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

PASO 7 - ACTIVIDAD COLABORATIVA 4

ELABORADO POR

DIEGO FRANCISCO BALLEN

LEIDY JOHANNA RAMIREZ

HERNAN ESTEBAN TOVAR

YESSICA KATHERINE GALINDO

DIEGO FERNANDO ORTIZ

TUTOR

NILSON ALBEIRO FERREIRA MANZANARES

GRUPO 8

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

NOVIEMBRE DE 2017

TABLA DE CONTENIDO

Pág.

INTRODUCCIÓN……....3

OBJETIVOS……4

DESARRLLO DEL TRABAJO……5

CONCLUSIONES……...……..120

REFERENCIAS BIBLIOGRÁFICAS……..……121

INTRODUCCION

En el siguiente informe se dan conocer las diferentes prácticas correspondientes a la actividad colaborativa 4 del diplomado de profundización de cisco CCNA, donde se realizan 14 prácticas en el programa de Cisco Packet tracer, donde algunas prácticas se realizaran desde cero (creando desde la topología hasta las configuraciones de cada dispositivo para establecer la conectividad y el objetivo de cada practica) y también se realizaran las practicas desde un archivo pka, en el cual se aplicaran las configuraciones solicitadas en dichas prácticas.

Con ello se pretende conocer y poner en práctica temas como Enrutamiento Dinámico, OSPF de una sola área, Listas de control de acceso, DHCP y Traducción de direcciones IP para IPv4.

OBJETIVOS

Obj. General

- Comprender los temas de Enrutamiento Dinámico, OSPF de una sola área, Listas de control de acceso, DHCP y Traducción de direcciones IP para IPv4.

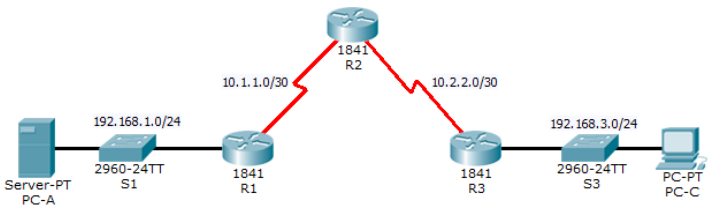
Obj. Especifico

- Realizar las diferentes prácticas del momento 6 del *Diplomado De Profundización Cisco* en el programa de *cisco Packet tracer.*
- Analizar cada una de las prácticas realizadas.
- Documentar cada práctica, para tener mayor claridad en temas relacionados con cada una de ellas.

DESARROLLO DE LAS PRÁCTICAS

4.4.1.2 Packet Tracer - CONFIGURAR IP ACL PARA MITIGAR LOS ATAQUES

Tipología



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

OBJETIVOS

- Verificar la conectividad entre los dispositivos antes de la configuración del firewall.
- Uso ACL para garantizar el acceso remoto a los routers sólo está disponible desde la estación de administración de PC- C.
- Configurar ACL en R1 y R3 para mitigar los ataques.
- Verificar la funcionalidad ACL.

ANTECEDENTES / ESCENARIO

El acceso a los routers R1 , R2 y R3 sólo se permitirá desde el PC -C , la estación de administración . PC- C también se utiliza para la prueba de conectividad a PC- A, un servidor que proporciona DNS , SMTP , FTP y HTTPS servicios.

Procedimiento operativo estándar es aplicar las ACL en los routers de borde para mitigar las amenazas comunes basados en la fuente y / o la dirección IP de destino. En esta actividad , se crea ACL en los routers de borde R1 y R3 para lograr este objetivo . A continuación, compruebe la funcionalidad ACL de hosts internos y externos.

Los routers han sido pre- configurado con lo siguiente:

o Habilitar contraseña: **ciscoenpa55**
o Contraseña para la consola : **ciscoconpa55**
o nombre de usuario para las líneas VTY : **SSHadmin**
o contraseña para las líneas VTY : **ciscosshpa55**
o direccionamiento IP
o enrutamiento estático

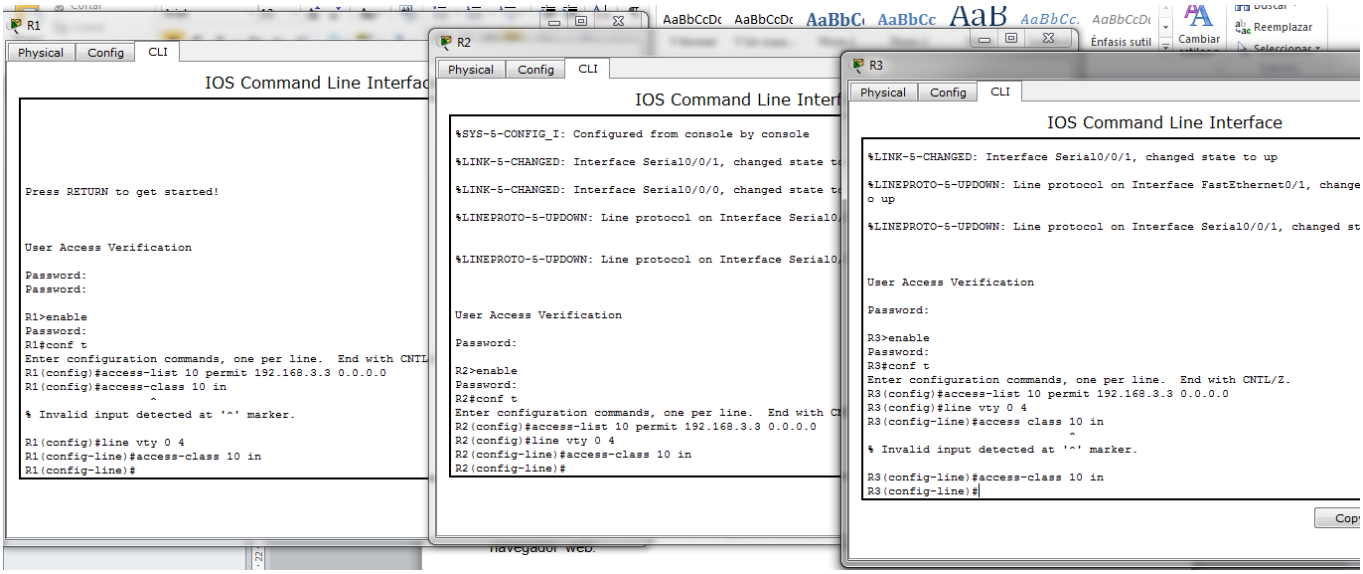
PARTE 1 : VERIFICAR LA CONECTIVIDAD DE RED BÁSICA

Desde PC- A se verifica la conectividad a PC- C y R2

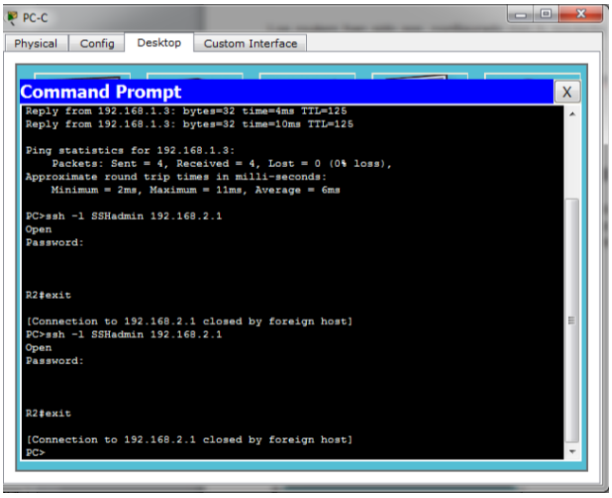
Se abre un navegador web en el servidor de PC- A (192.168.1.3) para mostrar la página web.

PARTE 2 : EL ACCESO SEGURO A LA ROUTERS

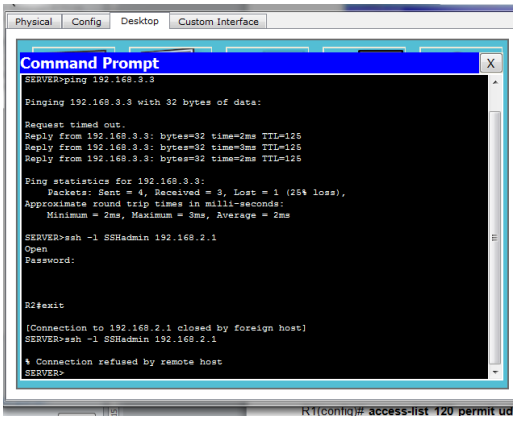
Se utiliza el comando access-list para crear un numerada IP ACL en R1 , R2 y R3, para Configurar ACL 10 y bloquear todo el acceso remoto a los enrutadores excepto de PC- C . Luego se usa el comando access-class para aplicar la lista de acceso para el tráfico entrante en las líneas VTY.



Se verifica el acceso exclusivo de la estación de administración de PC –C; estableciendo una sesión de SSH para 192.168.2.1 desde el PC -C , la cual es exitosa.



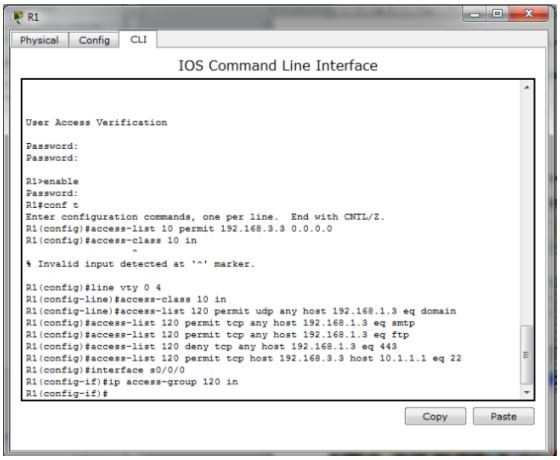
Establecer una sesión de SSH para 192.168.2.1 desde el PC –A, donde se observa falla.



PARTE 3 : CREAR UN IP ACL 120 NUMERADO EN R1

Permitir que cualquier host externo para acceder DNS , SMTP y servicios FTP en el servidor de PC- A, negar cualquier acceso al host externo para HTTPS servicios en PC -A, y permiten PC- C para acceder a R1 a través de SSH.
Para ello se usan comandos **access-list**

Donde se configurar ACL 120 para permitir y negar el tráfico especificado específicamente y se utiliza el comando ***access-list*** para crear un numerada IP ACL, se anexa la interfaz ***S0 / 0 / 0 ,*** se usa el comando ***ip access-group*** para aplicar la lista de acceso para el tráfico entrante en la interfaz S0 / 0 / 0.

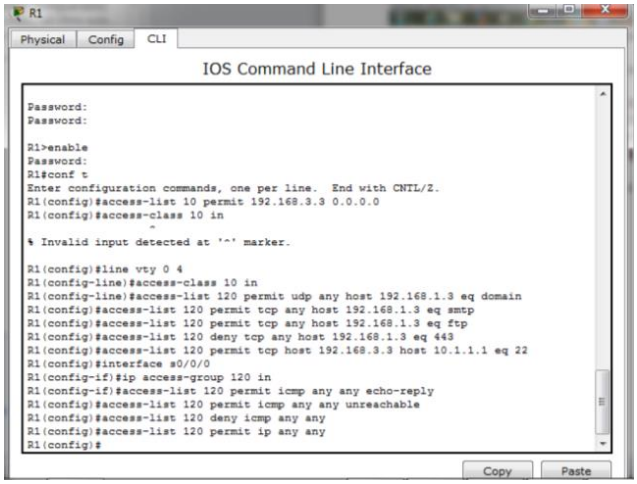


Ahora el PC- C no puede acceder a la PC –A.

PARTE 4: MODIFICAR UNA ACL EXISTENTE EN R1

Permiso respuestas de eco ICMP y mensajes de destino inaccesible desde la red externa (con respecto a R1); negar todos los otros paquetes ICMP entrantes.

La PC -A no puede hacer ping correctamente la interfaz loopback en R2.
Para solucionar este problema, se realizan los cambios necesarios en ACL 120 para permitir y denegar el tráfico especificado. Para ello se utiliza el comando access-list el cual crea un numerada IP ACL.

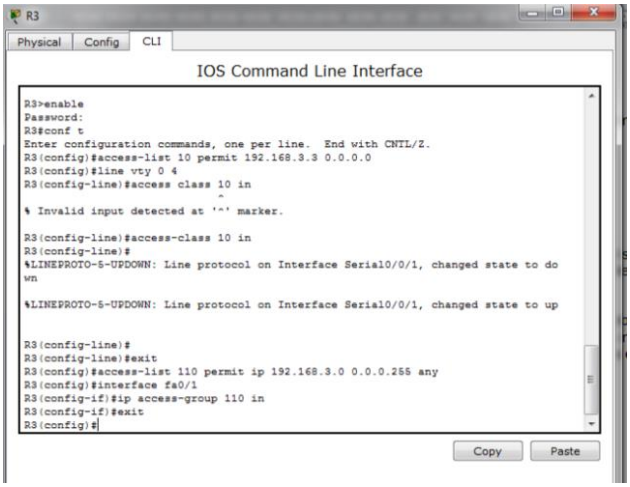


Ahora si, el PC- A puede hacer ping correctamente la interfaz loopback en R2.

PARTE 5: CREAR UN IP ACL NUMERADA 110 EN R3

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

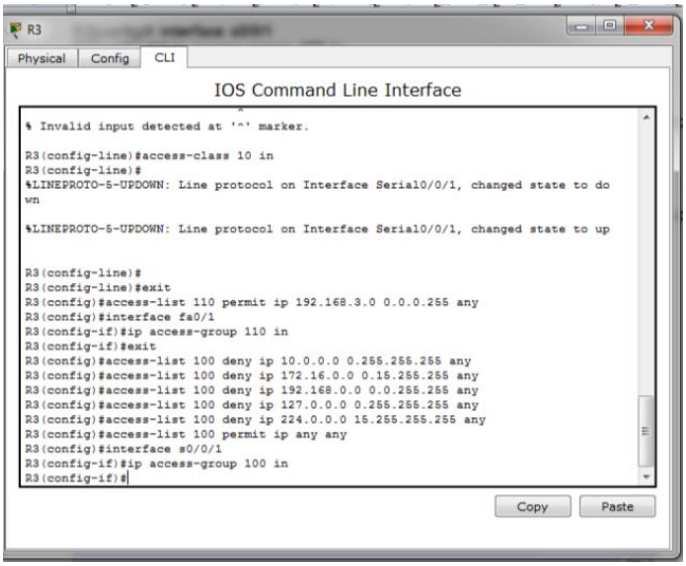
Se configura ACL 110 para permitir sólo el tráfico de la red interior, para ello se usa el comando ***access-list*** y se logra crear un numerada IP ACL, luego se anexa la ACL a la interfaz F0 / 1, utilizando el comando ip ***access-group*** y se aplica la lista de acceso para el tráfico entrante en la interfaz F0 / 1.



PARTE 6 : CREAR UN NUMERADA IP ACL 100 EN R3

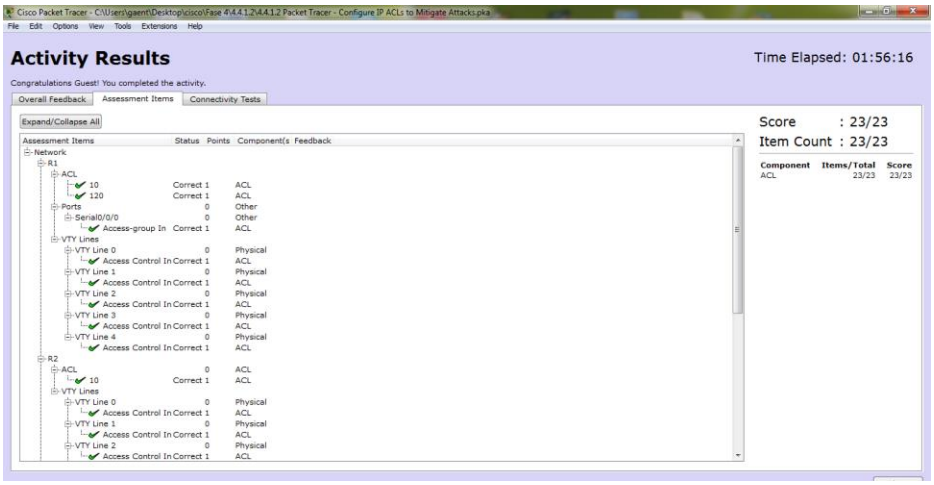
En R3, bloquear todos los paquetes que contienen la dirección IP de origen desde el siguiente conjunto de direcciones: 127.0.0.0/8~~number=plural , cualquier RFC 1918 direcciones privadas, y cualquier dirección de multidifusión IP .

Se configura ACL 100 para bloquear todo el tráfico especificado de la red exterior.
También debería bloquear el tráfico procedente de su propio espacio de direcciones interno si no es una dirección RFC 1918 , para ello se hace uso del comando ***access-list*** y se crea un numerada IP ACL y posteriormente se aplica la ACL a la interfaz Serial 0/0/1. Utilizando para ello el comando ***ip access-group*** y se aplica la lista de acceso para el tráfico entrante en la interfaz Serial 0/0/1.



Como se puede observar en la img. Se realiza prueba ingresando a la interfaz Serial 0/0/1 y efectivamente se deja caer.
Sucede porque las respuestas de eco ICMP son bloqueados por la ACL ya que provienen del espacio de direcciones 192.168.0.0/16.

Resultados:



Conclusiones De Practica: 4.4.1.2 Configure IP ACLs to Mitigate Attacks*

Después de haber realizado la anterior práctica se logra experimentar los cambios que suceden en la red al digitar determinados comandos en dispositivos como el Router o el pc sea el servidor o el pc final.

Los cambios identificados al ingresar comando como ***access-list:*** se logra crear un numerada IP ACL, para luego aplicar la ACL a la interfaz que se esté trabajando.

Otro comando que se resaltó en la práctica fue el comando ip ***access-group***: con el cual se aplica la lista de acceso para el tráfico entrante en la interfaz que se esté trabajando.

Ampliando un poco más la información con respecto al comando **access-list,** Se concluye que: Se logran brindar y denegar permisos para acceder a protocolos que se deseen utilizar en distintos hots de la red, es decir con este comando se colocan los permisos específicos para cada hots teniendo en cuenta su funcionalidad según sea la asignada o la necesidad requerida por el administrador de la red.

Como ejemplo de ello se observó en el R1 con este comando se permitió que cualquier host externo pueda acceder a DNS , SMTP y servicios FTP en el servidor de PC- A, y se negó cualquier acceso al host externo para HTTPS servicios en PC -A, de igual manera se permitió que PC- C pueda acceder a R1 a través de SSH.

Para identificar la funcionalidad que cada comando genera en el sistema es recomendable realizar pruebas de conectividad antes y después de digitar dicho comando, pues con ello, se tendrán más claros la importancia de los mismos en una red.

7.3.2.4. Práctica de laboratorio: configuración básica de RIPv2 y RIPng

Topología

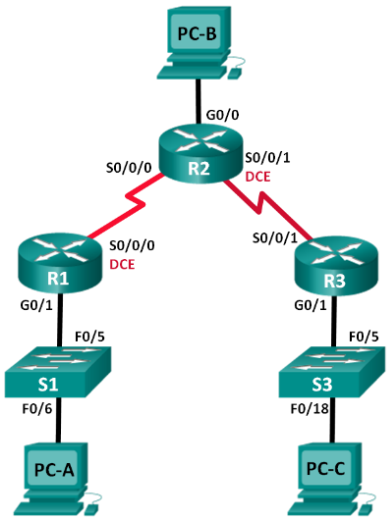


Tabla de direccionamiento

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	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Objetivos

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

Parte 2: configurar y verificar el routing RIPv2

Configurar y verificar que se esté ejecutando RIPv2 en los routers.

Configurar una interfaz pasiva.

Examinar las tablas de routing.

Desactivar la sumarización automática.

Configurar una ruta predeterminada.

Verificar la conectividad de extremo a extremo.

Parte 3: configurar IPv6 en los dispositivos

Parte 4: configurar y verificar el routing RIPng

Configurar y verificar que se esté ejecutando RIPng en los routers.

