Paso 7 – Actividad Colaborativa 4

Enrutamiento En Soluciones De Red

Viviana Stefany González Muriel Código. 1’114.83.1465

Julián José Arara Castillo Código: 94.042.200

Erlin Walter Hurtado Hensen Código 94.309.999

Joan Sebastian Ocampo Código 87.064.165

Tutor: José Ignacio Cardona

Grupo: 203092_22

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

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

PALMIRA

2017

Introducción

El presente es el cuarto trabajo del diplomado de profundización CISCO donde se logra interiorizar de manera práctica, conceptos fundamentales para el buen desarrollo del proceso de aprendizaje. Con esto se busca identificar y solucionar problemas propios de enrutamiento mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces. Así pues, se exponen y realizan 14 ejercicios los cuales van desde el enrutamiento dinámico, OSPF de una sola área, listas de control de acceso, DHCP y traducción de direcciones IP para IPv4, entre otras.

El proceso empieza con una práctica de laboratorio donde se realiza una configuración básica de RIPv2 y RIPng mostrando una topología sencilla de tres routers, dos de ellos con switches y un computador por cada uno y el último sólo con un dispositivo final (PC) conectado directamente. Como es conocido, RIP versión 2 o RIPv2 es un protocolo de routing vector distancia sin clase y es utilizado para el enrutamiento de direcciones IPv4 en redes pequeñas. Por su parte, RIP de última generación o RIPng es un protocolo de routing vector distancia para enrutar direcciones IPv6. Ambos tienen la misma distancia administrativa y limitación de 15 saltos.

El segundo ejercicio trata sobre la configuración de OSPFv2 básico de área única donde se configura una 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. El tercer ejercicio es similiar al segundo, la diferencia es que se configurará OSPFv3, 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 el cuarto ejercicio se debe configurar una IP ACL's para mitigar ataques donde verificará la conectividad entre dispositivos antes de la configuración del firewall, se usará ACL´s para asegurar que el acceso remoto a los enrutadores esté disponible solo desde una estación de administración específica, se configurarán ACL's en routers y se verificarán la funcionalidad de los ACL's creados. En el siguiente ejercicio, se realizará una configuración de una ACL estándar. Las listas de control de acceso (ACL) estándar son secuencias de comandos de configuración de enrutadores que controlan si un enrutador permite o niega paquetes en función de la dirección de origen. Posteriormente se configurará una ACL nobrada estándar en donde un administrador senior de la red ha encargado que se cree una ACL estándar para evitar el acceso a un servidor de archivos. Debe denegarse el acceso a todos los clientes de una red y una estación de trabajo específica de una red diferente.

Como siguiente ejercicio, se configurará una ACL en las líneas VTY donde como administrador de red, debe tener acceso remoto al enrutado o router. Este acceso no debe estar disponible para otros usuarios de la red. Por lo tanto, se configurará y aplicará una lista de control de acceso (ACL) que permite a una PC el acceso a las líneas Telnet, pero niega todas las otras direcciones IP de origen. Como finalización de la parte de ACL, se configurara una ACL para IPv6 donde según la topología, los registros indican que una computadora en la red 2001: DB8: 1: 11 :: 0/64 está actulizando repetidamente su página web, lo que causa un ataque

de denegación de servicio (DoS) contra el Server3. Hasta que el cliente pueda ser identificado y limpiado, se debe bloquear el acceso HTTP y HTTPS a esa red con una lista de acceso.

A continuación, se realizará la configuración de DHCPv4 básico en un router, donde según la situación y topología presentada, una 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. Luego, se realizará la configuración de DHCPv4 en un switch configurará DHCPv4 para VLAN únicas y múltiples en un switch Cisco 2960, se habilitará el routing en el switch para permitir la comunicación entre las VLAN y se agregará rutas estáticas para permitir la comunicación entre todos los hosts. Siguiendo, se configurará DHCPv6 sin estado y con estado, donde primero se configurará la red para que utilice SLAAC. Una vez que se verificó la conectividad, se configurarán los parámetros de DHCPv6 y se modificará la red para que utilice DHCPv6 sin estado y una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado.

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. DHCPv4 es para IPv4 y DHCPv6 es para IPv6.

En el siguiente ejercicio, se muestra una situación con IdT y DHCP en donde se debe configurar un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP. Conectados a este, deben haber cinco dispositivos de hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Se configurarán las terminales para solicitar direcciones DHCP del servidor de DHCP y se presentarán las respectivas reflexiones.

Como penúltimo ejercicio, se configurará NAT dinámica y estática. 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. El ejercicio consiste en que una ISP proporciona 30 direcciones IP públicas a una empresa en el espacio de direcciones IP públicas 209.165.200.224/27. Se debe seleccionar un rango para la asignación estática y el otro rango para la asignación dinámica.

En el útlimo ejercicio, se configurará un conjunto de NAT con sobrecarga y PAT. Este se divide en dos parte, en la primera se entrega un rango de direcciones IP públicas y se realiza NAT con sobrecarga. La segunda parte consta de la entrega de una única dirección IP para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Se usará la traducción de la dirección del puerto (PAT) para convertir varias direcciones internas en la única dirección pública utilizable.

Objetivos

Objetivo general

Interiorizar de manera práctica, conceptos fundamentales para el buen desarrollo del proceso de aprendizaje teniendo como base los temas vistos en la unidad cuatro del diplomado de profundización CISCO.

Objetivos específicos

- Identificar y solucionar problemas propios de enrutamiento mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces.
- Realizar y practicar el enrutamiento dinámico, OSPF de una sola área, DHCP y traducción de direcciones IP para IPv4.
- Configurar, aplicar y verificar el funcionamiento de las ACL’s.

7.3.2.4 Práctica de laboratorio - Configuración básica de RIPv2 y RIPng

Topología

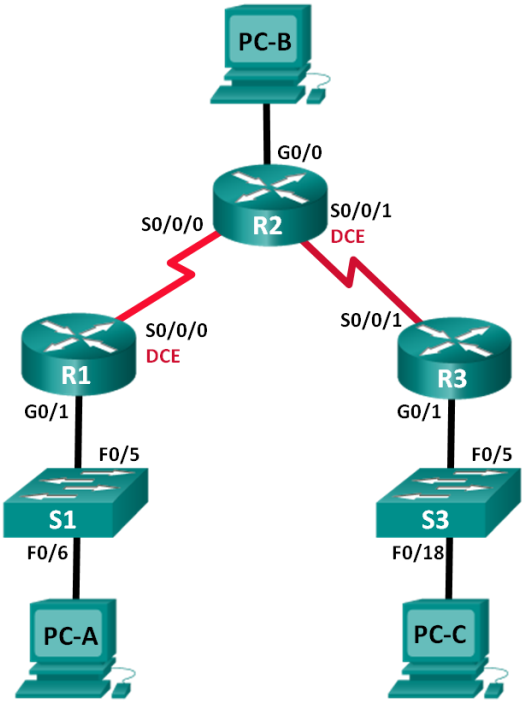


Tabla de direccionamiento

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

Información básica/situación

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

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

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

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

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

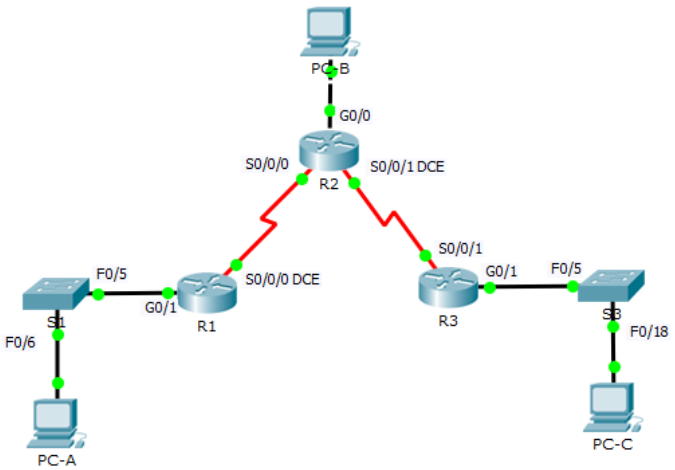
Recursos necesarios

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

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

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

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



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

Respuesta. Como el laboratorio se realiza en PT, no se hace necesario inicializar y volver a cargar los routers o switches

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.

Configuración de los routers

```
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#service password-encryption
R1(config)#enable secret class
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging sunchronous
                           ^
% Invalid input detected at '^' marker.

R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo para personal autorizado#

R1(config)#interface g0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
R1(config-if)#description LAN connection to S1
R1(config-if)#no shutdown

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

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

R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#description connection to R2
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

```
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#service password-encryption
R2(config)#enable secret class
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo para personal autorizado#

R2(config)#int g0/0
R2(config-if)#ip address 209.165.201.1 255.255.255.0
R2(config-if)#description LAN connection to PC-B
R2(config-if)#no shutdown

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

R2(config-if)#exit
```

```
R2(config)#int s0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#description connection to 10.1.1.1 R1
R2(config-if)#no shutdown

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

R2(config-if)#int s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

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
R2(config-if)#description connection to 10.2.2.1 R3
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exi
R2(config)#copy r s
                ^
% Invalid input detected at '^' marker.

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

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

```
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#service password-encryption
R3(config)#enable secret class
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo para personal autorizado#

R3(config)#int g0/1
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#description LAN connection to S3
R3(config-if)#no shutdown

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)#description connection to 10.2.2.2 R2
R3(config-if)#no shutdown

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

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

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

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

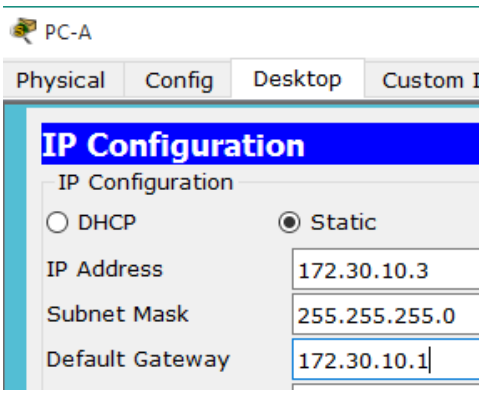
Configuración de los switches

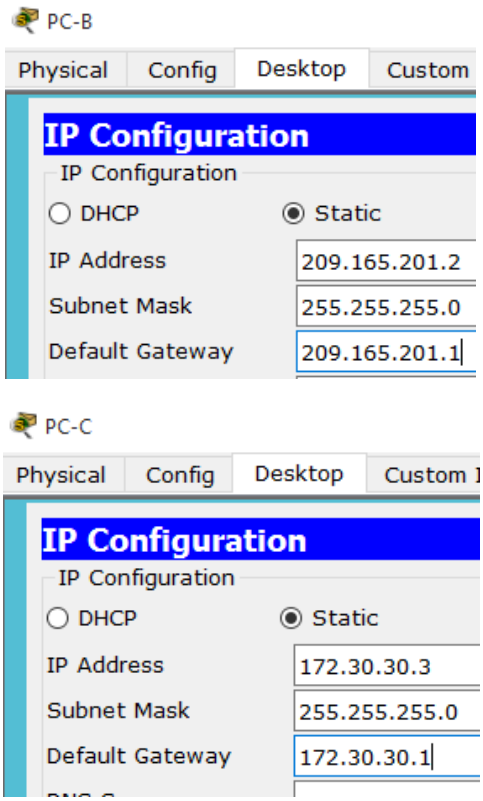
```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#service password-encryption
S1(config)#enable secret class
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#

S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#service password-encryption
S3(config)#enable secret class
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#

S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

Paso 4. Configurar los equipos host.

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

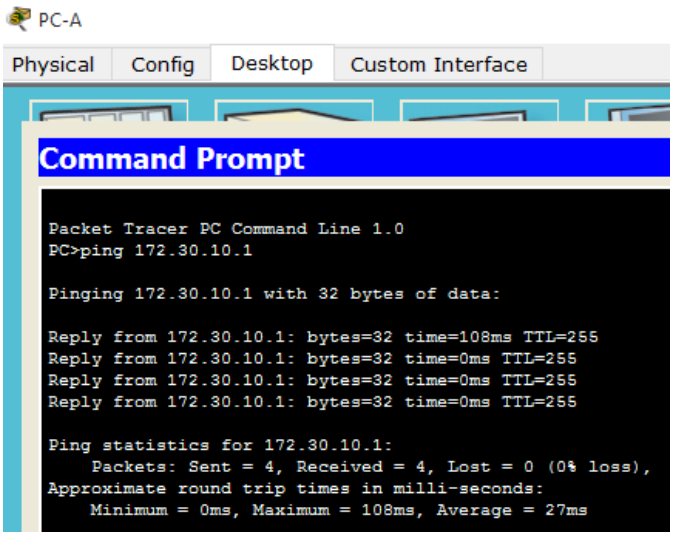


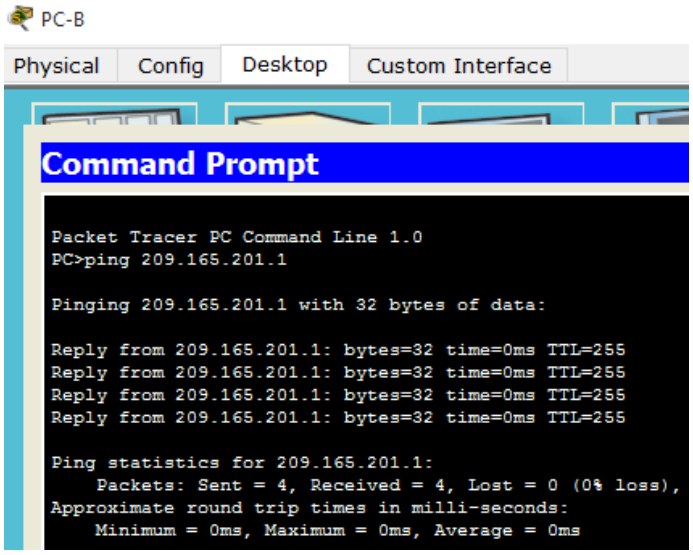


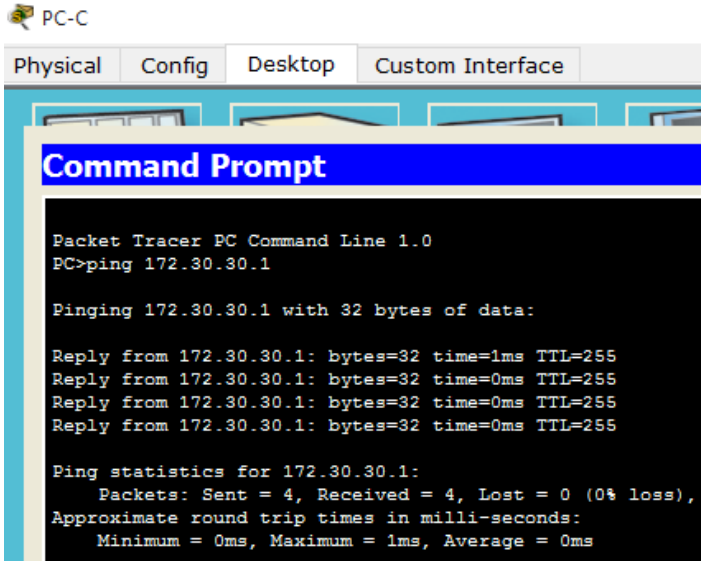
Paso 5. Probar la conectividad.

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.

```
R1#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

```
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

R2#ping 10.2.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

```
R3#ping 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/15 ms
```

Parte 2: Configurar y verificar el routing RIPv2

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

Paso 1. Configurar el enrutamiento RIPv2.

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

R1# config t

R1(config)# router rip

R1(config-router)# version 2

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

R1(config-router)# network 172.30.0.0

R1(config-router)# network 10.0.0.0

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

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

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

```
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)#passive-interface g0/1
R3(config-router)#network 172.30.0.0
R3(config-router)#network 10.0.0.0
```

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

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
```

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

Paso 2. Examinar el estado actual de la red.

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

R2# show ip interface brief

```
R2#show ip interface 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
```

b. Verifique la conectividad entre las computadoras.

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

Respuesta. De la PC-A no se puede hacer ping a PC-B ya que no hay una ruta que llegue a PC-B y como se pudo observar, esta red no está participando en RIP

```
PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Request timed out.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.

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

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

Respuesta. No se puede hacer ping ya que en el R1 y R3 no existe una ruta para la red específica

```
PC>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.

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

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

Respuesta. De la PC-C no se puede hacer ping a PC-B ya que no hay una ruta que llegue a PC-B y como se pudo observar, esta red no está participando en RIP

```
PC>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

Respuesta. No se puede hacer ping ya que en el R3 y R1 no existe una ruta para la red específica

```
PC>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

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

c. Verifique que RIPv2 se ejecute en los routers.

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

R1# show ip protocols

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 22 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      00:00:16
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?

Respuesta. Muestra las actualizaciones del protocolo. Las envía por dirección multicast vía los puertos

```
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

R2#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: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
```

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

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

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

Respuesta. Después de la información de las interfaces aparece un espacio donde muestra la información de RIPv2

```
!
router rip
 version 2
 passive-interface GigabitEthernet0/1
 network 10.0.0.0
 network 172.30.0.0
!
```

d. Examinar la 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, 00:00:08, Serial0/0/1
                   [120/1] via 10.1.1.1, 00:00:18, Serial0/0/0
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

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

R1# show ip route

```
R1#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, 00:00:26, Serial0/0/0
     172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
```

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

R3# show ip route

```
R3#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, 00:00:04, 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#debug ip rip
RIP protocol debugging is on
R2#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: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0

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

Paso 3. Desactivar la sumarización automática.

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

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

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

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

R1(config-router)# end

R1# clear ip route *

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

R1#clear ip route *
```

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

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

R2# show ip route

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:56, Serial0/0/1
                      is possibly down, routing via 10.1.1.1, Serial0/0/0
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:16, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:00, Serial0/0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

R1# show ip route

```
R1#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, 00:00:20, 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, 00:00:20, Serial0/0/0
```

R3# show ip route

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:22, 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, 00:00:22, 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

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

R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.30.0/24 via 0.0.0.0 in 1 hops

R2#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
```

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

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

Respuesta. 172.30.30.0/24 y 172.30.10.0/24 sin clase

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

Respuesta. Si, es correcto

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 t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

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)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 5. Verificar la configuración de enrutamiento.

c. Consulte la tabla de routing en el R1.

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 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, 00:00:23, 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, 00:00:23, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:23, 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?

Respuesta. Como se puede observar, hay un Gateway de last resort, esto quiere decir que existe una puerta de enlace que hace que se conecte a internet y la ruta por defecto que se muestra en la tabla de ruteo está aprendida por 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?

Respuesta. El R2 tiene una ruta estática predeterminada para 0.0.0.0 vía 209.165.201.2 la cual está directamente conectada a G0/0

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

Gateway of last resort is 209.165.201.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
     172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:01, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:20, 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?

Respuesta. Si, es correcto

```
PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=2ms TTL=126
Reply from 209.165.201.2: bytes=32 time=12ms TTL=126
Reply from 209.165.201.2: bytes=32 time=11ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 6ms
```

```
PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

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

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 3ms
```

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?

Respuesta. Es correcto, los pings fueron satisfactorios

```
PC>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=3ms TTL=125
Reply from 172.30.30.3: bytes=32 time=11ms 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
```

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

Parte 3: Configurar IPv6 en los dispositivos

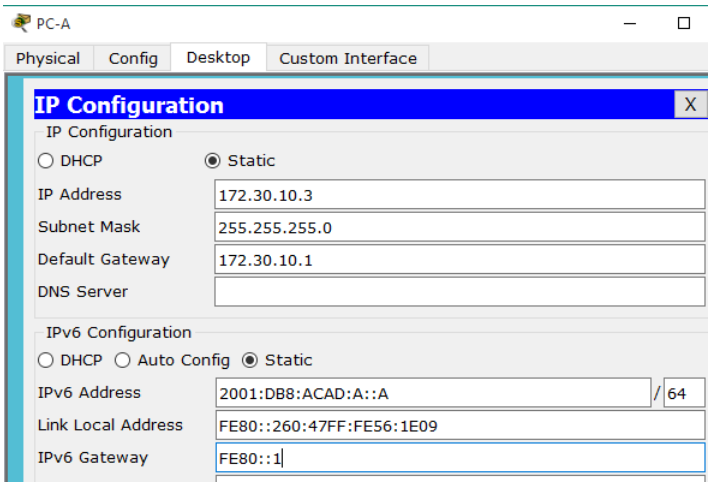
En la parte 3, configurará todas las interfaces con direcciones IPv6 y verificará la conectividad.

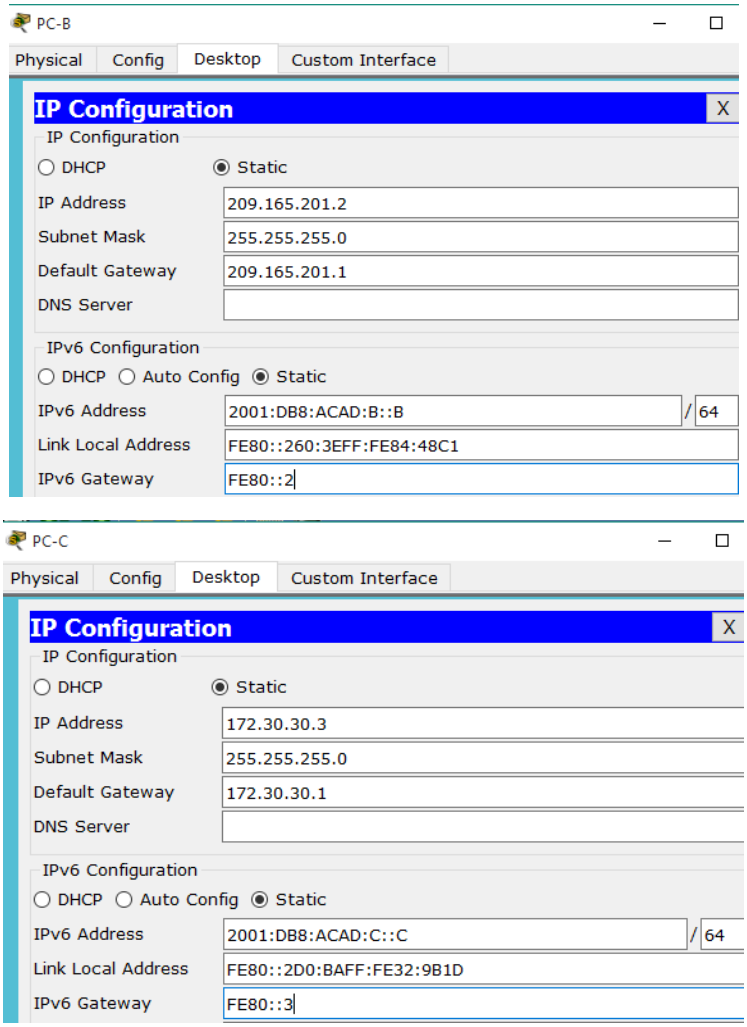
Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6/longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:BD8:ACAD:A::1/64 FE80::1 link-local	N/A
	S0/0/0	2001:BD8:ACAD:12::1/64 FE80::1 link-local	N/A
R2	G0/0	2001:BD8:ACAD:B::2/64 FE80::2 link-local	N/A
	S0/0/0	2001:BD8:ACAD:12::2/64 FE80::2 link-local	N/A
	S0/0/1	2001:BD8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	G0/1	2001:BD8:ACAD:C::3/64 FE80::3 link-local	N/A
	S0/0/1	2001:BD8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A	NIC	2001:BD8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:BD8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:BD8:ACAD:C::C/64	FE80::3

Paso 1. Configurar los equipos host.

