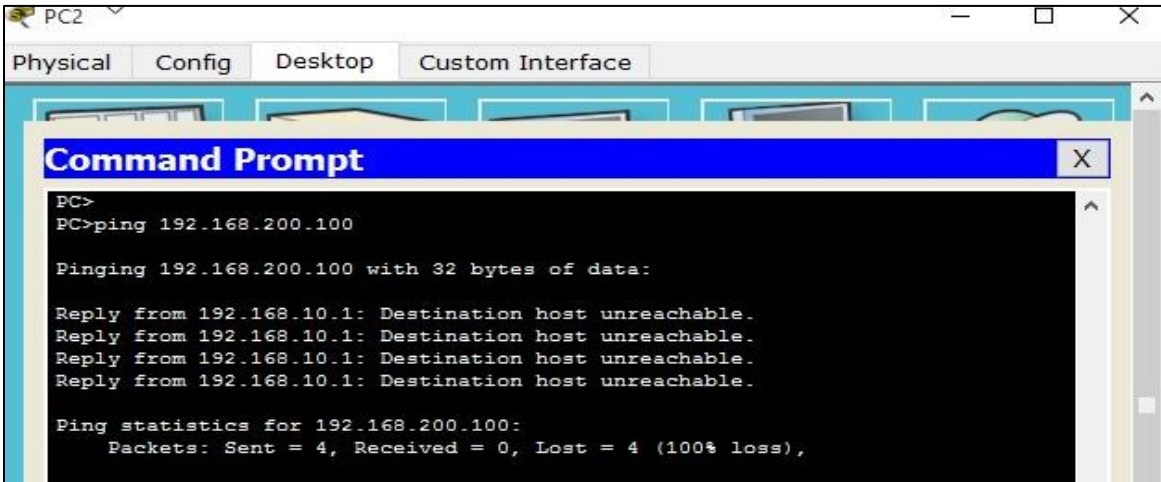
```
!
!
ip access-list standard File_Server_Restrictions
 permit host 192.168.20.4
 deny any
!
```

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**.

probamos la conectividad de los 3 PC's al servidor de archivos (file server) y comprobamos lo afirmado por el enunciado.

- Desde el PC2 al File Server: el ping no fue exitoso.



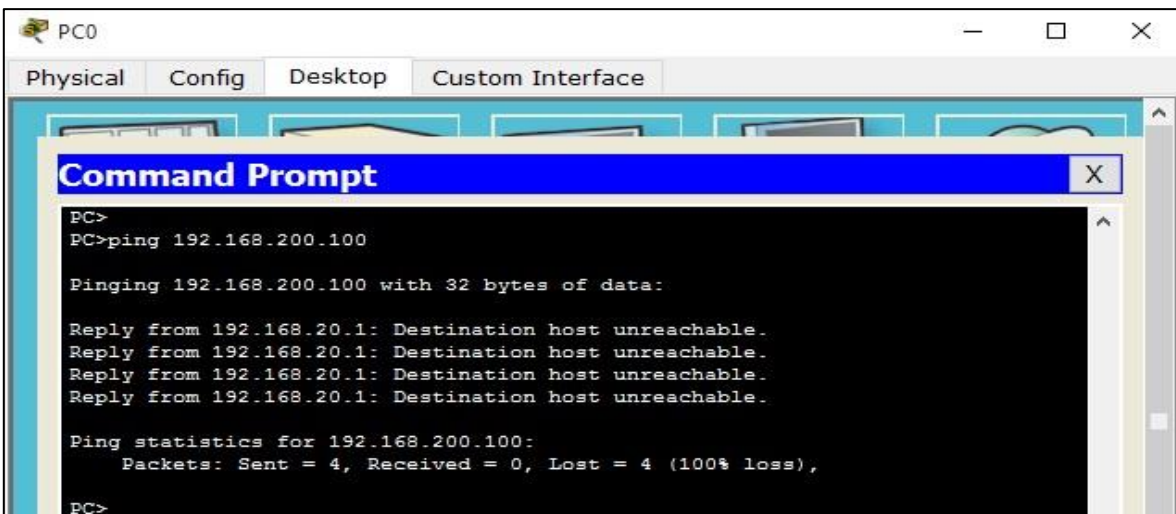
```
PC2
Physical Config Desktop Custom Interface
Command Prompt
PC>
PC>ping 192.168.200.100

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),
```