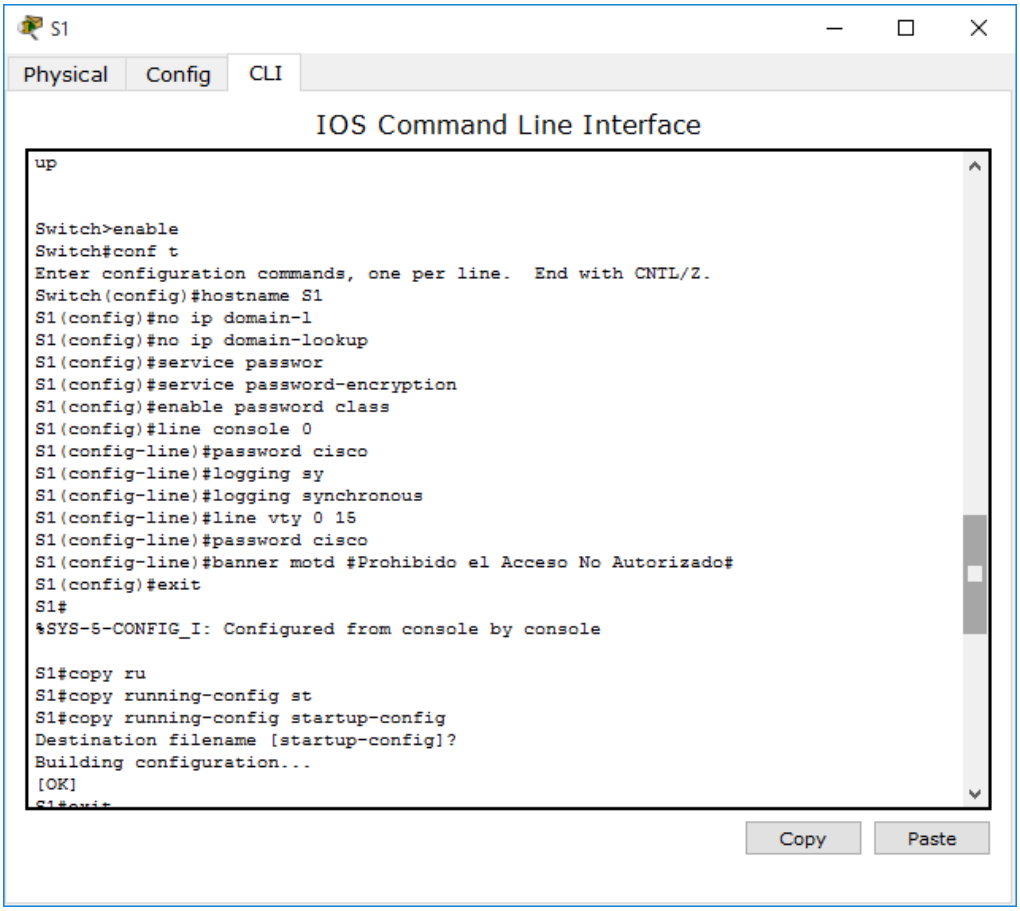
Examinar las tablas de routing.

Configurar una ruta predeterminada.

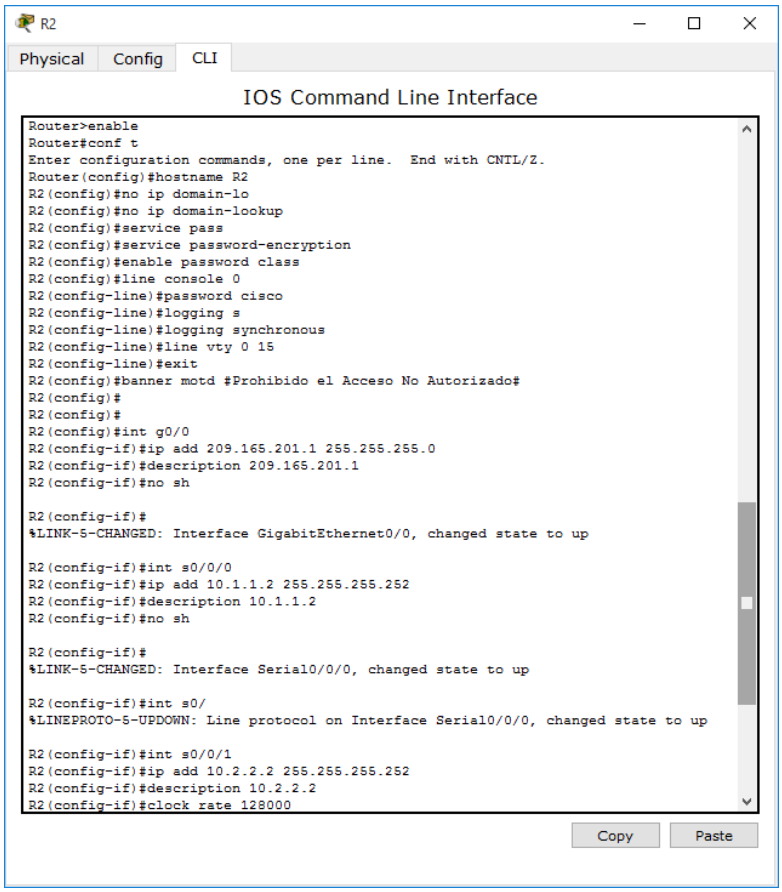
Verificar la conectividad de extremo a extremo.

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

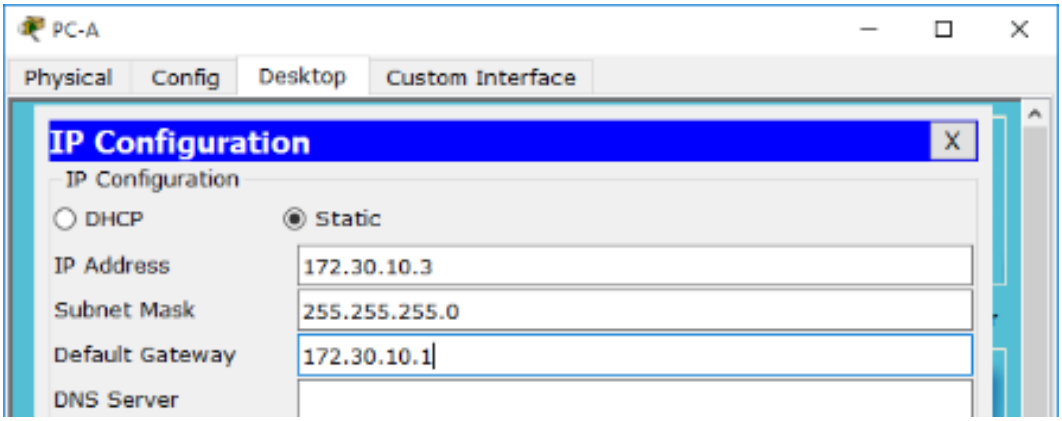
Configuración de los Switches S1 y S3



Configuración de los Router R1, R2 y R3

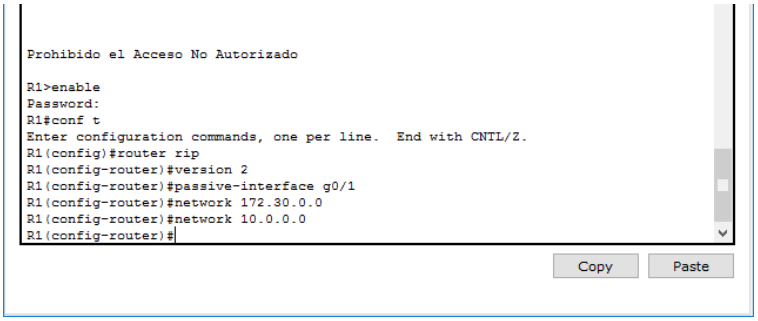


Direccionamiento de los Host

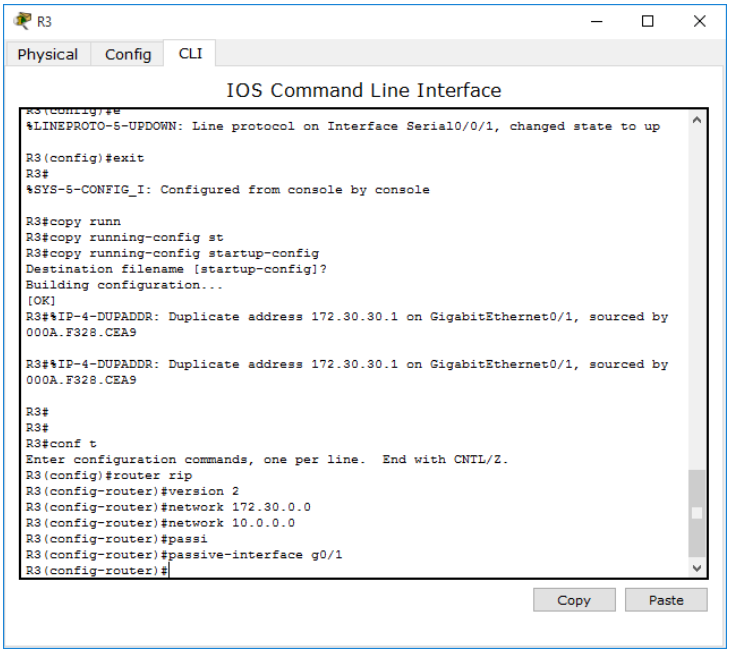


Luego se recomienda verificar la conectividad.

Parte 2: configurar y verificar el routing RIPv2



Configuración de RIP versión 2 en R3



Para la Configuración de RIP versión 2 en R2, se incluye la network 10.0.0.0, no se ejecuta el comando passive-interface en g0/0, pues se conecta a ella la red 209.165.201.0, la cual no está participando en RIP v2.

Estado Actual de la Red

```
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
R2#
```

Verifique la conectividad entre las computadoras.

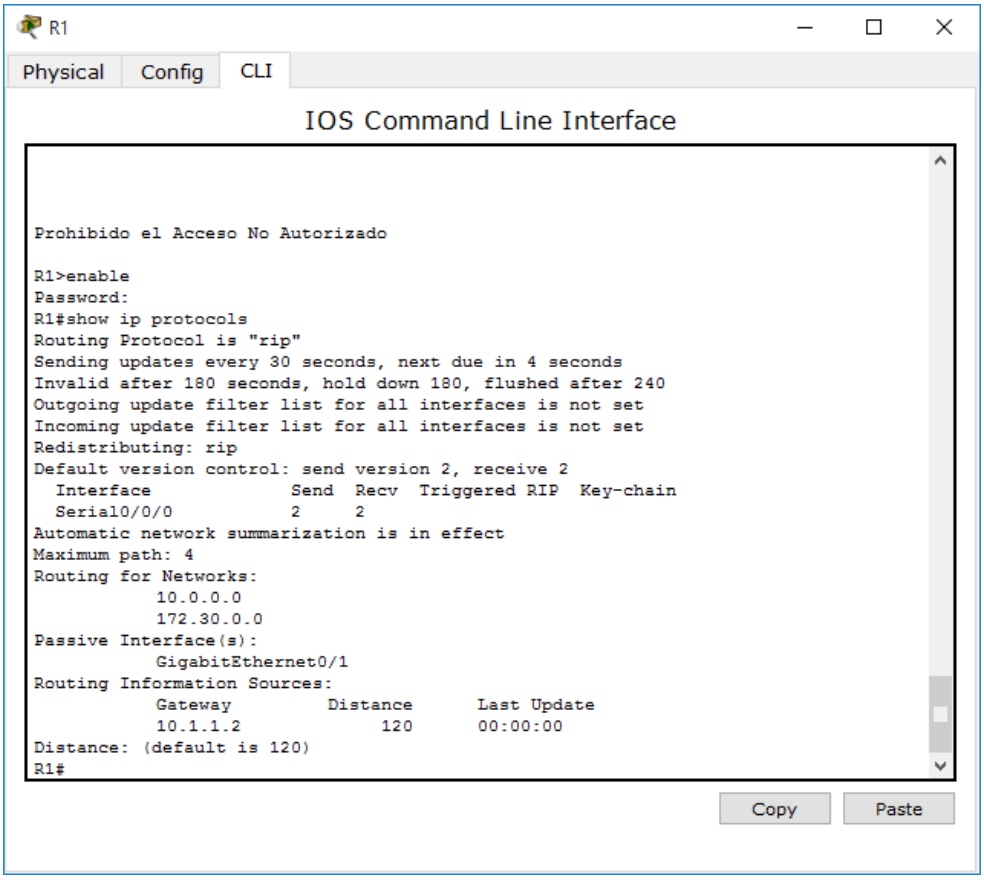
¿Es posible hacer ping de la PC-A a la PC-B? **No** ¿Por qué? **Porque no hay una ruta establecida, pues PC-B está en la red que no está participando en RIP.**

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

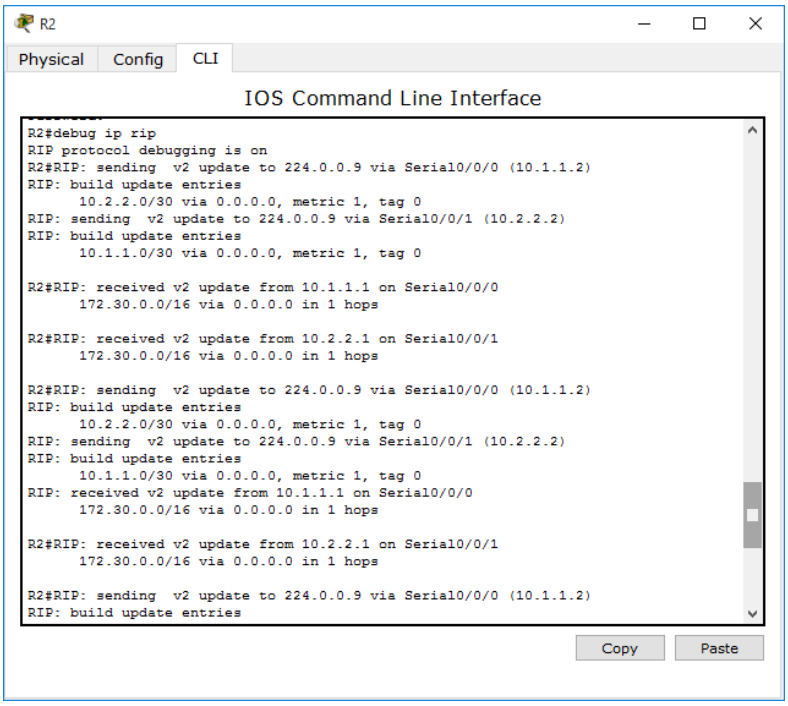
¿Es posible hacer ping de la PC-C a la PC-B? **No** ¿Por qué? **Porque PC-B pertenece a la LAN que no está participando en RIP**

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

Verificación del funcionamiento del RIPv2 en R1



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



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

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

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

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

2#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

2#undebug allRIP: 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

2#undebug allRIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
IP: build update entries
     10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
IP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
IP: build update entries
     10.1.1.0/30 via 0.0.0.0, metric 1, tag 0

2#undebug allRIP: received v2 update from 10.2.2.1 on Serial0/0/1
     172.30.0.0/16 via 0.0.0.0 in 1 hops
```

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

Desactivación de la Sumarización automática en los router

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#no aut
R3(config-router)#no auto-summary
R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#clear ip route *
```

Se ingresa el comando clear ip route * para borrar la tabla de ruteo

```
172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
   172.30.0.0/16 [120/1] via 10.1.1.1, 00:01:10, Serial0/0/0
                 is possibly down, routing via 10.2.2.1, Serial0/0/1
   172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:13, Serial0/0/0
   172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:09, Serial0/0/1
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
   209.165.201.0/24 is directly connected, GigabitEthernet0/0
```

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

172.30.30.0/24 via 0.0.0.0, metric 2, tag 0

172.30.10.0/24 via 0.0.0.0, metric 2, tag 0

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

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

Verificar la configuración de enrutamiento.

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

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

Consulte la tabla de routing en el R2.

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

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

Verifique la conectividad.

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

¿Tuvieron éxito los pings? **Si**

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

¿Tuvieron éxito los pings? **SI**

Configurar IPv6 en los dispositivos

```
R1(config)#int g0/1
R1(config-if)#ipv6 add 2001:db8:acad:a::1/64
R1(config-if)#ipv6 add fe80::1 link-l
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#int s0/0/0
R1(config-if)#ipv6 add 2001:db8:acad:12::1/64
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#
```

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.

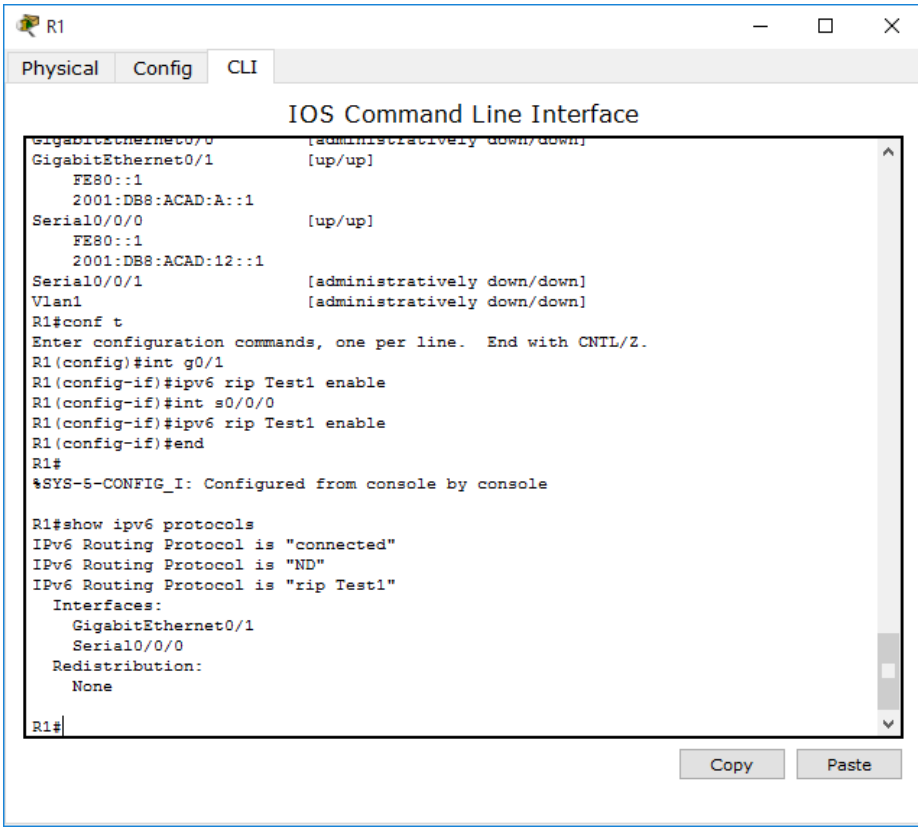
Se ingresa el comando show ipv6 interface brief

```
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]
R1#
```

Configurar y verificar el routing RIPng

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

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



¿En qué forma se indica RIPng en el resultado?

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

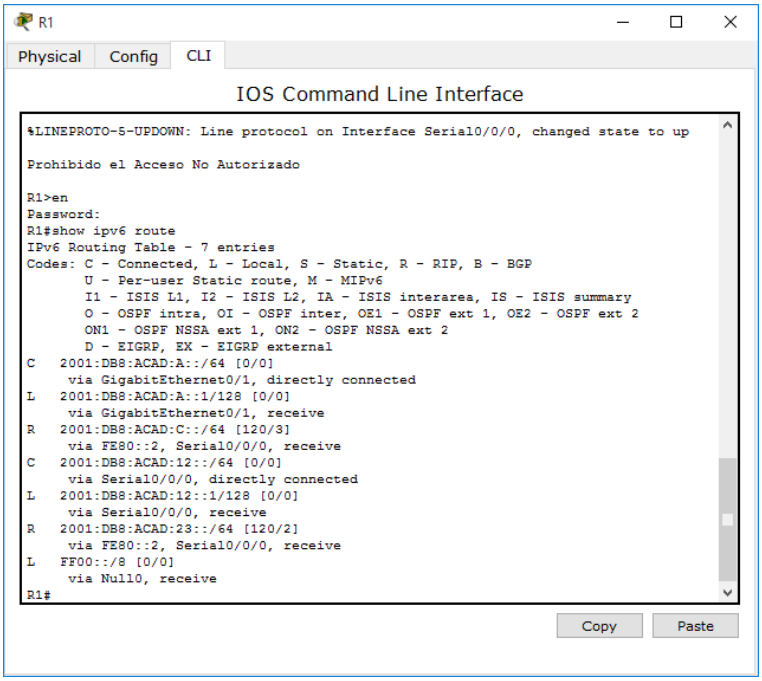
Packet Tracer no soporta el comando Show Ipv6 rip Test1,

¿Cuáles son las similitudes entre RIPv2 y RIPng?

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

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.

El comando es show ipv6 route.



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

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

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

Verifique la conectividad entre las computadoras.

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

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

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

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

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

Configurar y volver a distribuir una ruta predeterminada.

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

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

Configuración de los enlaces seriales en R2

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

Copy Paste

Verificación de la tabla de ruteo por show ipv6 route

R2

Physical Config CLI

IOS Command Line Interface

```
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
R2#
```

Copy Paste

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

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

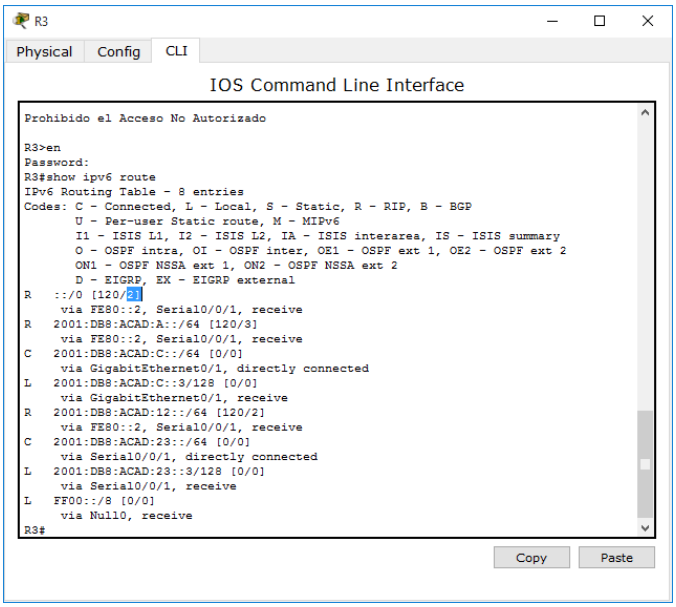
S ::/0 [1/0]

via 2001:DB8:ACAD:B::B, receive

Consulte las tablas de routing del R1 y el R3.