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





Paso 2. Configurar IPv6 en los routers.

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

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.

```
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#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)#no shutdown
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R2(config)#ipv6 unicast-routing
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 shutdown
R2(config-if)#exit
R2(config)#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 shutdown
R2(config-if)#exit
R2(config)#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)#no shutdown
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R3(config)#ipv6 unicast-routing
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)#exit
R3(config)#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 shutdown
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

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.

Respuesta. El comando que se usó fue ***show ipv6 interface brief*** o ***show run***

```
R1#show ipv6 interface 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]
```

```
.
interface GigabitEthernet0/1
 description LAN connection to S1
 ip address 172.30.10.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
!
interface Serial0/0/0
 description connection to R2
 ip address 10.1.1.1 255.255.255.252
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:12::1/64
 clock rate 128000
```

```
R2#show ipv6 interface 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]
```

```
interface GigabitEthernet0/0
 description LAN connection to PC-B
 ip address 209.165.201.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:B::2/64
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description connection to 10.1.1.1 R1
 ip address 10.1.1.2 255.255.255.252
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:12::2/64
!
interface Serial0/0/1
 description connection to 10.2.2.1 R3
 ip address 10.2.2.2 255.255.255.252
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:23::2/64
 clock rate 128000
```

```
R3#show ipv6 interface brief
GigabitEthernet0/0         [administratively down/down]
GigabitEthernet0/1         [up/up]
    FE80::3
    2001:DB8:ACAD:C::3
Serial0/0/0                [administratively down/down]
Serial0/0/1                [up/up]
    FE80::3
    2001:DB8:ACAD:23::3
Vlan1                      [administratively down/down]
```

```
interface GigabitEthernet0/1
 description LAN connection to S3
 ip address 172.30.30.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:C::3/64
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 description connection to 10.2.2.2 R2
 ip address 10.2.2.1 255.255.255.252
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:23::3/64
```

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

```
PC>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=36ms 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=0ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

```
PC>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=0ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time=0ms 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 = 1ms, Average = 0ms
```

```
PC>ping 2001:DB8:ACAD:C::3

Pinging 2001:DB8:ACAD:C::3 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::3: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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

```
R1#ping 2001:DB8:ACAD:12::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/7 ms


R2#ping 2001:DB8:ACAD:23::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7 ms
```

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(config)#int g0/1
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#exit
```

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(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#exit
R2(config)#int s0/0/1
R2(config-if)#ipv6 rip Test2 enable
R2(config-if)#end
```

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

```
R3(config)#int g0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#exit
R3(config)#int s0/0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

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
```

¿En qué forma se indica RIPng en el resultado?

Respuesta. El RIPng está indicado por el nombre del proceso “rip Test1”

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

R1# show ipv6 rip Test1

```
R1#show ipv6 rip Test1
                   ^
% Invalid input detected at '^' marker.
```

Respuesta. PT no soporta el comando

¿Cuáles son las similitudes entre RIPv2 y RIPng?

Respuesta. Tanto RIPv2 y RIPng usan la métrica como conteo de saltos, tienen una distancia administrativa de 120 y envían actualizaciones cada 30 segundos.

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

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?

Respuesta. En el R1 se descubrieron 2 rutas mediante RIPng

```
R1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:DB8:ACAD:A::/64 [0/0]
     via GigabitEthernet0/1, 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, 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
R   2001:DB8:ACAD:23::/64 [120/2]
     via FE80::2, Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

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

Respuesta. En el R2 se descubrieron 2 rutas mediante RIPng

```
R2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:DB8:ACAD:A::/64 [120/2]
     via FE80::1, Serial0/0/0, 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
R   2001:DB8:ACAD:C::/64 [120/2]
     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
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?

Respuesta. En el R3 se descubrieron 2 rutas mediante RIPng

```
R3#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:DB8:ACAD:A::/64 [120/3]
     via FE80::2, Serial0/0/1, receive
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, 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
```

g. Verifique la conectividad entre las computadoras.

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

Respuesta. No, no es posible

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

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

Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

Respuesta. Si, es posible

```
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=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=17ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms 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 = 17ms, Average = 8ms
```

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

Respuesta. No, no es posible

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

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

Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Reply from 2001:DB8:ACAD:C::3: Destination host unreachable.
Request timed out.
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?

Respuesta. Si, es posible

```
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=3ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=14ms 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=12ms 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 = 3ms, Maximum = 14ms, Average = 10ms
```

¿Por qué algunos pings tuvieron éxito y otros no?

Respuesta. El ping falló a la PC-B ya que no hay una ruta configurada para la red 2001:DB8:ACAD:B::/64

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

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

Respuesta. El comando que se usó fue ipv6 route ::/0 2001:DB8:ACAD:B::B

```
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

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)#int s0/0/0
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#exit
R2(config)#int s0/0/1
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 3. Verificar la configuración de enrutamiento.

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

R2# show ipv6 route

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

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

Respuesta. Ya que como se observa en la tabla de ruteo del R2, se cuenta con una ruta estática predeterminada determinada por la letra S.

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

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

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

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

Respuesta. La ruta para el tráfico de Internet se proporciona con RIPng con una métrica de 2

Paso 4. Verifique la conectividad.

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

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

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

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

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

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

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=12ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 8ms
```

¿Tuvieron éxito los pings?

Respuesta. Si, es correcto

Reflexión

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

   Respuesta. La idea de deshabilitar la sumarización automática para RIPv2 es no resumir las redes a su dirección con clase en routers fronterizos. Así, RIPv2 incluye todas las subredes y sus máscaras correspondientes en sus actualizaciones de routing.

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

   Respuesta. Tanto R1 y R3 descubrieron la ruta a Internet por las actualizaciones de RIP recibidas desde el R2 donde se configuró la ruta estática predeterminada

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

   Respuesta. RIPng se habilita en una interfaz y RIPv2 en el modo de configuración del router. El proceso de propagación de una ruta predeterminada en RIPng es parecido a RIPv2, excepto que en RIPng se debe especificar una ruta estática predeterminada IPv6.

8.2.4.5 Práctica de laboratorio - Configuración de OSPFv2 básico de área única

Topología

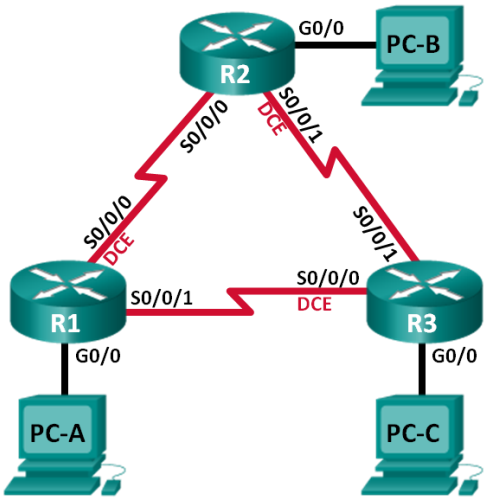


Tabla de direccionamiento

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

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.

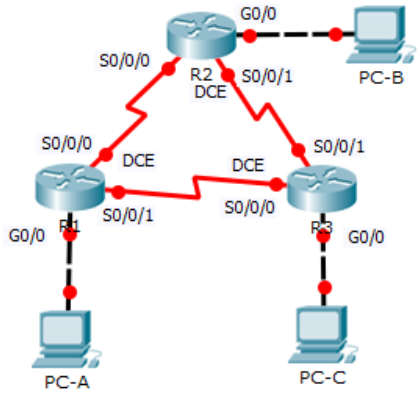
Recursos necesarios

- 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.

Respuesta. Como el laboratorio se realiza en PT, no se hace necesario inicializar y volver a cargar los routers.

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)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#

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

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)#exit
R1(config)#int s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

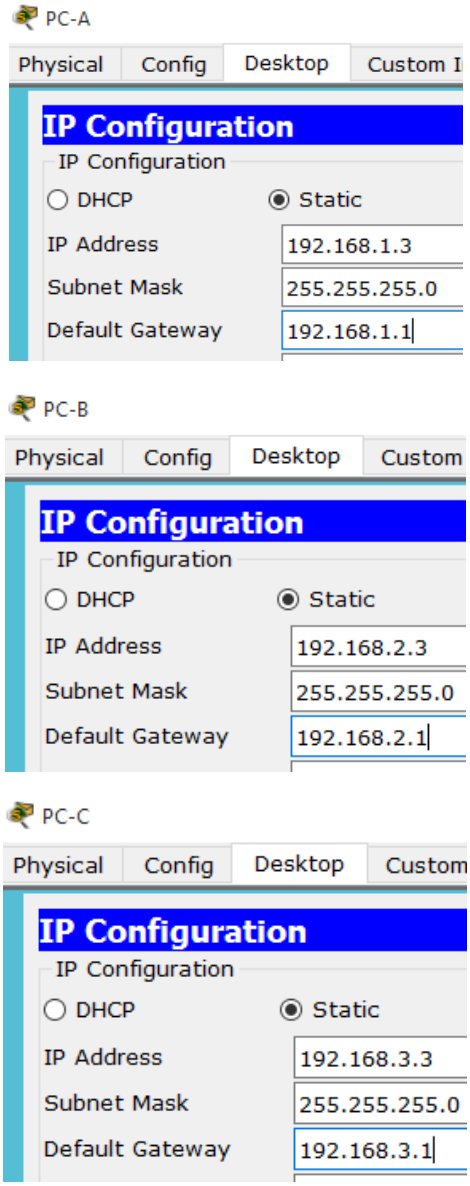
```
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#

R2(config)#int g0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown

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)#exit
```

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

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

R2(config-if)#exit
R2(config)#int s0/0/
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
0
R2(config)#int s0/0/1
R2(config-if)#ip address 192.168.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

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

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

```
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#service password-encryption
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#banner motd#
                       ^
% Invalid input detected at '^' marker.

R3(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#
```

```
R3(config)#int s0/0/0
R3(config-if)#ip address 192.168.13.2 255.255.255.252
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R3(config-if)#exit
R3(config)#int s0/0/1
R3(config-if)#ip address 192.168.23.2 255.255.255.252
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R3(config-if)#exit
R3(config)#int g0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown

R3(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
```

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.

PC-A

Physical | Config | Desktop | Custom Interface

Command Prompt

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

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

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

PC-B

Physical | Config | Desktop | Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>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=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms 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 = 1ms, Average = 0ms
```

PC-C

Physical | Config | Desktop | Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=1ms TTL=255
Reply from 192.168.3.1: bytes=32 time=0ms TTL=255
Reply from 192.168.3.1: bytes=32 time=0ms TTL=255
Reply from 192.168.3.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
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 = 1/7/18 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 = 1/9/22 ms


R2#ping 192.168.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms

R2#ping 192.168.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/15 ms

R3#ping 192.168.13.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/10 ms

R3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms
```

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

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

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(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
```

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(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
R2(config-router)#network 192.168.23.0 0.0.0.3 area 0
00:55:07: %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
```

```
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)#
00:53:54: %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)#
00:54:04: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/1 from LOADING
to FULL, Loading Done


R1(config-router)#
00:55:13: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING
to FULL, Loading Done

R1(config-router)#
00:56:50: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

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
192.168.23.1      0   FULL/  -        00:00:38    192.168.12.2    Serial0/0/0
192.168.23.2      0   FULL/  -        00:00:37    192.168.13.2    Serial0/0/1
```

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, 00:04:23, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:02:46, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:02:36, Serial0/0/0
                        [110/128] via 192.168.13.2, 00:02:36, Serial0/0/1
```

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

Respuesta. Para visualizar solamente las rutas OSPF en la table de routing se usaría el comando ***show ip route ospf***

```
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 00:08:50, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:07:14, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.12.2, 00:07:04, Serial0/0/0
                     [110/128] via 192.168.13.2, 00:07:04, Serial0/0/1
```

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
    192.168.13.1         110      00:08:11
    192.168.23.1         110      00:08:01
    192.168.23.2         110      00:08:01
  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 8 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x00c59a
        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

Respuesta. PT no soporta el comando

```
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 00:00:01
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 192.168.13.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.1
  Suppress hello for 0 neighbor(s)
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 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)
```

Paso 7: Verificar la conectividad de extremo a extremo.

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

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=9ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 3ms

PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 3ms
```

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=3ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms 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 = 3ms, Average = 1ms

PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=12ms TTL=126
Reply from 192.168.3.3: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 4ms
```

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=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=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 = 2ms, Average = 1ms

PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=16ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=3ms 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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 6ms
```

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

Parte 3: Cambiar las asignaciones de ID del router

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

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

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

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

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

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

R1(config)# interface lo0

R1(config-if)# ip address 1.1.1.1 255.255.255.255

R1(config-if)# end

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

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

R3#copy 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]

R2#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1

R3#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1
```

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      00:03:26
    2.2.2.2              110      00:03:26
    3.3.3.3              110      00:03:26
  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

```
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/  -        00:00:30    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#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R1#
00:10:19: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Adjacency forced to reset

00:10:19: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

00:10:19: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Adjacency forced to reset

00:10:19: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
```

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]:

R2#yes
Translating "yes"
% Unknown command or computer name, or unable to find computer address

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

R2#
00:11:48: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Adjacency forced to reset

00:11:48: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

00:11:48: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Adjacency forced to reset

00:11:48: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 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#
00:12:59: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Adjacency forced to reset

00:12:59: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

00:12:59: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Adjacency forced to reset

00:12:59: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on Serial0/0/1 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

```
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      00:13:54
    2.2.2.2              110      00:03:52
    3.3.3.3              110      00:02:15
    11.11.11.11          110      00:01:02
    22.22.22.22          110      00:01:02
    33.33.33.33          110      00:01:02
  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

```
R1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       0   FULL/  -        00:00:39    192.168.12.2    Serial0/0/0
33.33.33.33       0   FULL/  -        00:00:38    192.168.13.2    Serial0/0/1
```

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

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

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  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)# router ospf 1

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

```
R1(config)#router ospf 1
R1(config-router)#passive-interface g0/0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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 interface g0/0

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

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

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

Gateway of last resort is not set

     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:13:05, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/65] via 192.168.23.2, 00:13:05, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
     192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0/30 [110/128] via 192.168.23.2, 00:13:05, Serial0/0/1
                        [110/128] via 192.168.12.1, 00:13:05, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.1/32 is directly connected, Serial0/0/1
---

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, 00:14:11, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:14:11, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:14:11, Serial0/0/0
                        [110/128] via 192.168.23.1, 00:14:11, Serial0/0/1
     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
```

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

```
R1#show ip ospf neighbor


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

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)#
00:24:50: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

00:24:50: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Interface down or detached

R2(config-router)#
```

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

R1# show ip ospf neighbor

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:30    192.168.13.2    Serial0/0/1
```

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 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
```

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, 00:08:40, 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, 00:05:50, 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, 00:09:13, 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, 00:05:53, 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
```

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)#
00:32:21: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING
to FULL, Loading Done

R2(config-router)#
```

g. Vuelva a emitir los comandos ***show ip route*** y ***show ip 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, 00:04:11, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:11, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:04:11, Serial0/0/0
                        [110/128] via 192.168.13.2, 00:04:11, Serial0/0/1
R1#show ip ospf neighbor


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

```
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, 00:05:09, Serial0/0/0
O    192.168.2.0/24 [110/129] via 192.168.13.1, 00:04:59, 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, 00:05:09, 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#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
11.11.11.11       0   FULL/  -        00:00:36    192.168.13.1    Serial0/0/0
```

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

Respuesta. Para llegar a la red 192.168.2.0/24, el R3 usa la interfaz S0/0/0

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

Respuesta. La métrica de costo acumulado para la red 192.168.2.0/24 en el R3 es de 129

¿El R2 aparece como vecino OSPF en el R1?

Respuesta. Como se puede observar, el R2 sí aparece como vecino del R1

¿El R2 aparece como vecino OSPF en el R3?

Respuesta. Como se puede observar, el R2 no aparece como vecino del R3

¿Qué indica esta información?

Respuesta. El tráfico de la red 192.168.2.0/24 puede llegar al R3 pero por el R1. La S0/0/1 del R2 sigue estando como interfaz pasiva así que la información OSPF no se está enviando por esa interfaz

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

Respuesta. Los comandos que se usaron fueron ***router ospf 1*** y ***no passive-interface s0/0/1***

```
R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/1
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
02:15:29: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

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

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

Gateway of last resort is not set

     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.13.1, 00:19:11, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.23.1, 00:01:21, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.23.1, 00:01:21, Serial0/0/1
                        [110/128] via 192.168.13.1, 00:01:21, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
```

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

Respuesta. Para llegar a la red 192.168.2.0/24, el R3 usa la interfaz S0/0/1

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

Respuesta. La métrica de costo acumulado para la red 192.168.2.0/24 en el R3 es de 65

¿El R2 aparece como vecino OSPF del R3?

Respuesta. Si, el R2 aparece como vecino OSPF del R3

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
11.11.11.11       0   FULL/  -        00:00:36    192.168.13.1    Serial0/0/0
22.22.22.22       0   FULL/  -        00:00:35    192.168.23.1    Serial0/0/1
```

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 interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 000c.cf2a.7d01 (bia 000c.cf2a.7d01)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 1017 multicast, 0 pause input
     0 input packets with dribble condition detected
     57 packets output, 3648 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, 00:33:21, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:33:21, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.12.2, 00:33:21, Serial0/0/0
                     [110/128] via 192.168.13.2, 00:33:21, 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

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

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

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 interface s0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  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)
```

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.
R1(config-router)#
```

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.
R2(config-router)#
```

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

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

R3# show ip ospf interface g0/0

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

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 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 00:00:05
  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 interface s0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 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 00:00:02
  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

```
R1#show ip route ospf
O    192.168.2.0 [110/6576] via 192.168.12.2, 00:05:41, Serial0/0/0
O    192.168.3.0 [110/6576] via 192.168.13.2, 00:04:39, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/12952] via 192.168.12.2, 00:04:29, Serial0/0/0
                     [110/12952] via 192.168.13.2, 00:04:29, 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.

R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 100
% 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 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?

Respuesta. Para ayudar a OSPF a determinar la ruta correcta, se debe cambiar el ancho de banda de referencia a un valor superior, a fin de admitir redes con enlaces más rápidos que 100 Mb/s.

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 interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 54 bits/sec, 0 packets/sec
  5 minute output rate 54 bits/sec, 0 packets/sec
     577 packets input, 41624 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
     604 packets output, 42604 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 [110/65] via 192.168.12.2, 00:08:24, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:07:49, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.12.2, 00:07:39, Serial0/0/0
                     [110/128] via 192.168.13.2, 00:07:39, 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)#int s0/0/0
R1(config-if)#bandwidth 128
```

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

R1# show ip route ospf

```
R1#show ip route ospf
O    192.168.2.0 [110/129] via 192.168.13.2, 00:00:17, Serial0/0/1
O    192.168.3.0 [110/65] via 192.168.13.2, 00:09:12, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 00:00:17, 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

Respuesta. PT no soporta el comando así que se usa ***show ip ospf interface***

```
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 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 00:00:09
  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 22.22.22.22
  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 [110/782] via 192.168.12.2, 00:00:22, Serial0/0/0
O    192.168.3.0 [110/782] via 192.168.13.2, 00:00:22, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/845] via 192.168.12.2, 00:00:22, Serial0/0/0
                     [110/845] via 192.168.13.2, 00:00:22, 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.

Respuesta. El proceso se hace de la siguiente manera: Costo a 192.168.3.0/24: S0/0/1 del R1 + G0/0 del R3 (781+1=782). Costo a 192.168.23.0/30: S0/0/1 del R1 y S0/0/1 del R3 (781+64=845).

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 [110/65] via 192.168.13.1, 00:18:18, Serial0/0/0
O    192.168.2.0 [110/65] via 192.168.23.1, 00:18:18, Serial0/0/1
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0 [110/128] via 192.168.23.1, 00:09:23, Serial0/0/1
```

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

```
R3(config)#int s0/0/0
R3(config-if)#bandwidth 128
R3(config-if)#int s0/0/1
R3(config-if)#bandwidth 128
```

```
R2(config)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/1
R2(config-if)#ba
R2(config-if)#bandwidth 128
```

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

Respuesta El nuevo costo acumulado a la red 192.168.23.0/24 es 1562. Esto sucede ya que cada enlace serial tiene un costo de 781 y la ruta a la red 192.168.23.0/24 atraviesa dos enlaces seriales. 781 + 781 = 1562.

```
R1#show ip route ospf
O    192.168.2.0 [110/782] via 192.168.12.2, 00:08:14, Serial0/0/0
O    192.168.3.0 [110/782] via 192.168.13.2, 00:08:14, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:00:22, Serial0/0/0
                     [110/1562] via 192.168.13.2, 00:00:22, 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 [110/782] via 192.168.12.2, 00:09:43, Serial0/0/0
O    192.168.3.0 [110/782] via 192.168.13.2, 00:09:43, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:01:50, Serial0/0/0
                     [110/1562] via 192.168.13.2, 00:01:50, 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(config)#int s0/0/1
R1(config-if)#ip ospf cost 1565
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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 [110/782] via 192.168.12.2, 00:11:20, Serial0/0/0
O    192.168.3.0 [110/1563] via 192.168.12.2, 00:00:21, Serial0/0/0
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:00:21, Serial0/0/0
```

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.

Respuesta. La ruta a la red 192.168.3.0/24 en el R1 ahora atraviesa el R2 ya que es la ruta con el menor costo acumulado. La ruta con el menor costo acumulado es: S0/0/0 del R1 + S0/0/1 del R2 + G0/0 del R3 o 781 + 781 + 1 = 1563. Este es menor que el costo acumulado de S0/0/1 R1 + G0/0 R3 o 1565 + 1 = 1566.

Reflexión

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

   Respuesta. Las asignaciones de ID de router controlan el proceso de elección de router designado (DR) y router designado de respaldo (BDR) en una red de accesos múltiples. Si la ID del router está asociada a una interfaz activa, puede cambiar si la interfaz deja de funcionar. Por esta razón, se debe establecer con la dirección IP de una interfaz loopback (que siempre está activa) o con el comando ***router-id***

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

   Respuesta. El proceso de elección de DR/BDR no es preocupación en la práctica ya que los enlaces seriales que se usan son enlaces punto a punto, así que no se realiza una elección de DR/BDR. Sin embargo, si se contara con una red de accesos múltiples, como Ethernet o Frame Relay si se haría necesario el proceso de elección de DR/BDR

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

   Respuesta. Es necesario configurar una interfaz OSPF como pasiva ya que así se evita que se envíen los mensajes de routing por la interfaz especificada. Sin embargo, la red a la que pertenece la interfaz especificada se sigue anunciando en los mensajes de routing que se envían por otras interfaces.