- Desde el PC0 al Fileserver: el ping no fue exitoso



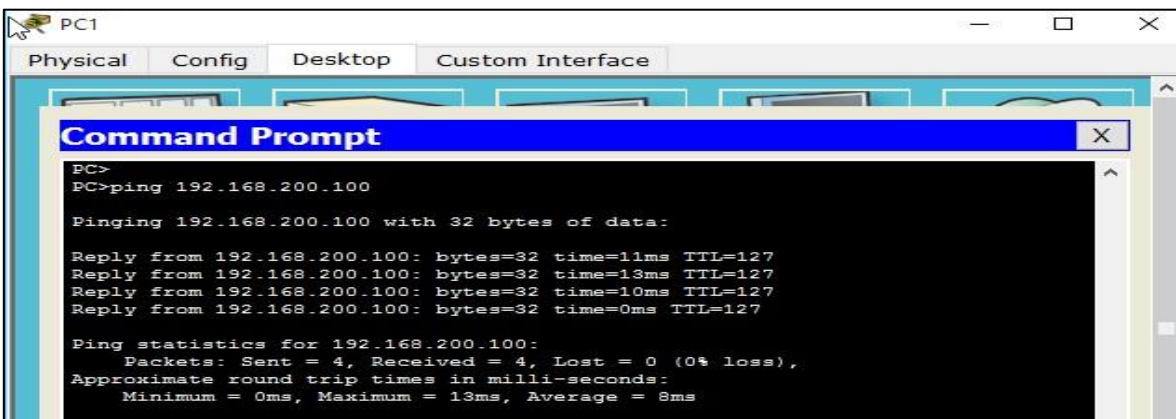
```
PC0
Physical Config Desktop Custom Interface
Command Prompt
PC>
PC>ping 192.168.200.100

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>
```

- Ping desde el PC1 al Fileserver: el ping fue satisfactorio como se esperaba..



```
PC1
Physical Config Desktop Custom Interface
Command Prompt
PC>
PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

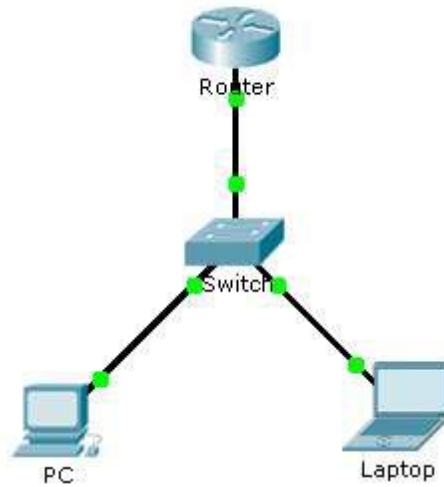
Reply from 192.168.200.100: bytes=32 time=11ms TTL=127
Reply from 192.168.200.100: bytes=32 time=13ms TTL=127
Reply from 192.168.200.100: bytes=32 time=10ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 8ms
```