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

La tabla de ruteo se muestra distribuida con una métrica de 2, por medio de RIPng



Verifique la conectividad.

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

¿Tuvieron éxito los pings? **Si**

Reflexión

¿Por qué desactivaría la sumarización automática para RIPv2?

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

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

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

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

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

Conclusiones De Practica: 7.3.2.4 configuración básica de RIPv2 y RIPng

Por medio del comando passive-interface [Interface] se puede evitar que las actualizaciones de RIP se envíen por dicha interface y asi evitar el tráfico innecesario dentro de la red.

Los comandos debug ip rip, show ip protocolos y show run, nos permiten revisar dentro del dispositivo de red, la versión del RIP que se encuentra configurado.

Para RIPv2 es importante desactivar la sumarización de direcciones en los router de tal manera que estos dispositivos no resuman las rutas, esto se logra por medio de los comandos router rip, seguido de no auto-summary desde el modo de configuración de la terminal.

El comando show ipv6 rip [Nombre del proceso de nivel local] no es soportado por Packet Tracer.

8.2.4.5 Práctica de laboratorio: configuración de OSPFv2 básico de área única

Topología

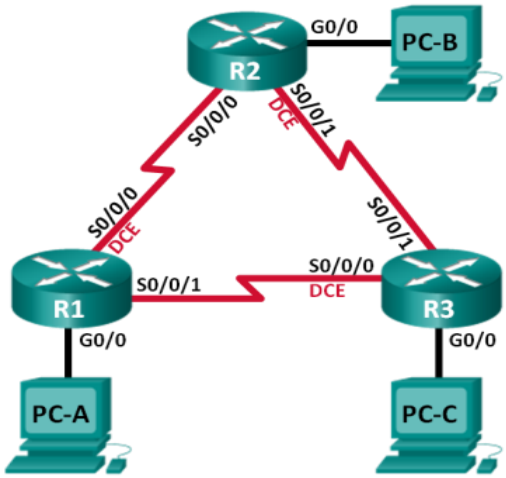


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPF

Parte 3: cambiar las asignaciones de ID del Router

Parte 4: configurar interfaces OSPF pasivas

Parte 5: cambiar las métricas de OSPF

Información básica/situación

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

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

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 según sea necesario.

Paso 3: configurar los parámetros básicos para cada Router.

```
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#banner motd % Unauthorized access is strictly prohib
R1(config)#int g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

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

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 shut
```

```
R1(config)#int s0/0/1
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config-if)#no shut

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

R1#
R1#copy runn
R1#copy running-config st
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Paso 4: configurar los equipos host.

Paso 5: Probar la conectividad.

```
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 = 1/4/16 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 = 1/5/22 ms
```

Parte 2: Configurar y verificar el enrutamiento OSPF

Paso 1: Configure el protocolo OSPF en R1.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.3 area 0
R1(config-router)#network 192.168.13.0 0.0.0.3 area 0
R1(config-router)#
```

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

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

```
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

O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:06:12, 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, 00:04:20, 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 192.168.12.1, 00:04:20, Serial0/0/0
                        [110/128] via 192.168.23.2, 00:04:20, Serial0/0/1
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.1/32 is directly connected, Serial0/0/1
R2#
```

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

Paso 4: verificar la configuración del protocolo OSPF.

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

```
R3#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 192.168.23.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.3.0 0.0.0.255 area 0
    192.168.13.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.13.1         110      00:09:19
    192.168.23.1         110      00:09:03
    192.168.23.2         110      00:09:03
  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

```
R3#show ip ospf
 Routing Process "ospf 1" with ID 192.168.23.2
 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 4 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.

El comando “show ip ospf interface brief” no se puede implementar en Packet Tracer. Se puede utilizar el comando “show ip ospf interface”

Paso 7: Verificar la conectividad de extremo a extremo.

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.

```
R1(config)#interface lo0

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

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

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

Guarde la configuración en ejecución en la configuración de inicio de todos los Routers.

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.

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.

```
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      00:01:03
  2.2.2.2              110      00:01:03
  3.3.3.3              110      00:01:03
  192.168.13.1         110      00:13:18
```

Se emita el comando show ip ospf neighbor para mostrar los cambios de ID de Router de los Routers vecinos.

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

```
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
```

```
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      00:14:03
  2.2.2.2              110      00:14:03
  3.3.3.3              110      00:00:33
  11.11.11.11          110      00:00:25
  22.22.22.22          110      00:00:25
  33.33.33.33          110      00:00:25
  192.168.13.1         110      00:26:18
```

e. Se emita el comando show ip ospf neighbor en el R1 para verificar que se muestren las nuevas ID de los Routers R2 y R3.

Parte 4: configurar las interfaces pasivas de OSPF

Paso 1: configurar una interfaz pasiva.

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

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

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

```
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
```

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

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

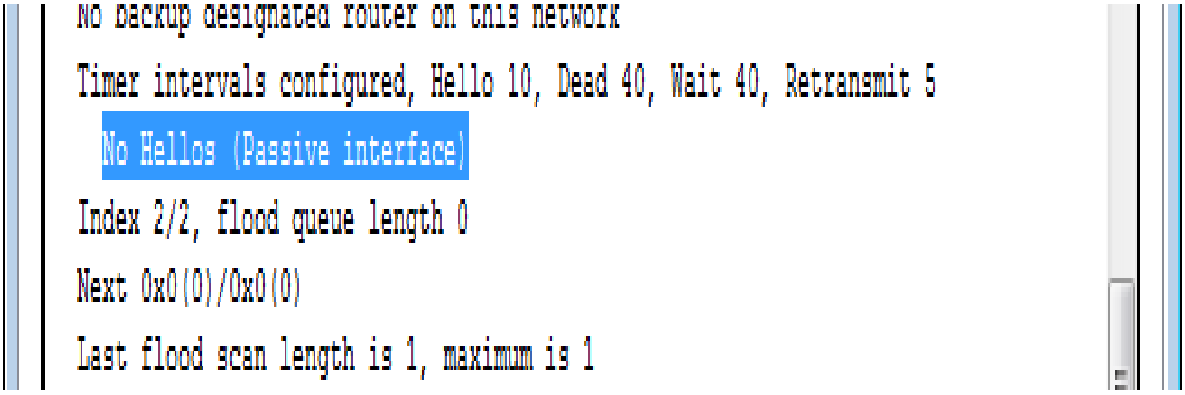
Emita el comando show ip ospf neighbor en el R1 para verificar que el R2 aparezca como un vecino OSPF.

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)#
00:33:04: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

00:33:04: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Interface down or detached
```

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.

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.



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.

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

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

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

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

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

¿Qué indica esta información?

La interfaz S0/0/1 en el Router R2 se configuro como interfaz pasiva, por esta razón la información de routing OSPF no se anuncia en esa interfaz. Métrica de costo acumulado para la red 192.168.2.0/24 en el R3 es 129 debido a que el tráfico debe pasar a través de dos enlaces seriales con un costo de 64 cada uno, el enlace LAN Gigabit 0/0 del R2 tiene un costo de uno, lo que da el costo de uno.

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

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

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

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

La métrica de costo acumulado para la red 192.168.2.0/24 en el R3 es 65, el enlace serial tiene un costo 64 y el enlace LAN tiene un costo de 1.

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

Parte 5: cambiar las métricas de OSPF

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

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

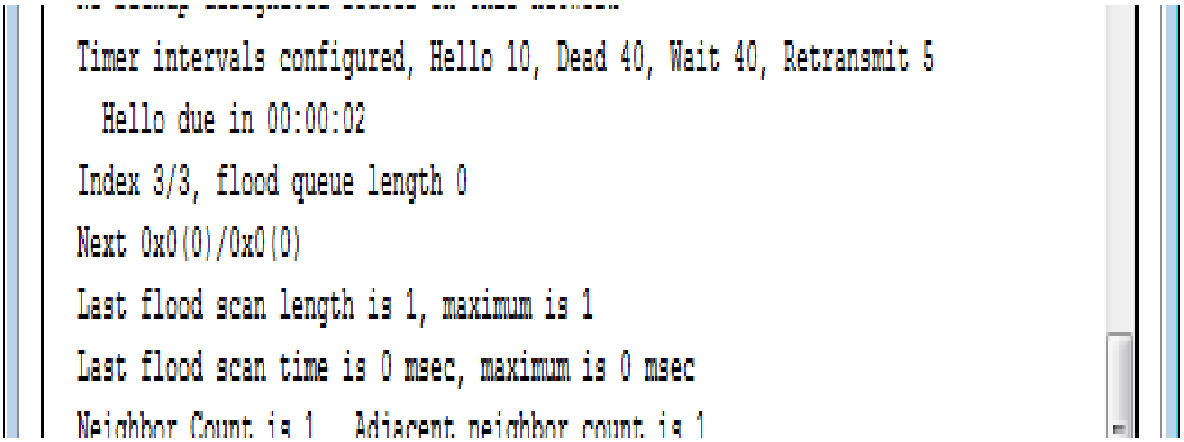
```
R1#show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 00e0.b02c.5d01 (bia 00e0.b02c.5d01)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  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
```

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

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

```
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
```

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

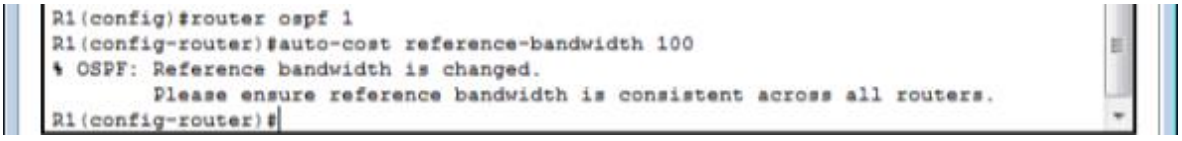


Emita el comando auto-cost reference-bandwidth 10000 en el R1 para cambiar la configuración de ancho de banda de referencia predeterminado. Con esta configuración, las interfaces de 10 Gb/s tendrán un costo de 1, las interfaces de 1 Gb/s tendrán un costo de 10, y las interfaces de 100 Mb/s tendrán un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

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

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).

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



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

En la actualidad los equipos admiten cada vez más velocidades de enlaces más rápidas que 100Mb/s que es el valor predeterminado, por lo que para obtener un cálculo más preciso del costo de estos enlaces más rápidos, se necesita una configuración del ancho de banda de referencia predeterminado más alta.

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

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

```
R1#show interface s0/0/0
Serial0/0/0 is up, line protocol is up (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
```

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.

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

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
O    192.168.2.0 [110/881] via 192.168.12.2, 00:01:30, Serial0/0/0
O    192.168.3.0 [110/164] via 192.168.13.2, 00:13:16, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/6540] via 192.168.13.2, 00:01:30, Serial0/0/1
R1#
```

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

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

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
O    192.168.2.0 [110/881] via 192.168.12.2, 00:06:38, Serial0/0/0
O    192.168.3.0 [110/881] via 192.168.13.2, 00:01:20, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/7257] via 192.168.12.2, 00:01:20, Serial0/0/0
                     [110/7257] via 192.168.13.2, 00:01:20, 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.

Costos a la red 192.168.3.0/24: el enlace serial S0/0/1 de R1 tiene un costo de 781 más el costo de la interfaz gigabit de R3 que es de 1 lo que da un costo acumulado de 782.

Costo a la red 192.168.23.0/30: el enlace serial S0/0/1 de R1 tiene un costo de 781 y el enlace serial S0/0/1 de R 3 tiene un costo 64, lo que da un total de 845

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.

Se emita el comando bandwidth 128 en todas las interfaces seriales restantes de la topología.

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

El nuevo costo es de 7257

Paso 3: cambiar el costo de la ruta.

Emita el comando show ip route ospf en el R1.

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.

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.

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

El protocolo OSPF elige la ruta con menor costo, en este caso 1665 ya que el costo del enlace serial S0/0/0 de R1 y el enlace serial S0/0/1 de R2 tienen un costo de 881 cada uno y el enlace gigabit G0/0 de R3 tiene un costo de 1.

Reflexión

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

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.

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

Los enlaces seriales utilizados son enlaces punto a punto, así que no se realiza una elección de DR/BDR, ya que el proceso de elección de DR/BDR es solo un problema en una red de accesos múltiples, como Ethernet

¿Por qué querría configurar una interfaz OSPF como pasiva?

Se configuran interfaz como pasivas para no saturar la red con información innecesaria y liberar ancho de banda, los enlaces seriales si deben estar activas para que publiquen la red a sus vecinos.

Conclusiones De Practica: 8.2.4.5 configuración de OSPFv2 básico de área única

El protocolo OSPF elige la ruta con menor costo acumulado. Predeterminadamente OSPF calcula el costo de un enlace con la configuración del ancho de banda, se puede configurar el costo de un enlace con el comando “ip ospf cost” y el costo que se le quiera dar al enlace, solo se pude configurar un enlace a la vez.

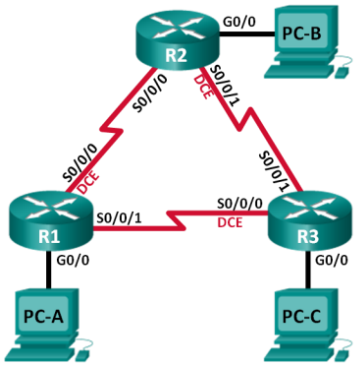
Se configuran interfaz como pasivas para no saturar la red con información innecesaria y liberar ancho de banda, los enlaces seriales si deben estar activas para que publiquen la red a sus vecinos.

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.

Se configuro y verifico mediante el comando ping el correcto funcionamiento del protocolo de comunicación OSPF.

8.3.3.6 Práctica de laboratorio: configuración de OSPFv3 básico de área única

Topología



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

Tabla de direccionamiento

Objetivos

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

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

Información básica/situación

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

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

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

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

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

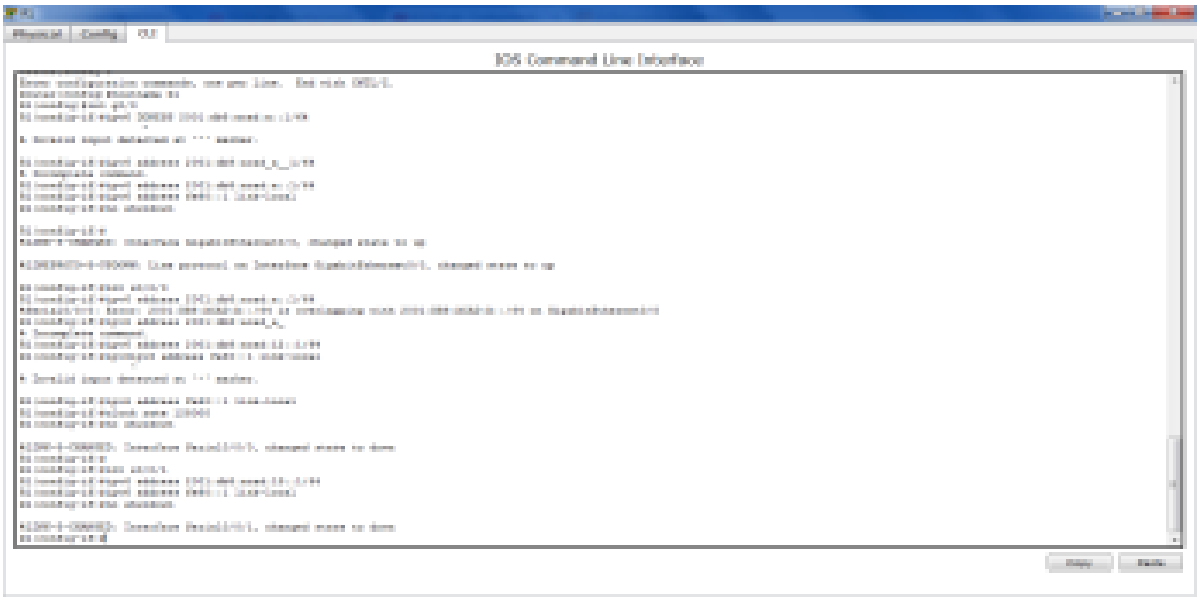
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

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

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

Step 3: configurar los parámetros básicos para cada router.

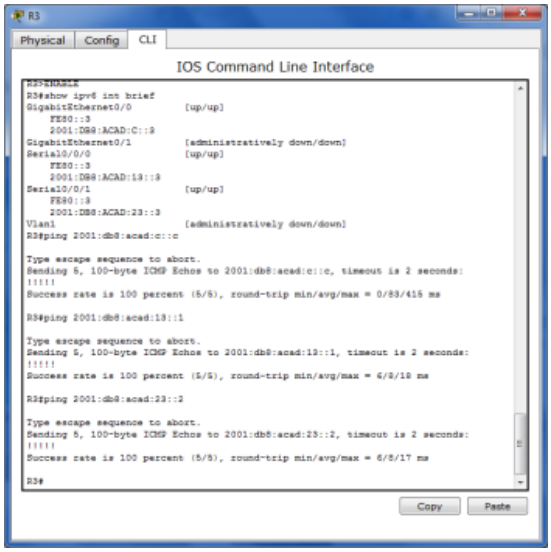
a. Desactive la búsqueda del DNS.
b. Configure el nombre del dispositivo como se muestra en la topología.
c. Asigne **class** como la contraseña del modo EXEC privilegiado.
d. Asigne **cisco** como la contraseña de vty.
e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso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

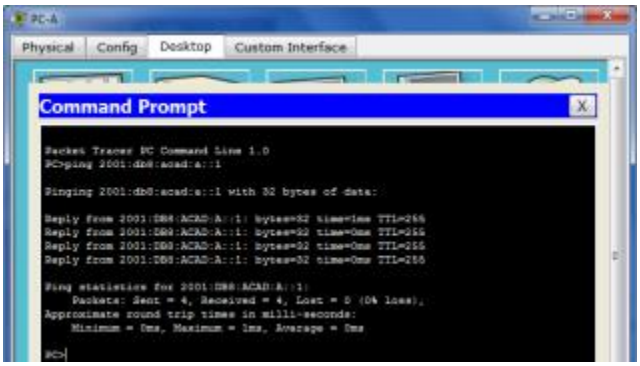


Step 4: configurar los equipos host.(tanto PCA como PC-B y PC-C)

Step 5: Probar la conectividad.

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





Part 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.

Step 1: asignar ID a los routers.

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

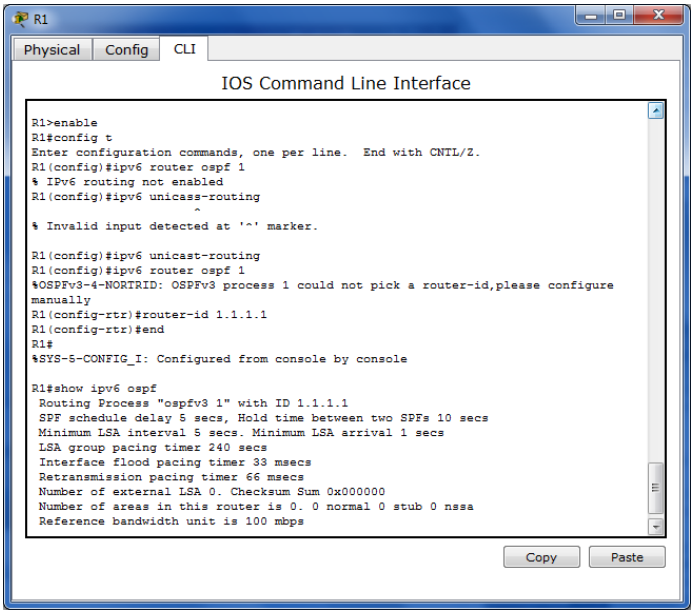
a. Emita el comando **ipv6 router ospf** para iniciar un proceso OSPFv3 en el router.

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

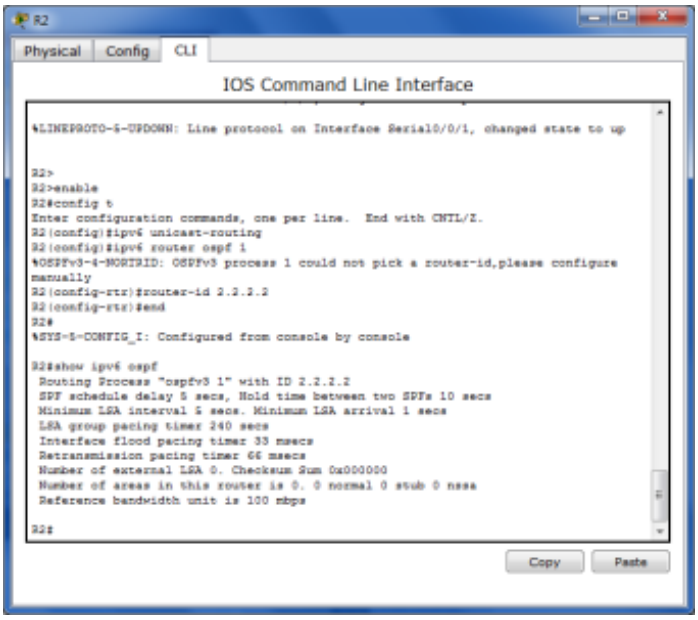
Nota: la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

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

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



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



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

R2# **show ipv6 ospf**

Routing Process "ospfv3 1" with ID 2.2.2.2

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

Router is not originating router-LSAs with maximum metric

<Output Omitted>

Step 2: configurar OSPFv6 en el R1.

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

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

R1(config)# **interface g0/0**

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

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

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

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

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

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

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

```
R1#
*Mar 19 22:14:43.251: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on
Serial0/0/0 from LOADING to FULL, Loading Done
R1#
*Mar 19 22:14:46.763: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on
Serial0/0/1 from LOADING to FULL, Loading Done
```

Step 3: verificar vecinos de OSPFv3.

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

```
R1# show ipv6 ospf neighbor

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

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

Verificar la configuración del protocolo OSPFv3.