8.3.3.6 Práctica de laboratorio – Configuración de OSPFv3 básico de área única

Topología

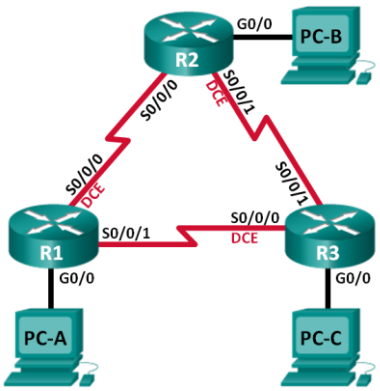


Tabla de direccionamiento

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

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

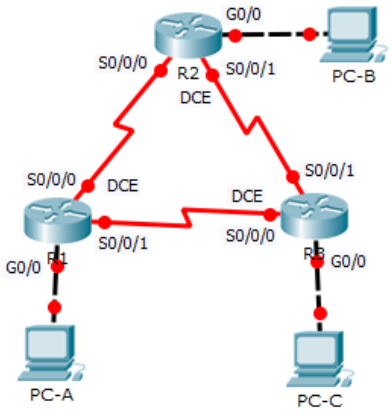
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

- 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.

Respuesta. Como se usa PT para realizar la práctica, no se hace necesario inicializar y volver a cargar los routers.

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.

```
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#service password-encryption
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#
```

```
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#service password-encryption
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#
```

```
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#service password-encryption
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#
```

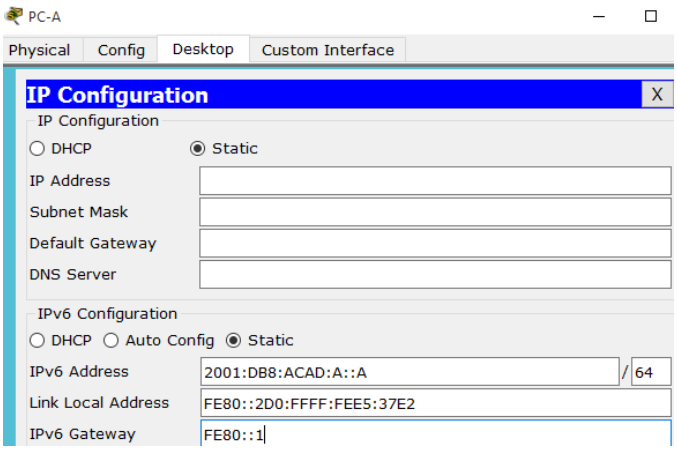
h. Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.
i. Habilite el routing de unidifusión IPv6 en cada router.
j. Copie la configuración en ejecución en la configuración de inicio

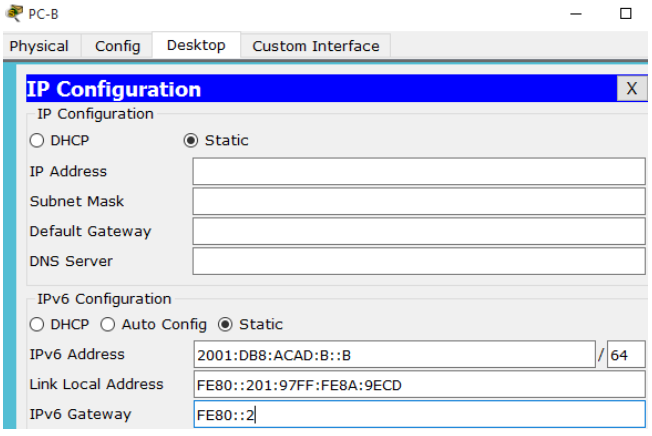
```
R1(config)#int g0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

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)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

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

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

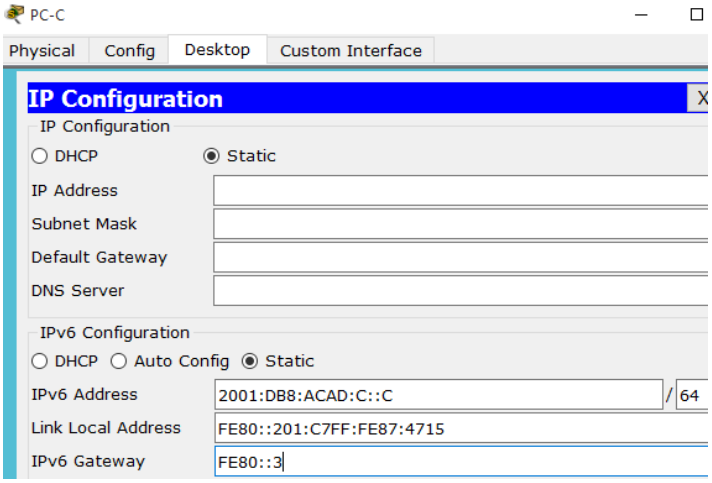
```
R2(config)#int g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

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 shutdown

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

R2(config-if)#int s0/0/1
%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
R2(config-if)#no shutdown

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

```
R3(config)#int g0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown

R3(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

R3(config-if)#int s0/0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:13::3/64
R3(config-if)#ipv6 FE80::3 link-local
                   ^
% Invalid input detected at '^' marker.

R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown

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

R3(config-if)#int s0/0/1
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown

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

Paso 4: Configurar los equipos host.

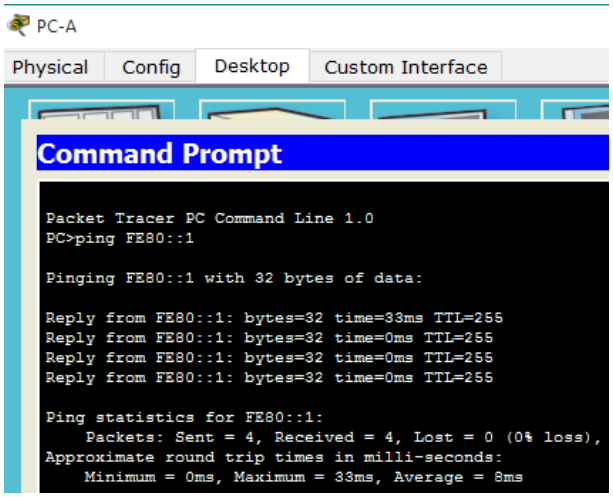


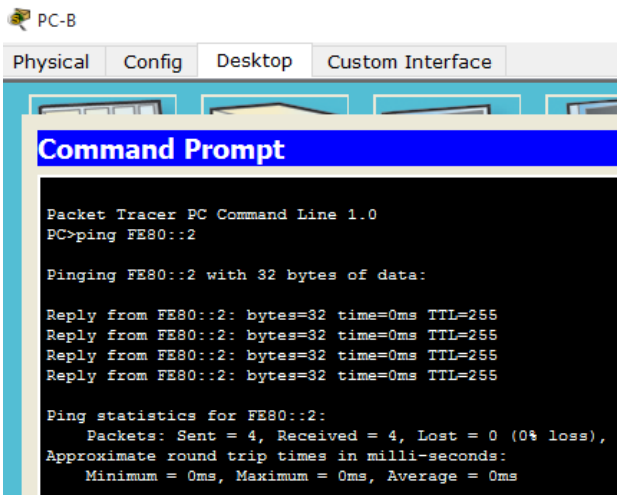


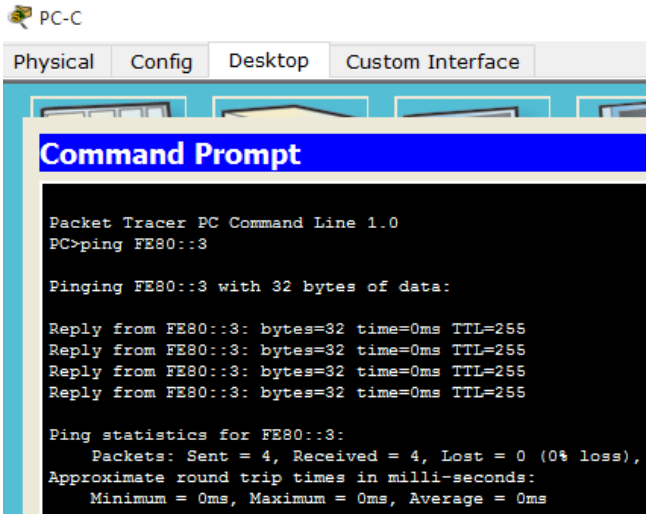


Paso 5: Probar la conectividad.

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.








```
R1#ping 2001:DB8:ACAD:12::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

R1#ping 2001:DB8:ACAD:13::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
```

```
R2#ping 2001:DB8:ACAD:12::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:12::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms

R2#ping 2001:DB8:ACAD:23::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/17 ms
```

```
R3#ping 2001:DB8:ACAD:13::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:13::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/10 ms

R3#ping 2001:DB8:ACAD:23::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:23::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/17 ms
```

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

```
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
```

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

```
R2(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure
manually
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
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
```

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

R2# show ipv6 ospf

```
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#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#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

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

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

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

```
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)#
00:59:39: %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)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
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)#int s0/0/1
01:00:54: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done

R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
01:00:56: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to
FULL, Loading Done

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

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

```
R1#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           0   FULL/  -        00:00:36    3               Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:35    3               Serial0/0/0
```

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 interface
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
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 00:00:07
  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 00:00:09
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
```

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

Respuesta. PT no admite el comando

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

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

```
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?

Respuesta. Para ver solo las rutas OSPF en la tabla de routing, se utiliza el comando ***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
```

Paso 7: Verificar la conectividad de extremo a extremo.

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

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

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

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=2ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

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=17ms 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=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 = 17ms, Average = 5ms
```

```
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=3ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=10ms 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=1ms 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 = 10ms, Average = 3ms

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=2ms 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=5ms 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>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=1ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=4ms TTL=126
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms 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 = 4ms, Average = 2ms

PC>ping 2001:db8:ACAD:B::B

Pinging 2001:db8:ACAD:B::B with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=8ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=3ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 3ms
```

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

Parte 3: Configurar las interfaces pasivas de OSPFv3

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

Paso 1: Configurar una interfaz pasiva.

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 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  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)
```

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

R1(config)# ipv6 router ospf 1

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

```
R1(config)#ipv6 router ospf 1
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

R1# show ipv6 ospf interface g0/0

```
R1#show ipv6 ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 1
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  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)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
01:30:54: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

01:30:54: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Interface down or detached

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

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/  -        00:00:34    3               Serial0/0/1
```

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

R2# show ipv6 ospf interface s0/0/0

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

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
```

```
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(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

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 [110/129]
     via FE80::3, Serial0/0/1, 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#show ipv6 ospf neighbor

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

```
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
R3#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/  -        00:00:35    4               Serial0/0/1
1.1.1.1           0   FULL/  -        00:00:33    4               Serial0/0/0
```

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

Respuesta. La interfaz que usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64 es la S0/0/1

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

Respuesta. La métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1 es de 129

¿El R2 aparece como vecino OSPFv3 en el R1?

Respuesta. Como se observa, el R2 no aparece como vecino OSPFv3 en el R1

¿El R2 aparece como vecino OSPFv3 en el R3?

Respuesta. Como se observa, el R2 sí aparece como vecino OSPFv3 en el R3

¿Qué indica esta información?

Respuesta. El tráfico de la red 2001:DB8:ACAD:B::/64 puede llegar al R1 pero por el R3. La S0/0/0 del R2 sigue estando como interfaz pasiva así que la información OSPF no se está enviando por esa 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(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.

```
R1#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           0   FULL/  -        00:00:30    3               Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:39    3               Serial0/0/0
```

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?

   Respuesta. Si. A pesar de que el ID de proceso sea diferente en los routers, se puede intercambiar información. La ID de proceso OSPFv3 se usa localmente en el router.

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

   Respuesta. Al eliminar el comando ***network*** en OSPFv3 ayuda a prevenir los errores en las direcciones IPv6. Esto es ya que una interfaz IPv6 puede tener múltiples direcciones IPv6 asignadas a la misma. Al asignar una interfaz a un área OSPFv3, todas las redes multicast en esa interfaz pueden ser asignadas automáticamente a esta y tendrán una ruta IPv6 creada en la tabla de routing.

4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks

Addressing Table

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

Background / Scenario

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

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

The routers have been pre-configured with the following:

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

Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

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

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

```
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=11ms TTL=125
Reply from 192.168.3.3: bytes=32 time=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 12ms, Average = 6ms
```

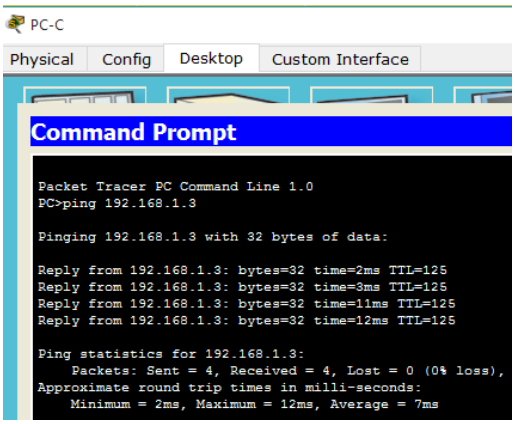
b. From the command prompt, establish a SSH session to R2 Lo0 interface (192.168.2.1) using username *SSHadmin* and password *ciscosshpa55*. When finished, exit the SSH session.

PC> ssh -l SSHadmin 192.168.2.1

```
SERVER>SSH -l SSHadmin 192.168.2.1
Open
Password:



R2#exit

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

Step 2: From PC-C, verify connectivity to PC-A and R2.

a. From the command prompt, ping PC-A (192.168.1.3).

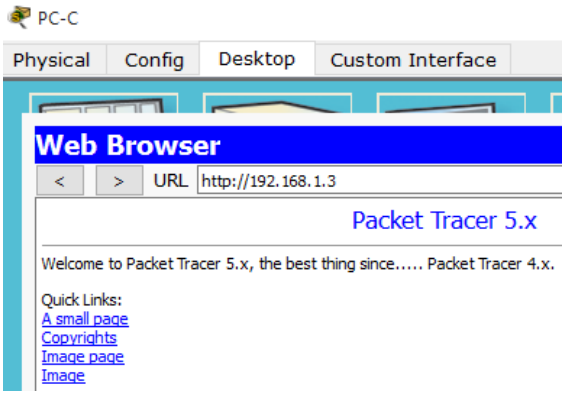


b. From the command prompt, establish a SSH session to R2 Lo0 interface (192.168.2.1) using username *SSHadmin* and password *ciscosshpa55*. Close the SSH session when finished.

PC> ssh -l SSHadmin 192.168.2.1

```
PC>SSH -l SSHadmin 192.168.2.1
Open
Password:

Password:



R2#exit

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

c. Open a web browser to the PC-A server (192.168.1.3) to display the web page. Close the browser when done.



Part 2: Secure Access to Routers

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.

Use the ***access-list*** command to create a numbered IP ACL on R1, R2, and R3.

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

```
R1#config 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
```

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

```
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
```

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

```
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
```

Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

Use the ***access-class*** command to apply the access list to incoming traffic on the VTY lines.

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

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

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

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

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

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

Step 3: Verify exclusive access from management station PC-C.

a. Establish a SSH session to 192.168.2.1 from PC-C (should be successful).

PC> ssh –l SSHadmin 192.168.2.1

```
PC>SSH -l SSHadmin 192.168.2.1
Open
Password:



R2#
```

b. Establish a SSH session to 192.168.2.1 from PC-A (should fail).

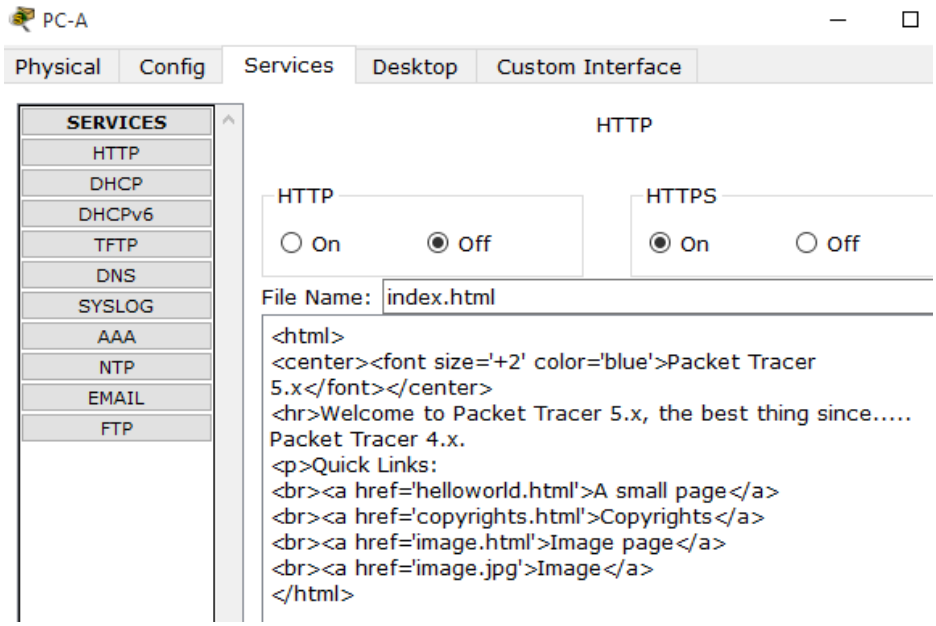
```
SERVER>SSH -l SSHadmin 192.168.2.1

% Connection refused by remote host
SERVER>
```

Part 3: Create a Numbered IP ACL 120 on R1

Permit any outside host to access DNS, SMTP, and FTP services on server PC-A, deny any outside host access to HTTPS services on PC-A, and permit PC-C to access R1 via SSH.

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server PC-A.



Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

Use the ***access-list*** command to create a numbered IP ACL.

R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp

R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443

R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22

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

Step 3: Apply the ACL to interface S0/0/0.

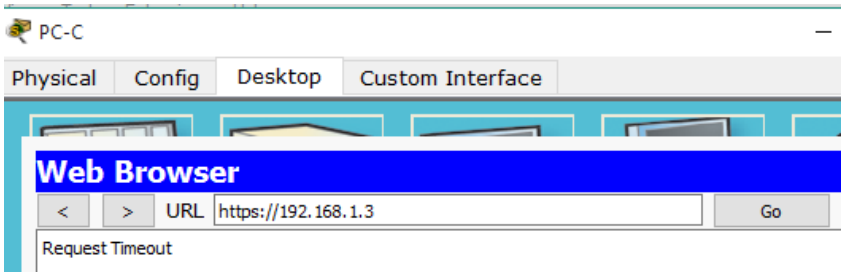
Use the ***ip access-group*** command to apply the access list to incoming traffic on interface S0/0/0.

R1(config)# interface s0/0/0

R1(config-if)# ip access-group 120 in

```
R1(config)#int s0/0/0
R1(config-if)#ip access-group 120in
% Incomplete command.
R1(config-if)#ip access-group 120 in
R1(config-if)#exit
```

Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.



Part 4: Modify An Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to R1); deny all other incoming ICMP packets.

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.

```
SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the ***access-list*** command to create a numbered IP ACL.

R1(config)# access-list 120 permit icmp any any echo-reply

R1(config)# access-list 120 permit icmp any any unreachable

R1(config)# access-list 120 deny icmp any any

R1(config)# access-list 120 permit ip any any

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

Step 3: Verify that PC-A can successfully ping the loopback interface on R2.

```
SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=10ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 3ms
```

Part 5: Create a Numbered IP ACL 110 on R3

Deny all outbound packets with source address outside the range of internal IP addresses on R3.

Step 1: Configure ACL 110 to permit only traffic from the inside network.

Use the ***access-list*** command to create a numbered IP ACL.

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

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

Step 2: Apply the ACL to interface F0/1.

Use the ip access-group command to apply the access list to incoming traffic on interface F0/1.

R3(config)# interface fa0/1

R3(config-if)# ip access-group 110 in

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

Part 6: Create a Numbered IP ACL 100 on R3

On R3, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

Step 1: Configure ACL 100 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).

Use the ***access-list*** command to create a numbered IP ACL.

R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any

R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any

R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any

R3(config)# access-list 100 permit ip any any

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

Step 2: Apply the ACL to interface Serial 0/0/1.

Use the ***ip access-group*** command to apply the access list to incoming traffic on interface Serial 0/0/1.

R3(config)# interface s0/0/1

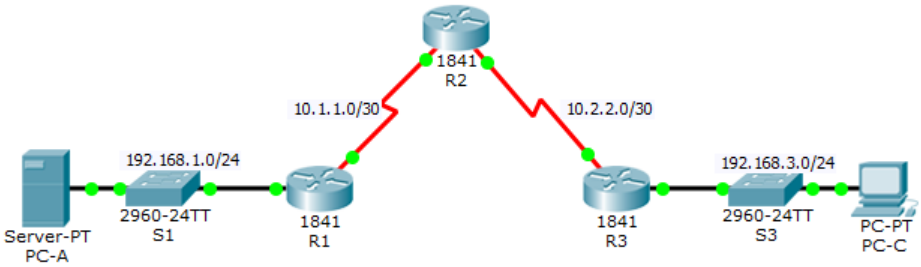
R3(config-if)# ip access-group 100 in

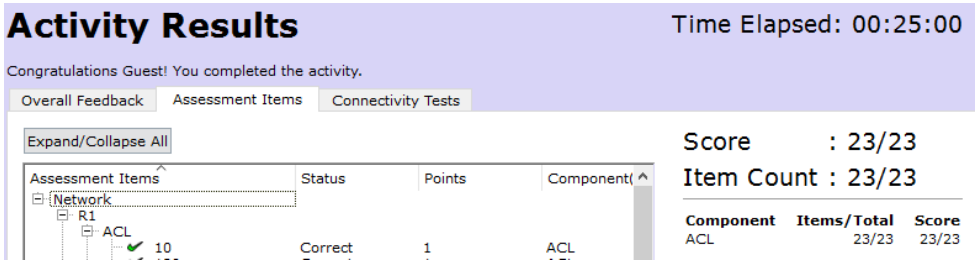
```
R3(config)#int s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#exit
```

Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

From the PC-C command prompt, ping the PC-A server. The ICMP echo replies are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=6ms TTL=128
Reply from 192.168.3.3: bytes=32 time=3ms TTL=128
Reply from 192.168.3.3: bytes=32 time=4ms TTL=128
Reply from 192.168.3.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```





9.2.1.10 Packet Tracer - Configuring Standard ACLs

Addressing table

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

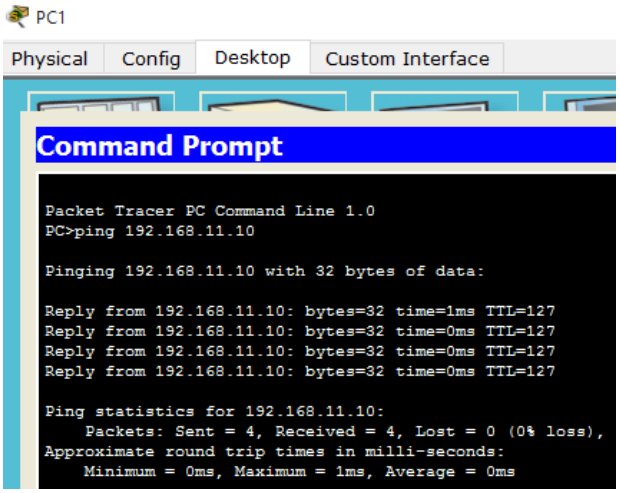
Background / Scenario

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

Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.

