

**UNIDAD 4. CONFIGURACIÓN DE VLANS DESARROLLO DE PRÁCTICAS EN PACKET  
TRACER CURSO DE PROFUNDIZACIÓN CISCO CCNA2**

**PRESENTADO POR:**

**CAMILO ANDRÉS VARGAS VEGA  
JOHN JAVI AGUDELO  
LINA MARCELA HERNÁNDEZ  
CRISTIAN CAMILO ESCUDERO  
ROSA MARÍA RODRÍGUEZ**

**GRUPO: 203092\_30**

**TUTOR:**

**GERARDO GRANADOS ACUÑA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS  
NOVIEMBRE - 2017**

## TABLA DE CONTENIDO

INTRODUCCION .....	3
4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks_Instructor .....	6
7.3.2.4 Lab - Configuring Basic RIPv2 and RIPv2 .....	19
8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2.....	40
8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3.....	95
9.2.1.10 Packet Tracer Configuring Standard ACLs Instructions IG .....	108
9.2.1.11 Packet Tracer - Configuring Named Standard ACLs Instructions IG.....	117
9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines Instructions IG .....	128
9.5.2.6 Packet Tracer - Configuring IPv6 ACLs Instructions IG.....	132
10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router.....	140
10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch.....	164
10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6 .....	179
10.3.1.1 IoE and DHCP Instructions.....	212
11.2.2.6 Lab - Configuring Dynamic and Static NAT .....	215
11.2.3.7 Lab - Configuring NAT Pool Overload and PAT .....	237
CONCLUSIONES.....	244
BIBLIOGRAFIA .....	244

## INTRODUCCION

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

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

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

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

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

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

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

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

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

Básicamente el grupo colaborativo realizará la programación básica de RIPv2 y RIPv6 que consistirá en el enrutamiento de direcciones IPv4 que incluyen de manera automática la máscara de subred, esto debido a que el protocolo del enrutador es sin asignación de clase, resume de manera automática los límites de las redes principales, también se ejecutarán los comandos pertinentes para realizar la configuración de OSPFv2 básico de área sueltas, específicamente diseñada para el protocolo IPv4, cuya finalidad es detectar las posibles fallas del enlace, cambios en la topología de la red con una alta convergencia en una estructura de routing con bucles.

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

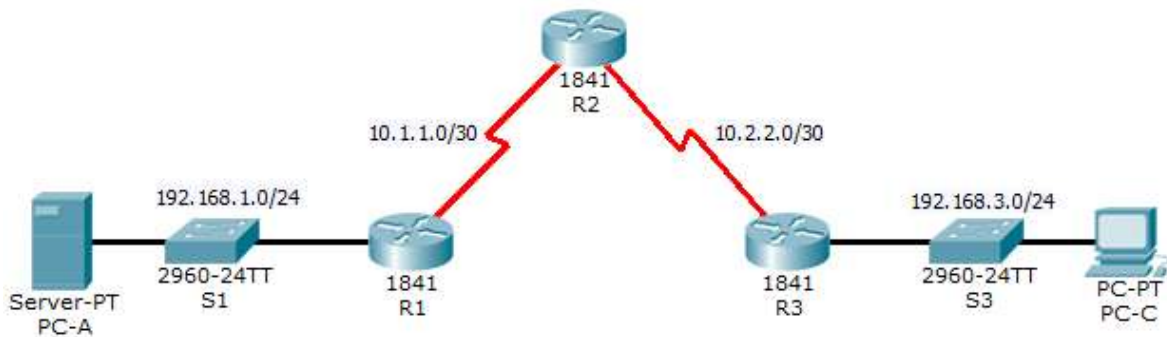
Realizaremos la configuración de DHCPv6 sin estado y con estado la cual consistirá en la determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

De una manera muy práctica estableceremos las condiciones necesarias para crear una pequeña red doméstica mediante IdT y DHCP, que consistirá en la programación del router que permite identificar cualquier ID que esté conectado a dicha red desde cualquier lugar. Nos introduciremos en las direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

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

## DESARROLLO DE LOS LABORATORIOS

### 4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks\_Instructor

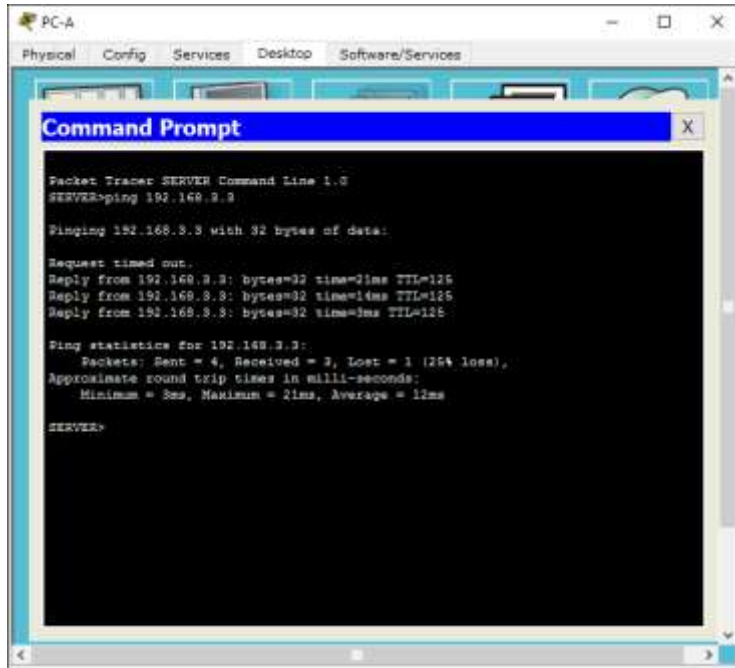


#### Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

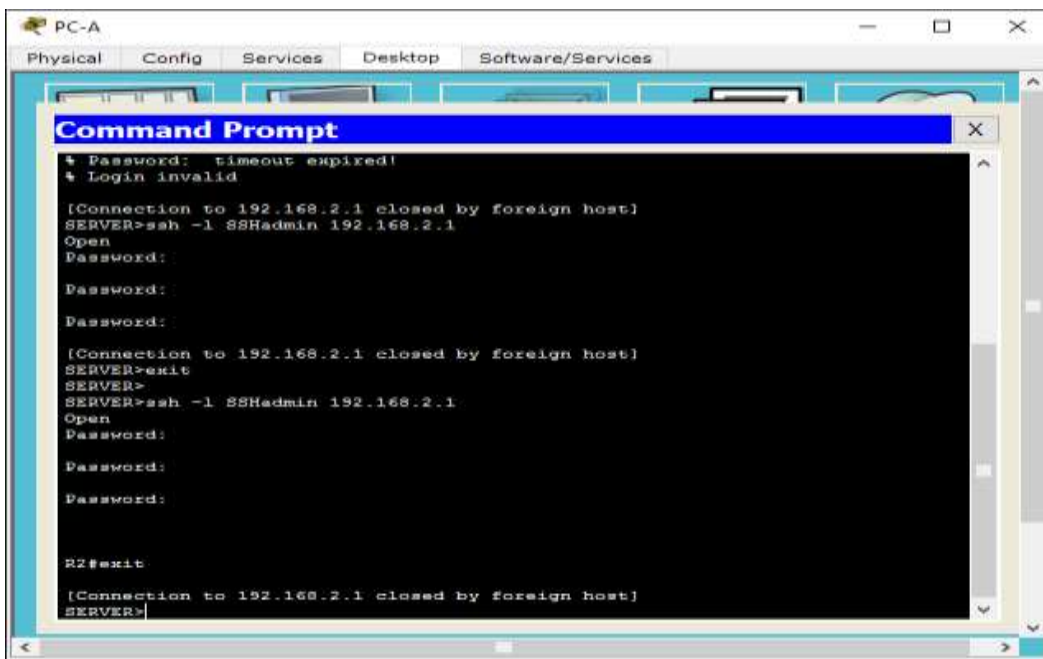
**Step 1: From PC-A, verify connectivity to PC-C and R2.**

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

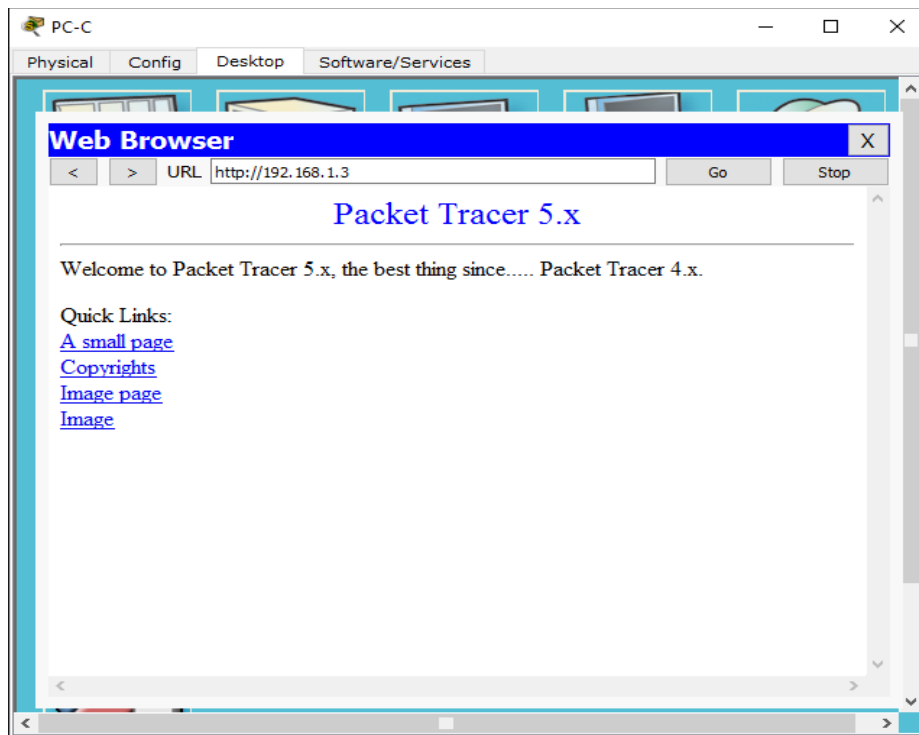
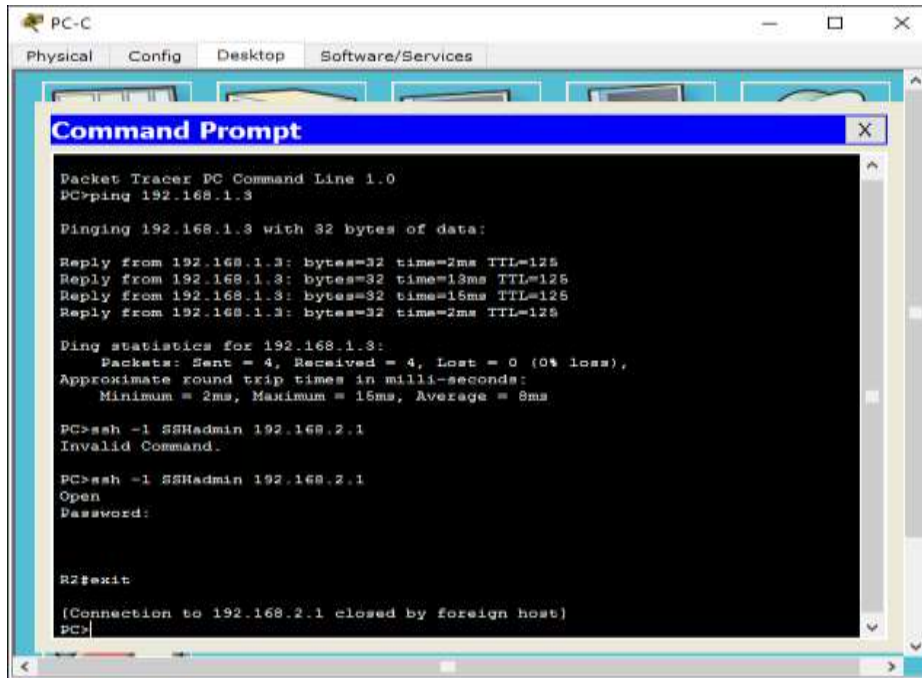


b. From the command prompt, establish a SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. When finished, exit the SSH session.

PC> ssh -l SSHAdmin 192.168.2.1



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

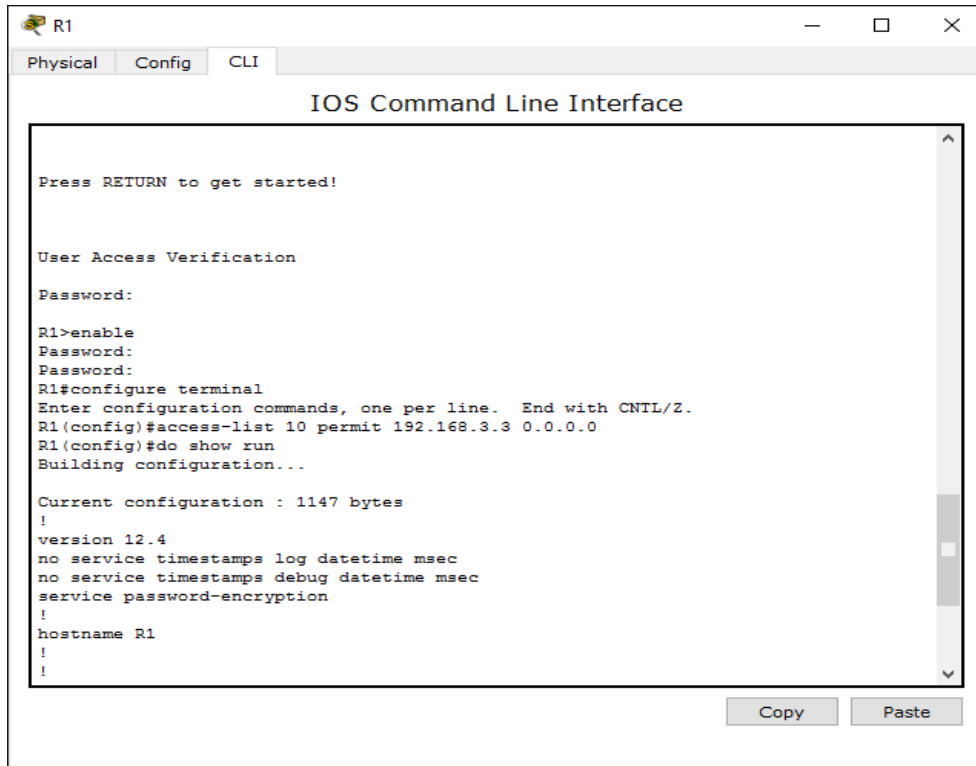


## Part 2: Secure Access to Routers



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

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



```
R1
Physical Config CLI
IOS Command Line Interface

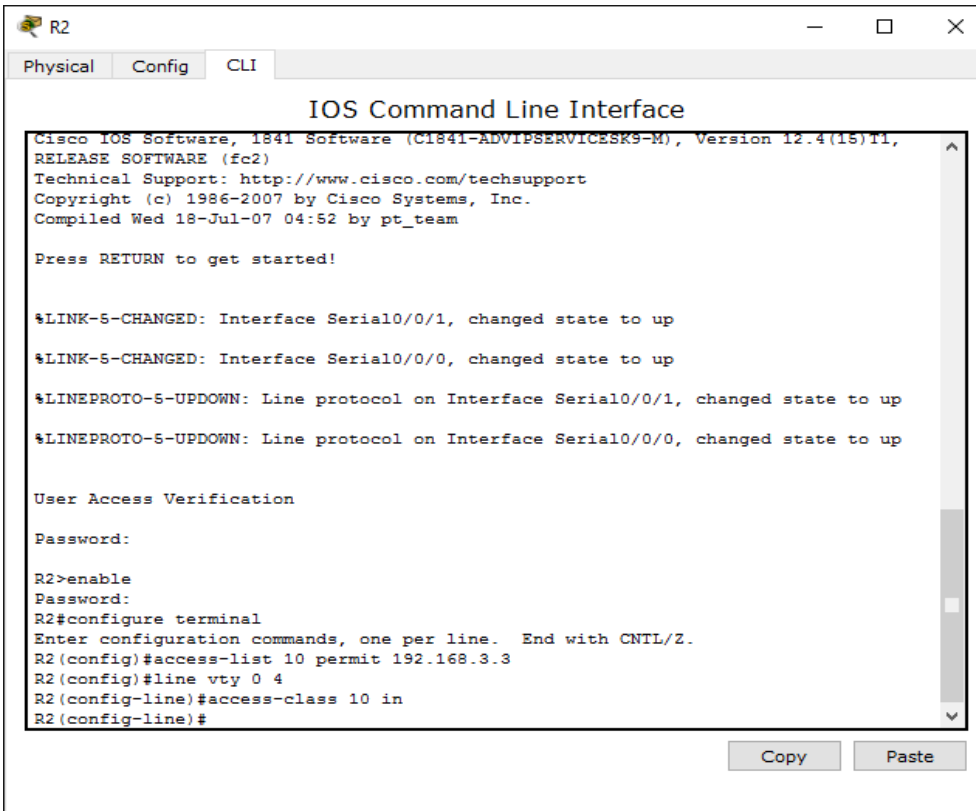
Press RETURN to get started!

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R1(config)#do show run
Building configuration...

Current configuration : 1147 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
```



```
R2
Physical Config CLI
IOS Command Line Interface

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

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

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#
```

```
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

User Access Verification

Password:
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#
```

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

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

```
PC-C
Physical Config Desktop Software/Services
Command Prompt
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 15ms, Average = 8ms

PC>ssh -l SSHadmin 192.168.2.1
Invalid Command.

PC>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
PC>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#exit

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

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

```
PC-A
Physical Config Services Desktop Software/Services
Command Prompt
Password:

[Connection to 192.168.2.1 closed by foreign host]
SERVER>exit
SERVER>
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:

Password:

Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh l SSHadmin 192.168.2.1
Invalid Command.

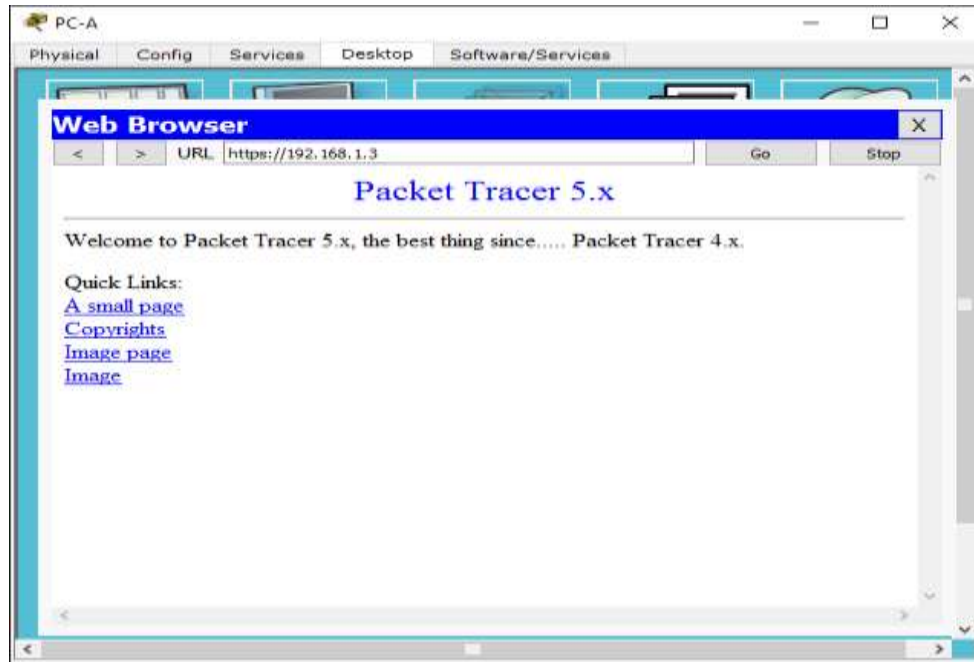
SERVER>ssh -l SSHadmin 192.168.2.1
Invalid Command.

SERVER>ssh -l SSHadmin 192.168.2.1
Invalid Command.

SERVER>
```

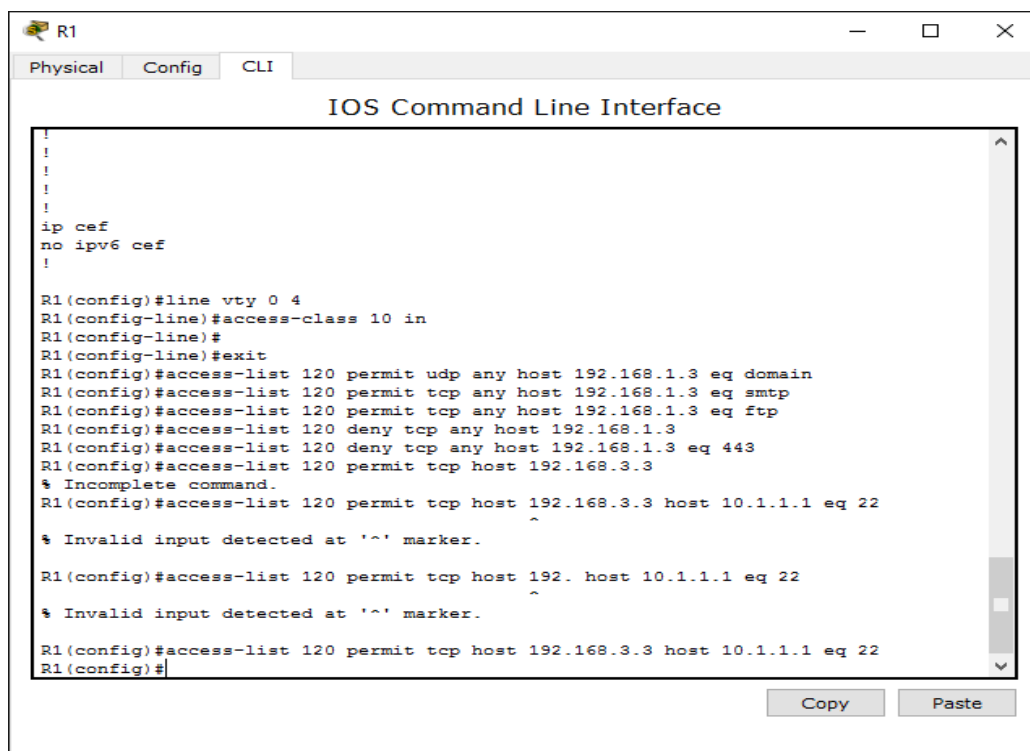
**Part 3: Create a Numbered IP ACL 120 on R1**

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

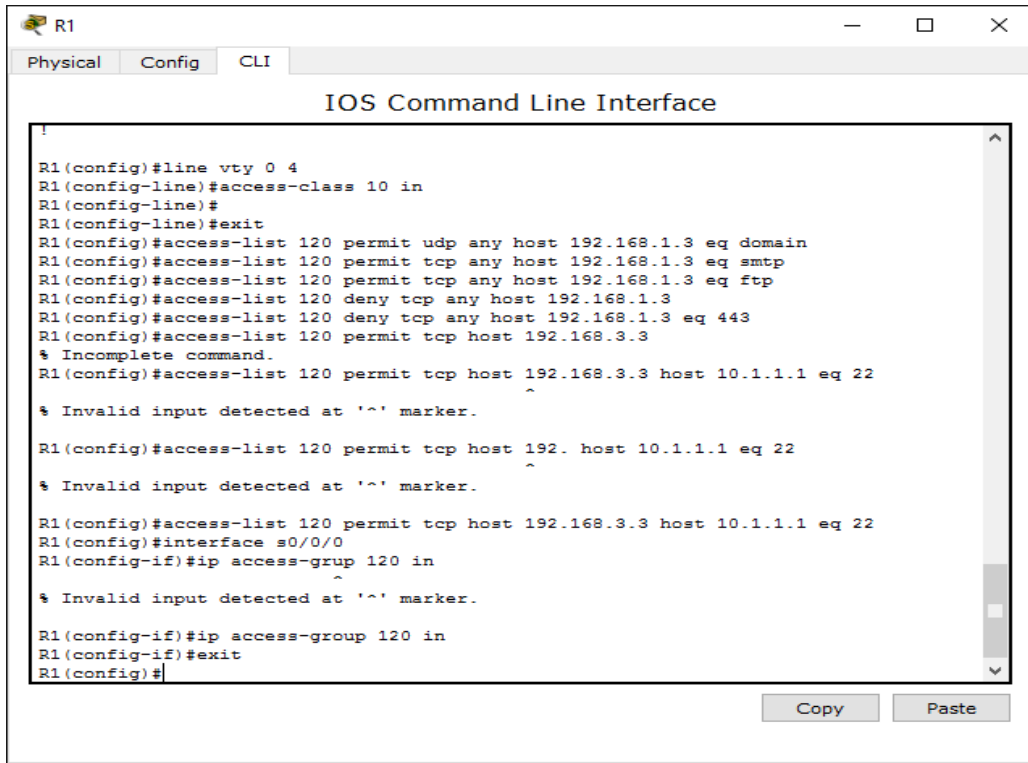


**Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.**

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

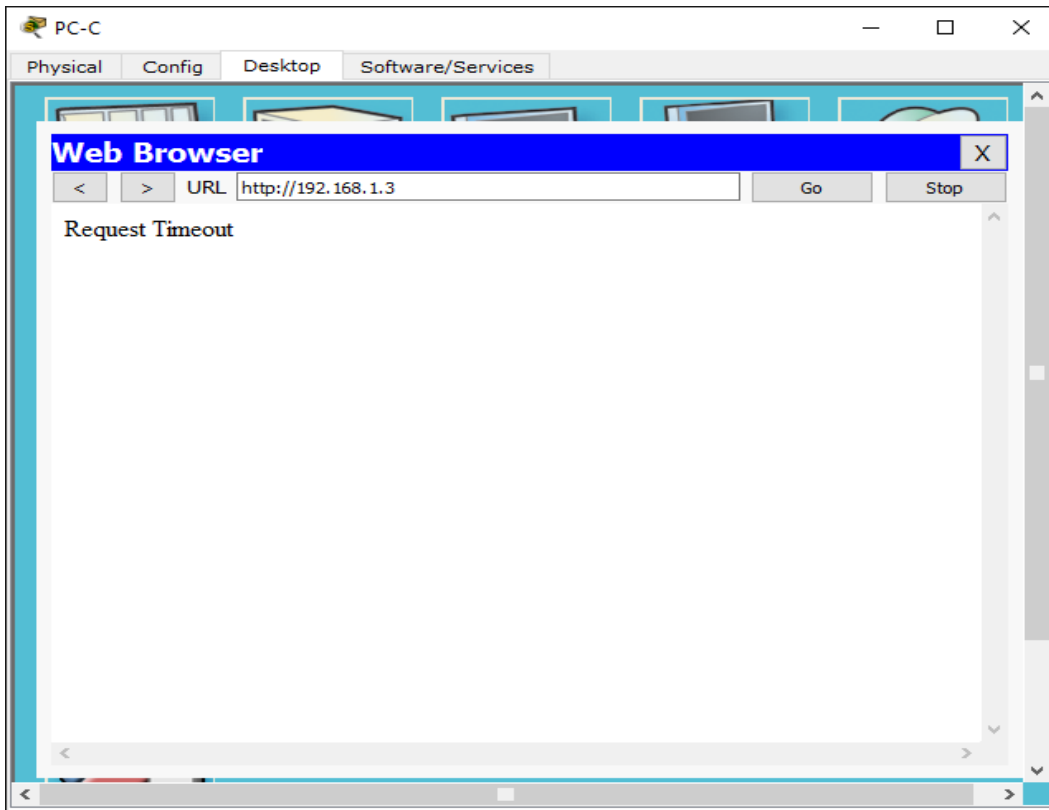


### Step 3: Apply the ACL to interface S0/0/0.



```
R1
Physical Config CLI
IOS Command Line Interface
!
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#
R1(config-line)#exit
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3
% Incomplete command.
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
% Invalid input detected at '^' marker.
R1(config)#access-list 120 permit tcp host 192. host 10.1.1.1 eq 22
% Invalid input detected at '^' marker.
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#interface s0/0/0
R1(config-if)#ip access-grup 120 in
% Invalid input detected at '^' marker.
R1(config-if)#ip access-group 120 in
R1(config-if)#exit
R1(config)#
```

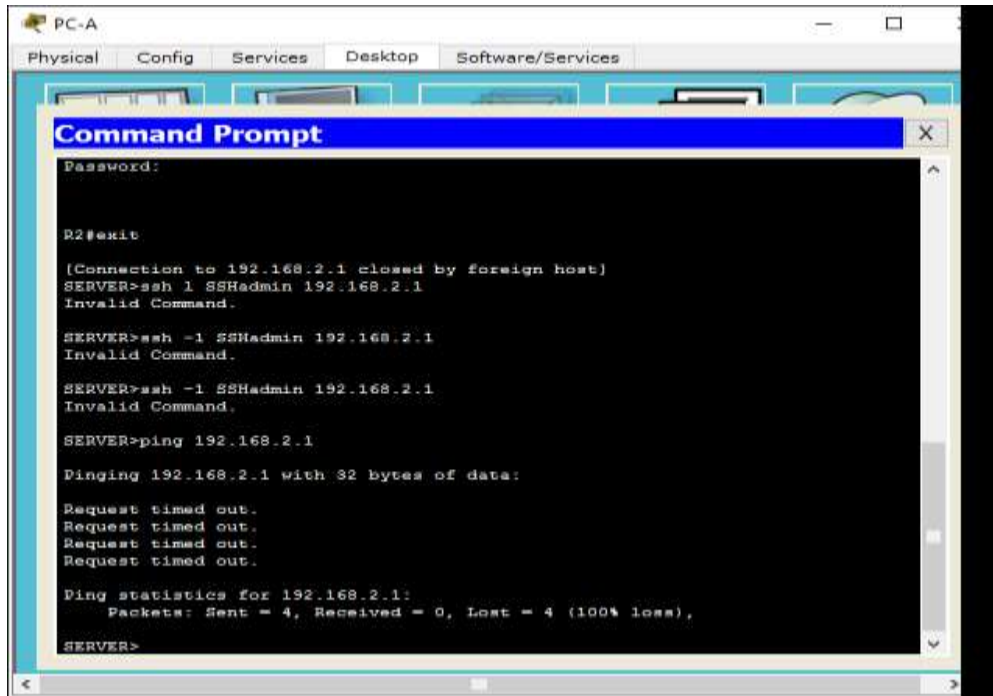
### Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.



#### Part 4: Modify An Existing ACL on R1

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

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



```
PC-A
Physical Config Services Desktop Software/Services
Command Prompt
Password:
R2#exit
[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh 1 SSHadmin 192.168.2.1
Invalid Command.
SERVER>ssh -1 SSHadmin 192.168.2.1
Invalid Command.
SERVER>ssh -1 SSHadmin 192.168.2.1
Invalid Command.
SERVER>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
SERVER>
```

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

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

```

R1
Physical Config CLI
IOS Command Line Interface
R1(config-line)#
R1(config-line)#exit
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3
% Incomplete command.
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
% Invalid input detected at '^' marker.
R1(config)#access-list 120 permit tcp host 192. host 10.1.1.1 eq 22
% Invalid input detected at '^' marker.
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#interface s0/0/0
R1(config-if)#ip access-grup 120 in
% Invalid input detected at '^' marker.
R1(config-if)#ip access-group 120 in
R1(config-if)#exit
R1(config)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#
Copy Paste

```

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

```

PC-A
Physical Config Services Desktop Software/Services
Command Prompt
Invalid Command.
SERVER>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
SERVER>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=11ms TTL=254
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms
SERVER>

```

**Part 5: Create a Numbered IP ACL 110 on R3**

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

```
R3
Physical Config CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

User Access Verification
Password:
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#configure terminal
^
% Invalid input detected at '^' marker.
R3(config-line)#exit
R3(config)#access-list 110 permit ip 192.168.3.0.0.0.0.255 any
^
% Invalid input detected at '^' marker.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#
```

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

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

```
R3
Physical Config CLI
IOS Command Line Interface
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

User Access Verification
Password:
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#configure terminal
^
% Invalid input detected at '^' marker.
R3(config-line)#exit
R3(config)#access-list 110 permit ip 192.168.3.0.0.0.0.255 any
^
% Invalid input detected at '^' marker.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#
```

**Part 6: Create a Numbered IP ACL 100 on R3**

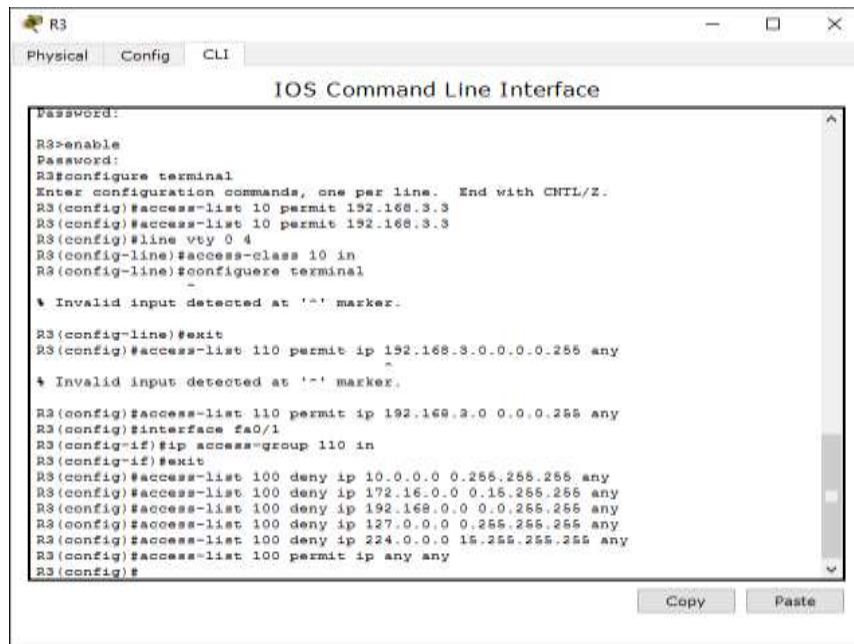


On **R3**, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

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

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

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



```
R3
Physical Config CLI
IOS Command Line Interface
Password:
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#configure terminal
^ Invalid input detected at '^' marker.
R3(config-line)#exit
R3(config)#access-list 110 permit ip 192.168.3.0.0.0.0.255 any
^ Invalid input detected at '^' marker.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#exit
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#
```

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

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

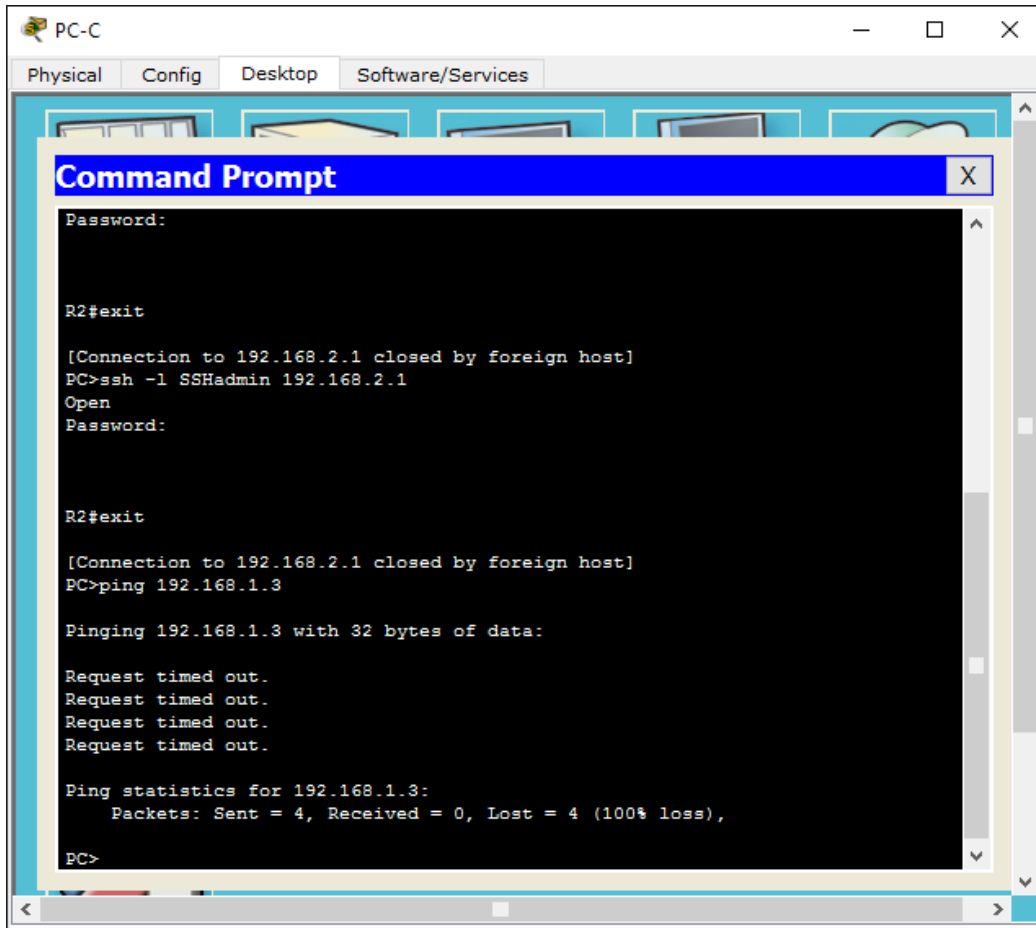
```
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#access-list 10 permit 192.168.3.3
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#configuere terminal
^
% Invalid input detected at '^' marker.