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

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/1
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
```

Step 4: verificar las interfaces OSPFv3.

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

```
R1# show ipv6 ospf interface
Serial0/0/1 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 7
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/3/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 6
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1
```

No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

b.

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

R1# **show ipv6 ospf interface brief**

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

Step 5: verificar la tabla de routing IPv6.

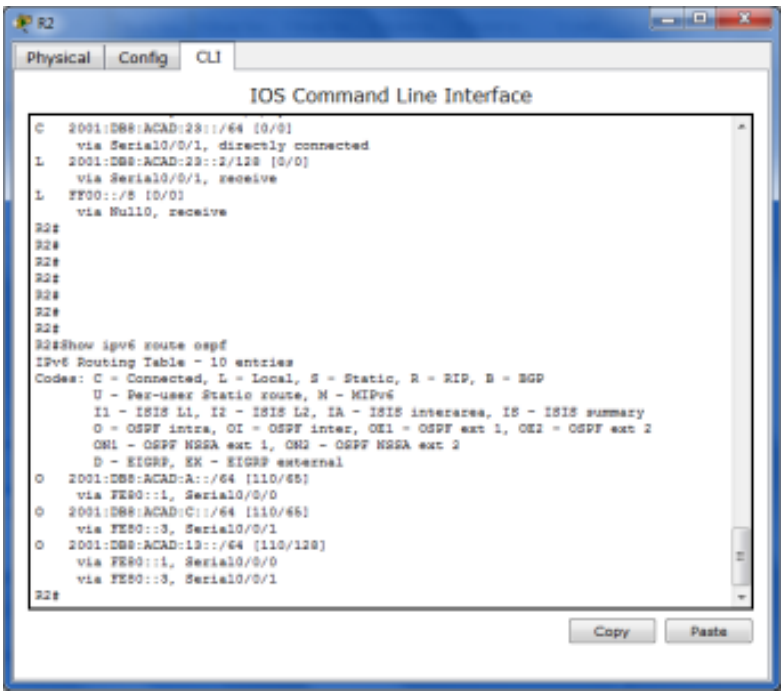
Emita el comando **show ipv6 route** para verificar que todas las redes aparezcan en la tabla de routing.

R2# **show ipv6 route**
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O 2001:DB8:ACAD:A::/64 [110/65]
via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:B::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:B::2/128 [0/0]
via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:C::/64 [110/65]
via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]

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

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

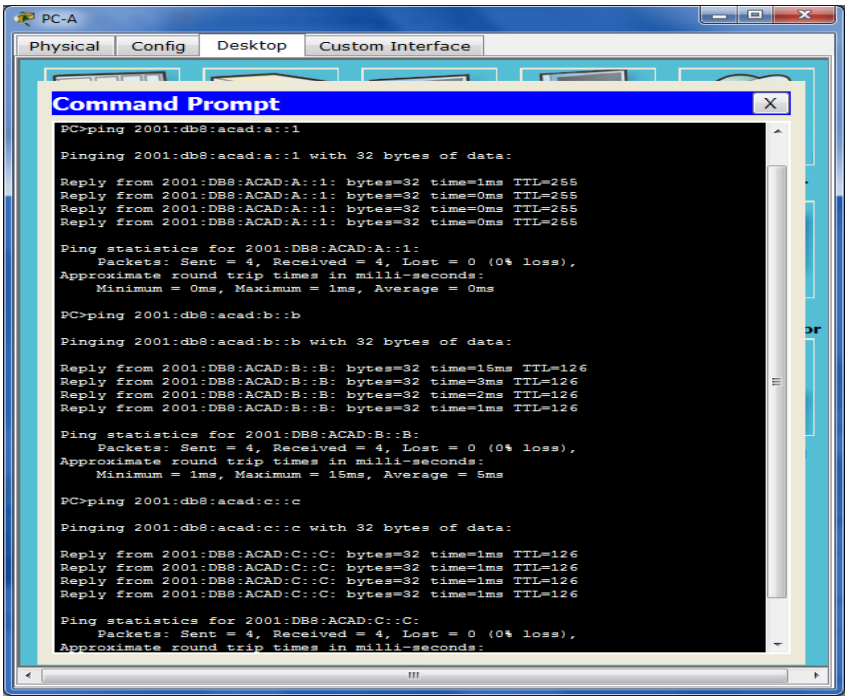
Show ipv6 route ospf



Step 6: Verificar la conectividad de extremo a extremo.

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

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



Part 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.

Step 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**

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3

Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 1.1.1.1, local address FE80::1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

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

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

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**
GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Wait time before Designated router selection 00:00:34
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

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

R2# **show ipv6 route ospf**
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

```
        IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
        ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:DB8:ACAD:A::/64 [110/65]
     via FE80::1, Serial0/0/0
O   2001:DB8:ACAD:C::/64 [110/65]
     via FE80::3, Serial0/0/1
O   2001:DB8:ACAD:13::/64 [110/128]
     via FE80::3, Serial0/0/1
     via FE80::1, Serial0/0/0
```

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

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

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

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

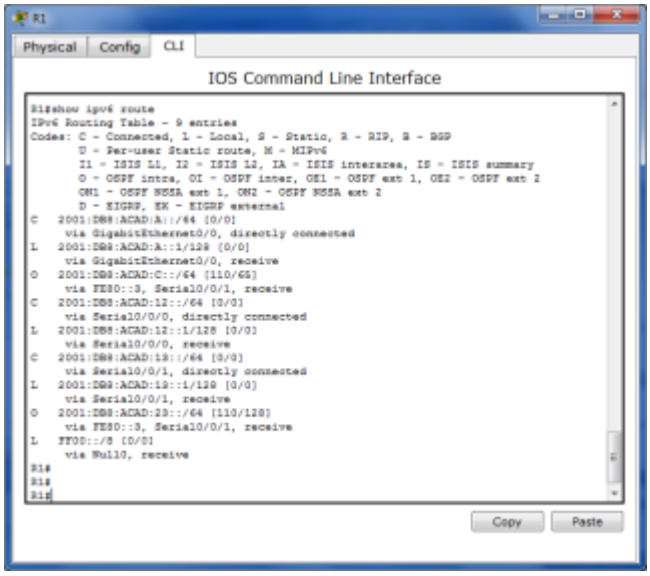
```
R1# show ipv6 ospf neighbor

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

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

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

```
R2# show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 6
  Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
```

Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 3
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

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



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

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

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

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

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

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64? ***S0/0/1***

¿Cuál es la métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1? ***129***

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

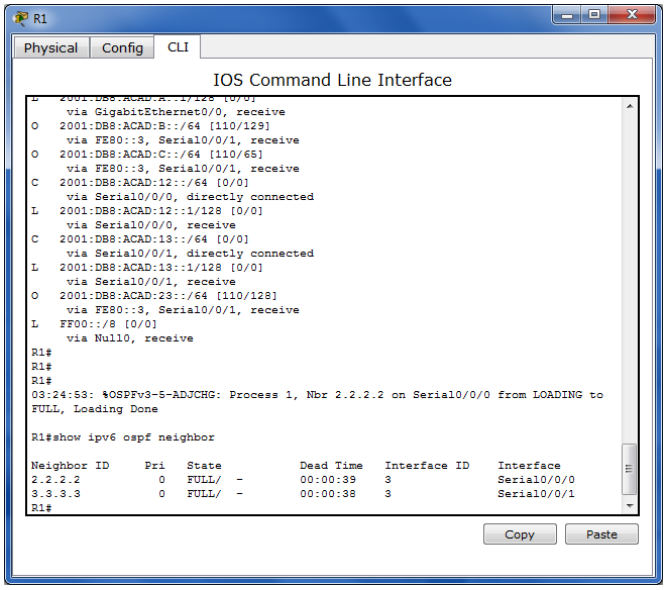
¿El R2 aparece como vecino OSPFv3 en el R3? ***SI***

¿Qué indica esta información?

Como se ha desactivado la interfase como pasiva solo esta el camino R1-R3-R2

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

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



Reflexión

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

   Si porque los procesos de ospf pueden variar ya que son locales y no afectan a los demás router, lo que debe coincidir para todas en es área.

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

   Eliminando este comando network ayuda a prevenir errores en las direcciones ipv6 ya que esta puede tener múltiples direcciones asignadas.

Conclusiones De Práctica: 8.3.3.6 configuración de OSPFv3 básico de área única

ospfv3 es un protocolo de enrutamiento para ipv6como protocolo de estado de enlace que se utiliza para identificar los vecinos de la red y se identifica la adyacencia, utilizada para asignar ID a los router, y configurar interfaces pasivas, por ejemplo Maneja información como la métrica o costo de la interface.

Teniendo en cuenta que enOSPFv3 solo se trabajan direcciones ipv6 para asignar la ID del router se debe realizar de forma manual utilizando el comando el comando **router-id**.

Se utiliza el comando **passive-interface** configurando una interfaz como pasiva con el objetivo de reducir el tráfico en las redes LAN, evitando que se envíen actualizaciones como lo hace la interfaz dinámica.

9.2.1.10 Packet Tracer - Configuración de las ACL estándar

Topología

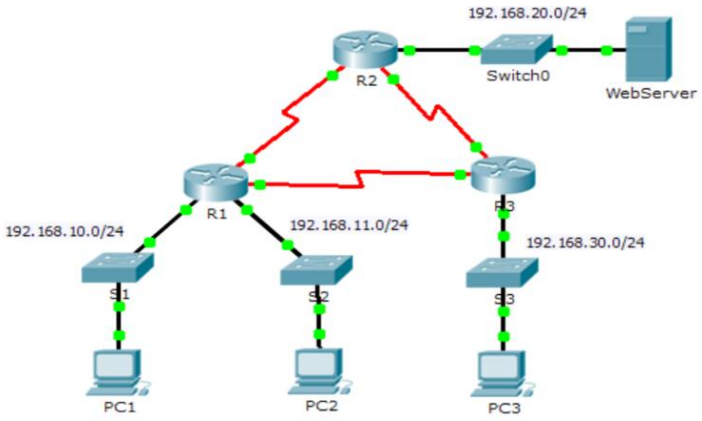


Tabla de direccionamiento

DISPOSITIVO	INTERFACE	DIRECCIÓN IP	MASCARA DE SUBRED	PUERTA DE ENLACE
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos

Parte 1: Planear una implementación de ACL
Parte 2: Configurar, Aplicar, y verificar una ACL estándar

Antecedentes / Escenario

Listas de control de acceso estándar (ACL) son scripts de configuración del router que controlan si un router permisos o niega paquetes basados en la dirección de origen. Esta actividad se centra en la definición de criterios de filtrado, configurar ACL estándar, aplicando las ACL a interfaces de routers y verificar y probar la implementación de ACL. Los

routers ya están configurados, incluyendo direcciones IP y Enhanced Interior Gateway Protocol Routing (EIGRP) de enrutamiento.

Parte 1: Planear una implementación de ACL

Paso 1: Investigar la configuración de red actual.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tiene conectividad completa. Compruebe que la red tiene conectividad total por la elección de un PC y ping a otros dispositivos en la red. Usted debe ser capaz hacer ping con éxito todos los dispositivos.

```
Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=15ms TTL=126
Reply from 192.168.30.10: bytes=32 time=14ms TTL=126
Reply from 192.168.30.10: bytes=32 time=15ms TTL=126
Reply from 192.168.30.10: bytes=32 time=14ms 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 = 14ms, Maximum = 15ms, Average = 14ms
```

Paso 2: Evaluar dos políticas de red e implementaciones ACL plan.

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

- La red 192.168.11.0/24 no se permite el acceso **al** servidor web en el 192.168.20.0/24 la red.
- Se permite Todo otro acceso.

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

Las siguientes políticas de red se implementan en R3:

- La red 192.168.10.0/24 no se le permite comunicarse con la red 192.168.30.0/24.
- Se permite Todo otro acceso.

Para restringir el acceso desde la red 192.168.10.0/24 a la red 192.168.30 / 24 sin interferir con el resto del tráfico, tendrá que ser creado en R3 una lista de acceso. El mosto ACL colocado en la interfaz de salida a PC3. Una segunda regla debe crearse en R3 para permitir que el resto del tráfico.

Parte 2: Configurar, Aplicar, y verificar una ACL estándar
Paso 1: Configurar y aplicar una ACL estándar numerada en R2.

a. Crear una ACL utilizando el número 1 en R2 con una declaración que niega el acceso a la 192.168.20.0/24 la red de la red 192.168.11.0/24.

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

Por defecto, una lista de acceso niega todo el tráfico que no coincide con una regla. Para permitir que el resto del tráfico, configure la siguiente declaración:

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

Para el ACL para filtrar realidad tráfico, debe ser aplicado a alguna operación router. Aplicar la ACL mediante la colocación que el tráfico de salida en la interfaz Gigabit Ethernet 0/0.

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

Paso 2: Configurar y aplicar una ACL estándar numerada en R3.

a. Crear una ACL utilizando el número 1 **en** R3 con una declaración que niega el acceso a la 192.168.30.0/24 red de la (192.168.10.0/24) red PC1.

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

Por defecto, una ACL deniega todo el tráfico que no coincide con una regla. Para permitir que el resto del tráfico, crear un segundo gobernar por ACL 1.

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

Aplicar la ACL por lo pone para el tráfico saliente en la interfaz Gigabit Ethernet 0/0.

R3 (config) # **interface GigabitEthernet0 / 0**

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

Paso 3: Verifique la configuración y funcionalidad ACL.

a. En R2 y R3, introduzca el comando access-list espectáculo para verificar las configuraciones de ACL. Introduzca el show ejecutar o mostrar ip interface gigabitethernet 0/0 comando para verificar las ubicaciones de ACL.

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

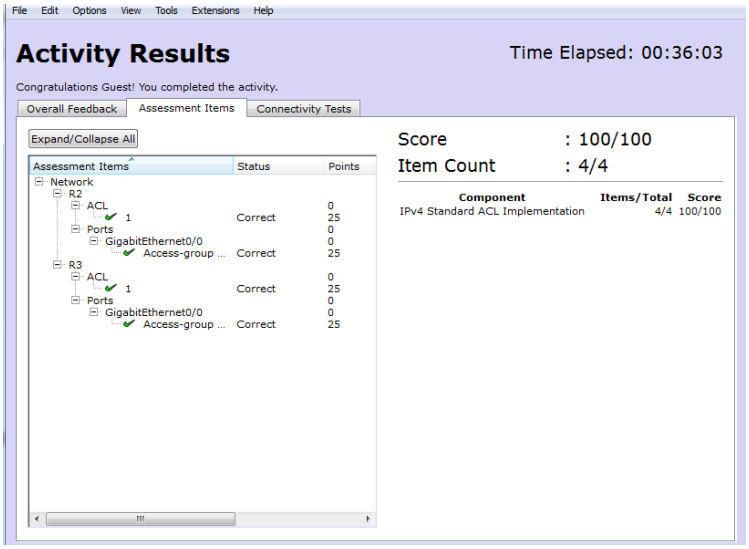
```
R2#show ip interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.20.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is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

Nota: De igual manera como se hace con el R2 se realiza con el R3.

Con los dos ACL en su lugar, el tráfico de red está restringido de acuerdo a las políticas que se detallan en la Parte 1. Uso las siguientes pruebas para verificar las implementaciones de ACL:

- Un ping desde 192.168.10.10 a 192.168.11.10 con éxito.
- Un ping desde 192.168.10.10 a 192.168.20.254 tiene éxito.
- Un ping desde 192.168.11.10 a 192.168.20.254 falla.
- Un ping desde 192.168.10.10 a 192.168.30.10 con falla.
- Un ping desde 192.168.11.10 a 192.168.30.10 con éxito.
- Un ping desde 192.168.30.10 a 192.168.20.254 tiene éxito

VERIFICACIÓN



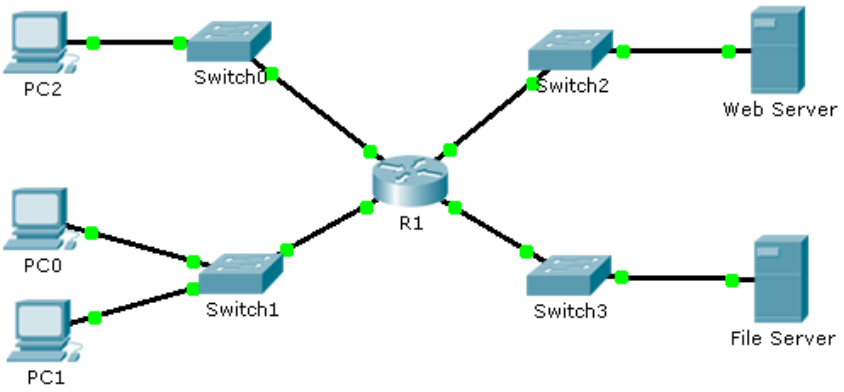
Conclusiones De Practica: 9.2.1.10 Configuring Standard ACLs*

Mediante la implementación de las listas de control de acceso se puede filtrar el tráfico de red previniendo ataques de usuarios no autorizados, además es posible usarse para definir el tráfico a la traducción de direcciones NAT o para filtrar protocolos distintos a TCP/IP. En el caso de IP para establecer que debe permitirse y denegarse debe establecerse la IP junto con la máscara de subred la cual posee la siguiente estructura 0.0.0.255 llamada mascara inversa de esta manera el valor de la máscara se subdivide y el resultado determina que bit de dirección se tiene en cuenta en el procesamiento del tráfico.

El proceso interno es muy sencillo cuando el trafico entra en el router este compara las entradas de ACL de acuerdo al orden de entrada en el router este observa hasta que encuentra una coincidencia, si llega al final de la lista sin encontrar coincidencia el tráfico se rechaza.

9.2.1.11 Packet Tracer - Configuring Named Standard ACLs

Topología



Addressing Table

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

Objectives

Part 1: Configure and Apply a Named Standard ACL

Part 2: Verify the ACL Implementation

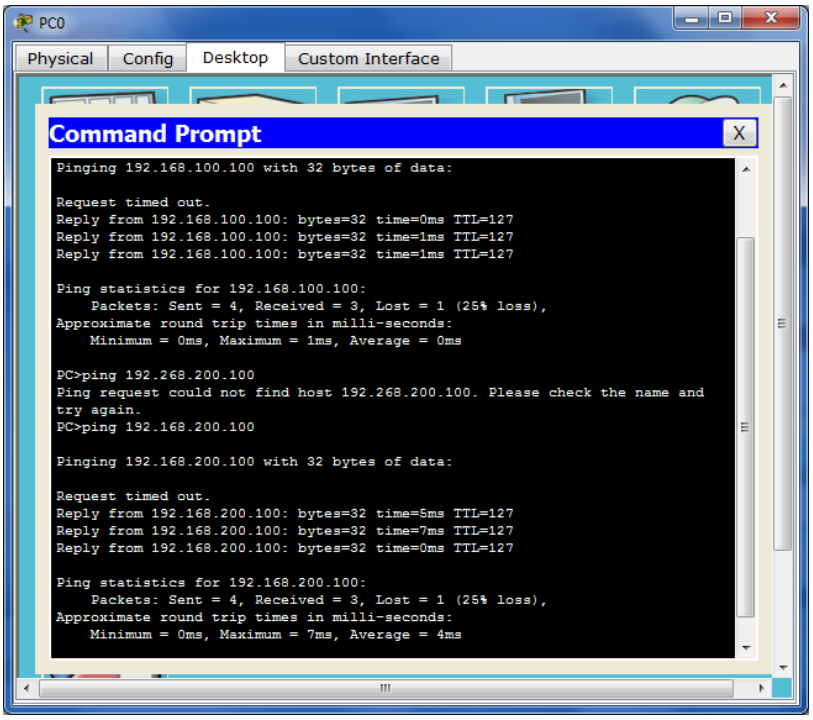
Background / Scenario

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

Part 1: Configure and Apply a Named Standard ACL

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

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



Step 2: Configure a named standard ACL.

Configure the following named ACL on **R1**.

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

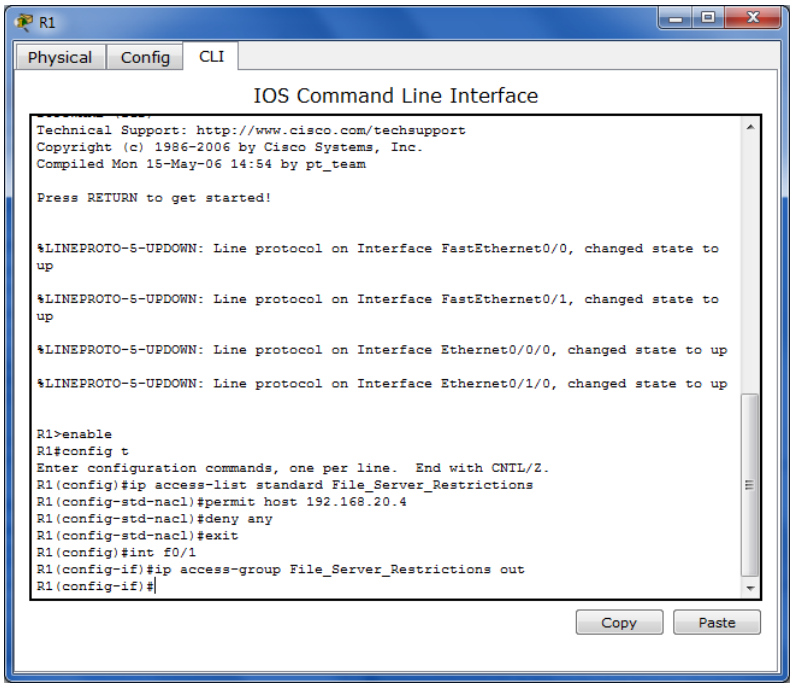
Note: For scoring purposes, the ACL name is case-sensitive.

Step 3: Apply the named ACL.

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

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

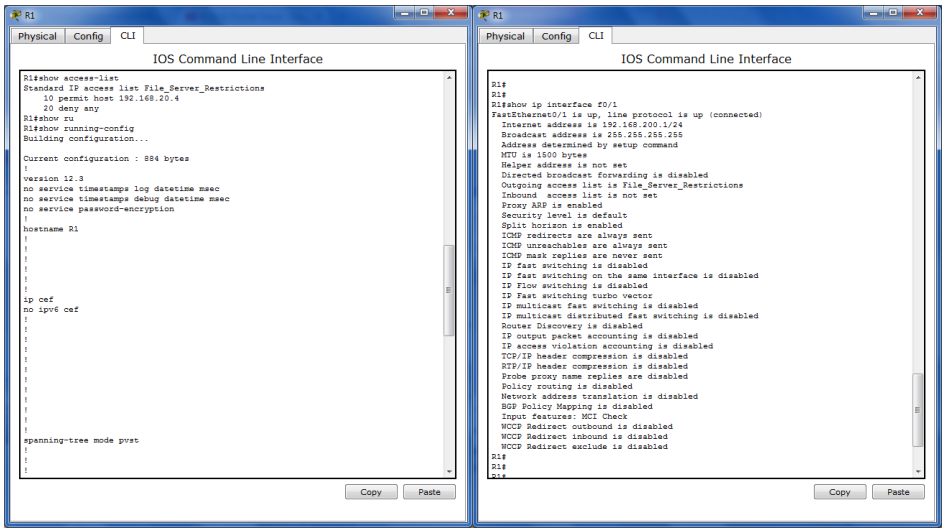
b. Save the configuration.



Part 2: Verify the ACL Implementation

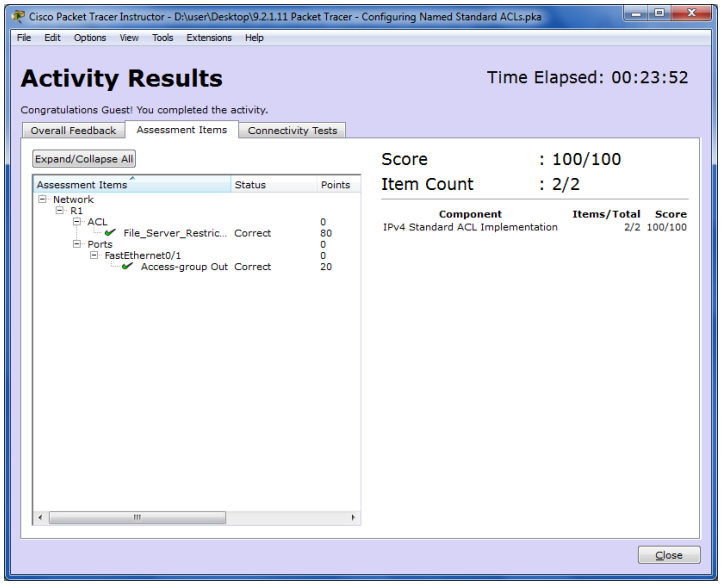
Step 1: Verify the ACL configuration and application to the interface.

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.



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**.



Conclusiones De Practica: 9.2.1.11 Configuring Named Standard ACLs *

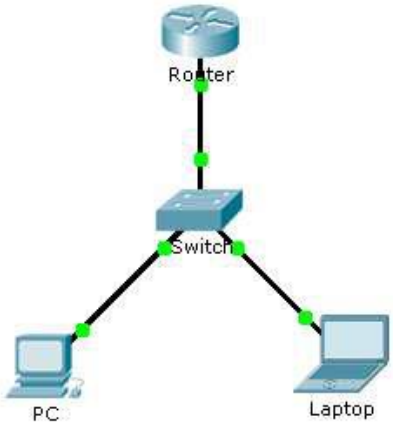
Las listas de control de acceso ACL, utiliza reglas para implementar seguridad y permisos para el acceso con privilegios. En este caso se utiliza para impedir o restringir el acceso a un servidor de archivos, negando así el acceso de cliente de una red de trabajo especifica en acceso a una red diferente a la que está conectada.

Para trabajar las ACL se utilizan los comandos **ip access-list standard File_Server_Restrictions** y **permit host dirección host**.

se puede reconocer que existen 2 tipos de listas de control de acceso la estandar en la que solo debemos trabajar con una dirección de origen y la extendida en la que se debe especificar el protocolo, la dirección de origen y también la dirección de destino. En nuestro ejercicio simplemente trabajamos con ACL estandar.

9.2.3.3 PACKET TRACER - CONFIGURING AN ACL ON VTY LINES

TOPOLOGIA



Addressing Table

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

Part 1: Configure and Apply an ACL to VTY Lines

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

Step 2: Configure a numbered standard ACL.

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

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)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#
```

