Trabajo Colaborativo 4.

Enrutamiento En Soluciones De Red

Preparado por

Carlos Andrés Gutiérrez C.C 6391734

Jairo Armando Cubillos Villamil C.C 6.408.174

Johan Alberto Mora C.C 14.651.804

Andrés Felipe Hernández C.C 6.393546

Yilber Didimo Buitrago C.C 7.318.012

Grupo

203092_20

Presentado a

José Ignacio Cardona

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E EINGENIERIA, ECBTI
PROGRAMA DE INGENIERIA DE SISTEMAS
CEAD PALMIRA
NOVIEMBRE DE 2017

INTRODUCCIÓN

Dada la importancia de la presente unidad para el desarrollo y puesta en marcha de los protocolos de seguridad, e implementación de enrutamiento en IPv4 e IPv6, procesamiento de paquetes de bloqueos, accesos y peticiones de los usuarios, asignaciones de direccionamiento estático y dinámicos, establecimiento de la NAT con sus respectivas sobrecarga tanto dinámica como nativa, configuraciones de la red y PAT, Configuración de OSPFv2 y OSPFv3 con sus áreas resueltas, y de igual manera la configuración de una ACL en VTY Líneas.

El grupo colaborativo conformado por cada uno de sus integrantes realizarán el desarrollo teórico-práctico del componente, analizaran cada uno de los contenidos y entraran en consenso y debate con sus partes, dando así las pautas con el material en cada una de las practicas, los integrantes del grupo cuentan con material de consulta, no solo en la plataforma de la universidad, de igual manera en la plataforma Cisco, con el fin de resolver inquietudes y novedades en cada uno de los puntos a resolver, se cuenta con el apoyo del tutor de curso, de la mano con el director del diplomado, quienes establecerán las pautas y resolverán las posibles novedades o dudas.

Para dar comienzo a la presente unidad, se desarrollarán de manera sistemática una serie de ejercicios (laboratorios) detallando en pormenor los pasos, aplicaciones y comandos que darán origen a preguntas con el ánimo de reforzar el procedimiento y afianzar la labor realizada.

Se establecerá mediante ejecución las ordenes de sentencia de las ACL, que consiste en la decisión que emite el router en el momento de enviar o recibir paquetes, mediante el IOS realiza una verificación si cumple o no el paquete de manera satisfactoria el requerimiento, cuando se cumple la condición, no se seguirán ejecutando las verificaciones o las llamadas sentencias de condición

Se estudiará la ACL estándar su importancia en el servicio para el bloqueo especifico de una red o un Host, en el análisis se entenderá la autenticación de todo el tráfico y la denegación del mismo.

Se realizará un ejercicio en donde se logrará activar y desactivas la ACL numerada o nombrada, con el fin de incorporar en la dinámica de la unidad los pasos necesarios para comprender y realizar el procedimiento del comando especifico.

Es importante destacar el grado de importancia que tiene el simulador Cisco Packet Tracer, ya que, sin la ejecución del mismo, la interpretación y grado de análisis serían nulos, pese a que algunos comandos no los permite ejecutar, es importante tener en cuenta que la visión que ofrece nos permite adquirir conocimiento y desarrollar si se quiere la crítica necesaria para inferir en decisiones de implementación y diseño en una red.

Se configurará una ACL en VTY Líneas, con el fin de establecer la necesidad de manera remota el acceso a una Telnet específica, con el fin de denegar peticiones a usuarios o intrusos que no tengan el acceso o perfil, es decir deniegue el resto de las direcciones IP

El análisis de IPv6 ACL le permitirá al grupo establecer mediante el protocolo la programación del enrutamiento, dando origen a la petición, ya sea desde IPv4 a 6 respectivamente.

Básicamente el grupo colaborativo realizará la programación básica de RIPv2 y RIPng que consistirá en el enrutamiento de direcciones IPv4 que incluyen de manera automática la máscara de subred, esto debido a que el protocolo del enrutador es sin asignación de clase, resume de manera automática los límites de las redes principales, también se ejecutarán los comando pertinentes para realizar la configuración de OSPFv2 básico de área sueltas, específicamente diseñada para el protocolo IPv4, cuya finalidad es detectar las posibles fallas del enlace, cambios en la topología de la red con una alta convergencia en una estructura de routing con bucles.

El desarrollo y configuración de OSPFv3 básico de área sueltas, les permitirá a los integrantes del grupo analizar el protocolo IPv6 ya que este fue diseñado de manera específica para dicho protocolo, en donde se utilizarán los comandos en

CLI para verificación del OSPFv3 en donde se utilizará un router de servicio integrado 1942 con IOS versión 15.2 (4) M3, básicamente se determinará con este procedimiento el estado básico de las redes, funcionalidad en su topología

El procedimiento de configuración de DHCPv4 básico en el router de la ONU se realizará mediante asignación manual del direccionamiento IP, cada uno de los integrantes del pequeño grupo colaborativo estará en la disposición y capacidad de realizar dicha ejecución que consiste en protocolizar varias subredes sin crear conflictos con cambios internos de la red mediante comandos básicos, se establecerá de igual forma la configuración de un Switch en DHCPv4 con el propósito de asignar de manera estática el direccionamiento a otros hots

Realizaremos la configuración de DHCPv6 sin estado y con estado la cual consistirá en la determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

De una manera muy práctica estableceremos las condiciones necesarias para crear una pequeña red doméstica mediante IdT y DHCP, que consistirá en la programación del router que permite identificar cualquier ID que esté conectado a dicha red desde cualquier lugar

Nos introduciremos en las direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

Por último, analizaremos el protocolo que proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única

dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

OBJETIVOS

OBJETIVO GENERAL

Adquirir conocimientos y habilidades en el estudio de la unidad 4 enrutamiento en soluciones de red, realizando los ejercicios planteados en el momento 7 del Diplomado de Profundización CISCO (Diseño e Implementación de Soluciones Integradas LAN / WAN).

OBJETIVOS ESPECIFICOS

- Reunir los saberes y competencias designados para esta unidad.
- Conocer la estructura y características principales de las redes convergentes.
- Analizar las posibles soluciones
- Conocer y aplicar la configuración básica para un Switch y un Router.
- Identificar los protocolos de seguridad usados en los Switch.
- Configurar y aplicar una ACL nombrada estándar
- Configurar y aplicar una ACL nombrada estándar
- Aprender armar y configurar Redes y los parámetros básicos de los dispositivos
- configurar y verificar el routing

Desarrollo Ejercicio 4.4.1.2

Práctica de laboratorio: 4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks_Instructor

Topología

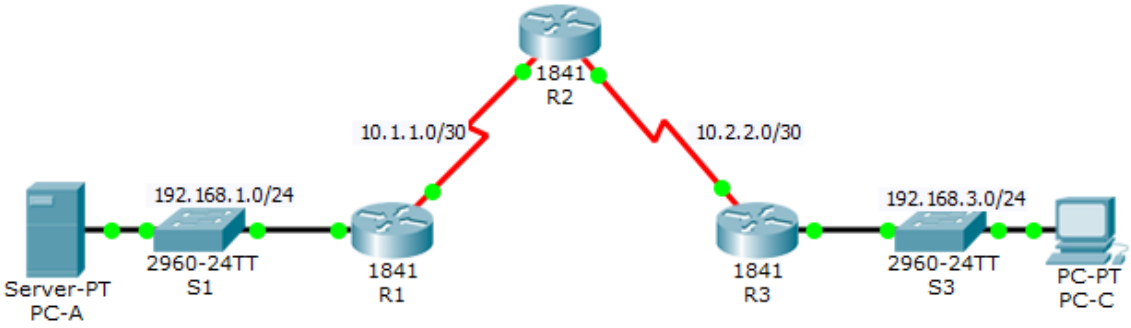


Tabla de direccionamiento

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

Objetivos

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

Antecedentes / escenario

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

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

Los enrutadores se han preconfigurado con lo siguiente:

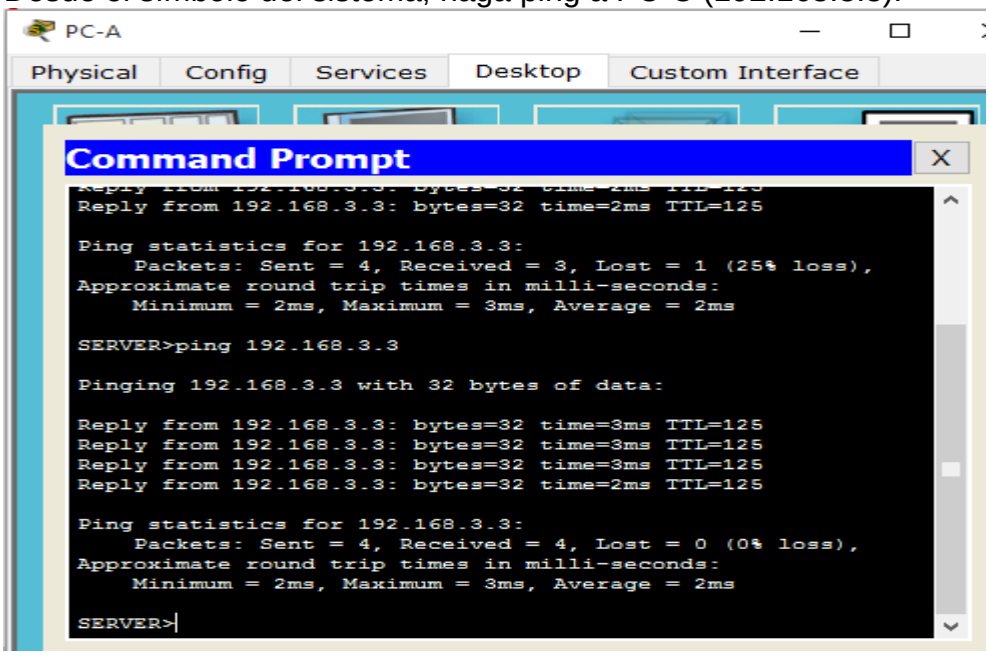
- Habilitar contraseña: **ciscoenpa55**
- Contraseña para la **consola: ciscoconpa55**
- Nombre de usuario para líneas VTY: **SSHadmin**
- Contraseña para líneas VTY: **ciscosshpa55**
- direccionamiento IP
- Enrutamiento estático

Parte 1: verificar la conectividad de red básica

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

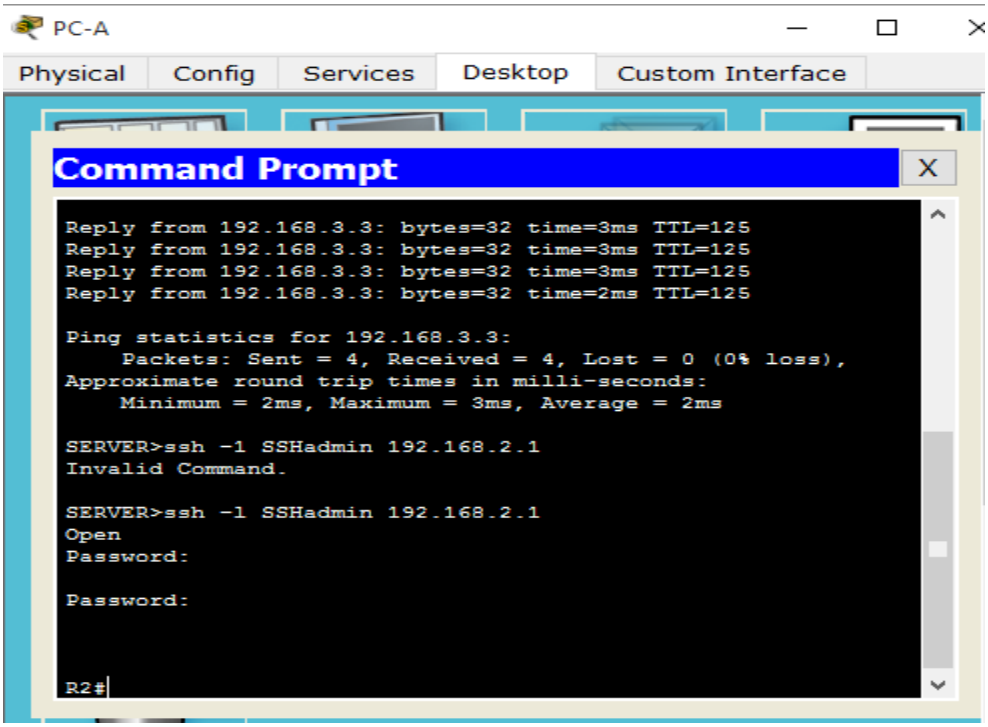
Paso 1: desde la PC-A, verifique la conectividad con PC-C y R2.

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



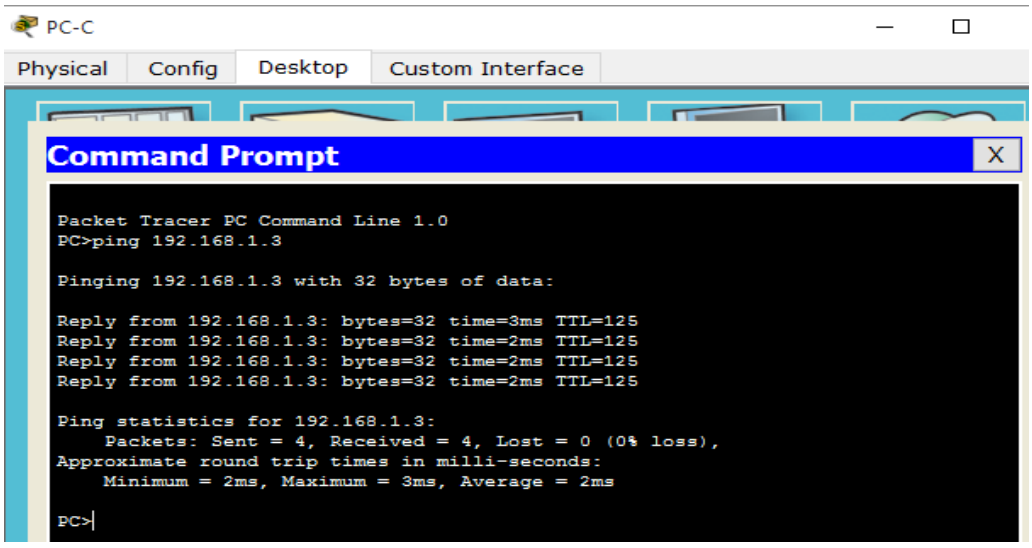
b. Desde el símbolo del sistema, establezca una sesión SSH a la interfaz R2 Lo0 (192.168.2.1) utilizando un nombre de usuario SSHadmin y contraseña ciscosshpa55. Cuando termine, salga de la sesión SSH.

PC> ssh -l SSHadmin 192.168.2.1



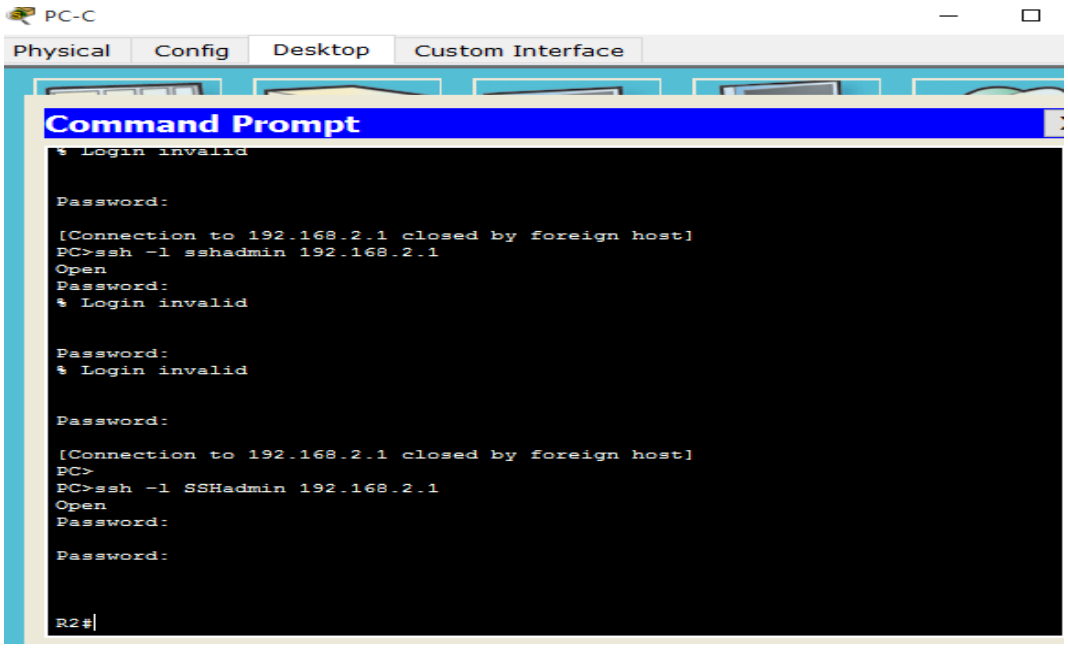
Paso 2: desde PC-C, verifique la conectividad con PC-A y R2.

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

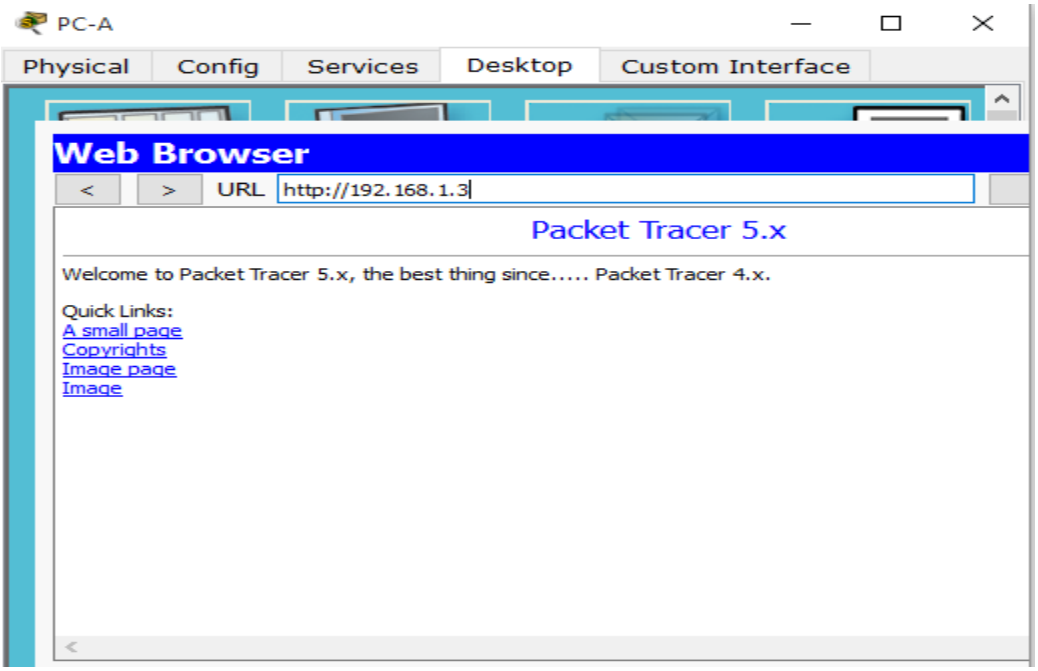


b. Desde el símbolo del sistema, establezca una sesión SSH a la interfaz R2 Lo0 (192.168.2.1) utilizando un nombre de usuario SSHadmin y contraseña ciscosshpa55. Cierre la sesión SSH cuando haya terminado.

PC> ssh -l SSHadmin 192.168.2.1



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



Parte 2: Acceso seguro a enrutadores

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

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

R1 (config) # access-list 10 permission 192.168.3.3 0.0.0.0

R2 (config) # access-list 10 permission 192.168.3.3 0.0.0.0

R3 (config) # access-list 10 permission 192.168.3.3 0.0.0.0

```
Password:
Password:

R1>enable
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R1(config)#
```

```
Password:

R2>enable
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)#
```

```
Password:

R3>enable
Password:
Password:
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#
```

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

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

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

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

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

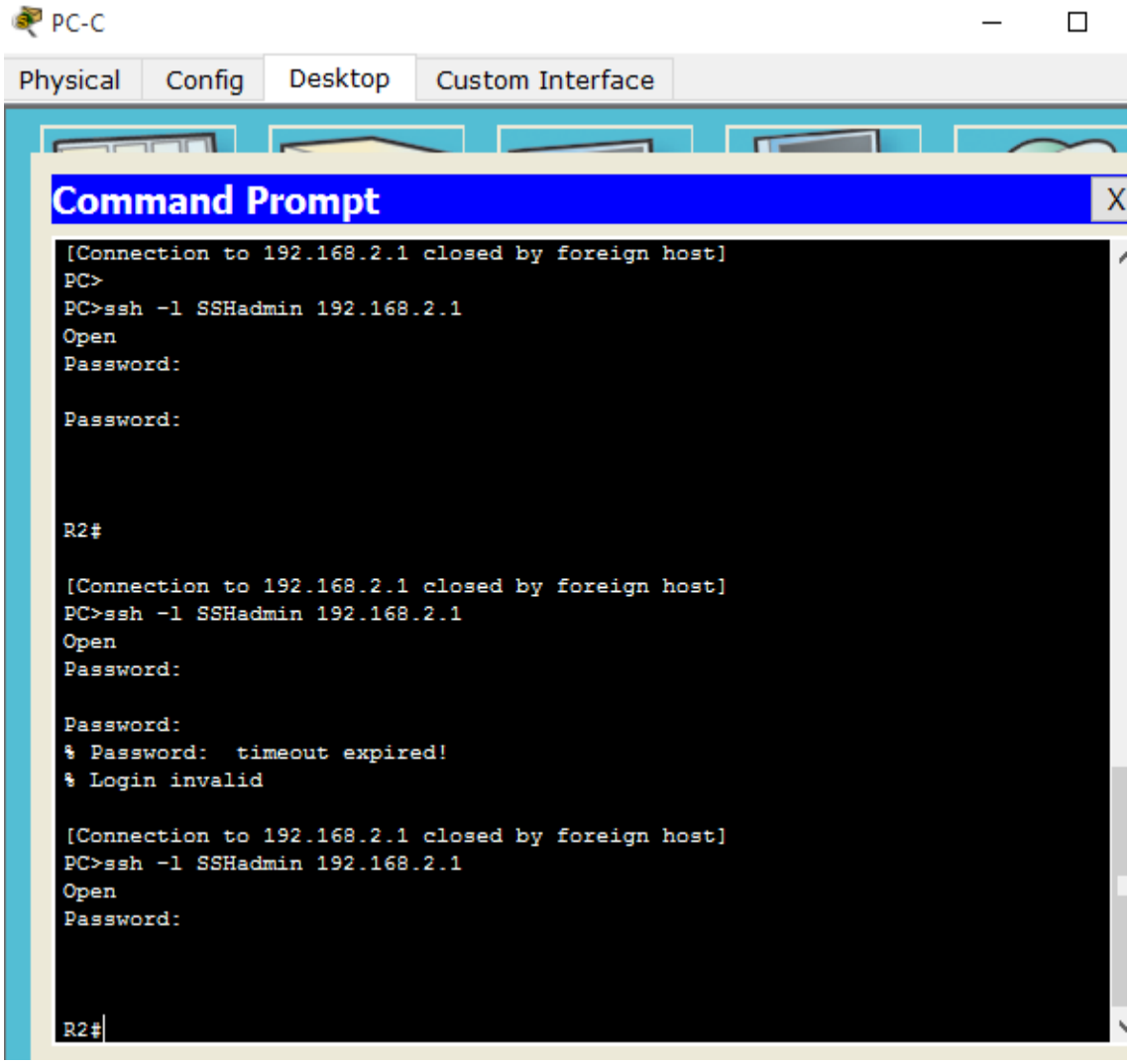
```
R1(config)#line vty 0 15
R1(config-line)#acces-class 10 in
                    ^
% Invalid input detected at '^' marker.

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

```
R2(config)#line vty 0 15
R2(config-line)#access-class 10 in
R2(config-line)#
```

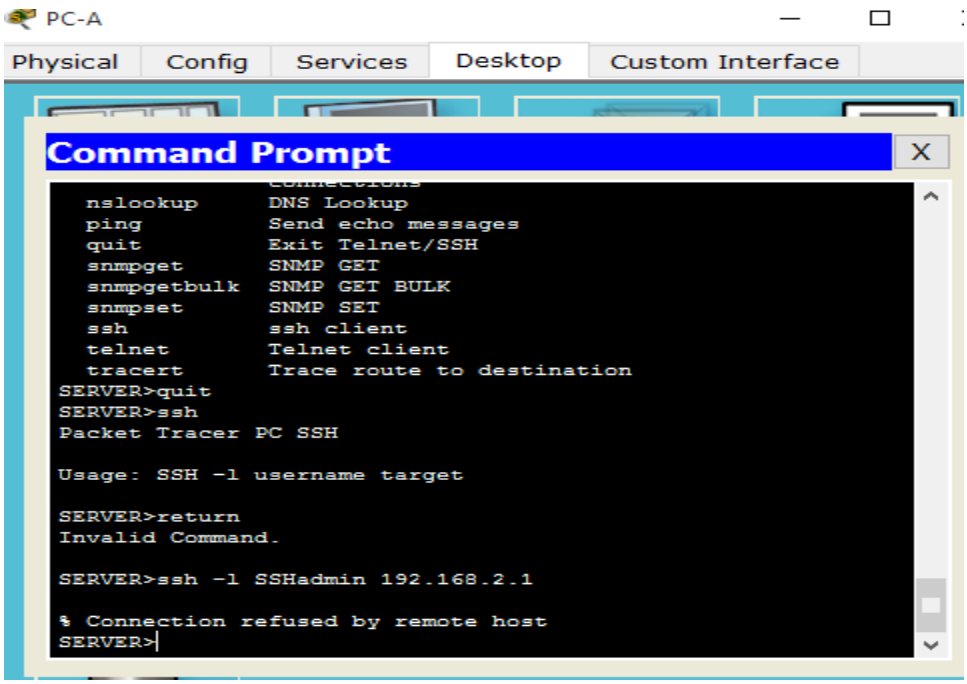
```
R3(config)#line vty 0 15
R3(config-line)#access-class 10 in
R3(config-line)#
```

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

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



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

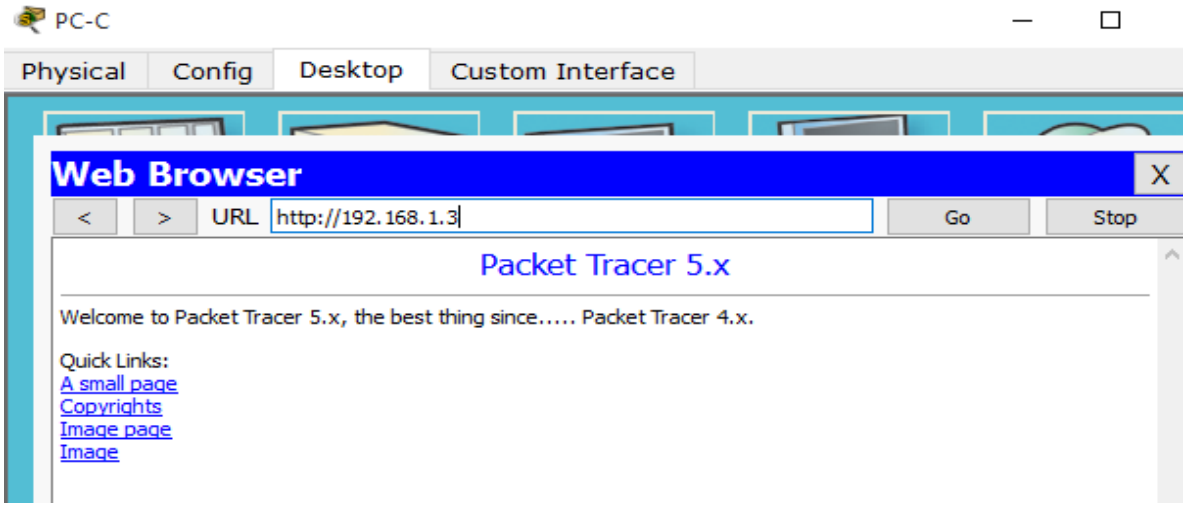


Parte 3: Cree una ACL IP numerada 120 en R1

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

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

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



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

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

R1(config)# **access-list 120 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)#access-class 10 in
R1(config-line)#
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)#
```

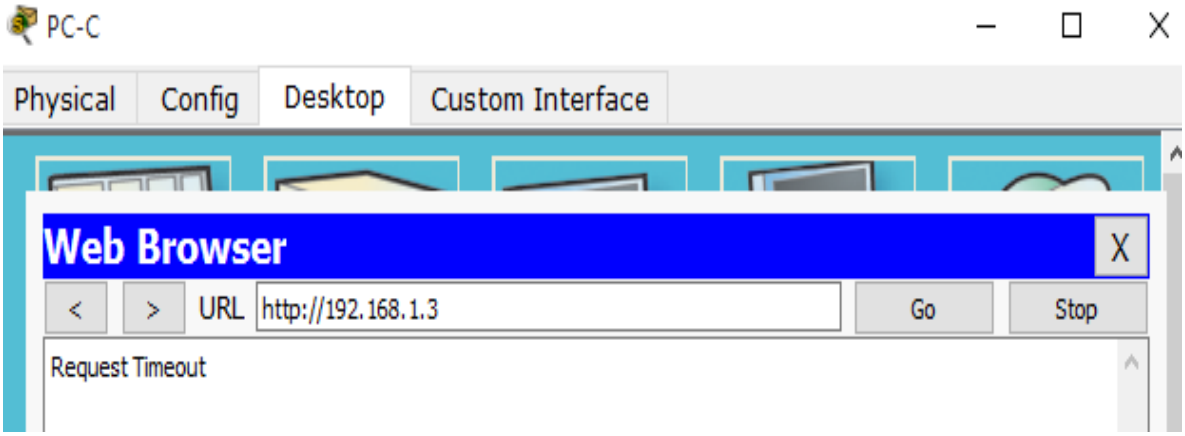
Paso 3: aplique la ACL a la interfaz S0 / 0/0.

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

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

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

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



Parte 4: Modificar una ACL existente en R1

Permitir respuestas de eco ICMP y mensajes inalcanzables de destino desde la red externa (en relación con R1); negar todo otro paquete entrantes ICMP.

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

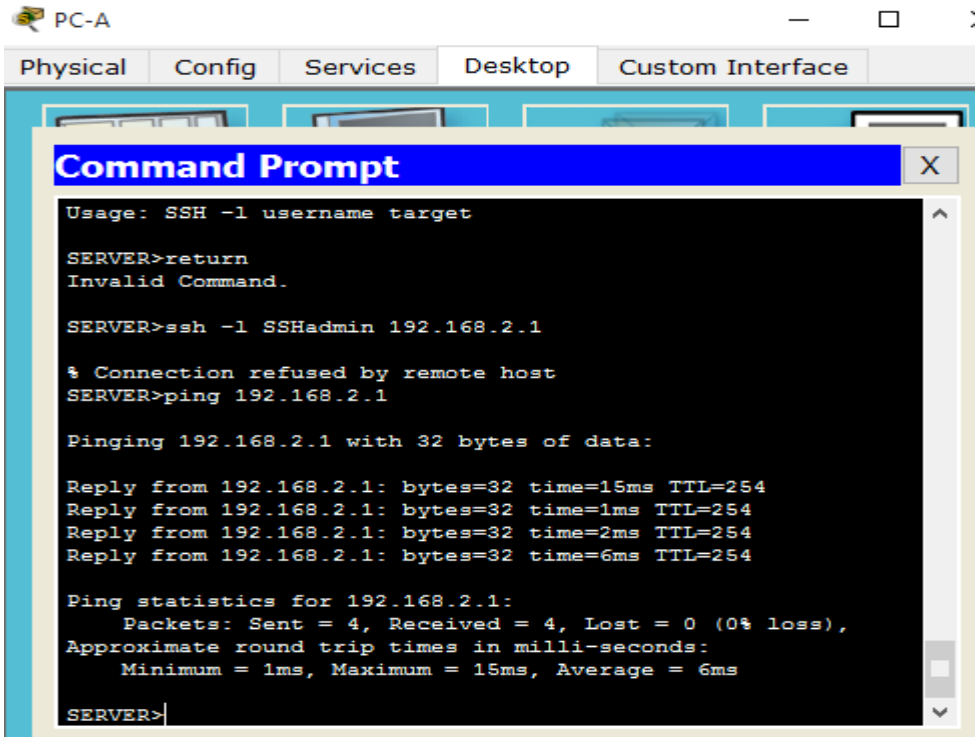
Paso 2: Realice los cambios necesarios en la ACL 120 para permitir y denegar el tráfico especificado.

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

R1(config)# **access-list 120 permit icmp any any echo-reply**
R1(config)# **access-list 120 permit icmp any any unreachable**
R1(config)# **access-list 120 deny icmp any any**
R1(config)# **access-list 120 permit ip any any**

```
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)#
```

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



Parte 5: Crear una ACL IP numerada 110 en R3

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

Paso 1: configure la ACL 110 para permitir solo el tráfico desde la red interna.
Use el comando access-list para crear una ACL IP numerada.

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

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

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

R3(config)# **interface fa0/1**
R3(config-if)# **ip access-group 110 in**

```
R3(config)#int f0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#
```

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

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

Paso 1: configure la ACL 100 para bloquear todo el tráfico especificado de la red externa. También debe bloquear el tráfico proveniente de su propio espacio de direcciones internas si no es una dirección RFC 1918 (en esta actividad, su espacio de direcciones internas es parte del espacio de direcciones privadas especificado en RFC 1918).

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

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

```
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)#
```

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

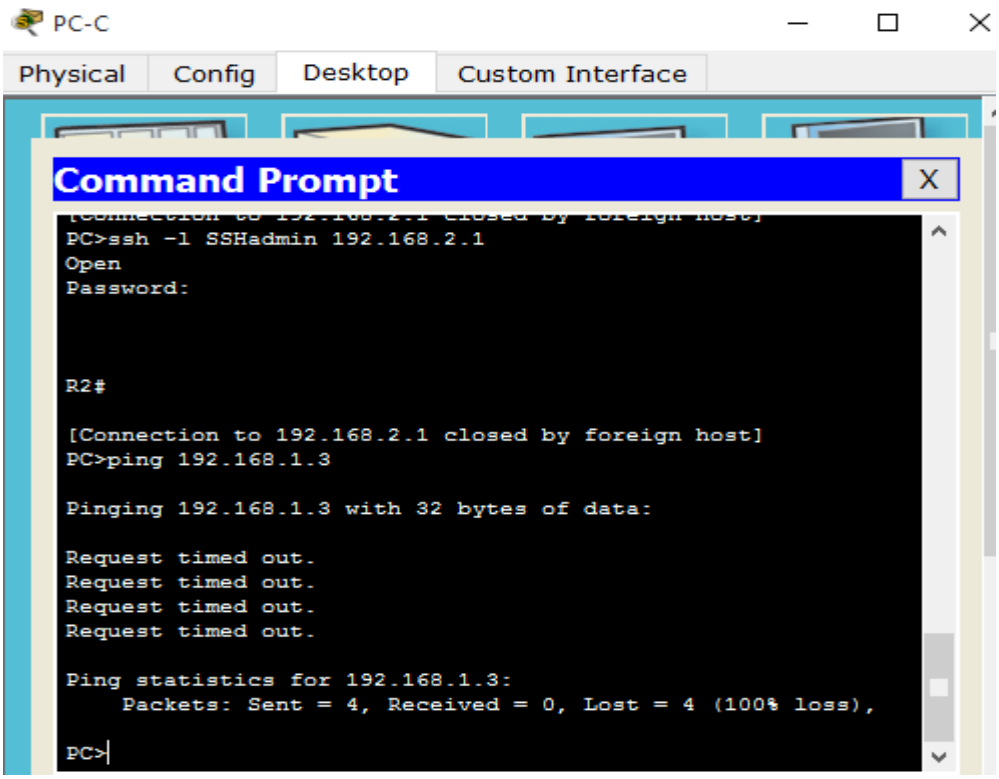
Use el comando ip access-group para aplicar la lista de acceso al tráfico entrante en la interfaz Serial 0/0/1.

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

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

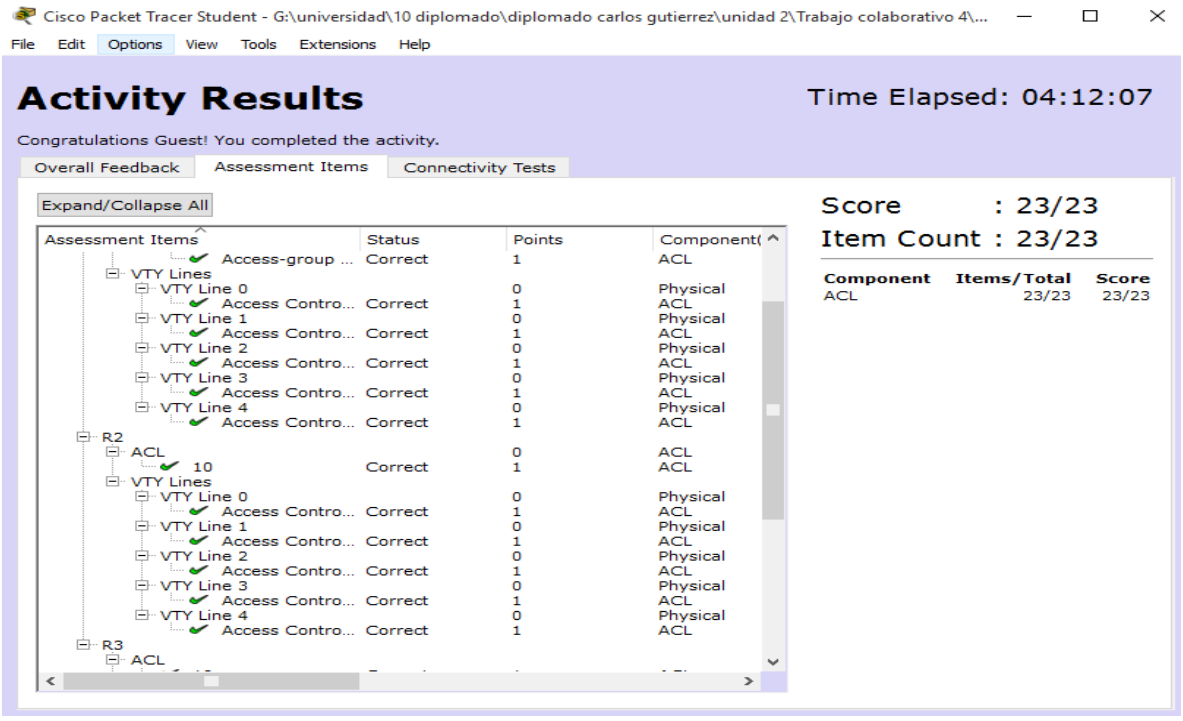
Paso 3: Confirme que la interfaz de entrada de tráfico especificada Serial 0/0/1 se elimine.

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



Paso 4: verifica los resultados.

Su porcentaje de finalización debe ser del 100%. Haga clic en Comprobar resultados para ver los comentarios y la verificación de cuál de los componentes requeridos han sido completados Las respuestas de eco ICMP están bloqueadas por la ACL, ya que se obtener del espacio de direcciones 192.168.0.0/16.



Desarrollo Ejercicio 7.3.2.4

Lab - Configuring Basic RIPv2 and RIPng

Topología

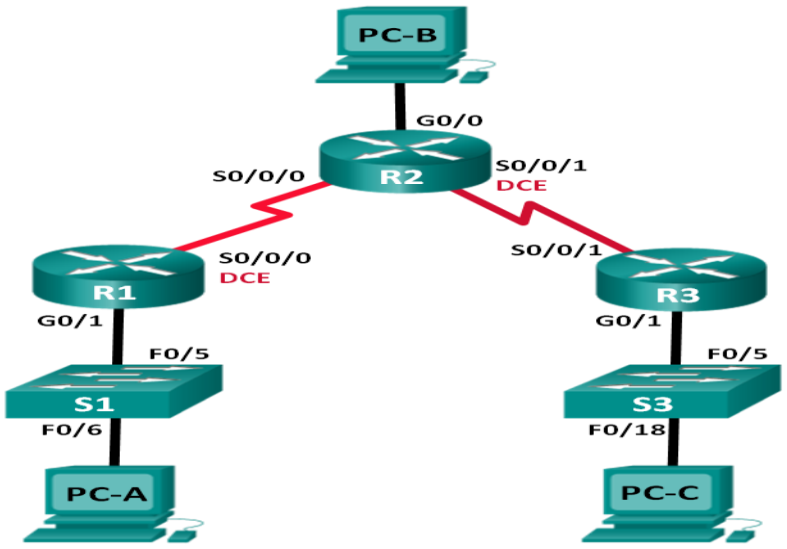


Tabla de direccionamiento

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 RIPng

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

Información básica/situación

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

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

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

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

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

Recursos necesarios

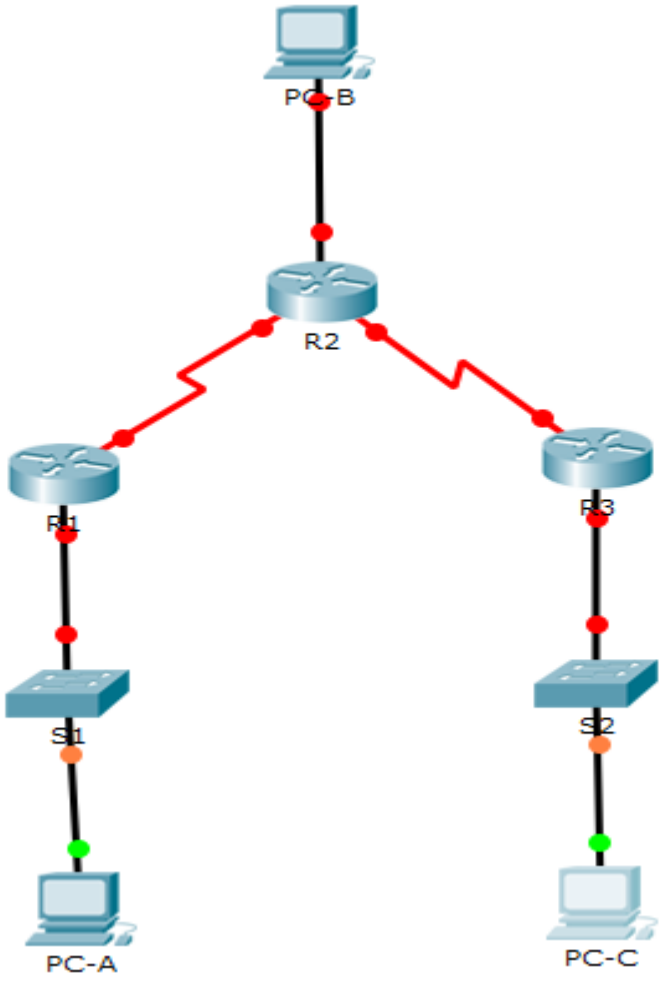
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4) M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

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

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

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

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



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

a. Desactive la búsqueda del DNS.
b. Configure los nombres de los dispositivos como se muestra en la topología.
c. Configurar la encriptación de contraseñas.
d. Asigne **class** como la contraseña del modo EXEC privilegiado.

e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

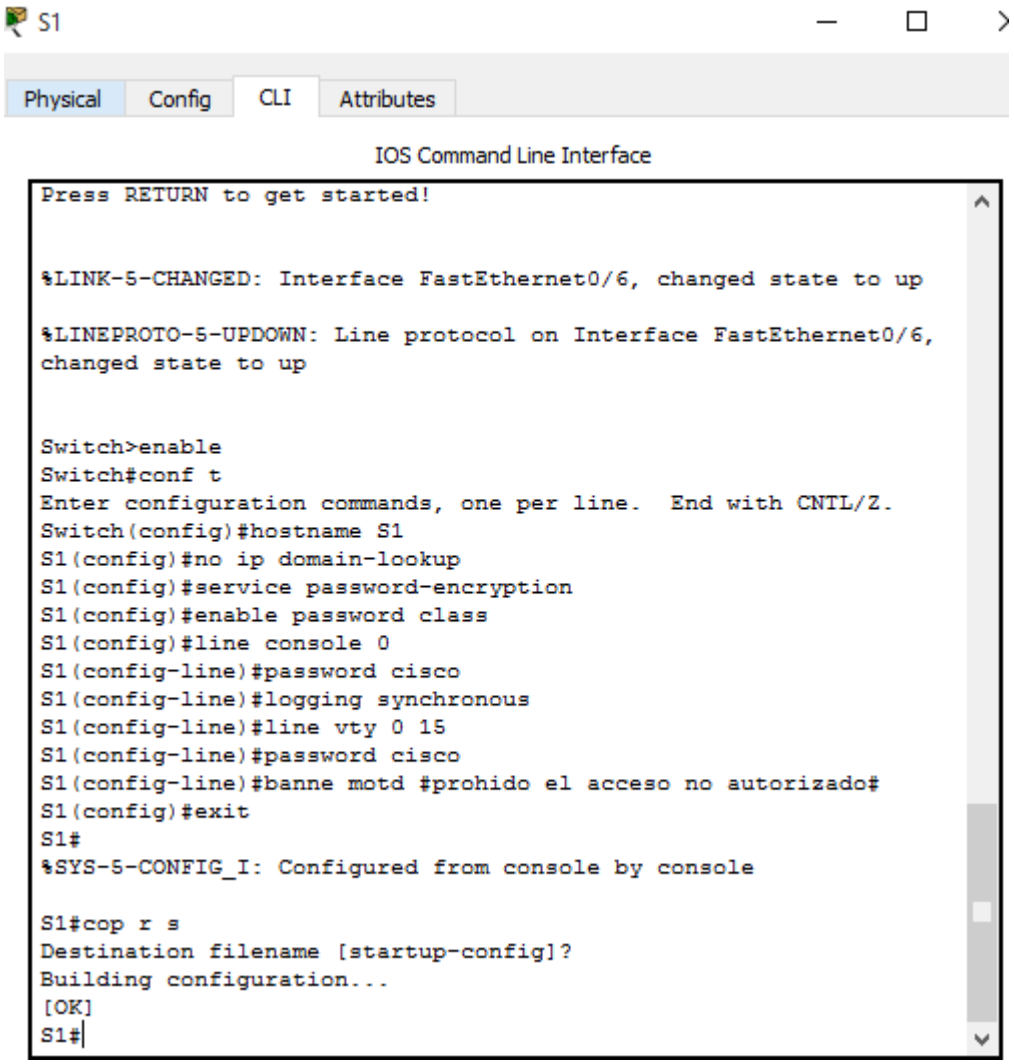
g. Configure **logging synchronous** para la línea de consola.

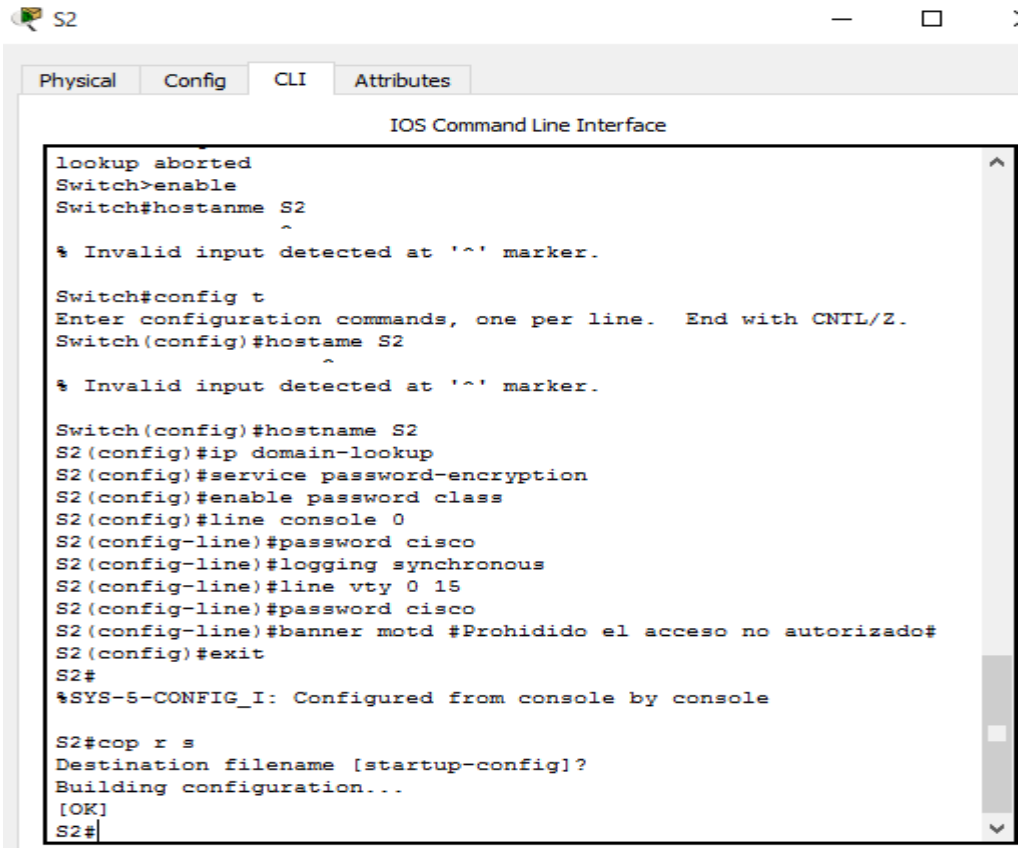
h. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.

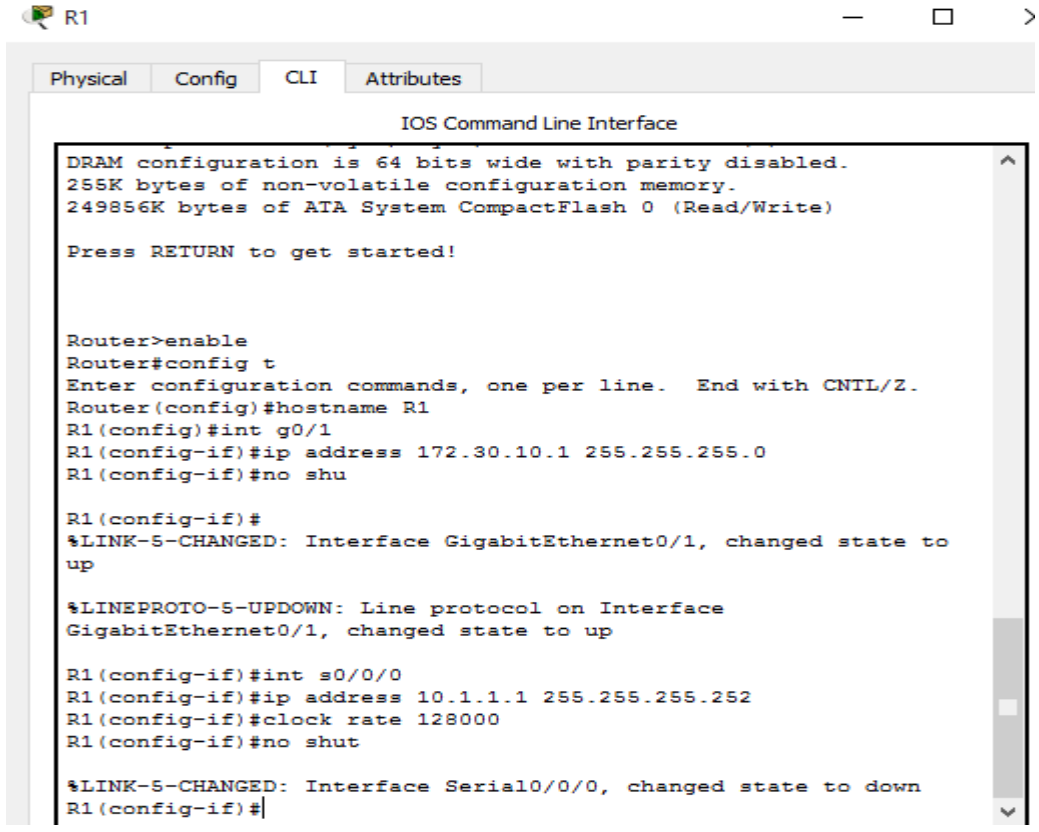
i. Configure una descripción para cada interfaz con una dirección IP.

j. Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.

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




S2
Physical
Config
CLI
Attributes
IOS Command Line Interface
lookup aborted
Switch>enable
Switch#hostanme S2
^
% Invalid input detected at '^' marker.
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostame S2
^
% Invalid input detected at '^' marker.
Switch(config)#hostname S2
S2(config)#ip domain-lookup
S2(config)#service password-encryption
S2(config)#enable password class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#logging synchronous
S2(config-line)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#banner motd #Prohidido el acceso no autorizado#
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
S2#


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#no shu
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)#int s0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#

R2

Physical | Config | CLI | Attributes

IOS Command Line Interface

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

R2(config-if)#int s0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut

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

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

                ^
% Invalid input detected at '^' marker.

R2(config-if)#int s0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#no shu

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
```

R3

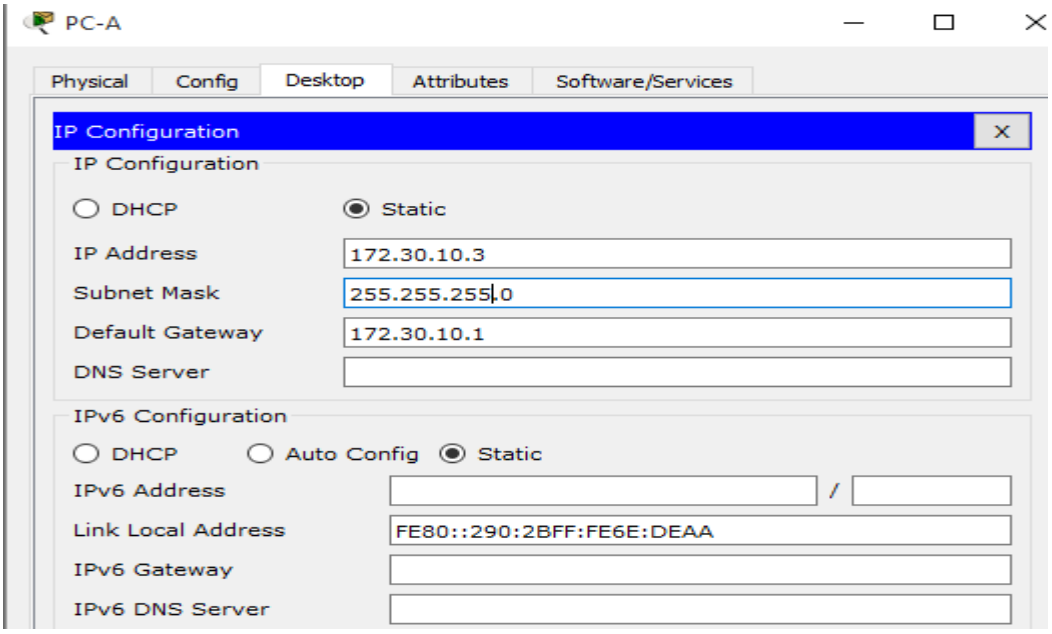
Physical | Config | CLI | Attributes

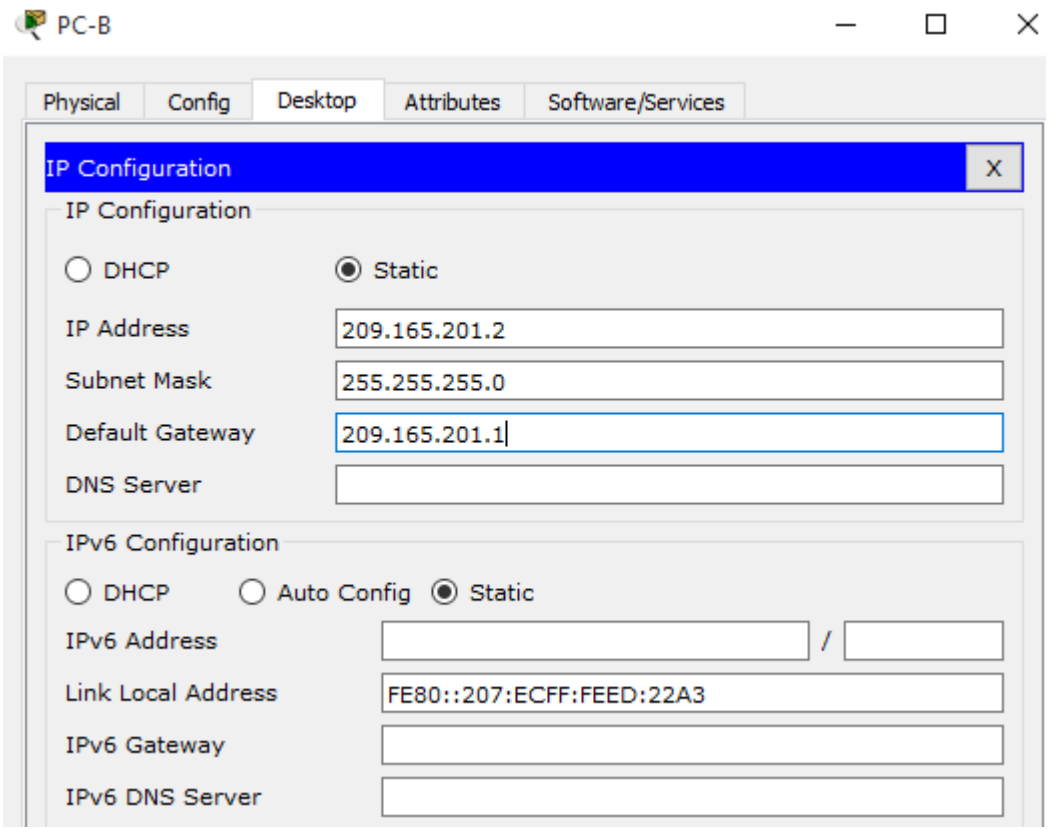
IOS Command Line Interface

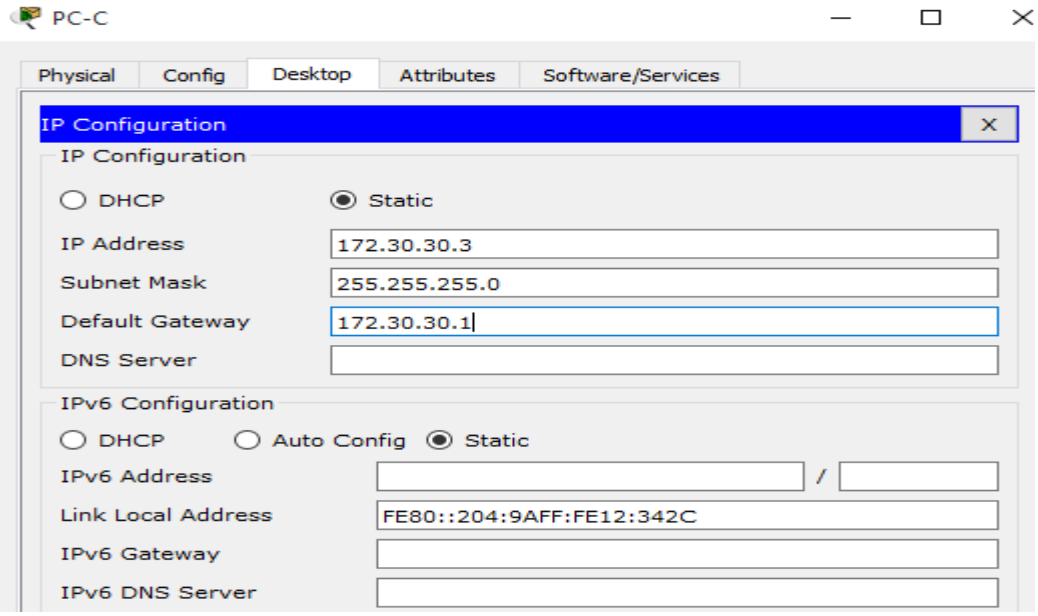
```
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!



Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#int g0/1
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#no shu

R3(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

R3(config-if)#int s0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shu

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

Paso 4. configurar los equipos host.

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





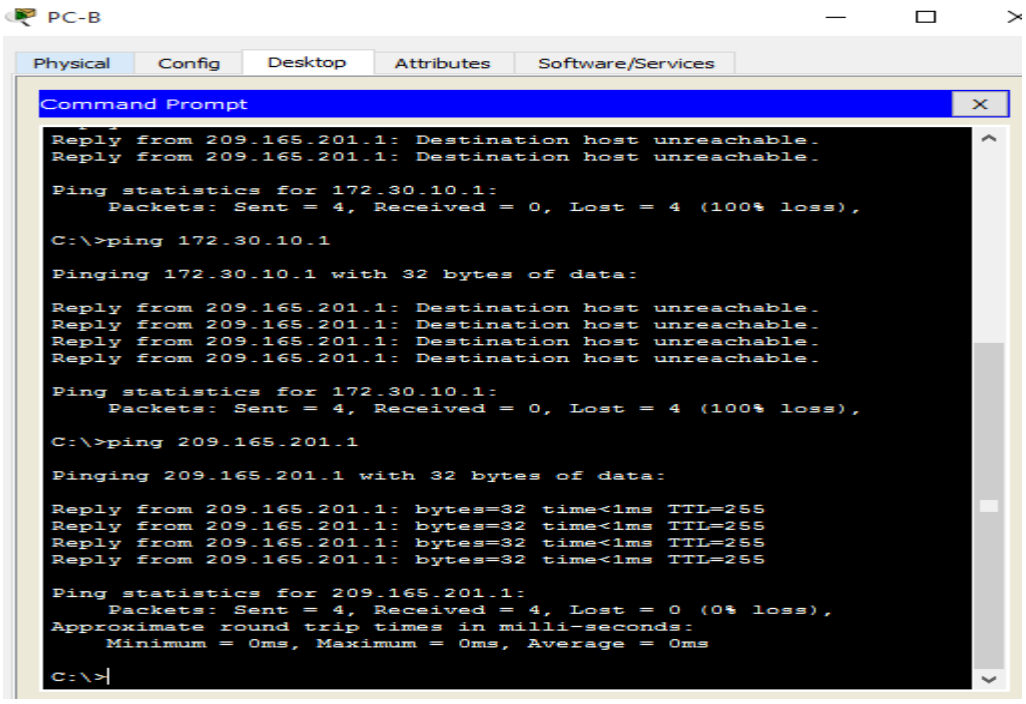


Paso 5. Probar la conectividad.

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

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

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



Parte 2: configurar y verificar el routing RIPv2

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

Paso 1. Configurar el enrutamiento RIPv2.

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

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.

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

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

```
R3>enable
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 172.30.0.0
R3(config-router)#network 10.0.0.0
R3(config-router)#passive-interface g0/1
R3(config-router)#
```

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

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#passive-interface g0/0
R2(config-router)#
```

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

b. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? **No** ¿Por qué? **Porque no hay una ruta establecida, pues PC-B está en la red que no está participando en RIP.**

¿Es posible hacer ping de la PC-A a la PC-C? **No** ¿Por qué? **Porque R1 y R3 no tienen rutas específicas para la subred del router remoto**

¿Es posible hacer ping de la PC-C a la PC-B? **No** ¿Por qué? **Porque PC-B pertenece a la LAN que no está participando en RIP**

¿Es posible hacer ping de la PC-C a la PC-A? **No** ¿Por qué? **Porque entre R1 y R3 no existen rutas**

a. Verifique que RIPv2 se ejecute en los routers.

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

R1# **show ip protocols**

```
R1>enable
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 15 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
           10.0.0.0
           172.30.0.0
Passive Interface(s):
           GigabitEthernet0/1
Routing Information Sources:
           Gateway         Distance      Last Update
           10.1.1.2              120      00:00:11
Distance: (default is 120)
```

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

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

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

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

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

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

```
R3#show run
Building configuration...

Current configuration : 882 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX152492C5
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
```

d. Examinar el sumarización automática de las rutas.

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

R2# show ip route

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R    172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:28, Serial0/0/1
                   [120/1] via 10.1.1.1, 00:00:08, 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.

```
     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, 00:00:04, 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
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

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

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

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

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

Paso 3. Desactivar la sumarización automática.

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

   R1(config)# router rip

   R1(config-router)# no auto-summary

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

```
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#
```

```
R3(config)#router rip
R3(config-router)#no auto-summary
R3(config-router)#
```

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

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

R1# **clear ip route ***

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

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

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

R2# **show ip route**

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:05, 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, 00:00:05, Serial0/0/0
```

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

Gateway of last resort is not set

     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, 00:00:20, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:21, 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
```

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:15, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:15, Serial0/0/1
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1
```

d. 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 via 0.0.0.0, metric 2, tag 0
172.30.10.0/24 via 0.0.0.0, metric 2, tag 0

```
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.30.0/24 via 0.0.0.0 in 1 hops
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.10.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.30.0/24 via 0.0.0.0 in 1 hops
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0

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

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

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

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

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

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

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

R2(config)# **router rip**

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

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

Paso 5. Verificar la configuración de enrutamiento.

c. Consulte la tabla de routing en el R1.

R1# **show ip route**

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

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

Por medio de la existencia del Gateway de último alcance y la ruta por defecto mostrada en las tablas de ruteo, son aprendidas por medio de RIP

d. Consulte la tabla de routing en el R2.

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

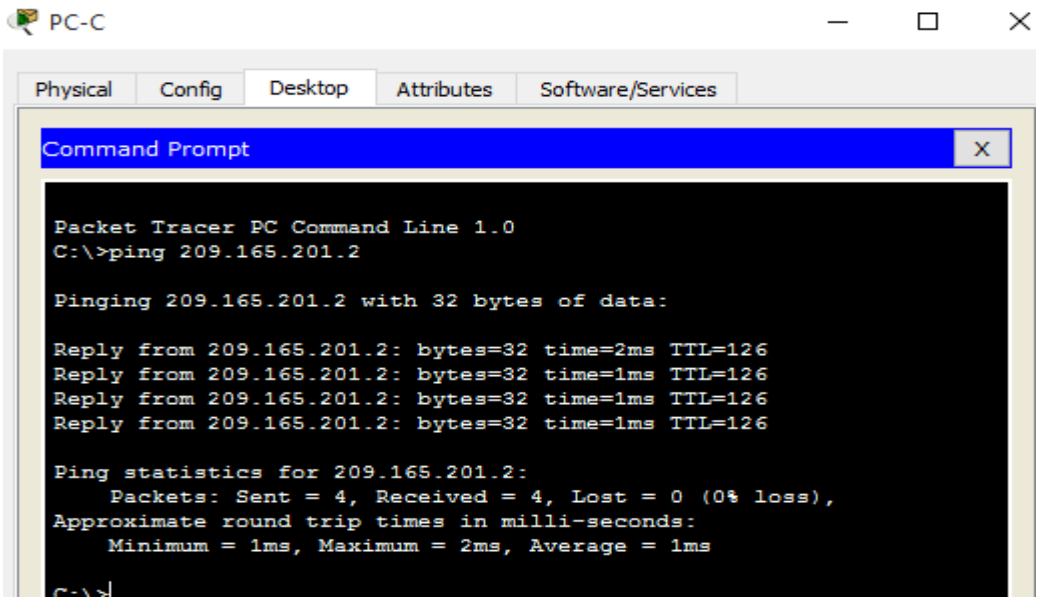
R2 tiene una ruta por defecto por medio de la dirección 209.165.201.2 conectada a la red por la interfaz G0/0

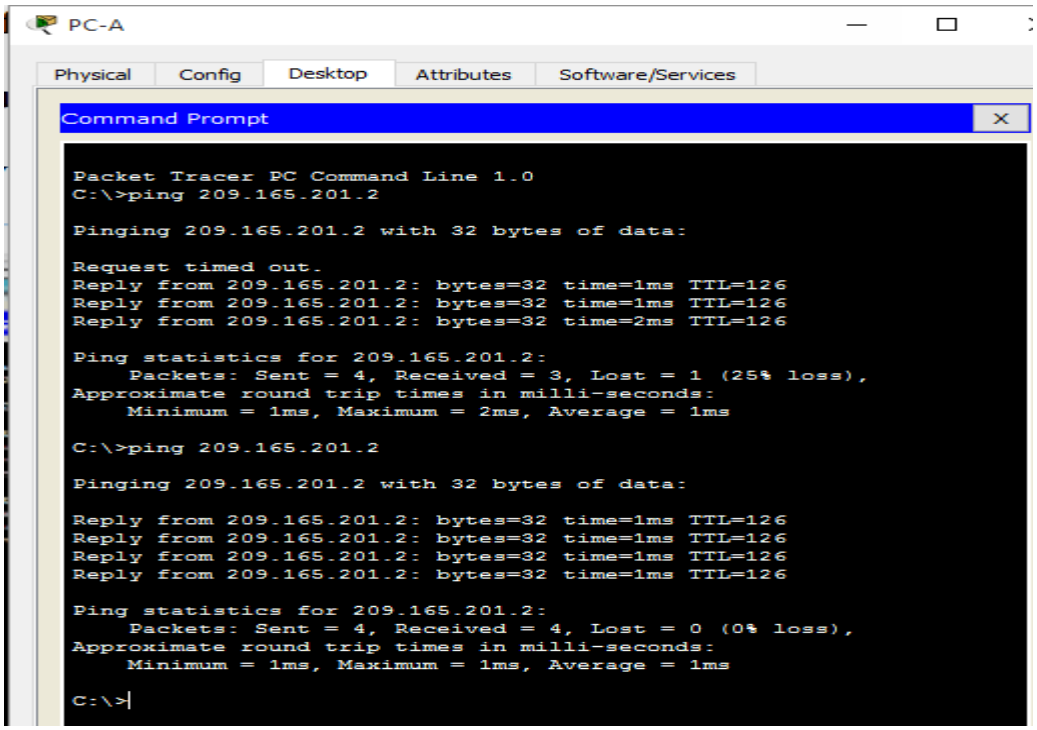
```
Gateway of last resort is 209.165.201.2 to network 0.0.0.0

     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, 00:00:09,
Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:27,
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
```

Paso 6. Verifique la conectividad.

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

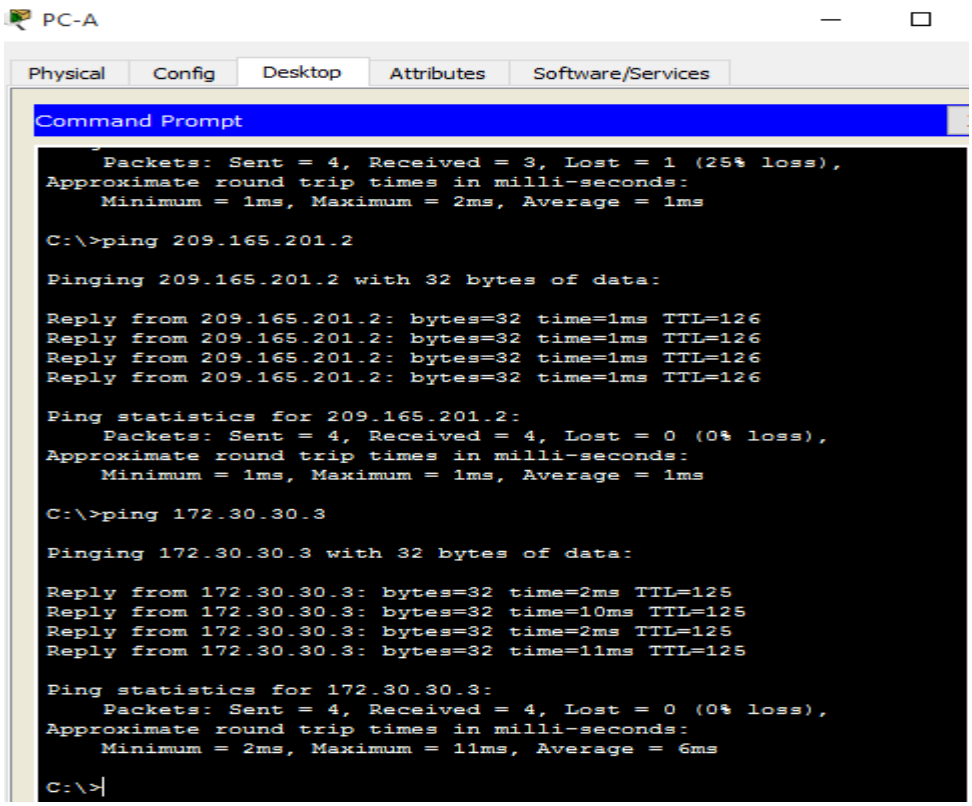
¿Tuvieron éxito los pings? **SI**





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

¿Tuvieron éxito los pings? **SI**



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

Parte 3: configurar IPv6 en los dispositivos

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

Tabla de direccionamiento

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

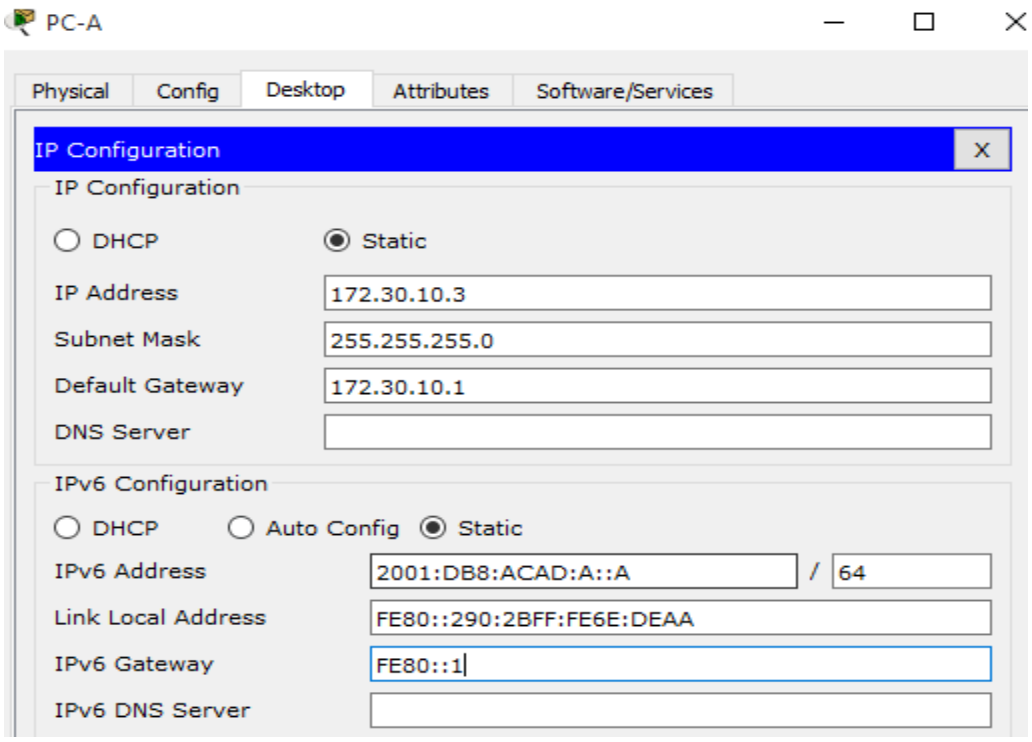
Paso 1. configurar los equipos host.

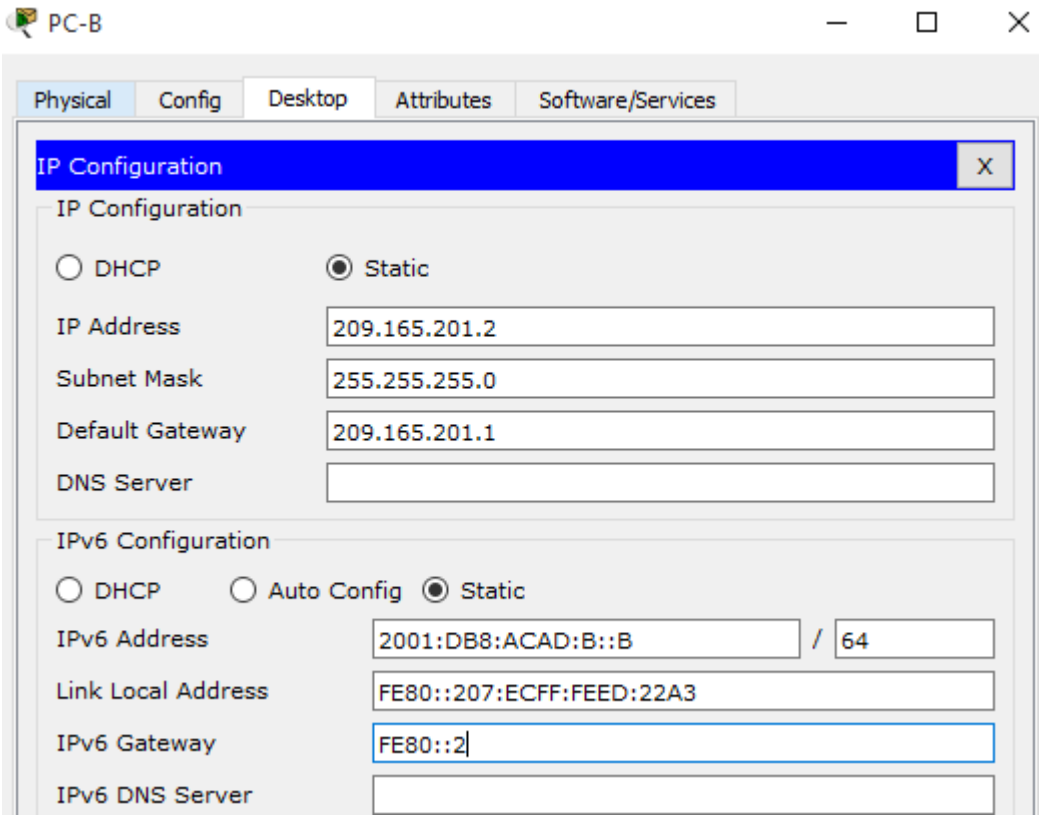
Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

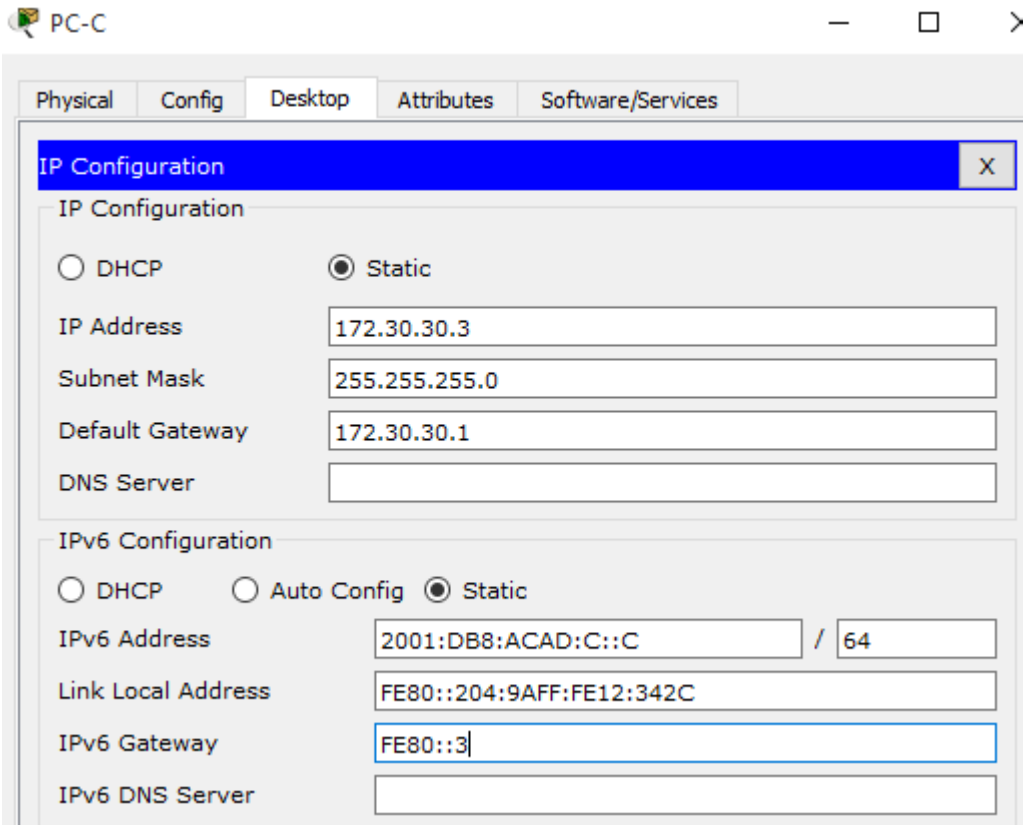
```
R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#IPV6 ADDRESS FE80:1 LINK-LOCAL
                                  ^
% Invalid input detected at '^' marker.

R1(config-if)#IPV6 ADDRESS FE80::1 LINK-LOCAL
R1(config-if)#INT S0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#IPV6 ADDRESS FE80::1 LINK-LOCAL
R1(config-if)#
```

```
R2>
R2>ENABLE
R2#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#INT G0/0
R2(config-if)#IPV6 ADDRESS 2001:DB8:ACAD:B::2/64
R2(config-if)#IPV6 ADDRESS FE80::2 LINK-LOCAL
R2(config-if)#INT S0/0/0
R2(config-if)#IPV6 ADDRESS 2001:DB8:ACAD:12::2/64
R2(config-if)#IPV6 ADDRESS FE80::2 LINK-LOCAL
R2(config-if)#INT S0/0/1
R2(config-if)#IPV6 ADDRESS 2001:DB8:ACAD:23::2/64
R2(config-if)#IPV6 ADDRESS FE80::2 LINK-LOCAL
R2(config-if)#
```

```
R3>ENABLE
R3#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#INT G0/1
R3(config-if)#IPV6 ADDRESS 2001:DB8:ACAD:C::3/64
R3(config-if)#IPV6 ADDRESS FE80::3 LINK-LOCAL
R3(config-if)#INT S0/0/1
R3(config-if)#IPV6 ADDRESS 2001:DB8:ACAD:23::3/64
R3(config-if)#IPV6 ADDRESS FE80::3 LINK-LOCAL
R3(config-if)#END
```




PC-B
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
IP Configuration
DHCP
Static
IP Address
209.165.201.2
Subnet Mask
255.255.255.0
Default Gateway
209.165.201.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:ACAD:B::B
/
64
Link Local Address
FE80::207:ECFF:FEED:22A3
IPv6 Gateway
FE80::2
IPv6 DNS Server


PC-C
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
IP Configuration
DHCP
Static
IP Address
172.30.30.3
Subnet Mask
255.255.255.0
Default Gateway
172.30.30.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:ACAD:C::C
/
64
Link Local Address
FE80::204:9AFF:FE12:342C
IPv6 Gateway
FE80::3
IPv6 DNS Server

Paso 2. configurar IPv6 en los routers.

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

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

b. Habilite el routing IPv6 en cada router.

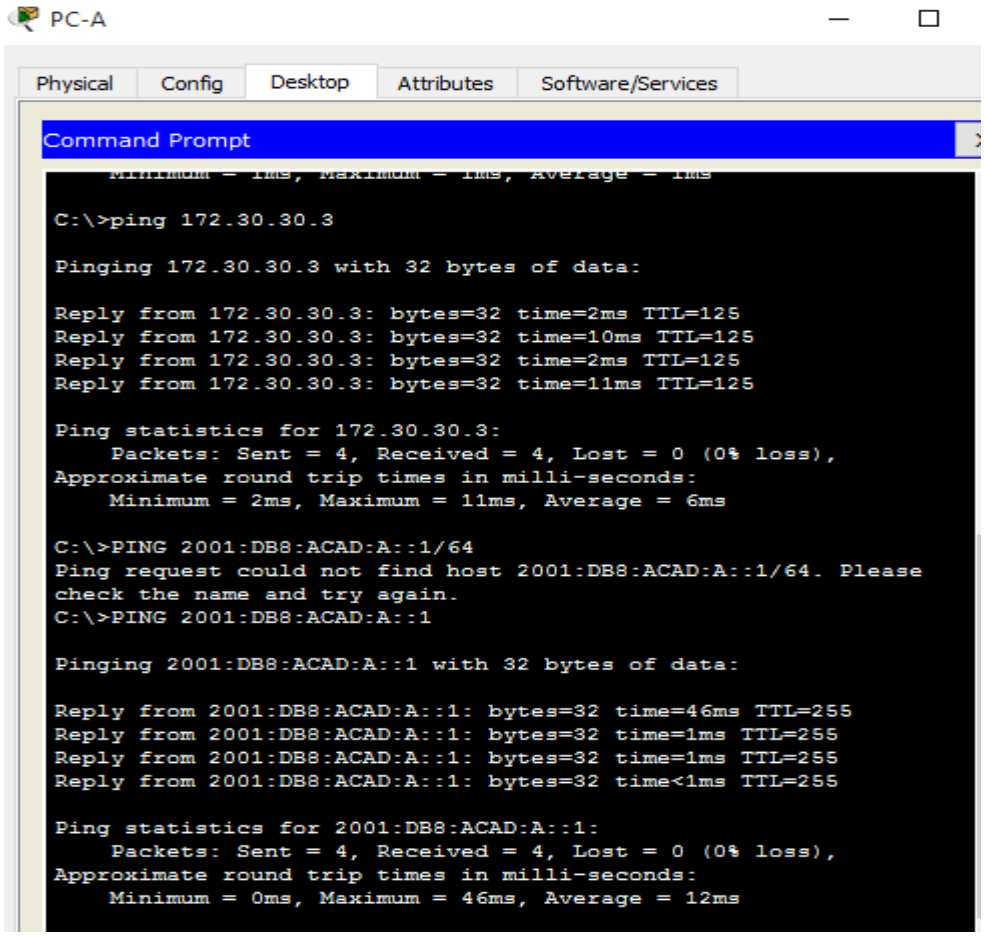
c. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.

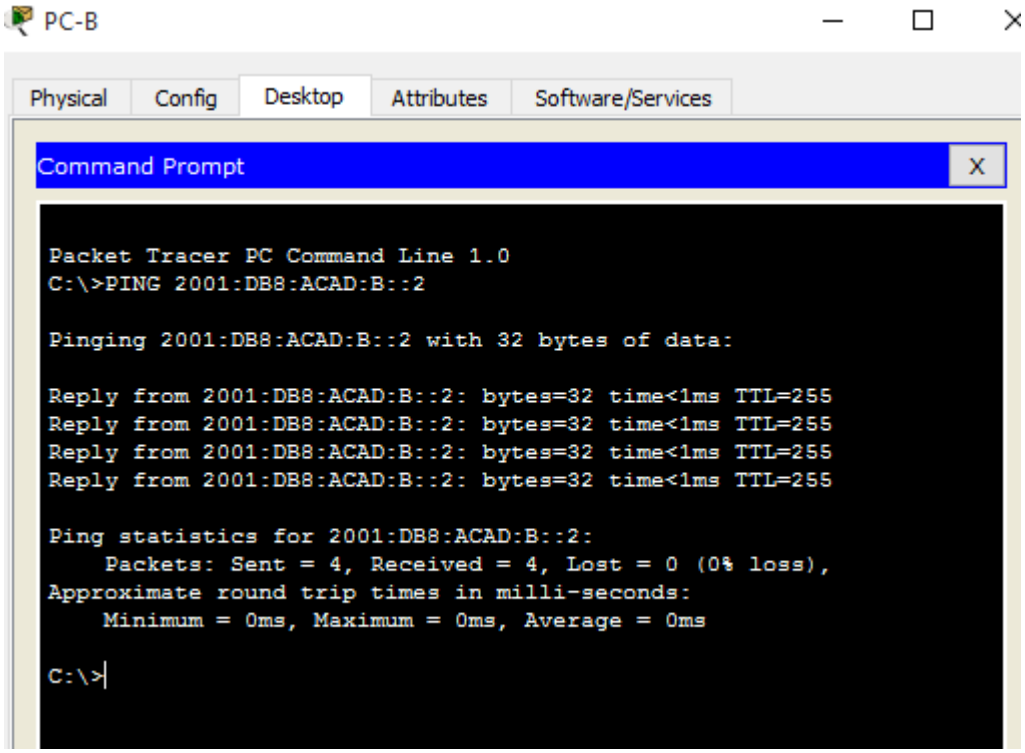
```
R1>ENABLE
R1# SHOW IPV6 INT BRIEF
GigabitEthernet0/0          [administratively down/down]
GigabitEthernet0/1          [up/up]
    FE80::1
    2001:DB8:ACAD:A::1
Serial0/0/0                 [up/up]
    FE80::1
    2001:DB8:ACAD:12::1
Serial0/0/1                 [administratively down/down]
Vlan1                       [administratively down/down]
```

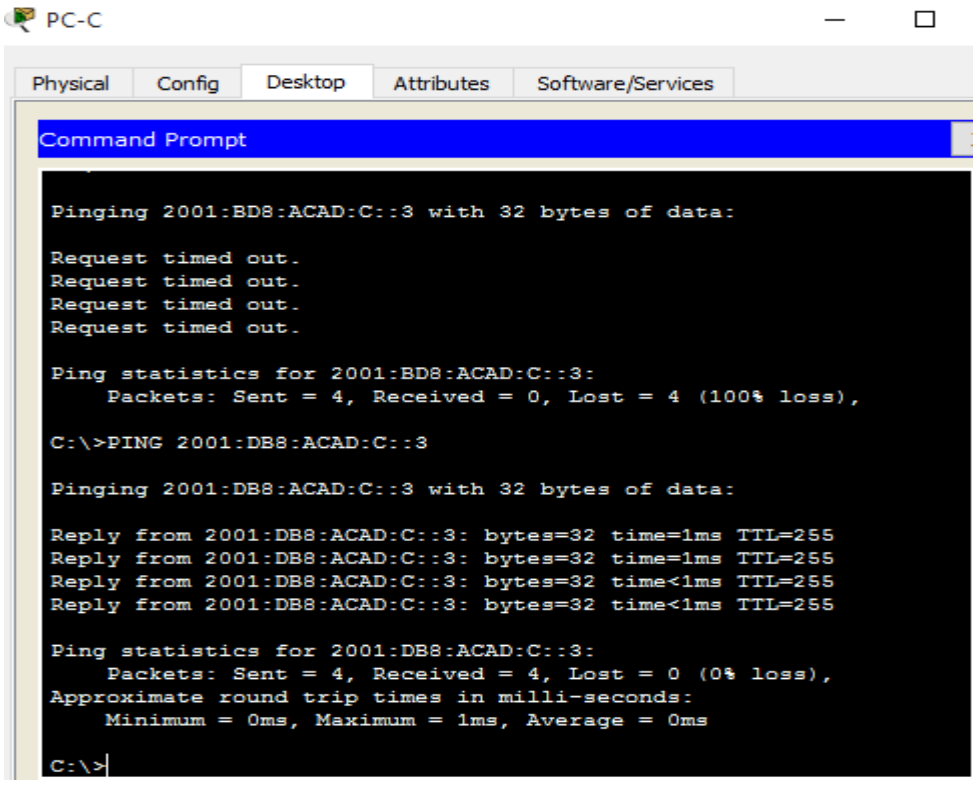
```
R2>ENABLE
R2#SHOW IPV6 INT BRIEF
GigabitEthernet0/0          [up/up]
    FE80::2
    2001:DB8:ACAD:B::2
GigabitEthernet0/1          [administratively down/down]
Serial0/0/0                 [up/up]
    FE80::2
    2001:DB8:ACAD:12::2
Serial0/0/1                 [up/up]
    FE80::2
    2001:DB8:ACAD:23::2
Vlan1                       [administratively down/down]
```

```
R3#SHOW IPV6 INT BRIEF
GigabitEthernet0/0          [administratively down/down]
GigabitEthernet0/1          [up/up]
    FE80::3
    2001:BD8:ACAD:C::3
Serial0/0/0                 [administratively down/down]
Serial0/0/1                 [up/up]
    FE80::3
    2001:BD8:ACAD:23::3
Vlan1                       [administratively down/down]
```

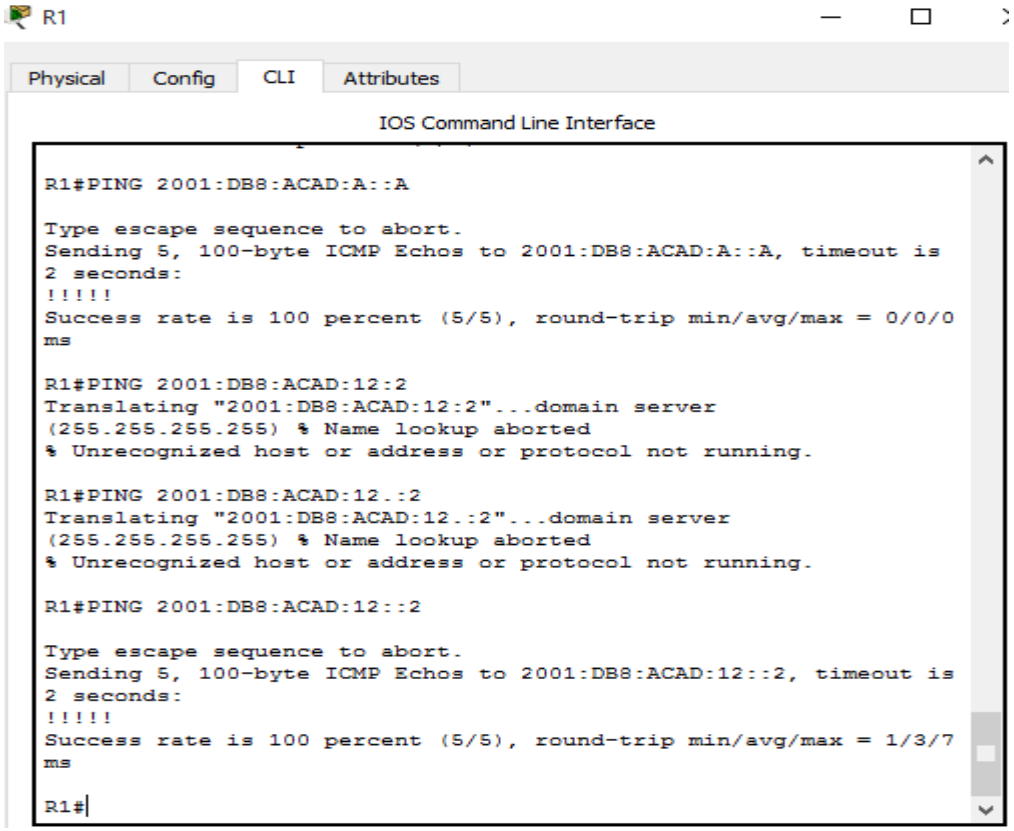
d. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.

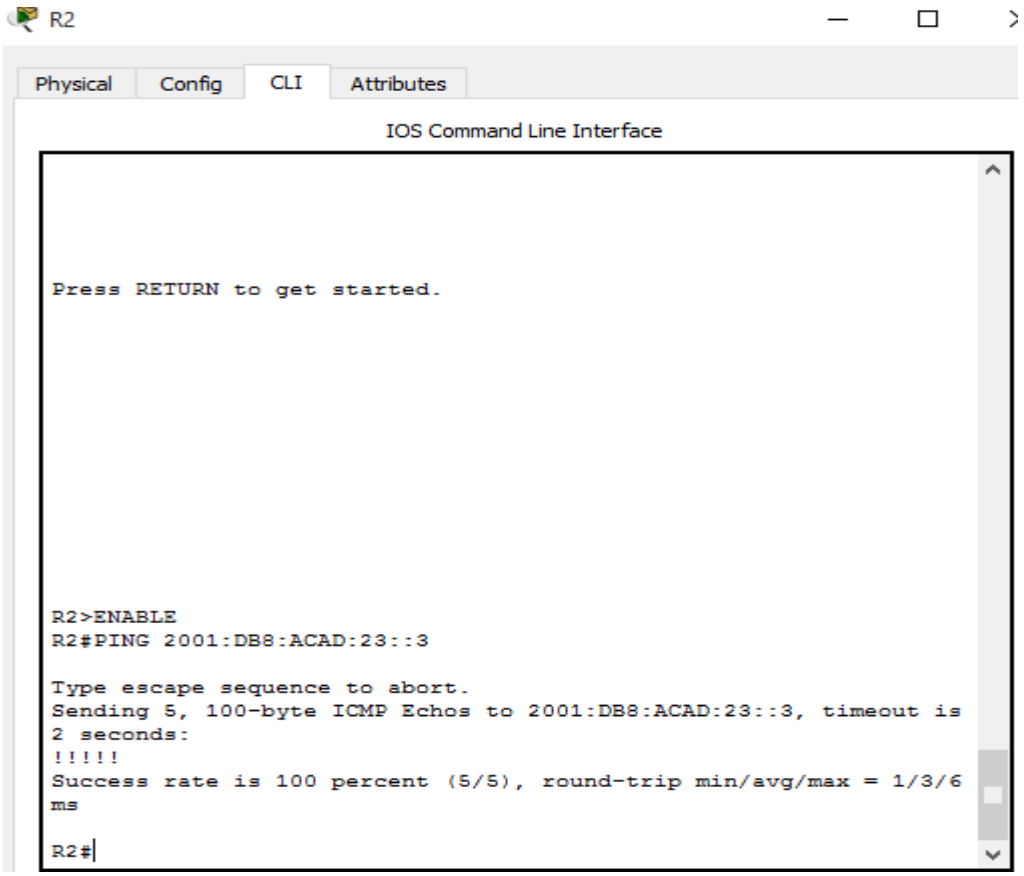

PC-A
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=10ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms 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 = 2ms, Maximum = 11ms, Average = 6ms
C:\>PING 2001:DB8:ACAD:A::1/64
Ping request could not find host 2001:DB8:ACAD:A::1/64. Please
check the name and try again.
C:\>PING 2001:DB8:ACAD:A::1
Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=46ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB8:ACAD:A::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 46ms, Average = 12ms


PC-B
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>PING 2001:DB8:ACAD:B::2
Pinging 2001:DB8:ACAD:B::2 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::2: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB8:ACAD:B::2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>



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





Parte 4: configurar y verificar el routing RIPng

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

Paso 1. configurar el routing RIPng.

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

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

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

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#int g0/1
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#int s0/0/0
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#
```

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

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#
```

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

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#int g0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#
```

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

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

R1# **show ipv6 protocols**

```
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test1"
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
  Redistribution:
    None

R1#
```

¿En qué forma se indica RIPng en el resultado?

El RIPng es distingue en el resultado pues aparece listado con el nombre del proceso. “RIP Test1

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

R1# **show ipv6 rip Test1**

¿Cuáles son las similitudes entre RIPv2 y RIPng?

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

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

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

```
R1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:BD8:ACAD:C::/64 [120/3]
     via FE80::2, Serial0/0/0
R   2001:BD8:ACAD:23::/64 [120/3]
     via FE80::2, Serial0/0/0
C   2001:DB8:ACAD:A::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:A::1/128 [0/0]
     via GigabitEthernet0/1, receive
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, directly connected
L   2001:DB8:ACAD:12::1/128 [0/0]
     via Serial0/0/0, receive
R   2001:DB8:ACAD:23::/64 [120/2]
     via FE80::2, Serial0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

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

```
R2#show ipv6 route
IPv6 Routing Table - 11 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:BD8:ACAD:C::/64 [120/2]
     via FE80::3, Serial0/0/1
R   2001:BD8:ACAD:23::/64 [120/2]
     via FE80::3, Serial0/0/1
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, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
     via GigabitEthernet0/0, receive
R   2001:DB8:ACAD:C::/64 [120/2]
     via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

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

```
R3#show ipv6 route
IPv6 Routing Table - 11 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:BD8:ACAD:C::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:BD8:ACAD:C::3/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:BD8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:BD8:ACAD:23::3/128 [0/0]
     via Serial0/0/1, receive
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, directly connected
L   2001:DB8:ACAD:C::3/128 [0/0]
     via GigabitEthernet0/1, receive
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, directly connected
L   2001:DB8:ACAD:23::3/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R3#
```

g. Verifique la conectividad entre las computadoras.

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

```
C:\>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),
```

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

```
C:\>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=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=11ms 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 = 2ms, Maximum = 11ms, Average = 4ms
```

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

```
C:\>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),
```

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

```
C:\>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=5ms 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=10ms 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 = 5ms, Maximum = 11ms, Average = 9ms
```

¿Por qué algunos pings tuvieron éxito y otros no? **Porque no hay una ruta notificada para la red donde se encuentra el PC-B**

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

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

El comando usado fue R2(config)#ipv6 route ::/0 2001:db8:acad:b::b

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

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**

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

Paso 3. Verificar la configuración de enrutamiento.

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

R2# **show ipv6 route**

```
R2#show ipv6 route
IPv6 Routing Table - 12 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   ::/0 [1/0]
     via 2001:DB8:ACAD:B::B
R   2001:BD8:ACAD:C::/64 [120/2]
     via FE80::3, Serial0/0/1
R   2001:BD8:ACAD:23::/64 [120/2]
     via FE80::3, Serial0/0/1
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, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
     via GigabitEthernet0/0, receive
R   2001:DB8:ACAD:C::/64 [120/2]
     via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R2#
```

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

Se muestra en la tabla de ruteo en R2, representada como

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

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

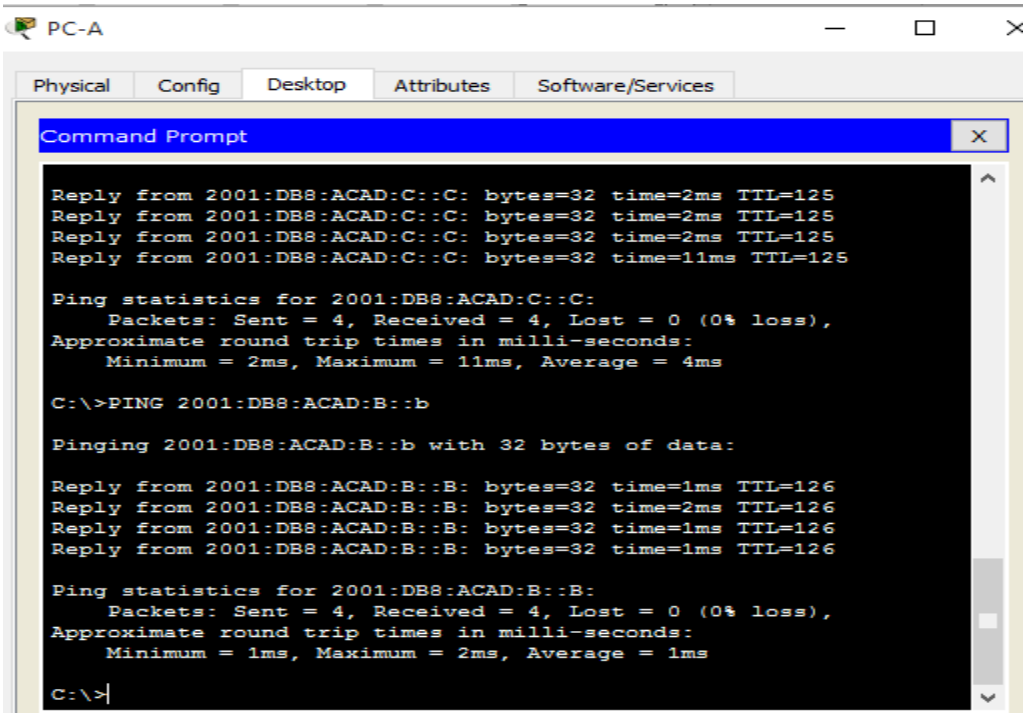
¿Cómo se proporciona la ruta para el tráfico de Internet en sus tablas de enrutamiento? **La tabla de ruteo se muestra distribuida con una métrica de 2, por medio de RIPng**

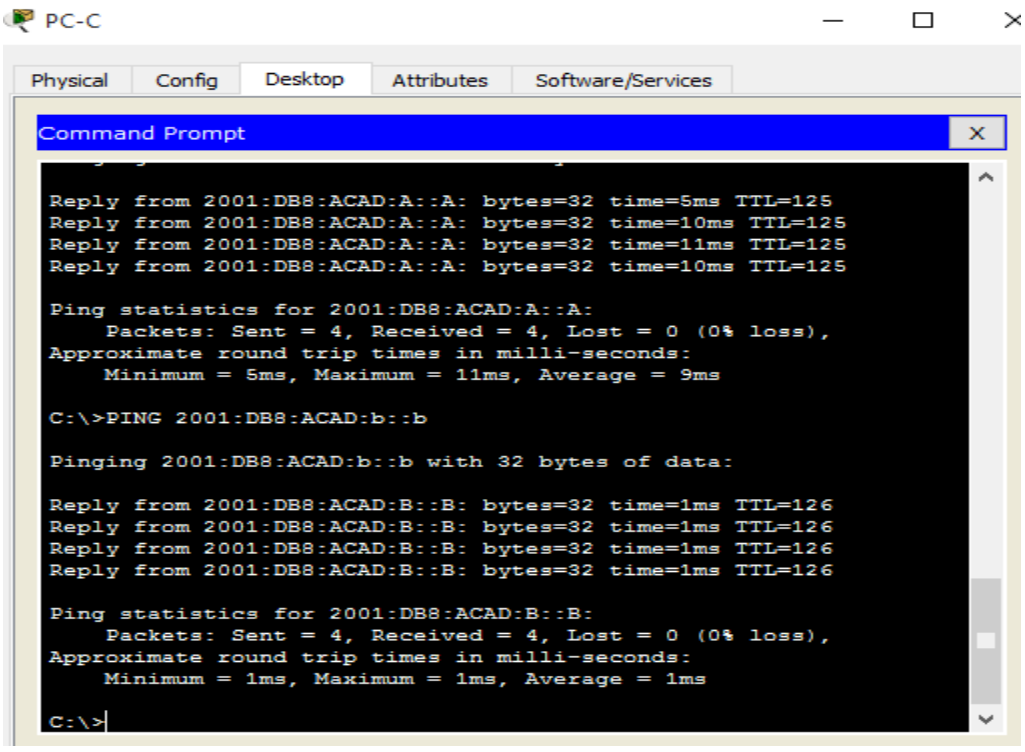
```
R3>enable
R3#show ipv6 route
IPv6 Routing Table - 12 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   ::/0 [120/2]
     via FE80::2, Serial0/0/1
C   2001:BD8:ACAD:C::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:BD8:ACAD:C::3/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:BD8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:BD8:ACAD:23::3/128 [0/0]
     via Serial0/0/1, receive
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, directly connected
L   2001:DB8:ACAD:C::3/128 [0/0]
     via GigabitEthernet0/1, receive
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, directly connected
L   2001:DB8:ACAD:23::3/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R3#
```

Paso 4. Verifique la conectividad.

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

¿Tuvieron éxito los pings? **Si**





Reflexión

¿Por qué desactivaría la sumarización automática para RIPv2?

Es necesario para que los router no sumaricen las rutas hacia la clase mayor, lo que facilite la conectividad entre redes discontinuas

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

Dichas rutas fueron aprendidas por medio de las actualizaciones del RIP, recibidas desde el router R2, donde fue configurada la ruta por defecto

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

RIPv2 se configura notificando las redes y RIPng se debe configurar desde las interfaces.

Desarrollo Ejercicio 8.2.4.5

Práctica de laboratorio: configuración de OSPFv2 básico de área única

Topología

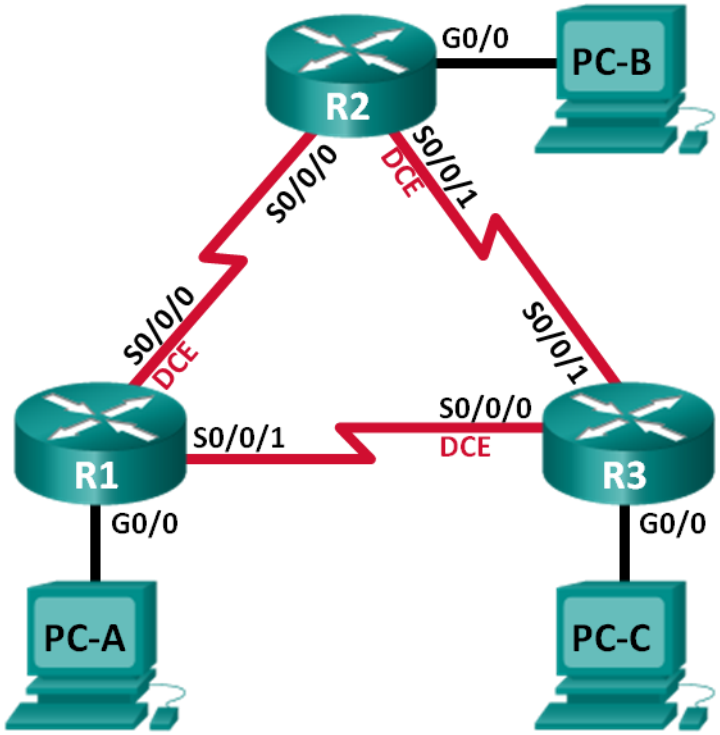


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPF

Parte 3: cambiar las asignaciones de ID del router

Parte 4: configurar interfaces OSPF pasivas

Parte 5: cambiar las métricas de OSPF

Información básica/situación

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

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

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

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

Recursos necesarios

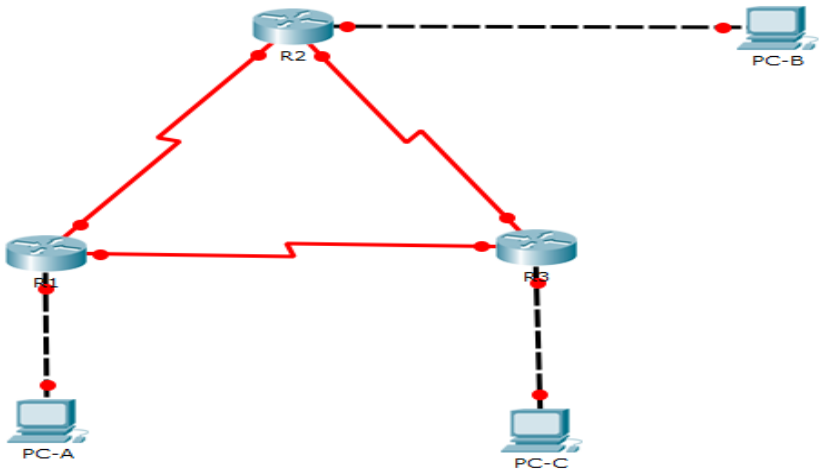
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet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

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

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

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

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



Paso 3. configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

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

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

d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

e. Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.

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

g. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.

h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.

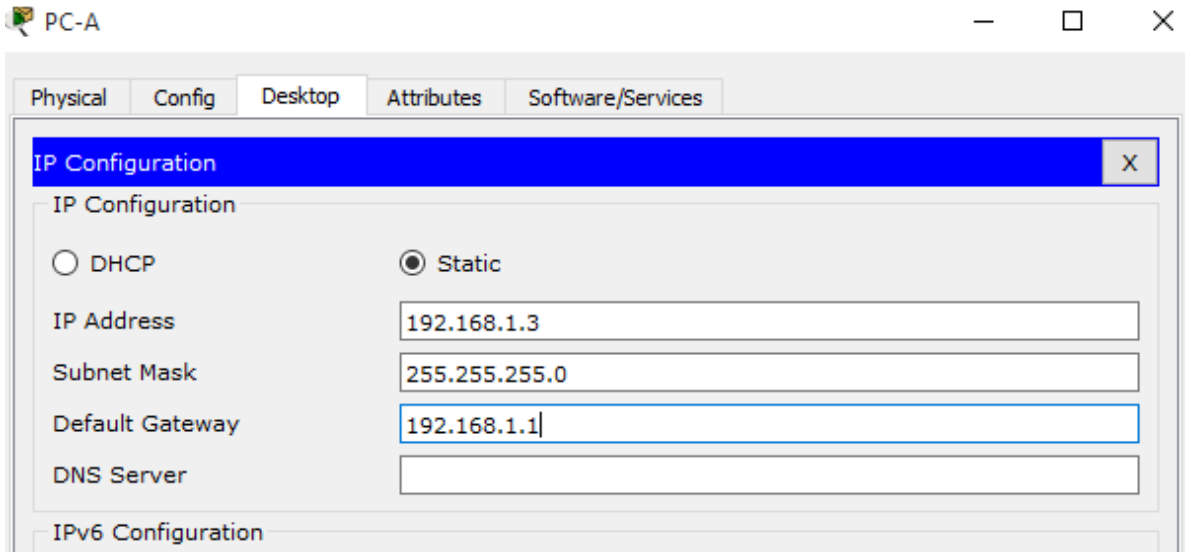
i. Copie la configuración en ejecución en la configuración de inicio

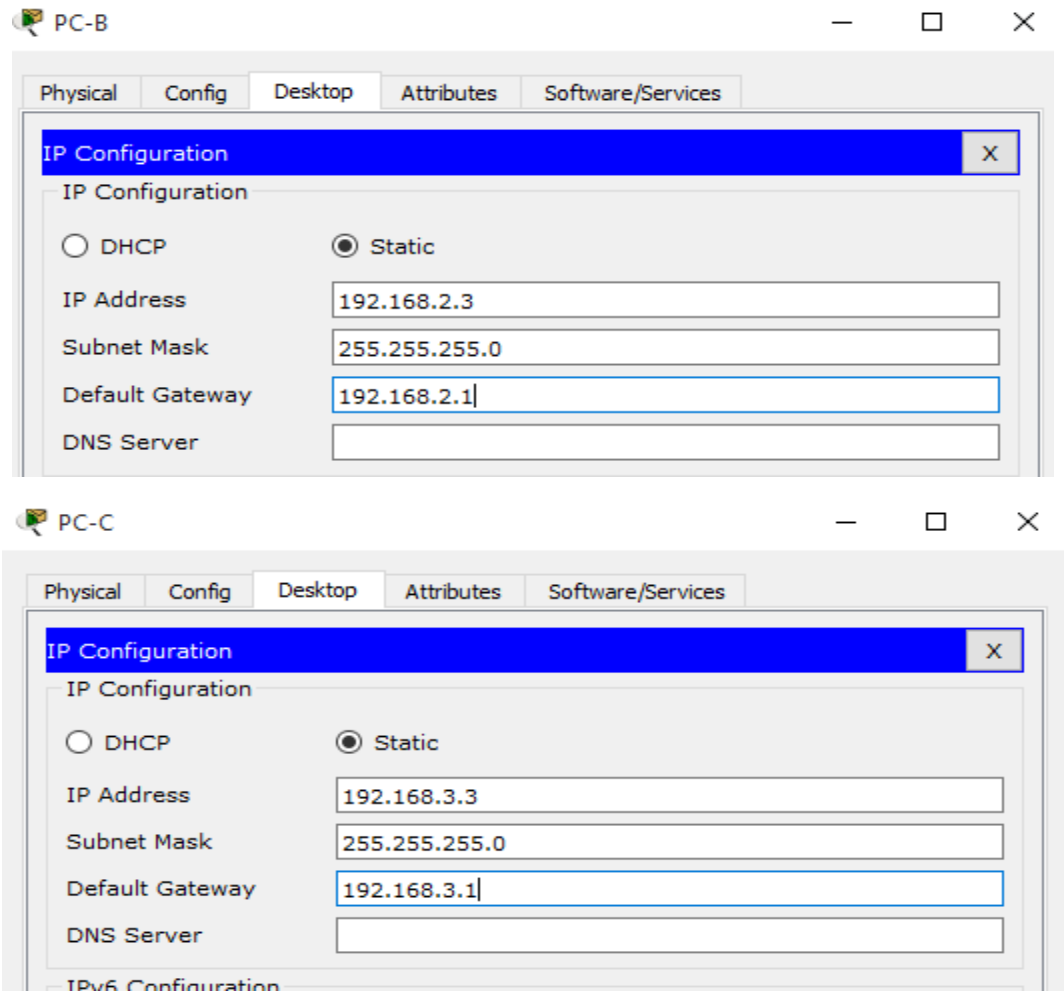
```
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#banner motd #El acceso no autorizado esta prohibido#
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#int g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shu

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

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

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

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
R1(config-if)#int s0/0/1
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shu

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

```
R2(config)#no ip pdomain-lookup
                ^
% Invalid input detected at '^' marker.

R2(config)#no ip domain-lookup
R2(config)#enable secret class
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#int g0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shu

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

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

R2(config-if)#int s0/0/0
R2(config-if)#ip address 192.168.12.2 255.255.255.252
R2(config-if)#no shu

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

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
no shu
R2(config-if)#int s0/0/1
R2(config-if)#ip address 192.168.3.1 255.255.255.252
R2(config-if)#no shu

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#int s0/0/1
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#no shu
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R3(config-line)#password cisco
R3(config-line)#line console vty 0 15
                ^
% Invalid input detected at '^' marker.

R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#enable secret class
R3(config)#line console 0
R3(config-line)#logging synchronous
R3(config-line)#banner motd
                ^
% Invalid input detected at '^' marker.

R3(config-line)#banner motd #El acceso no autorizado esta prohibido#
R3(config)#int s0/0/0
R3(config-if)#ip address 192.168.13.2 255.255.255.252
R3(config-if)#no shu

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

R3(config-if)#int s0/0/0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R3(config-if)#int s0/0/1
R3(config-if)#ip address 192.168.23.2 255.255.255.252
R3(config-if)#no shu

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

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3(config-if)#int s0/0/0
R3(config-if)#clock rate 128000
R3(config-if)#no shu
R3(config-if)#exit
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

Paso 4. configurar los equipos host.





Paso 5 Probar la conectividad.

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

```
R1>enable
Password:
R1#ping 192.168.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6
ms

R1#ping 192.168.13.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8
ms
```

PC-A

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

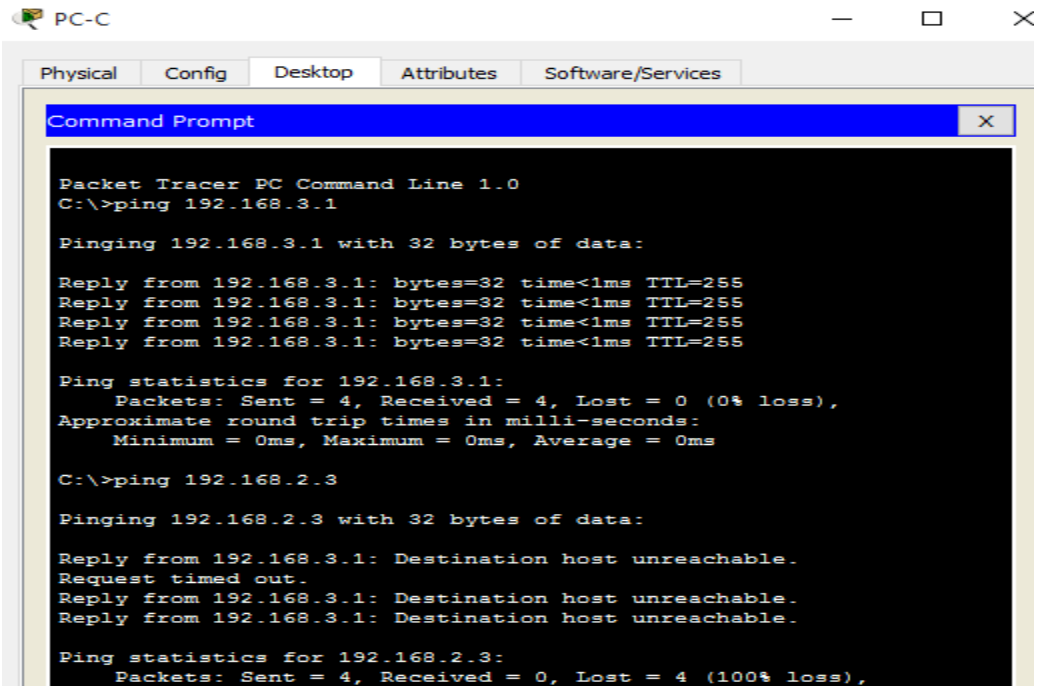
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC-B

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

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

Pinging 192.168.2.1 with 32 bytes of data:

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

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

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Request timed out.

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



Parte 2: Configurar y verificar el enrutamiento OSPF

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

Paso 1: Configure el protocolo OSPF en R1.

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

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

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

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

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

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

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

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

```
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
R2(config-router)#
00:57:15: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R2(config-router)#network 192.168.23.0 0.0.0.3 area 0
R2(config-router)#
```

```
R3>enable
Password:
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0
R3(config-router)#network 192.168.3.0 0.0.0.3 area 0
01:00:57: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R3(config-router)#network 192.168.23.0 0.0.0.3 area 0
R3(config-router)#
```

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

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

R1# show ip ospf neighbor

```
R1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.12.2      0   FULL/  -        00:00:39    192.168.12.2    Serial0/0/0
192.168.23.2      0   FULL/  -        00:00:36    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**

```
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, 00:08:12, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:30, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 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, 00:04:19, Serial0/0/1

R1#
```

¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing? **show ip route ospf**

Paso 4: verificar la configuración del protocolo OSPF.