R3(config-line)#exit
R3(config)#access-list 110 permit ip 192.168.3.0.0.0.0.255 any
^
% Invalid input detected at '^' marker.

R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#exit
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#
```

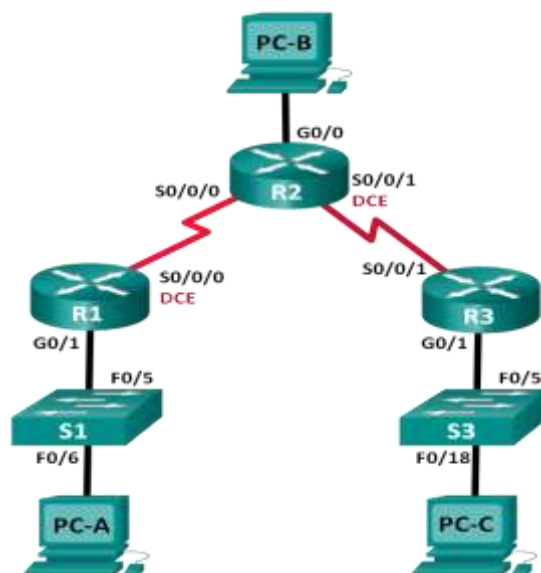
**Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.**

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



### 7.3.2.4 Lab - Configuring Basic RIPv2 and RIPvng

#### 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	255.255.255.2 52	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.2 52	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.2 52	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.2 52	N/A
S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

### Objetivos

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

#### Parte 2: configurar y verificar el routing RIPv2

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

#### Parte 3: configurar IPv6 en los dispositivos

#### **Parte 4: configurar y verificar el routing RIPng**

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

#### **Información básica/situación**

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

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

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

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

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

## Recursos necesarios

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

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

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

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

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

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

- a. Desactive la búsqueda del DNS.
- b. Configure los nombres de los dispositivos como se muestra en la topología.
- c. Configure la encriptación de contraseñas.
- d. Asigne **class** como la contraseña del modo EXEC privilegiado.
- e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- g. Configure **logging synchronous** para la línea de consola.
- h. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- i. Configure una descripción para cada interfaz con una dirección IP.
- j. Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.
- k. Copie la configuración en ejecución en la configuración de inicio.

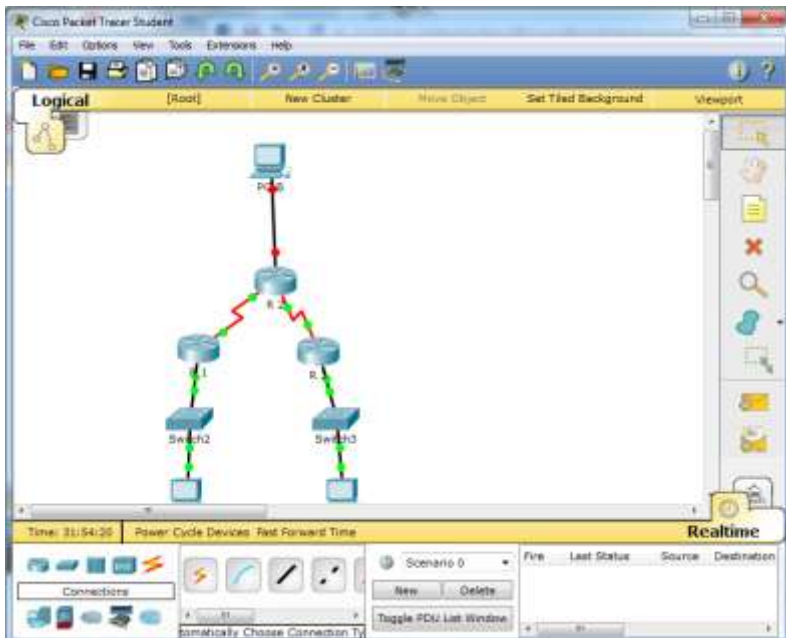
#### Paso 4. configurar los equipos host.

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

#### Paso 5. Probar la conectividad.

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

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



## Parte 2: configurar y verificar el routing RIPv2

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

### Paso 1. Configurar el enrutamiento RIPv2.

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

```
R1# config t
```

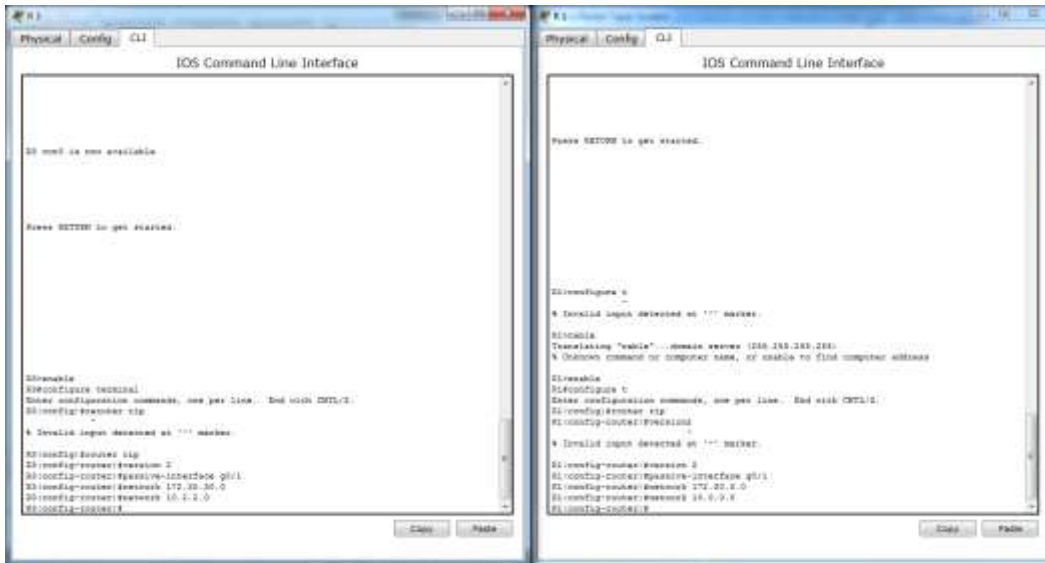
```
R1(config)# router rip
```

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

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

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

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



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

- b. Configure RIPv2 en el R3 y utilice la instrucción **network** para agregar las redes apropiadas y evitar actualizaciones de routing en la interfaz LAN.
- c. Configure RIPv2 en el R2. No anuncie la red 209.165.201.0.

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

**Paso 2. examinar el estado actual de la red.**

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

R2# **show ip interface brief**

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



b. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? NO ¿Por qué? NO HAY UNA RUTA QUE LLEGUE A PCB

¿Es posible hacer ping de la PC-A a la PC-C? NO ¿Por qué? R1 Y R3 NO TIENEN RUTAS HACE LA SUBREDESPECIFICA EN EL ROUTER REMOTO

¿Es posible hacer ping de la PC-C a la PC-B? NO ¿Por qué? PC B NO PARTICIPA EN RIP, NI EXISTE UNA RUTA

¿Es posible hacer ping de la PC-C a la PC-A? NO ¿Por qué? R1 Y R3 No Poseen Rutas Hacia La Red Especifica Remota

c. Verifique que RIPv2 se ejecute en los routers.

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

R1# **show ip protocols**

Routing Protocol is "rip"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Sending updates every 30 seconds, next due in 7 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Redistributing: rip

Default version control: **send version 2, receive 2**

Interface	Send	Recv	Triggered	RIP	Key-chain
-----------	------	------	-----------	-----	-----------

Serial0/0/0	2	2			
-------------	---	---	--	--	--

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

10.0.0.0

172.30.0.0

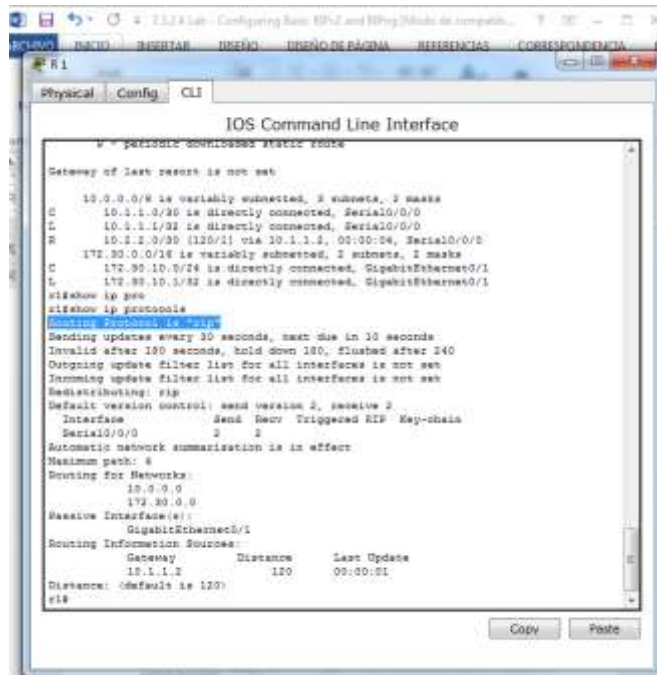
Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

Gateway	Distance	Last Update
10.1.1.2	120	

Distance: (default is 120)



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

**RIP: received v2 update from 10.1.1.1 on Serial0/0/0  
172.30.0.0/16 via 0.0.0.0 in 1 hops**

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

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

router rip

version 2

d. Examinar el sumarización automática de las rutas.

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

dirección de red principal con clase 172.30.0.0 y no muestra ninguna de las subredes de esta red.

**R2# show ip route**

<Output Omitted>

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

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

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

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

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

R 172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1

[120/1] via 10.1.1.1, 00:00:09, Serial0/0/0

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

C 209.165.201.0/24 is directly connected, GigabitEthernet0/0

L 209.165.201.1/32 is directly connected, GigabitEthernet0/0

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

**R1# show ip route**

<Output Omitted>

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

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

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

R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0

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

C 172.30.10.0/24 is directly connected, GigabitEthernet0/1

L 172.30.10.1/32 is directly connected, GigabitEthernet0/1

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

**R3# show ip route**

<Output Omitted>

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

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

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

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

172.30.0.0/16 y 10.1.1.0/16

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

### **Paso 3. Desactivar la sumarización automática.**

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

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

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

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

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

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

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

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

```
R2# show ip route
```

```
<Output Omitted>
```

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

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

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

```
L    10.1.1.2/32 is directly connected, Serial0/0/0
C    10.2.2.0/30 is directly connected, Serial0/0/1
L    10.2.2.2/32 is directly connected, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R    172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:01, Serial0/0/1
     [120/1] via 10.1.1.1, 00:01:15, Serial0/0/0
R    172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0
R    172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04, Serial0/0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.0/24 is directly connected, GigabitEthernet0/0
L    209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

R1# **show ip route**

<Output Omitted>

Gateway of last resort is not set

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

R3# **show ip route**

<Output Omitted>

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

L 172.30.30.1/32 is directly connected, GigabitEthernet0/1

R 172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1

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

**R2# debug ip rip**

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

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

172.30.30.0/24

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

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

a. Desde el R2, cree una ruta estática a la red 0.0.0.0 0.0.0.0, con el comando **ip route**.

Esto envía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet al establecer un gateway de último recurso en el router R2.

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

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

R2(config)# **router rip**

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

**Paso 5. Verificar la configuración de enrutamiento.**

c. Consulte la tabla de routing en el R1.

R1# **show ip route**

<Output Omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

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

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

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

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

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

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

C 172.30.10.0/24 is directly connected, GigabitEthernet0/1

L 172.30.10.1/32 is directly connected, GigabitEthernet0/1

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

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

HAY UN GATWAY DE ULTIMO ALCANCE, ES DECIR UNA PUERTA D ENELACE QUE NO CONECTAA INERNET, Y EN LA TRBAL DE RUTO ESTA PRENDIDA PARA RIP

d. Consulte la tabla de routing en el R2.

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

R2, TIENE UNA RUTA ESTÁTICA POR DEFECTO ATREVES DE LA 209.165.201.2 QUE ESTÁ CONECTADA A LA GIGABIT 0

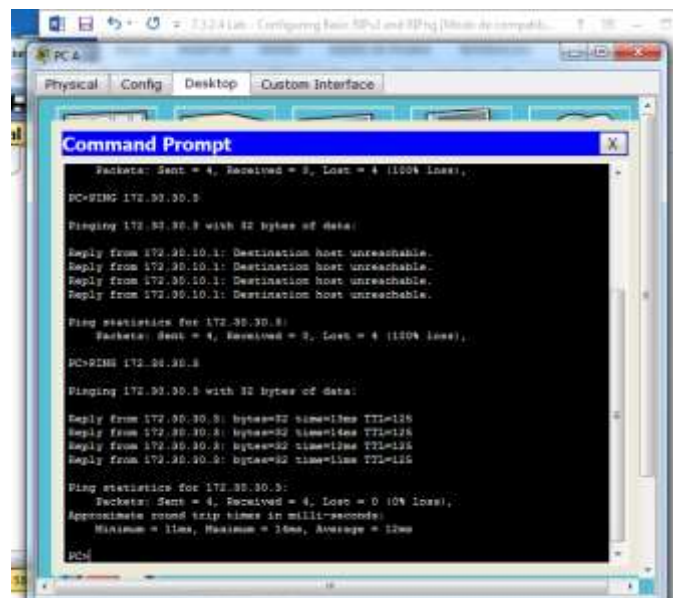
### Paso 6. Verifique la conectividad.

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

¿Tuvieron éxito los pings? SI

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

¿Tuvieron éxito los pings? SI



```
Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>PING 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>PING 172.30.30.5
Pinging 172.30.30.5 with 32 bytes of data:
Reply from 172.30.30.5: bytes=32 time=13ms TTL=126
Reply from 172.30.30.5: bytes=32 time=14ms TTL=126
Reply from 172.30.30.5: bytes=32 time=13ms TTL=126
Reply from 172.30.30.5: bytes=32 time=13ms TTL=126
Ping statistics for 172.30.30.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 16ms, Average = 13ms
PC>
```

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

### Parte 3: configurar IPv6 en los dispositivos

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

## Tabla de direccionamiento

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

### Paso 1. configurar los equipos host.

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

### Paso 2. configurar IPv6 en los routers.

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

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



- b. Habilite el routing IPv6 en cada router.
- c. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.

Show ipv6 interface brief



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

#### Parte 4: configurar y verificar el routing RIPng

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

##### Paso 1. configurar el routing RIPng.

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



Interfaces:

Serial0/0/0

GigabitEthernet0/1

Redistribution:

None

¿En qué forma se indica RIPng en el resultado?

Indica el nombre del proceso "rip Test1"

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

R1# **show ipv6 rip Test1**

RIP process "Test1", port 521, multicast-group FF02::9, pid 314

Administrative distance is 120. Maximum paths is 16

Updates every 30 seconds, expire after 180

Holddown lasts 0 seconds, garbage collect after 120

Split horizon is on; poison reverse is off

Default routes are not generated

Periodic updates 1, trigger updates 0

Full Advertisement 0, Delayed Events 0

Interfaces:

GigabitEthernet0/1

Serial0/0/0

Redistribution:

None

¿Cuáles son las similitudes entre RIPv2 y RIPng?

Tanto RIPv2 y RIPng tienen distancia administrativa de 120, ambas usan conteo de saltos como métrica y envían autorizaciones cada 30 seg

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

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

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

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

g. Verifique la conectividad entre las computadoras.

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

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

¿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? **YES**

¿Por qué algunos pings tuvieron éxito y otros no?

**No hay una ruta que se notifique para esa red para PC-B**

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

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

---

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

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

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

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

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

### **Paso 3. Verificar la configuración de enrutamiento.**

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

```
R2# show ipv6 route
```

```
IPv6 Routing Table - 10 entries
```

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

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

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

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

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

D - EIGRP, EX - EIGRP external

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

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

**Tiene una ruta estatica por defecto en R2**

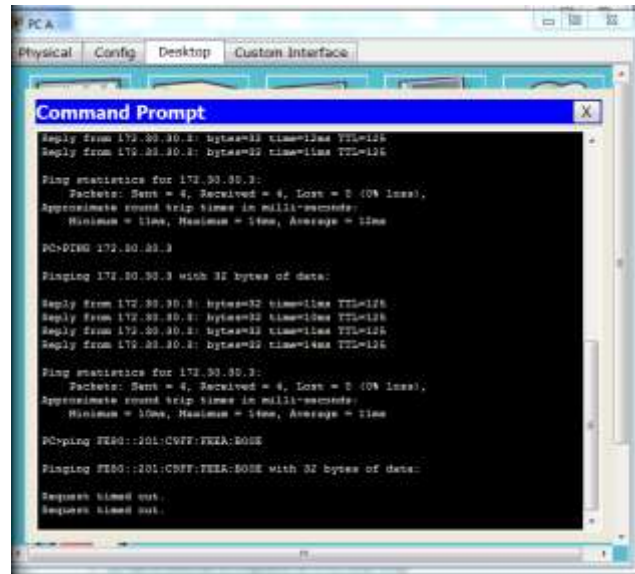
b. Consulte las tablas de routing del R1 y el R3.

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

**La tabla de ruteo de muestra distribuida gracias a Ripng, con una métrica de 2**

**Paso 4. Verifique la conectividad.**

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



¿Tuvieron éxito los pings? **Si**

## Reflexión

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

Para que los routers no sumaricen hacia la clase mayor y así puede haber conectividad entre redes discontinuas

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

Aprendieron de las actualizaciones de rip enviadas desde el router, donde fue configurada la ruta por defecto en R2

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

Rip versión 2 se configura notificando las redes y el v6 notificando las interfaces

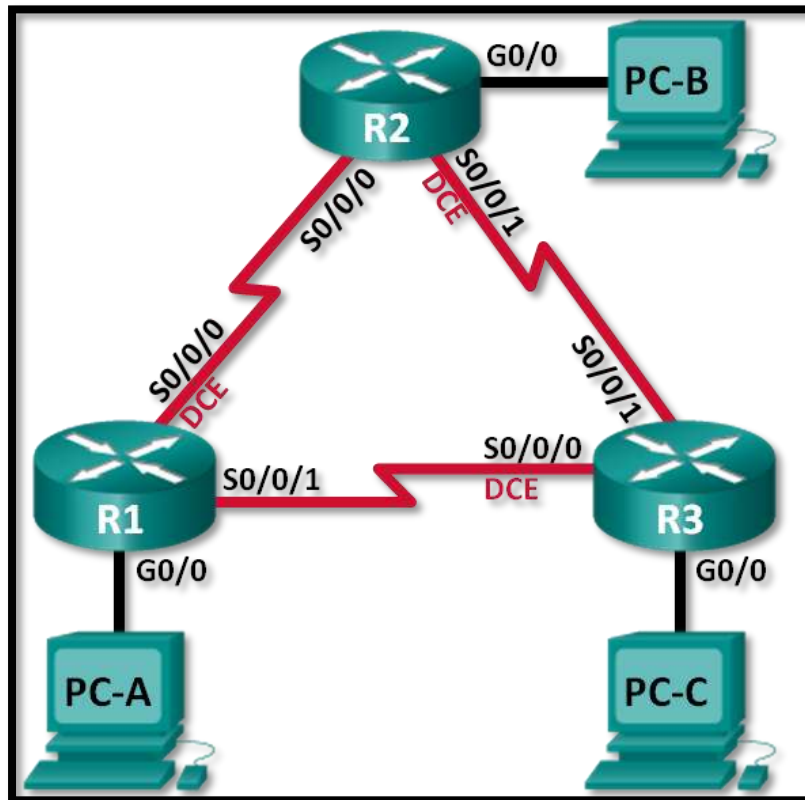
## Tabla de resumen de interfaces del router

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

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

## 8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2

### 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	255.255.255.2 52	N/A
	S0/0/1	192.168.13.1	255.255.255.2 52	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.2 52	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.2 52	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.2 52	N/A
	S0/0/1	192.168.23.2	255.255.255.2 52	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

## Objetivos

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

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

**Parte 3: cambiar las asignaciones de ID del router**

**Parte 4: configurar interfaces OSPF pasivas**

**Parte 5: cambiar las métricas de OSPF**

## Información básica/situación

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

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

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

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

### Recursos necesarios

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

### 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 consola y la contraseña de vty.
- e. Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.
- f. Configure **logging synchronous** para la línea de consola.
- g. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.
- i. Copie la configuración en ejecución en la configuración de inicio

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

**Step 5: Probar la conectividad.**

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

**Part 2: Configurar y verificar el enrutamiento OSPF**

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

**Step 1: Configure el protocolo OSPF en R1.**

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

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

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

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

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

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

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

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

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

```
R1#
```

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

```
R1#
```

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

```
R1#
```

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

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

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

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

```
R1#show ip ospf neighbor  
  
Neighbor ID      Pri   State           Dead Time   Address      Interface  
192.168.23.1     0     FULL/ -         00:00:39   192.168.12.2 Serial0/0/0  
192.168.23.2     0     FULL/ -         00:00:35   192.168.13.2 Serial0/0/1  
R1#
```

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

## R1# show ip route

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

Gateway of last resort is not set

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

```

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

Gateway of last resort is not set

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

```

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

- show ip route ospf

#### Step 4: verificar la configuración del protocolo OSPF.

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

```
R1# show ip protocols
```

```
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "ospf 1"
```

```
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set
```

```
Router ID 192.168.13.1
```

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

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Routing Information Sources:

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

Distance: (default is 110)

```
R1#show ip protocols

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

R1#
```

### Step 5: verificar la información del proceso OSPF.

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

R1# **show ip ospf**

Routing Process "ospf 1" with ID 192.168.13.1

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

Supports only single TOS(TOS0) routes

Supports opaque LSA  
Supports Link-local Signaling (LLS)  
Supports area transit capability  
Supports NSSA (compatible with RFC 3101)  
Event-log enabled, Maximum number of events: 1000, Mode: cyclic  
Router is not originating router-LSAs with maximum metric  
Initial SPF schedule delay 5000 msec  
Minimum hold time between two consecutive SPFs 10000 msec  
Maximum wait time between two consecutive SPFs 10000 msec  
Incremental-SPF disabled  
Minimum LSA interval 5 secs  
Minimum LSA arrival 1000 msec  
LSA group pacing timer 240 secs  
Interface flood pacing timer 33 msec  
Retransmission pacing timer 66 msec  
Number of external LSA 0. Checksum Sum 0x000000  
Number of opaque AS LSA 0. Checksum Sum 0x000000  
Number of DCbitless external and opaque AS LSA 0  
Number of DoNotAge external and opaque AS LSA 0  
Number of areas in this router is 1. 1 normal 0 stub 0 nssa  
Number of areas transit capable is 0  
External flood list length 0  
IETF NSF helper support enabled  
Cisco NSF helper support enabled  
Reference bandwidth unit is 100 mbps

#### Area BACKBONE(0)

Number of interfaces in this area is 3

Area has no authentication

SPF algorithm last executed 00:22:53.756 ago

SPF algorithm executed 7 times

Area ranges are



Number of LSA 3. Checksum Sum 0x019A61  
Number of opaque link LSA 0. Checksum Sum 0x000000  
Number of DCbitless LSA 0  
Number of indication LSA 0  
Number of DoNotAge LSA 0  
Flood list length 0

```
R1#show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 9 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x01b5a9
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
R1#
```

#### Step 6: verificar la configuración de la interfaz OSPF.

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

R1# **show ip ospf interface brief**

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

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

**R1# show ip ospf interface**

Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 192.168.13.1, Network Type POINT\_TO\_POINT, Cost: 64

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

Transmit Delay is 1 sec, State POINT\_TO\_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
oob-resync timeout 40

Hello due in 00:00:01

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2

Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up

Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 192.168.13.1, Network Type POINT\_TO\_POINT, Cost: 64

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

Transmit Delay is 1 sec, State POINT\_TO\_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
oob-resync timeout 40

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

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

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

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

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

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

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=36ms TTL=128
Reply from 192.168.3.3: bytes=32 time=16ms TTL=128
Reply from 192.168.3.3: bytes=32 time=0ms TTL=128
Reply from 192.168.3.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 13ms

PC>
```

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

### Part 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.

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

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

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

```
R1(config)#interface lo0
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#no shutdown
```

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

```
R2(config)#interface lo0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#no shutdown
```

```

R3(config)#interface lo0

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

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

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

```

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

R1# **show ip protocols**

\*\*\* IP Routing is NSF aware \*\*\*

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

**Router ID 1.1.1.1**

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

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Routing Information Sources:

Gateway	Distance	Last Update
3.3.3.3	110	00:01:00
2.2.2.2	110	00:01:14

Distance: (default is 110)

```
R1#show ip protocols

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

R1#
```

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

R1# **show ip ospf neighbor**

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

R1#

```
R1#show ip ospf neighbor

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

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

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

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

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

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

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

```
R1(config)# end
```

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

- b. Recibirá un mensaje informativo en el que se le indique que debe volver a cargar el router o usar el comando **clear ip ospf process** para que se aplique el cambio. Emita el comando **clear ip ospf process** en los tres routers. Escriba **yes** (sí) como respuesta al mensaje de verificación de restablecimiento y presione Enter.
- c. Establezca la ID del router R2 **22.22.22.22** y la ID del router R3 **33.33.33.33**. Luego, use el comando **clear ip ospf process** para restablecer el proceso de routing de OSPF.

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

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

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

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

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

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

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



R1# **show ip protocols**

\*\*\* IP Routing is NSF aware \*\*\*

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

**Router ID 11.11.11.11**

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

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

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

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

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

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

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

Distance: (default is 110)

```

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

```

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

**R1# show ip ospf neighbor**

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

```

R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
22.22.22.22     0     FULL/ -         00:00:30   192.168.12.2  Serial0/0/0
33.33.33.33     0     FULL/ -         00:00:30   192.168.13.2  Serial0/0/1
R1#

```

#### Part 4: configurar las interfaces pasivas de OSPF

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

##### Step 1: configurar una interfaz pasiva.

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

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

```
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
    0      1    no      no      Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
```

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

```
R1#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1#
```

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

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

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

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

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

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

```
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
```

0 1 no no Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
oob-resync timeout 40

**No Hellos (Passive interface)**

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

```
R1#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24, Area 0
Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R1#
```

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

R2# **show ip route**

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

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

Gateway of last resort is not set

2.0.0.0/32 is subnetted, 1 subnets

C 2.2.2.2 is directly connected, Loopback0

O 192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.2.0/24 is directly connected, GigabitEthernet0/0

L 192.168.2.1/32 is directly connected, GigabitEthernet0/0

O 192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1

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

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

L 192.168.12.2/32 is directly connected, Serial0/0/0

192.168.13.0/30 is subnetted, 1 subnets

O 192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1

[110/128] via 192.168.12.1, 00:58:32, Serial0/0/0

192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.23.0/30 is directly connected, Serial0/0/1

L 192.168.23.1/32 is directly connected, Serial0/0/1

```

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

Gateway of last resort is not set

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

```

R3#show ip route

```

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

```

Gateway of last resort is not set

```

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:07:41, Serial0/0/0

```

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

```

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

Gateway of last resort is not set

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

```



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

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

R1# **show ip ospf neighbor**

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

```
R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
22.22.22.22     0    FULL/ -         00:00:31   192.168.12.2 Serial0/0/0
33.33.33.33     0    FULL/ -         00:00:31   192.168.13.2 Serial0/0/1
R1#
```

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

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

R2(config-router)# **passive-interface default**

R2(config-router)#

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

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

```

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

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

R2(config-router)#

```

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

R1# **show ip ospf neighbor**

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

```

R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
33.33.33.33     0    FULL/ -         00:00:33   192.168.13.2  Serial0/0/1
R1#

```

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

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

Serial0/0/0 is up, line protocol is up

Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 22.22.22.22, Network Type POINT\_TO\_POINT, Cost: 64

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

0 64 no no Base

Transmit Delay is 1 sec, State POINT\_TO\_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
oob-resync timeout 40

**No Hellos (Passive interface)**

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

```
R2#show ip ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.2/30, Area 0
  Process ID 1, Router ID 22.22.22.22, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
R2#
```

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

```

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

Gateway of last resort is not set

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

```

R1#show ip route

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

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

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

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

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

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

P - periodic downloaded static route

Gateway of last resort is not set

1.0.0.0/32 is subnetted, 1 subnets

C 1.1.1.1/32 is directly connected, Loopback0

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

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

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

```

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

Gateway of last resort is not set

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

```

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

\* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route

Gateway of last resort is not set

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

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

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

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

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

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

```

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

```

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

```

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

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:00:57, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 00:19:27, Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
           [110/128] via 192.168.12.2, 00:00:57, Serial0/0/0
R1#

```

R1#show ip route

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

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

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

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
\* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route

Gateway of last resort is not set

1.0.0.0/32 is subnetted, 1 subnets  
C 1.1.1.1/32 is directly connected, Loopback0  
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks  
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0  
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0  
O 192.168.2.0/24 [110/65] via 192.168.12.2, 00:00:57, Serial0/0/0  
O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:19:27, Serial0/0/1  
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks  
C 192.168.12.0/30 is directly connected, Serial0/0/0  
L 192.168.12.1/32 is directly connected, Serial0/0/0  
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks  
C 192.168.13.0/30 is directly connected, Serial0/0/1  
L 192.168.13.1/32 is directly connected, Serial0/0/1  
192.168.23.0/30 is subnetted, 1 subnets  
O 192.168.23.0/30 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1  
[110/128] via 192.168.12.2, 00:00:57, Serial0/0/0  
R1#



```

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

Gateway of last resort is not set

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:20:16, Serial0/0/0
O       192.168.2.0/24 [110/129] via 192.168.13.1, 00:01:51, Serial0/0/0
       192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
       192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:07:41, Serial0/0/0
       192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/0
L       192.168.13.2/32 is directly connected, Serial0/0/0
       192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.2/32 is directly connected, Serial0/0/1
R3#

```

R3#show ip route

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

Gateway of last resort is not set

```

    3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:20:16, Serial0/0/0
O       192.168.2.0/24 [110/129] via 192.168.13.1, 00:01:51, Serial0/0/0

```

192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.3.0/24 is directly connected, GigabitEthernet0/0

L 192.168.3.1/32 is directly connected, GigabitEthernet0/0

192.168.12.0/30 is subnetted, 1 subnets

O 192.168.12.0/30 [110/128] via 192.168.13.1, 00:07:41, Serial0/0/0

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

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

L 192.168.13.2/32 is directly connected, Serial0/0/0

192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.23.0/30 is directly connected, Serial0/0/1

L 192.168.23.2/32 is directly connected, Serial0/0/1

R3#

¿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?