Part 2: Verify the ACL Implementation

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

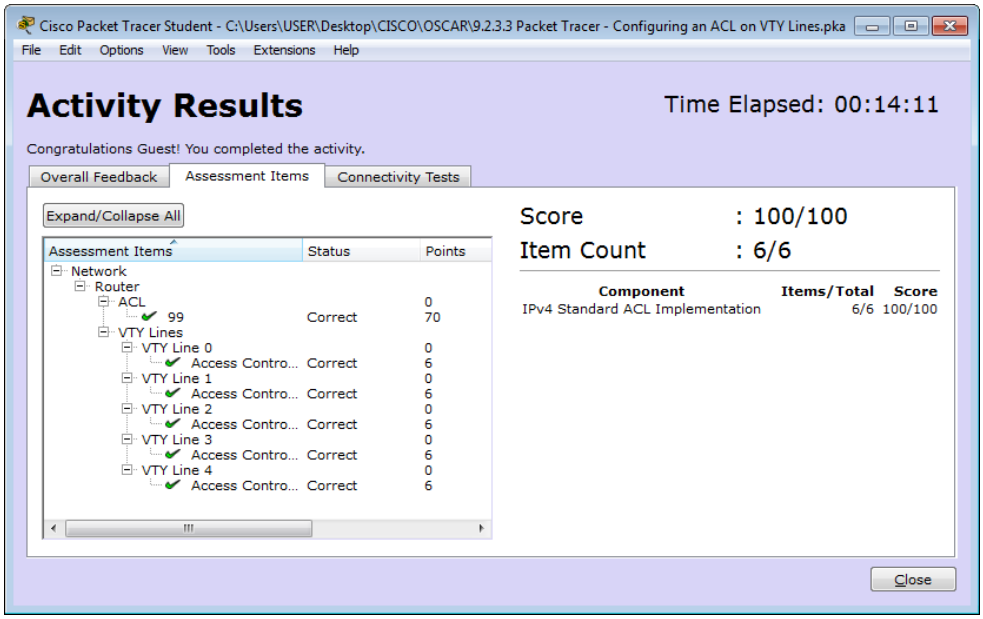
Use the show access-lists to verify the ACL configuration. Use the show run command to verify the ACL is applied to the VTY lines.

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

```
!
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.



Conclusiones De Practica: 9.2.3.3 Configurar una ACL en VTY Lines (Instructor Version) *

(ACL) para permitir el acceso de direcciones IP específicas, lo que asegura que solo la computadora del administrador tenga permiso para acceder al router mediante telnet o SSH.

Las ACL ayudan a restringir el acceso de administración remota a los dispositivos de red, sin embargo no cifran los datos que se envían por la red. Si otro programa en un host diferente en la red captura o detecta esa información, la red no es segura.

Las ACL de vty no dependen de interfaces.

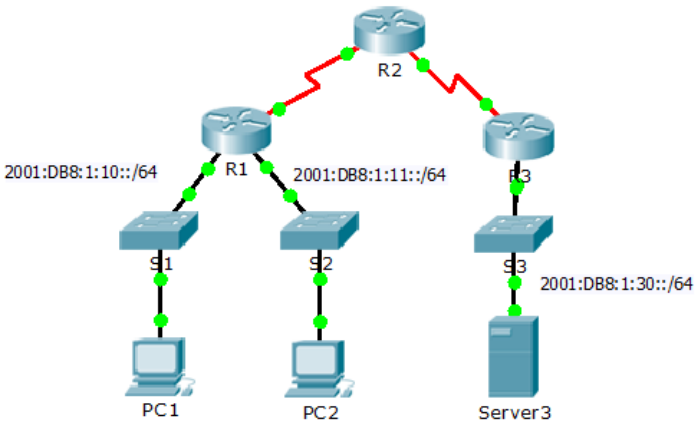
Las ACL Limitan el tráfico de la red para aumentar su rendimiento.

Cuando se crea y configura una ACL en un router, y se desea filtrar el acceso por líneas VTY, luego de la configuración por medio del comando access-list [Numero de ACL] permit host [Direccion IP] se debe asignar la ACL accediendo a la configuración de línea por medio del comando Line vty 0 15, para asignarla se usa el comando access-class [Numero de ACL] in, el comando in es importante pues configura el sentido de entrada al filtrado de la lista de acceso.

Para complementar un poco la conclusión del ejercicio que desarrolla se puede argumentar que las listas ACL o de control de acceso para telnet se trabajan o utilizan para generar seguridad para los privilegios que se le otorga a los usuarios de una red determinada, para el acceso a las VTY creando protección de los puertos permitiendo o denegando acceso.

9.5.2.6. Packet Tracer - Configuring IPv6 ACLs

Topology



Addressing Table

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

Objectives

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

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

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

Bloqueo por listas de acceso a HTTP y HTTPS para cortar el ataque a server 3

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

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

Para permitir el paso de otro tráfico se ingresa

R1(config-ipv6-acl)#permit ip any any

Se configura la interfaz g0/1 al ser la más cercana al origen, y se aplica la ACL para aplicar los bloqueos

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#ipv6 tr
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

Verify the ACL implementation

Acceso desde PC1 Exitoso

Accesso desde PC2 fallido

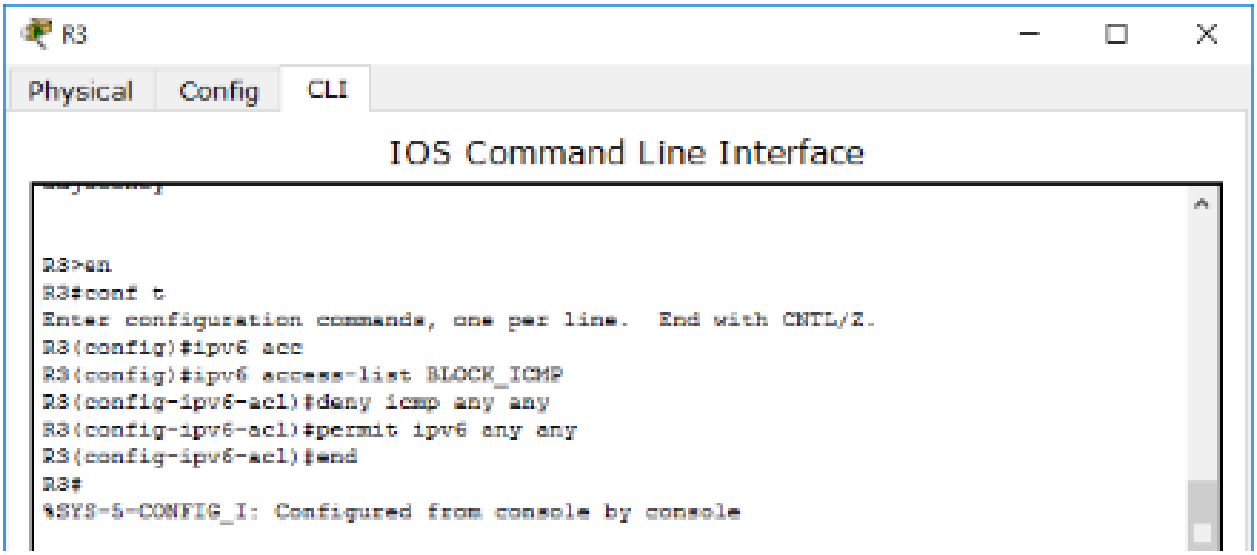
Se realiza el ping desde la PC2 hacia la dirección del servidor, para evidenciar que se bloquea solamente el tráfico web

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

Creación de una lista de acceso para cortar un ataque distribuido de denegación de servicios al servidor.

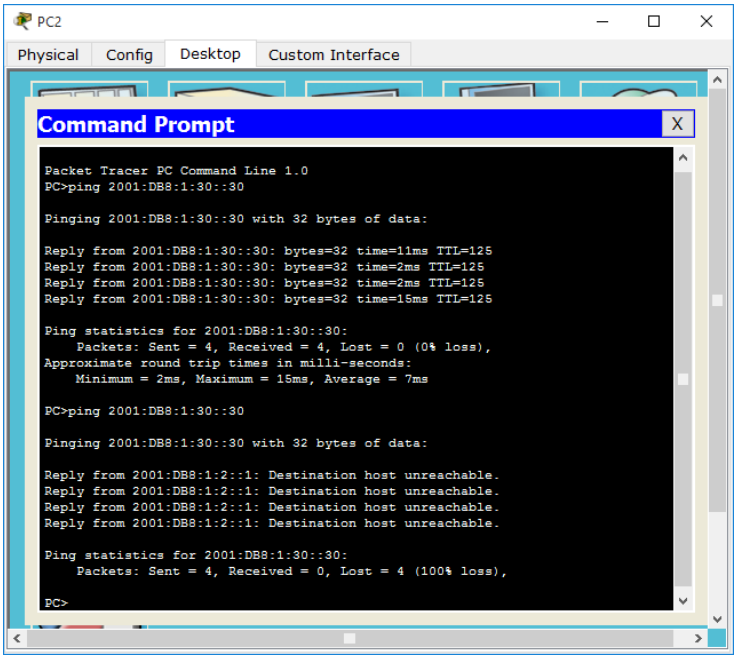
Se denegara el servicio de trafico icmp desde cualquier origen hacia cualquier destino, se autoriza ipv6 para cualquier origen o destino.

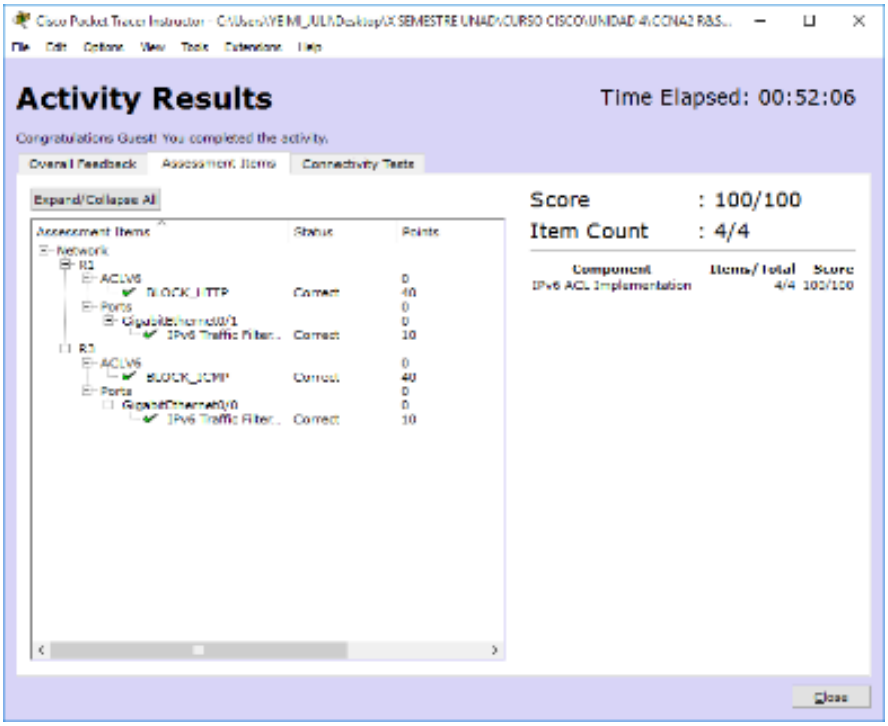
Se configura la interfaz g0/0 en R3 para la lista de acceso BLOCK_ICMP de salida



Verify that the proper access list functions

Se verifica que los ping desde y PC1 y PC2 son fallidos, pero el trafico web desde PC1 es exitoso.





Conclusiones De Practica: 9.5.2.6 Configuring IPv6 ACLs*

Por medio de las ACLs se logran detener y prevenir ataques masivos dentro de la red, permitiendo denegar o autorizar tráfico dentro de determinada red, brindándole cierto nivel de seguridad a la red

Para la implementación de las listas de acceso se deben crear en el router, puesto que este dispositivo no las trae por default, así las cosas se crean por medio de la sentencia en modo de configuración de terminal ipv6 access-list [nombre ACL], luego de la creación se debe identificar la interfaz donde se va a aplicar el filtrado de trafico de acuerdo a la ACL desde el modo de configuración de interfaz se ingresa el comando ipv6 traffic-filter [nombre ACL], para terminar este comando se coloca out si es lista de acceso de salida o in, si es de entrada.

10.1.2.4 Práctica de laboratorio: configuración de DHCPv4 básico en un router

Topología

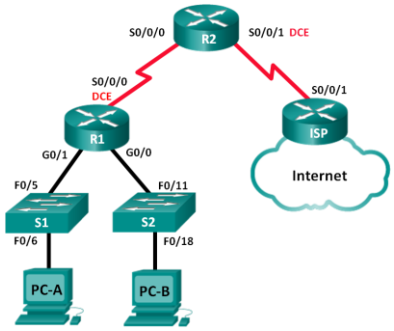


Tabla de direccionamiento

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

Objetivos

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

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

Información básica/situación

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

direcciones IP, los servidores DNS preferidos y los gateways predeterminados. A medida que aumenta el tamaño de la red, esto se convierte en un problema administrativo cuando los dispositivos se trasladan de una red interna a otra.

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

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

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

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

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

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

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

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

Step 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.

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

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

R1

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname  R1
R1(config)#int g0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut

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

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

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
R1(config-if)#exit
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)# no ip domain lookup
R1(config)#
```

De igual manera se realiza la configuración con el R2.

ISP

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int s0/0/1
ISP(config-if)#ip address 209.165.200.225 255.255.255.224
ISP(config-if)#no shut

ISP(config)#enable secret class
ISP(config)#line con 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#no ip domain lookup
```

h. Configure EIGRP for R1.

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 192.168.2.252 0.0.0.3
R1(config-router)#no auto-summary
```

i. Configure EIGRP y una ruta predeterminada al ISP en el R2.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router eigrp 1
R2(config-router)#network 192.168.2.252 0.0.0.3
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.253 (Serial0/0/0) is up: new
adjacency

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

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

```
ISP>en
Password:
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 192.168.0.0 255.255.252.0 209.165.200.226
ISP(config)#
```

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

Step 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.

Step 5: verificar que los equipos host estén configurados para DHCP.

Part 5: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

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

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

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

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

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

Nota: los comandos requeridos para la parte 2 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar DHCP en el R1 y el R2 sin consultar el apéndice.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
                  ^
% Invalid input detected at '^' marker.

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

R2(dhcp-config)#exit
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#domain-name ccna-lab.com
                  ^
% Invalid input detected at '^' marker.

R2(dhcp-config)#lease 2
```

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?

Las PC no han recibido la IP del servidor DHCP en el router R2 porque primero el router R1 tiene que ser configurado como agente DHCP

Step 2: configurar el R1 como agente de retransmisión DHCP.

Configure las direcciones IP de ayuda en el R1 para que reenvíen todas las solicitudes de DHCP al servidor de DHCP en el R2.

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

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

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

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

PC-A

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 00E0.A36C.7CA4
   Link-local IPv6 Address.....: FE80::2E0:A3FF:FE6C:7CA4
   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-A2-87-2D-20-00-E0-A3-6C-7C-A4
```

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?

PCA: 192.168.1.10

PCB: 192.168.0.10

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

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

```
R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.10     00E0.A36C.7CA4           --                     Automatic
192.168.0.10     000C.CFA4.791E           --                     Automatic
```

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

Se muestra la dirección MAC que identifica las computadoras

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

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

No es posible observar el resultado

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)?