9.2.3.3 CONFIGURING AN ACL ON VTY LINES

9.2.3.3 PACKET TRACER - CONFIGURING AN ACL ON VTY LINES

Topology



Addressing Table

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

Objectives

Part 1: Configure and Apply an ACL to VTY Lines

Part 2: Verify the ACL Implementation

Part 1: Configure and Apply an ACL to VTY Lines

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

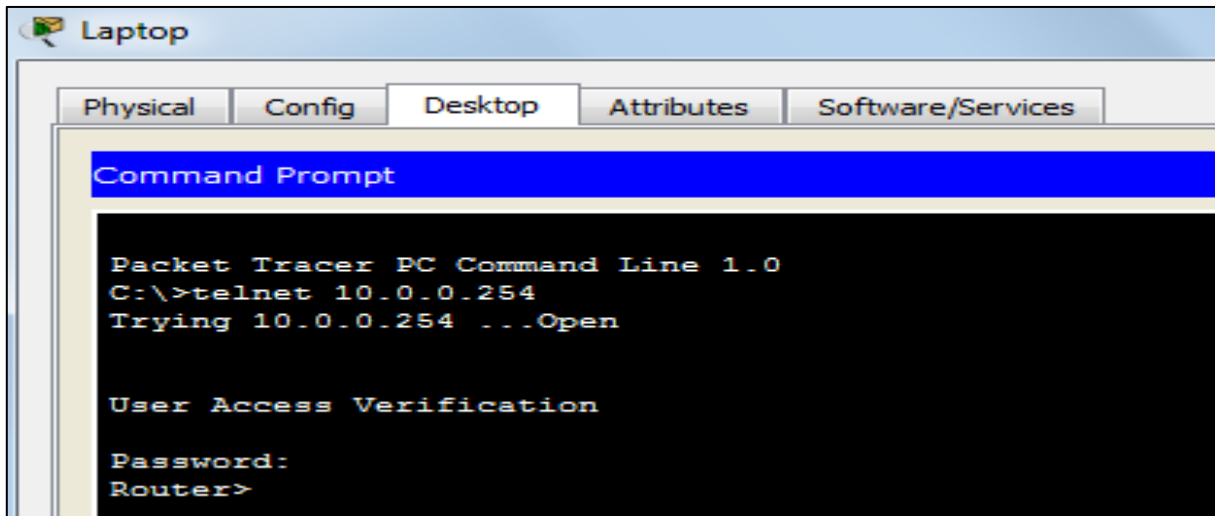
Both computers should be able to Telnet to the **Router**. The password is **cisco**.

The screenshot shows a PC Command Prompt window with the following text:

```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open

User Access Verification

Password:
Router>
```



Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on **Router**.

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

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

```
Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#
```

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

Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must

place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration

mode for lines 0 – 4 and use the **access-class** command to apply the ACL to all the VTY lines:

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

```
Router(config-line)# access-class 99 in
```

```
Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99?
<1-199> WORD
Router(config-line)#access-class 99 ?
  in  Filter incoming connections
  out Filter outgoing connections
Router(config-line)#access-class 99 in
Router(config-line)#
```

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the VTY lines.

Use the **show access-lists** to verify the ACL configuration. Use the **show run** command to verify the ACL is applied to the VTY lines.

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



```
Router#show running-config
Building configuration...

Current configuration : 621 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
```

```
interface FastEthernet0/0
 ip address 10.0.0.254 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
access-list 99 permit host 10.0.0.1
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class 99 in
 password cisco
 login
line vty 5 15
 access-class 99 in
 password cisco
 login
!
```

Step 2: Verify that the ACL is working properly.

Both computers should be able to ping the **Router**, but only **PC** should be able to Telnet to it.

| Fire | Last Status | Source | Destination |
|---|-------------|--------|-------------|
|  | Successful | PC | Router |
|  | Successful | Laptop | Router |

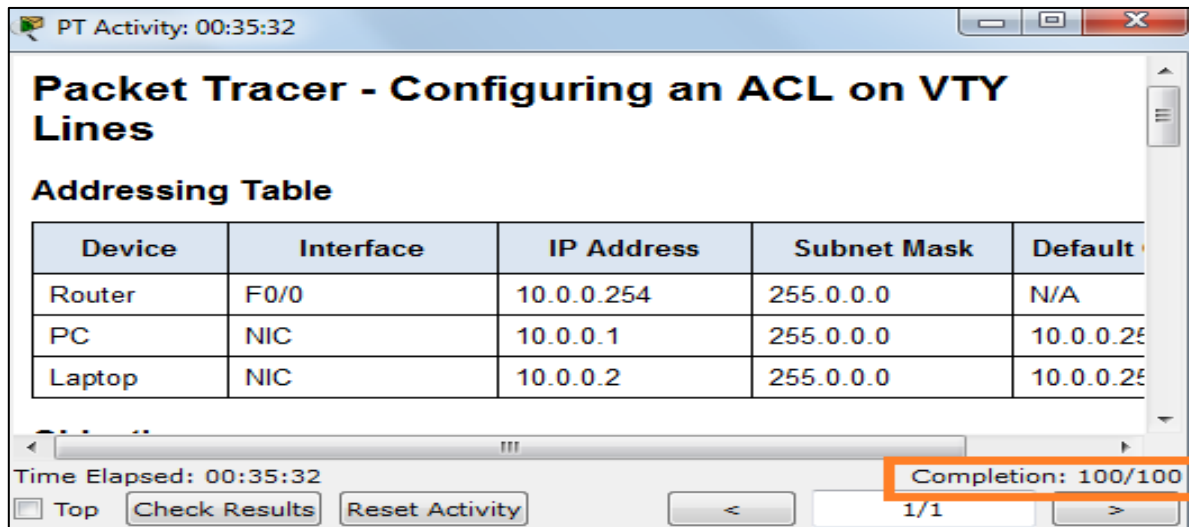
```
C:\>telnet 10.0.0.254
Trying 10.0.0.254 ...Open
```

```
User Access Verification
```

```
Password:
Router>
```