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

R1# **show ip protocols**

```
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
    192.168.12.2         110      00:03:33
    192.168.13.1         110      00:03:33
    192.168.23.2         110      00:03:33
  Distance: (default is 110)
```

Paso 5: verificar la información del proceso OSPF.

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

R1# **show ip ospf**

```
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 2 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x01ae41
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Paso 6: verificar la configuración de la interfaz OSPF.

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

R1# show ip ospf interface brief

La versión del Packet Tracer 7.0 no acepta el brief

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

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**

```
R1#show ip ospf interface

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 192.168.13.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  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 192.168.23.2
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 192.168.13.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  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 192.168.12.2
  Suppress hello for 0 neighbor(s)
R1#
```

Paso 7: Verificar la conectividad de extremo a extremo.

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

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

PC-A

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=5ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>
```

PC-C

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

```
Pinging 182.168.1.3 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Request timed out.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 182.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>
```

PC-B

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>192.168.1.3
Invalid Command.

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

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

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

C:\>
```

Parte 3. cambiar las asignaciones de ID del router

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

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

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

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

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

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

R1(config)# interface lo0

R1(config-if)# ip address 1.1.1.1 255.255.255.255

R1(config-if)# end

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int lo0

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

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

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

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#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int 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)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int 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)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

c. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.

```
R1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

```
R2#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R3#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

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

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

Readonly ROMMON initialized

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

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

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

Readonly ROMMON initialized

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

IOS Image Load Test

___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
##########################
```

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

Readonly ROMMON initialized

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

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

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**

```
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      00:13:58
    2.2.2.2              110      00:14:19
    3.3.3.3              110      00:13:58
    192.168.12.2         110      00:14:55
    192.168.13.1         110      00:16:41
    192.168.23.2         110      00:14:29
  Distance: (default is 110)
```

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

```
R1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:31    192.168.12.2    Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:34    192.168.13.2    Serial0/0/1
```

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

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

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

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

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

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

R1(config)# **end**

```
R1(config)#router ospf 1
R1(config-router)#router-id 11.11.11.11
R1(config-router)#Reload or use "clear ip ospf process" command,
for this to take effect


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

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.

```
R1#
00:26:20: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:26:20: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached

00:26:20: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:26:20: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R2#
00:26:40: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:26:40: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached

R2#
00:26:41: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from LOADING to FULL, Loading Done
```

```
R3#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R3#
00:27:04: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:27:04: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
```

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

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


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

R2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R2#
00:29:56: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:29:56: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
```

```
R3(config)#router ospf 1
R3(config-router)#router-id 33.33.33.33
R3(config-router)#Reload or use "clear ip ospf process" command,
for this to take effect


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

R3#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R3#
00:31:21: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:31:21: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
```

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

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 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      00:32:46
    2.2.2.2              110      00:06:53
    3.3.3.3              110      00:06:02
    11.11.11.11          110      00:01:43
    22.22.22.22          110      00:03:34
    33.33.33.33          110      00:01:43
    192.168.12.2         110      00:33:44
    192.168.13.1         110      00:35:30
    192.168.23.2         110      00:33:18
  Distance: (default is 110)
```

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
22.22.22.22       0   FULL/  -        00:00:35    192.168.12.2    Serial0/0/0
33.33.33.33       0   FULL/  -        00:00:37    192.168.13.2    Serial0/0/1
R1#
```

Parte 4: configurar las interfaces pasivas de OSPF

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

Paso 1: configurar una interfaz pasiva.

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

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

```
GigabitEthernet0/0 is up, line protocol is up
  Internet address 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 00:00:07
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

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

```
R1#show ip ospf int 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)
```

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**

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

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:12:04, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:10:12, 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, 00:10:12, Serial0/0/1

R1#
```

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

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

R1# **show ip ospf neighbor**

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       0   FULL/  -        00:00:37    192.168.12.2    Serial0/0/0
33.33.33.33       0   FULL/  -        00:00:39    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)#

```
R2(config)#router ospf 1
R2(config-router)#passive-interface default
R2(config-router)#
01:11:04: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
```

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

R1# **show ip ospf neighbor**

```
R1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:38    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**

```
R2#show ip ospf int 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 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)
```

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, 00:44:57, 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, 00:44:57, Serial0/0/1
```

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

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

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

R2(config-router)#

```
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#
01:21:42: %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
     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, 00:01:37, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:51:27, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.13.2, 00:51:27, Serial0/0/1
```

```
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, 00:59:57, Serial0/0/0
O    192.168.2.0/24 [110/129] via 192.168.13.1, 00:04:27, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:59:57, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
```

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

¿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? **Indica que no manda por esa interface paquetes Hello, el R2 tiene esa interface pasiva**

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

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

```
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/1
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, 01:11:14, Serial0/0/0
O    192.168.2.0/24 [110/129] via 192.168.13.1, 00:15:44, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 01:11:14, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1

R3#
```

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

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3 y cómo se calcula? **El costo es 65, esta se calcula de una link de 1.544 cuesta 64 mas 1 que es la gibatyte son 65 que es la metrica que da**

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

Parte 5 cambiar las métricas de OSPF

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

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

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

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

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

R1# **show interface g0/0**

```
R1#show int g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0002.173e.2101 (bia 0002.173e.2101)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 100 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
     242 packets output, 15488 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
```

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**

```
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 00:59:42, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 01:49:33, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 01:49:33, Serial0/0/1
```

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**

```
R1#show ip ospf int 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)
```

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**

```
R1#show ip ospf int 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 00:00:07
  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 33.33.33.33
  Suppress hello for 0 neighbor(s)
```

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

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

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

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

```
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.

```
R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across
all routers.
```

```
R3(config)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across
all routers.
```

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**

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

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

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**

```
R1#show ip ospf int 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: 6476
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  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 33.33.33.33
  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
O    192.168.2.0 [110/6576] via 192.168.12.2, 00:07:50, Serial0/0/0
O    192.168.3.0 [110/6576] via 192.168.13.2, 00:06:14, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/12952] via 192.168.13.2, 00:06:14, Serial0/0/1
```

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**

```
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?

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

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

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

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

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

```
R1#show int s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 57 bits/sec, 0 packets/sec
  5 minute output rate 59 bits/sec, 0 packets/sec
     1041 packets input, 72524 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
     1091 packets output, 76036 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
```

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**

```
R1#show ip route ospf
O    192.168.2.0 [110/164] via 192.168.12.2, 00:11:05, Serial0/0/0
O    192.168.3.0 [110/164] via 192.168.13.2, 00:11:05, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/6540] via 192.168.13.2, 00:11:05, Serial0/0/1
```

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

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

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

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

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

R1# **show ip route ospf**

```
R1#show ip route ospf
O    192.168.2.0 [110/881] via 192.168.12.2, 00:09:06,
Serial0/0/0
O    192.168.3.0 [110/164] via 192.168.13.2, 00:56:40,
Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/6540] via 192.168.13.2, 00:56:40,
Serial0/0/1
```

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

R1# **show ip ospf interface brief**

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

R1#show ip ospf int brief
```

El packet tracer 7.0 no acepta el comando

```
R1#show ip ospf int

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)
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  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 22.22.22.22
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 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 00:00:05
  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 33.33.33.33
  Suppress hello for 0 neighbor(s)
```

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

```
R1(config)#int s0/0/1
R1(config-if)#bandwidth 128
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

R1# **show ip route ospf**

```
R1#show ip route ospf
O    192.168.2.0 [110/881] via 192.168.12.2, 00:23:45, Serial0/0/0
O    192.168.3.0 [110/881] via 192.168.13.2, 00:03:41, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/7257] via 192.168.13.2, 00:03:41, Serial0/0/1
```

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

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

R3# **show ip route ospf**

```
R3#show ip route ospf
O    192.168.1.0 [110/6477] via 192.168.13.1, 01:14:24, Serial0/0/0
O    192.168.2.0 [110/7357] via 192.168.13.1, 00:26:51, Serial0/0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0 [110/7257] via 192.168.13.1, 00:26:51, Serial0/0/0
```

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

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

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

El costo acumulado es 1562. suma 781+781=1562

```
R1#show ip route ospf
O    192.168.2.0 [110/881] via 192.168.12.2, 00:32:03, Serial0/0/0
O    192.168.3.0 [110/881] via 192.168.13.2, 00:12:00, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/7257] via 192.168.13.2, 00:12:00, Serial0/0/1
```

Paso 3: cambiar el costo de la ruta.

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

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

R1# **show ip route ospf**

```
R1#show ip route ospf
O    192.168.2.0 [110/881] via 192.168.12.2, 00:32:03, Serial0/0/0
O    192.168.3.0 [110/881] via 192.168.13.2, 00:12:00, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/7257] via 192.168.13.2, 00:12:00, Serial0/0/1
```

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#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0/1
R1(config-if)#ip ospf cost 1565
R1(config-if)#
```

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**

```
R1#show ip route ospf
O    192.168.2.0 [110/881] via 192.168.12.2, 00:42:32, Serial0/0/0
O    192.168.3.0 [110/1665] via 192.168.13.2, 00:04:14, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/8041] via 192.168.13.2, 00:04:14, Serial0/0/1
```

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**. Por qué ahora el costo es mayor al ir por el serial s0/0/01, de 1565. Se va por el serial 0/0/0**

Reflexión

1. ¿Por qué es importante controlar la asignación de ID de router al utilizar el protocolo OSPF? **porque si no hay un nombre de router ID usa un look back más alta, sino hay usa la ip más alta dentro de sus interfaces activas, y si esta se desactiva cambia el nombre o ID del route, por lo tanto, va a ver problemas al elegir el DR y el BDR.**

2. ¿Por qué el proceso de elección de DR/BDR no es una preocupación en esta práctica de laboratorio? **por que la elección del router designado (DR) y del router designado de respaldo (BDR) se hace en redes ethernet y en este laboratorio estamos usando redes punto a punto y no hay problemas en elegir el DR o BDR.**

3. ¿Por qué querría configurar una interfaz OSPF como pasiva? **porque una interface pasiva me permite hacer que si no hay un route en esa interface no es necesario enviar paquetes hello por seguridad lo que ahorar recurso de red como ancho de banda, etc.**

Desarrollo Ejercicio 8.3.3.6

Práctica de laboratorio: configuración de OSPFv3 básico de área única

Topología

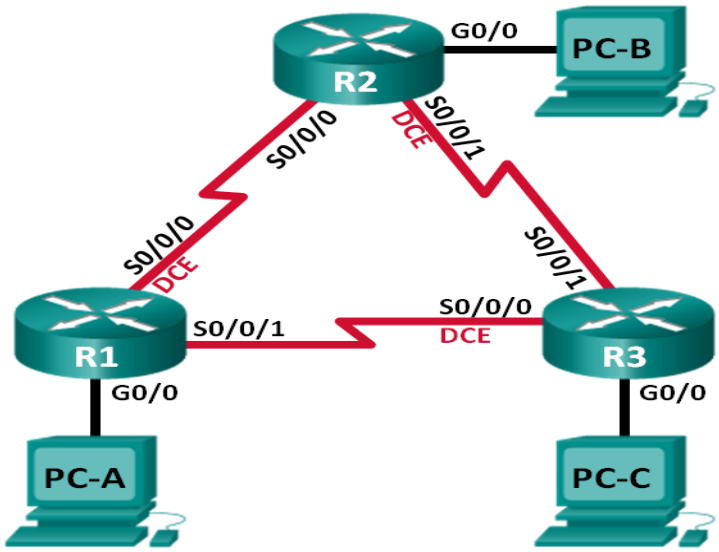


Tabla de direccionamiento

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

Información básica/situación

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

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

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

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

Recursos necesarios

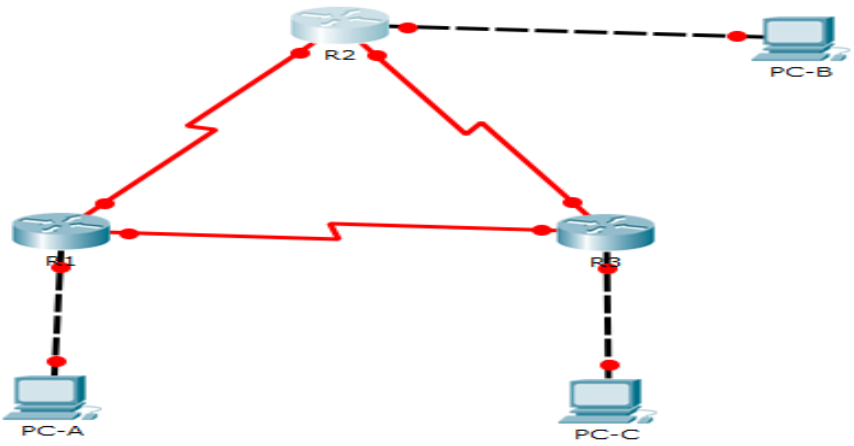
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet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

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

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

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

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



Paso 3: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

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

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

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

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

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

g. Cifre las contraseñas de texto no cifrado.

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

i. Habilite el routing de unidifusión IPv6 en cada router.

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

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#enable secret class
R1(config)#login
% Incomplete command.
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#banner motd #El acceso no autorizado esta prohibido#
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#enable secret class
R2(config)#login
% Incomplete command.
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#banner motd #El accceso no autorizado esta prohibido#
R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#service password-encryption
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

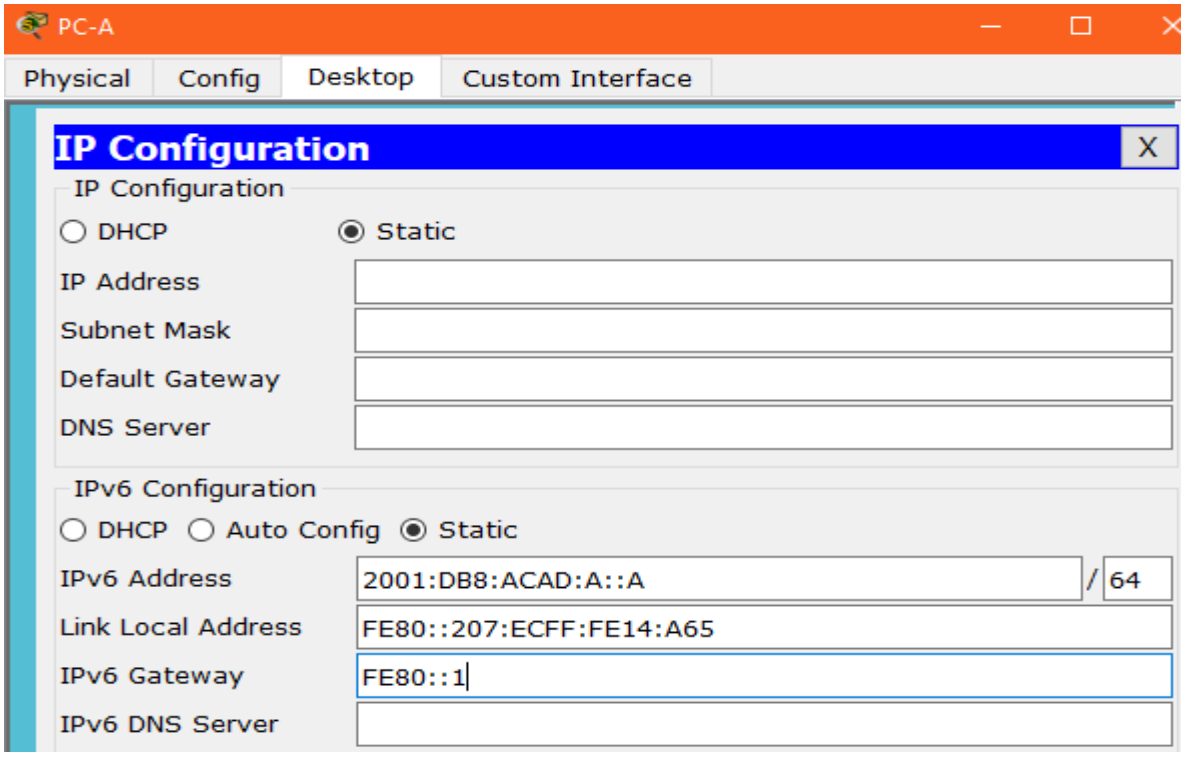
```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#no ip Domain-lookup
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#enable secret class
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#banner motd # El acceso no autorizado esta prohibido#
R3(config)#line console 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

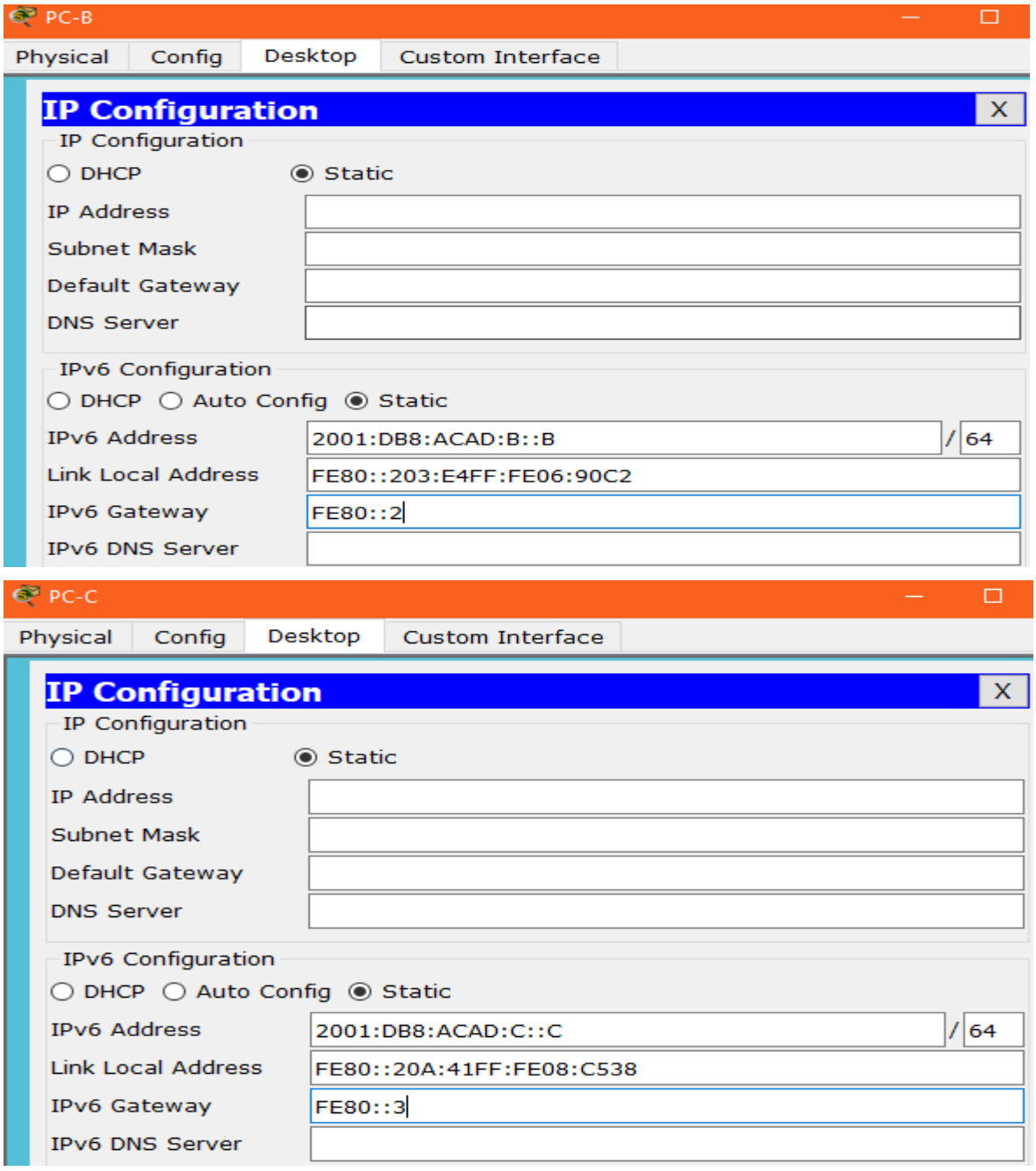
```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 LINK-LOCAL
R1(config-if)#int S0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 LINK-LOCAL
R1(config-if)#CLOCK RATE 128000
This command applies only to DCE interfaces
R1(config-if)#NO SHU

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#int g0/0
R1(config-if)#NO SHU

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

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

R1(config-if)#int S0/0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:13::1/64
R1(config-if)#ipv6 address FE80::1 LINK-LOCAL
R1(config-if)#NO SHU

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#EXIT
R1(config)#IPV6 UNICAST-ROUTING
R1(config)#END
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#COP R S
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

```
R2(config)#INT G0/0
R2(config-if)#IPV6 ADDRESS 2001:DB8:ACAD:B::2/64
R2(config-if)#IPV6 ADDRESS FE80::2 LINK-LOCAL
R2(config-if)#NO SHU

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

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

R2(config-if)#INT S0/0/0
R2(config-if)#IPV6 ADDRESS 2001:DB8:ACAD:12::2/64
R2(config-if)#IPV6 ADDRESS FE80::2 LINK-LOCAL
R2(config-if)#NO SHU

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

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

R2(config-if)#INT S0/0/1
R2(config-if)#IPV6 ADDRESS 2001:DB8:ACAD:23::2/64
R2(config-if)#IPV6 ADDRESS FE80::2 LINK-LOCAL
R2(config-if)#CLOCK RATE 128000
This command applies only to DCE interfaces
R2(config-if)#NO SHU

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#EXIT
R2(config)#IPV6 UNICAST-ROUTING
R2(config)#EXIT
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#COP R S
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R3(config-if)#int S0/0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:13::3/64
R3(config-if)#IPV6 ADDRESS FE80::3 LINK-LOCAL
R3(config-if)#CLOCK RATE 128000
R3(config-if)#NO SHU

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

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

R3(config-if)#int S0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#IPV6 ADDRESS FE80::3 LINK-LOCAL
R3(config-if)#NO SHU

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

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3(config-if)#EXIT
R3(config)#IPV6 UNICAST-ROUTING
R3(config)#EXIT
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#COP R S
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

PASO 4: configurar los equipos host.

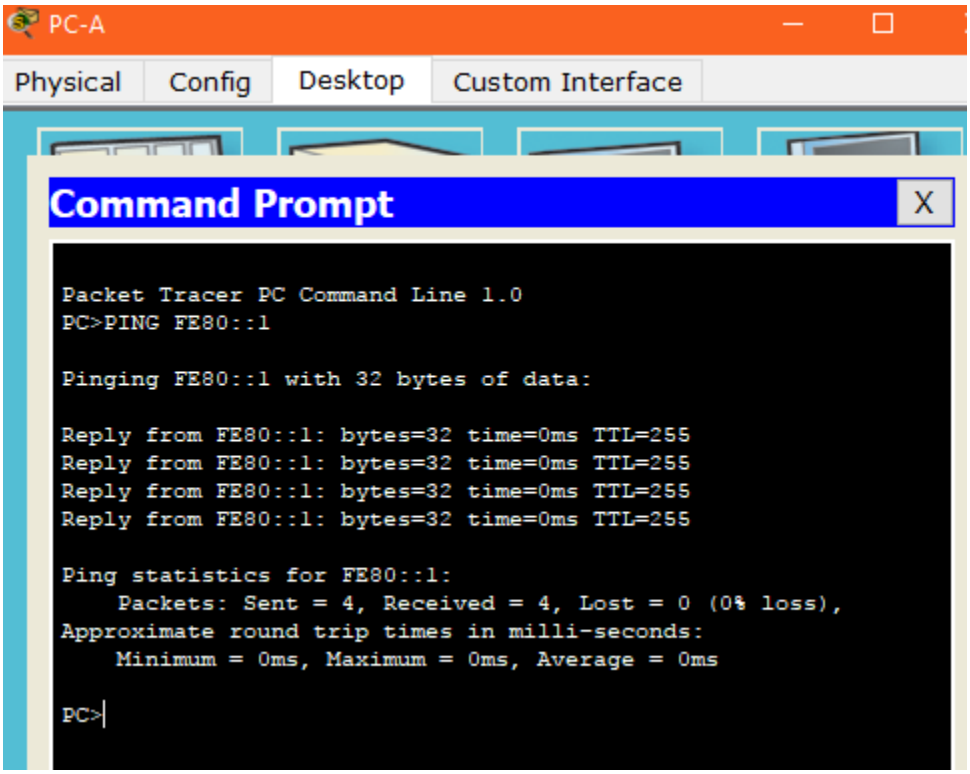


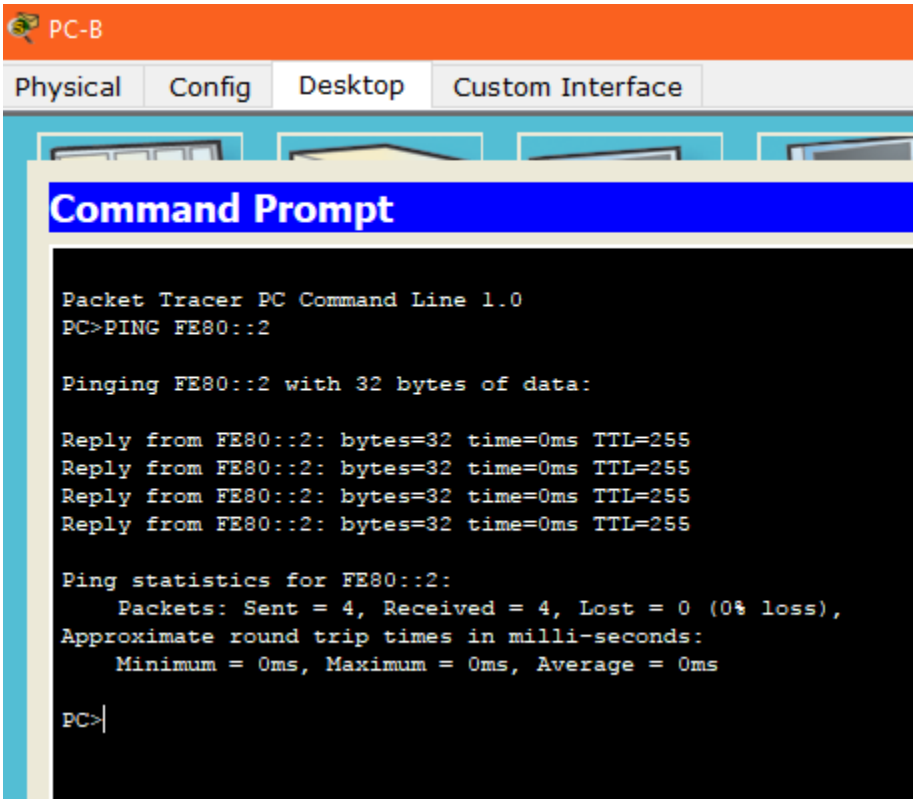


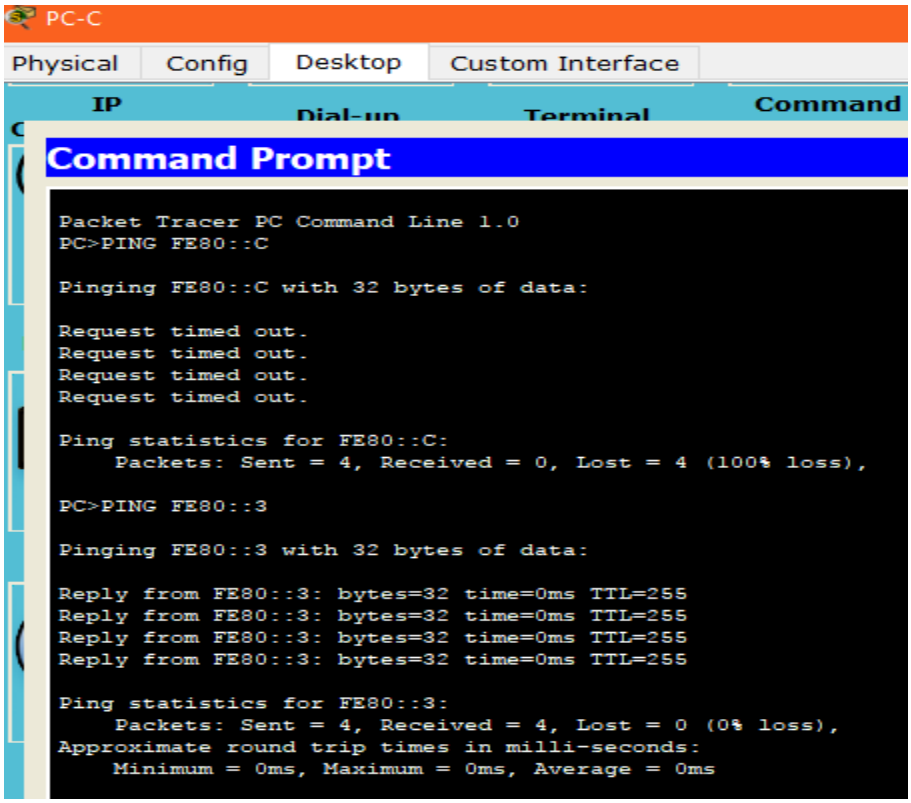
Paso 5. Probar la conectividad.

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

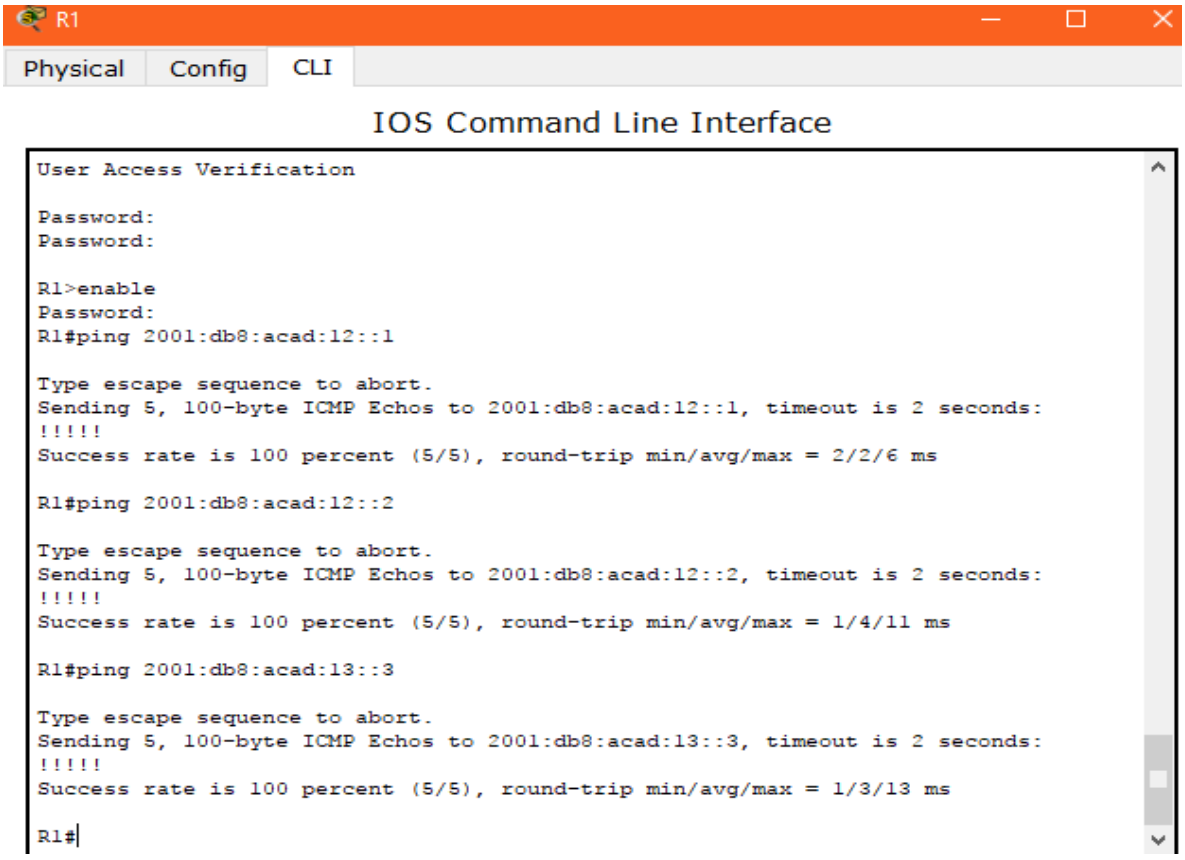
Ping de los pc a su respectivo Gateway exitosos


PC-A
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>PING FE80::1
Pinging FE80::1 with 32 bytes of data:
Reply from FE80::1: bytes=32 time=0ms TTL=255
Reply from FE80::1: bytes=32 time=0ms TTL=255
Reply from FE80::1: bytes=32 time=0ms TTL=255
Reply from FE80::1: bytes=32 time=0ms TTL=255
Ping statistics for FE80::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>


PC-B
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>PING FE80::2
Pinging FE80::2 with 32 bytes of data:
Reply from FE80::2: bytes=32 time=0ms TTL=255
Reply from FE80::2: bytes=32 time=0ms TTL=255
Reply from FE80::2: bytes=32 time=0ms TTL=255
Reply from FE80::2: bytes=32 time=0ms TTL=255
Ping statistics for FE80::2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>



Ping del R1 al R2 y R3 son exitosos



Parte 2. configurar el routing OSPFv3

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

Paso 1. asignar ID a los routers.
OSPFv3 sigue utilizando una dirección de 32 bits para la ID del router. Debido a que no hay direcciones IPv4 configuradas en los routers, asigne manualmente la ID del router mediante el comando **router-id**.

a. Emita el comando **ipv6 router ospf** para iniciar un proceso OSPFv3 en el router.
R1(config)# **ipv6 router ospf 1**

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**

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

d. Emita el comando **show ipv6 ospf** para verificar las ID de router de todos los routers.
R2# **show ipv6 ospf**

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure
manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ipv6 ospf
 Routing Process "ospfv3 1" with ID 1.1.1.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 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
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure
manually
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#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 msecs
 Retransmission pacing timer 66 msecs
 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#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure
manually
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ipv4 ospf
          ^
% Invalid input detected at '^' marker.

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 msecs
 Retransmission pacing timer 66 msecs
 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
```

Paso 2. configurar OSPFv6 en el R1.

Con IPv6, es común tener varias direcciones IPv6 configuradas en una interfaz. La instrucción network se eliminó en OSPFv3. En cambio, el routing OSPFv3 se habilita en el nivel de la interfaz.
a. Emita el comando **ipv6 ospf 1 area 0** para cada interfaz en el R1 que participará en el routing OSPFv3.

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

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

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

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

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.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
01:21:32: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

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

```
R3#con t
% Ambiguous command: "con t"
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
01:23:49: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to
FULL, Loading Done

R3(config-if)#
01:23:50: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
```

Paso 3. verificar vecinos de OSPFv3.

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

R1# **show ipv6 ospf neighbor**

```
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:34    3               Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:35    3               Serial0/0/1
R1#
```

Paso 4. verificar la configuración del protocolo OSPFv3.

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

R1# **show ipv6 protocols**

```
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
```

Paso 5. verificar las interfaces OSPFv3.

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

R1# **show ipv6 ospf interface**

```
R1#show ipv6 ospf int
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  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 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 4
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  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
```

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**

EL packet tracer no acepta el comando.

```
R1#show ipv6 ospf int brief
                        ^
% Invalid input detected at '^' marker.

R1#
```

Paso 6. verificar la tabla de routing IPv6.

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

R2# **show ipv6 route**

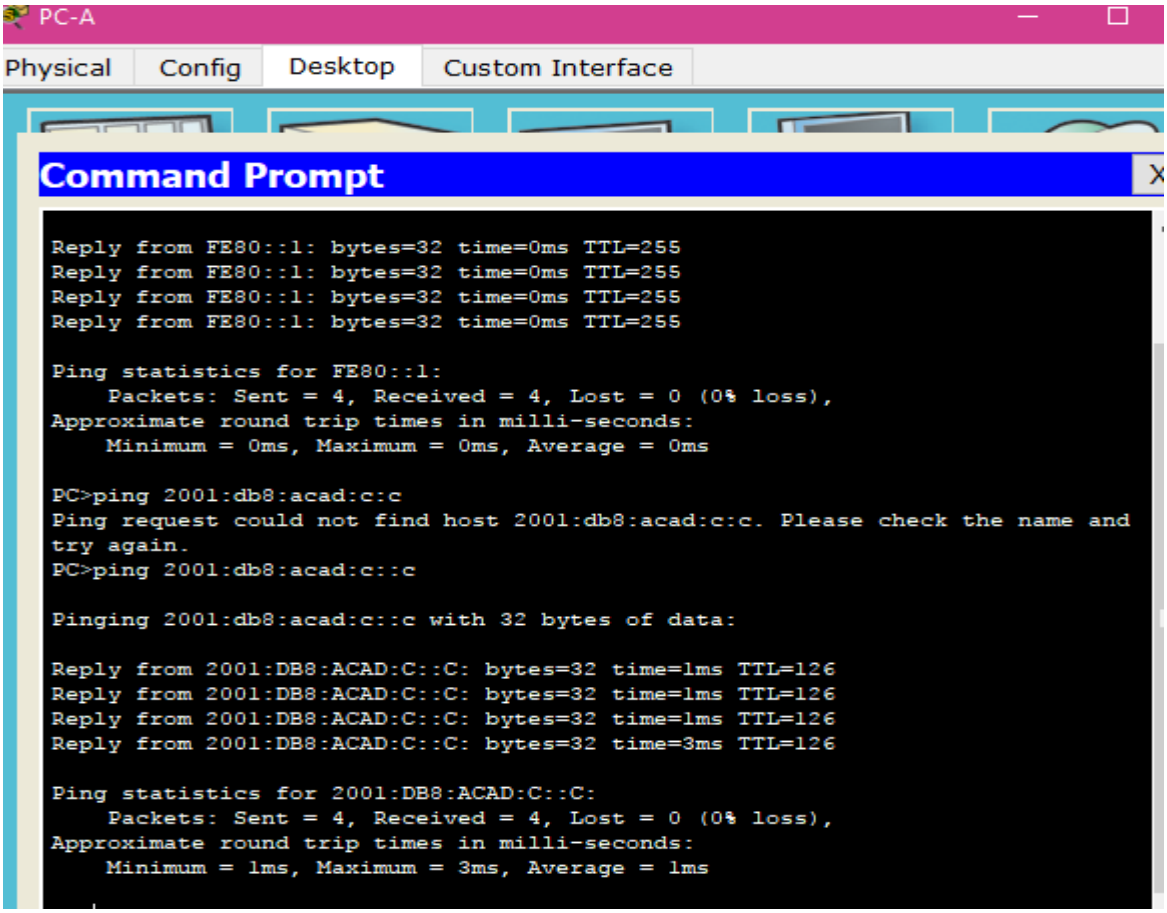
```
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - 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, receive
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, receive
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::1, Serial0/0/0, receive
     via FE80::3, Serial0/0/1, receive
C   2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

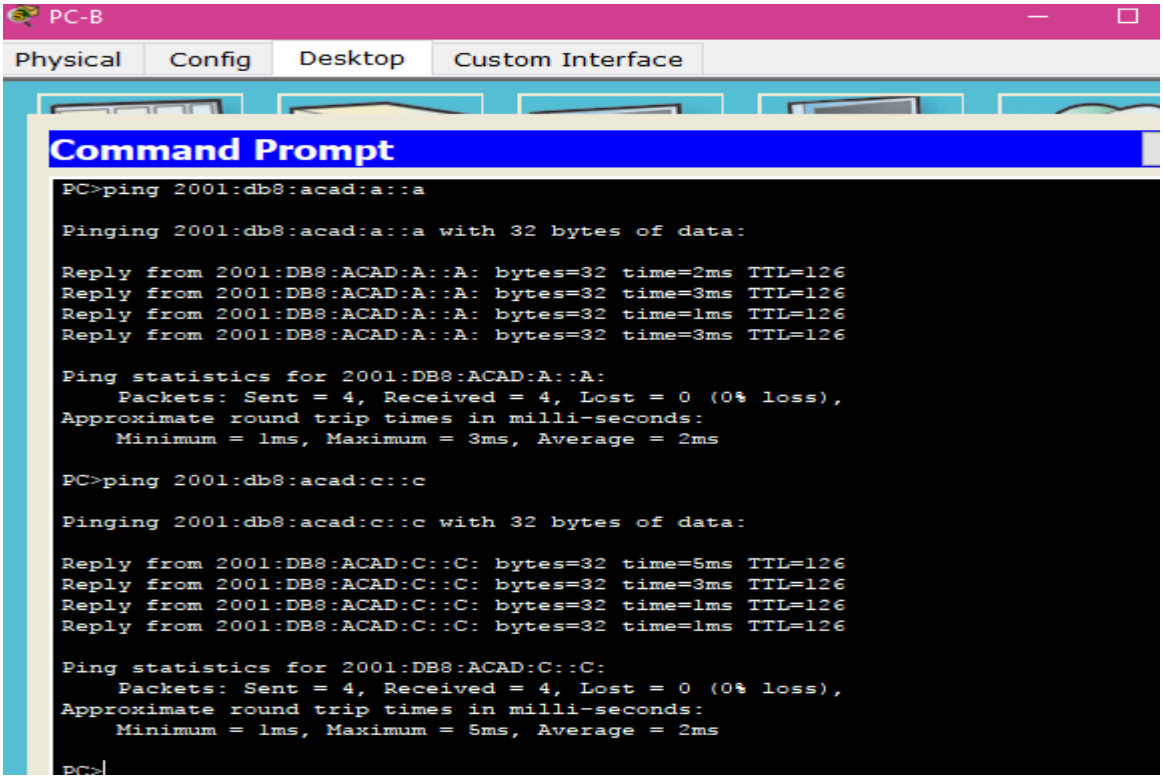
¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing? **show ipv6 ospf**

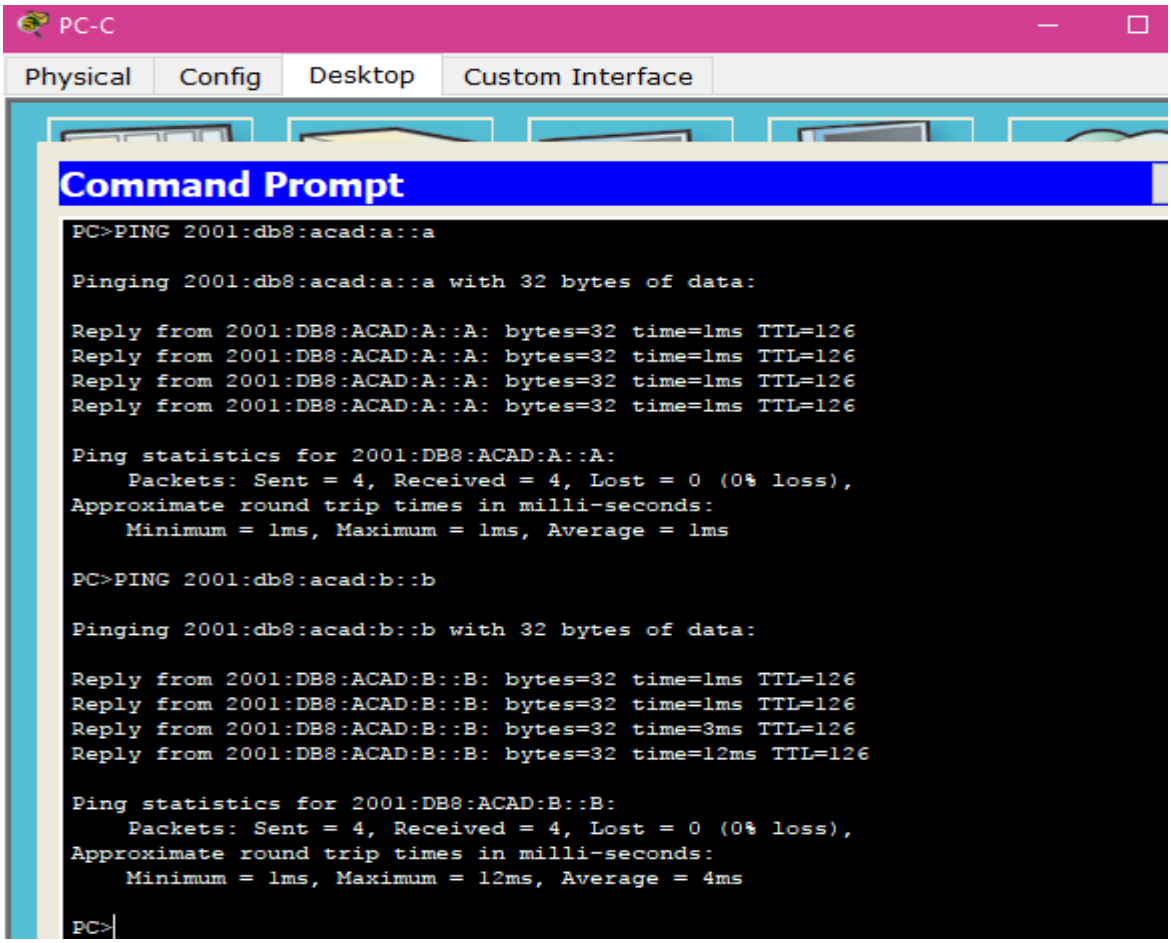
Paso 7. Verificar la conectividad de extremo a extremo.

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

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


PC-A
Physical
Config
Desktop
Custom Interface
Command Prompt
Reply from FE80::1: bytes=32 time=0ms TTL=255
Reply from FE80::1: bytes=32 time=0ms TTL=255
Reply from FE80::1: bytes=32 time=0ms TTL=255
Reply from FE80::1: bytes=32 time=0ms TTL=255
Ping statistics for FE80::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 2001:db8:acad:c:c
Ping request could not find host 2001:db8:acad:c:c. Please check the name and try again.
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=1ms 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=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 = 3ms, Average = 1ms


PC-B
Physical
Config
Desktop
Custom Interface
Command Prompt
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=2ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=3ms TTL=126
Ping statistics for 2001:DB8:ACAD:A::A:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 2ms
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=5ms 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=1ms 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 = 5ms, Average = 2ms
PC>



Parte 8. configurar las interfaces pasivas de OSPFv3

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

Paso 1. configurar una interfaz pasiva.

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

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

```
R1#show ipv6 ospf int g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  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)
```

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#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtr)#passive-int g0/0
R1(config-rtr)#
```

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

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

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

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

R2# **show ipv6 route ospf**

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

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

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

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

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

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-inter default
R2(config-rtr)#
02:12:36: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Interface down or detached
```

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

R1# **show ipv6 ospf neighbor**

```
R1#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           0   FULL/  -        00:00:37    3               Serial0/0/1
R1#
```

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

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

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

```
R1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       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, directly connected
L   2001:DB8:ACAD:A::1/128 [0/0]
     via GigabitEthernet0/0, receive
O   2001:DB8:ACAD:C::/64 [110/65]
     via FE80::3, Serial0/0/1, receive
C   2001:DB8:ACAD:12::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::1/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:ACAD:13::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:13::1/128 [0/0]
     via Serial0/0/1, receive
O   2001:DB8:ACAD:23::/64 [110/128]
     via FE80::3, Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
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, receive
C   2001:DB8:ACAD:C::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:C::3/128 [0/0]
     via GigabitEthernet0/0, receive
O   2001:DB8:ACAD:12::/64 [110/128]
     via FE80::1, Serial0/0/0, receive
C   2001:DB8:ACAD:13::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:13::3/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::3/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

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

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

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-int s0/0/1
R2(config-rtr)#
```

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

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

```
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, receive
O   2001:DB8:ACAD:B::/64 [110/65]
     via FE80::2, Serial0/0/1, receive
C   2001:DB8:ACAD:C::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:C::3/128 [0/0]
     via GigabitEthernet0/0, receive
O   2001:DB8:ACAD:12::/64 [110/128]
     via FE80::1, Serial0/0/0, receive
     via FE80::2, Serial0/0/1, receive
C   2001:DB8:ACAD:13::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:13::3/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::3/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

```
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:30    3               Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:31    3               Serial0/0/1
R1#
```

```
R3#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
1.1.1.1           0   FULL/  -        00:00:37    4               Serial0/0/0
2.2.2.2           0   FULL/  -        00:00:36    4               Serial0/0/1
R3#
```

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64? **Serial 0/0/1**

¿Cuál es la métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1? **65**
¿El R2 aparece como vecino OSPFv3 en el R1? **Si**

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

¿Qué indica esta información?

Todo el tráfico de la red desde R1 será enrutador a través de R3 y el R2. Cuando La interfaz 0 de R2 está configurada como pasiva OSPFv3 no manda ruteo a través de esta interfaz

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

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:30    3               Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:31    3               Serial0/0/1
R1#
```

Reflexión

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

Si, por que el proceso de OSPF es solo usado y afecta localmente en un route y necesita conseguir el reproceso usado en otro route, la misma variable no tiene que coincidir.

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

Eliminando el comando network en OSPFv3 ayuda a prevenir los errores en las direcciones IPV6.