No es posible observar el resultado el comando no está implementado en Packet Tracer

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

```
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
```

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.

G0/0

```
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 00d0.ff1b.bd01 (bia 00d0.ff1b.bd01)
  Internet address is 192.168.0.1/24
  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 104 bits/sec, 0 packets/sec
     2 packets input, 154 bytes, 0 no buffer
     Received 2 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
```

Reflexión

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

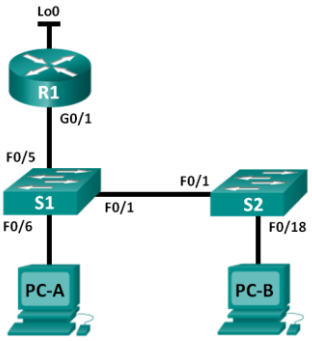
Es preferible que un router tenga todos los servicios DHCP como servidor y no que cada router tenga DHCP por que disminuye los recursos de hardware y además se hace más fácil la administración de forma centralizada.

Conclusiones De Practica: 10.1.2.4 configuración de DHCPv4 básico en un router

La función principal del agente DHCP es retransmitir los mensajes DHCP entre clientes y servidores en distintas redes IP, este recibe la difusión DHCP de la subred y la reenvía a la dirección IP especificada en una subred distinta, el agente se configura con una IP estática y conoce la IP del servidor DHCP este intercepta los mensajes enviados por los clientes enrutandolos hacia el servidor DHCP, es importante resaltar que el servidor como el agente DHCP debe tener una IP fija y una puerta de enlace predeterminada para atravesar el enrutador.

10.1.2.5 Práctica de laboratorio: configuración de DHCPv4 básico en un switch

Topología



NOTA: en el ejercicio se utiliza el switch 3560 porque soporta DHCP.

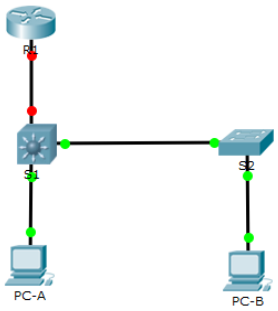


Tabla de direccionamiento

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

Objetivos

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

Parte 2: cambiar la preferencia de SDM

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

Parte 3: configurar DHCPv4

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

Parte 4: configurar DHCP para varias VLAN

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

Parte 5: habilitar el routing IP

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

Información básica/situación

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

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

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

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

Parte 6: armar la red y configurar los parámetros básicos de los dispositivos

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

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

Paso 3: configurar los parámetros básicos en los dispositivos.

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

Parte 7: cambiar la preferencia de SDM

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

Paso 1: mostrar la preferencia de SDM en el S1.

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

```
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
```

¿Cuál es la plantilla actual?

Aunque no se puede realizar este punto ya que packet tracer no acepta el comando pero la plantilla debe ser default en casi todos los casos.

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

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

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

¿Qué plantilla estará disponible después de la recarga? ***lanbase-routing***

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

S1# **reload**

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

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

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

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

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

number of unicast mac addresses: 4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes: 0.75K
number of directly-connected IPv4 hosts: 0.75K
number of indirect IPv4 routes: 16
number of IPv6 multicast groups: 0.375k
number of directly-connected IPv6 addresses: 0.75K
number of indirect IPv6 unicast routes: 16
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.125k
number of IPv4/MAC security aces: 0.375k
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 0.375k

number of IPv6 security aces: 127

Parte 8: configurar DHCPv4

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

Paso 1: configurar DHCP para la VLAN 1.

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.

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.

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.

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.

default-router 192.168.1.1

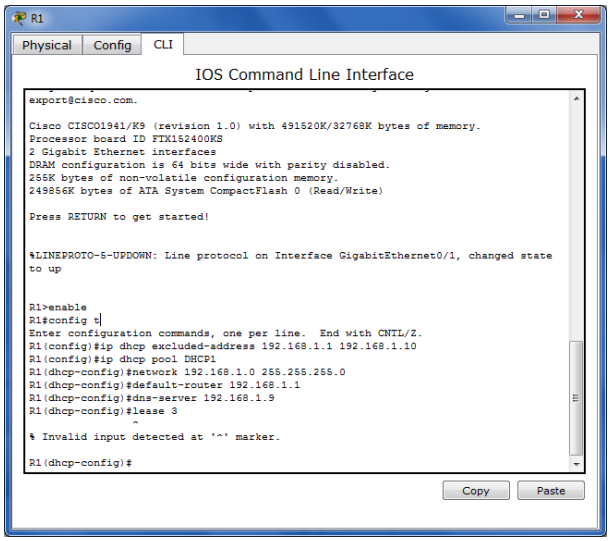
e. Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.

dns-server 192.168.1.9

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

lease 3 packet tracer no acepta este tipo de comando.

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



Paso 2: verificar la conectividad y DHCP.

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

Para la **PC-A**, incluya lo siguiente:

Dirección IP: **192.168.1.11**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **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? ***SI***

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

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

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

Parte 9: configurar DHCPv4 para varias VLAN

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

Paso 1: asignar un puerto a la VLAN 2.

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

S1(config)#int f0/6

S1(config-if)#switchport mode access

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.

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.

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.

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.

default-router 192.168.2.1

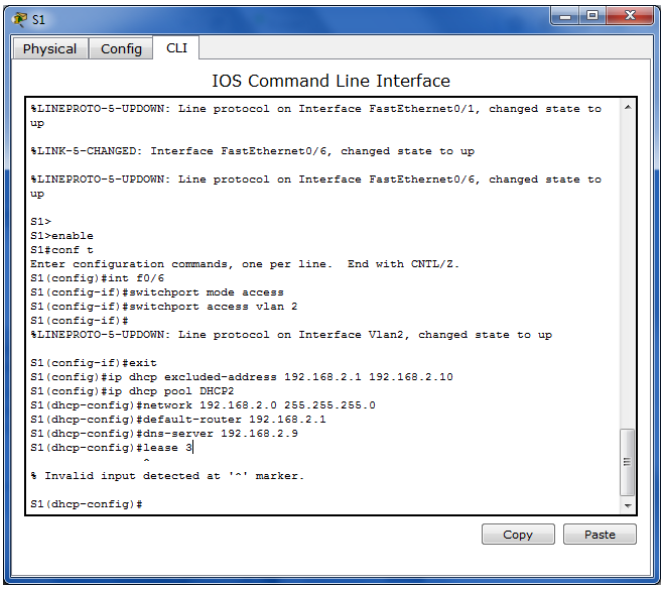
e. Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.

dns-server 192.168.2.9

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

lease 3 este comando no lo permite packet tracer

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



Paso 3: verificar la conectividad y DHCPv4.

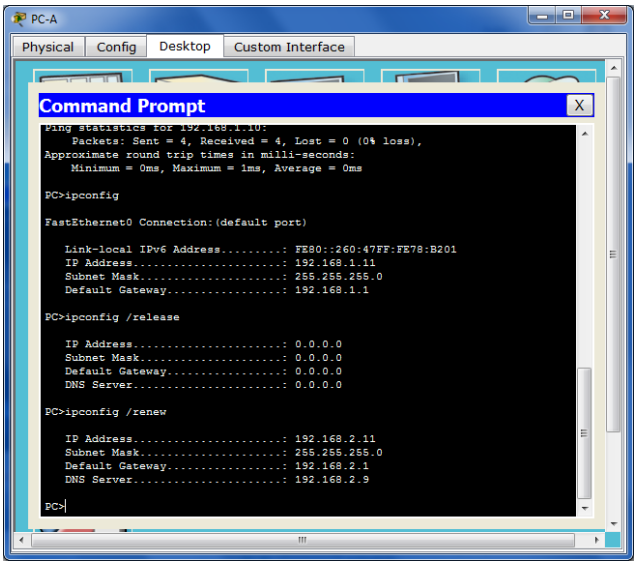
a. En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: 192.168.2.11

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.2.1



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

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

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

¿Los pings eran correctos? ¿Por qué?

Para la PC-A fue exitoso porque la puerta de enlace esta en la misma red, pero para elPC-B no fue exitoso porque esta en otra red diferente

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

¿Qué resultado arrojó este comando?

Host Gateway Last Use Total Uses Interface

ICMP redirect cache is empty

No hay una puerta de enlace establecida por lo tanto no hay tabla de rutas en el switch

Parte 10: habilitar el routing IP

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

Paso 1: habilitar el routing IP en el S1.

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

S1(config)# **ip routing**

b. Verificar la conectividad entre las VLAN.

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

¿Qué función realiza el switch? ***Está cumpliendo la función de ruteo entre paquetes de las VLAN.***

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

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

Muestra que Hay 2 redes directamente conectadas la vlan1 y la vlan 2

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?

Muestra que hay 2 redes directamente conectadas la 1 y la publica 209, no hay entrada para la red 2

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

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

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

Para que haya comunicación todas las rutas deben ser agregadas a la tabla de ruteo.

Paso 2: asignar rutas estáticas.

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

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

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.

ip route 192.168.2.0 255.255.255.0 g0/1

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

¿Cómo está representada la ruta estática predeterminada?

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

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

¿Cómo está representada la ruta estática?

S 192.168.2.0/24 is directly connected, GigabitEthernet0/1

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

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

Reflexión

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

   Porque estas direcciones podrían ser dadas dinámicamente para algunos hots.

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

   El switch asina las direcciones ip por mediod e la asignación de la VLAN ye l asignamiento del puerto de las vlan y allí se conecta al host.

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

   Puede llevar a caba funciones de servidor de DCHP, y puede establecer rutas estáticas y ruteo entre las VLAN.

Conclusiones De Practica: 10.1.2.5 configuración de DHCPv4 básico en un Switch

DHCP es un protocolo que configure dinámicamente los hots, el servidor DHCPv4 tiene la facultad de asignar y administrar direcciones IPv4 vinculadas a VLAN específicas. Esto se puede trabajar con el switch 2960 el cual funciona como dispositivo de capa 3 permitiendo

trabajar el routing y rutas estáticas de igual forma únicas y múltiples esta última para permitir una comunicación constante entre los hosts de la red a trabajar.

Para su configuración para las VLAN se utilizan una serie de configuraciones y comando de acuerdo a los requerimientos, por ejemplo se deben excluir las 10 primeras direcciones de host válidas de la red para evitar que estas dinámicamente sean dadas a otros hosts el comando es **ip dhcp excluded-address + las direcciones a excluir**, con el comando **ip dhcp pool** se da el nombre al pool de DHCP de direccionamiento, de igual forma se debe asignar la red, el Gateway predeterminado, el servidor DNS, y DHCPv4 maneja un tiempo de arrendamiento que se debe determinar en días lo que el cliente debe estar pendiente de estar actualizando periódicamente.

10.2.3.5. Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado

Topología

Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

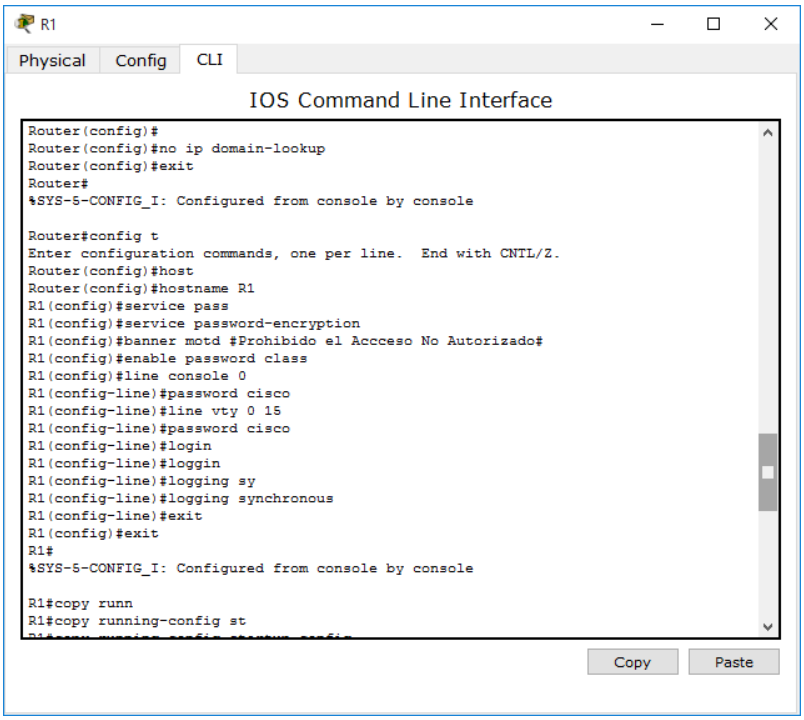
Parte 4: configurar la red para DHCPv6 con estado

PUESTO QUE EN PKT EL SWTCH 2960 NO SOPORTA TODAS LAS CARATERISTICAS IPV6, SE USARA UN SWITCH 3560 PARA EL PROCEDIMIENTO

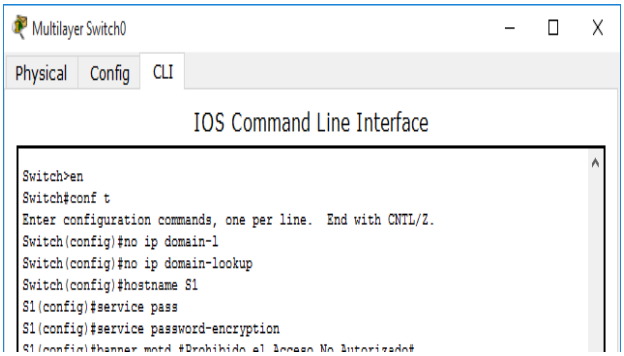
Para el inicio se debe aclarar que Packet Tracer no soporta los comandos

S1# **show sdm prefer**
S1# **config t**
S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**
S1(config)# **end**
S1# **reload**

Configuración Básica del Router

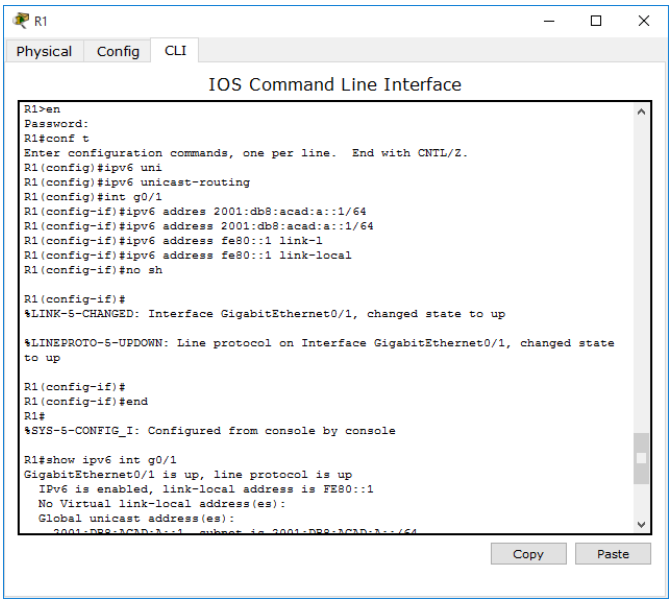


Configuración Básica de S1



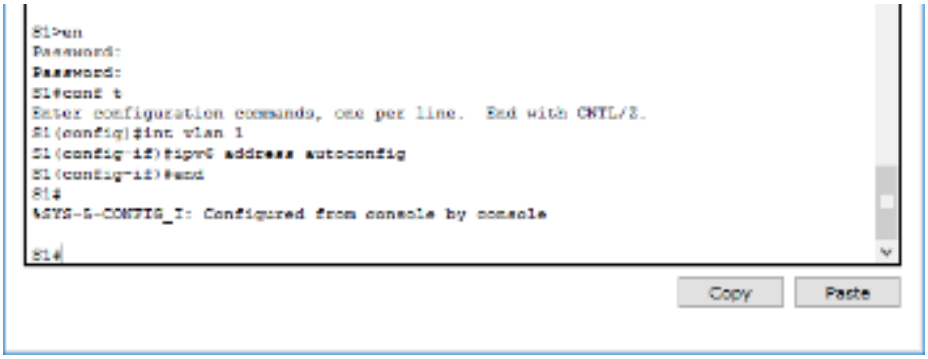
Configurar la red para SLAAC

Configurar R1

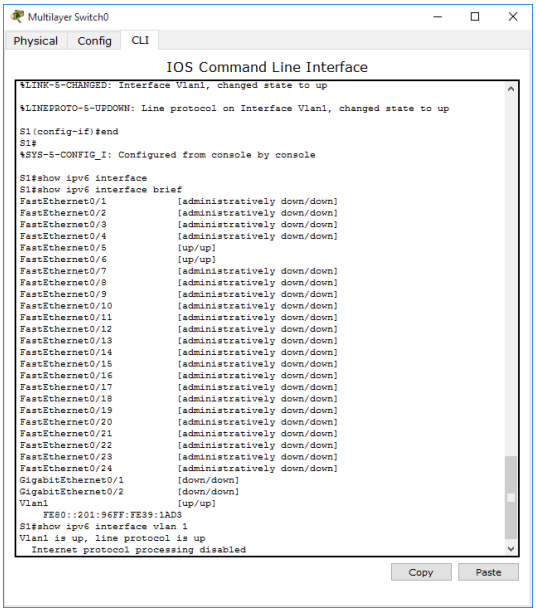


Configurar S1

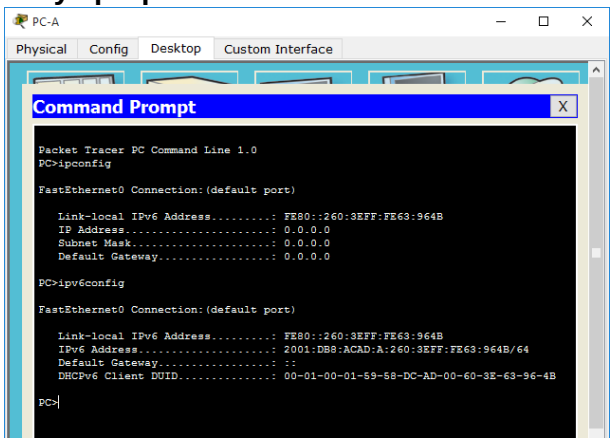
Se usa la autoconfiguración de direcciones sin estado SLAAC por medio del comando ipv6 address autoconfig



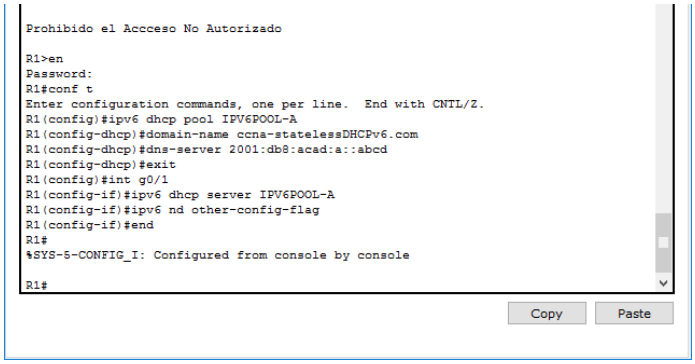
Packet tracert al no soportar la característica para mostrar las direcciones autoconfiguradas, no mostrara la dirección asignada



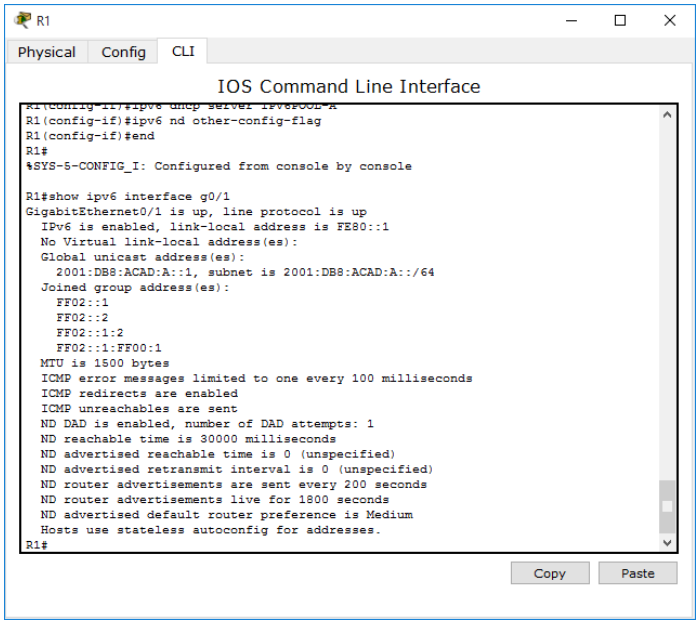
Verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.