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

CHECK RESULTS



PT Activity: 00:35:32

Packet Tracer - Configuring an ACL on VTY Lines

Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default |
|--------|-----------|------------|-------------|------------|
| 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 |

Time Elapsed: 00:35:32

Completion: 100/100

Top

Activity Results

Time Elapsed: 00:36:42

Congratulations Guest! You completed the activity.

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

Congratulations Guest! You completed the activity.

Overall Feedback

Assessment Items

Connectivity Tests

Expand/Collapse All

Score : 100/100

Item Count : 6/6

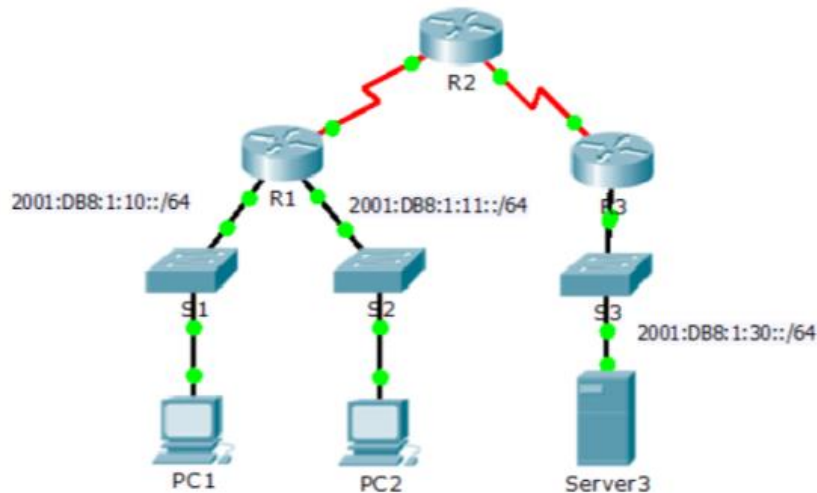
| Assessment Items | Status | Points |
|----------------------|---------|--------|
| [-] Network | | |
| [-] Router | | |
| [-] ACL | | 0 |
| [-] ✓ 99 | Correct | 70 |
| [-] VTY Lines | | |
| [-] VTY Line 0 | | 0 |
| [-] ✓ Access Cont... | Correct | 6 |
| [-] VTY Line 1 | | 0 |
| [-] ✓ Access Cont... | Correct | 6 |
| [-] VTY Line 2 | | 0 |
| [-] ✓ Access Cont... | Correct | 6 |
| [-] VTY Line 3 | | 0 |
| [-] ✓ Access Cont... | Correct | 6 |
| [-] VTY Line 4 | | 0 |
| [-] ✓ Access Cont... | Correct | 6 |

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

9.5.2.6 CONFIGURING IPV6 ACLs

9.5.2.6 PACKET TRACER - CONFIGURING IPV6 ACLS

Topology



Addressing Table

Addressing Table

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

Objectives

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

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

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

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

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

Configure an ACL named **BLOCK_HTTP** on **R1** with the following statements.

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

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

- Allow all other IPv6 traffic to pass.

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

Step 2: Apply the ACL to the correct interface.