DESARROLLO EJERCICIO 9.2.1.10

Packet Tracer - Configuración de ACL estándar

Topología

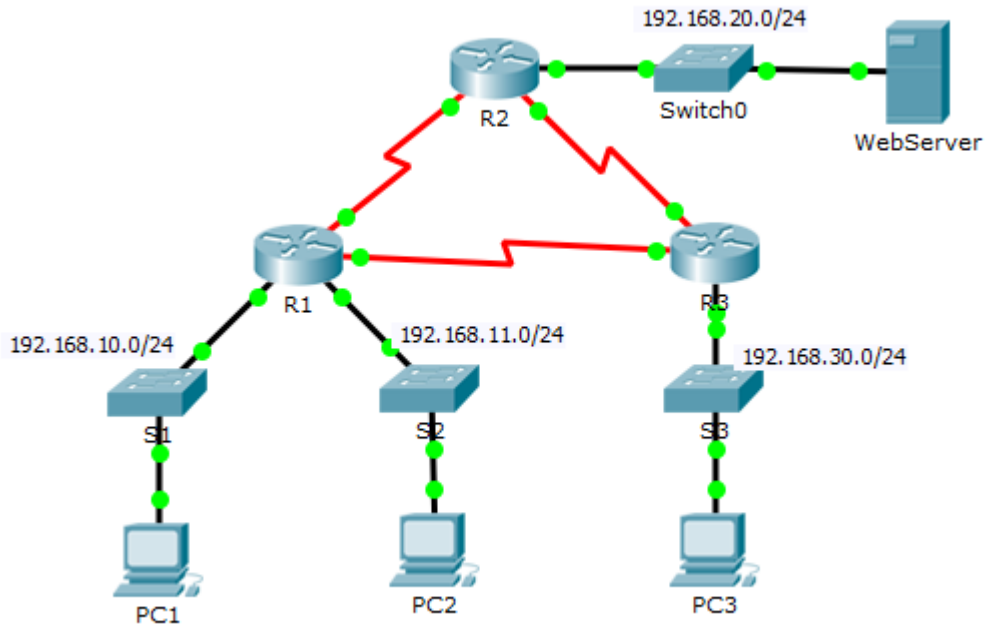


Tabla de direccionamiento

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

Objetivos

Parte 1: planificar una implementación de ACL
Parte 2: configurar, aplicar y verificar una ACL estándar

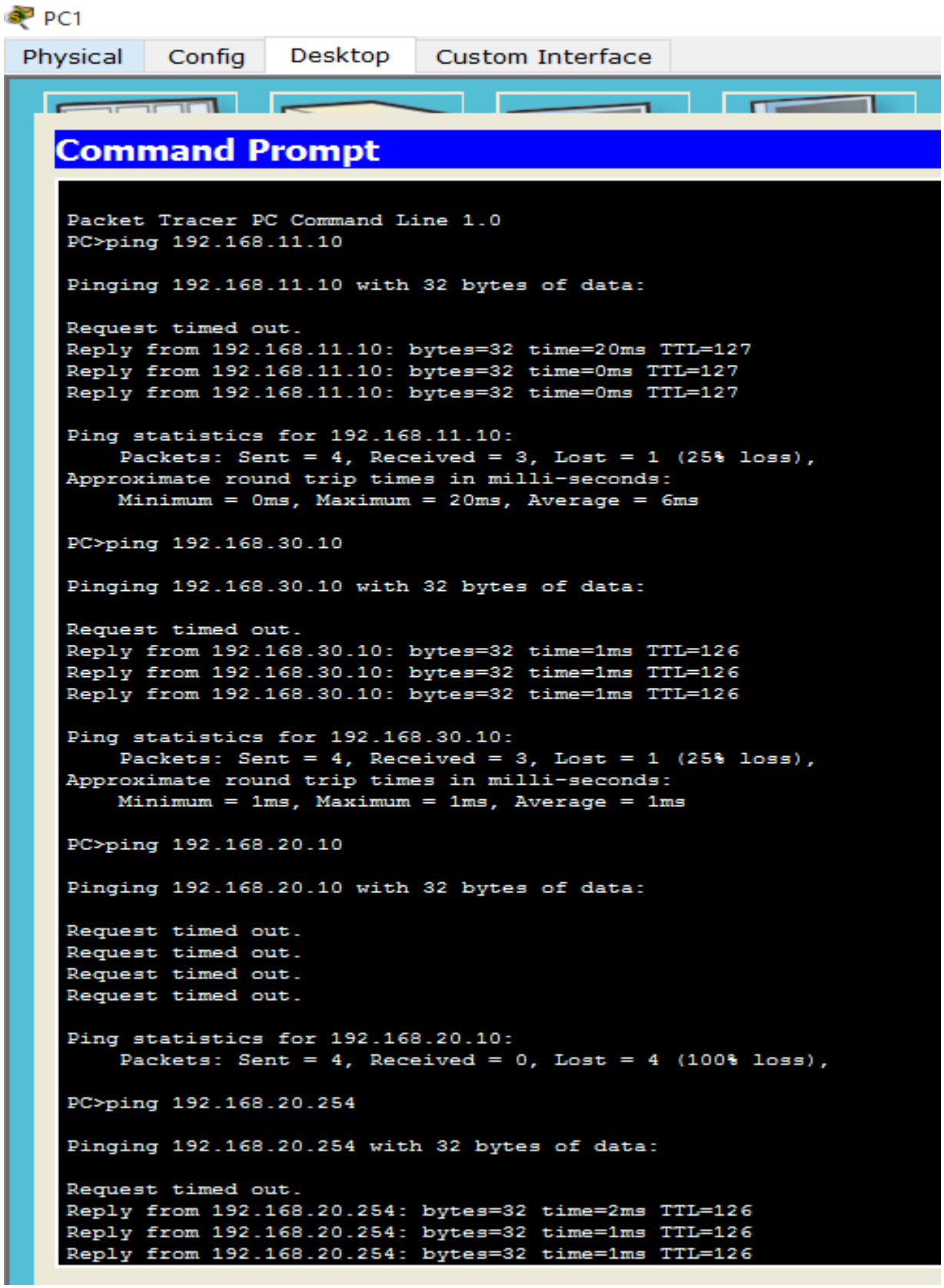
Antecedentes / escenario

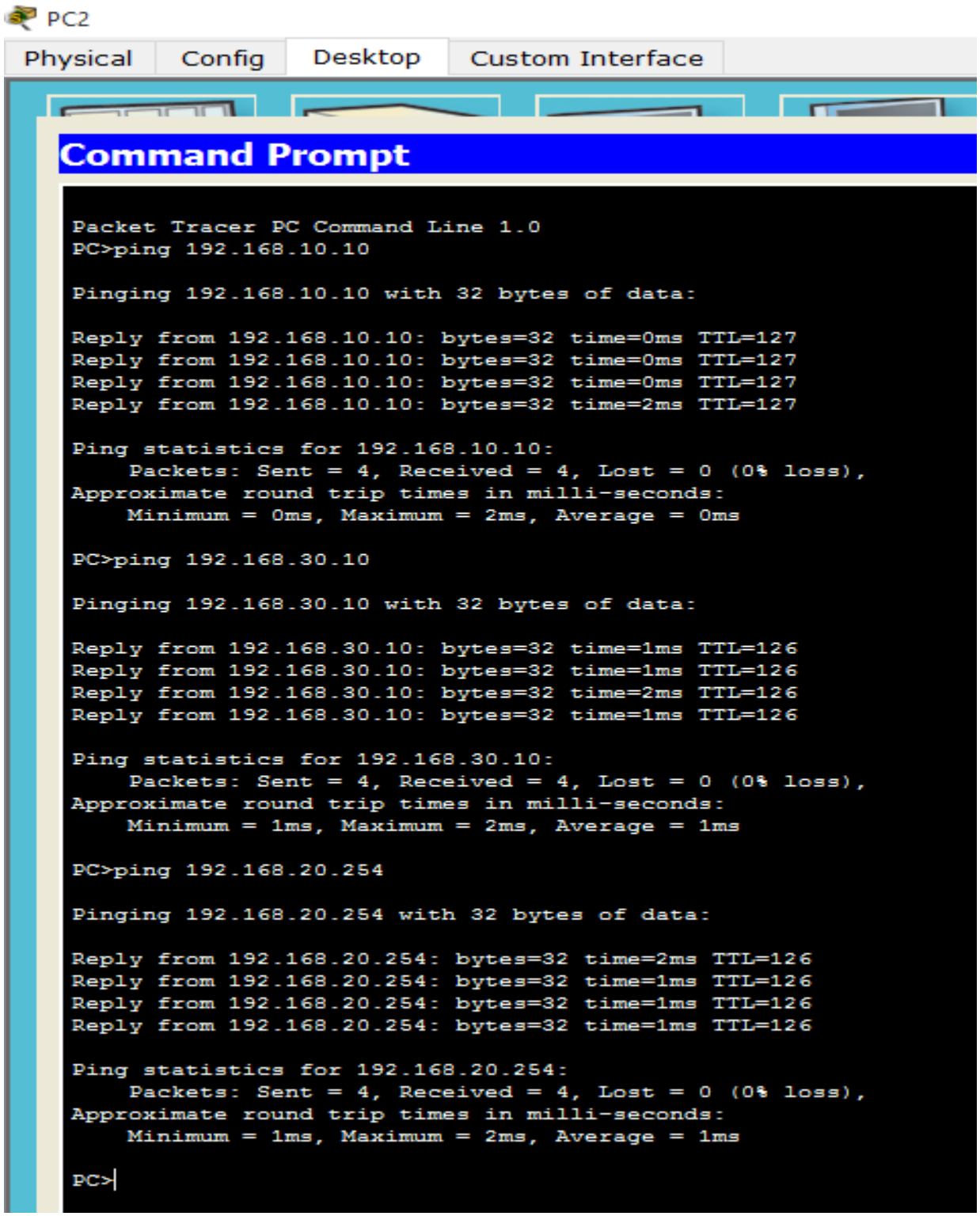
Las listas de control de acceso (ACL) estándar son secuencias de comandos de configuración del enrutador que controlan si un enrutador permite o niega paquetes según la dirección de origen. Esta actividad se enfoca en definir el filtrado criterios, configurar ACL estándar, aplicar ACL a las interfaces del enrutador y verificar y probando la implementación de ACL. Los enrutadores ya están configurados, incluidas las direcciones IP y Enrutamiento del protocolo de enrutamiento de puerta de enlace interior mejorado (EIGRP).

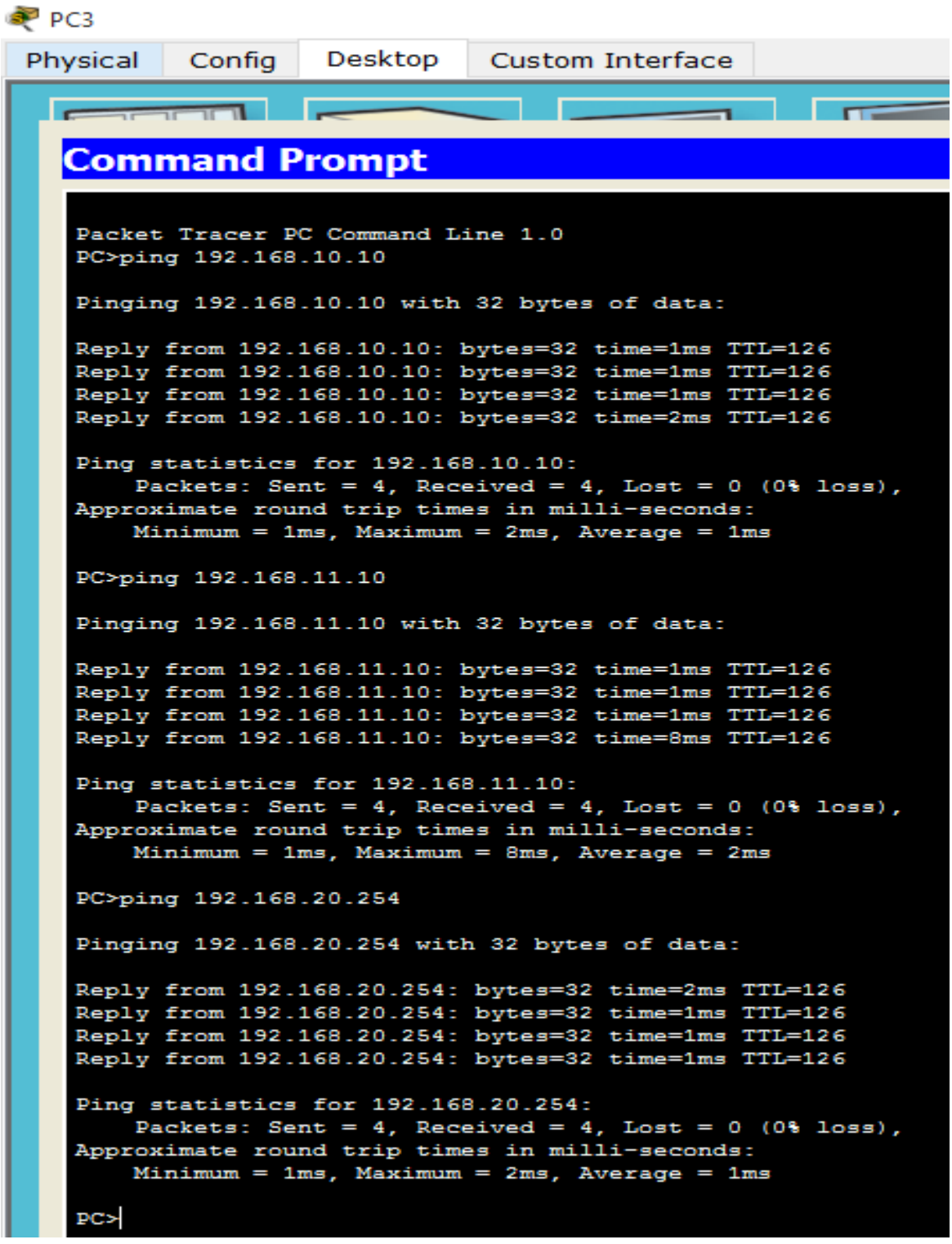
Parte 1: planificar una implementación de ACL

Paso 1: investigue la configuración de red actual.

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


PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>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=20ms TTL=127
Reply from 192.168.11.10: bytes=32 time=0ms TTL=127
Reply from 192.168.11.10: bytes=32 time=0ms 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 = 20ms, Average = 6ms
PC>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=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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
PC>ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.20.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.20.254
Pinging 192.168.20.254 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.254: bytes=32 time=2ms 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


PC2
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time=0ms TTL=127
Reply from 192.168.10.10: bytes=32 time=0ms TTL=127
Reply from 192.168.10.10: bytes=32 time=0ms TTL=127
Reply from 192.168.10.10: bytes=32 time=2ms TTL=127
Ping statistics for 192.168.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
PC>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=2ms 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 = 2ms, Average = 1ms
PC>ping 192.168.20.254
Pinging 192.168.20.254 with 32 bytes of data:
Reply from 192.168.20.254: bytes=32 time=2ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.20.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>



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

a. Las siguientes políticas de red se implementan en R2:

- La red 192.168.11.0/24 no tiene acceso permitido al WebServer en laRed 192.168.20.0/24.

- El resto del acceso está permitido.

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

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

La red 192.168.10.0/24 no puede comunicarse con la red 192.168.30.0/24.
El resto del acceso está permitido.

Para restringir el acceso de la red 192.168.10.0/24 a la red 192.168.30 / 24 sin interferir con otro tráfico, se deberá crear una lista de acceso en R3. El ACL debe colocarse en la interfaz de salida para PC3. Se debe crear una segunda regla en R3 para permitir que todos los demás tráficos.

Parte 2: configurar, aplicar y verificar una ACL estándar

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

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

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

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

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

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

R2(config)# **interface GigabitEthernet0/0**
R2(config-if)# **ip access-group 1 out**

```
R2#confi 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)#
```

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

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

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

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

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

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

R3(config)# **interface GigabitEthernet0/0**
R3(config-if)# **ip access-group 1 out**

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#int g0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
```

Paso 3: Verificar la configuración y funcionalidad de ACL.

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

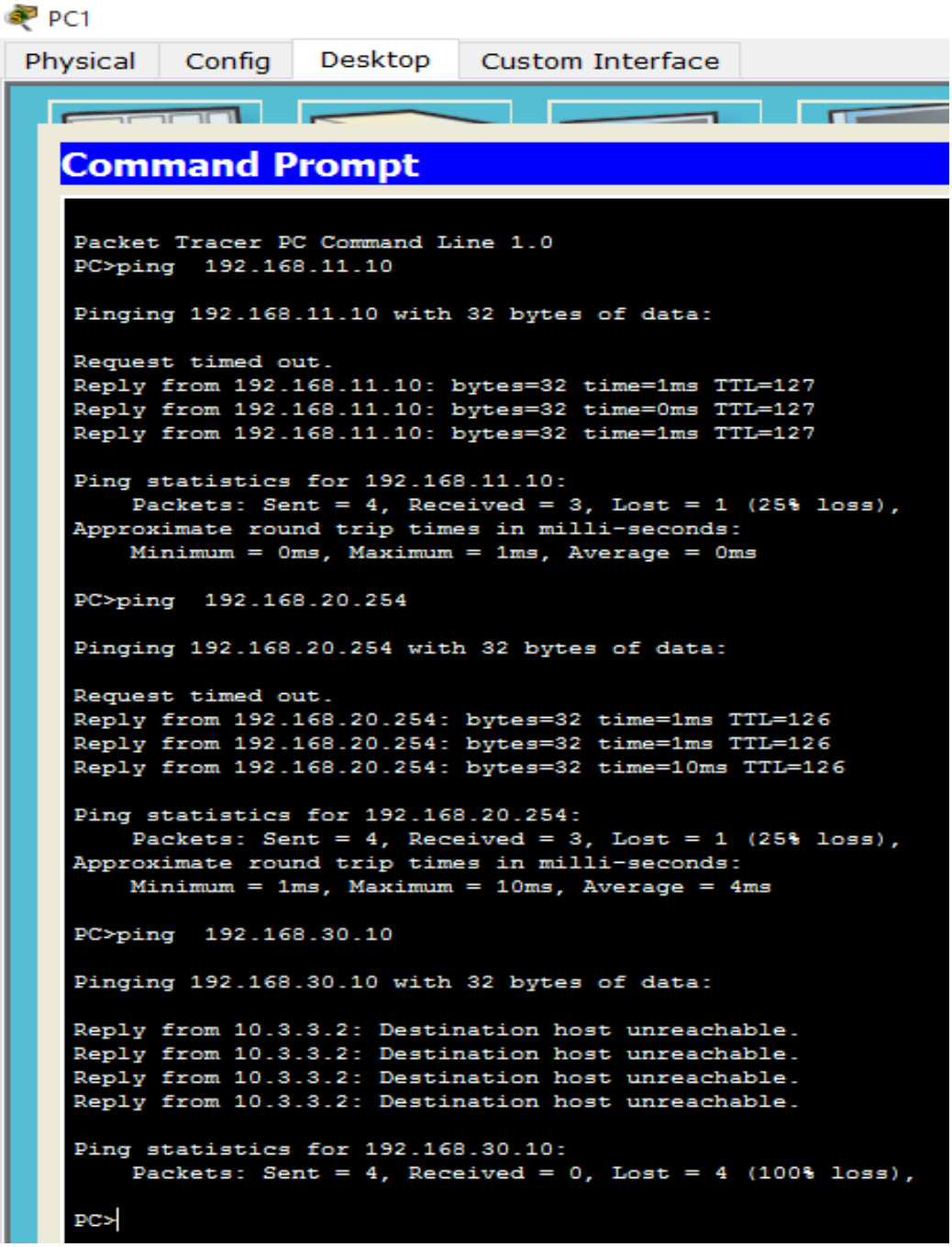
```
R2#show access-list
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255
    20 permit any
R2#
```

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

b. Con las dos ACL en su lugar, el tráfico de red está restringido según las políticas detalladas en Parte

1. Use las siguientes pruebas para verificar las implementaciones de ACL:

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



PC2

Physical | Config | Desktop | Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 1923.168.20.254
Ping request could not find host 1923.168.20.254. Please check the name and try again.
PC>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

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

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

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

PC>
```

PC3

Physical | Config | Desktop | Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

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

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>ping 192.168.20.254
```

DESARROLLO EJERCICIO 9.2.1.11

Packet Tracer: configuración de las ACL estándar designadas

Topología

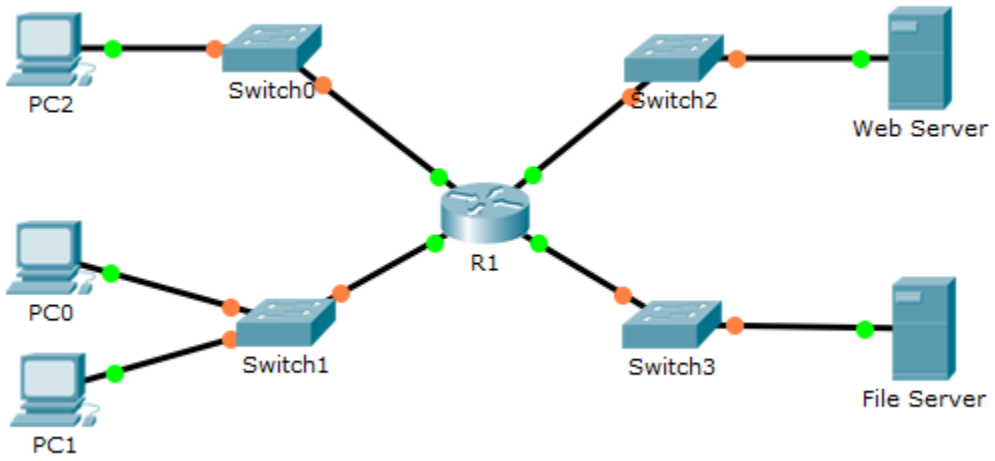


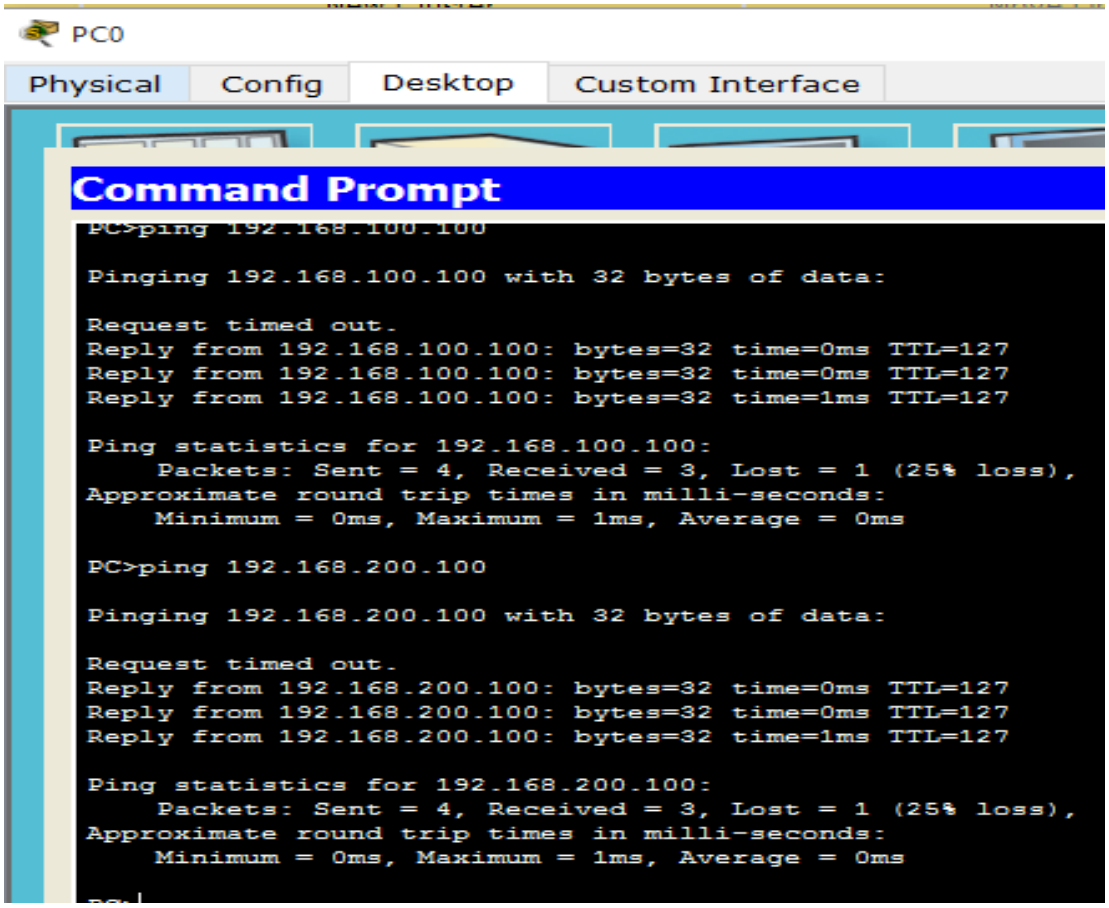
Tabla de direccionamiento

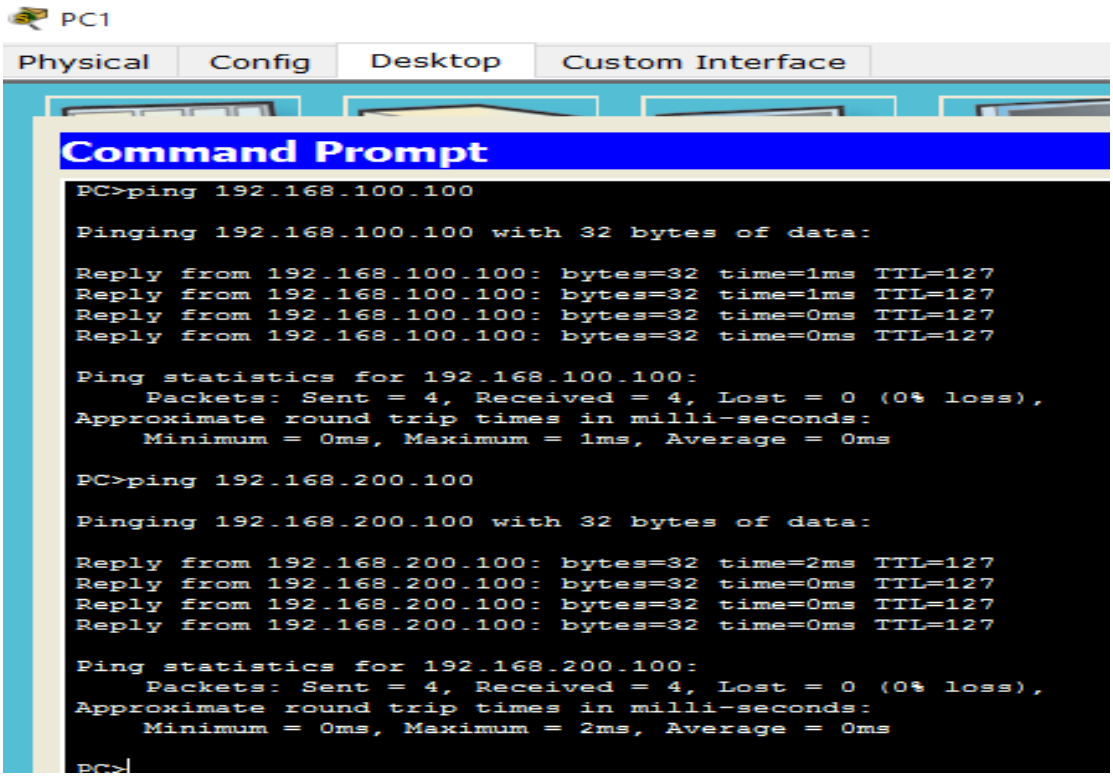
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

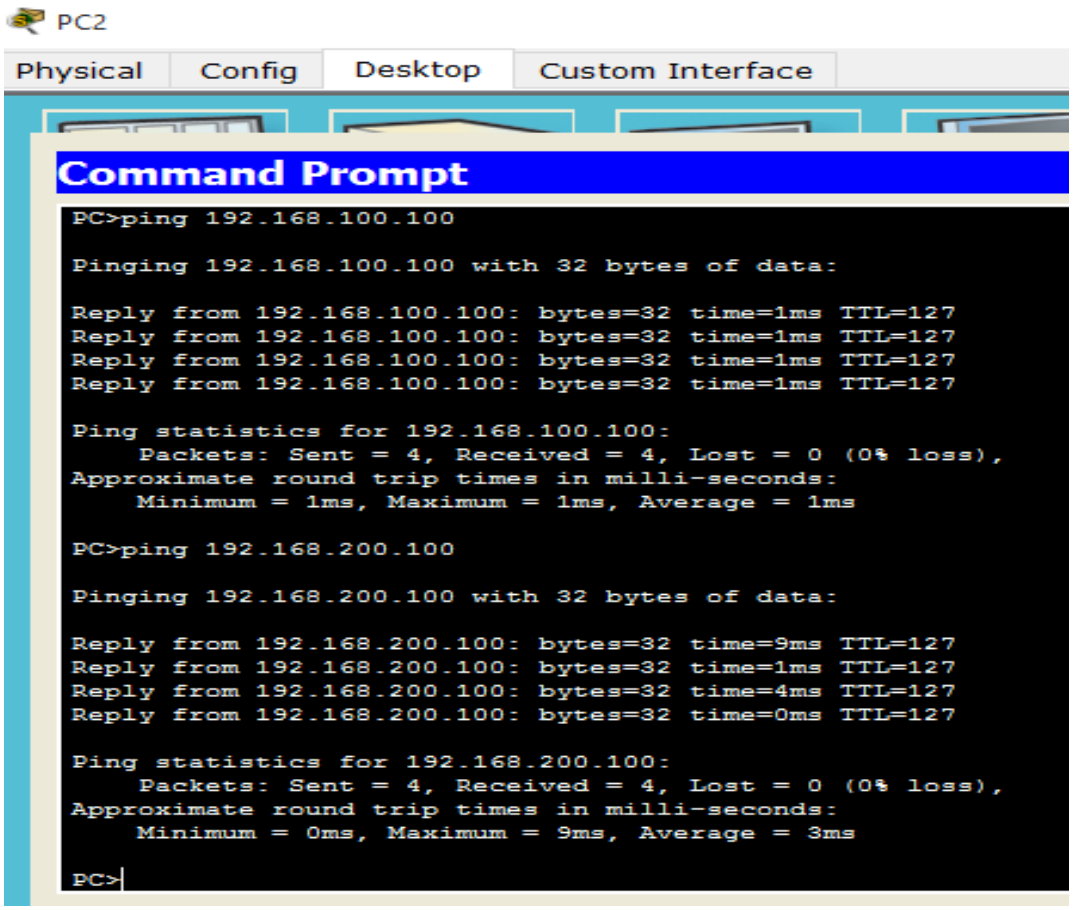
Parte 1: configurar y aplicar una ACL estándar designada

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

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


PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
PC>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.100.100: bytes=32 time=0ms 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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms


PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
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=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
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=2ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms 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 = 2ms, Average = 0ms



Paso 2: configure una ACL estándar nombrada.

Configure la siguiente ACL nombrada en R1.

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

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#deny any
R1(config-std-nacl)#
```

Paso 3: aplique la ACL nombrada.

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

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

b. Guarde la configuración**.**

```
R1(config)#interface FastEthernet 0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#
```

Parte 2: Verificar la implementación de ACL

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

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

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

```
R1# show ip int f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.200.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is File_Server-Restrictions
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables 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
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R1#
```

Paso 2: Verifique que la ACL esté funcionando correctamente.

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

- PC0, se conecta a un Servidor Web, pero sin establecer conexión a File Server (ok)

PC0

Physical | Config | Desktop | Custom Interface

Command Prompt

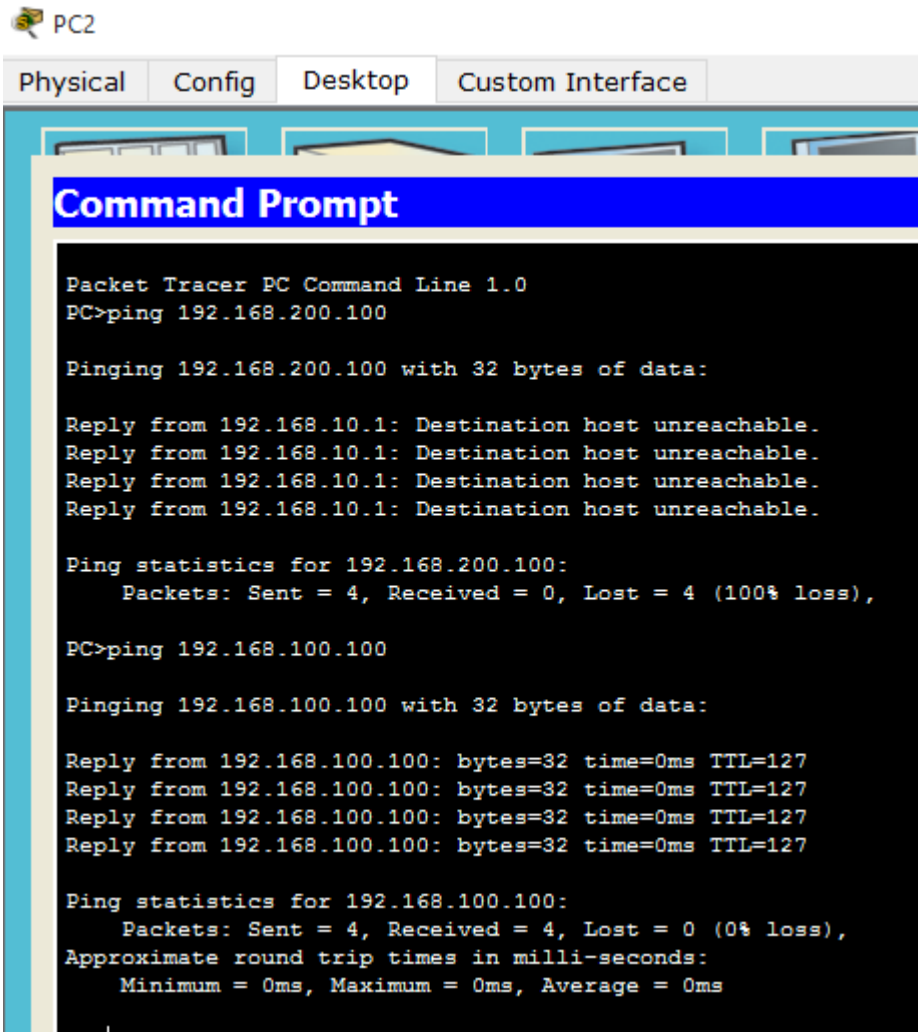
```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

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

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

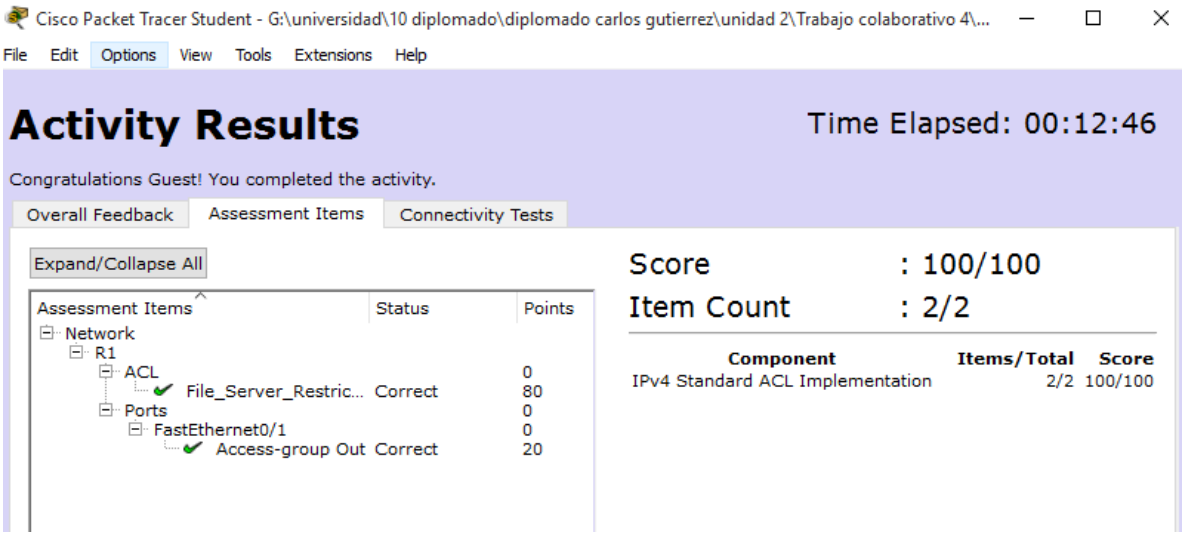
PC1

Physical | Config | Desktop | Custom Interface

Command Prompt

```
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=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms 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

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 = 10ms, Average = 2ms

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```


PC2
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.200.100
Pinging 192.168.200.100 with 32 bytes of data:
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Ping statistics for 192.168.200.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms


Cisco Packet Tracer Student - G:\universidad\10 diplomado\diplomado carlos gutierrez\unidad 2\Trabajo colaborativo 4\...
File
Edit
Options
View
Tools
Extensions
Help
Activity Results
Time Elapsed: 00:12:46
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Network
R1
ACL
0
File_Server_Restric...
Correct
80
Ports
0
FastEthernet0/1
0
Access-group Out
Correct
20
Score
: 100/100
Item Count
: 2/2
Component
Items/Total
Score
IPv4 Standard ACL Implementation
2/2
100/100

DESARROLLO EJERCICIO 9.2.3.3

Packet Tracer - Configuración de una ACL en líneas VTY Instrucciones IG

Topología

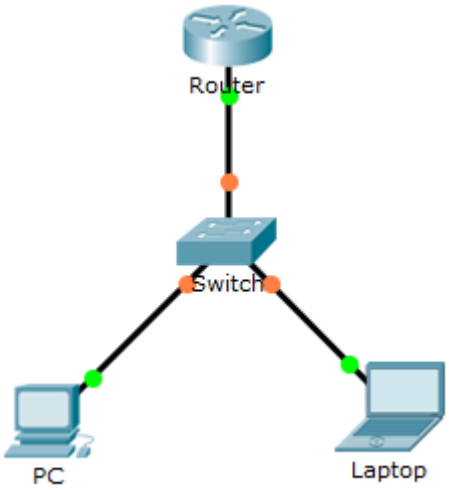


Tabla de direccionamiento

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

Objetivos

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

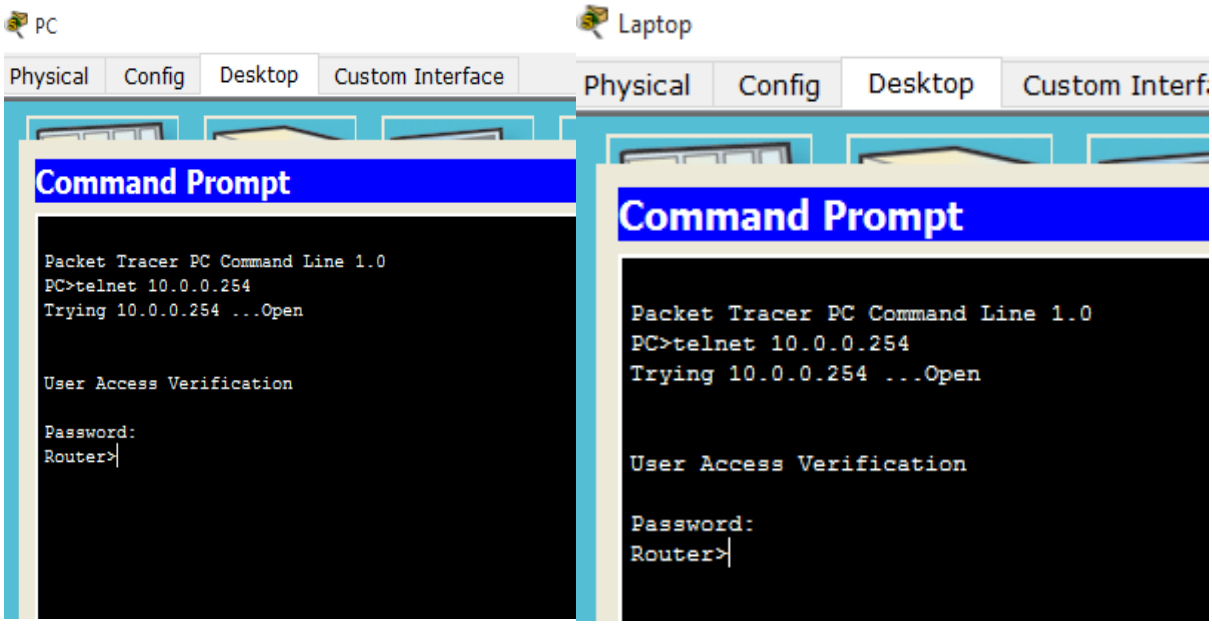
Situación

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

Parte 1: configurar y aplicar una ACL a líneas VTY

Paso 1: Verifique el acceso de Telnet antes de que se configure la ACL.

Ambas computadoras deberían poder Telnet al Enrutador. La contraseña es Cisco.



Paso 2: configure una ACL estándar numerada.

Configure la siguiente ACL numerada en el router.

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

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

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

Se debe permitir el acceso a las interfaces del enrutador, mientras que el acceso a Telnet debe estar restringido. Por lo tanto, debemos colocar la ACL en las líneas Telnet 0 a 4. Desde el indicador de configuración de Router, ingrese line configuración modo para las líneas 0 - 4 y use el comando access-class para aplicar la ACL a todas las líneas VTY

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

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#
```

Parte 2: Verificar la implementación de ACL

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

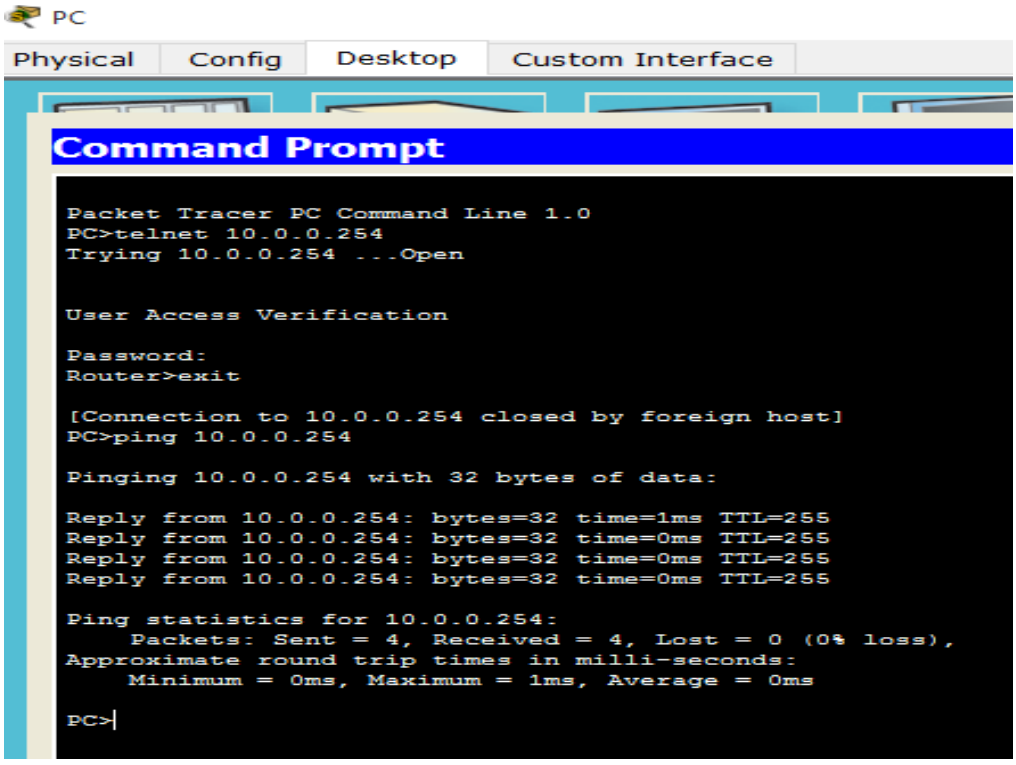
Use las listas de acceso del programa para verificar la configuración de ACL. Use el comando show run para verificar el ACL es aplicado a las líneas VTY.

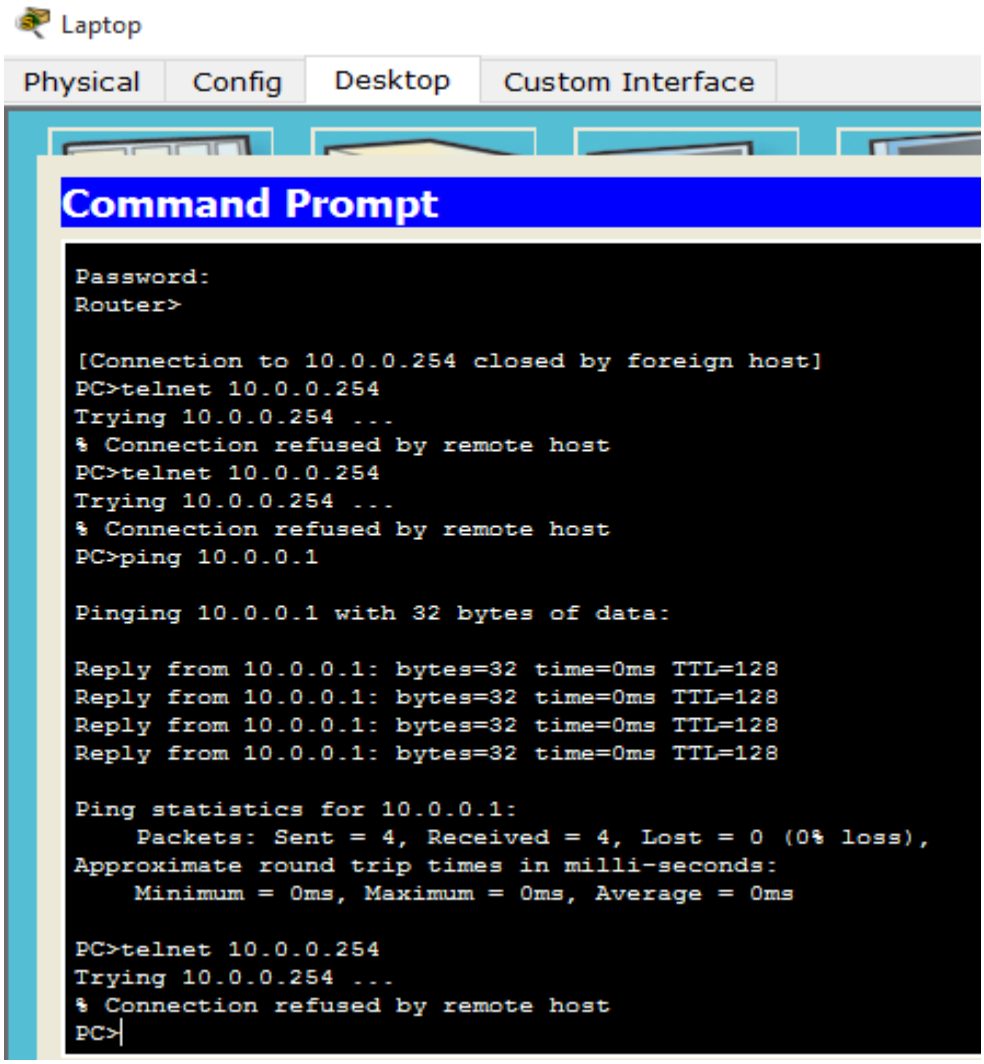
```
Router#show access-lists
Standard IP access list 99
    10 permit host 10.0.0.1
Router#show run
Building configuration...

Current configuration : 617 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
```

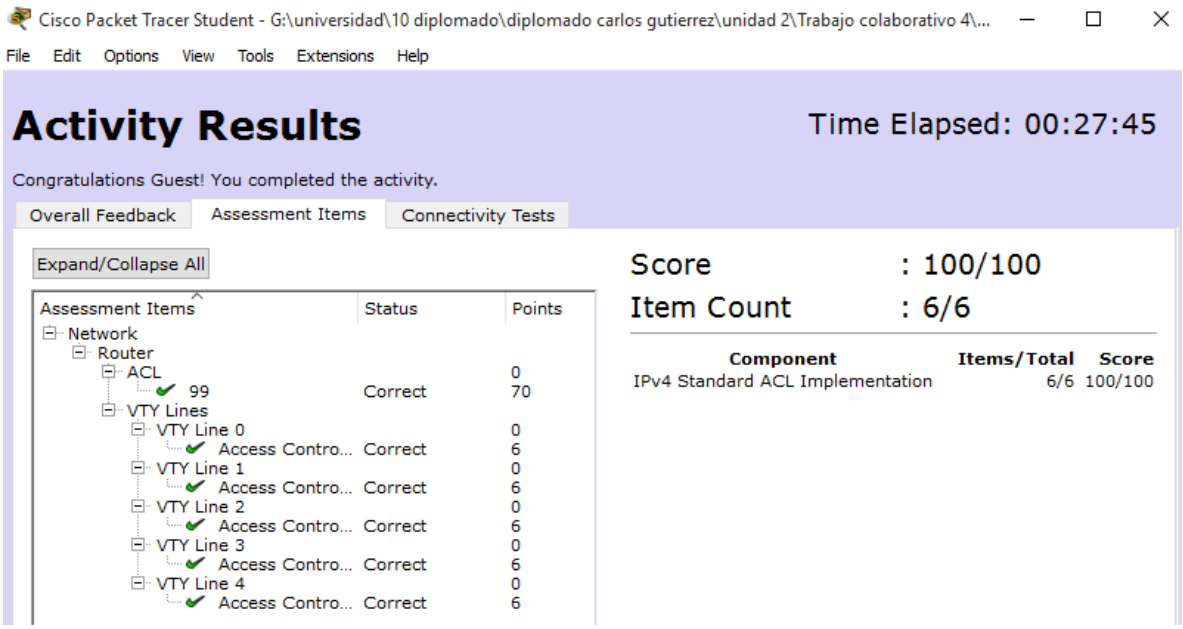
```
interface FastEthernet0/0
 ip address 10.0.0.254 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
access-list 99 permit host 10.0.0.1
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class 99 in
 password cisco
 login
line vty 5 15
 access-class 99 in
 password cisco
 login
!
!
!
end
```

Paso 2: Verifique que la ACL esté funcionando correctamente.

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




Laptop
Physical
Config
Desktop
Custom Interface
Command Prompt
Password:
Router>
[Connection to 10.0.0.254 closed by foreign host]
PC>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
PC>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
PC>ping 10.0.0.1
Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=0ms TTL=128
Reply from 10.0.0.1: bytes=32 time=0ms TTL=128
Reply from 10.0.0.1: bytes=32 time=0ms TTL=128
Reply from 10.0.0.1: bytes=32 time=0ms TTL=128
Ping statistics for 10.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
PC>


Cisco Packet Tracer Student - G:\universidad\10 diplomado\diplomado carlos gutierrez\unidad 2\Trabajo colaborativo 4\...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:27:45
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Network
Router
ACL 0
99 Correct 70
VTY Lines
VTY Line 0 0
Access Contro... Correct 6
VTY Line 1 0
Access Contro... Correct 6
VTY Line 2 0
Access Contro... Correct 6
VTY Line 3 0
Access Contro... Correct 6
VTY Line 4 0
Access Contro... Correct 6
Score : 100/100
Item Count : 6/6
Component
Items/Total
Score
IPv4 Standard ACL Implementation 6/6 100/100

DESARROLLO EJERCICIO 9.5.2.6

Packet Tracer: configuración de las ACL de IPv6.

Topología

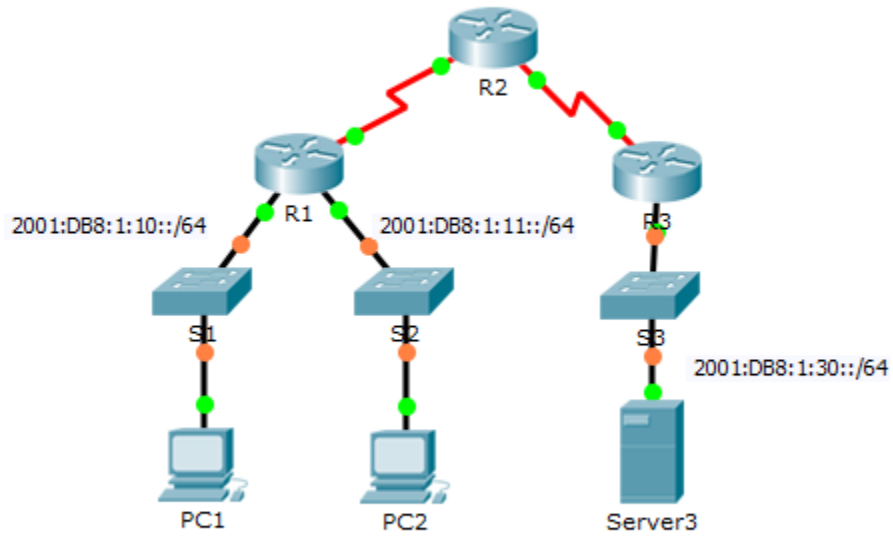


Tabla de direccionamiento

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

Objetivos

Parte 1: configurar, aplicar y verificar una ACL de IPv6
Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Parte 1: configurar, aplicar y verificar una ACL de IPv6

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

Paso 1: configure una ACL que bloqueará el acceso HTTP y HTTPS.

Configure una ACL llamada BLOCK_HTTP en R1 con las siguientes instrucciones.

a. Bloquee el tráfico HTTP y HTTPS para que no llegue a Server3.

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

b. Permita que pase el resto del tráfico de IPv6.

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

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#
```

Paso 2: aplique la ACL a la interfaz correcta.

Aplique la ACL en la interfaz más cercana al origen del tráfico que se bloqueará.