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




```
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=2ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

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=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=2ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

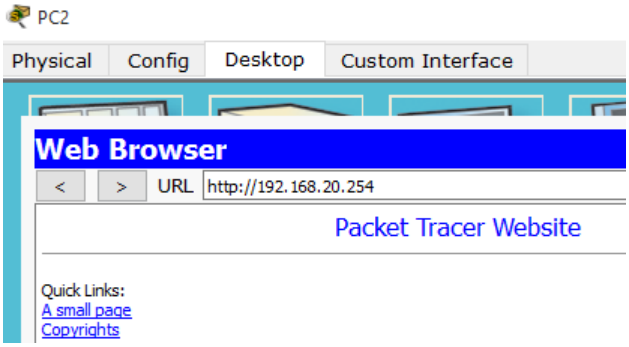
```
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=0ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time=1ms TTL=254
Reply from 192.168.20.1: bytes=32 time=1ms TTL=254
Reply from 192.168.20.1: bytes=32 time=1ms TTL=254
Reply from 192.168.20.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
PC>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=3ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

```
R1#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#ping 192.168.11.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

R1#ping 192.168.30.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/13 ms

R1#ping 192.168.20.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/8 ms

R1#ping 192.168.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/10 ms

R1#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/11 ms

R1#ping 10.3.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms

R1#ping 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/14 ms

 R1#ping 10.2.2.1

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
 !!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 2/7/12 ms

 R1#ping 10.1.1.2

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
 !!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms
```

Step 2: Evaluate two network policies and plan ACL implementations.

a. The following network policies are implemented on R2:
   - The 192.168.11.0/24 network is not allowed access to the WebServer on the 192.168.20.0/24 network.
   - All other access is permitted.



To restrict access from the 192.168.11.0/24 network to the WebServer at 192.168.20.254 without interfering with other traffic, an ACL must be created on R2. The access list must be placed on the outbound interface to the WebServer. A second rule must be created on R2 to permit all other traffic.

b. The following network policies are implemented on R3:
   - The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
   - All other access is permitted.

```
PC>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

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

Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

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

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

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

R2(config)# access-list 1 permit any

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

R2(config)# interface GigabitEthernet0/0

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

```
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#int g0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#exit
```

Step 2: Configure and apply a numbered standard ACL on R3.

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

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

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

R3(config)# access-list 1 permit any

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

R3(config)# interface GigabitEthernet0/0

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

```
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)#exit
```

Step 3: Verify ACL configuration and functionality.

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

R2

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

```
access-list 1 deny 192.168.11.0 0.0.0.255
access-list 1 permit any
!
```

```
R2# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.20.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP 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
```

R3

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

```
!
access-list 1 deny 192.168.10.0 0.0.0.255
access-list 1 permit any
!
```

```
R3#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound  access list is not set
  Proxy ARP is enabled
```

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

- A ping from 192.168.10.10 to 192.168.11.10 succeeds

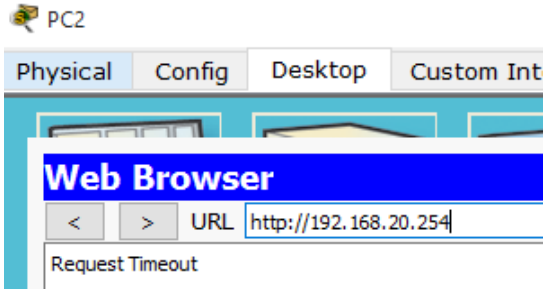
```
PC>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time=0ms TTL=127
Reply from 192.168.11.10: bytes=32 time=1ms 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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- A ping from 192.168.10.10 to 192.168.20.254 succeeds.

```
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=7ms TTL=126
Reply from 192.168.20.254: bytes=32 time=13ms 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 = 13ms, Average = 5ms
```

- A ping from 192.168.11.10 to 192.168.20.254 fails.

```
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),
```



- A ping from 192.168.10.10 to 192.168.30.10 fails.

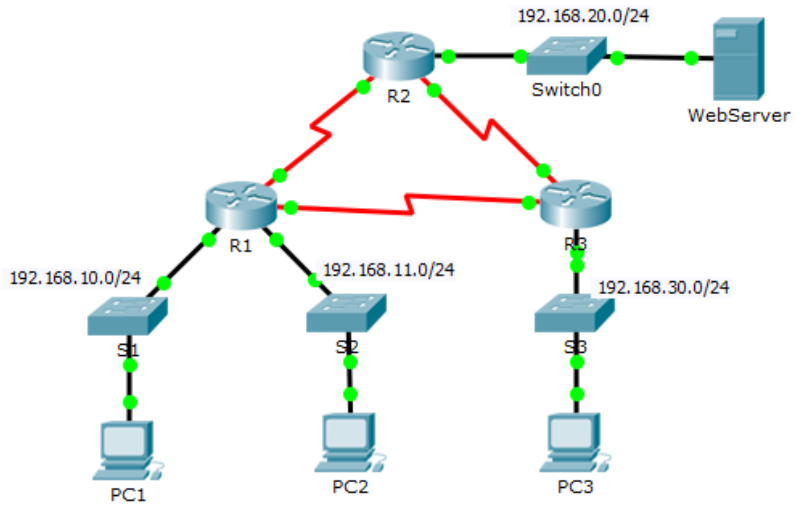
```
PC>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

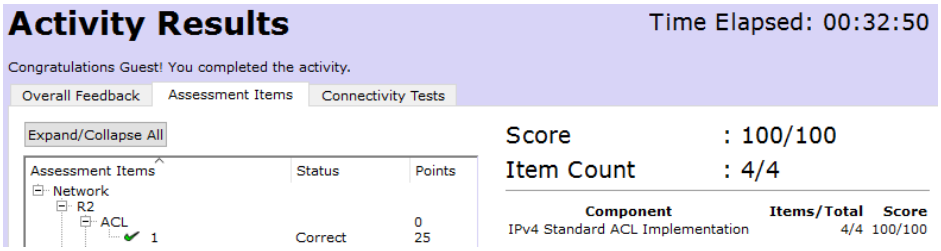
- A ping from 192.168.11.10 to 192.168.30.10 succeeds.

```
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=2ms TTL=126
Reply from 192.168.30.10: bytes=32 time=12ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=11ms 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 = 12ms, Average = 6ms
```

- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

```
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=9ms TTL=126
Reply from 192.168.20.254: bytes=32 time=10ms TTL=126
Reply from 192.168.20.254: bytes=32 time=14ms TTL=126
Reply from 192.168.20.254: bytes=32 time=4ms 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 = 4ms, Maximum = 14ms, Average = 9ms
```





9.2.1.11 Packet Tracer - Configuring Named Standard ACLs

Addressing table

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

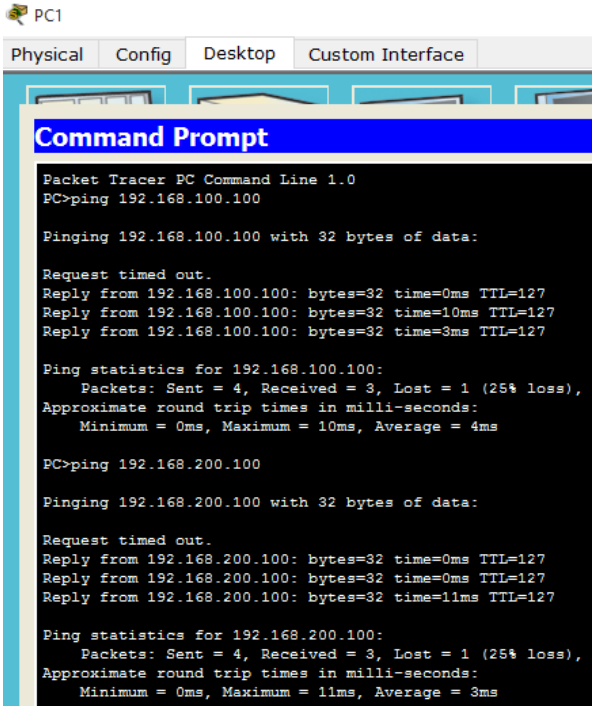
Background / Scenario

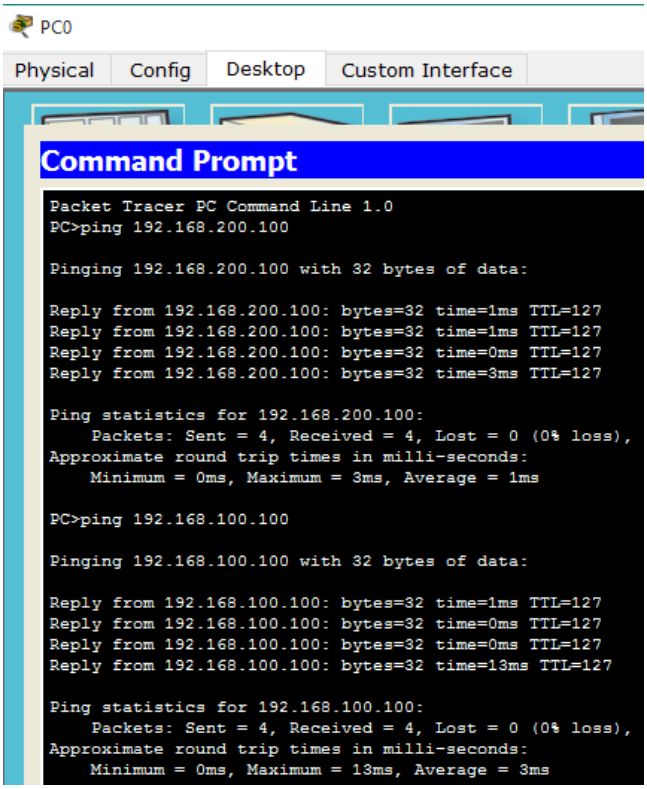
The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied access.

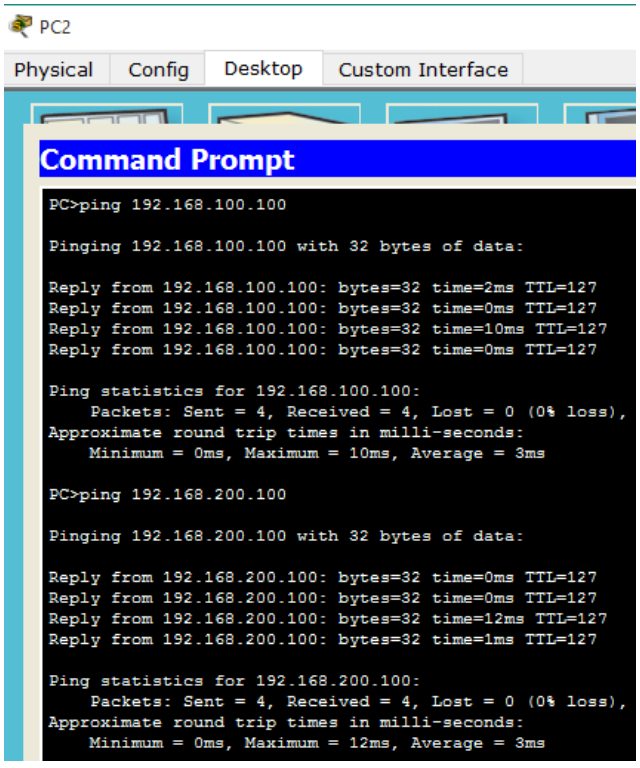
Part 1: Configure and Apply a Named Standard ACL

Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the Web Server and File Server.







Step 2: Configure a named standard ACL.

Configure the following named ACL on R1.

R1(config)# ip access-list standard File_Server_Restrictions

R1(config-std-nacl)# permit host 192.168.20.4

R1(config-std-nacl)# deny any

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

Note: For scoring purposes, the ACL name is case-sensitive.

Step 3: Apply the named ACL.

a. Apply the ACL outbound on the interface Fast Ethernet 0/1.

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

```
R1(config)#int f0/1
R1(config-if)#
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

b. Save the configuration.

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

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the interface.

Use the ***show access-lists*** command to verify the ACL configuration. Use the ***show run*** or ***show ip interface fastethernet 0/1*** command to verify that the ACL is applied correctly to the interface.

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

```
!
ip access-list standard File_Server_Restrictions
 permit host 192.168.20.4
 deny any
!
```

```
R1# show ip interface 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
```

Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the Web Server, but only PC1 should be able to ping the File Server.

PC1

Physical | Config | Desktop | Custom Interface

Command Prompt

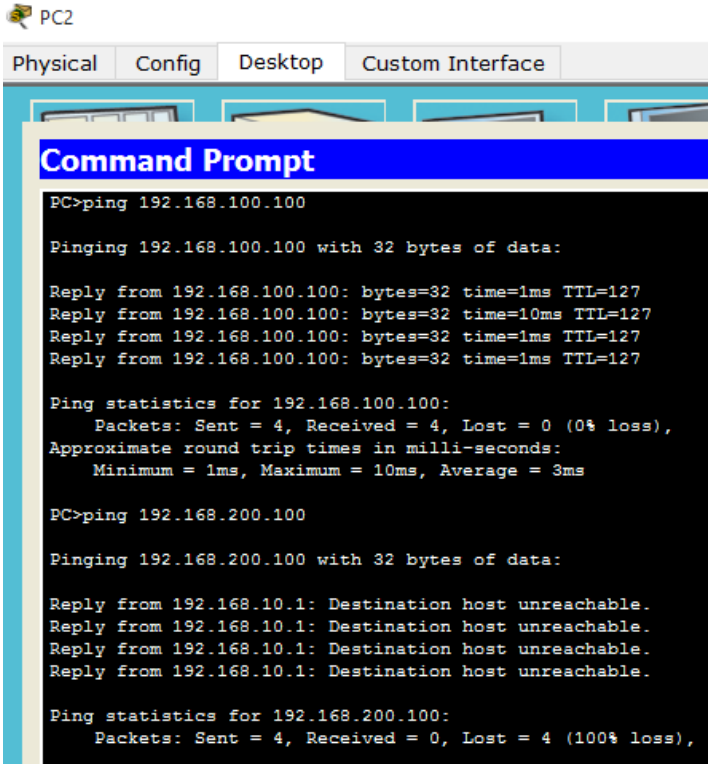
```
PC>ping 192.168.100.100

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=10ms 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

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 = 5ms

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=12ms 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 = 12ms, Average = 3ms
```

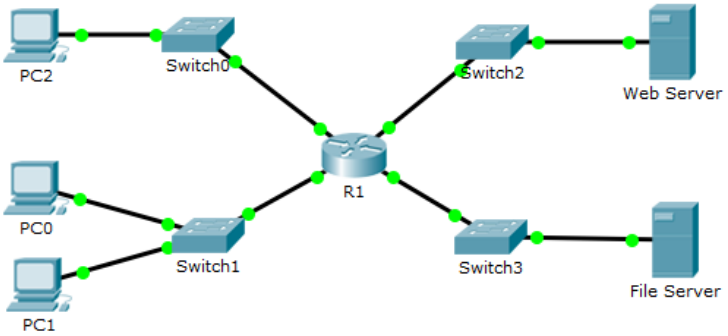
PC0

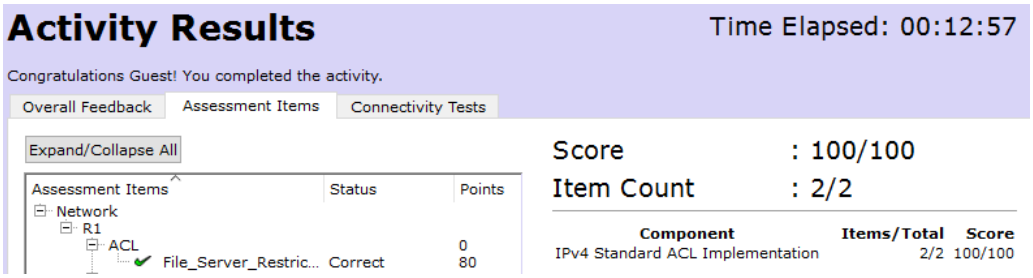
Physical | Config | Desktop | Custom Interface

Command Prompt

```
    Minimum = 0ms, Maximum = 11ms, Average = 3ms

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

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

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

PC>ping 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=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
```







9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines

Addressing table

Device	Interface	IP address	Subnet mask	Default gateway
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	
Laptop	NIC	10.0.0.2	255.0.0.0	

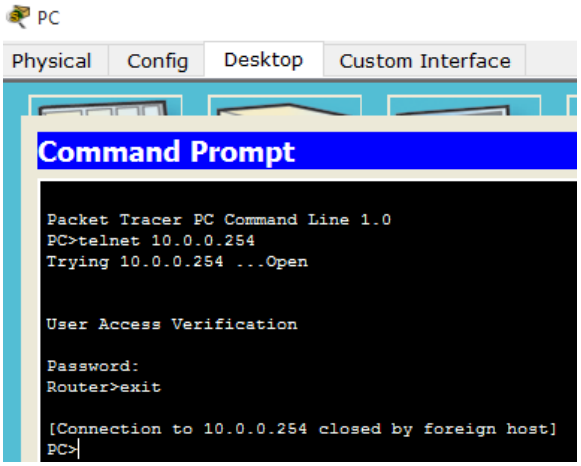
Background

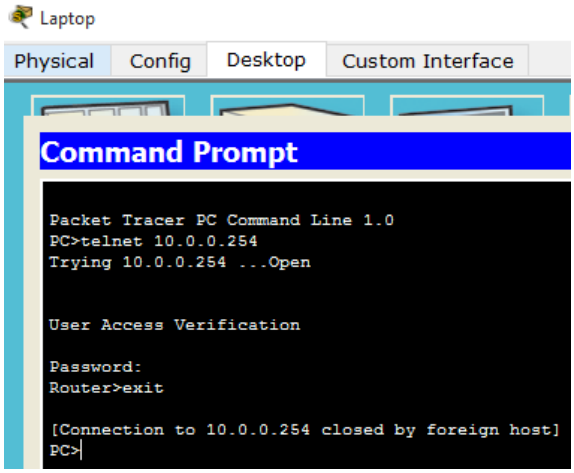
As network administrator, you must have remote access to your router. This access should not be available to other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows PC access to the Telnet lines, but denies all other source IP addresses.

Part 1: Configure and Apply an ACL to VTY Lines

Step 1: Verify Telnet access before the ACL is configured.

Both computers should be able to Telnet to the Router. The password is *cisco.*





Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on Router.

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

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Because we do not want to permit access from any other computers, the implicit deny property of the Access list satisfies our requirements.

Step 3: Place a named standard ACL on the router.

Access to the Router interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of Router, enter line configuration mode for lines 0 – 4 and use the ***access-class*** command to apply the ACL to all the VTY lines:

Router(config)# line vty 0 15

Router(config-line)# access-class 99 in

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

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the VTY lines.

Use the ***show access-lists*** to verify the ACL configuration. Use the ***show run*** command to verify the ACL is applied to the VTY lines.

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

```
access-list 99 permit host 10.0.0.1
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class 99 in
 password cisco
 login
line vty 5 15
 access-class 99 in
 password cisco
 login
!
```

Step 2: Verify that the ACL is working properly.

Both computers should be able to ping the Router, but only PC should be able to Telnet to it.

PC

Physical | Config | Desktop | Custom Interface

Command Prompt

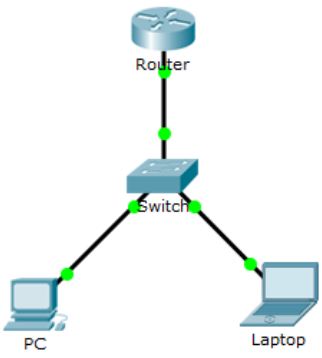
```
PC>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=1ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255

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

PC>telnet 10.0.0.254
Trying 10.0.0.254 ...Open


User Access Verification

Password:
Router>exit

[Connection to 10.0.0.254 closed by foreign host]
PC>
```

Laptop

Physical | Config | Desktop | Custom Interface

Command Prompt

```
PC>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=1ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255
Reply from 10.0.0.254: bytes=32 time=0ms TTL=255

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

PC>telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host
PC>
```



Activity Results

Time Elapsed: 00:08:28

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

Score : 100/100

Item Count : 6/6

Component	Items/Total	Score
IPv4 Standard ACL Implementation	6/6	100/100

9.5.2.6 Packet Tracer - Configuring IPv6 ACLs

Addressing table

Device	Interface	IPv6 address/prefix	Default gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Part 1: Configure, Apply, and Verify an IPv6 ACL

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

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

Configure an ACL named BLOCK_HTTP on R1 with the following statements.

a. Block HTTP and HTTPS traffic from reaching Server3.

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

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

b. Allow all other IPv6 traffic to pass.

R1(config)# permit ipv6 any any

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

Step 2: Apply the ACL to the correct interface.

Apply the ACL on the interface closest the source of the traffic to be blocked.