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

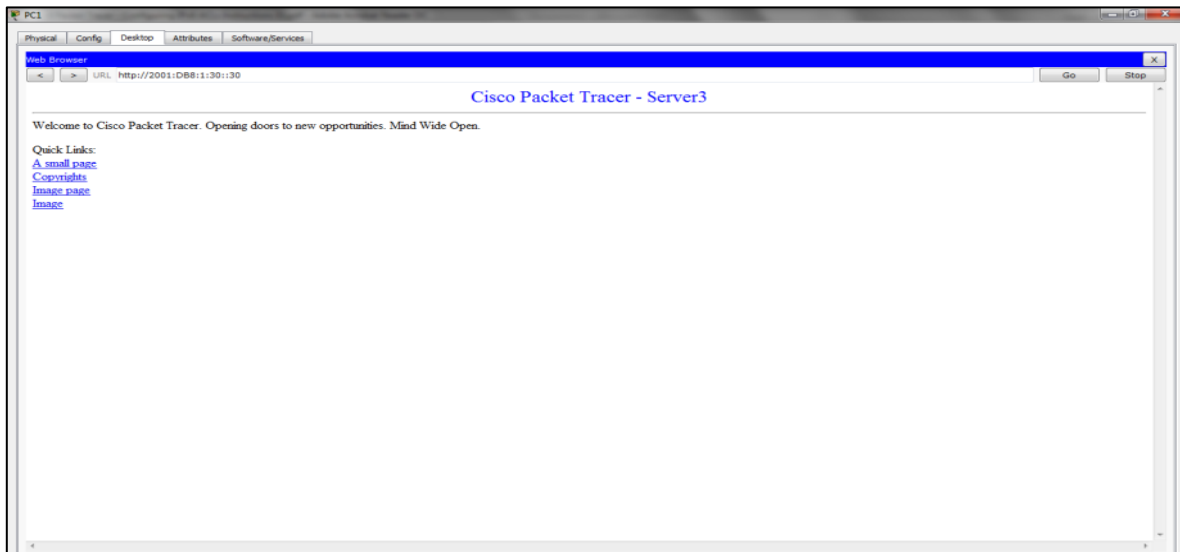
```
R1(config)# interface GigabitEthernet0/1
```

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

Step 3: Verify the ACL implementation.

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

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

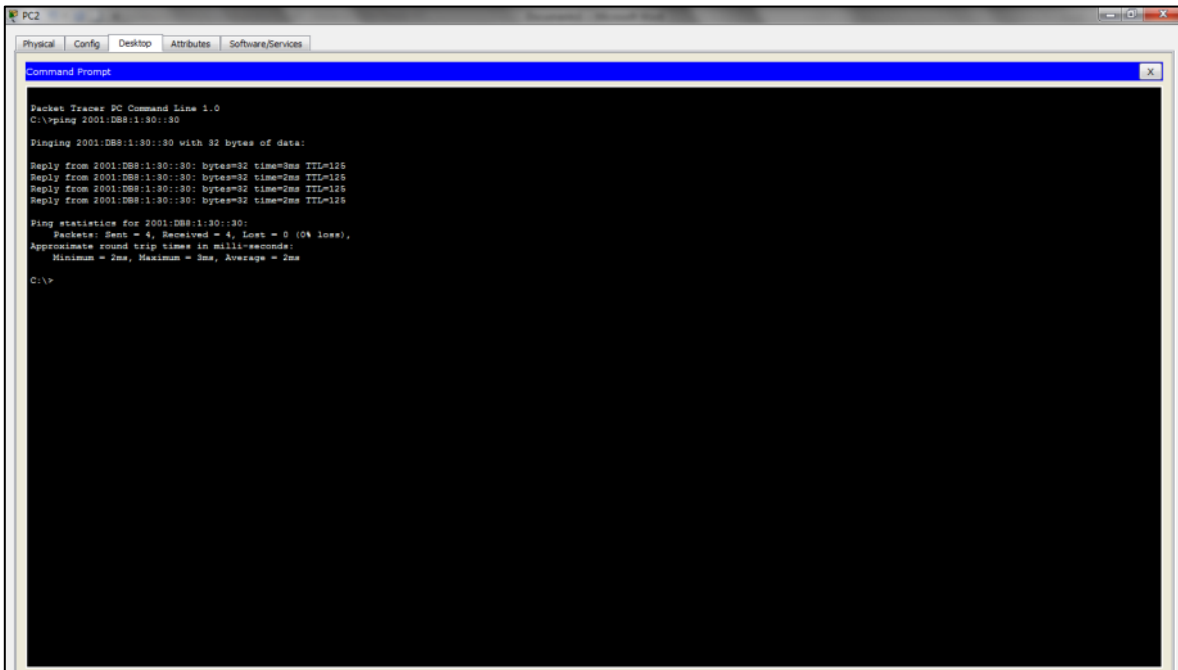


- Open the **web browser** of **PC2** to <http://2001:DB8:1:30::30> or <https://2001:DB8:1:30::30>. The website should be blocked