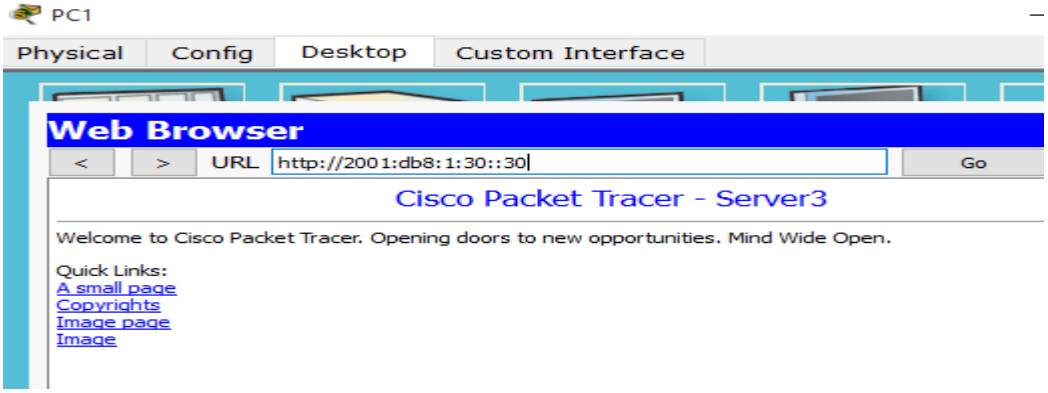
R1(config)# **interface GigabitEthernet0/1**
R1(config-if)# **ipv6 traffic-filter BLOCK_HTTP in**

```
R1(config)#int g0/1
R1(config-if)#ipvg traffic-filter BLOCK_HTTP in
                 ^
% Invalid input detected at '^' marker.

R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

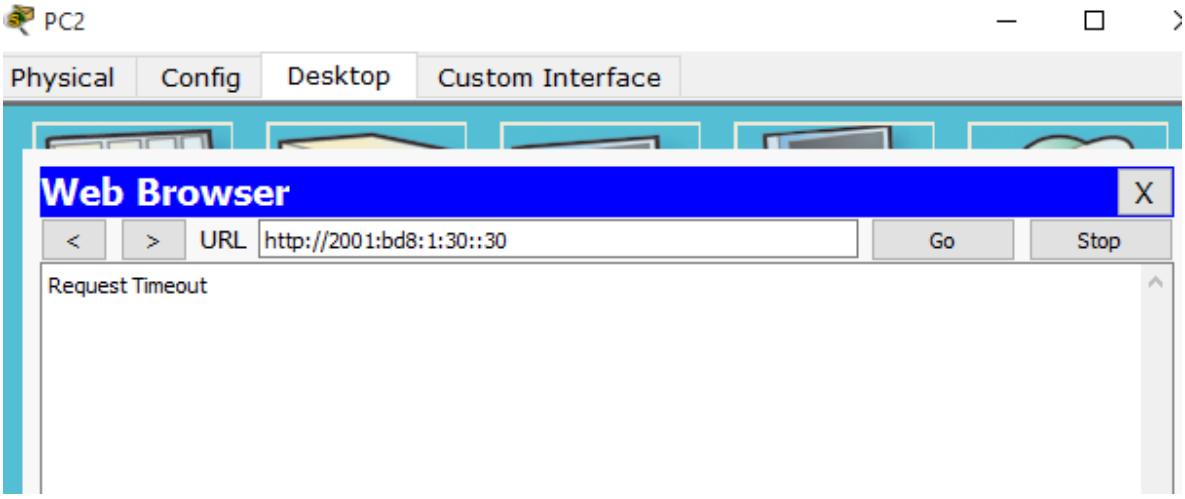
Paso 3: Verifica la implementación de ACL.

Verifique que la ACL esté funcionando según lo previsto llevando a cabo las siguientes pruebas:

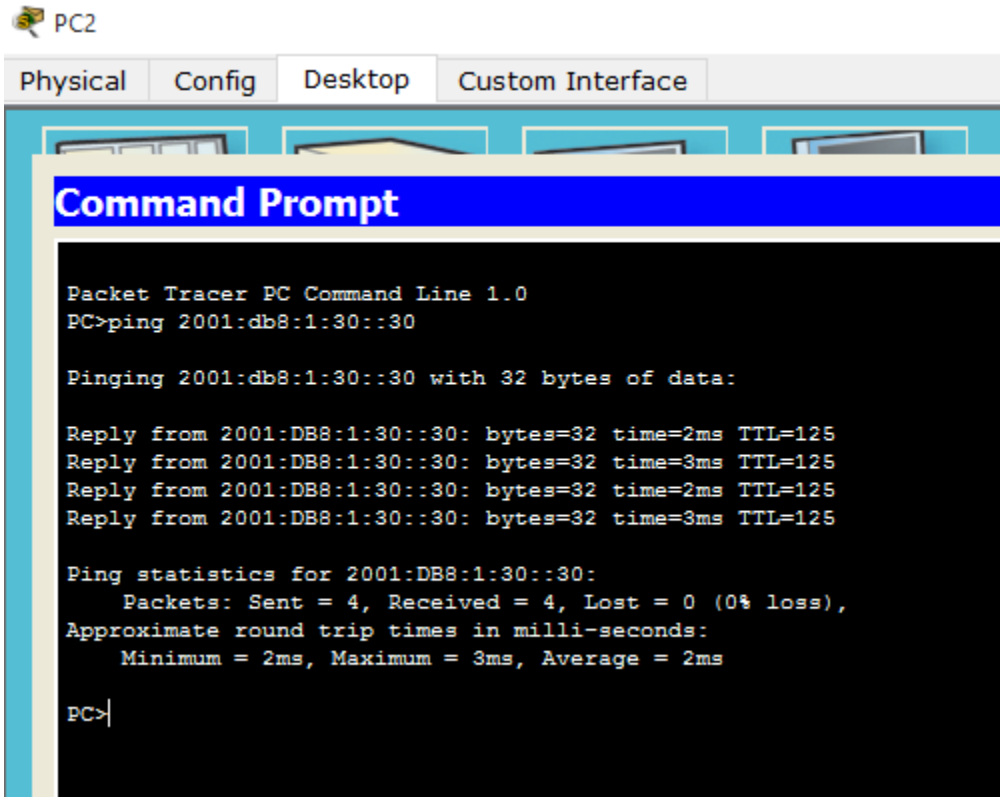
Abra el navegador web de PC1 a http: // 2001: DB8: 1: 30 :: 30 o https: // 2001: DB8: 1: 30 :: 30. el sitio web debería aparecer



Abra el navegador web de PC2 a http: // 2001: DB8: 1: 30 :: 30 o https: // 2001: DB8: 1: 30 :: 30. El sitio web debe estar bloqueado



Ping de PC2 a 2001: DB8: 1: 30:: 30. El ping debería ser exitoso.



Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Los registros ahora indican que su servidor recibe pings de muchas direcciones IPv6 diferentes en un ataque de Denegación de Servicio Distribuido (DDoS). Debe filtrar las solicitudes de ping ICMP a su servidor.

Paso 1: crea una lista de acceso para bloquear ICMP.

Configure una ACL llamada BLOCK_ICMP en R3 con las siguientes declaraciones:

a. Bloquee todo el tráfico ICMP desde cualquier host a cualquier destino.

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

b. Permita que pase el resto del tráfico de IPv6.

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

```
R3>enable
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
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#
```

Paso 2: aplique la ACL a la interfaz correcta.

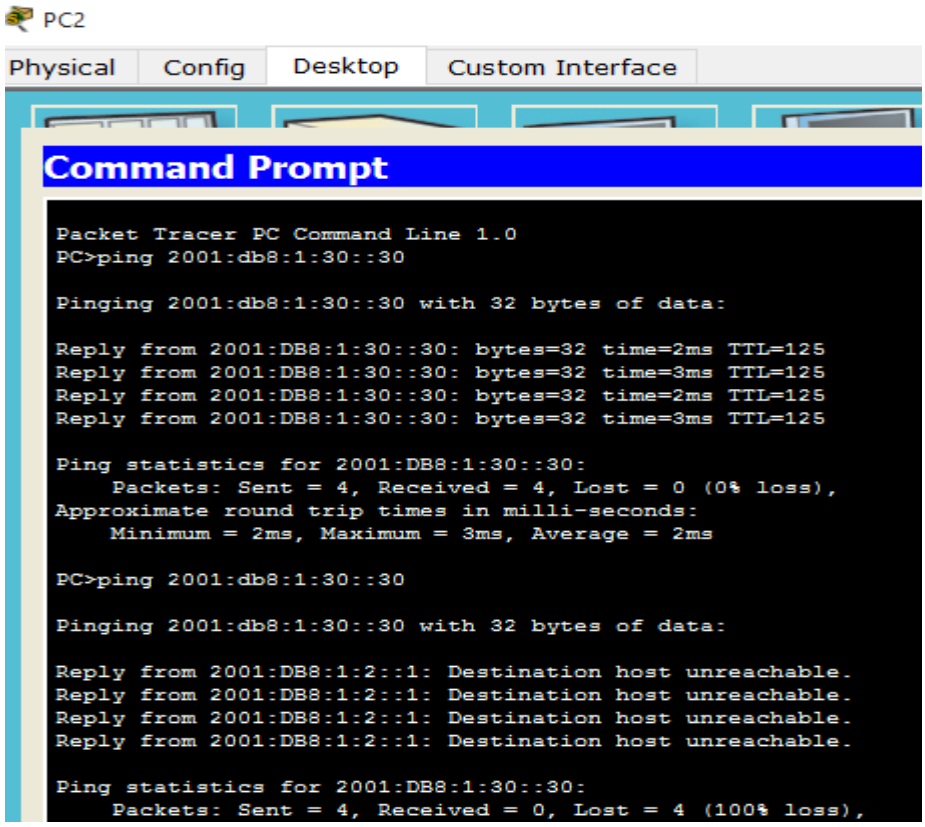
En este caso, el tráfico ICMP puede provenir de cualquier fuente. Para garantizar que el tráfico ICMP esté bloqueado independientemente de su origen o de los cambios que se produzcan en la topología de la red, aplique la ACL más cercana al destino.

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

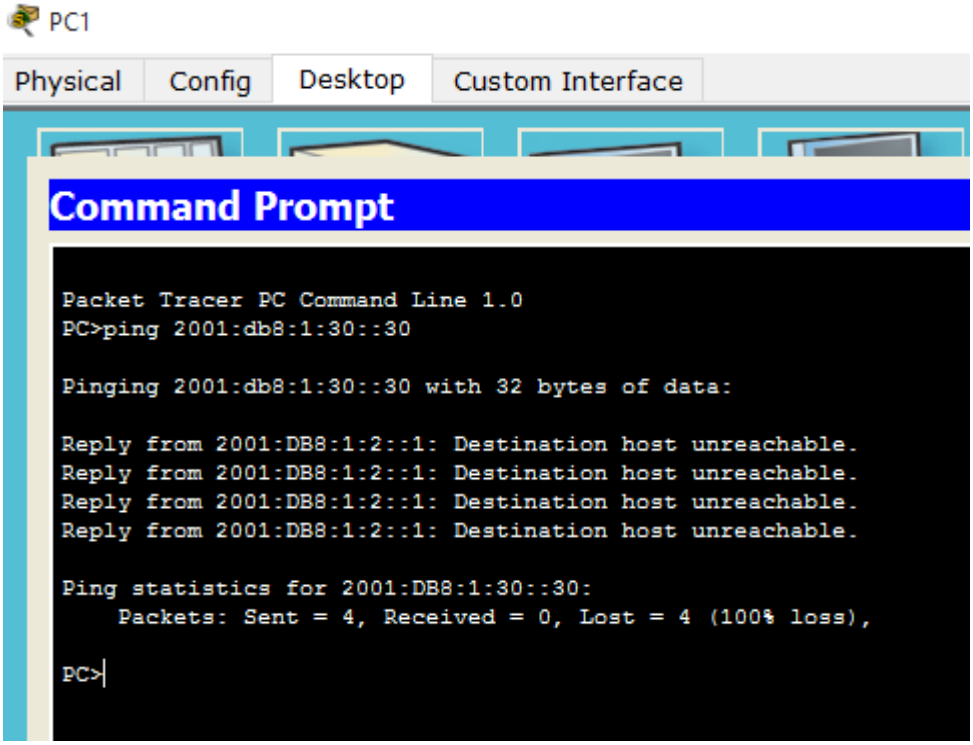
```
R3(config-if)#int g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

Paso 3: Verifique que la lista de acceso adecuada funcione.

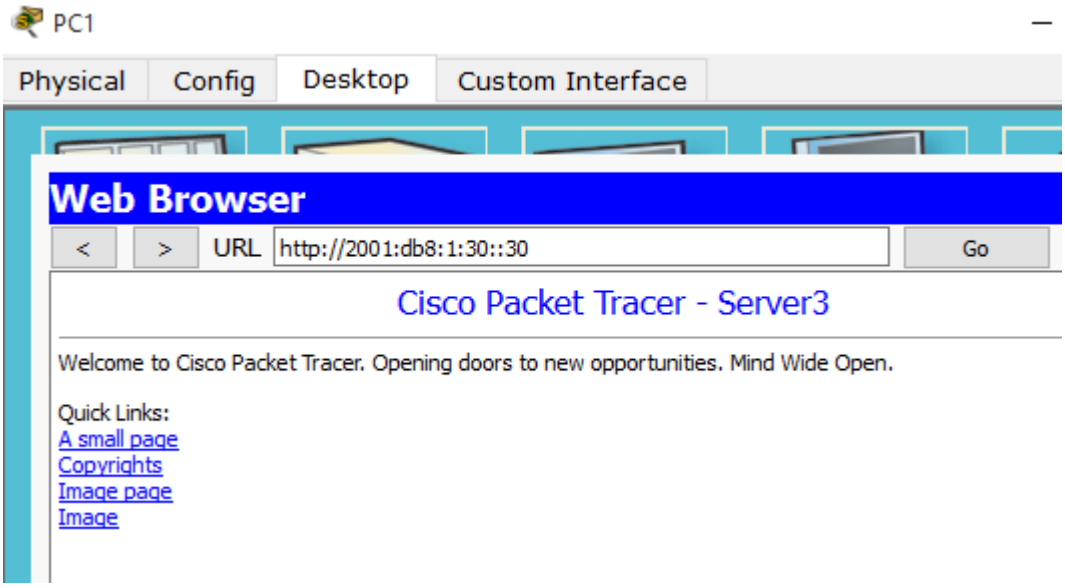
a. Ping de PC2 a 2001: DB8: 1: 30::30. El ping debería fallar.

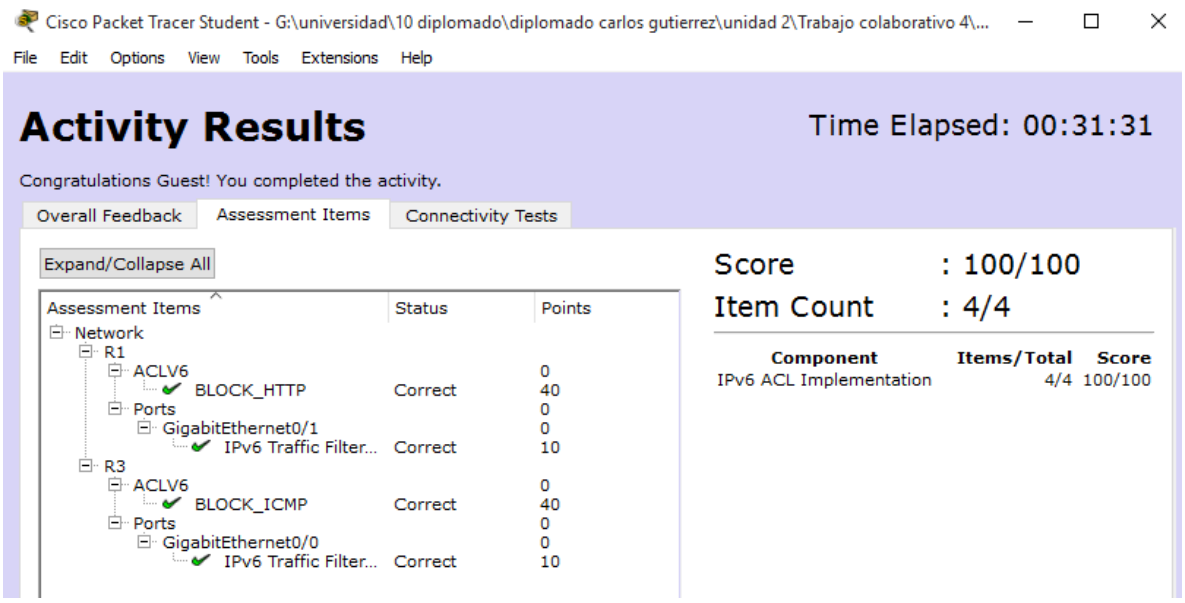


b. Ping de PC1 a 2001: DB8: 1: 30::30. El ping debería fallar.



Abra el navegador web de PC1 a http: // 2001: DB8: 1: 30::30 o https: // 2001: DB8: 1: 30::30. El sitio web debería mostrarse.





DESARROLLO EJERCICIO 10.1.2.4

Práctica de laboratorio: configuración de DHCPv4 básico en un router

Topología

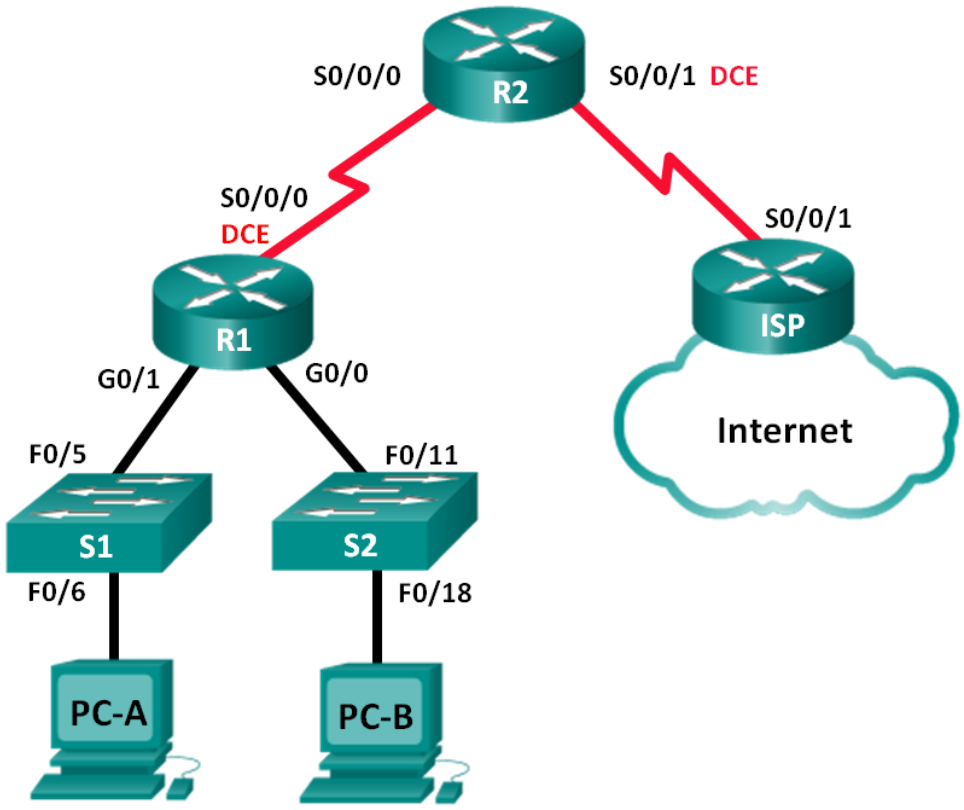


Tabla de direccionamiento

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

Objetivos

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

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

Información básica/situación

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

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

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

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

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

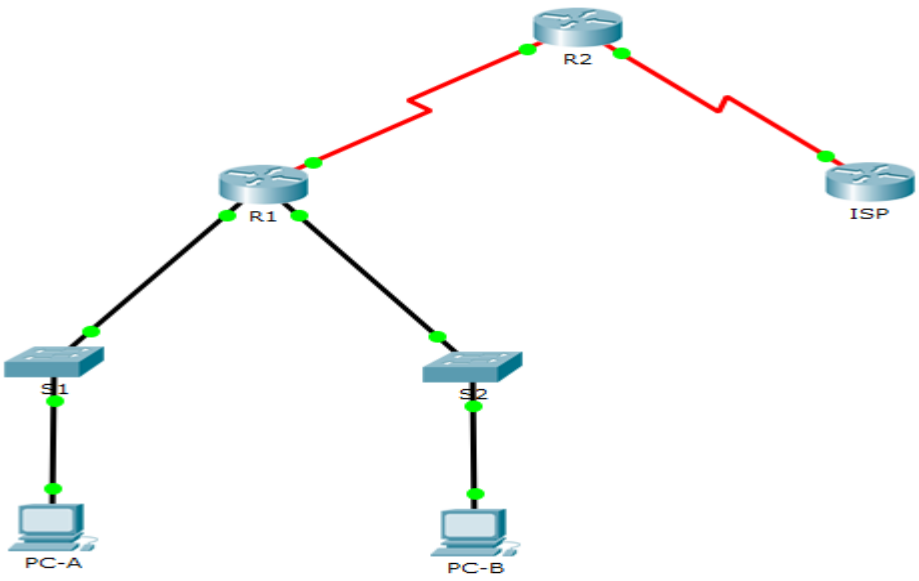
Recursos necesarios

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

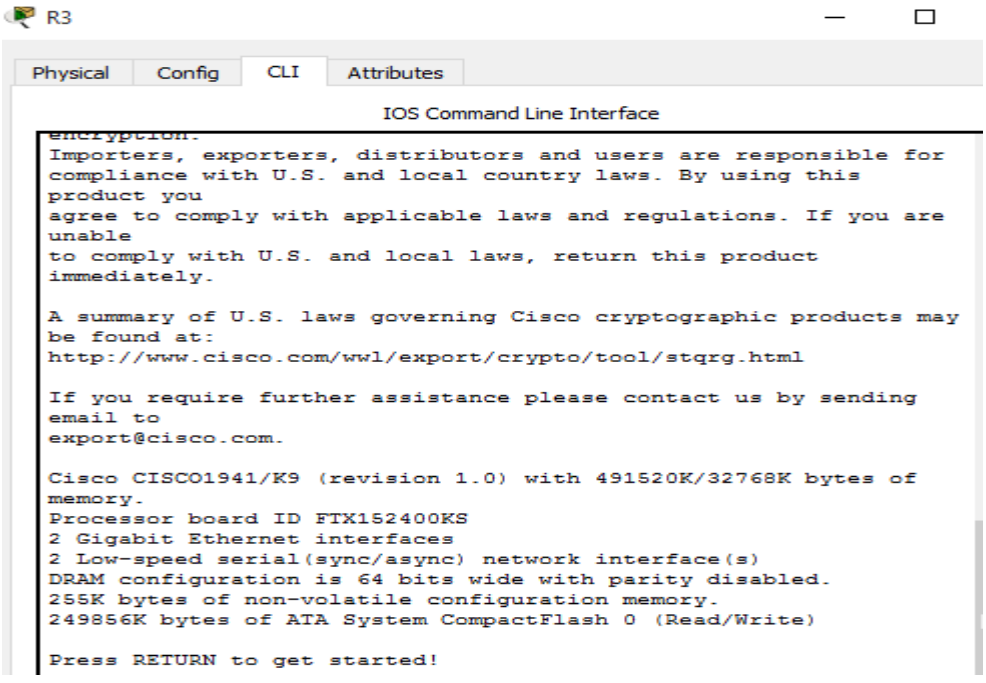
Parte 1. armar la red y configurar los parámetros básicos de los dispositivos En la parte 1, establecerá la topología de la red y configurará los routers y switches con

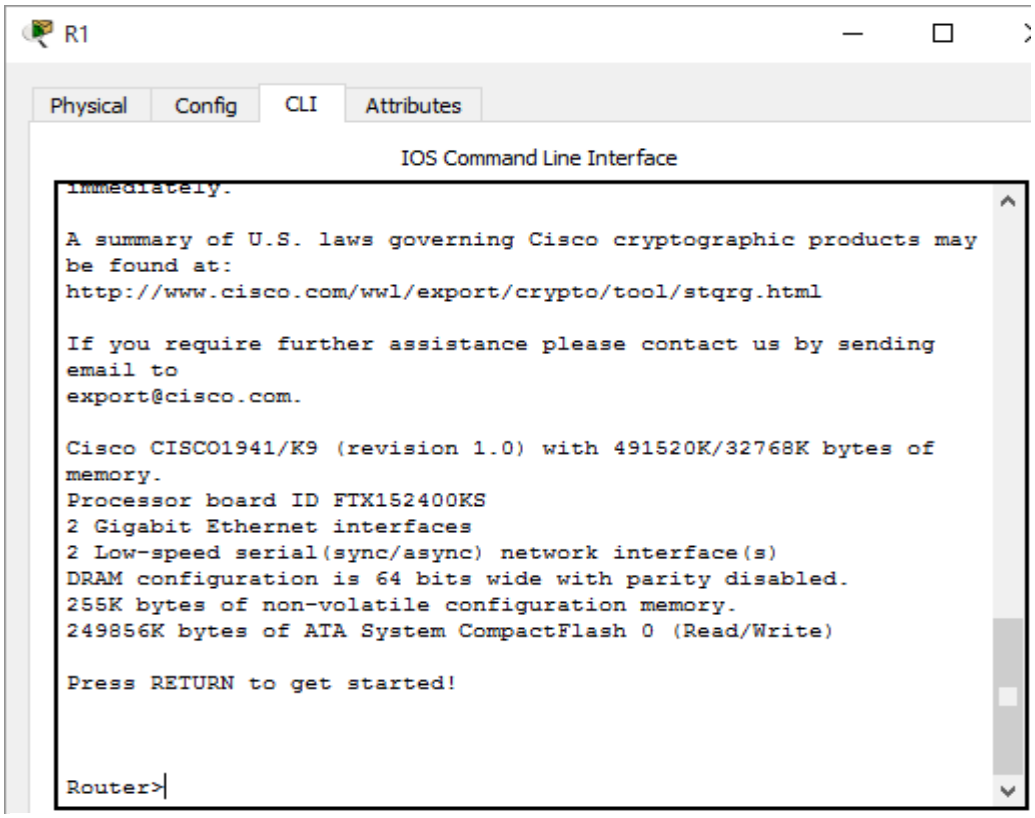
los parámetros básicos, como las contraseñas y las direcciones IP. Además, configurará los parámetros de IP de las computadoras en la topología.

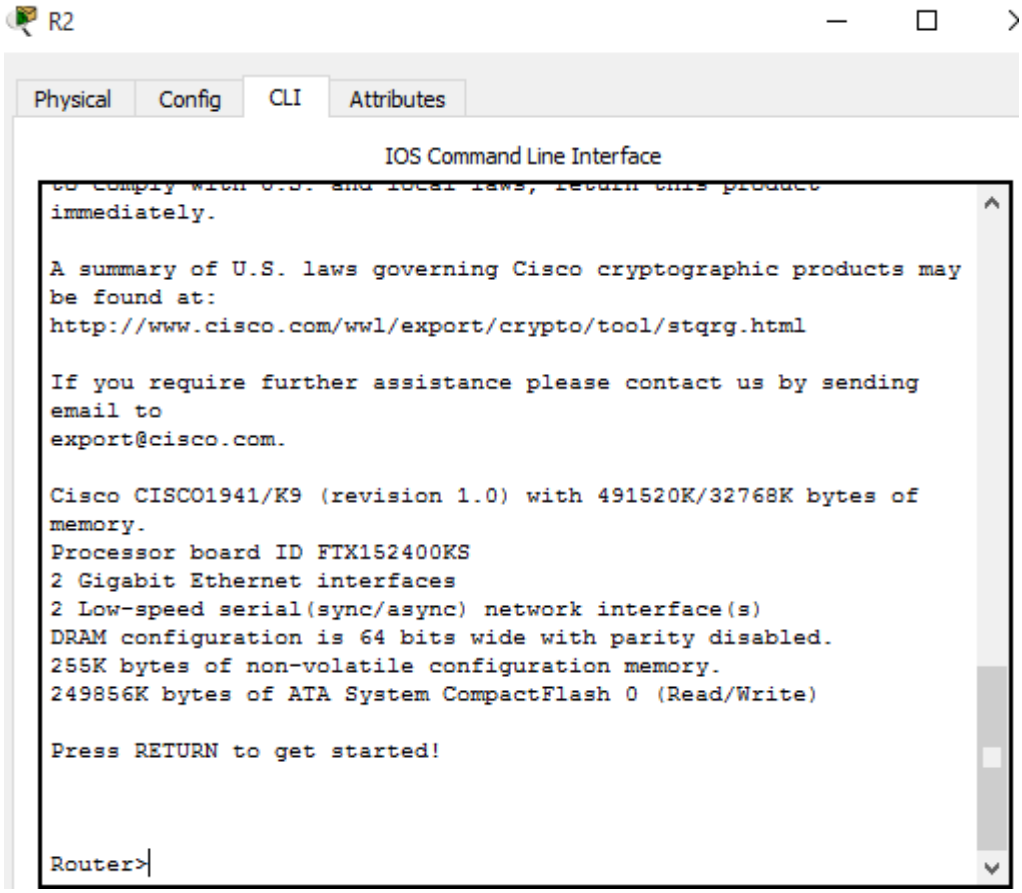
Paso 1. realizar el cableado de red tal como se muestra en la topología.

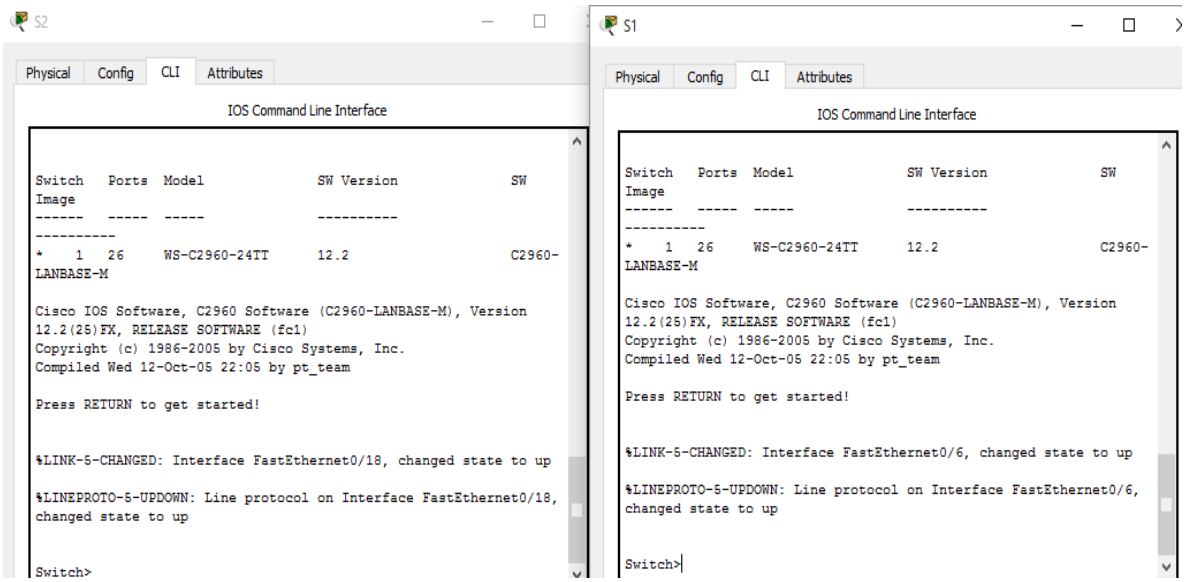


Paso 2. inicializar y volver a cargar los routers y los switches.




R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/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.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
Router>


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/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.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
Router>



Paso 3. configurar los parámetros básicos para cada router.

a. Desactive la búsqueda DNS.

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

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

d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostaname R1
                    ^
% Invalid input detected at '^' marker.

Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line console o
                    ^
% Invalid input detected at '^' marker.

R1(config-line)#logging synchronous
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret class
R1(config)#banne motd #El acceso no autorizado esta prohibido#
R1(config)#service password-encryption
R1(config)#
```

```
Router(config)#no ip domain-lookup
Router(config)#hostname R"
R"(config)#hostname R2
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#exit
R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#enable secret class
R2(config)#banner motd #El acceso no autorizado esta prohibido#
R2(config)#service password-encryption
R2(config)#
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#exit
R3(config)#line console 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#enable secret class
R3(config)#banner motd #El acceso no autorizado esta prohibido#
R3(config)#service password-encryption
R3(config)#
```

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

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

```
R1(config)#int g0/0
R1(config-if)#ip add 192.168.0.1 255.255.255.0
R1(config-if)#no shu

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

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

R1(config-if)#int g0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shu

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

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

R1(config-if)#int s0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#ip add 192.168.2.253 255.255.255.252
R1(config-if)#no shu

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
```

```
R2(config)#int s0/0/0
R2(config-if)#ip add 192.168.2.254 255.255.255.252
R2(config-if)#no shu

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

R2(config-if)#no shu
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#int s0/0/1
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#ip add 209.165.200.226 255.255.255.224
R2(config-if)#no shu

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

```
ISP(config)#int s0/0/1
ISP(config-if)#ip add 209.165.200.225 255.255.255.224
ISP(config-if)#no shu

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
```

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**

```
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 192.168.2.255 0.0.0.3
R1(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.254
(Serial0/0/0) is up: new adjacency

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

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**

```
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router eigrp 1
R2(config-router)#network 192.168.2.252 0.0.0.3
R2(config-router)#redistribute static
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
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**

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

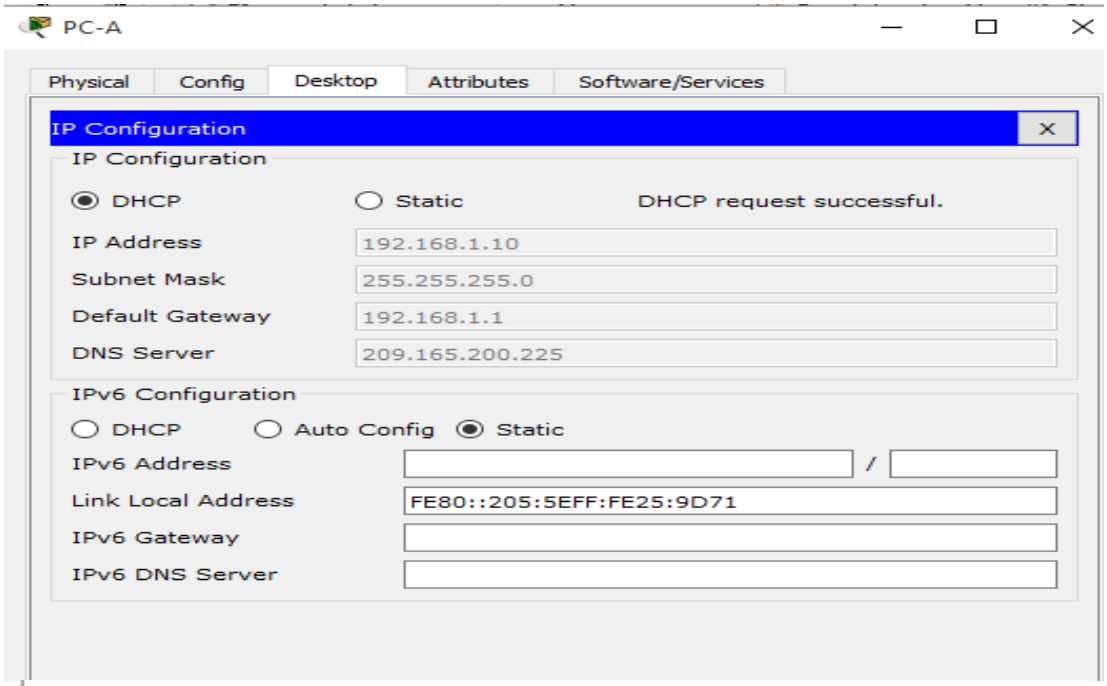
```
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#end
```

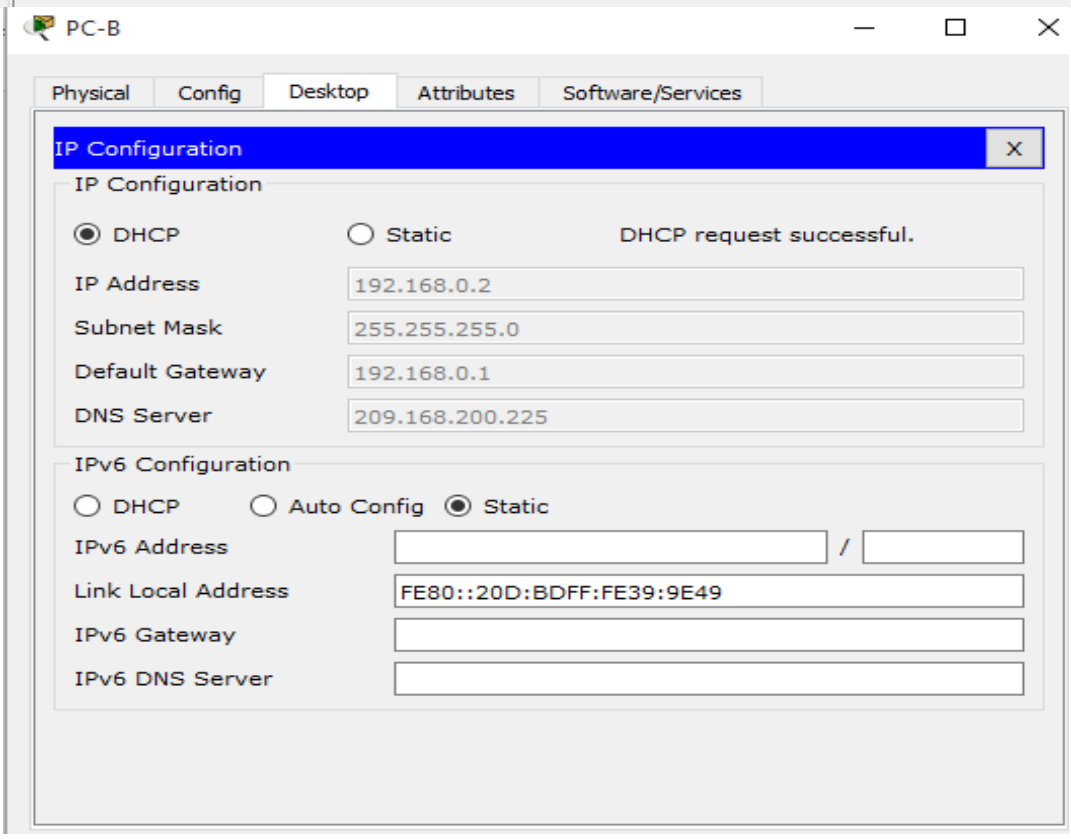
Paso 4. verificar la conectividad de red entre los routers.

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

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#end
ISP#
%SYS-5-CONFIG_I: Configured from console by console

ISP#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#ping 192.168.2.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/6
ms

ISP#ping 192.168.2.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/8
ms

ISP#
```

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





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

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

Paso 1. configurar los parámetros del servidor de DHCPv4 en el router R2.
En el R2, configure un conjunto de direcciones DHCP para cada LAN del R1. Utilice el nombre de conjunto **R1G0** para G0/0 LAN y **R1G1** para G0/1 LAN. 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 **ccnalab.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.

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

```
R2#ip dhcp excluded-address 192.168.0.1 192.168.0.9
     ^
% Invalid input detected at '^' marker.

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
                ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#lease 2
                ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#exit
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#defaul%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.0.1.

R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.168.200.225
R2(dhcp-config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.0.1.

R2(dhcp-config)#
```

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.

En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando **ipconfig /all**. ¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué? **No, Porque el R2 está en otra red.**

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

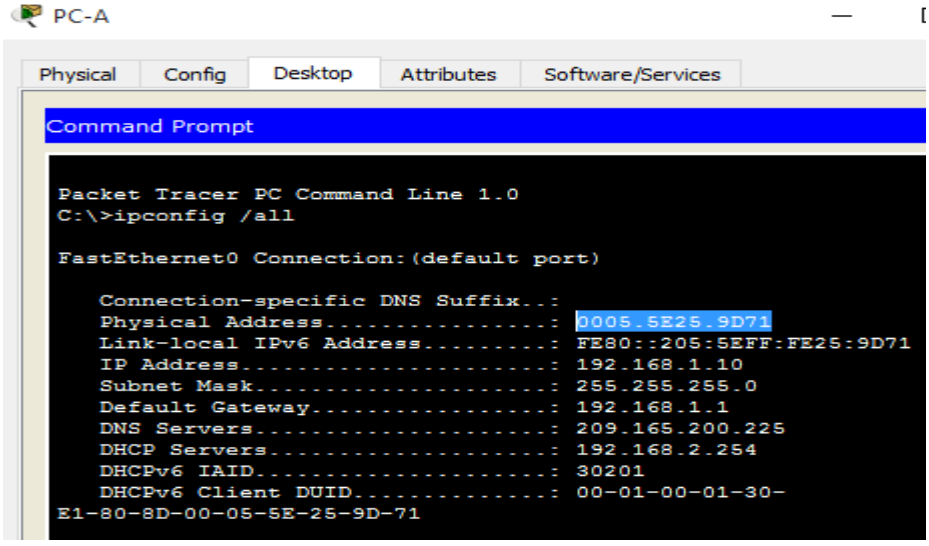
Configure las direcciones IP de ayuda en el R1 para que reenvíen todas las solicitudes de DHCP al servidor de DHCP en el R2. En las líneas a continuación, escriba los comandos necesarios para configurar el R1 como agente de retransmisión DHCP para las LAN del R1.

R1(config)# **interface g0/0**
R1(config-if)# **ip helper-address 192.168.2.254**
R1(config-if)# **exit**
R1(config-if)# **interface g0/1**
R1(config-if)# **ip helper-address 192.168.2.254**

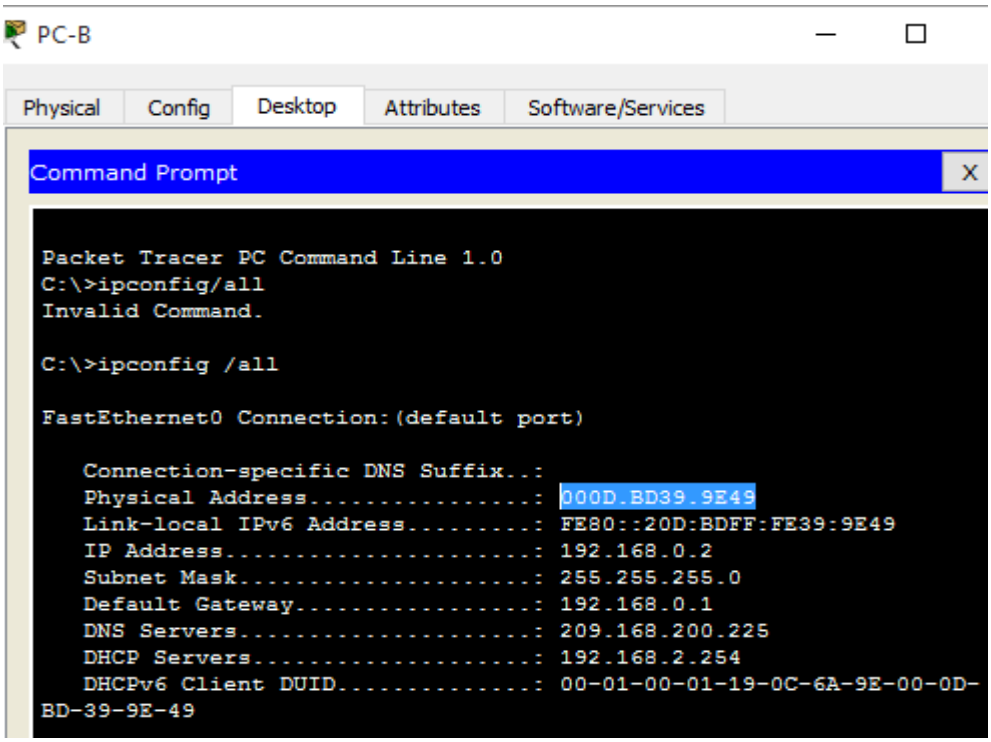
Paso 3. registrar la configuración IP para la PC-A y la PC-B.

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

PC-A IP: 192.168.1.10
MAC: 0005.5E25.9D71



PC-B IP: 192.168.0.2
MAC: 000D.BD39.9E49



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?

La IP: 192.168.1.10 y la IP: 192.168.0.2 respectivamente

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

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

```
R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.10     0005.5E25.9D71           --                     Automatic
192.168.0.2      000D.BD39.9E49           --                     Automatic
R2#
```

Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado? **La MAC correspondiente a cada Ip y el type**

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.

```
Automatic
R2#show ip dhcp server
                ^
% Invalid input detected at '^' marker.

R2#show ip dhcp server statistics
                ^
% Invalid input detected at '^' marker.

R2#
```

¿Cuántos tipos de mensajes DHCP se indican en el resultado? **El Packete Tracer no acepta este comando**

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

```
R2#show ip dhcp pool

Pool R1G1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.254     1    / 2     / 254

Pool R1G0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.0.1          192.168.0.1      - 192.168.0.254     1    / 2     / 254
R2#
```

En el resultado del comando **show ip dhcp pool**, ¿a qué hace referencia el índice actual (Current índex)? **A la dirección ip del router 1 de la interface g0/0**

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

```
R2#show run
Building configuration...

Current configuration : 1426 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 192.168.1.1 192.168.0.9
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 209.168.200.225
!
```

e. En el R1, 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.

```
R1#show ip int 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 unreachables 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
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
```

```
R1#show ip int 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 unreachables 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
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude 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?

No es beneficioso porque requiere más uso de hardware para su funcionamiento normal, es preferible que solo un router tenga todo el manejo del DHCP de forma centralizada. Igualmente, en agentes de retransmisión es más difícil la administración de los mismos.

DESARROLLO EJERCICIO 10.1.2.5

Práctica de laboratorio: configuración de DHCPv4 básico en un switch

Topología

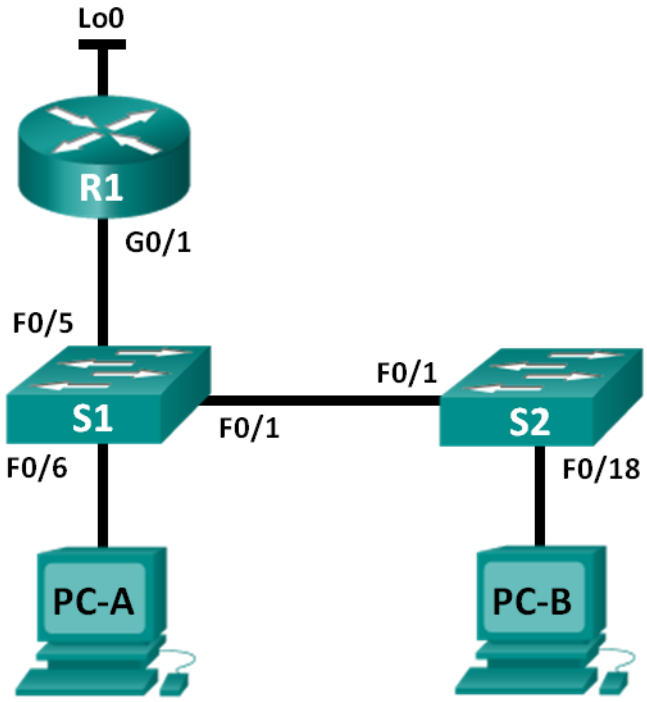


Tabla de direccionamiento

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

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
Parte 2: cambiar la preferencia de SDM

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

Parte 3: configurar DHCPv4
- Configurar DHCPv4 para la VLAN 1.
- Verificar la conectividad y DHCPv4.

Parte 4: configurar DHCP para varias VLAN

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

Parte 5: habilitar el routing IP
- Habilite el routing IP en el switch.
- Crear rutas estáticas.

Información básica/situación

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

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

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

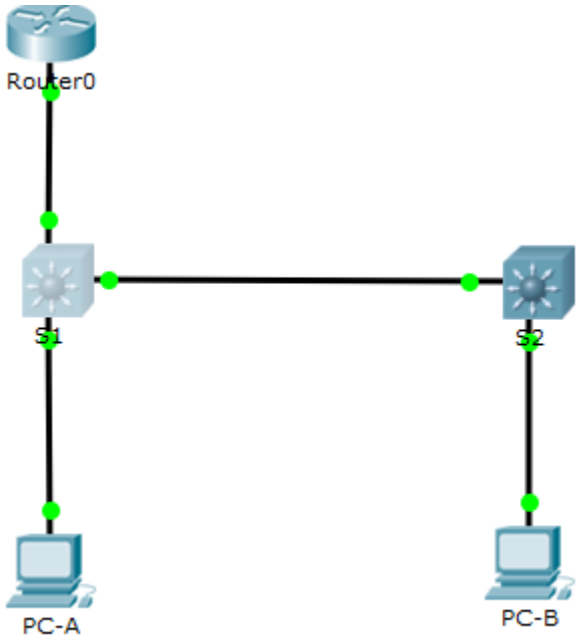
Nota: asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

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

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

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



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

Paso 3: configurar los parámetros básicos en los dispositivos.

a. Asigne los nombres de dispositivos como se muestra en la topología.
Proceso: Ejecutado en S1, S2 y R1

b. Desactive la búsqueda del DNS. Proceso:
Ejecutado en S1, S2 y R1

c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty. Proceso:
Ejecutado en S1, S2 y R1

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#no ip domain-lookup
S1(config)#
```

```
S2(config-line)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#line console vty 0 15
                 ^
% Invalid input detected at '^' marker.

S2(config-line)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#enable secret class
S2(config)#no ip domain-lookup
S2(config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

```
Router>enable
Router#confi t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#enable secret class
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

```
R1#confi t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g 0/1
R1(config-if)#ip add 192.168.1.10 255.255.255.0
R1(config-if)#no shu

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

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

R1(config-if)#int lo 0

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

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

R1(config-if)#ip add 209.165.200.255 255.255.255.255.224
                                     ^
% Invalid input detected at '^' marker.

R1(config-if)#ip add 209.165.200.255 255.255.255.224
Bad mask /27 for address 209.165.200.255
R1(config-if)#ip add 209.165.200.225 255.255.255.224
R1(config-if)#no shu
R1(config-if)#
```

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.

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int vlan 1
S1(config-if)#ip add 192.168.1.1 255.255.255.0
S1(config-if)#no shu

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up

S1(config-if)#int vlan 2
S1(config-if)#ip add 192.168.2.1 255.255.255.0
S1(config-if)#no shu
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Parte 2: Cambiar la preferencia de SDM

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

Paso 1: mostrar la preferencia de SDM en el S1.

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

S1# **show sdm prefer**

```
S1#show sdm prefer
 The current template is "dual-ipv4-and-ipv6 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:                  4K
  number of IPv4 IGMP groups:                       250
  number of IPv4 unicast routes:                    0
  number of IPv6 multicast groups:                  0.375k
  number of directly-connected IPv6 addresses:      0
  number of indirect IPv6 unicast routes:           0
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      125
  number of IPv4/MAC security aces:                 375
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0.625k
  number of IPv6 security aces:                     0.125K
```

¿Cuál es la plantilla actual?

Respuesta:
Como se visualiza en la ejecución del comando es "dual-ipv4-and-ipv6 default"

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

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

S1(config)# **sdm prefer lanbase-routing**

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#sdm prefer lanbase-routing
                       ^
% Invalid input detected at '^' marker.

S1(config)#
```

¿Qué plantilla estará disponible después de la recarga? **Default – no se pudo cambiar**

Packet tracer no soporta este comando, pero si fuera ejecutado cambiaria a en **lanbaserouting.**

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

S1# **reload** System configuration has been modified. Save? [yes/no]: **no** Proceed with reload? [confirm]

Nota: la nueva plantilla se utilizará después del reinicio, incluso si no se guardó la

configuración en ejecución. Para guardar la configuración en ejecución, responda **yes** (sí) para guardar la configuración modificada del sistema.

```
S1#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 00E0.B085.90E6
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 2 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4416183
flashfs[0]: Bytes available: 59600201
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
################################
```

Respuesta:
No fue soportado el cambio a este parámetro de configuración por packet tracer

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

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

S1# **show sdm prefer**

```
S1#show sdm prefer
 The current template is "dual-ipv4-and-ipv6 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:                  4K
  number of IPv4 IGMP groups:                       250
  number of IPv4 unicast routes:                    0
  number of IPv6 multicast groups:                  0.375k
  number of directly-connected IPv6 addresses:      0
  number of indirect IPv6 unicast routes:           0
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      125
  number of IPv4/MAC security aces:                 375
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0.625k
  number of IPv6 security aces:                     0.125K
```

Desarrollo:

No se cambió por no soportar packet tracer la ejecución del comando como parámetro final.

Parte 3: configurar DHCPv4

En la parte 3, configurará DHCPv4 para la VLAN 1, revisará las configuraciones IP en los equipos host para validar la funcionalidad de DHCP y verificará la conectividad de todos los dispositivos en la VLAN 1.

Paso 1: configurar DHCP para la VLAN 1.

a. Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#
```

El comando es el visualizado en la imagen: **ip dhcp excluded-address (rango)**

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

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

El comando es el visualizado en la imagen: **ip dhcp pool DHCP1**

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

```
S1(config)#ip dhcp pool DHCP1
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#
```

El comando es el visualizado en la imagen: network **ipv4 mascara**

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

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

El comando es el visualizado en la imagen: **default-router "ipv4"**

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

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

El comando es el visualizado en la imagen: **dns-server “ipv4”**

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

```
S1(dhcp-config)#lease 3
                   ^
% Invalid input detected at '^' marker.

S1(dhcp-config)#
```

El comando no fue soportado por packet tracer

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

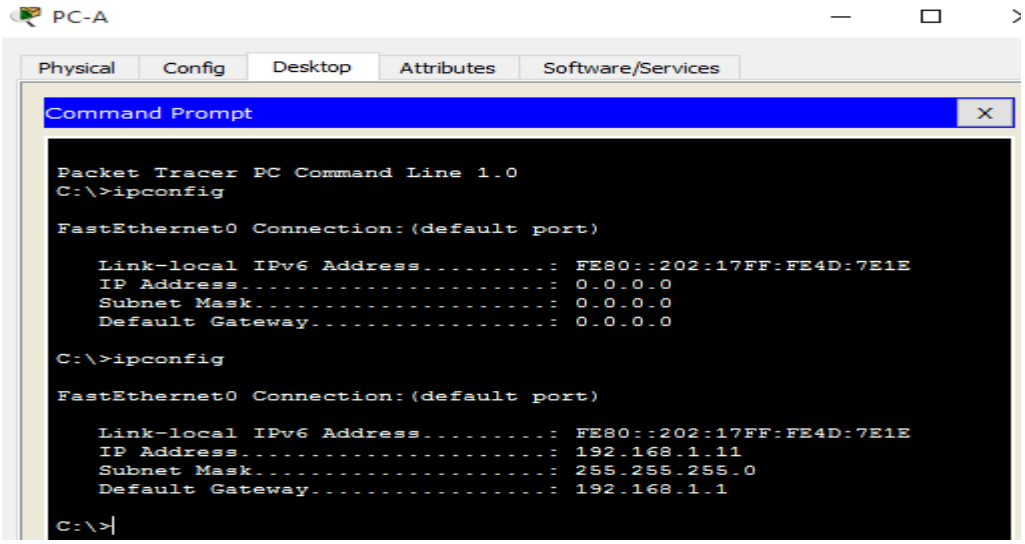
```
S1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

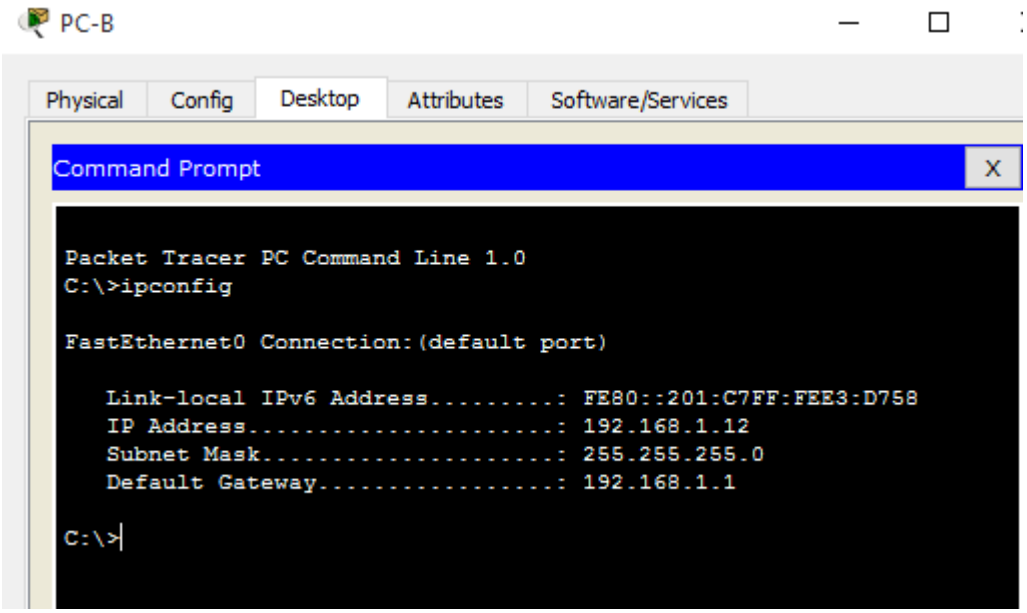
Paso 2: verificar la conectividad y DHCP.