R1(config)# interface GigabitEthernet0/1

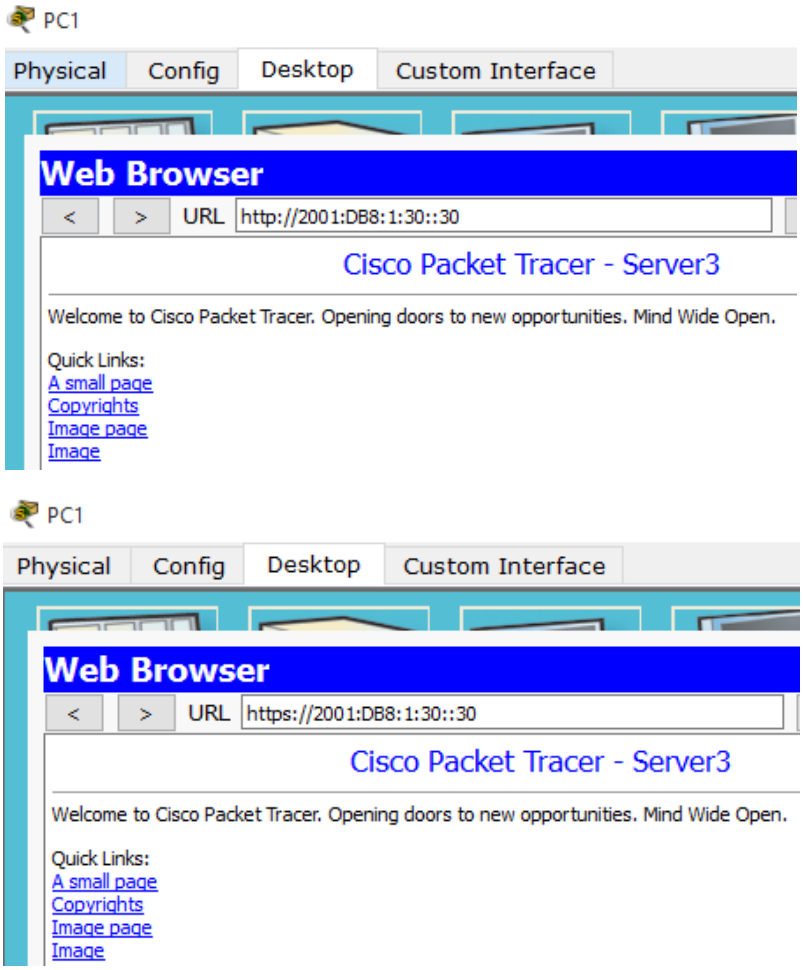
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in

```
R1(config)#int g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

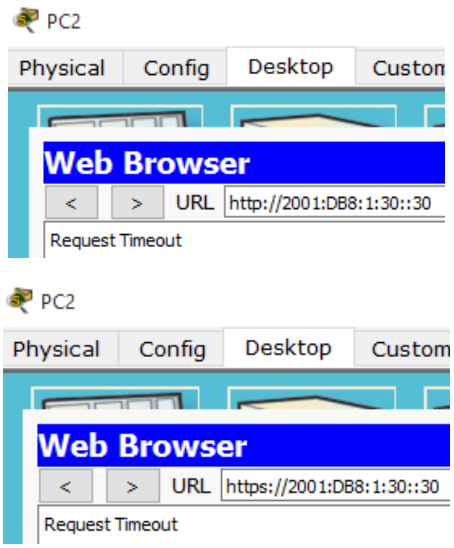
Step 3: Verify the ACL implementation.

Verify the ACL is operating as intended by conducting the following tests:

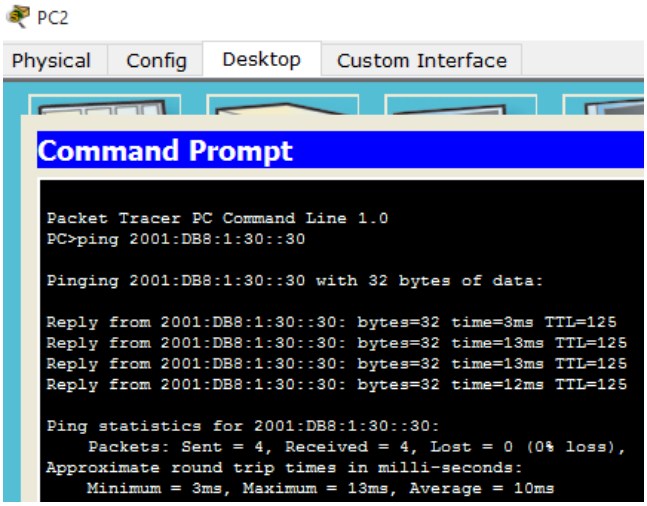
- Open the web browser of PC1 to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.



- Open the web browser of PC2 to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked



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



Part 2: Configure, Apply, and Verify a Second IPv6 ACL

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

Step 1: Create an access list to block ICMP.

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

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

R3(config)# deny icmp any any

b. Allow all other IPv6 traffic to pass.

R3(config)# permit ipv6 any any

```
R3(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)#exit
```

Step 2: Apply the ACL to the correct interface.

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

R3(config)# interface GigabitEthernet0/0

R3(config-if)# ipv6 traffic-filter BLOCK_ICMP out

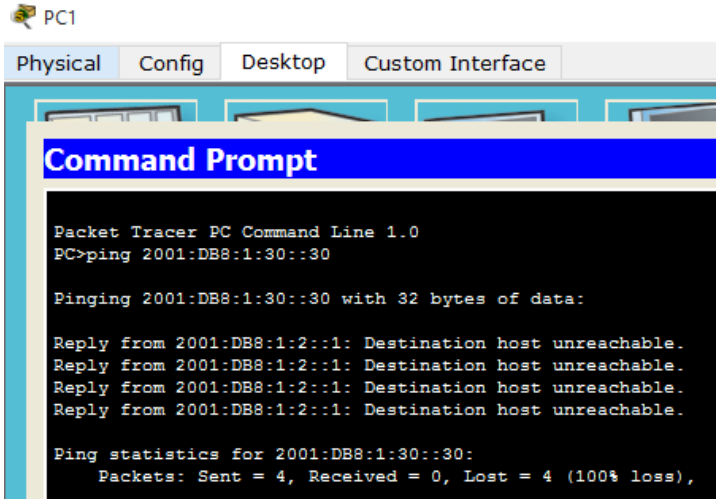
```
R3(config)#int g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 3: Verify that the proper access list functions.

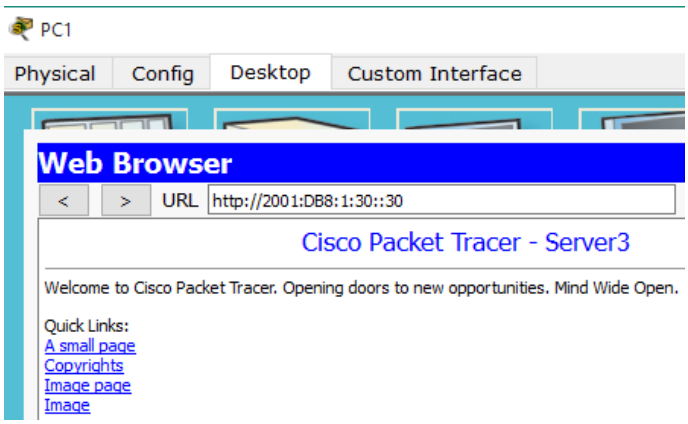
a. Ping from PC2 to 2001:DB8:1:30::30. The ping should fail.

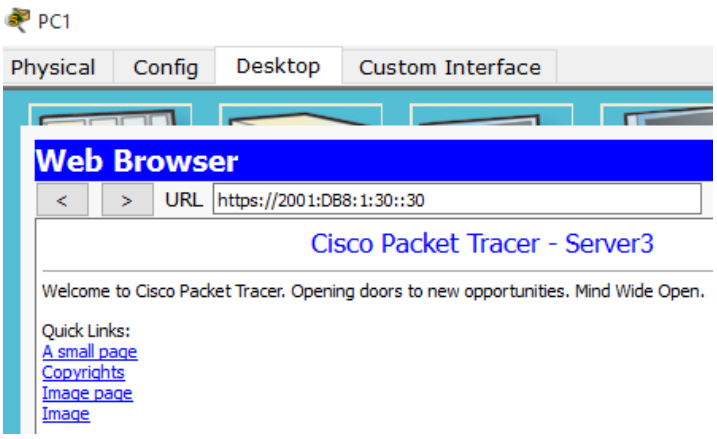
```
PC>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

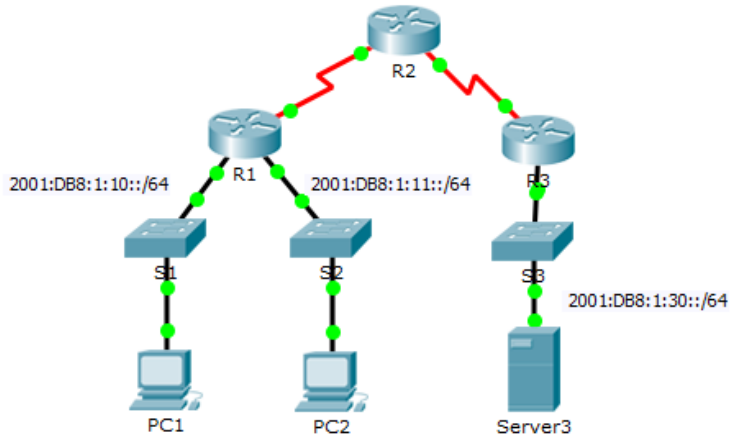
b. Ping from PC1 to 2001:DB8:1:30::30. The ping should fail.

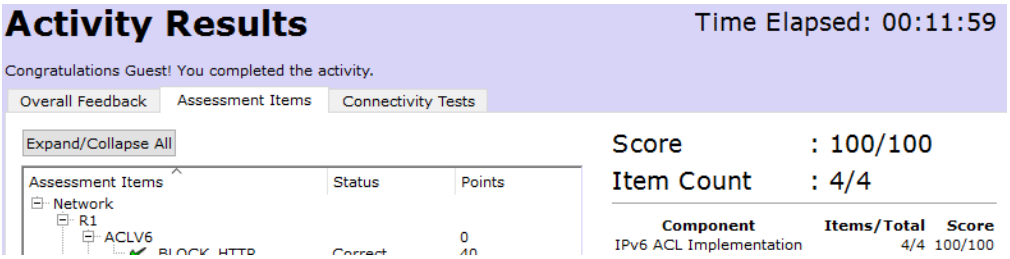


Open the web browser of PC1 to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should display.









10.1.2.4 Práctica de laboratorio – Configuración de DHCPv4 básico en un router

Topología

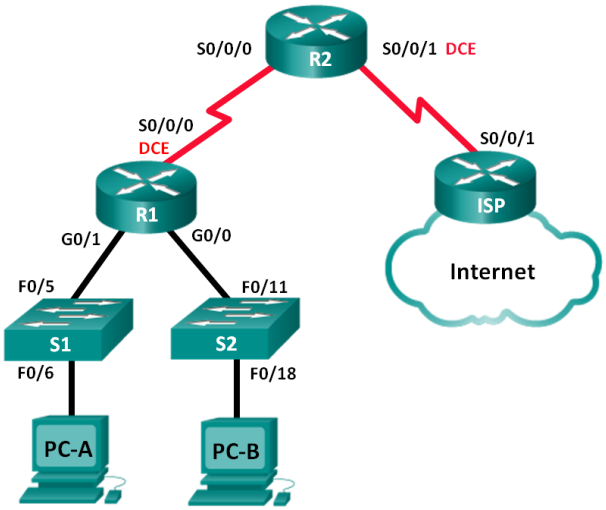


Tabla de direccionamiento

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	255.255.255.0	DHCP
PC-B	NIC	DHCP	255.255.255.0	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.

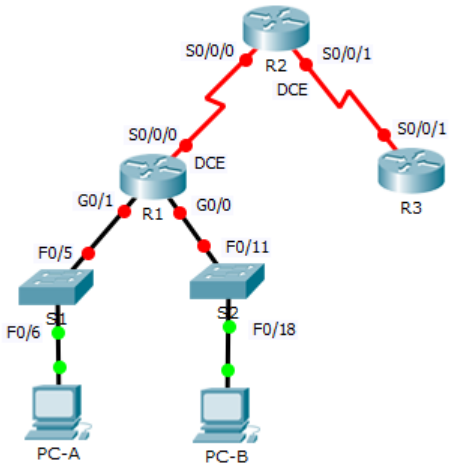
Recursos necesarios

- 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.

Respuesta. Como el laboratorio se realiza en PT, no se hace necesario inicializar y volver a cargar los routers

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(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
```

```
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
```

```
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line cvty 0 4
                  ^
% Invalid input detected at '^' marker.

ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#service password-encryption
```

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

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

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

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

ISP(config-if)#exit
```

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 address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

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

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

R1(config-if)#int g0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

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

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

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

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

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 192.168.2.252 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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(config)#router eigrp 1
R2(config-router)#network 192.168.2.252 0.0.0.3
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is up: new
adjacency

R2(config-router)#redistribute static
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

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

ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226

```
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#exit
ISP#
%SYS-5-CONFIG_I: Configured from console by console
```

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

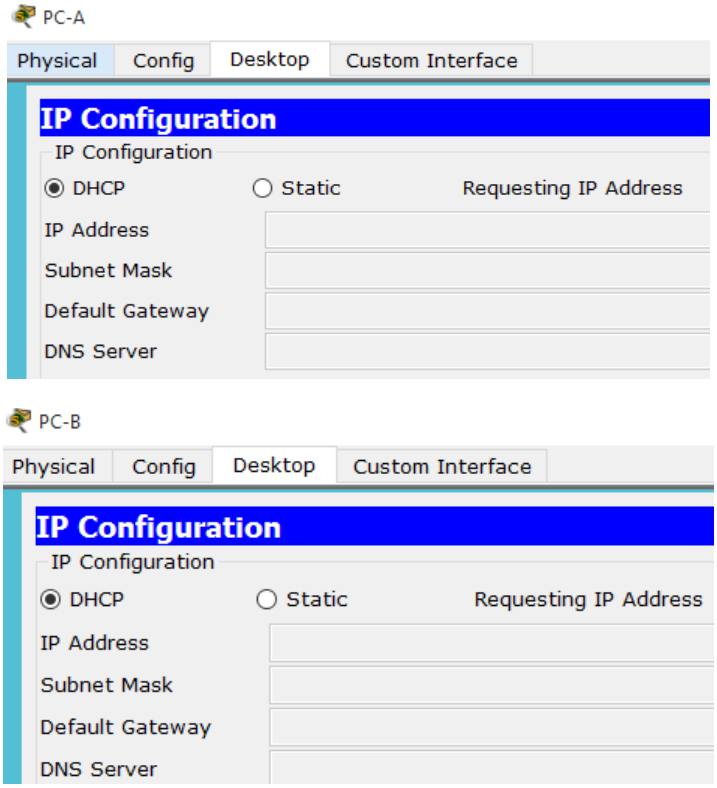
```
R1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]

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

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

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

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

```
R1#ping 192.168.2.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms

R1#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/18 ms

R1#ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/22 ms


R2#ping 192.168.0.1

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

R2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/18 ms

R2#ping 192.168.2.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/19 ms

R2#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms


ISP#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/19 ms

ISP#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/9 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 = 2/8/26 ms

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 = 1/2/10 ms

ISP#ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms
```

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 ccna-lab.com, un servidor DNS (209.165.200.225) y un tiempo de arrendamiento de dos días.

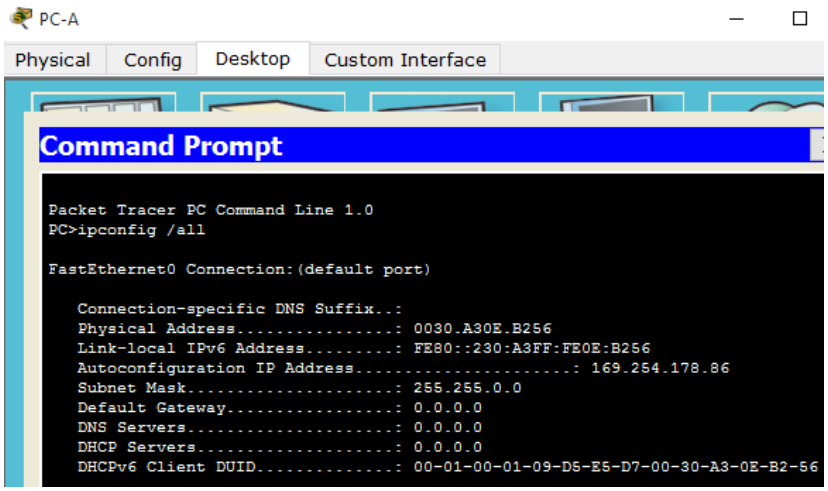
En las líneas a continuación, escriba los comandos necesarios para configurar los servicios DHCP en el router R2, incluso las direcciones DHCP excluidas y los conjuntos de direcciones DHCP.

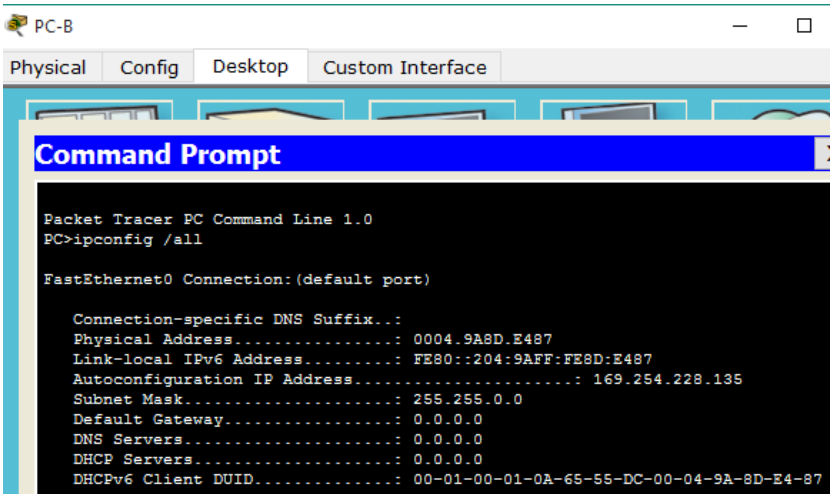
```
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name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

R2(dhcp-config)#domain-name R1G1
                  ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#lease 2
                  ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#exit
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

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?

Respuesta. Ninguno de los equipos host recibió una dirección IP de servidor ya que primero se debe configurar el R1 como agente de retransmisión DHCPv4.





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.

Respuesta. Los comandos usados fueron los siguientes: ***int g0/0, int g0/1, ip helper-address 192.168.2.254***

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

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

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....................: 0030.A30E.B256
   Link-local IPv6 Address.....: FE80::230:A3FF:FE0E:B256
   IP Address.....................: 192.168.1.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.....................: 192.168.1.1
   DNS Servers.....................: 209.165.200.225
   DHCP Servers.....................: 192.168.2.254
   DHCPv6 Client DUID.....: 00-01-00-01-09-D5-E5-D7-00-30-A3-0E-B2-56
```

PC-B

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....................: 0004.9A8D.E487
   Link-local IPv6 Address.....: FE80::204:9AFF:FE8D:E487
   IP Address.....................: 192.168.0.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.....................: 192.168.0.1
   DNS Servers.....................: 209.165.200.225
   DHCP Servers.....................: 192.168.2.254
   DHCPv6 Client DUID.....: 00-01-00-01-0A-65-55-DC-00-04-9A-8D-E4-87
```

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?

Respuesta. Según el pool DHCP que se configuró en el R2, las primeras direcciones IP disponibles que la PC-A y la PC-B pueden arrendar es 192.168.1.10 y 192.168.0.10 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.

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

   Respuesta. Como se observa, el comando también muestra las direcciones MAC físicas de cada dirección IP a las cuales se arrendaron. En el espacio Leae expiration debía aparecer un 2 (sugerencia) pero PT no admite el comando

```
R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.10     0030.A30E.B256           --                     Automatic
192.168.0.10     0004.9A8D.E487           --                     Automatic
```

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

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

   Respuesta. PT no admite el comando

```
R2#show ip dhcp server statistics
                   ^
% Invalid input detected at '^' marker.

R2#show ip dhcp server statistics
                   ^
% Invalid input detected at '^' marker.
```

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

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

   Respuesta. PT no admite el comando

```
R2#show ip dhcp pool
                   ^
% Invalid input detected at '^' marker.
```

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

   Respuesta. PT no admite el comando. En su lugar, se escribe el comando ***show run***

```
R2#show run | section dhcp
                  ^
% Invalid input detected at '^' marker.
```

```
!
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 209.165.200.225
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 209.165.200.225
!
```

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

Respuesta. PT no admite el comando

```
R2#show run interface
                    ^
% Invalid input detected at '^' marker.
```

Reflexión

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

Respuesta. Tener varios routers que funcionen como servidores de DHCP independiente para cada subred agregaría más complejidad y disminuiría la administración centralizada de la red. En cambio, al usar agentes de retransmisión DHCP, sería mucho mpas fácilde administrar y estaría mejor centralizada

10.1.2.5 Práctica de laboratorio – Configuración de DHCPv4 básico en un Switch

Topología

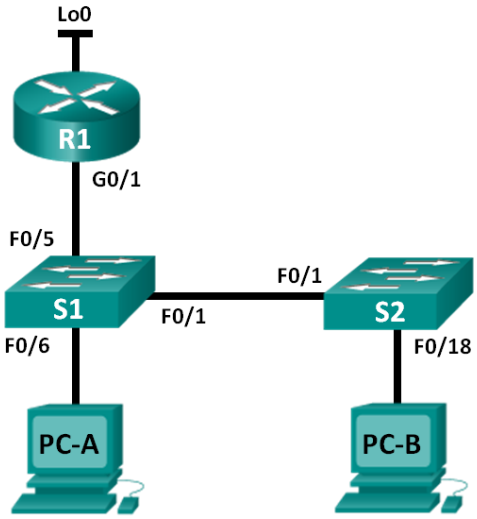


Tabla de direccionamiento

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

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.

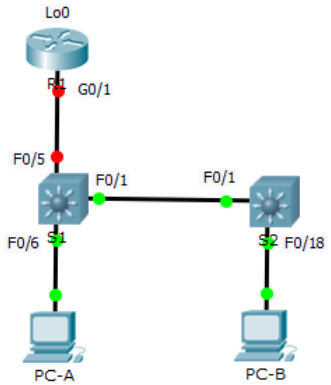
Nota: asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

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.

Respuesta. Como el laboratorio se realiza en PT, no hay necesidad de inicializar y volver a cargar los routers y switches

Paso 3: Configurar los parámetros básicos en los dispositivos.

a. Asigne los nombres de dispositivos como se muestra en la topología.
b. Desactive la búsqueda del DNS.
c. Asigne *class* como la contraseña de enable y asigne *cisco* como la contraseña de consola y la contraseña de vty.

```
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#service-password encryption
                  ^
% Invalid input detected at '^' marker.

R1(config)#service password-encryption
R1(config)#enable secret class
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
```

```
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#service password-encryption
S1(config)#enable secret class
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
```

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname s
s(config)#hostname S2
S2(config)#line vty 0 4
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#logging synchronous
S2(config-line)#exit
S2(config)#enable secret class
S2(config)#service password-encryption
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

```
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 209.165.200.225 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#int g0/1
R1(config-if)#ip address 192.168.1.10 255.255.255.0
R1(config-if)#no shutdown

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

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

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

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

```
S1(config)#int vlan1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shutdown

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 vlan2
S1(config-if)#ip address 192.168.2.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1(config)#vlan 2
S1(config-vlan)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

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

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

```
S1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
S2#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

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

¿Cuál es la plantilla actual?