- Todo el tráfico hacia la red 192.168.2.0/24 desde el R3 se enrutará a través del R1.
- La interfaz S0/0/1 en el R2 sigue configurada como interfaz pasiva, por lo que la información de routing OSPF no se envía por esta interfaz.
- El costo acumulado de 129: Se debe a que el tráfico del R3 a la red 192.168.2.0/24 debe pasar a través de dos enlaces seriales T1 (1,544 Mb/s) (con un costo igual de 64 cada uno), además del enlace LAN Gigabit 0/0 del R2 (con un costo de 1).

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

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

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

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

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

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

Gateway of last resort is not set

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

```
R3#show ip route
```

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

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

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
\* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route

Gateway of last resort is not set

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

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

S0/0/1

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

- 65

Serial T1 (1,544 Mb/s) (con un costo de 64) + el enlace LAN Gigabit 0/0 del R2 (con un costo de 1).

¿El R2 aparece como vecino OSPF del R3?

SI

## Part 5: cambiar las métricas de OSPF

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

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

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

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

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

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

```
GigabitEthernet0/0 is up, line protocol is up
```

```
Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
```

```
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
```

```
Full Duplex, 100Mbps, media type is RJ45
```

```
output flow-control is unsupported, input flow-control is unsupported
```

```
ARP type: ARPA, ARP Timeout 04:00:00
```

Last input never, output 00:17:31, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue: 0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
0 packets input, 0 bytes, 0 no buffer  
Received 0 broadcasts (0 IP multicasts)  
0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
0 watchdog, 0 multicast, 0 pause input  
279 packets output, 89865 bytes, 0 underruns  
0 output errors, 0 collisions, 1 interface resets  
0 unknown protocol drops  
0 babbles, 0 late collision, 0 deferred  
1 lost carrier, 0 no carrier, 0 pause output  
0 output buffer failures, 0 output buffers swapped out

```

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

```

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

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

R1# **show ip route ospf**

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

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

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

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

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

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

Gateway of last resort is not set

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

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

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

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

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

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1

Topology-MTID Cost Disabled Shutdown Topology Name

0 1 no no Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40



Hello due in 00:00:05  
Supports Link-local Signaling (LLS)  
Cisco NSF helper support enabled  
IETF NSF helper support enabled  
Index 1/1, flood queue length 0  
Next 0x0(0)/0x0(0)  
Last flood scan length is 0, maximum is 0  
Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 0, Adjacent neighbor count is 0  
Suppress hello for 0 neighbor(s)

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

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

R1# **show ip ospf interface s0/0/1**

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

oob-resync timeout 40  
Hello due in 00:00:04  
Supports Link-local Signaling (LLS)  
Cisco NSF helper support enabled  
IETF NSF helper support enabled  
Index 3/3, flood queue length 0  
Next 0x0(0)/0x0(0)  
Last flood scan length is 1, maximum is 1  
Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 1, Adjacent neighbor count is 1  
Adjacent with neighbor 192.168.23.2  
Suppress hello for 0 neighbor(s)

```
R1#show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 33.33.33.33
  Suppress hello for 0 neighbor(s)
R1#
```

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

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

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

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

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

Please ensure reference bandwidth is consistent across all routers.

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

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

```
GigabitEthernet0/0 is up, line protocol is up
```

```
Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
```

```
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
```

```
Topology-MTID Cost Disabled Shutdown Topology Name
```

```
0 10 no no Base
```

```
Transmit Delay is 1 sec, State DR, Priority 1
```

```
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
```

```
No backup designated router on this network
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
oob-resync timeout 40
```

```
Hello due in 00:00:02
```

```
Supports Link-local Signaling (LLS)
```

```
Cisco NSF helper support enabled
```

```
IETF NSF helper support enabled
```

```
Index 1/1, flood queue length 0
```

```
Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 0, maximum is 0
```

```
Last flood scan time is 0 msec, maximum is 0 msec
```

```
Neighbor Count is 0, Adjacent neighbor count is 0
```

```
Suppress hello for 0 neighbor(s)
```

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

R1# **show ip ospf interface s0/0/1**

Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 1.1.1.1, Network Type POINT\_TO\_POINT, Cost: 6476

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	6476	no	no	Base

Transmit Delay is 1 sec, State POINT\_TO\_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40

Hello due in 00:00:05

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2

Suppress hello for 0 neighbor(s)

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

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

R1# **show ip route ospf**

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

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

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

Gateway of last resort is not set

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

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

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

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

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

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

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

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

Esto se hace con el fin de calcular exactamente las métricas con los datos correctos, recordemos que estos equipos calculan los mismos con datos predeterminados.

## Step 2: cambiar el ancho de banda de una interfaz.

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

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

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

```
R1# show interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
```

```
Hardware is WIC MBRD Serial
```

```
Internet address is 192.168.12.1/30
```

```
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation HDLC, loopback not set
```

```
Keepalive set (10 sec)
```

```
<Output Omitted>
```

```

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

```

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

R1# **show ip route ospf**

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

Gateway of last resort is not set

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

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

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

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

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

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

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

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



Gateway of last resort is not set

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

192.168.23.0/30 is subnetted, 1 subnets

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

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

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

R1# **show ip ospf interface brief**

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

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

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

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

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

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

Gateway of last resort is not set

- O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1  
 192.168.23.0/30 is subnetted, 1 subnets
- O 192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1  
 [110/845] via 192.168.12.2, 00:00:09, Serial0/0/0

```

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

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

Costo a 192.168.3.0/24:

- S0/0/1 del R1 + G0/0 del R3 (781+1=782).

Costo a 192.168.23.0/30:

- S0/0/1 del R1 y S0/0/1 del R3 (781+64=845).

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

R3# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

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

Gateway of last resort is not set

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

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

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

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

¿Cuál es el nuevo costo acumulado a la red 192.168.23.0/24 en el R1? ¿Por qué?  
1562.

Cada enlace serial tiene un costo de 781 y la ruta a la red 192.168.23.0/24 atraviesa dos enlaces seriales.

781 + 781 = 1562.

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

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

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

#### R1# show ip route ospf

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

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

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

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

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

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

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

+ - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0

O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1

[110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0

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

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

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

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

```
R1(config)#int s 0/0/1
R1(config-if)#ip ospf cost 1565
R1(config-if)#
```

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

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

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

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

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

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

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

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

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

+ - replicated route, % - next hop override

Gateway of last resort is not set

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

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

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

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

OSPF elige la ruta con el menor costo acumulado. La ruta con el menor costo acumulado es:

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

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

De esta manera observamos claramente cual de estas es la ruta con menor costo acumulado.

### Reflexión

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

El ID es el que permite la elección del router ID y BDR.

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

Este es fundamental en su configuración para las redes de acceso multiple.

¿Por qué querría configurar una interfaz OSPF como pasiva?

Para no enviar información de ruteo innecesaria.

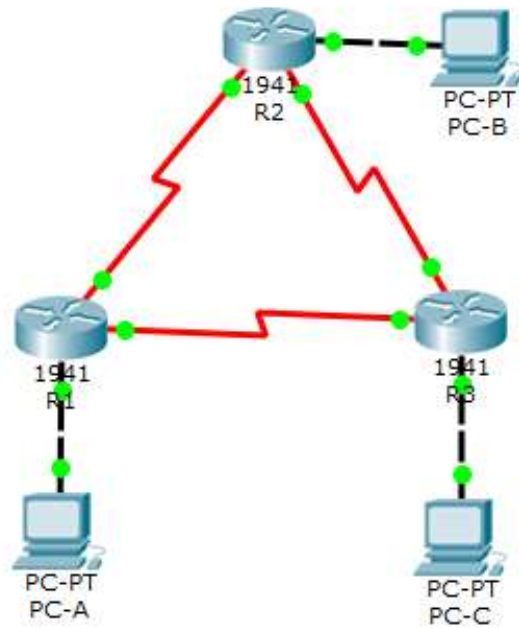
## Tabla de resumen de interfaces del router

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

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

### 8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3

#### ➤ Topología



➤ **Tabla de direccionamiento**

<b>Dispositivo</b>	<b>Interfaz</b>	<b>Dirección IPv6</b>	<b>Gateway predeterminado</b>
<b>R1</b>	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
<b>R2</b>	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



<b>R3</b>	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
<b>PC-A</b>	NIC	2001:DB8:ACAD:A::A/64	FE80::1
<b>PC-B</b>	NIC	2001:DB8:ACAD:B::B/64	FE80::2
<b>PC-C</b>	NIC	2001:DB8:ACAD:C::C/64	FE80::3

➤ **Objetivos**

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

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

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

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

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

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

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

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de vty.
- e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- f. Configure **logging synchronous** para la línea de consola.

```
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable password class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging syn
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

- g. Cifre las contraseñas de texto no cifrado.
- h. Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.
- i. Habilite el routing de unidifusión IPv6 en cada router.
- j. Copie la configuración en ejecución en la configuración de inicio

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

#### **Paso 5: Probar la conectividad.**

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

```

R2>en
Password:
R2#ping 2001:db8:acad:b::b

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:b::b, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/8 ms

R2#ping 2001:db8:acad:12::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:12::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/23 ms

R2#ping 2001:db8:acad:23::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:23::3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/24 ms

R2#

```

## ➤ Parte 2: configurar el routing OSPFv3

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

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

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

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

```

R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#

```

**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)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#

```

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

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

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

- 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
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
R2#
```

## Paso 2: configurar OSPFv6 en el R1.

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

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

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

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

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

```

R2(config)#int g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#int s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#
R2(config-if)#
02:01:40: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 ospf 1 area 0

```

```

R3(config)#int g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int s0/0/1
02:05:33: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
02:05:45: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to
FULL, Loading Done

```

### Paso 3: verificar vecinos de OSPFv3.

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

```

%SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 ospf neighbor

```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
2.2.2.2	0	FULL/ -	00:00:37	3	Serial0/0/0
3.3.3.3	0	FULL/ -	00:00:38	3	Serial0/0/1

```

R1#

```

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

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

```

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

```

### Paso 5: verificar las interfaces OSPFv3.

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

```

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

```

- Para mostrar un resumen de las interfaces con OSPFv3 habilitado, emita el comando **show ipv6 ospf interface brief**. (PK No soporta el comando)

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

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



```

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

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

Se debería poder hacer ping entre todas las computadoras de la topología.

```

Pinging 2001:db8:acad:b::b with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=15ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 15ms, Average = 4ms

PC>ping 2001:db8:acad:c::c

Pinging 2001:db8:acad:c::c with 32 bytes of data:

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

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 3ms

```

### ➤ Parte 3: configurar las interfaces pasivas de OSPFv3

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

#### Paso 1: configurar una interfaz pasiva.

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

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

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

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

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

```

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

```

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

```

```

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

```

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

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

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
02:51:40: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

02:51:40: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Interface down or detached
```

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

```
R1#show ipv6 ospf neighbor

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

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

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

- d. Si todas las interfaces OSPFv3 en el R2 son pasivas, no se anuncia ninguna información de routing. Si este es el caso, el R1 y el R3 ya no deberían tener una ruta a la red 2001:DB8:ACAD:B::/64. Esto se puede verificar mediante el comando **show ipv6 route**.
- e. Ejecute el comando **no passive-interface** para cambiar S0/0/1 en el R2 a fin de que envíe y reciba actualizaciones de routing OSPFv3. Después de introducir este

comando, aparece un mensaje informativo que explica que se estableció una adyacencia de vecino con el R3.

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
03:01:26: %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?

Usa el serial s0/0/1

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

Para llegar a la red B desde R1 el costo acumulado es de 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?

Que todo el tráfico hacia a la red 2001:DB8:ACAD:B::/64 Desde el R1 se enruta a través de R3. La interfaz S0/0/0 en el r2 sigue configurada como interface pasiva por lo que la información de routing OSPFv3 no se anuncia en esta interface. El costo acumulado de 129 debe a que el tráfico de R3 a la red 192.168.2.0/24 debe pasar de los dos enlaces seriales.

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

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#
03:12:06: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

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

```

R2#show ipv6 ospf neighbor
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
3.3.3.3         0    FULL/ -         00:00:33   4             Serial0/0/1
1.1.1.1         0    FULL/ -         00:00:39   3             Serial0/0/0
R2#

```

## ➤ 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 se puede intercambiar la información de ruteo entre ambos; ya que la ID del proceso OSPFv3 se usa solo localmente en el router, no es necesario que coincida con cada ID del proceso que se usa en los otros router.

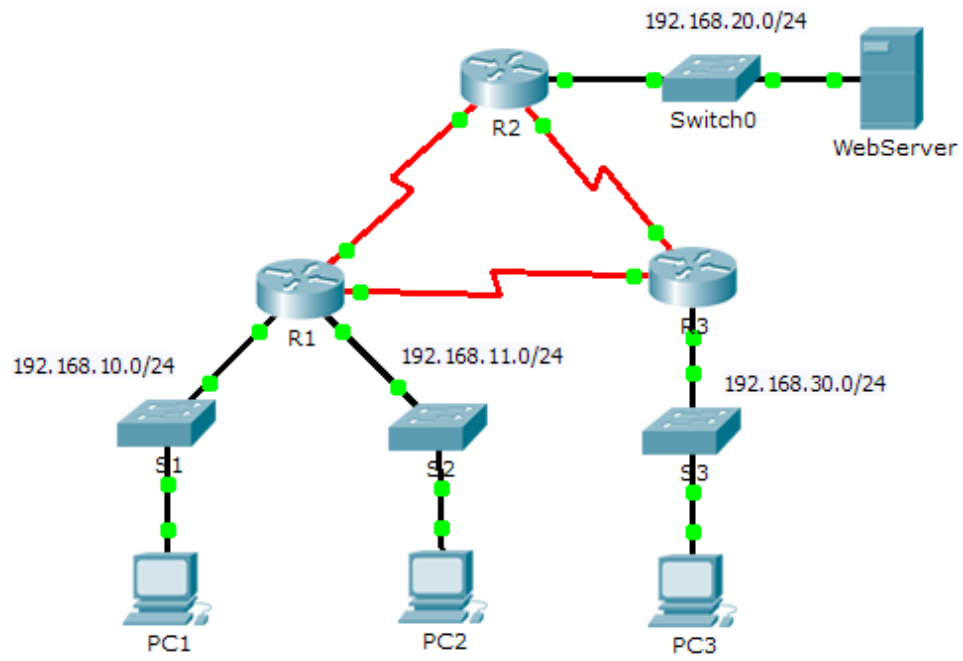
2. ¿Cuál podría haber sido la razón para eliminar el comando **network** en OSPFv3?

Eliminar las instrucciones **network** ayuda a evitar errores en las direcciones IPv6.

Además, una interface IPv6 pueden tener multiples direcciones IP asignadas a ella. Al asignar una interface a un área OSPFv3 todas las redes multicast en esa interface y tendrán una ruta creada en la tabla de ruteo de IPv6.

### 9.2.1.10 Packet Tracer Configuring Standard ACLs Instructions IG

#### Topology



## Addressing Table

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

### Objectives

#### Part 1: Plan an ACL Implementation

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

### Background / Scenario

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

#### Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.

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

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

a. The following network policies are implemented on **R2**:

- The 192.168.11.0/24 network is not allowed access to the **WebServer** on the 192.168.20.0/24 network.
- All other access is permitted.

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

b. The following network policies are implemented on **R3**:

- The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.10.0/24 network to the 192.168.30.0/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must be placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

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

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

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

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

b. By default, an access list denies all traffic that does not match a rule. To permit all

other traffic, configure the following statement:

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

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

```
R2(config)# interface GigabitEthernet0/0
```

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

```
R2>en
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#interface g0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

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

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

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

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

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

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

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

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

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

Step 3: Verify ACL configuration and functionality.

- a. On **R2** and **R3**, enter the **show access-list** command to verify the ACL



configurations. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.

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

R2

Physical	Config	CLI	Attributes
----------	--------	-----	------------

IOS Command Line Interface

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

```
R2#
R2#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.20.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
--More--
```

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

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
access-list 1 deny 192.168.10.0 0.0.0.255
access-list 1 permit any
!
R3#
R3#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
 Internet address is 192.168.30.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is 1
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
--More--
```

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

- A ping from 192.168.10.10 to 192.168.11.10 succeeds.

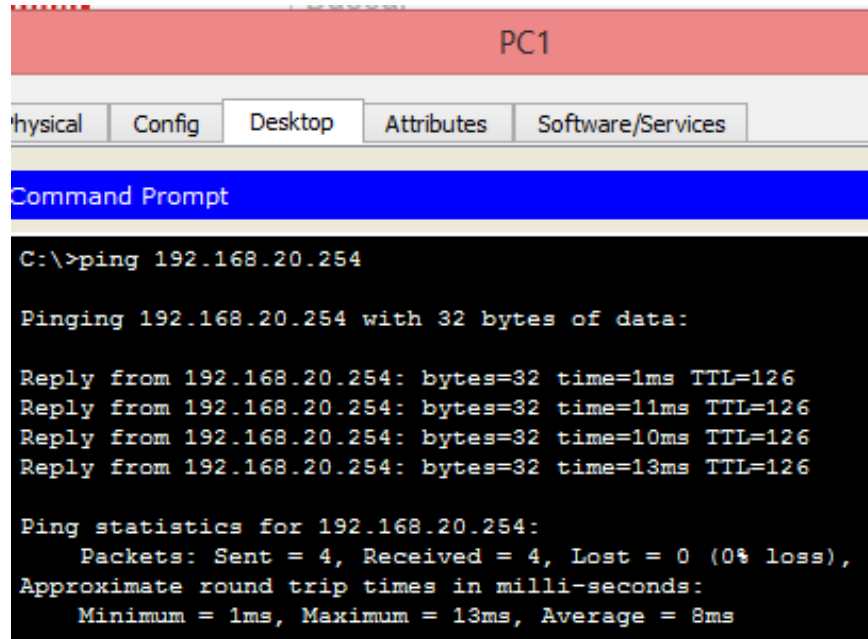
```
PC1
Physical Config Desktop Attributes Software/Services
Command Prompt
Pinging 192.168.11.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

192

- A ping from 192.168.10.10 to 192.168.20.254 succeeds.



The screenshot shows a network simulation window for PC1. The window has tabs for Physical, Config, Desktop, Attributes, and Software/Services. The Desktop tab is active, displaying a Command Prompt. The Command Prompt shows the execution of the command 'ping 192.168.20.254'. The output indicates that the ping was successful, with four replies received from 192.168.20.254. The ping statistics show that all four packets were received, with a 0% loss rate. The approximate round trip times in milliseconds are: Minimum = 1ms, Maximum = 13ms, and Average = 8ms.

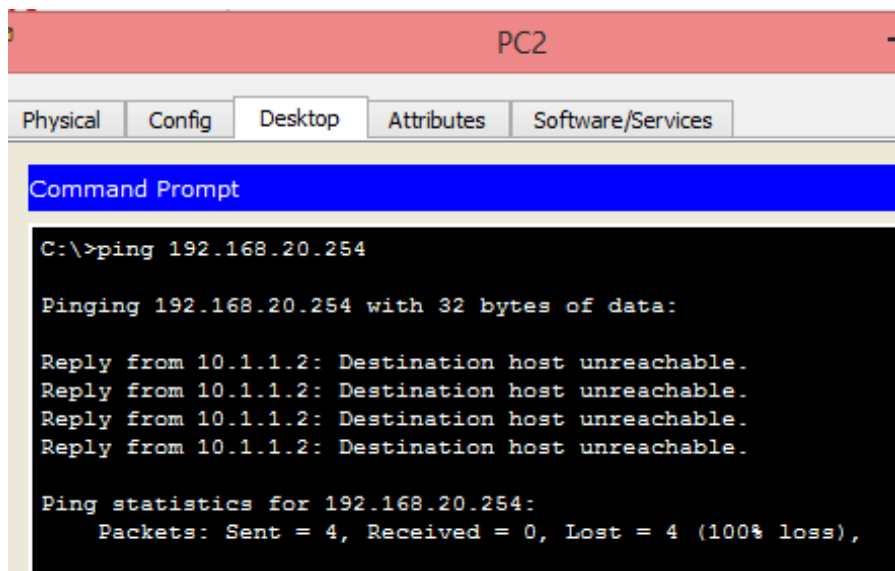
```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=11ms TTL=126
Reply from 192.168.20.254: bytes=32 time=10ms TTL=126
Reply from 192.168.20.254: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 8ms
```

- A ping from 192.168.11.10 to 192.168.20.254 fails.



The screenshot shows a network simulation window for PC2. The window has tabs for Physical, Config, Desktop, Attributes, and Software/Services. The Desktop tab is active, displaying a Command Prompt. The Command Prompt shows the execution of the command 'ping 192.168.20.254'. The output indicates that the ping failed, with four replies received from 10.1.1.2, all stating 'Destination host unreachable'. The ping statistics show that all four packets were lost, with a 100% loss rate.

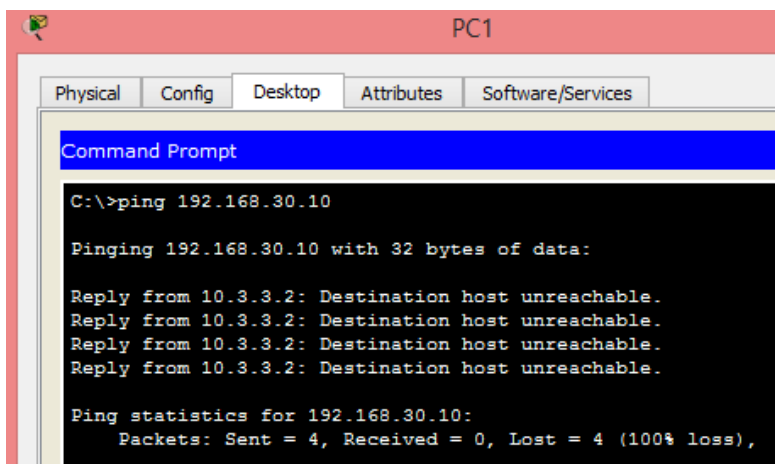
```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

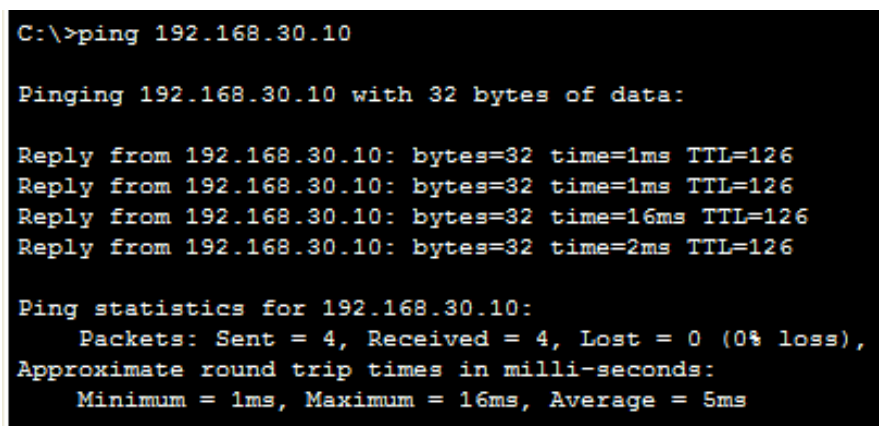
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

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

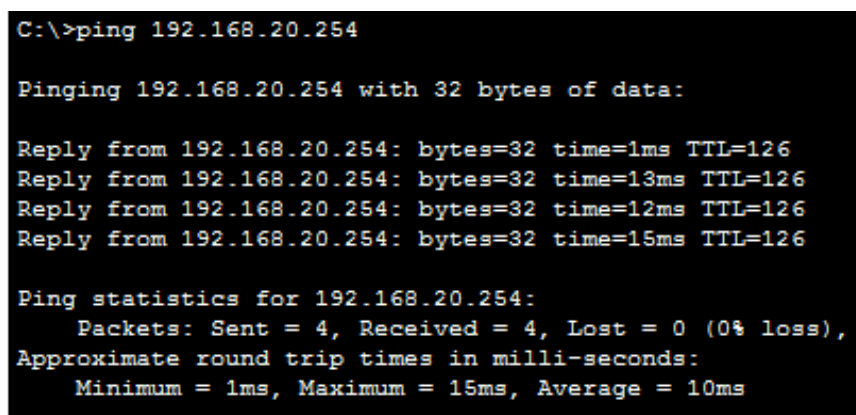
- A ping from 192.168.10.10 to 192.168.30.10 fails.



- A ping from 192.168.11.10 to 192.168.30.10 succeeds.



- A ping from 192.168.30.10 to 192.168.20.254 succeeds.



Activity Results Time Elapsed: 00:37:01

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points
Network		
R2		
ACL		0
1	Correct	25
Ports		0
GigabitEthernet0/0		0
Access-grou...	Correct	25
R3		
ACL		0
1	Correct	25
Ports		0
GigabitEthernet0/0		0
Access-grou...	Correct	25

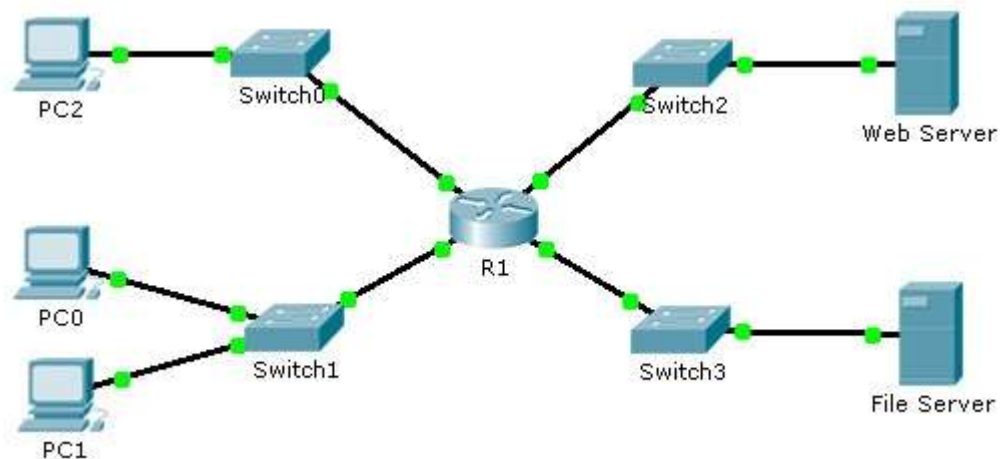
Score : 100/100

Item Count : 4/4

Component	Items/Total	Score
IPv4 Standard ACL Implementation	4/4	100/100

### 9.2.1.11 Packet Tracer - Configuring Named Standard ACLs Instructions IG

#### Topología



#### Tabla de direcciones

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

### Objetivos

**Parte 1: Configurar y aplicar una ACL estándar con nombre**  
**Parte 2: Verificar la implementación del ACL**

### Escenario

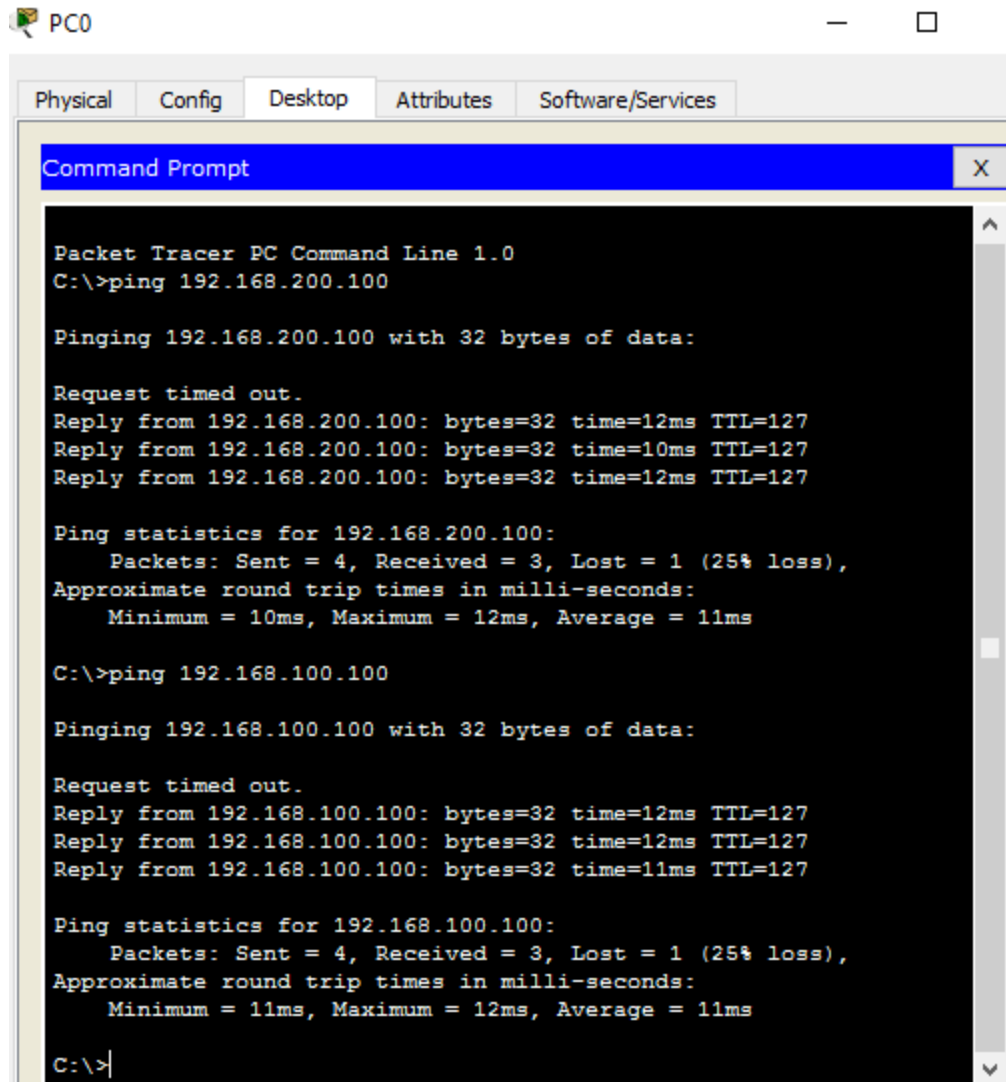
El administrador de red senior le ha encargado que cree un ACL de nombre estándar para impedir el acceso a un servidor de archivos. Se debe denegar el acceso a todos los clientes de una red y una estación de trabajo específica de una red diferente.

### Parte 1: Configurar y aplicar una ACL estándar con nombre

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

Las tres estaciones de trabajo deben poder hacer ping tanto en el servidor Web como en el servidor de archivos.

Realizamos el ping desde PC0 (192.168.20.3) primero a File Server (192.168.200.100) y luego a Web Server (192.168.100.100)



The screenshot shows a Packet Tracer PC Command Line window for PC0. The window has tabs for Physical, Config, Desktop, Attributes, and Software/Services. The Command Prompt is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time=12ms TTL=127
Reply from 192.168.200.100: bytes=32 time=10ms TTL=127
Reply from 192.168.200.100: bytes=32 time=12ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms

C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms

C:\>|
```

R/ en los dos casos el ping es satisfactorio.

Ahora desde PC2 (192.168.10.3) primero a File Server (192.168.200.100) y luego a Web Server (192.168.100.100)

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=11ms TTL=127
Reply from 192.168.200.100: bytes=32 time=11ms TTL=127
Reply from 192.168.200.100: bytes=32 time=12ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 8ms

C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=11ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 8ms

C:\>
```

R/ en los dos casos el ping es satisfactorio.

## **Paso 2: Configure una ACL estándar nombrada.**

Configure la siguiente ACL con nombre en R1.

Ingresamos a R1 para permitir que la lista de acceso permita el paso de la PC1 (192.168.20.4) y niegue cualquier otro tráfico

```
R1>en
R1#conf t
```



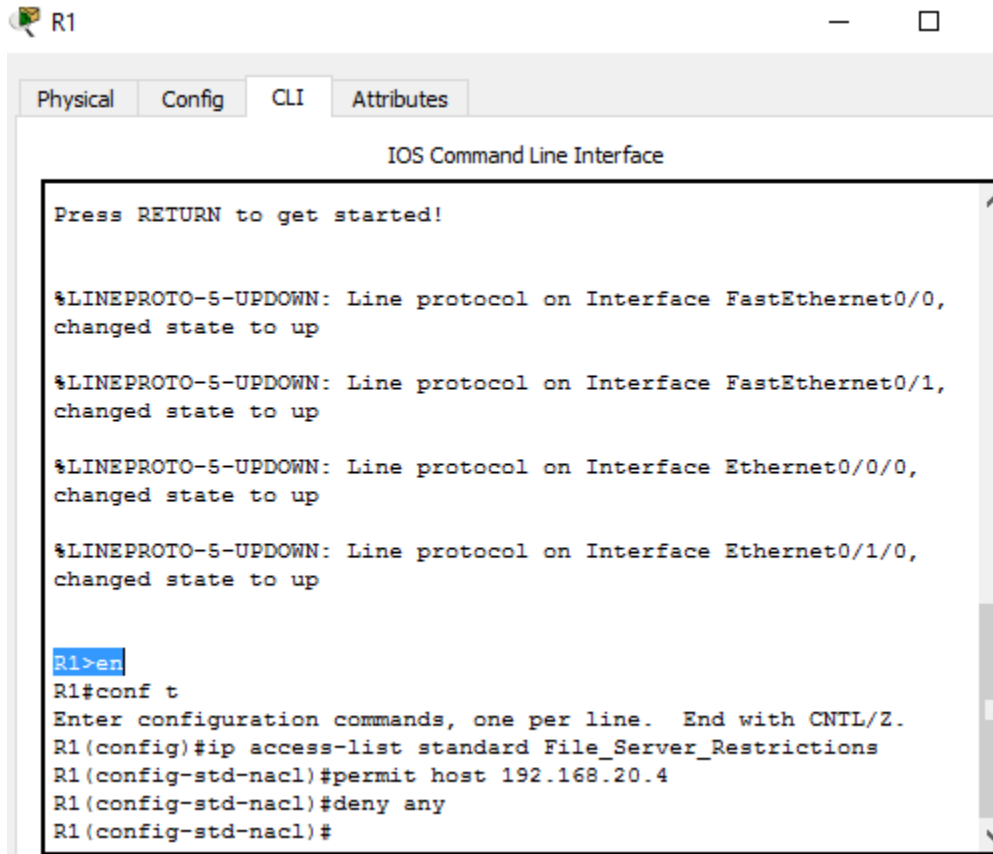
Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#ip access-list standard File_Server_Restrictions
```

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

```
R1(config-std-nacl)#deny any
```

```
R1(config-std-nacl)#
```



The screenshot shows a window titled 'R1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output includes the following text:

```
Press RETURN to get started!  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,  
changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,  
changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0,  
changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1/0,  
changed state to up  
  
R1>en  
R1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#ip access-list standard File_Server_Restrictions  
R1(config-std-nacl)#permit host 192.168.20.4  
R1(config-std-nacl)#deny any  
R1(config-std-nacl)#
```

**Nota:** Para propósitos de puntuación, el nombre ACL distingue entre mayúsculas y minúsculas

### Paso 3: Aplicar la ACL nombrada.

- a. Aplicar la ACL de salida en la interfaz Fast Ethernet 0/1.