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***

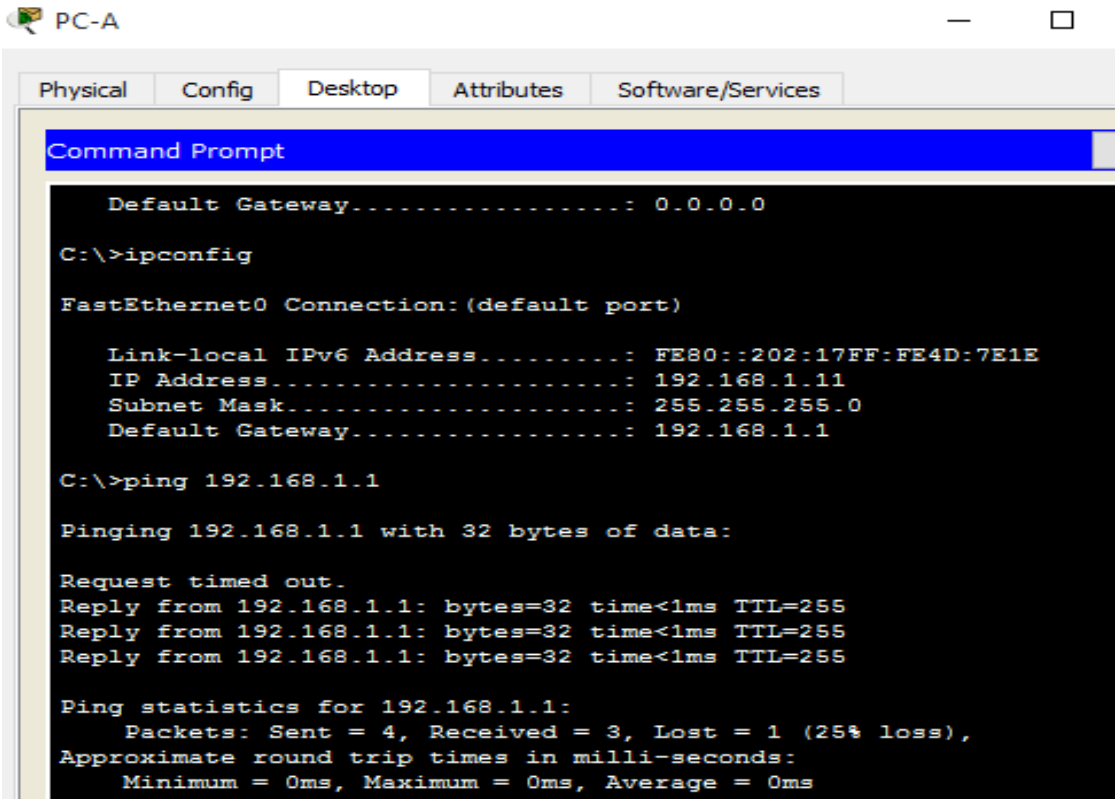
Para la PC-B, incluya lo siguiente:
Dirección IP: ***192.168.1.12***
Máscara de subred: ***255.255.255.0***
Gateway predeterminado: ***192.168.1.1***



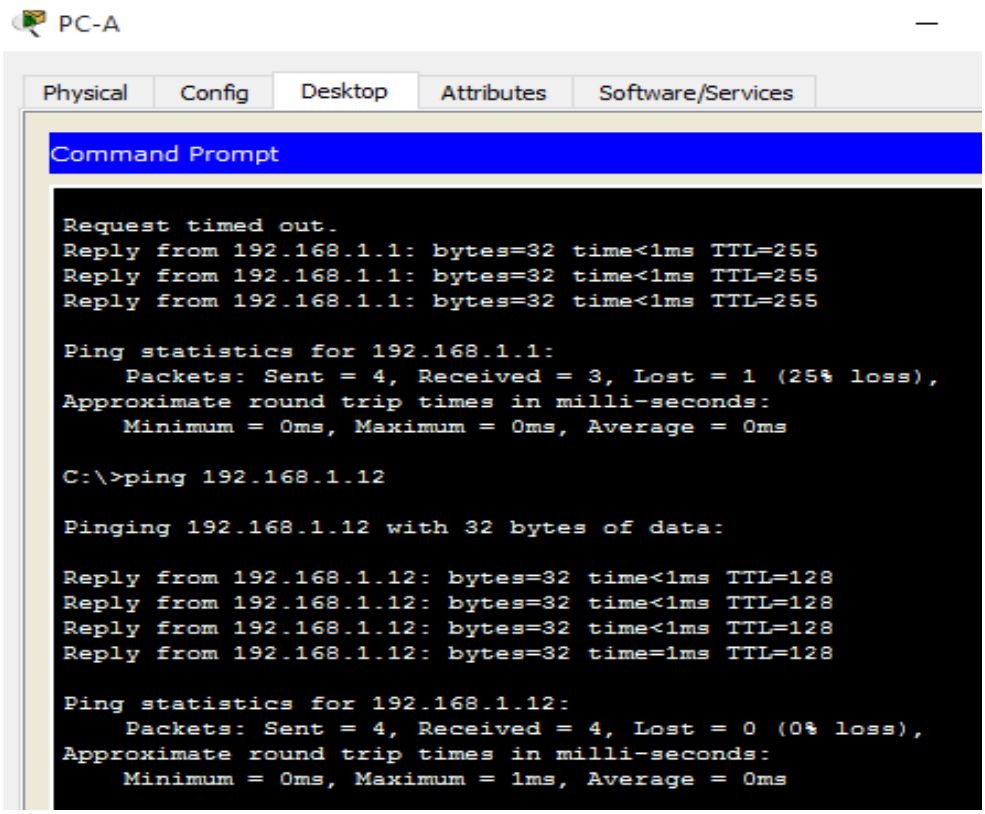


b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

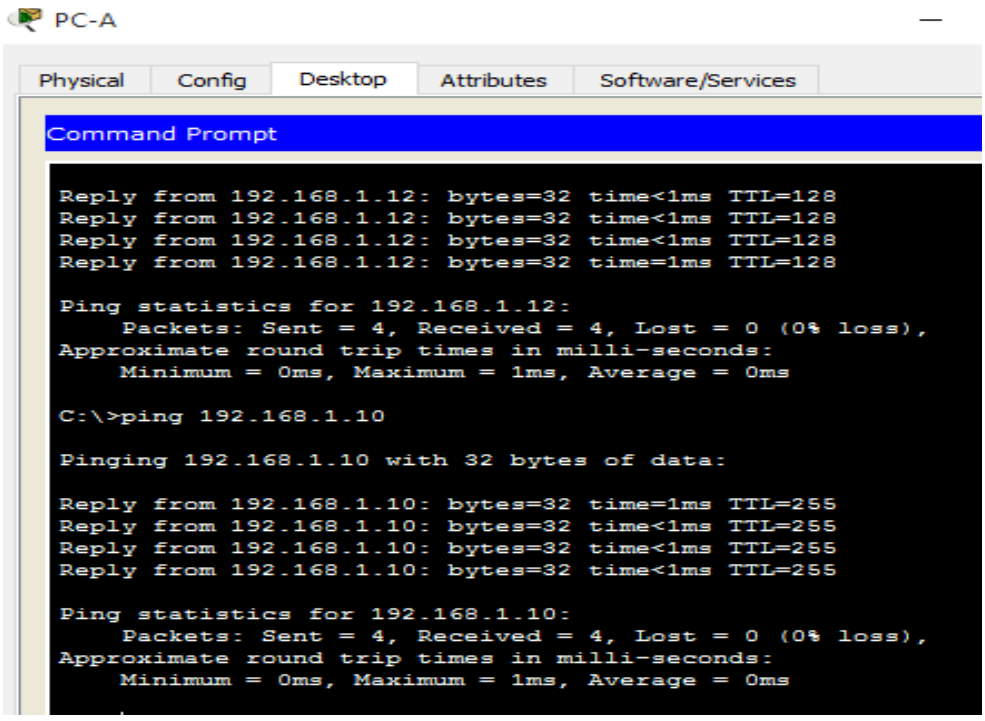
¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1?
Satisfactorio



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



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



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

Parte 14:configurar DHCPv4 para varias VLAN En la parte 4, asignará la PC-A un puerto que accede a la VLAN 2, configurará DHCPv4 para la VLAN 2, renovará la configuración IP de la PC-A para validar DHCPv4 y verificará la conectividad dentro de la VLAN.

Parte 4: configurar DHCPv4 para varias VLAN

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

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#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed
state to up

S1(config-if)#
```

*El comando es el visualizado en la imagen**: switchport mode Access / switchport Access vlan 2***

Paso 2: Configurar DHCPv4 para la VLAN 2.

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

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

El comando es el visualizado en la imagen: **ip dhcp excluded-address (rango)**

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
S1(dhcp-config)#
```

El comando es el visualizado en la imagen: **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
S1(dhcp-config)#
```

El comando es el visualizado en la imagen: network **ipv4 mascara**

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
S1(dhcp-config)#
```

El comando es el visualizado en la imagen: **default-router "ipv4"**

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
S1(dhcp-config)#
```

El comando es el visualizado en la imagen: **dns-server "ipv4"**

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

```
S1(dhcp-config)#lease 3
                  ^
% Invalid input detected at '^' marker.

S1(dhcp-config)#
```

El comando no fue soportado por packet tracer

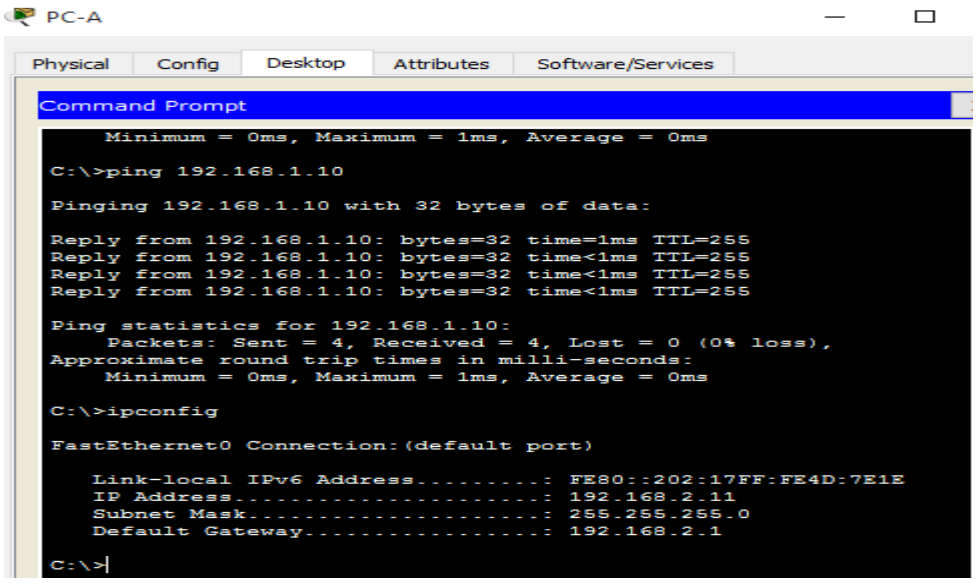
g. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
S1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Paso 3: verificar la conectividad y DHCPv4.

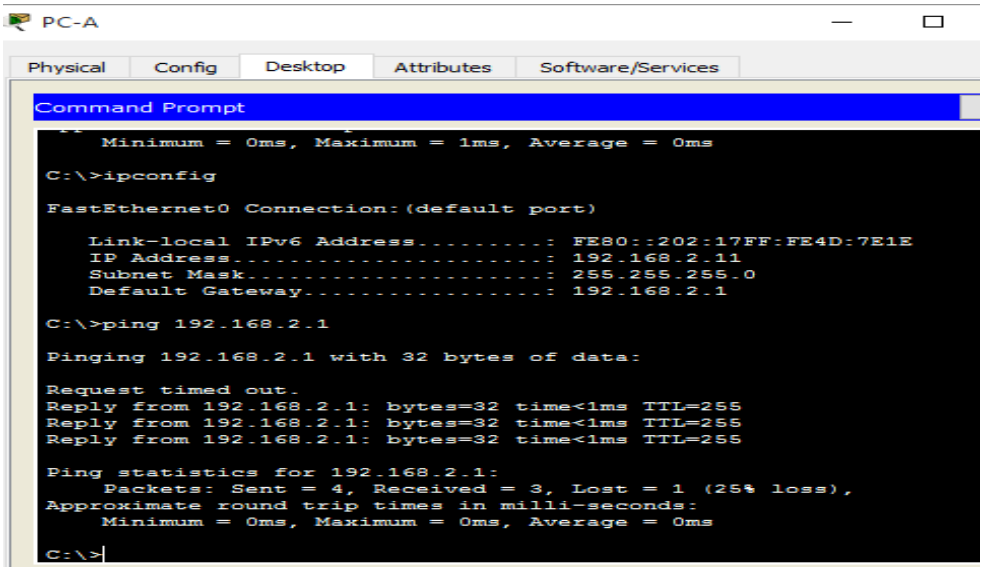
a. En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

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***

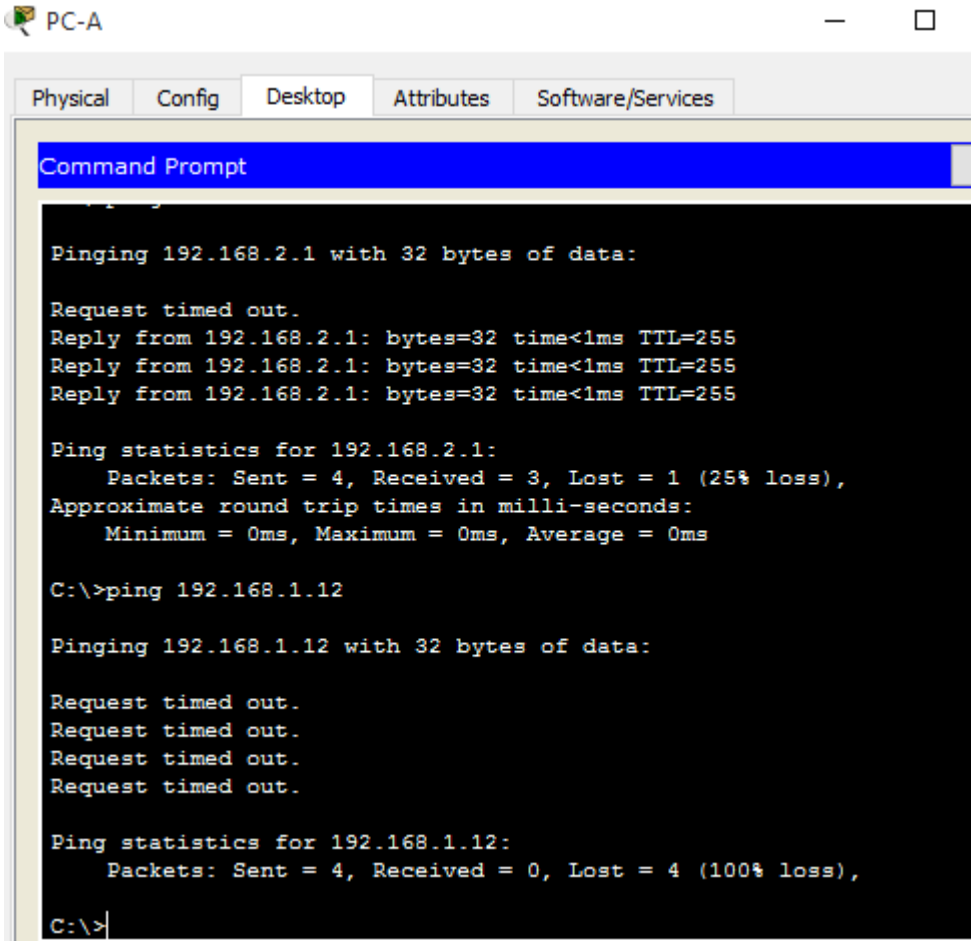


b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado de la VLAN 2 y a la PC-B.

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



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



¿Los pings eran correctos? ¿Por qué?

El ping al Gateway es satisfactorio desde la PC- A por estar en la misma red de la PC-A, caso contrario de la PC-B, por esta razón este segundo ping de PC-A a PC-B no lo fue.

c. Emita el comando **show ip route** en el S1. ¿Qué resultado arrojó este comando?

Dice que no hay puerta de enlace actualizada ni tabla de ruteo.

Parte 5: habilitar el routing IP

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

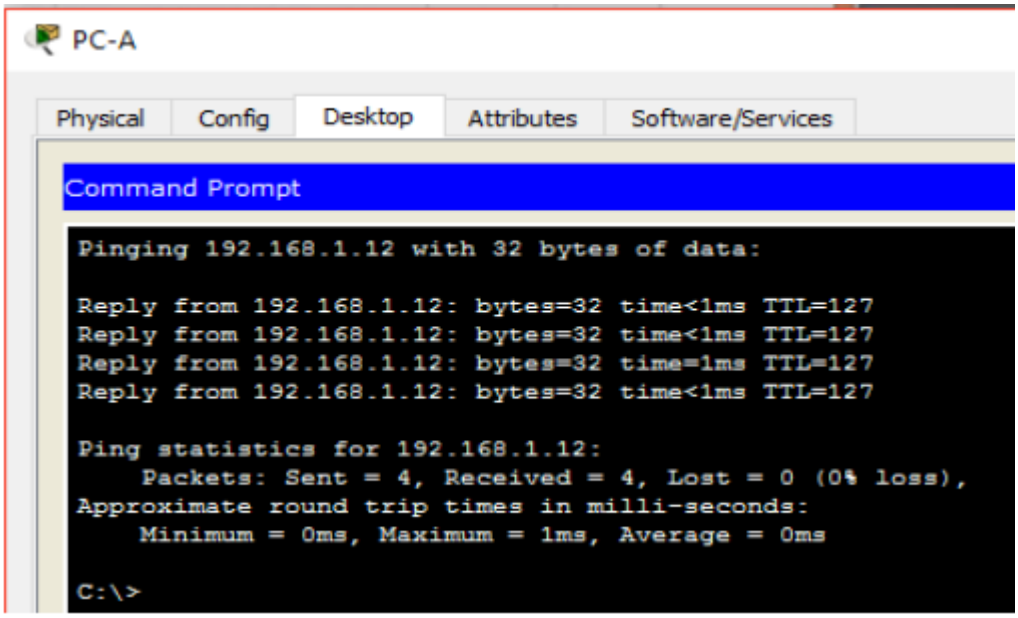
Paso 1: habilitar el routing IP en el S1.

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

S1(config)# **ip routing**

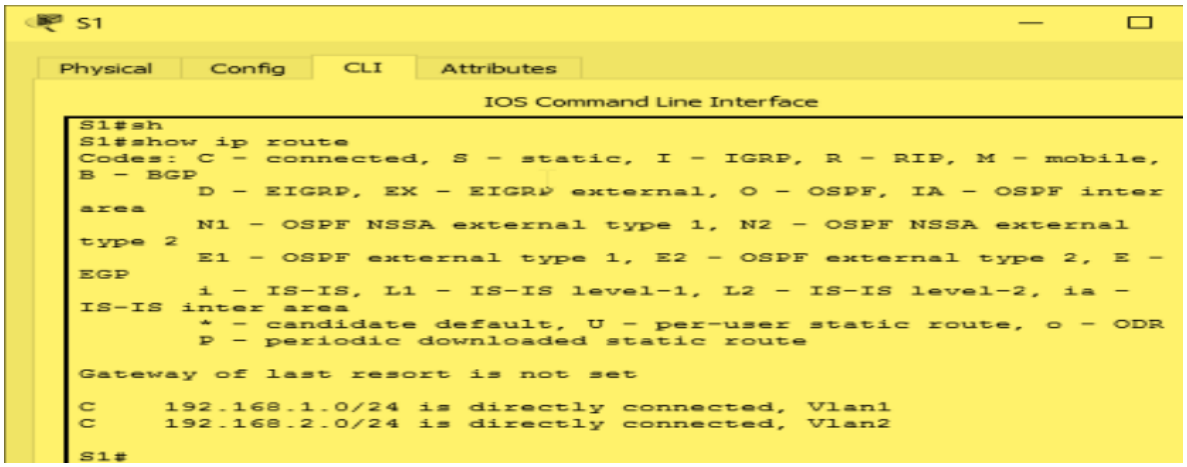
```
S1#configure ter
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip rout
S1(config)#ip routing
```

b. Verificar la conectividad entre las VLAN. ¿Es posible hacer ping de la PC-A a la PC-B? ***Satisfactorio***



¿Qué función realiza el switch?
Cumple la función de enrutador entre las Vlan

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



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

Se observan dos redes directamente conectadas (vlan 1 - 2).

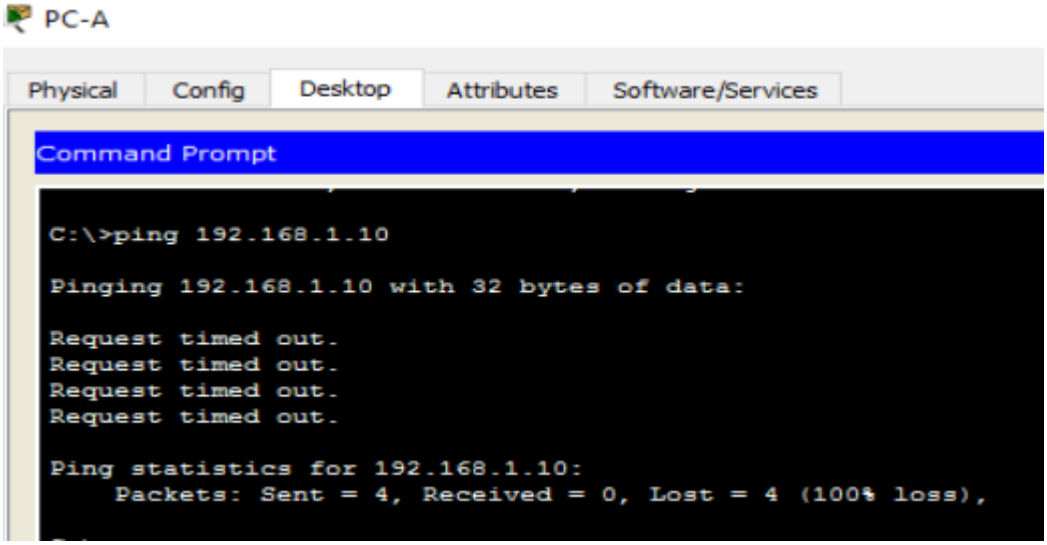
d. Vea la información de la tabla de routing para el R1.

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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.10/32 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
```

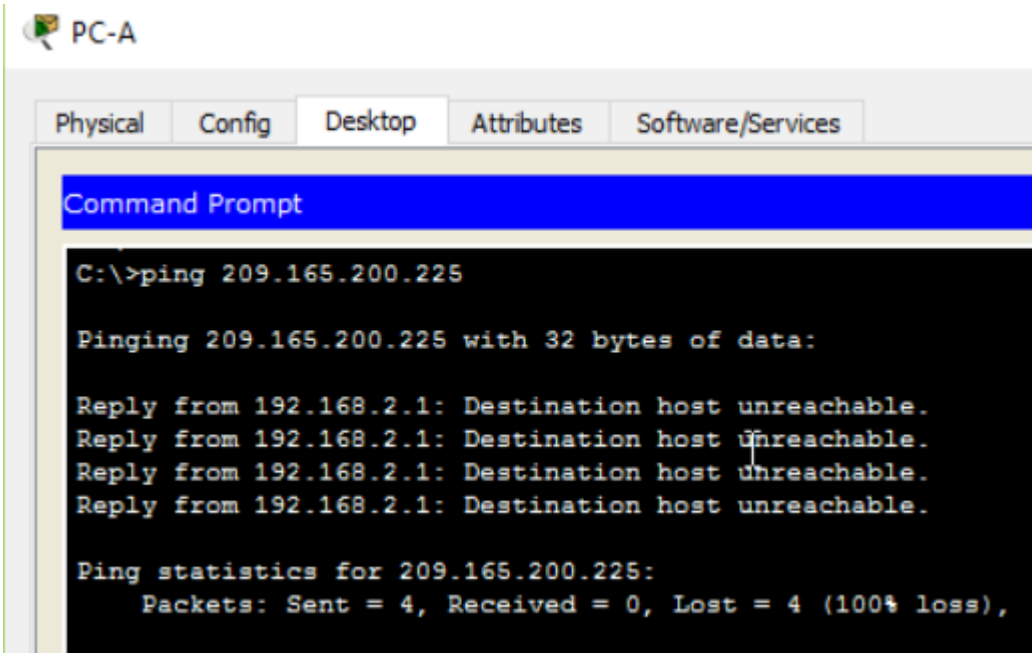
¿Qué información de la ruta está incluida en el resultado de este comando?

De igual forma que el S1 se muestran dos redes directamente conectadas, solo que este muestra la red 1 (192.168.1.0) y la publica 209.165.200.224, y no se evidencia la entrada para la red 2 (192.168.2.0).

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



f. ¿Es posible hacer ping de la PC-A a la interfaz Lo0? **No satisfactorio**



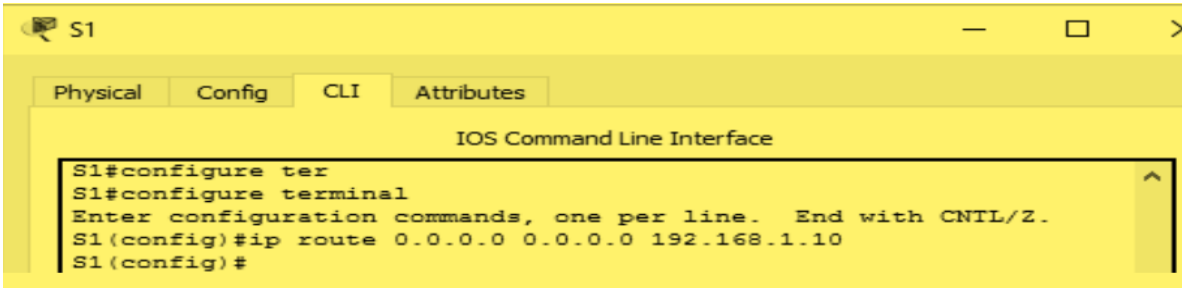
Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Se deben incluir todas las rutas en la tabla de ruteo para que se pueda garantizar esta comunicación.

Paso 2: Asignar rutas estáticas.

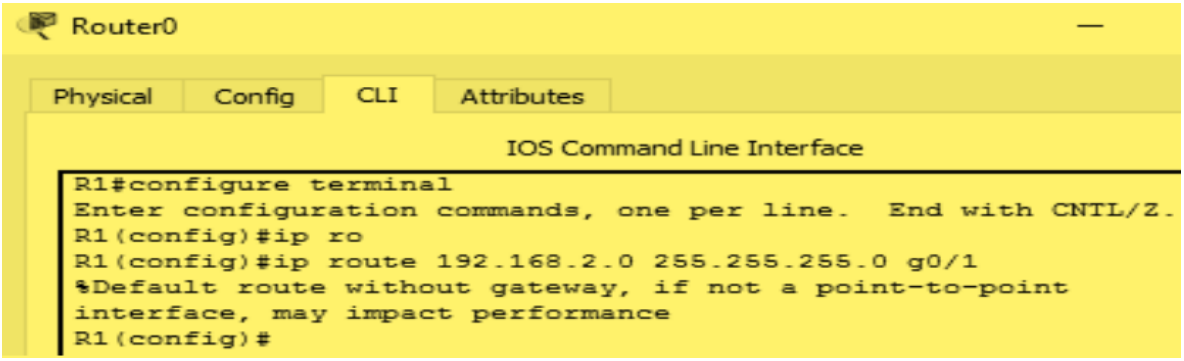
Habilitar el routing IP permite que el switch enrute entre VLAN asignadas en el switch. Para que todas las VLAN se comuniquen con el router, es necesario agregar rutas estáticas a la tabla de routing del switch y del router.

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



El comando es el visualizado en la imagen: **ip route ipv4 / mascara / ipv4 router**

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



El comando es el visualizado en la imagen: **ip route xxxxxx**

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

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

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

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

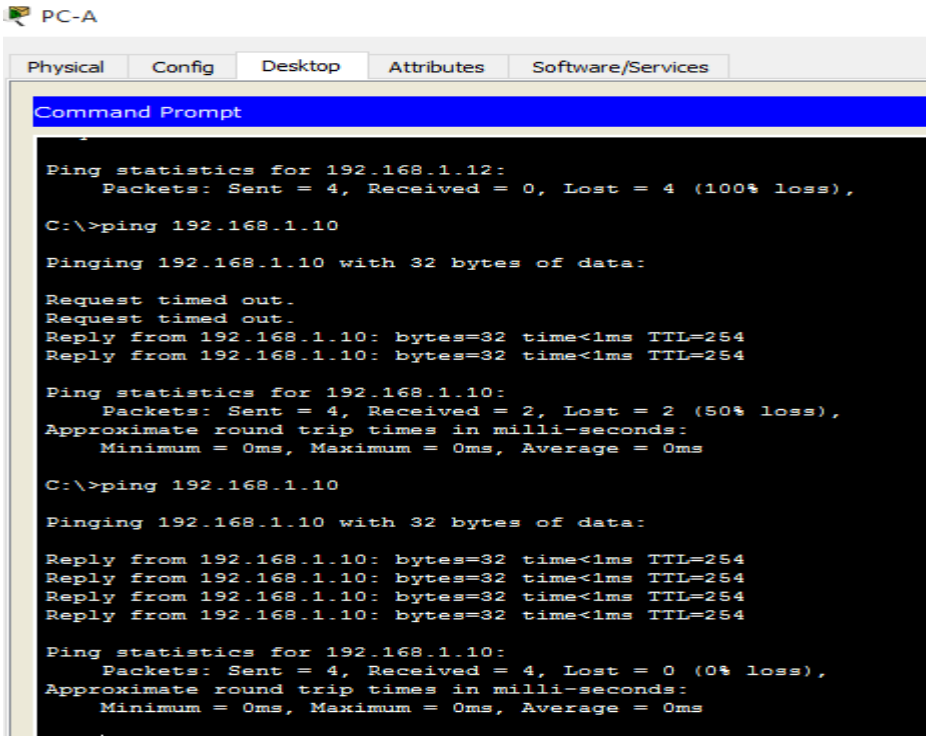
¿Cómo está representada la ruta estática predeterminada? Como: ***S* 0.0.0.0/0 [1/0] via 192.168.1.10***

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

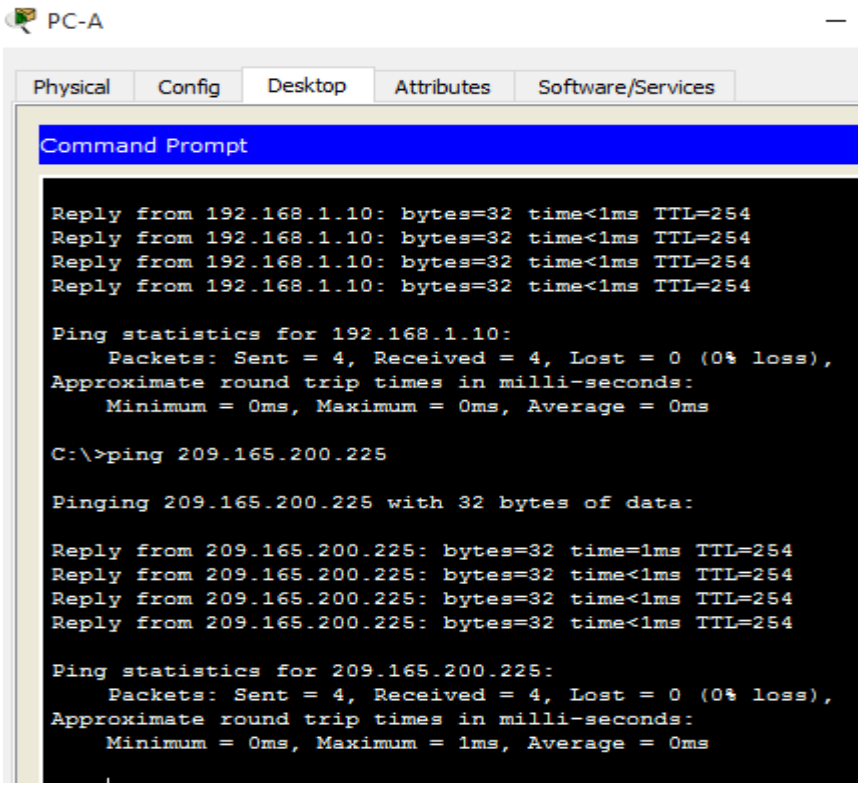
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.10/32 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
```

¿Cómo está representada la ruta estática? Como: ***S 192.168.2.0/24 is directly connected, GigabitEthernet0/1***

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



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



Reflexión

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

Por la ventana de tiempo que existe cuando se excluyen estas direcciones antes de crear el pool de direcciones y se podrían dar de forma dinámica hacia unos equipos finales (hosts).

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

Las asigna basándose en la vlan de cada vlan con relación a su puerto conectado.

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

Este switch puede tener funciones de dhcp, en mi caso para el ejercicio no lo use, use uno 3560 ya que el 2960 no me soportaba el comando ip route.

DESARROLLO EJERCICIO 10.2.3.5

Práctica de laboratorio: 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::1	64	No aplicable
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

Objetivos

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

Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Solo mediante configuración automática de dirección sin estado (SLAAC)
- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
- Mediante DHCPv6 con estado

Con SLAAC (se pronuncia “slaac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

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

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

Nota: la plantilla **default bias** que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla **dual-ipv4-and-ipv6** o la plantilla **lanbase-routing** en SDM.

La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

S1# **show sdm prefer**

```
Switch#show sdm prefer
 The current template is "desktop IPv4 and IPv6 default"
template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  2K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    3K
    number of directly-connected IPv4 hosts:        2K
    number of indirect IPv4 routes:                 1K
  number of IPv6 multicast groups:                  1.125k
  number of directly-connected IPv6 addresses:      2K
  number of indirect IPv6 unicast routes:           1K
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0.625k
  number of IPv6 security aces:                     0.5K
```

Siga estos pasos para asignar la plantilla **dual-ipv4-and-ipv6** como la plantilla de SDM predeterminada:

S1# **config t**

S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**

S1(config)# **end**

S1# **reload**

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#reload
```

Recursos necesarios

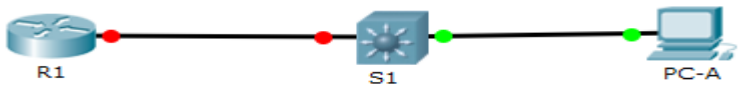
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para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

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

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

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

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



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

Paso 3. Configurar R1

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo.

c. Cifre las contraseñas de texto no cifrado.

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

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#anable secret class
           ^
% Invalid input detected at '^' marker.

R1(config)#enable secret class
R1(config)#service password-encryption
R1(config)#banner motd #EL acceso no autorizado esta prohibido#
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Paso 4. 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.

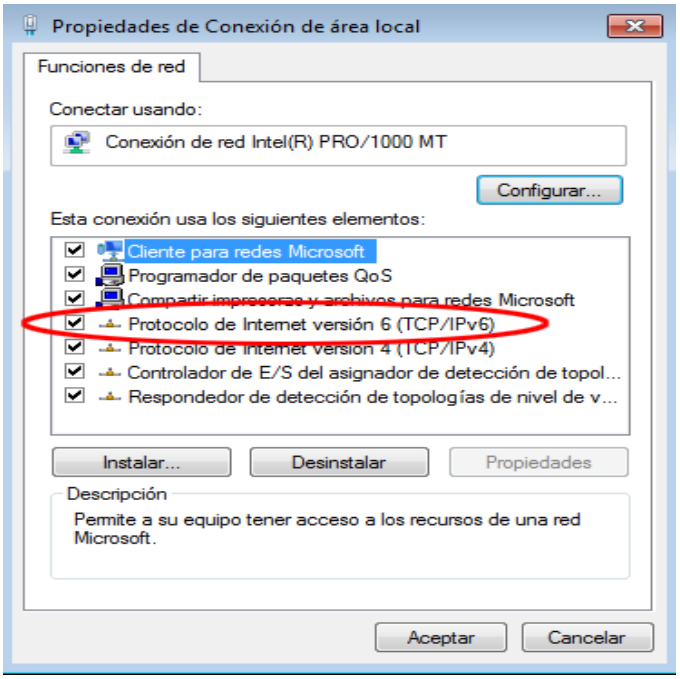
```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#service password-encryption
Switch(config)#banner motd #El acceso no autorizado esta
prohibido#
Switch(config)#enable secret class
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#logging synchronous
Switch(config-line)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

```
S1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES NVRAM  down                  down
FastEthernet0/2        unassigned      YES NVRAM  down                  down
FastEthernet0/3        unassigned      YES NVRAM  down                  down
FastEthernet0/4        unassigned      YES NVRAM  down                  down
FastEthernet0/5        unassigned      YES NVRAM  down                  down
FastEthernet0/6        unassigned      YES NVRAM  up                    up
FastEthernet0/7        unassigned      YES NVRAM  down                  down
FastEthernet0/8        unassigned      YES NVRAM  down                  down
FastEthernet0/9        unassigned      YES NVRAM  down                  down
FastEthernet0/10       unassigned      YES NVRAM  down                  down
FastEthernet0/11       unassigned      YES NVRAM  down                  down
FastEthernet0/12       unassigned      YES NVRAM  down                  down
FastEthernet0/13       unassigned      YES NVRAM  down                  down
FastEthernet0/14       unassigned      YES NVRAM  down                  down
FastEthernet0/15       unassigned      YES NVRAM  down                  down
FastEthernet0/16       unassigned      YES NVRAM  down                  down
FastEthernet0/17       unassigned      YES NVRAM  down                  down
FastEthernet0/18       unassigned      YES NVRAM  down                  down
FastEthernet0/19       unassigned      YES NVRAM  down                  down
FastEthernet0/20       unassigned      YES NVRAM  down                  down
FastEthernet0/21       unassigned      YES NVRAM  down                  down
FastEthernet0/22       unassigned      YES NVRAM  down                  down
FastEthernet0/23       unassigned      YES NVRAM  down                  down
FastEthernet0/24       unassigned      YES NVRAM  down                  down
GigabitEthernet0/1     unassigned      YES NVRAM  down                  down
GigabitEthernet0/2     unassigned      YES NVRAM  down                  down
Vlan1                  unassigned      YES NVRAM  administratively down down
S1#
```

Parte 2. Configurar la red para SLAAC

Paso 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.

Paso 2. Configurar R1

a. Habilite el routing de unidifusión IPv6.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 unicast-routing
```

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

```
R1(config)#int g0/1
R1(config-if)#ipv6 add 2001:db8:acad:a::1/64
R1(config-if)#
```

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

```
R1(config-if)#ipv6 add  fe80::1 link-local
```

d. Active la interfaz G0/1.

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

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
```

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

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

R1# **show ipv6 interface g0/1**

```
R1#show ipv6 int 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
  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.
```

Paso 4. Configurar el S1.

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

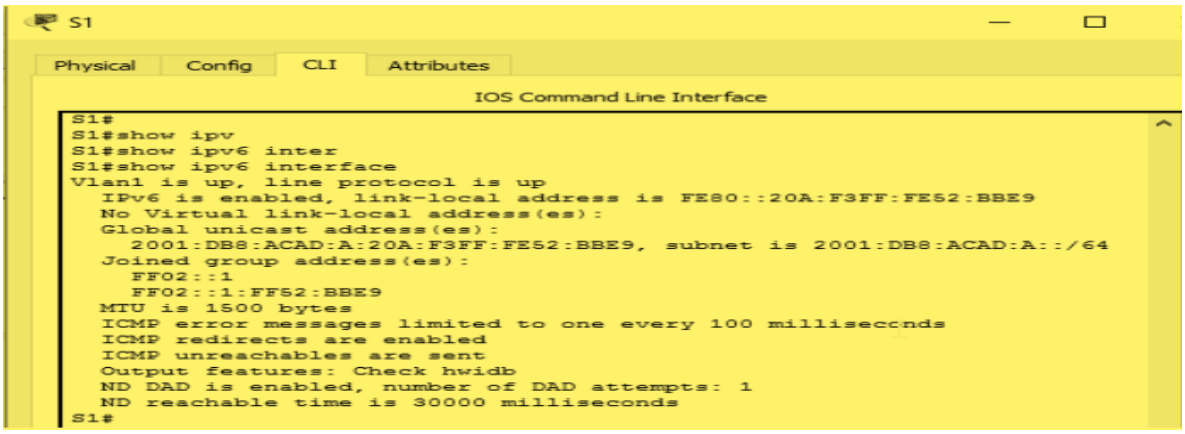
S1(config)# **interface vlan 1**
S1(config-if)# **ipv6 address autoconfig**
S1(config-if)# **end**

```
S1(config)#int vlan 1
S1(config-if)#ipv6 add autoconfig
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

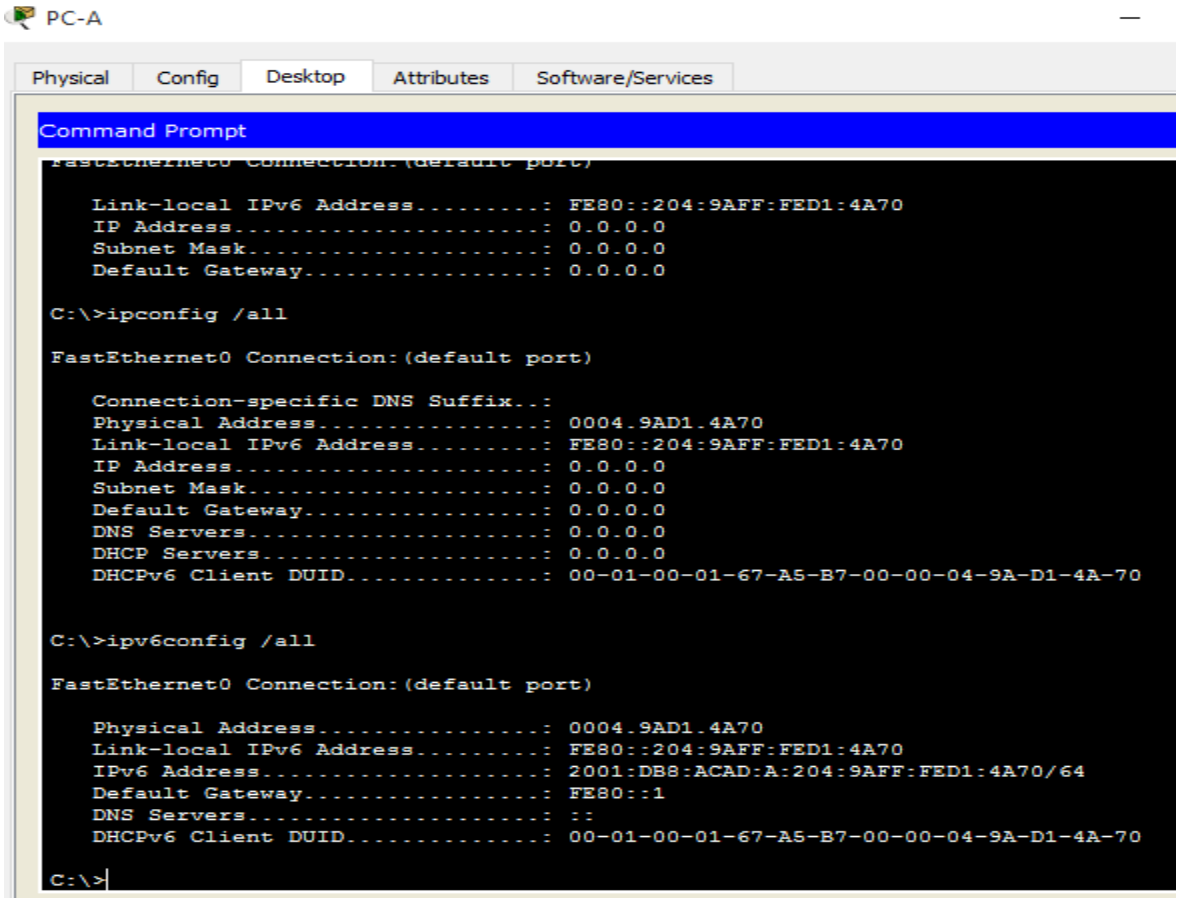
Use el comando **show ipv6 interface** para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

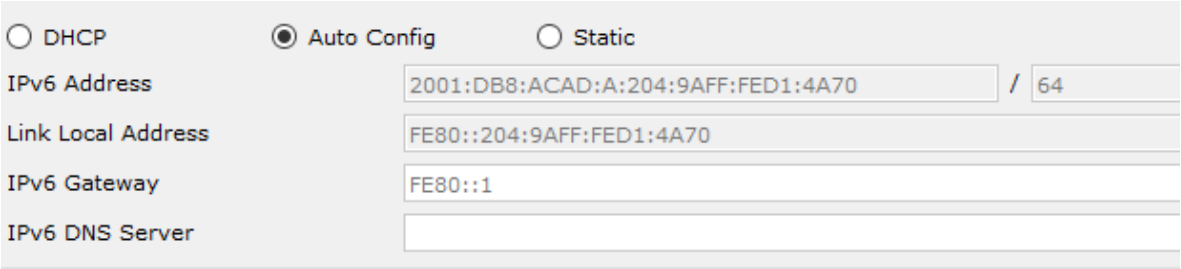
S1# **show ipv6 interface**



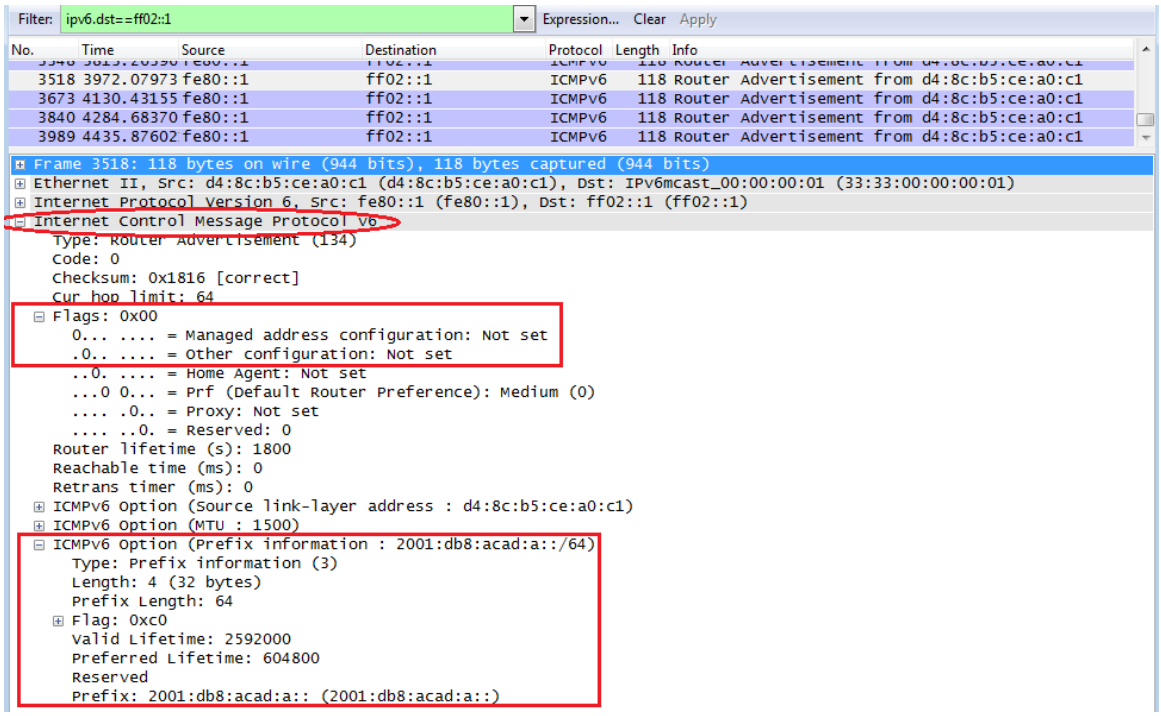
Paso 6. verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

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





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



Parte 3. Configurar la red para DHCPv6 sin estado

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

a. Cree un pool de DHCP IPv6.

R1(config)# **ipv6 dhcp pool IPV6POOL-A**

```
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#
```

b. Asigne un nombre de dominio al pool.

R1(config-dhcpv6)# **domain-name ccna-statelessDHCPv6.com**

```
R1(config-dhcpv6)#domain-name ccna-statelessDHCPV6.com
R1(config-dhcpv6)#
```

c. Asigne una dirección de servidor DNS.

R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**
R1(config-dhcpv6)# **exit**

```
R1(config-dhcpv6)#dns-server 2001:db8:acad:a::abcd
R1(config-dhcpv6)#exit
R1(config)#
```

d. Asigne el pool de DHCPv6 a la interfaz.

R1(config)# **interface g0/1**
R1(config-if)# **ipv6 dhcp server IPV6POOL-A**

```
R1(config)#int g0/1
R1(config-if)#ipv6 dhcp server IPV6POOL-A
R1(config-if)#
```

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

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

```
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 2. Verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

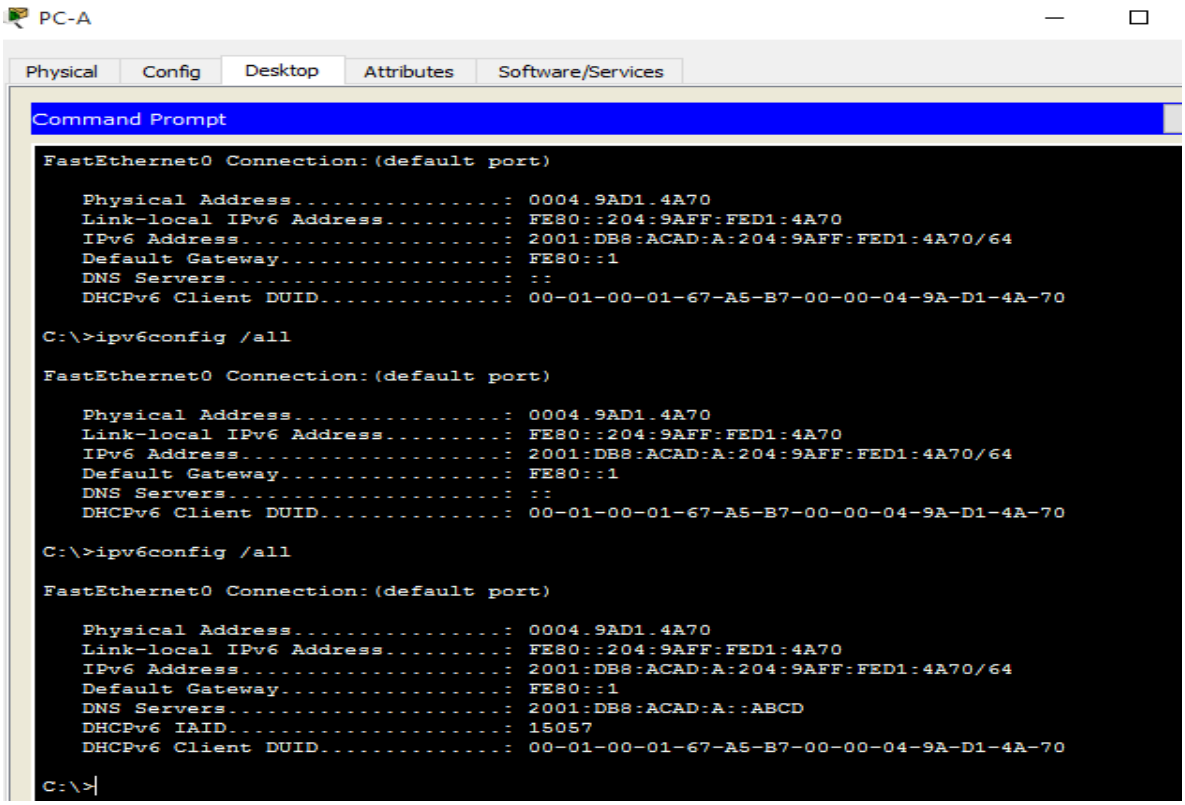
Use el comando **show ipv6 interface g0/1** para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando **show** verifica que se haya establecido other-config-flag.

R1# **show ipv6 interface g0/1**

```
R1#show ipv6 int 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
  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
  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.
```

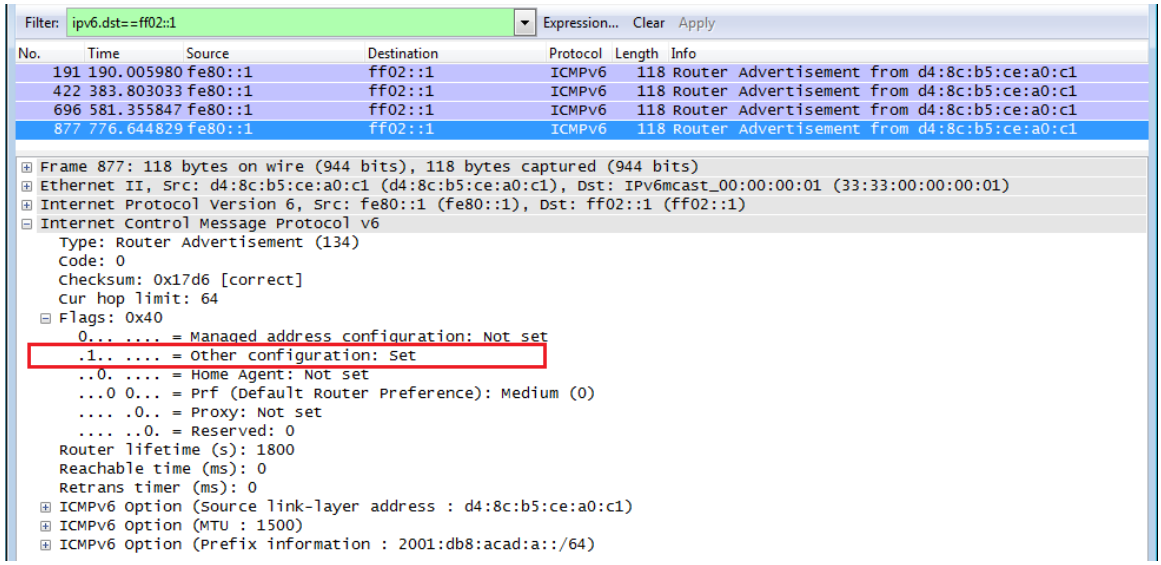
Paso 3. Ver los cambios realizados en la red en la PC-A.

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



Paso 4. ver los mensajes RA en Wireshark.

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



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

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

R1# **show ipv6 dhcp binding**
R1# **show ipv6 dhcp pool**

```
R1#show ipv6 dhcp binding
Client:  (GigabitEthernet0/1)
  DUID: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
  IA PD: IA ID 15057, T1 0, T2 0
    Prefix: 0.0.0.0/0
            preferred lifetime 0, valid lifetime 0
            expires at Noviembre 22 2017 8:26:37 pm (0 seconds)
```

```
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-statelessDHCPV6.com
  Active clients: 0
```

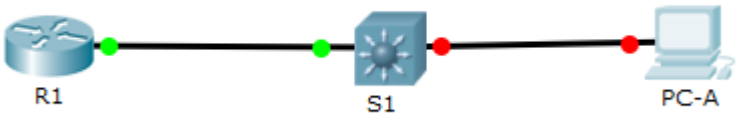
Paso 6. Restablecer la configuración de red IPv6 de la PC-A.

a. Desactive la interfaz F0/6 del S1.

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

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

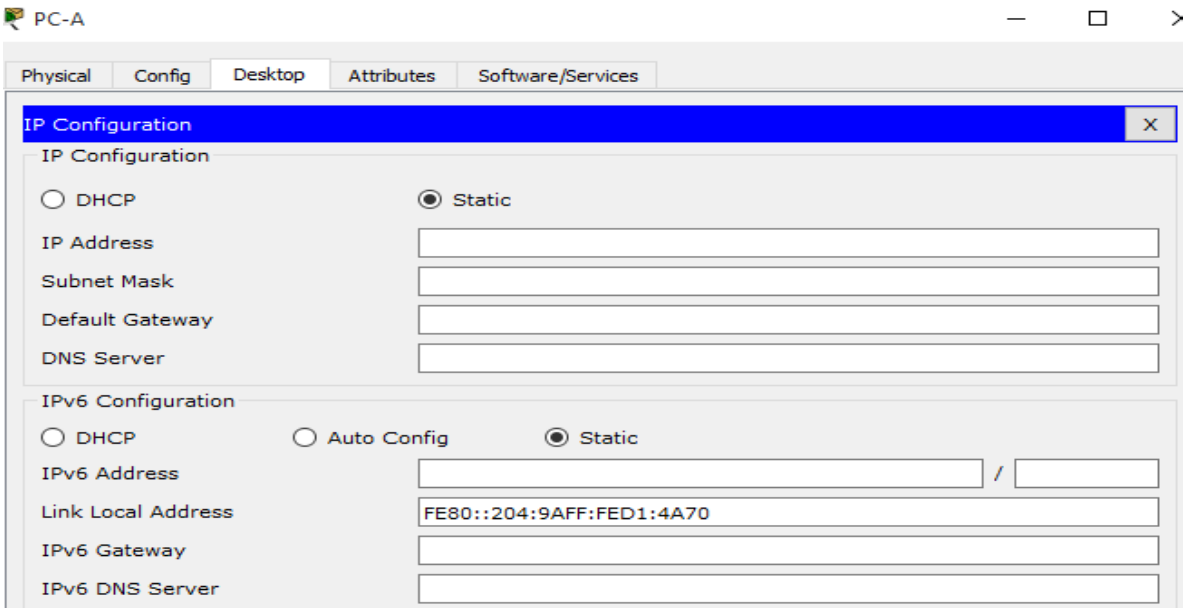
```
S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
changed state to down
```

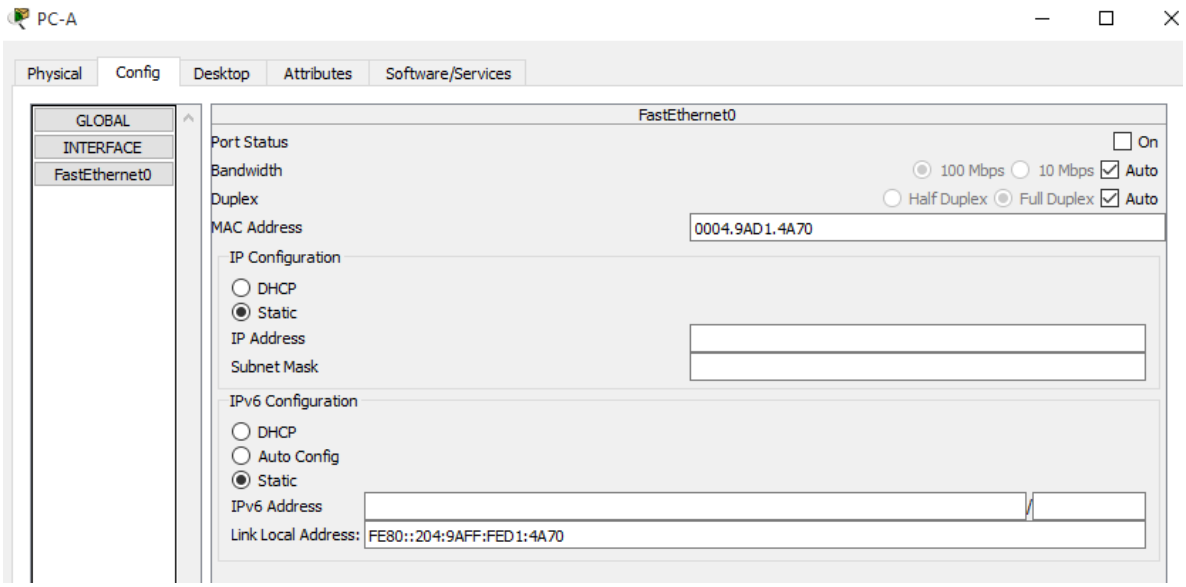


b. Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.

c. Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.

1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.





2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) y, a continuación, haga clic en Aceptar para aceptar el cambio. configurar la red para DHCPv6 con estado

Parte 4 configurar la red para DHCPv6 con estado

Paso 1. Preparar la PC-A.

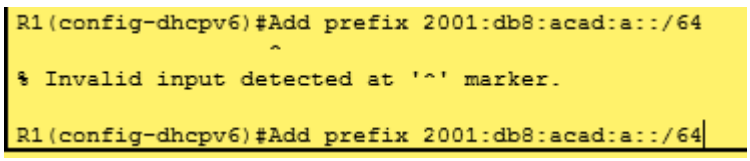
a. Inicie una captura del tráfico en la NIC con Wireshark.

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

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

a. Agregue el prefijo de red al pool.

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



Nota:

El comando no es soportado por packet tracer

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

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

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

```
R1(config-dhcpv6)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

c. Verifique la configuración del pool de DHCPv6.