Respuesta. PT no admite el comando

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

En el Switch real, debe aparecer algo como lo siguiente. La plantilla actual debería ser "default"

```
S1# show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

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

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

¿Qué plantilla estará disponible después de la recarga?

Respuesta. PT no admite el comando

```
S1(config)#sdm prefer lanbase-routing
                ^
% Invalid input detected at '^' marker.
```

En el Switch real, debe aparecer algo como lo siguiente. La plantilla que estará disponible es routing

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

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

S1# reload

```
S1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
S1#reload
Proceed with reload? [confirm]
```

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

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

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

S1# show sdm prefer

Respuesta. PT no admite el comando

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

Parte 3: Configurar DHCPv4

En la parte 3, configurará DHCPv4 para la VLAN 1, revisará las configuraciones IP en los equipos host para validar la funcionalidad de DHCP y verificará la conectividad de todos los dispositivos en la VLAN 1.

Paso 1: Configurar DHCP para la VLAN 1.

a. Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.

   Respuesta. Se usó el comando ***ip dhcp excluded-address 192.168.1.1 192.168.1.10***

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

   Respuesta. Se usó el comando ***ip dhcp pool DHCP1***

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

   Respuesta. Se usó el comando ***network 192.168.1.0 255.255.255.0***

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

   Respuesta. Se usó el comando ***default-router 192.168.1.1***

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

   Respuesta. Se usó el comando ***dns-server 192.168.1.9***

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

   Respuesta. Se usó el comando ***lease 3***

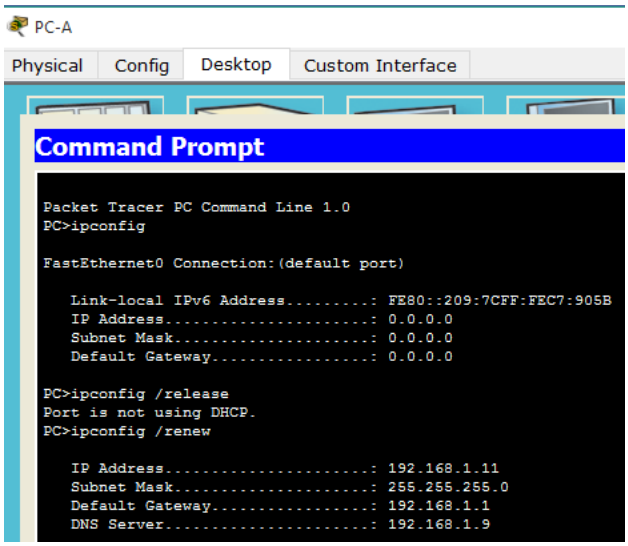
g. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#ip dhcp pool DHCP1
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.1.1
S1(dhcp-config)#dns-server 192.168.1.9
S1(dhcp-config)#lease 3
                   ^
% Invalid input detected at '^' marker.

S1(dhcp-config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

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:

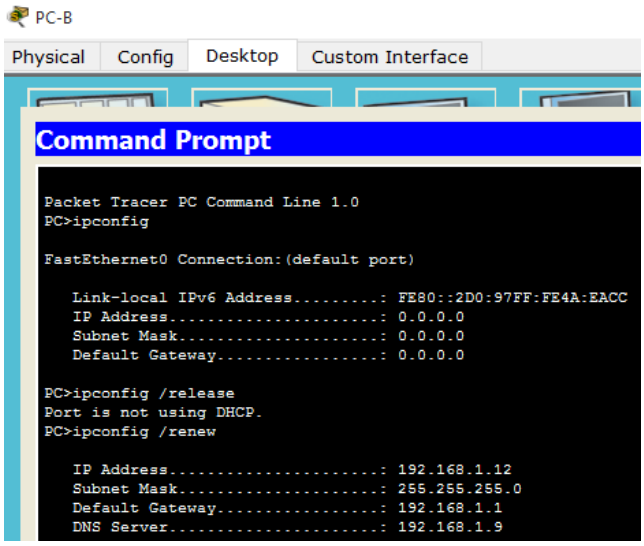


Dirección IP: 192.168.1.11

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?

Respuesta. Si, es correcto

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

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

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

Respuesta. Si, es correcto

```
PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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

Respuesta. Si, es correcto

```
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255
Reply from 192.168.1.10: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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

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.

Respuesta. Se usó el comando ***S1(config)#int f0/6*** y ***S1(config-if)#switchport access vlan 2***

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

Paso 2: Configurar DHCPv4 para la VLAN 2.

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

   Respuesta. El comando que se usó fue ***ip dhcp excluded-address 192.168.2.1 192.168.2.10***

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

   Respuesta. El comando que se usó fue ***ip dhcp pool DHCP2***

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

   Respuesta. El comando que se usó fue ***network 192.168.2.0 255.255.255.0***

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

   Respuesta. El comando que se usó fue ***default-router 192.168.2.1***

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

   Respuesta. El comando que se usó fue ***dns-server 192.168.2.9***

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

Respuesta. El comando que se usó fue ***lease 3***

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

```
S1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)#ip dhcp pool DHCP2
S1(dhcp-config)#network 192.168.2.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.2.1
S1(dhcp-config)#dns-server 192.168.2.9
S1(dhcp-config)#lease 3
                   ^
% Invalid input detected at '^' marker.

S1(dhcp-config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

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:

```
PC>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

PC>ipconfig /renew

   IP Address......................: 192.168.2.11
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.2.1
   DNS Server......................: 192.168.2.9
```

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?

Respuesta. Si, es correcto

```
PC>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=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms 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 = 1ms, Average = 0ms
```

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

Respuesta. No, no se puede hacer ping de la PC-A a la PC-B

```
PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

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

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

¿Los pings eran correctos? ¿Por qué?

Respuesta. El ping de la PC-A a su Gateway predeterminado si es correcto ya que se encuentran en la misma red, en cambio a la PC-B no fue correcto ya que se encuentran en distintas redes. Se debe habilitar routing para que los pings puedan ser satisfactorios

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

¿Qué resultado arrojó este comando?

Respuesta. El resultado es que no se encuentra configurado una puerta de enlace o un default Gateway

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

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

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#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip routing
```

b. Verificar la conectividad entre las VLAN.

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

Respuesta. Si, si fue posible hacer el ping

```
PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=2ms TTL=127
Reply from 192.168.1.12: bytes=32 time=0ms TTL=127
Reply from 192.168.1.12: bytes=32 time=0ms TTL=127
Reply from 192.168.1.12: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

¿Qué función realiza el switch?

Respuesta. Desde que se activó el routing, el Switch está ruteando entre VLAN's

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 not set

C    192.168.1.0/24 is directly connected, Vlan1
C    192.168.2.0/24 is directly connected, Vlan2
```

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

Respuesta. Se incluyen dos redes conectadas. La 192.168.1.0/24 y la 192.168.2.0/24

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

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

Respuesta. Aparecen todas las redes directamente conectadas

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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.10/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
```

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

Respuesta. No, no es posible hacer el ping

```
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

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

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

Respuesta. No, no es posible hacer el ping

```
PC>ping 209.165.200.225

Pinging 209.165.200.225 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.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

Respuesta. Se deben agregar rutas a ambas tablas de ruteo en ambos dispositivos

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.

Respuesta. Se usó el comando ***ip route 0.0.0.0 0.0.0.0 192.168.1.10***

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.10
```

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

Respuesta. Se usó el comando ***ip route 192.168.2.0 255.255.255.0 g0/1***

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 192.168.2.0 255.255.255.0 g0/1
%Default route without gateway, if not a point-to-point interface, may impact
performance
```

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

¿Cómo está representada la ruta estática predeterminada?

Respuesta. La ruta estática predeterminada se representa con una S a la red 192.168.2.0/24 por la interfaz G0/1

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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.10/32 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
R1#
```

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

¿Cómo está representada la ruta estática?

Respuesta. La ruta estática predeterminada se representa con una S* a la red 0.0.0.0/0 por 192.168.1.10

```
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
```

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

Respuesta. Si, es posible realizar el ping

```
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254
Reply from 192.168.1.10: bytes=32 time=11ms TTL=254
Reply from 192.168.1.10: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

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

Respuesta. Si, es posible realizar el ping

```
PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=11ms TTL=254
Reply from 209.165.200.225: bytes=32 time=0ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

Reflexión

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

   Respuesta. Las direcciones estáticas fueron excluidas antes de configurar o crear el pool de DHCPv4 ya que una ventana de tiempo existe cuando se excluyen las direcciones y podrían ser dadas dinámicamente hacia un host

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

   Respuesta. La asignación se realiza por DHCP para cada VLAN y se determina una interface para cada VLAN, esto con el fin de que los switch puedan realizar de manera eficaz la asignación correspondiente de las IP a cada host

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

   Respuesta. En este caso, es un Switch de capa 3 y se lleva a cabo con el comando ***ip routing***

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	N/A
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Solo mediante configuración automática de dirección sin estado (SLAAC)
- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
- Mediante DHCPv6 con estado

Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

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

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

Nota: la plantilla default bias que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla ***dual-ipv4-and-ipv6*** o la plantilla ***lanbase-routing*** en SDM. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

S1# show sdm prefer

Respuesta. Como se está trabajando en PT, esta versión no soporta el comando

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

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

Respuesta. Como se está trabajando en PT, esta versión no soporta los comandos

```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
                  ^
% Invalid input detected at '^' marker.

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

Recursos necesarios

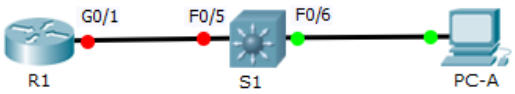
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para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

Respuesta. Como el laboratorio se realiza en PT, no se hace necesario incializar y volver a cargar el router ni el switch

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(config)#no ip domain-lookup
Router(config)#hostanme R1
                  ^
% Invalid input detected at '^' marker.

Router(config)#hostname R1
R1(config)#service password-encryption
R1(config)#banner motd#
                     ^
% Invalid input detected at '^' marker.

R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#

R1(config)#enable secret class
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

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.

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#service password-encryption
S1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#

S1(config)#enable secret class
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#int range f0/1-4, f0/7-24, g0/1
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

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

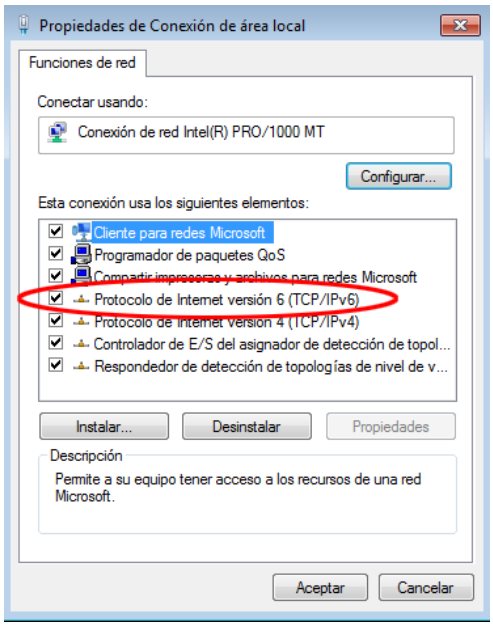
```
S1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

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.

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza. De forma física, quedaría de la siguiente forma



b. Inicie una captura del tráfico en la NIC con Wireshark.

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza.

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.

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza. De forma física, quedaría de la siguiente forma

Paso 2: Configurar R1

a. Habilite el routing de unidifusión IPv6
b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.
c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.
d. Active la interfaz G0/1.

```
R1(config)#ipv6 unicast-routing
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
R1(config-if)#no shutdown

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

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

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 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  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 address autoconfig
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

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

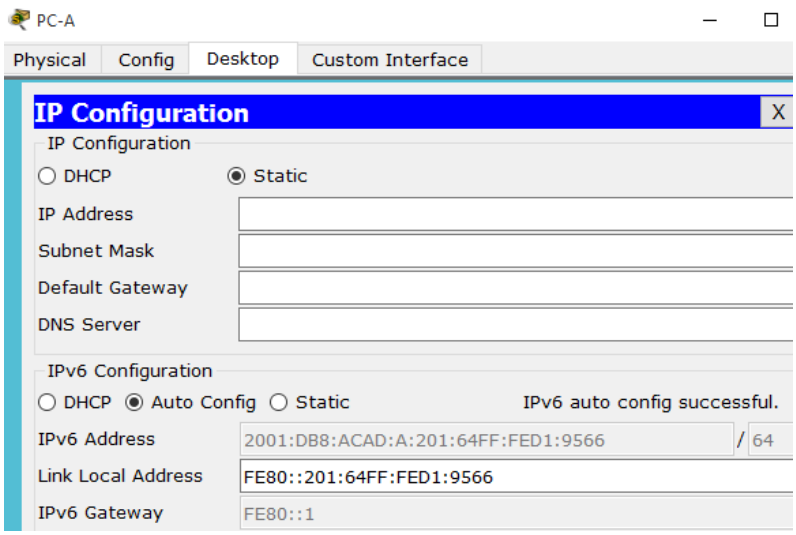
S1# show ipv6 interface

Respuesta. PT no soporta la característica. El comando show ipv6 interface brief solo muestra la dirección link-local y el S1 no tiene una dirección unicast global

```
S1#show ipv6 interface
S1#show ipv6 interface brief
FastEthernet0/1            [administratively down/down]
FastEthernet0/2            [administratively down/down]
FastEthernet0/3            [administratively down/down]
FastEthernet0/4            [administratively down/down]
FastEthernet0/5            [up/up]
FastEthernet0/6            [up/up]
FastEthernet0/7            [administratively down/down]
FastEthernet0/8            [administratively down/down]
FastEthernet0/9            [administratively down/down]
FastEthernet0/10           [administratively down/down]
FastEthernet0/11           [administratively down/down]
FastEthernet0/12           [administratively down/down]
FastEthernet0/13           [administratively down/down]
FastEthernet0/14           [administratively down/down]
FastEthernet0/15           [administratively down/down]
FastEthernet0/16           [administratively down/down]
FastEthernet0/17           [administratively down/down]
FastEthernet0/18           [administratively down/down]
FastEthernet0/19           [administratively down/down]
FastEthernet0/20           [administratively down/down]
FastEthernet0/21           [administratively down/down]
FastEthernet0/22           [administratively down/down]
FastEthernet0/23           [administratively down/down]
FastEthernet0/24           [administratively down/down]
GigabitEthernet0/1         [administratively down/down]
GigabitEthernet0/2         [down/down]
Vlan1                      [up/up]
    FE80::201:C7FF:FEE8:9686
S1#show ipv6 interface vlan 1
Vlan1 is up, line protocol is up
  Internet protocol processing disabled
```

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.

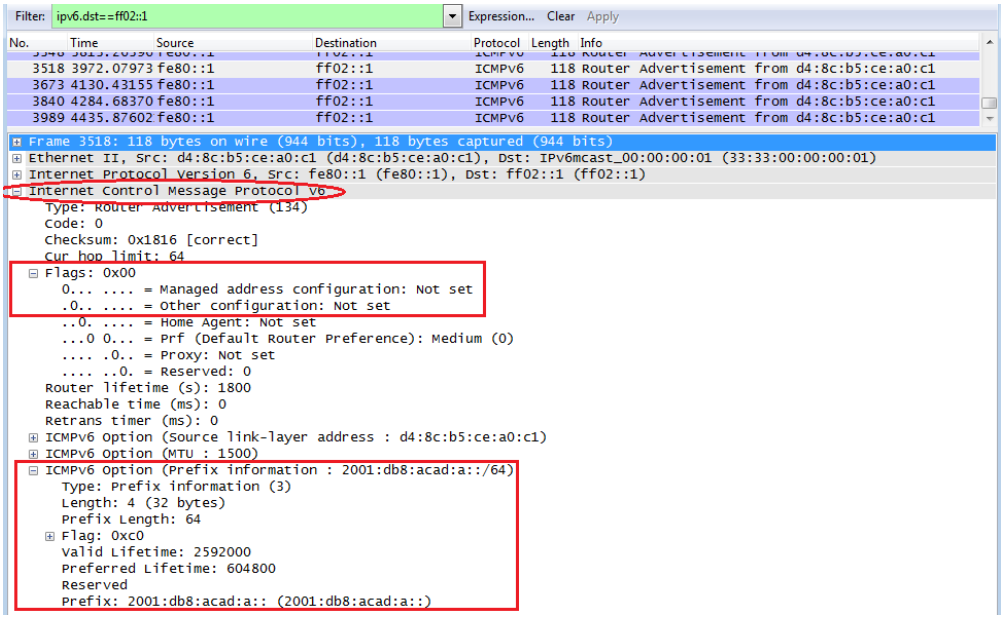



```
PC>ipv6config /all

FastEthernet0 Connection:(default port)

   Physical Address.................: 0001.64D1.9566
   Link-local IPv6 Address.........: FE80::201:64FF:FED1:9566
   IPv6 Address....................: 2001:DB8:ACAD:A:201:64FF:FED1:9566/64
   Default Gateway.................: ::
   DNS Servers.....................: ::
   DHCPv6 Client DUID..............: 00-01-00-01-7C-E0-70-A5-00-01-64-D1-95-66
```

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.

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza. De forma física, quedaría de la siguiente forma



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

b. Asigne un nombre de dominio al pool.

R1(config-dhcpv6)# domain-name ccna-statelessDHCPv6.com

c. Asigne una dirección de servidor DNS.

R1(config-dhcpv6)# dns-server 2001:db8:acad:a::abcd

R1(config-dhcpv6)# exit

d. Asigne el pool de DHCPv6 a la interfaz.

R1(config)# interface g0/1

R1(config-if)# ipv6 dhcp server IPV6POOL-A

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)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#domain-name ccna-statelessDHCPv6.com
R1(config-dhcp)#dns-server 2001:DB8:ACAD:A::ABCD
R1(config-dhcp)#exit
R1(config)#int g0/1
R1(config-if)#ipv6 dhcp server IPV6POOL-A
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.

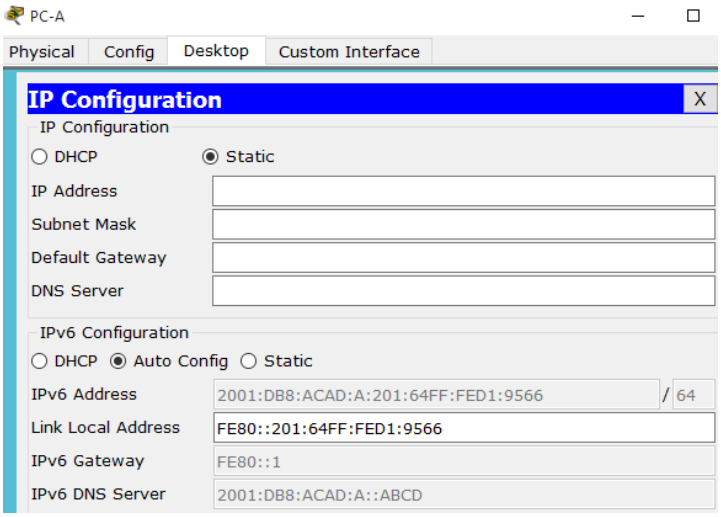
Use el comando ***show ipv6 interface g0/1*** para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando show verifica que se haya establecido other-config-flag.

R1# show ipv6 interface g0/1

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

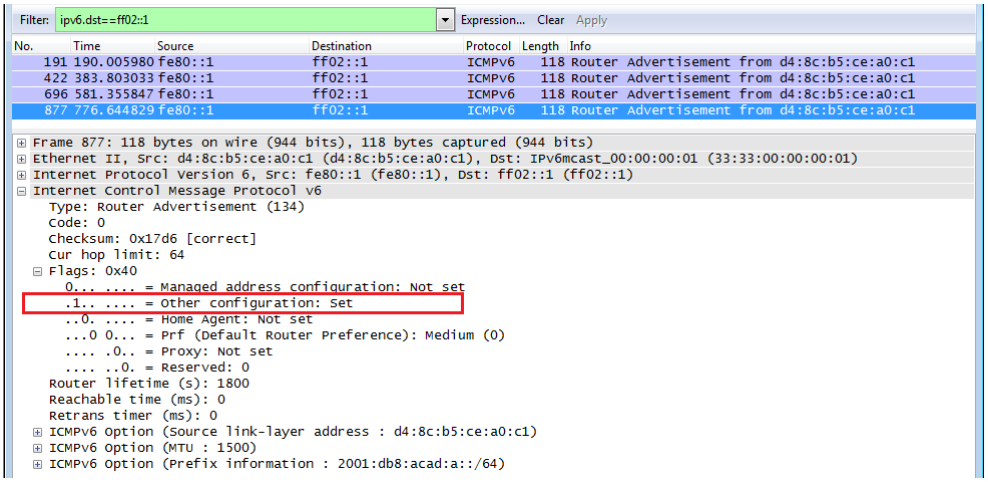


```
PC>ipv6config /all

FastEthernet0 Connection:(default port)

   Physical Address.................: 0001.64D1.9566
   Link-local IPv6 Address.........: FE80::201:64FF:FED1:9566
   IPv6 Address....................: 2001:DB8:ACAD:A:201:64FF:FED1:9566/64
   Default Gateway.................: ::
   DNS Servers.....................: ::
   DHCPv6 IAID.....................: 27382
   DHCPv6 Client DUID..............: 00-01-00-01-7C-E0-70-A5-00-01-64-D1-95-66
```

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.

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza. De forma física, quedaría de la siguiente forma



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

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

R1# show ipv6 dhcp binding

R1# show ipv6 dhcp pool

```
R1#show ipv6 dhcp binding
Client:  (GigabitEthernet0/1)
  DUID: 00-01-00-01-7C-E0-70-A5-00-01-64-D1-95-66
  IA PD: IA ID 27382, T1 0, T2 0
    Prefix: 0.0.0.0/0
            preferred lifetime 0, valid lifetime 0
            expires at Noviembre 25 2017 7:7:56 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

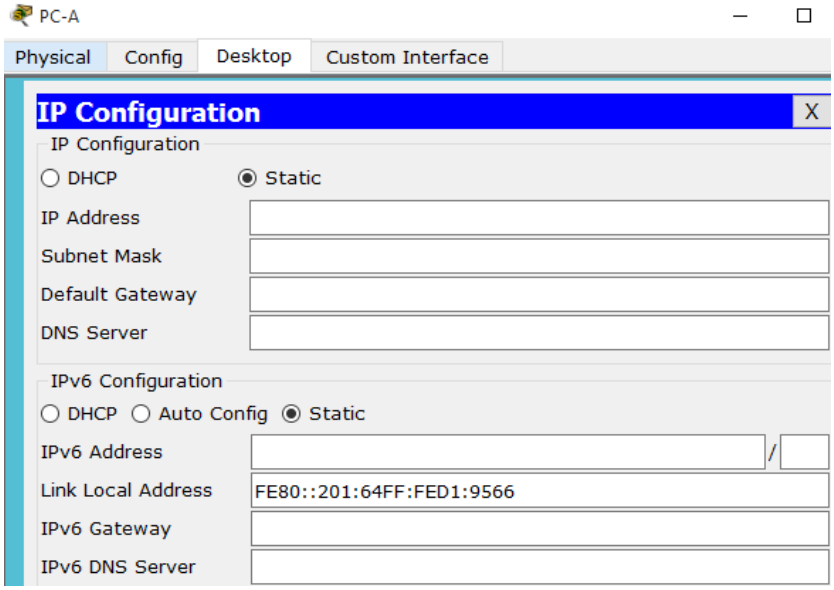
S1(config-if)# shutdown

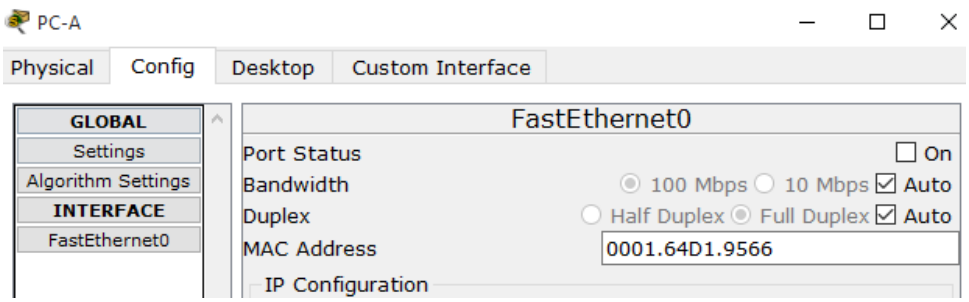
```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/6
S1(config-if)#shutdown

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.

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza.

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





Parte 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.

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza.

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.

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza. De forma física, quedaría de la siguiente forma:

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

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)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcp)#address prefix 2001:DB8:ACAD:A::/64
                ^
% Invalid input detected at '^' marker.

R1(config-dhcp)#address prefix 2001:db8:acad:a::/64
                ^
% Invalid input detected at '^' marker.

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

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
```