Parte 3: configurar la red para DHCPv6 sin estado

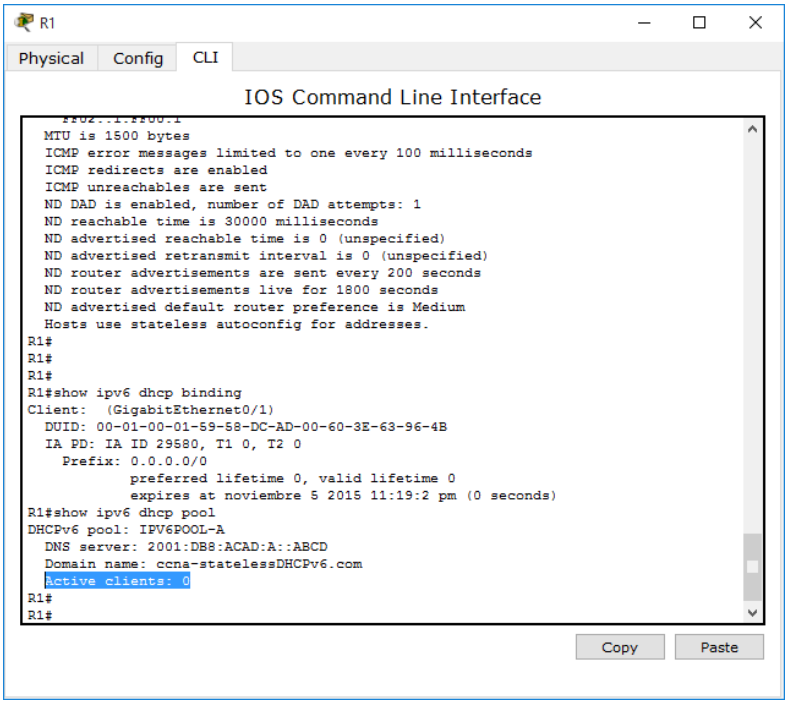


Se verifica que la configuración en la interfaz g0/1 haya sido efectiva mediante el comando show ipv6 interface g0/1



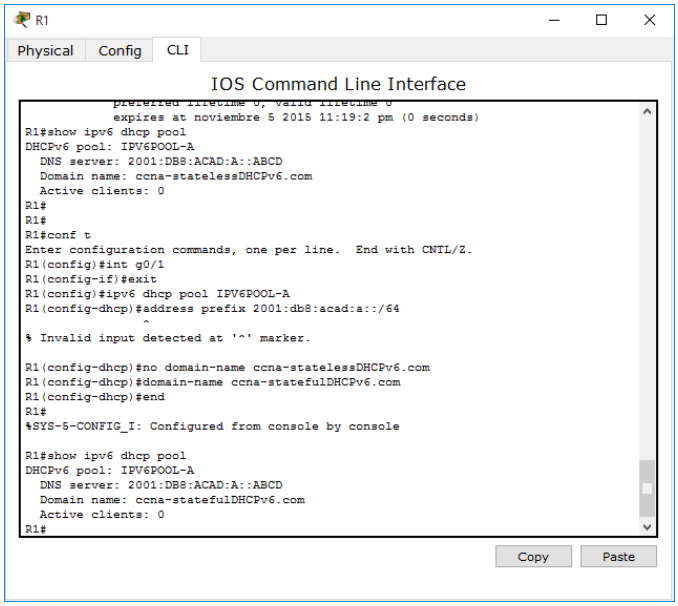
Se verifican las nuevas configuraciones de red en la PC-A

Se verifica que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6 por medio de los comandos show ipv6 dhcp binding y show ipv6 dhcp pool, en este último se nota el 0 en los clientes activos.

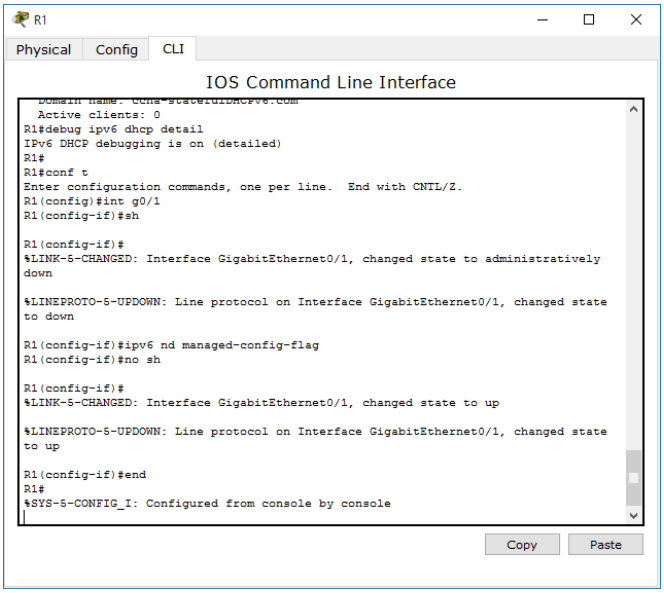


Configurar la red para DHCPv6 con estado

Luego de quitar las características de IPv6 en PC-A se cambia el pool de DHCPv6 en R1, dentro del proceso se resalta que pkt no soporta el comando address prefix 2001:db8:acad:a::/64, además se cambia el nombre del pool, y se muestran los cambios por medio de show ip dhcp pool



Establecer el indicador en G0/1 para DHCPv6 con estado, donde es necesario apagar la interfaz para que al encenderla reciba el mensaje RA



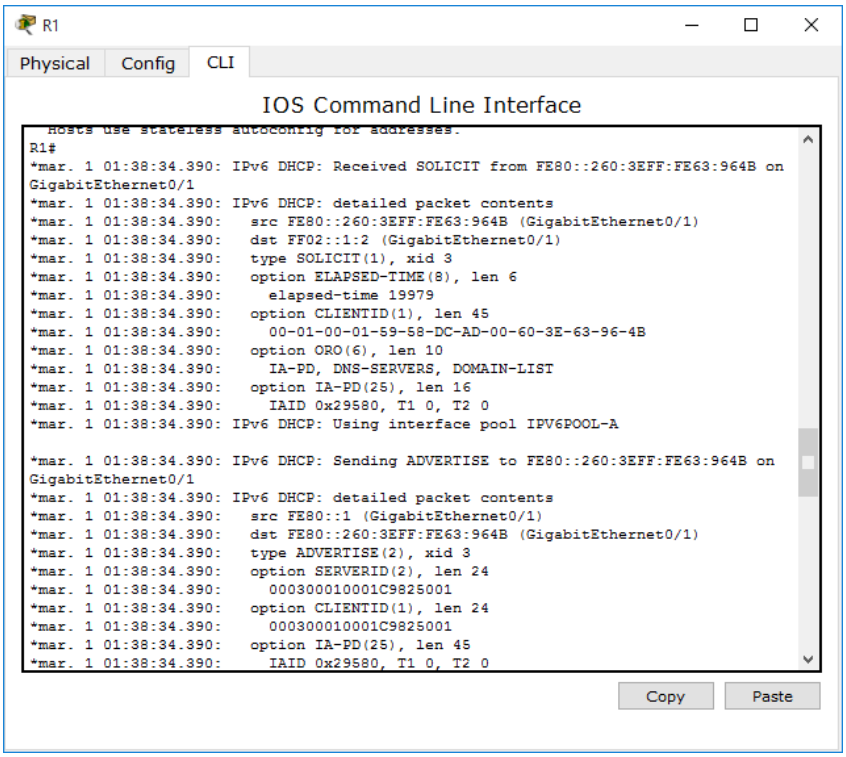
Se deberá encender de nuevo la interfaz fa0/6 en S1

Verificar la configuración de DHCPv6 con estado en el R1

Se verifica por medio de show ipv6 interface g0/1 y en PC-A se activa la opción DHCP para que le sea asignada la configuración

Aquí se denota la importancia del comando address prefix 2001:db8:acad:a::/64 pues pkt al no soportarlo, no se le asigna dirección unicast al PC-A

Se detiene el debug ejecutado con anterioridad por medio de undebug all, y se obtiene



Reflexión

1. ¿Qué método de direccionamiento IPv6 utiliza más recursos de memoria en el router configurado como servidor de DHCPv6: DHCPv6 sin estado o DHCPv6 con estado? ¿Por qué?

   DHCPv6 con estado requiere de más memoria pues requiere que el router almacene dinámicamente el estado de información de los clientes, mientras que en DHCPv6 sin estado los clientes no utilizan el servidor, por consiguiente no demandan uso de memoria.

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

   Cisco recomienda la DHCPv6 sin estado cuando se implementan y desarrollan redes en IPv6 sin CNR (Cisco Network Registrar)

Conclusiones De Practica: 10.2.3.5 configuración de DHCPv6 sin estado y con estado

Durante el desarrollo de la práctica, ser resalta que no se realizaron los puntos en los que se incluían el whireshark, pues el proceso se realiza a través de Packet Tracer y este no admite dicha herramienta. Además se encuentran obstáculos en la aplicación de comandos de configuración IPv6 por presentar incompatibilidad como es el caso de address prefix 2001:db8:acad:a::/64.

Por medio de DHCPv6 es posible obtener parámetros como direcciones desde servidores DHCP en redes con IPv6, es importante tener en cuenta que el sistema DHCPv6 sin estado, no requiere que los clientes utilicen el servidor lo que representa una nula demanda de memoria, mientas que en DHCPv6 con estado, se hace necesario que la información dinámica de los clientes se almacene, lo que se traduce un uso de memoria más alto.

Cuando se va a establecer el indicador en G0/1 para DHCPv6 con estado, es necesario apagar la interfaz para que al encenderla reciba el mensaje de anuncio de router RA y reciba las configuraciones automáticamente.

10.3.1.1 IdT y DHCP

Objetivo

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

Situación

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

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

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

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

REFLEXIÓN

¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica? ¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?

Los Router ofrecen más opciones para implementar planes de seguridad y son más sólidos en cuanto a capacidad de procesamiento y de ancho de banda.

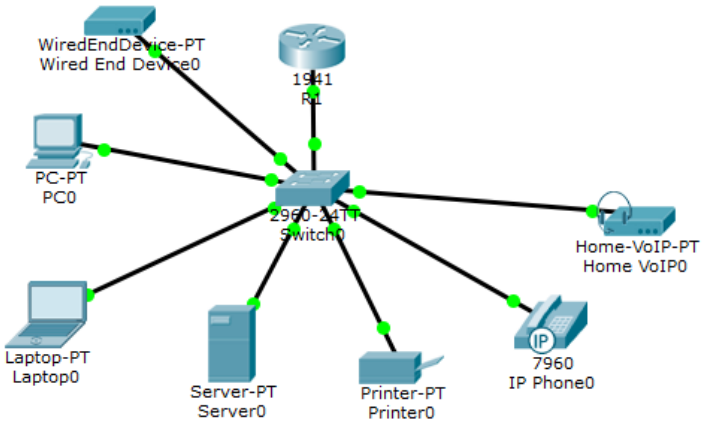
¿Cómo cree que las pequeñas y medianas empresas pueden usar la asignación de direcciones IP de DHCP en el mundo de las redes IPv6 e IdT? Mediante la técnica de la lluvia de ideas, piense y registre cinco respuestas posibles.

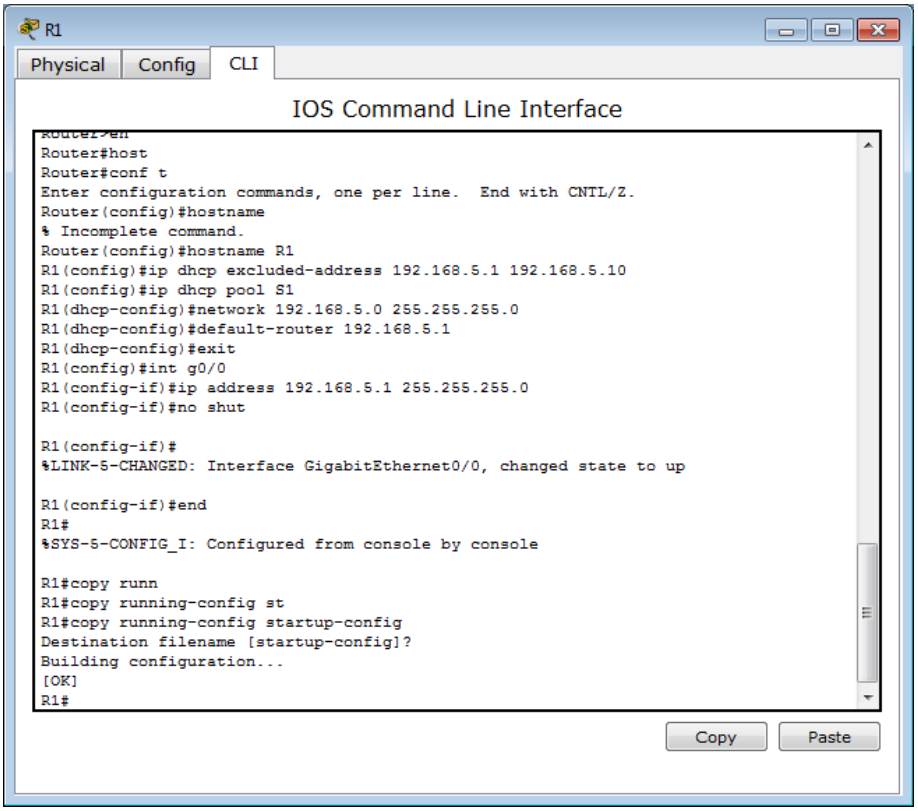
Mediante DHCP no es necesario configurar cada terminal, por lo que simplificaría el trabajo de configuración de direcciones en una empresa.

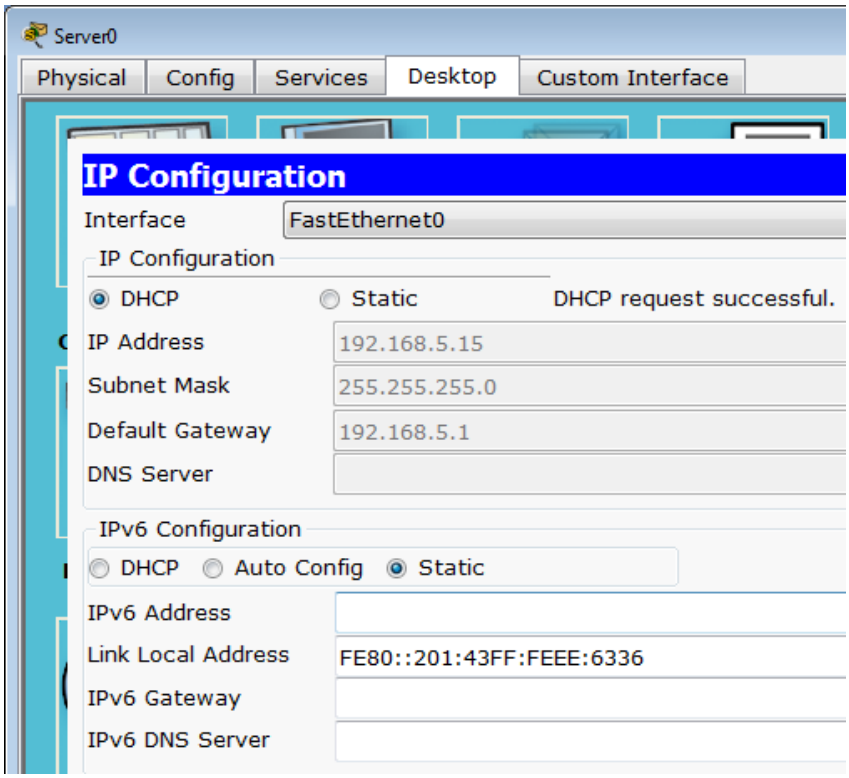
El propietario de una casa podría encender la lavadora o la secadora desde cualquier lugar, según la ubicación de un servidor DNS y su propia dirección de servidor de DHCP.

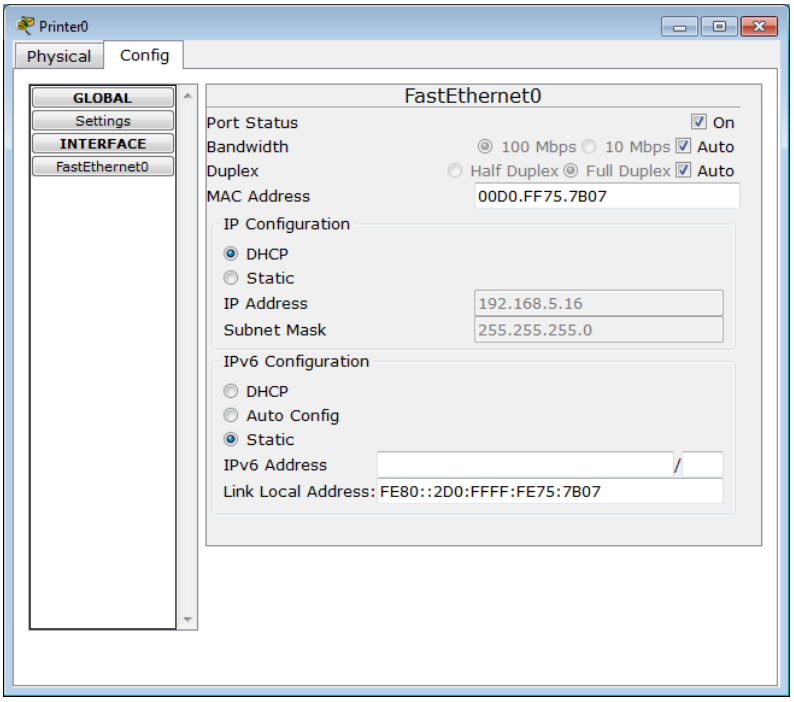
Se puede asignar direcciones IP a cámaras de seguridad para acceder desde cualquier terminal en la misma red.

Se podrían controlar los televisores para apagarlos, encenderlos, seleccionar canales para grabar, grabar programas y más mediante un servidor DNS y un servidor de DHCP personal.









Conclusiones De Practica: 10.3.1.1 IoE and DHCP

Los Router ofrecen más opciones para implementar planes de seguridad y son más sólidos en cuanto a capacidad de procesamiento y de ancho de banda.

La principal ventaja del protocolo DHCP es que no tenemos que conocer los parámetros de la red, como rango de direcciones, máscara de red o puerta de enlace. Simplemente conectamos y el servidor DHCP se encarga de asignar automáticamente la dirección IP, no es necesario el conocer que direcciones IPya se han configurado. Una desventaja es que tiene menor seguridad que la asignación de dirección fija.

11.2.2.6 Práctica de laboratorio: configuración de NAT dinámica y estática

Topología

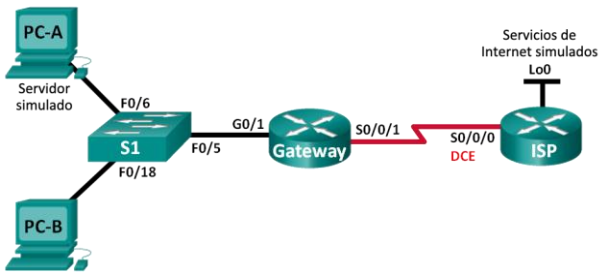


Tabla de direccionamiento

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
Server ISP	NIC	192.31.7.2	255.255.255.0	192.31.7.1
PC-A (servidor simulado)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

Información básica/situación

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

En esta práctica de laboratorio, un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/27. Esto proporciona 30 direcciones IP públicas a la empresa. Las direcciones 209.165.200.225 a 209.165.200.241 son para la asignación estática, y las direcciones 209.165.200.242 a 209.165.200.254 son para la asignación dinámica. Del ISP al router de gateway se usa una ruta estática, y del gateway al router ISP se usa una ruta predeterminada. La conexión del ISP a Internet se simula mediante una dirección de loopback en el router ISP.

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

Part 11: armar la red y verificar la conectividad

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

Step 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.

Step 2: configurar los equipos host.

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

Step 4: configurar los parámetros básicos para cada router.

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

Step 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**

Step 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
```

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

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

Step 7: Guardar la configuración en ejecución en la configuración de inicio.

Step 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.

```
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=19ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=3ms 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 = 19ms, Average = 5ms
```

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
```

Part 12: configurar y verificar la NAT estática.

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

Step 1: configurar una asignación estática.

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

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

Step 2: Especifique las interfaces.

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

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

Step 3: probar la configuración.

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

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---

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

192.168.1.20 = 209.165.200.225

¿Quién asigna la dirección global interna? **Router NAT pool**

¿Quién asigna la dirección local interna? **El administrador de red**

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

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:1	192.168.1.20:1	192.31.7.1:1	192.31.7.1:1

--- 209.165.200.225 192.168.1.20 --- ---

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? **65-66-67-68-69-70-71**

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

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

Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23
--- 209.165.200.225 192.168.1.20 --- ---

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

¿Qué protocolo se usó para esta traducción? **web**

¿Cuáles son los números de puerto que se usaron?

Global/local interno: 1034

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.

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

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

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

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

Gateway# **show ip nat statics**
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago

Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39 Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

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

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

Part 13: configurar y verificar la NAT dinámica

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

Step 1: borrar las NAT.

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

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

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

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

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

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

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

Step 4: definir el conjunto de direcciones IP públicas utilizables.

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

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

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

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

Step 6: probar la configuración.

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

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
icmp	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.242	192.168.1.21	---	---

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

192.168.1.21 = 209.165.200.242

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

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

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

c. Muestre la tabla de NAT.

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.242:1038	192.168.1.21:1038	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1039	192.168.1.21:1039	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1040	192.168.1.21:1040	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1041	192.168.1.21:1041	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1042	192.168.1.21:1042	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1043	192.168.1.21:1043	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1044	192.168.1.21:1044	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1045	192.168.1.21:1045	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1046	192.168.1.21:1046	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1047	192.168.1.21:1047	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1048	192.168.1.21:1048	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1049	192.168.1.21:1049	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1050	192.168.1.21:1050	192.31.7.1:80	192.31.7.1:80

tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80 192.31.7.1:80
--- 209.165.200.242 192.168.1.22 --- ---

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

¿Qué números de puerto se usaron?