R1# **show ipv6 dhcp pool**

```
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**

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

Paso 3. Establecer el indicador en G0/1 para DHCPv6 con estado.

Nota: la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.
R1(config)# **interface g0/1**
R1(config-if)# **shutdown**

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

```
R1(config-if)#IPV6 nd managed-config-flag
R1(config-if)#no shu

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#
```

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

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

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

```
S1(config)#int f0/6
S1(config-if)#no shu

%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#
```

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

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

R1# **show ipv6 interface g0/1**

```
R1#show ipv6 int 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::1:2
    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
  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.
```

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.

Nota:

No se pudo asignar una ipv6 unicast por lo que ese comando no se soportó en el punto a, Parte 4, paso 2.

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

R1# **show ipv6 dhcp pool**

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

Nota:

El resultado debería ser 1 como clientes activos, por no haber soportado la asignación de la pv6 unicast no aparece ninguno.

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**

```
R1#show ipv6 dhcp binding
Client:  (GigabitEthernet0/1)
  DUID: 00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
  IA PD: IA ID 15057, T1 0, T2 0
    Prefix: 0.0.0.0/0
            preferred lifetime 0, valid lifetime 0
            expires at Noviembre 22 2017 8:59:10 pm (0 seconds)
```

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

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

R1# **u all**

Se ha desactivado toda depuración posible

```
R1#u 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. 1 03:42:13.467:     elapsed-time 0
*Mar. 1 03:42:13.467:   option CLIENTID(1), len 45
*Mar. 1 03:42:13.467:     00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:13.467:   option ORO(6), len 10
*Mar. 1 03:42:13.467:     IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 03:42:13.467:   option IA-PD(25), len 16
*Mar. 1 03:42:13.467:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:13.467: IPv6 DHCP: Using interface pool IPV6POOL-A

*Mar. 1 03:42:13.467: IPv6 DHCP: Sending ADVERTISE to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:13.467: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:13.467:   src FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467:   dst FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467:   type ADVERTISE(2), xid 4
*Mar. 1 03:42:13.467:   option SERVERID(2), len 24
*Mar. 1 03:42:13.467:     0003000100902B731501
*Mar. 1 03:42:13.467:   option CLIENTID(1), len 45
*Mar. 1 03:42:13.467:     00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:13.467:   option IA-PD(25), len 45
*Mar. 1 03:42:13.467:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:13.467:     option IAPREFIX(26), 29
*Mar. 1 03:42:13.467:       preferred 0, valid 0, prefix 0.0.0.0/0

*Mar. 1 03:42:13.467: IPv6 DHCP: Received REQUEST from FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:13.467: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:13.467:   src FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467:   dst FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467:   type REQUEST(3), xid 2
*Mar. 1 03:42:13.467:   option ELAPSED-TIME(8), len 6
*Mar. 1 03:42:13.467:     elapsed-time 0
*Mar. 1 03:42:13.467:   option SERVERID(2), len 24
*Mar. 1 03:42:13.467:     0003000100902B731501
*Mar. 1 03:42:13.467:   option CLIENTID(1), len 45
*Mar. 1 03:42:13.467:     00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:13.467:   option ORO(6), len 10
*Mar. 1 03:42:13.467:     IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 03:42:13.467:   option IA-PD(25), len 45
*Mar. 1 03:42:13.467:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:13.467:     option IAPREFIX(26), 29
*Mar. 1 03:42:13.467:       preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 03:42:13.467: IPv6 DHCP: Using interface pool IPV6POOL-A
*Mar. 1 03:42:13.467: IPv6 DHCP: Creating binding for FE80::204:9AFF:FED1:4A70 in pool IPV6POOL-A
*Mar. 1 03:42:13.467: IPv6 DHCP: Allocating IA_PD 15057 in binding for FE80::204:9AFF:FED1:4A70
*Mar. 1 03:42:13.467: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for FE80::204:9AFF:FED1:4A70, IAID 15057

*Mar. 1 03:42:13.467: IPv6 DHCP: Sending REPLY to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:13.467: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:13.467:   src FE80::1 (GigabitEthernet0/1)
```

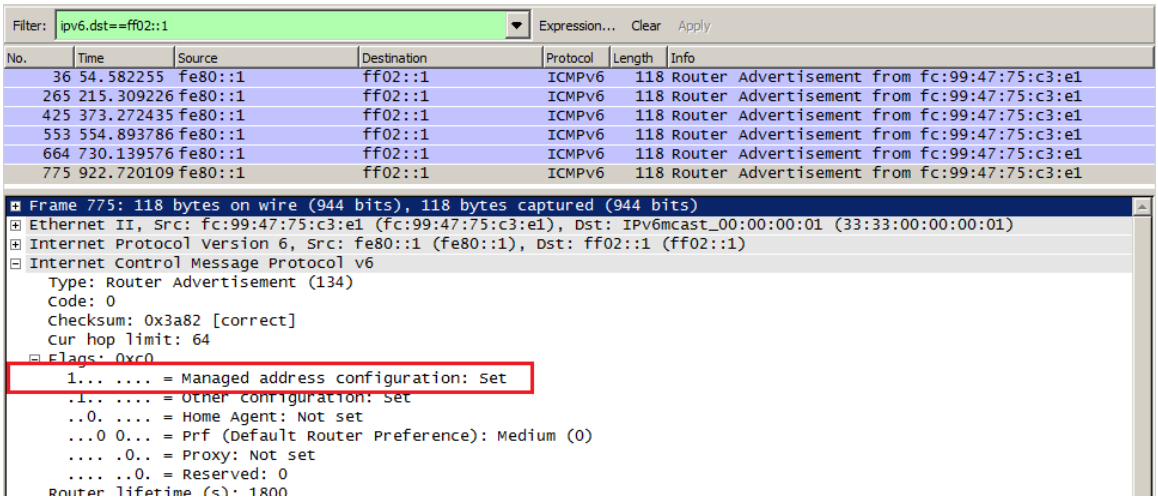
```
*Mar. 1 03:42:13.467: IPv6 DHCP: Sending REPLY to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:13.467: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:13.467:   src FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467:   dst FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:13.467:   type REPLY(7), xid 2
*Mar. 1 03:42:13.467:   option SERVERID(2), len 24
*Mar. 1 03:42:13.467:     00030001100902B731501
*Mar. 1 03:42:13.467:   option CLIENTID(1), len 45
*Mar. 1 03:42:13.467:     00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:13.467:   option IA-PD(25), len 41
*Mar. 1 03:42:13.467:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:13.467:     option IAPREFIX(26), 29
*Mar. 1 03:42:13.467:       preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 03:42:13.467:   option DNS-SERVERS(23), len 20
*Mar. 1 03:42:13.467:     2001:DB8:ACAD:A::ABCD
*Mar. 1 03:42:13.467:   option DOMAIN-LIST(24), len 5
*Mar. 1 03:42:13.467:     ccna-StatefulDHCPv6.com

*Mar. 1 03:42:20.981: IPv6 DHCP: Received SOLICIT from FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:20.981: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:20.981:   src FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:20.981:   dst FF02::1:2 (GigabitEthernet0/1)
*Mar. 1 03:42:20.981:   type SOLICIT(1), xid 5
*Mar. 1 03:42:20.981:   option ELAPSED-TIME(8), len 6
*Mar. 1 03:42:20.981:     elapsed-time 0
*Mar. 1 03:42:20.981:   option CLIENTID(1), len 45
*Mar. 1 03:42:20.981:     00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:20.981:   option ORO(6), len 10
*Mar. 1 03:42:20.981:     IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 03:42:20.981:   option IA-PD(25), len 16
*Mar. 1 03:42:20.981:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:20.981: IPv6 DHCP: Using interface pool IPV6POOL-A

*Mar. 1 03:42:20.981: IPv6 DHCP: Sending ADVERTISE to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:20.981: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:20.981:   src FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:20.981:   dst FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:20.981:   type ADVERTISE(2), xid 5
*Mar. 1 03:42:20.981:   option SERVERID(2), len 24
*Mar. 1 03:42:20.981:     00030001100902B731501
*Mar. 1 03:42:20.981:   option CLIENTID(1), len 45
*Mar. 1 03:42:20.981:     00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:20.981:   option IA-PD(25), len 45
*Mar. 1 03:42:20.981:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:20.981:     option IAPREFIX(26), 29
*Mar. 1 03:42:20.981:       preferred 0, valid 0, prefix 0.0.0.0/0
```

```
*Mar. 1 03:42:23.515: IPv6 DHCP: Received REQUEST from FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:23.515: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:23.515:   src FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:23.515:   dst FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:23.515:   type REQUEST(3), xid 4
*Mar. 1 03:42:23.515:   option ELAPSED-TIME(8), len 6
*Mar. 1 03:42:23.515:     elapsed-time 0
*Mar. 1 03:42:23.515:   option SERVERID(2), len 24
*Mar. 1 03:42:23.515:     00030001100902B731501
*Mar. 1 03:42:23.515:   option CLIENTID(1), len 45
*Mar. 1 03:42:23.515:     00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:23.515:   option ORO(6), len 10
*Mar. 1 03:42:23.515:     IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 03:42:23.515:   option IA-PD(25), len 45
*Mar. 1 03:42:23.515:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:23.515:     option IAPREFIX(26), 29
*Mar. 1 03:42:23.515:       preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 03:42:23.515: IPv6 DHCP: Using interface pool IPV6POOL-A
*Mar. 1 03:42:23.515: IPv6 DHCP: Creating binding for FE80::204:9AFF:FED1:4A70 in pool IPV6POOL-A
*Mar. 1 03:42:23.515: IPv6 DHCP: Allocating IA_PD 15057 in binding for FE80::204:9AFF:FED1:4A70
*Mar. 1 03:42:23.515: IPv6 DHCP: Allocating prefix 0.0.0.0/0 in binding for FE80::204:9AFF:FED1:4A70, IAID 15057

*Mar. 1 03:42:23.515: IPv6 DHCP: Sending REPLY to FE80::204:9AFF:FED1:4A70 on GigabitEthernet0/1
*Mar. 1 03:42:23.515: IPv6 DHCP: detailed packet contents
*Mar. 1 03:42:23.515:   src FE80::1 (GigabitEthernet0/1)
*Mar. 1 03:42:23.515:   dst FE80::204:9AFF:FED1:4A70 (GigabitEthernet0/1)
*Mar. 1 03:42:23.515:   type REPLY(7), xid 4
*Mar. 1 03:42:23.515:   option SERVERID(2), len 24
*Mar. 1 03:42:23.515:     00030001100902B731501
*Mar. 1 03:42:23.515:   option CLIENTID(1), len 45
*Mar. 1 03:42:23.515:     00-01-00-01-67-A5-B7-00-00-04-9A-D1-4A-70
*Mar. 1 03:42:23.515:   option IA-PD(25), len 41
*Mar. 1 03:42:23.515:     IAID 0x15057, T1 0, T2 0
*Mar. 1 03:42:23.515:     option IAPREFIX(26), 29
*Mar. 1 03:42:23.515:       preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 03:42:23.515:   option DNS-SERVERS(23), len 20
*Mar. 1 03:42:23.515:     2001:DB8:ACAD:A::ABCD
*Mar. 1 03:42:23.515:   option DOMAIN-LIST(24), len 5
*Mar. 1 03:42:23.515:     ccna-StatefulDHCPv6.com
```

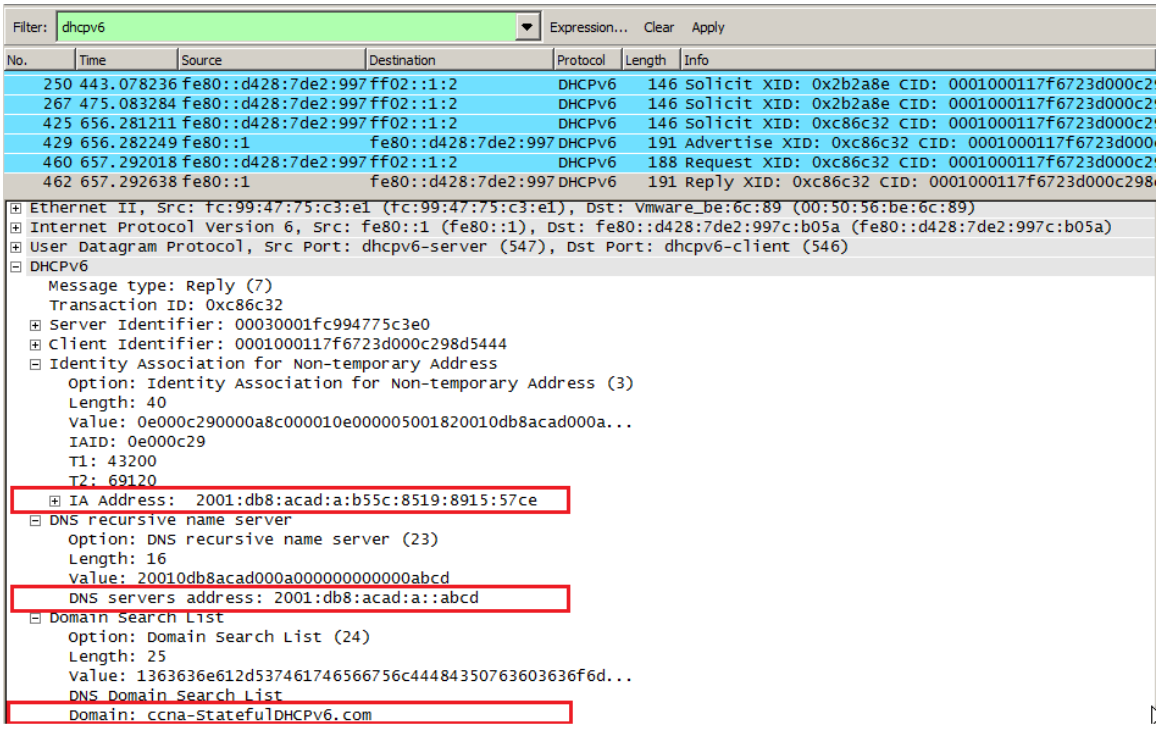
Paso 6. Verificar DHCPv6 con estado en la PC-A.

a. Detenga la captura de Wireshark en la PC-A.

b. Expanda el mensaje RA más reciente que se indica en Wireshark. Verifique que se haya establecido el indicador **Managed address configuration** (Configuración de dirección administrada).



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.



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?

DHCPv6 con estado utiliza más memoria porque almacena dinámicamente en el router información de los clientes.

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

El tipo de dirección recomendada DHCPv6 es sin estado, por la implementación de redes ipv6 sin necesidad de registro de red cisco.

DESARROLLO EJERCICIO 10.3.1.1

IdT y DHCP

Objetivo

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

Situación y Desarrollo

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:

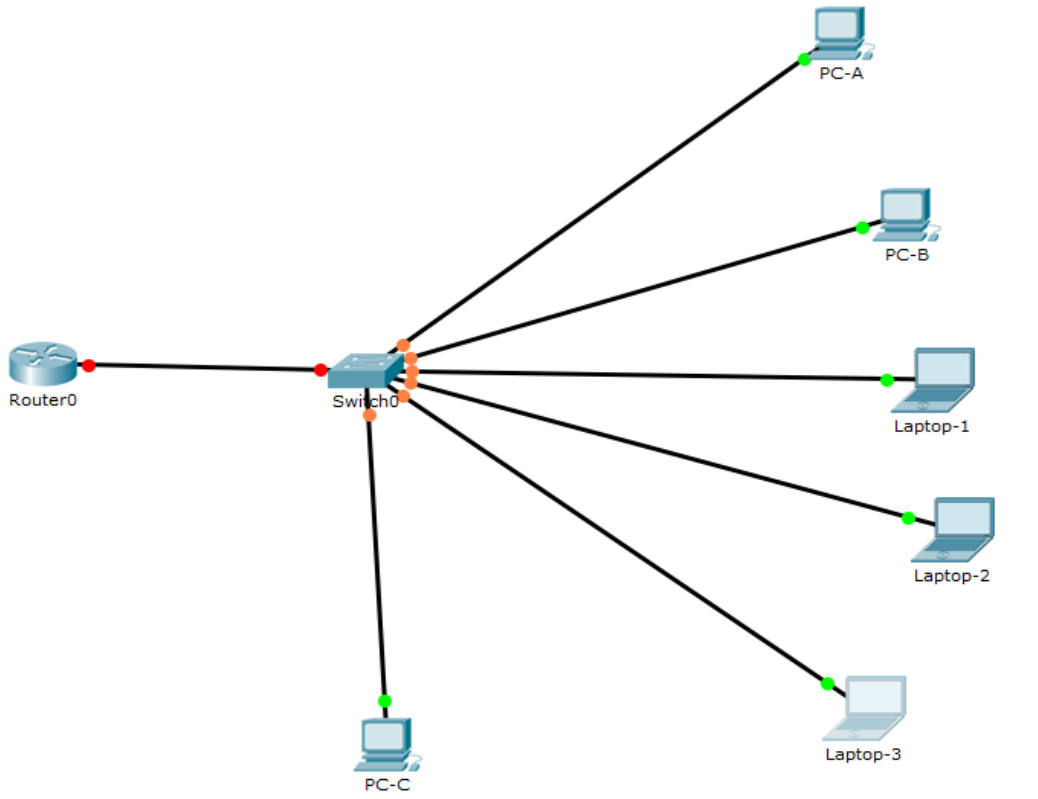
- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.

Se asigna un rango de direcciones al R1 para las direcciones a ser asignadas a los clientes que se conectaran a través de DHCP.

Nota:

Se le asignaran todos los parámetros de configuración al R1 y S1, claves de modo EXE privilegiado class y configuración global cisco.

Desarrollo:



- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #El acceso no autorizado esta prohibido#
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Asignación de rango a R1 para direcciones a ser asignadas a clientes por DHCP y configuraciones para DHCP.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp exclude-add 192.168.1.2 192.168.1.12
                               ^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp excluded-add 192.168.1.2 192.168.1.12
R1(config)#ip dhcp pool JSDP
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#int g0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shu

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)#
```

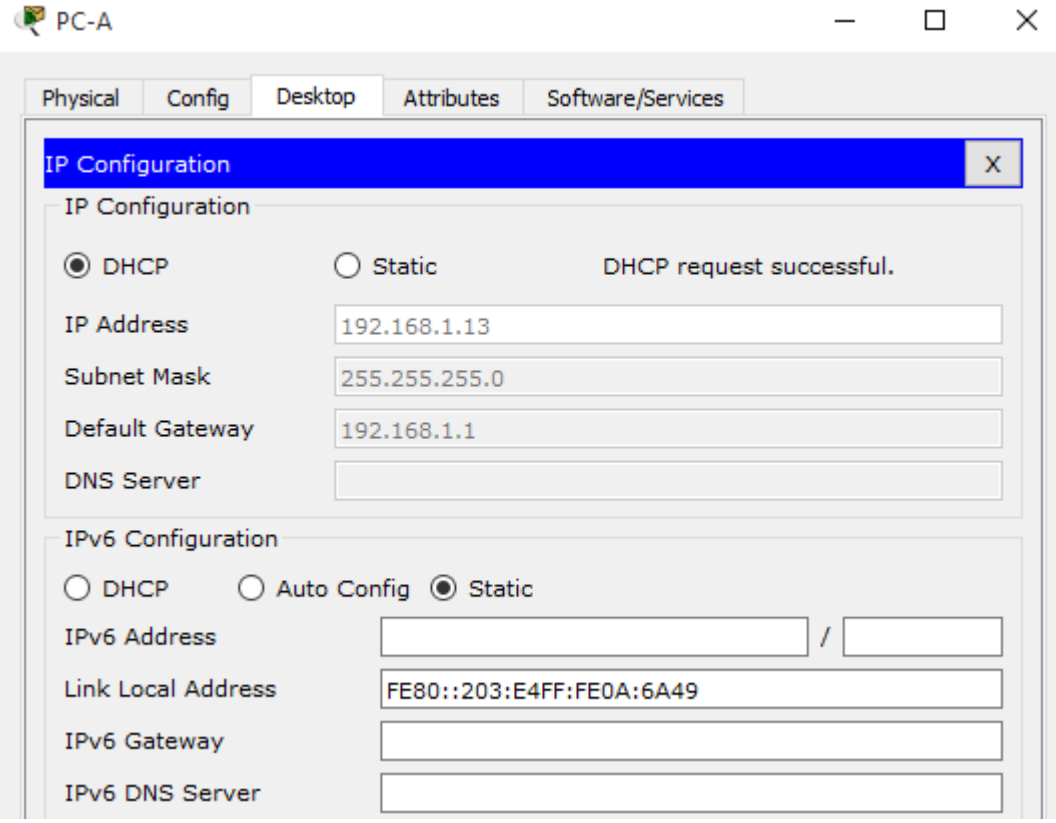
Configuración de parámetros DHCP S1 – puertos modo Trunk

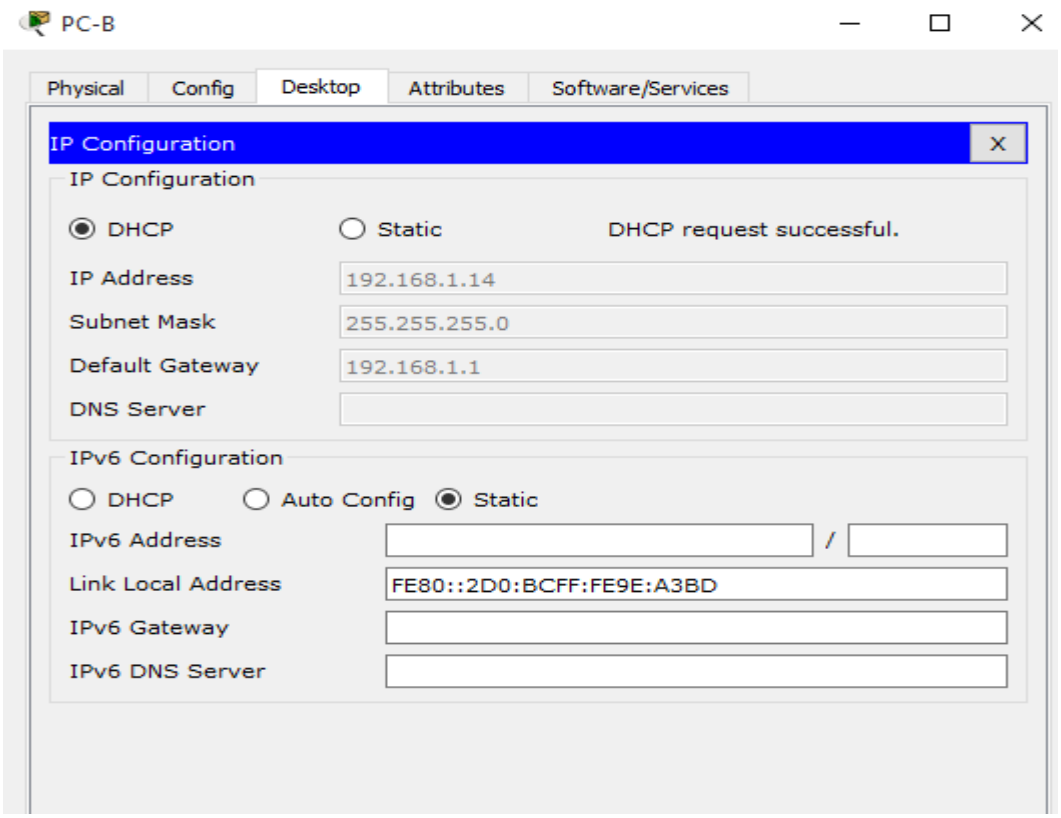
```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#int g0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down

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

S1(config-if)#no shu
S1(config-if)#
```

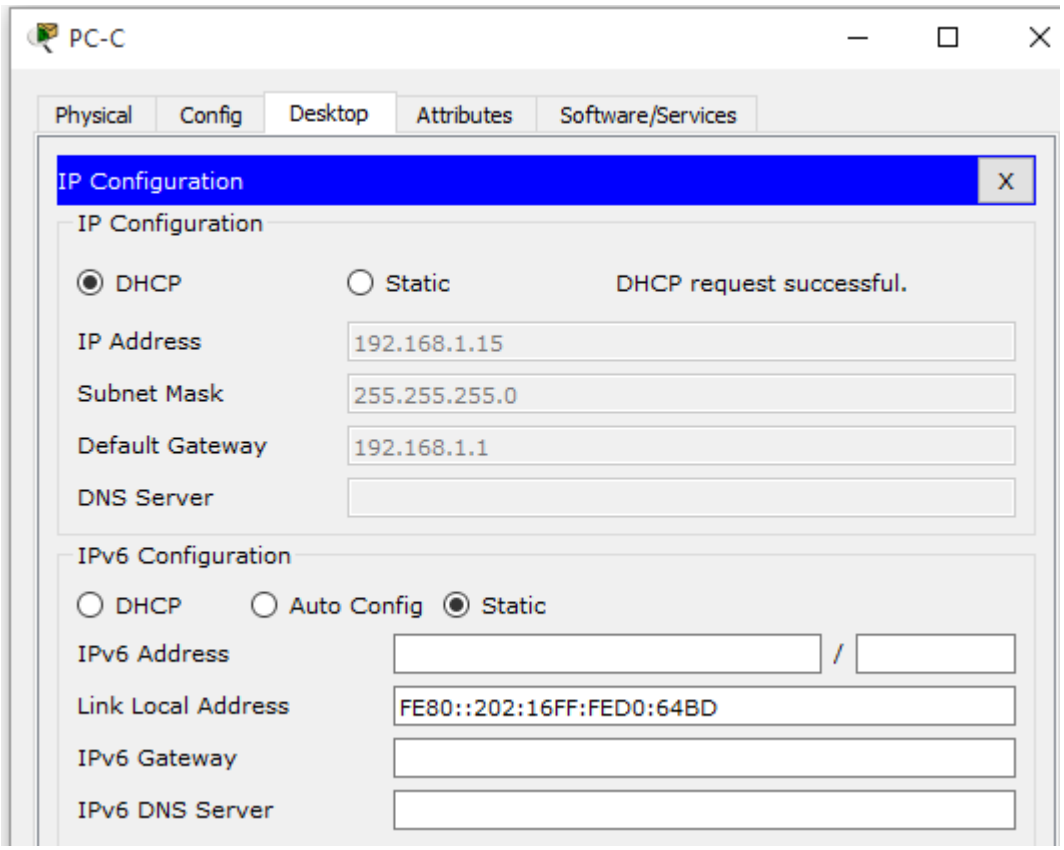
- Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones DHCP del servidor de DHCP.

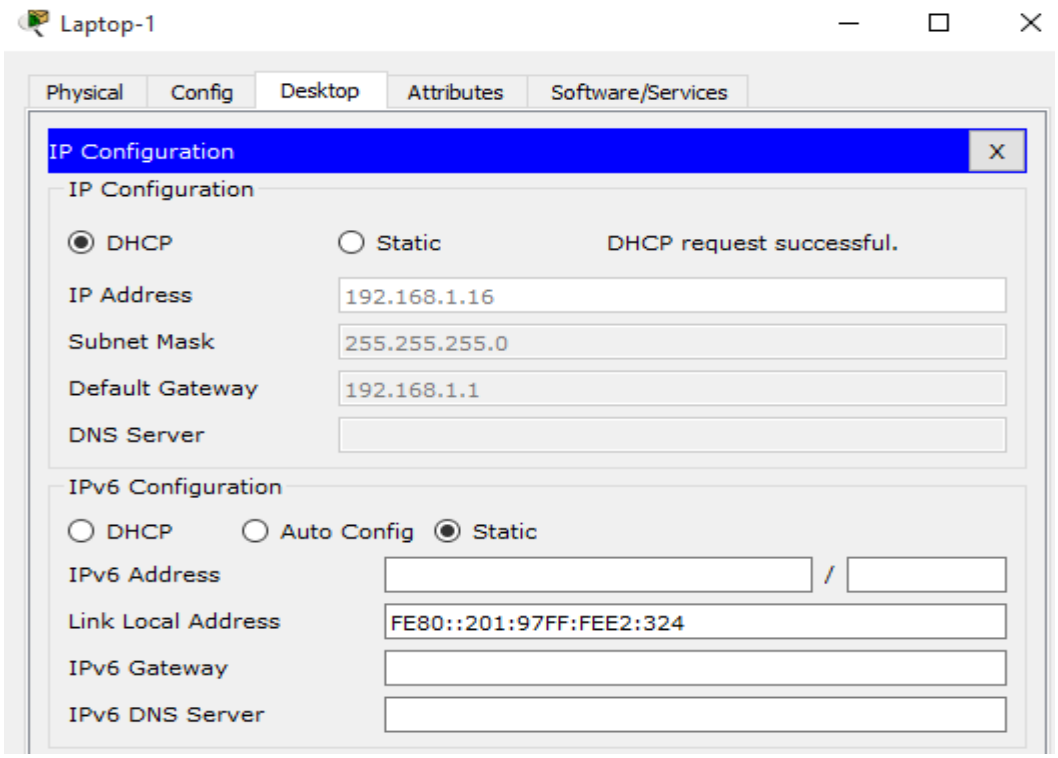
• Muestre los resultados que validen que cada terminal garantiza una dirección IP del servidor. Utilice un programa de captura de pantalla para guardar la información del resultado o emplee el comando de la tecla ImprPant.

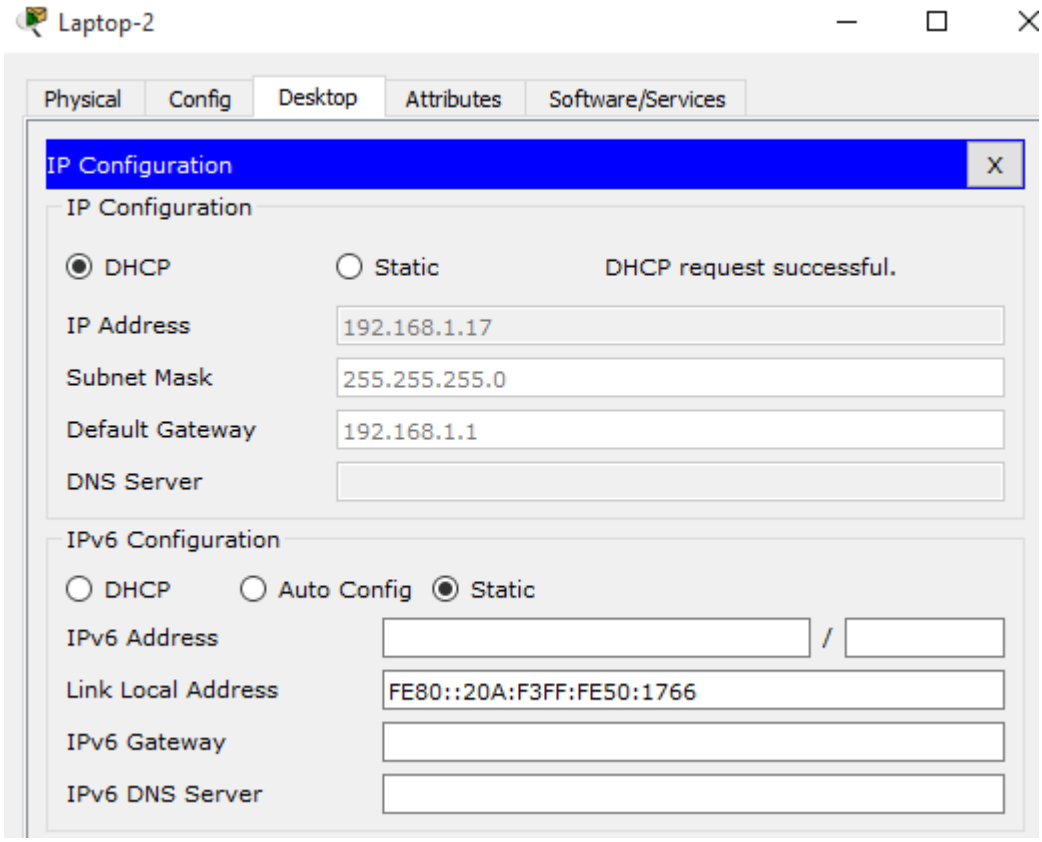
Se evidencia la asignación de direcciones de rango asignado DHCP a los equipos hosts terminales (usuarios finales):

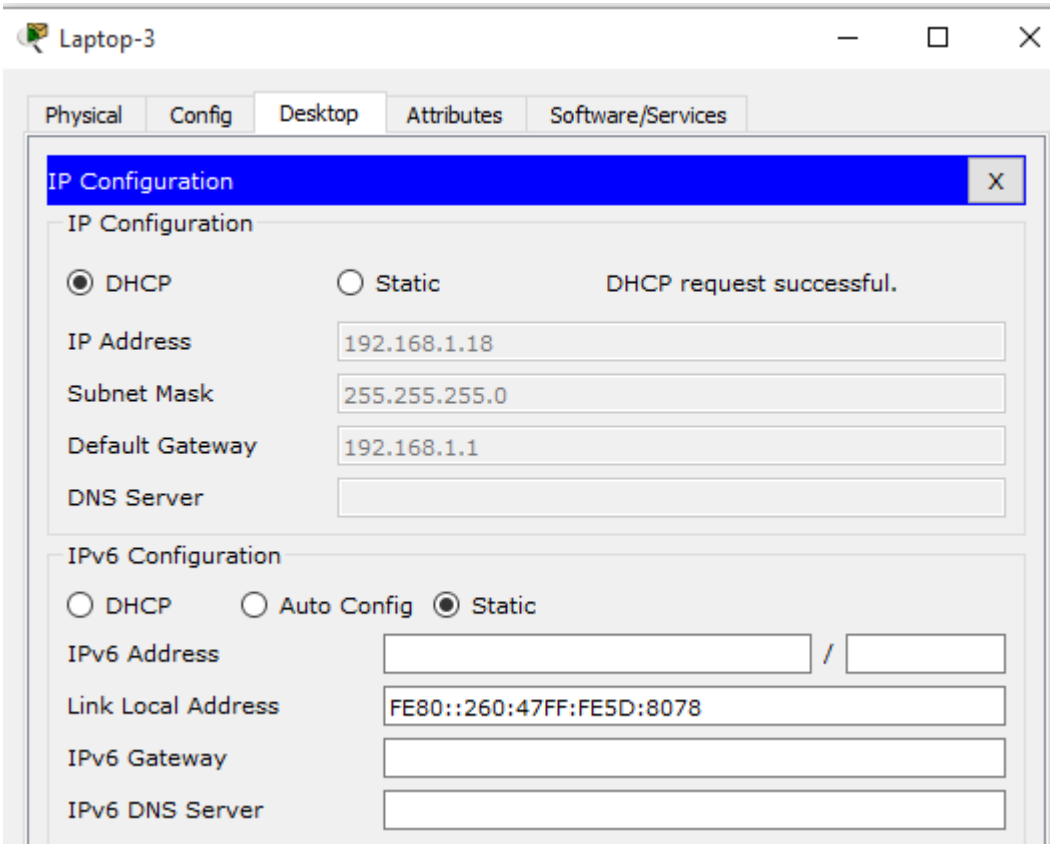



PC-B
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:BCFF:FE9E:A3BD
IPv6 Gateway
IPv6 DNS Server


PC-C
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.15
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::202:16FF:FED0:64BD
IPv6 Gateway
IPv6 DNS Server


Laptop-1
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.16
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FEE2:324
IPv6 Gateway
IPv6 DNS Server


Laptop-2
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.17
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::20A:F3FF:FE50:1766
IPv6 Gateway
IPv6 DNS Server



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

Es un protocolo de comunicación realmente muy interesante e importante para optimizar procesos de configuración de grandes redes de comunicación dependiendo las necesidades de los clientes y / u organización.

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?

Los dispositivos cisco brindan una mayor garantía de seguridad y adicional es fácil de configurar para 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.

1. Para la optimización de administración de redes.
2. Para la asignación de rangos específicos a ciertas áreas específicas.
3. Para la identificación de grupos de usuarios como visitantes.
4. Para configuraciones de clientes en redes centralizadas.
5. Por temas de compactibilidad con clientes locales y remotos.

DESARROLLO EJERCICIO 11.2.2.6

Práctica de laboratorio: configuración de NAT dinámica y estática

Topología

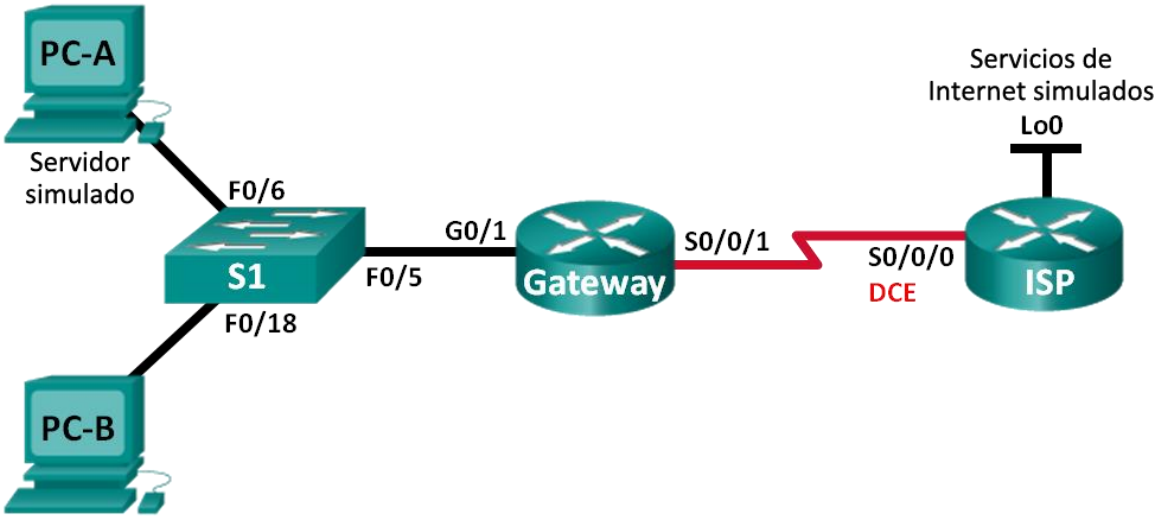


Tabla de direccionamiento

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

Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada. En esta práctica de laboratorio, un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/27. Esto proporciona 30 direcciones IP públicas a la empresa. Las direcciones 209.165.200.225 a 209.165.200.241 son para la asignación estática, y las direcciones 209.165.200.242 a 209.165.200.254 son para la asignación dinámica. Del ISP al router de gateway se usa una ruta estática, y del gateway al router ISP se usa una ruta predeterminada. La conexión del ISP a Internet se simula mediante una dirección de loopback en el router ISP.

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

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

Recursos necesarios

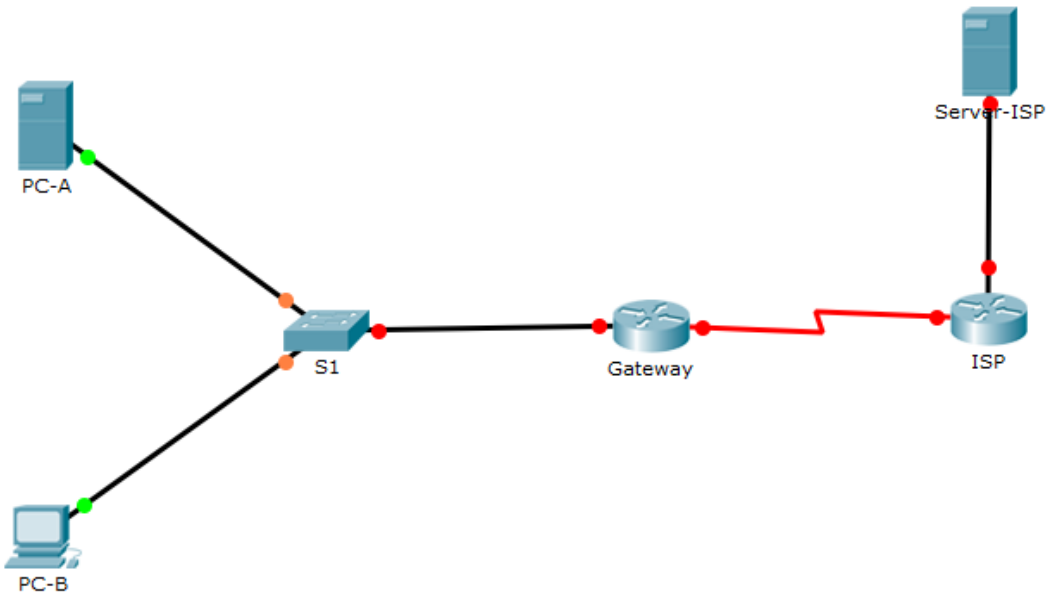
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4) M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

Parte 1. armar la red y verificar la conectividad

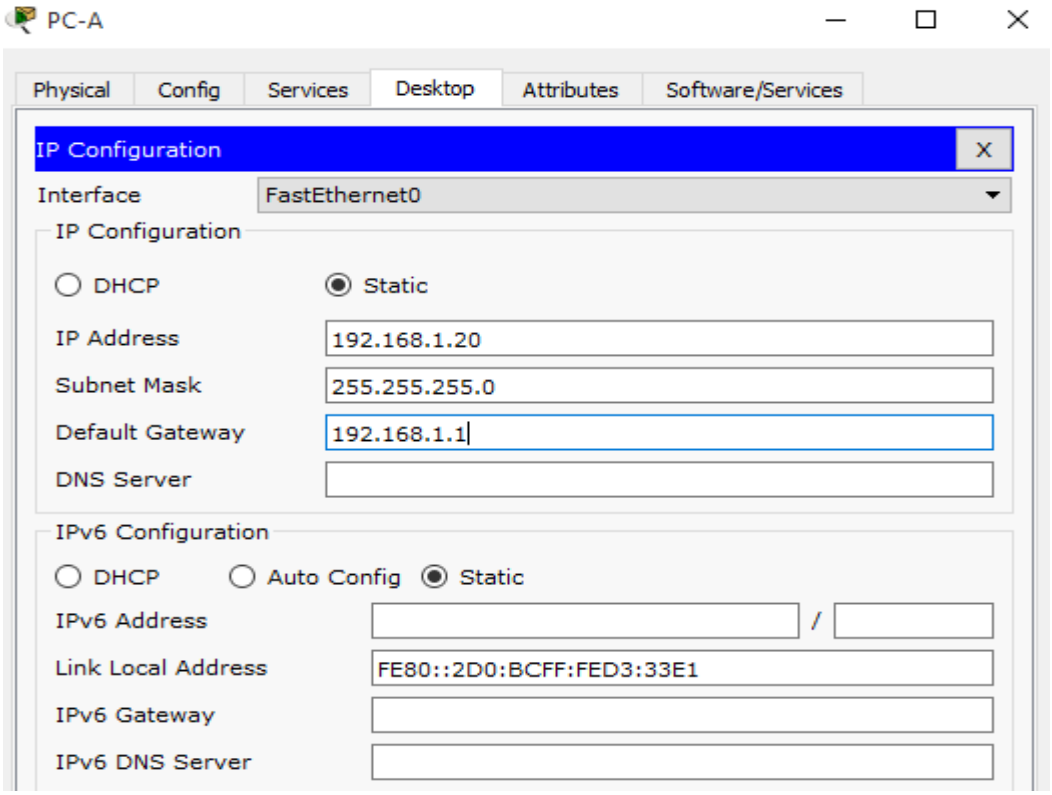
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

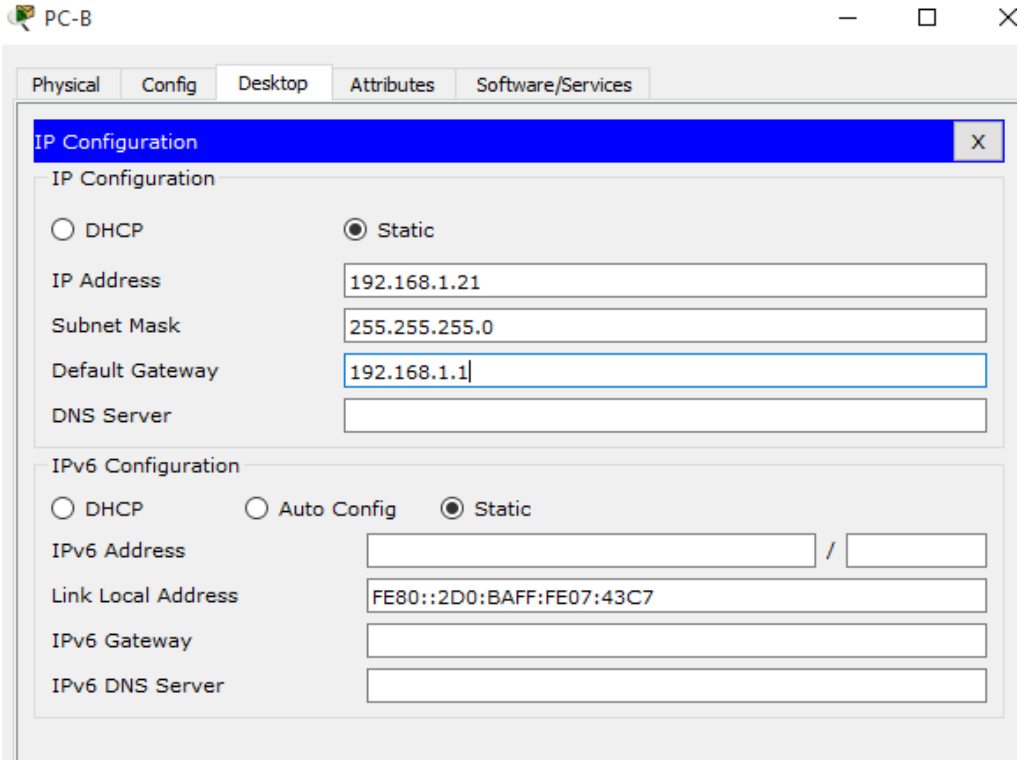
Paso 1. realizar el cableado de red tal como se muestra en la topología.

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



Paso 2. configurar los equipos host.





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

Paso 4. configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

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

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

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

Gateway(config-if)#int s0/0/1
Gateway(config-if)#int add 209.165.201.18 255.255.255.252
                   ^
% Invalid input detected at '^' marker.

Gateway(config-if)#ip add 209.165.201.18 255.255.255.252
Gateway(config-if)#no shu

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Gateway(config-if)#
Gateway(config-if)#exit
Gateway(config)#no ip domain-lookup
Gateway(config)#
```

```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#int s0/0/0
ISP(config-if)#clock rate 128000
ISP(config-if)#ip add 209.165.201.17 255.255.255.252
ISP(config-if)#no shu

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

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

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

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

ISP#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

c. Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.

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

e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

```
Gateway#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#enable secret class
Gateway(config)#line console 0
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#line vty 0 15
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#logging syncrhonous
                                  ^
% Invalid input detected at '^' marker.

Gateway(config-line)#exit
Gateway(config)#logging syncrhonous
                       ^
% Invalid input detected at '^' marker.

Gateway(config)#logging synchronous
                       ^
% Invalid input detected at '^' marker.

Gateway(config)#line vty 0 15
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#banner motd #EL acceso no autorizado esta prohibido#
Gateway(config)#service password-encryption
Gateway(config)#
```

```
ISP>
ISP>enable
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exec-timeout 5 0
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#end
ISP#
%SYS-5-CONFIG_I: Configured from console by console

ISP#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

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

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

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

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

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

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

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

Paso 6. configurar el routing estático.

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

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

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

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

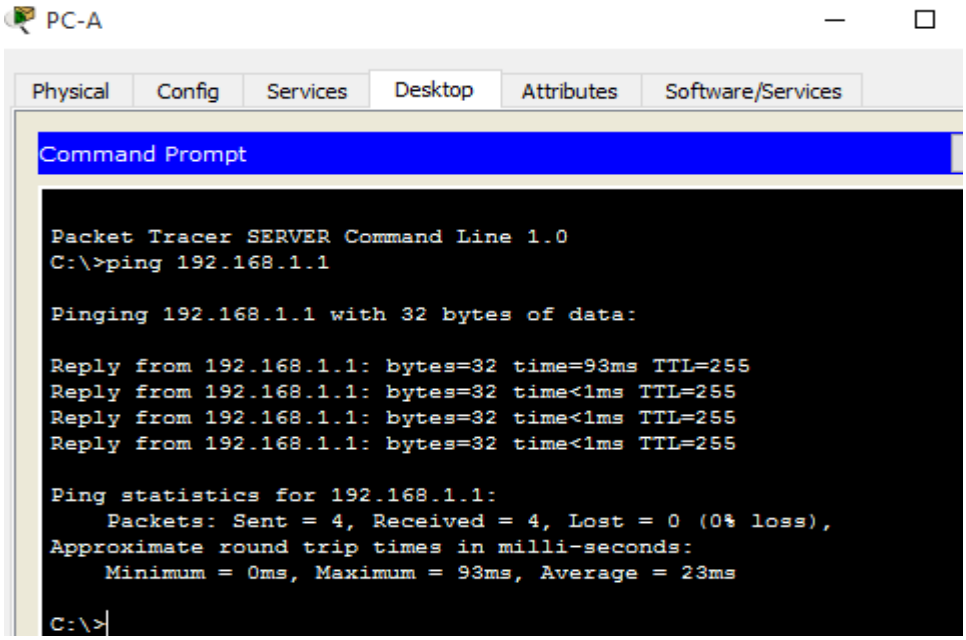
Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

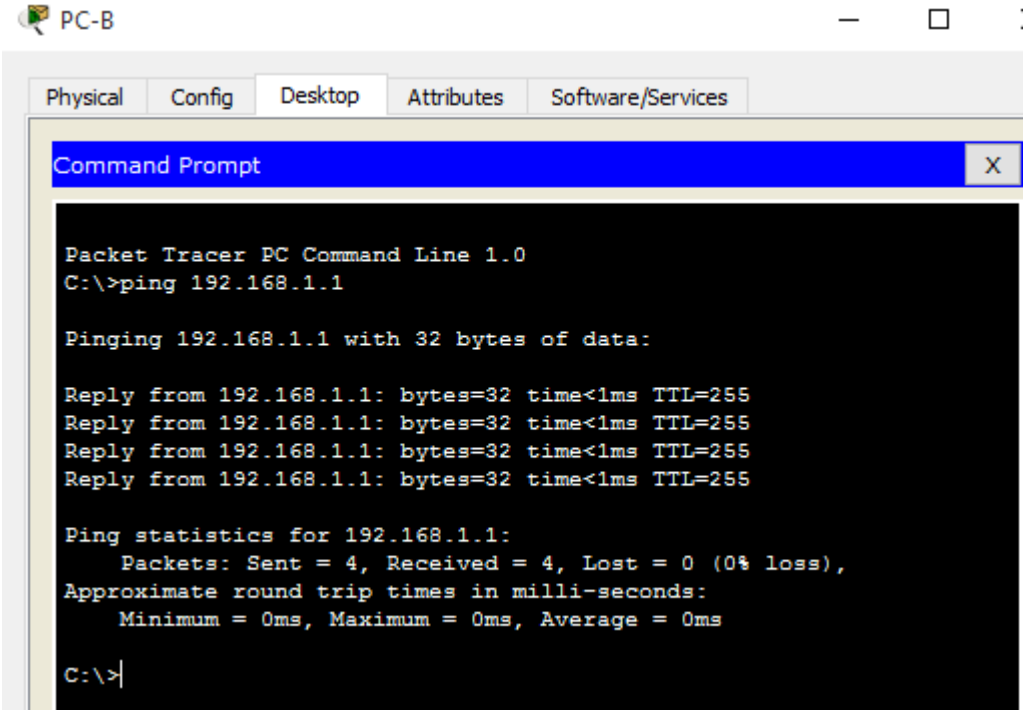
```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

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

Paso 8. Verificar la conectividad de la red

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





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

```
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#
```

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

Gateway of last resort is not set

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

Parte 2. configurar y verificar la NAT estática.

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

Paso 1. configurar una asignación estática.

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

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

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

Paso 2. Especifique las interfaces.

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

Gateway(config)# **interface g0/1**

Gateway(config-if)# **ip nat inside**

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

Gateway(config-if)# **ip nat outside**

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

Paso 3. probar la configuración.

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

Gateway# **show ip nat translations**

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

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

192.168.1.20 = esta es la IP del PC, es decir lo que está dentro. La traducción es 209.165.200.225.l

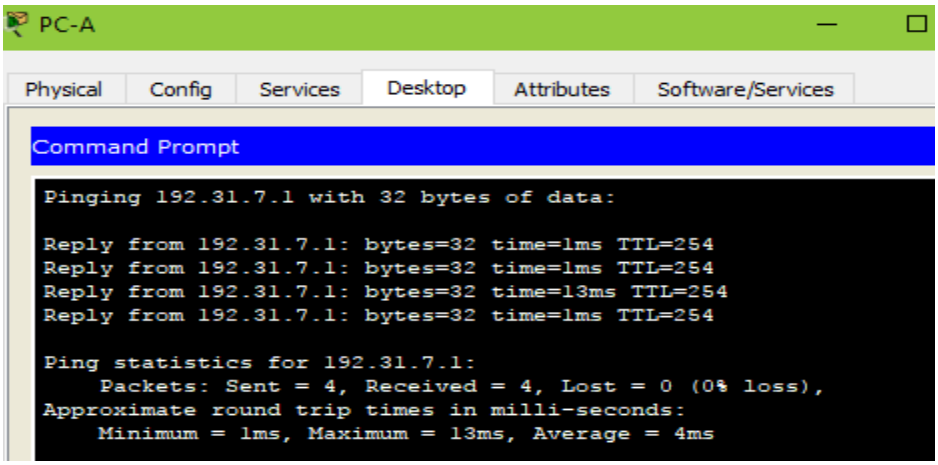
¿Quién asigna la dirección global interna?

Es asignada por el router ó por el proveedor de internet.

¿Quién asigna la dirección local interna?

La asignamos nosotros los administradores de red

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



Gateway# **show ip nat translations**

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:21192.168.1.20:21    192.31.7.1:21      192.31.7.1:21
icmp 209.165.200.225:22192.168.1.20:22    192.31.7.1:22      192.31.7.1:22
icmp 209.165.200.225:23192.168.1.20:23    192.31.7.1:23      192.31.7.1:23
icmp 209.165.200.225:24192.168.1.20:24    192.31.7.1:24      192.31.7.1:24
---  209.165.200.225   192.168.1.20       ---                ---
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.
¿Qué número de puerto se usó en este intercambio ICMP? **El puerto 10**.