```
R1(config-std-nacl)#exit
```

```
R1(config)#int f0/1
```

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

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

```
R1(config)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#
```

- b. Guardar la configuración.

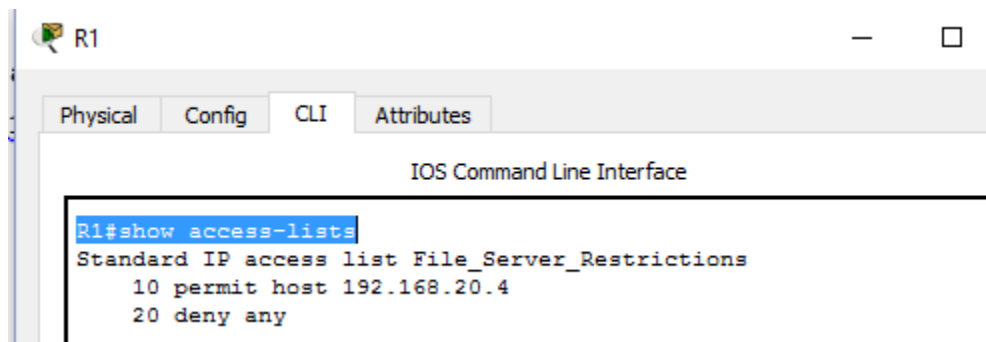
```
R1(config-if)#end
```

## Part 2: Verificar la implementación del ACL

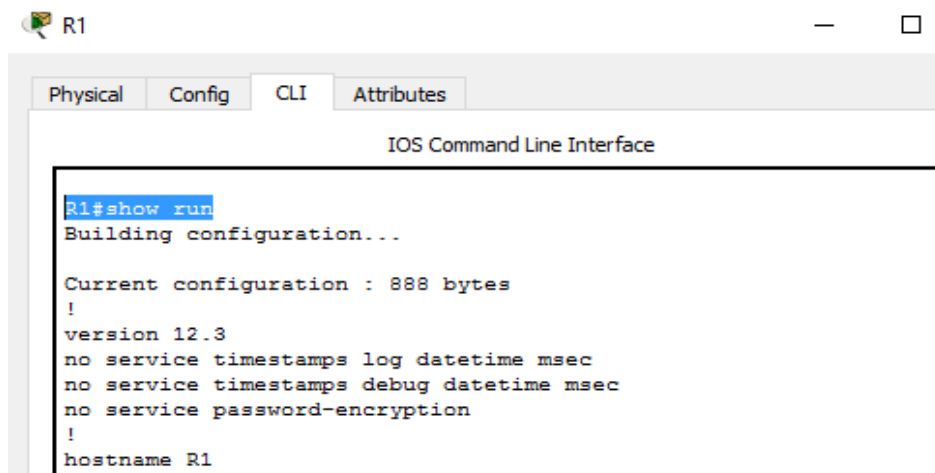
### Paso 1: Verificar la configuración y la aplicación de ACL en la interfaz.

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

Ingresamos nuevamente a R1 para ver las configuraciones



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1#show access-lists
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.20.4
 20 deny any
```



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1#show run
Building configuration...

Current configuration : 888 bytes
!
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
.
```

Y podemos comprobar las restricciones de la configuración realizada previamente

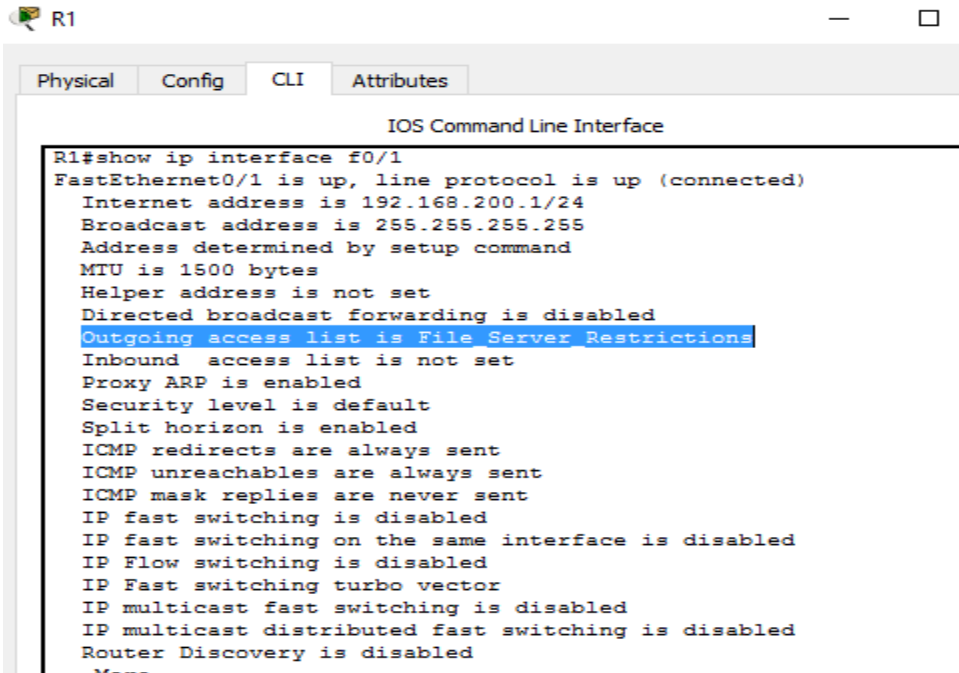


The image shows two screenshots of a Cisco IOS CLI interface. The top screenshot shows the configuration of an access list named 'File Server Restrictions'. The bottom screenshot shows the configuration of interface FastEthernet0/1, where the access list is applied to the output traffic.

```
!
!
!
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard File Server Restrictions
 permit host 192.168.20.4
 deny any
!
```

```
!
!
!
interface FastEthernet0/0
 ip address 192.168.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.200.1 255.255.255.0
 ip access-group File Server Restrictions out
 duplex auto
 speed auto
!
```

Ahora revisamos para interface F0/1



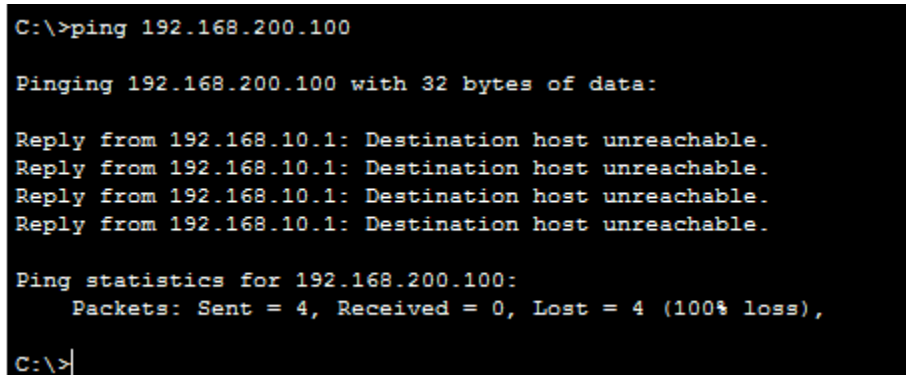
```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1#show ip interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
 Internet address is 192.168.200.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is File Server Restrictions
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is disabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP Fast switching turbo vector
 IP multicast fast switching is disabled
 IP multicast distributed fast switching is disabled
 Router Discovery is disabled
 V----
```

**Paso 2: Compruebe que la ACL funciona correctamente.**

Las tres estaciones de trabajo deben poder hacer ping al servidor Web, pero sólo PC1 debe poder hacer ping al servidor de archivos.

Hacemos ping desde todas las terminales ping hacia File Server o servidor de archivos (192.168.200.100)

Iniciamos con PC2



```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

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

C:\>
```

R/ El ping falla

Ahora desde PC0 a File Server

```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

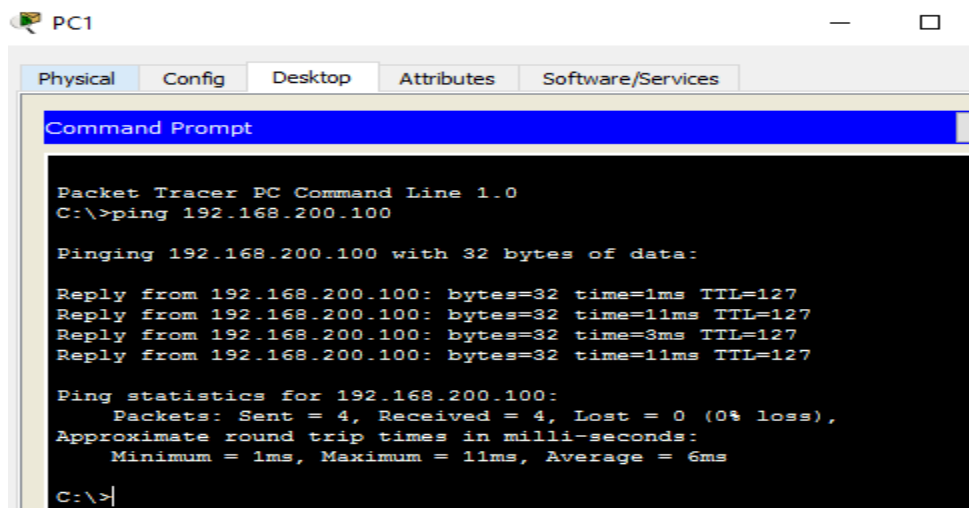
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

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

C:\>
```

R/ El ping falla

Probamos desde PC1



```
PC1
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=11ms TTL=127
Reply from 192.168.200.100: bytes=32 time=3ms TTL=127
Reply from 192.168.200.100: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 6ms

C:\>
```

R/ El ping es satisfactorio

Ahora probamos con el Servidor web haciendo ping desde las tres estaciones.

Desde PC0 a WebServer (192.168.100.100)

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=13ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 6ms

C:\>|
```

R/ El ping es satisfactorio

Desde PC1 a WebServer (192.168.100.100)

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=11ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>|
```

R/ El ping es satisfactorio

## Desde PC2 a WebServer (192.168.100.100)

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=13ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 7ms

C:\>
```

R/ El ping es satisfactorio

Se comprueba que todas las estaciones PC0, PC1 y PC2 pueden hacer ping a Web Server pero únicamente la PC1 hace ping a File Server o servidor de archivos.

Lista de resultados

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:31:29

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

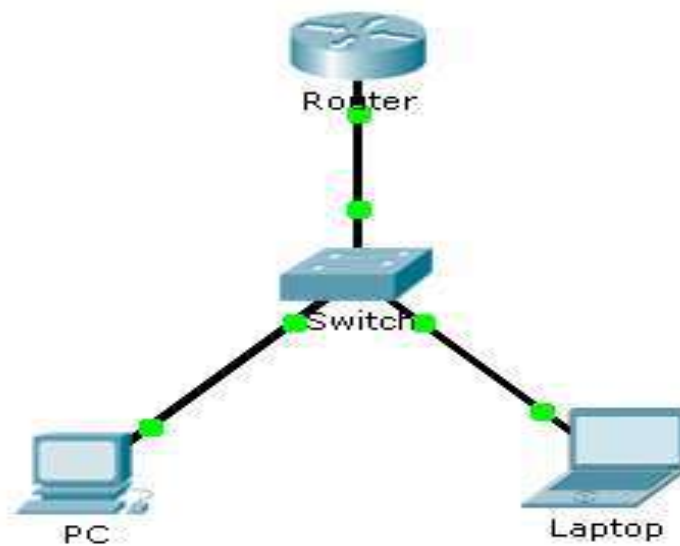
Assessment Items	Status	Points
Network		
R1		
ACL		0
File_Server_Restri...	Correct	80
Ports		0
FastEthernet0/1		0
Access-group ...	Correct	20

Component	Items/Total	Score
IPv4 Standard ACL Implementation	2/2	100/100

Score : 100/100  
Item Count : 2/2

### 9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines Instructions IG

#### Topology



#### Addressing Table

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



## 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.

```
Pinging 10.0.0.254 with 32 bytes of data:
Reply from 10.0.0.254: bytes=32 time=2ms
Reply from 10.0.0.254: bytes=32 time=0ms
Reply from 10.0.0.254: bytes=32 time=0ms
Reply from 10.0.0.254: bytes=32 time=1ms

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Reply from 10.0.0.1: bytes=32 time=0ms TTL=64
Reply from 10.0.0.1: bytes=32 time=0ms TTL=64
Reply from 10.0.0.1: bytes=32 time=0ms TTL=64

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0
```

```
Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=1ms TTL=64
Reply from 10.0.0.254: bytes=32 time=1ms TTL=64
Reply from 10.0.0.254: bytes=32 time=0ms TTL=64
Reply from 10.0.0.254: bytes=32 time=0ms TTL=64

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

PC>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=5ms TTL=64
Reply from 10.0.0.1: bytes=32 time=12ms TTL=64
Reply from 10.0.0.1: bytes=32 time=0ms TTL=64
Reply from 10.0.0.1: bytes=32 time=9ms TTL=64

Ping statistics for 10.0.0.1:
```

Cisco Packet Tracer Student - C:\Users\USER\Desktop\CISCO\OSCAR\9.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines.pka

File Edit Options View Tools Extensions Help

## Activity Results

Time Elapsed: 00:14:11

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points
Network		
Router		
ACL		0
✓ 99	Correct	70
VTY Lines		
VTY Line 0		0
✓ Access Contro...	Correct	6
VTY Line 1		0
✓ Access Contro...	Correct	6
VTY Line 2		0
✓ Access Contro...	Correct	6
VTY Line 3		0
✓ Access Contro...	Correct	6
VTY Line 4		0
✓ Access Contro...	Correct	6

Score : 100/100  
Item Count : 6/6

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

Close

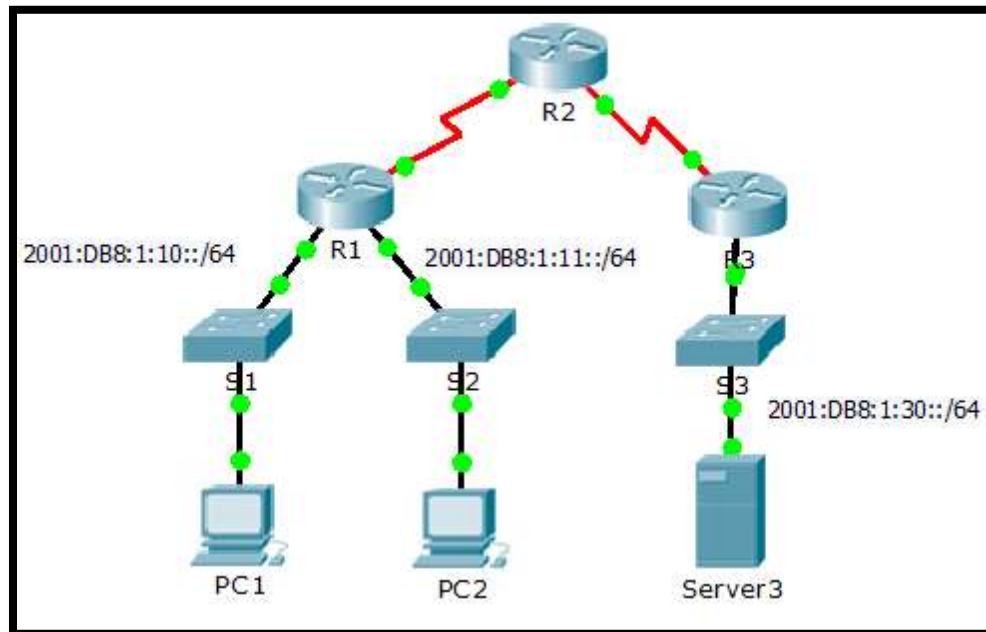
## CONCLUSIONES DEL EJERCICIO

- ✓ (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.

### 9.5.2.6 Packet Tracer - Configuring IPv6 ACLs Instructions IG

#### Topology



#### Addressing Table

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

#### Objectives

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

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

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

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can

be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

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

Configure an ACL named **BLOCK\_HTTP** on R1 with the following statements.

a. Block HTTP and HTTPS traffic from reaching **Server3**.

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

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

b. Allow all other IPv6 traffic to pass.

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

### Step 2: Apply the ACL to the correct interface.

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

```
R1(config)# interface GigabitEthernet0/1
```

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

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list block http
      ^
% Invalid input detected at '^' marker.

R1(config)#ipv6 access-list BLOCK HTTP
      ^
% Invalid input detected at '^' marker.

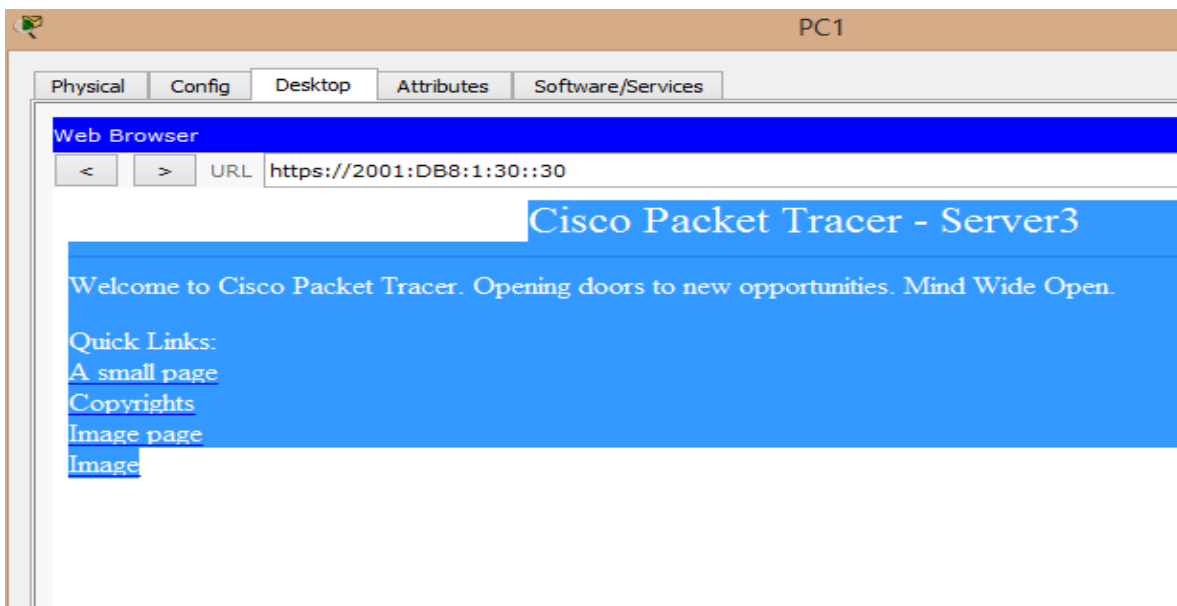
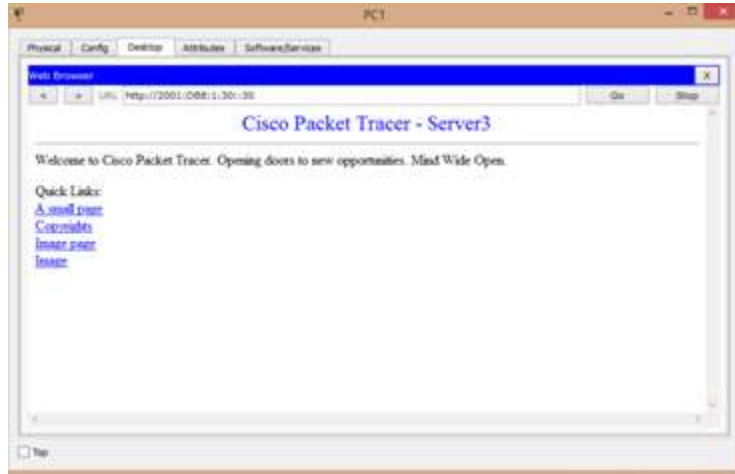
R1(config)#IPV6 ACCESS-LIST BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#EXIT
R1(config)#INT G0/1
R1(config-if)#IPV6 TRAFFIC-FILTER BLOCK
% Incomplete command.
R1(config-if)#IPV6 TRAFFIC-FILTER BLOCK_HTTP IN
R1(config-if)#
```

### Step 3: Verify the ACL implementation.

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

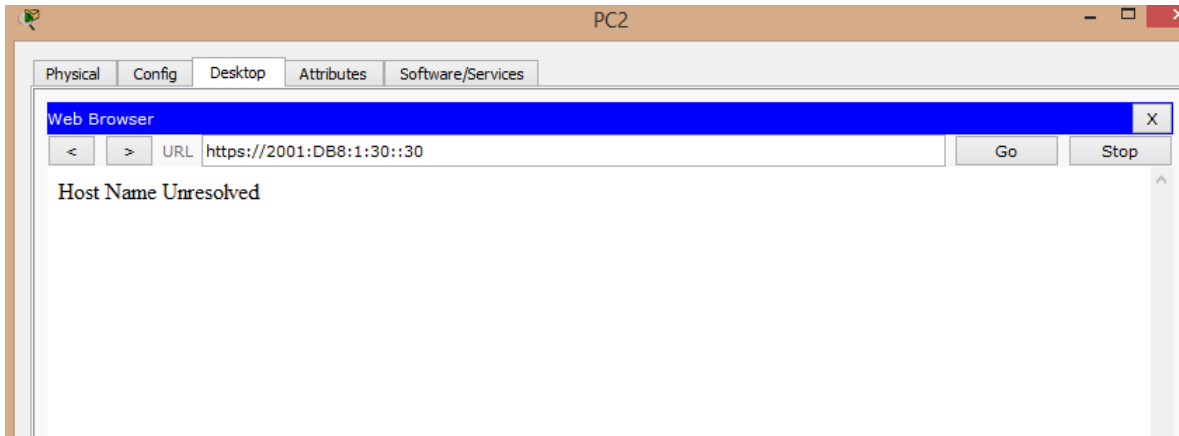
- Open the **web browser** of **PC1** to <http://2001:DB8:1:30::30> or <https://2001:DB8:1:30::30>.

The website should appear.

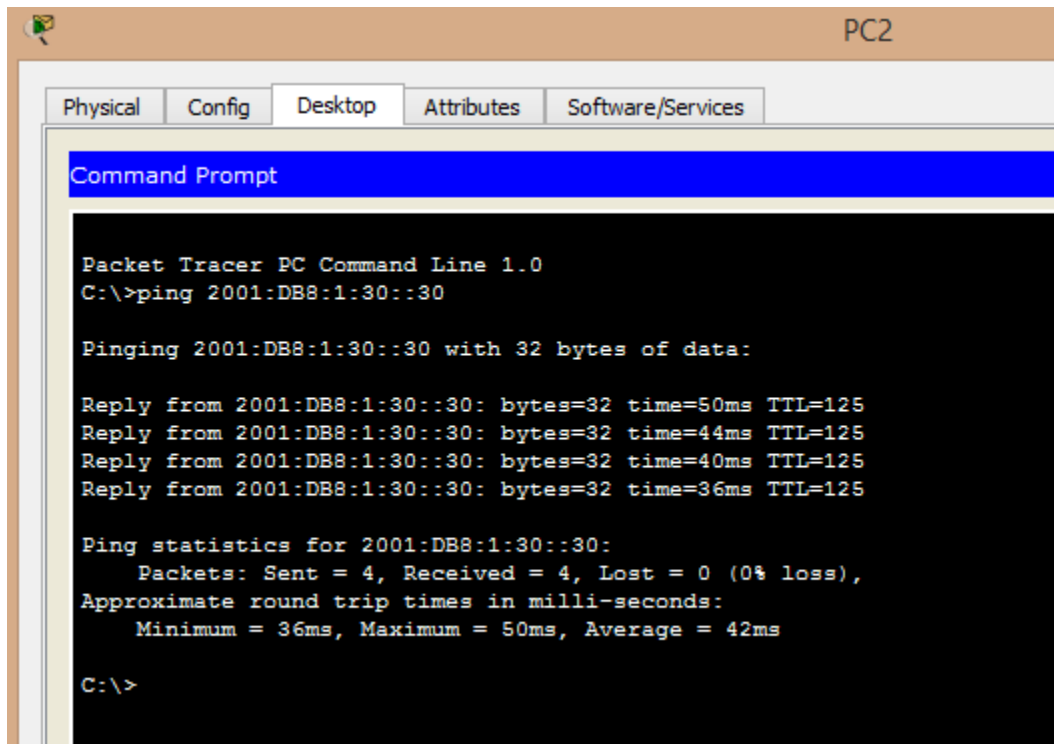


- Open the **web browser** of **PC2** to <http://2001:DB8:1:30::30> or <https://2001:DB8:1:30::30>.

The website should be blocked



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



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

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

### Step 1: Create an access list to block ICMP.

Configure an ACL named **BLOCK\_ICMP** on **R3** with the following statements:

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

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


b. Allow all other IPv6 traffic to pass.

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



```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#EXIT
R3(config)#show run
-
! Invalid input detected at "" marker.
R3(config)#sh run
-
! Invalid input detected at "" marker.
R3(config)#end
R3#
ADVISE-0-COMMID_1: Configured from console by console
R3#show run
Building configuration...

Current configuration : 1395 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
```



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

Current configuration : 2035 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
interface Serial0/0/0
 no ip address
 clock rate 1000000
 shutdown
!
interface Serial0/0/1
 no ip address
 ipv6 address FE85::8 link-local
 ipv6 address 2001:2001:1:2::1/64
 ipv6 mlag 1
!
interface Vlan1
 no ip address
 shutdown
!
ipv6 router mlag 1
 mlag router-id 3.3.3.3
 no shutdown
!
ip classless
ip flow-export version 9
!
ipv6 access-list BLOCK_ICMP
 deny icmp any any
 permit ipv6 any any
!
!
!
!
line con 0
line aux 0
line vty 0 4
```

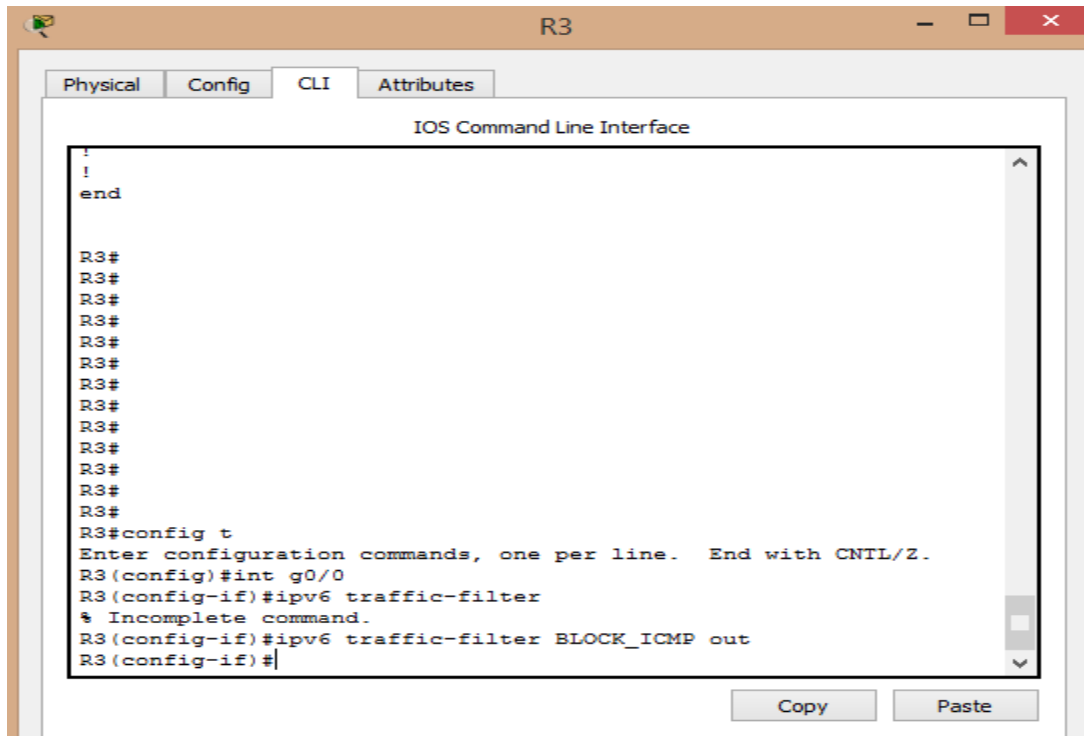
**Step 2: Apply the ACL to the correct interface.**



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

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

R3(config-if)# **ipv6 traffic-filter BLOCK\_ICMP out**



### Step 3: Verify that the proper access list functions.

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

```
PC2
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 2001:DB8:1:30::30

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

Reply from 2001:DB8:1:30::30: bytes=32 time=50ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=44ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=40ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=36ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 50ms, Average = 42ms

C:\>ping 2001:DB8:1:30::30

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

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

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

C:\>
```

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

```
PC1
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:30::30

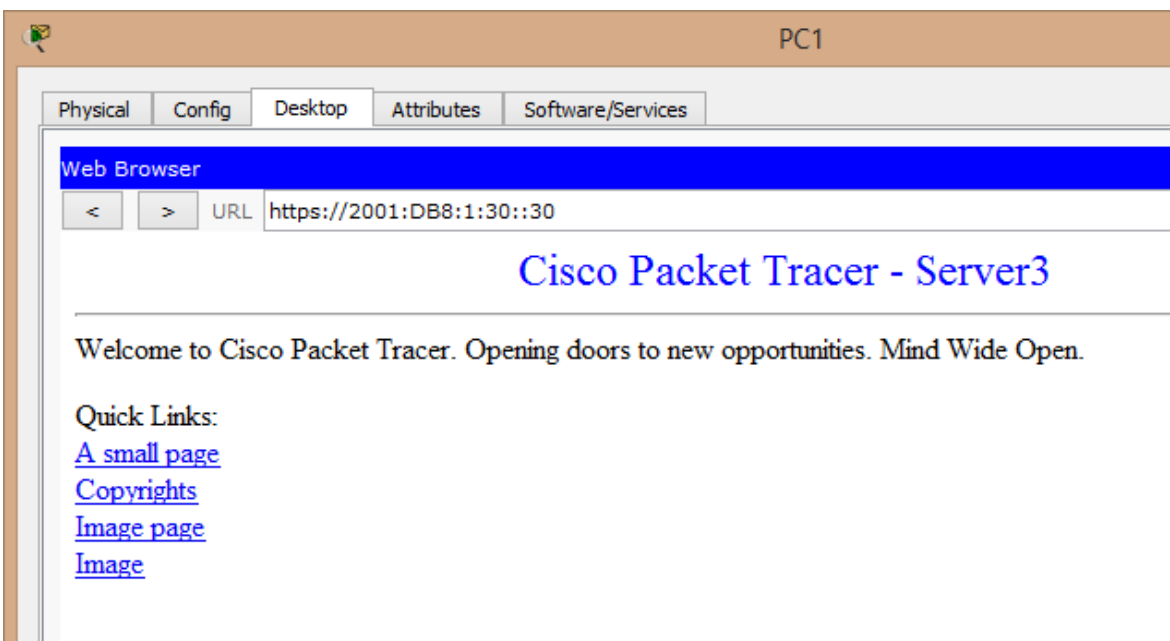
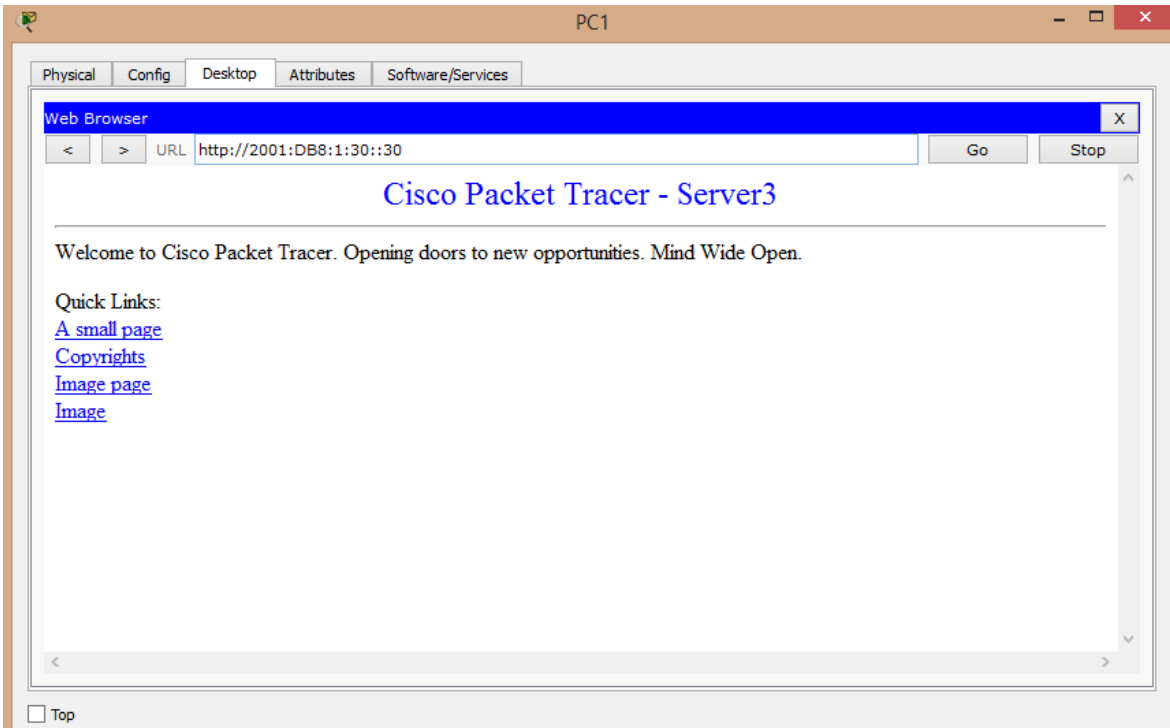
Pinging 2001:DB8:1:30::30 with 32 bytes of data:

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

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

C:\>|
```

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



## TABLA DE RESULTADOS

Cisco Packet Tracer - D:\1. UNAD iNG sIST\001- UNAD ULT SEMESTRE\01- Diplomado\producto\trab c...