Interno: **1025**

Externo: **80**

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

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

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

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

Step 7: eliminar la entrada de NAT estática.

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

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

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

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

b. Borre las NAT y las estadísticas.

c. Haga ping al ISP (192.31.7.1) desde ambos hosts.

```
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=19ms TTL=254
Reply from 192.31.7.1: bytes=32 time=16ms TTL=254
Reply from 192.31.7.1: bytes=32 time=19ms TTL=254
Reply from 192.31.7.1: bytes=32 time=3ms 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 = 3ms, Maximum = 19ms, Average = 14ms
```

d. Muestre la tabla y las estadísticas de NAT.

   Gateway# **show ip nat statistics**
   Total active translations: 4 (0 static, 4 dynamic; 2 extended)
   Peak translations: 15, occurred 00:00:43 ago
   Outside interfaces:
     Serial0/0/1
   Inside interfaces:
     GigabitEthernet0/1
   Hits: 16 Misses: 0
   CEF Translated packets: 285, CEF Punted packets: 0
   Expired translations: 11
   Dynamic mappings:
   -- Inside Source
   [Id: 1] access-list 1 pool public_access refcount 4
    pool public_access: netmask 255.255.255.224
          start 209.165.200.242 end 209.165.200.254
          type generic, total addresses 13, allocated 2 (15%), misses 0

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

Gateway# **show ip nat translation**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.243:512	192.168.1.20:512	192.31.7.1:512	192.31.7.1:512
---	209.165.200.243	192.168.1.20	---	---
icmp	209.165.200.242:512	192.168.1.21:512	192.31.7.1:512	192.31.7.1:512
---	209.165.200.242	192.168.1.21	---	---

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

Reflexión

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

   Por qué se ahorran IP's publicas mayor seguridad debido a que no se muestra la IP de los Host hacia internet por que se usan IP globales asignadas por gateway

2. ¿Cuáles son las limitaciones de NAT?

   Hay un tiempo de retraso en el Gateway y algunos servicios no pueden salir hacia internet como por ejemplo SNMP

Conclusiones De Practica: 11.2.2.6 configuración de NAT dinámica y estática

La implementación de NAT es un mecanismo utilizado en la red creado para solucionar la escasez de direcciones IPV4 publicas su función es conectar una o más redes LAN internas a internet mediante una sola IP publica o conjunto de estas. en el caso de la NAT estática se mapea la dirección IP privada con una dirección IP publica de forma tal que cada equipo en la red privada tiene asignado una IP publica para acceder a internet. Para la NAT dinámica se utiliza un pool de IP's privadas que son mapeadas de forma dinámica y a demanda.

11.2.3.7 Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT

Topología

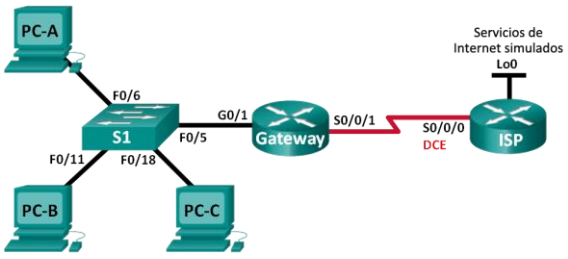


Tabla de direccionamiento

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

Objetivos

Parte 1: armar la red y verificar la conectividad

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

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direccionesa 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.

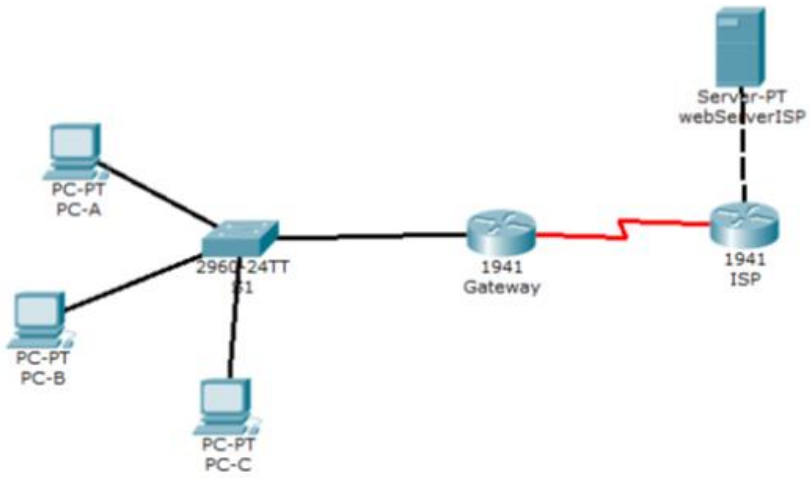
Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden 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.

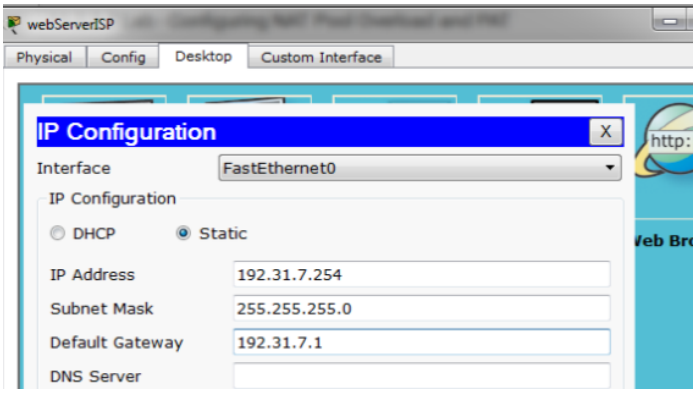
PARTE 1: ARMAR LA RED Y VERIFICAR LA CONECTIVIDAD

Como Packet tracer no soporta los comandos en el Router, para ello entonces se agrega un servidor web en la G0 de ISP.

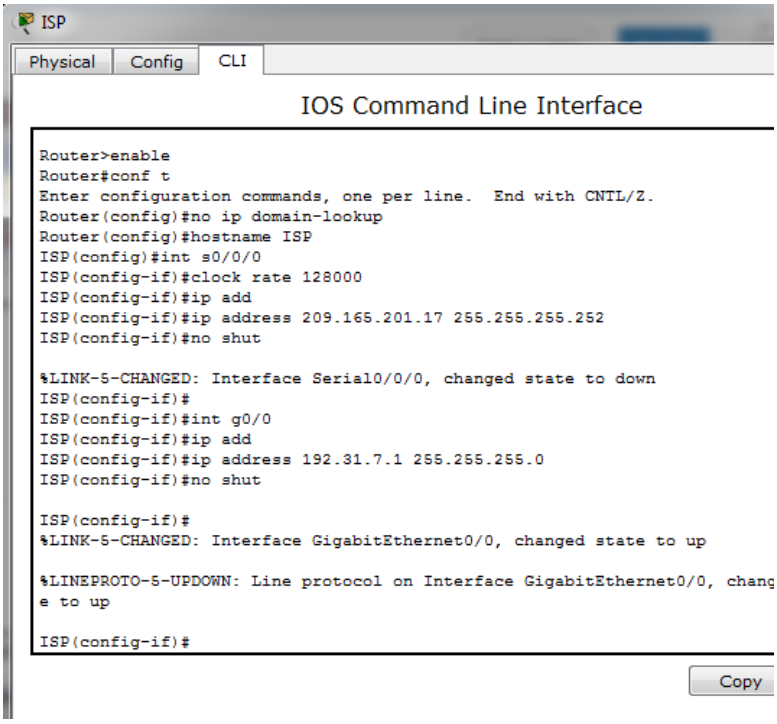


Se configuran las direcciones ip de los dispositivos (Pc, Switch, Router)

Configuración del servidor web.



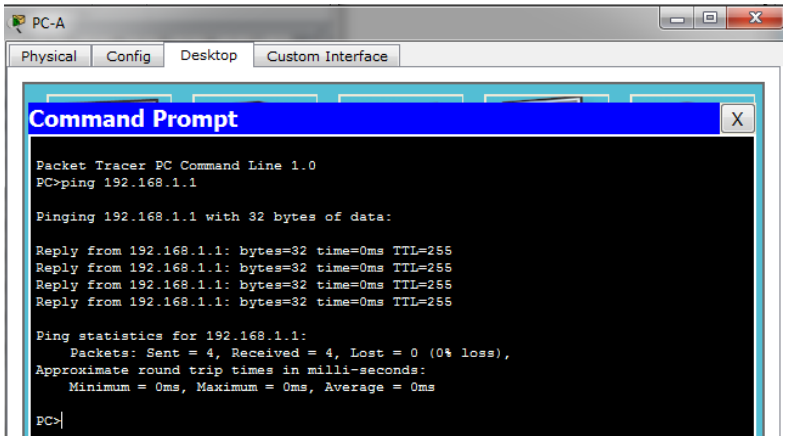
ISP



Configuración del routing estático.

e. 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**
f. 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**

Se verifica la conectividad



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.

Step 8: definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

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

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

Step 9: definir el conjunto de direcciones IP públicas utilizables.

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

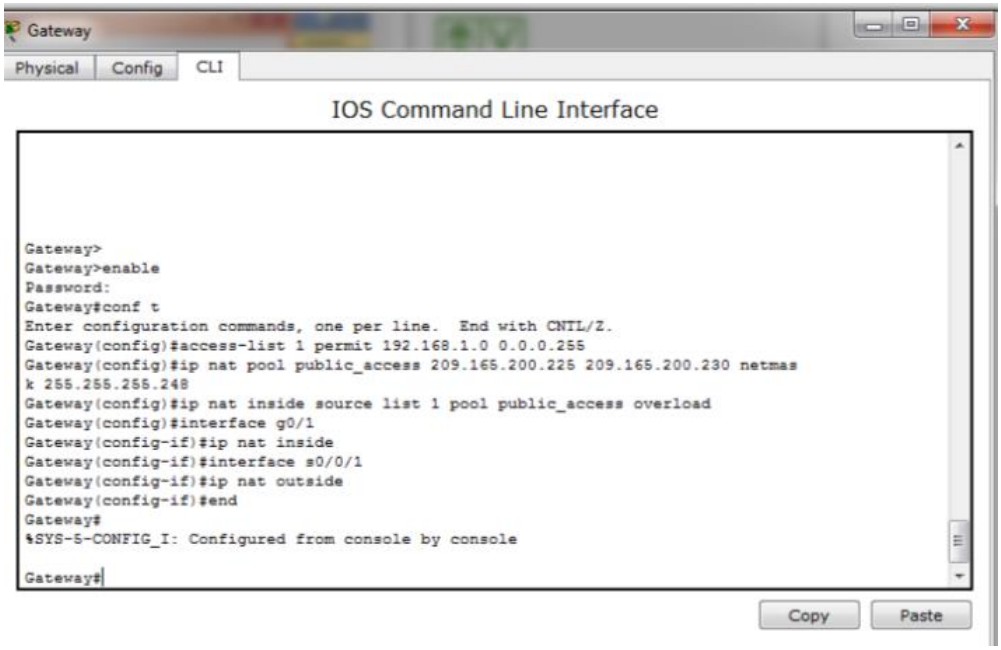
Step 10: definir la NAT desde la lista de origen interna hasta el conjunto externo.

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

Step 11: Especifique las interfaces.

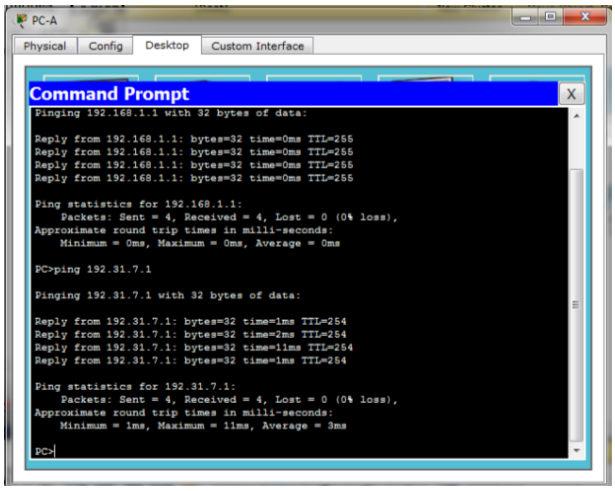
Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

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



Step 12: verificar la configuración del conjunto de NAT con sobrecarga.

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



b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
Serial0/0/1
Inside interfaces:
GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6, allocated 1 (16%), misses 0

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

c. Muestre las NAT en el router Gateway.

Gateway# **show ip nat translations**
Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:0 192.168.1.20:1	192.31.7.1:1	192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1	192.31.7.1:1	192.31.7.1:2

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

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior?

Rta: Hay 3:

- **192.168.1.20**
- **192.168.1.21**
- **192.168.1.22**

¿Cuántas direcciones IP globales internas se indican?

Rta: 1.

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas?

Rta: Se usan 12 puertos en conjunto con las direcciones globales internas.

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

Rta: El ping falla porque solo conoce el lugar de la direcciones ip *Inside global* en su tabla de ruteo, pero las direcciones ip *inside local* no están notificadas.

Part 14: CONFIGURAR Y VERIFICAR PAT

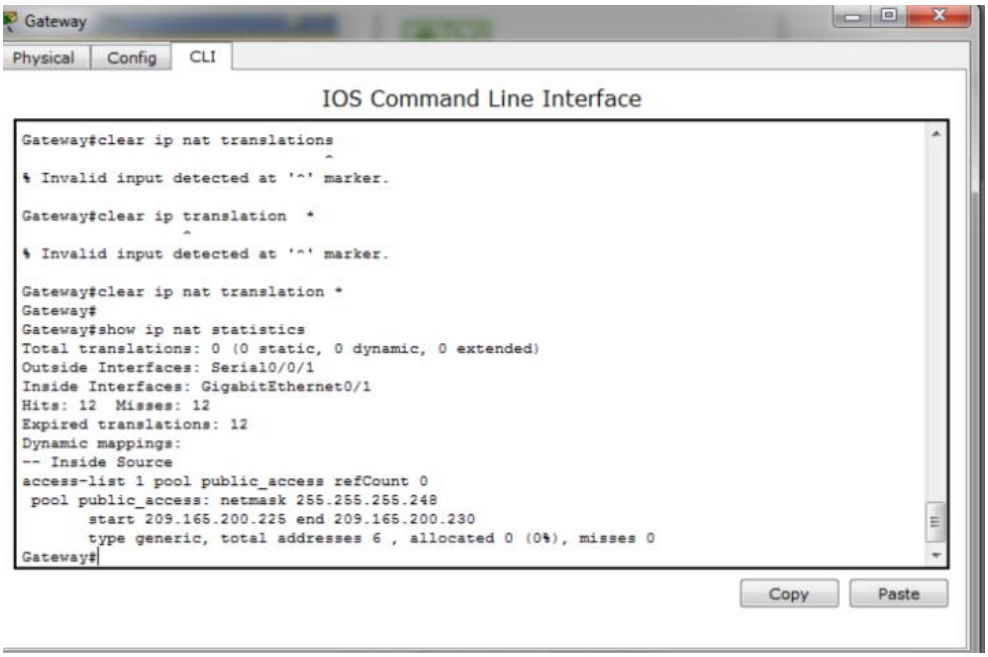
En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Step 1: borrar las NAT y las estadísticas en el router Gateway.

Se realiza con: **clear ip nat translation ***

Step 2: verificar la configuración para NAT.

a. Verifique que se hayan borrado las estadísticas.



b. Verifique que las interfaces externa e interna estén configuradas para NAT.

Outside Interfaces: Serial0/0/1

Inside Interfaces: GigabitEthernet0/1

c. Verifique que la ACL aún esté configurada para NAT.

Access-list 1 poo public_access refCount 0

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

*Gateway# **show ip nat statistics***

Step 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**

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

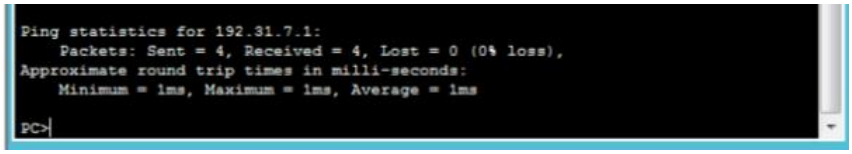
Gateway(config)# **no ip nat inside source list 1 pool public_access overload**

Step 5: asociar la lista de origen a la interfaz externa.

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

Step 6: probar la configuración PAT.

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.



b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
Serial0/0/1
Inside interfaces:
GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

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

c. Muestre las traducciones NAT en el Gateway.

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.18:3	192.168.1.20:1	192.31.7.1:1	192.31.7.1:3
icmp	209.165.201.18:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.201.18:4	192.168.1.22:1	192.31.7.1:1	192.31.7.1:4

Reflexión

¿Qué ventajas tiene la PAT?

PAT minimiza el número de direcciones públicas necesitadas para ingresar a internet, y PAT al igual que NAT sirve para esconder las direcciones privadas hacia la red externa.

Conclusiones De Practica: 11.2.3.7 configuración de un conjunto de NAT con sobrecarga y PAT

Después de haber realizado la práctica se recomienda para tener éxito en una nueva realización de la práctica, al empezar la realización de la topología teniendo en cuenta que Packet tracer no soporta los comandos en el Router, es importante agregar un servidor web en la G0/0 de ISP.

Al configurar el servidor web se debe tener en cuenta colocar sus direcciones dentro del mismo grupo de la red, para establecer conectividad.

Después de cada configuración realizada también se recomienda estar verificando la conectividad por medio de ping realizados desde cualquier host al Gateway. Con ello se evita que al terminar las configuraciones de la red no se lleve una sorpresa insatisfactoria y deba iniciar todas las configuraciones anteriormente realizadas.

Cuando se realiza ping desde el Router ISP a una de los hots, sucede que el ping falla porque solo conoce el lugar de la direcciones ip ***Inside global*** en su tabla de ruteo, pero las direcciones ip ***inside local*** no están notificadas.

Para finalizar se recuerda que la importancia de la **PAT** en una red es minimizar el número de direcciones públicas necesitadas para ingresar a internet y **PAT** al igual que **NAT** sirve para esconder las direcciones privadas hacia la red externa.

CONCLUSIONES

Con la realización de las anteriores prácticas se logró comprender con mayor profundidad temas relacionados con Enrutamiento Dinámico, OSPF de una sola área, Listas de control de acceso, DHCP y Traducción de direcciones IP para IPv4.

Para ello se realizó una serie de 14 practicas donde se realizó documentación de las mismas y también se trabajó en el programa de Packet tracer.

Dichas prácticas se realizaron algunas desde cero (creando desde la topología hasta las configuraciones de cada dispositivo para establecer la conectividad y el objetivo de cada practica) y también se realizaron las practicas desde un archivo pka, en el cual se aplicaron las configuraciones solicitadas en dichas prácticas.

BIBLIOGRAFIA

Cisco . (2017). Cisco Networking Academy. *Práctica de laboratorio: configuración básica de RIPv2 y RIPng*

Cisco . (2017). Cisco Networking Academy. *Práctica de laboratorio: configuración de OSPFv2 básico de área única*

Cisco. (2017). Cisco Networking Academy. *Práctica de laboratorio: configuración de OSPFv3 básico de área única*

Cisco. (2017). Cisco Networking Academy. *Práctica de laboratorio: configuración de DHCPv4 básico en un router*

Cisco. (2017). Cisco Networking Academy. *Práctica de laboratorio: configuración de DHCPv4 básico en un switch*

Cisco. (2017). Cisco Networking Academy. *Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado*

Cisco. (2017). Cisco Networking Academy. *IdT y DHCP*

Cisco. (2017). Cisco Networking Academy. *Práctica de laboratorio: configuración de NAT dinámica y estática*

Cisco. (2017). Cisco Networking Academy. *Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT*

Cisco. (2017). Cisco Networking Academy. *Packet Tracer: Configure IP ACLs to Mitigate Attacks*

Cisco. (2017). Cisco Networking Academy. *Packet Tracer: Configuring Standard ACLs*

Cisco. (2017). Cisco Networking Academy. *Packet Tracer: Configuring Named Standard ACLs*

Cisco. (2017). Cisco Networking Academy. *Packet Tracer: Configuring an ACL on VTY Lines*

Cisco. (2017). Cisco Networking Academy. *Packet Tracer: Configuring IPv6 ACLs*

Cisco Networking Academy. (s.f.). *Capítulo 7: Routing dinámico.* Recuperado el 15 de Noviembre de 2017, de UNIDAD 4 Enrutamiento en soluciones de red.

Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

Cisco Networking Academy. (s.f.). *Capítulo 8: Capítulo 8: OSPF de área única.* Recuperado el 17 de Noviembre de 2015, de UNIDAD 4 Enrutamiento en soluciones de red. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

Cisco Networking Academy. (s.f.). *Capítulo 9: Listas de control de acceso.* Recuperado el 15 de Noviembre de 2017, de UNIDAD 4 Enrutamiento en soluciones de red. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

Cisco Networking Academy. (s.f.). *Capítulo 10: DHCP.* Recuperado el 15 de Noviembre de 2017, de UNIDAD 4 Enrutamiento en soluciones de red. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Cisco Networking Academy. (s.f.). *Capítulo 11: Traducción de direcciones de red para IPv4.* Recuperado el 15 de Noviembre de 2017, de UNIDAD 4 Enrutamiento en soluciones de red. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1