El website esta bloqueado:



- Ping from **PC2** to 2001:DB8:1:30::30. The ping should be successful.
El pin si ha sucedido:



```
PC2
Physical  Config  Desktop  Attributes  Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:30::30: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\>
```

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
R3>en
R3#conf t
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
```

b. Allow all other IPv6 traffic to pass.

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

R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#int g0/0
```

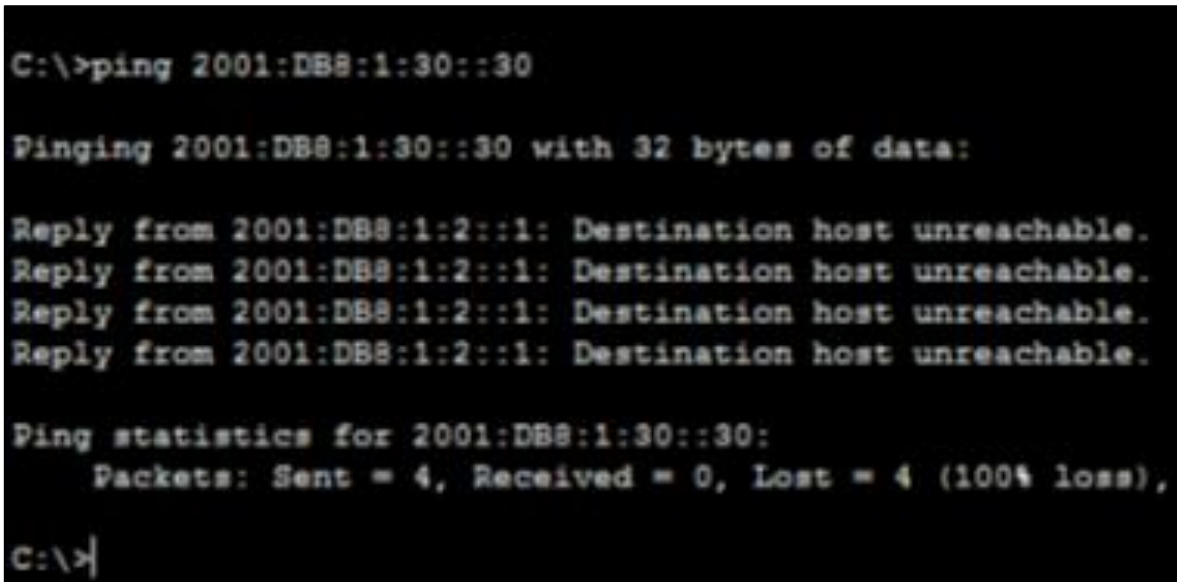
Step 2: Apply the ACL to the correct interface.

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(config-ipv6-acl)#int g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

Step 3: Verify that the proper access list functions.