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.

```
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  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1026192.168.1.20:1026  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1027192.168.1.20:1027  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1028192.168.1.20:1028  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1029192.168.1.20:1029  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1030192.168.1.20:1030  192.31.7.2:23      192.31.7.2:23
tcp 209.165.200.225:1031192.168.1.20:1031  192.31.7.2:23      192.31.7.2:23
```

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

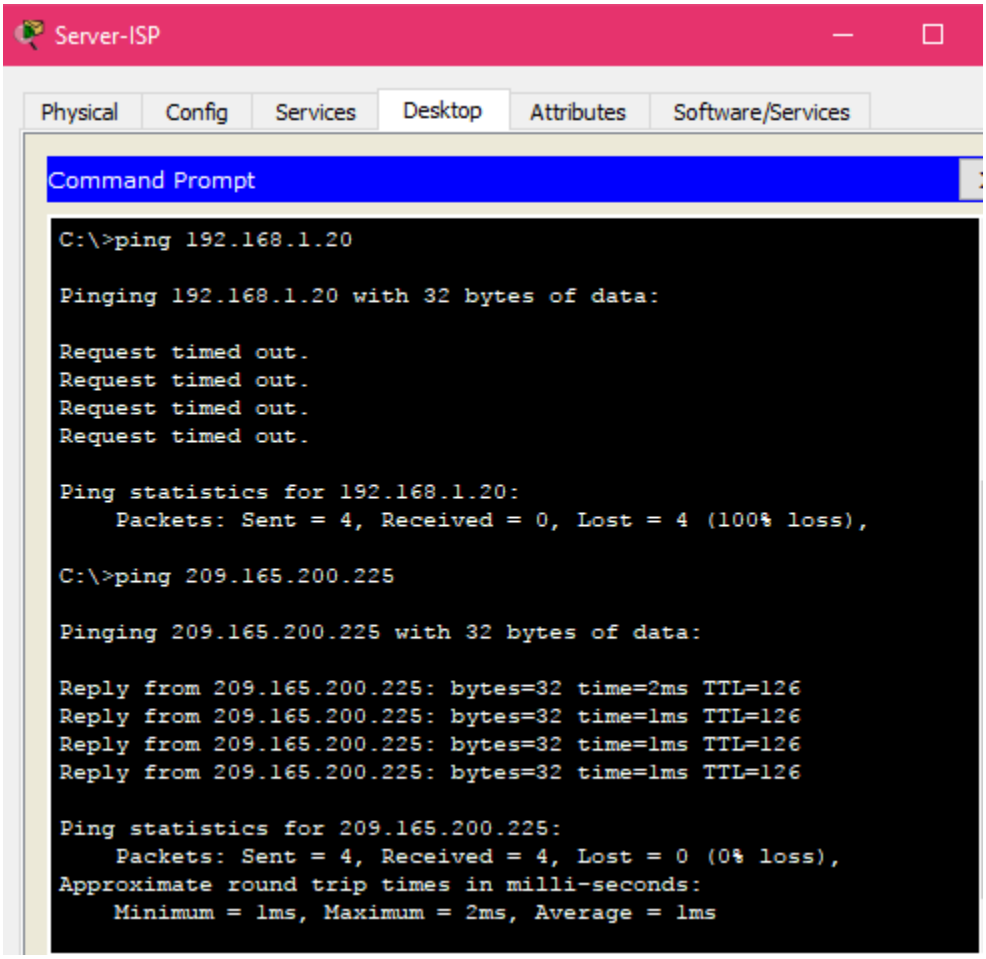
¿Qué protocolo se usó para esta traducción? **Web .**

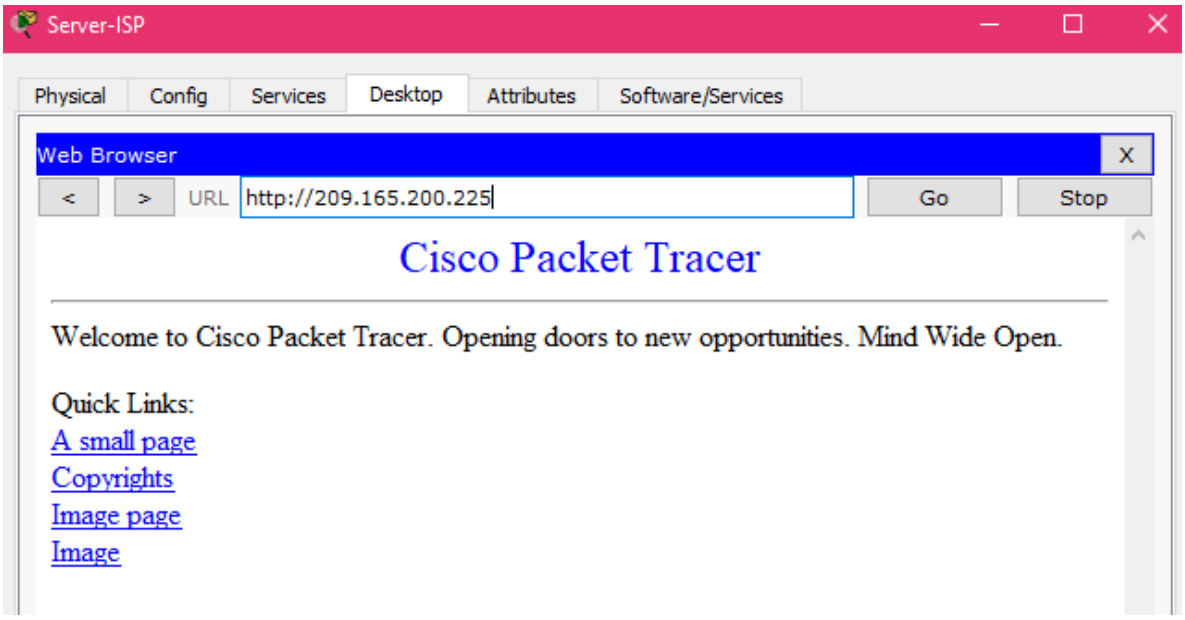
¿Cuáles son los números de puerto que se usaron?

Global/local interno: **1025 y 1025.**

Global/local externo: **80 y 80**

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





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

Gateway# **show ip nat translations**

```
Password:
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  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1026192.168.1.20:1026  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1027192.168.1.20:1027  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1028192.168.1.20:1028  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1029192.168.1.20:1029  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1030192.168.1.20:1030  192.31.7.2:23      192.31.7.2:23
tcp 209.165.200.225:1031192.168.1.20:1031  192.31.7.2:23      192.31.7.2:23
tcp 209.165.200.225:1032192.168.1.20:1032  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:80 192.168.1.20:80     192.31.7.2:1025    192.31.7.2:1025
tcp 209.165.200.225:80 192.168.1.20:80     192.31.7.2:1026    192.31.7.2:1026
tcp 209.165.200.225:80 192.168.1.20:80     192.31.7.2:1027    192.31.7.2:1027
tcp 209.165.200.225:80 192.168.1.20:80     192.31.7.2:1028    192.31.7.2:1028
tcp 209.165.200.225:80 192.168.1.20:80     192.31.7.2:1029    192.31.7.2:1029
tcp 209.165.200.225:80 192.168.1.20:80     192.31.7.2:1030    192.31.7.2:1030
tcp 209.165.200.225:80 192.168.1.20:80     192.31.7.2:1031    192.31.7.2:1031
```

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

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

```
Gateway#show ip nat statistics
Total translations: 16 (1 static, 15 dynamic, 15 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 172  Misses: 43
Expired translations: 28
Dynamic mappings:
Gateway#
```

Parte 3. configurar y verificar la NAT dinámica

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

Paso 1. borrar las NAT.

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

Gateway# **clear ip nat translation ***

```
Gateway#clear ip nat translation *
Gateway#
```

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

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

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

Paso 3. verificar que la configuración de interfaces NAT siga siendo válida.
Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

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

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

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

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

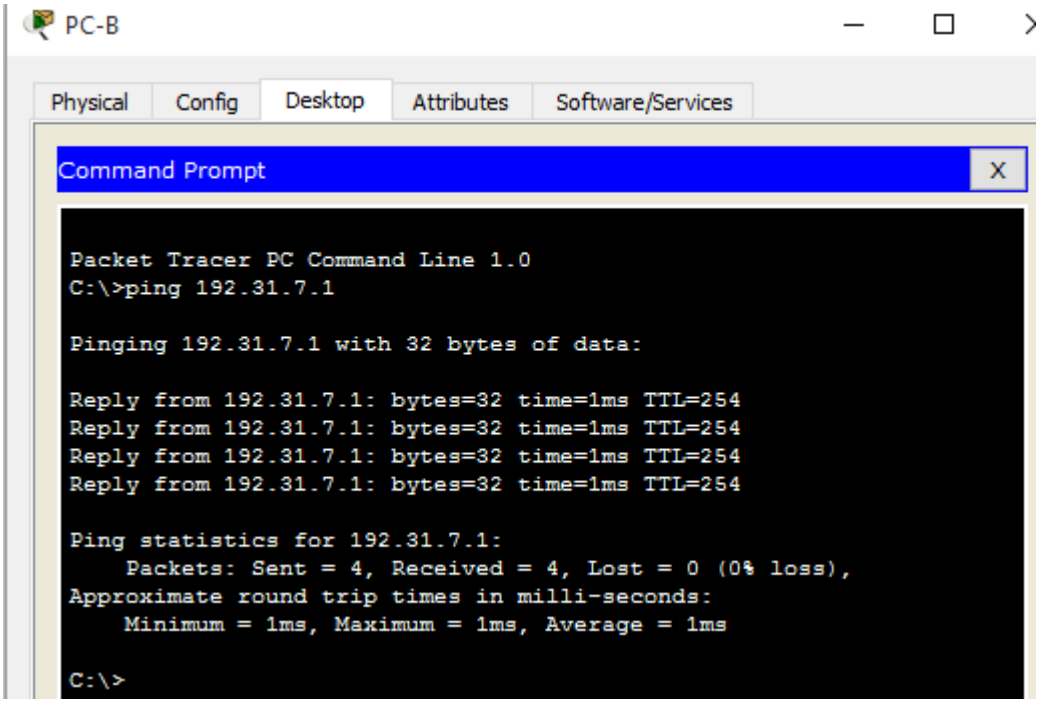
Nota: recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

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

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

Paso 6. probar la configuración.

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



Gateway# **show ip nat translations**

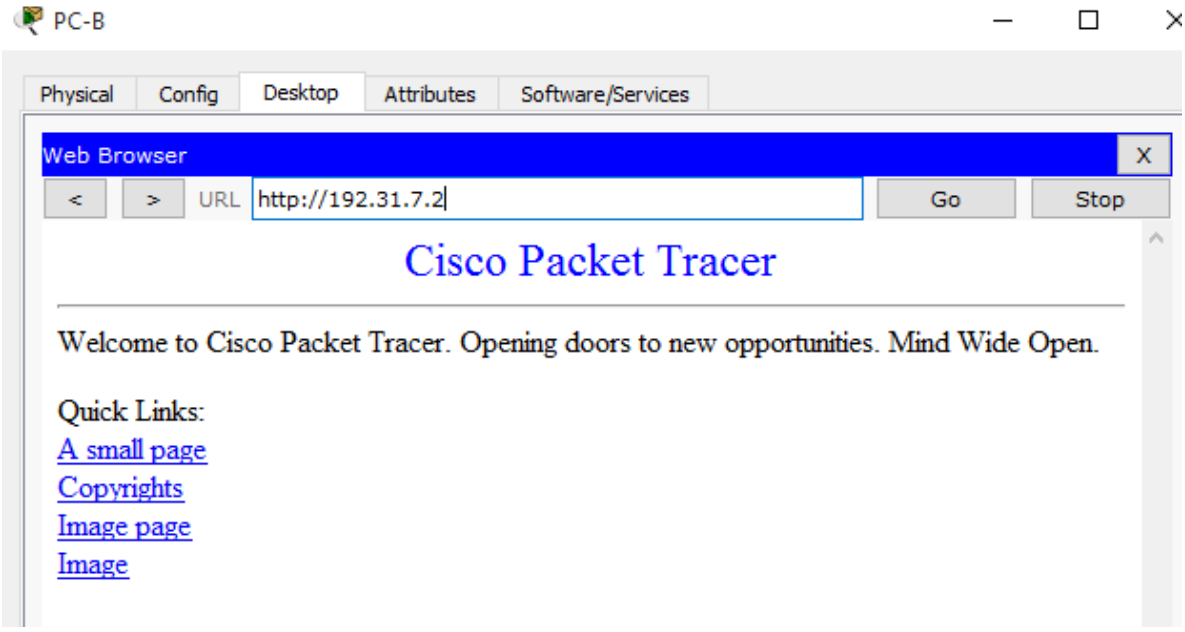
```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.242:10192.168.1.21:10    192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.242:11192.168.1.21:11    192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.242:12192.168.1.21:12    192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.242:5 192.168.1.21:5     192.31.7.1:5       192.31.7.1:5
icmp 209.165.200.242:6 192.168.1.21:6     192.31.7.1:6       192.31.7.1:6
icmp 209.165.200.242:7 192.168.1.21:7     192.31.7.1:7       192.31.7.1:7
icmp 209.165.200.242:8 192.168.1.21:8     192.31.7.1:8       192.31.7.1:8
icmp 209.165.200.242:9 192.168.1.21:9     192.31.7.1:9       192.31.7.1:9
---  209.165.200.225   192.168.1.20       ---                ---
```

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

192.168.1.21 = 209.165.200.242

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo. ¿Qué número de puerto se usó en este intercambio ICMP? **10,11,12 y 9**

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



c. Muestre la tabla de NAT.

```
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  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1026192.168.1.20:1026  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1027192.168.1.20:1027  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1028192.168.1.20:1028  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1029192.168.1.20:1029  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.225:1030192.168.1.20:1030  192.31.7.2:80      192.31.7.2:80
tcp 209.165.200.242:1025192.168.1.21:1025  192.31.7.2:80      192.31.7.2:80
```

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

¿Qué números de puerto se usaron?

Interno: 1025.

Externo: 80

¿Qué número de puerto bien conocido y qué servicio se usaron? **El http usa el 80**

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

Gateway# **show ip nat statistics**

```
Gateway#show ip nat statistics
Total translations: 8 (1 static, 7 dynamic, 7 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 121  Misses: 20
Expired translations: 13
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
 pool public_access: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13 , allocated 1 (7%), misses 0
```

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

Paso 7. eliminar la entrada de NAT estática.

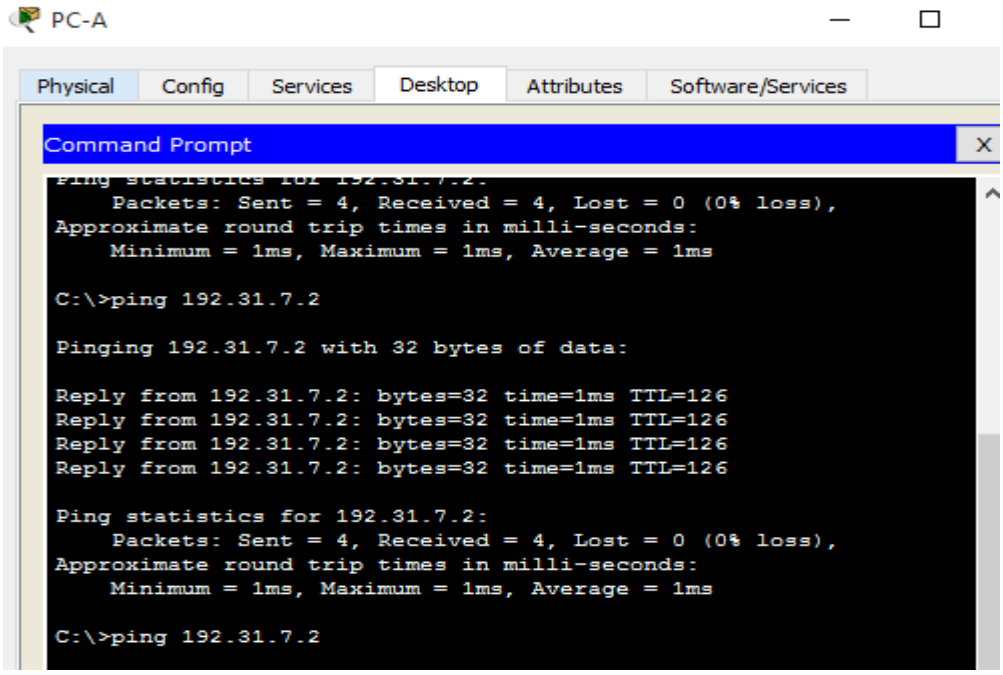
En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT. a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

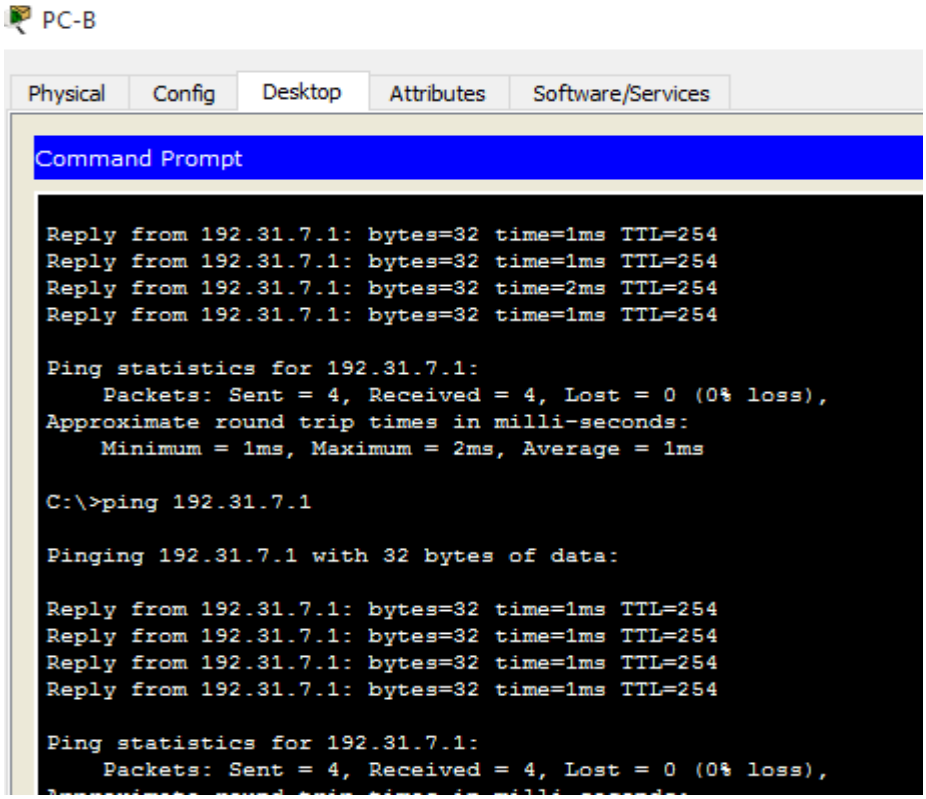
Gateway(config)# **no ip nat inside source static 192.168.1.20 209.165.200.225**

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

b. Borre las NAT y las estadísticas.

c. Haga ping al ISP (192.31.7.1) desde ambos hosts.





d. Muestre la tabla y las estadísticas de NAT.

Gateway# **show ip nat statistics**

```
Gateway#show ip nat statistics
Total translations: 6 (0 static, 6 dynamic, 6 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 150  Misses: 49
Expired translations: 37
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 6
 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# **show ip nat translation**

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.242:17192.168.1.21:17    192.31.7.1:17      192.31.7.1:17
icmp 209.165.200.242:18192.168.1.21:18    192.31.7.1:18      192.31.7.1:18
icmp 209.165.200.242:19192.168.1.21:19    192.31.7.1:19      192.31.7.1:19
icmp 209.165.200.242:20192.168.1.21:20    192.31.7.1:20      192.31.7.1:20
icmp 209.165.200.242:21192.168.1.21:21    192.31.7.1:21      192.31.7.1:21
icmp 209.165.200.242:22192.168.1.21:22    192.31.7.1:22      192.31.7.1:22
icmp 209.165.200.242:23192.168.1.21:23    192.31.7.1:23      192.31.7.1:23
icmp 209.165.200.242:24192.168.1.21:24    192.31.7.1:24      192.31.7.1:24
icmp 209.165.200.243:10192.168.1.20:10    192.31.7.2:10      192.31.7.2:10
icmp 209.165.200.243:11192.168.1.20:11    192.31.7.2:11      192.31.7.2:11
icmp 209.165.200.243:12192.168.1.20:12    192.31.7.2:12      192.31.7.2:12
icmp 209.165.200.243:5 192.168.1.20:5     192.31.7.2:5       192.31.7.2:5
icmp 209.165.200.243:6 192.168.1.20:6     192.31.7.2:6       192.31.7.2:6
icmp 209.165.200.243:7 192.168.1.20:7     192.31.7.2:7       192.31.7.2:7
icmp 209.165.200.243:8 192.168.1.20:8     192.31.7.2:8       192.31.7.2:8
icmp 209.165.200.243:9 192.168.1.20:9     192.31.7.2:9       192.31.7.2:9
tcp 209.165.200.242:1025192.168.1.21:1025  192.31.7.2:80      192.31.7.2:80
```

Reflexión

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

Se ahorra un espacio o se ahorran IPv4, cada computadora en una red privada tiene su IP, pero, salen con una sola IP pública o con un grupo pequeño de IP públicas. De esa manera se ahorran las IP públicas, para que se puedan seguir usando en internet. Hay seguridad por que no muestro las IP de mis computadoras.

2. ¿Cuáles son las limitaciones de NAT?

En el Gateway hay un pequeño delay, en hacer la traducción o el NAT hay una pequeña demora y que hay muchos servicios adentro que no pueden salir a internet (no se le pueden hacer NAT) como SNMP, por ejemplo.

Desarrollo Ejercicio 11.2.3.7

Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT

Topología

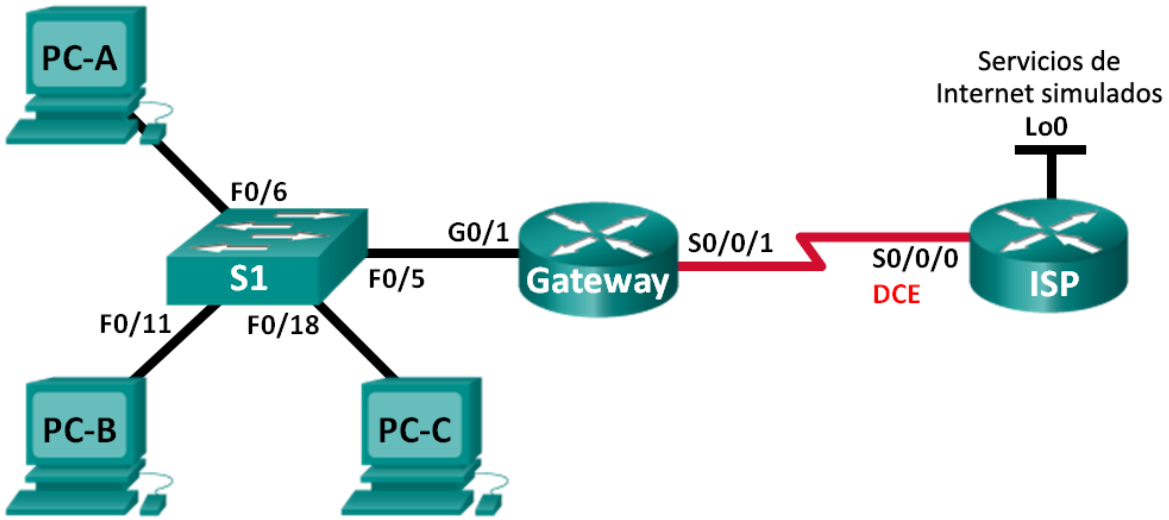


Tabla de direccionamiento

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

Objetivos

Parte 1: armar la red y verificar la conectividad
Parte 2: configurar y verificar un conjunto de NAT con sobrecarga
Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

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

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

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

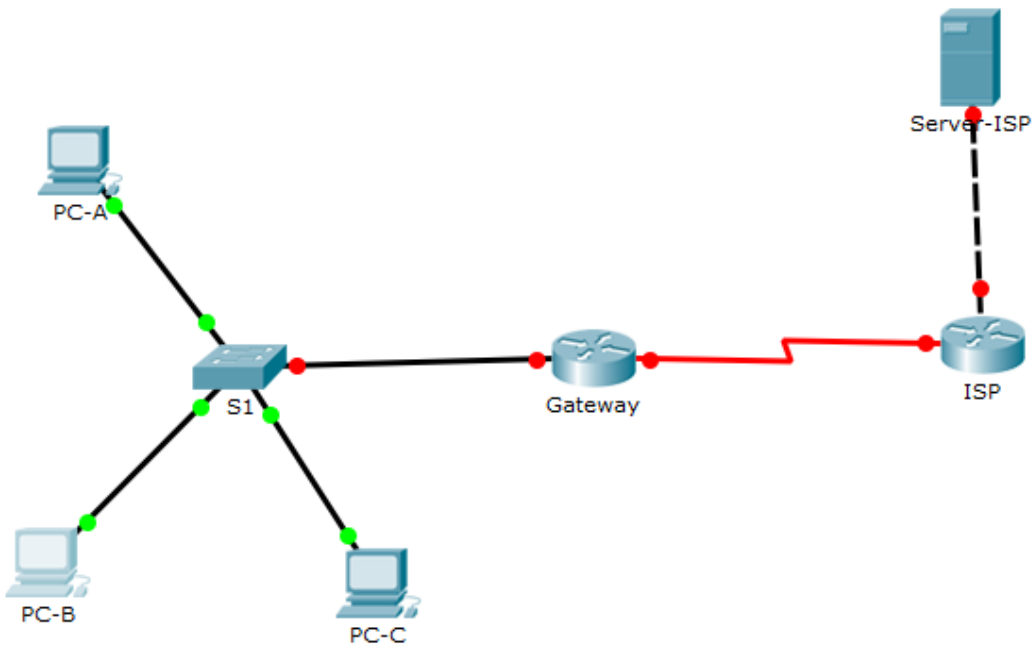
Recursos necesarios

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

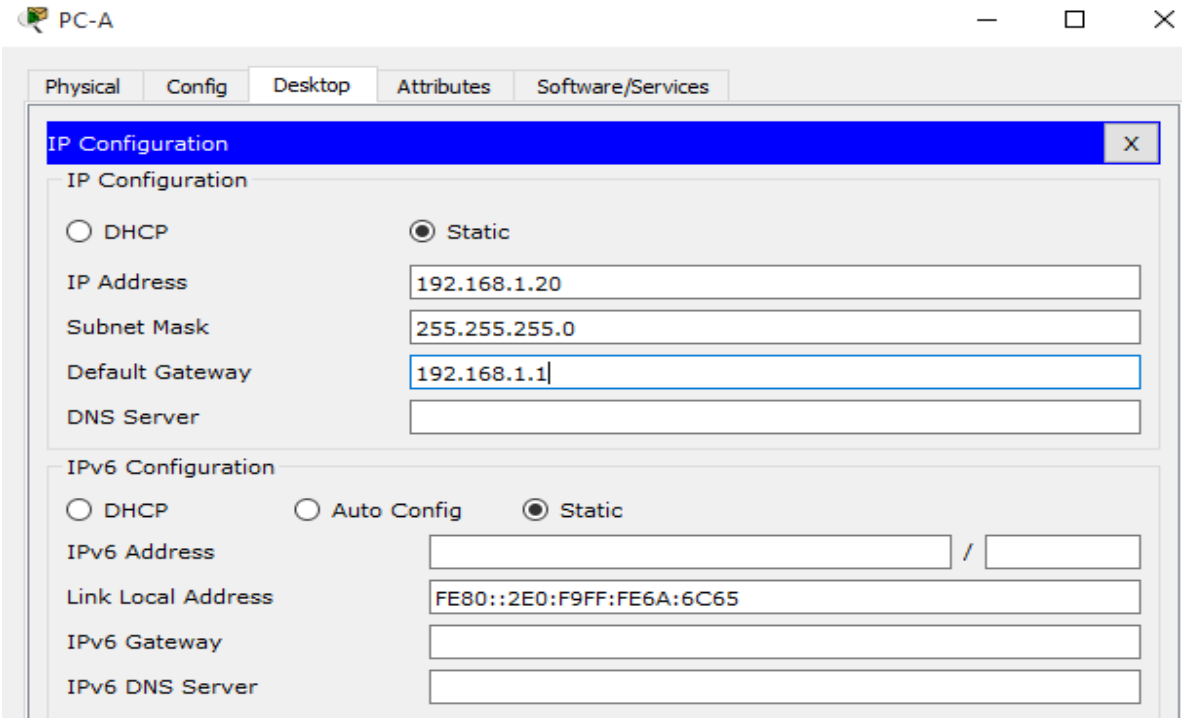
Parte 1. armar la red y verificar la conectividad

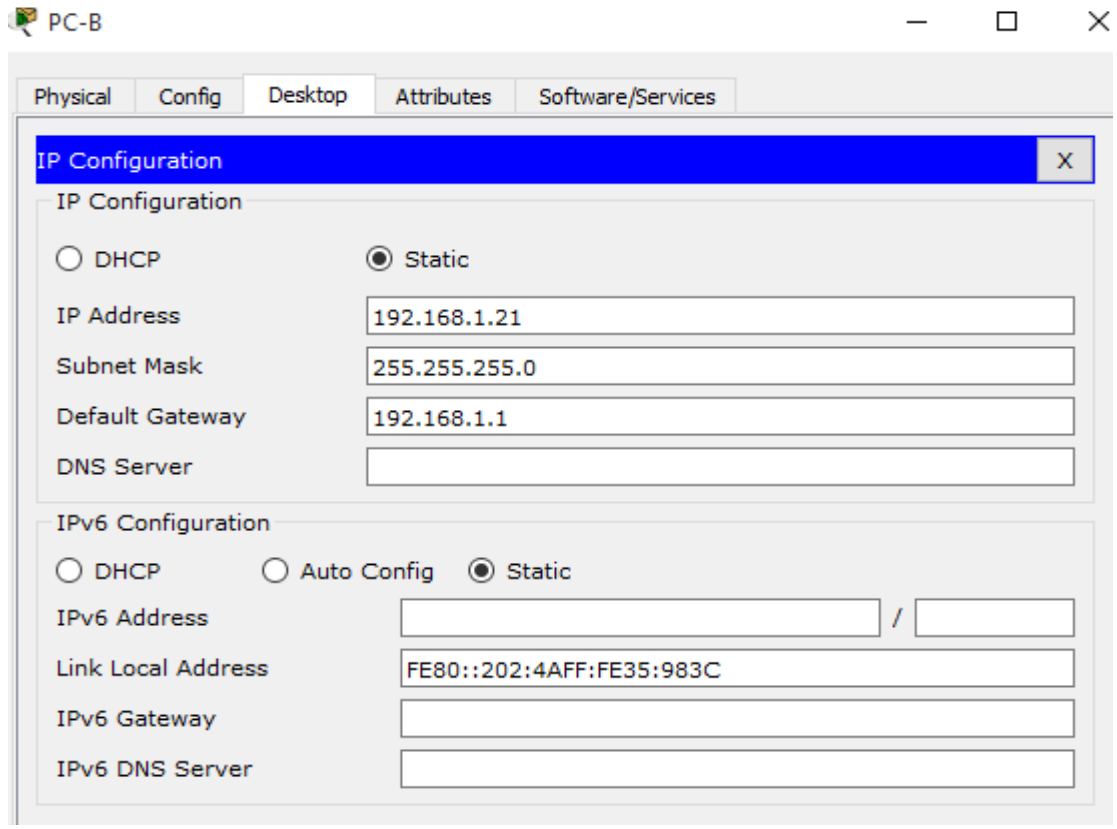
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

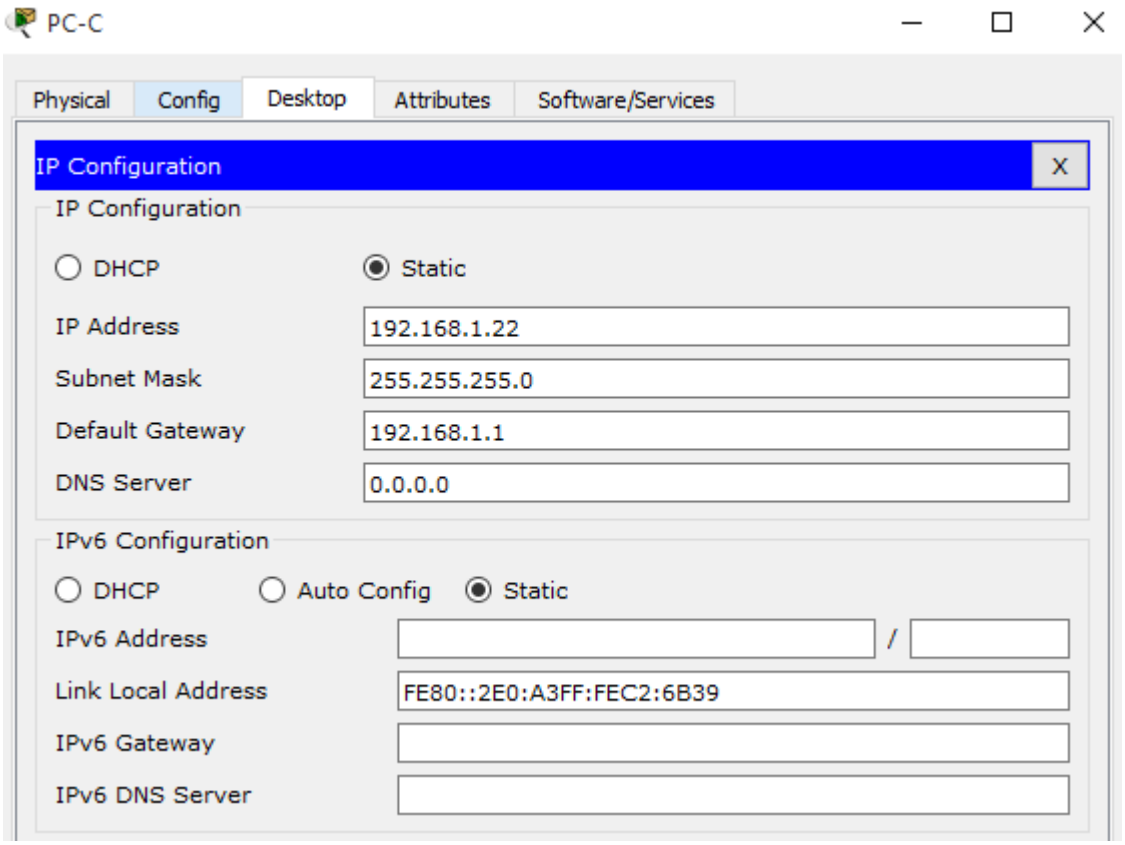
Paso 1. realizar el cableado de red tal como se muestra en la topología.

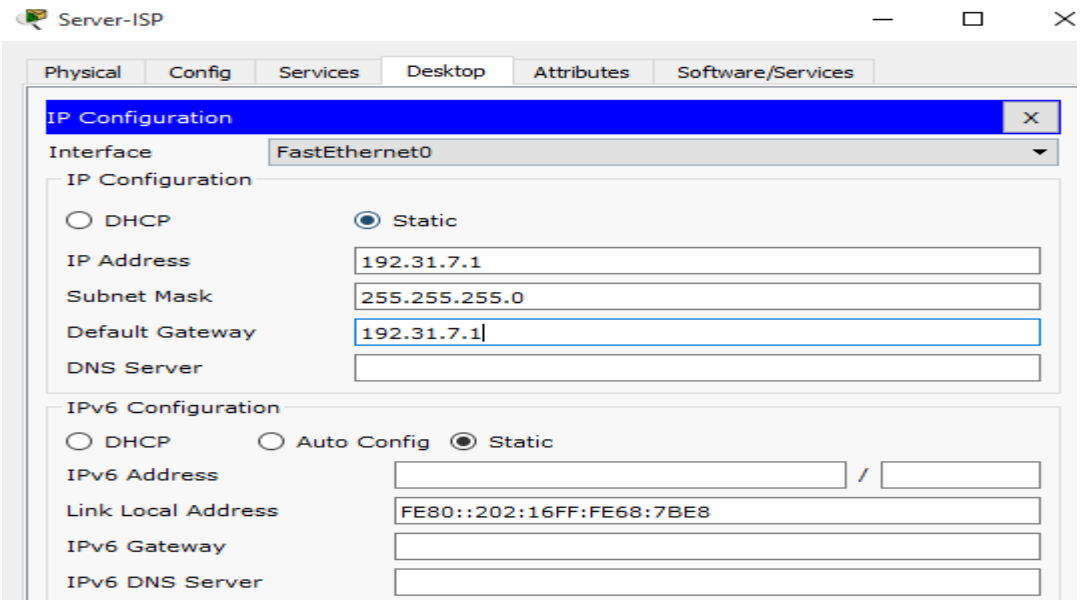


Paso 2. configurar los equipos host.



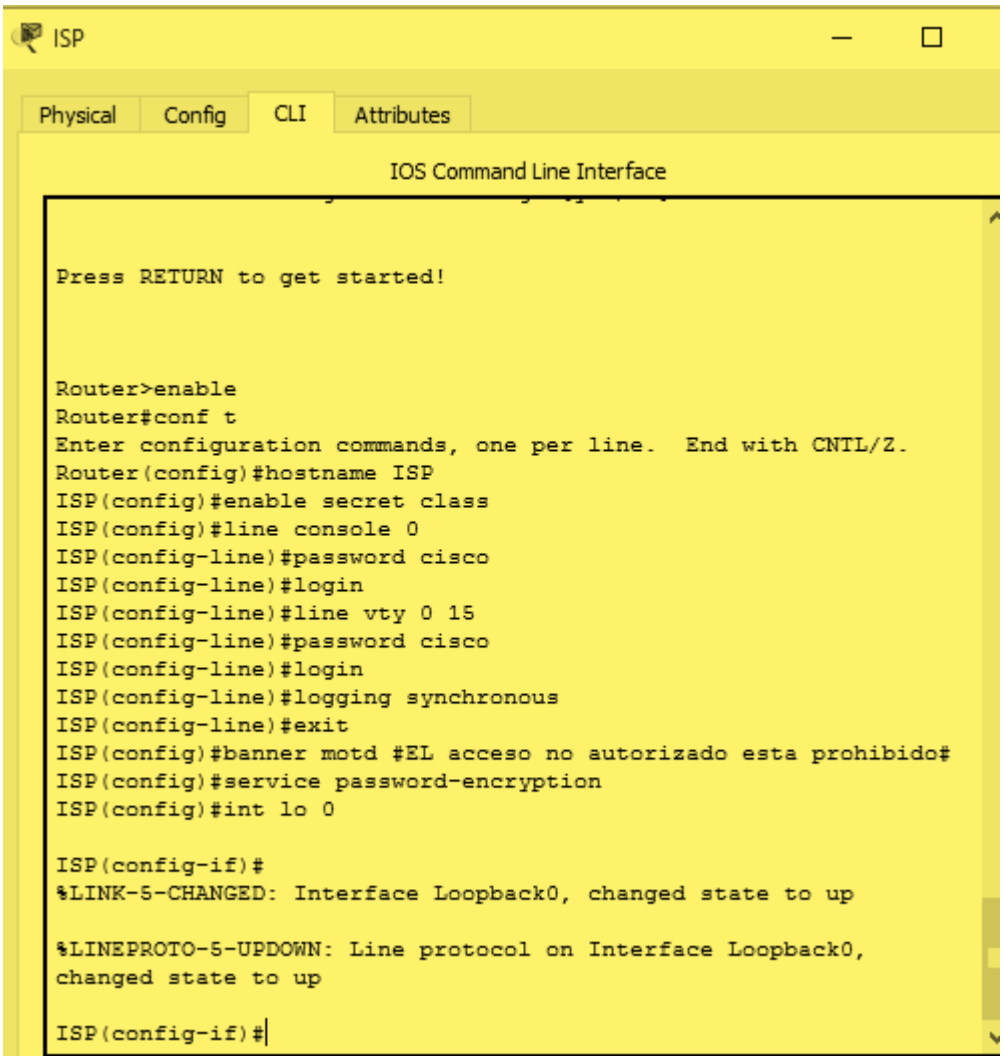

PC-B
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.21
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::202:4AFF:FE35:983C
IPv6 Gateway
IPv6 DNS Server


PC-C
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.22
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2E0:A3FF:FEC2:6B39
IPv6 Gateway
IPv6 DNS Server



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

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#enable secret class
Router(config)#line console o
                           ^
% Invalid input detected at '^' marker.

Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#loggin synchronous
Router(config-line)#exit
Router(config)#banner motd #El acceso no autorizado esta prohibido#
Router(config)#service password-encryption
Router(config)#hostname
% Incomplete command.
Router(config)#hostname  gateway
gateway(config)#int g0/1
gateway(config-if)#ip add 192.168.1.1 255.255.255.0
gateway(config-if)#no shu

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

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

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

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

gateway#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
gateway#
```



Paso 4. configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

c. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

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

e. Asigne **cisco** como la contraseña de consola y la contraseña de vty. f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

```
ISP(config-if)#int s0/0/0
ISP(config-if)#ip add 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shu

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

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

ISP(config-if)#int g0/1
ISP(config-if)#ip add 192.31.7.1 255.255.255.252
ISP(config-if)#no shu

ISP(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
%IP-4-DUPADDR: Duplicate address 192.31.7.1 on
GigabitEthernet0/1, sourced by 0002.1668.7BE8

ISP(config-if)#
```

Paso 5. configurar el routing estático.

a. Cree una ruta estática desde el router ISP hasta el router Gateway.

ISP(config)# **ip route 209.165.200.224 255.255.255.248 209.165.201.18**

```
ISP(config)#ip route 209.165.200.224 255.255.255.248 209.165.201.18
ISP(config)#
```

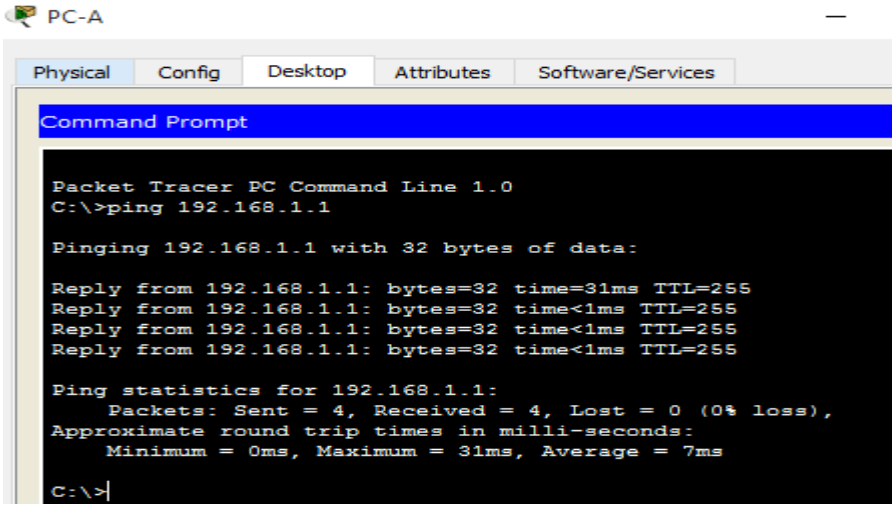
b. Cree una ruta predeterminada del router Gateway al router ISP.

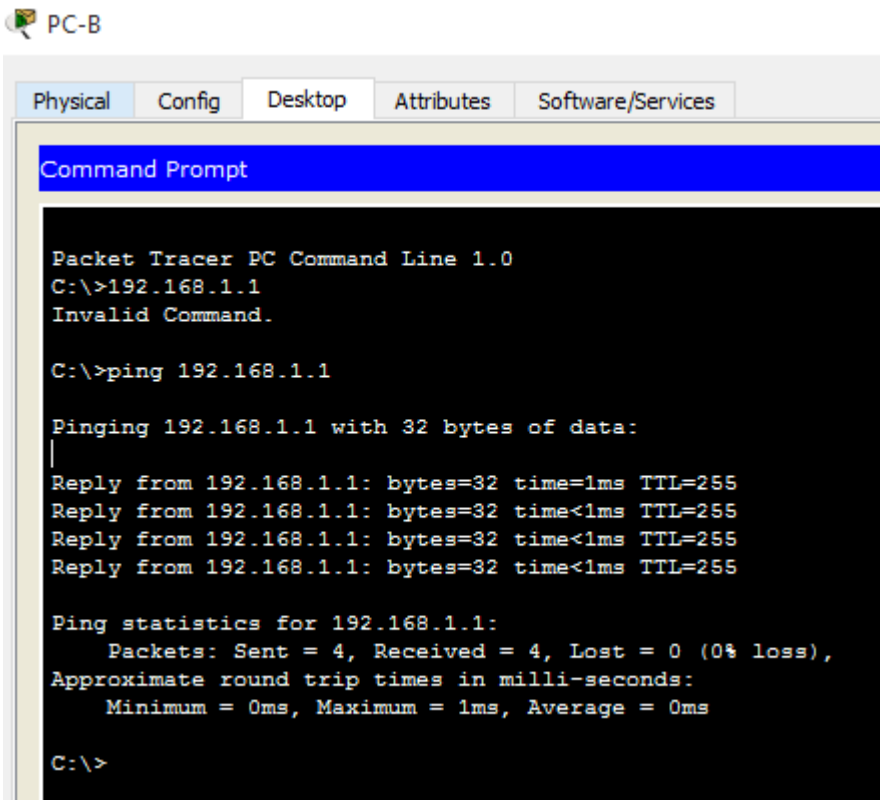
Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

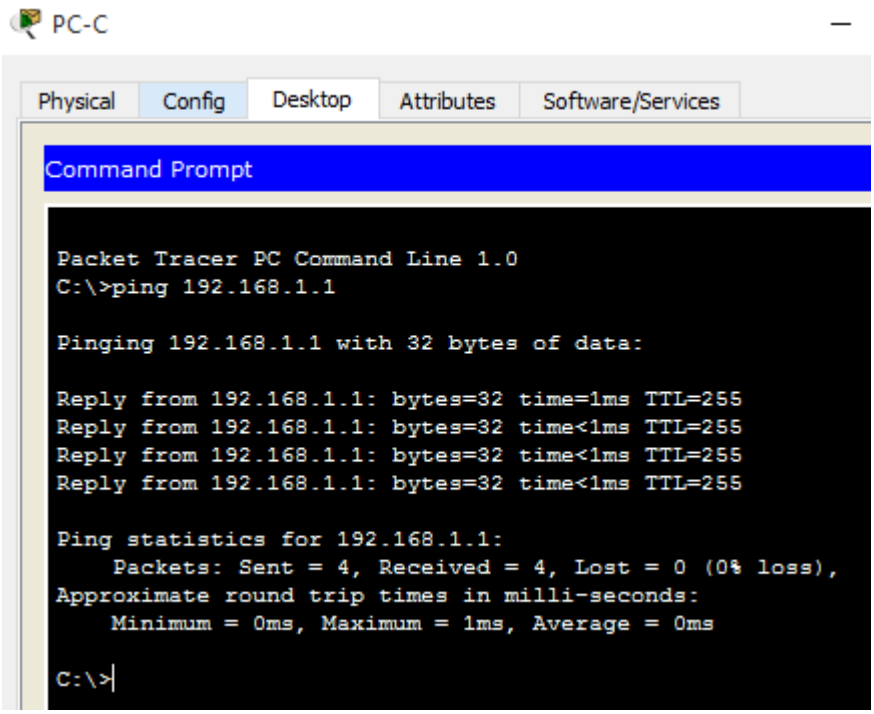
```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#
```

Paso 6. Verificar la conectividad de la red

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







b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.

```
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
```

Parte 2. configurar y verificar el conjunto de NAT con sobrecarga

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

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

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

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

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

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

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

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

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

Paso 4. Especifique las interfaces.

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

Gateway(config)# **interface g0/1**

Gateway(config-if)# **ip nat inside**

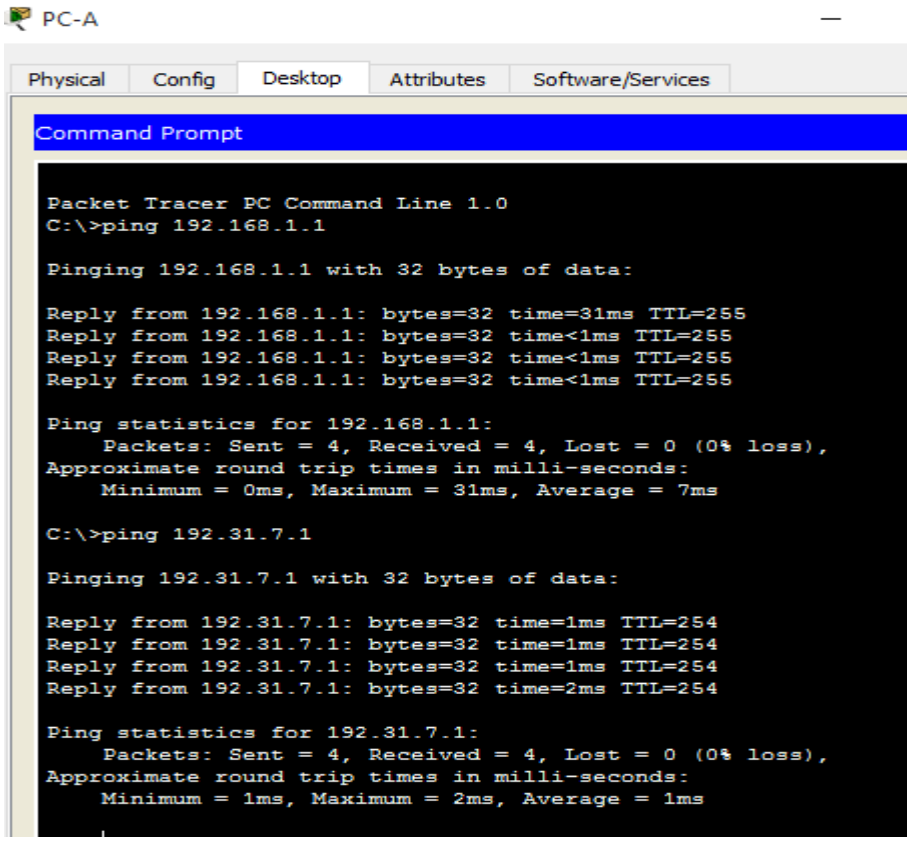
Gateway(config-if)# **interface s0/0/1**

Gateway(config-if)# **ip nat outside**

```
Gateway#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#int g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip nat outside
Gateway(config-if)#end
Gateway#
%SYS-5-CONFIG_I: Configured from console by console

Gateway#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
Gateway#
```

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

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



PC-B

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

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

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

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

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

PC-C

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

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

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=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

C:\>
```

b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**

```
Gateway#show ip nat statistics
Total translations: 20 (0 static, 20 dynamic, 20 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 32  Misses: 32
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 20
 pool public_access: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.230
       type generic, total addresses 6 , allocated 1 (16%),
misses 0
```

c. Muestre las NAT en el router Gateway.

Gateway# **show ip nat translations**

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:1024192.168.1.22:17    192.31.7.1:17      192.31.7.1:1024
icmp 209.165.200.225:1025192.168.1.22:18    192.31.7.1:18      192.31.7.1:1025
icmp 209.165.200.225:1026192.168.1.22:19    192.31.7.1:19      192.31.7.1:1026
icmp 209.165.200.225:13192.168.1.21:13    192.31.7.1:13      192.31.7.1:13
icmp 209.165.200.225:14192.168.1.21:14    192.31.7.1:14      192.31.7.1:14
icmp 209.165.200.225:15192.168.1.21:15    192.31.7.1:15      192.31.7.1:15
icmp 209.165.200.225:16192.168.1.21:16    192.31.7.1:16      192.31.7.1:16
icmp 209.165.200.225:17192.168.1.20:17    192.31.7.1:17      192.31.7.1:17
icmp 209.165.200.225:18192.168.1.20:18    192.31.7.1:18      192.31.7.1:18
icmp 209.165.200.225:19192.168.1.20:19    192.31.7.1:19      192.31.7.1:19
icmp 209.165.200.225:20192.168.1.20:20    192.31.7.1:20      192.31.7.1:20
```

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 puertos distintos para 12 paquetes distintos.**

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PCA? ¿Por qué?

El ping falla; porque cuando se hace NAT las computadoras no muestras sus direcciones IP, por que salen con una IP que está en el borde (Gateway) gracias a NAT. Si alguien de afuera quiere hacer un ping a una de las PCs no se va a poder porque el ISP simplemente conoce la IP de afuera (Gateway) con la que se usa NAT y no va a poder hacer ping ni a PC-A, ni PC-B ni a PC-C, porque su dirección 192.168.1.20 no se muestra para la salida, sino se muestra una IP que es la 225. Para salir hacia internet. Entonces el ISP no

puede hacer un ping a ninguna de las 3 PCs porque NAT las protege, no deja que ISP las conozca por su IP original si no por la que les asigna NAT

```
ISP#ping 192.168.1.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

ISP#ping 192.168.1.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.21, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

ISP#ping 192.168.1.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.22, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Parte 3. configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Paso 1. borrar las NAT y las estadísticas en el router Gateway.

```
Gateway#clear ip nat translation *
```

Paso 2. verificar la configuración para NAT.

a. Verifique que se hayan borrado las estadísticas.

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 44  Misses: 44
Expired translations: 44
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.230
       type generic, total addresses 6 , allocated 0 (0%), misses 0
```

b. Verifique que las interfaces externa e interna estén configuradas para NAT.

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 44  Misses: 44
Expired translations: 44
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.230
       type generic, total addresses 6 , allocated 0 (0%), misses 0
```

c. Verifique que la ACL aún esté configurada para NAT.

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 44  Misses: 44
Expired translations: 44
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.230
       type generic, total addresses 6 , allocated 0 (0%), misses 0
```

¿Qué comando usó para confirmar los resultados de los pasos a al c? **show ip nat statistics**

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

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

```
Gateway(config)#no ip nat inside source list 1 pool public_access overload
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
Gateway(config)#
```

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

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

```
Gateway(config)#no ip nat inside source list 1 pool public_access overload
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
Gateway(config)#
```

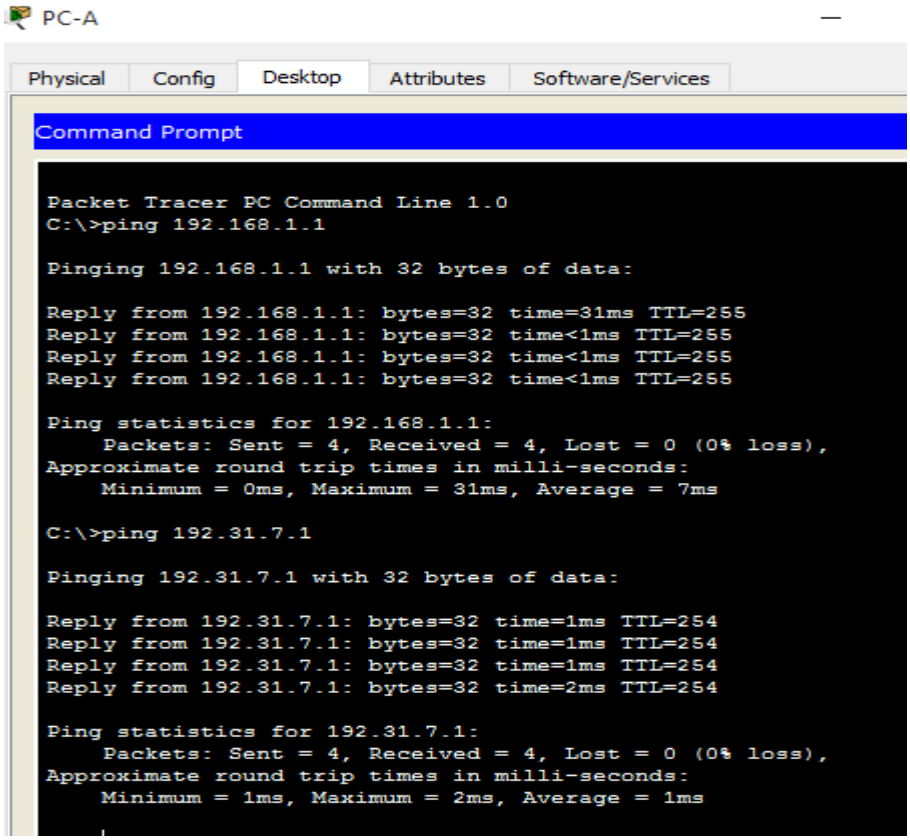
Paso 5. asociar la lista de origen a la interfaz externa.

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

```
Gateway(config)#ip nat inside source list 1 interface s0/0/1 overload
Gateway(config)#
```

Paso 6. probar la configuración PAT.

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.



PC-B

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

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

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

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

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

PC-C

Physical | Config | Desktop | Attributes | Software/Services

Command Prompt

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

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=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

C:\>
```

b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 56  Misses: 56
Expired translations: 56
Dynamic mappings:
```

c. Muestre las traducciones NAT en el Gateway.

Gateway# **show ip nat translations**

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.201.18:1024192.168.1.22:25    192.31.7.1:25      192.31.7.1:1024
icmp 209.165.201.18:1025192.168.1.22:26    192.31.7.1:26      192.31.7.1:1025
icmp 209.165.201.18:1026192.168.1.22:27    192.31.7.1:27      192.31.7.1:1026
icmp 209.165.201.18:1027192.168.1.22:28    192.31.7.1:28      192.31.7.1:1027
icmp 209.165.201.18:21 192.168.1.21:21    192.31.7.1:21      192.31.7.1:21
icmp 209.165.201.18:22 192.168.1.21:22    192.31.7.1:22      192.31.7.1:22
icmp 209.165.201.18:23 192.168.1.21:23    192.31.7.1:23      192.31.7.1:23
icmp 209.165.201.18:24 192.168.1.21:24    192.31.7.1:24      192.31.7.1:24
icmp 209.165.201.18:25 192.168.1.20:25    192.31.7.1:25      192.31.7.1:25
icmp 209.165.201.18:26 192.168.1.20:26    192.31.7.1:26      192.31.7.1:26
icmp 209.165.201.18:27 192.168.1.20:27    192.31.7.1:27      192.31.7.1:27
icmp 209.165.201.18:28 192.168.1.20:28    192.31.7.1:28      192.31.7.1:28
```

Reflexión

¿Qué ventajas tiene la PAT?

Lo que hace PAT ya no utiliza IPs simplemente utiliza su interface que tiene asignada una sola IP y que no utiliza un rango de IPs para diferenciar cada paquete que sale, sino un rango de puertos, por eso se llama PAT (port address translation).

Al utilizarse una sola 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, y hay seguridad porque el ISP no puede hacer ping a ninguna de las computadoras por que no las conoce, solo conoce la translation por la IP que ha salido y el puerto. El ISP solo puede responder solicitudes, pero no puede hacer solicitudes ni a PC-A, ni a PC-B ni a PC-C

CONCLUSIONES

- Con el desarrollo de la presente practica se logró conocer que con los ACLs de IPv6 podremos bloquear o impedir el acceso y/o permitir acceso según configuración de dicha listas, lo que nos favorece redundando en la seguridad de la red que estemos administrando.

- Se logra aprender y permitir el direccionamiento mediante interfaces específicas en el router que estemos trabajando, y como evidenciamos en la práctica podremos evitar fallas generadas por presencia de bucles en los host.

- La finalidad de algunos laboratorios vistos en este momento 7, fue el manejo de la configuración de direccionamiento IPV6 en un host mediante SLAACs y la configuración del protocolo DHCPv6 que establece automáticamente los direccionamientos a los host, pero para esta actividad se especificó los dos usos de DHCPv6 que son con estado y sin estado donde con estado toda la información de direccionamiento debe obtenerse desde el servidor DHCPv6 y sin estado no utiliza el servidor.

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