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:14:34

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

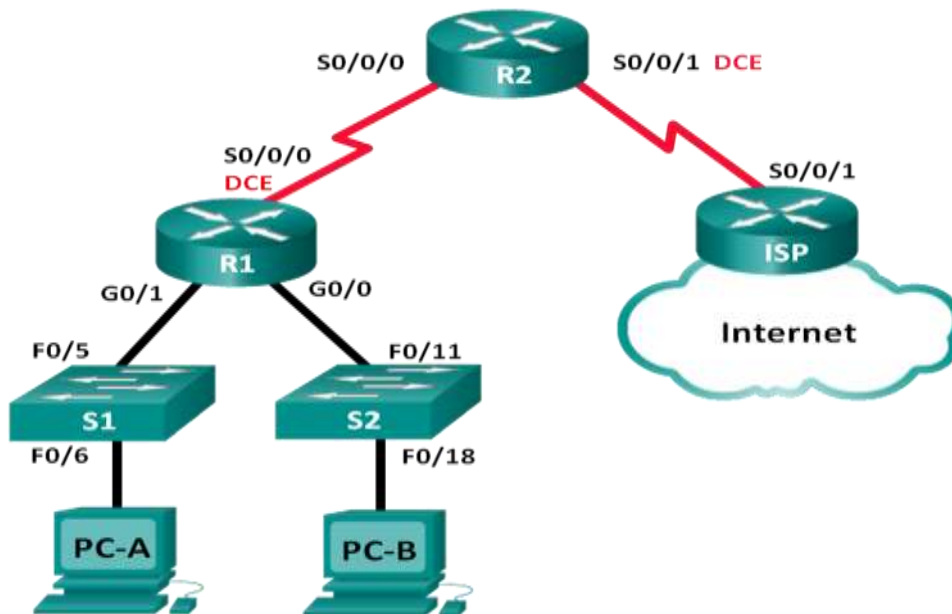
Assessment Items	Status	Points
Network		
R1		
ACLV6		0
BLOCK_HTTP	Correct	40
Ports		0
GigabitEthernet0/1		0
IPv6 Traffic Filte...	Correct	10
R3		
ACLV6		0
BLOCK_ICMP	Correct	40
Ports		0
GigabitEthernet0/0		0
IPv6 Traffic Filte...	Correct	10

Component	Items/Total	Score
IPv6 ACL Implementation	4/4	100/100

Score : 100/100  
Item Count : 4/4

### 10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router

#### Topologia



#### 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	255.255.255.2 52	N/A
R2	S0/0/0	192.168.2.254	255.255.255.2 52	N/A
	S0/0/1 (DCE)	209.165.200.2 26	255.255.255.2 24	N/A
ISP	S0/0/1	209.165.200.2 25	255.255.255.2 24	N/A
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

## Objetivos

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

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

## Información básica/situación

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

En esta situación, la empresa creció en tamaño, y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su tarea es configurar

el router R2 para asignar direcciones IPv4 en dos subredes diferentes conectadas al router R1.

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

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

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

### **Recursos necesarios**

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

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

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

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

**Paso 2. Inicializar y volver a cargar los routers y los switches.**

**Paso 3. Configurar los parámetros básicos para cada router.**

- d. Desactive la búsqueda DNS.
- e. Configure el nombre del dispositivo como se muestra en la topología.
- f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- g. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- h. Configure **logging synchronous** para evitar que los mensajes de consola interrumpen la entrada de comandos.
- i. Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.
- j. Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.

Para R1

```
Router>en
```

```
Router#conf t
```

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

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

```
Router(config)#hostname R1
```

```
R1(config)#enable secret class
```

```
R1(config)#line console 0
```

```
R1(config-line)#password cisco
```

```
R1(config-line)#logging syn
```

```
R1(config-line)#logging synchronous
```

```
R1(config-line)#login
```

```
R1(config-line)#exit
```

```
R1(config)#line vty 0 15
```

```
R1(config-line)#password cisco
```

```
R1(config-line)#login
```

```
R1(config-line)#exit
```

```
R1(config)#banner motd%
```

```
^
```

% Invalid input detected at '^' marker.

R1(config)#banner motd %

Enter TEXT message. End with the character '%'.  
prohibido el acceso no autorizado%

R1(config)#service password-encryption

R1(config)#int

R1(config)#interface g0/0

R1(config-if)#ip address 192.168.0.1 255.255.255.0

R1(config-if)#no shu

R1(config-if)#no shutdown

R1(config-if)#

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

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

R1(config-if)#interface g0/1

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

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

R1(config-if)#cl

R1(config-if)#clock rate 128000



```
R1(config-if)#ip address 192.168.2.253 255.255.255
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
R1(config-if)#ip address 192.168.2.253 255.255.252
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
R1(config-if)#ip address 192.168.2.253 255.255.255.252
```

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

```
R1#copy running-config startup-config
```

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

```
Building configuration...
```

```
[OK]
```

```
R1#
```

## **Para R2**

```
Router>en
```

```
Router#conf t
```

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

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

```
Router(config)#hostname R2
```

```
R2(config)#enable secret class
```

```
R2(config)#line console 0
```

```
R2(config-line)#password cisco
```

```
R2(config-line)#logging syn
```

```
R2(config-line)#logging synchronous
```

```
R2(config-line)#login
```

```
R2(config-line)#exit
```

```
R2(config)#line vty 0 15
```

```
R2(config-line)#password cisco
```

```
R2(config-line)#login
```

```
R2(config-line)#exit
```

```
R2(config)#banner motd %
```

Enter TEXT message. End with the character '%'.  
prohibido el acceso no autorizado

prohibido el acceso no autorizado%

R2(config)#int

R2(config)#interface

% Incomplete command.

R2(config)#service password-enc

R2(config)#service password-encryption

R2(config)#int

R2(config)#interface s0/0/0

R2(config-if)#ip address 192.168.2.254 255.255.255.252

R2(config-if)#no sh

R2(config-if)#no shutdown

R2(config-if)#

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

R2(config-if)#int s0

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

R2(config-if)#int s0/0/1

R2(config-if)#clo

R2(config-if)#clock rate 128000

R2(config-if)#ip address 209.165.200.226 255.255.255.224

R2(config-if)#no shutdown

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

R2(config-if)#

R2>en

Password:

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

### **Para ISP**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#logging sy
ISP(config-line)#logging synchronous
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#banner motd %
Enter TEXT message. End with the character '%'.
prohibido el acceso no autorizado%

ISP(config)#int s0/0/1
ISP(config-if)#ip address 209.165.200.255 255.255.255.224
Bad mask /27 for address 209.165.200.255
```

ISP(config-if)#ip address 209.165.200.225 255.255.255.224

ISP(config-if)#no sh

ISP(config-if)#no shutdown

ISP(config-if)#

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

ISP(config-if)#

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

ISP(config-if)#exit

ISP(config)#exit

ISP#

%SYS-5-CONFIG\_I: Configured from console by console

ISP#copy ru

ISP#copy running-config st

ISP#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

ISP#

h. Configure EIGRP for R1.

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

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

R1(config-router)# **network 192.168.1.0 0.0.0.255**

R1(config-router)# **network 192.168.2.252 0.0.0.3**

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

```

R1
-----
Physical  Config  CLI
-----
IOS Command Line Interface

R1#conf t
Enter configuration commands, one per line. End with
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy ru
R1#copy running-config
% Incomplete command.
R1#copy running-config st
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#en
R1#conf t
Enter configuration commands, one per line. End with
R1(config)#router eigrp 1
R1(config-router)#network 192.168.0.0 0.0.0.255
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 192.168.2.252 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#

```

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

```

R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.252 0.0.0.3
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225

```

```

R2
-----
Physical  Config  CLI
-----
IOS Command Line Interface

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

R2(config-router)#redistribute static
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

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

```

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

```

ISP (config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226

```

```
ISP
Physical Config CLI
IOS Command Line Interface
prohibido el acceso no autorizado
User Access Verification
Password:
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)#exit
ISP#
%SYS-5-CONFIG_I: Configured from console by console
ISP#copy r
ISP#copy running-config st
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

**Paso 4: verificar la conectividad de los routers.**

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

```
ISP#ping 192.168.2.253
```

Type escape sequence to abort.

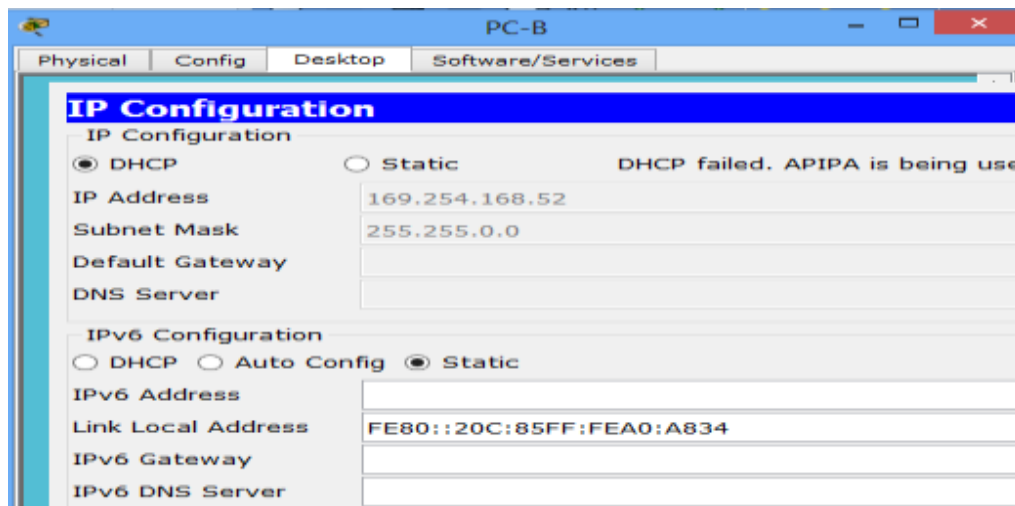
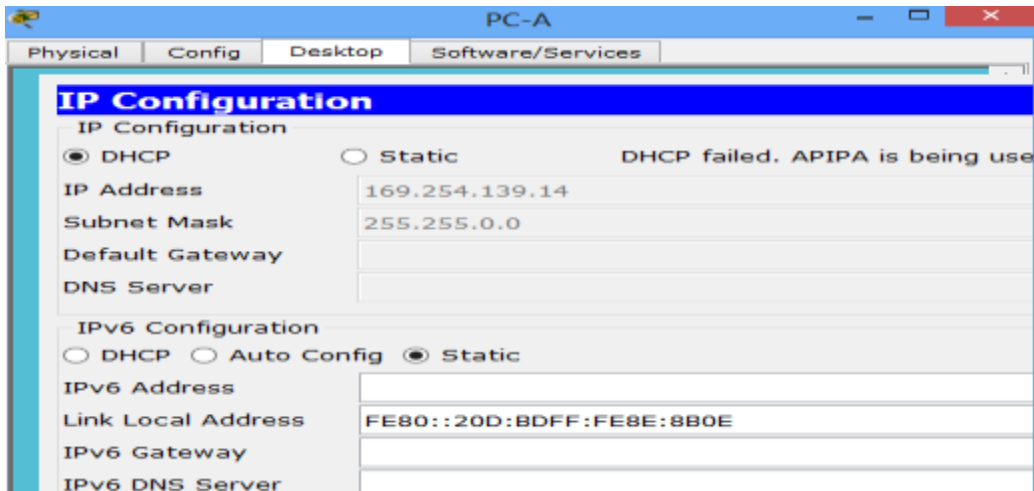
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2 seconds:

```
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms

```
ISP#
```

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



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

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

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

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

Excluya las primeras nueve direcciones en cada LAN del R1; empiece por .1. El resto de las direcciones deben estar disponibles en el conjunto de direcciones DHCP. Asegúrese de que cada conjunto de direcciones DHCP incluya un gateway predeterminado, el dominio 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>en
```

```
Password:
```

```
R2#conf t
```

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

```
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
```

```
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
```

```
R2(config)#ip dhcp pool R1G1
```

```
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
```

```
R2(dhcp-config)#default-router 192.168.1.1
```

```
R2(dhcp-config)#dns-server 209.165.200.225
```

```
R2(dhcp-config)#exit
```

```
R2(config)#ip dhcp pool R1G0
```

```
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
```

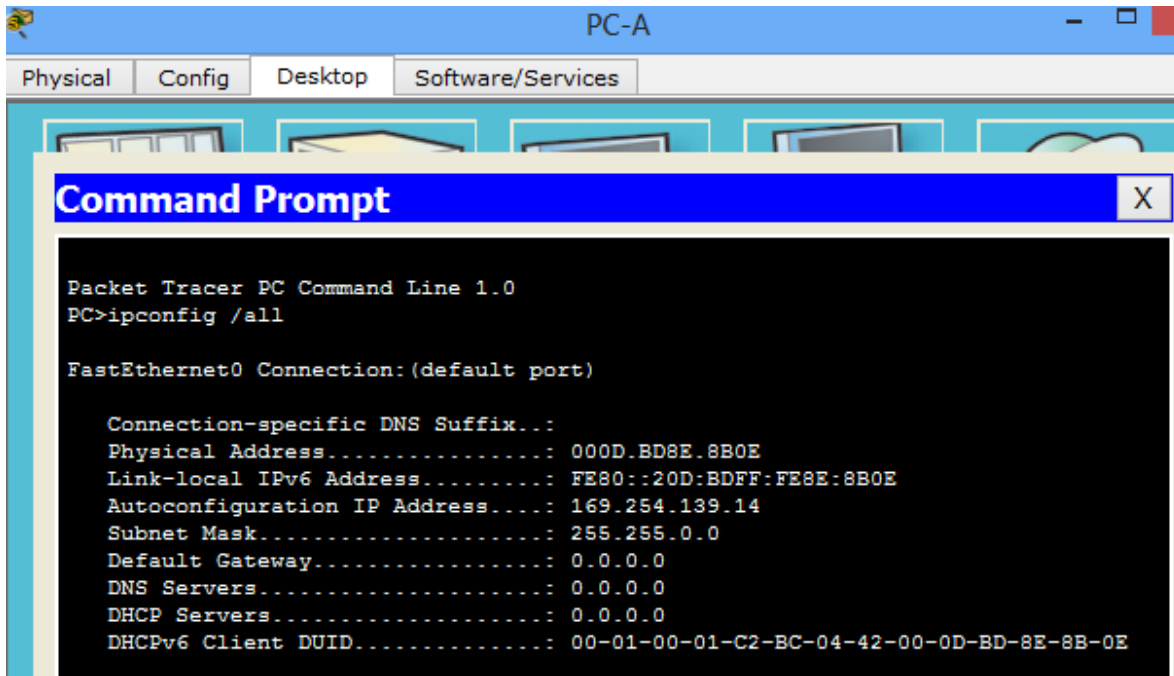
```
R2(dhcp-config)#default-router 192.168.0.1
```

```
R2(dhcp-config)#dns-server 209.165.200.225
```

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

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





No porque el R2 se encuentra en otra red.

## **Paso 2: configurar el R1 como agente de retransmisión DHCP.**

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

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

```
R1>en
```

```
Password:
```

```
R1#conf t
```

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

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

```
R1(config-if)#ip helper-address 192.168.2.254
```

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

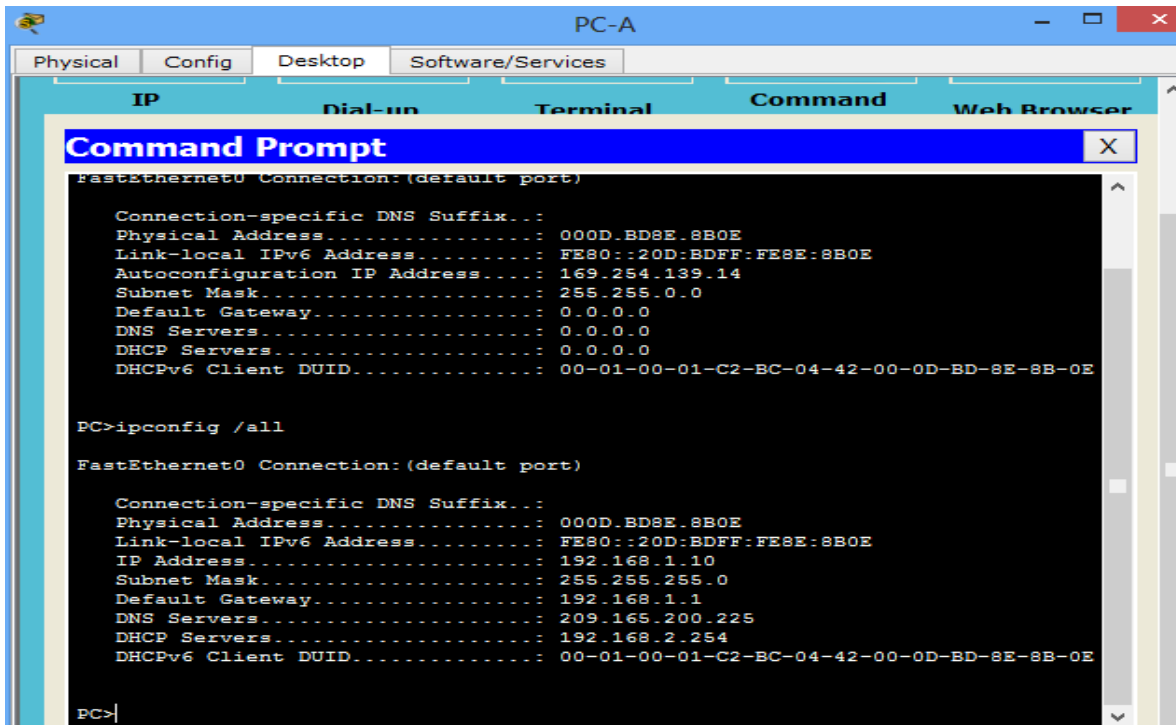
```
R1(config)#interface g0/1
```

```
R1(config-if)#ip helper-address 192.168.2.254
```

R1(config-if)#

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

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



```
PC-B
Physical Config Desktop Software/Services
Command Prompt
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix... :
Physical Address..... : 000C-85A0-A834
Link-local IPv6 Address..... : FE80::20C:85FF:FEA0:A834
Autoconfiguration IP Address... : 169.254.168.52
Subnet Mask..... : 255.255.0.0
Default Gateway..... : 0.0.0.0
DNS Servers..... : 0.0.0.0
DHCP Servers..... : 0.0.0.0
DHCPv6 Client DUID..... : 00-01-00-01-40-96-1A-D9-00-0C-85-A0-A8-34

PC>ipconfig /all

FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix... :
Physical Address..... : 000C-85A0-A834
Link-local IPv6 Address..... : FE80::20C:85FF:FEA0:A834
IP Address..... : 192.168.0.10
Subnet Mask..... : 255.255.255.0
Default Gateway..... : 192.168.0.1
DNS Servers..... : 209.165.200.225
DHCP Servers..... : 192.168.2.254
DHCPv6 Client DUID..... : 00-01-00-01-40-96-1A-D9-00-0C-85-A0-A8-34

PC>
```

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

Para la PC-A: 192.168.1.10

Para la PC-B: 192.168.0.10

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

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

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

```
prohibido el acceso no autorizado
prohibido el acceso no autorizado
User Access Verification
Password:
R2>en
Password:
R2#show ip dhcp binding
IP address      Client-ID/      Lease expiration      Type
Hardware address
192.168.1.10    000D.BD8E.8B0E    --                     Automatic
192.168.0.10    000C.85A0.A834    --                     Automatic
R2#
```

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?

Packet Tracer no acepta este comando.

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)?

Packet Tracer no acepta este comando.

```
prohibido el acceso no autorizado
prohibido el acceso no autorizado
User Access Verification
Password:
R2>en
Password:
R2#show ip dhcp binding
IP address      Client-ID/      Lease expiration      Type
                Hardware address
192.168.1.10    000D.BD8E.8B0E    --                     Automatic
192.168.0.10    000C.85A0.A834    --                     Automatic
R2#show ip dhcp server statistics
^
% Invalid input detected at '^' marker.
R2#show ip dhcp pool
^
% Invalid input detected at '^' marker.
```

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

Packet Tracer no acepta este comando `show run | section dhcp`.

Pero si acepta `show run`

```
R2#show run | section dhcp
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
R2#show run
```

```
Building configuration...
```

```
Current configuration : 1463 bytes
```

```
!
```

```
version 15.1
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
service password-encryption
!
hostname R2
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 209.165.200.225
ip dhcp pool R1G0
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 209.165.200.225
!
no ip cef
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX15242D5Z
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
```

```
shutdown
!  
interface GigabitEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
  
!  
interface Serial0/0/0  
ip address 192.168.2.254 255.255.255.252  
  
!  
interface Serial0/0/1  
ip address 209.165.200.226 255.255.255.224  
clock rate 128000  
  
!  
interface Vlan1  
no ip address  
shutdown  
  
!  
router eigrp 1  
redistribute static  
network 192.168.2.252 0.0.0.3  
  
  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 209.165.200.225  
  
!  
ip flow-export version 9  
  
!  
banner motd ^C  
prohibido el acceso no autorizado
```

```
prohibido el acceso no autorizado^C
!  
line con 0  
password 7 0822455D0A16  
logging synchronous  
login  
!  
line aux 0  
!  
line vty 0 4  
password 7 0822455D0A16  
login  
line vty 5 15  
    password 7 0822455D0A16  
    login  
!  
end  
R2#
```

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

En R2 no funciona si no en R1.

```
R1#show ip interface g0/0  
GigabitEthernet0/0 is up, line protocol is up (connected)  
Internet address is 192.168.0.1/24  
Broadcast address is 255.255.255.255  
Address determined by setup command  
MTU is 1500 bytes
```



Helper address is 192.168.2.254  
Directed broadcast forwarding is disabled  
Outgoing access list is not set  
Inbound access list is not set  
Proxy ARP is enabled  
Security level is default  
Split horizon is enabled  
ICMP redirects are always sent  
ICMP unreachable are always sent  
ICMP mask replies are never sent  
IP fast switching is disabled  
IP fast switching on the same interface is disabled  
IP Flow switching is disabled  
IP Fast switching turbo vector  
IP multicast fast switching is disabled  
IP multicast distributed fast switching is disabled  
Router Discovery is disabled  
IP output packet accounting is disabled  
IP access violation accounting is disabled  
TCP/IP header compression is disabled  
RTP/IP header compression is disabled  
Probe proxy name replies are disabled  
Policy routing is disabled  
Network address translation is disabled  
BGP Policy Mapping is disabled  
Input features: MCI Check  
WCCP Redirect outbound is disabled  
WCCP Redirect inbound is disabled  
WCCP Redirect exclude is disabled

R1#

```
R1#show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 192.168.2.254
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
```

Input features: MCI Check  
WCCP Redirect outbound is disabled  
WCCP Redirect inbound is disabled  
WCCP Redirect exclude is disabled

R1#

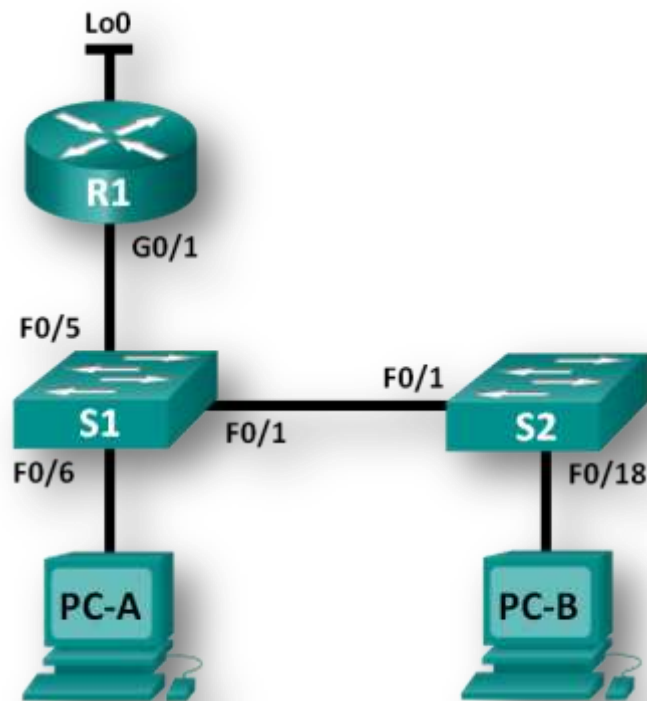
## **Reflexión**

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

Tener un servidor DHCP de enrutador separado para cada subred añadiría más complejidad, disminuiría la administración centralizada de la red, así como requeriría que cada enrutador trabajara más duro administrando su propio DHCP mientras ya enrutaba el tráfico. Un servidor DHCP (RT / PC) dedicado es más fácil de gestionar y es más centralizado

## 10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch

### Topología



### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.2	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

### Objetivos

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

**Parte 2: cambiar la preferencia de SDM**

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

**Parte 3: configurar DHCPv4**

- Configurar DHCPv4 para la VLAN 1.

- Verificar la conectividad y DHCPv4.

#### **Parte 4: configurar DHCP para varias VLAN**

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

#### **Parte 5: habilitar el routing IP**

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

### **Información básica/situación**

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

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

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

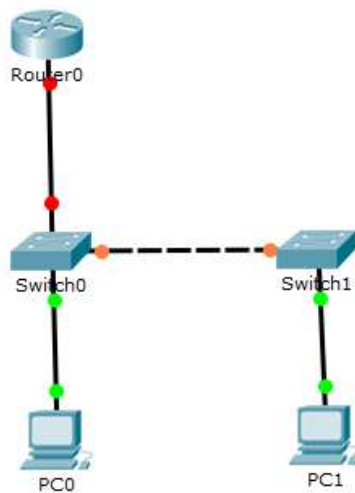
**Nota:** asegúrese de que el router y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

### Recursos necesarios

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

### Parte 6: ARMAR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

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



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

**Paso 3:** Configurar los parámetros básicos en los dispositivos.

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

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

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/1
Router(config-if)#ip address 192.168.1.10 255.255.255.0
Router(config-if)#no shut

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

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

Router(config-if)#int lo 0

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ip address 209.165.200.225 255.255.255.224
Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shut
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

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

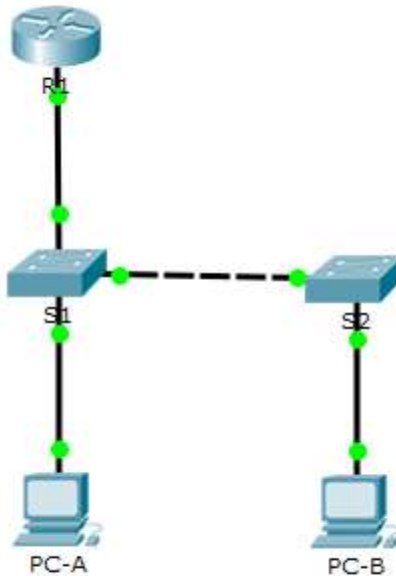
```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#int vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shut

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#int vlan 2
S1(config-if)#ip address 192.168.2.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#
S1(config-if)#
```

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?

**Las respuestas variarán, "predeterminado" o "ipv4 dual e ipv6 predeterminado" o "enrutamiento base LAN"**

**Paso 2: Cambiar la preferencia de SDM en el S1.**

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

```
S1(config)# sdm prefer lanbase-routing
```

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

¿Qué plantilla estará disponible después de la recarga? Enrutamiento base LAN.

- 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]
```

```
S1#reload  
Proceed with reload? [confirm]
```

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

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

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

```
S1# show sdm prefer
```

```
The current template is "lanbase-routing" template.
```

```
The selected template optimizes the resources in
```

the switch to support this level of features for  
0 routed interfaces and 255 VLANs.

number of unicast mac addresses:	4K
number of IPv4 IGMP groups + multicast routes:	0.25K
number of IPv4 unicast routes:	0.75K
number of directly-connected IPv4 hosts:	0.75K
number of indirect IPv4 routes:	16
number of IPv6 multicast groups:	0.375k
number of directly-connected IPv6 addresses:	0.75K
number of indirect IPv6 unicast routes:	16
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.125k
number of IPv4/MAC security aces:	0.375k
number of IPv6 policy based routing aces:	0
number of IPv6 qos aces:	0.375k
number of IPv6 security aces:	127

## **Parte 8: CONFIGURAR DHCPV4**

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

### ***Paso 1: Configurar DHCP para la VLAN 1.***

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

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

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

S1 (config)#ip dhcp pool DHCP1

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

S1 (dhcp-config)#network 192.168.1.0 255.255.255.0

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

S1 (dhcp-config)#default-router 192.168.1.1

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

S1 (dhcp-config)#dns-server 192.168.1.9

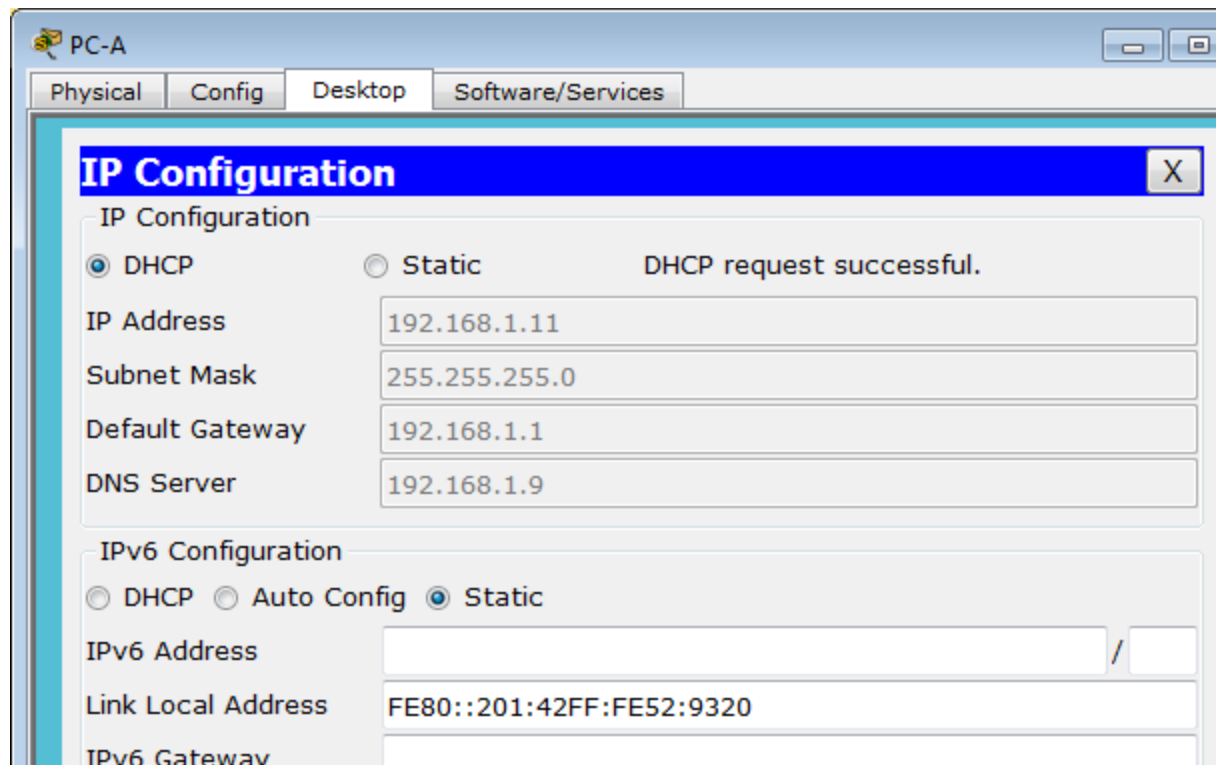
- f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

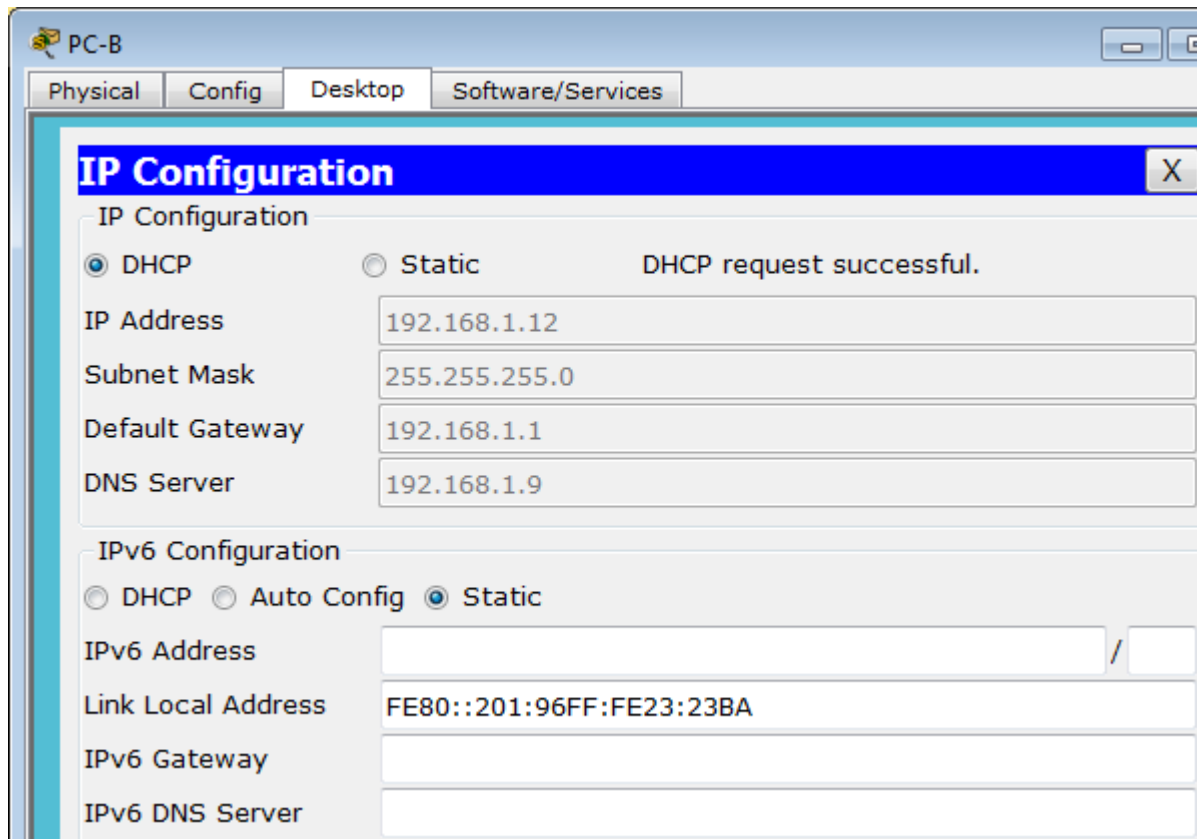
S1 (dhcp-config)#lease 3

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

**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 fa0/6

S1 (config)# switchport mode access

S1 (config)# switchport access vlan 2

### ***Paso 2: Configurar DHCPv4 para la VLAN 2.***

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

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

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

S1( config) # ip dhcp pool DHCP2

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

S1( dhcp-config) # network 192.168.2.0 255.255.255.0

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

S1( dhcp-config) # default-router 192.168.2.1

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

S1( dhcp-config) # dns-server 192.168.2.9

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

S1( dhcp-config) # lease 3

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

### **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?

Debido a que la puerta de enlace predeterminada está en la misma red que la PC-A, PC-A puede hacer ping a la puerta de enlace predeterminada. PC-B está en una red diferente; Por lo tanto, el ping de PC-A no tiene éxito

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

¿Qué resultado arrojó este comando?

No se ha establecido ninguna puerta de enlace predeterminada y no hay ninguna tabla de enrutamiento en el conmutador

### **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?

El switch está enrutando entre VLANs

- 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?

El conmutador muestra una tabla de enrutamiento que muestra las VLAN como redes conectadas directamente 192.168.1.0/24 y 192.168.2.0/24.

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

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

Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.10/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.224/27 is directly connected, Loopback0
L    209.165.200.225/32 is directly connected, Loopback0
```

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

La salida del enrutador muestra redes conectadas directamente de 192.168.1.0 y 209.165.200.224 pero no tiene ninguna entrada para la red 192.168.2.0

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

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

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

Para que se produzca la comunicación entre todas las redes, se deben agrgar rutas a las tablas de enrutamiento.