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



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

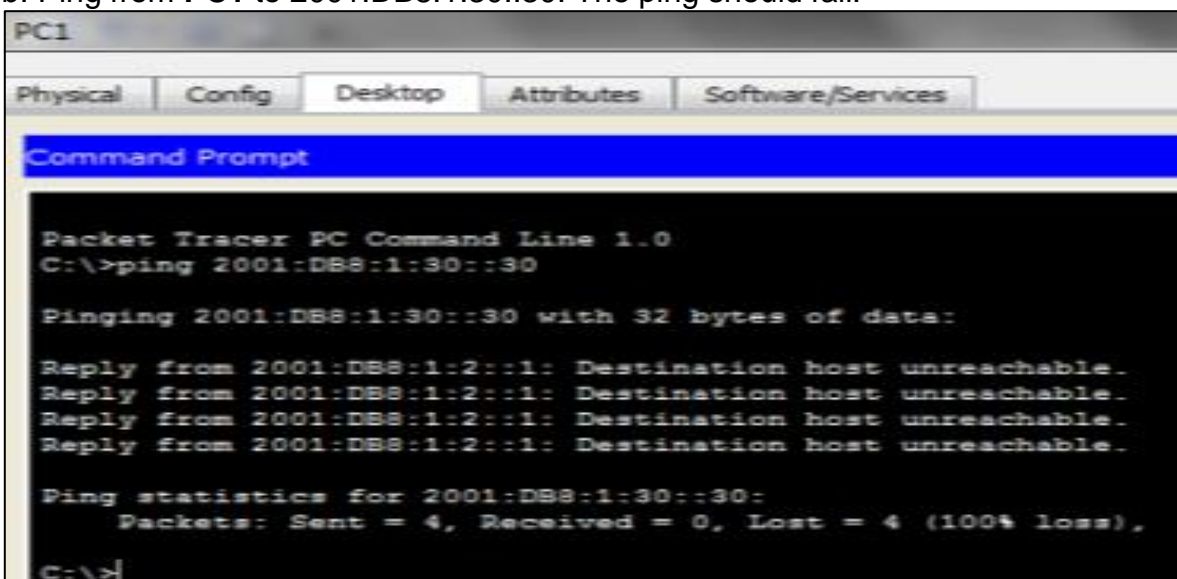
Pinging 2001:DB8:1:30::30 with 32 bytes of data:

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

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

C:\>
```

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



```
PC1
Physical Config Desktop Attributes Software/Services
Command Prompt

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

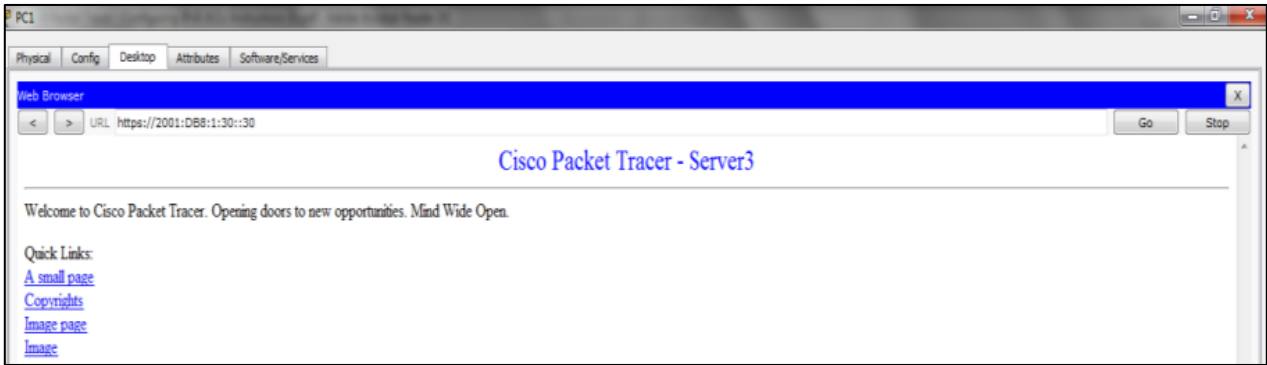
Pinging 2001:DB8:1:30::30 with 32 bytes of data:

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

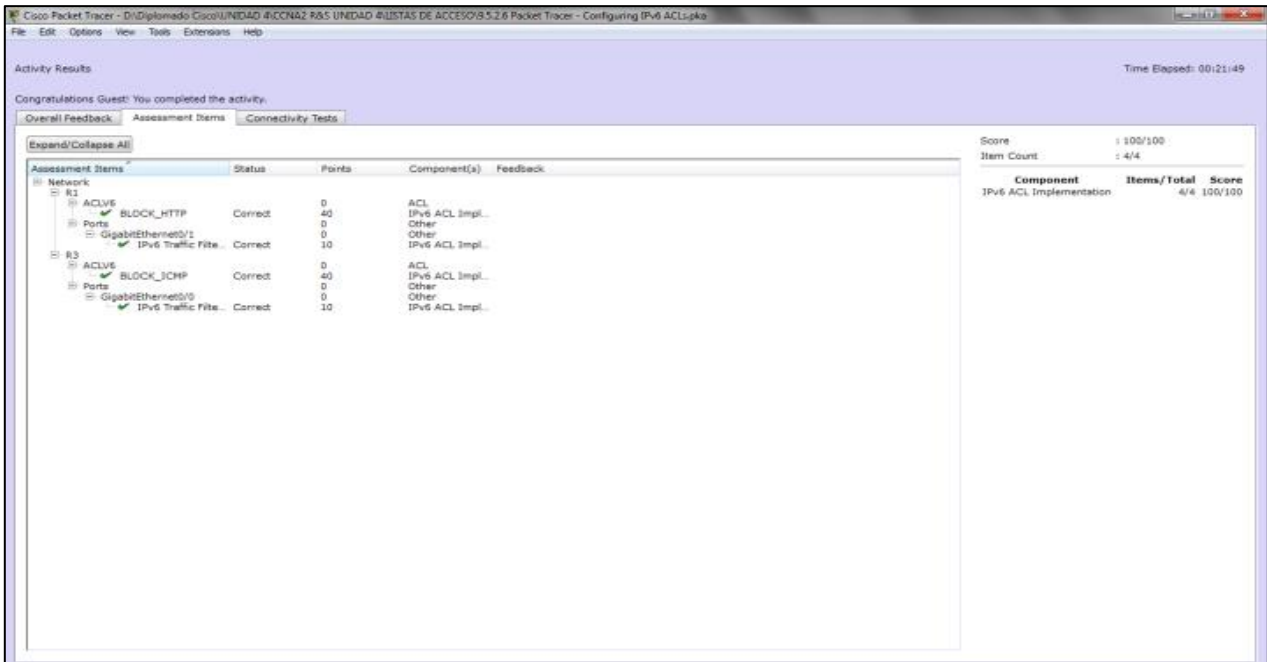
Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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



CHECK RESULTS



CONCLUSIONES

Después de haber analizado la actividad anterior se ha llegado a la conclusión, de que la unidad 4 del módulo de DIPLOMADO DE CISCO permite a los estudiantes practicar en cuanto a los Enrutamiento en soluciones de red

Se concluye que los estudiantes aprendieron a desenvolverse en los diferentes escenarios virtuales para aplicarlo en un entorno real configurando los parámetros de Enrutamiento Dinámico, OSPF de una sola área, Listas de control de acceso, DHCP y Traducción de direcciones IP para IPv4.

Aprendimos que entre las ventajas del enrutamiento dinámico encontramos que el administrador tiene menos trabajo en el mantenimiento de la configuración cuando agrega o quita redes. Los protocolos reaccionan automáticamente a los cambios de topología. La configuración es menos propensa a errores.

Es más escalable, el crecimiento de la red normalmente no representa un problema.

Así mismo, las ventajas de OSPF ofrece rápida convergencia y escalabilidad en redes mucho mayores. Al ser un estándar abierto soporta dispositivos de todos los fabricantes. Cada router posee una imagen completa y sincronizada de la red.

Por otra parte, concluimos que el enrutamiento DHCP ofrece ventajas en cuanto a la Administración de direcciones IP, Configuración de cliente de red centralizada, Compatibilidad con clientes BOOTP, Compatibilidad con clientes locales y remotos, Inicio de red, Amplia compatibilidad de red.

Por último, El Diplomado de profundización de Cisco, es un proyecto esencial en la formación a distancia y virtual de cada aprendiz de Ingeniería de Sistemas, ya que será el instrumento que guiará al estudiante a investigar, indagar y solucionar cada actividad para luego aplicarla en el campo profesional, laboral y personal.

Se espera haber capturado la atención del lector, así como también haber cumplido con las expectativas del tutor con la realización de la guía asignada

BIBLIOGRAFIA

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

Entre Redes y Servidores. Listas de Control de Acceso en Router Cisco. Recuperado de <https://alexalvarez0310.wordpress.com/category/listas-de-control-de-acceso-en-router-cisco/>

Ampliación de redes (2º I.T.I.S.). Configuración de routers: listas de control de acceso Recuperado de: http://virtualbook.weebly.com/uploads/2/9/6/2/2962741/ac__list.pdf