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

R1# debug ipv6 dhcp detail

```
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)#int g0/1
R1(config-if)#shutdown

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

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

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

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

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

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

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 shutdown

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

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

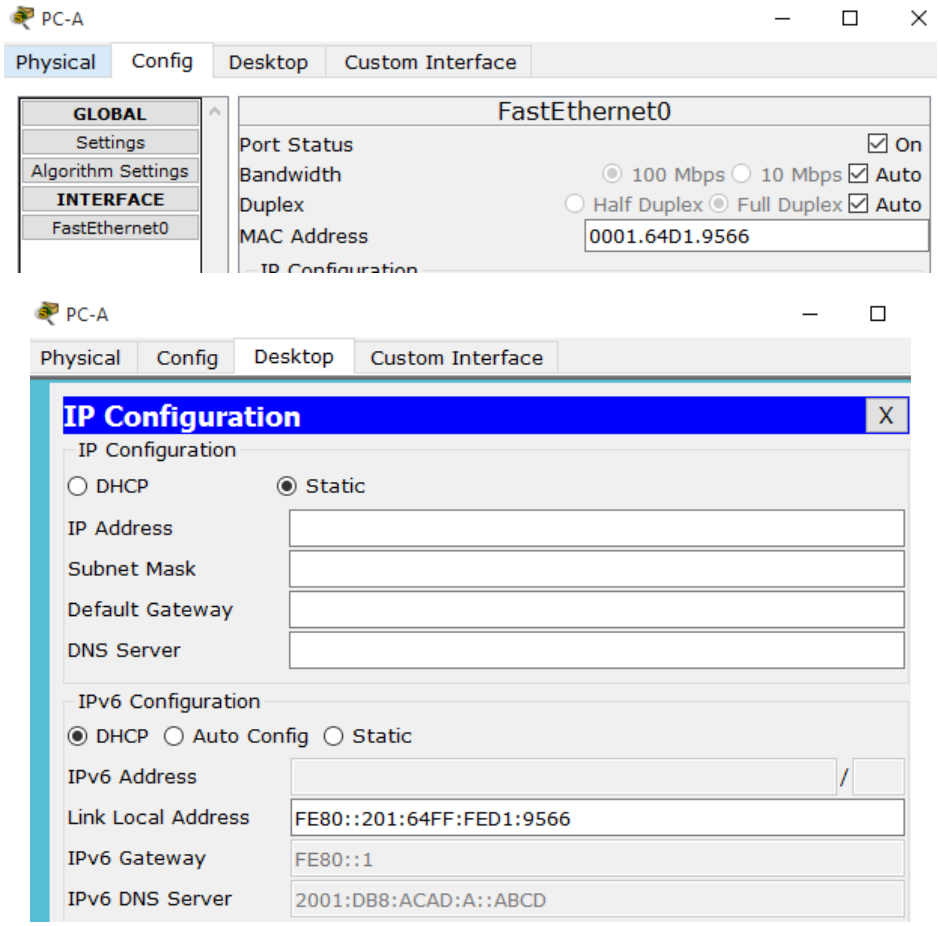
a. Emita el comando ***show ipv6 interface g0/1*** para verificar que la interfaz esté en el modo DHCPv6 con estado.

R1# show ipv6 interface g0/1

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

Respuesta. Se debe tener en cuenta que algunos comandos no funcionaron en PT pero en físico sí deberían funcionar. En este punto no se muestra una dirección unicast a la PC-A ya que no se admite el comando ***R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64***



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

R1# show ipv6 dhcp pool

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

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: 00-01-00-01-7C-E0-70-A5-00-01-64-D1-95-66
  IA PD: IA ID 27382, T1 0, T2 0
    Prefix: 0.0.0.0/0
            preferred lifetime 0, valid lifetime 0
            expires at Noviembre 25 2017 7:36:59 pm (0 seconds)
```

```
PC>ipv6config /all

FastEthernet0 Connection:(default port)

   Physical Address.................: 0001.64D1.9566
   Link-local IPv6 Address.........: FE80::201:64FF:FED1:9566
   IPv6 Address....................: ::/0
   Default Gateway.................: FE80::1
   DNS Servers.....................: 2001:DB8:ACAD:A::ABCD
   DHCPv6 IAID.....................: 27382
   DHCPv6 Client DUID..............: 00-01-00-01-7C-E0-70-A5-00-01-64-D1-95-66
```

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

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

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 01:35:08.070: IPv6 DHCP: Received SOLICIT from FE80::201:64FF:FED1:9566 on
GigabitEthernet0/1
*Mar. 1 01:35:08.070: IPv6 DHCP: detailed packet contents
*Mar. 1 01:35:08.070:   src FE80::201:64FF:FED1:9566 (GigabitEthernet0/1)
*Mar. 1 01:35:08.070:   dst FF02::1:2 (GigabitEthernet0/1)
*Mar. 1 01:35:08.070:   type SOLICIT(1), xid 4
*Mar. 1 01:35:08.070:   option ELAPSED-TIME(8), len 6
*Mar. 1 01:35:08.070:     elapsed-time 0
*Mar. 1 01:35:08.070:   option CLIENTID(1), len 45
*Mar. 1 01:35:08.070:     00-01-00-01-7C-E0-70-A5-00-01-64-D1-95-66
*Mar. 1 01:35:08.070:   option ORO(6), len 10
*Mar. 1 01:35:08.070:     IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar. 1 01:35:08.070:   option IA-PD(25), len 16
*Mar. 1 01:35:08.070:     IAID 0x27382, T1 0, T2 0
*Mar. 1 01:35:08.070: IPv6 DHCP: Using interface pool IPV6POOL-A
```

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

```
*Mar. 1 01:35:08.070: IPv6 DHCP: Sending REPLY to FE80::201:64FF:FED1:9566 on
GigabitEthernet0/1
*Mar. 1 01:35:08.070: IPv6 DHCP: detailed packet contents
*Mar. 1 01:35:08.070:   src FE80::1 (GigabitEthernet0/1)
*Mar. 1 01:35:08.070:   dst FE80::201:64FF:FED1:9566 (GigabitEthernet0/1)
*Mar. 1 01:35:08.070:   type REPLY(7), xid 4
*Mar. 1 01:35:08.070:   option SERVERID(2), len 24
*Mar. 1 01:35:08.070:     00030001000197776A01
*Mar. 1 01:35:08.070:   option CLIENTID(1), len 45
*Mar. 1 01:35:08.070:     00-01-00-01-7C-E0-70-A5-00-01-64-D1-95-66
*Mar. 1 01:35:08.070:   option IA-PD(25), len 41
*Mar. 1 01:35:08.070:     IAID 0x27382, T1 0, T2 0
*Mar. 1 01:35:08.070:     option IAPREFIX(26), 29
*Mar. 1 01:35:08.070:       preferred 0, valid 0, prefix 0.0.0.0/0
*Mar. 1 01:35:08.070:   option DNS-SERVERS(23), len 20
*Mar. 1 01:35:08.070:     2001:DB8:ACAD:A::ABCD
*Mar. 1 01:35:08.070:   option DOMAIN-LIST(24), len 5
*Mar. 1 01:35:08.070:     ccna-StatefulDHCPv6.com
```

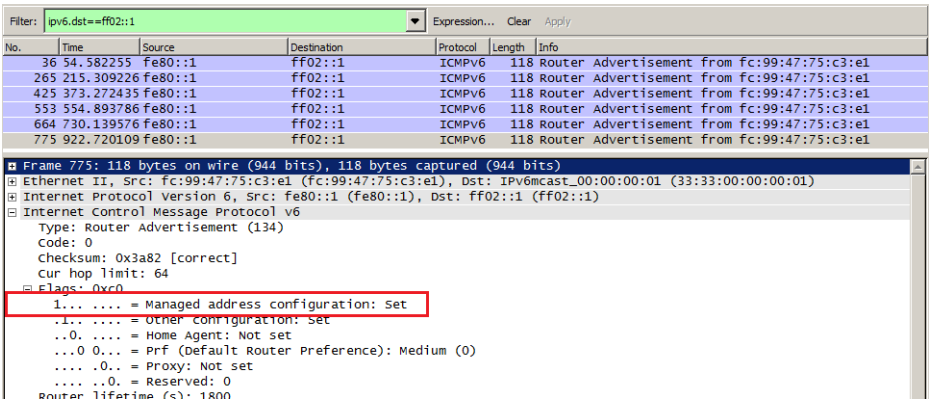
Paso 6: Verificar DHCPv6 con estado en la PC-A.

a. Detenga la captura de Wireshark en la PC-A.

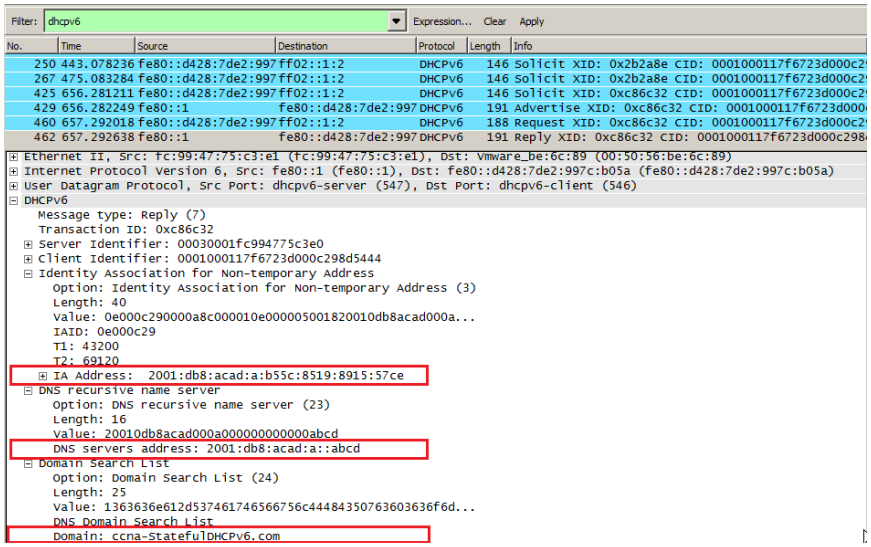
Respuesta. Como se realiza la práctica en PT, esta parte no se realiza.

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).

Respuesta. Como se realiza la práctica en PT, esta parte no se realiza. De forma física, quedaría de la siguiente forma:



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?

   Respuesta. DHCPv6 con estado utiliza más recursos de memoria ya que este método de direccionamiento requiere que el router guarde dinámicamente el estado de información a cerca de los clientes DHCPv6. En DHCPv6 sin estado, los clientes no usan el servidor DHCP para obtener la información de direccionamiento.

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

   Respuesta. El tipo de asignación dinámica de direcciones IPv6 que recomienda CISCO es la de DHCPv6 sin estado cuando implementa y desarrolla redes IPv6 sin un Registro de Red Cisco (CNR)

IdT y DHCP

Situación

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

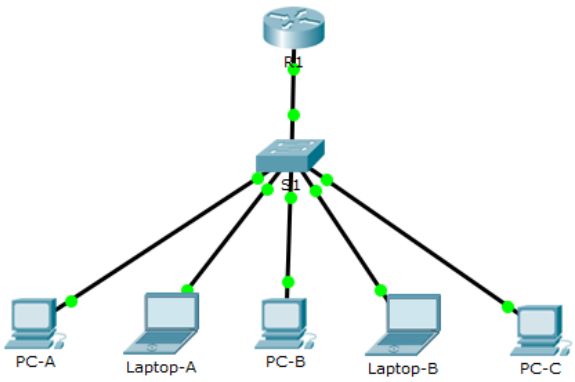
Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

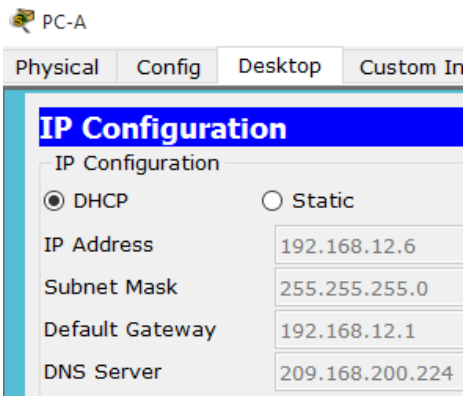
Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

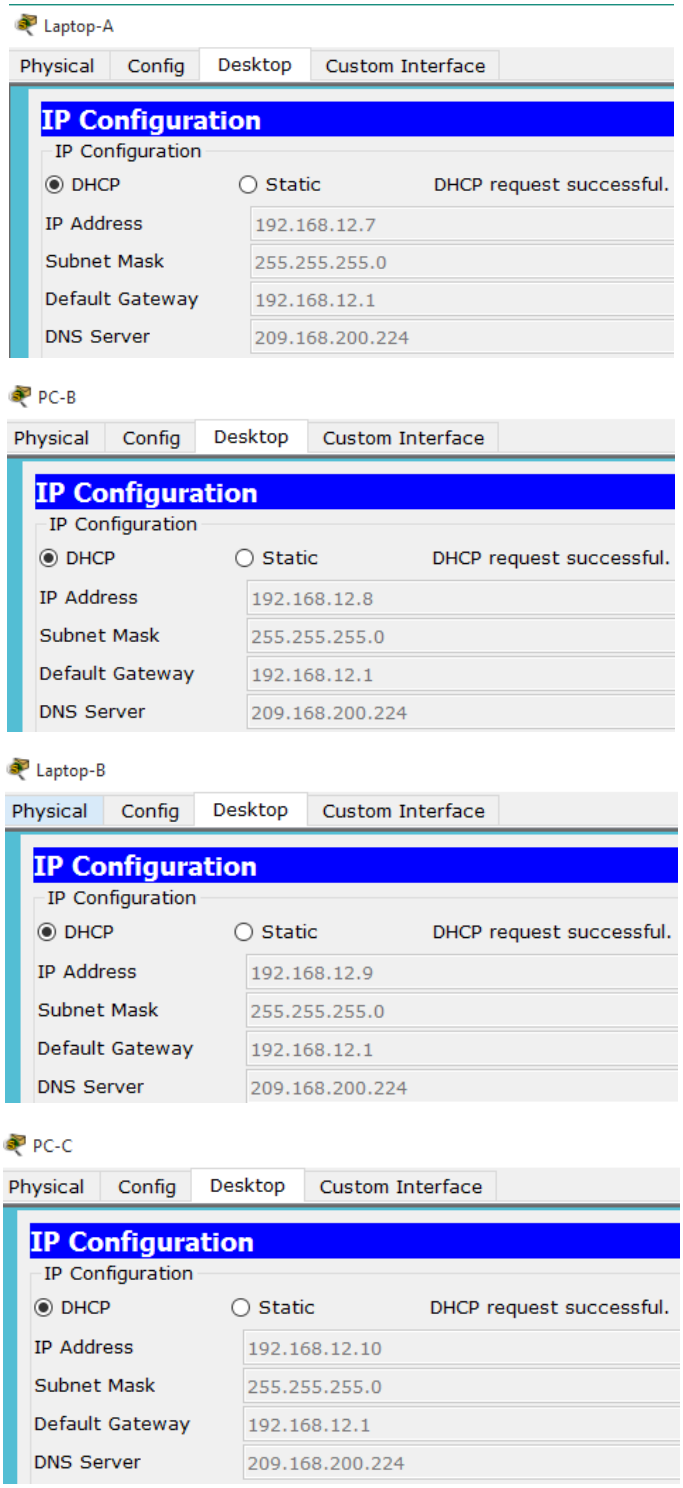
- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.

```
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#service password-encryption
R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Acceso solo a personal autorizado#

R1(config)#enable secret class
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#int g0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown

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)#exit
R1(config)#ip dhcp excluded address 192.168.12.1 192.168.12.5
                                   ^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp excluded-address 192.168.12.1 192.168.12.5
R1(config)#ip dhcp pool HOME-DOMESTIC
R1(dhcp-config)#network 192.168.12.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.12.1
R1(dhcp-config)#dns-server 209.168.200.224
R1(dhcp-config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

- 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.

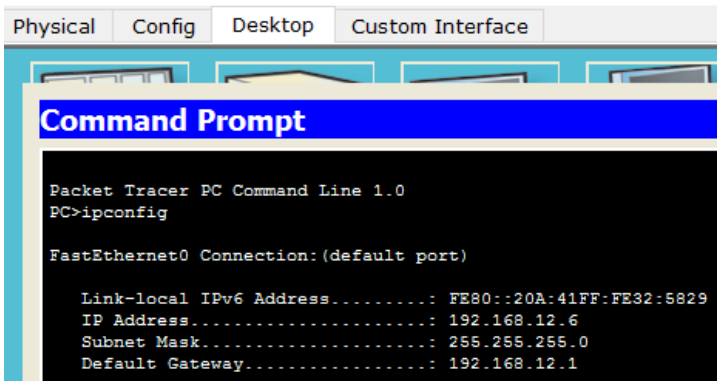




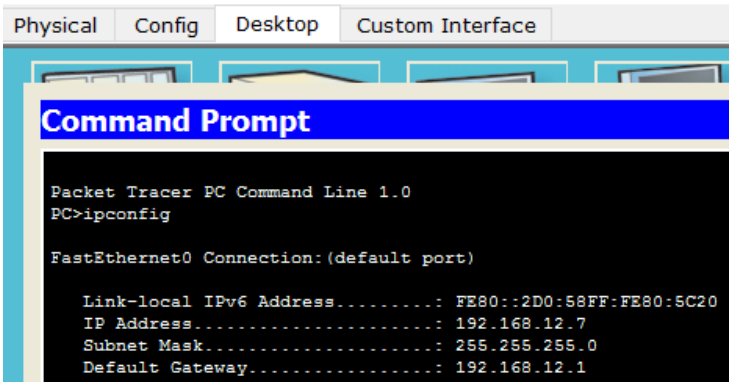


- Muestre los resultados que validen que cada terminal garantiza una dirección IP del servidor. Utilice un programa de captura de pantalla para guardar la información del resultado o emplee el comando de la tecla ImprPant.

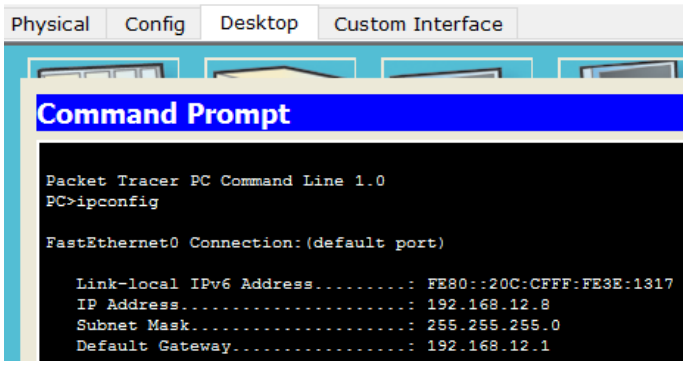
PC-A



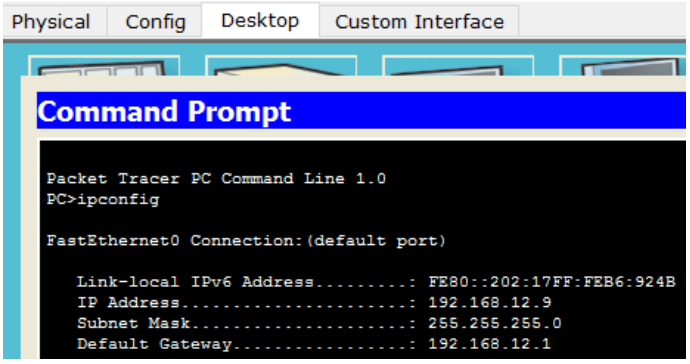
Laptop-A

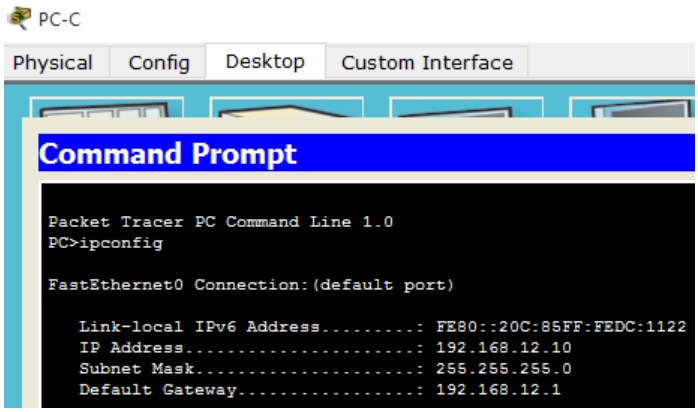


PC-B



Laptop-B





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

  Respuesta. La configuración de DHCP es importante para la optimización de procesos de las empresasy por supuesto, redes domésticas. DHCP se puede ajustar a las necesidades de los clientes, sean individuales como de empresas grandes, mediana y pequeñas y por supuesto organizaciones.

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?

   Respuesta. Los routers de Cisco brindan entre otras cosas, mayor seguridad y sobre todo, la configuración de DHCP en un router es sencilla

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.

   Respuesta. Para la administración de direcciones IP, para la configuración de cliente de red centralizada, para la compatibilidad con clientes locales y remotos, para la amplia compatibilidad de red y para la asignación de rangos específicos a ciertas áreas específicas.

11.2.2.6 Práctica de laboratorio – Configuración de NAT dinámica y estática

Topología

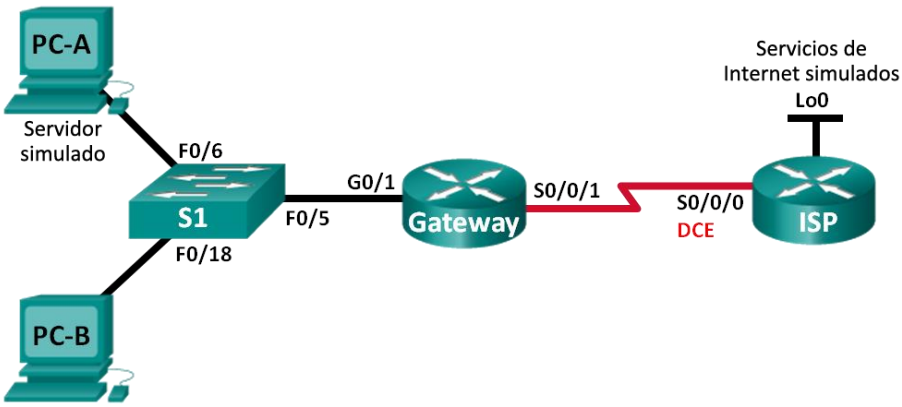


Tabla de direccionamiento

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

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

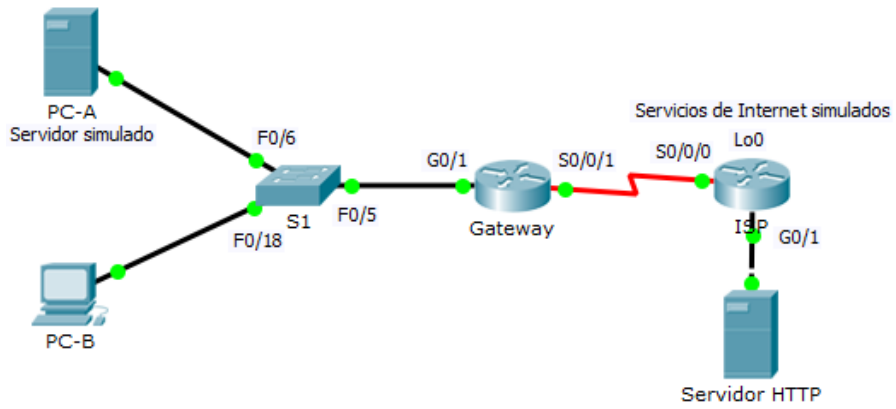
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar 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

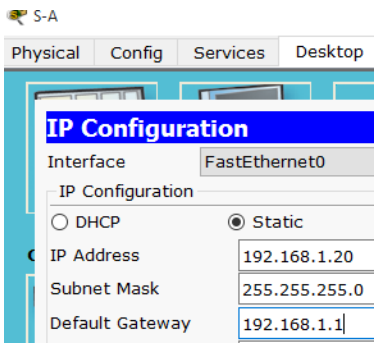
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

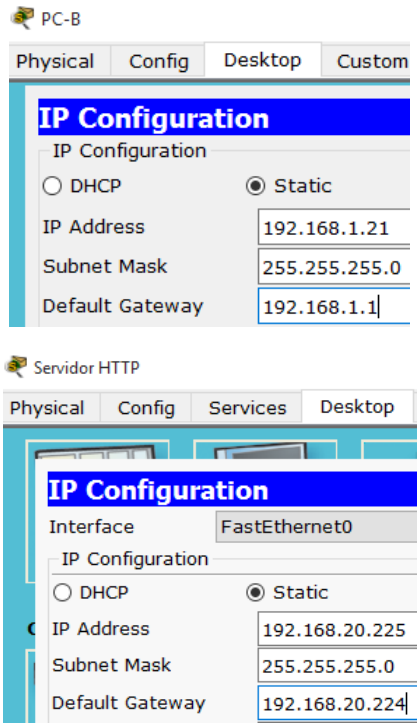
Paso 1: Realizar el cableado de red tal como se muestra en la topología.