### **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.

S1 (config) # ip route 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.

Router(config)#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?

Gateway de último recurso es 192.168.1.10 a la red o.o.o.o

Dos redes directamente conectadas y una red estático.

- d. Vea la información de la tabla de routing para el R1.  
¿Cómo está representada la ruta estática?

S 192.168.2.0/24 está conectado directamente, GigabitEthernet0 / 1

- e. ¿Es posible hacer ping de la PC-A al R1? satisfactorio  
¿Es posible hacer ping de la PC-A a la interfaz Lo0? satisfactorio



## Reflexión

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

Las direcciones estáticas fueron excluidas punto de crear pool el DHCPv4 un ventana de tiempo existes cuando se excluye la direcciones y podría ser dado dinámicamente hacia el hosts.

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

Los switch fue asignada la configuración IP basándose en la asignamiento de VLAN y el asignamiento en el puerto de Vlan en puerto asignado en el puerto donde está conectado el host

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

Este switch 2960 puede tener funciones del servidor DHCP y puede establecer estáticas y entre VLAN

## Tabla de resumen de interfaces del router

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

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

### Apéndice A: comandos de configuración

#### Configurar DHCPv4

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

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

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

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

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

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

### Configurar DHCPv4 para varias VLAN

```
S1(config)# interface f0/6
```

```
S1(config-if)# switchport access vlan 2
```

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

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

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

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

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

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

### Habilitar routing IP

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

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

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

## 10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6

### Topología



### Tabla de direccionamiento

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

### Objetivos

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

**Parte 2: configurar la red para SLAAC**

### Parte 3: configurar la red para DHCPv6 sin estado

### Parte 4: configurar la red para DHCPv6 con estado

#### Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Solo mediante configuración automática de dirección sin estado (SLAAC)
- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
- Mediante DHCPv6 con estado

Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

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

encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

**Nota:** la plantilla **default bias** que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla **dual-ipv4-and-ipv6** o la plantilla **lanbase-routing** en SDM. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

```
S1# show sdm prefer
```

Siga estos pasos para asignar la plantilla **dual-ipv4-and-ipv6** como la plantilla de SDM predeterminada:

```
S1# config t
```

```
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
```

```
S1(config)# end
```

```
S1# reload
```

### Recursos necesarios

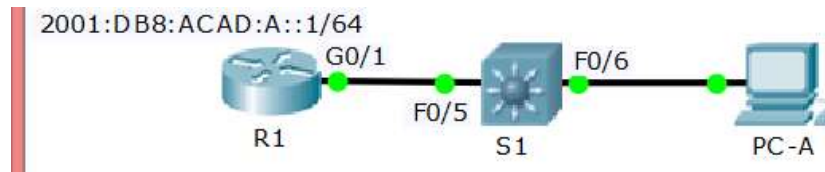
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para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

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

### Part 11: armar la red y configurar los parámetros básicos de los dispositivos

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

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



**Nota: Para desarrollar esta práctica utilizo el switch 3560-24PS, debido a que el switch 2960 no soporta muchos de los comandos para IPv6**

Step 2: inicializar y volver a cargar el router y el switch según sea necesario.

Inicializar y volver a cargar el switch

```
Switch#era
Switch#erase st
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0006.2ACA.717D
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
##### [OK]
#####
Restricted Rights Legend
```

## Inicializar y volver a cargar el router

```
Router>en
Router#er
Router#erase st
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with
ECC disabled

Readonly ROMMON initialized

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

IOS Image Load Test

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

### Step 3: Configurar R1

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.

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

```
Router>en
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#service password-encryption
R1(config)#banner motd #El acceso no autorizado esta prohibido!#
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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



#### Step 4: configurar el S1.

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

```
Switch>en
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#service password-encryption
S1(config)#banner motd #El acceso no autorizado esta prohibido!#
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#interface range f0/1-4,f0/7-24,g0/1-2
S1(config-if-range)#shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S1(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
changed state to down

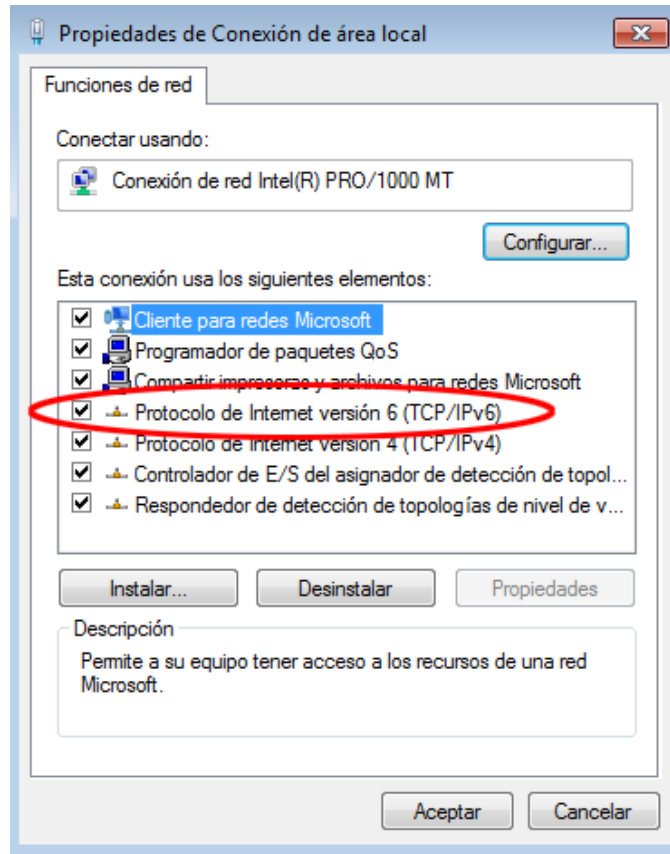
S1(config-if-range)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

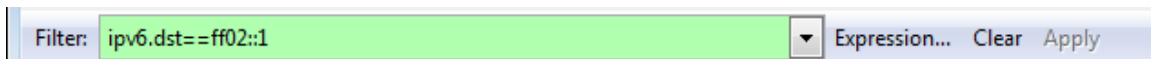
## Part 12: configurar la red para SLAAC

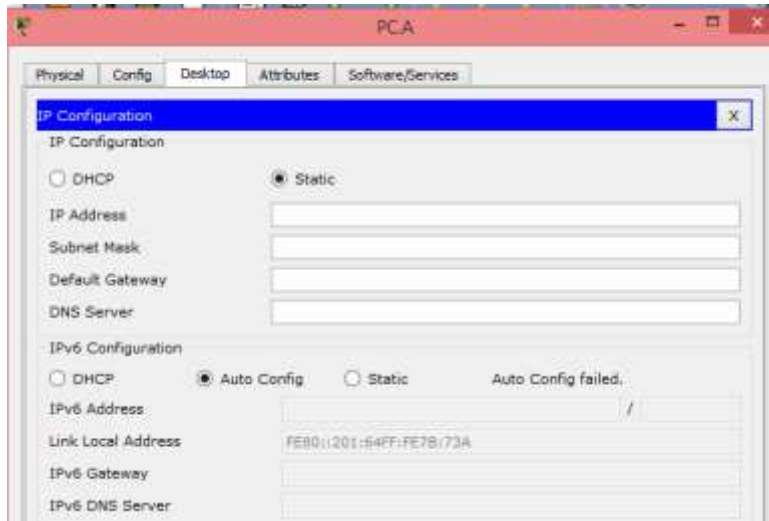
### Step 1: preparar la PC-A.

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



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





## Step 2: Configurar R1

- Habilite el routing de unidifusión IPv6.
- Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.
- Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.
- Active la interfaz G0/1.

```
R1>en
Password:
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#no shutdown

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

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
```

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

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

```
R1# show ipv6 interface g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
```

IPv6 is enabled, link-local address is FE80::1

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF00:1

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.

```

R1>en
Password:
R1#show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FE02::1
    FE02::2
    FE02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachable are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
D1#|

```

#### Step 4: configurar el S1.

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

```
S1(config)# interface vlan 1
```

```
S1(config-if)# ipv6 address autoconfig
```

```
S1(config-if)# end
```

```

S1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 1
S1(config-if)#no shut

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up

S1(config-if)#ipv6 address autoconfig
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

```

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

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

Vlan1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40

No Virtual link-local address(es):

Stateless address autoconfig enabled

Global unicast address(es):

**2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40**, subnet is 2001:DB8:ACAD:A::/64

[EUI/CAL/PRE]

valid lifetime 2591988 preferred lifetime 604788

Joined group address(es):

FF02::1

FF02::1:FFE8:8A40

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

Output features: Check hwidb

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND NS retransmit interval is 1000 milliseconds

**Default router is FE80::1 on Vlan1**

```

S1#show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::2D0:97FF:FE53:61E6
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A:2D0:97FF:FE53:61E6, subnet is
2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF53:61E6
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachable are sent
  Output features: Check hwidb
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
S1#

```

```

S1#show ipv6 interface brief
FastEthernet0/1      [down/down]
FastEthernet0/2      [down/down]
FastEthernet0/3      [down/down]
FastEthernet0/4      [down/down]
FastEthernet0/5      [up/up]
FastEthernet0/6      [up/up]
FastEthernet0/7      [down/down]
FastEthernet0/8      [down/down]
FastEthernet0/9      [down/down]
FastEthernet0/10     [down/down]
FastEthernet0/11     [down/down]
FastEthernet0/12     [down/down]
FastEthernet0/13     [down/down]
FastEthernet0/14     [down/down]
FastEthernet0/15     [down/down]
FastEthernet0/16     [down/down]
FastEthernet0/17     [down/down]
FastEthernet0/18     [down/down]
FastEthernet0/19     [down/down]
FastEthernet0/20     [down/down]
FastEthernet0/21     [down/down]
FastEthernet0/22     [down/down]
FastEthernet0/23     [down/down]
FastEthernet0/24     [down/down]
GigabitEthernet0/1   [down/down]
GigabitEthernet0/2   [down/down]
Vlan1                [up/up]

```

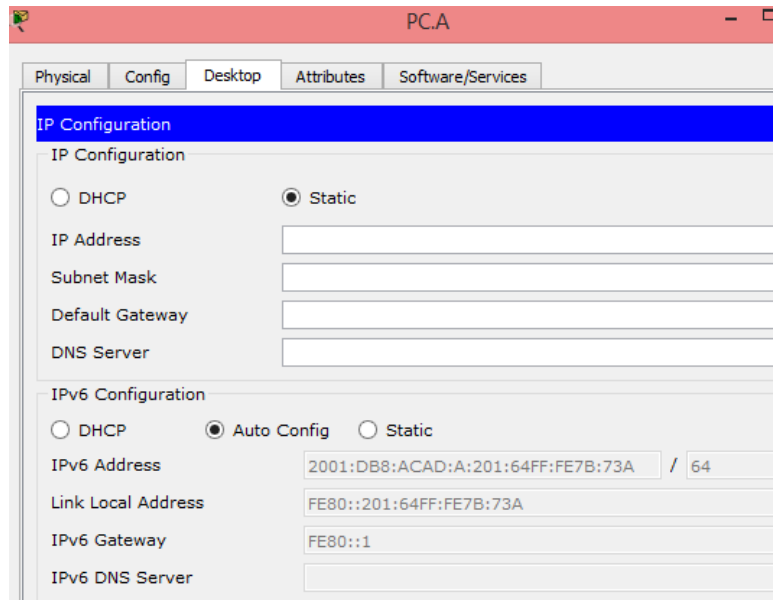
FE80::2D0:97FF:FE53:61E6 → Link-local  
2001:DB8:ACAD:A:2D0:97FF:FE53:61E6 → Global unicast address





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

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

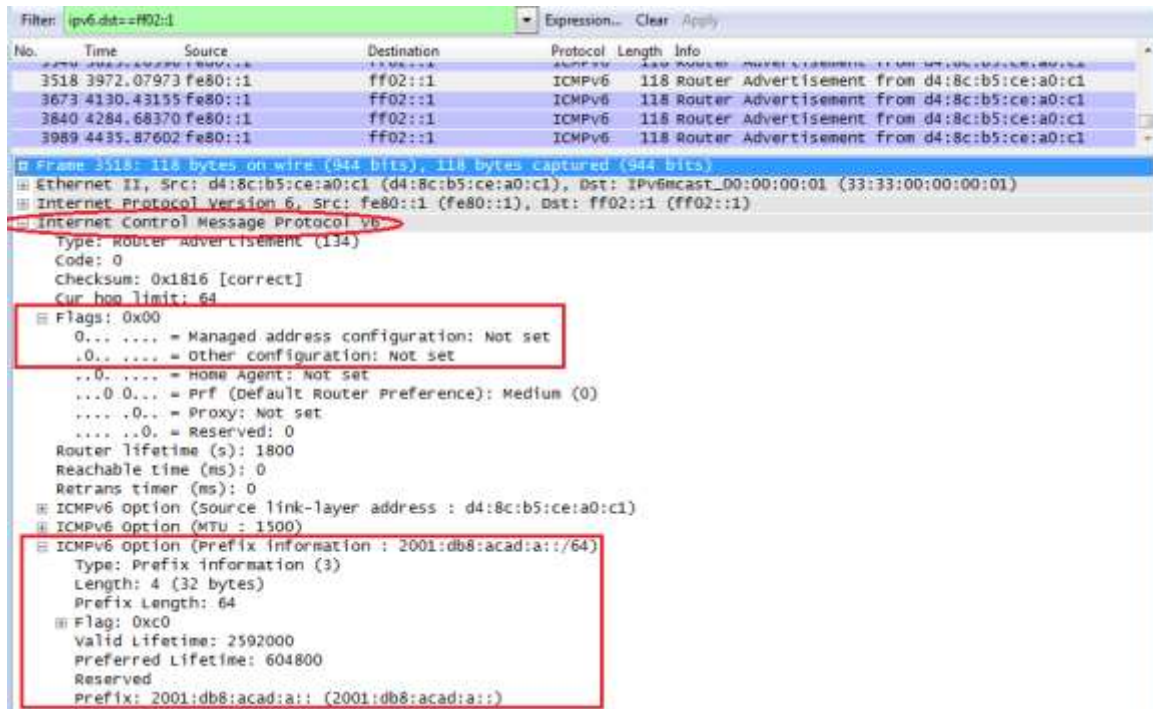


```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Physical Address. . . . . : 0001.647B.073A
    Link-local IPv6 Address . . . . . : FE80::201:64FF:FE7B:73A
    IPv6 Address . . . . . : 2001:DB8:ACAD:A:201:64FF:FE7B:73A/64
    Default Gateway . . . . . : FE80::1
    DNS Servers . . . . . : 
    DHCPv6 Client DUID. . . . . : 00-01-00-01-5B-CC-4D-CC-00-01-64-7B-07-3A
```

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



### Part 13: configurar la red para DHCPv6 sin estado

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

- Cree un pool de DHCP IPv6.

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

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

```
R1(config-dhcpv6)# dns-server 2001:db8:acad:a::abcd
```

```
R1(config-dhcpv6)# exit
```
- Asigne el pool de DHCPv6 a la interfaz.

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

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

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

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

```

R1>en
Password:
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)#dns-server 2001:db8:acad:a::abcd
R1(config-dhcpv6)#exit
R1(config)#interface g0/1
      ^
% Invalid input detected at '^' marker.

R1(config)#interface g0/1
R1(config-if)#ipv6 dhcp server IPV6POOL-A
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

```

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

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

```
R1# show ipv6 interface g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
```

```
IPv6 is enabled, link-local address is FE80::1
```

```
No Virtual link-local address(es):
```

```
Global unicast address(es):
```

```
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
```

```
Joined group address(es):
```

```
FF02::1
```

```
FF02::2
```

```
FF02::1:2
```

```
FF02::1:FF00:1
```

```
FF05::1:3
```

```
MTU is 1500 bytes
```

```
ICMP error messages limited to one every 100 milliseconds
```

```
ICMP redirects are enabled
```

```
ICMP unreachable are sent
```

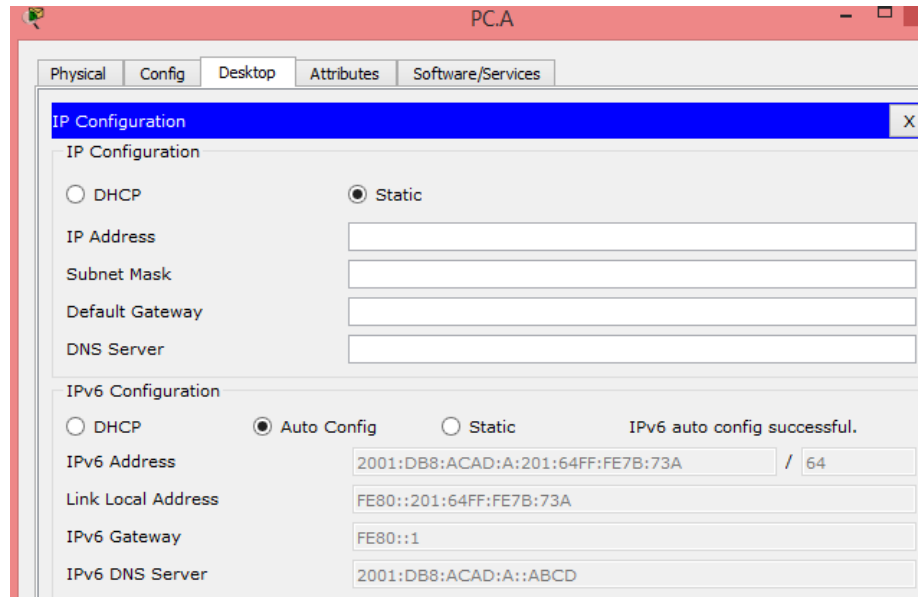
ND DAD is enabled, number of DAD attempts: 1  
ND reachable time is 30000 milliseconds (using 30000)  
ND advertised reachable time is 0 (unspecified)  
ND advertised retransmit interval is 0 (unspecified)  
ND router advertisements are sent every 200 seconds  
ND router advertisements live for 1800 seconds  
ND advertised default router preference is Medium  
Hosts use stateless autoconfig for addresses.

Hosts use DHCP to obtain other configuration.

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

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

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



```
C:\>ipconfig /all

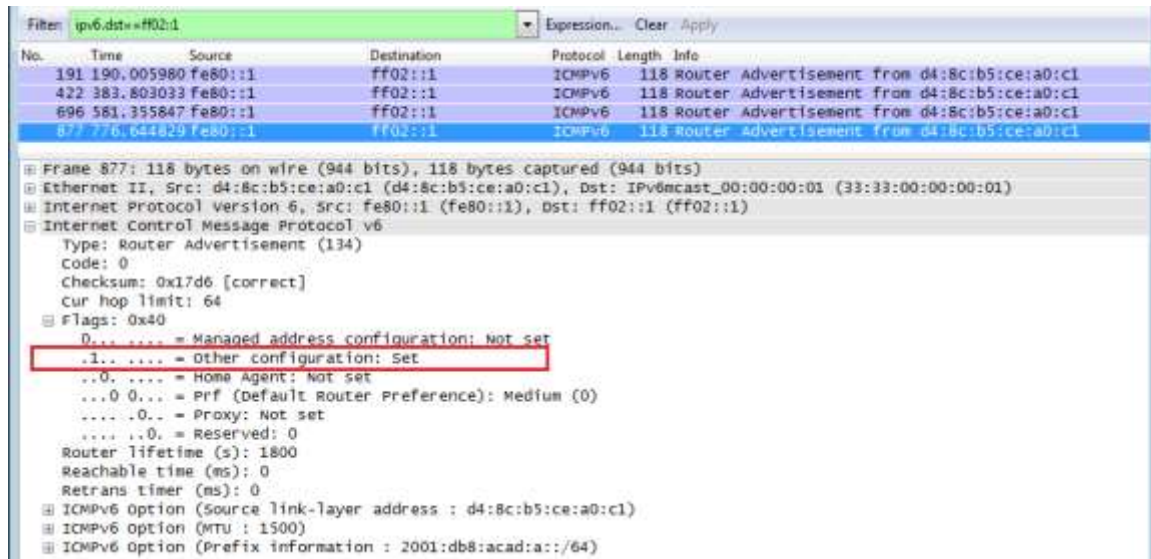
FastEthernet0 Connection: (default port)

    Physical Address. . . . . : 0001.647B.073A
    Link-local IPv6 Address . . . . . : FE80::201:64FF:FE7B:73A
    IPv6 Address. . . . . : 2001:DB8:ACAD:A:201:64FF:FE7B:73A/64
    Default Gateway. . . . . : FE80::1
    DNS Servers. . . . . : 2001:DB8:ACAD:A::ABCD
    DHCPv6 IAID. . . . . : 28032
    DHCPv6 Client DUID. . . . . : 00-01-00-01-5B-CC-4D-CC-00-01-64-7B-07-3A

C:\>
```

**Step 4: ver los mensajes RA en Wireshark.**

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



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

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

**R1# show ipv6 dhcp binding**

**R1# show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-statelessDHCPv6.com

**Active clients: 0**

```
R1>en
Password:
R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
  DUID: 00030001000197668401
  IA PD: IA ID 29782, T1 0, T2 0
  Prefix: 0.0.0.0/0
         preferred lifetime 0, valid lifetime 0
         expires at mayo 15 2017 2:57:36 pm (0 seconds)
Client: (GigabitEthernet0/1)
  DUID: 00-01-00-01-5B-CC-4D-CC-00-01-64-7B-07-3A
  IA PD: IA ID 28032, T1 0, T2 0
  Prefix: 0.0.0.0/0
         preferred lifetime 0, valid lifetime 0
         expires at mayo 15 2017 2:57:36 pm (0 seconds)
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-statelessDHCPv6.com
  Active clients: 0
R1#
```

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

- a. Desactive la interfaz F0/6 del S1.

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

```
S1(config)# interface f0/6
```

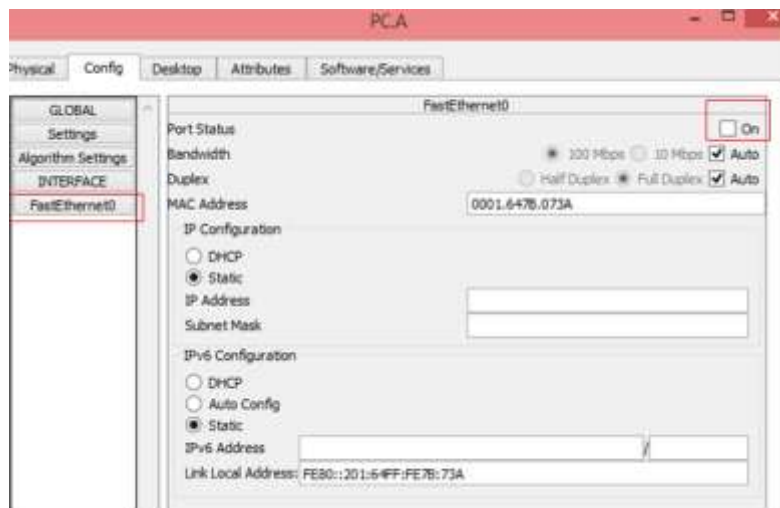
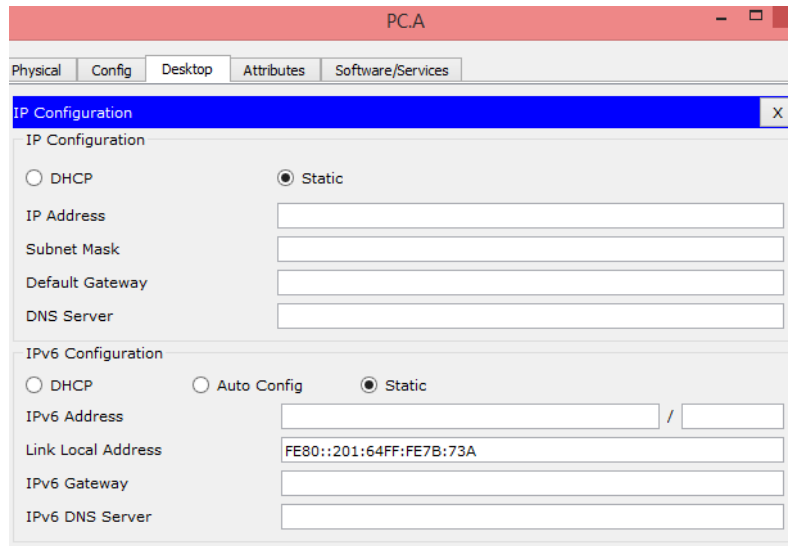
```
S1(config-if)# shutdown
```

```
S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
changed state to down
```

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

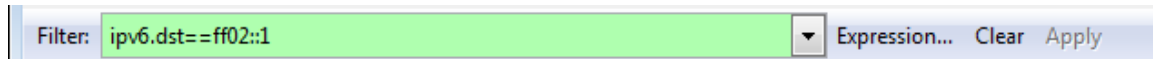




## Part 14: configurar la red para DHCPv6 con estado

### Step 1: preparar la PC-A.

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



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

- Agregue el prefijo de red al pool.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
```

```
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```

```
R1>en
Password:
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#address prefix 2001:db8:acad:a::/64
% Invalid input detected at '^' marker.
```

PT no soporta este comando

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

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

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

```
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
```

```
R1(config-dhcpv6)# end
```

```
R1(config-dhcpv6)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool
```

DHCPv6 pool: IPV6POOL-A

Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (0 in use, 0 conflicts)

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-StatefulDHCPv6.com

Active clients: 0

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

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

R1# **debug ipv6 dhcp detail**

IPv6 DHCP debugging is on (detailed)

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

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

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

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

R1(config-if)# **shutdown**

R1(config-if)# **ipv6 nd managed-config-flag**

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

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

```

R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/1
R1(config-if)#shutdown

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

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

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

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

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

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

```

habilitar la interfaz F0/6 en el S1.

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

```

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

```

```

S1>enable
Password:
S1#conf te
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#no shut down

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

```

#### Step 4: verificar la configuración de DHCPv6 con estado en el R1.

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

```

R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1

```

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:2

FF02::1:FF00:1

FF05::1:3

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

**Hosts use DHCP to obtain routable addresses.**

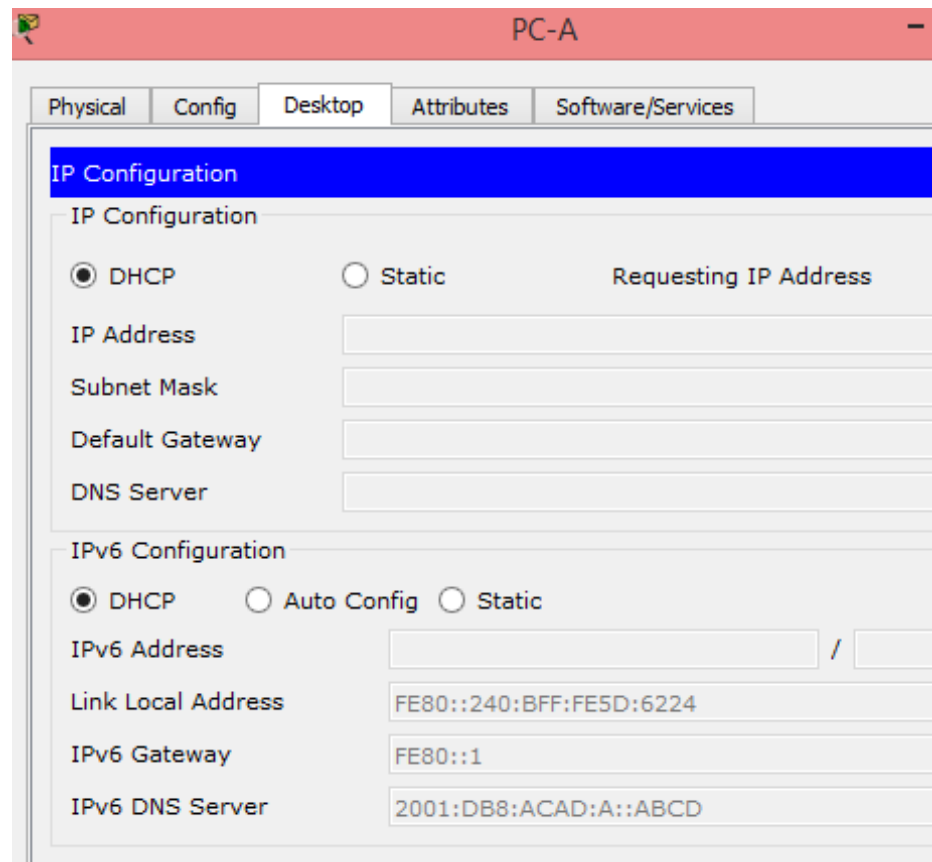
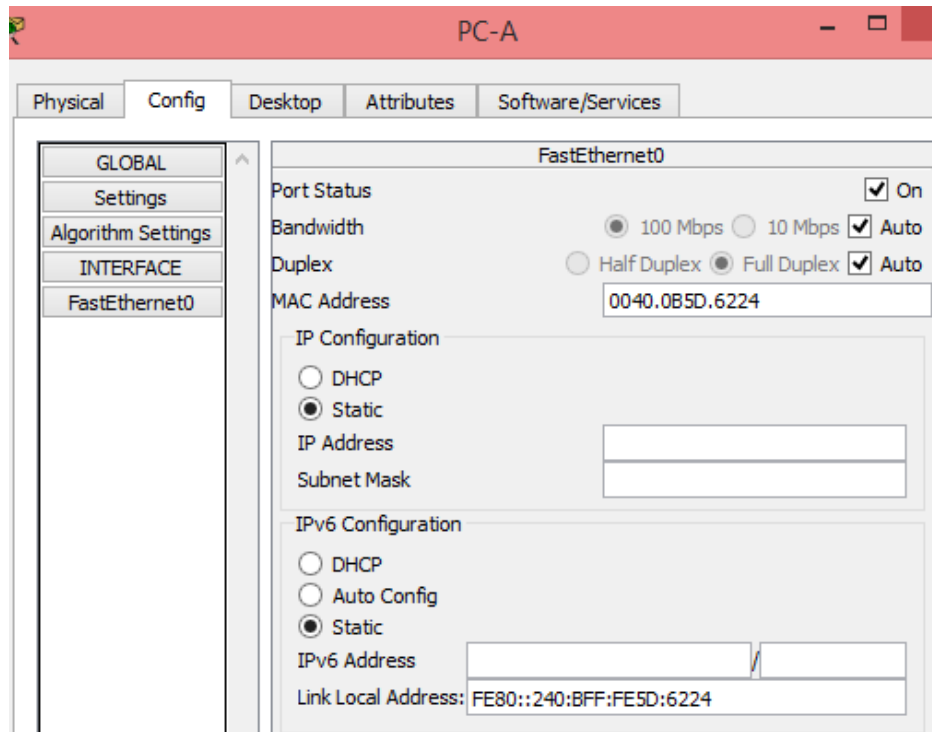
Hosts use DHCP to obtain other configuration.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface

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

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

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



**Nota: no hay una direccion IPv6 porque Packet tracer no soporta el comando *R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64***

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

```
R1# show ipv6 dhcp pool
```

```
DHCPv6 pool: IPV6POOL-A
```

```
Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (1 in use, 0 conflicts)
```

```
DNS server: 2001:DB8:ACAD:A::ABCD
```

```
Domain name: ccna-StatefulDHCPv6.com
```

```
Active clients: 1
```

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

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

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

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

```
DUID: 0001000117F6723D000C298D5444
```

```
Username : unassigned
```

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

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

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

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

```

R1#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-09-48-D2-9E-00-40-0B-5D-62-24
IA PD: IA ID 2319, T1 0, T2 0
Prefix: 0.0.0.0/0
        preferred lifetime 0, valid lifetime 0
        expires at mayo 16 2017 11:33:21 am (0 seconds)
Client: (GigabitEthernet0/1)
DUID: 000300010007EC355301
IA PD: IA ID 2319, T1 0, T2 0
Prefix: 0.0.0.0/0
        preferred lifetime 0, valid lifetime 0
        expires at mayo 16 2017 11:33:21 am (0 seconds)
...

```

```

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

```

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

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

R1# **u all**

Se ha desactivado toda depuración posible

```

R1#undebg all
All possible debugging has been turned off
D1#

```

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

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

\*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from

FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1



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

```
R1#show ipv6 dhcp
*mar. 1 01:11:34.643: IPv6 DHCP: Received SOLICIT from FE80::204:9AFF:FE47:5340 on
GigabitEthernet0/1
*mar. 1 01:11:34.643: IPv6 DHCP: detailed packet contents
*mar. 1 01:11:34.643:   src FE80::204:9AFF:FE47:5340 (GigabitEthernet0/1)
*mar. 1 01:11:34.643:   dst FF02::1:2 (GigabitEthernet0/1)
*mar. 1 01:11:34.643:   type SOLICIT(1), xid 5
*mar. 1 01:11:34.643:   option ELAPSED-TIME(8), len 6
*mar. 1 01:11:34.643:     elapsed-time 0
*mar. 1 01:11:34.643:   option CLIENTID(1), len 24
*mar. 1 01:11:34.643:     000300010007EC355301
*mar. 1 01:11:34.643:   option ORO(6), len 10
*mar. 1 01:11:34.643:     IA-PD, DNS-SERVERS, DOMAIN-LIST
*mar. 1 01:11:34.643:   option IA-PD(25), len 16
*mar. 1 01:11:34.643:     IAID 0x2319, T1 0, T2 0
```

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

\*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A  
 on GigabitEthernet0/1  
 \*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents  
 \*Mar 5 16:42:39.779: src FE80::1  
 \*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)  
 \*Mar 5 16:42:39.779: type REPLY(7), xid 1039238  
 \*Mar 5 16:42:39.779: option SERVERID(2), len 10  
 \*Mar 5 16:42:39.779: 00030001FC994775C3E0  
 \*Mar 5 16:42:39.779: option CLIENTID(1), len 14  
 \*Mar 5 16:42:39.779: 00010001  
 R1#17F6723D000C298D5444  
 \*Mar 5 16:42:39.779: option IA-NA(3), len 40  
 \*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120  
 \*Mar 5 16:42:39.779: option IAADDR(5), len 24

\*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE

\*Mar 5 16:42:39.779: preferred 86400, valid 172800

\*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16

\*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD

\*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26

\*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com

```
*mar. 1 01:11:34.643: IPv6 DHCP: Sending REPLY to FE80::204:9AFF:FE47:5340 on
GigabitEthernet0/1
*mar. 1 01:11:34.643: IPv6 DHCP: detailed packet contents
*mar. 1 01:11:34.643:   src FE80::1 (GigabitEthernet0/1)
*mar. 1 01:11:34.643:   dst FE80::204:9AFF:FE47:5340 (GigabitEthernet0/1)
*mar. 1 01:11:34.643:   type REPLY(7), xid 3
*mar. 1 01:11:34.643:   option SERVERID(2), len 24
*mar. 1 01:11:34.643:     0003000100902BE4E701
*mar. 1 01:11:34.643:   option CLIENTID(1), len 24
*mar. 1 01:11:34.643:     000300010007EC355301
*mar. 1 01:11:34.643:   option IA-PD(25), len 41
*mar. 1 01:11:34.643:     IAID 0x2319, T1 0, T2 0
*mar. 1 01:11:34.643:   option IAPREFIX(26), 29
*mar. 1 01:11:34.643:     preferred 0, valid 0, prefix 0.0.0.0/0
*mar. 1 01:11:34.643:   option DNS-SERVERS(23), len 20
*mar. 1 01:11:34.643:     2001:DB8:ACAD:A::ABCD
*mar. 1 01:11:34.643:   option DOMAIN-LIST(24), len 5
*mar. 1 01:11:34.643:     ccna-statelessDHCPv6.com
```

### Step 5: verificar DHCPv6 con estado en la PC-A.

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

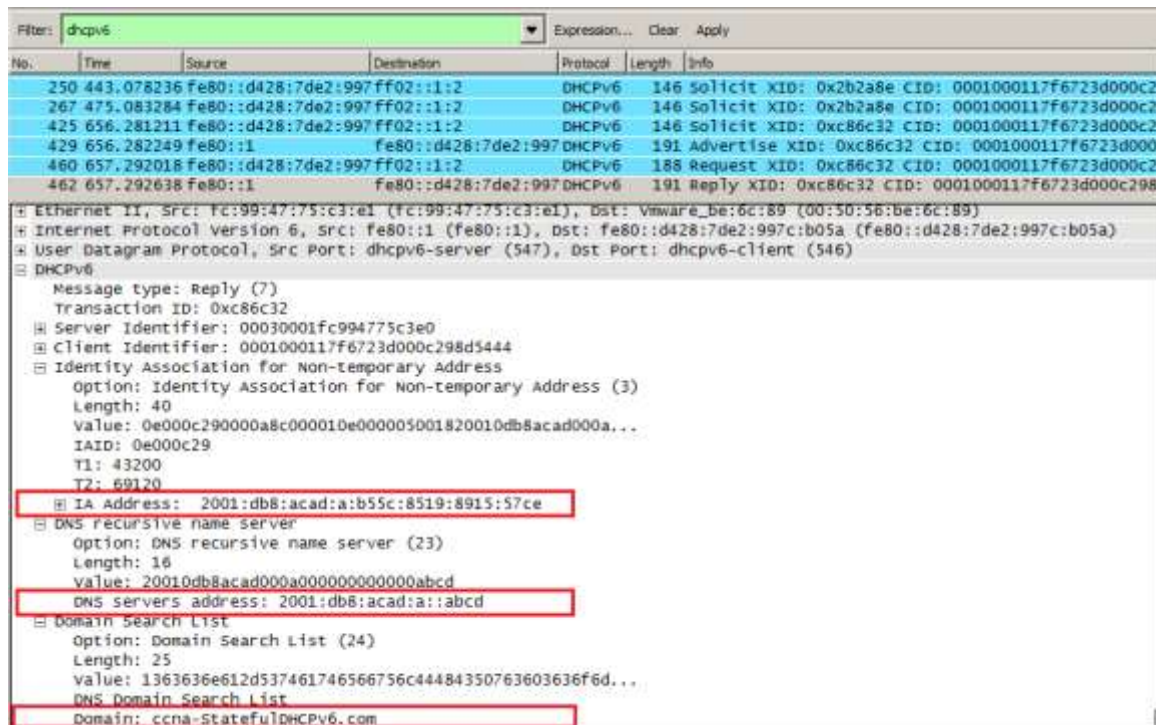
Filter: `ipv6.dst==ff02::1` Expression... Clear Apply

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

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

- Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: IPv6mcast\_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
  - Type: Router Advertisement (134)
  - Code: 0
  - Checksum: 0x3a82 [correct]
  - cur hop limit: 64
  - Flags: 0xc0
    - 1... .. = Managed address configuration: Set
    - ..1... .. = Other configuration: Set
    - ..0... .. = Home Agent: Not set
    - ...0 0... = Prf (Default Router Preference): Medium (0)
    - ....0... = Proxy: Not set
    - .... ..0. = Reserved: 0
  - Router lifetime (s): 1800

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



## 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?

**DHPv6 con estado usa más recursos de memoria. El DHCPv6 con estado requiere que el router guarde dinámicamente el estado de información acerca de los clientes de DHCPv6. En DHCPv6 sin estado los clientes no usan el servidor DHCP para obtener las direcciones, así que no necesitan ser guardadas.**

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 implementa y desarrolla redes en IPv6 sin un registro de red Cisco (CNR).**

## Tabla de resumen de interfaces del router

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

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

### 10.3.1.1 IoE and DHCP Instructions

#### Objetivo

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

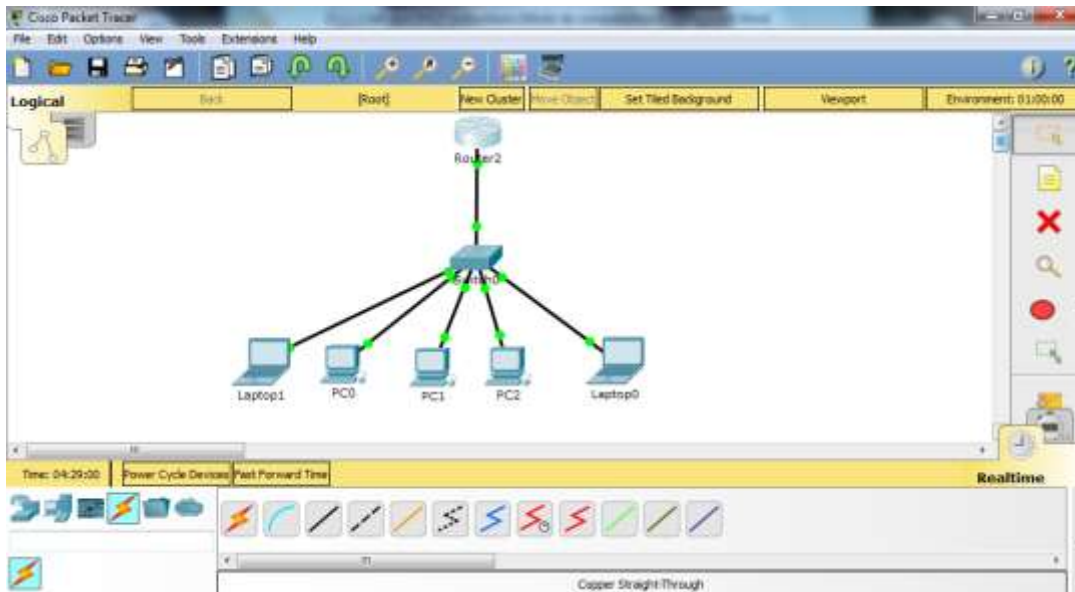
## Situación

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

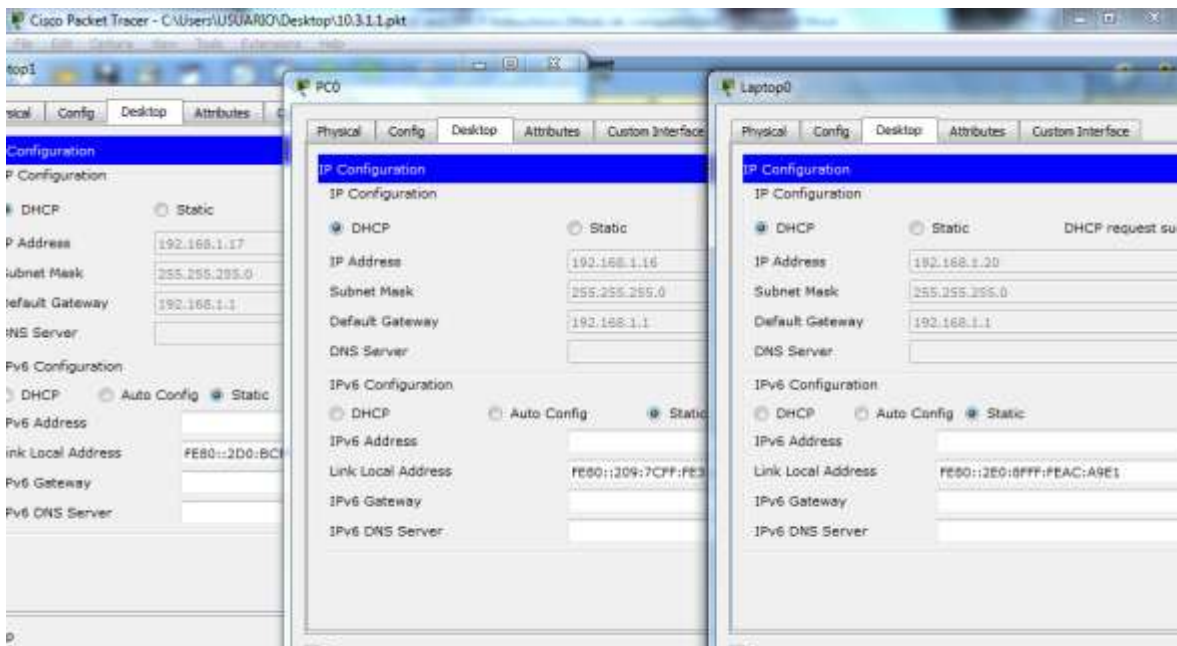
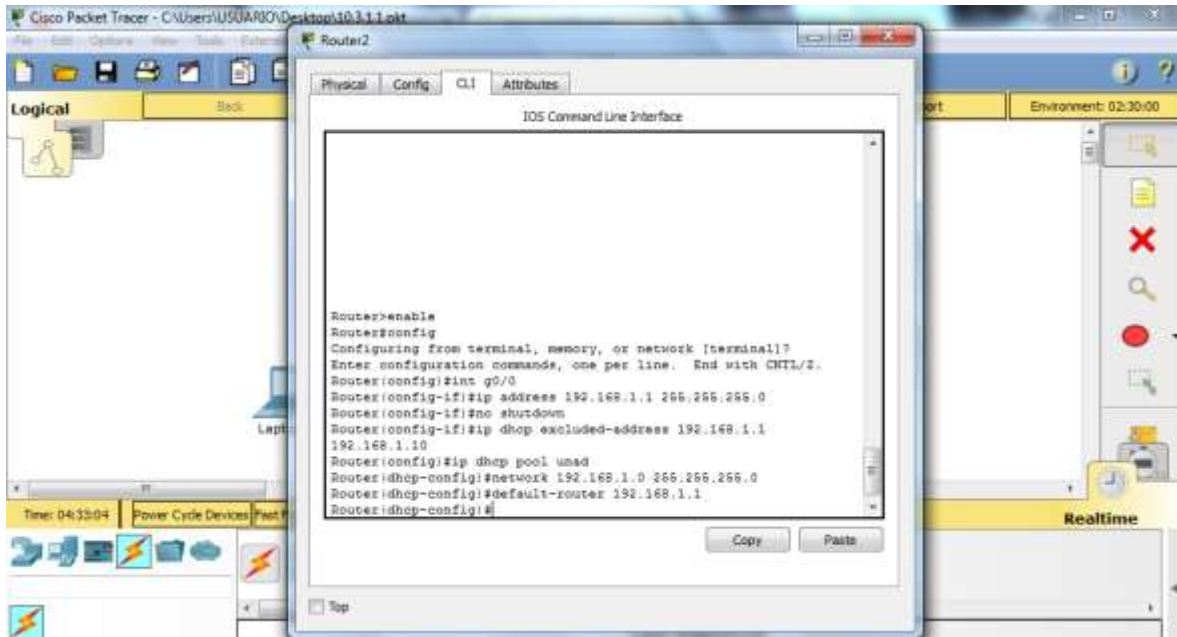
Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

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

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







## Recursos necesarios

Software de Packet Tracer

## Reflexión

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

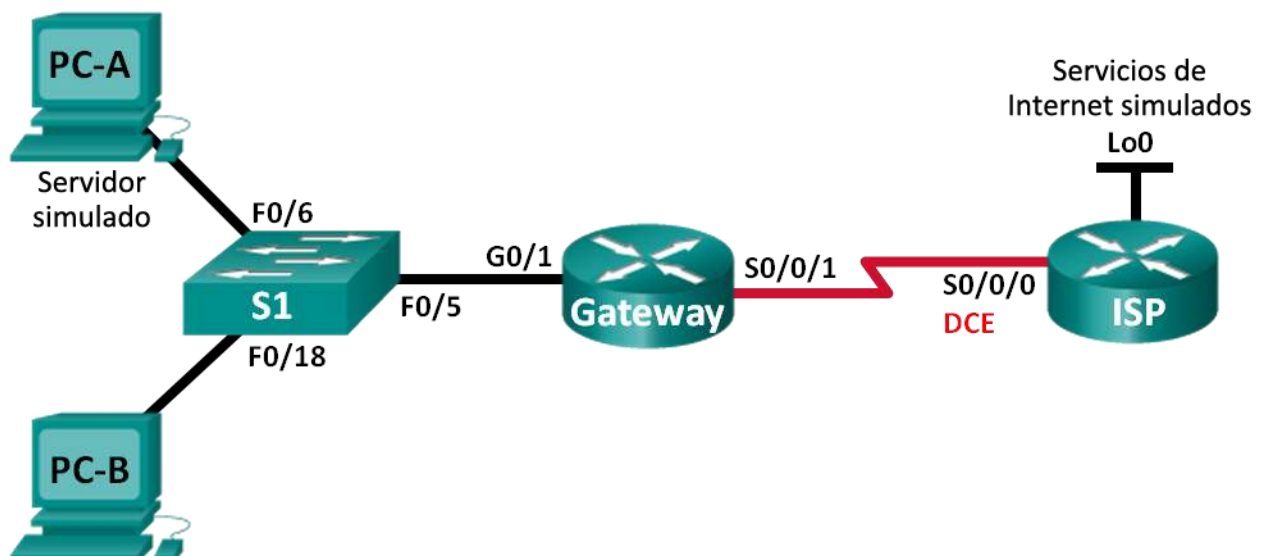
DHCP proporciona un mecanismo a través del cual los equipos que usan el Protocolo de transmisión de Control/Protocolo de Internet (TCP/IP) pueden obtener parámetros de configuración de protocolo de automáticamente a través de la red con nuestro router teniendo mas direcciones ip para usar en nuestra red y no limitándonos a las pocas direcciones ip que nos puede brindar un ISR

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

- Servidor dhcp
- Router cisco
- Proveedor de internet
- ISR

### 11.2.2.6 Lab - Configuring Dynamic and Static NAT

#### Topología



## Tabla de direccionamiento

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

## Objetivos

**Parte 1: armar la red y verificar la conectividad**

**Parte 2: configurar y verificar la NAT estática**

**Parte 3: configurar y verificar la NAT dinámica**

## Información básica/situación

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

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



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

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

### **Recursos necesarios**

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

### **Part 15: armar la red y verificar la conectividad**

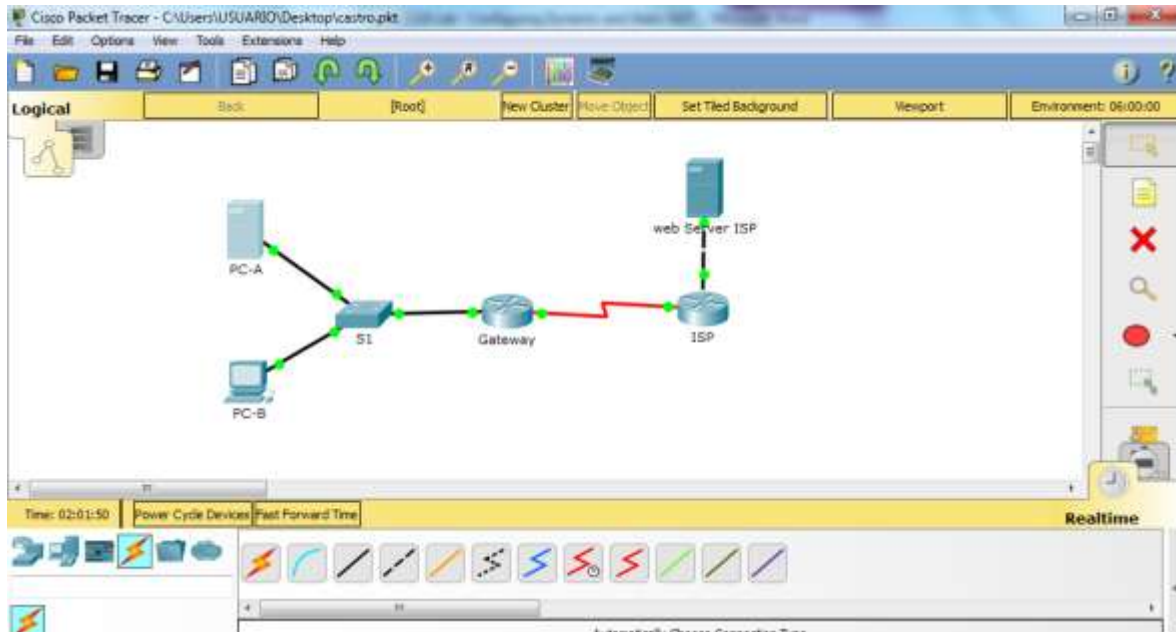
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

#### **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.

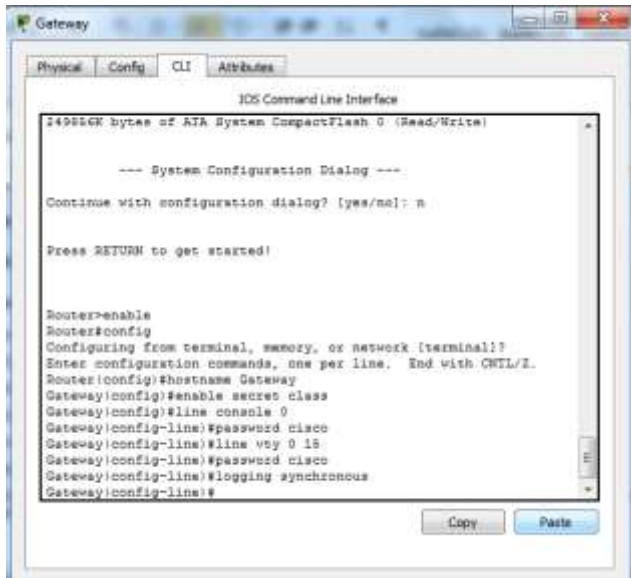
#### **Step 2: configurar los equipos host.**

#### **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 interrumpen la entrada del comando.



Gateway

Physical Config CLI Attributes

IOS Command Line Interface

```
249856K bytes of ATA System CompactFlash 0 (Read/Write)

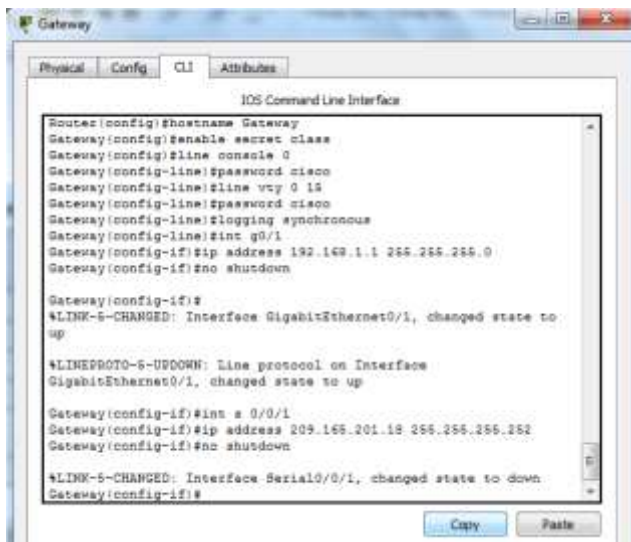
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CTRL/Z.
Router(config)#hostname Gateway
Gateway(config)#enable secret class
Gateway(config)#line console 0
Gateway(config-line)#password cisco
Gateway(config-line)#line vty 0 15
Gateway(config-line)#password cisco
Gateway(config-line)#logging synchronous
Gateway(config-line)#
```

Copy Paste



Gateway

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#hostname Gateway
Gateway(config)#enable secret class
Gateway(config)#line console 0
Gateway(config-line)#password cisco
Gateway(config-line)#line vty 0 15
Gateway(config-line)#password cisco
Gateway(config-line)#logging synchronous
Gateway(config-line)#int g0/1
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config-if)#no shutdown

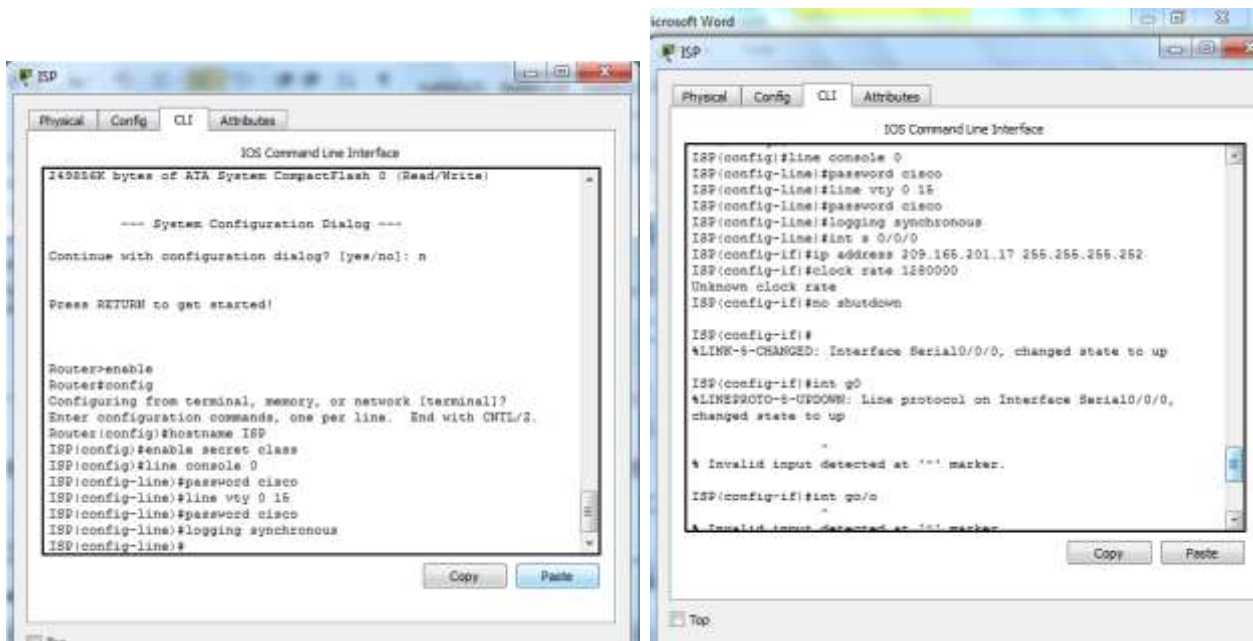
Gateway(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

Gateway(config-if)#int s 0/0/1
Gateway(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway(config-if)#no shutdown

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

Copy Paste



### 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
```

No se puede realizar este punto ya que el programa no acepta estos comandos para simular el servidor web en el router por lo cual se pone el servidor web isp

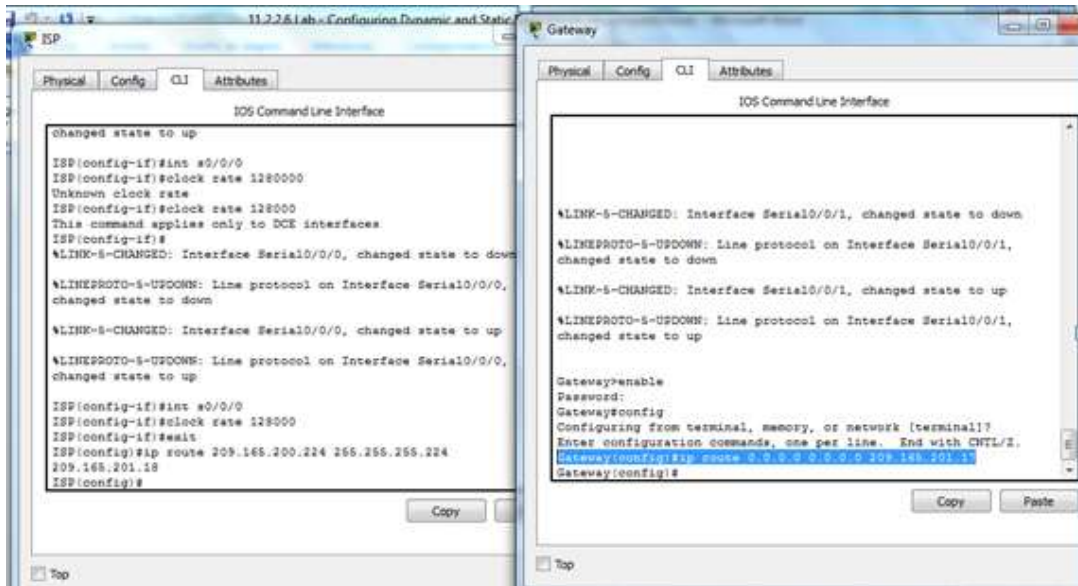
### Step 6: configurar el routing estático.

- 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(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**

- Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.
- 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.

**Part 16: 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.

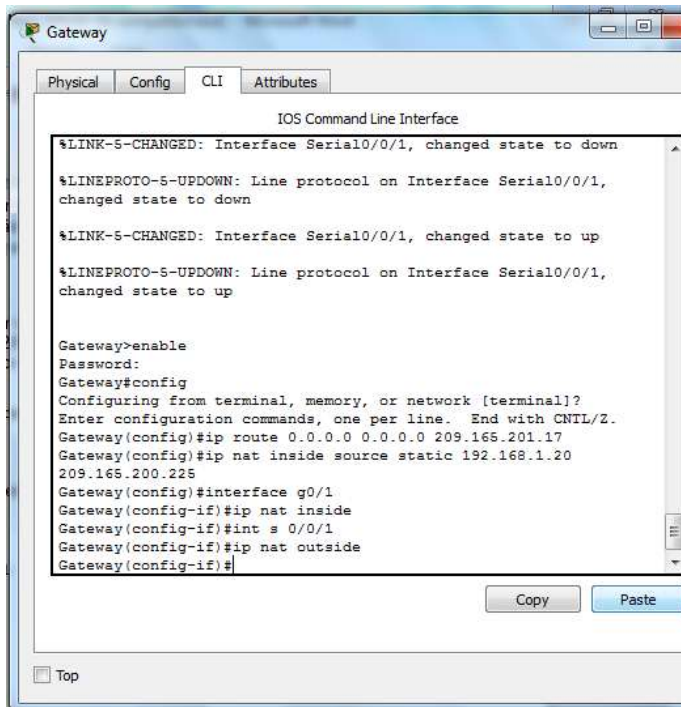
Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
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.

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

```
Gateway# show ip nat translations
```

```
Pro Inside global    Inside local    Outside local    Outside global
```

```
--- 209.165.200.225  192.168.1.20    ---            ---
```

```

Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
Gateway(config)#ip nat inside source static 192.168.1.20
209.165.200.225
Gateway(config)#interface g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#int s 0/0/1
Gateway(config-if)#ip nat outside
Gateway(config-if)#exit
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console

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

```

Copy Paste

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

192.168.1.20 = **209.165.200.225**

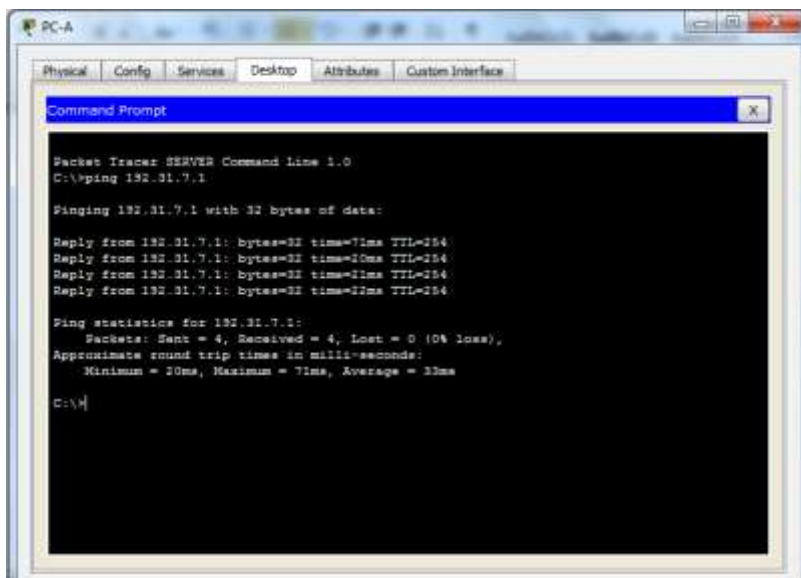
¿Quién asigna la dirección global interna?

**El router por el pool nat**

¿Quién asigna la dirección local interna?