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.

Respuesta. Como se realiza el laboratorio en PT, no se hace necesario inicilizar y volver a cargar los routers y switches

Paso 4: Configurar los parámetros básicos para cada router.

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

```
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#int lo0

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

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

ISP(config-if)#ip address 192.31.7.1 255.255.255.255
ISP(config-if)#int s0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

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

```
ISP(config)#int g0/1
ISP(config-if)#ip address 192.168.20.224
% Incomplete command.
ISP(config-if)#ip address 192.168.20.224 255.255.255.0
ISP(config-if)#no shutdown

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

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

```
Router(config)#hostname Gateway
Gateway(config)#no ip domain-lookup
Gateway(config)#service password-encryption
Gateway(config)#enable secret class
Gateway(config)#line vty 0 4
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#line console 0
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#int g0/1
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config-if)#no shutdown

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

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

Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip address 209.165.201.18
% Incomplete command.
Gateway(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway(config-if)#no shurdown
                    ^
% Invalid input detected at '^' marker.

Gateway(config-if)#no shutdown

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

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

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

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

Respuesta. PT no admite los comandos

```
ISP#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#username webuser privilege 15 secret webpass
ISP(config)#ip http server
                ^
% Invalid input detected at '^' marker.

ISP(config)#ip http authentication local
                ^
% Invalid input detected at '^' marker.
```

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
```

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

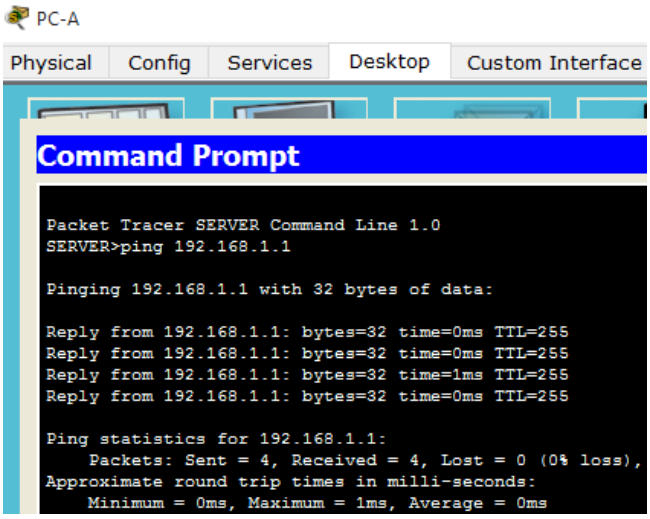
```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

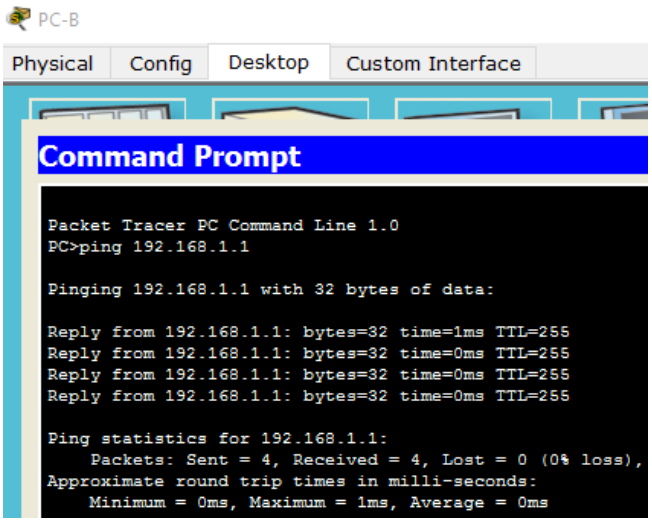
Paso 7: Guardar la configuración en ejecución en la configuración de inicio.

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

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

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
```

```
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

     192.31.7.0/32 is subnetted, 1 subnets
C       192.31.7.1/32 is directly connected, Loopback0
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/1
L       192.168.20.224/32 is directly connected, GigabitEthernet0/1
     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
```

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)#end
Gateway#
%SYS-5-CONFIG_I: Configured from console by console
```

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 = 209.165.200.225

¿Quién asigna la dirección global interna?

Respuesta. La dirección global interna está asignada por el router donde se encuentra la NAT pool

¿Quién asigna la dirección local interna?

Respuesta. La dirección local interna está asignada por el administrador de red

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

Gateway# show ip nat translations

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:10192.168.1.20:10    192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.225:11192.168.1.20:11    192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.225:12192.168.1.20:12    192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.225:9 192.168.1.20:9     192.31.7.1:9       192.31.7.1:9
---  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?

Respuesta. Los números de puerto que se usaron para el intercambio fueron los 10, 11, 12 y 9

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.

```
SERVER>telnet 209.165.201.17
Trying 209.165.201.17 ...Open


User Access Verification

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  192.31.7.1:23      192.31.7.1:23
tcp 209.165.200.225:1026192.168.1.20:1026  209.165.201.17:23  209.165.201.17:23
```

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?

Respuesta. Para la traducción, se usó el protocolo TCP

¿Cuáles son los números de puerto que se usaron?

Global/local interno: 1026

Global/local externo: 23

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

```
ISP#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/22 ms
```

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

Gateway# show ip nat translations

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:10192.168.1.20:10    209.165.201.17:10  209.165.201.17:10
icmp 209.165.200.225:6 192.168.1.20:6     209.165.201.17:6   209.165.201.17:6
icmp 209.165.200.225:7 192.168.1.20:7     209.165.201.17:7   209.165.201.17:7
icmp 209.165.200.225:8 192.168.1.20:8     209.165.201.17:8   209.165.201.17:8
icmp 209.165.200.225:9 192.168.1.20:9     209.165.201.17:9   209.165.201.17:9
---  209.165.200.225   192.168.1.20       ---                ---
```

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

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

Gateway# show ip nat statistics

```
Gateway#show ip nat statics
                         ^
% Invalid input detected at '^' marker.

Gateway#show ip nat statistics
Total translations: 5 (1 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 158  Misses: 26
Expired translations: 22
Dynamic mappings:
```

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

Parte 3: Configurar y verificar la NAT dinámica

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

Paso 1: Borrar las NAT.

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

Gateway# clear ip nat translation *

Gateway# clear ip nat statistics

Respuesta. PT no soporta el segundo comando

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

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

```
Gateway(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console
```

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.

```
Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 160  Misses: 27
Expired translations: 22
Dynamic mappings:
```

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#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)#ip nat pool public_access 209.165.200.242 209.165.200.254 netmask
255.255.255.224
```

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)#end
Gateway#
%SYS-5-CONFIG_I: Configured from console by console

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

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

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

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.242:5 192.168.1.21:5     192.31.7.1:5       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
---  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?

Respuesta. El número de puerto que se usó para el intercambio fue el 5

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.*

Respuesta. Se ingresa al servidor HTTP web que se adicionó por la interfaz G0/1 con dirección IP 192.168.20.225. Este paso se adicionó ya que los comandos del punto 1, paso 5 no funcionaron y se quería probar


```
Gateway#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.225   192.168.1.20       ---                ---
tcp 209.165.200.242:1025192.168.1.21:1025  192.168.20.225:80  192.168.20.225:80
```

c. Muestre la tabla de NAT.

¿Qué protocolo se usó en esta traducción?

Respuesta. Se usó el protocolo TCP

¿Qué números de puerto se usaron?

Interno: 1025

Externo: 80

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

Respuesta. El puerto 80 y el servicio web

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: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 172  Misses: 32
Expired translations: 27
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
```

b. Borre las NAT y las estadísticas.

```
Gateway#clear ip nat translation *
```

c. Haga ping al ISP (192.31.7.1) desde ambos hosts.

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=4ms 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 = 4ms, Average = 2ms
```

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=10ms 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 = 10ms, Average = 3ms
```

d. Muestre la tabla y las estadísticas de NAT.

Gateway# show ip nat statistics

```
Gateway#clear ip nat translation *
Gateway#show ip nat statistics
Total translations: 8 (0 static, 8 dynamic, 8 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 180  Misses: 40
Expired translations: 27
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 8
 pool public_access: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13 , allocated 2 (15%), misses 0
```

Gateway# show ip nat translation

```
Gateway#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.243:10192.168.1.21:10    192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.243:11192.168.1.21:11    192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.243:12192.168.1.21:12    192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.243:9 192.168.1.21:9     192.31.7.1:9       192.31.7.1:9
```

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

Reflexión

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

   Respuesta. NAT debe utilizarse ya que puede ayudar a conserva las direcciones IPv4 públicas. Esto se logra al permitir que las redes utilicen direcciones IPv4 privadas internamente y al proporcionar la traducción a una dirección pública solo cuando sea necesario. NAT tiene el beneficio adicional de proporcionar cierto grado de privacidad y seguridad adicional a una red, ya que oculta las direcciones IPv4 internas de las redes externas.

2. ¿Cuáles son las limitaciones de NAT?

   Respuesta. Entre sus limitaciones o desventajas se tienen: El rendimiento de la red, en especial, en el caso de los protocolos en tiempo real como VoIP. NAT aumenta los retrasos de switching porque la traducción de cada dirección IPv4 dentro de los encabezados del paquete lleva tiempo. Otra desventaja del uso de NAT es que se pierde el direccionamiento de extremo a extremo. Muchos protocolos y aplicaciones de Internet dependen del direccionamiento de extremo a extremo desde el origen hasta el destino. También se reduce el seguimiento IPv4 de extremo a extremo. El uso de NAT también genera complicaciones para los protocolos de tunneling como IPsec, ya que NAT modifica los valores en los

encabezados que interfieren en las verificaciones de integridad que realizan IPsec y otros protocolos de tunneling.

11.2.3.7 Práctica de laboratorio – Configuración de un conjunto de NAT con sobrecarga y PAT

Topología

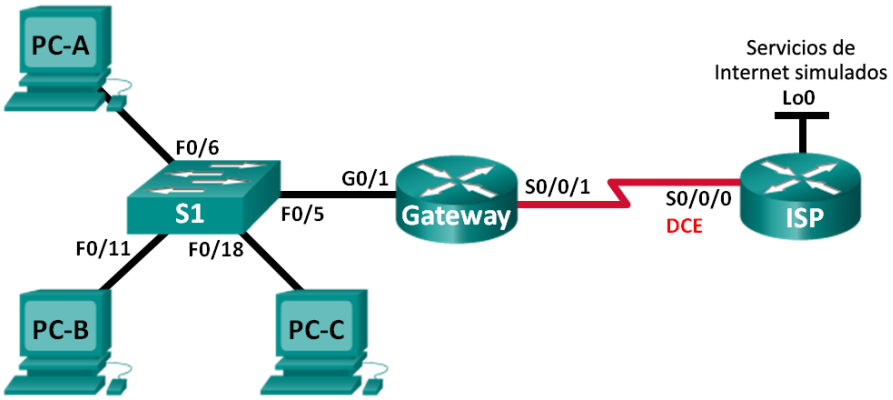


Tabla de direccionamiento

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	255.255.255.252	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

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.

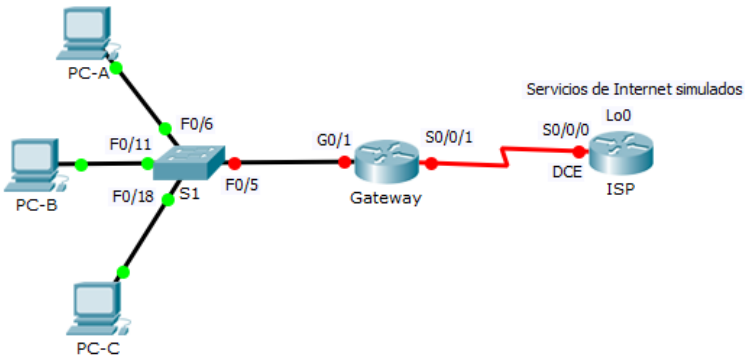
Recursos necesarios

- 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

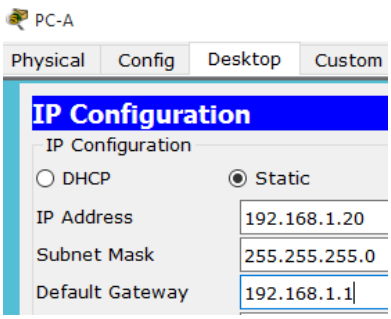
Parte 1: Armar la red y verificar la conectividad

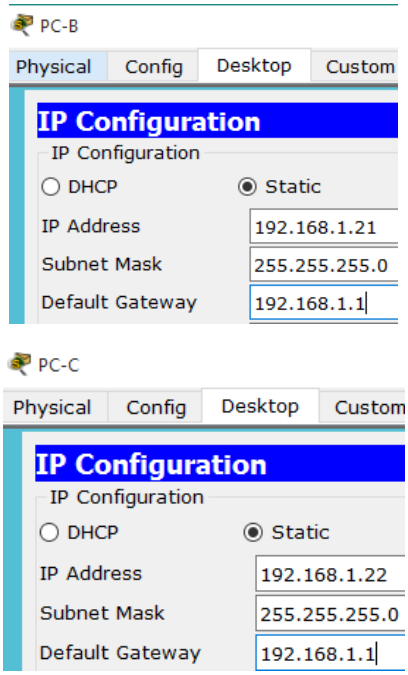
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

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



Paso 2: Configurar los equipos host.





Paso 3: Inicializar y volver a cargar los routers y los switches.

Respuesta. Como el laboratorio se usa en PT, no se hace necesario inicializar y volver a cargar los routers y switches

Paso 4: Configurar los parámetros básicos para cada router.

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

```
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.165.201.17
% Incomplete command.
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
ISP(config-if)#int lo0

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

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

ISP(config-if)#ip address 192.31.7.1 255.255.255.255
ISP(config-if)#no shutdown
ISP(config-if)#end
ISP#
%SYS-5-CONFIG_I: Configured from console by console

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

```
Router(config)#hostname Gateway
Gateway(config)#no ip domain-lookup
Gateway(config)#service password-encryption
Gateway(config)#enable secret class
Gateway(config)#line vty 0 4
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#line console 0
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#int g0/1
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config-if)#no shutdown

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

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

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

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

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

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

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

Paso 5: Cconfigurar 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
```

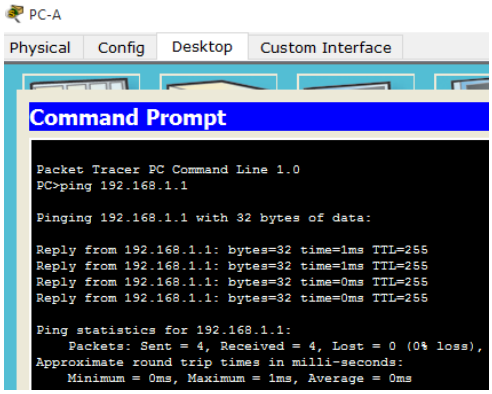
b. Cree una ruta predeterminada del router Gateway al router ISP.

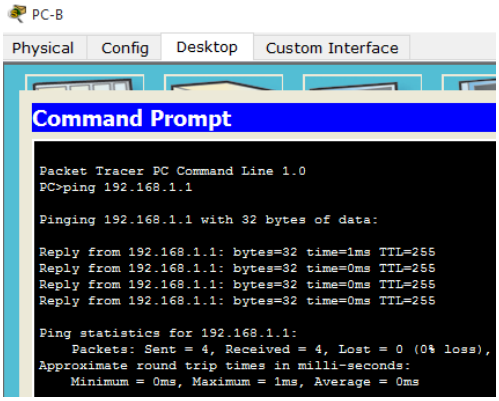
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17

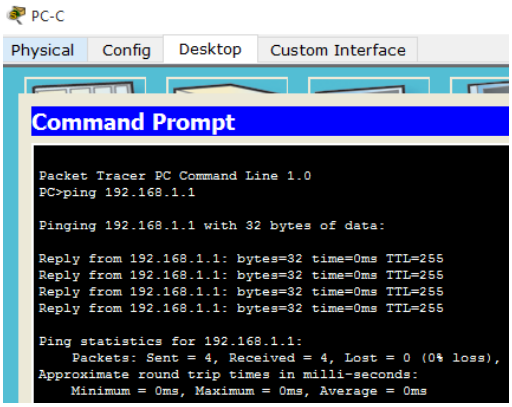
```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

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.

```
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

     192.31.7.0/32 is subnetted, 1 subnets
C       192.31.7.1/32 is directly connected, Loopback0
     209.165.200.0/29 is subnetted, 1 subnets
S       209.165.200.224/29 [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
```

```
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

```
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

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

Paso 4: Especifique las interfaces.

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

Gateway(config)# interface g0/1

Gateway(config-if)# ip nat inside

Gateway(config-if)# interface s0/0/1

Gateway(config-if)# ip nat outside

```
Gateway(config)#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
```

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>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=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

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

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

```
PC>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=3ms 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 = 3ms, Average = 1ms
```

b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# show ip nat statistics

```
Gateway#show ip nat statistics
Total translations: 8 (0 static, 8 dynamic, 8 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 16  Misses: 16
Expired translations: 8
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 8
 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 209.165.200.225:1024192.168.1.22:9     192.31.7.1:9       192.31.7.1:1024
icmp 209.165.200.225:1025192.168.1.22:10    192.31.7.1:10      192.31.7.1:1025
icmp 209.165.200.225:1026192.168.1.22:11    192.31.7.1:11      192.31.7.1:1026
icmp 209.165.200.225:1027192.168.1.22:12    192.31.7.1:12      192.31.7.1:1027
icmp 209.165.200.225:10192.168.1.21:10    192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.225:11192.168.1.21:11    192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.225:12192.168.1.21:12    192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.225:13192.168.1.20:13    192.31.7.1:13      192.31.7.1:13
icmp 209.165.200.225:14192.168.1.20:14    192.31.7.1:14      192.31.7.1:14
icmp 209.165.200.225:15192.168.1.20:15    192.31.7.1:15      192.31.7.1:15
icmp 209.165.200.225:16192.168.1.20:16    192.31.7.1:16      192.31.7.1:16
icmp 209.165.200.225:9 192.168.1.21:9     192.31.7.1:9       192.31.7.1:9
```

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?

Respuesta. Se indican tres direcciones locales internas: 192.168.1.20, 192.168.1.21 y 192.168.1.22

¿Cuántas direcciones IP globales internas se indican?

Respuesta. Se indica una dirección IP global interna: 209.165.200.225

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas?

Respuesta. En este caso se usaron ocho números de puerto

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

Respuesta. El ping falla ya que el router conoce el lugar de las direcciones internas globales es su tabla de ruteo, en cambio, las direcciones internas locales no están contenidas en la tabla de ruteo o no están notificadas

```
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)
```

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: 28  Misses: 28
Expired translations: 28
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: 28  Misses: 28
Expired translations: 28
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: 28  Misses: 28
Expired translations: 28
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?

Respuesta. Se usó el comando ***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 pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

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

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

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

Paso 5: Asociar la lista de origen a la interfaz externa.

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

```
Gateway(config)#ip nat inside source list 1 interface s0/0/1 overload
```

Paso 6: Probar la configuración PAT.

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=10ms 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 = 10ms, Average = 3ms
```

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

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

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

b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# show ip nat statistics

```
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 52  Misses: 52
Expired translations: 40
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 209.165.201.18:1024192.168.1.22:17    192.31.7.1:17      192.31.7.1:1024
icmp 209.165.201.18:1025192.168.1.22:18    192.31.7.1:18      192.31.7.1:1025
icmp 209.165.201.18:1026192.168.1.22:19    192.31.7.1:19      192.31.7.1:1026
icmp 209.165.201.18:1027192.168.1.22:20    192.31.7.1:20      192.31.7.1:1027
icmp 209.165.201.18:17 192.168.1.21:17     192.31.7.1:17      192.31.7.1:17
icmp 209.165.201.18:18 192.168.1.21:18     192.31.7.1:18      192.31.7.1:18
icmp 209.165.201.18:19 192.168.1.21:19     192.31.7.1:19      192.31.7.1:19
icmp 209.165.201.18:20 192.168.1.21:20     192.31.7.1:20      192.31.7.1:20
icmp 209.165.201.18:21 192.168.1.20:21     192.31.7.1:21      192.31.7.1:21
icmp 209.165.201.18:22 192.168.1.20:22     192.31.7.1:22      192.31.7.1:22
icmp 209.165.201.18:23 192.168.1.20:23     192.31.7.1:23      192.31.7.1:23
icmp 209.165.201.18:24 192.168.1.20:24     192.31.7.1:24      192.31.7.1:24
```

Reflexión

¿Qué ventajas tiene la PAT?

Respuesta. PAT tiene varias ventajas, entre ellas: Con PAT, se pueden asignar varias direcciones a una o más direcciones, debido a que cada dirección privada también se rastrea con un número de puerto. PAT garantiza que los dispositivos usen un número de puerto TCP distinto para cada sesión con un servidor en Internet. Cuando llega una respuesta del servidor, el número de puerto de origen, que se convierte en el número de puerto de destino en la devolución, determina a qué dispositivo el router reenvía los paquetes. El proceso de PAT

también valida que los paquetes entrantes se hayan solicitado, lo que añade un grado de seguridad a la sesión.

Conclusiones

El desarrollo de la actividad práctica permitió interiorizar conceptos y procedimientos necesarios para el buen desempeño profesional, trayendo a colación temas base para el manejo del mundo del networking. Lo anterior con la implementación de una metodología de enseñanza-aprendizaje que permitió retomar cada temática estudiada en los diferentes capítulos.

Para el desarrollo de esta etapa hemos abarcado con los capítulos anteriores uno gran cantidad de conocimiento que este a su vez nos lleva a poder resolver los ejercicios planteados en este capítulo con ellos aprendimos nuevas reglas de configuración, protocolos y seguridad, ante todo.

Referencias bibliográficas

CISCO. (2017). Módulo CP CCNA2. CCNA R&S: Routing and switching essentials. Capítulos 7, 8, 9, 10 y 11. Recuperado de https://www.netacad.com/es/

Oracle. (2015). Ventajas del us de DHCP. Recuperado de https://docs.oracle.com/cd/E24842_01/html/820-2981/dhcp-overview-12a.html