**El administrador de la red**

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

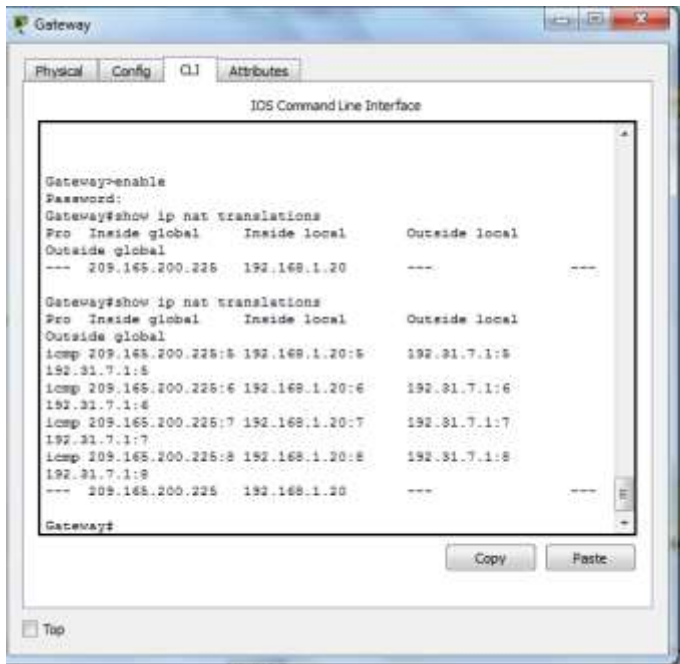


Gateway# **show ip nat translations**

```

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   ---            ---

```

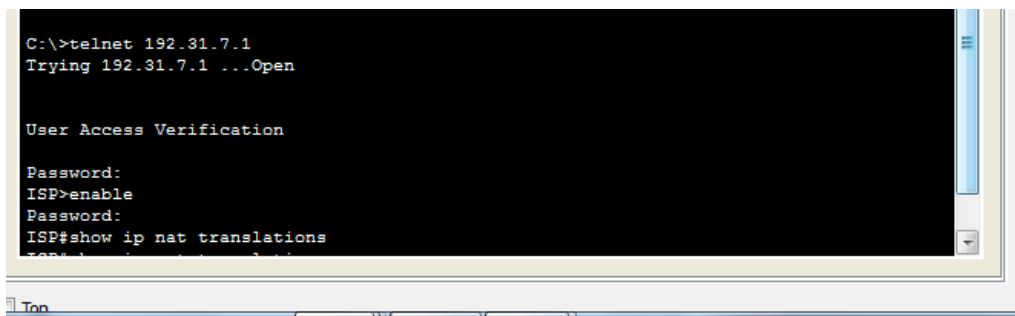


Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

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

**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? **tcp**

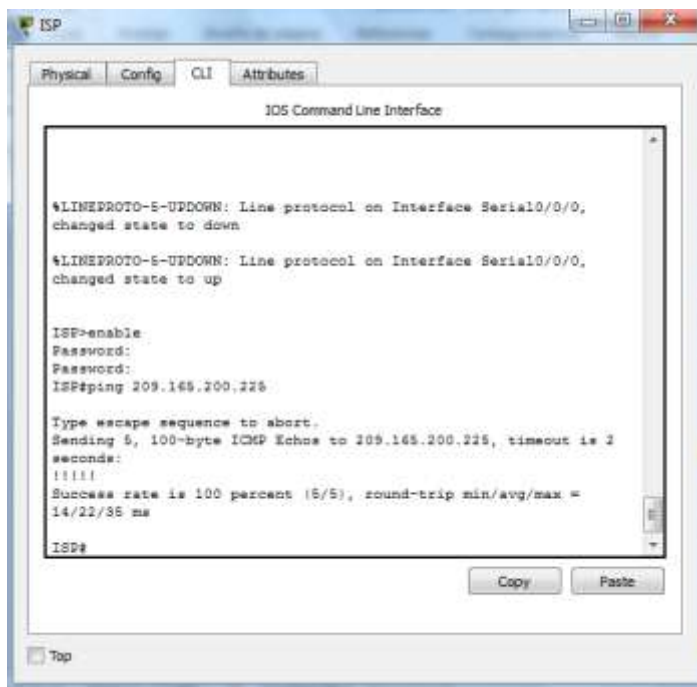
¿Cuáles son los números de puerto que se usaron?

Global/local interno: **1025192**

Global/local externo: **23**

```
192.31.7.1:12
icmp 209.165.200.225:9 192.168.1.20:9 192.31.7.1:9
192.31.7.1:9
--- 209.165.200.225 192.168.1.20 ---
tcp 209.165.200.225:1025192 192.168.1.20:1025 192.31.7.1:23
192.31.7.1:23
Gateway#
```

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



```
ISP
Physical Config CLI Attributes
IOS Command Line Interface

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

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

ISP-enable
Password:
Password:
ISP#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 209.165.200.225, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
14/22/35 ms
ISP#
```

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

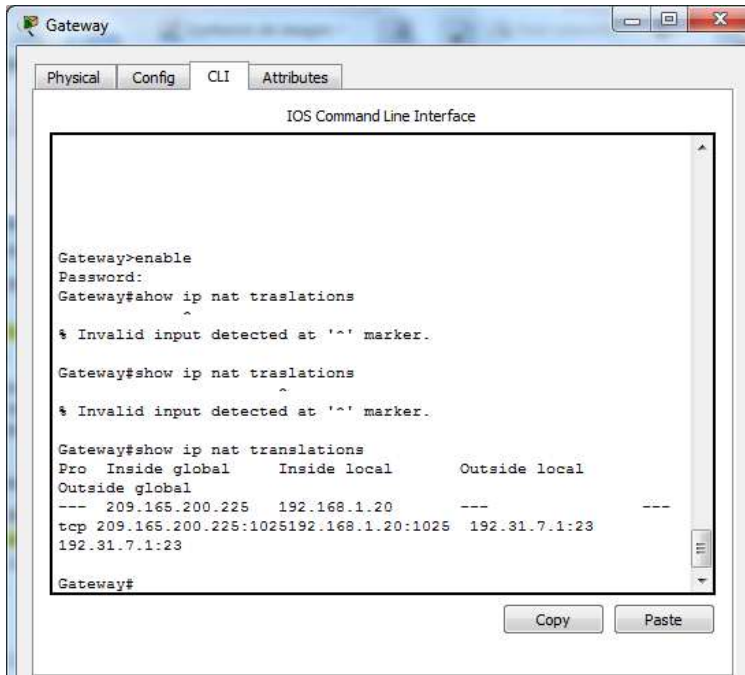
Gateway# **show ip nat translations**

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:

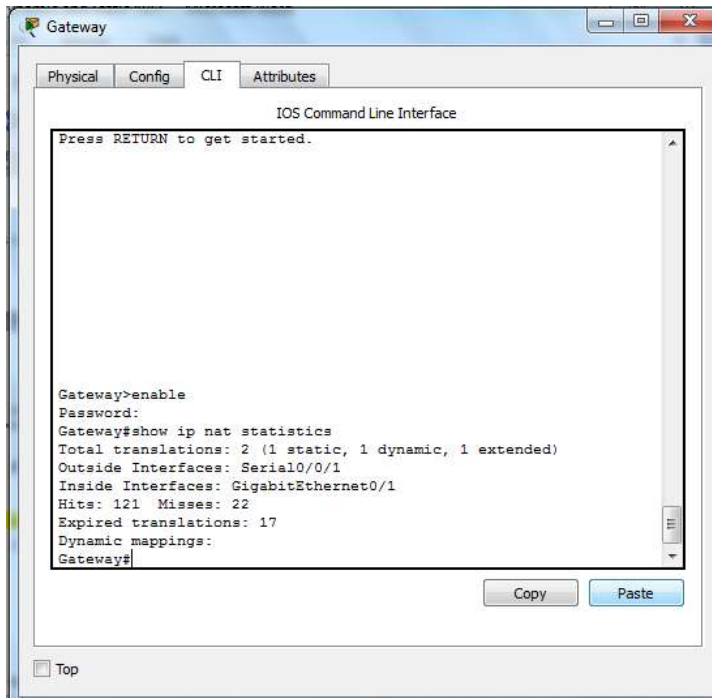
Total doors: 0

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.



The screenshot shows a window titled "Gateway" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and results:

```
Gateway>enable
Password:
Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 121 Misses: 22
Expired translations: 17
Dynamic mappings:
Gateway#
```

### Part 17: 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.

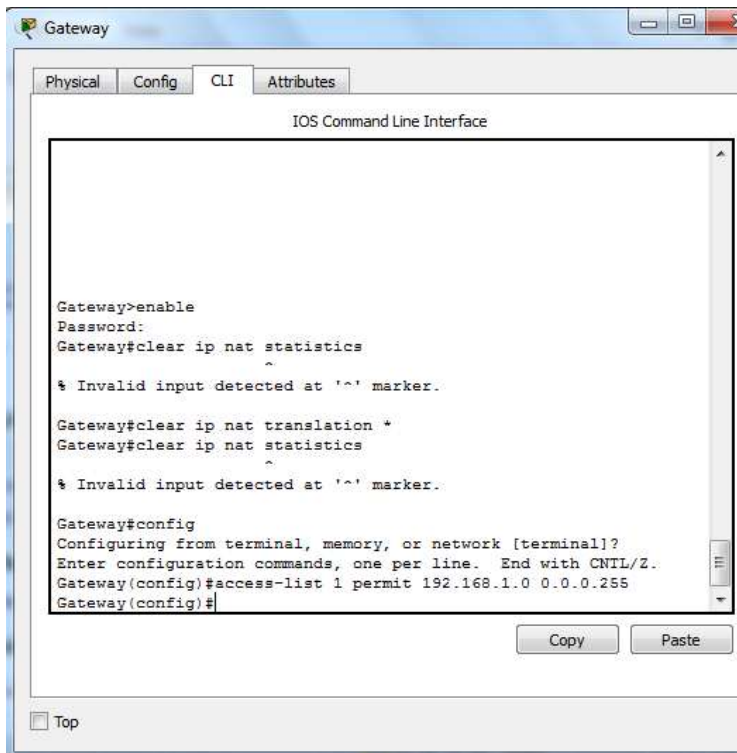
```
Gateway# clear ip nat translation *
```

```
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.

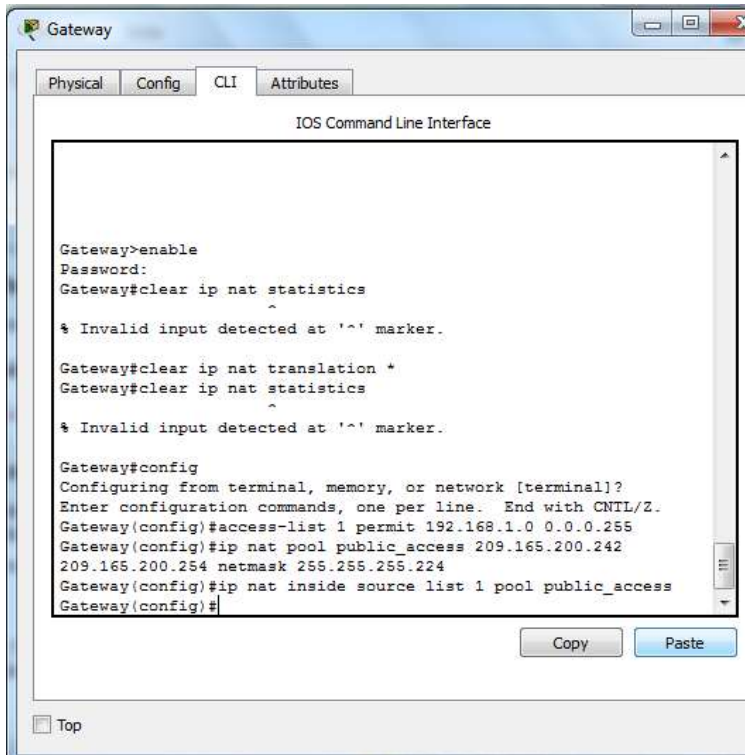
**Step 4: definir el conjunto de direcciones IP públicas utilizables.**

```
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.**

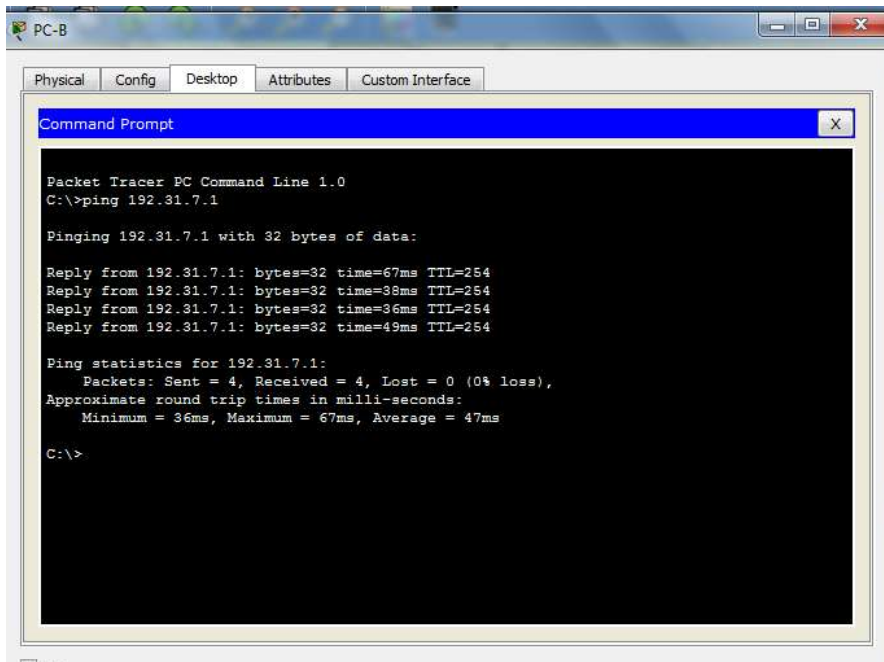
**Nota:** recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

```
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

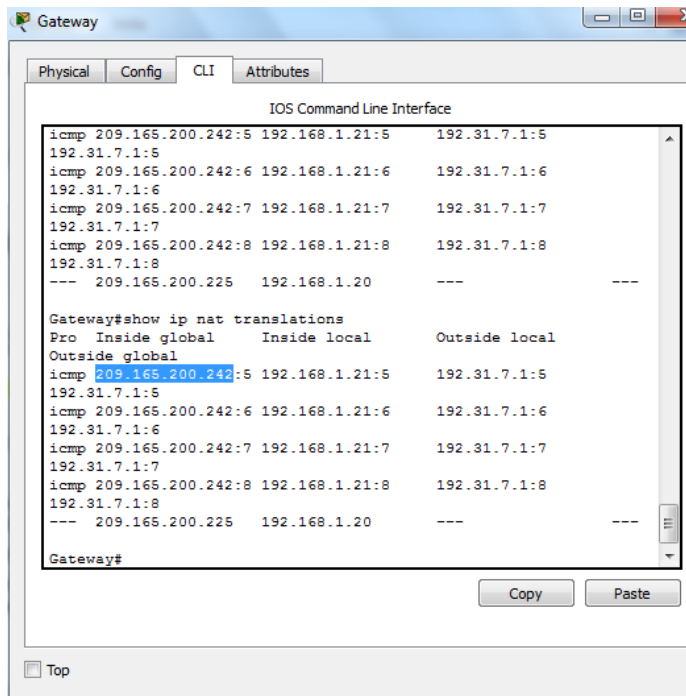
--- 209.165.200.242 192.168.1.21 --- ---

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

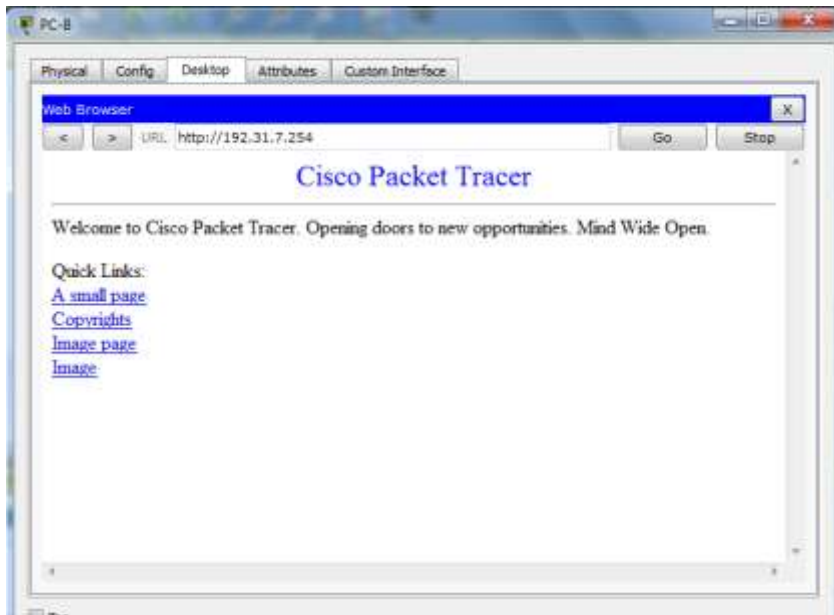
192.168.1.21 = 209.165.200.242 \_\_\_\_\_

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

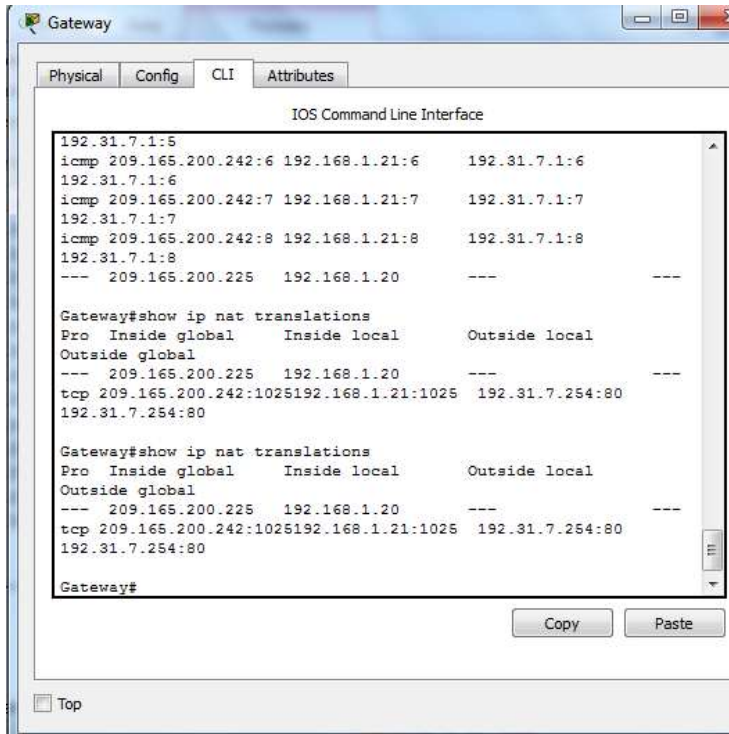


- b. En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.



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? **tcp**

¿Qué números de puerto se usaron?

Interno: **1025**

Externo: **80**

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

- 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
```

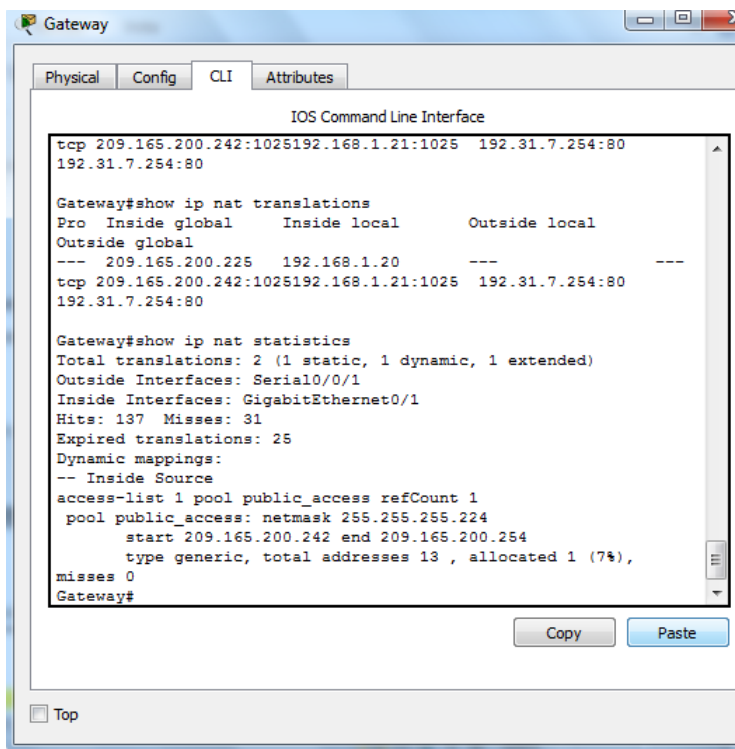
Total doors: 0

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.



The screenshot shows a Gateway CLI window with the following content:

```
IOS Command Line Interface

tcp 209.165.200.242:1025192.168.1.21:1025 192.31.7.254:80
192.31.7.254:80

Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local
Outside global
--- 209.165.200.225    192.168.1.20      ---
tcp 209.165.200.242:1025192.168.1.21:1025 192.31.7.254:80
192.31.7.254:80

Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 137 Misses: 31
Expired translations: 25
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13 , allocated 1 (7%),
misses 0
Gateway#
```

### 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.
- 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

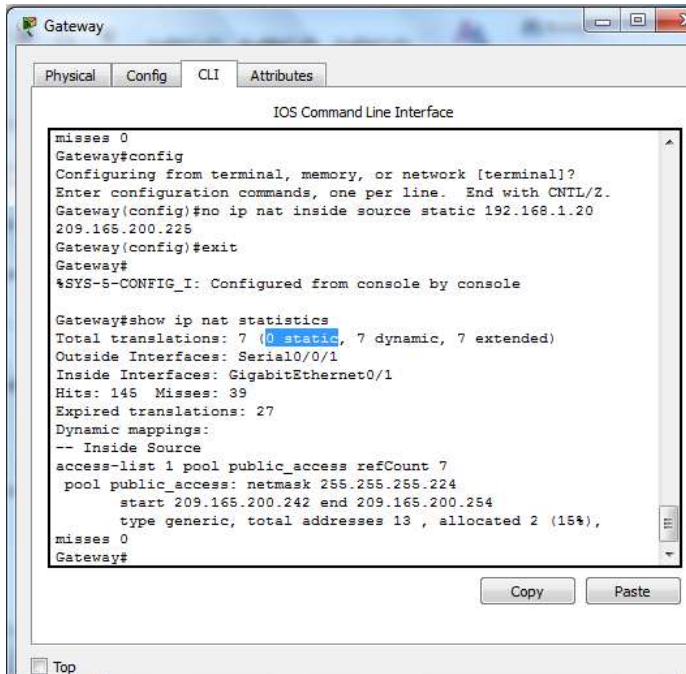
type generic, total addresses 13, allocated 2 (15%), misses 0

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?

para ocultar las ip internas usando esto como seguridad

2. ¿Cuáles son las limitaciones de NAT?

Necesita la información ip y el numero de puerto en la cabecera de ip y tcp para la traslación aumentando la latencia

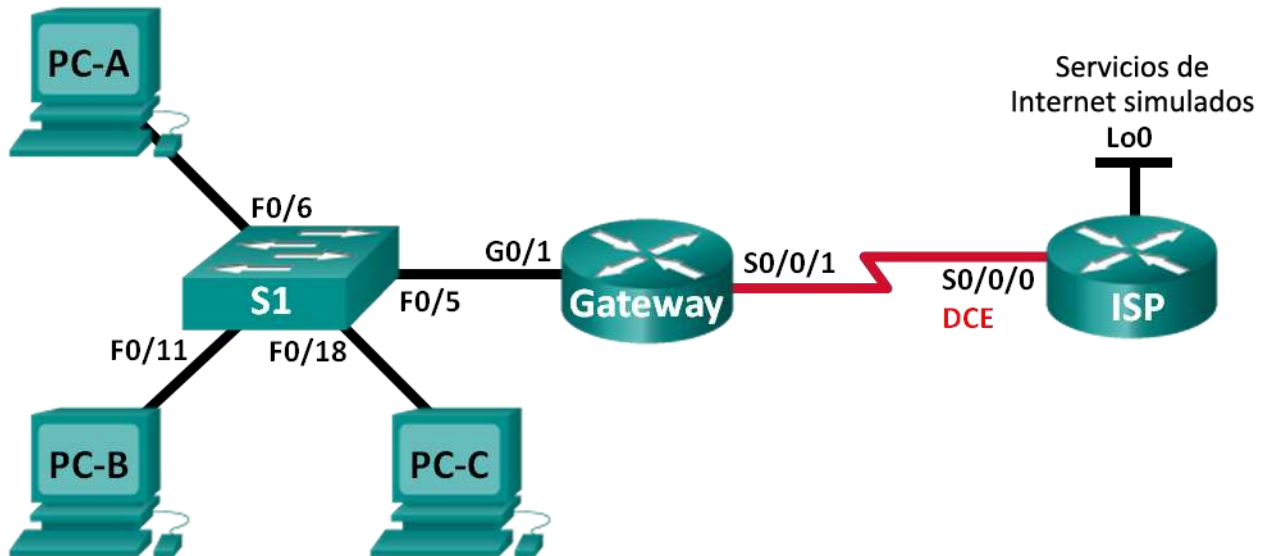
## Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

**Nota:** para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

### 11.2.3.7 Lab - Configuring NAT Pool Overload and PAT

#### Topología



#### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

#### Objetivos

**Parte 1: armar la red y verificar la conectividad**

**Parte 2: configurar y verificar un conjunto de NAT con sobrecarga**

**Parte 3: configurar y verificar PAT**

## Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto.

En la parte 2, el ISP asignó una única dirección IP, 209.165.201.18, a su empresa para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Usará la traducción de la dirección del puerto (PAT) para convertir varias direcciones internas en la única dirección pública utilizable. Se probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

**Nota:** los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota:** asegúrese de que los routers y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

## Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

### **Part 18: 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.**

**Step 2: configurar los equipos host.**

**Step 3: inicializar y volver a cargar los routers y los switches.**

**Step 4: configurar los parámetros básicos para cada router.**

- Desactive la búsqueda del DNS.
- Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

**Step 5: configurar el routing estático.**

- Cree una ruta estática desde el router ISP hasta el router Gateway.  
**ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18**
- Cree una ruta predeterminada del router Gateway al router ISP.  
**Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17**

**Step 6: Verificar la conectividad de la red**

- Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.
- Verifique que las rutas estáticas estén bien configuradas en ambos routers.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-A	Gateway	ICMP		0.000	N	0	(e...)	(delete)
	Successful	PC-B	Gateway	ICMP		0.000	N	1	(e...)	(delete)
	Successful	PC-C	Gateway	ICMP		0.000	N	2	(e...)	(delete)

### Part 19: configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

#### Step 1: definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

#### Step 2: definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

#### Step 3: definir la NAT desde la lista de origen interna hasta el conjunto externo.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

#### Step 4: Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
```

```
Gateway(config-if)# ip nat inside
```

```
Gateway(config-if)# interface s0/0/1
```

```
Gateway(config-if)# ip nat outside
```

#### Step 5: verificar la configuración del conjunto de NAT con sobrecarga.

a. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-A	192.31.7.1	ICMP		0.000	N	0	(e...)	(delete)
	Successful	PC-C	192.31.7.1	ICMP		0.000	N	1	(e...)	(delete)
	Successful	PC-B	192.31.7.1	ICMP		0.000	N	2	(e...)	(delete)

b. Muestre las estadísticas de NAT en el router Gateway.



```

Gateway
Physical Config CLI Attributes
IOS Command Line Interface
Gateway#show ip nat st
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 14 Misses: 14
Expired translations: 14
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6 , allocated 0 (0%), misses 0
Gateway#

```

c. Muestre las NAT en el router Gateway.

```

Gateway
Physical Config CLI Attributes
IOS Command Line Interface
Gateway#show ip nat translations
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:1024 192.168.1.21:6    192.31.7.1:6      192.31.7.1:1024
icmp 209.165.200.225:32 192.168.1.20:32  192.31.7.1:32     192.31.7.1:32
icmp 209.165.200.225:6  192.168.1.22:6   192.31.7.1:6     192.31.7.1:6

```

**Nota:** es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? **3**

¿Cuántas direcciones IP globales internas se indican? **1**

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? **3**

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

**El ping fallaría debido a que el router conoce la ubicación de la dirección global interna en la tabla de routing, pero la dirección local interna no se anuncia.**

## Part 20: 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.**

**Step 2: verificar la configuración para NAT.**

- Verifique que se hayan borrado las estadísticas.
- Verifique que las interfaces externa e interna estén configuradas para NAT.
- Verifique que la ACL aún esté configurada para NAT.

¿Qué comando usó para confirmar los resultados de los pasos a al c?

**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.**

- Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.
- Muestre las estadísticas de NAT en el router Gateway.
- Muestre las traducciones NAT en el Gateway.

The screenshot shows a window titled "Gateway" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and results:

```
Gateway#show ip nat statistics
Total translations: 3 (0 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 20 Misses: 20
Expired translations: 17
Dynamic mappings:
Gateway#show ip nat tr
Gateway#show ip nat translations |
% Invalid input detected at '^' marker.

Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.201.18:1024192.168.1.22:2      192.31.7.1:2      192.31.7.1:1024
icmp 209.165.201.18:1025192.168.1.21:2      192.31.7.1:2      192.31.7.1:1025
icmp 209.165.201.18:2 192.168.1.20:2    192.31.7.1:2      192.31.7.1:2
```

## Reflexión

¿Qué ventajas tiene la PAT?

PAT minimiza la cantidad de direcciones públicas necesarias para proporcionar acceso a Internet y que los servicios de PAT, como los de NAT, sirven para “ocultar” las direcciones privadas de las redes externas.

## CONCLUSIONES

Retomando como punto de partida cada una de las unidades del presente diplomado se da por sentado la importancia de la corporación Cisco en el mundo de las comunicaciones, en materia de aporte tecnológico, configuraciones topológicas, grados de seguridad, convergencias, niveles de escalamiento, soporte técnico, desarrollo de software en cada uno de sus avances tecnológicos, aportes lógicos que permiten cada vez la confiabilidad en el mundo de las comunicaciones, hoy por hoy la información y la privacidad cumple un papel preponderante en cada uno de los usuarios que confían de manera plena en los equipos que hacen parte de las estructuras en materia de red física y lógica.

En la presente unidad cada uno de los integrantes del pequeño grupo colaborativo nos dimos a la tarea de entender los puntos como planteamiento de desarrollo de todo en componente, aprendimos las distinciones de los protocolos IPv4 y IPv6, las restricciones y configuraciones de los switch y router tanto en la capa dos como en la tres, se redefine en la unidad la importancia de la optimización de los costos en la puesta en marcha de la construcción de una red,

Establecimos las razones correspondientes a la configuración del direccionamiento IP estático mediante protocolo IPv4, su aplicabilidad y alcances.

Desarrollamos la configuración de OSPFv2 básico de áreas sueltas, específicamente diseñada para el protocolo IPv4, cuya finalidad es detectar las posibles fallas del enlace, cambios en la topología, este punto creemos que es fundamental en materia de gestión de la red en IPv4

Los participantes del grupo establecieron en una análisis de campo la NAT con sus respectivas sobrecarga tanto dinámica como nativa, configuraciones de la red y PAT, Configuración de OSPFv2 y OSPFv3 con sus áreas resueltas, y de igual manera la configuración de una ACL en VTY

Se ejecutaron las sentencias (comandos) ACL, que consiste en la decisión que emite el router en el momento de enviar o recibir paquetes, mediante el IOS realiza una verificación si cumple o no el paquete de manera satisfactoria el requerimiento, cada uno de los integrantes está en la capacidad de resolver novedades en dicha configuración

Se aclararon inquietudes mediante la ejecución y programación de la ACL estándar su importancia en el servicio para el bloqueo específico de una red o un Host, en el análisis se entenderá el autenticación de todo el tráfico

El grupo enfatizó en el desarrollo y programación de configuración en una ACL en VTY Líneas, con el fin de establecer la necesidad de manera remota el acceso a una Telnet específica, con el fin de denegar peticiones a usuarios o intrusos que no tengan el acceso o perfil.

Podemos definir con la seguridad que nos confiere el desarrollo de presente unidad, no solo la importancia en nuestros campos profesionales, también la capacidad de dar soluciones básicas en materia de desarrollo y configuraciones en las redes Cisco.

Mediante los laboratorios que desarrollamos se permitieron lograr que cada estudiante pudiera armar una red, de la misma manera verificar la conectividad, al igual que la configuración y verificación.

Se utilizó la herramienta de simulación Packet Tracer y se establecieron escenarios LAN/WAN que nos permitieron realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento, evaluando el comportamiento de enrutadores, mediante el uso de comandos de administración de tablas de enrutamiento, bajo el uso de protocolos de vector distancia y estado enlace.

Se utilizó comandos de configuración avanzada en Router y switch y se implementó RIP,

OSPF en enrutamiento estático; bajo un esquema de direccionamiento IP sin clase, por lo tanto el RIPv2 es un protocolo de routing vector distancia, usado para enrutar direcciones IPv4 en pequeñas redes que tienen un límite de salto de 15 y el protocolo routing RIPng se usó para enrutar direcciones IPv6 con límite de salto de 15 de esta manera se dio soluciones a las redes en conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN. Es importante tener en cuenta que si una ruta no puede superar los 15 saltos de lo contrario se considera inalcanzable.

Configuramos esquemas de conmutación soportadas en Switches, mediante el uso de Protocolos basados en STP y VLANs en escenarios corporativos y residenciales, se comprendió el modo de operación de las VLAN y las bondades de administrar dominios de broadcast independientes, en escenarios soportados a nivel de capa 2 al interior de una red jerárquica convergente.

Se identificó problemas propios de conmutación y enrutamiento, utilizando las estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces, soportado en modelos de arquitecturas de comunicación estratificadas por niveles, y se resolvieron problemas de configuración, conectividad y enrutamiento bajo el uso de herramientas y comandos de administración del IOS en contextos LAN y WAN.

El beneficio de usar agentes de retransmisión DHCP es que permite tener un único servidor DHCP en vez de varios Router que funcionen como servidores, permitiendo una mejor administración de la red

Un switch multicapa puede realizar las funciones usuales de un switch y a la vez puede funcionar como servidor DHCP, y como enrutador. Cuando realizan la función de servidor DHCP estos Switches asignan la información IP a los host dependiendo de la VLAN a la que pertenecen.

Resulta de gran importancia excluir las direcciones IP estáticas antes de configurar un pool DHCPv4 debido a que cabe la posibilidad de que estas direcciones excluidas se entreguen a un host, causando un funcionamiento indeseado en la red al crear listas de acceso en Ipv6 solo se puede hacer con nombre ya que no acepta números como en Ipv4.

En Ipv6 solo se puede trabajar un tipo de lista la cual es equivalente a la extendida de Ipv4.

Al crear listas de acceso se pueden restringir determinado tráfico hacia una interfaz determinada.

Se puede control tanto el tráfico de salida como el tráfico de entrada dentro de una red permitiendo o denegando funcionalidades en la red.

## **BIBLIOGRAFIA**

- Cisco NetAcademy – Capítulos 7 al 10 [[www.netacad.com](http://www.netacad.com)] – Consultado el 21 de mayo de 2017
- Protocolo DHCP – [<http://es.ccm.net/contents/261-el-protocolo-dhcp>] – Consultado el 17 de mayo de 2017
- Network
- ACLs – [[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_ACLs.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)] – Consultado el 20 de mayo de 2017
- Dynamic Routing Protocols [<http://www.ciscopress.com/articles/article.asp?p=24090>] – Consultado el 15 de mayo de 2017